МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур,
О.А. Кожухівська, В.В. Марченко

МАТЕМАТИЧНІ МЕТОДИ КРИПТОЛОГІЇ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ - 2021

УДК 004.056 (075.8)
М 34

Рекомендовано до друку Вченою радою Державного університету телекомунікацій, протокол № 5 від 01.11. 2021 р.

Р е ц е н з е н т и:

М – 34 Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021 – 244 с.

У навчальному посібнику розглянуті питання з таких розділів математики, як множини, групи, многочлени та їх корені, поля Галуа, теорія чисел, а також основи класичної криптографії та криптографічні алгоритми, приведений аналіз і приклади ЕЦП, розглянуті поняття використання квантової криптографії для шифрування і дешифрування, а також для використання в ЕЦП. У навчальному посібнику приведено 14 практичних робіт з елементами теоретичного матеріалу, прикладами виконання цих практичних робіт, також завдань для самостійного виконання студентами.

Зміст навчального посібника відповідає спеціальності 125 – Кібербезпека і може бути використаний студентами всіх кафедр Навчально-наукового інституту Захисту інформації Державного університету телекомунікацій, а також споріднених спеціальностей інших вищих навчальних закладів.

Ключові слова: Множини, первісні корені, шифрування і дешифрування, ЕЦП, квантова криптографія.

УДК 004.056 (075.8)

Н а в ч а л ь н е в и д а н н я

В авторській редакції

Зміст **Стор.**

ВСТУП

“По-справжньому безпечною можна вважати лише систему, що вимкнена, замурована в бетонний корпус, замкнена в приміщенні зі свинцовими стінами й охороняється збройною вартою, - але й у цьому випадку сумніви не залишають мене”.
Юджин Х. Спаффорд

Невід’ємна складова державної політики щодо охорони інформаційних ресурсів України, передбаченої законодавством, - підготовка фахівців у сфері захисту інформації та інформаційної безпеки. Пошук і дослідження математичних методів перетворення інформації становлять основу дисципліни “Прикладна криптологія” - фундаменту спеціальної підготовки студентів за напрямом "Інформаційна та кібернетична безпека".

Професіональне розуміння криптографічних алгоритмів, уміння оцінити їх сильні та слабкі сторони, розробка і використання новітніх методів криптографії неможливі без серйозної математичної бази, адже криптографія грунтується на результатах таких розділів, як теорія чисел, алгебра, теорія скінченних полів, складність обчислень, теорія інформації, теорія ймовірностей та ін. Тому конкретний математичний апарат у навчальному посібнику подано саме так, як його застосовує і тлумачить криптографія. У навчальному посібнику, проте, не слід шукати зв’язку між окремими розділами, бо ставилася ідея висвітлити взаємозв’язок математики, зокрема дискретної, та криптографії.

До навчального посібника ввійшли розділи про множини і алгебраїчні структури, многочлени та їх корені, теорія чисел, основи теорії полів Галуа. Через обмежений обсяг навчального посібника сюди, на жаль, не потрапили теорія скінченних автоматів, теорія інформації, теорія ймовірностей і математична статистика. Друга частина містить основи класичної криптографії, принципи побудови сучасних криптосистем із закритим та відкритим ключами, методи контролю цілісності та автентичності інформації. Приведений короткий аналіз булевих функцій та перетворювань Уолша - Адамара і їх використання в криптографії. Розглянутий аналіз двоключових схем, їх використання для електронного цифрового підпису (ЕЦП), наведені їх слабкі сторони при використанні в ЕЦП, приведені поняття безключового ЕЦП.

Розкрито математичний зміст криптографічних інструментів – однобічних функцій з лазівкою, хеш-функцій, генераторів псевдовипадкових чисел. Розглянуто використання еліптичних кривих для ЕЦП. В третьому розділі приведено поняття використання квантової криптографії для шифрування і дешифрування, а також для використання в ЕЦП.

Необхідний рівень математичної освіти читача відповідає типовій підготовці студента, який прослухав курси математичного аналізу, аналітичної

геометрії та лінійної алгебри. Аби увага з криптографії не перемістилася на математику, у певних місцях автори навмисно поступилися суворістю доведень на користь змісту й практичної доцільності навчального матеріалу. Наприкінці навчального посібника вміщено список літератури для додаткового ознайомлення читачів з викладеного матеріалу.

Зацікавленому читачеві запропоновано велику кількість практичних вправ для закріплення матеріалу, розвитку математичного мислення та набуття конкретних умінь і навичок у криптографії. З цією ж метою у навчальному посібнику приведено 14 практичних робіт з елементами теоретичного матеріалу, прикладами виконання цих практичних робіт, а також завдань для самостійного виконання студентами.

Зміст навчального видання відповідає спеціальності 125 – Кібербезпека і може бути використаний студентами всіх кафедр Навчально-наукового інституту Захисту інформації Державного університету телекомунікацій, а також споріднених спеціальностей інших вищих навчальних закладів.

1 Алгебраїчні структури і многочлени над полем

Множини з алгебраїчними операціями. Півгрупи і моноїди

Під алгебраїчною системою або алгебраїчною структурою будемо розуміти деяку множину S з однією або декількома операціями на ній. В елементарній арифметиці використовуються дві операції – додавання і множення, важливою властивістю яких є асоціативність. Найбільш вивченими алгебраїчними системами, які мають одну асоціативну операцію, являються групи.

Групою <G, *> називається деяка множина *G* з бінарною операцією "*" на ній, для якої справедливі наступні умови:

- замкнутість – будь-якій парі $(a,b) \in G$ ставиться в однозначну відповідність третій елемент $c \in G$, можливо співпадаючий з одним із початкових елементів a або b (алгебраїчна система <**G**, *> з цією властивістю називається групоїдом);
- операція "*" асоціативна, тобто для $\forall\ a, b, c \in G$ $a*(b*c)=(a*b)*c$

(алгебраїчна система <**G**, *> із властивостями замкнутості і асоціативності – **пів група***);*

- у множині *G* існує одиничний елемент *e,* такий, що для $\forall\ a \in G$ $a*e=e*a=a$ (алгебраїчна система <***G,*** *>, яка задовольняє властивостям замкнутості, асоціативності і яка має одиничний елемент, що називається ***моноїдом****);*
- для $\forall\ a \in G$ існує обернений елемент $a^1 \in G$, такий, що $a*a^1=a^1*a=e$, якщо група ***G*** додатково задовольняє умові комутативності;
- для $\forall\ a, b \in G$ $a*b=b*a$, то вона називається ***комутативною*** *або* ***абелевою*** на честь видатного норвежського математика Н. Абеля.

В залежності від використовуваних операцій і позначень розрізняють адитивні і мультиплікативні групи, загальна характеристика яких представлена в табл. 1.1.

Мультиплікативна група *G* називається ***циклічною****, якщо в ній є* такий елемент, що кожний елемент $b \in G$ є степенем елемента *a,* тобто існує ціле число *k,* таке, що $b = a$. Елемент *a* називається створюючим елементом мультиплікативної групи *G*. Із цього визначення виходить, що будь-яка циклічна група комутативна.

Таблиця 1.1

Вид групи	**Вид операції**	**Результат операції**	**Одиничний елемент**	**Обернений елемент**
Адитивна	**Додавання**	**Сума *a+Ь***	**0**	***-a***
Мультиплікативна	**Множення**	**Добуток *ab***	**1**	a^{-1}

Виконання операцій в групах задовольняє наступним правилам (табл. 1.2).

Таблиця 1.2

Мультиплікативна група	**Адитивна група**
$a^{-n} = (a^{-1})^n$ $a^m a^n = a^{mn}$ $(a^n)^m = a^{nm}$	$-n(a) = n(-a)$ $ma + na = (m+n)a$ $m(na) = (mn)a$

Приклади адитивних груп:

- множина цілих чисел Z;
- множина раціональних чисел Q;
- множина дійсних чисел R;
- множина поліномів степеня не вище *n* з цілими коефіцієнтами.

Приклади мультиплікативних груп:

- множина ненульових раціональних чисел;
- множина коренів *n*-го степеня із одиниці.

Група називається ***кінцевою,*** якщо вона складається із кінцевого числа елементів. Число елементів кінцевої групи називається її ***порядком.*** Для позначення порядку групи використовується позначення **|*G*|** або ***#G***.

Кільця:

Кільцем <R, +, •> називається множина *R* з двома бінарними операціями + і •, такими, що:

- множина *R* являється адитивною абелевою групою;
- операція перемноження асоціативна, тобто для $\forall$ *a, b, c* $\in R$ $a(bc) = (ab)c$;
- виконуються закони дистрибутивності, тобто для $\forall$ *a, b, c* $\in R$ $a(b+c) = ab + ac$ $(b+c)a = ba + ca$.

Прикладами кілець являються:

- кільце цілих чисел **Z;**
- кільце цілих чисел за модулем *p* ***Z****/p* (кільце відрахувань за модулем *p,* в якому операції + і • являються операціями додавання і перемноження за модулем *p).*

Кільце називається ***кільцем з одиницею***, якщо воно має мультиплікативну одиницю, тобто, якщо існує такий елемент 1 $\in$ ***R,*** що $a1 = 1a = a$ для $\forall$ $a \in$ ***R***.

Кільце називається ***комутативним, якщо*** операція перемноження комутативна.

Кільце називається ***цілісним кільцем*** *або* областю цілісності, якщо воно являється комутативним кільцем з одиницею $e \neq 0$, в якому рівність *ab=0* тягне за собою *a* = 0 або *b*=0.

Підмножина ***S*** кільця ***R*** називається ***підкільцем*** цього кільця, якщо воно замкнуте відносно операцій додавання і перемноження і утворює кільце відносно цих операцій.

Нехай ***R***— довільне кільце. Якщо існує натуральне число $p \neq \{1,2,3,...\}$, таке, що для кожного $r \neq$ ***R*** виконується рівність *pr = 0,* то найменше із таких чисел

називається ***характеристикою*** **кільця *R***. Якщо таких натуральних чисел не існує, то характеристика кільця дорівнює 0. ***Порядок*** кільця *R* визначається порядком адитивної групи кільця і, отже, дорівнює числу елементів кільця.

Поля:

Полем <F, +, •> називається множина ***F*** з двомя бінарними операціями + і •, такими, що:

- ***F*** являється адитивною абелевою групою з одиничним елементом 0:
- елементи ***F***, які відрізняються від 0, утворюють мультиплікативну абелеву групу, одиничним елементом якої являється 1;
- операції додавання і перемноження зв'язані законом дистрибутивності;
- для операцій додавання і перемноження існують обернені операції: віднімання і ділення (крім ділення на ноль).

Приклади полів:

- множина раціональних чисел ***Q*;**
- множина дійсних чисел ***R***;
- множина комплексних чисел ***C***.

Якщо поле представляє собою кінцеву множину, яка складається із q елементів, то таке поле називається ***кінцевим полем*** **або** ***полем Галуа*** і позначається $GF(q)$ або F_k . Кінцеві поля існують тільки тоді, коли число елементів q являється простим числом або степенем простого числа: $q=p^m$, де p - просте число, m - натуральне число. При цьому p називається ***характеристикою*** кінцевого поля $GF(q)$, q ***-порядком*** поля, а m- ***степенем*** поля $GF(q)$ над його підполем $GF(p)$. При $m = 1$ поле називається ***простим,*** в протилежному випадку поле називається ***розширеним.*** Якщо ж p – складне число, то алгебраїчна система $<F, +, * >$, де додавання і перемноження модулярні операції, полем не являється, ця система утворює кільце, де ділення навіть на ненульовий елемент можливо не завжди.

В будь-якому полі множина усіх елементів утворює при операції додавання адитивну абелеву групу, аналогічно множина усіх ненульових елементів поля утворює при операції перемноження мультиплікативну циклічну групу.

Для кожного допустимого значення q існує рівно одне поле, тобто усі кінцеві поля порядку q ізоморфні. Наприклад, якщо $q = p$ - просте число, то елементами поля являються числа 0, 1, ...,$p-1$, а додавання і перемноження являються звичайними додаваннями і перемноженнями за модулем p, тобто $GF(p)=Z/p$. Отже, кільце лишків за модулем простого числа є просте поле. Якщо t являється степенем простого числа, то елементами такого поля являються усі поліноми степеня m і менше, коефіцієнти яких лежать в простому полі $GF(p)$. Правила перемноження і додавання таких поліномів отримуються із звичайного перемноження і додавання поліномів і наступного приведення результату за модулем деякого спеціального полінома $g(x)$ степеня m. Цей поліном володіє тією властивістю, що його не можна розкласти на множники, використовуючи тільки поліноми з коефіцієнтами із $GF(p)$. Такі поліноми називаються ***незвідними*** і за своєю сутністю вони аналогічні простим числам.

Наприклад, поліном $g(x)=1+x+x^3$ являється незвідним над *GF(2)* і може використовуватися для побудови розширеного поля *GF*(8). Необхідно відмітити, що зведення полінома за модулем *g(x)* еквівалентно діленню на *g(x)* і взяттю залишку. З цим зв'язано поняття порівняння

$$a(x)\equiv b(x) \bmod g(x),$$

що інтерпретується як: *a(x)* порівнянно з *b(x)* за модулем *g(x),* і означає, що обидва поліноми мають однакові лишки при діленні на *g(x),* або що $a(x)$-$b(x)$ ділиться на поліном $g(x)$. Отже, поняття порівнянності поліномів аналогічно поняттю порівнянності цілих чисел.

Мультиплікативна група ненульових елементів довільного кінцевого поля *GF(q)* являється циклічною. Утворюючий елемент α циклічної групи називається ***примітивним елементом*** цього поля *GF(q).* Усі елементи кінцевого поля можна представити наступним чином:

$$GF(q)=\left\{0,\alpha,\alpha^2,....,\alpha^{q-2},\alpha^{q-1}=\alpha^0=1\right\},$$

де α - примітивний елемент поля.

Інший метод виконання множення ненульових елементів *GF(q)* полягає в тому, щоб знайти їх логарифми, додати їх за модулем *q-1* і перейти до антилогарифму. Існування логарифмів в кінцевому полі означає, що є представлення елементів кінцевого поля, яке зручне для виконання множення, і інше представлення, яке зручне для виконання додавання. Найбільш зручний метод полягає, при виконанні додавання, в представленні елемента поля у вигляді вектора довжиною *m,* компонентами якого являються коефіцієнти відповідного полінома, і при виконанні множення, в представленні елемента поля у вигляді степеня примітивного елемента. В табл. 1.3 показаний взаємозв'язок таких представлень елементів поля *GF*(8).

Таблиця 1.3

0	000
1	100
α^1	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

Використовуючи такого рода таблиці, легко виконувати арифметичні операції. Наприклад, нехай необхідно обчислити значення $f(\alpha)=(\alpha^2+\alpha^5)\alpha+(1+\alpha^3)\alpha$. За допомогою табл. 1.3 отримуємо

$\alpha^2+\alpha^5=(001)+(111)=(110)=\alpha^3$,

$1+\alpha^3=(100)+(110)=(010)=\alpha$,

отже, $f(\alpha)=\alpha^3\alpha+\alpha\alpha=\alpha^4+\alpha^2=(011)+(001)=(010)=\alpha$.

Іншим підходом виконання операцій в кінцевих полях являється використання ***логарифма Зеча*** *z(n)*, що задається рівнянням:

$$\alpha^{z(n)} = 1 + \alpha^{n}.$$

Використовуючи цей метод, можна виконувати арифметичні операції в кінцевому полі, працюючи тільки з логарифмами і не звертаючись до антилогарифмів. В цьому випадку сума елементів α^m і α^n може бути обчислена наступним чином:

$$\alpha^m + \alpha^n = \alpha^m(1 + \alpha^{n-m}) = \alpha^{m+z(n-m)}.$$

Для поля *GF*(8) логарифми Зеча приведені в табл. 1.4.

Таблиця 1.4

n	-∞	0	1	2	3	4	5	6
Z(n)	0	-∞	3	6	1	5	4	2

1.2 Многочлени над полем

Многочлен над полем F - це функція виду $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, де $a_i \in F, i = 0,1\ldots,n$, $a_0 \neq 0$. Ціле число $n \geq 0$ називається степенем многочлена і позначається $\deg f$.

Аналогічно визначається **многочлен над комутативним кільцем**. Множина $R[x]$ усіх многочленів від однієї змінної над комутативним кільцем R також є кільцем.

Якщо $a_0 = 1$, по многочлен називається зведеним (нормованим, унітарним). Многочлен $g(x)$ називається дільником многочлена $f(x)$, якщо існує многочлен $h(x)$, такий, що $f(x) = g(x)h(x)$, $f, g, h \in R[x]$.

Спільним дільником двох многочленів називається многочлен, що ділить обидва зазначені многочлени.

Тому дільники многочленів визначаються з точністю до константи.

Найбільшим спільним дільником $d = (f, g)$ двох многочленів $f, g \in F[x]$ називається многочлен $d \in F[x]$, такий, що будь-який загальний дільник h многочленів f і g ділить d.

Звичайно, в якості (f, g) вибирається нормований многочлен.

<u>Визначення.</u> Многочлен ненульового степеня називається незвідним, якщо він ділиться тільки на константи і сам на себе.

НСД і НСК чисел і многочленів над полем Q.

Числа 1,2,3,…називаються натуральними. Число 0, а також числа виду $\pm a$, де a натуральне число, називаються цілими числами. Відношення двох цілих

чисел називається раціональним дробом і є записом результату ділення одного числа на інше. Ділення на нуль не визначено. Множина раціональних дробів є полем. Позначення - Q .

Простим числом називається натуральне число, у якого є точно два нерівних натуральних дільники.

Основна теорема арифметики: кожне натуральне число єдиним, з точністю до порядку співмножників, чином представляється у виді добутку степенів простих чисел.

Найбільшим спільним дільником двох цілих чисел a і b називається найбільше ціле число, що ділить як a так і b. Позначення: (a,b) або НСД(a,b) . Якщо НСД$(a,b)=1$, то числа a і b називаються взаємно простими.

Найменшим спільним кратним натуральних чисел a і b називається найменше натуральне число НСК(a,b), що ділиться як на a, так і на b.

Очевидно, НСК$(a,b)=\frac{ab}{(a,b)}$.

Алгоритм Евкліда для визначення НСД двох натуральних чисел $a,b\ (a>b)$. Основну роль грає операція ділення чисел із залишком, тобто представлення виду $a=kb+r$, $b>r\geq 0$.

Запишемо числа a,b. Знайдемо залишок r_1 від ділення a на b, запишемо його слідом за a,b: a,b,r_1. В отриманому списку розглянемо останні два числа.

Знайдемо залишок r_2 від ділення першого з них на друге: $b=k_1r_1+r_2$, допишемо r_2 в список: a,b,r_1,r_2. Діємо далі аналогічно, поки вперше (на k-ому кроці) не виникне ситуація, коли $r_k=0$. Тоді $(a,b)=r_{k-1}$.

Схема алгоритму Евкліда для многочленів $a(x)$ і $b(x)$ над полем F.

Операція ділення із залишком відповідає запису виду $a(x)=k(x)b(x)+r(x)$, $\deg b>\deg r\geq 0$. Якщо вперше на k-ому кроці виявляється, що $r_k=0$, процес обчислення залишків від ділення зупиняється і $(a(x),b(x))=r_{k-1}(x)$.

Корені поліномів і формули Вієта

Поліном $f(x)\in F[x]$ може розглядатися не тільки як функція, але і як запис деякої послідовності дій над змінною x.

Не виключено, що зазначена послідовність дій може бути виконана з об'єктом, що не належить полю F, але при цьому операції в полі необхідно інтерпретувати як більш складні.

Виявляється, що відповідним чином узгоджуються операції у полі і його підполі. Обчислення значення полінома можна проводити не тільки для змінних $x\in F$, але й для об'єктів, що належать розширенню цього поля.

Означення. **Коренем многочлена** $f(x)\in F[x]$ називається елемент X, що належить якому-небудь розширенню $\tilde{F}\supseteq F$, такий, що $f(X)=0$.

Теорема. Існує розширення $\tilde{F} \supseteq F$ поля F, у якому заданий нормований многочлен $f(x) \in F[x]$ представляється як добуток з $n = \deg f$ співмножників: $f(x) = \prod_{i=1}^{n} (x - X_i)$, де X_i - корені многочлена $f(x)$.

Наслідок. Незвідний над полем F многочлен не має коренів у цьому полі.

Із заданим коренем X_k можуть співпадати кілька інших коренів. Кількість усіх коренів, рівних X_k, **називається кратністю** кореня X_k.

Означення. **Кратністю кореня** C многочлена $f(x)$ називається число h, таке, що $f(x)$ ділиться на $(x-c)^h$, але не ділиться на $(x-c)^{h+1}$.

Теорема (Ф. Вієт). Нехай $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ - нормований многочлен над полем F, а $x_0, \ldots, x_{n-1}$ - його корені.

Тоді мають місце наступні співвідношення (формули Вієта):

$$a_1 = -(x_1 + x_2 + \ldots + x)_n,$$
$$a_2 = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n,$$
$$a_3 = -(x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n),$$
$$\ldots\ldots\ldots\ldots$$
$$a_n = (-1)^n x_1x_2 \ldots x_n.$$

1.3 Модульна арифметика

Лишки за модулем m.

Кожне ціле число a можна розділити з остачею на натуральне число m: $a = km + r$, $0 \le r < m$. .

Остача від ділення числа на m називається лишком (у даному випадку - лишком числа a за модулем m). Операція, що співставляє числу a його лишок за модулем m, називається зведенням a за модулем m.

Означення. Два цілих числа a і b конгруентні за модулем m, якщо їхня різниця ділиться на m.

Конгруенції за модулем.

Відношення конгруентності записується у виді: $a \equiv b \pmod m$, $a \equiv b$ (m). Замість знака конгруенції часто використовується знак рівності. Числа, що мають однакові остачі від ділення на m, конгруентні за модулем m.

Стандартні значення лишків за модулем m належать множині 0,1, …,m-1 (так звана система найменших додатних лишків).

Лишок суми за модулем m дорівнює сумі лишків, зведеної, якщо необхідно, ще раз за модулем m. Аналогічною властивістю володіє лишок добутку.

Відношення конгруентності дозволяє розбити множину цілих чисел на класи. Елементи одного класу мають однакові лишки за модулем m. Очевидно,

класи не перерізаються. Кожному класу відповідає один найменший додатний лишок і навпаки.

Лишок суми або добутку за модулем m елементів $a \in A$ і $b \in B$ не залежить від вибору цих елементів, а залежить лише від вибору класів *A* і *B*.

Можна побудувати кільце, елементами якого є класи лишків, а операції виконуються через дії над відповідними найменшими додатними лишками.

Наприклад, якщо $c \equiv a + b (\mathrm{mod}\, m)$, то клас, що містить c, є множиною виду $C = \{c, c+m, c+2m, \ldots\}$. Оскільки множина Z цілих чисел є кільцем, то наша відповідність між класами і лишками $c = \varphi(C)$ є гомоморфізмом кілець. Образ цього гомоморфізму (кільце класів лишків за модулем m) називається фактором-кільцем кільця цілих чисел за модулем m і звичайно позначається Z/mZ. Зауважимо, що нулем у кільці лишків Z/mZ є клас $0 = \{0, m, 2m, \ldots\}$.

При зашифруванні інформації використовуються взаємно однозначні перетворення даних. Для перебування зворотних елементів у кільці Z/mZ можна використовувати розширений алгоритм Евкліда.

1.4 Розширений алгоритм Евкліда

Цей алгоритм призначений для пошуку цілочисельного розв'язку x, y, d рівняння $xa + yb = d$, $a > b$, $d = (a,b)$, де a і b також цілі числа.

Розглянемо схему розширеного алгоритму Евкліда на прикладі чисел 15 і 25. Ми будемо знаходити залишки і (неповні) частки від розподілу двох чисел, тобто користуватися рівностями виду $A = kB + r$, де всі числа цілі і $0 \le r < B$.

Оскільки повинна виконуватися нерівність $a > b$, то змінимо позначення: $r_0 = 25$ $r_1 = 15$.

Випишемо послідовність рядків:

$r_0 = 25$ $x_0 = 1$ $y_0 = 0$

$r_1 = 15$ $x_1 = 0$ $y_1 = 1$

$(d_2 = 1, r_2 = 10)$

Пояснення. Ділимо r_0 на r_1 з остачею. Одержуємо: $r_0 = d_2 r_1 + r_2$, тобто $25 = 1*15 + 10$, звідси $d_2 = 1$, $r_2 = 10$. Перевіряємо: $r_2 = 0$? Ні – працюємо далі. Обчислюємо: x_2, y_2 : $x_2 = x_0 - x_1 d_2 = 1$, $y_2 = y_0 - y_1 d_2 = -1$. Формуємо черговий рядок: r_2, x_2, y_2.

Вихідними даними для кроку 2 будуть рядки $r_1 x_1 y_1$ (з попереднього кроку) і r_2 x_2 y_2. З цими рядками діємо аналогічно.

Якщо чергова остача від ділення дорівнює 0, виписуємо розв'язок з даних попереднього кроку (див. нижче).

$r_2 = 10$ $x_2 = 1$ $y_2 = -1$ ($d_3 = 1$, $r_3 = 5$)

$r_3 = 5$ $x_3 = -1$ $y_3 = 2$ $(d_4 = 2, r_4 = 0)$.

При формуванні чергового рядка остачу $r^4 = 0$ виписуємо рішення з даних попереднього кроку:

НСД (25,15) = $r^3 = 5$, $x = x^3 = -1$, $y = y^3 = 2$, $xr^0 + yr_1 = -25 + 30 = 5$ = НСД (25,15).

1.5 Існування оберненого елемента в кільці лишків

Алгоритм Евкліда показує, що для взаємно простих чисел a і m завжди існує число b таке, що $ab \equiv 1 \bmod m$.

Таке число називається оберненим до a за модулем m і позначається a^{-1}.

Дійсно, якщо $d = (a, m) = 1$, то відносно x і y розв'язуване рівняння $xa + ym = d = 1$. Приводячи за модулем m обидві частини зазначеної рівності, одержимо конгруенцію $xa \equiv 1 (\bmod m)$, тобто $x \equiv a^{-1} (\bmod m)$.

Якщо модуль є простим числом $m = p$, усі ненульові лишки за модулем p взаємно прості з модулем. Отже, кільце $Z / pZ = GF(p)$.

1.6 Розширення простого поля

За аналогією з кільцем лишків за модулем $m = p$, можна побудувати кільце лишків поліномів за модулем нормованого незвідного полінома $f(x)$ над полем Z/pZ.

Для цього досить розглянути множину залишків від ділення всіх поліномів із коефіцієнтами з Z/pZ та помітити, що розширений алгоритм Евкліда може бути переформульований для розв'язування рівняння аналогічного $xa + ym = d = 1$, а саме: $u(x)a(x) + v(x)m(x) = d(x) = (a(x), m(x))$.

Якщо покласти $m(x) = f(x)$, то, при $\deg a < \deg f$, $(a(x), f(x)) = d(x) = 1$ і співвідношенні $u(x)a(x) + v(x)f(x) = 1$, після зведення за модулем $f(x)$ дає $u(x) \equiv a(x)^{-1} \bmod f(x)$. Тому всі ненульові елементи нашого кільця оборотні, тобто воно є полем.

Оскільки коефіцієнти поліномів обчислюються за правилами арифметики $Z/pZ = GF(p)$, то число p є характеристикою нашого поля F. Очевидно, що кількість елементів q поля F дорівнює кількості поліномів степеня, меншого $\deg f$.

Для визначення q зауважимо, що набору коефіцієнтів кожного полінома степеня меншого $\deg f$, відповідає вектор, кількість координат якого дорівнює $\deg f$. Кожна координата може приймати лише значення $0,1,\ldots, p-1$. Отже, $q = p^{\deg f}$. Таким чином, $F = GF(p^{\deg f})$.

Довільний вектор можна розглядати як набір коефіцієнтів деякого полінома**.** При цьому сумі поліномів буде відповідати сума зазначених векторів.

Результатом добутку векторів є вектор коефіцієнтів залишку від ділення добутку поліномів на $f(x)$.

У підсумку, елементи поля $F = GF(p^t)$ можна розглядати як t - вимірні вектори з координатами з підполя $GF(p)$.

Число t називається степенем розширення $GF(p)$.

Елемент a поля $GF(p)$ представляється в поле $GF(p^t)$ t - вимірним вектором (розширеним числом) виду $(0,\ldots,0,a)$.

1.7 Вектори і лінійні форми. Базис лінійного простору

Лінійним векторним простором над полем F називається множина L, елементи якої називаються векторами і для якого виконуються наступні аксіоми.

1. На множині L задане додавання - бінарна комутативна операція, тобто $\forall \bar{x}, \bar{y} \in L \ \exists \ \bar{z} \in L : \bar{z} = \bar{x} + \bar{y} = \bar{y} + \bar{x}.$ Результат додавання називається сумою.
2. Додавання векторів асоціативно.
3. На множині L задане множення векторів на елементи поля F, тобто відображення виду $(a, X) \to b, \ a, b \in F, x \in L.$ При цьому $(ab)\bar{x} = a(b\bar{x})$ і $(a+b)\bar{x} = (a\bar{x}) + (b\bar{x}).$
4. Існування нульового вектора: $\bar{x} + \bar{0} = \bar{x}$.
5. Існування протилежного вектора: $\bar{x} + (-\bar{x}) = \bar{0}$.
6. $1 \cdot \bar{x} = \bar{x}$.

Лінійною комбінацією векторів $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k$ з коефіцієнтами $c_1, c_2, \ldots, c_k$ називається вектор $\bar{h} = c_1\bar{x}_1 + c_2\bar{x}_2 + \ldots + c_k\bar{x}_k$.

Система векторів $\bar{x}_1, \bar{x}_2 \ldots \bar{x}_k$ називається **лінійно незалежною**, якщо рівність $\bar{h} = \bar{0}$ можлива в тому і тільки тому випадку, коли $c_1 = c_2 = \ldots = c_k = 0$.

Лінійно незалежна підсистема системи векторів називається **максимальною**, якщо при введенні до неї будь-якого вектора із системи система стає лінійно залежною. Кількість векторів у максимальній лінійно незалежній підсистемі називається **рангом** відповідної системи векторів.

Лінійний векторний простір називається скінченно вимірним, якщо в ньому існує максимальна лінійно незалежна система, що складається зі скінченного числа векторів.

Розглянемо множину L, елементами якої є упорядковані послідовності n елементів поля F. Відносно покомпонентної суми і покомпонентного множення на елемент поля F побудована множина L є лінійним векторним простором над F і позначається F^n. Очевидно, система $B = \{\bar{e}_i = (0,\cdots,0,1,0,\cdots,0)\}$, де $i = 1,2,\ldots,n$, а одиниця знаходиться на i-ому місці, є максимальною лінійно незалежною системою. Можна показати, що всі належні F^n максимальні лінійно незалежні системи складаються з однакового числа елементів.

Базисом лінійного векторного простору називається система векторів така, що будь-який вектор простору однозначно представляється у виді лінійної комбінації векторів базису.

Очевидно, базис є максимальною лінійно незалежною підсистемою всього простору.

Будь-який скінченно вимірний лінійний простір L над полем F є **ізоморфним** F^n при деякому n.

Кількість n векторів у базисі називається **розмірністю лінійного векторного простору** L. Розмірність простору L позначається $\dim L$. Якщо $\dim L = n$, то лінійний векторний простір називається n- вимірним.

1.8 Лінійні перетворення і матриці над полем

Відображення $f: F^n \to F^m$ називається **лінійним оператором** з F^n у F^m, якщо виконуються наступні умови.

$\forall \bar{x}, \bar{y} \in F^n$, $\forall k \in F$, $f(\bar{x}+\bar{y}) = f(\bar{x}) + f(\bar{y})$, $f(k\bar{x}) = kf(\bar{x})$.

Матрицею A розміру $m \times n$ над полем F називається прямокутна таблиця, що складається з m рядків і n стовпців і містить $m \times n$ елементів з F.

Елементи a_{ij} матриці індексуються номером рядка i та стовпця j, на перетину яких він знаходиться.

Транспонуванням матриці A розміру $m \times n$ називається операція побудови матриці A^T (інше позначення - A') розміру $n \times m$, де $a'_{ij} = a_{ji}$.

Сумою матриць $A=(a_{ij})$ і $B=(b_{ij})$ розміру $m \times n$ називається матриця $C=(c_{ij})$, де $c_{ij} = a_{ij} + b_{ij}$. Множення матриці на константу виконується покомпонентно.

Лінійною формою над кільцем R з вектором змінних $\bar{x} = (x_1, x_2 \ldots, x_k)$ і коефіцієнтами $\bar{c} = (c_1, c_2, \ldots, c_k)$ називається функція $l(\bar{a}, \bar{x}) = c_1x_1 + c_2x_2 + \ldots + c_kx_k$. Для лінійної форми часто використовується позначення $\langle \bar{c}, \bar{x} \rangle$. Зауважимо, що можливий випадок $\langle \bar{x}, \bar{x} \rangle = 0$, при $\bar{x} \neq \bar{0}$.

Добуток $AB = C$ матриці A розміру $m \times n$ на матрицю B розміру $r \times s$ визначено лише у випадку, коли $n = r$ і $m = s$.

В окремому випадку множення матриці-рядка $\bar{c} = (c_1, c_2, \ldots, c_k)$ на матрицю-стовпець $\bar{x} = (x_1, x_2 \ldots, x_k)$, результат визначається як $\langle \bar{c}^T, \bar{x} \rangle$ (тобто, при цьому $\bar{c}$ розглядається як вектор).

У загальному випадку елемент c_{ij} матриці $(c_{ij})=(a_{ij})(b_{ij})$ визначається як $c_{ij} = \langle A_i, B_j \rangle$, де A_i - рядок матриці A з номером i, а B_j - стовпець матриці B з номером j.

Рангом матриці називається ранг системи її векторів-стовпців.

Теорема. Ранг матриці дорівнює рангу системи її векторів-ків.

Матриця $A=(a_{ij})$ розміру $m \times n$ називається квадратною, якщо $m = n$. Число стовпців квадратної матриці називається її порядком. Діагоналлю з номером h

квадратної матриці $A=(a_{ij})$ порядку n називається підмножина її елементів виду $a_{ij},(j-i)\equiv h(\mathrm{mod}n).$ При $h=0$ діагональ називається головною, всі інші діагоналі називаються побічними.

Множина квадратних матриць є некомутативним кільцем.

Нулем є матриця 0, що складається з усіх нулів. Одиницею - матриця E, у якої всі елементи головної діагоналі дорівнюють одиниці, а інші елементи - нулю.

Множення квадратної матриці порядку n на матрицю-стовпець можна розглядати як операцію над векторами. Така операція є лінійним перетворенням n- мірного векторного простору. **Матриця називається оборотною,** якщо вона здійснює взаємно однозначне перетворення.

Нехай A - оборотна матриця. **Матрицею, оберненою до A, називається матриця A^{-1}, для якої виконуються умови $AA^{-1}=A^{-1}A=E$.**

Підстановочні матриці. Визначник матриці над $GF(2^t)$.

Підстановкою порядку n на множині V з n елементів називається взаємно однозначне відображення множини V на себе.

Нехай V упорядковано, тоді йому відповідає послідовність номерів $1,2,\ldots,n$ Після застосування підстановки порядок розташування елементів зміниться і прийме вигляд $\alpha_1,\alpha_2,\ldots,\alpha_n$.

Підстановку можна представити у виді дворядкового запису: $\begin{pmatrix}1 & 2 & \ldots & n\\ \alpha_1 & \alpha_2 & \ldots & \alpha_n\end{pmatrix}=\begin{pmatrix}i\\ \alpha_i\end{pmatrix}$. Очевидно, що зворотне перетворення має вигляд $\begin{pmatrix}\alpha_i\\ i\end{pmatrix}$.

Розглянемо квадратну матрицю $A=(a_{ij})$ порядку n, у якої елементи з індексами i,α_i дорівнюють одиниці, а інші дорівнюють нулю. Наприклад, для підстановки $\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$ одержимо $A=\begin{pmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}$.

Очевидно, $\begin{pmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 0\end{pmatrix}\begin{pmatrix}1\\ 2\\ 3\\ 4\end{pmatrix}=\begin{pmatrix}2\\ 4\\ 3\\ 1\end{pmatrix}$, тобто матриця реалізує задану підстановку.

Виходячи з визначення підстановки, підстановочні матриці оборотні. Якщо матриця A - підстановочна, то $A^{-1}=A^T$.

Критерій оборотності матриці формулюється за допомогою поняття визначника (детермінанта). Детермінант матриці A над полем F є елементом поля F. Він є функцією всіх елементів матриці і позначається через $\det A$. Детермінант записується також у виді $|A|$.

Матриця A оборотна тоді і тільки тоді, коли $\det A\neq 0$.

Розглянемо випадок, коли матриця A порядку n визначена над полем $GF(2^t)$

Розглянемо всі $n!$ підстановочних матриць порядку n. Уявимо собі, що кожна з них записана у виді таблиці на окремому листі паперу у клітинку. Проріжемо у кожній таблиці віконця у тих клітинках, де елементи відповідної матриці дорівнюють одиниці. Одержимо, таким чином, сукупність підстановок у виді трафаретів.

Накладемо кожен трафарет π на матрицю A і перемножимо всі елементи, щоб у віконцях з'явилися матриці A. Результат $\pi(A)$ назвемо членом визначника матриці, що відповідає підстановці π.

Знайдемо суму над полем $GF(2^t)$ усіх $n!$ членів визначника. Результат назвемо визначником матриці над полем $GF(2^t)$.

Анулюючий і мінімальний многочлен матриці над полем.

Многочленом $f(x)$ від матриці A над полем F називається результат послідовності операцій, записаної у формі многочлена $f(x)$ з коефіцієнтами з поля F, при $x = A$.

Визначення. Анулюючим многочленом матриці A називається многочлен $f(x)$, такий, що $f(A) = 0$.

Визначення. Мінімальним многочленом матриці A над полем F називається нормований многочлен $m(x)$ найменшого степеня, для якого $m(A) = 0$.

<u>Теорема</u>. Мінімальний многочлен матриці ділить будь-який анулюючий многочлен тієї ж матриці.

<u>Теорема.</u> Степінь мінімального многочлена матриці не перевершує її порядку.

Розглянемо послідовність $A^0\bar{x} = \bar{x}, A\bar{x}, A^2\bar{x}, \ldots, A^k\bar{x}_k, \ldots$, n- мірних векторів.

На кожному кроці k будемо перевіряти, чи є система отриманих векторів залежною, чи ні. На деякому кроці $k \le n$ вектори уперше виявляться лінійно залежними, тобто при деяких коефіцієнтах виконається співвідношення $(a_0 + a_1 A + \ldots + A^k)\bar{x} = 0$.

Многочлен $g(x) = a_0 + a_1 x + \ldots a_{k-1}x^{k-1} + x^k$ називається мінімальним многочленом матриці A відносно вектора $\bar{x}$. Мінімальний многочлен єдиний.

<u>Теорема.</u> Мінімальний многочлен суми векторів є найменшим спільним кратним мінімальних многочленів векторів - доданків.

<u>Теорема</u>. Мінімальний многочлен матриці A відностно будь-якого вектора $\bar{x}$ ділить мінімальний многочлен матриці.

Нехай A - квадратна матриця над скінченним полем F і $\bar{x} \neq \bar{0}$. Послідовність $\bar{x}, A\bar{x}, A^2\bar{x}, \ldots, A^k\bar{x}_k, \ldots$ є періодичною. Довжина періоду залежить від властивостей мінімального многочлена матриці A відносно вектора $\bar{x}$.

Очевидно, найменше спільне кратне мінімальних многочленів базисних векторів відносно матриці A є мінімальним многочленом цієї матриці.

Можна розглядати матриці, елементами яких є функції, скажемо, від змінної x. У цьому випадку визначник матриці також є функцією від x.

Многочлен $\Delta(x)=\det(A-xE)$ називається **характеристичним многочленом** матриці A.

Теорема Гамільтона-Келі. Кожна матриця є коренем свого характеристичного многочлена.

Група підстановок.

Підстановкою називається взаємно однозначне відображення скінченної множини на себе.

Звичайно підстановки записують у виді двох рядків. Верхній рядок є операндом підстановки, а нижній - результатом її дії на операнд.

Наприклад, $T=\begin{pmatrix} a & b & c & d & e \\ b & a & d & e & c \end{pmatrix}$.

Елементи скінченної множини завжди можна перенумерувати, отже, операнд будь-якої підстановки можна записати у виді *1, 2,..., n*, де *n* - кількість елементів в операнді: $T=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ (тобто, запис підстановки в канонічному виді).

Число *n* називається степенем підстановки.

Результат послідовної дії підстановок T_1, T_2 називається їхнім добутком і записується T_1T_2.

Добуток двох підстановок визначається, виходячи з того, що, якщо перша підстановка переводить *j* на місце *i*, а друга підстановка переводить *k* на місце *j*, то в добутку *k* переходить на місце *i*.

Таким чином, якщо $T_1=\begin{pmatrix} i \\ \alpha_i \end{pmatrix}, T_2=\begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix}$, то $T_1T_2=\begin{pmatrix} i \\ \beta_i \end{pmatrix}$, наприклад, при $T_1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ і $T_2=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $T_1T_2=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

Легко бачити, що $T_1T_2 \neq T_2T_1$, однак дужки в добутках можна розставляти довільно. Існує **«одинична» підстановка** *I*, така, що для всіх *T* : *IT=TI=T*. Для нашого прикладу $I=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

Для будь-якої підстановки T існує **обернена підстановка** T^{-1}, така, що $T^{-1}T=TT^{-1}=I$. Для побудови T^{-1} досить переставити місцями рядки в підстановці T, а потім упорядкувати стовпчики так, щоб числа у верхньому рядку йшли у зростаючому порядку.

Множина підстановок степеня *n* із зазначеною операцією множення є групою. Ця група позначається S_n і називається симетричною групою n-ого степеня. Порядок групи S_n дорівнює $n!$.

У деякому розумінні підстановки степеня *n* можуть бути сконструйовані з підстановок меншого степеня.

Справа в тім, що підстановки степеня $n< N$ можуть діяти на операнді з *N* елементів, якщо вважати, що кожний з *N-n* додаткових елементів не переміщується (переходять у себе). Наприклад, при доповненні кожного

операнда елементами $n+1,\ n+2\ \ldots\ N$, можна вважати, що $\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n & n+1 & \ldots & N \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n & n+1 & \ldots & N \end{pmatrix}$.

Виходячи з цього, можна говорити про те, що підстановки меншого степеня включаються у множину підстановок більшого степеня і, у свою чергу, утворюють **підгрупу групи** S_n**.**

1.9 Цикли і транспозиції. Подібні підстановки

Кожну підстановку *T* можна представити у виді добутку $T = P_1 \ldots P_k$ **деяких спеціальних підстановок, що називаються циклами**, причому, цикли $P_1 \ldots P_k$ попарно незалежні. Останнє означає, що підстановки P_i і P_j, при $P_i \neq P_j$, якщо не брати до уваги елементи, які залишаються нерухомими, діють на підмножинах операнда підстановки *T*, що не перетинаються.

Нехай $1 < k < n$ і P - підстановка степеня n, причому $P \neq I$. **Підстановка *P* називається *k*-членним циклом, якщо вона не переміщує *N-k* елементів, а її дію на решту *k* елементів** $i_1, i_2, \ldots, i_k$ **можна представити у вигляді циклічної діаграми переходів:** $i_1 \to i_2 \to i_3 \to \ldots \to i_k \to i_1$**.** У цій діаграмі дозволяється тільки один перехід від елемента з більшим індексом до елемента з меншим індексом, а саме: $i_k \to i_1$.

Наприклад, трічленний цикл п'ятого степеня: $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$. Тут елементи *4* і *5* нерухомі, причому $i_1 = 1$, $i_2 = 3$, $i_3 = 2$.

Циклічна діаграма переходів може бути виписана, починаючи з будь-якого свого елементу. Цикл записують у виді, аналогічному діаграмі переходів: $(i_1, i_2, \ldots, i_k)$**.** Одиничну підстановку розглядають як добуток одночленних циклів виду $I = (i)$.

Для запису підстановки у вигляді добутку незалежних циклів досить виписати всі різні діаграми переходів. Наприклад, підстановка може бути представлена як $T = (1679)(2354)(8)$**.** Одночленні цикли при такому запису часто ігноруються.

Запис підстановки у виді добутку незалежних циклів називається циклічним записом.

Найбільш простим циклом, очевидно, є підстановка, що переставляє місцями тільки два елементи. Такий **двочленний цикл називається транспозицією.** Транспозиції не обов'язково є незалежними циклами.

Можна показати, що якщо підстановка степеня *N* розкладається в добуток *r* попарно незалежних циклів (включаючи й одночленні цикли), то її можна представити у вигляді добутку *n-r* транспозицій. Величина $\delta(\pi) = n - r$ **називається декрементом підстановки.**

Підстановка називається регулярною, якщо її циклічний запис складається з циклів рівної довжини.

Підстановка називається повноцикловою, якщо її цикловий запис складається з одного циклу.

Підстановка π називається парною (непарною), якщо її декремент $\delta(\pi)=n-r$ парний (непарний) відповідно.

Знаком (характером) підстановки називається значення $\varepsilon(\pi)=(-1)^{\delta(\pi)}$.

У загальному випадку визначник матриці A порядку n над полем F виражається як знакозмінна сума всіх членів визначника, що відповідають підстановкам групи S_n: $\det A=\sum_{\pi}\varepsilon(\pi)A(\pi)$.

Корені з підстановок.

Визначення. Степенем π^k довільної підстановки π називається *k*-кратний добуток підстановки саму на себе.

Для запису π^k в цикловому виді досить кожен цикл підстановки π перетворити в такий спосіб.

Нехай $\pi=(1679)(2354)(8)$, $k=2$. Вибираємо елементи з кроком k, починаючи з кожного, скажемо, першого елемента поточного циклу. Записуємо їх послідовно. При першому повторенні серед обраних елементів закриваємо результуючий цикл. Якщо символи вхідного циклу не вичерпані, вибираємо один з елементів, що не входять у результуючий цикл і діємо аналогічно. Після вибору всіх елементів циклу переходимо до наступного циклу вхідної підстановки.

Примітка. Вибір елементів із кроком k означає вибір елементів з номерами $i, i+k(\mathrm{mod}\,h), i+2k(\mathrm{mod}\,h)$ і т.д., де h - довжина відповідного циклу.

Отже, $(1679)\to(1,7)(6,9)$. Наступні цикли дають $(2354)\to(25)(34)$, $(8)\to(8)$. У підсумку, $\pi^k=(1,7)(6,9)(25)(34)(8)$.

Задача знаходження π, виходячи з π^k, не однозначна. Елементи циклу $(1,7)$ в цикловому запису вхідної підстановки могли знаходитися в будь-якому місці і бути до того ж циклічно зсунуті.

Єдине, що відомо, це відстань між елементами, тобто вони були розташовані у вхідній підстановці як $1*7$ або $7*1$.

Для добування коренів степеня k з підстановок необхідно враховувати усі варіанти можливого взаємного розташування елементів циклів, що залежить від k, n і довжин циклів вхідної підстановки.

Подібні підстановки.

Підстановки одного степеня $A,B\in S_n$ називаються подібними, якщо існує підстановка $X\in S_n$ така, що $X^{-1}AX=B$.

Рівняння $X^{-1}AX=B$ відносно X називається **рівнянням подібності**.

Цикловою структурою підстановки називається запис виду $(c_1^{k_1},\ldots,c_s^{k_s})$, де s- кількість різних довжин циклів у циклічному запису підстановки, c_j довжина одного з її циклів, а k_j- кількість циклів довжини c_j, що входять у підстановку.

Теорема. Підстановки подібні в тому і тільки тому випадку, коли їхні циклові структури однакові.

Розв'язок рівняння подібності полягає в наступному.

1. Записуємо A, B в цикловій формі.

2. Якщо циклові структури не однакові, то розв'язків немає.

3. Підписуємо циклові записи підстановок B, A друг під другом таким чином, щоб під кожним циклом з'явився цикл рівної довжини.

4. У кожній групі циклів однакової довжини в одному із рядків, їскажемо, нижньому, довільно переставляємо цикли місцями. При кожній конфігураці розташування циклів у групі кожен цикл, незалежно від інших, виписуємо з кожного місця. Перетворення робимо з кожною групою циклів незалежно.

Кожна з множини отриманих дворядкових записів (підстановок) є розв'язком рівняння подібності.

2 Елементи теорії чисел

2.1 Деякі визначення і твердження

Велику роль в теорії чисел (і криптографії) відіграють прості числа. ***Простим*** *числом* називається число, яке ділиться без залишку тільки на одиницю і само на себе. Іншими словами, простим називається число $p \geq 3$, яке не ділиться без залишку на одне із наступних чисел 2, 3, ...,p-1. Число 2 також являється простим.

Важливим являється також поняття взаємної простоти двох натуральних чисел. ***Взаємно простими*** називаються два цілих додатніх числа, найбільший загальний дільник яких дорівнює 1, що базується на наступному твердженні.

Твердження 2.1

Якщо $НСД(a,n) = 1$ і $(a \times b) \equiv (a \times c) \bmod n$, то $b \equiv c \bmod n$.

Доведення

Із порівняння $(a \times b) \equiv (a \times c) \bmod n$ виходить: $ab - ac \equiv 0 \bmod n \Rightarrow a(b-c) = Qn$, де Q - ціле додатнє число або 0. Якщо Q — 0, то твердження виконується. Якщо $Q \neq 0$, із рівності $a(b - c) = Qn$ виходить, що в правій частині утримується множник n, який може міститися тільки в значенні b — c, так як a і n являються взаємно простими числами, тобто не містять загальних множників, крім одиниці. Таким чином, $b - c = qn$, де q - ціле додатнє число, тобто $b \equiv c \bmod n$.

Користуючись доведеним вище твердженням, доведемо наступне.

Про існування оберненого елемента

Твердження 2.2

Для будь-якого цілого числа $a > 0$, взаємно простого з модулем n , існує обернене за mod n число, яке позначається знаком a^{-1}, таке, що $a * a^{-1} \equiv 1 \bmod n$. Число a^{-1} називається мультиплікативно оберненим за модулем n.

Доведення

Розглянемо множину значень $\{1,2,....,n-1\}$. Перемножуючи кожне із них на *a* за mod *n*, отримуємо множину $\{(a \bmod n),(2a \bmod n,...,((n-1)a \bmod n))\}$, яка містить по одному разу числа 1,2,..,*n*-1, тобто для деякого значення *i* виконується умова $ia \bmod n = 1$. Це виходить із протиріччя, яке виникає при припущенні про існування двох однакових значень. Нехай, наприклад, *ha* mod *n* = *ka* mod *n*. Тоді з урахуванням умови НСД(*a*, *n*) = 1 із останньої умови отримаємо $h = k \bmod n \Rightarrow h = k$. Останнє суперечить тому, що ми перемножали на *a* тільки різні числа. Указане значення і являється мультиплікативно оберненим (до числа *a)* елементом за модулем *n*.

Наслідок 2.1

Якщо модуль *p* являється простим числом, то для будь-якого числа $0 < a < p$ існує мультиплікативно обернений елемент за модулем *p*.

Можна показати, що якщо $НСД(a,n) \neq 1$, то не існує числа *b*, такого, що $ab \equiv 1 \bmod n$. Дійсно, нехай $НСД(a,n) = d$, тобто $a = dq$ і $n = dp$. Перемножуючи на *a* за модулем *n* кожне число із множини значень $\{1,2,....,dp-1\}$, отримаємо наступний ряд залишків $\{(a \bmod n),(2a \bmod n,...,((dp-1)a \bmod n))\}$. Покажемо, що кожний із цих залишків ділиться без остачі на *d*, тобто містить множник *d*. Візьмемо будь-яке число *b*, таке, що $0 < b < dp$, і обчислимо залишок від ділення *ab* на $n: r = nb - Qn = dqb - Qdp = d(qb - Qp)$, де *Q* – деяке натуральне число. Із рівності $r = d(qb - Qp)$ виходить, що залишок ділиться на *d* (одночасно ми довели твердження про подільність залишка, яке сформульовано нижче). Таким чином, в указаному ряду *n-1* залишків утримуються тільки залишки, які діляться націло на *d*. Оскільки серед них немає одиниці, то це означає, що не існує числа *b*, при якому $ab \equiv 1 \bmod n$. Що ми і хотіли показати.

Про подільність залишку

Твердження 2.3

Нехай для цілих додатних чисел *a* і *b* маємо $a > b$ і $НСД(a,b) = d$, тоді для залишку *r* від ділення *a* на *b* виконується рівність $НСД(b,r) = d$.

Дане твердження лежить в основі алгоритму Евкліда, який дозволяє швидко обчислювати найбільший спільний дільник двох цілих додатних чисел.

Теорема Ферма

Теорема Ферма стверджує наступне: для будь-якого простого числа *p* і будь-якого додатного числа *a*, яке не ділиться на *p*, виконується порівняння

$\alpha^{p-1} \equiv 1 \bmod p$.

Доведення

Розглянемо множину чисел $\{1,2,....,p-1\}$, яку позначимо як Z_p. Якщо усі елементи Z_p перемножити на *a* за модулем *p,* то, використовуючи твердження 2.2, легко показати, що в результаті отримаємо деяку перестановку елементів Z_p. Іншими словами, в наборі *{a mod p, 2a mod p, ...,{ p -1l)a mod p}* міститься $(p-1)$ різних чисел, тобто, кожне із чисел $1,2,....,p-1$ зустрічається рівно по одному разу. Перемножуючи числа $\alpha,2\alpha,...,(p-1)\alpha$, отримаємо:

$\alpha \times 2\alpha \times ... \times (p-1)\alpha = (p-1)!\alpha^{p-1}$.

Поділивши на p ліву і праву частини останнього співвідношення, отримаємо

$$\left[\alpha \times 2\alpha \times ..... \times (p-1)\alpha\right] \bmod p = (p-1)!\alpha^{p-1} \bmod p;$$

$$\left[(\alpha \bmod p) \times (2\alpha \bmod p) \times ... \times ((p-1)\alpha \bmod p)\right] \bmod p \equiv (p-1)!\alpha^{p-1} \bmod p.$$

Оскільки добуток не змінюється від перестановки місць співмножників, то ліву частину останнього порівняння можна представити у вигляді

$$\left[(\alpha \bmod p) \times (2\alpha \bmod p) \times ... \times ((p-1)\alpha \bmod p)\right] \bmod p \equiv 1 \times 2 \times ... \times (p-1) = (p-1)!$$

Із останніх двох співвідношень виходить

$$(p-1)! \equiv (p-1)!\alpha^{p-1} \bmod p.$$

Числа $(p$-1)! і p являються взаємно простими, тому в останньому виразі на підставі твердження 2.2 можна ліву і праву частини скоротити на $(p$— 1)!, звідки витікає порівняння

$$\alpha^{p-1} \equiv 1 \bmod p.$$

Тепер не представляє складності вивести наступні формули:

$$\alpha^p \equiv \alpha \bmod p \text{ і } b = c \bmod (p-1) \Rightarrow \alpha^b \equiv \alpha^c \bmod p.$$

2.2 Функція Ейлера

В узагальненні теореми Ферма використовується поняття функції Ейлера, яка часто буде нам зустрічатися в подальшому. Функція Ейлера відіграє важливу роль в теорії чисел. Вона позначається символом $\varphi(n)$ і визначається як число додатних цілих чисел, які менше n і являються взаємно простими з n.

Очевидно, що для простого p маємо $\varphi(p)=p-1$. Використовуючи твердження про мультиплікативність функції Ейлера для числа $n = pq$, яке являється добутком двох простих чисел p і q, можна легко отримати

$$\varphi(n)=\varphi(pq)=\varphi(p) \text{ x } \varphi(q)=(p-1) \text{ x } (q-1).$$

Цю часткову формулу легко отримати і без використання властивості мультиплікативності функції Ейлера. Дійсно, розглянемо множину чисел {1,2, ..., $(pq$- 1}}. Неважко відмітити, що усі числа, які не перевищують значення pq і не являються взаємно простими з $pq = n$, складають наступні дві множини $\{p, 2p, ...,(q-1)p\}$ і $\{q, 2q, .., (p-1)q\}$. В першій міститься q - 1 , а у другій p - 1 різних чисел. Віднімаючи із n - 1 значення q -1 і p - 1 , отримаємо

$$\varphi(n)=pq-1-(q-1)-(p-1)=pq-(p+q)+1=(p-1) \text{ x } (q-1).$$

Проте в загальному випадку, коли в канонічному розкладанні числа n міститься порівняно велике число простих співмножників і їх степенів, при обчисленні функції Ейлера використовується те, що вона являється мультиплікативною функцією, тобто для двох взаємно простих чисел a і b виконується співвідношення $\varphi(ab) = \varphi(a) * \varphi(b)$.

Оскільки в канонічному розкладанні довільного числа n містяться тільки взаємно прості співмножники виду p^S, де $s > 1$, то для обчислення функції Ейлера достатньо навчитися обчислювати функцію Ейлера від чисел виду p і вміти розкладати число n на прості множники.

Нехай дано число p^S. Розглянемо множину чисел

$$\{1,2, ...,p, ...,2p. ...,3p, ...,p^{S-1}p\}.$$

Неважко бачити, що усі числа, що входять в цю множину і не є взаємно простими з p^S, складають підмножину $\{p, 2p, 3p, ...,p^{S-1}p\}$ із p^{S-1} чисел. Звідси отримаємо

$$\varphi(p^S)= p^S- p^{S-1}= p^{S-1}(p-1).$$

Використовуючи цю формулу і властивість мультиплікативності, можна легко обчислити функцію Ейлера від довільного заданого числа, якщо ми зможемо розкласти його на множники.

Теорема Ейлера

Теорема Ейлера, яка є узагальненням теореми Ферма, стверджує, що для будь-яких взаємно простих чисел a і n виконується порівняння

$$\alpha^{\varphi(n)} \equiv 1 \bmod n .$$

Доведення

Доведення аналогічно доведенню теореми Ферма. Оскільки для простого n маємо $\varphi(n)= (n-1)$, то в цьому випадку порівняння $\alpha^{\varphi(n)} \equiv 1 \bmod n$ безпосередньо випливає із теореми Ферма (є просто іншою формою запису останньої). Доведення для довільного n покладається на визначенні функції Ейлера: $\varphi(n)$ дорівнює числу додатних цілих чисел, менших n і взаємно простих з n. Множина таких цілих чисел включає $\varphi(n)$ значень, які можна прономерувати наступним чином;

$$\Phi = \{x_1, x_2,..., x_{\varphi(n)}\}.$$

Перемножуючи кожний елемент цієї множини на a за модулем n, отримаємо множину

$$\Phi' = \{(\alpha x_1 \bmod n), (\alpha x_2 \bmod n),...., (\alpha x_{\varphi(n)} \bmod n)\}.$$

Покажемо, що останні дві множини включають одні і ті ж елементи. Дійсно, для всіх значень i= 1,2, ... $\varphi(n)$ числа a і x є взаємно простими з n, тому число ax також є взаємно простим з n. Отже, усі елементи S є цілими числами, меншими n (множення ми виконували за модулем n) і взаємно простими з n. У множині

Ф′ немає повторень, тому що якщо *(a * b)* ≡ *(a * c)* mod *n* , то *b* ≡ *c* mod *n*, оскільки за умовою теореми, що доводиться, *a* і *n* являються взаємно простими числами. Дійсно, із умови *ax* mod *n* = *ax* mod *n* виходить $x_i = x_j$. що суперечить тому, що в множині *Ф* усі числа різні. Перемножуючи усі елементи множини *Ф′*, а потім усі елементи множини *Ф*, отримаємо рівність

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) \equiv \prod_{i=1}^{\phi(n)} x_i ,$$

із якої виходить порівняння

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n),$$

$$a^{\phi(n)} X\left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i (\bmod n).$$

$$\alpha^{\varphi(n)} \equiv 1(\bmod n).$$

Із останнього порівняння випливають наступні співвідношення:

$\alpha^{\varphi(n)-1} \equiv 1(\bmod n)$ і

$b \equiv c \bmod \varphi(n) \Rightarrow \alpha^k \equiv \alpha^c \bmod n\, n.$

2.3 Алгоритм Евкліда

Нехай **MOD(*a*, *b)*** є операція взяття залишку від ділення *a* на *b,* а **QUO*(a*, *b*)** є частка від ділення *a* на *b*. Алгоритм Евкліда дозволяє без розкладання двох цілих чисел на множники знаходити їх найбільший спільний дільник. В даному алгоритмі використовується наступне твердження: якщо *a = bq + r,* де *b* ≠0, і число *d* ділить *a* і *b,* то воно ділить і *r*, тобто, маємо *d* | *(a- bq).* Це твердження дійсне для будь-якого дільника, включаючи найбільший спільний дільник *d*= НСД(a, b). Звідси виходить, що НСД(*a,b*) = НСД [*b,* **MOD** *(a, b)*].

Для будь-якого *a* маємо також НСД(a,0) = |*a*| . Нехай задані ціле число *a* і ненульове ціле число *b.* Алгоритм Евкліда передбачає виконання наступної послідовності ділень, де прийняте позначення $a_0 = a$ і $a_1 = b$:

$a_0 = a_1 q_1 + a_2,$ $\quad 0 < a_2 < |a_1|,$

$a_1 = a_2 q_2 + a_3,$ $\quad 0 < a_3 < |a_2|,$

... ...

$a_{k-2} = a_{k-1} q_{k-1} + a_k,$ $\quad 0 < a_k < |a_{k-1}|,$

$a_{k-1} = a_k q_k + 0.$

Процес ділення має кінцеве число кроків, оскільки лишки спадають за абсолютною величиною $|a_1| > a_2 > a_3 > \ldots > 0$ (значення a_1 може бути від'ємним, тому воно прийнято за абсолютною величиною; решта лишків додатні). Значення a_k являється найбільшим спільним дільником. З урахуванням указаного вище твердження маємо

$$НСД(\alpha_0, \alpha_1) = НСД(\alpha_1, \alpha_2) = \ldots = НСД(\alpha_k, 0) = \alpha_k ,$$

тобто насправді a_k являється найбільшим спільним дільником чисел a і b. Одночасно ми показали, що приведений нижче алгоритм працює правильно. Позначимо операцію призначення наступним чином: $x:=y$ означає призначення змінній x значення y, $a(x,y):=(x_1,y_1)$ означає виконання операцій $x:=x_1$, $y:=y_1$.

Алгоритм Евкліда (знаходження НСД(a, b))

ВХІД: a і $b \neq 0$.

1 . [Ініціалізація] $(a_0, a_1) := (a,b)$.

2. [Основний цикл] Поки a ≠ 0 виконувати$(a_0, a_1):= [a_1,$ **MOD** $(a_0,,a_1)]$

3. Повернути $d:=a_0$.

ВИХІД: $d=НСД(a, b)$.

2.4 Розширений алгоритм Евкліда

В будь-якому рядку описаного вище алгоритму Евкліда кожний лишок представляє собою лінійне представлення ділимого і дільника. Легко бачити, що, починаючи з одного із ненульових лишків (наприклад, останнього, тобто починаючи з a_k) і представляючи лишки, отримані на наступних кроках алгоритму Евкліда, через лишки, отримані на попередніх кроках, можна представити значення a_i , (відповідно a_k) в наступному вигляді $a_i = ax'+by'$ (відповідно, $a_k = ax + by$), де x і y - деякі цілочисельні коефіцієнти. Розширений алгоритм Евкліда дозволяє обчислювати значення коефіцієнтів x і y в указаному лінійному представленні НСД(a,b), тобто у виразі $a_k = ax + by$. Робота розширеного алгоритму Евкліда організується так, що значення x' і y' обчислюються за d серії кроків, в кожному із яких ми представляємо a в вигляді указаного лінійного представлення.

Кожний лишок, обчислений в процесі роботи алгоритму Евкліда, можна представити у вигляді $ax_i+ by_i$. Розглянемо наступну послідовність такого представлення лишків:

$a_0=a,$	$a_0=ax_0+by_o,$
$a_1=b,$	$a_1=ax_1+by_1,$
$a_2=a_0-a_1q_1,$	$a_2=ax_2+by_2,$
...	...
$a_i=a_{i-2}-a_{i-1}q_{i-1},$	$a_i=ax_i+by_i,$
...	...
$a_k=a_{k-2}-a_{k-1}q_{k-1},$	$a_k=ax_k+by_k,$
$0=a_{k-1}-a_kq_k,$	$0=ax_{k+1}=by_{k+1}.$

В лівому стовпці фактично приведена послідовність ділень, яка отримана в алгоритмі Евкліда, але записана у вигляді виразу для обчислення лишків. В правому стовпці кожний лишок представлений у вигляді, який нас цікавить, $a_i + by_i$. Поки що ми не знаємо коефіцієнтів. Нашою метою являється обчислення x_i і

y_i для будь-якого i, а, отже, і для $i=k$. Очевидно, що $x_0=1$, $y_0=0$ і $x_1=0$, $y_1=1$. Порівнюючи обидві частини на i-му кроці, отримаємо

$$a_i=ax_i+by_i=a_{i-2}-a_{i-1}q_{i-1}=(ax_{i-2}+by_{i-2})-(ax_{i-1}+by_{i-1})=a(x_{i-2}-x_{i-1}q_{i-1})+b(y_{i-2}-y_{i-1}q_{i-1}),$$

звідки отримується наступна індуктивна процедура обчислення x_i і y_i.

$$Q_{i-1}=QUO(a_{i-2},,a_{i-1}),$$
$$a_i=a_{i-2}-a_{i-1}q_{i-1},$$
$$x_i=x_{i-2}-x_{i-1}q_{i-1},$$
$$y_i=y_{i-2}-y_{i-1}q_{i-1}.$$

Відзначимо, що значення a_i може бути обчислене як MOD(a_{i-2},a_{i-1}), але перевага приведеного вище виразу полягає в тому, що a_i обчислюється аналогічно обчисленню коефіцієнтів x_i і y_i. Цей факт використовується в наступному алгоритмі.

Розширенний алгоритм Евкліда
ВХІД: *a* і *b* ≠0
1. Ініціалізація] (a_0,a_1)*:= (a,b); (x_0, x_1) :=(1,0); (y_o,y_1):= (0, 1).*
2. [Основний цикл] Поки а ≠ 0 виконувати
*{q:=*QUO*(a_0,a_1);*
(a_0,a_1):=(a_1,a_0-a_1q);
(x_0,x_1):=(x_1,x_0-x_1q);
(y_0,y_1):=(y_1,y_0-y_1q)}.
3 . Повернути (d, x, y) := (a_0,x_0,y_0)
ВИХІД: *d, x, y,* такі, що *d = НСД(a, b) = ax +by.*

2.5 Показники і первісні корені

Для взаємно простого з модулем n числа a, згідно теореми Ейлера, існує деяке додатнє $\gamma = \varphi(n)$, для якого виконується умова $a^\gamma \equiv 1 \pmod n$. У випадку простого модуля p маємо $\gamma = p-1$. Представляє інтерес знайти найменше із чисел γ, для яких виконується вказана умова.

Визначення
Нехай НСД (a, n) = 1. Найменше із чисел γ, для яких виконується порівняння $a^\gamma \equiv 1 \pmod n$, називається ***показником,*** якому число a належить за модулем n.

Твердження 2.1
Якщо a за модулем n належить показнику δ, то числа a^0 , a^1 ,..., $a^{\delta-1}$ за модулем n непорівнянні.

Доведення
Нехай $a^h \equiv a^k \pmod n$, $0 < h < l < \delta$. Тоді отримаємо $a^{h-k} \equiv 1 \pmod n$, де $0 < h - k < \delta$. Але за визначенням δ є найменше із чисел γ, для яких виконується порівняння $a^\gamma \equiv 1 \pmod n$. Протиріччя доводить твердження.

Твердження 2.2

а) Якщо a за модулем n належить показнику δ, то $a^{\gamma} = a^{\gamma-1} \pmod{n}$ тоді і тільки тоді, коли $\gamma \equiv \gamma^{1} \pmod{\delta}$.

б) Якщо $\gamma = 0$, то маємо порівняння $a^{\gamma} \equiv 1 \pmod{n}$, яке виконується тоді і тільки тоді, коли γ ділиться на показник δ.

Доведення

Нехай r і r' є найменші невід'ємні лишки чисел γ і γ' за модулем δ. Тоді при деяких q і q' маємо: $\gamma = \delta q + r$, $\gamma' = \delta q' + r'$. Оскільки $a^{\delta} \equiv 1 \pmod{n}$, то отримуємо $a^{\gamma} = (a^{\delta})^{q} a^{r} \delta \equiv a$, звідки

$$a^{r} \equiv (mod\ n) \text{ і } a^{\gamma} \equiv (a^{\delta})^{q} a^{r'} \equiv a^{r'} (mod\ n).$$

Отже, a^{γ} і $a^{\gamma'} \pmod{n}$ рівні тоді і тільки тоді, коли $a^{r} \equiv a^{r'} (mod\ n)$, тобто тоді і тільки тоді, коли $r=r'$. Дійсно, $r<\delta$ і $r'<\delta$ і із $a^{r} \equiv a^{r'} (mod\ n)$, виходить $r=r'$. В іншому випадку ми маємо протиріччя: $a^{|r-r'|} = 1 (mod\ n)$ при $0< |r-r'| <\delta$.

Наслідок 2.1

Показники, яким числа a належать за модулем n, являються дільниками $\varphi(n)$.

Дійсно, нехай a за модулем n належить показнику δ. Із $a^{\varphi(m)} \equiv 1 \pmod{n}$ виходить, що $\varphi(n)$ ділиться на δ. Найбільший із цих дільників є само $\varphi(n)$.

Первісні корені

Цікаве питання про існування чисел, що належать показнику $\varphi(n)$. Такі числа існують і називаються первісними коренями за модулем n.

Твердження 2.3

Якщо число a за модулем n належить показнику $\varepsilon'\varepsilon$, то $a^{\varepsilon'}$ належить показнику ε.

Доведення

Дійсно, нехай $a^{\varepsilon'}$ належить показнику δ. Тоді $(a^{\varepsilon'})^{\delta} \equiv 1 \pmod{n}$, тобто $a^{\varepsilon'\delta} \equiv 1 \pmod{n}$, із чого виходить, що $\varepsilon'\delta$ ділиться на $\varepsilon'\varepsilon$, тобто δ ділиться на ε. З іншої сторони, $a^{\varepsilon'\varepsilon} \equiv 1 \pmod{n}$, звідки $(a^{\varepsilon'})^{\varepsilon} \equiv 1 \pmod{n}$, звідки, за твердженням 2.3, виходить, що ε' ділиться на δ. Таким чином, $\varepsilon' | \delta$ і $\delta | \varepsilon'$, тому $\delta = b$.

Твердження 2.4

Якщо a за модулем n належить показнику u, а b - показнику v, причому НСД $(u, v) = 1$, то ab належить показнику uv.

Доведення

Дійсно, нехай ab належить показнику δ. Тоді $(ab)^{\delta} \equiv 1 \pmod{n} \Rightarrow (ab)^{v\delta} \equiv 1 \pmod{n} \Rightarrow a^{v\delta} b^{v\delta} \equiv 1 \pmod{n} \Rightarrow a^{v\delta} \equiv 1 \pmod{n}$, звідки виходить, що $v\delta$ ділиться на n. Але оскільки НСД $(u, v) = 1$, то δ ділиться на u. Розмірковуючи аналогічним образом, отримаємо, що δ ділиться на v. Внаслідок того, що $u | \delta$, $v | \delta$ і НСД$(a, b)=1$, то $(uv) | \delta$, тобто δ ділиться і на uv. З іншої сторони, із $a^{u} b^{u} \equiv (a^{u})^{v} (b^{u})^{v} \equiv (ab)^{uv} \equiv 1 \pmod{n}$ виходить, що uv ділиться на δ. Оскільки $(uv) | \delta$ і $\delta | (uv)$, то $\delta = uv$.

В теорії чисел доводяться теореми про існування первісних коренів модуля p за модулем p^k і за модулем $2p^k$, де p - просте непарне число і k- довільне додатне ціле число.

Твердження 2.5

Існують первісні корені за модулем p, де p - просте непарне число.

Доведення

Нехай $\delta_1, \delta_2, \ldots, \delta_k$ - усі різні показники, яким за модулем p належать числа 1.2,..., $(p-1)$. Нехай найменше спільне кратне чисел $\delta_1, \delta_2, \ldots, \delta_k$ є НСК($\delta_1, \delta_2, \ldots, \delta_k$)=$\tau$, канонічне розкладання якого має вигляд $\tau = q_1^{\alpha 1} q_2^{\alpha 2} \ldots q_k^{\alpha k}$. Кожний множник $q_s^{\alpha s}$ цього розкладання ділить щонайменше один із показників $\delta_1, \delta_2, \ldots, \delta_k$, наприклад, число δ (це як раз той показник, який містить множник $q_s^{\alpha s}$ і вносить його в розкладання τ). Показник δ можна записати у вигляді $\delta_j = zq_s^{\alpha s}$. Нехай a_j - одне із чисел ряду 1,2, ...,p-1, що належать показнику δ_j. Згідно твердженню 2.4 число $h_j = z_j^{\cdot}$ належить показнику $q_s^{\alpha s}$. Оскільки показники $q_1^{\alpha 1}$,$q_2^{\alpha 2} \ldots q_k^{\alpha k}$ являються попарно взаємно простими, то згідно твердженню 2.5 добуток $g = h_1 h_2 \ldots h_k$ належить показнику $q_1^{\alpha 1} q_2^{\alpha 2} \ldots q_k^{\alpha k} = \tau$. У відповідності із наслідком до твердження 2.1 показник τ являється дільником числа $p-1$**:** $\tau | (p-1)$.

Оскільки показники $\delta_1, \delta_2, \ldots, \delta_k$, до кожного із яких відноситься хоча б одне із чисел ряду (1,2,...,p-1), ділять τ, то всі значення 1,2,…,p-1 являються розв'язками порівняння $x^\tau \equiv 1 \bmod p$ (див. твердження 2.4). В теорії чисел доводиться, що для простого p порівняння $a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 = 0 \bmod p$ має не більше n розв'язків, якщо хоча б один із коефіцієнтів $a_1, a_2, .., a_n$ не кратний p. Із цього твердження виходить, що $p - 1 \le \tau$. Оскільки $\tau : (p-1)$ і $p-1 \le \tau$, то $\tau = p - 1$. Отже, g являється первісним коренем за модулем p.

Таким чином, існують первісні корені за модулем простого числа. Цей факт враховується при розгляді методу відкритого розприділення ключів Діффі-Хеллмана. Представляють інтерес також наступні твердження про існування первісних коренів за модулями p^α і $2p^\alpha$, де p - непарне просте число, які ми приводимо без доведення.

Твердження 2.6

Нехай g - первісний корень за модулем простого числа p. Можна указати t з умовою, що u, яке визначається рівністю $(g + pt)^{p-1} = 1 + pu$, не ділиться на p. Відповідно $g + pt$ буде первісним коренем за модулем p^α при будь-якому $\alpha > 1$.

Твердження 2.7

Нехай $\alpha > 1$ і g_1 - первісний корень за модулем p^a, де p - непарне просте число. Непарне із чисел g' і $g' + p^\alpha$ буде первісним коренем за модулем $2p^\alpha$.

Представляє інтерес задача пошуку первісних коренів за модулем p. Ця задача розв'язується методом, що використовує наступне твердження.

Твердження 2.8

Нехай $q_1, q_2, \ldots, q_k$ - різні прості дільники функції Ейлера $\varphi(n)$ від числа n. Для того, щоб число g, взаємно просте з n, було первісним коренем за модулем n, необхідно і достатньо, щоб це g не задовольняло ні одному із порівнянь:

$$g^{c/q1} \equiv 1 \pmod n,\ g^{c/q2} \equiv 1 \pmod n, \ldots,\ g^{c/qk} \equiv 1 \pmod n \equiv 1 \pmod n.$$

Індекси за модулями p^α і $2p^\alpha$

По відношенню до первісних коренів g вводиться поняття індексу (при основі g) за модулем.

Твердження 2.9

Нехай p - просте непарне, $\alpha \geq 1$; n - одне із чисел p^α і $2p^\alpha$; $c = \varphi(n)$, g - первісний корень за модулем n. Якщо γ пробігає найменші невід'ємні лишки $\gamma = 0, 1, ..., c-1$ за модулем c, то g^γ пробігає приведену систему лишків за модулем n.

Дійсно, g відноситься до показника c і g^γ пробігає c чисел, взаємно простих з n, які являються попарно непорівнянними за модулем n.

Для чисел a, взаємно простих з n, розглядається поняття про індекс (дискретний логарифм), що представляє аналогію поняттю про логарифм. Якщо $a \equiv g^\gamma \pmod n$ (передбачається, що $\gamma \geq 0$), тоді γ називається індексом числа a за модулем n при основі g і позначається символом $\gamma = \text{ind}_g a$ (або просто $\gamma = \text{ind}\, a$). Із твердження 2.9 виходить, що будь-яке a, взаємно просте з n, має деякий єдиний індекс серед чисел ряду $\gamma = 0,1,...,c-1$. Знаючи γ', таке, що $\gamma' = \text{ind}_g a$, ми можемо указати усі індекси числа a: це будуть усі невід'ємні числа класу $\gamma = \gamma' \pmod c$. Дійсно, маємо $a \equiv g^{\gamma'} \pmod n$ і $a \equiv g^\gamma \pmod n$, тому $g^{\gamma-\gamma'} \equiv 1 \pmod n$ і, оскільки g відноситься до показника $c = \varphi(n)$, то $c \mid (\gamma - \gamma')$, тобто γ з $\gamma' \pmod c$.

Із визначення індексу виходить безпосередньо, що числа з даним індексом γ утворюють клас чисел за модулем n.

Розглянемо наступні властивості індексів:

$$\text{ind}_g ab...l \equiv \text{ind}_g a + \text{ind}_g ab + ... + \text{ind}_g l \pmod c$$

і, зокрема,

$$\text{ind}_g a^n \equiv n\, \text{ind}_g a \pmod c.$$

Дійсно, перемножуючи порівняння $a = g^{\text{ind}a + \text{ind}b} \pmod m$, $a = g^{\text{ind}b} \pmod m$,.., $l = g^{\text{ind}\, l} \pmod m$, знаходимо $ab...l \equiv g^{inda + indb + ... + indl} \pmod m$, сума $\text{ind}_g a + \text{ind}_g b + ... + \text{ind}_b l$ являється одним із індексів добутку $ab,...,l$.

2.6 Квадратичні лишки

Означення. Число $a \in Z_n^*$ називається *квадратичним лишком* або *квадратом* за модулем n, якщо існує таке $x \in Z_n^*$, що $x^2 \equiv a \pmod n$. Якщо такого x не існує, то число a називається квадратичним нелишком. Множина усіх квадратичних лишків за модулем n позначається через Q_n, нелишків – через $\overline{Q}_n$. За означенням $0 \notin Z_n^*$, отже $0 \notin Q_n$ та $0 \notin \overline{Q}_n$.

Теорема. Нехай p – непарне просте число, g – генератор Z_p^*. Тоді число a є квадратичним лишком за модулем p тоді і тільки тоді, коли $a = g^i \pmod p$, де i – парне ціле.

Доведення. Якщо $a = g^{2k} \pmod p$, то $a = b^2 \pmod p$, де $b = g^k \pmod p$.

Нехай $a = g^k \pmod p$ – елемент Z_p^*. Піднесемо його до квадрату:

$$a^2 = g^{2k} \pmod p \equiv g^i \pmod p.$$

Оскільки $2k \pmod{p-1} = i$ – парне число, то звідси і випливає твердження про те, що квадрат довільного елемента $a \in Z_p^*$ представляється у вигляді $g^i \pmod{p}$ лише для парного i.

Наслідок $|Q_p| = (p-1)/2$, $|\overline{Q_p}| = (p-1)/2$.

Тобто половина елементів Z_p^* є квадратичними лишками, а половина – ні.

Приклад. Число $a = 3$ є генератором Z_7^*. Степені a наведені у наступній таблиці:

I	0	1	2	3	**4**	**5**	6
$a^i \bmod 7$	1	3	2	6	4	5	1

Звідси $Q_7 = \{1, 2, 4\}$, $\overline{Q}_7 = \{3, 5, 6\}$.

Схема множення квадратичних лишків та нелишків аналогічна схемі додавання парних та непарних цілих чисел:

лишок * лишок = лишок
лишок * нелишок = нелишок
нелишок * нелишок = лишок

Приклад. Дослідимо операції множення лишків та нелишків в групі Z_7^*.

$$2 \in Q_7, 4 \in Q_7 : 2 * 4 = 8 \equiv 1 \in Q_7,$$
$$2 \in Q_7, 5 \in \overline{Q}_7 : 2 * 5 = 10 \equiv 3 \in \overline{Q}_7,$$
$$5 \in \overline{Q}_7, 6 \in \overline{Q}_7 : 5 * 6 = 30 \equiv 2 \in Q_7.$$

Твердження. Нехай n – добуток двох різних простих чисел p та q, $n = p * q$. Тоді число $a \in Z_n^*$ є квадратичним лишком за модулем n тоді і тільки тоді, коли $a \in Q_p$ та $a \in Q_q$. Звідси $|Q_n| = |Q_p| * |Q_q| = (p-1)(q-1)/4$ та $|\overline{Q_n}| = 3(p-1)(q-1)/4$.

Приклад. Нехай $n = 21$. Тоді $|Q_{21}| = (2 * 6)/4 = 3$, $Q_{21} = \{1, 4, 16\}$, $|\overline{Q}_{21}| =. (3 * 2 * 6)/4 = 9$, $\overline{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$.

Означення. Нехай $a \in Q_n$. Якщо $x \in Z_n^*$ задовольняє $x^2 \equiv a \pmod{n}$, то x називається *квадратним коренем* числа a за модулем n.

Теорема. Нехай p – просте, $p \equiv 3 \pmod 4$, $a \in Q_p$. Тоді розв'язком рівняння

$$x^2 \equiv a \pmod{p}$$

будуть числа r та $-r$, де $r = a^{\frac{p+1}{4}} \pmod{p}$.

Доведення. $r^2 \equiv a^{\frac{p+1}{2}} \pmod{p} \equiv \sqrt{a^{p+1}} \pmod{p} \equiv \sqrt{a^{p-1} \cdot a^2} \pmod{p} \equiv \sqrt{1 \cdot a^2} \pmod{p} \equiv a \pmod{p}$, оскільки за теоремою Ферма $a^{p-1} \pmod{p} \equiv 1$.

Доведення теореми можна провести, використовуючи критерій Ейлера. Оскільки a – квадратичний лишок за модулем p, то

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} = 1.$$

Враховуючи, що число p можна подати у вигляді $p = 4m + 3$ для деякого натурального m, то $\frac{p-1}{2} = 2m + 1$. Тобто $a^{\frac{p-1}{2}} = a^{2m+1} \equiv 1 (\text{mod } p)$, $a^{2m+2} \equiv a \pmod{p}$. Візьмемо квадратний корінь лівої та правої частин останньої рівності:

$$a^{m+1} \equiv \pm\sqrt{a} \pmod{p}.$$

Приклад. Обчислити $\sqrt{5}$ та $\sqrt{3}$ в Z_{11}^*.

$p = 11$ – просте, $p \equiv 3 \pmod 4$, $\frac{p+1}{4} = 3$.

$\sqrt{5} : 5^3 \pmod{11} \equiv 4$. $\quad -4 \equiv 7 \pmod{11}$.

Перевірка: $4^2 \pmod{11} \equiv 5$, $7^2 \pmod{11} \equiv 5$.

$\sqrt{3} : 3^3 \pmod{11} \equiv 5$. $\quad -5 \equiv 6 \pmod{11}$.

Перевірка: $5^2 \pmod{11} \equiv 3$, $6^2 \pmod{11} \equiv 3$.

Теорема. Нехай $n = p * q$, де p, q – непарні прості числа. Число $a \in Z_n^*$ є квадратичним лишком за модулем n тоді і тільки тоді, коли a є квадратичним лишком за модулем p та q. Тобто

$a \in Q_n \Leftrightarrow a \in Q_p$ та $a \in Q_q$.

Звідси $|Q_n| = |Q_p| * |Q_q| = (p - 1)(q - 1) / 4$.

Приклад. Нехай $n = 21 = 3 * 7$. $a \in Q_{21} \Leftrightarrow a \in Q_3$ та $a \in Q_7$.

$Q_3 = \{1\}$, поширимо остачі до 21 за модулем 3: {1, 4, 7, 10, 13, 16, 19}.

$Q_7 = \{1, 2, 4\}$, поширимо остачі до 21 за модулем 7: {1, 2, 4, 8, 9, 11, 15,16,18}.

$|Q_{21}| = |Q_3| * |Q_7| = 1 * 3 = 3$. Числа, спільні в двох множинах поширених остач, і є квадратичними лишками за модулем 21.

$Q_{21} = \{1, 4, 16\}$.

2.7 Порядки чисел за модулем

Нехай G скінченна група, і $a \in G$. Послідовність степенів елемента a утворює підгрупу групи G. **Ця підгрупа є скінченною і називається циклічною, а елемент a називається її породжуючим елементом.**

У послідовності степенів елемента a, рано чи пізно, виникнуть рівні елементи: $a^x = a^y$, тобто виникне випадок, коли $a^d = 1, d \neq 0$.

Мінімальне число d із зазначеною властивістю називається порядком елемента a.

Таким чином, у послідовності степенів елемента a лише d елементів різні:

$1, a, a^2, ..., a^{d-1}$. Отже, порядок циклічної підгрупи дорівнює *d*. Очевидно, цей порядок повинен ділити порядок *n* всієї групи. **Таким чином, порядок групи ділиться на порядки її елементів.**

У кільці *Z/mZ* числа, взаємно прості з модулем, утворюють групу за множенням.

Розглянемо степені числа *a* за модулем *m*, де *a* і *m* взаємно прості.

Нехай *m=11*. Лишки степенів числа 2 для показників 0,1,2,…,10 такі: 1,2,4,8,5,10,9,7,3,6,1. Аналогічно, ті ж степені числа 3 порівнянні відповідно з числами 1,3,9,5,4,1,3,9,5,4,1. У кожному випадку є періодичність.

Найменша довжина періоду числа *a* за модулем *m* називається порядком (показником) числа *a* за модулем *m*.

Порядок числа *a* за модулем *m* позначається $ord_m a$**.**

Порядок $d = ord_m a$ **є найменшим позитивним числом, для якого виконується порівняння** $a^d = 1 (m)$.

Порядки чисел за модулем *m* різні. Існують числа, що є порядком одночасно для всіх чисел, взаємно простих з *m* . Одне з них дорівнює значенню **функції Ейлера** $\varphi(m)$**, що визначається як кількість чисел у послідовності** $1, \ldots, m$**, взаємно простих з *m*.**

Функція Ейлера є мультиплікативною: якщо (*a*, *b*) =1, то $\varphi(ab) = \varphi(a)\varphi(b)$ і $\varphi(1) = 1$.

Нехай $m = p_1^a p_2^b \cdots p_s^t$, тоді $\varphi(m) = p_1^{a-1} p_2^{b-1} \cdots p_s^{t-1} (p_1 - 1) \cdots (p_s - 1)$.

Число *g* називається первісним коренем (первісним елементом) за модулем *m*, якщо його порядок за модулем *m* дорівнює $\varphi(m)$**.**

При $m = p$ **первісні корені завжди існують.**

Відомо, що в кожному скінченному полі також існує первісний елемент (генератор поля). Степені первісного елемента *g* представляють усі ненульові елементи поля.

Зокрема, якщо *g* первісний елемент поля *GF*(*p*) , то порівняння $g^x \equiv a \bmod p$ розв'язується для ненульових лишків *a* за модулем *p*.

Показник *x* у цьому порівнянні називається дискретним логарифмом числа *a* за основою *g*. Дискретні логарифми часто називають індексами і позначають $inda$ або $ind_g a$.

Із теореми Ейлера відомо, що якщо (*a*,*m*)=1, то $a^{\varphi(m)} \equiv 1 \bmod m$.

З теореми Ейлера випливає також мала теорема Ферма: $a^{p-1} \equiv 1 \bmod p$, де *p*-просте (*a*, *p*) =1.

Ці теореми інтенсивно використовуються в асиметричній криптографії і, крім того, дуже корисні для скорочення обчислень.

Як наслідок, з теореми Ейлера випливає, що **елемент *g* є первісним коренем за модулем *p* тоді і тільки тоді, коли виконуються співвідношення:** $a^{(p-1)/p} \neq 1 \bmod p$**, де** $p - 1 = \prod_{i=1}^{k} p_i^{a_i}$ **.**

Зауважимо, що **в кожному скінченному полі** F_q**, при** $x \in F_q$**,** $x \neq 0$**, виконується співвідношення** $x^{q-1}=1$**.** Це зв'язано з тим, що число q -1 є порядком мультиплікативної групи поля.

Щоб врахувати значення x = 0, перемножимо обидві частини зазначеного співвідношення на x. Отримаємо, що **для будь-якого елемента** x **кінцевого поля вірне співвідношення** $x^q = x$**.**

Нагадаємо, що розширення скінченного поля може бути представлене як кільце лишків многочленів за модулем незвідного многочлена $f(x)$ над простим полем $h(x) \equiv r(x) \bmod f(x)$.

Для деяких незвідних многочленів послідовність $1, x, x^2 \bmod f(x), \cdots, x^k \bmod f(x), \cdots$ пробігає всі можливі лишки, тобто всі елементи поля. **Такі многочлени називаються примітивними.**

<u>Конгруенції з одним невідомим.</u>

Загальний метод розв'язку лінійних конгруенцій з одним невідомим.

Порівняння виду $ax \equiv b \bmod m$ можуть мати кілька розв'язків, мати єдиний розв'язок або не мати розв'язків взагалі.

Якщо $(a,m) = 1$**, то розв'язок єдиний:** $x \equiv a^{-1} b$**.**

Відзначимо, що якщо модуль і коефіцієнти конгруенції $A \equiv B \bmod m$ розділити або помножити як цілі числа на те саме число, то отримана конгруенція буде істинною.

Це випливає з того, що якщо $A - B$ ділиться на m, а m ділиться на p, то $A - B$ ділиться на p.

Теорема. Розв'язки конгруенції $ax \equiv b \bmod m$ існують тоді і тільки тоді, коли $d = (a,m)$ ділить b.

В цьому випадку, крім вихідного порівняння, розв'язується порівняння виду $\frac{a}{d} x \equiv \frac{b}{d} \bmod \frac{m}{d}$ з єдиним розв'язком x_0.

Очевидно, всі розв'язки вихідного порівняння в діапазоні $0 \le x \le m-1$ є числами виду $x_0 + j\frac{m}{d} \bmod m$**,** $j = 0,1,\ldots,d-1$**.**

Зокрема, якщо m просте, то порівняння $ax \equiv b \bmod m$ має не більше одного розв'язку.

2.8 Китайська теорема про лишки

Розглянемо системи конгруенцій:

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n},$$

де числа m_i - попарно взаємно прості. Тобто, вимагається знайти ціле число x, яке при діленні на m_i дає остачу a_i, якщо НСД$(m_i, m_j) = 1$ при $i \neq j$.

Теорема

Нехай $m_1, m_2, \ldots, m_n$ - попарно взаємно прості числа, тобто НСД(m_i, m_j) = 1 для всіх i і j, менших або рівних n, де $i \neq j$. Тоді система конгруенцій

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

має розв'язок, єдиний по модулю, рівному цілому числу $m_1 m_2 \ldots m_n$. Далі,

$$M_j = \frac{\prod_{i=1}^{n} m_i}{m_j},$$

якщо і z_j - розв'язок конгруенції $M_j z_j \equiv a_j \pmod{m_j}$ для кожного j, тоді розв'язок має вигляд

$$x = \left[\left[\sum_{j=1}^{n} M_j z_j\right]\right]_{m_1 m_2 \ldots m_n}$$

Доведення

Нехай x визначене згідно теореми. Тоді при будь-якому k, $1 \le k \le n$,.

$$x = \left[\left[\sum_{j=1}^{n} M_j z_j\right]\right]_{m_1 m_2 \ldots m_n}$$

отже

$$\begin{aligned} x &\equiv \sum_{j=1}^{n} M_j z_j \left(\mod \prod_{i=1}^{n} m_i\right), \\ &\equiv \sum_{j=1}^{n} M_j z_j \pmod{m_k}, \\ &\equiv M_k z_k \pmod{m_k}, \\ &\equiv a_k \pmod{m_k}, \end{aligned}$$

тому x задовольняє n конгруенціям, $x \equiv a_k \pmod{m_k}$ при $1 \le k \le n$. Якщо x' також задовольняє n конгруенціям, тоді $x - x' \equiv 0 \pmod{m_i}$ при $1 \le i \le n$. Оскільки НСД (m_i, m_i) = 1 при і $\neq$ j, одержуємо

$$x \equiv x' \left(\mod \prod_{i=1}^{n} m_i \right),$$

тобто, розв'язок x єдиний за модулем

$$\prod_{i=1}^{n} m_i$$

Приклад 1

Знайти розв'язки системи конгруенцій

$x \equiv 5 \pmod 4$;

$x \equiv 7 \pmod{11}$.

Оскільки числа 4 і 11 - взаємно прості, існує ціле число, а саме 10 таке, що $(4)(10) \equiv 7 \pmod{11}$, і існує ціле число (а саме 3) таке, що $(11)(3) \equiv 5 \pmod 4$. Отже, $(4)(10) + (11)(3) \equiv 73$, яке конгруентне 29 по модулю 44, задовольняє обом вищенаведеним конгруенціям.

Приклад 2

Знайдемо відповідь на питання про мавп і горіхи, розв'язуючи систему конгруенцій

$$x \equiv 4 \pmod 5;$$
$$x \equiv 3 \pmod 4;$$
$$x \equiv 2 \pmod 7;$$
$$x \equiv 6 \pmod 9.$$

Маємо $M_1 = 4 * 7 * 9 = 252$, $M_2 = 5 * 7 * 9 = 315$, $M_3 = 180$ і $M_4 = 140$. Оскільки числа 5 і 252 - взаємно прості, існує ціле число z_1 таке, що $252\, z_1 \equiv 4 \pmod 5$ або, що те ж саме, $2\, z_1 \equiv 4 \pmod 5$, або $z_1 \equiv 2 \pmod 5$. Отже, z_1 може бути рівне 7. Оскільки числа 4 і 315 - взаємно прості, існує ціле число z_2 таке, що $315\, z_2 \equiv 3 \pmod 4$ або, що те ж саме, $3\, z_2 \equiv 3 \pmod 4$. Отже, z_2 може бути рівне 1.

Приклад 3

Оскільки числа 7 і 180 - взаємно прості, існує ціле число z_3 таке, що $180\, z_3 \equiv 2 \pmod 7$ або, що те ж саме, $5\, z_3 \equiv 2 \pmod 7$. Отже, z_3 може бути рівне 6. Оскільки числа 9 і 140 - взаємно прості, існує ціле число z таке, що $140\, z_4 \equiv 6 \pmod 9$ або, що те ж саме, $5\, z_4 \equiv 6 \pmod 9$. Отже, z_4 може бути рівне 3. Звідси $x = (7)(252)+(1)(315)+(6)(180)+(3)(140) \pmod{5 * 4 * 7 * 9}$ або $x \equiv 3579 \pmod{1260}$ і $x = 1059$ - найменший додатний цілочисельний розв'язок.

Китайську теорему про лишки можна таким чином узагальнити на випадок модулів $m_1, m_2, ..., m_n$, які не є взаємно простими.

Теорема

Система конгруенцій

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

має розв'язок тоді і тільки тоді, коли НСД(m_i, m_j) ділить $a_i - a_j$ при всіх i і j, де $1 \le i \le j \le n$. Якщо розв'язок існує, він єдиний за модулем НСК ($m_1, m_2, ..., m_n$).

Доведення

Для $n = 1$ справедливість теореми очевидна. Покажемо техніку доведення, розглядаючи випадок $n = 2$. Нехай задані конгруенції

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}.$$

Маємо $x = a_1 + k\, m_1$.

Підставляючи це значення у друге рівняння, одержуємо

$a_1 + k\, m_1$ ($a_2 \equiv \mod m_2$) або $k\, m_1 \equiv a_2 - a_1 \mod m_2$).

Оскільки НСД(m_1, m_2) ділить $a_1 - a_2$, існує розв'язок для k, а $x + k\, m_1$ є розв'язком для обох конгруенцій. Оскільки m_1 і m_2 ділять НСК(m_1, m_2), то $x + km_1 +$ НСК(m_1, m_2) також є розв'язком. Якщо як x_1 так і x_2 - розв'язки обох конгруенцій, то $x_1 - x_2$ ділиться як на m_1, так і на m_2, і тому ділиться на НСК(m_1, m_2). Для $n = 1$ справедливість теореми очевидна. Покажемо техніку доведення, розглядаючи випадок $n = 2$. Нехай задані конгруенції

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}.$$

Маємо $x = a_1 + km_1$.

Підставляючи це значення у друге рівняння, одержуємо

$a_1 + km_1 \equiv a_2 \pmod{m_2}$, або $km_1 \equiv (a_2 - a_1) \pmod{m_2}$.

Оскільки НСД (m_1, m_2) ділить $a_1 - a_2$, існує розв'язок для k, а $x + km_1$ є розв'язком для обох конгруенцій. Оскільки m_1 і m_2 ділять НСК(m_1, m_2), то $x + km_1 +$ НСК(m_1, m_2) також є розв'язком. Якщо як x_1, так і x_2 - розв'язки обох конгруенцій, то $x_1 - x_2$ ділиться як на m_1, так і на m_2, і тому ділиться на НСК (m_1, m_2).

Тепер припустимо, що є система конгруенцій

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k},$$
$$x \equiv a_{k+1} \pmod{m_{k+1}}$$

і є значення таке, що $x = a_i \pmod{m_i}$ при $1 \le i \le k$. Тому кожний розв'язок конгруенції $x \equiv a_i \pmod{m_i}$ при $1 \le i \le k$ має вигляд $+ u\, M_k$, де

$M_k =$ НСК($m_1, m_{2,} \cdots, m_k$).

Підставляючи це значення в останню конгруенцію, маємо

$$\overline{x} + uM_k \equiv a_{k+1} (\mathrm{mod}\, m_{k+1}) .$$

Якщо існує розв'язок для u, тоді $+ u M_k$ є розв'язок для всіх $k + 1$ конгруенцій. Розв'язок цієї конгруенції існує, якщо НСД $(M_k, m_{k+1}) \mid (- a_{k+1})$. Але для всіх i

$$\overline{x} - a_{k+1} = \overline{x} - a_i + a_i - a_{k+1}$$

а оскільки $- a_i$ ділиться на m_i і $a_i - a_{k+1}$ ділиться на НСД (m_i, m_{k+1}), то

НСД $(m_i, m_{k+1}) \mid (- a_{k+1})$ для всіх i.

Таким чином, НСД $(M_k, m_{k+1}) \mid (- a_{k+1})$ (Щоб переконатись у цьому, підберіть найвищий степінь простого числа, який ділить M_k і m_{k+1}).

Покажіть, що це число ділить M_k і m_{k+1} для деякого i. Ми показали, що розв'язок існує. Доведіть самостійно єдиність розв'язку по модулю НСК $(m_1, m_2, \cdots, m_n)$.

Приклад

Знайти розв'язок:

$x \equiv 5 \pmod 6$;
$x \equiv 3 \pmod{10}$;
$x \equiv 8 \pmod{15}$.

Розв'язок конгруенції $x \equiv 5 \pmod 6$ має вигляд $5 + 6t$. Підставляючи цю величину в другу конгруенцію, одержуємо $5 + 6t \equiv 3 \pmod{10}$. Тому $6t \equiv 8 \pmod{10}$ і $t \equiv 3 \pmod{10}$. Тому, $t = 3 + 10u$. Підставляючи t у третє рівняння, маємо $3 + 10u \equiv 8 \pmod{10}$. Тому $10u \equiv 5 \pmod{10}$ і $u = 2 \pmod{15}$. Звідси u = $2 + 15v$ для деякого v і $t = 3 + 10 (2 + 15v) = 150v + 23$, а $x = 5 + 6 (150v + 23) = 203 + 6 * 10 * 15v$.

Отже, $x = 203$ є розв'язком.

Властивості функції φ

Нехай $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ - розкладання на прості множники числа n. Кожний додатний дільник числа n або рівний 1, або ділиться на p_i при деякому i, і кожне ціле число, взаємно просте з n, не має жодного з вказаних чисел як дільник. Деякі властивості числа n залежать від кількості цілих чисел s, $1 £ s £ n$, що не містять жодне з p_i як дільник. Наприклад, якщо $n = 40 = 2^3 * 5$, тоді цілі числа s, $1 £ s £ n$ і їх розкладання на множники мають вигляд (див. табл. 2.1):

Кожне з цілих чисел, виділених жирним шрифтом, не ділиться ні на 2, ні на 5 і є числом, взаємно простим з $n = 40$. Кількість чисел s, $1 £ s £ n$, взаємно простих з n, позначається $f(40) = 16$.

Таблиця 2.1

1 = 1	**11 = 11**	**21 = 3 · 7**	**31 = 31**
2 = 2	12 = $2^2 \cdot 3$	22 = 2 · 11	32 = 2^5
3 = 3	**13 = 13**	**23 = 23**	**33 = 3 · 11**
4 = 2^2	14 = 2 · 7	24 = 23 · 3	34 = 2 · 17
5 = 5	15 = 3·5	25 = 5^2	35 = 5 · 7
6 = 2·3	16 = 2^4	26 = 2 · 13	36 = $2^2 \cdot 3^2$
7 = 7	**17 = 17**	**27 = 3^3**	**37 = 37**
8 = 2^3	18 = 2 · 3^2	28 = 2^2 · 7	38 = 2 · 19
9 = 3^2	**19 = 19**	**29 = 29**	**39 = 3 · 13**
10 = 2 · 5	20 = 2^2 · 5	30 = 2 · 3 · 5	40 = 2^3 · 5

Означення

Нехай $f(n)$ - кількість додатних цілих чисел, менших n і взаємно простих з n, тобто $f(n)$ - кількість приведених лишків за модулем n. Функція f називається **тотієнт-функцією Ейлера** або **функцією Ейлера** ***f***.

З наведеної вище таблиці розкладання на множники виходить, що

f(1) = 1; f(5) = 4; f(9) = 6;
f(2) = 1; f(6) = 2; f(10) = 4;
f(3) = 2; f(7) = 6; f(11) = 10;
f(4) = 2; f(8) = 4; f(12) = 4.

Будь-яке додатне ціле число n може бути виражене за допомогою додатних цілих чисел, що не перевищують і взаємно прості з кожним дільником числа n. Наприклад, 6 = 2 * 3 має чотири дільники: 1, 2, 3 і 6. З наведеної вище таблиці виходить, що $f(1) + f(2) + f(3) + f(6) = 1 + 1 + 2 + 2 = 6$.

Теорема Гаусса

Якщо n - додатне ціле число, то $\sum_{d:n} \varphi(d) = n$, де дільники d є додатними дільниками числа n.

Доведення

Нехай d - додатний дільник числа n. Нехай $C(d)$ - множина додатних цілих чисел 1 £ m £ n, для яких НСД(m, n) = d. $C(d)$ і $C(d')$ не перетинаються, якщо $d \neq d'$, оскільки довільне ціле число може мати з числом n тільки один найбільший спільний дільник. Згідно відомої теореми $C(d)$ є також множиною додатних цілих чисел m, 1 £ m £ n, для яких НСД(m/d, n/d) = 1. Але кількість додатних цілих чисел, менших n/d і взаємно простих з n/d, співпадає із значенням функції $f(n/d)$. Оскільки об'єднання цих множин є множина цілих чисел між 1 і n, то $\sum_{d/n} \varphi(n/d) = \sum_{d/n} \varphi(d) = n$ для кожного d, яке ділить n, є відповідне n/d, яке ділить n. Отже $n = \sum_{d/n} \varphi(n/d)$, що і доводить теорему.

Приклад

Нехай n = 12. Дільниками 12 є 1, 2, 3, 4, 6 і 12. Згідно наведеній вище

таблиці значень функції Ейлера f

$f(1) + f(2) + f(3) + f(4) + f(6) + f(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$

Для ілюстрації доведення теореми в окремому випадку $d = 1, 2, 3, 4, 6$ і 12 знаходимо, що відповідні значення n/d рівні, відповідно, $n/d = 12, 6, 4, 3, 2$ і 1, так що дві згадані суми рівні.

Тепер перейдемо до способів обчислення $f(n)$ для будь-якого цілого додатного числа n. Розв'язати вказану задачу допоможуть три наступні теореми.

Теорема

Якщо числа m і n - взаємно прості, то $f(m\,n) = f(m)\,f(n)$.

Доведення

Нехай числа m і n - взаємно прості. Ціле число є взаємно простим з $m\,n$ тоді і тільки тоді, коли воно взаємно просте і з m, і з n. Нехай число a - взаємно просте з m і нехай $a < m$. Розглянемо послідовність $a,\ a + m,\ a + 2\,m,\ \ldots,\ a + (n - 1)\,m$. Ніякі два з цих чисел не конгруентні по модулю n, оскільки, якщо $a + j\,m = a + k\,m \pmod{n}$, то $n \mid (j\,m - k\,m)$. Звідси $n \mid m\,(j - k)$. Оскільки числа m і n - взаємно прості, то $n \mid (j - k)$, що неможливо. Отже, дана послідовність є повною системою лишків за модулем n, і кожен елемент даної послідовності конгруентний за модулем n з цілим додатним числом, меншим n. Отже, кількість цих елементів, взаємно простих з n, рівна $f(n)$. Оскільки існують $f(m)$ таких послідовностей, то існує $f(m)\,f(n)$ чисел, взаємно простих одночасно і з m, і з n, які менше mn і взаємно прості з mn. Тому $f(mn) = f(m)\,f(n)$.

Наприклад, нехай $m = 8$ і $n = 15$. Тоді $f(8) = 4$, оскільки тільки 1, 3, 5 і 7 - додатні цілі числа, які менше 8 і взаємно прості з 8.

Також $f(15) = 8$, оскільки тільки 1, 2, 4, 7, 8, 11, 13 і 14 - додатні цілі числа, які менше 15 і взаємно прості з 15. Отже, $f(120) = f(15)\,f(8) = 32$, що можна перевірити безпосередньо. Відповідно до твердження теореми говорять, що f - мультиплікативна функція щодо взаємно простих множників. Тепер покажемо, як обчислювати $f(n)$, коли n є степенем єдиного простого числа.

Теорема

Якщо p - просте число, то $f(p^k) = p^k - p^{k-1}$.

Доведення

Числа, що не перевищують p^k і що не є взаємно простими з p^k, мають вид $p,\ 2p,\ 3p,\ \ldots,\ (p^{k-1})p$. Оскільки є p^{k-1} таких цілих чисел, то існує $p^k - p^{k-1}$ цілих чисел, взаємно простих з p^k. Отже, $f(p^k) = p^k - p^{k-1}$.

Наслідок 1

Ціле додатне число p є простим тоді і тільки тоді, коли $f(p) = p - 1$.

Доведення

Якщо p - просте число, то з теореми безпосередньо витікає, що $f(p) = p - 1$. З другого боку, якщо число p не є простим, у нього є дільник d, відмінний від p і від 1. Оскільки, за означенням, $f(p) \le p - 1$ і d є одним з $p - 1$ додатних цілих чисел, менших p, маємо $f(p) \le p - 2$, що є суперечність.

Наслідок 2. $f(2k) = 2k - 1$.

На основі властивості мультиплікативності $f(mn) = f(m)\,f(n)$ для взаємно простих чисел m і n в поєднанні із співвідношенням $f(p^k) = p^k - p^{k-1}$ можна для будь-якого цілого додатного числа n одержати явний вираз для $f(n)$, використовуючи розкладання n на прості множники.

Теорема

Якщо n - ціле додатне число з розкладанням на прості множники вигляду

$$n = p_1^{a_1}\, p_2^{a_2} \cdots p_t^{a_t},$$

то

$$\phi(n) = \prod_{t=1}^{t} [p_t^{a_i = t}\,(p_t - 1)] = n \prod_{t=1}^{t} \left(1 - \frac{1}{p_t}\right).$$

Приклад

Оскільки $n = 40 = 2^3 * 5$, $f(40) = 40\,(1 - 1/2)(1 - 1/5) = 40\,(1/2)\,(4/5) = 16$, що співпадає зі значенням, одержаним в одному з прикладів на початку цього розділу. Окрім цього, раніше було показано, що $n = 39616304 = 24 - 72 - 133 - 231$, тому

$$f(9616304) = 2^3\,(2 - 1)\,7^1\,(7 - 1)\,13^2\,(13 - 1)\,23^0\,(23 - 1) =$$

$$= 8 * 1 * 7 * 6 * 169 * 12 * 1 * 22 = 14990976.$$

Існують обмеження, що стосуються кількості цілих чисел s, $1 \pounds s \pounds n$, взаємно простих з n. Один з таких обмежуючих зв'язків встановлює наступна теорема.

Теорема

Якщо є ціле число і більше 2, то $f(n)$ - парне.

Доведення

Якщо $n = 2^k m$, де m - ціле непарне число і $k > 1$, то $f(2^k m) = f(2^k)\,f(m) = 2^{k-1}\,f(m)$ і, отже, $f(n)$ - парне. Якщо $n = p^k m$, де p - непарне просте число і числа p^k і m - взаємно прості, тоді $f(p^k m) = f(p^k)\,f(m) = (p^k - p^{k-1})\,f(m)$. Але $p^k - p^{k-1} = p^{k-1}(p - 1)$ і $p - 1$ - парне число, оскільки p - непарне. Отже, $f(n)$ - парне.

Теорема

Якщо n - ціле число, тоді ненульовий клас приведених лишків утворює групу щодо множення за модулем n.

Доведення

Якщо числа a і b - взаємно прості з n, то число $a\,b$ - також взаємно просте з n, тому наш клас лишків замкнутий щодо множення. Якщо число a - взаємно просте з n, то конгруенція $ax^{o} \equiv 1 \pmod{n}$ має єдиний розв'язок, і, отже, існує величина, зворотна до a.

Нехай число p - просте. Оскільки {1, 2, ..., p - 1} - множина приведених лишків за модулем p, то [1], [2],..., [p - 1] утворюють групу щодо множення. Наступна теорема показує, що добуток [1] * [2] *, …,* [p - 1] всіх ненульових класів лишків завжди є класом лишків [p - 1] = [-1]. На мові конгруентності це еквівалентно твердженню, що 1* 2 *, …, * (p - 1)º ≡ 1 (mod p).

Теорема Уїлсона

Ціле додатне число p є простим тоді і тільки тоді, коли (p - 1)! º ≡ 1 (mod p).

Доведення

Якщо число p - просте, то p º ≡ 0 (mod p) і p - 1º ≡1 (mod p). Коли p - просте, ненульовий клас лишків по модулю p утворює групу щодо множення, так що кожен клас лишків є спареним зі своїм оберненням і дає в добутку [1]. Таким чином, якщо 1 £ u £ p - 1, то існує єдине ціле число u, 1 £ u^{-1} £ p - 1 таке, що $u \cdot u^{-1} \equiv 1 \pmod p$. Маємо $u = u^{-1}$ або $u^1\, u^{-1}$. Для u = 1 маємо u^{-1} = 1, а також $u^2 = u u^{-10} \equiv 1 \pmod p$. Якщо існує ціле число a, 1 < a £ p - 1 таке, що $a^{20} \equiv 1 \pmod p$, то a^2 - 1 = (a - 1)(a + 1)^0 ≡ 0 (mod p) і p | (a - 1)(a + 1). Таким чином, p | (a - 1) або p | (a + 1). Оскільки a – 1¹ = 0 і a < p, одержуємо, що p (a - 1).

Доведення

Таким чином, p | (a + 1), звідки p < a + 1; і оскільки a < p - 1, це має наслідком a + 1 < p. Одержуємо, що p = a + 1 або a = p - 1. Таким чином, для 1 £ u £ p - 1 тільки u = 1 і u = p - 1 володіють такою властивістю, що $u^{2\,0} \equiv 1 \pmod p$. Отже, одержуємо

(p - 1)! = l ($u_1\, u_1^{-1}$)($u_2\, u_2^{-1}$) … ($u_k\, u_k^{-1}$)(p - 1) º 1 · 1 · 1· … · 1 · (p - 1) = p - 1 = -1 (mod p), де u_j - одне з цілих чисел 2, 3, ..., (p - 2), і k = (p - 3) / 2.

Якщо число p не є простим, то p = $r \cdot s$, де 1 < r, s < p. Оскільки (p - 1)! ділиться на r, то (p - 1)! º ≡0 (mod r), так що (p - 1)! º ≡1 (mod r). Тому p повинно бути простим.

Наприклад, нехай p = 5. Тоді (p - 1)! = 4! = 24 º ≡ 1 (mod 5). Звернемо увагу, що в теоремі йде мова про те, що добуток (p - 1)! не може бути конгруентним -1, якщо число p не є простим. За допомогою теореми можна перевіряти простоту числа p, встановлюючи, чи справедлива конгруенція (p - 1)! º ≡1 (mod p). Проте, такий критерій не використовується для великих значень p, оскільки обчислення (p - 1)! (mod p) практично недоцільне.

Тепер розглянемо теорему Уїлсона з точки зору алгебри. Вже відомо, що Z_p - {[0]} утворює групу відносно множення. Тому кожен ненульовий елемент з Z_p має мультиплікативну інверсію - обернений елемент відносно множення. Доведення приведеної вище теореми Уїлсона показує, що тільки [1] і [p - 1] співпадають зі своїми оберненими елементами. Отже, в добутку [1] [2] [3] …

[p - 1] кожен елемент є спареним зі своїм оберненим елементом, так що [1] [2] [3] … [p - 1] = [1] [p - 1] = [p - 1] або, що те ж саме, $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv p \equiv 1 \pmod{p} \equiv 1 \pmod{p}$.

Легко показати, що у циклічній групі парного порядку існують тільки два елементи, які співпадають зі своїми оберненими елементами. Цими елементами у даному випадку є [1] і [p - 1].

Функція f, що розглядається нами, названа на честь Леонарда Ейлера, перу якого належить найбільша кількість математичних праць. Творча спадщина Ейлера могла б скласти більше 75 об'ємних томів. Йому належать відкриття практично у всіх областях математики. Тільки в теорії чисел йому належить більше 140 оригінальних робіт, включаючи доведення цілого ряду малих теорем Ферма. Він вважається основоположником топології, а також цілих розділів математичного аналізу. Багато які з нині існуючих систем математичних позначень введені Ейлером.

2.9 Властивості степеневих конгруенцій

Квадратичною конгруенцією називається конгруенція виду $x^2 \equiv a(n)$ **,** де x - невідомий лишок.

Ціле число a називається квадратичним лишком за модулем n, якщо конгруенція $x^2 \equiv a(n)$ розв'язувана. Якщо конгруенція розв'язувана, то для складеного модуля число розв’язків, як правило, більше двох. Питання про можливість розв'язання квадратичної конгруенції за складеним модулем, факторизація якого невідома, є нерозв’язуваною проблемою.

Очевидно, якщо $x^2 \equiv a(n)$, то a є квадратичним лишком за модулем будь-якого простого дільника числа n. Для модулів, що є простими числами, проблема легко піддається аналізу.

Теорема. Число ненульових квадратичних лишків дорівнює числу квадратичних нелишків.

Нехай p - непарне просте число. Нехай a квадратичний лишок за модулем p. Очевидно, при $a = 0(p)$ існує єдиний розв’язок: $x = 0(p)$.

Усі ненульові лишки за модулем p знаходяться серед чисел $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, отже, їхні квадрати складають список $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ і конгруенція $x^2 \equiv a(p)$ має розв’язок, якщо a належить до цього списку.

Далі, якщо $x^2 \equiv k^2(p)$, то існують два очевидних розв’язки $\pm k$. Крім того, кількість розв’язків не може перевищувати степеня многочлена в лівій частині, тобто двох. Щоб переконатися, що розв’язків саме два, досить показати, що $k \neq -k(p)$. Однак, якщо це не так, то $2k = 0(p)$, що вірно тільки для $k = 0(p)$.

Зауважимо тепер, що в нашому списку квадратичних лишків усі лишки попарно неконгруентні. Дійсно, якщо, наприклад, $a \equiv k^2 \equiv l^2 (p)$ і $1 \le k < l \le \frac{p-1}{2}$, то конгруенція $x^2 \equiv a(p)$ мала б чотири розв'язки: $\pm k$, $\pm l$, що неможливо. Таким чином, кількість ненульових квадратичних розв'язків дорівнює $\frac{p-1}{2}$. Отже, кількість квадратичних нелишків також дорівнює $\frac{p-1}{2}$.

Степеневі конгруенції виду $x^k \equiv a \bmod p$.

Нехай g - первісний елемент простого поля. Тоді існують числа *y* і *b*, такі що $x = g^y$, $a = g^b$, тому $g^{ky} = g^b$.

Оскільки $ord_p g = p-1$, то $ky \equiv b \bmod (p-1)$. Властивості останньої конгруенції цілком характеризують можливість розв'язання вихідного рівняння. Будь-який його розв'язок *y* приводить до розв'язку $x = g^y$ конгруенції $x^k \equiv a \bmod p$. При великих значеннях змінних розв'язуванню задачі перешкоджає необхідність явного виразу числа *a* у виді $a \equiv g^b$.

У загальному випадку розв'язати задачу знаходження *b* обчислювально неможливо (проблема дискретного логарифму).

Відомий наступний результат: нехай p - просте, (*a*,*p*)=1, $h = ord_p a$, тоді порівняння $x^h \equiv 1 \bmod p$ має розв'язків $\varphi(h)$. При $h = \varphi(p)$ отримуємо, що число первісних коренів у полі *GF*(*p*) дорівнює $\varphi(p-1)$.

Умова розв'язуваності степеневої конгруенції.

Покажемо, що розв'язуваність конгруенції $x^n \equiv a(p)$ еквівалентна виконанню умови $a^{(p-1)/d} \equiv 1 \bmod p$, де $d = (n, p-1)$.

Перехід до індексів показує, що $n\,indx \equiv inda \bmod (p-1)$. Необхідна і достатня умова розв'язуваності останньої конгруенції полягає в тому, щоб *inda* ділився на $d = (n, p-1)$, тобто $inda \equiv 0 \bmod d$.

Домножуючи модуль і обидві частини останньої конгруенції на $\frac{p-1}{d}$, отримаємо «рівність показників»: $\frac{p-1}{d} inda \equiv 0 \bmod (p-1)$. Піднесення g у відповідні степені показує, що умова $inda \equiv 0 \bmod d$ еквівалентна умові $a^{(p-1)/d} \equiv 1 \bmod p$.

***Наслідок 1* (критерій Ейлера).** Розв'язуваність конгруенції $x^2 \equiv a (\bmod p)$ еквівалентна виконанню умови $a^{(p-1)/2} \equiv 1 \bmod p$.

***Наслідок 2*.** Нехай g - примітивний елемент поля $GF(p)$. Тоді a квадратичний лишок в тому і тільки в тому випадку, коли в представленні $a = g^j (p)$ число j -парне.

Дійсно, якщо $x^2 \equiv a(p)$, то дискретне логарифмування дає $2y = j(p-1)$, де модуль парний, отже, j ділиться на два.

Первісний корінь у кільці лишків за модулем $m = p^r$.

Відомо, що в кільці Z/p^rZ лишків за модулем $m = p^r$ (яке не є полем) існує первісний елемент γ, степені якого представляють усі лишки, взаємно прості з модулем. Ці лишки утворюють в Z/p^rZ мультиплікативну групу $U(p^r)$ з $\varphi(p^r)$ елементів.

Можна показати, що якщо γ_p - первісний корінь у полі $GF(p)$, то одне з чисел $\gamma = \gamma_p + kp$, де $k \in \{0,1\}$, задовольняє умові $(\gamma_p + kp)^{p-1} \neq 1 (\mathrm{mod}\, p^2)$ і є первісним коренем при будь-якому модулі виду p^α, $\alpha > 1$. Пара чисел a, p, для яких виконується співвідношення $a^{p-1} = 1 \bmod p^2$, зустрічаються рідко. Тому у багатьох випадках первісний корінь за модулем p є одночасно первісним елементом для всіх кілець Z/p^rZ.

Простий вид первісного кореня в кільці лишків за модулем $m = p^r$ дозволяє звести розв'язування порівняння виду $f(x) \equiv 0 \bmod n$ до розв'язування порівняннь за дільниками n виду p^r. Виявляється, якщо відомі розв'язки за модулем p, то розв'язки за модулем p^r знайти досить просто. Остаточні розв'язки (за модулем n) знаходяться з допомогою китайської теореми про залишки.

Важлива теорема.

Можна показати, що для многочлена від однієї змінної з коефіцієнтами з $GF(p)$ кількість коренів, що належать $GF(p)$, не перевищує степеня многочлена.

Квадратичний закон взаємності Гаусса. Символи Лежандра і Якобі. Означення і властивості символу Лежандра.

Існують алгоритми для визначення, чи є дане число квадратичним лишком за простим модулем, чи ні. Один з алгоритмів пов'язаний з обчисленням значення символу Лежандра, який для непарного простого p визначається так:

$$\left(\frac{a}{p}\right) = 0, a \equiv 0 \bmod p;\ \ 1, \exists x:\ x^2 \equiv a \bmod p\ a \neq 0 \bmod p;\ \ -1, \neg\exists x:\ x^2 \equiv a \bmod p\ a \neq 0 \bmod p.$$

Значення $\left(\frac{a}{p}\right)$ називається квадратичним характером числа a за простим модулем p.

Основні властивості символу Лежандра.

$$a_1 = a(p) \Rightarrow \left(\frac{a_1}{p}\right) = \left(\frac{a}{p}\right);$$

Критерій Ейлера: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p;$

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right);$$

$$(a,p)=1\Rightarrow\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right);$$

$$\left(\frac{1}{p}\right)=1,\ \left(\frac{-1}{p}\right)=(-1)^{(p-1)/2};$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Квадратичний закон взаємності Гаусса: для будь-яких простих непарних чисел p і q виконується рівність $\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$. Символ Лежандра $\left(\frac{a}{p}\right)$ можна обчислити за допомогою наступної послідовності дій.

1. Якщо $a<0$, то виділяємо співмножник $\left(\frac{-1}{p}\right)$;

2. Приводимо a за модулем p;

3. Розкладаємо a в добуток степенів простих чисел, використовуючи мультиплікативність символу Лежандра: $\left(\frac{a}{p}\right)=\left(\frac{p_1}{p}\right)^{a_1}\ldots\left(\frac{p_k}{p}\right)^{a_t}$, потім видаляємо співмножники, які є квадратами;

4. Виділяємо двійки, наприклад, якщо $p_1=2$, обчислюємо $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$;

5. Для кожного непарного співмножника p_i застосовуємо квадратичний закон взаємності (зменшуємо величини чисел, що беруть участь в обчисленнях);

6. При необхідності переходимо до п.**1**.

Приклад. $\left(\frac{126}{53}\right)=\left(\frac{20}{53}\right)=\left(\frac{2}{53}\right)^2\left(\frac{5}{53}\right)=(-1)^{26\cdot2}\left(\frac{53}{5}\right)=\left(\frac{-2}{5}\right)=(-1)^2(-1)^3=-1$

При використанні комп'ютерів звичайно застосовується критерій Ейлера.

Визначення і властивості символу Якобі

Існує алгоритм, що обчислює символ Якобі, який дозволяє, принаймні, вирішити питання, чи є число x квадратичним лишком за непарним модулем без його факторизації.

Нехай n непарне і має наступний канонічний розклад: $n=\prod_{i=1}^{k}p_i^{a_i}$.

Символ Якобі числа x за модулем n, при $(x,n)=1$, визначається як добуток значень символів Лежандра $\left(\frac{x}{n}\right)=\left(\frac{x}{p_1}\right)^{a_1}\ldots\left(\frac{x}{p_k}\right)^{a_t}$.

Символ Якобі має практично всі ті ж властивості, що і символ Лежандра, але за значенням символу Якобі, рівному одиниці, не можна стверджувати, що відповідний лишок – квадратичний.

Для квадратичного лишку символ Якобі, проте, дорівнює одиниці. Отже, коли $\left(\frac{x}{n}\right)=-1$, то x - квадратичний нелишок за модулем n.

Нехай x, x_1, x_2 - цілі, n, n_1, n_2 - непарні числа, більші одиниці.

Властивості символу Якобі.

$x_1 = x_2 (n) \Rightarrow \left(\frac{x_1}{n}\right)=\left(\frac{x_2}{n}\right)$;

$\left(\frac{x_1 x_2}{n}\right)=\left(\frac{x_1}{n}\right)\left(\frac{x_2}{n}\right)$;

$(x_2, n)=1 \Rightarrow \left(\frac{x_2{}^2 x_1}{n}\right)=\left(\frac{x_1}{n}\right)$;

$\left(\frac{1}{n}\right)=1,\ \left(\frac{-1}{n}\right)=(-1)^{(n-1)/2}$;

$\left(\frac{x}{n_1 n_2}\right)=\left(\frac{x}{n_1}\right)\left(\frac{x}{n_2}\right)$;

$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$.

Квадратичний закон взаємності Гаусса. Для будь-яких взаємно простих непарних чисел m і n виконується рівність $\left(\frac{m}{n}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}\left(\frac{n}{m}\right)$.

Приклад. Обчислимо символ Якобі $\left(\frac{12}{35}\right)$.

$$\left(\frac{12}{35}\right)=\left(\frac{2^2\cdot 3}{35}\right)=\left(\frac{35}{3}\right)(-1)^{\frac{(35-1)(3-1)}{4}}=-\left(\frac{2}{3}\right)=-(-1)^{\frac{3\cdot 3-1}{8}}=1\ .$$

<u>Алгоритм знаходження квадратного кореня в простому полі.</u>

Даний алгоритм призначений для розв'язання відносно y порівняння виду $x=y^2(p)$ за простим модулем $p>2$. Перед тим як приступити до обчислень, необхідно переконатися в наявності розв'язків конгруенції, тобто в тому, що $\left(\frac{x}{p}\right)=1$

Алгоритм розбивається на 3 випадки, в залежності від представлення p у виді $p=4k+3$, $p=8k+5$, $p=8k+1$. В алгоритмі істотно використовується критерій Ейлера, який для розв'язуваного порівняння дає: $\left(\frac{x}{p}\right)\equiv x^{(p-1)/2}\equiv 1 \bmod p$.

Випадок $p=4k+3$. Маємо $1=\left(\frac{x}{p}\right)\equiv x^{(p-1)/2}\equiv x^{2k+1} \bmod p$. Помножимо на x ліву і праву частину порівняння, отримаємо: $x\equiv x^{2k+2} \bmod p$. Показник праворуч парний, отже, одне з рішень $y\equiv x^{k+1} \bmod p$. Оскільки рішень не може бути більше двох, то остаточна відповідь: $y\equiv \pm x^{k+1} \bmod p$.

Випадок $p = 8k + 5$. Оскільки $1 = \left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \equiv x^{4k+2} \bmod p$, то $x^{2k+1} \equiv \pm 1 \bmod p$.

Таким чином, вірно одне з двох співвідношень $x^{2k+2} \equiv \pm x \bmod p$. Оскільки x і k відомі, то можна перевірити, яке із співвідношень виконується. Таким чином, можливі наступні два підвипадки. Якщо вірно $x^{2k+2} \equiv x \bmod p$, то, очевидно, $y \equiv \pm x^{k+1} \bmod p$. Інакше, $x^{2k+2} \equiv -x \bmod p$.

Якщо обидві частини останньої конгруенції помножити на число у відомому парному степені, то квадратний корінь з його лівої частини легко записати явно. Ми підберемо зазначений множник так, щоб, крім того, змінився знак у правої частини конгруенції.

Таким множником може бути число $2^{4k+2} = 2^{(p-1)/2} = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1(p)$, оскільки $p^2 - 1 = (8k)^2 + 80k + 24$. Отже, $y \equiv \pm 2^{2k+1} \cdot x^{k+1} \bmod p$.

Випадок $p = 8k + 1$. Насамперед, для роботи алгоритму необхідна наявність (довільного) квадратичного нелишку a за модулем p. Щоб його знайти, приходиться вибирати навмання число, скажемо, a і перевіряти співвідношення $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv -1 \bmod p$.

Уточнимо вигляд числа p: $p = 8k + 1 = 2^l h + 1$, де h - непарне, очевидно, $l \geq 3$. Основна ідея алгоритму – побудувати співвідношення виду $x^h \cdot a^{2m} = 1 \bmod p$.

У випадку успіху досить перемножити обидві частини порівняння на x і витягти корінь з обох частин (враховуючи, що число $h+1$ парне). Тому, виходячи з порівняння $x^{p-1} = 1(p)$, ми будемо будувати співвідношення, у яких показник при x буде знижуватися вдвічі, поки не стане рівним h. Ділення показників на двійки - це послідовне здобуття квадратних коренів з одиниці. На кожному кроці може з'явитися лише один із коренів: 1 або (-1). При цьому в нас буде досить даних, щоб з'ясувати, який випадок реально має місце. Змінювати знак у (-1) ми будемо за допомогою множення частин порівняння на степені числа a, причому так, щоб показник степеня в добутку таких додаткових множників завжди залишався парним.

Опис алгоритму знаходження квадратного кореня у простому полі.

Очевидно, $1 = x^{p-1} = x^{2^l h}(p)$. Оскільки x квадратичний лишок, то $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \equiv 1(p)$ і ми можемо знизити показник у два рази: $x^{2^{l-1} h} = 1(p)$.

Після другого ділення показника на два в правій частині вийде ± 1. Ми можемо вибрати істинний варіант, обчислюючи ліву частину порівняння безпосередньо.

Якщо в правій частині виходить 1, то рухаємося далі. Зауважимо, що (-1) в правій частині може з'явитися не раніше чим на другому кроці, тобто при показнику $2^{l-2} h$ і нижче. Припустимо, що в правій частині при зазначеному показнику вийшла (-1): $x^{2^{l-2} h} = -1(p)$. Оскільки a - квадратичний нелишок, то

$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv a^{2^{l-1}h} \equiv -1(p)$ і, крім того, показник при a більше показника при x. Помножимо обидві частини порівняння $x^{2^{l-2}h} = -1(p)$ на $a^{2^{l-1}h} \equiv -1(p)$, отримаємо $x^{2^{l-2}h} a^{2^{l-1}h} = 1(p)$.

З лівої частини порівняння легко витягнути квадратний корінь, тобто $x^{2^{l-3}h} a^{2^{l-2}h} = \pm 1(p)$.

Як і раніше, просто з'ясувати, який з варіантів має місце насправді і, при необхідності, помножити порівняння на $a^{2^{l-1}h} \equiv -1(p)$ і т.д., поки показник при x не виявиться рівним h. Після останнього кроку показник при a буде відомим і парним, як сума парних чисел. В результаті, виникає порівняння виду $x^h \cdot a^{2m} \equiv 1 \bmod p$, звідки, помноживши обидві частини на x, одержимо: $y = \pm x^{h+1/2} a^m \bmod p$.

Приклад. Розв'язати конгруенцію $y^2 = 8(41)$.

З'ясовуємо, насамперед, чи є конгруенція розв'язуваною. Це дійсно так, оскільки $\left(\frac{8}{41}\right) = \left(\frac{2}{41}\right)^3 = \left(\frac{2}{41}\right) = (-1)^{\frac{41 \cdot 41 - 1}{8}} = (-1)^{5 \cdot 42} = 1$.

Далі з'ясовуємо, який з трьох випадків представлення p має місце. Очевидно, має місце випадок $p = 8k + 1$. Записавши $p = 2^3 \cdot 5 + 1$, отримаємо $h = 5$, $l = 3$.

Знайдемо квадратичний нелишок за модулем 41. Можна вибрати $a = 3$, оскільки $\left(\frac{3}{41}\right) = 3^{\frac{41-1}{2}} = 3^4 = -1(41)$. Приступимо до знаходження кореня, враховуючи, що $3^{20} = -1(41)$.

З теореми Ейлера маємо $8^{p-1} = 8^{8 \cdot 5} = 1(41)$. Розділимо показник на два. При цьому значення кореня дорівнює 1, тому що 8 - квадратичний нелишок і $8^{4 \cdot 5} = 8^{\frac{p-1}{2}} = 1(41)$.

Показник можна знову розділити на два. Отже, $8^{2 \cdot 5} = \pm 1(41)$. Оскільки $8^5 = 9(41)$, то $8^{2 \cdot 5} = 81 = -1(41)$. Необхідно домогтися значення 1 у правій частині рівняння. Помножимо обидві частин на 3^{20}, одержимо $8^{2 \cdot 5} 3^{20} = 1(41)$. Як слід було очікувати, показник при трійці парний.

Нам залишився один крок, щоб знизити показник при вісімці до $h = 5$. Ділимо показники на два й обчислюємо значення лівої частини: $8^5 3^{10} = \pm 1(41)$, $8^5 3^8 3^2 = 9\left(3^4\right)^2 3^2 = 9(-1)^2 9 = -1(41)$, тобто $8^5 3^{10} = -1(41)$. Нам знову необхідно помножити обидві частини рівняння на 3^{20}, що дає $8^5 3^{10} 3^{20} = 1(41)$. Показник при 8 дорівнює $h = 5$. В останньому рівнянні, помноживши обидві частини рівняння на 8, одержимо $8^6 3^{30} = 8(41)$, що дозволяє записати квадратний корінь з 8 у виді $y = \pm 8^3 3^{15} = \pm 7(41)$. Перевірка: $(\pm 7)^2 = 49 = 8(41)$.

3 Дискретні логарифми

Проблема обчислення дискретного логарифму є не лише цікавою, а й вкрай корисною для систем захисту інформації. Ефективний алгоритм знаходження дискретного логарифму значною мірою знизив би безпеку систем ідентифікації користувача та схеми обміну ключей.

Означення. Нехай G – скінченна циклічна група порядка n. Нехай g – генератор G та $b \in G$. ***Дискретним логарифмом*** числа b за основою g називається таке число x ($0 \le x \le n - 1$), що $g^x = b$ та позначається $x = \log_g b$.

Проблема дискретного логарифму. Нехай p – просте число, g – генератор множини Z_p^*, $y \in Z_p^*$. Знайти таке значення x ($0 \le x \le p - 2$), що $g^x \equiv y \pmod p$. Число x називається ***дискретним логарифмом*** числа y за основою g та модулем p.

Узагальнена проблема дискретного логарифму. Нехай G – скінченна циклічна група порядка n, g – її генератор, $b \in G$. Необхідно знайти таке число x ($0 \le x \le n - 1$), що $g^x = b$.

Розширенням узагальненої проблеми може стати задача розв'язку рівняння $g^x = b$, коли знято умову циклічності групи G, а також умову того, що g – генератор G (в такому випадку рівняння може і не мати розв'язку).

Приклад. $g = 3$ є генератором Z_7*: $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$.

$\log_3 4 = 4 \pmod 7$, тому що розв'язком рівняння $3^x = 4$ буде x = 4.

Теорема. Нехай a – генератор скінченної циклічної групи G порядка n. Якщо існує алгоритм, який обчислює дискретний логарифм за основою a, то цей алгоритм може також обчислити дискретний логарифм за будь-якою основою b, яка є генератором G.

Доведення. Нехай $k \in G$, $x = \log_a k$, y = $\log_b k$, z = $\log_a b$. Тоді $a^x = b^y = (a^z)^y$, звідки $x = zy \bmod n$. Підставимо в останню рівність замість змінних логарифмічні вирази:

$$\log_a k = (\log_a b)\,(\log_b k) \bmod n$$

або

$$\log_b k = (\log_a k)\,(\log_a b)^{-1} \bmod n.$$

З останньої рівності випливає справедливість теореми.

Примітивний алгоритм

Для знаходження $\log_g b$ (g – генератор G порядка n, $b \in G$) будемо обчислювати значення g, g^2, g^3, g^4, ... поки не отримаємо b. Часова оцінка алгоритму – O(n). Якщо n – велике число, то час обчислення логарифму є достатньо великим і тому алгоритм є неефективним.

Алгоритм великого та малого кроку

Першим детермінованим алгоритмом для обчислення дискретного логарифму був алгоритм великого та малого кроку, запропонований Шанком (Shank).

Для обчислення $\log_g b$ в групі Z_n^* необхідно зробити наступні кроки:

1. Обчислити $a = \lceil \sqrt{n} \rceil$;

2. Побудувати список $L_1 = 1, g^a, g^{2a}, ..., g^{a^2}$ (за модулем n);

3. Побудувати список $L_2 = b, bg, bg^2, ..., bg^{a-1}$ (за модулем n);

4. Знайти число z, яке зустрілося в L_1 та L_2.

Тоді $z = bg^k = g^{la}$ для деяких k та l. Звідси $b = g^{la-k} = g^x$; $x = la - k$.

Два питання постають при дослідженні роботи наведеного алгоритму:

1. Чи завжди знайдеться число, яке буде присутнім в обох списках?

2. Як ефективно знайти значення z?

Запишемо $x = sa + t$ для деяких s, t таких, що $0 \le s, t < a$. Тоді $b = g^x = g^{sa+t}$. Домножимо рівність на g^{a-t}, отримаємо: $bg^{a-t} = g^{s(a+1)}$. Значення зліва обов'язково зустрінеться в L_2, а справа – в L_1.

Відсортуємо отримані списки L_1 та L_2 за час $O(a * \log a)$. За лінійний час проглядаємо списки зліва направо, порівнюючи їх голови: якщо вони рівні, то значення z знайдене, якщо ні – то видалити менше число і продовжити перевірку.

Приклад. Розв'язати порівняння: $2^x \equiv 11 \pmod{13}$.

$a = \lceil \sqrt{13} \rceil = 4$;

L_1: $1, 2^4 \equiv 3, 2^8 \equiv 9, 2^{12} \equiv 1, 2^{16} \equiv 3$;

L_2: $11, 11 * 2 \equiv 9, 11 * 2^2 \equiv 5, 11 * 2^3 \equiv 10$;

Число 9 зустрілося в обох списках. $11 * 2 \equiv 2^8$, $11 \equiv 2^7$, звідки $x = 7$.

Відповідь: $x = 7$.

Інший підхід до реалізації алгоритму великого та малого кроку можна отримати, якщо рівність $b = g^{sa+t}$ ($a = \lceil \sqrt{n} \rceil$, $0 \le s, t < a$) переписати у вигляді $b * (g^{-a})^s = g^t$. Обчислимо g^{-a} та складемо таблицю значень g^t, $0 \le t < a$. Далі починаємо знаходити значення $b * (g^{-a})^s$, $s = 0, 1, \ldots$ перевіряючи їх наявність у таблиці g^t. Як тільки знаходяться такі s та t, алгоритм зупиняється.

Приклад. Обчислити $\log_2 3$ в групі Z_{19}^*.

$3 = 2^x = 2^{sa+1}$, $3 * (2^{-a})^s = 2^t$. Складемо таблицю 2^t, $0 \le t < \lceil \sqrt{19} \rceil = 5$:

t	0	1	2	3	4
2^t	1	2	4	8	16

$2^{-1} \equiv 10 \pmod{19}$, оскільки $2 * 10 \equiv 1 \pmod{19}$.

Тоді $3 * (2^{-5})^s \pmod{19} \equiv 3 * (10^5)^s \pmod{19} \equiv 3 * 3^s \pmod{19}$

Обчислюємо $3 * 3^s$, $s = 0, 1, \ldots$:

s	0	1	2
$3 * 3^s$	3	9	8

Значення 8, яке отримали при $s = 2$, присутнє в таблиці 2^t, $0 \le t < 5$.

Звідси $3 * (2^{-5})^2 = 2^3$ або $3 = (2^5)^2 * 2^3 = 2^{5*2+3} = 2^{13}$.

Відповідь: $3 = 2^{13}$, тобто $\log_2 3 = 13$.

Алгоритм Поллард - ро

Нехай G – циклічна група з порядком n (n – просте). Розіб'ємо елементи групи G на три підмножини S_1, S_2 та S_3, які мають приблизно однакову потужність. При цьому необхідно виконання умови: $1 \notin S_2$. Визначимо послідовність елементів x_i наступним чином:

$$x_0 = 1,\ x_{i+1} = \begin{cases} b \cdot x_i, x_i \in S_1 \\ x_i^2, x_i \in S_2 \\ a \cdot x_i, x_i \in S_3 \end{cases}, \quad i \geq 0. \qquad (3.1)$$

Ця послідовність у свою чергу утворить дві послідовності c_i та d_i , що задовольняють умові

$$x_i = a^{c_i} b^{d_i}$$

та визначаються наступним чином:

$$c_0 = 0,\ c_{i+1} = \begin{cases} c_i, x_i \in S_1 \\ (2 \cdot c_i) \bmod n, x_i \in S_2 \\ (c_i + 1) \bmod n, x_i \in S_3 \end{cases}, i \geq 0 \qquad (3.2)$$

та

$$d_0 = 0,\ d_{i+1} = \begin{cases} (d_i + 1) \bmod n, x_i \in S_1 \\ (2 \cdot d_i) \bmod n, x_i \in S_2 \\ d_i, x_i \in S_3 \end{cases}, i \geq 0. \qquad (3.3)$$

Алгоритм буде працювати циклічно, шукаючи таке знчення i, для якого $x_i = x_{2i}$. Для таких значень будуть мати місце рівність $a^{c_i} b^{d_i} = a^{c_{2i}} b^{d_{2i}}$ або $b^{d_i - d_{2i}} = a^{c_{2i} - c_i}$. Логарифмуючи останню рівність за основою a, матимемо:

$$(d_i - d_{2i}) * \log_a b \equiv (c_{2i} - c_i) \bmod n .$$

Якщо $d_i \neq d_{2i} \pmod n$, то це рівняння може бути ефективно розв'язано для обчислення $\log_a b$.

Алгоритм

Вхід: генератор a циклічної групи G з порядком n та елемент $b \in G$.

Вихід: дискретний логарифм $x = \log_a b$.

1. $x_0 \leftarrow 1,\ c_0 \leftarrow 0,\ d_0 \leftarrow 0$.
2. for $i = 1, 2, \ldots d_0$
   2.1. За значеннями x_{i-1}, c_{i-1}, d_{i-1} та x_{2i-2}, c_{2i-2}, d_{2i-2} обчислити значення x_i, c_i, d_i та x_{2i}, c_{2i}, d_{2i} , використовуючи формули (3.1), (3.2), (3.3).
   2.2. if ($x_i = x_{2i}$) then
   $r \leftarrow (d_i - d_{2i}) \bmod n$;
   if ($r = 0$) then return (FALSE); // розв'язку не знайдено

$x \leftarrow r^{-1} (c_i - c_{2i}) \bmod n$.
return (x).

Якщо алгоритм завершується невдачею (повертає FALSE), то можна запустити його, вибравши інші початкові значення c_0, d_0 з інтервалу [1; n - 1] та поклавши $x_0 = a^{c_0} b^{d_0}$.

Приклад. Обчислити $\log_2 9$ в групі Z_{19}^*.

Побудуємо наступну таблицю значень послідовностей x_i, c_i, d_i:

i	x_i	a_i	b_i	x_{2i}	a_{2i}	b_{2i}
1	9	0	1	18	1	1
2	18	1	1	4	4	2
3	17	2	1	4	8	6
4	4	4	2	4	16	14
5	17	4	3	4	32	30
6	4	8	6	4	64	62

На 6 кроці отримали $x_6 = x_{12}$. Підставивши їх значення, отримаємо:

$$2^8 * 9^6 = 2^{64} * 9^{62} \text{ або } 2^{8-64} = 9^{62-6}, \; 2^{-56} = 9^{56}.$$

Логарифмуємо рівність: $-56 * \log_2 9 = 56 \pmod{18}$, оскільки $|Z_{19}^*| = 18$.

Враховуючи, що $-56 \pmod{18} \equiv 16$, $56 \pmod{18} \equiv 2$, перепишемо рівність у вигляді $16 * \log_2 9 = 2 \pmod{18}$ або $8 * \log_2 9 = 1 \pmod 9$. $\log_2 9 = 8^{-1} \pmod 9 = 8$.

Відповідь: $\log_2 9 = 8$.

Індексний алгоритм

Алгоритм, що базується на обчисленні індексів, є найпотужнішим при обчисленні дискретного логарифму. Необхідно побудувати відносно невелику підмножину S елементів групи G, яка називається ***множниковою основою***. Ця підмножина повинна обиратися таким чином, щоб як можна більша частина елементів G могла бути представлена у вигляді добутку її елементів. При обчисленні значення $\log_a b$ (a – генератор G, $b \in G$) спочатку обчислюються значення логарифмів елементів з S (які заносяться в тимчасову базу даних), а потім на їх основі обчислюється логарифм числа b.

Алгоритм

Вхід: генератор a циклічної групи G порядка n та елемент $b \in G$.

Вихід: дискретний логарифм $x = \log_a b$.

1. Побудувати множину S – множникову основу. Нехай $S = \{p_1, p_2, \ldots, p_t\}$. В якості значень p_i можна обрати, наприклад, i - те просте число.

2. Побудувати систему лінійних рівнянь, розв'язком якої будуть значення $\log_a p_i$. Для цього виконаємо наступні кроки:

2.1. Обрати деяке ціле k, $0 \le k \le n - 1$ та обчислити a^k .

2.2. Спробувати представити значення a^k у вигляді добутку чисел з S:

$$a^k = \prod_{i=1}^{t} p_i^{c_i}\ ,\ \mathrm{c_i} \geq 0.$$

Якщо така рівність знайдена, то записати рівняння:

$$k = \sum_{i=1}^{t} c_i \log_a p_i \pmod{n}.$$

2.3. Повторювати кроки 2.1 та 2.2, поки не отримаємо $t + c$ лінійних рівнянь. Невелике ціле число c ($1 \leq c \leq 10$) обирається таким чином, щоб складена система рівнянь мала єдиний розв'язок з великою ймовірністю (якщо скласти лише t рівнянь з t невідомими, то з великою ймовірністю два з цих рівнянь будуть залежними і тоді система буде мати більше одного розв'язку).

3. Розв'язати утворену систему рівнянь, отримати значення $\log_a p_i$, $1 \leq i \leq t$.

4. Обчислення $\log_a b$.

4.1. Обрати деяке ціле k, $0 \leq k \leq n - 1$ та обчислити $b * a^k$.

4.2. Спробувати представити значення $b * a^k$ у вигляді добутку чисел з S:

$$b * a^{\mathrm{k}} = \prod_{i=1}^{t} p_i^{d_i}\ ,\ d_i \geq 0.$$

Якщо такого представлення знайти не вдається, виконати знову 2.1. Інакше, прологарифмувавши останню рівність, отримаємо:

$$x = \log_a b = (\sum_{i=1}^{t} d_i \log_a p_i - k) \bmod n.$$

Приклад. Обчислити $\log_2 12$ в групі Z_{19}^*.

1. Нехай $S = \{2, 3, 5\}$ – множникова основа.

2. Будуємо систему рівнянь для знаходження значень $\log_2 p_i$, де $p_i \in S$. Оскільки множина S містить 3 елементи, то достатньо отримати 3 лінійно незалежні рівняння.

$k = 5$: $2^5 \pmod{19} \equiv 13$ – не представимо у вигляді добутку чисел з S.

$k = 7$: $2^7 \pmod{19} \equiv 14$ – не представимо у вигляді добутку чисел з S.

$k = 2$: $2^2 \pmod{19} \equiv 4 = 2^2$. Перше рівняння: $2 = 2\log_2 2$.

$k = 10$: $2^{10} \pmod{19} \equiv 17$ – не представимо у вигляді добутку чисел з S.

$k = 15$: $2^{15} \pmod{19} \equiv 12 = 2^2 * 3$. Друге рівняння: $15 = 2\log_2 2 + \log_2 3$.

$k = 11$: $2^{11} \pmod{19} \equiv 15 = 3 * 5$. Третє рівняння: $11 = \log_2 3 + \log_2 5$.

3. Система рівнянь за модулем 18 (порядок Z_{19}^* дорівнює 18) має вигляд:

$$\begin{cases} 2 = 2\log_2 2 \pmod{18} \\ 15 = 2\log_2 2 + \log_2 3 \pmod{18} \\ 11 = \log_2 3 + \log_2 5 \pmod{18} \end{cases}.$$

Її розв'язком буде:

$$\log_2 2 = 1,\ \log_2 3 = 13,\ \log_2 5 = 16.$$

4. Обчислення $\log_2 12$.

$k = 3$: $12 * 2^3 \pmod{19} \equiv 1$ – не представимо у вигляді добутку чисел з S.

$k = 7$: $12 * 2^7 \pmod{19} \equiv 16 = 2^4$.

$\log_2 12 + 7 \equiv 4\log_2 2 \pmod{18}$, $\log_2 12 \equiv (4\log_2 2 - 7) \pmod{18} = 15$.

Відповідь: $\log_2 12 = 15$.

Алгоритм Поліга – Хеллмана

Алгоритм Поліга – Хеллмана ефективно розв'язує задачу дискретного логарифму в групі G порядка n, якщо число n має лише малі прості дільники.

Нехай $g, h \in G$, $|G| = p^s$, p – просте. Тоді значення $x = \log_g h$ можна подати у вигляді:

$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{s-1} p^{s-1}$$

Піднесемо рівняння $h = g^x$ до степеня p^{s-1}:

$$h^{p^{s-1}} = \left(g^{p^{s-1}}\right)^x = \left(g^{p^{s-1}}\right)^{x_0 + x_1 p + x_2 p^2 + \ldots + x_{s-1} p^{s-1}} =$$

$$\left(g^{p^{s-1}}\right)^{x_0} * \left(g^{p^s}\right)^{x_1} * \left(g^{p^s}\right)^{p x_2} * \ldots * \left(g^{p^s}\right)^{p^{s-2} x_{s-1}} = \left(g^{p^{s-1}}\right)^{x_0},$$

оскільки $g^{p^s} = 1$ (g – генератор групи, p^s – її порядок).

Таким чином, з рівності $h^{p^{s-1}} = \left(g^{p^{s-1}}\right)^{x_0}$ знаходимо x_0.

Далі, маючи значення $x_0, x_1, \ldots, x_{i-1}$, можна обчислити x_i з рівняння

$$\left(h \cdot g^{-\sum_{j=0}^{i-1} x_j p^j}\right)^{p^{s-(i+1)}} = \left(g^{p^{s-1}}\right)^{x_i}. \qquad (3.4)$$

Приклад. Обчислити $\log_3 7$ в Z_{17}^*.

Необхідно розв'язати рівняння $3^x = 7$ в групі, порядок якої дорівнює $16 = 2^4$.

Представимо x у двійковій системі числення: $x = x_0 + 2x_1 + 4x_2 + 8x_3$.

1. Обчислення x_0.

Піднесемо рівняння $3^x = 7$ до степеня $2^3 = 8$:

$$3^{8(x_0 + 2x_1 + 4x_2 + 8x_3)} = 7^8,\ 3^{8x_0 + 16x_1 + 32x_2 + 64x_3} = -1,$$

$$3^{8x_0} * (3^{16})^{x_1} * (3^{16})^{2x_2} * (3^{16})^{4x_3} = -1.$$

Оскільки $3^{16} \pmod{17} \equiv 1$, то останнє рівняння прийме вигляд $3^{8x_0} = -1$.

Враховуючи, що $3^8 \pmod{17} \equiv -1$, маємо: $(-1)^{x_0} = -1$, $x_0 = 1$.

2. Обчислення x_1.

Домножимо рівність $3^{x_0 + 2x_1 + 4x_2 + 8x_3} = 7$ на $3^{-x_0} = 3^{-1} \pmod{17} = 6$, отримаємо:

$3^{2x_1 + 4x_2 + 8x_3} = 7 * 6$ або $3^{2x_1 + 4x_2 + 8x_3} = 8$.

Піднесемо рівняння до степеня 4: $3^{8x_1 + 16x_2 + 32x_3} = 8^4$, $3^{8x_1} = -1$, $x_1 = 1$.

3. Обчислення x_2.

Обчислення x_2 згідно (3.4).

4 Тести на простоту

Проблема належності заданого натурального числа до класу простих чи складених чисел є дуже цікавою не тільки в математиці, а й в комп'ютерних науках. Відрізнити просте число від складеного, а також розкласти останнє на прості множники є однією з найважливіших задач арифметики. Пошук великих простих чисел необхідний, наприклад, для забезпечення надійності систем кодування інформації з відкритим ключем. Безпека останніх базується на твердженні, що операція множення двох великих простих чисел є односторонньою функцією.

Для перевірки числа на простоту користуються ймовірнісними (Ферма, Соловея – Штрассена, Мілера - Рабіна) та правдивими тестами.

4.1 Ймовірнісні тести

Означення. Тест на простоту називається ***ймовірнісним***, якщо в результаті його застосування не можна дати чіткої відповіді на запитання "чи є задане число простим, чи ні?", але можна виявити часткову інформацію стосовно простоти.

Наведені нижче тести дають наступну інформацію про непарне ціле число n:

- Якщо тест визначає, що n є складним, то це дійсно так.
- Якщо тест визначає, що n є простим, то з ймовірністю, близькою до 1, можна вважати, що число є простим.

Тест Ферма.

Тест базується на теоремі Ферма, яка стверджує, що якщо n – просте, то для довільного a, $1 \le a \le n$ - 1 має місце рівність $a^{n-1} \equiv 1 \pmod{n}$. Якщо для заданого n знайдеться хоча б одне таке a, що $a^{n-1} \not\equiv 1 \pmod{n}$, то n не є простим.

Означення. Нехай n – непарне складене число. Число a, $1 \le a \le n - 1$, таке що $a^{n-1} \not\equiv 1 \pmod{n}$, називається ***свідком Ферма*** (свідком складеності) для n.

Означення. Нехай n – непарне складене число, a – ціле число, $1 \le a \le n - 1$. Число n називається ***псевдопростим*** за основою a, якщо $a^{n-1} \equiv 1 \pmod{n}$. Число a називається ***брехунцем Ферма*** (брехунцем простоти) для n.

Очевидно, що для довільного складеного n число $a = 1$ завжди буде брехунцем Ферма, оскільки $1^{n-1} \equiv 1 \pmod{n}$.

Алгоритм

Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.

Вихід: визначення, чи є число n простим.

1. for $i \leftarrow 1$ to t do

   1.1. Обрати довільне ціле a, $2 \le a \le n - 2$.

1.2. Обчислити $k \leftarrow a^{n-1} \bmod n$.

1.3. if $k \neq 1$ then return (“складене”).

2. return (“просте”).

Якщо алгоритм дасть відповідь “складене”, то дійсно число є складеним. Якщо відповідь буде “просте”, то або n є дійсно простим, або n є складеним та має велику кількість брехунців. Чим більше значення параметра t, тим більше тестів буде зроблено і тим більша ймовірність того, що n є простим.

Приклад. Розглянемо складене число $n = 15$ та знайдемо його свідки та брехунці Ферма. Для цього складемо наступну таблицю:

a	1	2	3	4	5	6	7
$a^{14} \bmod 15$	1	4	9	1	10	6	4
a	8	9	10	11	12	13	14
$a^{14} \bmod 15$	4	6	10	1	9	4	1

Свідками Ферма є числа 2, 3, 5, 6, 7, 8, 9, 10, 12, 13.

Брехунцями Ферма є числа 1, 4, 11, 14.

Позначимо через $F(n)$ множину брехунців числа Ферма:

$$F(n) = \{a \in Z_n \mid a^{n-1} \equiv 1 \pmod n\}.$$

Тоді

$$|F(n)| = \prod_{p|n} НСД(n-1, p-1).$$

Приклад. Дільниками $n = 15$ будуть 3 та 5. Кількість його брехунців дорівнює

$$|F(15)| = НСД(14, 2) * НСД(14, 4) = 2 * 2 = 4.$$

З вище наведеного прикладу маємо: $F(15) = \{1, 4, 11, 14\}$.

Тест Ферма зручно використовувати для перевірки числа n на складеність, оскільки для більшості натуральних чисел кількість свідків більша за кількість брехунців. Але існують складені числа, які є псевдопростими за довільною основою (взаємно простою із заданим числом). Такі числа називаються числами Кармайкла і найменше з них дорівнює $561 = 3 * 11 * 17$.

Означення. Додатнє складене число n називається числом ***Кармайкла***, якщо для кожного a, $1 \le a \le n - 1$ має місце рівність: $a^n \equiv a \pmod n$.

Якщо n – число ***Кармайкла***, то для довільного a, $1 \le a \le n - 1$, для якого $НСД(a, n) = 1$, має місце рівність:

$$a^{n-1} \equiv 1 \pmod n.$$

Критерій Корсельта. Для того, щоб складене число n було числом Кармайкла, необхідно і достатньо виконання двох умов:

- n не ділиться на квадрат простого числа;

- $n - 1$ ділиться на $p - 1$ для будь-якого простого дільника p числа n.

Доведення.

Необхідність. Маємо: $n \mid a^n - a$ для всіх a. Доведемо, що n є вільним від квадратів та з $p \mid n$ випливає $p - 1 \mid n - 1$.

Якщо n не є вільним від квадратів, то воно має деякий нетривіальний дільник a^2. Тобто $a^2 \mid n \mid a^n - a$. Але звідси випливає $a^2 \mid a^n - a$, або $a \mid a^{n-1} - 1$, чого не може бути.

Нехай $p \mid n$, a – генератор мультиплікативної групи Z_p , a має порядок $p - 1$ та $a^{p-1} \equiv 1 \pmod p$. Тоді $p \mid n \mid a * (a^{n-1} - 1)$. Оскільки $a < p$, то p не ділить a. Звідси p повинно ділити $a^{n-1} - 1$, тобто $a^{n-1} \equiv 1 \pmod p$. Оскільки $p - 1$ – найменша степінь a, для якої $a^{p-1} \equiv 1 \pmod p$, але ми маємо $a^{n-1} \equiv 1 \pmod p$, то $n - 1$ повинно ділитися на $p - 1$.

Достатність. Маємо число n, вільне від квадратів, яке задовольняє умові: $p \mid n \Rightarrow p - 1 \mid n - 1$. Необхідно довести, що $n \mid a^n - a$ для всіх a.

Відомо, що число a, вільне від квадратів, ділить число b тоді і тільки тоді, коли кожен із простих дільників a ділить число b. Отже нам достатньо довести, що $p \mid a^n - a$ для всіх простих p , що ділять n ($p \mid n$), або те ж саме, що $a^{n-1} \equiv 1 \pmod p$ ($a \neq 0$). Але враховуючи, що $p - 1 \mid n - 1$, рівність можна замінити на $a^{p-1} \equiv 1 \pmod p$, яка є вірною, оскільки це – мала теорема Ферма.

Приклад. Простими дільниками числа 561 є 3, 11, 17. При цьому жоден з них не входить до розкладу навіть двічі, а число 560 ділиться на 2, 10 та 16:

$$560 : 2 = 280,\ 560 : 10 = 56,\ 560 : 16 = 35.$$

Найменшим числом Кармайкла є 561, яке було знайдене самим Кармайклом у 1910 році. Показано, що кількість чисел Кармайкла нескінченна, причому в натуральному ряді від 1 до n їх не менше ніж $n^{2/7}$.

Приклад. Наступними за 561 числами Кармайкла будуть:

$1105 = 5 \cdot 13 \cdot 17$ (4 | 1104, 12 | 1104, 16 | 1104),
$1729 = 7 \cdot 13 \cdot 19$ (6 | 1728, 12 | 1728, 18 | 1728),
$2465 = 5 \cdot 17 \cdot 29$ (4 | 2464, 16 | 2464, 28 | 2464),
$2821 = 7 \cdot 13 \cdot 31$ (6 | 2820, 12 | 2820, 30 | 2820),
$6601 = 7 \cdot 23 \cdot 41$ (6 | 6600, 22 | 6600, 40 | 6600),
$8911 = 7 \cdot 19 \cdot 67$ (6 | 8910, 18 | 8910, 66 | 8910).

Твердження. Кожне число Кармайкла є добутком хоча б трьох простих чисел.

Приклад. Числа Кармайкла в межі до 100000:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361.

Приклад. Найменшими числами Кармайкла з k = 3, 4, , ..., 9 простими множниками будуть:

k	
3	$561 = 3 \cdot 11 \cdot 17$
4	$41041 = 7 \cdot 11 \cdot 13 \cdot 41$
5	$825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
6	$321197185 = 5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137$
7	$5394826801 = 7 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 73$
8	$232250619601 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 73 \cdot 163$
9	$9746347772161 = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641$

Теорема (Чернік, 1939). Якщо $p = 6m + 1$, $q = 12m + 1$, $r = 18m + 1$ є простими числами, то число pqr є числом Кармайкла.

Приклад. Якщо покласти $m = 1$, то отримаємо $p = 7$, $q = 13$, $r = 19$ – всі прості числа. Отже $n = 7 * 13 * 19 = 1729$ – число Кармайкла. Перевірено, що при $m \le 100$ лише для $m = 1, 6, 35, 45, 51, 55, 56, 100$ отримуються числа Кармайкла.

Теорема. Позначимо через $C_3(x)$ кількість чисел Кармайкла, менших x, які мають в точності 3 простих множника. Тоді для великих x має місце оцінка:

$$C_3(x) = O(x^{5/14 + O(1)}).$$

Доведення. Якщо n є числом Кармайкла з трьома простими множниками p, q, r ($2 < p < q < r$), то $n - 1 \equiv 0 \pmod{p - 1}$, $n - 1 \equiv 0 \pmod{q - 1}$, $n - 1 \equiv 0 \pmod{r - 1}$.

Нехай g = НСД ($p - 1$, $q - 1$, $r - 1$) та a, b, c такі, що $p - 1 = g * a$, $q - 1 = g * b$, $r - 1 = g * c$, $a < b < c$. Звідси $gbc + b + c \equiv 0 \bmod a$, $gac + a + c \equiv 0 \bmod b$, $gab + a + b \equiv 0 \bmod c$. Оскільки a, b, c є взаємно простими, то ці три конгруенції можна замінити однією: $g * (a * b + a * c + b * c) + a + b + c \equiv 0 \bmod (a * b * c)$. Це вірно, оскільки з того, що НСД(a, b, c) = 1 та $c \equiv 0 \bmod$ НСД(a, b), $b \equiv 0 \bmod$ НСД(a, c), $a \equiv 0 \bmod$ НСД(b, c) випливає НСД(a, b) = НСД(a, c) = НСД(b, c) = 1. Отже якщо відомі a, b, c, то можна визначити g за модулем $a * b * c$.

Будемо рахувати кількість N четвірок (g, a, b, c), що задовольняють вище описаним умовам та нерівності $g^3 * a * b * c \le x$. Таким чином $C_3(x) \le N$. Запишемо $N = N_1 + N_2 + N_3$, де N_1 – кількість четвірок (g, a, b, c), для яких $g > a * b * c$, N_2 – кількість четвірок (g, a, b, c), для яких $G < g \le a * b * c$, $G = x^{3/14}$, N_3 – кількість четвірок (g, a, b, c), для яких $g \le G$ та $g \le a * b * c$.

Оцінка N_1.

Означення. Узагальнені числа Кармайкла. Нехай $k \in Z$. Множину чисел $C_k = \{n \in N: \min(n, n + k) > 1, a^{n+k} \equiv a \pmod{n}$ для будь-якого $a \in N\}$ будемо називати узагальненими числами Кармайкла k – го порядку.

Таким чином, усі звичайні числа Кармайкла разом із усіма простими числами будуть належити до C_0.

Теорема. Узагальнений критерій Корсельта. Нехай $k \in Z$. Число n належить C_k тоді і тільки тоді, коли

1) $n > \max(1, 1 - k)$;

2) n є вільним від квадратів;

3) $p - 1 \mid n + k - 1$ для всіх простих p, що ділять n.

Лема. Для всіх $k, n \in Z$ наступні умови еквівалентні:

а) $p - 1 \mid n + k - 1$ для всіх простих p, що ділять n ;

б) $p - 1 \mid n / p + k - 1$ для всіх простих p, що ділять n.

Доведення. Нехай p – просте, $p \mid n$, $m = n / p$. Тоді

$$p - 1 \mid m * p + k - 1 \Leftrightarrow p - 1 \mid m * p + p * (k - 1) - (p - 1) * (k - 1) \Leftrightarrow$$
$$p - 1 \mid m * p + p * (k - 1) \Leftrightarrow p - 1 \mid m + k - 1.$$

Остання еквівалентність має місце, оскільки p – просте.

Лема. Якщо $n \in C_k$, то n – вільне від квадратів.

Доведення. Нехай $p^2 \mid n$ для деякого простого p. Тоді $p^2 \mid n \mid p^{n+k} - p$, звідки $p^2 \mid p^{n+k} - p$, або $p \mid p^{n+k-1} - 1$, що неможливо.

Теорема. Якщо число q вибрано довільним чином, то ймовірність того, що воно просте, асимптотично дорівнює $1 / \log q$. Якщо відомо, що обране довільним чином число q не ділиться на p, то ймовірність його простоти збільшується на множник $p / (p - 1)$.

Наприклад, ймовірність того, що $p = 6m + 1$ є простим для деякого обраного навмання m, дорівнює $(2 / 1 * (3 / 2) * 1 / \log(6m + 1) = 3 / \log(6m + 1)$, оскільки заздалегідь відомо, що $6m + 1$ не ділиться ні на 2, ні на 3.

Річард Пінч, провівши велику кількість обчислень, виявив, що кількість чисел Кармайкла у натуральному ряді до 10^{12} дорівнює 8241, до 10^{13} – 19279, до 10^{14} – 44706, до 10^{15} – 105212. З іншого боку, декількома авторами наводилася верхня межа для $C(n)$ – кількість чисел Кармайкла від 1 до n. Одна з них (і яка на сьогодні вважається найбільш точною):

$$C(n) \le n^{1 - \{1 + o(1)\} \log\log\log n / \log\log n}$$

Теорема (Чіполла, 1904). Існує нескінченно багато складених псевдопростих чисел за основою b.

Доведення. Нехай $y_p = \dfrac{b^{2p} - 1}{b^2 - 1}$, де p – непарне просте число, НСД $(p, b^2 - 1) = 1$. Тоді $y_p = \dfrac{b^p - 1}{b - 1} \cdot \dfrac{b^p + 1}{b + 1}$ – складене непарне ціле число. Враховуючи, що $b^{2p} - 1$ ділиться на $\dfrac{b^{2p} - 1}{b^2 - 1}$, то $b^{2p} \equiv 1 \pmod{y_p}$.

$$y_p - 1 = \frac{b^{2p} - 1}{b^2 - 1} - 1 = \frac{b^{2p} - 1 - b^2 + 1}{b^2 - 1} = b^2 \cdot \frac{b^{2p-2} - 1}{b^2 - 1} = b^2 \cdot (b^{p-1} + 1) \cdot \frac{b^{p-1} - 1}{b^2 - 1}.$$

Оскільки $y_p - 1$ - парне, а також за теоремою Ферма $b^{p-1} \equiv 1 \pmod{p}$ (вираз b^{p-1} - 1 ділиться на p), то $y_p - 1 \equiv 0 \pmod{2p}$.

Отже $b^{y_p-1} = (b^{2p})^{\frac{y_p-1}{2p}} \equiv 1 \pmod{y_p}$.

Всі числа y_p є псевдопростими за основою b.

Приклад. Нехай $b = 2$, $p = 5$. Тоді $y_5 = \dfrac{2^{10}-1}{2^2-1} = 341 = 11 * 31$.

Оскільки $2^{340} \equiv 1 \pmod{341}$, то складене число 341 є псевдопростим за основою 2.

Тест Соловея – Штрассена.

Тест Соловея – Штрассена базується на критерії Ейлера: якщо n – просте, то

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

для всіх значень a, для яких НСД(a, n) = 1.

Означення. Нехай n – непарне складене число, a – ціле число, $1 \le a \le n-1$.

1. Якщо НСД (a, n) > 1 або $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \pmod{n}$, то число a називається ***свідком Ейлера*** (свідком складеності) для n.

2. Якщо НСД (a, n) = 1 та $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, то число n називається ***псевдопростим*** за основою a. Число a називається ***брехунцем Ейлера*** (брехунцем простоти) для n.

Алгоритм

Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.

Вихід: визначення, чи є число n простим.

1. for $i \leftarrow 1$ to t do
   1.1. Обрати довільне ціле a, $2 \le a \le n-2$.
   1.2. Обчислити $k \leftarrow a^{(n-1)/2} \bmod n$.
   1.3. if $k \neq 1$ and $k \neq n-1$ then return (“складене”).
   1.4. Обчислити символ Якобі $j \leftarrow \left(\frac{a}{n}\right)$.
   1.5. if $k \neq j \pmod{n}$ then return (“складене”).
2. return (“просте”).

Тест Міллера – Рабіна.

Тест Мілера – Рабіна найбільш часто використовується на практиці та називається сильним тестом на простоту.

Лема. Якщо $n = 1 + 2^s * r$, де r – непарне, то

$$a^{n-1} - 1 = (a^r - 1) * (a^r + 1) * (a^{2*r} + 1) * \ldots * (a^{2^{s-1}*r} + 1).$$

Доведення індукцією по s. При $s = 0$ вираз є істинним. Нехай розкладання на множники є вірним для $s = k$. Тоді при $s = k + 1$ маємо:

$$a^{n-1} - 1 = a^{2^{k+1}*r} - 1 = (a^{2^k*r} - 1) * (a^{2^k*r} + 1),$$

що вірно.

Теорема. Нехай n – непарне просте число, причому $n - 1 = 2^s * r$, де r – непарне. Нехай a – таке натуральне число, що НСД(a, n) = 1. Тоді має місце одна із рівностей:

$$a^r \equiv 1 \pmod{n}$$

або

$$a^{2^j r} \equiv -1 \pmod{n} \text{ для деякого } j,\ 0 \le j \le s - 1.$$

Доведення. Оскільки має місце розкладання

$$a^{n-1} - 1 = (a^r - 1) * (a^r + 1) * (a^{2*r} + 1) * \ldots * (a^{2^{s-1}*r} + 1),$$

а при простому n за теоремою Ферма ліва частина обертається в 0, то і права частина також повинна дорівнювати 0. Тобто має місце одна із рівностей, наведених в умові теореми.

Означення. Нехай n – непарне складене число, $n - 1 = 2^s * r$, де r – непарне, a – натуральне число, $1 \le a \le n - 1$.

1. Якщо $a^r \ne 1 \pmod{n}$ та $a^{2^j r} \ne -1 \pmod{n}$ для всіх j, $0 \le j \le s - 1$, тоді a називається ***сильним свідком*** (свідком складеності) для n.

2. Якщо $a^r \equiv 1 \pmod{n}$ або $a^{2^j r} \equiv -1 \pmod{n}$ для деякого j, $0 \le j \le s - 1$, тоді a називається ***сильним брехунцем*** для n, а само число n – ***сильним псевдопростим*** за основою a. Кількість сильних брехунців числа n будемо позначати через $sl(n)$ (*strong liars*).

Алгоритм

Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.
Вихід: визначення, чи є число n простим.
1. Записати $n - 1 = 2^s * r$, де r – непарне.
2. for $i = 1$ to t do
   2.1. Обрати довільне ціле a, $2 \le a \le n - 2$.
   2.2. Обчислити $y \leftarrow a^r \pmod{n}$.
   2.3. if $y \ne 1$ and $y \ne n - 1$ then
      $j \leftarrow 1$
      while $j \le s - 1$ and $y \ne n - 1$ do
         $y \leftarrow y^2 \bmod n$
         if $y = 1$ then return (“складене”).
         $j \leftarrow j + 1$
      if $y \ne n - 1$ then return (“складене”).
3. return (“просте”).

Твердження. Якщо число n після t циклів тесту Міллера – Рабіна дає відповідь "просте", то ймовірність того що n є дійсно простим, дорівнює $1 - \frac{1}{4^k}$.

Твердження. Якщо a – сильний брехунець числа n, то a буде брехунцем Ейлера для числа n.

Приклад. $n = 29$ – просте число. $n - 1 = 28 = 2^2 * 7$. s = 2, r = 7.

Нехай $a = 10$, НСД(10, 29) = 1.

$a^r \pmod n \equiv 10^7 \pmod{29} \equiv 17 \neq 1$.

Вираз $a^{2^j r}$ будемо обчислювати для $j = 0, 1$ ($0 \leq j \leq 1$), поки не отримаємо -1.

j = 0: $a^r \pmod n \equiv 10^7 \pmod{29} \equiv 17 \neq -1$.

j = 1: $a^{2r} \pmod n \equiv (10^7)^2 \pmod{29} \equiv -1$, 29 може бути простим.

Нехай $a = 19$, НСД(19, 29) = 1.

$a^r \pmod n \equiv 19^7 \pmod{29} \equiv 12 \neq 1$.

j = 0: $a^r \pmod n \equiv 19^7 \pmod{29} \equiv 12 \neq -1$.

j = 1: $a^{2r} \pmod n \equiv (19^7)^2 \pmod{29} \equiv -1$, 29 може бути простим.

Приклад. $n = 221 = 13 * 17$ – складене число. $n - 1 = 220 = 2^2 * 55$. $s = 2$, $r = 55$.

Нехай $a = 5$, НСД(5, 221) = 1.

$a^r \pmod n \equiv 5^{55} \pmod{221} \equiv 112 \neq 1$.

Вираз $a^{2^j r}$ будемо обчислювати для $j = 0, 1$ ($0 \leq j \leq 1$), поки не отримаємо -1.

j = 0: $a^r \pmod n \equiv 5^{55} \pmod{221} \equiv 112 \neq -1$.

j = 1: $a^{2r} \pmod n \equiv (5^{55})^2 \pmod{221} \equiv 168 \neq -1$, що підтверджує складеність 221.

Число 5 є сильним свідком для 221.

Приклад.

Нехай $a = 21$, НСД(21, 221) = 1.

$a^r \pmod n \equiv 21^{55} \pmod{221} \equiv 200 \neq 1$.

j = 0: $a^r \pmod n \equiv 21^{55} \pmod{221} \equiv 200 \neq -1$.

j = 1: $a^{2r} \pmod n \equiv (21^{55})^2 \pmod{221} \equiv -1$, 221 може бути простим.

Число 21 є сильним брехунцем для 221, а 221 є сильним псевдопростим за основою 21.

Якщо перебрати в якості a всі значення від 1 до 220, то можна побачити, що число 221 має 6 наступних сильних брехунців: 1, 21, 47, 174, 200, 220, а $sl(221) = 6$.

Твердження. Нехай n – непарне складене число. Тоді, якщо $n \neq 9$, то кількість його сильних брехунців не більша за $\varphi(n) / 4$.

Твердження. Нехай $n = p * q$ – добуток двох простих чисел,

d = НСД(p - 1, q - 1). Тоді кількість брехунців числа n дорівнює

$$sl(n) = r^2 * (2 + (4^t - 4) / 3),$$

де $d = 2^t * r$, r – непарне.

Приклад. $n = 221 = 13 * 17$. d = НСД(12, 16) = $4 = 2^2 * 1$, $r = 1$, $t = 2$.

$sl(221) = 1^2 * (2 + (4^2 - 4) / 3) = 2 + 4 = 6$.

Твердження. Нехай $n = p * q$ – добуток двох простих чисел, $p = 2 * r + 1$, $q = 4 * r + 1$, r – непарне. Тоді кількість брехунців досягає своєї верхньої межі:

$$sl(n) = \varphi(n) / 4$$

Приклад. При $r = 1$ маємо: $p = 3$, $q = 5$, $n = p * q = 15$.

$$sl(15) = \varphi(15) / 4 = (3 - 1) * (5 - 1) / 4 = 2 * 4 / 4 = 2.$$

Число 15 дійсно має двох сильних брехунців.

4.2 Істинні тести

Означення. Тест на простоту називається ***істинним***, якщо в результаті його застосування можна однозначно встановити, чи є задане число простим, чи ні.

Решето Ератосфена.

Найпростіший метод встановлення як простоти, так і складеності чисел був відомий ще у давнину і називається він решетом Ератосфена.

Виписати в ряд числа від 2 до n. Перше число в ряду є простим. Викреслити з ряду числа, які є кратними 2. Далі взяти друге число, що стоїть в ряду і викреслити всі числа, кратні йому. І так далі брати i-те число та викреслювати кратні йому числа, поки $i < \sqrt{n}$. Числа, що залишаться в ряду після операцій викреслення, є простими.

Цей метод є ефективним, коли число n невелике ($n < 10.000.000.000$). При цьому його можна використовувати не тільки для тестування на простоту, а й для пошуку простих чисел у вказаному інтервалі та для розв'язку задачі факторизації.

Теорема Вільсона

Число n є простим тоді і тільки тоді, коли $n \mid (n - 1)! + 1$.

Приклад наведено в табл. 4.1.

Таблиця 4.1

n	$(n - 1)! + 1$
2	2
3	3
5	25
7	721

5 Бульові функції і властивості криптографічних примітивів

Безпека симетричних блокових алгоритмів шифрування залежить від властивостей бульових функцій (БФ), які реалізують різні криптографічні примітиви, що входять в їх склад.

Перетворення інформації, яке здійснюється криптографічними примітивами, можна формалізувати у вигляді відображення деякого простору $GF(2)^n$ n-мірних векторів над полем $GF(2)$ $X=(x_1,x_2, ...,x_n)$ в інший простір $GF(2)^m$ m-мірних двійкових векторів $Y=(y_1,y_2, ...,y_m)$, де для будь-якого $i \in \{1, ..., n\}$ і будь-якого $j \in \{1, ...,m\}$, $x_i \in GF(2)$, $y_j GF(2)$. Відображення такого виду будемо задавати у вигляді векторної бульової функції (ВБФ) $Y=\varphi(X)$: $GF(2)^n \rightarrow GF(2)^m$, яка являється об'єднанням складених БФ $f_i(X)$, що здійснюють відображення $GF(2)^n \rightarrow GF(2)$, тобто $\varphi(X)=\{f_1(X),f_2(X),...,f_m(X)\}$.

Для опису БФ будемо використовувати їх представлення у вигляді таблиці істинності і у вигляді алгебраїчної нормальної форми (АНФ). АНФ передбачає наступний опис БФ:

$$f(x) = a_0 \oplus \sum_{1 \le i \le n} a_i x_i \oplus \sum_{1 \le i_1 \le i_2 \le n} a_{i_1 i_2} x_{i_1} x_{i_2} \oplus .... \oplus$$
$$\sum_{1 \le i_1 < .. < i_k \le n} a_{i_1 .. i_k} x_{i_1} ... x_{i_k} \oplus ... \oplus a_{12..n} x_1 x_2 ... x_n ,$$

де $X \in GF(2)^n$, а всі коефіцієнти $a \in GF(2)$. Таким чином, АНФ БФ над полем $GF(2)^n$ представляє собою суму взятих з визначеними коефіцієнтами різних добутків змінних. Кількість перемножувальних змінних в крайньому правому елементі АНФ являється алгебраїчним степенем нелінійності БФ $f(X)$ і позначається як $deg(f)$.

5.1 Перетворення Уолша-Адамара

При проведенні диференційного і лінійного криптоаналізу, а також дослідженні кореляційних властивостей бульових функцій (БФ), які описують примітиви блокових алгоритмів шифрування, основним апаратом аналізу являється перетворення Уолша-Адамара - різновидність дискретного перетворення Фур'є над кінцевим полем Галуа. Це перетворення дозволяє безпосередньо оцінити такі показники якості БФ, як:

- збалансованність;
- нелінійність;
- кореляційна імунність.

Крім цього, за допомогою перетворення Уолша-Адамара можна отримати оцінки автокореляційних властивостей БФ і різних показників розповсюдження змін.

Можна очікувати, що БФ не можуть задовольнити усім показникам одночасно, тому виникає задача деякого компромісу (оптимізації) у виборі БФ, що задовольняють тим чи іншим показникам.

Під перетворенням Уолша-Адамара (ПУА) функції *f(X), X*$\in GF(2)^n$, відносно вектора $\alpha \in GF(2)^n$ розуміється лінійне **перетворення** $GF(2)^n \to Z$, що приймає значення в області дійсних чисел і має наступний вигляд:

$$U_\alpha(f) = \sum_{X \in GF(2)^n} f(X)(-1)^{\langle \alpha, X \rangle} \quad , \tag{5.1}$$

де знак " $\langle \ \rangle$ " означає скалярний добуток двох векторів.

Для спряженої функції $\hat{f}(X) = (-1)^{f(X)}$, що здійснює відображення із $GF(2)^n$ у множину {-1, 1}, ПУА перетворюється до наступного вигляду:

$$\hat{U}_\alpha(f) = \sum_{X \in GF(2)^n} (-1)^{f(X)}(-1)^{\langle \alpha, X \rangle} = \sum_{X \in GF(2)^n} (-1)^{f(X) \oplus \langle \alpha, X \rangle} . \tag{5.2}$$

Очевидно, що при ПУА БФ *f(X)* ця функція і функція $\langle \alpha, X \rangle = \alpha_1 x_1 \oplus .... \oplus \alpha_n x_n$ приймають дійсні значення в полі *GF(2)*, а при перетворенні спряженої функції *f(X)* дійсні значення приймає функція $f(X) \oplus \langle \alpha, X \rangle$. Виходячи із взаємозвязку БФ *f(X)* і спряженої їй функції $\hat{f}(X)$, отримаємо, що $U_\alpha(f) = \left\langle S(f), \hat{S}(\langle \alpha, X \rangle) \right\rangle$ і $\hat{U}_\alpha(f) = \left\langle \hat{S}(f), \hat{S}(\langle \alpha, X \rangle) \right\rangle$, де скалярний добуток характеристичних послідовностей $\langle S', S'' \rangle = \sum_{i=1}^{n} s_i' s_i''$ приймає значення із *Z*, а самі перетворення зв'язані співвідношеннями:

$$\hat{U}_\alpha(f) = 2^n \delta(\alpha) - 2U_\alpha(f) , \tag{5.3}$$

$$U_\alpha(f) = 2^{n-1} \delta(\alpha) - \frac{\hat{U}_\alpha(f)}{2}, \tag{5.4}$$

де $\delta(\alpha) = 1$ для α = (0, ...,0} і $\delta(\alpha)$ = 0 для $\alpha \neq$ (0, ...,0).

Обернене перетворення Уолша-Адамара (ОПУА) задається виразами:

$$f(x) = \frac{1}{2^n} \sum_{\alpha \in GF(2)^n} U_\alpha (-1)^{\langle \alpha, X \rangle}, \; f(x) = \frac{1}{2^n} \sum_{\alpha \in GF(2)} \hat{U}_\alpha(f)(-1)^{\langle \alpha, X \rangle} . \tag{5.5}$$

Якщо 2^n значень таблиці істинності $S(f)$ БФ $f(X)$ і 2^n значень дійсної функції $U_\alpha(f)$ записати у вигляді вектор-стовпців $[S(f)]$ і $[U_\alpha(f)]$, то лінійне перетворення Уолша-Адамара задається матрицею Адамара H_n в наступному вигляді:

$$[U_\alpha(f)]=\mathrm{H_n}[S(f)] \tag{5.6}$$

Аналогічно $\left[\hat{U}_\alpha(f)\right]=H_n[S(f)]$. Матриця H_n формується ітеративно:

$$H_n=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\otimes H_{n-1}=\begin{bmatrix}H_{n-1} & H_{n-1}\\ H_{n-1} & -H_{n-1}\end{bmatrix}, H_0=[1], \tag{2.8}$$

де $\otimes$ означає кронекеровський добуток матриць.

Кронекеровський добуток матриці A розмірності $m\times n$ і матриці B розмірності $s\times t$ – це матриця розмірності $ms\times nt$, що задається як

$$A\otimes B=\begin{bmatrix}a_{11}B & a_{12}B & \dots & a_{1n}B\\ a_{21}B & a_{22}B & \dots & a_{2n}B\\ \dots & \dots & \dots & \dots\\ a_{m1}B & a_{m2}B & \dots & a_{mn}B\end{bmatrix}, \tag{5.9}$$

де a_{ij} - елемент i-ого рядка і j-го стовпця матриці A.

Матрицею ***Адамара*** називається матриця $\boldsymbol{H}$ з елементами із множини {-1, 1}, якщо справедлива наступна рівність $HH^T=n\boldsymbol{I_n}$, де H^T -транспонована матриця H, I_n - одинична матриця порядку n.

Основними властивостями матриць Адамара являються:

1. для $\forall\ s,t|(s+t)=n$ $\boldsymbol{H_n=H_S\otimes H_t}$;
2. $H^2{}_n=2^nI_n$;
3. Якщо записати матрицю за допомогою її рядків h_i,

$$H_n=\begin{bmatrix}h_0\\ h_1\\ \dots\\ h_{2^n-1}\end{bmatrix},$$

тоді кожний рядок h_i матриці H_n являється характеристичною послідовністю лінійної функції $\langle\alpha,X\rangle$, де вектор $\alpha\in GF(2)^n$, а його цілочисельне представлення рівне i. У свою чергу кожна характеристична послідовність $\hat{S}(f_{лзн})$ лінійної функції від n змінних являється рядком матриці H_n. Звідси виходить, що рядки матриць H_n і $\overline{H_n}$ покривають послідовності усіх афінних функцій над $GF(2)^n$. Тут $\bar{H}_n$ - матриця, усі елементи якої являються інверсними по відношенню до елементів матриці H_n.

У відповідності із властивостю (5.5) обернене ПУА буде задано співвідношенням:

$$[S(f)] = 2^{-n} H_n[U_\alpha(f)], \left[\hat{S}(f)\right] = 2^{-n} H_n\left[\hat{U}_\alpha(f)\right].$$

Алгоритм перетворення Уолша- Адамара має складність $O(n2^n)$ операцій.

5.2 Збалансованість БФ

Для уникнення прямих статистичних атак на примітиви криптоалгоритму необхідно, щоб виконувалися наступні умови:

- усі складені БФ, що реалізують перетворення, повинні бути збалансовані;
- перетворення в цілому повинно бути регулярним.

БФ $f(X)$, $X \in GF(2)^n$ називається з*балансованою,* якщо кількість одиниць в її таблиці істинності дорівнює кількості нулів, тобто $\#\{X|f(X)=0\} = \#\{X|f(X)\} = 2^{a-1}$.

Відображення $Y=\varphi(X) : GF(2)^n \to GF(2)^m$ при $n > m$ називається ***регулярним***, якщо Y рівно 2^{n-m} разів приймає усі 2^m різних значень із $GF(2)^m$, в той час як X проходить 2^n значень із $GF(2)^n$. Очевидно, що кожне регулярне відображення $Y=\varphi(X) : GF(2)^n \to GF(2)^m$ при $m=n$ являється **бієктивним** відображенням.

Необхідною умовою регулярності відображення $Y=\varphi(X) : GF(2)^n \to GF(2)^m$ при $n \geq m$ являється збалансованість будь-яких лінійних комбінацій складених БФ, що реалізують векторну БФ $\varphi(X)=\{f_1(X), f_2(X), \ldots, f_m(X)\}$. Під лінійною комбінацією елементів вектора $\varphi(X)=\{f_1(X), f_2(X), \ldots, f_m(X)\}$ для будь-яких $\lambda=(\lambda_1, \ldots, \lambda_m) \in GF(2)^m$ розуміється сума $\sum_{i=1}^{m} \lambda_i f_i(x)$,

Збалансованість БФ в термінах ПУА еквівалентна умові $\hat{U}_\alpha(f) = 0$, $U_\alpha(f) = \frac{1}{2^{n-1}}$, де α=(0,….,0), тобто значення ПУА в точці "0" визначає степінь відхилення БФ $f(X)$ від збалансованості.

Наприклад, БФ $f(X)$, $X \in GF(2)^6$, що має вигляд $f(X)= x_1x_2 \oplus x_3x_4 \oplus x_5x_6$, являється незбалансованою, так як значення компоненти спектру ПУА даної функції, представленої на рис. 5.1, в точці 0 $\hat{U}_0(f) = 8$. На рис. 5.1 значення i, що відкладені по осі абсцис, являються цілочисельним представленням вектора α. Таблиця істинності даної БФ має вигляд:

$S(f)$ =
=[00010001000111100001000100011110001110100011110111011100001].

Для побудови збалансованих БФ можна використати наступну властивість: якщо одна із функцій $f_1(X)$ або $f_2(Z)$, де $X, Z \in GF(2)^n$, являється збалансованою БФ, тоді функція $f(X,Z) = f_1(X) \oplus f_2(Z)$ також буде збалансованою БФ (рис. 5.1):

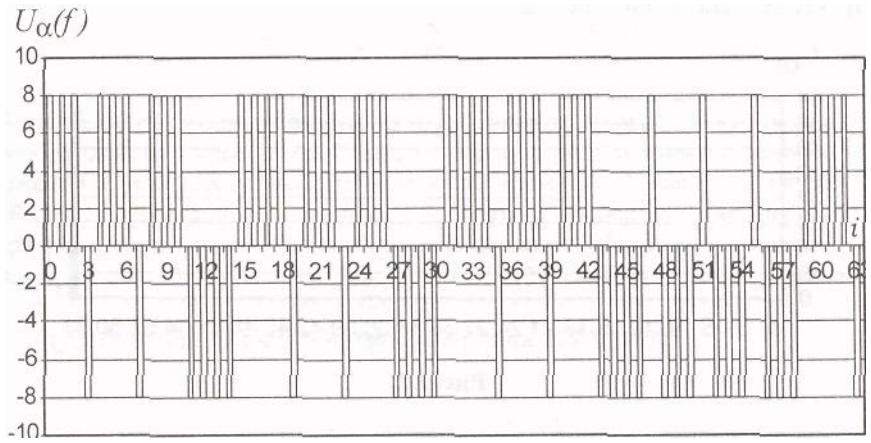


Рис. 5.1.

Показник збалансованості БФ являється самим простим і, як правило, розглядається в об'єднанні з іншими показниками.

5.3 Кореляційні властивості БФ

Суттєвим підсиленням властивості збалансованості БФ *f(X)* являється вимога збалансованості усіх часткових функцій, отриманих із початкової функції фіксуванням будь-яких її *k* або менше змінних. Указана вимога дозволяє забезпечити стійкість криптографічних перетворювань до статистичних атак при фіксованих значеннях бітів на вході перетворення. Ця властивість зв'язана з показником кореляційної імунності (КІ). При цьому БФ *f(X)*, $X \in GF(2)^n$ називається ***кореляційно-імунною*** порядку *k* (Cl(k)), $1< k <n$, якщо значення компонентів спектру УФ $\hat{U}_\alpha(f) = 0$ для всіх $\alpha \in GF(2)^n$, вага Хеммінга яких $1<wt(\alpha)\leq k$.

Отже, БФ являється КІ порядку *k*, якщо значення функції *Y=f(X)* статистично незалежні від будь-якого набору із *k* компонентів довільного вектора-аргумента $X \in GF(2)^n$. Якщо деяка функція являється кореляційно-імунною порядку *k*, то вона буде мати кореляцію з деякими наборами компонентів вектора *X* розміром, більшим, чим *k*, тобто існують вектори $\alpha \in GF(2)^n$ такі, що $wl(\alpha)>k$, $U_\alpha \neq 0$. Звідси виходить, що максимальний порядок КІ БФ *Y=f(X)*, $X \in GF(2)^n$ не перевищує значення *n-1*. Єдиними функціями, що досягають максимального порядку *k=n-1*, являються афінні БФ: $f(x_1,x_2,\ldots,x_n)= x_1 \oplus x_2 \oplus \ldots \oplus x_n$ і $f(x_1,x_2,\ldots,x_n)= x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1$. Для $n=6$ таблиця істинності БФ подібного вигляду має наступні значення:

S(f)=[01101001100101101001011001101001100101100110100101101001100
10110**],**

а спектр представлений на рис. 5.2.

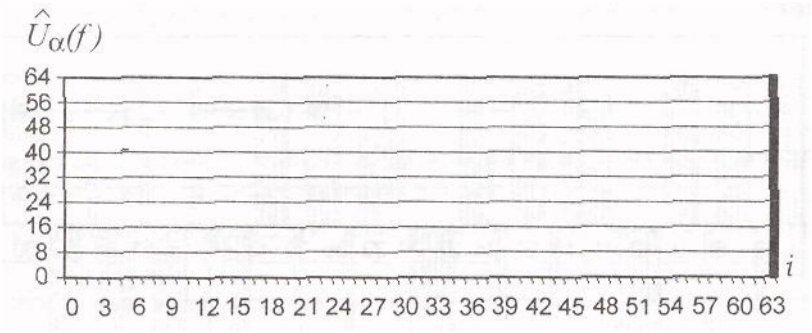


Рис. 5.2.

Досягнення максимуму показазника КІ БФ являється достатньо сильною вимогою, тому уведемо альтернативні поняття - кореляційно-ефективних БФ, для яких не менше чим на половині векторів ваги $1 \le w \le q$ значення компонентів спектру U_a рівні 0. Наприклад, спектр U_a (рис.5.3) БФ $f(X), X \in GF(2)^n$, $n=7$, $f(x) = x_1x_5x_7 \oplus x_2x_7 \oplus x_4x_6 \oplus x_4 \oplus x_3$ має 88 нульових значень ($\approx 69\%$), що дозволяє віднести дану БФ до класу кореляційно-ефективних БФ.

Кореляційно-імунна степеня k БФ $f(X)$ називається ідеальною кореляційно-імунною степеня k або ***резилентною*** функцією, якщо вона являється збалансованою функцією.

При синтезі БФ, що забезпечують високу стійкість до різницевого, лінійного і кореляційного криптоаналізу, велике значення має автокореляційна функція (АКФ) БФ. Під ***автокореляцією*** БФ $f(X)$ відносно вектора $\beta \in GF(2)^n$ розуміється функція вигляду:

$$r_\beta(f) = \frac{1}{2^n} \sum_{X \in GF(2^n)} \hat{f}(X)\hat{f}(X \oplus \beta). \qquad (5.10)$$

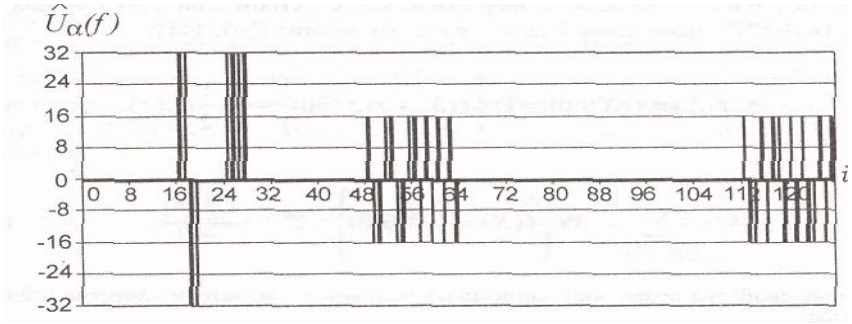


Рис. 5.3

У звичайного перетворення Фур'є енергетичний спектр (квадрат модуля перетворення Фур'є) і АКФ відіграють важливу роль і мають широку область додатків. Звязок між енергетичним спектром і АКФ виражає відома теорема Вінера-Хінчина**,** яка доводить, що обернене перетворення енергетичного спектру реалізується в автокореляційній функції. Це співвідношення можна перенести на

випадок ПУА, АКФ БФ *f(X)*. $X \in GF(2)^n$ звязано з енергетичним спектром $\hat{U}^2{}_\alpha(f)$ функції *f(X)* через пряме і обернене ПУА:

$$\hat{U}_\alpha(r_\beta(f)) = \sum_{\beta \in GF(f)^n} r_\beta(f)(-1)^{\langle \beta,\alpha \rangle} = \frac{1}{2^n}\hat{U}^2_\alpha(f), \alpha \in GF(2)^n\ , \qquad (5.11)$$

$$r_\beta(f) = \frac{1}{2^n}\sum_{\alpha \in GF(2)^n}\hat{U}(f)(-1)^{\langle \beta,\alpha \rangle}, \beta \in GF(2)^n, \qquad (5.12)$$

тобто ПУА АКФ БФ *f(X)* співпадає з енергетичним спектром цієї функції. Для АКФ БФ *f(X)*, $X \in GF(2)^n$ справедливі наступні співвідношення:

$$\Pr\{f(X) \neq f(X \oplus \beta)\} = \Pr\left\{\hat{f}(X) \neq \hat{f}(X \oplus \beta)\right\} = \frac{1}{2} - \frac{1}{2}r_\beta(f), \qquad (5.13)$$

$$\sum_{\beta \in GF(2)^n} \Pr\left\{\hat{f}(X) \neq \hat{f}(X \oplus \beta)\right\} = 2^{n-1} - \frac{\hat{U}_0^2(f)}{2^{n+1}}. \qquad (5.14)$$

Ці властивості дозволяють записувати основні показники якості БФ в термінах АКФ.

5.4 Критерії розповсюдження змін для БФ

Важливими характеристиками якості криптографічних перетворювань являються поняття критерію строгого лавинного ефекту - КСЛЕ (SAC -strict avalanche criterion) і критерію розповсюдження - КР (PC -propagation criterion). Основна сутність їх полягає в оцінюванні імовірності зміни значення БФ в залежності від зміни частини бітів аргументів цих функцій.

Нехай різниця $\Delta f(X,\beta) = f(X) \oplus f(X \oplus \beta)$, де $X,\beta \in \mathrm{GF}(2)^n$; $f(X) \in GF(2)$, тоді *БФ f(X)* задовольняє:

- КСЛЕ, якщо різниця $\Delta f(X,\beta)$ являється збалансованою функцією для будь-яких α, вага яких ***wt***(α)=1;
- КСЛЕ порядка *k* (SAC(k)), якщо будь-яка функція, що отримана із *f(X)* шляхом підстановки констант на місця довільних її *k* змінних, що задовольняють КСЛЕ.

Переходячи до спектральних властивостей, БФ *f(X)* задовольняє КСЛЕ, якщо АКФ $r_\beta(f) = 0$ для будь-яких векторів $\beta \in \mathrm{GF}(2)^\tau$, вага яких ***wt***($\beta$)=1, що у відповідності з (5.11) рівнозначно виконанню умови: обернене перетворення над $\hat{U}^2_\alpha(f)$ повинне задовольняти рівності

$$\sum_{\alpha \in GF(2)^n}\hat{U}^2_\varepsilon(f)(-1)^{\langle \alpha,\beta \rangle} = 0.$$

Бульова функція *f(X)*, $X \in \mathrm{GF}(2)^n$ задовольняє:

- КР степеня $1 \le n$ (PC(l)), якщо при заміні $1 \le i \le l$ довільних

вхідних бітів на свої доповнення функція *f(X)* змінюється з імовірністю $Pr\{f(X) \neq f(X \oplus \beta) = 0.5$, що еквівалентно збалансованності різниці $\Delta f(X, \beta)$ для будь-яких β, вага яких $1 \leq wt(\beta) \leq l$;

- КР степеня $l \leq n$ і порядку $k \leq n-1$ (РС(l)/k), якщо будь-яка функція, що отримана із БФ *f(X)* фіксацією будь-яких її *k* змінних, що задовольняють РС(l).

В термінах спектральних властивостей БФ задовольняє КР степеня *l* (РС(l)), якщо її АКФ $r_\beta(f) = 0$ на всіх векторах $\beta \in GF(2)^n$, вага Хеммінга яких лежить в границях $1 \leq wt(\beta) \leq l$. Очевидно, що КР являється узагальненням КСЛЕ, точніше, КСЛЕ еквівалентний КР РС(1).

Бульові функції вигляду $f(X) = \bigoplus_{i=1}^{n-1} \bigoplus_{j=i+1}^{n} x_i x_j$ задовольняють наступним показникам:

- SAC(*n*-2);
- *PC(k)/m* при $k+m \leq n-1$ або ($k+m=1$ і *k*-парне);
- РС(2)/(*n*-2);
- РС(*n*) при парному *n;*
- РС(*n*-l) при непарному *n* і *a(n)* буде збалансованою БФ.

Наприклад, над векторним простором $GF(2)^n$ при n=8 таблиця істинності БФ $f(X) = \bigoplus_{i=1}^{7} \bigoplus_{j=i+1}^{8} x_i x_j$ має вигляд:

S(f)=[00010111011111001111110111010000l111U011101000111010001000
000101111110111010001110100010000001111010001000000110000001000l0l11011
111101110100011101000100000011110100010000001100000010001011111101000
1000000110000 0010001011110000001000101110001011101111110].

Спектр ПУА БФ представлений на рис.5.4, а АКФ $r_\beta(f) = 0$ на всіх векторах β, вага яких $wt(\beta) \geq 1$.

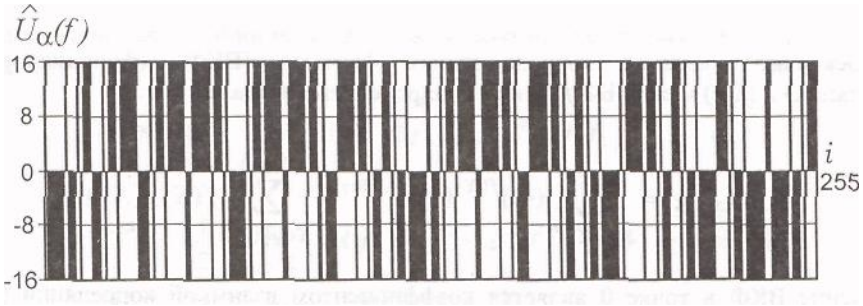


Рис. 5.4

Таким чином, розглянута БФ має наступні показники: РС(8), РС(6)/2, РС(2)/6.

Як і у випадку з кореляційною імунністю, критерію розповсюдження ненульового степеня (а тим більше ненульового порядку) досягнути досить важко.

5.5 Дослідження нелінійності БФ

При аналізі ефективності криптографічних перетворювань, зокрема, у відношенні лінійного криптоаналізу, однією із основних характеристик являється нелінійність БФ, що реалізують дане перетворювання, яка показує степінь віддаленості БФ від множини афінних або лінійних БФ. Нелінійність БФ являється важливим показником, оскільки лінійні функції порівняно легко відкриваються криптоаналітичними методами.

Під ***афінними*** функціями $f_{афф}(X) \in A$, де $A = \{f_{афф}(X)\}$, $X \in GF(2)^n$ розуміються БФ наступного вигляду

$$f_{афф}(X) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus ... \oplus \alpha_n x_n \oplus c\,, \qquad (5.15)$$

де $\alpha, c \in GF(2)$. При c=0 афінні функції утворюють підмножину ***лінійних*** функцій $£ = \{f_{аф}(X)\}$, кожна із яких являється скалярним добутком вигляду $£_{лін}(X)=(\alpha, X)$.

Віддаленість БФ від множини афінних A або лінійних £ БФ оцінюється через відстань Хеммінга $d(f, g)$ між двома БФ $f\{X)$ і $g(X)$, яка визначає кількість значень функцій, що відрізняються:

$$d(f,g) = \#\{f(X) \neq g(X) : X \in GF(2)^n\} = wt(S(f) \oplus S(g))\,. \qquad (5.16)$$

Відомо, що відстань (5.16) можна визначити через спряжені функції

$$d(f,g) = 2^{n-1} \sum_{X \in GF(2)^n} \hat{f}(X)\hat{g}(X) = 2^{n-1} - \frac{1}{2}\left\langle \hat{S}(f), \hat{S}(g) \right\rangle. \qquad (5.17)$$

Оскільки взаємна кореляційна функція (ВКФ) (функція кроскореляції) $R_t(f,g)$ між БФ $f(X)$ і $g(X)$ визначається виразом:

$$R_t(f,g) = \sum_{X \in GF(2)^n} (-1)^{f(X)} (-1)^{g(X \oplus t)} = \sum_{X \in GF(2)^n} \hat{f}(X)\hat{g}(X \oplus t)\,, \qquad (5.18)$$

а значення ВКФ в точці 0 являється коефіцієнтом взаємної кореляції (КВК)

$$r(f,g) = \frac{R_0(f,g)}{2^n} = \frac{1}{2^n} \sum_{X \in Gf(2)^n} \hat{f}(X)\hat{g}(X) = \frac{1}{2}\left(\sum_{\substack{X \in Gf(2)^n \\ f(X)=g(X)}} \hat{f}(X)\hat{g}(X) - \sum_{\substack{X \in Gf(2)^n \\ f(X)\neq g(X)}} \hat{f}(X)\hat{g}(X) - \right), \qquad (5.19)$$

тобто

$$r(f,g) = \Pr\{f(X) = g(X)\} - \Pr\{f(X) \neq g(X)\}, \qquad (5.20)$$

то КВК і відстань Хеммінга звязані між собою наступним співвідношенням:

$$r(f,g)=\frac{2^n-d(f,g)}{2^n}-\frac{2^n-d(f,\bar{g})}{2^n}=\frac{1}{2^n}(d(f,\bar{g})-d(f,g))=1-\frac{d(f,g)}{2^{n-1}}. \qquad (5.\ 21)$$

Для підсумкової кореляції будь-якої БФ *f(X)* з набором усіх лінійних функцій справедлива рівність Парсеваля:

$$\sum_{f_{лін}\in\lambda} r^2(f,f_{лін})=\frac{1}{2^{2n}}\sum_{\alpha\in GF(2)^n}\hat{U}_\alpha^2=1\ . \qquad (5.\ 22)$$

Отже, сумарна кореляція не залежить від виду функції *f(X)* і для будь-якої БФ *f(X)* завжди існує кореляція якою-небудь лінійною функцією, тобто існує така $f_{лін}\in$ £, що $r(f,f_{лін})\neq 0$.

На підставі вищесказаного дамо визначення ***нелінійності*** БФ *f(X):* $GF(2)^n \to GF(2)$, під якою розуміється значення мінімальної відстані Хеммінга між функцією *f(X)* і функціями $f_{аф}(X)\in A$:

$$NL(f)=\min_{f_{афф}\in A} d(f,f_{аф})\ . \qquad (5.23)$$

Аналогічно нелінійність NL(f ") можна виразити через відстань до лінійних функцій:

$$NL(f)=\min_{f_{аф}\in A}\min\{d(f,f_{лін}),2^n-d(f,\bar{f}_{лін})\}=2^{n-1}-\frac{1}{2}\max_{f_{лін}\in A}\left|d(f,f_{лін})-d(f,\bar{f}_{лін})\right|=$$

$$=\ 2^{n-1}-2^{n-1}\max_{f_{лін}\in\lambda}\left|r(f,f_{лін})\right|\ , \qquad (5.\ 24)$$

де

$$r(f,f_{лін})=\Pr\{f(X)=f_{лін}(X)\}-\Pr\{f(X)\neq f_{лін}(X)\}=$$

$$2\left(PR\{f(X)=\langle\alpha,X\rangle\}-\frac{1}{2}\right)=\frac{1}{2^n}\left\langle\hat{S}(f),\hat{S}(\langle\alpha,X\rangle)\right\rangle=\frac{1}{2^n}\hat{U}_\alpha(f)\ . \qquad (5.\ 25)$$

Функції $r(f,f_{лін})$ використовуються в якості лінійної характеристики функції *f(X)* по лінійній функції $f_{лін}(X)=\langle\alpha,X\rangle$ і застосовуються при проведенні лінійного криптоаналізу.

Підставивши співвідношення (5.25) у вираз (5.24), отримаємо значення нелінійності функції *f(X)* в термінах ПУА:

$$NL(f)=2^{n-1}-\frac{1}{2}\max_{\alpha\in GF(2)}\left|\hat{U}_\alpha(f)\right|\ , \qquad (5.\ 26)$$

тобто для визначення нелінійності БФ необхідно визначити максимальне значення компоненти спектру ПУА. Використовуючи це співвідношення, можна достатньо просто визначити нелінійність БФ при малих значеннях *n.*

На підставі теореми Парсеваля верхня границя значення нелінійності NL(f) для будь-яких БФ *f(X), X*∈ *GF*(2)^n визначається нерівністю

$$NL(f) \le \begin{cases} \left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor, & для\ n - непарного \\ 2^{n-1} - 2^{\frac{n}{2}-1}, & для\ n - парного \end{cases}, \qquad (5.\ 27)$$

де $\lfloor \bullet \rfloor$ означає максимальне парне ціле, менше або рівне значенню аргумента. Аналогічно для будь-якої функції збалансованої БФ справедливі нерівності:

$$NL(f) \le \begin{cases} \left\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \right\rfloor, для\ n - непарного \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2, для\ n - парного \end{cases}. \qquad (5.\ 28)$$

Протилежним поняттю нелінійності являється *лінійність* БФ *f (X): GF*(2)^n $\rightarrow$ *GF*(2), яка визначається із наступного виразу:

$$L(f) = \max_{f_{лін} \in \lambda} \left| r(f, f_{лін}) \right| . \qquad (5.\ 29)$$

Таким чином, у відповідності з виразами (5.24), (5.29) лінійність і нелінійність БФ *f(X)* зв'язані рівностями:

$$NL(f) = 2^{n-1}(1 - L(f)) , \qquad (5.30)$$

$$L(f) = 1 - \frac{1}{2^{n-1}} NL(f) . \qquad (5.31)$$

Із рівності Парсеваля (5.22) виходить, що лінійність знаходиться в границях

$$2^{\frac{n}{2}} \le L(f) \le 1 . \qquad (5.32)$$

Для підстановочного перетворення $Y = \varphi(X), X \in GF(2)^n, Y \in GF(2)^m$, де $\varphi(X)$ - векторна БФ, поняття нелінійності і лінійності визначаються наступними співвідношеннями:

$$NL(\varphi(X)) = \min_{\substack{c \in GF(2)^n \\ c \ne 0}} NL\langle c, \varphi \rangle , \qquad (5.\ 33)$$

$$L(\varphi(X)) = \min_{\substack{c \in GF(2)^n \\ c \ne 0}} L\langle c, \varphi \rangle . \qquad (5.\ 34)$$

де мінімум і максимум знаходяться не тільки відносно усіх складених БФ, але і будь-яких лінійних комбінацій даних БФ.

Досягнути найкращих показників нелінійності і лінійності для векторної БФ складно, тому на практиці використовується поняття середньої нелінійності і лінійності векторної БФ $\varphi(X)$, які визначаються із виразів:

$$NL(\varphi(X)) = \min_{\substack{c\in GF(2)^n \\ c\neq 0}} NL\langle c,\varphi\rangle \ , \tag{5.35}$$

$$\overline{L}(\varphi(X)) = \min_{\substack{c\in GF(2)^n \\ c\neq 0}} L\langle c,\varphi\rangle \quad . \tag{5.36}$$

Обмеження нелінійності і лінійності для векторних БФ $\varphi(X)$ співпадають з границями для складених БФ, тобто визначаються виразами (5.27, 5.28, 5.32).

5.6 БФ, які досягають максимальної нелінійності

Бульова функція являється ***абсолютно нелінійною,*** якщо для $\forall\beta \in GF(2)^n, \beta \neq 0$, виконується рівність

$$\#\{X \in GF(2)^n : f(X) = f(X \oplus \beta)\} = \#\{X \in GF(2)^n : f(X) \neq f(X \oplus \beta)\} = \frac{2^n}{2},$$

що еквівалентно рівності $r_\beta(f) = 0$,

В термінах ПУА БФ *f(X), X*$\in$ $GF(2)^n$ являється абсолютно нелінійною або інакше ***бент-функцією,*** якщо для $\forall\alpha \in Gf(2)^n$ виконується рівність

$$\hat{U}_\alpha(f) = \pm 2^{n/2}. \tag{5.37}$$

Тобто, це БФ, для яких відстань Хеммінга до множини усіх афінних функцій *A* над $GF(2)^n$ максимальна і має постійну величину

$$d(f_{бент}, f_{аф}) \overset{\forall f_{аф}\in A}{=} const .$$

Основними властивостями множин бент-функцій $B=\{f_{бент}(X)\}$ являються:

- кількість змінних *n* для будь-якої $f_{бент}(X) \in B, X \in GF(2)^n$ парне, а алгебраїчний степінь $deg(f_{бент}) \leq n/2;$
- бент-функції $f_{бент}(X) \in B$ - незбалансовані функції, такі, що

$$\#\{f_{бент}(X) = 1\} = 2^{n-1} \pm 2^{\frac{n}{2}-1}, a\#\{f_{бент}(X) = 0\} = 2^{n-1} \mp 2^{\frac{n}{2}-1};$$

- бент-функції $f_{бент}(X) \in B$ мають максимальне значення нелінійності і, відповідно, мінімальне значення лінійності:

$$NL(f_{бент}(X)) = 2^{n-1} - 2^{\frac{n}{2}-1}, L(f_{бент}(X)) = 2^{-n/2};$$

- єдиною множиною функцій, задовольняючих КР степеня *n* - РС(n), являється множина бент-функції *B,* тобто для $\forall\beta \in GF(2)^n$, вага Хеммінга якої $1 \leq wt(\beta) \leq n$, різницева функція $\Delta f(X,\beta) = f(X) \oplus f(X \oplus \beta)$ являється збалансованою функцією;

- коефіцієнт взаємної кореляції між бент-функцією і множиною усіх лінійних БФ має постійне значення за абсолютною величиною $\left| r(f_{бент}, f_{лін}) \right|^{\forall f_{лін} \in \lambda} = \frac{1}{2^{n/2}}$.

Існують наступні, найпростіші, методи побудови бент-функцій:

- БФ $f(X)$, $X \in GF(2)^n$ виду $f(X) = \bigoplus_{i=1}^{n-1} \bigoplus_{j=i+1}^{n} x_i y_j$ являється бент-функцією (приклад розглянутий на рис. 5.4);
- якщо $f(X)$ і $g(X)$ є відповідно бент- і афінна БФ, то $h(X) = f_{бент}(X) \oplus g_{аф}(X)$ являється бент-функцією;
- якщо g - довільна БФ від m змінних, тоді функції $f(X)$, $X \in GF(2)^n$, де $n=2m$, наступного виду

$$f(X) = g(x_1, x_2, ..., x_m) \oplus x_1 x_{m+1} \oplus x_2 x_{m+2} \oplus ... \oplus x_m x_n$$

являються бент-функціями.

Аналогічно, якщо перейти до векторних БФ, то функція $\varphi(X) = (f_1(X), ..., f_m(X))$ являється векторною бент-функцією, якщо для будь-яких $\lambda \in GF(2)^m$ БФ $\phi(X) = \langle \lambda, \varphi(X) \rangle$ також є векторна бент-функція, тобто кожна нетривіальна лінійна комбінація складених функцій являється бент-функцією. Векторні бент-функції існують тільки для парного значення $n > 2m$.

5.7 Узагальнення показників якості підстановочних перетворювань

З метою спрощення аналізу показників якості криптографічних перетворювань над початковими векторами необхідно проводити афінне перетворювання координат, так як алгебраїчний степінь, збалансованність, нелінійність і кількість векторів, на яких виконується критерій нерозповсюдження - усі інваріантні відносно афінного перетворювання координат. В якості афінного перетворювання координат можна використати перемноження вектора A"$eGF(2)$" на невироджену матрицю порядка n над полем GF(2).

Таким чином, узагальнюючи викладені результати, сформулюємо необхідні вимоги до усього підстановочного перетворювання і до формуючих його компонентних БФ:

1.Регулярність відображення $Y = \varphi(X) : GF(2)^n \to Gf(2)^m$ при $n \geq m$, тобто збалансованність усіх складених БФ і їх будь-яких лінійних комбінацій.

2.Високий алгебраїчний степінь нелінійності $deg(f)$ складених БФ.

3.Відповідність БФ показникам кореляційної імунності.

4.Відповідність БФ КСЛЕ і КР із множини SAC(k), PC(k)/l, тобто низькі автокореляційні показники.

5.Висока нелінійність $NL(f)$ компонентних БФ.

6.Висока нелінійність $NL(\varphi(X))$ або середня нелінійність $\overline{NL}(\varphi(X))$ векторного перетворювання.

6 Двоключові криптосистеми

6.1 Порівняльна характеристика одноключових і двоключових шифрів

Криптографічні системи (шифри) з секретним ключем, які називаються також симетричними, вирішують проблеми збереження інформації в таємниці і забезпечення контролю цілісності інформації. Перша із цих задач визначає сутність одноключової криптографії.

Головними вимогами, які пред'являються до симетричних шифрів, являється їх стійкість. Абсолютно (безумовно) стійкими криптосистемами являються шифри з ключем одноразового використання. Такі шифри достатньо прості в плані здійснюваних процедур зашифрування і розшифрування, проте вимагають розприділенин надмірно великого об'єму ключового матеріалу, що робить їх використання дуже дорогим.

Задача розприділення ключів по захищенним каналам являється фундаментальною. При її розв'язанні одночасно вирішується і задача аутентифікації ключів. Дійсно, отримувач повинен не тільки отримати секретний ключ, але також і переконатися, що якраз цей ключ був відправлений законним відправником (зокрема, центром розприділення ключів). Проблема розприділення секретних ключів в певній степені приховує проблему їх аутентифікації. Необхідно мати на увазі, що і друга проблема являється фундаментальною. Більш того, вона являється фундаментальною і в двоключовій криптографії, яка надає найбільш економічні і зручні механізми розприділення секретних ключів. Ці питання будуть обговорюватися нижче.

Абсолютна стійкість шифру розглядається тільки по відношенню до атак на основі шифротексту. Дійсно, якщо ключ використовується однократно, то атака на основі відомого або спеціально підібраного тексту втрачає своє значення. На практиці найбільше розповсюдження отримали шифри другого типу, а саме шифри з кінцевим ключем (звичайно від 64 до 256 бітів). Такі шифри являються умовно стійкими. Завжди є теоретична можливість визначення ключа шифрування шляхом повного перебору всього простору ключів, якщо є шифротекст, перевищуючий інтервал одиничності. Проте на практиці така атака неспроможна внаслідок надзвичайно великого часу, який вимагається для перебору. У зв'язку з цим такі шифри називають також практично стійкими.

Якщо розглядати атаки на основі відомих або спеціально підібраних текстів, то в принципі можуть бути знайдені деякі способи обчислення ключа. Алгоритми шифрування повинні бути такими, щоб забезпечити високу обчислювальну складність найкращого алгоритму атаки. У зв'язку з цим шифри з кінцевим ключем називають також обчислювально стійкими.

Обчислювально стійкі шифри знайшли на практиці суттєво більш широке застосування у порівнянні з теоретичними (безумовно) стійкими криптосистемами, оскільки вони незалежні від ряду суттєвих для практичного використання недоліків, зв'язаних з бажанням досягнути абсолютної стійкості. Крім усунення технологічних недоліків, перехід до обчислювально стійких шифрів дає можливість побудувати якісно нові криптосистеми - двоключові шифри,

що називаються також криптосистемами з відкритим ключем. В останньому терміні підкреслюється принципове значення використання загальновідомого ключа. Необхідність використання секретного ключа очевидна, оскільки він необхідний в шифрах будь-якого типу.

Принципово новим, що вноситься двоключовими шифрами, являється *можливість побудови криптографічних протоколів, які розв'язують задачі взаємодії сторін, які не довіряють друг другу.* Поява такої можливості пов'язана з тим, що в двоключових шифрах секретний ключ, що виробляється деяким користувачем (абонентом), залишається відомим тільки йому. В протоколах, заснованих на одноключових (симетричних) криптосистемах, розв'язуються задачі, в яких взаємодіючі сторони *довіряють* друг другу, що зв'язано з тим, що секретний ключ повинен бути відомим, що найменше, двом сторонам. Для реалізації задач протоколів, основаних на двоключових шифрах, необхідно знання другими сторонами тільки відкритого ключа. Наприклад, секретний ключ може бути використаний для вироблення цифрового електронного підпису до деякого документу, який буде представляти собою деяке число, що залежить від секретного ключа і від кожного біту документа (або від хеш-функції останнього). Якщо хоча б іще один учасник протоколу знав би секретний ключ, то і він міг би зробити такий же підпис, тобто, неможливо було б однозначно установити учасника, підписавшого даний документ (тобто, хто виробив двійковий вектор, який інтерпретується як число або повідомлення із спеціальною структурою і представлений як електронний цифровий підпис до даного документа). Питання перевірки правильності підпису вирішується з використанням загальнодоступного відкритого (публічного) ключа. Таким чином, підписати документ може тільки єдина сторона, що являється власником секретного ключа, а перевірити підпис може будь-який бажаючий.

Очевидно, що реалізація такого узагальненого механізму функціонування системи електронного цифрового підпису (ЕЦП) вимагає наявності визначеного зв'язку між секретним і відкритим ключами, тобто вони повинні бути залежними між собою. Нижче будуть розглянуті декілька варіантів того, як це може бути реалізовано.

6.2 Від відкритого розприділення ключів до електронного цифрового підпису

6.2.1 Система розприділення ключів Діффі-Хеллмана

Зародження двоключової криптографії і основні криптосистеми з відкритим ключем зв'язані з використанням функції піднесення до великого дискретного степеня за модулем великого простого числа

$$f(x\} = a^x (\mathrm{mod}\ p),$$

де x- ціле число, $1 \le x \le p-1$, p - $к$-бітове просте число, a - первісний корень за модулем p.

Використовуючи дану функцію, ученими Діффі і Хеллманом була показана можливість побудови практично стійких секретних систем, які *не вимагають*

передачі секретного ключа. Запропонована ними система отримала назву метода відкритого росповсюдження ключів. В ній кожний абонент вибирає випадковим чином секретний ключ *x* і виробляє відкритий ключ *y,* що відповідає вибраному секретному ключу, у відповідності з формулою

$$y = a^x (\mathrm{mod}\ p).$$

Системою Діффі-Хеллмана називається наступний спосіб використання дискретного піднесення до степеня для обміну секретними ключами між користувачами мережі із застосуванням тільки відкритих повідомлень. Вибирається велике просте число *p* і відповідний йому первісний корінь $\alpha < p$ (Для забезпечення стійкості розглядаємої системи відкритого шифрування на число *p* накладається наступна умова: розкладання числа *p-1* на множники повиннно містити, як мінімум, один великий простий множник; розмір числа *p* повинен бути не менше 512 бітів).

Механізм розприділення секретних ключів по відкритому каналу полягає в наступному. Кожний абонент вибирає випадковий секретний ключ *x* і виробляє відкритий ключ *y,* що відповідає вибраному секретному ключу, у відповідності з формулою

$$y = a^x (\mathrm{mod}\ p).$$

Два абоненти *A* і *B* можуть установити секретний зв'язок без передачі секретного ключа наступним чином. Абонент *A* бере із довідника відкритий ключ y_B абонента *B* і, використовуючи свій секретний ключ x_A, обчислює загальний секретний ключ:

$$Z_{AB} = (y_B)^{X_A} = (\alpha^{X_D})^{X_A} = \alpha^{X_D X_A} (\mathrm{mod}\ p).$$

Аналогічно поступає абонент *B*:

$$Z_{AB} = (y_A)^{X_B} = (\alpha^{X_A})^{X_B} = \alpha^{X_D X_A} (\mathrm{mod}\ p).$$

Таким чином, оба абоненти сформували однаковий секретний ключ Z_{AB} без використання будь-якого заздалегідь обговореного загального секрета. Володіючи тільки їм відомим секретом і використовуючи його в якості майстер-ключа, дана пара абонентів може зашифрувати направлені друг другу повідомлення. Указані вище обчислення легко здійснювані для достатньо великих значень *p,* α, *y* (наприклад, числа в двійковому представленні мають довжину 4096 бітів і більше). Атакуючому відомі значення $y_B = \alpha^{X_B} (\mathrm{mod}\ p)$ і $y_A = \alpha^{X_A} (\mathrm{mod}\ p)$, але для того, щоб обчислити Z_{AB}, він повинен розв'язати задачу дискретного логарифмування і визначити або x_a, або $x_в$. Легко знайти велике значення *p* (більше 1024 бітів), для якого задача дискретного логарифмування являється важко розв'язуємою. Якщо будуть знайдені обчислювально ефективні методи рішення задачі дискретного логарифмування, то метод Діффі-Хеллмана виявиться неспроможним. У зв'язку з цим говорять, що даний метод відкритого розприділення ключів заснований на складності дискретного логарифмування. В даний час в загальному випадку задача дискретного логарифмування практично

нерозв'язувана, що дає можливість широкого практичного застосування методу Діффі-Хеллмана і багаточисельних систем ЕЦП, заснованих на складності обчислення дискретних логарифмів,

Не треба упускати із виду проблему аутентифікації відкритих ключів. Коректність протоколів з використанням асиметричних шифрів може бути забезпечена тільки у випадку, якщо всі відкриті ключі в довіднику відкритих ключів являються справжніми. Якщо відкритий ключ якого-небудь абонента порушник зможе підмінити, то секретні повідомлення, що надіслані даному абоненту, будуть доступні порушнику. Таким чином, двоключові шифри забезпечують вирішення проблеми розповсюдження секретних ключів, проте проблема аутентифікації зберігається і має фундаментальний характер, хоча вимога підтвердження автентичності (аутентифікації) відноситься уже до відкритого, а не до секретного ключа. В неявному вигляді аутентифікація відкритого ключа включає в себе аутентифікацію секретного ключа.

6.2.2 Відкритий шифр Ель-Гамаля

В розглянутій вище двоключовій криптосистемі здійснюється відкрите розприділення ключів, але самі процедури зашифрування і розшифрування здійснюються за допомогою симетричного шифру. Існують двоключові шифри, в яких зашифрування здійснюється за відкритим ключем, а розшифрування за секретним. Такий шифр може бути побудований на основі методу Діффі-Хеллмана шляхом використання одноразового відкритого ключа. Розглянемо спосіб шифрування, запропонований Ель-Гамалем. Щоб направити користувачеві i секретне повідомлениеня T, відправник діє у відповідності з наступним алгоритмом:

1. Вибрати випадкове число x' (за своєю суттю x' являється одноразовим секретним ключем).

2. Обчислити значення $y' = a^{x'} \pmod p$, яке фактично являється одноразовим відкритим ключем.

3. Використовуючи відкритий ключ отримувача, обчислити значення $Z = y^n \pmod p$, яке є одноразовий загальний секретний ключ відправника i-го користувача.

4. Здійснити зашифрування повідомлення T за допомогою перемноження за модулем p повідомлення на одноразовий загальний секретний ключ:
$C=y^R T \pmod p$.

5. Відправити криптограму (y', C) i-му користувачеві.

Неважко бачити, что сутність відкритого шифрування Ель-Гамаля полягає у використанні перемноження за модулем повідомлення на одноразовий загальний секрет. Для того, щоб i-ий абонент міг правильно розшифрувати повідомлення, в криптограму разом з шифротекстом C включається також і одноразовий відкритий ключ відправника, що приводить до збільшення розміру криптограми приблизно в 2 рази у порівнянні з початковим текстом. Легко показати, що i-ий користувач, отримавши криптограму (y', C), може обчислити початковий текст: $T = C/(y')^x = C/Z \pmod p$.

Важливим моментом у відкритому шифрі Ель-Гамаля являється використання одноразового відкритого ключа. Такий прийом являється принциповим при побудові систем ЕЦП, заснованих на складності дискретного логарифмування, і є подальшим розвитком криптографічних застосувань функції піднесення у велику степінь за модулем великого простого числа.

7 Системи ЕЦП на основі задачі дискретного логарифмування

7.1 Загальні положення

Нехай є деякий документ. Маючи криптографічно стійку хеш-функцію, ми можемо ототожнювати підписування хеш-функції *h* від документу з підписуванням самого документа. В системах ЕЦП це робиться для того, щоб підпис до документу мав порівняно невеликий фіксований розмір незалежно від розміру самого документа. Це має важливе технологічне значення, проте не являється принциповим для розуміння механізму дії системи ЕЦП. Підпис повинен залежати від секретного ключа і від значення *h*. Спробуємо задати рівняння перевірки підпису *s* в наступному вигляді:

$$H=y^S \pmod p.$$

Якщо власник секретного ключа може для даного значення *h* обчислити підпис *s*, то ми б мали уже систему ЕЦП. За цією формулою, використовуючи відкритий ключ підписуючого, будь-який бажаючий може перевірити справжність підпису. Проте легко прийти до висновку, що в загальному випадку власник секретного ключа не зможе обчислити значення *s*, яке буде задовольняти умові $h = y^S = \alpha^{xS} \pmod p$, оскільки для знаходження *s* вимагається представити значення хеш-функції *h* у вигляді степеня α, а саме $h = \alpha^w \pmod p$, тобто для обчислення підпису потрібно вирішити задачу дискретного логарифмування. Значить, треба знайти деяке інше рівняння перевірки підпису, наприклад, наступне:

$$\alpha^h = y^S \pmod p.$$

Очевидно, що, знаючи тільки відкритий ключ *y,* знайти значення *s*, яке буде задовольняти другому рівнянню перевірки підпису, обчислювально складно. При цьому власник секретного ключа *x* може легко обчислити підпис *s*, оскільки він може скористатися співвідношенням $\alpha^h = y^S = \alpha^{xS} \pmod p$, із якого виходить рівняння обчислення підпису:

$h= xs \pmod{(p-1)}$, тобто $s = h/x \pmod{(p-1)}$.

Отже, необхідно здійснити перемноження за модулем *p—1* на елемент, обернений значенню секретного ключа. Він існує і являється єдиним, якщо *x* являється взаємно простим з *p*-1. Це деяке несуттєве обмеження на вибір секретного ключа, яке можна було б прийняти, проте все ж даний варіант ЕЦП

неспроможний, оскільки після надання для перевірки підпису перевіряючий може не тільки переконатися, що значення *s* було сформовано власником секретного ключа, але і обчислити сам секретний ключ. Секретний ключ став би відомим більше чим одному користувачеві. Системи ЕЦП не повинні допускати такої можливості. Не дивлячись на поточну невдачу, ми можемо вияснити для себе корисний факт: *значення хеш-функції документа доцільно використовувати як степінь її числа або як множник цього степеня.* Це надасть можливість обчислення підпису за відомим секретним ключем. Тепер наша задача полягає в тому, щоб зробити обчислювально неможливим знаходження секретного ключа за сформованим підписом. Спробуємо забезпечити цю властивість шляхом використання одноразового додаткового відкритого ключа *r*, який формується підписувачем за формулою

$$r = \alpha^k \pmod p,$$

де *k* випадкове число, що вибирається. Тепер у нас появився додатковий параметр, який дає надію на нові можливості. Використаємо наступне рівняння перевірки підпису:

$$\alpha^h = y^S r \pmod p.$$

Йому відповідає рівняння формування підпису *s* =(*x/kh)* (mod (*p-1*)). Тепер уже за значеннями *s, r* і *h* обчислення секретного ключа являється обчислювально складною задачою. Легко побачити, що значення одноразового секретного ключа *k* необхідно тримати в секреті (при знанні *k* перевіряючий легко зможе обчислити секретний ключ). Так як він необхідний тільки для формування підпису, то його краще *знищити зразу після обчислення підпису.* Відмітимо також, що при формуванні параметра *r* необхідно вибрати таке число *k,* яке являється взаємно простим з числом *p – 1*. Тоді при *h*, взаємно простому з *p-1,* існує і можна знайти число, обернене до *kh,* і обчислити *s*. Однак значення хеш-функції являється випадковим і в загальному випадку може містити загальний множник з *p -1*. Це показує ще одну обставину, яку необхідно враховувати при побудові системи ЕЦП. А саме, бажано отримати таке рівняння формування підпису, в якому знаменник містить параметри, які ми можемо вибрати таким шляхом, щоб вони мали значення, взаємно просте з *p – 1*. В розглядаємому прикладі підписом служить пара чисел (*s, r*), тобто підпис став в два рази довшим, але ми суттєво наблизилися до того, що обчислення секретного ключа стало неможливим за значеннями параметрів, використовуваних для перевірки підпису. Однак важливо, щоб наявність підпису до одного документу не давала можливість сформувати підпис до другого документу. Може бути, що це обчислювально можливо і без обчислення секретного ключа. Аналіз даного питання показує, що це дійсно так. Наприклад, нехай маємо підпис (*s, r*) до документу, що відповідає значенню хеш-функції *h.* Розглянемо документ, хеш-функція від якого дорівнює *h',* і постараємося сформувати правильний підпис (*s' r '*) до нього. Нам необхідно вибрати такі значення *s'* і *r'*, щоб виконувалася умова $a^h = yV \pmod p$. Ліву частину останнього співвідношення можна перетворити наступним способом:

$$a''' - -(a'')'''''' = (y\ г)'''''' = 0''')''''''\ г'''''' = y\ ''''''\ г''''''\ (\mathrm{mod}\ p).$$

Із останнього співвідношення видно, що можна взяти пару чисел *s' = sh'/h* (mod (*p-1*)) і *r'- r'^llh (modp),* які будуть являтися дійсним підписом до другого документу. Таким чином, ми приходимо до висновку, що останнє рівняння перевірки підпису все ще вимагає модернізації, оскільки, маючи один зразок підпису, можна легко обчислити правильний підпис до будь-якого іншого документу, хоча до появлення першого правильного підпису це зробити обчислювально складно. Проводячи аналогічний аналіз наступних рівнянь перевірки підпису

$$a \text{ - } (yr)''(modp) \text{ і } (or)^{*}=y' \text{ (mod}p),$$

виявляємо, що вони також допускають формування нових підписів без знання секретного ключа при умові, що є один правильний підпис, сформоваий з використанням секретного ключа. При проведенні такого аналізу легко прийти до висновку, що відносно простим варіантом модернізації являється використання значення одноразового відкритого ключа не тільки як основи одного із співмножників, наявних в рівнянні перевірки підпису, але також і в якості степеня того ж самого або іншого співмножника. Проаналізуємо наступне рівняння перевірки і формування підпису:

$$_{a}'''' = yV(\text{mod } (p) \text{ і } s \text{ - } (hr - kVx) \text{ } (mod\ p - I).$$

Для коректного формування підпису необхідно вибрати випадковий секретний ключ, взаємно простий з *p*- 1. Для заданої хеш-функції *h* сформувати підпис без знання секретного ключа представляється обчислювально складною задачою, зв'язаною з розв'язуванням проблеми дискретного логарифмування. Дана пара рівнянь може використовуватися в якості системи ЕЦП, хоча деяким недоліком останньої являється указане обмеження (НСД(*r,*(*p— 1*))= 1) на вибір секретного ключа. З метою усунення обмеження на вибір секретного ключа спробуємо інший варіант ЕЦП, отримуваний із попереднього шляхом перестановки параметрів *s* і *h:*

$$h^{fr} = yV(\text{mod } p) \text{ і } s \text{ - } (hx + k)lr \text{ (mod } (p\text{-}1)).$$

Тепер необхідно сформувати значення *r,* взаємно просте з *p* - I. До виконаня цієї перевірки треба виконати операцію піднесення до великого цілого степеня, що трохи ускладнює знаходження значення, взаємно простого з *p - 1*. Крім того, ця операція перевірки на взаємну простоту повинна тепер виконуватися при кожній процедурі підписування повідомлень (якщо використовувати одне і те ж значення *r* для підписуваня двох різних повідомлень, то можна зробити два різних рівняння формування підпису з двома невідомими *x* і *A,* що дозволить легко обчислити секретний ключ *x*). З цими незначними недоліками можна було б змиритися, але кінцева дискредитація

нашого удосконалення зв'язана з тим, що без знання секретного ключа можна сформувати правильний підпис до будь-якого заданого документа. Дійсно, нехай h є хеш-функція від нього. Виберемо довільне k і обчислимо значення $r = ct'y'^{1}' (\mathrm{mod}\ p)$.

Якщо НСД (r, (p - 1)) > 1, то виберемо інше k і будемо повторювати обчислення до тих пір, поки не отримаємо НСД (r, (p - 1)) = 1. Після цього обчислимо підпис s за формулою s = A/f (mod (p- 1)). Легко перевірити, що отримані значення (r, s) задовольняють рівнянню перевірки підпису.

У випадку системи ЕЦП з рівнянням перевірки підпису $a^{hr} = \hat{r}$ (mod p) для довільного значення s можна аналогічним способом без знання секретного ключа сформувати значення хеш-функції $h = k/r$, для якого (r, s) являється правильним підписом. Однак тепер це не є принциповим недоліком, оскільки при стійкій хеш-функції обчислювально неможливо підібрати документ, хеш-функція від якого була б рівною наперед заданому випадковому h (В розглядаємому випадку це зв'язано з тим, що при формуванні r довільно вибираються k і s, але не представляється можливим отримати наперед задані значення для r, $к$, h, тобто, останнє являється обчислювально складним). Якби замість хеш-функції використовувалося значення повідомлення h (де, припустимо, $m < p$), то ми могли б говорити, що в останньому прикладі є можливість сформувати випадкове повідомлення m і підпис до нього. Тільки в рідкісних випадках використання систем ЕЦП така обставина являється суттєвим недоліком, що робить недопустимим застосування аналогічної ЕЦП. Використання значення хеш-функції (в рівнянні перевірки підпису) від повідомлень будь-якого (в тому числі і малого) розміру знімає цю проблему у випадку ЕЦП, які допускають можливість без знання секретного ключа знайти деяке випадкове h і правильний до нього підпис (h'', s). Багато варіантів ЕЦП, які розглядаються як стійкі, мають цю особливість. Застосовуючи піднесення значення r до степеня h або r, можна отримати дуже велике число різних варіантів стійких ЕЦП.

Певний інтерес представляє ЕЦП з рівнянням обчислення підпису $s = xr + kh$ (mod (p - 1)), в якому відсутня операція ділення, тобто не треба вводити обмеження вибору значень, взаємно простих з модулем p- 1.

Однак це не знімає перераховані зауваження до розглядаємих систем ЕЦП. Усунення недоліків може бути досягнуто застосуванням в якості степеня деякої стійкої хеш-функції $F'(r, h)$ від двох аргументів - h і r (легко бачити, що r повинно входити в рівняння безпосередньо, оскільки при використанні хеш-функції від r навіть при відомому секретному ключі обчислення правильного підпису буде обчислювально нездійсненно). Ця модернізація уводить додаткову процедуру - обчислення функції F або F', що несуттєво збільшує складність формування і перепровірки підпису. Можливі варіанти усунення згаданих недоліків і іншими способами, наприклад, використанням в якості степенів обох функцій F і F' або функції $F''(h)$ разом з початковим значенням h. Використання тільки значення $F''(h)$ в якості степеня (або співмножника степеня) уводить

визначену специфіку, наприклад, може виявитися, що, підбираючи разом *r*, *F''(A)* і *h* , можна знайти такі значення цих трьох параметрів, які задовольняють рівнянню перевірки підпису. Однак при використанні стійкої хеш-функції в цьому випадку практично не можливо здійснити знаходження значення *h*, яке б давало необхідне значення *F''(h).* Якщо б в рівняння перевірки підпису входило безпосередньо значення підписуваного повідомлення *m,* то уведення замість *m* значення *F''(m)* мало б принциповий характер. При початковому використанні значення стійкої хеш-функції *h(m)* від повідомлення *m* уведення функції *F''(h)* принципових змін не вносить, оскільки значення деяких підібраних *h* , *s* і *r*, які задовольняють рівнянню перевірки підпису, являються випадковими, а обчислення повідомлення, яке нібито підписане, є практично нерозв'язуваною задачою. Тому заміна *h(m)* на *F''(h(m))* в конкретному сенсі еквівалентна простій зміні алгоритму хешування початкового документу, тобто, це не впливає на властивості рівнянь перевірки і формування підпису. Відразу відмітимо, що уведення функцій *h(m)*, *F* і *F''* окремо або усіх відразу не приведе автоматично до усунення усіх слабкостей системи ЕЦП. Після їх введення необхідно провести відповідний аналіз заново сформованої системи ЕЦП.

7.2 Скорочення довжини підпису

Крім розглянутих вище варіантів стійких ЕЦП, заснованих на задачі дискретного логарифмування, існує багато інших. Для практичного використання можна рекомендовати ті із них, які вимагають виконання перевірки і формування підпису з найменшою трудомісткістю, але стійкість яких не нижче складності задачі дискретного логарифмування. Відмітимо також, що рівняння перевірки підпису і відповідні йому рівняння формування підпису можуть бути задані в різних формах, наприклад, представлених в табл. 7.1.

Таблиця 7.1 Варіанти задавання систем ЕЦП

Рівняння перевірки підпису	Рівняння для обчислення *,v*	
	За модулем *p - 1* (*a* - первісний корінь за mod p)	За модулем *q* (*a*— число, що належить показнику *q за mod p)*
$a^a = y^b r^c \pmod p$	*a = bx + ck (mod p-1)*	*a = bx + ck mod q*
$y^a = a^b r^c \pmod p$	*Ax = b + ck (mod p-1)*	*ax = b + ck mod q*
$r^a = a^b y^c \pmod p$	*Ak = b + cx (mod p-1)*	*ak = b + cx mod q*
$r^a a^b = y^c \pmod p$	*Ak + b = cx (mod p-1)*	*ak + b + cx mod q*
$r^a a^b y^c = 1 \pmod p$	*ak + b + cx= (mod p-1)*	*ak + b + cx =1 mod q*

Рівняння перевірки підпису може бути задано в двох варіантах: за модулем *p - 1* або за модулем деякого числа *q,* що являється дільником числа *p-1* і має розмір 160 і більше бітів. Відомо, що будь-який дільник числа *p - 1* являється

показником за модулем простого *p.* Для будь-якого показника існують числа β що не перевершують *p - 2,* для яких виконуються наступні умови:1) $\beta^q = 1 (\text{mod } p)$ і 2) усі числа $\beta, \beta^1, \beta^2, ..., \beta^q$ являються непорівнянними між собою за модулем *p.* Ці умови забезпечують можливість використання рівнянь формування підпису за модулем *q,* який за розміром значно менше *p,* що приводить до отримання значень $s < q$. Причому для формування підпису без знання секретного ключа необхідно вирішити задачу дискретного логарифмування за модулем *p,* тобто, таке скорочення розміру числа *s* не знижує початкової стійкості системи ЕЦП.

Таким чином, використання рівняння обчислення підпису за модулем дільника числа *p - 1* дозволяє скоротити довжину одного із параметрів підпису, а саме значення *s*. При цьому незалежно від довжини простого модуля *p* останній завжди можна вибирати таким способом, щоб довжина *q* не перевищувала 160-256 бітів. Це дозволяє скоротити довжину підпису *(s, r)* майже в два рази в порівнянні із випадком використання рівняння обчислення підпису за модулем *p - 1*. Дійсно, значення r $(r < p)$ має довжину приблизно рівну довжині *p,* яка із міркувань забезпечення високої стійкості повинна бути біля 1000 бітів або більше. Для вказаної довжини модуля *p* при використанні 160-бітового показника *q* можна оцінити, що довжина підпису скорочується приблизно в 1,7 рази. При цьому з метою підвищення стійкості ЕЦП можна збільшувати розмір модуля *p,* зберігаючи розмір показника *q*. Стійкість ЕЦП буде визначатися тільки довжиною простого числа *p* і правильністю вибору рівняння перевірки підпису.

При виборі варіанту з обчисленням підпису за модулем *q* ми будемо вважати, що в якості *a* вибирається деяке число, що відноситься до показника *q* за модулем *p,* тобто, таке число, для якого виконується співвідношення

$$\alpha^q = 1 \bmod p,$$

де *q* являється дільником числа *p - 1* необхідного розміру. Припускається, що при формуванні простого числа *p* забезпечується наявність дільника, який має необхідний розмір, наприклад 160 або 256 бітів. При цьому в розкладанні числа *p - 1* на множники бажано мати один із дільників великого розміру, який суттєво перевищує розмір *q,* оскільки наявність великого простого дільника у великому степені знижує складність задачі дискретного логарифмування за модулем *p.* Існують різні способи формування простих чисел, що задовольняють цим умовам. В табл. 7.2 приводяться прийнятні для застосування варіанти ЕЦП, які задані рівняннями перевірки і формування підпису. В табл. 7.2 використовуються **с**истеми ЕЦП із скороченою довжиною підпису, де $r' = r \pmod q$ і $a^q = 1 \pmod p$.

В системах ЕЦП, представлених в табл. 7,2, в якості r' можна взяти значення деякої хеш-функції F від r, тобто взяти $r' = F(r)$. Є також можливість скоротити другий параметр підпису, а саме, значення *r*. Ідея такого скорочення спирається на той факт, що, якщо права і ліва частини рівняння перевірки

підпису порівнянні за модулем *p,* то залишки від ділення лівої і правої частин на *p* будуть порівнянні за модулем *q*. Здійснюється це наступним способом.

Таблиця 7.2

Рівняння для обчислення s	Рівняння перевірки підпису
$r'k = s + hx(\mathrm{mod}\, q)$	$r^{r'} = a^h y^s (\mathrm{mod}\ p)$
$r'k = h + sx(\mathrm{mod}\, q)$	$r^{r'} = a^h y^s (\mathrm{mod}\ p)$
$sk = r' + hx(\mathrm{mod}\, q)$	$r^s = a^{r'} y^h (\mathrm{mod}\ p)$
$sk = h + r'x(\mathrm{mod}\, q)$	$r^s = a^h y^{r'} (\mathrm{mod}\ p)$
$hk = s + r'x(\mathrm{mod}\, q)$	$r^h = a^s y^{r'} (\mathrm{mod}\ p)$
$hk = r' + sx(\mathrm{mod}\, q)$	$r^h = a^{r'} y^s (\mathrm{mod}\ p)$

Вибирається рівняння перевірки підпису вигляду $R^a = a^b y^c (\mathrm{mod}\ \ p)$ і перетворюється до еквівалентного вигляду

$$R \equiv a^u y^v (\mathrm{mod}\ \ p), \text{ тобто, } (R\ \ \mathrm{mod}\ \ p) \equiv (a^u y^v \mathrm{mod}\ \ p),$$

де $u = ba^{-1}(\mathrm{mod}\ \ q)$, $v = ca^{-1}(\mathrm{mod}\ \ q)$, а R формується з використанням випадково вибираємого числа *k,* яке являється одноразовим секретним ключем, у відповідності з формулою $R = a^{k1}(\mathrm{mod}\ \ p)$. Потім рівняння перевірки перетворюють до вигляду $(R \bmod p) \equiv ((a^u y^v \bmod p) \bmod q)$, тобто $((R \bmod p) \bmod q) = ((a^u y^v \bmod p) \bmod q)$. В останній формулі необхідно задати залежність пари чисел *u* і *v* від хеш-функції документу, що підписується, *h* і підпису (*r*, *s*), де $r = ((R \bmod p) \bmod q)$. Тепер уже обидва елементи підпису (тобто *r* і *s)* мають значення, що не перевищують *q*. Довжина підпису скорочується в 4 — 6 разів (в залежності від довжини модулів *q* і *p*). Аналогічну конструкцію мають перші варіанти американського і російського стандартів цифрового підпису, які прийняті в 90-х роках. В якості параметру *r* можна взяти значення хеш-функції: $r = F(R \bmod p)$. В цьому випадку рівняння перевірки підпису має вигляд

$$r = F(a^u y^v \bmod p).$$

Відмітимо, що в останньому рівнянні пара чисел *u* і *v* залежать від *h* і $r = F(R \bmod p)$. Таблиця 7.3 показує можливі варіанти представлення параметрів *u* і *v* через *h,r* і *s*. Відмітимо, що в цих варіантах немає проблеми вибору значень, обернених числам *h, r* і *s,* які зв'язані із забезпеченням взаємної простоти з модулем, оскільки вирази для формування підпису записуються за модулем простого числа *q*. Це являється ше однією перевагою переходу до модуля *q*. В табл. 7.3 приведені варіанти задавання ЕЦП із скороченою довжиною підпису *(r,* s).

Таблиця 7.3

Параметр *u*	Параметр *v*
$r^{-1}s \bmod q$	$r^{-1}h \bmod q$
$r^{-1}h^{-1}s \bmod q$	$r^{-1}h^{-1} \bmod q$
$r^{-1}s \bmod q$	$r^{-1}h^{-1} \bmod q$
$h^{-1}s \bmod q$	$r^{-1}h^{-1} \bmod q$
$h^{-1}r \bmod q$	$s^{-1}h^{-1}s \bmod q$

Дуже значною перевагою ЕЦП, заснованих на складності задачі дискретного логарифмування, являється те, що вони дозволяють розробити варіанти із відносно малим розміром підпису. При цьому, якщо будуть запропоновані нові методи дискретного логарифмування, які вимагають збільшення розміру модуля *p,* то останнє можна зробити без збільшення розміру підпису. У випадку цифрового підпису RSA збільшення розміру модуля приводить до збільшення розміру підпису.

7.3 Приклади аналізу слабких ЕЦП

Під слабкими системами ЕЦП будемо розуміти ті із них, які допускають підробку підпису. Останнє означає формування підпису до деякого апріорі заданого повідомлення без знання секретного ключа. Як ми уже згадували, багато які системи ЕЦП, що розглядаються як стійкі, допускають можливість формування без знання секретного ключа випадкових значень *h* і *(r,s),* які задовольняють рівнянню перевірки підпису, тобто *(r,s)* являється правильним підписом до *h.* Однак ці ж системи ЕЦП практично не дозволяють обчислити правильний підпис до заданого документу або вказаної хеш-функції, якщо секретний ключ невідомий.

Приклади, які розглядаються нижче для слабких ЕЦП, складені в близькій аналогії до побудови стійких ЕЦП. Однак деякі зовнішні незначні відмінності вносять недопустиму слабкість - можливість формування потенціальним порушником (який не знає секретного ключа) правильного підпису до заданого значення *h.* В основі такої підробки лежить ідея представлення параметра *r* у вигляді $r = a^z y^w s \bmod p$, де значення степенів *w* і *z* вибираються наперед (фіксуються), а потім виражаються через значення *h, s* і *r* (замість *r* може фігурувати *r', F(r)* або *F'(h,r)* в залежності від конкретного вигляду рівняння перевірки підпису. При цьому виявляється така ситуація: значення *r, r', F(r)* і *F'(h,r)* залежать від одного або обох значень *w* і *z,* а останні залежать від *r*. Це протиріччя знімається тим, що величини *w* і *z* розглядаються як зафіксовані, що досягається вписуванням за рахунок вибору значень *h* і *s* з врахуванням обчислених (за фіксованими *w* і *r*) значень *r, r', F(r)* і *F'(h,r).*

Приклад 7.1. Рівняння підпису виду $r = y^h a^{rs} \bmod p$. Здійснимо підробку підпису без знання секретного ключа. Нехай заданий деякий документ, хеш-функція від якого дорівнює *h.* Далі діємо за наступним алгоритмом.

1. Вибрати деяке значення *z*.
2. Обчислити $r = a^z y^h \bmod p$.
3. Якщо НСД (*r*, (*p*- *1*))> 1, то повторити кроки 1 і 2, поки не виконається умова НСД(*r*,(*p*- *1*))= 1.
4. Обчислити $s = z / r (\bmod (p-1))$, тобто отримаємо $z = sr (\bmod (p-1))$.
5. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r, s)*.

Підставляючи в ліву частину рівняння перевірки підпису значення $r = y^h a^{rs} \bmod p$, бачимо, що права і ліва частини співпадають, тобто сформований підпис є правильним.

Приклад 7.2. Рівняння підпису виду $a^r = y^{hs} r^s \bmod p$. Нехай заданий деякий документ, хеш-функція від якого дорівнює *h*. Зловмисник може діяти за наступною схемою.

1. Вибрати деяке значення *r*, таке, що НСД (*r*,(*p-1*)) = 1.
2. Обчислити $r = a^z y^{-h} (\bmod p)$.
3. Обчислити $s = r / z (\bmod (p-1))$.
4. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r,s)*.

Підставляючи в праву частину рівняння перевірки підпису значення $sz = r (\bmod p-1)$ і $r = a^z y^{-h} (\bmod p)$ отримаємо $y^{hs} a^{zs} y^{-hs} = a^r (\bmod p)$,тобто права частина співпадає з лівою. Це означає, що сформований підпис правильний.

Приклад 7.3. Рівняння підпису виду $a^{hs} = y^r r^s \bmod p$. Нехай заданий деякий документ, хеш-функція від якого рівна *h*. Зловмисник може діяти за наступною схемою.

1. Вибрати деяке значення *w*, таке, що НСД (*w*,(*p-1*)) = 1.
2. Обчислити $r = a^h y^{-w} (\bmod p)$.
3. Обчислити $s = r / w (\bmod p-1)$
4. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r,s)*.

Підставляючи в праву частину рівняння перевірки підпису значення $r = ws (\bmod (p-1))$ і $r = a^h y^{-w} (\bmod p)$, отримаємо $y^{ws} a^{hs} y^{-ws} = a^{hs} (\bmod p)$. Співпадіння лівої і правої частин рівняння перевірки показує, що сформований (без знання секретного ключа) підпис являється правильним.

Приклад 7.4. Рівняння підпису виду $a^{hs} = y^{rf(h)} r^s \bmod p$, де *f(h)* є довільна функція від *h*. Нехай заданий деякий документ, хеш-функція від якого рівна *h*. Підробка підпису здійснюється у відповідності із наступним алгоритмом.

1. Вибрати деяке значення *w*, таке, що НСД (*w*,(*p-1*)) = 1.
2. Обчислити $r = a^h y^{-w} (\bmod p)$.
3. Обчислити $s = (rf(h) / w) (\bmod (p-1))$.
4. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r,s)*.

Підставляючи в праву частину рівняння перевірки підпису значення добутку $rf(h) = ws (\bmod (p-1))$ і $r = a^h y^{-w} (\bmod p)$, отримаємо $y^{ws} a^{hs} y^{-ws} = a^{hs} (\bmod p)$. Співпадіння лівої і правої частин рівняння перевірки показує, що сформований підпис *(r,s)* являється правильним.

Приклад 7.5. Рівняння підпису виду $r^{f(h)} = a^h y^{rs} \bmod p$, де *f(h)* є довільна функція від *h*. Для того, щоб підробити підпис до деякого документу, порушник може діяти наступним способом.

1. Обчислити хеш-функцію *h* від документу.
2. Якщо НСД (*f(h)*,(*p-1*)) > 1, то модифікувати документ, зберігаючи його семантичний зміст, і повторити крок 1, в іншому випадку перейти до наступного кроку алгоритму.
3. Вибрати значення $z = h / f(h) (\mathrm{mod}(p-1))$ і $w = rs / f(h) (\mathrm{mod}(p-1))$.
4. Обчислити $r = a^z y^w (\mathrm{mod}\ p)$.
5. Обчислити $s = (wf(h)/r)\ (\mathrm{mod}(p-1))$.
6. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r,s)*.

Підставляючи в ліву частину рівняння перевірки підпису значення, $r = a^z y^w (\mathrm{mod}\ p)$,отримаємо $r^{f(h)} = a^{zf(h)} y^{wf(h)} = a^h y^{rs} (\mathrm{mod}\ p)$. Співпадіння лівої і правої частин рівняння перевірки показує правильність сформованого підпису *(r,s)* до документу, підібраному порушником.

Приклад 7.6. Рівняння підпису виду $r^{F(r)} = a^{hs} y^{sf(h)} \bmod p$, де *f(h)* і *F(r)* є довільні функції від *h* і *r* відповідно. Для того, щоб підробити підпис до деякого документу, порушник може діяти наступним способом.

Нехай заданий деякий документ. Підробка підпису здійснюється у відповідності із наступним алгоритмом.

1. Обчислити хеш-функцію *h* від документу.
2. Якщо НСД (*f(h)*,(*p-1*)) > 1, то модифікувати документ, зберігаючи його семантичний зміст, і повторити крок 1, в іншому випадку перейти до наступного кроку алгоритму.
3. Вибрати пару значень *z* і *w* таких, що $z / w = h / f(h)$.
4. Обчислити $r = a^z y^w (\mathrm{mod}\ p)$ і *F(r)*.
5. Якщо НСД (*F(r)*,(*p-1*)) > 1, то повторити кроки 3 і 4, в іншому випадку перейти до наступного кроку алгоритму.
6. Обчислити $s = wF(r) / f(h) (\mathrm{mod}(p-1))$.
7. Пред'явити в якості підпису до хеш-функції *h* пару чисел *(r,s)*.

Із виразу в п. 6 легко отримати $w = sf(h) / F(r) (\mathrm{mod}(p-1))$ і $z = wh / f(h) = sh / F(r) (\mathrm{mod}(p-1))$.

Підставляючи в ліву частину рівняння перевірки підпису значення $r = a^z y^w (\mathrm{mod}\ p)$, отримаємо $r^{F(r)} = a^{zF(r)} y^{wF(r)} = a^{sh} y^{sf(h)} \bmod p$. Співпадіння лівої і правої частин рівняння перевірки показує правильність сформованого підпису *(r,s)* до документу.

Способи підробки підпису, які розглянуті в цих прикладах, можуть бути використані і в схемах ЕЦП із скороченим підписом, причому в деяких випадках задача формування підпису без знання секретного ключа спрощується, оскільки не вимагається підбирати деякі значення таким способом, щоб вони були

взаємно простими з *p— 1*, оскільки модуль *q*, який використовується замість *p-1*, являється простим.

7.4 Системи ЕЦП з додатковими властивостями

Представляє інтерес побудувати таку систему ЕЦП, в якій було б обчислювально складним сформувати правильний підпис не тільки до заздалегідь заданого значення хеш-функції, але і до значення *h*, яке підбирається поряд із значеннями *r* і *s*. При наявності трьох параметрів налаштування задача формування підпису без знання секретного ключа сильно спрощується, однак в цьому випадку всі три указані значення попередньо не визначені і виявляються випадковими. При такому "налаштуванні" порушник може знайти "правильну" пару *h* і *(r, s)*, але підібрати повідомлення (документ), який відповідає отриманому значенню *h*, він не зможе (передбачається, що використовується стійка хеш-функція). Розглянемо, як можна отримати "правильну" пару *h* і *(r, s)* у випадку ЕЦП Ель-Гамаля, рівняння перевірки підпису якого має вигляд:

$$a^h = y^r r^s (\mathrm{mod}\, p).$$

Задамо наступну структуру числа $r = a^z y^{-w} (\mathrm{mod}\, p)$. Виберемо випадкові значення *h* і *s* такі, що НСД *(z, (p - 1))* = 1 і НСД (*w,(p- 1)*)= 1, і обчислимо значення $r = a^z y^{-w} (\mathrm{mod}\, p)$. Значення *h* і *s* визначимо за формулами:

$$h = sz (\mathrm{mod}\, (p-1)) \text{ і } s = r/w (\mathrm{mod}\, (p-1)).$$

Знайдені значення *h* і *(r, s)* задовольняють рівнянню перевірки підпису. Дійсно, права частина рівняння Ель-Гамаля переписується в наступному вигляді $y^r a^{zs} y^{-ws} = y^r a^h y^{-wr/w} = a^h (\mathrm{mod}\, p)$. Цей аналіз показує, що в рівнянні Ель-Гамаля небажано використовувати значення повідомлення *m,* оскільки в цьому випадку є можливість сформувати підпис до яких-небудь випадкових повідомлень. Даний факт має місце і в ЕЦП RSA, але не являється катастрофічним для переважної більшості застосувань систем цифрового підпису. Однак в деяких випадках така особливість може виявитися принциповою слабкістю.

Розглянемо ще одне інтересне порівняння із системою RSA. В останній перевірка підпису полягає в розшифруванні (відновленні) підписаного повідомлення. Це означає, що для значущих повідомлень (тобто, які мають деяку очікувану структуру) достатньо передати перевіряючому тільки підпис. Процедура перевірки підпису (розшифрування за відкритим ключем) відновлює повідомлення. Як ми бачили вище в розглянутих системах ЕЦП, заснованих на задачі дискретного логарифмування, необхідно пред'явити одночасно і підпис, і підписане повідомлення. Представляє інтерес перетворити останній тип ЕЦП таким способом, щоб процедура перевірки підпису відновлювала повідомлення. Це можна зробити, використовуючи наступне рівняння перевірки підпису:

$$m = a^s y^{F(r)} r (\mathrm{mod}\ p),$$

де *F(r)* - деяка функція від *r,* наприклад $F(r) = r' = r \bmod q$. Формування цифрового підпису до повідомлення *m* здійснюється наступним способом. Вибрати випадкове число *k* і обчислити значення *r* за формулою:

$$r = ma^k (\mathrm{mod}\ p),$$

Значення *s* обчислюється із співвідношення

$$s = -xF(r) - k(\mathrm{mod}\ (p-1)).$$

Перевірка підпису *(r, s)* полягає в підстановці даних значень в рівняння перевірки підпису, що приводить до отримання «значущого» повідомлення з очікуваною структурою. Фактично перевірка полягає в розшифруванні криптограми (*r, s*). Очевидно, що підстановка в рівняння перевірки будь-якої пари випадкових значень *r* і *s* приведе до отримання деякого значення *m,* яке буде випадковим. Якщо в деякому конкретному протоколі цього достатньо, щоб зробити висновок, що це незаконний підпис, то таку систему ЕЦП з відновленням повідомлення допустимо використовувати. Однак в ряді додатків необхідно підписувати випадкові повідомлення. В таких випадках можна використовувати наступну схему.

До повідомлення *m,* яке необхідно підписати і передати по відкритому каналу, приєднується заздалегідь установлений двійковий вектор *v,* який має, наприклад, розмір *l* = 64 бітів: $M \to m|v$.

Розглянемо приклади.

Виробляється підпис (*r, s)* для повідомлення *M.*

Перевіряюча сторона за значенням підпису *(r,s)* обчислює текст *M',* відповідаюче йому значення двійкового вектора $v' = M' \bmod 2$ і повідомлення $m' = M' div 2$.

Якщо *v'* дорівнює наперед узгодженому значенню *v,* тобто, якщо виконується умова *v'= v,* то приймається рішення, що повідомлення *m'* підписано власником секретного ключа, що відповідає відкритому ключу, за допомогою якого виконувалася перевірка підпису (імовірність того, що випадкове повідомлення може бути прийняте за підписане, достатньо мала і складає 2^{-l}).

Другим способом забезпечити можливість стійкого підписування довільних повідомлень являється використання значення деякої хеш-функції *h(m)* від повідомлення *m* в якості степеня при параметрі *r* в рівнянні перевірки підпису. В такій схемі ЕЦП з відновленням повідомлення параметр *r* формується у відповідності з формулою

$$r = m^{1/h} a^k (\mathrm{mod}\ p).$$

В цьому випадку рівняння перевірки підпису має вигляд

$$m = a^s y^r r^h (\mathrm{mod}\ p)$$

Значення параметру обчислюється із співвідношення

$$s = -xr - kh(\mathrm{mod}\ (p-1)).$$

Недоліком цього варіанту ЕЦП являється те, що повинна виконуватися умова НСД(*h*,(*p-1*)). Тому деякі повідомлення *m* потрібно модифікувати із збереженням семантичного змісту декілька разів, поки не буде отримано від нього значення *h*, взаємно просте з *p - 1*. Для практики це являється істотним недоліком. В цій схемі в якості підпису фігурують уже три параметри *(r, s, h*), що являється певним недоліком, зв'язаним із збільшенням його розміру. Цей недолік дещо згладжується, якщо використовувати схеми ЕЦП з скороченою довжиною підпису. Замість функції *h(m)* можна використовувати саме значення *m,* але тоді зникає властивість відновлення повідомлення із підпису, що було оригінальною метою модифікації ЕЦП.

В табл. 7.4 приведені більш складні схеми побудови систем ЕЦП з відновленням повідомлення, в яких значення *r* обчислюється за формулою $r = ma^k \pmod p$, а α відноситься до показника $q|(p-1)$, тобто $a^q \pmod p = 1$. В цих схемах забезпечується зменшення розміру параметра *s*. В табл. 7.4 приведені системи ЕЦП з відновленням повідомлення, де *a* ціле число - таке, що $a^q = 1 \pmod p$, $r' = r \bmod q$, а *f(h), f(r)* і *f(h, r)* є функції з областю значень $0 < f < q$.

Таблиця 7.4

Рівняння для обчислення значення s	Рівняння перевірки підпису	Підпис до *m*
$s + xr' f(h) + k = 0 \bmod q$	$m = a^s y^{r' f(h)} r \pmod p$	*(r, s, h)*
$s + xf(h,r) + k = 0 \bmod q$	$m = a^s y^{f(h,r)} r \pmod p$	*(r, s, h)*
$r' + xsf(h) + k = 0 \bmod q$	$m = a^{r'} y^{sf(h)} r \pmod p$	*(r, x, h)*
$r' + xs + k = 0 \bmod q$	$m = a^{r'} y^s r \pmod p$	*(r, s)*
$r' + xsf(r) + k = 0 \bmod q$	$m = a^{r'} y^{sf(h)} r \pmod p$	*(r, s)*
$sf(r) + xr' + k = 0 \bmod q$	$m = a^{sf(r)} y^{r'} r \pmod p$	*(r, s)*
$r's + xf(h,r) + k = 0 \bmod q$	$m = a^{r's} y^{f(h,r)} r \pmod p$	*(r, s, h)*
$r' f(h) + xs + k = 0 \bmod q$	$m = a^{r' f(h)} y^s r \pmod p$	*(r, s, h)*

Вище ми описали системи ЕЦП, засновані на складності задачі дискретного логарифмування за модулем простого числа. Очевидно, що для кожного із розглянутих варіантів ЕЦП даного типу може бути запропонований аналог для складеного модуля *N*. Рівняння перевірки і формування підпису зберігає свій вигляд повністю, якщо врахувати, що *p— 1* є функція Ейлера від модуля. При цьому усі варіанти скорочення розміру елементів підпису *r* і *s* і рівняння перевірки підпису з відновленням повідомлення можуть бути також реалізовані. Відмітимо деякі особливості, які зв'язані з використанням складеного модуля. При спеціальному виборі складеного модуля можна зробити так, що функція Ейлера від нього буде секретним елементом, тобто частиною секретного ключа, який відомий тільки одному користувачеві. З цією метою можна передбачити

наступні дії із сторони власника секретного ключа. Він вибирає два великих простих числа p і q і перемножує їх, отримуючи модуль $N = pq$. Значення N приймається в якості частини відкритого ключа (y, N), а значення простих співмножників тримається в секреті або знищується після обчислення $\varphi(N) = (p-1)(q-1)$. В цьому випадку формування підпису до повідомлення m для випадку рівняння перевірки виду $a^h = y^s \pmod p$ не дозволить перевіряючому обчислити секретний ключ, що було можливим при простому модулі p. Складною проблемою для перевіряючого являється обчислення значення $\varphi(N)$, оскільки він не знає розкладання модуля на множники. Систему ЕЦП з таким рівнянням перевірки можна назвати одноразовою ЕЦП, оскільки при формуванні підписів s_1 і s_2 до двох різних повідомлень виникають попередні вимоги для обчислення $\varphi(N)$ і секретного ключа x. Дійсно, при наявності двох підписів є наступна система із двох рівнянь з невідомими x і $\varphi(N)$:

$$h(m) = xs_1 \varphi(N);$$
$$h(m) = xs_2 \varphi(N).$$

Зауваження.

Практичні незручності одноразового підпису очевидні: після підписання одного документу поточний відкритий ключ не повинен бути використаний для формування підпису до другого документу (хоча для формування загального секрету у відповідності до системи Діффі-Хеллмана він може використовуватися далі). Його розгляд має тільки методичне значення. В цьому плані необхідно також указати, что значення a для деяких N (різні користувачі формують різні значення модуля) уже не буде первісним коренем, однак на коректність роботи розглядаємої системи одноразового підпису і його стійкості це практично не впливає (імовірність того, що для якого-небудь N число a виявиться пов'язаним з показником невеликого розміру, є незначним). Довжина числа a може бути вибрана порівняно невеликою (менше розміру використовуваних значень p і q), що дозволяє не розглядати випадки, коли НСД $(a, p) \neq 1$, або НСД $(a, q) \neq 1$.

Для забезпечення можливості підписування багатьох повідомлень без заміни секретного ключа x потрібно увести використання одноразового відкритого ключа $r = a^k \bmod N$. В результаті приходимо до приблизних варіантів ЕЦП, представлених в табл. 7.5. В даних прикладах одна і та ж хеш-функція h використовується для хешування повідомлення m і значення r. В табл. 7.5 приведені системи ЕЦП із складеним модулем $N = pq$.

Таблиця 7.5

Рівняння для обчислення x	Рівняння перевірки підпису	Показник, до якого (відноситьс я)	Підпис К m
$h(m) = xr + ks(\mathrm{mod}\,\varphi(N))$	$a^{h(m)} = y^r r^s \bmod N$	$\varphi(N)$	(r,s)
$h(m) = xr + ks(\mathrm{mod}\,\varphi(q))$	$a^{h(m)} = y^r r^s \bmod N$	$\varphi(q)$	(r,s)
$h(m) = xr + ks(\mathrm{mod}\,\delta)$	$a^{h(m)} = y^r r^s \bmod N$	$\delta \mid \varphi(q)$	(r,s)
$h(r) + xs + k = 0(\mathrm{mod}\,\delta)$, де $r = ma^k \bmod N$	$m = a^{h(r)} y^s r \bmod N$	$\delta \mid \varphi(q)$	(r,s)
$h(r)k = s + h(m)x(\mathrm{mod}\,\delta)$	$h(r) = h(a^{s/h(r)} y^{h(m)/h(r)} \bmod N$	$\delta \mid \varphi(q)$	$(h(r),s)$
$r'k = s + h(m)x(\mathrm{mod}\,\delta)$, де $r' = (a^k \bmod N) \bmod \delta$	$r' = (a^{s/r'} y^{h(m)/r'} \bmod N) \bmod \delta$	$\delta \mid \varphi(q)$	(r',s)

7.5 Сліпий підпис

Ряд важливих для практичного застосування криптографічних систем включають в себе як складову частину протокол сліпого підпису. До них відносяться системи тайного електронного голосування і електронних грошей. Смисл сліпого підпису полягає в тому, що власник секретного ключа повинен мати можливість здійснювати підписування повідомлення, представленого в зашифрованій формі. Необхідно, щоб сторона, яка підготовила повідомлення (документ), була впевнена в тому, що підписавший не прочитає його. Як це не дивно на перший погляд, але доцільність в системах сліпого підпису є. Більше того, без них не обійтися. Дотепне і красиве рішення побудови сліпого підпису на основі використання системи RSA було запропоновано Чаумом, воно базується на використанні особливостей перетворювань системи RSA. Чи можлива побудова деякого варіанту сліпого підпису з використанням ЕЦП, заснованих на складності дискретного логарифмування? Неважко побудувати протокол сліпого підпису з використанням будь-якої системи ЕЦП. Це рішення передбачає сам принцип обчислення підпису до повідомлень великого розміру, використовуваний на практиці. Як відомо, документи (повідомлення) великого розміру підписуються наступним способом.

Нехай дано повідомлення *m.* Від повідомлення *m* обчислюється хеш-функція *h(m),* значення якої має розмір 160- або 256-бітового числа. Формується підпис *S* до значення хеш-функції. Якщо використовувана хеш-функція являється криптографічно стійкою, то можна вважати, що підписування значення хеш-функції еквівалентно підписуванню самого повідомлення *m.* Враховуючи, що за значенням хеш-функції неможливо відновити само повідомлення, приходимо до наступного варіанту універсального сліпого підпису. Абонент *X* готує деяке повідомлення *m,* яке йому необхідно підписати у

абонента *Y* таким чином, щоб останній не знав його змісту, але в той же час підпис був правильний (дійсний). Потім *X* обчислює за наперед передбаченим алгоритмом значення хеш-функції *h(m),* яке він і забезпечить абоненту *Y* для підписування, а само повідомлення *m* тримає в секреті. Абонент *Y* підписує значення $h = h(m)$, тобто обчислює значення *S*. Природно, що за значенням *h* він не може визначити *m*. Абонент *X* отримує значення *S,* після чого, коли потрібно, він може представити повідомлення *m* і правильний до нього підпис *S*. Перевагою цього універсального варіанту сліпого підпису являється те, що він працює ефективно з повідомленнями будь-якого розміру.

Даний варіант універсального сліпого підпису підкреслює проблему забезпечення анонімності в повному об'ємі. Метою систем сліпого підпису являється забезпечення анонімності (невідслідковуваності), але підписуючий, отримавши можливість ознайомитися з деякими підписаними ним «всліпу» документами, має можливість обчислити значення хеш-функції і порівняти із списком хеш-функцій указуванням осіб, які представляли ці хеш-функції для підписування документів «всліпу». Таким чином, рішення задачі забезпечення анонімності в повному об'ємі на основі описаної системи універсального сліпого підпису з очевидністю вимагає використання інших додаткових механізмів.

Анонімність необхідна, наприклад, в системах електронних грошей, де підписуючим виступає банк, який підписує "всліпу" електронні банкноти одним клієнтам (покупці), тоді як представляють електронні гроші для нарахування на свій рахунок інші особи (продавці). Анонімність електронних грошей полягає в тому, що банк не повинен мати можливість визначати ту особу, від якої продавець отримав гроші при продажу свого товару.

На основі складності задачі дискретного логарифмування можуть бути розроблені різні часткові варіанти сліпого підпису. Розглянемо систему ЕЦП з відновленням повідомлення із наступним рівнянням перевірки підпису:

$$m = a^s y^r r (\mathrm{mod}\, p),$$

де $r = ma^k (\mathrm{mod}\, p)$. На основі цієї ЕЦП неважко здійснити підписування "всліпу». Для цього підготовимо документ $m' = ma' (\mathrm{mod}\, p)$, де *m* - випадкове число, що не перевищує *p* - 1. Представляємо *m'* для підписування. Від підписуючого отримаємо підпис *(s', r).* На основі отриманого підпису формуємо новий підпис (*s,r),* де $s = s' - t (\mathrm{mod}\, (p-1))$, який являється правильним для повідомлення *m.* Дійсно, підпис (*s',r*) задовольняє рівнянню

$$m' = a^{s'} y^r r = a^{s'} y^r r (\mathrm{mod}\, p).$$

Розділивши за модулем *p* ліву і праву частини рівняння на *a',* отримаємо

$$m = m' a^{-1} = a^{s'-1} y^r r = a^s y^r r (\mathrm{mod}\, p).$$

Отже, сформований нами підпис (*s,r*) являється правильним для повідомлення *m.* Якщо значення $s = s' - t (\mathrm{mod}\ (p-1))$ тримати в секреті від підписуючого, то він не зможе визначити значення *m.* В іншому випадку він зможе обчислити $m = m'a'$. Проблема забезпечення анонімності залишається відкритою і для цієї схеми. Дійсно, підписуючий може вести облік значень *m'* і *r* (Насправді для того, щоб порушити анонімність, достатньо фіксувати тільки *r).*

Вільною від указаного недоліку являється схема сліпого підпису Чаума (див. вище). Дійсно, деяка особа формує значення *m',* яке зв'язане з документом *m,* який необхідно підписати «всліпу», наступним співвідношенням $m' = k^e m (\mathrm{mod}\ N)$, де *k* - деяке випадкове число, що невідоме підписуючому, і *e* - експонента відкритого ключа *(e,N)* підписуючого. Останній, використовуючи свій секретний ключ, формує до повідомлення *m'* підпис $s' = (k^e m)^d (\mathrm{mod}\ N)$, де $s = m^d \bmod N$ є правильний підпис до документу *m.* Підписавший не може визначити значення *s* по *s'* , так як він не знає значення *k.* Навіть при ведені ним обліку підписаних значень *m'* з указуванням осіб, які ці значення формували для підписування, при пред'явленні йому в подальшому відповідних один одному значень *M* і *S* він не зможе доказово визначити значення *M* ' , яке містить в собі момент підписування документу *M.* Дійсно, для будь-якої пари *m'* і *s'* із облікового списку існує деяке *k*, таке, що $m' = k^e M \bmod N$. При цьому для відповідних значень *s'* і *S* буде виконуватися умова *s'= kS.* Більше того, підписуючий не зможе навіть переконливо доказати, що на момент підписування він не був ознайомлений з документом *M.*

7.6 Проблема безключового шифрування

В криптоаналізі відоме поняття безключового шифрування, що полягає в читанні шифртексту без відновлення секретного ключа, з використанням якого була отримана криптограма. А чи можливо здійснити «безключове шифрування», тобто деяке перетворення початкового тексту таким способом, щоб отримувач зміг його відновити, а порушник, який перехопив перетворенний текст, не зміг? До відкриття Діффі і Хеллманом двоключової криптографії ніхто серйозно би не сприйняв постановку такої задачі. Двоключова криптографія за своєю природою зв'язана із взаємодією користувачів криптосистеми. Можливо, зазначену задачу неможливо розв'язати з використанням тільки однієї передачі по каналу зв'язку. А з використанням протоколів можна попробувати. Уточнимо постановку задачі: розробити протокол «безключового шифрування», в якому не використовується передача ключа (секретного або відкритого), але який забезпечує захищену передачу повідомлень по відкритому каналу.

Двоключова (асиметрична) криптографія спирається на розприділення відкритих ключів і рішення проблеми їх аутентифікації іншими методами, тобто, для того, щоб деякий двоключовий шифр забезпечував рішення задачі організації секретного зв'язку з використанням відкритих каналів, необхідно попередньо вирішити задачу аутентифікації розподілених відкритих ключів.

Великі переваги шифрів з відкритим ключем зумовлені тим, що задача аутентифікації відкритих ключів розв'язується набагато простіше і набагато дешевше, чим задача розприділення секретних ключів від одноключових криптосистем, які вимагають використання захищених каналів. В останньому виді криптосистем аутентифікація ключів поєднана з процедурою їх розприділення. В асиметричних криптосистемах немає проблеми розприділення секретних ключів і ефективно розв'язується проблема аутентифікації відкритих ключів.

Після того, як Діффі і Хеллман надрукували свою парадоксальну ідею побудови криптографічного протоколу, що дозволяє здійснювати передачу секретного ключа по відкритому каналу, інтерес до розробки різного виду протоколів і використанню функції піднесення у великий дискретний степінь за модулем великого простого числа прокинувся у широких колах дослідників. Зокрема, одним із перших інтригуючих протоколів з'явився протокол "безключового шифрування», тобто, система, що дозволяє передати секретне повідомлення по відкритому каналу взагалі без використання передачі секретного ключа. З точки зору класичної одноключової криптографії сама постановка такої задачі носить відтінок абсурдності, але якраз рішення нестандартних задач і являється центральним змістом двоключової криптографії. Оскільки двоключові шифри вирішують таку задачу з використанням шифрування за відкритим ключем, то система «безключового шифрування» представляє інтерес як протокол, що розв'язує поставлену задачу без використання передачі не тільки секретного, але і відкритого ключа.

Розглянемо варіант побудови системи «безключового шифрування», що називається по імені свого винахідника трьохпроходним протоколом Шаміра. В дійсності застосовуються навіть два ключі шифрування, але ні один із них не передається по будь-якому каналу, тобто, вони використовуються локально кожним із взаємодіючих абонентів. В цьому протоколі використовується комутативний симетричний шифр, для якого виконується умова:

$$E_A(E_B(m)) = E_B(E_A(m)),$$

де E_K є функція шифрування по ключу K, а параметри A і B являються секретними ключами двох взаємодіючих абонентів A і B відповідно. Протокол включає наступні кроки:

1. Абонент A шифрує повідомлення m, отримує шифртекст $c_1 = E_A(m)$ і посилає c_1 абоненту B.
2. Абонент B зашифровує повідомлення c_1 (тепер повідомлення m зашифровано двічі з використанням двох різних ключів), отримує шифртекст $c_2 = E_B(c_1)=E_b(E_A(m))$ і посилає c_2 абоненту A.
3. Абонент A, використовуючи процедуру розшифрування D, що перетворює повідомлення c_2, отримує шифртекст $c_3=D_A(c)=D_A(E_B(E_A(m)))=D_A(E_A(E_B(m)))=E_B(m)$ і посилає c_3 абоненту B.

Отримавши значення c_3, абонент *B* легко відновлює повідомлення $m = D_B(E_B(m))$. Цей протокол взагалі не вимагає обміну ні секретними, ні відкритими ключами. Найбільш складною проблемою являється побудова шифруючих перетворювань, які володіють властивістю комутативності і забезпечують високу криптостійкість цього протоколу. Властивість комутативності забезпечується процедурою шифрування, що заключається в накладанні за допомогою операції XOR $\oplus$ на повідомлення *m* ключа, довжина якого дорівює довжині *m*. Нехай ключі *A* і *B* являються випадковими рівноймовірними ключами, тоді окремо кожна із процедур шифрування $c_a = m \oplus A$ і $c_B = m \oplus B$ забезпечує абсолютну стійкість криптографічного перетворювання. Однак такий спосіб шифрування неприйнятний в розглядаємому протоколі. Дійсно, в цьому випадку на кроках I, 2 і 3 по відкритому каналу пересилаються повідомлення $c_1 = m \oplus A$; $c_2 = m \oplus A \oplus B$; $c_3 = m \oplus B$, а, отже, потенціальний порушник може легко обчислити $m = c_1 \oplus c_2 \oplus c_3$.

Насправді в цій системі передавачем і приймачем використовуються ключі індивідуального використання, які не вимагають того, щоб їх знала яка-небудь інша сторона. Але оскільки ключовий обмін відсутній, то ми говоримо про «безключове шифрування». Суть полягає в тому, що і передавач, і приймач формують деякі секретні параметри, але при цьому зовсім не вимагається їх передача партнеру по сеансу. Передавач зашифровує повідомлення і посилає його приймачеві. Приймач іще раз зашифровує повідомлення і повертає двократно зашифроване повідомлення передавачеві. Передавач розшифровує повідомлення, перетворюючи його в однократно зашифроване по ключу приймача, і відправляє його ще раз приймачеві. Тепер приймач, знаючи свій секрет, по якому він здійснював шифрування, виконує процедуру розшифрування і відновлює повідомлення, яке і хотів йому відправити передавач. Схема достатньо проста, але необхідно знайти такі процедури шифруючих перетворювань, виконуваних двома сторонами, які були б прозорі один відносно іншого. Ніякої складності не представляє знайти деяке пряме перетворювання початкого повідомлення і обернене йому, але зовсім не очевидно, що між прямим і оберненим перетворюваннями можна виконати деяке інше перетворювання і отримати той же результат, який би виявився, якщо б інше перетворювання виконувалося б відразу над початковим повідомленням. Принаймі, такі комутуючі перетворювання необхідно спеціально підбирати.

Незалежно один від одного А. Шамір і Дж. Омура описали алгоритм шифрування, який може використовуватися в описаному вище протоколі і використовує операцію піднесення у велику дискретну степінь за модулем великого простого числа *p* в якості шифруючої процедури. Причому при зашифруванні і розшифруванні здійснюється піднесення в різний степінь. Нехай зашифроване повідомлення $m < p$ полягає в піднесенні до степеня, тобто, значення шифртекста дорівнює $c = m^e \pmod p$, тоді для правильного розшифрування треба знайти такий степінь *d*, що буде виконуватися умова $ed = 1(\mathrm{mod}\,(p-1))$. Із теорії чисел відомо, що остання умова справедлива для будь-якого *m*, якщо має місце умова $sd = 1 \pmod{(p-1)}$. Також відомо, що якщо

вибрати e взаємно простим з p-1, то для такого e існує і за допомогою розширеного алгоритму Евкліда легко знаходиться відповідне йому обернене (за модулем p- 1) число d, що задовольняє останній умові.

Таким чином, приходимо до працюючого протоколу «безключового шифрування», що включає передачу наступних значень c_1 ,c_2 і c_3:

$C_1 = me_A$, де e_A є ключ зашифрування абонента A;

$c_2 = c_1 e_A e_B \pmod p$, де e_B є ключ зашифрування абонента B;

$c_3 = C_2\ d_A = m\ e_A e_B d_A = m\ e_B\ (mod\ p)$, де d_A є ключ розшифрування абонента A.

Отримавши шифртекст c_3, абонент B легко розшифровує повідомлення $m = c_3$.

Дійсно, маємо $c_3\ d_B = m\ e_B d_B = m\ (mod\ p)$. В даному випадку за значеннями c_1, c_2 і c_3 порушник не може відновити повідомлення, що передається, оскільки для цього йому прийдеться розв'язувати задачу дискретного логарифмування, що являється обчислювально нездійсненною при правильному виборі простого числа p. Наприклад, порушник за значеннями c_2 і c_3 попробує обчислити d_A і відновити повідомлення $m = c_1\ d_A \pmod p$. Таким чином, ми маємо систему, в якій використовуються наступні параметри:

p - велике просте число, таке, що розкладання числа p- 1 містить, принаймі, один великий простий множник;

a - первісний корінь за модулем p.

Також передбачається, що передавач A формує пару чисел e_A і d_A, взаємно простих з $p - 1$, таких, що $e_A d_A = 1\ (mod\ (p - 1))$, а приймач B - пару чисел e_B і d_B, взаємно простих з p - 1, таких, що $e_B d_B = 1\ (mod\ (p- 1))$. Протокол передачі секретного повідомлення m від A до B включає наступні кроки:

1. Передавач обчислює значення $c_1 = m\ e_A\ (mod\ p)$ і відправляє c_1 приймачеві (цей крок відповідає вкладенню повідомленин в корпус і закриттю корпуса на перший замок.)

2. Приймач, отримавши значення c_1, обчислює $c_2 = c_1\ d_B = m\ e_A s_e\ (mod\ p)$ і відправляє c_2 передавачеві (цей крок відповідає додатковому блокуванню корпуса на другий замок.)

3. Передавач, отримавши значення c_2, обчислює $c_3 = c_2\ a_d = m\ e_A r_e\ d = m\ b_e\ (mod\ p)$ і відправляє c_3 приймачеві (цей крок відповідає відкриттю першого замка. Корпус з повідомленням залишається закритим тільки на замок, встановлений отримувачем.

4. Приймач, отримавши значення c_3, обчислює $c_4 = c_3\ d_B = m\ e_B d_B = m(mod\ p)$, тобто відновлює повідомлення, яке йому направлене передавачем.

В результаті виконання протоколу секретне повідомлення виявляється переправленим від одного абонента до іншого по відкритому каналу, причому для цього не потрібний обмін ключами (ні секретними, ні відкритими). Насправді можна, як би там не було, говорити про пересилку ключа в неявному вигляді. Дійсно, передаваєме зашифроване повідомлення містить в собі інформацію як про повідомлення, так і про використані ключі, однак розділення

цієї інформації представляє собою обчислювально складну задачу. Тільки власник пари відповідаючих один одному ключів зашифрування і розшифрування може накладати і повністю знімати «шифруючий ефект». В якості повідомлення цим способом може бути переданий по відкритому каналу секретний ключ, який потім може бути використаний для виконання шифрування повідомлень, що передаються з використанням деякого симетричного шифру. Іншими словами, розглянутий протокол може використовуватися як система відкритого розприділення ключів (але для цього ще треба вирішити проблему аутентифікації повідомлень, що передаються).

Однак необхідно мати на увазі, що в аналогічній системі відкритого розприділення ключів вирішення проблеми аутентифікації повідомлень являється суттєво більш складною задачою у порівнянні із системою Діффі-Хеллмана. Це зумовлено тим, що в протоколі «безключового шифрування» відсутні відкриті ключі, аутентифікацію яких можна забезпечити, не розкриваючи секретного ключа (той, хто сформував пару відповідаючих один одному відкритого і секретного ключів, повинен залишатися єдиним власником секретного ключа). Протокол «безключового шифрування» стикається з серйозною проблемою аутентифікації. При встановленні сеансу зв'язку законні абоненти якось повинні підтвердити свою автентичність. А це просто дуже зручно робити з використанням аутентифікованих ключів (відкритих або закритих). Оскільки повідомлення може бути змінено в процесі пересилання (наприклад, по розгалудженій комп'ютерній мережі), то кожне повідомлення повинно бути аутентифіковано. Якщо цього не виконувати, то ні про яку серйозну стійкість протоколу «безключового шифрування» говорити не приходиться.

Таким чином, цей гарний протокол демонструє нові можливості і ідеї, які зв'язані із застосуванням криптографічних протоколів, але для практичного застосування вимагає подальшого удосконалення. Наприклад, він може бути перетворений в систему відкритого розприділення ключів, в якій деякими додатковими методами вирішується проблема аутентифікації відкритих ключів. В розглянутому вище протоколі кожний із користувачів формував два різних ключі - один для зашифрування, а інший для розшифрування, але обидва ключі являються секретними, оскільки по одному із них можна легко обчислити інший. Щоб один із них можна було б зробити відкритим, необхідно перетворити процедуру обчислення одного із них по іншому в обчислювально складну задачу. Згадаємо, що один із ключів вибирається випадково, а інший обчислюється як число, взаємно обернене значенню першого ключа за модулем $p - 1$. Останнє значення представляє собою функцію Ейлера від простого числа p. Якщо взяти замість простого числа p деяке складене n, то розглянута вище система також працює. Коректність роботи системи тепер буде засновуватися на теоремі Ейлера, яка стверджує, що для будь-якого m, взаємно простого з p, виконується співвідношення

$$m^{\phi(n)} = 1(\mathrm{mod}\, n) \text{ , або } m^{k\phi(n)} = 1(\mathrm{mod}\, n) \text{, або } m^{k\phi(n)+1} = m(\mathrm{mod}\, n),$$

де k є довільне натуральне число. Із останнього співвідношення видно, що для обчислення пари ключів необхідно використати співвідношення

$$ed = 1 \bmod \varphi(n).$$

При цьому появилася додаткова забота - обчислення функції Ейлера від складеного модуля n. Для чисел порівняно малого розміру ця задача не представляє проблеми, але для великих чисел ця задача може виявитися обчислювально невиконуваною. Дійсно, для обчислення функції Ейлера попередньо виконується розкладання n на прості множники, але може виявитися так, що в розкладанні n будуть присутні два або більше простих співмножників великої довжини, наприклад два множники довжиною не менше 500 бітів. Тоді ми навряд чи зможемо виконати розкладання повністю, а, отже, ми не зможемо знайти значення $\varphi(n)$. Але цього не зможе зробити і порушник, тому що, навіть знаючи один із парних ключів, він не зможе обчислити інший.

Неважко тепер думати, що законному користувачеві необхідно вибрати два великих (довжною біля 500 бітів) простих числа p і q і сформувати n як добуток цих чисел: $n = pq$. Для виконання зашифрування шляхом піднесення в деяку цілу степінь за модулем n не треба знати розкладання n, але для обчислення парного ключа без цього не обійтися. Таким способом, законний користувач може обчислити значення функції Ейлера $\varphi(n) = (p-1)(q-1)$, а потім сформувати пару ключів e і d, таку, що $ed = 1 \bmod \varphi(n)$. Один із ключів можна надати для загального користування, наприклад, ключ e, який називається ключем зашифрування (encryption key) або відкритим ключем. Другий ключ - ключ розшифрування (decryption key) або закритий ключ —користувач повинен тримати в секреті, оскільки якраз він дозволяє прочитати все те, що зашифроване з використанням відкритого ключа. Вибір модуля n, що представляє собою добуток двох великих простих чисел, визначає також і той факт, що імовірність того, що яке-небудь повідомлення m виявиться не взаємно простим з d, являється дуже малою. Але можна строго показати, що навіть і в цьому зневажливому випадку розшифрування по ключу d виконується коректно.

Розглянуту модифікацію системи «безключового шифрування» не врятувало її як систему, що не вимагає передачі ніяких ключів взагалі, оскільки для вирішення проблеми аутентифікації потрібно використовувати відкриті ключі і здійснювати їх аутентифікацію. Однак, використовуючи обчислення за складеним модулем n, стає можливим вирішити проблему аутентифікації передаваємих повідомлень і протокол «безключового шифрування» буде працювати в тому сенсі, що він не вимагає передачі секретного ключа або формування загального секрету для двох користувачів, як це мало місце в системі Діффі-Хеллмана.

Найбільш суттєвим результатом проведення обчислень за складеним модулем являється можливість відкритого використання одного із ключів. В модернізованій системі відкритий ключ дає можливість розшифрування повідомлень, які будуть зашифровані закритим ключем. Той факт, що деяка криптограма $s = m^d \bmod n$ правильно розшифрується по відкритому ключу в

початковий текст, тобто, має місце співвідношення $m = s^e \bmod n$, може служити підтвердженням того, що даний початковий текст був зашифрований з використанням секретного (закритого) ключа. Оскільки секретний ключ відомий тільки законному користувачеві, а саме тому, хто згенерував пару відповідних один одному взаємно обернених за модулем *f(i)* ключів, то факт правильного розшифрування криптограми *s* показує, що текст був зашифрований користувачем, якому належить відкритий ключ *e,* що приводить до правильного розшифрування *m.* Значення *s* фактично являється підписом (або печаткою) відправника до повідомлення *m,* що передається. Поява можливості аутентифікувати джерело повідомлення (документа) представляє собою основний результат переходу від простого до складеного модуля із спеціальною структурою. Модифікована система отримала назву системи цифрового підпису RSA, яка знайшла надзвичайно широке практичне застосування. Авторами системи RSA являються Р. Рівест (R. Rivest), А. Шамір (A. Shamir) і Л. Адлеман (L. Adleman). Процедура шифрування повідомлення за закритим ключем називається підписуванням. Шифрування підпису за відкритим ключем називається процедурою перевірки підпису. Швидкість шифрування, що забезпечується двоключовими (асиметричними) шифрами, на декілька порядків нижче швидкості, якою володіють одноключові (симетричні) криптосистеми. Тому найбільш ефективні гібридні криптосистеми, в яких інформація шифрується за допомогою одноключових шифрів, а розприділення сеансових ключів здійснюється по відкритому каналу за допомогою двоключових шифрів. Наприклад, використовуючи криптосистему RSA, можна легко обмінятися сеансовим ключем з будь-яким абонентом, зашифрувавши сеансовий ключ за допомогою його відкритого ключа. Зашифрований сеансовий ключ можна безпечно передати по відкритому каналу зв'язку, оскільки необхідним для розшифрування секретним ключем володіє тільки абонент, відкритий ключ якого був використаний для зашифрування. Для безпосереднього засекречування інформації двоключові шифри знаходять обмежене застосування. Незамінне їх значення полягає в тому, що вони являються основою технологій електронного документообігу.

7.7 ЕЦП на еліптичних кривих

7.7.1 Основні властивості еліптичних кривих

З метою застосування еліптичних кривих (ЕК) в криптографічних додатках необхідно розглянути ряд їх властивостей і знайти такі сімейства кривих, які підходять для побудови ефективних криптографічних конструкцій.

Нехай *GF(q)* представляє собою кінцеве поле з характеристикою *p* потужності *q=p″*. Рівняння еліптичної кривої *E(GF(q))* в афінних координатах разом з деякою спеціальною точкою ***O***, яку назвемо «точкою в нескінченності» або нульовою точкою, має вигляд:

$$\text{E(GF(q)): } y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6. \qquad (7.1)$$

Якщо характеристика поля *p>3,* тоді *E(GF(q))*: $y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p)$. Найбільш важливими параметрами кривої *E(GF(q))* являються: дискримінант $\Delta = -16(4a^3 + 27b^2)$ і інваріант $j = \frac{1728(4a)^3}{\Delta}$. Коефіцієнти *a, b* ЕК *E(GF(q)* за відомим інваріантом визначаються наступним способом:

$$\begin{cases} a \equiv 3k (\mathrm{mod}\, p) \\ b \equiv 2k (\mathrm{mod}\, p) \end{cases},$$

де $k = \frac{j}{1728 - j} (\mathrm{mod}\, p), j \neq 0, j \neq 1728$.

Рівняння ЕК над кінцевими полями *GF(q)* з різними значеннями характеристик представлені в табл. 7.1.

Розгляне додаткові властивості ЕК:

1. Якщо дискримінант $\Delta \neq 0$, крива називається неособливою;

2. Якщо дві криві мають однаковий інваріант *j*, тоді вони являються ізоморфними кривими;

3. Для кожної ЕК *E(GF(p))* існують так звані скручені ЕК *E(GF(p))*, що визначаються виразом:

$$\text{E(GF(p))}: \; y^2 \equiv x^3 + ac^2 x + bc^3 (\mathrm{mod}\, p), \qquad (7.2)$$

Таблиця 7.1

P	*E(CV(g))*	***j***
2	$Y^2 + ay = x^3 + bx + c$	0
2	$y^2 + xy = x^3 + ax^2 + b$	1/b
3	$y^2 = x^3 + ax + b$	0
3	$y^2 = x^3 + ax^2 + b$	$\neq 0$
$\neq 2, \neq 3$	$y^2 = x^3 + ax + b$	$\frac{1728(4a)^3}{\Delta}$

де *c*- квадратичний нелишок за модулем *p.* Криві *E(GF(p))* і *E(GF(p))* ізоморфні, тому скручені криві можуть використовуватися для побудови ЕК заданого порядку:

дві ЕК: $y^2 = x^3 + ax + b_{(1)}$ і $y^2 = x^3 + ax + b_{(2)}$ ізоморфні, якщо $y_{(1)}=u^3 y_{(2)}$, $x_{(1)}=u^2 x_{(2)}$, $a_{(1)}=u^4 a_{(2)}$, $b_{(1)}=u^6 b_{(2)}$, де $u \in GF(q), u \neq 0$.

Якщо поліном від *x* в правій частині рівняння ЕК над полем характеристики $p \neq 2$ і $p \neq 3$ не має кратних коренів, тоді крива являється неособливою. Для кінцевих полів Галуа з характеристиками *p=2* і *p=3* вимога

неособливості виконується автоматично. Множина точок ЕК разом з нульовою точкою *O* породжує кінцеву абелеву групу *A* відносно операції додавання, що уводиться нижче.

7.7.2 Груповий закон додавання точок на ЕК

При характеристиці поля $p>3$ рівняння ЕК, згідно табл. 7.1, має вигляд

$$E(GF(p)):\ y^2 \equiv x^3 + ax + b (\mathrm{mod}\ p). \qquad (7.3)$$

Операція перетворення точки кривої еквівалентна запису: $-(x,y)=(x,-y)$. Операція додавання точок кривої $P_1=(x_1,y_1)$ і $P_2=(x_2,y_2)$ у вигляді $P_3=P_1+P_2$ визначається наступними порівняннями:

$$\begin{cases} x_3 \equiv \lambda^2 - x_2 - x_1 (\mathrm{mod}\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p), \end{cases} \qquad (7.4)$$

де

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

При $P_1=P_2=(x_1\ y_1)$, $y \neq 0$. результат подвоєння точки P_1 отримаємо із виразу $2P_1=(x_3\ y_3)$,
де

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\mathrm{mod}\ p) \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p) \end{cases}, \qquad (7.5)$$

де

$$\lambda = \frac{3x + a}{2y_1} \mathrm{mod}\ p.$$

Безпосередньо із виразів (7.4, 7.5) видно, что точка в нескінченності виявляється при подвоєнні точки P_1 нульовою координатою y або при додаванні двох різних точок з однаковою координатою x.

Точка в нескінченності являється точкою перетину для правої частини рівняння ЕК. В загальному випадку одиничним елементом групи може бути будь-яка точка перетину, а груповий закон додавання точок буде заданий іншими формулами. Однак всі операції додавання в групі ізоморфні. На рис. 7 1 - 7.3 представлена геометрична інтерпретація групового закону додавання точок на ЕК. Рис. 7.1 відповідає випадку додавання двох різних точок $P_1 + P_2= (x_3\ y_3)$. На рис. 7.2 відбувається подвоєння точки $2P_1=(x_2\ —y_2)$ і, нарешті, рис. 7.3 відповідає випадку додавання двох різних точок, але з однаковою координатою x

$$P_1 + P_2 = \mathrm{O}.$$

Ряд криптографічних алгоритмів з відкритим ключем будуються на основі таких функцій, в яких обчислюється кратне деякого елемента абелевої групи *A*. Як відомо, абелевою групою називається група елементів множини *A*, що задовольняє комутативному закону $ba=ab$ для всіх $a, b, e \in A$. Із визначення

виходить, що будь-яка циклічна група являється абелевою, тому в подальшому будемо використовувати термін циклічна група.

Груповий закон додавання точок ЕК, як елементів циклічної групи, володіє наступною криптографічною властивістю. Нехай P і G - елементи (точки) циклічної підгрупи A кривої $E(GF(q))$, причому G являється примітивним елементом (генератором) цієї підгрупи. Тоді, якщо $P = n * G$, де $n \in GF(g)$ - секретний ключ (випадкове число), "*" — означає багаторазове додавання точки G, то знаходження числа n за двома заданими елементами $P \in A$ і $G \in A$ являється обчислювально складною задачою. Задача знаходження індекса n за двома заданими елементами групи стає обчислювально невиконуваною при розмірностях n в 120 бітів і більше. Далі для простоти будемо використовувати позначення $nG = n * G$.

При побудові еліптичних криптографічних конструкцій використовується циклічна підгрупа групи точок еліптичної кривої E, визначеної над кінцевим полем $GF(q)$,

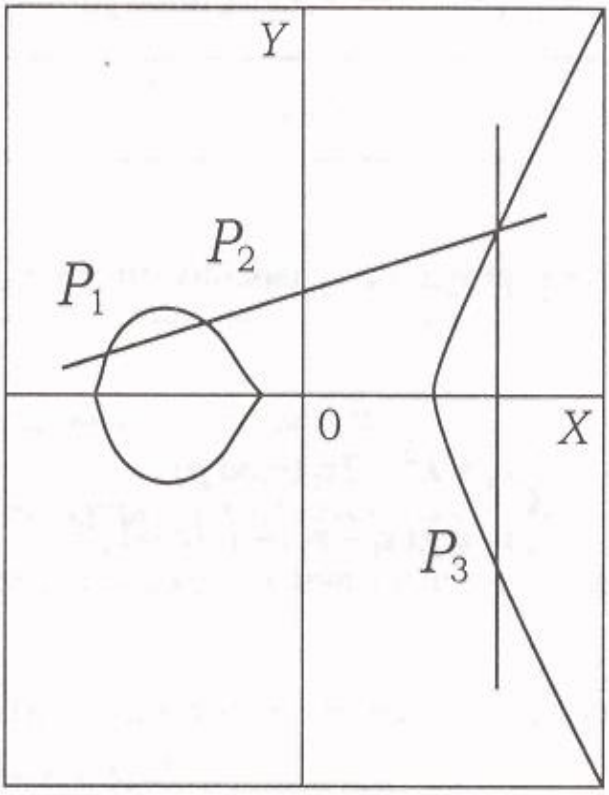


Рис.7.1.

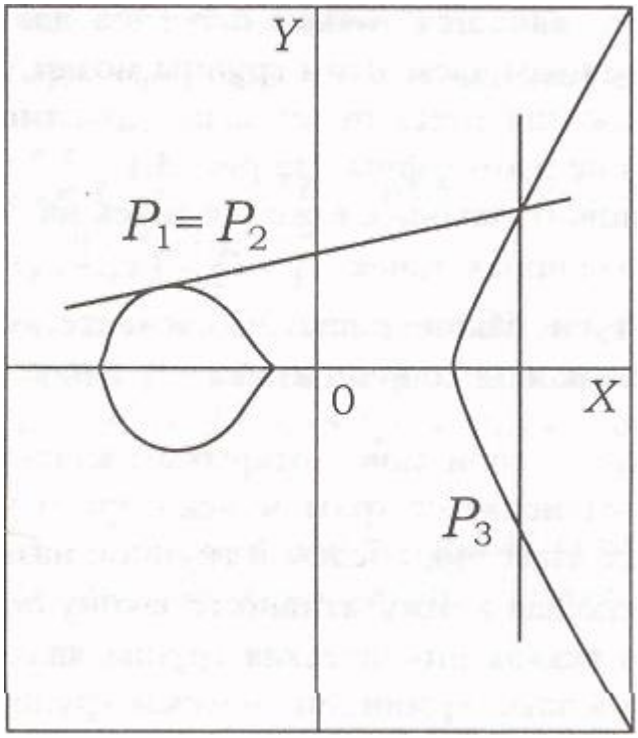


Рис. 7.2.

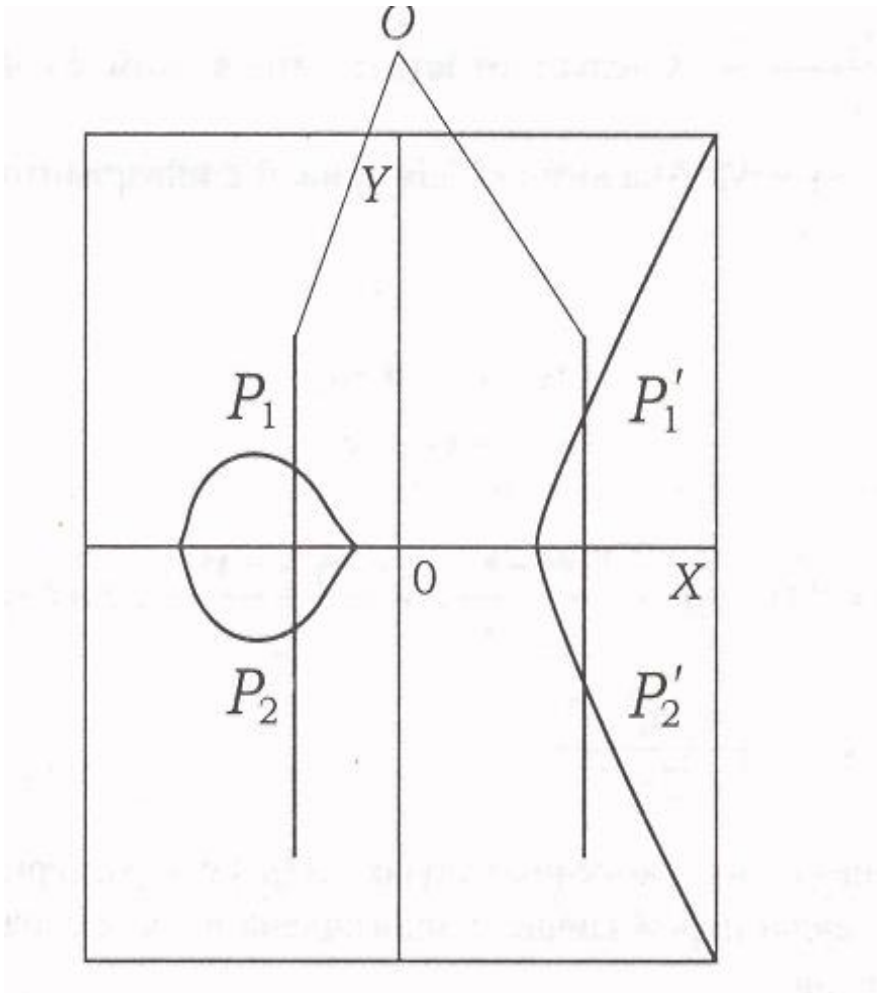


Рис. 7.3.

7.7.3 Груповий закон додавання точок ЕК над кінцевими полями з різною характеристикою *p*

Знайдемо вираз, який описує груповий закон додавання точок ЕК над полями з характеристикою $p \neq 2$ і $p \neq 3$. В цьому випадку рівняння кривих приймає вигляд, представлений в табл. 7.1 (вирази 1-4). Будемо розглядати криві з інваріантом *j=0*. Для таких кривих над розширеним кінцевим полем $GF(2^n)$ отримані формули, що визначають координати x_3, y_3:

$$\begin{cases} x_3 \equiv \lambda^2 + \lambda - a - x_1 - x_2, \\ y_3 \equiv -(\lambda + 1)x_3 - v, \end{cases} \tag{7.6}$$

де для випадку $P_1(x_1\ y_1) \neq P_2(x_2\ y_2)$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Якщо $P_1=P_2=(x_1\ y_1)$, маємо $\lambda = \frac{\partial y}{\partial x}$, диференціюючи даний вираз, отримаємо $\lambda = \frac{3x_2 + 2x_1}{2y_1 + x_1}$, $v = \frac{3x^3 + 2x^2 - 2y^2 - yx}{2y + x}$.

Необхідно відмітити, що в цьому випадку перетворення точки має вигляд $P_3=(x_3, -y_3-x_3)$. Аналогічно для кривої з інваріантом $j \neq 0$ над кінцевим полем $GF(3^n)$, де для

$$\begin{cases} x_3 \equiv \lambda^2 - a - x_1 - x_2, \\ y_3 \equiv -x_3\lambda - v \end{cases}$$

маємо:

$$P_1(x_1\ y_1) \neq P_2(x_2\ y_2), \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}. \tag{7.7}$$

Якщо $P_1=P_2=(x_1\ y_1)$, $\lambda = \frac{3x_2 + 2x_1 - a}{2y_1}$ і $v = \frac{3x^3 + 2x^2 - 2y^2}{2y}$.

Операції перемноження в кінцевих полях $GF(p^n)$ з характеристикою p=2 або $p=3$ проводяться за модулем породжуючого полінома поля, а додавання - за модулем 2 або 3 відповідно. Приведені групові закони додавання для кривих над полями з різними характеристиками можна використовувати в якості функцій криптографічного перетворювання для побудови різних протоколів захищеного обміну інформацією.

7.7.4 Способи підвищення швидкодії обчислень в циклічній групі точок ЕК

Перетворювання рівняння кривої a в проективні координати

В кільці цілих чисел Z_p і в полях Галуа *GF(q)* найбільш копіткою операцією являється інверсія. Щоб виключити дану операцію, необхідно перейти із афінних координат в проективні і зробити координату Z кратною знаменнику λ в виразах (7.4-7.7). Розглянемо рівняння кривої *E(GF(q)):* $Y^2 Z = X^3 + aXZ^2 + bZ^2$ над полем з характеристикою $p \neq 2$ і $p \neq 3$, що отримується переходом в проективні координати. В цьому випадку *E(GF(q))* можна розглядати як еквівалентний клас точок *(X, Y, Z)* на проективній площині p^2 над *GF(q).* Точка О в p^2 *GF(q)* представляє собою вагу ненульової точки з відношенням еквівалентності *(X, Y,Z) ~(aX, aY, aZ).* Позначимо ці точки як *(X, Y, Z)* . Відмітимо, що існує тільки одна точка з координатою Z=0 — це точка (0, 1, 0). Якщо Z=0, то і X=0, і існує тільки один клас еквівалентності з X=*0* і Z=*0*, а саме (0, 1,0). Як було показано раніше, це не що інше, як точка в нескінечнності O $\in$ E(GF(g)). Якщо P= *(X,Y,Z)* $\notin 0$, тоді, виконавши заміну *(X, Y, Z)* $= \frac{X}{Z}, \frac{Y}{Z}, 1,$ отримаємо однозначну відповідність точки (*X,Y,Z*) точці ($X = \frac{X}{Z}, Y = \frac{Y}{Z}$). Формули подвоєння точки для кривої над полем з $p \neq 3 и p \neq 3$ можна отримати із наступного представлення:

$$\begin{cases} X_3 = Z_3 x_3 \\ Y_3 = Z_3 y_3 \end{cases}, \tag{7.8}$$

де координата $Z_3 = 8Y_1^3 Z_z^3$ кратна λ. Після відповідних перетворювань отримаємо формули групового закону в проективних координатах. При подвоєнні точки вони мають вигляд:

$$\begin{cases} X_3 = 2Y_1 Z_1 [(3X_1^2 + aZ_a^2)^2 - 8X_1 Y_1^2 Z_1] \bmod p \\ Y_3 = 4Y_1^2 Z_1 \left[3X_1 \left(3X_1^2 + \alpha Z_a^2\right)^2 - 2Y_1^2 Z_1\right] - (2X_1^2 + \alpha Z_1^2)^3 \mid (\bmod p). \\ Z_3 = 8Y_1^3 Z_1^3 (\bmod p) \end{cases} \tag{7.9}$$

При додаванні двох різних точок візьмемо $Z_3 = Z_1 Z_2 (X_2 X_1 - X_1 Z_2)^3 (\bmod p)$, тоді:

$$\begin{cases} X_3 = (X_2 Z_1 - X_1 Z_2)\left[Z_1 Z_2 (Y_2 Z_1 - Y_1 Z_2)^2 - (X_2 Z_1 + X_1 Z_2) \cdot (X_2 Z_1 - X_1 Z_2)^2\right] (\bmod p) \\ Y_3 = (X_2 Z_1 - X_1 Z_2)^2 \left[Y_2 Z_1 (Y_2 Z_1 + 2Y_1 Z_2) - Y_1 Z_2 (X_2 Z_1 + 2X_1 Z_2)\right] - Z_1 Z_2 (Y_2 Z_1 - Y_1 Z_2)^3 (\bmod p) \end{cases} \tag{7.10}$$

Для кривих із табл. 7.1 з інтервалом $j \neq 0$ над розширеним полем GF(2^n), після здійснення аналогічного переходу до проективних координат, отримані наступні вирази, які описують груповий закон додавання точок:

при $P_1 = P_2$

$$\begin{cases} X_3 = X_1^4 + Z_1 X_1^3 (\mathrm{mod}\, g(x)) \\ Y_3 = (Z_1 X_1^6 + Z_1^3 X_1^4 + X_1 Y_1 Z_1) X_1 (\mathrm{mod}\, g(x)) \\ Z_3 = Z_1^2 X_1^2 (\mathrm{mod}\, g(x)) \end{cases} \qquad (7.11)$$

при $P_1 \neq P_2$

$$\begin{cases} X_3 = (X_2 Z_1 + X_1 Z_2)\left\langle Z_1 Z_2 \left[Z_1^2 (\alpha X_2^2 + Y_2^2) + Z_2^2 (\alpha X_1^2 + Y_1^2) + (Y_2 Z_1 + Y_1 Z_2) \cdot (X_2 Z_1 + X_1 Z_2) \right] \right\rangle \\ + X_2^2 Z_1^2 + X_1^2 Z_{12}^2 (\mathrm{mod}\, g(x)) \\ Y_3 = Z_1 Z_2 \left[(Y_2 Z_1 + Y_1 Z_2)^3 + \alpha (X_2 Z_1 + X_1 Z_2)^3 + (X_2^2 Z_1^2 + X_1^2 Z_2^2) \{ (Y_2 Z_1 + Y_1 Z_2) \cdot \right. \\ \left. (1+\alpha) + Y_1 X_2 (1 + X_2 Z_1) + Y_2 X_1 (1 + X_1 Z_2) \ \} \right] + X_2^2 Y_2 Z_1^3 + X_1^2 Y_2 Z_2^3 (\mathrm{mod}\, g(x)) \\ Z_3 = Z_1 Z_2 (X_2 Z_1 + X_1 Z_2)^3 (\mathrm{mod}\, g(x)) \end{cases} \qquad (7.12)$$

для кривих *E(GF(q))* над розширеним полем *GF(3)* з характеристикою *p=3* і інтервалом $j \neq 0$ при $P_1 = P_2$.

Відомо, що складність виконання перемноження в кінцевих полях оцінюється величиною *log^(q), •&*, ділення - *logq*, где *q* - кількість елементів (потужність) поля *GF(q).* Отже, не дивлячись на велику кількість операцій множення для групового закону в проективних координатах, результуюча кількість необхідних операцій для виконання перетворювання буде менше приблизно в *log(q)* раз у порівнянні з перетворюваннями в афінних координатах. Після виконання додавання в проективних координатах перехід до афінних координат здійснюється шляхом ділення X_3 і $У_3$ на координату Z_3.

Використання комплексного множення на ЕК

Для *ЕК £(GF(c/)), q-p",* визначеної рівнянням (7.2), існує відображення, що називається ендоморфізмом кривої *ф : (x,* у) —> (*Д**), *h(x, y)),* де (v, v) є *£(GF(q)),* $\phi(x,y) \in E(GF(q))$, $\phi(O) = O$, $f(x), h(x)$ - раціональні функції. Якщо група точок ЕК містить циклічну підгрупу *A*, таку, що порядок підгрупи ξ - просте число і не виконується умова подільності $\#E(GF(q)) \,|\, \xi^2$, тоді відображення ϕ переводить підгрупу *A* в себе або в нескінченно віддалену точку. В першому випадку ендоморфізм ЕК задає автоморфізм підгрупи *A*, для якого існує натуральне найменше число *l* - таке, що $\phi'(P) = P, P \in A, l \,|\, (\xi - 1)$. Так як ϕ являється автоморфізмом, тоді

$$\phi(P) = e(P), \qquad (7.13)$$

де $e < \xi$ - легко обчислюване число. Це відображення задає комплексне множення на ЕК. Наприклад, ЕК (7.2) з кофіцієнтами $a_1, a_2, \ldots, a, \in GF(p)$ має комплексне множення вигляду $\phi(x,y) = (x^p, y^p)$ з відповідним квадратним

характеристичним рівнянням. В табл. 7.2 представлені типи комплексного множення для різних рівнянь ЕК. Відображення вигляду $\phi(x,y)=(x^2,y^2)$ називається ендоморфізмом Фробеніуса.

Таблиця 7.2

Рівняння ЕК	Вид комплексного множення
$(7.3), a=0, p\equiv 1(\bmod 6)$	$\phi(x,y)=(wx-y)$ $w^3\equiv 1(\bmod p), \varphi^2+\varphi+1=0, e=\frac{1+\sqrt{-3}}{2}$
$(7.3), b=0, p\equiv 1(\bmod 4)$	$\phi(x,y)=(-x,iy)$ $i^2\equiv -1(\bmod p), \varphi^2+1=0, e=\frac{\sqrt{-1}}{2}$
$y^2+xy=x^3+1, p=2, n\geq 2$	$\phi(x,y)=(x_2,y_2)$ $\varphi^2+\varphi+2=0, e=\frac{-1+\sqrt{-7}}{2}$

Застосування властивостей комплексного множення для обчислення відображень в циклічній підгрупі *A* ЕК *E(GF(q))* дозволяє прискорити процедуру багатократного додавання точки *PeA* (множення точки на число) приблизно в два рази. В цьому випадку будь-яке число *m,* яке зв'язує дві точки, можна представити в вигляді

$$m<\sqrt{q}, m_1<\sqrt{q}\,. \qquad (7.14)$$

Після цього знаходяться точки m_0P, m_1P і на основі комплексного множення (7.14) точка *e(m,P).* Нарешті отримаємо $mP = (m_0P)+(e(m_1P))$. Спочатку комплексне множення було визначено для ЕК над полем комплексних чисел *C*, які визначаються своїм інваріантом *j*. Такого виду кривих дуже мало. Однак при переході до кінцевих полів, використовуючи метод побудови циклон ізогенез, можна розширити клас кривих, що володіють комплексним множенням.

Використання комплексного множення для відображення точок ЕК дозволяє понизити складність відображення майже в два рази в порівнянні з методом подвоєнь, заснованим на двійковому представленні числа, що зв'язує точки кривої.

7.7.5 Дослідження стійкості алгоритмів захисту інформації, які використовують еліптичні криптографічні конструкції

В п. 7.7.1 було показано, що стійкість алгоритмів захисту інформації визначається складністю знаходження індексу, який зв'язує два елементи абелевої групи точок на кривій. В якості показника ефективності захисту інформації (стійкості) при її перетворюванні на основі застосування групового

закону додавання в адитивній абелевій групі на ЕК доцільно застосовувати асимптотичну оцінку складності алгоритму аналізу в термінах O - символіки.

При використанні криптоалгоритмів, заснованих на дискретному логарифмуванні в кінцевх абелевих групах, складність розкриття суттєво залежить від порядку групи. При цьому алгоритм являється стійким, якщо в розкладанні порядку групи на прості множники зустрічається великий простий дільник. В іншому випадку шляхом переходу до підгруп і фактор-груп складність розкриття вдається значно понизити. Тому при оцінюванні складності аналізу криптоалгоритмів важливим являється обчислення порядку групи з наступним розкладанням його на прості множники. Для знаходження дискретного логарифму на ЕК можна застосовувати методи «зустрічі посередині» Сільвестра-Поліга-Хеллмана (СПХ), Полларда. Найбільш ефективними із них являються алгоритми СПХ і Полларда. Алгоритм СПХ має складність за часом S, = $O(\sqrt{r})$, а за пам'яттю S_c = $O(\sqrt{r})$, алгоритм Полларда має аналогічну часову складність і меншу складність за пам'яттю: $S_c = O(\log p)$. В обох випадках r означає найбільший простий множник порядку мультиплікативної групи поля p —*1*.

Застосовуючи дані алгоритми для адитивної циклічної групи точок ЕК, прийдемо до висновку, що стійкість аналогічних криптографічних конструкцій визначається як складність використовуваного алгоритму за визначенням індексу і дорівнює $O(\sqrt{\zeta p})$, де ζp - найбільший простий множник порядку групи точок ЕК. Крім того, для виключення відображення циклічної підгрупи групи точок ЕК на мультиплікативну групу деякого розширення $GF(p^n)$, яке є $GF(p^{n'})$, необхідно, щоб для вибраної кривої не виконувалися наступні умови подільності:

$$\#E(GF(p)) \mid (pn'-I), \qquad (7.15)$$

де I =1,2,.,., k. Необхідно використовувати криві, для яких ця властивість подільності не виконується при k > 30. В іншому випадку задача знаходження індексу на ЕК зводиться до задачі дискретного логарифмування в кінцевому полі. Відображення адитивної абелевої групи ЕК в мультиплікативну групу кінцевого поля засновано на використанні відображень Вейля. Це приводить до субекспоненціального алгоритму дискретного логарифмування в групі точок на кривій і відповідно до зниження стійкості криптосистеми, оскільки дискретні логарифми в кінцевих полях $GF(p'')$ можуть бути визначені за допомогою алгоритму Копперсміта із складністю $O(\exp(cn^{1/3})(\ln n)^{2/3}$, де c- невелика константа. Такого роду відображення не застосовується для невироджених кривих, інваріант яких не дорівнює нулю. Виходячи із цього факту, в п. 7.7.2 розглядалися тільки криві з ненульовим інваріантом. Крім того, атаки подібного виду на криптосистему можна ускладнити через побудову кривих з нульовим інваріантом, групу яких можна відобразити в мультиплікативну групу розширеного поля: $E(GF(p^n)) \mapsto GF(p^{\ln})$, де l- степінь розширення

початкового поля. Складність знаходження індексу в залежності від початкового поля і степеня розширення поля, де відображається група кривих, представлена в табл. 7.3. Із таблиці видно, що степінь розширення $l = 2$ забепечує порівнянну складність при малих розмірах ключа, тому необхідно відображати адитивну групу ЕК з нульовим інваріантом в мультиплікативну групу поля із степенем розширення $l > 4$.

Таблиця 7.3

Початкове поле GF(2'')	Складність знаходження індексу	Поле $GF(2^{ln})$	Складність знаходження індексу	Поле $GF(2^{4n})$	Складність знаходження індексу
$GF(2^{100})$	10^{15}	$GF(_2{}^{2*100})$	10^{17}	$GF(2^{4*100})$	10^{25}
$GF(2^{200})$	10^{30}	$GF(_2{}^{2*200})$	10^{25}	$GF(2^{4*200})$	$1O^{38}$
$GF(2^{300})$	10^{45}	$GF(_2{}^{2*300})$	10^{32}	$GF(2^{4*300})$	$1O^{45}$

В якості прикладу розглянемо дві криві над кільцем цілих чисел: $y^2 = x^3 + b \pmod p$, де $p = 5 \pmod 6$, і $y^2 = x^3 + ax \pmod p$, де $p = 3 \pmod 4$. Ці криві, згідно п. 7.7.2, мають порядок групи $\#E(GF(p)) = p + 1$, який ділить у відповідності з (7.7) число $p^2 - 1$. Тому задача дискретного логарифмування в групі на цих ЕК зводиться до задачі дискретного логарифмування в кінцевому полі $GF(p^2)$. Аналогічно вважається, що групу кривої $y^2 + y = x^3 + ax + b$ над полем $GF(2^n)$ можна відобразити в мультиплікативну групу поля $GF(2^{4n})$. Якщо порівнювати складність задач факторизації цілих чисел, дискретного логарифмування в мультиплікативних групах і дискретного логарифмування в адитивній абелевій групі точок ЕК, то останні виглядають кращими. Це показано в табл. 7.4, де представлене порівняння наближених оцінок складності криптоаналізу методів, заснованих, на розкладанні цілих чисел (РЦЧ), дискретному логарифмуванні в кінцевому полі (ДЛКП) і дискретному логарифмуванні в групі точок (ДЛГТ) ЕК для різних характеристик полів і в залежності від довжини ключа.

Приймаючи до уваги, що складність виконання перетворювання в абелевій групі ЕК оцінюється величиною $0(\log^2 q)$, а в мультиплікативній групі поля $0(\log^3 q)$, переваги використання перших для побудови криптосистем стають очевидними. Також необхідно відмітити, що криптографічні конструкції, складність аналізу яких перевищує значення 10, недоцільно застосовувати на практиці, так як ці значення перевершують можливості сучасних технологій з обробки інформації. Тому необхідно обмежуватися довжиною ключа до 400 бітів.

Таким чином, стійкість методів криптографічного перетворювання, заснованих на використанні групового закону додавання елементів адитивної абелевої групи на ЕК, помітно перевершують стійкість аналогічних методів, заснованих на використанні мультиплікативних полів. Виграш в стійкості особливо помітний при великих розмірах ключа. Ця обставина дозволяє використовувати

криптографічні конструкції подібного типу для побудови криптографічних протоколів різного призначення.

Таблиця 7.9

Довжина ключа (бітів)	Складність аналізу			
	РЦЧ для $\forall$ p	ДЛКП для $p=2$	ДЛКП для $p \neq 2$	ДЛГТ для $\forall p$
100	$1.3\text{-}10^{7}$	$1.3\text{-}10^{7}$	$1.6\text{-}10^{11}$	$1.1\text{-}10^{15}$
200	$7.2\text{-}10^{9}$	$7.2\text{-}10^{9}$	$9.6\text{-}10^{16}$	$1.3\text{-}1\ 0^{30}$
300	$7.1\text{-}10^{11}$	$7.1\text{-}10^{11}$	$3.8\text{-}10^{21}$	$1.4\text{-}10^{45}$
400	3.10^{13}	3.10^{13}	$3.4\text{-}1\ 0^{25}$	$1.6\text{-}\ 10^{60}$
500	$7.5\text{-}10^{14}$	$7.5\text{-}10^{14}$	$1.2\text{-}1\ 0^{24}$	$1.8\text{-}10^{75}$
600	$1.3\text{-}10^{16}$	$1.3\text{-}10^{16}$	$2.1\text{-}10^{32}$	$2\text{-}\ 10^{90}$
700	$1.7\text{-}10^{17}$	$1.7\text{-}10^{17}$	$2.1\text{-}10^{35}$	$2.3\text{-}10^{105}$
800	$1.8\text{-}10^{18}$	$1.8\text{-}10^{18}$	$1.4\text{-}10^{38}$	$2.6\text{-}10^{120}$
900	$1.7\text{-}10^{19}$	$1.7\text{-}10^{19}$	$6.5\text{-}10^{40}$	$2.9\text{-}10^{135}$
1000	$1.3\text{-}1\ 0^{20}$	$1.3\text{-}1\ 0^{20}$	$2.3\text{-}10^{43}$	$3.3\text{-I}0^{150}$

7.7.6 Алгоритми вибору ЕК

Синтез криптографічних конструкцій на ЕК, що задовольняють показникам стійкості, вимагають, в першу чергу, вибору наступних параметрів:

1) виду кінцевого поля;
2) характеристики поля і (або) його розширення;
3) рівняння ЕК;
4) порядку циклічної підгрупи точок ЕК;
5) генератора підгрупи точок ЕК.

Від вибору цих параметрів суттєво залежить стійкість криптографічних конструкцій і безпека протоколів на ЕК. Однією із головних умов являється те, що підгрупа групи точок вибраної кривої повинна бути циклічною з точкою, яка відіграє роль примітивного елементу (генератора) підгрупи. Якщо порядок групи - просте число, тоді будь-який елемент групи може служити її генератором.

Підходи до визначення порядку групи

Порядок групи точок ЕК являється залежним параметром і визначається видом кінцевого поля, характеристикою кінцевого поля, степенем його розширення, а також коефіцієнтами рівняння кривої. Відомо, що число розв'язків рівняння $x^n=a$ знаходиться із виразу $N(x^n) = a = \sum_{x^n} \chi(a)$, де сума приймається по всім мультиплікативним характерам χ, порядок яких ділить n.

Отже, порядок групи точок можна знайти через суми мультиплікативних характерів:

$$\#E(GF(p)) = p + 1 + \sum_{x \in GF(p)} \chi(x^3 + ax + b) \quad . \tag{7.16}$$

Або, інакше, $\#E(GF(p)) = 1 + N(y^2 - x^3 - ax - b = 0)$, де N - число розв'язків рівняння ЕК. Далі праву частину даної рівності можна розбити на два співмножники

$$\#E(GF(p)) = 1 + \sum_{\varsigma - \eta = 0} N(y^2 = \varsigma) N(x^3 + ax + b = \eta) \tag{7.17}$$

8 Криптографічний практикум

8.1 Завдання для практичних занять

Запропоновані теми для виконання практичних робіт направлені на закріплення матеріалу, що відноситься до двоключової криптографії, - системи відкритого розприділення ключів Діффі-Хеллмана, відкрите шифрування і системи цифрового електронного підпису. Для виконання даних практичних робіт необхідна програма, що реалізує арифметичні операції, алгоритм піднесення в дискретну степінь за модулем і обчислення мультиплікативно оберненого елемента в полі лишків. Програма, що включає вказані функції, може бути розроблена студентами в рамках самостійного завдання на курсову роботу або на практичних заняттях. При невеликих довжинах чисел розробка такої програми зазвичай являється нескладною задачою.

При виконанні завдань на практичних заняттях по відкритому шифруванню і відкритому розприділенню ключів доцільно акцентувати увагу слухачів на схожість системи відкритого розприділення ключів Діффі-Хеллмана і алгоритму відкритого шифрування Ель-Гамаля, яка полягає в тому, що в обох випадках використовується відкритий ключ відправника. У другому випадку він направляється отримувачу як частина криптограми. Специфіка відкритого шифрування Ель-Гамаля полягає у використанні загального секрету K (тобто ключа, що формується по відкритому ключу відправника і секретному ключу отримувача) в якості одноразового ключа шифрування, що здійснюється шляхом модульного множення блоку відкритого тексту на K.

При виконанні практичної роботи по ЕЦП Ель-Гамаля доцільно підкреслити важливість збереження згенерованого випадкового числа в таємниці, оскільки знання цього числа, яке використовується при генерації цифрового підпису, дозволяє обчислити секретний ключ. Доцільно також підкреслити, що система цифрового підпису Ель-Гамаля заснована на ідеях Діффі-Хеллмана і являється суттєвим її развитком.

При виконанні практичної роботи по «сліпому підпису» Чаума необхідно акцентувати увагу слухачів на тому, що зразок підпису до повідомлення M

повинен зберігатися в секреті від підписанта, оскільки його знання дозволяє підписанту легко обчислити значення M.

8.2 Відкрите шифрування

8.2.1 Система відкритого розприділення ключів Діффі - Хеллмана

Теоретична частина. В даній криптосистемі кожний абонент вибирає випадковий секретний ключ X і виробляє відкритий ключ Y у відповідності з формулою

$$Y = \alpha^X \pmod p.$$

Усі абоненти розміщують свої відкриті ключі в загальнодоступному словнику, який повинен бути сертифікований спеціально створеним довірчивим центром, щоб виключити можливі напади шляхом підміни відкритих ключів або введення помилкових відкритих ключів. Якщо два абоненти A і B хочуть установити секретний зв'язок, то вони поступають наступним чином. Абонент A бере із довідника відкритий ключ абонента B і, використовуючи свій секретний ключ, обчислює загальний секретний ключ:

$$Z_{AB} = (y_B)^{x_A} = (\alpha^{x_B})^{x_A} = \alpha^{x_A x_B} \pmod p,$$

де – y_A і y_B - відкриті ключі абонентів A і B; x_A і x_B – відповідні секретні ключі. Загальний секретний ключ Z_{AB} немає необхідності передавати по мережі зв'язку, оскільки абонент B по відомому із довідника відкритому ключу абонента A аналогічним способом обчислює значення

$$Z_{AB} = (y_A)^{x_B} = (\alpha^{x_A})^{x_B} = \alpha^{x_A x_B} \pmod p.$$

Передбачається, що опоненту (потенційному порушнику) можуть бути відомі значення y_A і y_B, які передаються по відкритому каналу, але для того, щоб обчислити Z_{AB}, він повинен розв'язати важку задачу дискретного логарифмування. Загальний секрет Z_{AB} може використовуватися абонентами для шифрування сеансових секретних ключів, а останні - для шифрування повідомлень з використанням симетричних методів шифрування.

Експериментальна частина. Викладач задає слухачам індивідуальні значення модуля p і параметра α. Для передбачуваних 10 користувачів слухачі вибирають 10 значень секретного ключа $x_1, x_2,\ldots,x_{10}$. Обчислюють відповідаючі їм відкриті ключі $y_1, y_2,\ldots,y_{10}$. Для всіх можливих пар значень (i,j), де i= 1, 2, ..., 10 і j= 1, 2, ..., 10, обчислюється загальний секретний ключ $Z_{(i,j)}$. Отримані результати оформляються у вигляді таблиці. Перевіряється виконання умови $Z_{(i,j)} = Z_{(j,i)}$.

8.2.2 Обчислення мультиплікативно обернених елементів в полі лишків

Теоретична частина. Для обчислення обернених елементів в полі лишків використовується розширений алгоритм Евкліда. Відомо, що якщо числа n і x являються взаємно простими і $x<n$, то для x існує єдине значення x' таке, що $x' < n$ і $xx' = 1 \pmod n$. Це число називається мультиплікативно оберненим елементом в полі лишків за модулем n і позначається як $x^{-1} \pmod n$. Використовуючи теорему Ейлера, можна записати $x^{\varphi(n)-1}x = x^{-1}x = 1 \pmod n$, звідки отримаємо $x^{\varphi(n)-1} = x^{-1} \pmod n$, тобто мультиплікативно обернений елемент можна обчислити за значенням функції Ейлера.

Експериментальна частина. Виконується обчислення мультиплікативно обернених елементів для ряду чисел x_i, $i = 1,2, ...10$, для трьох простих модулів p_1, p_2, p_3 і трьох складених модулів n_1, n_2 і n_3. Обчислення виконуються двома способами: 1) з використанням розширеного алгоритму Евкліда і 2) з використанням формули $x^{\varphi(n)-1} = x^{-1} \pmod n$. Складається порівняльна таблиця, що показує ідентичність результатів обчислення за двома способами.

8.2. 3 Відкрите шифрування Ель-Гамаля

Теоретична частина. Спосіб вікритого шифрування Ель-Гамаля включає в себе складеною частиною систему відкритого розприділення ключів Діффі-Хеллмана. Кожний користувач секретної мережі вибирає секретний ключ x, обчислює свій відкритий ключ $y = \alpha^x$ і розміщує y в сертифікований довідник. Шифрування повідомлення T, що відправляється користувачу t, здійснюється за допомогою наступного алгоритму:

- вибрати випадкове число R;
- обчислити $C' = \alpha^R \pmod p$, яке за своєю сутністю являється одноразовим відкритим ключем;
- використовуючи відкритий ключ i-го користувача, обчислити $C''=y^R\, T \pmod p$;
- відправити блок шифртексту (C',C'') користувачу i.

Розшифрування здійснюється користувачем i за наступним алгоритмом:

- обчислити значення $(C')^x = (\alpha^R)^x = \alpha^{Rx} \pmod p$, яке за своєю сутністю являється одноразовим загальним секретом Z_{AB} отримувача і відправника;
- обчислити значення $Z^{-1} = (\alpha^{Rx})^{-1} \pmod p$;
- розшифрувати криптограму C'': $T= C''Z^{-1} \pmod p$.

Експериментальна частина. За вказівкою викладача студентам індивідуально задаються значення простого числа p і параметра α. Студенти формують секретний ключ x_A і, використовуючи задані значення p і α, обчислюють відкритий ключ y_A. Використовуючи відкритий ключ, здійснюється зашифрування 10 різних повідомлень, фіксуючи для кожного із них значення R, R^{-1}, C', C'', Z, Z^{-1}. Перевіряється правильність розшифрування повідомлень. Отримані результати оформляються у вигляді таблиці.

8.2.4 Відкрите розприділення ключів з використанням криптосистеми RSA

Теоретична частина. В криптосистемі RSA сеансові ключі шифруються по відкритому ключу отримувача і розприділяються по відкритому каналу. Процедура зашифрування виражається формулою:

$$C = K^d \pmod{n}.$$

Отримувач розшифровує сеансовий ключ з використанням свого секретного ключа:

$$K = C^e \pmod{n}.$$

Експериментальна частина. Використовуючи задані значення простих чисел p і q, обчислити модуль n, потім сформувати відкритий і закритий ключі e і d. Використовуючи відкритий ключ, зашифрувати 10 різних ключів і, використовуючи закритий ключ, здійснити процедуру їх розшифрування. Перевірити коректність розшифрування. Результати оформити у вигляді таблиці.

9 Системи цифрового підпису

9.1 Електронний цифровий підпис Ель-Гамаля

Теоретична частина. Нехай для абонента A маємо секретний ключ x_A і відкритий ключ $y_A = \alpha^{x_A}$. Підписом абонента A під документом M, де $M < p$ служить пара чисел (r,s), де $0 \le r < p-1$ і $0 \le s < p-1$, яка задовольняє рівнянню

$$\alpha^M = y_A^r r^s \pmod{p}.$$

Це рівняння перевірки підпису абонента A. Дана система ЕЦП заснована на тому, що тільки дійсний власник секретного ключа α може виробити пару чисел (r, s), що задовольняють рівнянню перевірки підпису, за наступним алгоритмом:

1. Згенерувати випадкове число k, що задовольняє умові: $0<k<p-1$.
2. Обчислити $r = \alpha^k \pmod{p}$.
3. Обчислити s із рівняння $M = x_A r + ks \pmod{(p-1)}$.

Із теорії чисел відомо, що останнє рівняння має розв'язок для s, якщо НСД $(k, p-1) = 1$. Це рівняння легко отримати шляхом підстановки в рівняння перевірки підпису значення $r = \alpha^k \pmod{p}$:

$$\alpha^M = \alpha^{x_A r} \alpha^{ks} = y_A^r r^s \pmod{p}.$$

Необхідно відмітити, що для даного повідомлення може бути розроблено велике число різних підписів, що відповідають різним k. Однак розробити правильний підпис може тільки власник секретного ключа.

Особливістю даного ЕЦП являється те, що одне і те ж значення k не допускається використовувати для формування підпису для двох різних повідомлень, оскільки це дає можливість обчислення секретного ключа. Використані значення k повинні зберігатися в секреті. Зазвичай після створення підпису вони знищуються.

Експериментальна частина. Використовуючи задані значення простого числа p і параметра α, сформувати секретний ключ x_A, обчислити відповідний йому відкритий ключ y_A і обчислити значення електронного підпису для 10 різних повідомлень, фіксуючи отримані значення параметрів k, $r = \alpha \pmod p$, s, α^M, $y_A{}^r$, r^s, $y_A{}^r$, r^s. Здійснити перевірку підпису по відкритому ключу. Результати оформити у вигляді таблиці.

9.2 Знаходження чисел, що відносяться до заданого показника

Теоретична частина. Для будь-якого числа α, взаємно простого з модулем m, існують числа δ, такі, що $\alpha^\delta = 1 \bmod p$. Мінімальне із чисел δ, тобто число $\gamma = min\{ \delta \}$, називається показником числа α. Якщо α за модулем m належить показнику δ, то числа $\alpha^0, \alpha^1, \ldots, \alpha^{\delta-1}$ за модулем m непорівнянні. Показниками можуть бути тільки дільники числа $p-1$. Якщо модуль являється простим числом p, то кількість чисел $\psi(\gamma)$, що відносяться до показника γ, дорівнює функції Ейлера від числа γ, тобто $\psi(\gamma) = \varphi(\gamma)$. Якщо довжина числа γ значно менше довжини простого модуля, то знаходження чисел, що відносяться до показника γ, шляхом випадкового вибору чисел α і перевірки співвідношення $\alpha^\delta = 1 \bmod p$ являється обчислювально неефективним. В реальних системах ЕЦП із скороченою довжиною підпису простий модуль $p-1$ має розмір 1024 або 2048 бітів, а розмір показника y складає біля 160 бітів. Для знаходження числа α, що відноситься до показника γ, використовується наступний обчислювально ефективний спосіб.

1. Вибирається число α, що перевищує 1 і менше числа p.
2. Обчислюється значення $\gamma' = (p - 1)/\gamma$ і число $\delta = \alpha^{\gamma'} \bmod p$.
3. Якщо $g \neq 1$, то в якості числа α взяти число g. В іншому випадку повторити кроки 1-3.

Дійсно, для отриманого числа $\alpha \neq 1$ маємо $\alpha = \alpha^{(p-1)/\gamma} \bmod p$.Тому, згідно теореми Ферма, маємо $\alpha^\gamma = a^{(p-1)} = 1 \bmod p$, тобто число α відноситься до показника γ.

Експериментальна частина. Задаються декілька простих чисел p. Для кожного із них необхідно знайти розкладання числа $p - 1$, вибрати декілька значень в якості показників і для кожного із показників знайти декілька чисел, що відносяться до нього, за модулем p. Іншим варіантом являється наступне завдання. Необхідно сформувати велике просте число p, для якого можна знайти розкладання $p - 1$. Для модуля p знаходяться декілька чисел, що відносяться до показників, в якості яких прийняті дільники $p-1$.

9.3 Цифровий підпис Ель-Гамаля із скороченою довжиною параметрів

Теоретична частина. Рівняння перевірки підпису $\alpha^M = y_A^r r^s \pmod p$ може виконуватися також у випадку, коли в якості α приймається число, що відноситься до показника q, де $q /(p – 1)$. Для цього s повинно бути обчислене із наступного співвідношення:

$$M = x_A r + ks \pmod q.$$

Можна вибрати простий модуль p таким, щоб розкладання $p - 1$ містило простий множник q, розмір якого значно менше розміру p. Наприклад, для 2048-бітового модуля p довжина може складати 160 бітів. В цьому випадку обчислюване значення s буде мати розмір, що не перевищує 160 бітів. Завдяки цьому досягається скорочення довжини підпису майже в 2 рази (довжина параметру r залишається рівною розміру модуля).

Експериментальна частина. Використовуючи задані значення простого числа p, знайти розкладання числа $p - 1$. Вибрати в якості показника q один із дільників $p - 1$. Знайти первісний корінь α і число g, що відноситься до показника q. Сформувати секретний ключ x_A, обчислити відповідний йому відкритий ключ $Y_A = \alpha^{x_A} \bmod p$. Обчислити значення електронного підпису для 5 різних повідомлень, фіксуючи отримані значення параметрів k, $г = \alpha^k$, s, α^M, y_A^r, r^s, y_A^r , $r^s \pmod p$. Обчислити значення скороченого електронного підпису для тих же повідомлень, використовуючи нове значення відкритого ключа $y_A = g^{x_A} \pmod p$ і фіксуючи отримані значення параметрів k, $r = g^k$, s, g^M, y_A^r , $r^s \pmod p$. Здійснити перевірку підпису за відкритим ключем. Результати оформити в вигляді таблиці.

9.4 Цифровий підпис Ель-Гамаля із скороченою довжиною параметрів *s* і *r*

Теоретична частина. Рівняння перевірки підпису $\alpha^M = y_A^r r^s \bmod p$ може бути перетворено до наступного вигляду

$$r = \alpha^{M/s} y_A^{-r/s} \pmod p.$$

При цьому замість r в степені при y_A можна використати значення деякої хеш-функції від значення $к$, тобто $H(r)$. В цьому випадку рівняння перевірки підпису має вид $r = \alpha^{M/s} y_A^{-r/s} \pmod p$. Щоб перевірка була коректною, власник секретного ключа повинен обчислити параметр s із наступного рівняння

$$M = x_A H(r) + ks \pmod q.$$

Оскільки при перевірці підпису не вимагається виконувати ніяких обчислень з використанням параметра r, то перевірка підпису може бути здійснена у відповідності з рівнянням

$$H(r) = H(\alpha^{M/s} y_A^{-H(r)/s}) \pmod p.$$

В цьому випадку немає необхідності представляти перевіряючому значення *r*, що має порівняно велику довжину. Достатньо для перевірки представити значення *H(r)*, де розмір значення хеш-функції дорівнює, наприклад, 160 бітів. Цим досягається значне скорочення довжини підпису. Якщо використовується варіант із скороченою довжиною параметра *s*, то загальна довжина підпису складає порядка 320 бітів замість початкової довжини 2048 або 4096 бітів при 1024-бітовому або 2048-бітовому модулі *p* відповідно. Скорочення довжини підпису не зменшує стійкості системи ЕЦП, оскільки складність задачі дискретного логарифмування не змінюється, так як обчислення ведеться за модулем однакового розміру. В якості хеш-функції *H(r)* можна взяти наступну: H(r) = *r mod q*, де *q* -показник, що використовується при скороченні параметра *s*. Тоді приходимо до наступного рівняння перевірки підпису:
$r' = (\alpha^{M/s} y_A^{-r'/s})$ (mod *p*) mod *q*, де (*r', s*) є підпис до повідомлення *M*, а параметр *r'* обчислюється після вибору випадкового числа *k* у відповідності з формулою
$r' = (\alpha^k \bmod p)$ mod *q*. Рівняння для обчислення параметра *s* має вид:

$$M = x_A r' + ks \pmod{p-1}.$$

Експериментальна частина. Використовуючи задані значення простого числа *p*, знайти розкладання числа *p - 1*. Вибрати в якості показника *q* один із дільників *p-1*. Знайти первісний корінь α і число *g*, що відноситься до показника q. Сформувати секретний ключ x_A , обчислити відповідний йому відкритий ключ $y_A = \alpha^{x_A} \pmod{p}$. Обчислити значення електронного підпису для 5 різних повідомлень, фіксуючи отримані результати наступних значень:
$k,\ r' = (\alpha^k \bmod p) \bmod q,\ s,\ \alpha^{M/s} \bmod p,\ y_A^{r'/s} \bmod p,\ \alpha^{M/s} y_A^{-r'/s} \bmod p$.
Здійснити перевірку підпису за відкритим ключем. Результати оформити у вигляді таблиці. Виконати аналогічні обчислення у варіанті із скороченим розміром параметру *s*, використовуючи в якості бази число *g*.

9.5 Електронний цифровий підпис RSA

Теоретична частина. Теорема Ейлера: для будь-яких взаємно простих цілих чисел *M* і *n*, де *M*<*n*, виконується співвідношення:

$$M^{\varphi(n)} = 1 \pmod{n}.$$

В криптосистемі RSA в якості числа *M* використовується повідомлення, яке необхідно підписати або зашифрувати. Будемо вважати, що умова взаємної простоти чисел *M* і *n* виконується. Наприклад, це забезпечується тим, що в даній криптосистемі вибирається число *n*, яке дорівнює добутку двох великих простих множників, тому імовірність того, що випадкове повідомлення не буде взаємно простим з модулем, є зневажливо малою.

Формування ключів. Кожний користувач вибирає два великих не рівних між собою простих числа *p* і *q*, знаходить їх добуток *n = pq* і обчислює значення функції Ейлера від *n*:

$$\varphi(n) = (p-1)(q-1).$$

Значення n являється частиною відкритого ключа. Числа p і q являються частиною закритого ключа. Числа p і q повинні мати спеціальну структуру, зокрема, в крайньому випадку одно із чисел $(p - 1)$ або $(q - 1)$ повинно мати один великий простий множник. Розмір модуля n повинен бути не менше 1024 бітів. Потім вибирається ціле число d таке, що $d < \varphi(n)$ і НСД$(d, \varphi(n)) = 1$ і обчислюється e, що задовольняє умові

$$ed = 1 \pmod{\varphi(n)}.$$

Секретним ключем являється трійка чисел p, q, d. Відкритим ключем являється пара чисел n, e, яка повідомляється усім користувачам.

Процедура підписування наступна:

$$S = M^d \pmod{n}.$$

Процедура перевірки підпису має вигляд:

$$M' = S^e \pmod{n}.$$

Якщо $M' = M$, то повідомлення M признається підписаним.

Експериментальна частина. Використовуючи задані значення простих чисел p і q, обчислити модуль n, потім сформувати відкритий і закритий ключі e і d. Використовуючи закритий ключ, підписати 10 різних повідомлень і здійснити перевірку підпису за відкритим ключем. Результати оформити у вигляді таблиці.

9.6 Електронний цифровий підпис ДСТУ 4145-2002

Теоретична частина. Будемо використовувати наступні параметри підпису:

- просте число p - модуль ЕК;
- еліптичну криву E, що задається коефіцієнтами $a, b \in GF_p$;
- просте число q - порядок циклічної підгрупи групи точок ЕК;
- точку $P \in E(GF_p)$ з координатами (x_p, y_p): $P \neq O$, $qP = O$;
- секретний ключ - ключ підпису, що являється цілим числом d: $0 < d < q$;
- відкритий ключ - ключ перевірки підпису, що являється точкою $Q \in E(GF_p)$ з координатами (x_q, y_q): $dP = Q$.

Формування підпису здійснюється у відповідності з приведеним алгоритмом:

1. Генерується випадкове ціле число k, що задовольняє нерівності $0 < k < q$.
2. Обчислюється точка ЕК $C = kP$ і визначається значення $r = x_C \pmod{q}$, де x_C - координата точки C.
3. Обчислюється значення $s = (rd + ke) \pmod{q}$, де $e = M \pmod{eq}$, M - це повідомлення або хеш-функція від повідомлення, яке необхідно підписати.

Підписом є два двійкових вектори r і s. Перевірка підпису полягає у обчисленні координат точки ЕК: $C = (se^{-1} \pmod{q})P + ((q - r)e^{-1} \pmod{q})Q$, у визначенні значення $R = x_C \pmod{q}$ і перевірці виконання рівності $R = r$.

Експериментальна частина. Використовуючи задані значення простого числа p і коефіцієнтів рівняння ЕК, визначити порядок q циклічної підгрупи групи точок ЕК, генератор циклічної підгрупи - точку $P \in E(GF_p)$, сформувати секретний ключ d, обчислити відповідаючий йому відкритий ключ Q і

обчислити значення електронного підпису для 10 різних повідомлень, фіксуючи отримані значення параметрів *k, r, x, e, C*. Здійснити перевірку підпису за відкритим ключем. Результати оформити у вигляді таблиці.

9.7 “Сліпий “ підпис Чаума

Теоретична частина. Сліпий підпис Чаума заснований на криптосистемі RSA. Нехай користувач *A* бажає підписати деяке повідомлення *M* у користувача *B* таким чином, щоб останній не міг прочитати повідомлення, що підписується. Для цього необхідно здійснити наступні кроки.

Користувач *A* генерує випадкове просте число *k* - таке, що *НСД(k, n) = 1*, де *n* - частина відкритого ключа користувача *B*. Потім *A* обчислює значення $M' = k^e M \pmod n$ і пред’являє його користувачеві *B*, щоб останній підписав *M’* у відповідності із стандартною процедурою підписування в системі RSA. Підписуючий не може прочитати повідомлення *M*, оскільки воно перетворено шляхом накладання на нього "одноразового" ключа k^e з використанням операції модульного перемноження.

Користувач *B* підписує повідомлення *M’*: $S' = (k^e M)^d = kM^d \pmod n$. Відмітимо, що за значенням підпису *S'* до повідомлення *M '* підписуючий не має можливості обчислити M^d. Відмітимо також, що за значенням M^d легко обчислити *M*: $(M^e)^d = M \pmod n$. Це означає, що після отримання значення $S = M^d \pmod n$ користувач *A* повинен тримати його в секреті від підписавшого. Після отримання від користувача *B* значення *S'*, використовуючи розширений алгоритм Евкліда, користувач *A* обчислює для числа *k* мультиплікативно обернений елемент (k^{-1}) в полі лишків за модулем *n* і формує підпис користувача *B* до повідомлення *M*: $S = k^{-1} S' = k^{-1}kM^d = M^d \pmod n$.

Експериментальна частина. Використовуючи задані значення простих чисел *p* і *q*, обчислити модуль *n*, потім сформувати відкритий і закритий ключі *e* і *d*. Здійснити процедуру виробки підпису «всліпу» у відповідності з протоколом Чаума для 6 різних повідомлень, фіксуючи для кожного із них значення $k, k^{-1} \pmod n$, *M, M', S’* і *S*. Здійснити перевірку правильності отриманого підпису шляхом безпосереднього обчислення значення $S = M^d \pmod n$. Результати оформити у вигляді таблиці.

10 Генерація простих чисел

10.1 Генерація великих простих і псевдопростих чисел

Теоретична частина. Для генерації великих простих чисел можуть бути використані наступні три підходи:
- формуються випадкові числа заданого розміру і перевіряється, чи являються вони простими, за допомогою імовірнісних тестів (псевдопрості числа):
- за визначеною процедурою генеруються прості числа, перевірка яких здійснюється за допомогою детермінованих тестів на простоту;
- комбінована генерація простих чисел, при якій формуються псевдопрості числа (за першим варіантом) проміжного розміру, на основі яких потім формуються псевдопрості числа, що тестуються за допомогою детерміністичних тестів (цей підхід забезпечує прискорення процедури генерації псевдопростих чисел p з відомим розкладанням функції Ейлера від нього).

В першому випадку тести будуються на основі певних теорем із теорії чисел, сформульованих і доведених для простих чисел. Якщо число не задовольняє тесту, то воно не являється простим і відкидається. Для перевірки береться наступне випадкове число необхідного розміру. Якщо число проходить тест, то деякий змінний параметр, використовуваний для тестування, змінюється і тест повторюється знову. Число, що пройшло велику кількість дослідів визначеного типу, вважається псевдопростим, оскільки імовірність, що складене число може пройти усі тести, зневажливо мала. Для того, щоб виключити деякі можливі класи складених чисел, які можуть проходити тести конкретного типу, використовують декілька різних тестів, по кожному із яких виконується велике число досліджень. Перевагою генерації псевдопростих чисел являється порівняльна простота процедури. Недоліком першого підходу являється те, що після генерації великого псевдопростого числа p може виявитися досить складним визначення розкладання числа $p-1$, яке необхідно знати, наприклад, у випадку ЕЦП на основі складності задачі дискретного логарифмування із скороченою довжиною підпису. Розкладання числа $p - 1$ представляє інтерес також і для відсіювання деяких класів слабких простих чисел. Наступні два імовірнісних тести можуть бути застосовані разом. Нехай ми хочемо перевірити, чи являється число p простим.

Тест Ферма полягає в перевірці співвідношення $b^{p-1} = 1 \pmod{p}$ для великого числа різних значеннь b. Число різних використаних при тестуванні значень b, для яких виконується вказане співвідношення, визначає число виконаних досліджень за тестом Ферма. Однак відомий клас складених чисел, які проходять тест Ферма (числа Кармайкла). Приклади чисел із цього класу приведені в таблиці 10.1.

Тест Соловея-Штрассена полягає в перевірці рівностей $\frac{b}{p} = 1$, де $\frac{b}{p}$ - символ Лежандра для значень b, що являються квадратичними лишками за модулем p, і $\frac{b}{p} = -1$ для значення b, що являються квадратичними нелишками за

модулем *p* (квадратичним лишком називається число, що являється квадратом деякого числа *x* за модулем *p*, тобто, для квадратичного лишку існує квадратний корінь $b = x^2 \bmod p$).

Другий тест добре відсіює числа Кармайкла. Імовірність того, що складене число пройде одне дослідження за тестом Соловея-Штрассена, не перевишує значення 0.5. Це дозволяє отримати оцінку числа досліджень, які необхідно виконати у відповідності з даним тестом, щоб отримати необхідно низьку імовірність прийняти складене число в якості псевдопростого. Перший тест використовується в якості попереднього відбракування чисел. Другий тест проходять тільки числа, які пройшли перший тест.

Таблиця 10.1. Приклади чисел Кармайкла

Число	Розкладання	Число	Розкладання
561	3-11-17	6601	7-23-41
1105	5-13-17	8911	7-19-67
1729	7-13-19	41041	7-11-13-41
2465	5-17-29	825265	5-7-17-19-73
2821	7-13-31	413631505	5-7-I7-73-89-107

Прикладом другого підходу можна прийняти наступний.

В якості комбінованого підходу до формування псевдопростих чисел можна використати вибір псевдопростих чисел $q_1, q_2, ..., q_k$ проміжної (але достатньо великої) довжини, які використовуються в якості початкового набору $\{ q_1, q_2, ..., q_k \}$. Для генерації псевдопростих чисел збільшеної довжини, використовуючи на другому етапі розглянутий нижче варіант формування простих чисел з детерміністичною перевіркою на простоту (в результаті формуються псевдопрості числа). Перевагою комбінованого способу являється можливість формування простих чисел *p* із заданим розкладанням числа $p - 1$.

<u>Експериментальна частина.</u> Формуються декілька псевдопростих чисел *p*, які мають задану довжину і задане розкладання числа $p - 1$. Можливі два типи завдань, що відповідають двом варіантам генерації псевдопростих чисел - імовірнісному і комбінованому. У другому випадку формуються псевдопрості числа невеликої довжини, а в якості детерміністичного тесту використовується метод пробного ділення. У випадку генерації псевдопростих чисел з використанням імовірнісного тесту Соловея-Штрассена оцінюється імовірність прийняти складене число в якості псевдопростого. Щоб обійти проблему визначення значення символу Лежандра $\frac{b}{p}$ для випадково вибираємого значення *b*, в якості чисел *b* можна брати свідомо квадратичні лишки, генеруючи випадкові числа *x* і обчислюючи $b = x^2 \bmod b$. Для квадратичних лишків маємо $\frac{b}{p} = 1$. За визначенням символу Лежандра є значення $b^{\frac{p-1}{2}} \bmod p$.

10.2 Генерація (детерміністична) великих простих чисел з вибором розкладання функції Ейлера

Теоретична частина. Формується набір k простих чисел $\{ q_1, q_2 ,.., q_k \}$ порівняно невеликої довжини (наприклад, які мають 8-10 десяткових знаків). Причому числа $q_1, q_2 ,.., q_k$ перевіряються детерміністичним тестом на простоту, в якості якого можна взяти перевірку подільності на усі натуральні числа від 2 до $[\sqrt{q_i}\,]$ (метод пробного ділення $[g]$ вказує найменше ціле число, що не менше, чим число g). Із вказаного набору випадковим способом вибираються h простих чисел $m_1, m_2, \ldots, m_h$, обчислюється число p_1, що має наступну структуру:

$$p_1 = 1+2\prod_{i=1}^{i=h} m_i \,.$$

Потім вибирається деяке число P і перевіряється, чи виконуються для даного p_1 наступні дві умови:

1) $b^{r_1-1} = 1 (\mathrm{mod}\, p)$,

2) $b^{\frac{\kappa_1-1}{b_ш}} \neq 1 (\mathrm{mod}\, p)$ для всіх $m_i \in \{ m_1, m_2 ,.., m_h \}$.

Якщо після декількох спроб знайдеться деяке b, яке задовольняє указаним вище двом співвідношенням, то p являється простим числом. Якщо таке число не знайдено, то вибирається інший випадковий набір простих чисел $m_1, m_2 ,.., m_h$ із набору $q_1, q_2 ,.., q_k$. Сформоване таким способом число p_1 має довжину приблизно в h раз більше середньої довжини чисел $q_1, q_2 ,.., q_k$, (наприклад, від $8h$ до $10h$ десяткових знаків). Можна сформувати аналогічним способом наступний набір простих чисел $\{p_1, p_2 ,.., p_k\}$ і, показуючи їх в якості початкових, повторити процедуру, що розглядається, формуючи ще більш довгі прості числа. Перевагою даного способу являється те, що ми свідомо знаємо розкладання $p - 1$, крім того, ми можемо формувати це розкладання таким способом, щоб в ньому містилися прості числа необхідної довжини. Основним недоліком такого способу являється те, що формується тільки деякий підклас простих чисел заданої великої довжини. Однак потужність цього підкласу може бути задана такою, що цією обставиною атакуючий не зможе скористатися для розкриття тієї чи іншої двоключової криптосистеми, в якій ця процедура детерміністичної генерації простих чисел буде використовуватися. Цей детерміністичний тест заснований на наступній **теоремі:**

p -ціле непарне число, що перевищує 1. Якщо існує $b \leq p - 1$, таке, що виконуються наступні умови:

1) $b^{r_1-1} = 1 \mathrm{mod}\, p$,

2) $b^{\frac{\kappa_1-1}{b_ш}} \neq 1 \mathrm{mod}\, p$ для кожного простого дільника m_i числа $p - 1$, то число p являється простим.

Доведення

Припустимо, що p не являється простим. Тоді функція Ейлера від p має значення менше, чим $p - 1$, тобто $\varphi(p) < p - 1$. Розглянемо два випадки: а) НСД (b, p) = 1 і б) НСД (b, p) ≠ 1. У випадку а) порядок числа b повинен ділити $\varphi(p) < p - 1$, але за умовою теореми порядок b дорівнює $p - 1$. У випадку б) не існує цілих степенів n, для яких виконується умова $b^n = 1 \bmod p$. В обох випадках приходимо до протиріччя, яке доводить твердження теореми (пояснення до випадку б): якщо НСД (b, p) = $\delta \neq 1$, $\delta / b^n \bmod p$ для будь-якого n, оскільки для залишку r від ділення b^n на p маємо $НСД (b^n, r) = \delta$).

Експериментальна частина. Формуються декілька простих (псевдопростих) чисел p, що мають задану довжину і задане розкладання числа $p - 1$. Можливі два типи завдань, що відповідають двом варіантам генерації простих і псевдопростих чисел (детерміністичному і комбінованому). Оцінюється приблизна кількість можливих чисел, які можуть бути сформовані у відповідності з детерміністичним і комбінованим підходами.

10.3 Генерація (детерміністична) великих простих чисел за стандартом ДСТУ7624:2014

Теоретична частина. Для генерації великих простих чисел в ГОСТ Р 34.10-94 використовується детерміністичний тест, заснований на наступній **теоремі**: нехай $p = qN + 1$, де q - непарне просте число, N - парне і $p < (2q + 1)^2$. Число p являється простим, якщо виконуються наступні дві умови:

1. $2^{qN} = 1 \bmod p$.
2. $2^N \neq 1 \bmod p$.

Доведення. Нехай γ є порядок числа 2 за модулем p і p має наступне канонічне розкладання: $p = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_h^{\alpha_h - 1}$. Оскільки умова 1 γ ділить $p - 1$, тобто $\gamma / (p - 1)$. У зв'язку з умовою 2 γ не являється дільником числа $\frac{p-1}{q}$. Звідси виходить, що q / γ. Згідно теореми Ейлера $2^{\varphi(p)} = 1 \bmod p$ маємо $\varphi(p) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_h^{\alpha_h - 1}$ $(p_1 - 1)(p_2 - 1) \dots (p_h - 1)$. Нехай q співпадає з простим множником p_1. Із такого припущення виходить, що $p = qn'$ для деякого натурального числа n. Однак за умовою теореми маємо $p = qN + 1$. Оскільки $q > 1$ не може ділити число 1, то приходимо до протиріччя, із якого виходить, що q повинно ділити число $p - 1$, принаймі, для деякого одного із значень $i \in (1,2,\dots, h)$. Таким чином, існує деяке натуральне $n>2$, таке, що маємо: $p_i - 1 = qn$ і $p_i = qn + 1$. Отже, при деякому натуральному m отримаємо:

$p = mp_i = m(qn + 1) = qn + 1 \Rightarrow m = q(N - mn) + 1$.

При деякому натуральному $s \geq 0$ маємо $m = qs + 1$ і $p = (qn + 1)(qs + 1)$.

Нехай p є складене число, тоді $s \geq 2$ (оскільки N і n – парні числа, а $s = N - mn$), із чого виходить $p \geq (2q + 1)^2$. Це суперечить умові теореми, отже, $s = 0$ і число p являється простим.

Експериментальна частина Полягає у виконанні декількох кроків алгоритму детерміністичного формування простих чисел заданої довжини за ГОСТ Р 34.10-94. Схема побудови алгоритму описується наступним способом.

Нехай необхідно сформувати просте число p довжини $t \geq 17$ бітів. З цією метою будується спадаючий набір натуральних чисел $t_0, t_1, \ldots, t_s$, де $t_0 = t$ і $t_s < 17$ бітів, для яких виконується умова $t_i = [t_{i-1}/2]$. Послідовно виробляються прості числа $p_s, p_{s-1}, \ldots, p_0$, причому довжина числа p_i дорівнює значенню t_i, для всіх $i = 1, \ldots, s$. Початкове просте значення p_s формується шляхом випадкового вибору числа розміром менше 17 бітів і перевіркою на простоту методом пробного ділення. Генерація простого числа p_{i-1} за простим числом p_i здійснюється з використанням формули

$$P_i - 1 = p_i N + 1,$$

де N - випадкове парне число, таке, що довжина числа $p_i N + 1$ дорівнює значенню t_i. Число $p_i - 1$ вважається отриманим, якщо одночасно виконані наступні дві умови:

1. $2^{p_i N} = 1 \bmod (p_i - 1)$.
2. $2^N \neq 1 \bmod (p_i - 1)$.

Якщо хоча б одна із умов не виконана, то значення N збільшується на два, обчислюється нове значення $p_i - 1$, яке знову перевіряється на простоту за вказаними двома умовами. Така процедура виконується до тих пір, поки не буде отримано просте число $p_i - 1$.

11 Вступ в теорію та практику квантових обчислень.

Розділ присвячений розгляду найсучаснішого напрямку науки — квантової інформатики та її найбільш важливим додаткам квантової криптографії та квантовому криптоаналізі.

Ще в 1965 році майбутній співзасновник компанії INTEL Гордон Мур прогнозував щорічне подвоєння щільності транзисторів в напівпровідникових мікросхемах, тобто, експонентне зменшення розмірів елементів. Закон Мура справджується вже протягом 55 років і на сьогодні розмір елементів транзистора (і, відповідно, розмір області, в якій зберігається одиниця інформації — біт) становить долі мікрона. У зв'язку з цим виникає питання про принципові обмеження на розміри, швидкодію та теплообмін між елементами комп'ютерних схем. На думку фізика Р. Фейнмана "закони фізики не заперечують зменшення розмірів комп'ютера до тих пір, поки біти не досягнуть розмірів окремих атомів і закони квантової механіки не стануть домінуючими" . В той час стало питання, чи можливо створити комп'ютер, в якому поведінка системи бітів буде визначатись законами квантової механіки? Процес обчислень завжди вважався виключно класичним процесом. Робота окремих елементів квантового комп'ютера описується законами квантової фізики для звичайних обчислень (комп’ютера) стану окремого біта та передбаченністю результату операції над ним. Причому визначення стану біта (фізичне вимірювання) не впливає на його стан, різні фізичні реалізації логічної операції призводять до однакової зміни стану біта, і це робить можливим розглядати процес обчислень на класичному комп'ютері незалежно від його апаратного втілення.

В основі ж квантової механіки лежить *принцип невизначеності Гейзенберга* та ймовірностний характер станів окремих елементів, а також знищення стану квантового об'єкта (біта) при визначенні стану (вимірюванні), що, здається, знаходиться в повному протиріччі із вимогою повної визначеності, однозначності та зворотності комп'ютерних операцій.

Однак, на початку 80-х Полю Беньоффу (Paul Benioff), Річарду Фейнману (R.P. Feyman) та Давіду Дейчу (David Deutsch) вдалось поєднати дві дисципліни, що досі вважались взаємовиключними, — квантову фізику та інформатику. Вони показали, що квантова теорія не тільки не обмежує обчислювальних можливостей, але дозволяє суттєво їх розширити. Беньофф висловив ідею універсального квантового комп'ютера — машини, яка здійснює логічні операції, спираючись на квантові алгоритми, що не мають аналогів в класичній фізиці. Фейнман показав, що квантовий комп'ютер повинен бути більш потужним, аніж класичний, а Д. Дейч запровадив ідею квантового паралелізму, що описує здатність квантового комп'ютера працювати із квантовою суперпозицією чисел. Тим самим ці вчені заклали фундамент нової сучасної галузі досліджень — квантових інформаційних технологій або квантової інформатики.

На початку 90-х квантова інформатика набула прикладного змісту завдяки роботам Екерта (A. K. Ekert), Беннета (C. H. Bennett) та групи з Женевського університету. Виявилось, що такі "недоліки" квантового об'єкту, як можливість

одночасного перебування у сукупності станів та суттєвий вплив процесу вимірювання на стан об'єкта, відкривають нові можливості в криптографії.

Досягнення фізики останніх років (бозе-ейнштейнівська конденсація атомів газу, квантовий ефект Хола, штучні періодичні структури – квантові точки, колодязі тощо), а також розвиток лазерних та оптоволоконних технологій зробили можливим реалізацію найближчим часом квантового комп'ютера. На сьогодні квантова інформатика вбирає в себе досягнення різних дисциплін — фізики, теорії інформації, обчислювальних методів, телекомунікацій, матеріалознавства тощо і переживає період бурхливого розвитку, який можна порівняти тільки із розвитком ідей квантової фізики в кінці 19-го - початку 20-го сторіччя.

Дана робота має на меті ознайомлення із основними проблемами та напрямками розвитку квантової інформатики.

Деякі питання квантової механіки

Квантова інформатика в повній мірі використовує властивості квантових об'єктів, такі, як:

- здатність однієї частки перебувати в кількох станах одночасно (суперпозиція станів об'єкта);
- здатність системи із кількох часток перебувати в корельованиих (переплутаних) станах і пов'язана з цим нелокальність;
- суттєвий вплив процесу вимірювання на стан об'єкта;
- неможливість клонування квантових станів.

Розглянемо ці властивості докладніше.

Принципова відмінність квантової фізики від класичної полягає в тому, що:

1) закономірності квантової фізики носять статистичний (ймовірністний), а класичної фізики — динамічний (детерміністичний) характер;

2) процес вимірювання стану мікрооб'єкта істотно впливає на його стан і тому в квантовій фізиці, на відміну від класичної, неможливо абстрагуватися від фізичної природи процесу вимірювання. Внаслідок цього, стан квантового об'єкта описується через так звані базисні стани, що задаються можливостями вимірювального приладу.

Пояснимо це на прикладі. Так, стан фотона (кванта світла) заданої частоти характеризується його поляризацією. Поляризаційний стан фотона визначається за допомогою поляризатора-аналізатора, ось якого ми можемо розташувати довільним чином. Припустимо, ось поляризатора розташована вертикально. Якщо досліджуваний фотон був поляризований вертикально, то він пройде через поляризатор, якщо горизонтально — то не пройде. Таким чином, можливі стани поляризатора утворюють *базис;* вертикальній поляризації відповідає вектор стану $|1\rangle$, горизонтальній поляризації – вектор стану $|0\rangle$ (Використані позначення для так званих векторів стану були вперше запроваджені Діраком).

Стан фотона описують за допомогою амплітуди ймовірності або хвильової функції, яка в зазначеному вище базисі має вигляд:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \qquad (11.1)$$

Коефіцієнти α та β можуть бути комплексними. Відповідно, безпосередньо хвильова функція та коефіцієнти не є *спостережуваними* (їх неможливо виміряти). Із результатів вимірювання можна лише визначити квадрати модулів $|\alpha|^2$ та $|\beta|^2$, що характеризують ймовірність знайти систему в стані $|0\rangle$ або $|1\rangle$ відповідно.

Так, для вертикально поляризованого фотона $\alpha = 0, \beta = 1$, для горизонтально поляризованого навпаки, $\alpha = 1, \beta = 0$. Якщо фотон був поляризований під кутом 45° до вертикальної осі, то $\alpha = \beta = 1/\sqrt{2}$, тобто фотон з однаковою ймовірністю ½ пройде чи не пройде через поляризатор. Зазначимо також, що якщо обидві величини, a та β, відмінні від нуля, то кажуть, що фотон знаходиться в *суперпозиційному* стані, а якщо одна з них дорівнює нулю (тобто, в результаті експерименту ми визначаємо стан фотона з ймовірністю 1), то в *чистому* стані.

Зауважимо, що введені поняття пов'язані із вибором базису вимірювального приладу. Процес вимірювання за допомогою поляризатора переводить (проектує) фотон із стану $|\psi\rangle$ в стан $|1\rangle$ або знищує його. Повторне вимірювання не дає нової інформації про $|\psi\rangle$, оскільки стан фотона змінюється вже після першого вимірювання.

Квантові властивості притаманні і системам, що складаються з кількох квантових об'єктів. В таких системах можна спостерігати ефекти кореляції, які носять нелокальний характер. Знову звернемося до прикладу — процесу параметричної генерації. Він полягає в тому, що кристал з нелінійними оптичними властивостями (скажімо, KO_3) опромінюють лазерним випромінюванням оптичного діапазону (довжина хвилі 655 нм). На виході кристала утворюються два пучки інфрачервоного діапазону (довжина хвилі 1310 нм) із двічі меншою частотою. Цей процес можна представити як утворення двох "інфрачервоних" фотонів із одного "оптичного". В залежності від взаємної орієнтації кристала та поляризації вхідного випромінювання можливі дві принципово різні ситуації:

1) інфрачервоні фотони ведуть себе незалежним чином, як класичні частки, а вся система знаходиться в так званому *чистому* стані;

2) між інфрачервоними фотонами існує кореляція і стани фотонів *переплутані.* Розглянемо ці ситуації докладніше.

а) Незалежність фотонів означає, що вони мають різні, але визначені (за орієнтацією кристала) поляризації, наприклад, перший фотон знаходиться в стані $|1\rangle$, а інший — в стані $|0\rangle$. При вимірюванні стану одного фотона, скажімо, першого, ми не отримуємо інформації про стан іншого фотона, але при цьому і не змінюємо його. В цьому випадку як система, так і кожна з часток,

перебувають в чистому стані. Хвильова функція такої системи є добутком хвильових функцій її елементів, наприклад:

$$|\psi\rangle = |1\rangle_1 |0\rangle_2, \tag{11.2}$$

де нижні індекси позначають перший та другий фотон.

б) В разі корельованих фотонів обидві частки мають різні поляризації, але неможливо *апріорі* встановити, яка з них в якому стані. Кажуть, що фотони знаходяться в *переплутаних* (*entangled*) станах, хоча система в цілому може знаходитися в чистому стані. Головною особливістю переплутаних станів є те, що вимірюючи стан одного фотона, ми одразу ж змінюємо стан іншого і втрачаємо інформацію про стан системи в цілому. З іншого боку, для визначення стану системи необхідно одночасно зробити вимірювання за обома фотонами. Описана кореляція між фотонами зберігається навіть при розповсюдженні фотонів в різних напрямках (навіть при відстані між фотонами більше ніж 10 км). Поняття переплутаних станів може бути легко узагальнене на системи, що складаються із більшої кількості часток.

Хвильова функція системи в переплутаних станах не може бути представлена у вигляді добутку хвильових функцій окремих елементів в будь-якому базисі. Типовий приклад переплутаних станів системи з двох фотонів задається чотирма так званими *станами Белла:*

$$|\psi_+\rangle = \left(1/\sqrt{2}\right)\left\{|1\rangle_1 |0\rangle_2 + |0\rangle_1 |1\rangle_2\right\}, \tag{11.3}$$

$$|\psi_-\rangle = \left(1/\sqrt{2}\right)\left\{|1\rangle_1 |0\rangle_2 - |0\rangle_1 |1\rangle_2\right\}, \tag{11.4}$$

$$|\phi_+\rangle = \left(1/\sqrt{2}\right)\left\{|1\rangle_1 |1\rangle_2 + |0\rangle_1 |0\rangle_2\right\}, \tag{11.5}$$

$$|\phi_-\rangle = \left(1/\sqrt{2}\right)\left\{|1\rangle_1 |1\rangle_2 - |0\rangle_1 |0\rangle_2\right\}. \tag{11.6}$$

Підкреслимо, що переплутаність станів і ефекти кореляції спостерігаються лише в системах, в яких частки слабо взаємодіють одна з однією і з навколишнім середовищем. З ростом кількості часток взаємодія між частками та часток з навколишнім середовищем призводить до швидкого знищення когерентності.

Врешті-решт, відзначимо ще дві особливості квантових станів.

1) Стан квантової системи неможливо клонувати. Інакше кажучи, якщо ми маємо фотон у довільному і невідомому нам стані, ми не можемо створити ще один фотон в точнісінько такому ж стані, не знищивши перший фотон. Якби клонування було можливим, то створюючи копії квантового об'єкта, ми б могли вимірювати одночасно такі параметри стану, які відповідають некомутуючим операторам, а це заборонено принципом невизначеності Гейзенберга.

2) Стан квантової системи із часом змінюється завдяки впливу зовнішніх тіл (процес декогеренції). Будь-яка ізольованість квантової системи носить відносний характер.

11.1 Квантова криптографія

Криптографія (тайнопис) являє собою один із напрямків криптології – науки, що займається проблемами захисту інформації шляхом її перетворення. Основні напрямки застосування криптографічних методів – передача конфіденційної та достовірної інформації по каналах зв'язку (наприклад, через електронну мережу), встановлення достовірності та автентичності (достеменності) повідомлення, що передається, зберігання інформації (документів, баз даних) на носіях в зашифрованому вигляді тощо.

Серед проблем, які вирішує криптографія, найбільш вразливою завжди була проблема розподілу ключів. Ключ – це інформація (набір кодів), за допомогою якої здійснюється процедура шифрування даних при обміні між різними суб'єктами (сторонами). Як правило, зашифрована інформація передається по відкритих каналах, а ось обмін ключами між суб'єктами повинен відбуватись суворо конфіденційно, тобто, особисто або по закритих каналах. В поширеному протоколі, що обумовлюється так званим стандартом БЕЗ, довірені сторони повинні мати однаковий ключ для зашифрування і розшифрування інформації. Для забезпечення стійкості криптосистеми відносно можливих атак (тобто, для виключення розшифрування інформації сторонніми особами) ключ повинен бути випадковим та абсолютно секретним. Найскладнішою є вимога забезпечення абсолютної секретності ключа — навіть при передачі ключа по закритим каналам не виключена можливість непомітного для довірених сторін несанкціонованого втручання в канал сторонніх осіб (порушників).

Квантова криптографія значно полегшує задачу секретної передачі інформації. Вона вирішує проблему розподілу ключів, використовуючи властивість квантових систем змінювати свій стан в процесі вимірювання та неможливість клонування квантових станів. Процес "підслуховування" передбачає можливість копіювання (відтворення) стану носія інформації, що в разі передачі інформації за допомогою суто квантових об'єктів неможливо. Отже, будь-яка спроба несанкціонованого втручання в канал передачі інформації буде виявлена.

Основні фундаментальні властивості квантових систем, які використовуються в квантовій криптографії, наступні:

1) Вимірювання фізичних характеристик квантових систем (спостережуваних).

У результаті процесу вимірювання деякої фізичної величини стан квантової системи змінюється. Це обумовлено впливом на квантовий об'єкт вимірювального приладу, який принципово неможливо зробити як завгодно слабким. Чим точніше вимірювання, тим сильніший вплив, що воно здійснює, і лише при вимірюваннях дуже малої точності вплив на об'єкт вимірювання може бути досить слабким.

Крім того, збурювання, яке вноситься взаємодією квантового об'єкта з вимірювальним приладом, може бути передбачено тільки статистично й тому не може бути виключено. Цей факт перебуває в різкому протиріччі із класичною

теорією вимірювань, яка базується на припущенні, що взаємодія між об'єктом і приладом якщо й не може бути зроблена як завгодно малою, то принаймні може бути точно врахованою й, отже, у принципі її можна виключити.

На рис.11.1 приведена класифікація квантових технологій.

2) Неможливість точного клонування невідомих квантових станів (теорема про заборону клонування).

Внаслідок лінійності й унітарності квантової механіки неможливо створити точну копію невідомого квантового стану. Таким чином, зловмисник не може виготовити точну копію кубітів або кудитів, що передаються по комунікаційному каналу, щоб провести вимірювання над копією, а оригінал переслати законному користувачеві каналу, не проводячи над ним вимірювання. Цей факт лежить в основі більшості протоколів квантової криптографії, тому що змушує зловмисника вимірювати передавані кудити або переплутувати їх зі своїми допоміжними квантовими системами, що призводить до зміни станів цих кудитів. Ці зміни передаваних станів можуть виявити законні користувачі, виконуючи квантові вимірювання й обмінюючись результатами цих вимірювань по звичайному відкритому каналу зв'язку. Відзначимо, що ймовірність правильно клонувати довільний стан кубіту, створивши одну його копію, дорівнює 5/6. Якщо потрібно створити n копій невідомого стану кубіту, то ймовірність правильного клонування зменшується та при $n \to \infty$ прямує до 2/3 .

3) Неортогональні квантові стани неможливо розрізнити.

Квантова система із двома станами кубітів може перебувати не тільки в базисних станах $|0\rangle$ та $|1\rangle$ (які відповідають, наприклад, вертикальній та горизонтальній поляризації окремого фотону), але й у стані лінійної суперпозиції

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (11.7)$$

де α і β – комплексні числа, що задовольняють умові $|\alpha|^2 + |\beta|^2 = 1$. Вимірюючи стан кубіту, ми знайдемо, що кубіт з імовірністю $|\alpha|^2$ несе значення "0", а з імовірністю $|\beta|^2$ – значення "1".

Внаслідок законів квантової механіки неможливо виконати вимірювання, що дозволило б розрізнити стани $|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ та $|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, крім випадку, коли скалярний добуток $\langle\Psi_1|\Psi_2\rangle = 0$, тобто стани $|\Psi_1\rangle$ і $|\Psi_2\rangle$ ортогональні.

Аналогічно, вимірюючи довільний стан кудиту

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle, \qquad (11.8)$$

ми отримаємо "0" з імовірністю $|\alpha|^2$, "1" з імовірністю $|\beta|^2$ та "2" з імовірністю $|\gamma|^2$ Відзначимо, що суперпозиція квантових станів не має аналога в класичній фізиці.

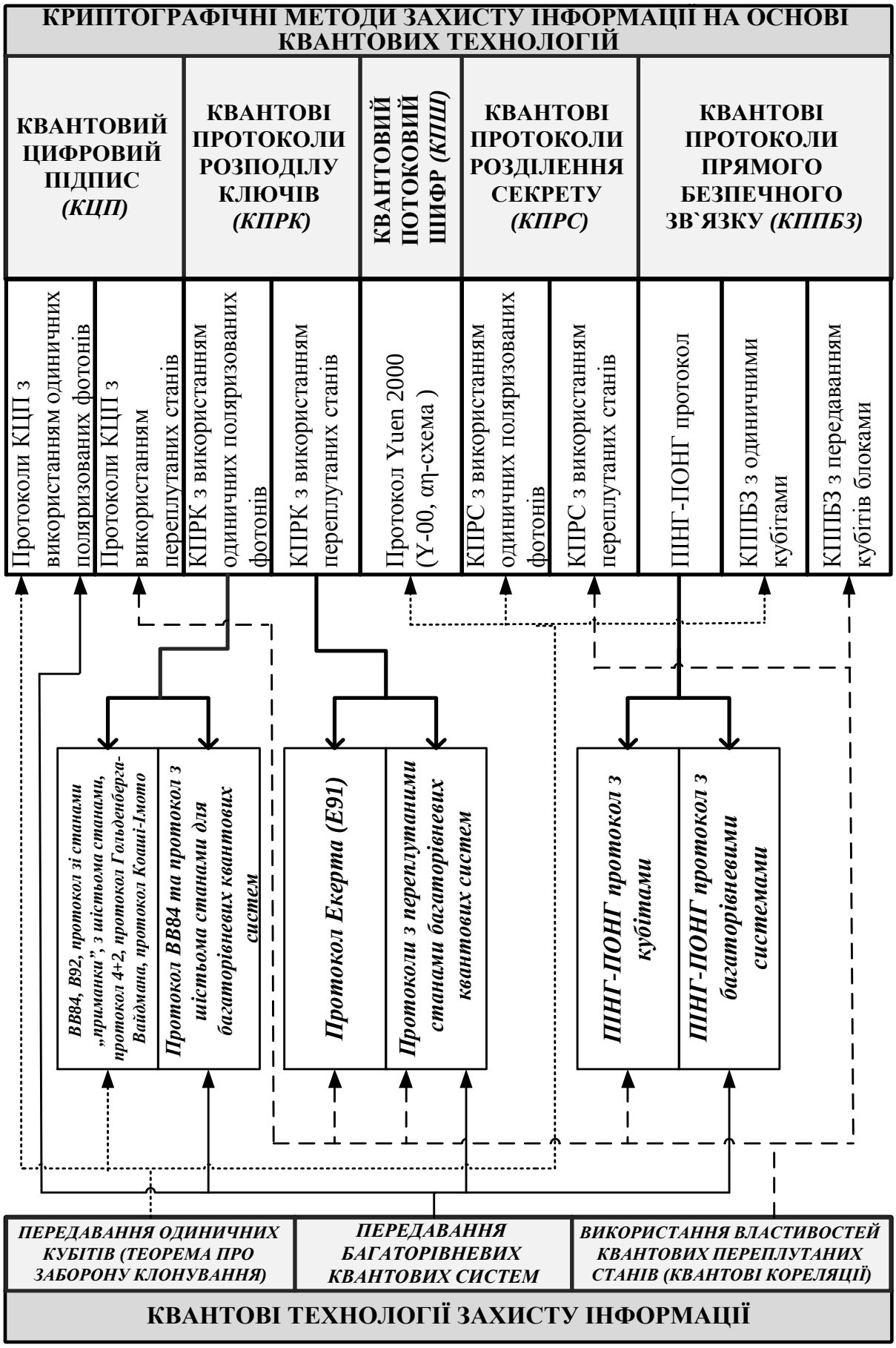


Рис. 11.1. Класифікація квантових технологій

4) Переплутування (квантові кореляції).

Дві або більше квантових системи можуть бути переплутані. Так, пара фотонів у синглетному поляризаційному стані наступна

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 - \left|0\right\rangle_2\left|1\right\rangle_1\right), \qquad (11.9)$$

де індекси позначають номери фотонів –це приклад максимально переплутаного стану двох кубітів. Такий стан називають парою Ейнштейна– Подольського– Розена (ЕПР-парою).

Якщо вимірювання виконується над одним із двох переплутаних кубітів в стані $\left|\Psi^{-}\right\rangle$ (11.9), наприклад, в базисі $\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$, який називається обчислювальним базисом, то результат буде "0" або "1" з однаковою ймовірністю 1/2. Стан другого кубіту антикорельований з першим, тобто, якщо перший кубіт в результаті вимірювання перейшов у стан $\left|0\right\rangle$, то другий перейде в стан $\left|1\right\rangle$, і навпаки. Без проведення вимірювання, однак, жодний із цих двох кубітів не перебуває в певному стані. Відзначимо, що переплутування, як і суперпозиція станів – винятково квантові ефекти, що не мають аналога для об'єктів класичної фізики.

Квантові протоколи розподілення секретних ключів пропонують інший підхід до вирішення цієї проблеми. Теоретично, квантова криптографія може забезпечити захищене від перехоплення розподілення ключа, оскільки, на відміну від класичної криптографії, вона заснована на законах фізики, а не на тому факті, що для успішного перехоплення потрібні були б величезні обчислювальні потужності. Внаслідок вищезазначених властивостей квантових систем, зловмисник вносить у передану окремими фотонами інформацію деяку кількість помилок, які можуть бути виявлені легітимними користувачами. Відзначимо, що закони квантової механіки дозволяють не тільки виявити збурювання станів, але й зв'язати рівень помилок при вимірюваннях у легітимних користувачів з кількістю інформації, що міг отримати зловмисник. Це дозволяє провести процедуру підсилення секретності, при якій довжина переданого ключа зменшується на деяке число бітів, що залежить від рівня помилок при передачі. У результаті кількість інформації про ключ, що може мати зловмисник після цієї процедури, обмежена зверху як завгодно малою величиною з імовірністю як завгодно близькою до одиниці. Таким чином, протоколи квантового розподілення ключів, на відміну від більшості класичних схем, мають теоретико-інформаційну стійкість, що не залежить від обчислювальних та інших технічних можливостей зловмисника.

11.2 Протоколи квантового поширення ключа

11.2.1 Протокол BB84

Ідея використати квантові об'єкти для захисту інформації від підробки й несанкціонованого доступу вперше була висловлена Стефаном Вейснером (Stephen Weisner) в 1970 р. Через 10 років Беннет і Брассард, які були знайомі з роботою Вейснера, запропонували використати квантові об'єкти для передачі секретного ключа. В 1984 р. вони опублікували статтю, у якій описувався протокол квантового поширення ключа BB84.

Носіями інформації в протоколі BB84 є фотони, які поляризовані під кутами 0, 45, 90, 135 градусів. Відповідно до законів квантової фізики за допомогою вимірювання можна розрізнити лише наступне: якщо для двох ортогональних станів відомо, що фотон поляризований або вертикально, або горизонтально, то шляхом вимірювання можна встановити, як саме; теж саме можна стверджувати щодо поляризації під кутами 45 і 135 градусів. Однак з вірогідністю відрізнити вертикально поляризований фотон від фотона, поляризованого під кутом 45, неможливо.

Ці особливості поводження квантових об'єктів лягли в основу протоколу квантового поширення ключа. Відправник кодує дані, що відправляють, задаючи певні квантові стани. Одержувач реєструє ці стани. Потім одержувач і відправник спільно обговорюють результати спостережень. В остаточному підсумку з як завгодно високою вірогідністю можна бути впевненим, що передані й прийняті кодові послідовності тотожні. Обговорення результатів стосується помилок, внесених шумами або зловмисником, і ні в найменшій мірі не розкриває вмісту переданого повідомлення. Може обговорюватися парність повідомлення, але не окремі біти. Відкритий канал зв'язку не обов’язково повинен бути конфіденційним, необхідно, щоб тільки забезпечував автентифікацію.

Щоб обмінятися ключем, Аліса й Боб використовують наступні дії:

1. Аліса посилає Бобу біт A_i, задаючи певні квантові стани - поляризацію в 0, 45, 90, 135 градусів. Відлік кутів можна вести від напрямку "вертикально нагору" по годинниковій стрілці.
2. Боб розпізнає двома аналізаторами: один розпізнає вертикально-горизонтальну поляризацію, інший — діагональну. Для кожного фотона Боб випадково вибирає один з аналізаторів і записує тип аналізатора й результат вимірів. Отриманий, так званий «сирий» ключ $B_i = A_i$ з імовірністю $P = 75\%$. Тобто, він містить 25% помилок.
3. По загальнодоступному каналу зв'язку Боб повідомляє Алісі, які аналізатори використалися, але не повідомляє, які результати були отримані.
4. Аліса по загальнодоступному каналу зв'язку повідомляє Бобу, які аналізатори він вибрав правильно. Ті фотони, для яких Боб невірно вибрав аналізатор, відкидаються.

5. Для виявлення перехоплення Аліса й Боб вибирають випадкову ділянку ключа й порівнюють його по загальнодоступному каналу зв'язку. Якщо відсоток помилок великий, то він може бути віднесений на рахунок Єви і процедура повторюється спочатку.

Як джерело світла може використатися діод або лазер. Як провідник використовують або простір, або оптичні кабелі.

11.2.2 Приклад шифрування протоколом BB84

Умовні позначення:

Ці правила можуть із легкістю бути замінені на протилежні (аби тільки Аліса й Боб домовилися між собою), однак у таблицях 11.1 і 11.2 прийняті саме ці позначення.

Таблиця 11.1

Позначення аналізатора	Поляризація фотонів
+	Прямокутний
X	Діагональний

Таблиця 11.2

Послідовність фотонів Аліси	|	/	/	—	\	|	|	—	—
Послідовність аналізаторів Боба	+	**X**	+	+	**X**	**X**	**X**	+	**X**
Результати вимірів Боба	0	**0**	**1**	**1**	1	0	1	1	**0**
Аналізатори обрані вірно	так	так		так	так			так	
Ключ	0	**0**		**1**	1			1	

Якби Єва робила перехоплення інформації за допомогою устаткування, подібного до устаткування Боба, то приблизно в 50 відсотках випадків вона вибрала б невірний аналізатор, не змогла б визначити стан отриманого нею фотона і відправила б фотон Бобу в стані, обраному навмання. При цьому в половині випадків вона вибере невірну поляризацію й, таким чином, приблизно в 25 відсотках випадків результати вимірювань Боба можуть відрізнятися від результатів Аліси. Це досить помітно й швидко виявиться. Однак, якщо Єва перехоплює тільки 10% інформації, тоді рівень помилок буде 2.5%, що менш помітно.

11.2.3 Зниження рівня помилок і збільшення таємності ключа

Внесені помилки можуть бути виявлені й усунуті за допомогою підрахунку парності так, що рівняється парність у блоках з декількох бітів, при цьому після перевірки один біт з кожного блоку відкидається. Беннет в 1991 році запропонував наступний протокол.

1. Відправник й одержувач домовляються про довільну перестановку бітів у рядках, щоб зробити положення помилок випадковими.
2. Рядки діляться на блоки розміру k (k вибирається так, щоб імовірність помилки в блоці була мала).
3. Для кожного блоку відправник й одержувач обчислюють і відкрито сповіщають один одного про отримані результати. Останній біт кожного блоку видаляється.
4. Для кожного блоку, де парність виявилася різною, одержувач і відправник роблять ітераційний пошук і виправлення невірних бітів.
5. Щоб виключити кратні помилки, які можуть бути не замічені, операції пунктів 1-4 повторюються для більшого значення k.
6. Для того щоб визначити, залишилися чи ні невиявлені помилки, одержувач і відправник повторюють псевдовипадкові перевірки:
   - Одержувач і відправник відкрито повідомляють про випадкове перемішування позицій половини бітів у їхніх рядках.
   - Одержувач і відправник відкрито порівнюють парності. Якщо рядки відрізняються, парності повинні не збігатися з імовірністю 1/2.
   - Якщо має місце відмінність, одержувач і відправник використають двійковий пошук і видалення невірних бітів.
7. Якщо відмінностей немає, після m ітерацій одержувач і відправник одержують ідентичні рядки з імовірністю помилки 2^{-m}.

Збільшення таємності ключа також може бути зроблене без додаткового обміну даними по відкритому каналу. Наприклад, при наявності в Аліси послідовності відправлених бітів A_i і послідовності прийнятих бітів B_i у Боба, обоє можуть зробити наступні перетворення:

$$A'_i = A_{2i} xor A_{2i+1}$$
$$B'_i = B_{2i} xor B_{2i+1},$$

що забезпечує таємність ключа від Єви, навіть якщо вона змогла перехопити й скопіювати кожен другий фотон, що пересилається.

11.2.4 Протокол Екерта

Якщо Аліса й Боб не збираються використати отриманий ними ключ відразу, то перед ними виникає нова проблема - як зберегти ключ у секреті? В 1991 р. Артур Екерт (Artur Ekert) запропонував протокол, що дозволяє вирішити обидві ці проблеми - поширення й зберігання ключа. Протокол

Екерта заснований на ефекті EPR (Einstein-Podolsky-Rosen). Ефект EPR виникає, коли сферично симетричний атом випромінює два фотони в протилежних напрямках у сторону двох спостерігачів. Фотони випромінюються з невизначеною поляризацією, але в силу їхньої симетрії поляризації завжди протилежні. Такі стани двох фотонів називаються зчепленими.

На основі ефекту EPR Екерт запропонував криптосхему, що гарантує безпеку пересилання й зберігання ключа. Відправник генерує деяку кількість EPR фотонних пар. Один фотон з кожної пари він залишає для себе, другий посилає своєму партнерові. При цьому, якщо ефективність реєстрації близька до одиниці, при одержанні відправником значення поляризації 1 його партнер зареєструє значення 0 і навпаки. Ясно, що в такий спосіб партнери кожний раз, коли потрібно, можуть одержати ідентичні псевдовипадкові кодові послідовності. Практично реалізація даної схеми проблематична через низьку ефективність реєстрації й вимірювання поляризації одиночного фотона.

Неефективність реєстрації є платою за таємність. Варто враховувати, що при роботі в однофотонному режимі виникають чисто квантові ефекти. При горизонтальній поляризації й використанні вертикального поляризатора результат очевидний - фотон не буде зареєстрований. При 45° поляризації фотона й вертикальному поляризаторі ймовірність реєстрації 50%. Труднощі також полягають у тому, що в цей час не всі зчеплені стани піддаються вимірюванню, не говорячи вже про створення ідеальних, що відбивають, ємностей для зберігання фотонів.

11.2.5 Практична реалізація протоколу BB84

Схема реалізації односпрямованого каналу із квантовим шифруванням показана на рис. 11.2, 11.3. Передавальна сторона перебуває ліворуч, а приймаюча - праворуч. Осередки Покеля служать для імпульсної варіації поляризації потоку квантів передавачем і для аналізу імпульсів поляризації приймачем. Передавач може формувати один із чотирьох станів поляризації (0, 45, 90 й 135 градусів). Властиво передані дані надходять у вигляді керуючих сигналів на ці осередки. Як канал передачі даних може використовуватися оптичне волокно. Як первинне джерело світла можна використати й лазер.

На приймаючій стороні після осередку Покеля ставиться кальцітна призма, що розщеплює пучок на два фотодетектори (ФД), які вимірюють дві ортогональні складові поляризації. При формуванні переданих імпульсів квантів доводиться вирішувати проблему їхньої інтенсивності. Якщо квантів в імпульсі 1000, є ймовірність того, що 100 квантів по шляху буде відведено зловмисником на свій приймач. Аналізуючи пізніше відкриті переговори між передавальною й приймаючою сторонами, він може одержати потрібну йому інформацію. В ідеалі число квантів в імпульсі повинне бути біля одного. Тут будь-яка спроба відводу частини квантів зловмисником приведе до істотного росту числа помилок у приймаючої сторони. У цьому випадку прийняті дані повинні бути відкинуті й спроба передачі повторена. Але, роблячи канал більш стійким до перехоплення, ми в цьому випадку

зіштовхуємося із проблемою "темнового" шуму (видача сигналу у відсутності фотонів на вході) приймача (адже ми змушені підвищувати його чутливість). Для того, щоб забезпечити надійне транспортування даних, логічному нулю й одиниці можуть відповідати певні послідовності станів, що допускають корекцію одинарних і навіть кратних помилок.

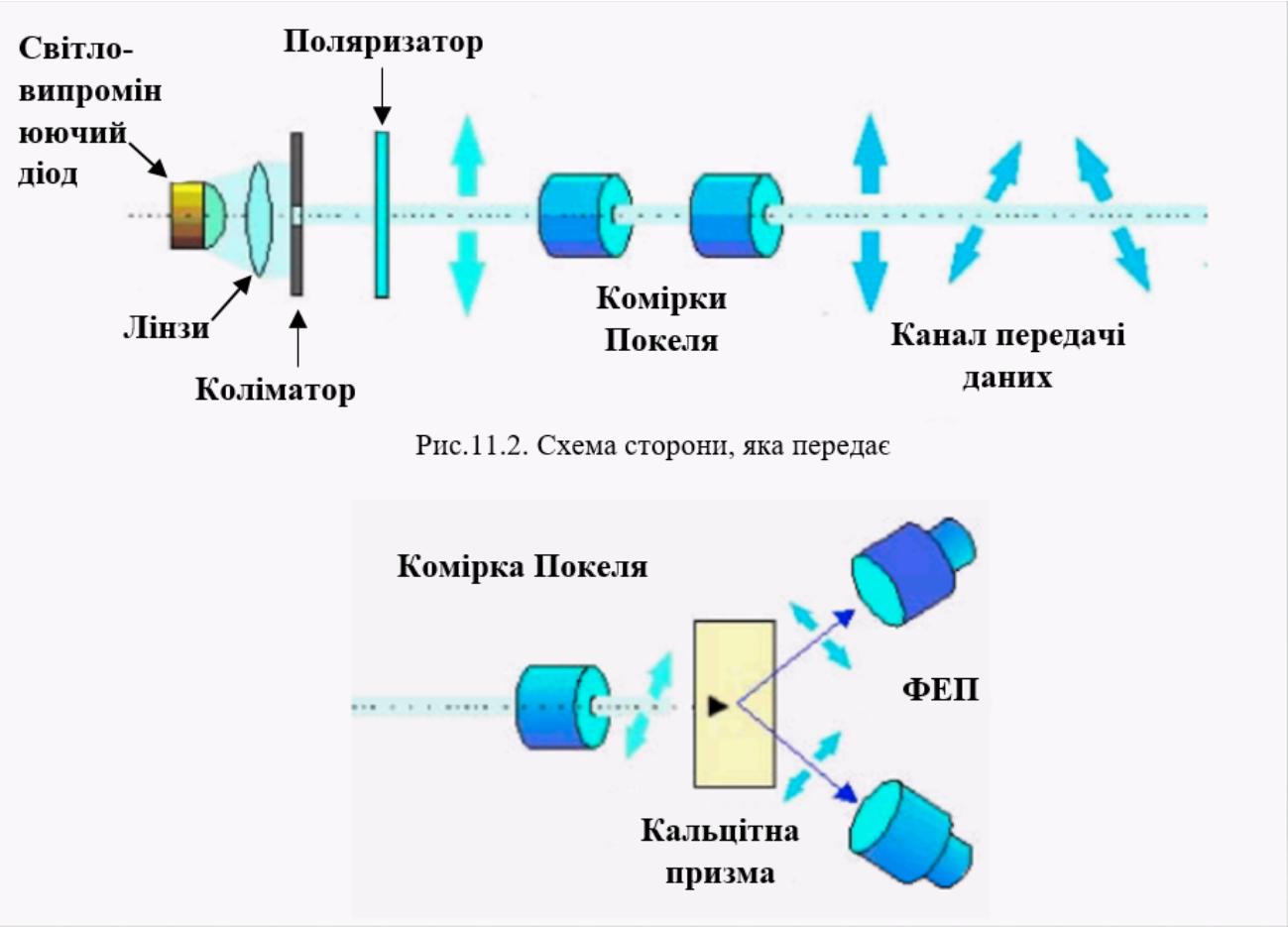


Рис.11.2. Схема сторони, яка передає

Рис.11.3. Схема реалізації односпрямованого каналу із квантовим шифруванням

11.2.6 Протокол B92

В протоколі B92 також використовуються як носії інформації фотони, однак, поляризовані тільки у двох станах. Такі стани поляризації більш зручні для передачі даних на більші відстані по оптичних кабелях.

В алгоритмі B92 приймач і передавач створюють систему, що базується на інтерферометрах Маха-Цендера. Відправник визначає кути фазового зрушення, що відповідають логічному нулю й одиниці ($F_A = p/2$), а приймач задає свої фазові зрушення для логічного нуля ($F_B = 3p/2$) і одиниці ($F_B = p$). У даному контексті зміна фази $2p$ відповідає зміні довжини шляху на одну довжину хвилі використовуваного випромінювання. Хоча фотони поводяться при детектуванні як частки, вони поширюються як хвилі.

Імовірність того, що фотон, відправлений відправником, буде детектовано одержувачем, дорівнює

$$P_d = \cos^2\left(\frac{F_A - F_B}{2}\right)$$

і характеризує інтерференцію амплітуд хвиль, що поширюються по верхньому й нижньому шляхах (див. рис. 11.4). Імовірність реєстрації буде варіюватися від 1 (при нульовій різниці фаз) до нуля. Тут передбачається, що відправник й одержувач використовують фазові зрушення $(F_A\ F_B) = (0,3p/2)$ для нульових

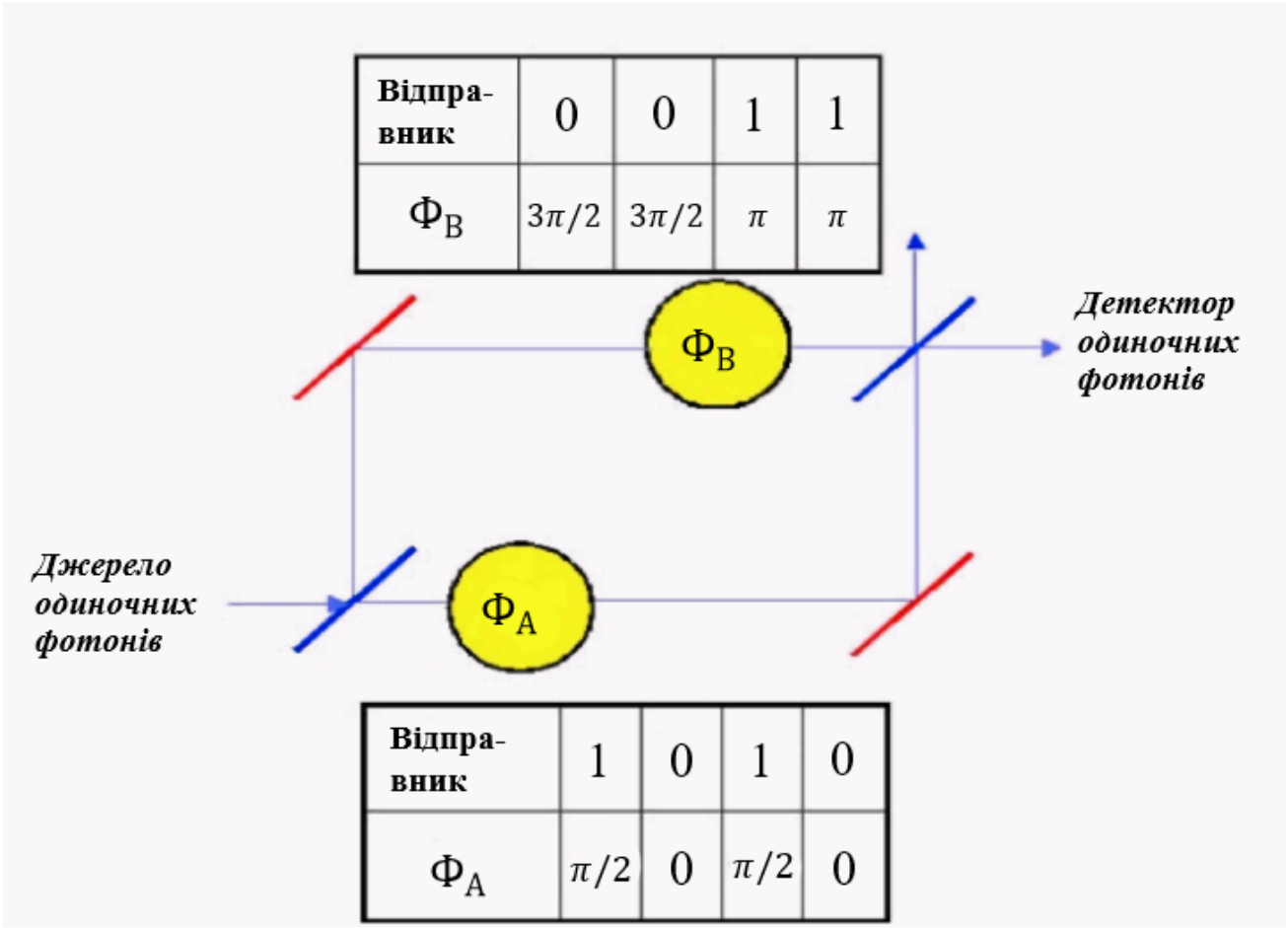


Рис. 11.4. Реалізація алгоритму B92

бітів і $(F_A\ F_B) = (p/2,p)$ для одиничних бітів (для алгоритму BB84 використовуються інші припущення).

Для реєстрації одиночних фотонів, крім ФД, можуть використовуватися твердотільні лавинні фотодіоди (германієві й InGaAs). Для зниження рівня шуму їх варто прохолоджувати. Ефективність реєстрації одиночних фотонів лежить у діапазоні 10-40%. При цьому варто враховувати також досить високе поглинання світла оптичним волокном (~0,3-3ДБ/км). Схема інтерферометра із двома волокнами досить нестабільна через різні властивості транспортних волокон і може успішно працювати тільки при малих

відстанях. Кращих характеристик можна досягти, мультиплексіруючи обидва шляхи фотонів в одне волокно (див. рис. 11.5).

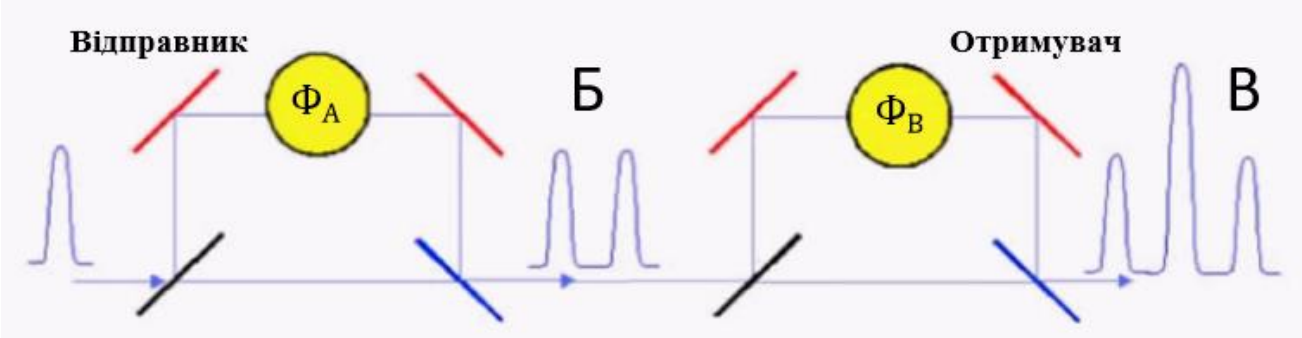


Рис. 11.5. Інтерферометр із одним транспортним волокном

У цьому варіанті відправник й одержувач мають ідентичні нерівноплічні інтерферометри Маха-Цендера (червоними кольорами відзначені дзеркала). Різниця фаз довгого й короткого шляхів БВ багато більше часу когерентності світлового джерела. Із цієї причини інтерференції в межах малих інтерферометрів не відбувається (Б). Але на виході інтерферометра одержувача вона можлива (В). Імовірність того, що фотонні амплітуди складуться (центральний пік вихідного сигналу інтерферометра В), дорівнює

$$P = \frac{1}{8}\left(1 + \cos\left(F_A - F_B\right)\right).$$

Развітлювачі пучка (напівпрозорі дзеркала) можуть бути замінені на оптоволоконні об'єднувачі (coupler). Практичні вимірювання для транспортного кабелю довжиною 14 км показали ефективність генерації біта ключа на рівні 2,2 * 10^{-3} при частоті помилок близько 1,2%.

11.2.7 Практичні аспекти квантової криптографії

При створенні практичних криптосистем, заснованих на квантовому поширенні ключа, доводиться зіштовхуватися з наступними проблемами:

- Низька швидкість передачі.
- Невеликі відстані.
- Неможливість створення квантових повторювачів.
- Інтенсивність імпульсів квантів.
- Атаки зловмисників на квантовий канал.

При формуванні переданих імпульсів квантів доводиться вирішувати проблему їхньої інтенсивності. У теоретичній частині ми виходимо із припущення, що повідомлення передається й приймається імпульсами по одному кванту. На практиці такого результату домогтися не вдається - джерело з ненульовою ймовірністю випромінює більше одного фотона. Якщо квантів в імпульсі 1000, є ймовірність того, що 100 квантів по шляху буде відведено

зловмисником на свій приймач. Аналізуючи пізніше відкриті переговори між передавальною й приймаючою сторонами, він може отримати потрібну йому інформацію. В ідеалі число квантів в імпульсі повинне бути біля одного. Тут будь-яка спроба відводу частини квантів зловмисником приведе до істотного росту числа помилок у приймаючої сторони. У цьому випадку прийняті дані повинні бути відкинуті й спроба передачі повторена. Але, роблячи канал більш стійким до перехоплення, ми в цьому випадку зіштовхуємося із проблемою "темнового" шуму (видача сигналу у відсутності фотонів на вході) приймача (адже ми змушені підвищувати його чутливість).

Атаки на квантову передачу класифікуються в такий спосіб:

- Некогерентні (індивідуальні).
- Когерентні (масові).
- Спільні.
- Колективні.

Практичні успіхи

Практичні роботи в області квантової криптографії ведуть такі компанії як IBM, Mitsubishi, Toshiba, лабораторії GAP-Optique, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут (Caltech), Magi, холдинг Qineti (табл. 11.3).

Таблиця 11.3

Організація	**Дослідники**	**Досягнуті результати**
IBM	Чарльз Беннетт, Жиль Броссард	
Gap-Optique	Николас Гисин	67 км
Mitsubishi		87 км, 7.2 біт/с
Toshiba Research Europe		100 км

Створена також комерційна квантова криптосистема id 3000 Clavis Quantum Key Distribution System, що підтримує:

- Безпечний обмін ключами на відстані до 100 км.
- Підтримку протоколу BB84.
- Убудований протокол просіювання ключа.
- Протокол шифрування й передачі файлів.
- Бітрейт = 1500 біт/с.

11.2.8 Стан робіт у галузі квантової криптографії та протоколів

Активні дослідження в області квантової криптографії ведуть IBM, GAP-Optique, Mitsubishi, Toshiba, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, молода компанія Magi і холдинг Qineti, підтримуваний британським міністерством оборони.

Квантова криптографія як сегмент ринку тільки починає формуватися, і тут поки що на рівні можуть грати й світові комп'ютерні корпорації, і невеликі починаючі компанії.

В IBM тривають фундаментальні дослідження в області квантових обчислень, початі групою Чарльза Беннетта. Ними займається корпорація лабораторії Almaden Research Center. Про практичні досягнення IBM у квантовій криптографії відомо не багато — ці роботи мало рекламуються.

Дослідникам з Лос-Аламоса вдалося передати фотонний ключ по оптоволокну на відстань 48 км зі швидкістю в кілька десятків кілобітів на секунду. Цього досить, щоб з'єднати між собою відділення банку або урядові заклади.

Створена при участі Женевського університету компанія GAP Optique під керівництвом Ніколаса Гисина об'єднує теоретичні дослідження із практичною діяльністю. Фахівцям цієї фірми вдалося передати ключ на відстань 67 км із Женеви в Лозанну за допомогою майже промислового зразка апаратури. Цей рекорд був побитий корпорацією Mitsubishi Electric, що передала квантовий ключ на відстань 87 км, щоправда, на швидкості в 1 байт/с.

Дослідження в області квантової криптографії ведуться й у європейському дослідницькому центрі Toshiba Research Europe Limited (TREL), розташованому в Кембриджі (Великобританія). Він спонсірується англійським урядом; у них беруть участь співробітники Кембриджського університету й Імперіала-коледжу в Лондоні. Зараз вони можуть передавати фотони на відстань до 100 км. Таким чином, технологія може бути використана тільки в межах одного міста. Є надія, що незабаром будуть випущені комерційні продукти.

Два роки тому доктори Ендрю Шилдс і його колеги з TREL і Кембриджського університету створили діод, здатний випускати одиничні фотони. В основі нового променевого діоду лежить "квантова точка" — мініатюрний шматочок напівпровідникового матеріалу діаметром 15 нм і товщиною 5 нм, що може при подачі на нього струму захоплювати лише по одній парі електронів і дірок. Рекомбінація одного електрона з однією діркою приводить до випущення фотона. При цьому струм, що подається на "квантову точку", підбирається так, щоб у рекомбінації брала участь тільки одна пара електрон — дірка. Але навіть якщо новий променевий діод випустить два фотони, які будуть характеризуватися різною довжиною хвилі, що дозволяє відітнути зайву частку за допомогою фільтра. Звичайні променеві діоди й лазери випускають фотони групами, що теоретично дає можливість доступу до визначення характеристик окремих фотонів, інші фотони продовжать свій шлях у незмінному виді.

Щоб обійти труднощі, пов'язані із створенням джерел окремих фотонів, Фредерик Гроссан з Інституту оптики в Орсе (Франція) розробив методику, що дозволяє шифрувати повідомлення за допомогою імпульсів, що складаються з кіль-

кох сотень фотонів. На її безпеку не впливає навіть ослаблення сигналу на більших відстанях. Гроссан відмовився від окремих квантів світла й запропонував усереднювати значення амплітуди й фази електричного поля групи фотонів. Як і поляризація окремого фотона, ці змінні зв'язані один з одним принципом невизначеності. Однак на відміну від поляризації фотона, що приймає одне із двох значень уздовж ортогонального напрямку, ці змінні можуть приймати безперервний ряд значень.

Подібні дослідження у квантовій криптографії ведуться одночасно декількома групами. Але тільки групі Гроссана вдалося продемонструвати практичні перспективи, а також створити апаратуру й ПЗ для роботи із квантовим ключем. При вимірюванні безперервного ряду значень уже не обов'язково реєструвати кожний фотон. У ході експериментальної демонстрації вдалося передати зашифровані дані зі швидкістю 75 кбіт/с — при тому, що більше половини фотонів губилося.

Така схема потенційно має набагато більшу швидкодію, чим схеми з рахунком одиничних фотонів. Це робить її, на думку розроблювачів, досить привабливою для швидкої передачі секретних даних на відстані менше 15 км. Перспективи її використання на більших дистанціях вимагають додаткового вивчення.

У дослідження високошвидкісної квантової криптографії поглибилася й корпорація NEC в особі свого інституту NEC Research Institute. Над прототипами комерційних систем квантової криптографії, що діють по оптоволоконних лініях зв’язку, працює підрозділ телекомунікаційного гіганта Verizon Communications — BBN Technologies.

Команда Північно-Західного університету (США) співробітничає з Telcordia Technologies і BBN Technologies, намагаючись довести технологію до комерційного застосування. Їм удалося передати зашифровані дані по оптоволокну зі швидкістю 250 Мбіт/с. Тепер необхідно довести, що схема дозволяє сигналам проходити крізь оптичні підсилювачі. У цьому випадку метод можна буде використати не тільки в спеціальних оптоволоконних лініях зв'язку між двома точками, а й у більш широких мережах. Ще ця команда працює над тим, щоб досягти швидкостей порядку 2,5 Гбіт/с. Дослідження Північно-Західного університету в області квантової криптографії фінансуються DARPA — оборонним відомством США.

Міністерством оборони Великобританії підтримується дослідницька корпорація Qineti, що активно вдосконалює технологію квантового шифрування. Ця компанія з'явилася на світ в результаті ділення британського агентства DERA (Defence Evaluation and Research Agency) в 2001 р., увібравши в собі всі неядерні оборонні дослідження. Про свої досягнення вона широкій публіці поки не повідомляє.

До досліджень приєдналося й кілька молодих компаній, у тому числі швейцарська Id Quantique (www.idquantique. com), що представила комерційну систему квантової криптографії, і Magi Technologies (www.magiqtech.com) з Нью-Йорка, що випустила прототип комерційної квантової криптографічної технології власної розробки. Magi Technologies була створена в 1999 р. на засоби великих фінансових інститутів. Крім власних співробітників, з нею взаємодіють науковці із цілого ряду університетів США, Канади, Великобританії й Німеччині. Віце-прези-

дентом Magi є Олексій Трифонов, який в 2000 р. захистив докторську дисертацію в Петербурзькому університеті. Рік назад Magi одержала 7 млн. доларів від декількох інвесторів, включаючи засновника Amazon.com Джеффа Безоса.

У продукті Magi засіб для розподілу ключів (quantum key distribution, QKD) названий Navajo — по імені індіанців Навахо, мову яких у Другій світовій війні американці використали для передачі секретних повідомлень, оскільки за межами США її ніхто не знав. Navajo здатний у реальному часі генерувати й поширювати ключі засобами квантових технологій і призначений для забезпечення захисту від внутрішніх і зовнішніх зловмисників. Продукт Navajo перебуває в стані бета-тестування й стане комерційно доступним наприкінці року. Кілька комунікаційних компаній тестують Navajo у своїх мережах.

Інтерес до квантової криптографії з боку комерційних і військових організацій росте, тому що ця технологія гарантує абсолютний захист. Творці технологій квантової криптографії впритул наблизилися до того, щоб випустити їх з лабораторій на ринок. Залишилося небагато почекати, і вже дуже незабаром квантова криптографія забезпечить надвисокий рівень безпеки для тих, у кого параноя є звичним станом психіки - банкірів і співробітників спецслужб.

12 Практичні роботи

12.1 Практична робота №1

Тема: Основні поняття теорії множин. Тотожності алгебри множин. Доведення законів алгебри множин. Скінченні множини. Потужність скінченної множини. Декартів добуток множин.

Мета: Пригадати означення множини, способи задання множин та дії, які можна виконувати над об'єктами множин.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Основні поняття теорії множин

Визначення ("інтуїтивне" визначення множини). Довільний набір об'єктів, що попарно розрізняються, називають ***множиною***.

Для множин натуральних, цілих, раціональних, дійсних та комплексних чисел використовуватимемо "класичні" позначення: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Вважатимемо, що множина $\mathbb{N}$ містить цілі додатні числа ($0 \notin \mathbb{N}$). Для множини, що не містить жодного елемента (порожньої множини) будемо використовувати позначення $\varnothing$.

Визначення. Множини A та B називають ***еквівалентними*** або рівними ($A = B$), якщо вони містять одні й ті самі елементи:

$$A = B \Leftrightarrow ((x \in A) \leftrightarrow (x \in B)).$$

Визначення. Множину B називають ***підмножиною*** множини A ($B \subset A$), а множину A – надмножиною множини B ($A \supset B$), якщо кожен елемент множини B належить множині A:

$$(B \subset A) \Leftrightarrow (A \supset B) \Leftrightarrow ((x \in B) \to (x \in A)).$$

Очевидно, що $\varnothing \subset A$ та $A \subset A$ для довільної множини A. Множину $B \subset A$, таку, що $B \neq \varnothing$, $B \neq A$, іноді називають ***власною підмножиною*** множини A.

Способи задавання множин

1. Вербальний (словесний) за допомогою опису характеристичних властивостей, які повинні мати елементи множин.

Наприклад, S – множина студентів жіночої статі у цій аудиторії.

2. Безпосереднє перелічення елементів множини.

Наприклад, $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{Маша, Петро, Василь\}$, $C = \{Зебра\}$.

3. Предикатний (характеристичний) за допомогою характеристичного предикату – деякої умови, вираженої у формі логічного твердження або процедури, яка повертає логічне значення, і дозволяє перевіряти, належить чи ні будь-який даний елемент множині. Якщо для даного елемента ця умова виконується, то він належить визначеній множині, у протилежному випадку – не належить. Тобто, множина задається у вигляді $\{x : P(x)\}$ або $\{x \mid P(x)\}$, де $P(x)$ – характеристичний предикат (характеристична властивість). Часто використовують позначення $A = \{x \in U : P(x)\}$ – множина A містить ті і тільки ті елементи x, що належать множині U та для яких правдиве висловлення $P(x)$.

Наприклад, $A = \{x \mid x - натуральне\ число\}$;

$B = \{x \mid x - \textit{цифра десяткової системи}\}$;

$C = \{x \mid x - \textit{парне число}\}$;

$D = \{x \in N : x = 1(\mathrm{mod}3)\} = \{1, 4, 7, \ldots, 3n+1, \ldots\}$;

E = { x : x – великі літери українського алфавіту } = { А, Б, …, Я}.

4. Задавання множин з використанням формул, які містять операції (об'єднання, переріз, доповнення тощо) над відомими множинами.

Операції над множинами

Визначення. Об'єднанням множин A та B називають множину

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}.$$

Визначення. Перерізом множин A та B називають множину

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}.$$

Якщо $A \cap B = \varnothing$, то множини A та B не перерізаються.

Визначення. Різницею множин A та B називають множину

$$A \setminus B = \{x : (x \in A) \wedge (x \notin B)\}.$$

Визначення. Симетричною різницею множин A та B називають множину

$$A \Delta B = \{x : (x \in A) \oplus (x \in B)\},$$

де операція $\oplus$ – логічна функція заперечення тотожності.

Очевидно, що $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Приклад 1. $\{1,2,3\} \setminus \{3,4\} = \{1,2\}$, $\{1,2,3\} \Delta \{3,4\} = \{1,2,4\}$.

Зауваження. Надалі вважатимемо, що визначена так звана універсальна множина U, що містить всі елементи, які будемо розглядати.

Визначення. Доповненням (запереченням) до множини A (відносно універсальної множини U) називають множину $\overline{A} = \{x \in U : (x \notin A)\}$.

Легко побачити, що $\overline{A} = U \setminus A$ та $A \setminus B = A \cap \overline{B}$.

Тотожності алгебри множин

Закони алгебри множин цілком аналогічні законам алгебри висловлень: операціям диз'юнкції, кон'юнкції та заперечення в алгебрі висловлень відповідають об'єднання, переріз та доповнення над множинами.

Основні тотожності алгебри множин

Введемо чотири пари основних законів алгебри множин.

Нехай A, B, C – довільні формули алгебри множин.

1. *Комутативність* (переставний закон): $A \cup B = B \cup A$,
$A \cap B = B \cap A$.
2. *Дистрибутивність* (розподільний закон):
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
3. *Нейтральність*: $A \cup \varnothing = A$,
$A \cap U = A$.
4. *Доповненість*: $A \cup \overline{A} = U$,

$$A \cap \overline{A} = \varnothing.$$

Інші закони алгебри множин

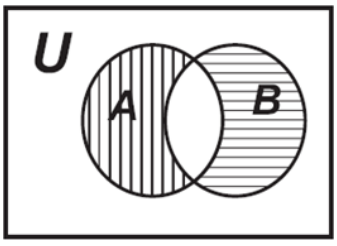
5. *Універсальні межі:* $A \cup U = U$,
$A \cap \varnothing = \varnothing.$
6. *Абсорбація* (поглинання): $A \cup (A \cap B) = A,$
$A \cap (A \cup B) = A.$
7. *Ідемпотентність:* $A \cup A = A,$
$A \cap A = A.$
8. *Асоціативність* (сполучний закон): $A \cup (B \cup C) = (A \cup B) \cup C,$
$A \cap (B \cap C) = (A \cap B) \cap C.$
9. *Єдиність доповнення:*
система рівнянь $\begin{cases} A \cup X = U, \\ A \cap X = \varnothing \end{cases}$ відносно X.
10. *Інволютивність:* $\overline{\overline{A}} = A.$
11.
12. *Закони (правила) де Моргана:* $(\overline{A \cup B}) = \overline{A} \cap \overline{B}$,
$(\overline{A \cap B}) = \overline{A} \cup \overline{B}.$

Діаграми Венна

Діаграми Венна (інша назва – круги Ейлера) допомагають наочно проілюструвати результати виконання операцій в алгебрі множин, а також “вгадати” деякі нескладні тотожності.

На діаграмі Венна універсальну множину зображують у вигляді прямокутника, кожну іншу множину – у вигляді круга (або іншої фігури). Якщо відомо, що множини не перерізаються, відповідні круги зображують такими, що не перерізаються. Якщо відомо, що $A \subset B$, круг множини A зображують всередині круга множини B. Якщо апріорі нічого не відомо про взаємне положення множин, відповідні круги зображують такими, що перерізаються, та жоден круг не лежить цілком всередині іншого.

Приклад 2. Зобразимо на діаграмі Венна симетричну різницю множин $A \Delta B$.



З наведеного рисунка легко “вгадується” тотожність $A \Delta B = (A \cup B) \setminus (A \cap B)$, однак ця тотожність потребує акуратного доведення.

Доведення законів алгебри множин

Модельне доведення

Модельний метод доведення базується на визначенні еквівалентності (рівності) множин та визначенні підмножини:

$$(A = B) \Leftrightarrow ((x \in A) \leftrightarrow (x \in B)) \Leftrightarrow (A \subset B) \wedge (B \subset A);$$

$$(A \subset B) \Leftrightarrow (B \supset A) \Leftrightarrow ((x \in A) \rightarrow (x \in B)).$$

Приклад 3. Доведемо тотожність поглинання: $A \cup (A \cap B) = A.$

$$(x \in (A \cup (A \cap B))) \Leftrightarrow (x \in A) \vee (x \in (A \cap B)) \Leftrightarrow$$

$$\Leftrightarrow (x \in A) \vee ((x \in A) \wedge (x \in B)) \Leftrightarrow (x \in A).$$

Зауваження. На останньому логічному переході ми використали закон поглинання для алгебри висловлень.

Приклад 4. Доведемо еквівалентність: $A \subset B \Leftrightarrow A \cup B = B.$

1. Нехай $A \subset B$, тобто $(x \in A) \Leftrightarrow (x \in B)$. Потрібно довести: $A \cup B = B$, тобто $(x \in A \cup B) \Leftrightarrow (x \in B)$.

$$(x \in A \cup B) \Leftrightarrow (x \in A) \vee (x \in B) \Leftrightarrow (x \in B),$$

оскільки $(x \in A) \Rightarrow (x \in B)$.

2. Нехай $A \cup B = B$. Тоді, з означення операції об'єднання множин, $(x \in A) \Rightarrow (x \in B)$, тобто $A \subset B$.

Приклад 5. Доведемо закон модулярності:

$$A \subset B \Leftrightarrow A \cup (B \cap C) = (A \cup C) \cap B.$$

Нехай $A \subset B$. Доведемо, що $A \cup (B \cap C) \subset (A \cup C) \cap B$.

$$(x \in A \cup (B \cap C)) \Rightarrow (x \in A) \vee ((x \in B) \wedge (x \in C)) \Rightarrow$$

$$\Rightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) \Rightarrow$$

$$\Rightarrow ((x \in A) \vee (x \in C)) \wedge (x \in B) \Rightarrow x \in (A \cup C) \cap B.$$

Доведемо, що $A \cup (B \cap C) \supset (A \cup C) \cap B$.

$$(x \in (A \cup C) \cap B \Rightarrow ((x \in A) \vee (x \in C)) \wedge (x \in B) \Rightarrow$$

$$\Rightarrow ((x \in A) \wedge (x \in B)) \vee ((x \in C) \wedge (x \in B)) \Rightarrow$$

$$\Rightarrow (x \in A) \vee ((x \in B) \wedge (x \in C)) \Rightarrow x \in A \cup (B \cap C).$$

Аксіоматичне доведення

Аксіоматичне доведення передбачає застосування чотирьох пар основних законів (комутативності, дистрибутивності, нейтральності та доповненості), без урахування змісту операцій над множинами.

Приклад 6. Доведемо закон склеювання: $(A \cap B) \cup (A \cap \overline{B}) = A.$

$$(A \cap B) \cup (A \cap \overline{B}) = A \cap (B \cup \overline{B}) = A \cap U = A.$$

Приклад 7. Доведемо еквівалентність: $A \cup B = B \Leftrightarrow A \cap B = A.$

1. Нехай $A \cup B = B$. Тоді $(A \cup B) \cap A = B \cap A$, та $A = B \cap A.$

2. Нехай $A \cap B = A$. Тоді $(A \cap B) \cup B = A \cup B$, та $B = A \cap B.$

Скінченні множини. Потужність скінченної множини

Скінченна множина – множина, що містить скінченну кількість елементів.

Визначення. *Потужність скінченної множини* A визначається як кількість елементів, що належать множині A.

Потужність скінченної множини A позначатимемо як $n(A)$ або $card(A)$.

Приклад. $n(\{1,2,18\})=3,\ \ n(\varnothing)=0,\ \ n(\{\varnothing\})=1.$

Теорема 1. Нехай A,B – скінченні множини, що не перерізаються, тобто $A\cap B=\varnothing$. Тоді $n(A\cup B)=n(A)+n(B)$.

Методом математичної індукції результат даної теореми узагальнюється на довільну скінченну кількість множин, що попарно не перерізаються.

Наслідок. Нехай A_k $(k=1,2,\ldots,n)$ – скінченні множини, що попарно не перерізаються. Тоді $n(A_1\cup A_2\cup\ldots\cup A_n)=\sum_{k=1}^{n}n(A_k)$.

Теорема 2. Нехай A та B – довільні скінченні множини. Тоді $n(A\cup B)=n(A)+n(B)-n(A\cap B)$.

Декартів добуток множин

Визначення. *Декартовим добутком* довільних множин A та B називають множину $A\times B$, що складається з упорядкованих пар вигляду (a,b), де $a\in A$, $b\in B$:

$$A\times B=\{(a,b):a\in A,b\in B\}.$$

Для випадку $A=B$ (“декартів квадрат”) часто використовують позначення $A\times A=A^{\times 2}=A^2$.

Приклад 8. Нехай $A=\{1,2,3\},\ \ B=\{a,b\}$. Тоді

$$A\times B=\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}.$$

Зауваження. Декартів добуток некомутативний.

$$B\times A=\{(a,1),(b,1),(a,2),(b,2),(a,3),(b,3)\}\neq A\times B.$$

Оскільки елементи множин A та B в декартовому добутку $A\times B$ можуть бути різної природи, доцільно вводити різні універсальні множини для першої і другої компонент декартового добутку: $A\subset U_1$, $B\subset U_2$. Універсальною множиною для декартового добутку в цьому разі вважатимемо $U=U_1\times U_2$.

Теорема 3. Нехай A та B – скінченні множини. Тоді

$$n(A\times B)=n(A)\cdot n(B).$$

Доведення. Нехай $A=\{a_1,a_2,\ldots,a_n\},\ \ B=\{b_1,b_2,\ldots,b_m\}$. Для доведення достатньо розмістити елементи множини $A\times B$ у вигляді таблиці, рядки якої відповідають елементам множини A, стовпці – елементам множини B:

	b_1	b_2	…	b_m
a_1	(a_1,b_1)	(a_1,b_2)	…	(a_1,b_m)
a_2	(a_2,b_1)	(a_2,b_2)	…	(a_2,b_m)
…	…	…	…	…
a_n	(a_n,b_1)	(a_n,b_2)	…	(a_n,b_m)

Очевидно, що таблиця містить $n \cdot m$ елементів, що доводить теорему.■

Означення декартового добутку узагальнюється на випадок довільної скінченної кількості множин.

Визначення. *Декартовим добутком* множин $A_1, A_2, ..., A_n$ називають множину $A_1 \times A_2 \times ... \times A_n$, що складається з упорядкованих n-ок вигляду $(a_1, a_2, ..., a_n)$, де $a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n$:

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) : a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}.$$

Для випадку $A_1 = A_2 = ... = A_n = A$ ("декартів степінь") часто використовують позначення $A^{\times n} = A^n$.

Доведення тотожностей, що містять декартів добуток

Для доведення тотожностей, що містять декартів добуток, зручно використовувати модельний метод.

Приклад 9. Доведемо тотожність $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

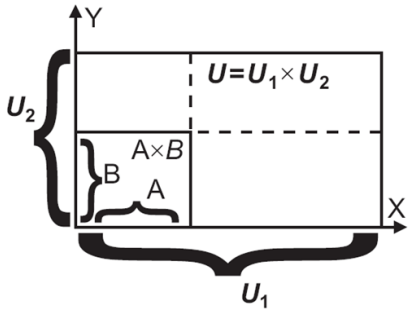
$(x, y) \in A \times (B \cup C) \Leftrightarrow (x \in A) \wedge (y \in (B \cup C) \Leftrightarrow (x \in A) \wedge ((y \in B) \vee (y \in C))$.

$(x, y) \in (A \times B) \cup (A \times C) \Leftrightarrow ((x, y) \in (A \times B)) \vee ((x, y) \in (A \times C)) \Leftrightarrow$

$\Leftrightarrow ((x \in A) \wedge (y \in B)) \vee ((x \in A) \wedge (y \in C)) \Leftrightarrow (x \in A) \wedge ((y \in B) \vee (y \in C))$.

Приклад 10. Зобразимо на діаграмі Венна множину $(A \times B)^C$.

Пригадаємо, що $(A \times B)^C = U \setminus (A \times B)$, де $U = U_1 \times U_2$.



З наведеного рисунку легко "вгадується" тотожність $(A \times B)^C = (U_1 \times B^C) \cup (A^C \times U_2)$, однак ця тотожність потребує акуратного доведення.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Для кожної із вказаних множин знайти потужність множини:

- Задати різними способами множину натуральних чисел, кратних 3 і не перевищуючих 35.
- Задати різними способами множину обласних центрів України.
- Задати різними способами множину днів тижня.
- Перелічіть елементи множини $\{x \mid x - \textit{ціле число, і } 3x < 100\}$.
- Перелічіть елементи множини

$$\{x \mid x - \textit{додатне непарне ціле число, і } x < 35\}.$$

- Перелічіть елементи множини

$$\{x \mid x - \textit{улюблені свята вашої родини}\}.$$

- Опишіть множину {4, 8, 12, 16, 20, 24, 28, 32, 36, 40} за допомогою характеристичної властивості.
- Опишіть множину {березень, квітень, травень} за допомогою характеристичної властивості.
- Опишіть множину {1, 5, 25, 125, 625, 3125} за допомогою характеристичної властивості.
- Опишіть множину {1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37} за допомогою характеристичної властивості.

2. Задані множини:

- $A=\{0,3,5,\{6,9\}\},\ B=\{2,3,9\},\ C=\{0,2,3,6\}.$

Визначити наступні множини: $B\setminus C,\ A\cap B,\ A\cup C,\ (A\cup B)\setminus C.$

- $A=\{1,4,8\},\ B=\{1,3,5\},\ C=\{0,\{3,4\},\{5,6\},8\}.$

Визначити наступні множини: $A\setminus B,\ A\cup C,\ A\cup B,\ (A\cap B)\cup(B\setminus C).$

- $A=\{2,3,\{8,9\}\},\ B=\{0,\{1,2\},3,5\},\ C=\{2,5,8\}.$

Визначити наступні множини: $A\cup B,\ C\setminus B,\ A\cup C,\ B\cup(A\cap C).$

- $A=\{1,2,3,4,5,6\}, B=\{1,3,5,7,9\}, C=\{2,4,6,8,10\}, U=\{1,2,3,4,5,6,7,8,9,10\}$

Визначити наступні множини: $A\cap B,\ B\times C,\ A\setminus C,\ A\cup(B\cap C).$

- $A=\{1,2,7,8,9\}, B=\{1,2,3,5,7\}, C=\{2,4,6,8,10\}, U=\{1,2,3,4,5,6,7,8,9,10\}.$В

изначити наступні множини: $A\cap C,\ B\setminus C,\ A\cup C,\ A\cap(B\cup C).$

- $A=[0,6),\ B=[1,7),\ C=[2,8].$

Визначити наступні множини: $C\setminus B,\ A\cup C,\ B\cap C,\ A\cap B.$

- $A=(3,7),\ B=(1,5],\ C=[4,8].$

Визначити наступні множини: $A\setminus B,\ B\cup C,\ A\cup B,\ A\cap(B\cup C).$

- $A=(5,8),\ B=[2,6),\ C=(4,7].$

Визначити наступні множини: $A\cap C,\ A\setminus B,\ B\cup C,\ (A\cap B)\setminus C.$

- $A=(3,8),\ B=[0,9),\ C=(2,5].$

Визначити наступні множини: $A\cap B,\ A\cup C,\ A\cup(B\cap C),\ A\cap C.$

- $A=[0,9),\ B=[2,5),\ C=[1,11].$

Визначити наступні множини: $B\cup C,\ A\setminus C,\ A\cup B,\ (A\cup B)\setminus C.$

3. Для кожної з наведених нижче множин використайте діаграми Венна і заштрихуйте ті її частини, які зображують задані множини:

- $A\cap B;$
- $A\cup B;$
- $A\setminus B;$
- $(A\cup B)\setminus(A\cap B);$
- $B\setminus(A\cap B);$
- $A\cap B\cap C;$
- $A\setminus(B\cap C);$
- $(A\cap B)\cup C;$

- $(A \cup B \cup C) \setminus (A \cap B \cap C)$;
- $(A \cap B) \cup (A \cap C) \cup (B \cap C)$.

12.2 Практична робота №2

Тема: Подільність цілих чисел. Ділення з остачею. Найбільший спільний дільник двох чисел. Найменше спільне кратне двох чисел.

Мета: Розглянути подільність цілих чисел націло та з остачею, пригадати найбільший спільний дільник та найменше спільне кратне двох чисел, ознайомитися з алгоритмом Евкліда пошуку НСД.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Числа, що вживаються при рахунку, утворюють ***множину натуральних чисел N***. У множині N визначені операції додавання "+" і множення "×", але зворотні операції віднімання "–" і ділення "/" не завжди здійсненні. Для того щоб виконувалася операція віднімання, в математиці вводять число нуль і цілі від'ємні числа.

Отже, натуральні числа, нуль і цілі від'ємні числа утворюють ***множину цілих чисел Z.*** У множині Z визначені операції додавання "+", множення "×" і здійсненна операція віднімання "–".

Операції "+" і "×" *комутативні*, *асоціативні* та пов'язані *дистрибутивним* законом.

Для будь-яких чисел $a, b, c \in Z$ справедливі твердження:

1 Комутативність $a + b = b + a, \quad a \times b = b \times a$.

2 Асоціативність $(a + b) + c = a + (b + c), \quad (a \times b) \times c = a \times (b \times c)$.

3 Дистрибутивність $(a + b) \times c = a \times c + b \times c$.

Таким чином, множина Z – *комутативне кільце*, яке називають ***кільцем цілих чисел***.

Подільність цілих чисел

Розглянемо питання про подільність чисел у множині ***Z***.

Визначення. Якщо для чисел $a, b \in Z$ у кільці цілих чисел Z існує таке число q, що $a = b \times q$, то говорять, що ***a* ділиться на *b*** або ***b* ділить *a***. Для позначення того факту, що b ділить a, записують $b \mid a$ або $b \vdots a$.

Якщо для чисел $a, b, q \in Z$ виконується рівність $a = b \times q$, то число a називають **кратним** чисел b та q, а самі числа b і q – **дільниками** числа a, тобто $a \vdots b$ та $a \vdots q$.

Розглянемо деякі властивості подільності цілих чисел, що випливають із визначення цілих чисел.

1 Якщо $\forall a \in Z$, то $0 \vdots a$.

2 Для $\forall a \in Z$ якщо $1 \vdots a$, то $a=\pm 1$.

3 Для $\forall a,b \in Z$ якщо $a \vdots b$, то $a \vdots (-b), (-a) \vdots b$ та $(-a) \vdots (-b)$.

4 Для $\forall a,b \in Z$ якщо $a \vdots b$ і $b \vdots a$, то $a=\pm$b.

5 Для $\forall a,b,c \in Z$ якщо $a \vdots b$ й $b \vdots c$, то $a \vdots c$.

6 Для $\forall a,b,c \in Z$ якщо $c \vdots a$ й $c \vdots b$, то $c \vdots (a+b)$.

7 Для $\forall a,b,c \in Z$ якщо $a \vdots b$, то $(a \times c) \vdots b$.

Ділення з остачею

Важливу роль у теорії подільності відіграє *теорема про ділення з остачею*.

Теорема 1. Якщо $a,b \in Z$ та $b > 0$, то завжди можна підібрати таку пару цілих чисел q та r, при яких виконується рівність $a = b \times q + r$, де $0 \le r < b$. При цьому числа q та r визначаються однозначно.

За даною теоремою можна стверджувати, що ціле число a тоді і тільки тоді кратне цілому числу $b \ne 0$, коли остача r від ділення a на b дорівнює нулю.

Найбільший спільний дільник двох чисел

Визначення. Ціле число δ називається ***спільним дільником*** цілих чисел $a_1, a_2, \ldots, a_n$, якщо кожне із цих чисел ділиться на δ.

Наприклад, для чисел 12, 18, 21, 36 спільний дільник $\delta = 3$.

Визначення. Ціле число d називається ***найбільшим спільним дільником*** (НСД) чисел $a_1, a_2, \ldots, a_n$, якщо d – спільний дільник чисел $a_1, a_2, \ldots, a_n$, що ділиться на будь-який спільний дільник цих чисел.

Наприклад, для чисел 12, 18, 36 спільними дільниками будуть числа 2, 3, 6, а НСД d=6.

Теорема 2. НСД чисел $a_1, a_2, \ldots, a_n$ визначається однозначно з точністю до знака. Інакше, якщо d_1 та d_2 найбільші спільні дільники чисел $a_1, a_2, \ldots, a_n$, то $d_1 = \pm d_2$.

Алгоритм Евкліда. Досить простою процедурою пошуку НСД є алгоритм Евкліда.

Нехай дані два числа $a,b \in Z$, причому $0 < b < a$. Необхідно визначити НСД. Для цього ділять a на b. Якщо $b \vdots a$, то найбільшим спільним дільником є число b. Якщо a не ділиться на b націло, то одержують частку q_0 та залишок r_1, причому $0 \le r_1 < b$. Далі ділять b на r_1, одержують частку q_1 і залишок r_2, причому $0 \le r_2 < r_1$Далі аналогічно ділять r_1 на r_2, при цьому одержують частку q_2 і залишок r_3, причому $0 \le r_3 < r_2$. І так далі. Цей процес закінчується в тому випадку, коли залишок від ділення буде дорівнювати нулю, тобто процес ділення є кінцевим, оскільки залишки $r_1, r_2, r_3, \ldots$, будучи натуральними числами, зменшуються. Останній залишок, що не дорівнює нулю, є найбільшим спільним дільником чисел a та b.

Алгоритм Евкліда можна сформулювати у вигляді теореми.

Теорема 3. Якщо

$$\begin{cases} a = b \times q_0 + r_1, & 0 \le r_1 < b \\ b = r_1 \times q_1 + r_2, & 0 \le r_2 < r_1 \\ r_1 = r_2 \times q_2 + r_3, & 0 \le r_3 < r_2 \\ \quad \dots \\ r_{n-2} = r_{n-1} \times q_{n-1} + r_n, & 0 \le r_n < r_{n-1} \\ r_{n-1} = r_n \times q_n \end{cases},$$

то $\text{НСД}(a,b) = r_n$.

Наприклад, щоб знайти НСД(2585, 7975) виконаємо такі дії:

7975=2585×3+220, $r_1 = 220$,

2585=220×11+165, $r_2 = 165$,

220=165×1+55, $r_3 = 55$,

165=55×3.

Відповідно до теореми НСД(2585, 7975)=55.

В алгоритмі Евкліда розгляд можна обмежитися тільки додатними числами, тому що НСД(a, b)=НСД(|a|, |b|). Програма знаходження НСД (a, b) згідно алгоритму Евкліда наведена нижче.

```
procedure Euclid (a,b: integer; var nsd);
var r:integer;
begin
 a:=abs(a);
 b:=abs(b);
 r:=a mod b;
 if r=0
   then
        nsd:=b;
   else
      while r<>0 do
        begin
        a:=b;
        b:=r;
        nsd:=r;
        r:=a mod b;
    end;
end;
```

Для знаходження НСД декількох чисел $a_1, a_2, \dots, a_n$ спочатку знаходять

$$d_1 = НСД(a_1, a_2),$$

потім

$$d_2 = НСД(d_1, a_3),$$

…,

$d_{n-1} = НСД(d_{n-2}, a_n)$.

У результаті одержимо $НСД(a_1, a_2, \ldots, a_n) = d_{n-1}$.

Теорема 4. Якщо $d = НСД(a,b)$, то існують такі числа $x, y \in Z$, що $a \times x + b \times y = d$.

Дану рівність називають *лінійним поданням* найбільшого спільного дільника чисел *a* та *b*.

Найменше спільне кратне двох чисел

Визначення. Дані числа $a_1, a_2, \ldots, a_m$. Кожне з чисел, що є кратним кожному з даних чисел, має назву їхнього спільного кратного (СК). Найменше з усіх кратних називається найменшим спільним кратним (НСК) заданих чисел.

Нехай $(a,b) = d$, тоді $a = a_1 d,\ b = b_1 d$ і $(a_1, b_1) = 1$ (властивості НСД). Нехай M – деяке кратне a та b, тобто $M = ka$ і $\frac{M}{b} = \frac{ka}{b} = \frac{ka_1 d}{b_1 d} = \frac{ka_1}{b_1} \in Z$. Оскільки $(a_1, b_1) = 1$, то k повинно ділитися на b_1, тобто $k = b_1 t$. Для СК буде правильною формула

$$M = ka = ak = ab_1 t = \frac{ab_1 d}{d} t = \frac{ab}{d} t.$$

Найменше значення СК буде за умови, що $t = 1$, тобто для НСК виконується формула $m = \frac{ab}{(a,b)}$, тоді $M = m \cdot t$.

Теорема 5. Сукупність спільних кратних чисел a та b дорівнює сукупності кратних для їхнього НСК.

Теорема 6. НСК a та b дорівнює відношенню добутку цих чисел до їхнього НСД.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Реалізація алгоритму Евкліда для визначення НСД (a, b) на мові С.
2. Узагальнення знаходження НСД для масиву, який складається з *m* чисел.
3. $(a,b) = 31,\ [a,b] = 238$. Чому дорівнює ab?
4. $ab = 33960,\ [a,b] = 968$. Чому дорівнює (a,b)?
5. Використовуючи алгоритм Евкліда, знайти НСД та НСК чисел 25245 та 129591.

12.3 Практична робота №3

Тема: Взаємно прості числа. Прості та складені числа. Канонічний розклад числа.

Мета: Дати визначення взаємно простим, простим та складеним числам, розглянути різні формули встановлення загального члена послідовності простих чисел, розглянути канонічний розклад числа та його використання при розв'язуванні задач.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Взаємно прості числа

Визначення. Якщо $\text{НСД}(a,b)=1$, то такі числа називаються ***взаємно простими числами***.

Наприклад, числа 21 і 25 є взаємно простими числами, оскільки НСД(21, 25)=1.

Визначення. Якщо $\text{НСД}(a_1, a_2,\ldots,a_n)=1$, то такі числа називаються ***попарно взаємно простими*** числами або ***взаємно простими***.

Властивості взаємно простих чисел.

Для $\forall a, b, c\in Z$:

1 Якщо два числа a та b взаємно прості і $a_1 \vdots a$ та $b_1 \vdots b$, то числа a_1 та b_1 – взаємно прості.

2 Якщо два числа a та b взаємно прості і $a \neq b$, то при будь-яких цілих додатних значеннях n і m числа a^n і b^m будуть взаємно простими.

3 Частки від ділення чисел a та b на їх найбільший спільний дільник d – взаємно прості

$$\text{НСД}\left(\frac{a}{d}, \frac{b}{d}\right)=1.$$

4 Якщо $c \vdots a\times b$ і $\text{НСД}(a,c)=1$, то $c \vdots b$.

5 Якщо НСД(a, b)=1, то число $(a\times b)\vdots c$ тоді й тільки тоді, коли $a\vdots c$ і $b\vdots c$.

6 Якщо НСД(a, c)=1 і НСД(b, c)=1, то НСД($a\times b$, c)=1.

Прості та складені числа

Розглянемо цілі додатні числа.

Число 1 має тільки один дільник, а саме 1. Кожне натуральне число n, відмінне від 1, має принаймні два дільники – 1 і саме число n.

Визначення. Відмінне від одиниці натуральне число n називається ***простим***, якщо $n>1$ і його дільниками є 1 і саме число n. Число n називається ***складеним***, якщо воно має дільники, відмінні від 1 і самого числа n.

Таким чином, якщо n – складене число, то у n є такий цілий дільник a, що $n=ab, 1<b<n, b=\frac{n}{a}$.

Слід зазначити, що число 1 не належить ні до простих, ні до складених чисел.

Якщо прості числа виписувати в ланцюжок за зростанням, то його початок буде такий: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,… . Очевидно, що усі парні числа, крім 2, – складені.

За означенням множину натуральних чисел можна розбити на три підмножини: 1) прості числа, 2) складені числа, 3) число 1, яке не відносять ні до простих, ані до складених.

Розглянемо деякі ***властивості простих і складених чисел***:

1 Будь-яке натуральне число або ділиться на дане просте число, або взаємно просте з ним.

2 Для будь-якого цілого числа $n>1$ найменший, відмінний від одиниці додатний дільник, – це завжди просте число, бо у противному разі можна було б вибрати ще менший дільник.

3 Якщо добуток декількох натуральних чисел ділиться на просте число *p*, то принаймні один із співмножників ділиться на це просте число *p*.

4 Найбільший простий дільник, відмінний від 1, будь-якого складеного числа *a* не більший ніж $\sqrt{a}$. Дійсно, за умови, що *q* – найбільший дільник числа *a*, маємо $a=qb$ і $b\geq q$, звідси $a\geq q^2$ або $q\leq\sqrt{a}$.

5 Простих чисел безліч. Це обумовлено тим, що для будь-яких різних простих чисел $p_1, p_2,...,p_k$ можна побудувати нове просте число, наприклад, таким буде простий дільник суми $p_1 p\cdot...\cdot p_k+1$, який розділивши всю суму, не може збігатися з жодним із простих чисел $p_1, p_2,...,p_k$.

Багато відомих математиків намагалися встановити формулу загального члена послідовності простих чисел. *Поліноміальні формули*, за якими для окремих цілих значень змінної можна побудувати ланцюжок простих чисел. Це, зокрема, формули:

- Ейлера n^2+n+17 при $0\leq n\leq 15$, n^2+n+41 при $0\leq n\leq 39$;
- Лежандра $2n^2+29$ при $0\leq n\leq 28$;
- Ескотта $n^2-79n+1601$ при $0\leq n\leq 79$.

Проте доведено, що не існує многочлена від однієї змінної, значення якого були б простими числами при всіх цілих значеннях змінної.

Велику історичну цінність являють собою дві *експоненціальні формули* для побудови можливих простих чисел

$$M_n=2^n-1 \qquad (3.1)$$

$$F_n=2^{2^n}+1, \qquad (3.2)$$

Де $n\in N$. Отримані за формулою (3.1) числа називаються **числами Марсенна**, а за формулою (3.2) – **числами Ферма**.

Чи буде число Марсенна 2^n-1 простим або складеним, залежить від значення показника n , а саме:

1. Якщо n – парне і $n \geq 4$, числа $2^n - 1$ завжди складені, бо тоді $2^n - 1 = (2^{n/2} - 1)(2^{n/2} + 1)$;

2. Коли n – непарне і складене, – числа $2^n - 1$ також складені. Дійсно при $n = ab,\ 3 \leq a < n,\ 3 \leq b < n$ маємо $2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)$;

3. Якщо $n = p$ просте, то число може виявитися і простим і складеним. Так, при $p = 2; 3; 5; 7; 13; 17; 19$ отримаємо відповідно прості числа Марсенна 3, 7, 31, 127, 8191, 131071, 524287, а при $p = 11; 23; 29; 67; 257$ числа Марсенна – складені.

Для аналізу простоти чисел Марсенна нині існує ефективний тест Люка-Лемера, за допомогою якого у 1998 році було доведено, що число Марсенна $M_n = 2^n - 1$ при $n = 3021377$ просте і містить 909526 десяткових знаків.

Серед чисел Ферма $F_n = 2^{2^n} + 1$ не відомо жодного простого, крім обчислених при $n = 0; 1; 2; 3; 4$. У 1739 році Ейлер довів, що число Ферма $F_n = 2^{2^5} + 1 = 4294967297$ складене та позначив загальний шлях для розкладання на множники чисел Ферма: усі дільники числа Ферма мають бути вигляду $m2^n + 1$.

Визначення. ***Прайморіалом*** $p^{\#}$ ***простого числа*** $p > 0$ називається добуток усіх простих чисел, менших або рівних p. Так, $2^{\#} = 2$, $5^{\#} = 2 \cdot 3 \cdot 5 = 30$. Звісно за умови, що q – наступне після p просте число, $q^{\#} = p^{\#} \cdot q$. Якщо розглянути числа вигляду $p^{\#} + 1$, то виявимо

$$2^{\#} + 1 = 3 \text{ – просте}$$
$$3^{\#} + 1 = 6 + 1 = 7 \text{ – просте}$$
$$5^{\#} + 1 = 30 + 1 = 31 \text{ – просте}$$
$$7^{\#} + 1 = 210 + 1 = 211 \text{ – просте}$$
$$11^{\#} + 1 = 2310 + 1 = 2311 \text{ – просте}$$
$$13^{\#} + 1 = 30030 + 1 = 30031 = 59 \cdot 509 \text{ – складене}$$

Хоча числа $p^{\#} + 1$ не завжди прості, проте вони не мають дільників, менших або рівних p. Поки знайдено тільки 16 простих чисел за <u>прайморіальною формулою</u> $p^{\#} + 1$, найбільше з яких відповідає $p = 24027$ та складається з 10387 десяткових знаків.

Решето Ератосфена – найпростіша процедура отримання послідовності простих чисел. Мета решета – визначити всі додатні прості числа, менші за деяку верхню цілу межу $n > 0$.

Розглянемо суть методу. Випишемо всі натуральні числа від 2 до n. Перше просте число цього ряду – 2. Отже, викреслюємо з ряду (як складені) всі числа, кратні 2, крім його самого:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13,…,*n*.

Тепер перше невикреслене число після двійки буде 3, і воно – просте. З ним, як і з числом 2, виконаємо аналогічну процедуру, тобто викреслимо за числом 3 всі числа, кратні 3:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13,…,*n*.

Якщо цими діями викреслені всі числа, кратні простим числам, меншим за $\sqrt{n}$, то всі числа будуть простими.

Приклад 1. Виписати за допомогою решета Ератосфена прості числа, менші за 100.

Розв'язання:

$n=100,\ \sqrt{n}=10$. Отже. У вихідній таблиці натуральних чисел від 2 до 100, з якої вже викреслені всі парні числа, крім 2, потрібно викреслити всі числа, кратні 3 (кожне третє число після 3), кратні 5 (кожне п'яте число після 5), кратні 7 (кожне сьоме число після 7) і на цьому зупинитися. Усі 25 чисел, що залишилися – прості.

Канонічний розклад числа

Основна теорема арифметики. Кожне відмінне від 1 натуральне число єдиним способом розкладається на прості множники.

Може виявитися, що в розкладанні числа $a \in N$ на прості множники будуть однакові числа, тому, якщо скористатися поняттям степеня, то число a можна записати так:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}, \qquad (3)$$

де $p_1 < p_2 < \ldots < p_n$ – прості числа, і кожне $\alpha_i > 0 (i = 1,2,\ldots,n)$ – натуральні числа, що називаються ***кратностями простих множників***.

Рівність (3) називається ***канонічною формою розкладання натурального числа a***.

Наслідки:

- Число $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ ділиться на число b тоді і тільки тоді, коли $b = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$, де $0 \le k_i \le \alpha_i (i = 1,2,\ldots,n)$.
- Число $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ тоді і тільки тоді буде точним l-тим степенем деякого цілого числа, коли всі показники $p_1, p_2, \ldots, p_n$ будуть подільними на число l.
- Кількість усіх дільників числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ можна обчислити за формулою

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_n + 1).$$

- Сума $S(a)$ усіх дільників вказаного числа дорівнює

$$S(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_n^{\alpha_n+1} - 1}{p_n - 1}.$$

Функції $\tau(a)$ та $S(a)$ визначені тільки для цілих додатних значень a (такі функції називають ***арифметичними***).

Приклад 2. Знайти кількість та суму всіх дільників числа 60.

Розв'язання:

Канонічне розкладання числа $60 = 2^2 \cdot 3 \cdot 5$. Отже,

$$\tau(60) = (2+1)(1+1)(1+1) = 12;$$

$$S(60)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=168.$$

Зауваження. Нехай $a=p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_n^{k_n}$, $b=p_1^{m_1}\cdot p_2^{m_2}\cdot\ldots\cdot p_n^{m_n}$ – відповідно канонічні розкладання на множники чисел a і b, причому деякі показники k_i і m_i $(i=\overline{1,n})$ можуть дорівнювати нулю. Тоді найбільший спільний дільник чисел a і b визначається за формулою:

$$\text{НСД}(a,b)=p_1^{t_1}\cdot p_2^{t_2}\cdot\ldots\cdot p_n^{t_n},\ \text{де}\ t_i=\min\{k_i;m_i\},\ i=\overline{1,n},$$

а найменше спільне кратне цих чисел дорівнюватиме

$$\text{НСК}(a,b)=p_1^{s_1}\cdot p_2^{s_2}\cdot\ldots\cdot p_n^{s_n},\ \text{де}\ s_i=\max\{k_i;m_i\},\ i=\overline{1,n}.$$

Приклад 3. Обчислити НСД та НСК чисел $a=1400$ і $b=294$.

Розв'язання:

Запишемо канонічні розкладання чисел:

$$a=1400=2^3\cdot3^0\cdot5^2\cdot7;\quad b=294=2\cdot3\cdot5^0\cdot7^2.$$

Тоді $\text{НСД}(a,b)=2\cdot3^0\cdot5^0\cdot7=14$; $\text{НСК}(a,b)=2^3\cdot3\cdot5^2\cdot7^2=29400$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Побудувати канонічну форму чисел 12348 та 867, знайти їх НСД та НСК.
2. Розглянути ознаки подільності чисел.
3. Перевірити, чи ділиться число b на 29, якщо відомо, що $116=87+29k-b$, $\forall k\in Z$.
4. Для числа $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}$ обчислити кількість дільників $\tau(a)$ та суму дільників $S(a)$.

a. $a=2^6\cdot3^4\cdot5^3\cdot41$;

b. $a=2^7\cdot3^2\cdot7^2\cdot97$;

c. $a=2^9\cdot3^4\cdot11^2\cdot41$;

d. $a=3^7\cdot7^3\cdot17\cdot19$.

12.4 Практична робота №4

Тема: Порівняння цілих чисел та їхні основні властивості.

Мета: Дати визначення порівнянним за модулем числа, розглянути основні властивості порівнянь та застосування даних властивостей при розв'язуванні прикладів.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Порівняння цілих чисел та їхні основні властивості

Нехай $m>1$ – ціле додатне число, яке назвемо ***модулем***.

Визначення. Два числа $a,b\in Z$ називаються ***порівнянними за модулем m*** ($m\in N;\ m\neq 1$), якщо їх різниця $a-b$ ділиться без остачі на число m, тобто $m\vdots(a-b)$. Таке співвідношення між числами a і b називають ***порівнянням (конгруенцією)*** чисел та записують так:

$a\equiv b \bmod m$.

У запису $a\equiv b \bmod m$ число b називається ***лишком числа a за модулем m***. Запис $a \bmod m$ (без дужок) означає лишок числа a, рівний деякому цілому числу від 0 до $m-1$. Операція $a \bmod m$ називається ***зведенням числа a за модулем m.***

Інколи порівняння скорочено записують як $a\equiv b(m)$, $a\overset{m}{\equiv}b$, а коли зрозуміло, за яким модулем записано порівняння, то $a\equiv b$. Порівняння $a\equiv 0(\bmod m)$ означає, що число a ділиться на m.

Наприклад, $77\equiv 5(\bmod 8);\ 102\equiv 0(\bmod 3)$.

Теорема 1.

Два числа $a,b\in Z$ порівнянні за модулем m тоді і тільки тоді, коли вони при діленні на m мають однакові залишки.

Доведення. Припустимо, що залишки від ділення a та b на m рівні r ($0\le r<m$). Покажемо, що $a\equiv b \bmod m$. Розділимо a на m та b на m з остачею. Одержимо

$a=m\times q_1+r,$

$b=m\times q_2+r.$

Віднімемо почленно з першої рівності другу, одержимо:

$a-b=(m\times q_1+r)-(m\times q_2+r)=m\times(q_1-q_2)$, де $(q_1-q_2)\in Z$.

Звідси випливає, що $m\vdots(a-b)$. А значить $a\equiv b \bmod m$.

Обернено. Нехай $a\equiv b \bmod m$. Покажемо, що числа a і b при діленні на m мають ту саму остачу.

З того, що $a\equiv b \bmod m$, випливає $m\vdots(a-b)$. За визначенням подільності

$$a-b=m\times t, \qquad (4.1)$$

де $t\in Z$.

Розділимо число b на m, одержимо

$$b = m \times q + r,\ (0 \le r < m) \qquad (4.2)$$

Підставимо рівність (4.2) у рівність (4.1). Одержимо
$a - (m \times q + r) = m \times t \Rightarrow a = m \times (t + q) + r$.

Таким чином, видно, що число *a* при діленні на *m* має той самий залишок, що і число *b*. Теорема доведена.■

Відзначимо найбільш часто використовувані факти.

Якщо $m \vdots a$, то $m \vdots (a - 0)$, а це значить, що $a \equiv 0 (\mathrm{mod} m)$, тобто будь-яке число, кратне *m*, порівняно з нулем за модулем *m*.

Якщо $a = m \times q + r$, де $0 \le r < m$, то $a \equiv r \bmod m$. Таким чином, $\forall a \in Z$ завжди порівнянно із залишком *r*, що отриманий при діленні *a* на *m*.

Часто залишок *r* називають ***відрахуванням***.

Розглянемо деякі властивості порівнянь.

Властивості порівнянь, що не залежать від модуля *m*.

1) Відношення $a \equiv b (\mathrm{mod} m)$ є відношенням еквівалентності, тобто задовольняє вимоги:
   - рефлексивності: $a \equiv a (\mathrm{mod} m)$;
   - симетричності: $a \equiv b (\mathrm{mod} m) \Rightarrow b \equiv a (\mathrm{mod} m)$;
   - транзитивності: $\left[(a \equiv b (\mathrm{mod} m)) \wedge (b \equiv c (\mathrm{mod} m))\right] \Rightarrow a \equiv c (\mathrm{mod} m)$.

2) Якщо $a \equiv b (\mathrm{mod} m)$ та $c \equiv d (\mathrm{mod} m)$, то
$a + c \equiv b + d (\mathrm{mod} m)$,
$a - c \equiv b - d (\mathrm{mod} m)$,
$ac \equiv bd (\mathrm{mod} m)$.

Тобто порівняння за тим самим модулем можна почленно складати, віднімати та множити.

3) Якщо $a \equiv b (\mathrm{mod} m)$ і k – довільне ціле число, то
$a + k \equiv b + k (\mathrm{mod} m)$,
$ak \equiv bk (\mathrm{mod} m)$.

4) Якщо $ka \equiv kb (\mathrm{mod} m)$ і числа k і m – взаємно прості, то
$a \equiv b (\mathrm{mod} m)$.

5) Будь-який доданок лівої та правої частини порівняння можна переносити з протилежним знаком в іншу частину, тобто,
якщо $a \equiv b + c (\mathrm{mod} m)$, то $a - c \equiv b (\mathrm{mod} m)$ або $a - b \equiv c (\mathrm{mod} m)$,
якщо $a + b \equiv c (\mathrm{mod} m)$, то $a \equiv c - b (\mathrm{mod} m)$ або $b \equiv c - a (\mathrm{mod} m)$.

Властивості порівнянь, що залежать від модуля *m*.

6) Якщо $a \equiv b (\mathrm{mod} m)$ і k – довільне натуральне число, то
$ka \equiv kb (\mathrm{mod} km)$

7) Якщо $ka \equiv kb (\mathrm{mod} km)$, де числа k і m – довільні натуральні числа, то
$a \equiv b (\mathrm{mod} m)$

8) Якщо $a \equiv b(\mathrm{mod}\, m)$ і k – довільне ціле число, то $a + km \equiv b(\mathrm{mod}\, m)$ або $a \equiv b + km(\mathrm{mod}\, m)$.

9) Обидві частини порівняння $a \equiv b(\mathrm{mod}\, m)$ можна розділити на їх спільний дільник *d*, якщо НСД$(d, m) = 1$.

10) Якщо $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$ для будь-якого цілого $n \geq 0$.

11) Якщо $a \equiv b(\mathrm{mod}\, m)$ і $f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x^1 + c_0$ – довільний многочлен із цілими коефіцієнтами, то
$f(a) \equiv f(b)(\mathrm{mod}\, m)$.

12) Якщо $a \equiv b(\mathrm{mod}\, m)$ і число d – дільник модуля m, то $a \equiv b(\mathrm{mod}\, d)$.

13) Якщо $ak \equiv bk(\mathrm{mod}\, m)$ і НСД$(k, m) = d$, то $a \equiv b(\mathrm{mod}\, \frac{m}{d})$.

14) Якщо $a \equiv b(\mathrm{mod}\, m)$, то множина спільних дільників чисел a і m збігається з множиною спільних дільників чисел *b* і m, зокрема НСД(*a*,*m*)=НСД(*b*,*m*).

15) Якщо $a \equiv b(\mathrm{mod}\, m_1)$, $a \equiv b(\mathrm{mod}\, m_2)$ і m – найменше спільне кратне модулів m_1 і m_2, то $a \equiv b(\mathrm{mod}\, m)$.

16) Якщо $a \equiv b(\mathrm{mod}\, m)$, то $a - b = mt$, де $t = 0, \pm 1, \pm 2, \ldots$. Отже, $a = b + mt$, де $t = 0, \pm 1, \pm 2, \ldots$.

“Модулярна арифметика” (обчислення за модулем) досить часто використовується в криптографії, бо, по-перше, її зручно реалізовувати на комп’ютері, а по-друге, завдяки їй скорочується діапазон проміжних значень і результатів, якщо у процесі обчислень замінювати будь-який проміжний результат іншим числом, порівнюваним з ним за модулем. Так, обчислюючи $a^8(\mathrm{mod}\, m)$, не обов’язково виконувати сім множень та одне велике зведення за модулем $a^8(\mathrm{mod}\, m) = a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a(\mathrm{mod}\, m)$.

Метод, що називається адитивним ланцюгом, дає можливість виконати у даному разі лише три множення і стільки ж зведень за модулем, а проміжні результати будуть не такими об’ємними
$a^8(\mathrm{mod}\, m) = ((a^2 \bmod m)^2 \bmod m)^2 \bmod m$.

Приклад 1. Знайти остачу від ділення числа $9^{75} - 95$ на 7.

Розв’язання.

$9 \equiv 2(\mathrm{mod}\, 7)$ і $95 \equiv 4(\mathrm{mod}\, 7) \Rightarrow 9^{75} - 95 \equiv 2^{75} - 4(\mathrm{mod}\, 7)$,

$2^3 = 8 \equiv 1(\mathrm{mod}\, 7) \Rightarrow 2^{75} = (2^3)^{25} = 8^{25} \equiv 1^{25}(\mathrm{mod}\, 7) = 1(\mathrm{mod}\, 7)$,

$9^{75} - 95 \equiv 1 - 4 = -3(\mathrm{mod}\, 7) = -3 + 7(\mathrm{mod}\, 7) = 4(\mathrm{mod}\, 7)$.

Остача від ділення $9^{75} - 95$ на 7 дорівнює 4.

Приклад 2. Перевірити порівняння $8^{30} \equiv 34(\mathrm{mod}\, 55)$.

Розв’язання.

Аналогічне розв’язанню у прикладі 1.

$$8^{30} = (8^2)^{15} = 64^{15} \equiv (64-55)^{15} \bmod 55 = 9^{15} \bmod 55 = (9^3)^5 \bmod 55 = (729)^5 \bmod 55 =$$
$$= (13 \cdot 55 + 14)^5 \bmod 55 \equiv 14^5 \bmod 55 = (14^2)^2 \cdot 14 \bmod 55 = 196^2 \cdot 14 \bmod 55 =$$
$$= (3 \cdot 55 + 31)^2 \cdot 14 \bmod 55 \equiv 31^2 \cdot 14 \bmod 55 = 961 \cdot 14 \bmod 55 = (17 \cdot 55 + 26) \cdot 14 \bmod 55 \equiv$$
$$\equiv 26 \cdot 14 \bmod 55 = 364 \bmod 55 = (6 \cdot 55 + 34) \bmod 55 \equiv 34 \bmod 55$$

Приклад 3. Задані три числа: 78, 210 і 346. Чи можна їх порівняти з числом 27 за модулем 11?

Розв'язання.

Віднімемо з даних чисел 27. Отримаємо числа 51, 183 і 319. Із цих трьох чисел лише 319 ділиться на 11, тому лише число 346 порівнянне з числом 27 по модулю 11, тобто

$346 \equiv 27 (\bmod 11)$.

Приклад 4. Показати, що $3^{121} \not\equiv 11 (\bmod 21)$.

Розв'язання.

Відомо, що, якщо $a \equiv b (\bmod m)$ то $(a, m) = (b, m)$. В даному випадку маємо:

$(3^{121}, 21) = 3$,

але $(11, 21) = 1$, отже, $3^{121} \not\equiv 11 (\bmod 21)$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Записати ряд чисел, ділення яких на число 7 дає залишок 1.
2. Знайдіть залишок від ділення
   a. 12^{2751} на 5;
   b. 11^{1201} на 1000;
   c. 7^{114} на 100;
   d. 17^{2001} на 1000.

12.5 Практична робота №5

Тема: Функція Ейлера. Теорема Ейлера. Теорема Ферма.

Мета: Ознайомитися з функцією Ейлера та її властивостями, розглянути теореми Ейлера та Ферма, розглянути приклади застосування теорем Ейлера та Ферма.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Функція Ейлера

Важливу роль у теорії чисел відіграє функція Ейлера.

Функцією Ейлера $\varphi(n)$ називається функція, що визначає для кожного числа $n \in N$ кількість цілих невід'ємних чисел, менших n і взаємно простих з n.

Приклад 1. Обчислити значення функції Ейлера $\varphi(24)$.

Розв'язання.

Випишемо натуральні числа від 1 до 24 та викреслимо числа, що мають нерівні одиниці спільні дільники з числом 24, тобто числа, що діляться на 2 і 3. Залишені числа 1, 5, 7, 11, 13, 17, 19, 23 утворять зведену систему лишків за модулем 24. Їх кількість 8, а відтак $\varphi(24) = 8$.

Властивості функції Ейлера:

1. Функція $\varphi(n)$ мультиплікативна, тобто для $\forall n \in N$ функція $\varphi(n) \neq 0$ і для будь-яких взаємно простих чисел n, m $(n, m \in N)$ справедлива рівність $\varphi(n \times m) = \varphi(n) \times \varphi(m)$.

2. Якщо p – просте число та $k \in N$, то

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right). \tag{5.1}$$

Звідси, якщо p – просте, то

$$\varphi(p) = p - 1 \tag{5.2}$$

3. Якщо канонічне розкладання числа $n \in N$ на прості множники має вигляд $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_s^{\alpha_s}$, де всі p_i – прості числа, то

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_s^{\alpha_s} \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \ldots \times \left(1 - \frac{1}{p_s}\right) = \\ &= n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \ldots \times \left(1 - \frac{1}{p_s}\right) = n \times \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)\end{aligned} \tag{5.3}$$

Наприклад,

$$\varphi(100) = \varphi(2^2 \times 5^2) = \varphi(2^2) \times \varphi(5^2) =$$

$$= 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40.$$

4. Сума значень функції Ейлера для всіх дільників d_j числа n дорівнює n, тобто

$$\sum_j \varphi(d_j) = n.$$

Приклад 2. Обчислити значення функції Ейлера
а) $\varphi(120)$; б) $\varphi(275)$; в) $\varphi(2452)$; г) $\varphi(729)$.

Розв'язання.

Розкладемо числа на прості множники і обчислимо за формулою (5.3):

а) $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 120 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 32$;

б) $\varphi(275) = \varphi(5^2 \cdot 11) = 275 \cdot \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right) = 200$;

в) $\varphi(2452) = \varphi(2^2 \cdot 613)$.

НСД(4, 613)=1 $\Rightarrow$ числа 4 і 613 взаємно прості. Мультиплікативність функції Ейлера обумовлює $\varphi(2452) = \varphi(2^2 \cdot 613) = \varphi(2^2)\varphi(613)$. Тоді за формулами (5.1) і (5.2) обчислимо

$$\varphi(2^2) = 2^2 \cdot \left(1 - \frac{1}{2}\right) = 2, \quad \varphi(613) = 613 - 1 = 612.$$

Тоді $\varphi(2452) = 2 \cdot 612 = 1224$;

г) $\varphi(729) = \varphi(3^6) = 3^6 \cdot \left(1 - \frac{1}{3}\right) = 729 \cdot \frac{2}{3} = 486$.

Приклад 3. Розв'язати рівняння
а) $\varphi(10^x) = 400$; б) $\varphi(21x) = 120$; в) $\varphi(x) = 16$.

Розв'язання.

а) $\varphi(10^x) = \varphi(2^x \cdot 5^x) = 10^x \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10^x \cdot \frac{2}{5}$;

$10^x \cdot \frac{2}{5} = 400$; $10^x = 1000$; $x = 3$.

б) для простого x маємо
$\varphi(21x) = \varphi(3 \cdot 7 \cdot x) = \varphi(3) \cdot \varphi(7) \cdot \varphi(x) = 2 \cdot 6 \cdot (x-1) = 12(x-1)$;
$12(x-1) = 120$; $x = 11$.

Якщо x складене число, тобто $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, то прості числа p_i можна вибрати тільки з ряду 2, 3, 5, 7, 11. Крім того,
$\varphi(22) = \varphi(11 \cdot 2) = \varphi(11) \cdot \varphi(2) = 10 \cdot 1 = 10$.

Перевіримо:
$\varphi(21 \cdot 22) = 12 \cdot 10 = 120$.

Отже, $x_1 = 11$, $x_2 = 22$.

в) число x може бути складеним $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$. Тоді

$$\varphi(x) = x \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right) = 16.$$

Значить p_i можуть бути простими числами з ряду 2, 3, 5, 7, 11, 13, 17. Перебором установимо, що підійдуть лише такі значення x:

$x = 17$, бо $\varphi(17) = 16$;

$x = 17 \cdot 2 = 34$, бо $\varphi(34) = \varphi(2)\varphi(17) = 1 \cdot 16 = 16$;

$x = 5 \cdot 2^3 = 40$, бо $\varphi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 16$;

$x = 3 \cdot 2^4 = 48$, бо $\varphi(48) = 48\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 16$;

Приклад 4. Визначити непарні прості числа p і q за умови, що значення функції Ейлера $\varphi(n)$, де $n = pq$, відомо.

Розв'язання.

$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq - (p+q) + 1$, а відтак множники p і q визначимо із системи:

$$\begin{cases} n = pq, \\ \varphi(n) = n - (p+q) + 1 \end{cases} \Rightarrow \begin{cases} q = \dfrac{n}{p}, \\ \varphi(n) = n - \left(p + \dfrac{n}{p}\right) + 1 \end{cases}$$

Із системи матимемо:

$$\varphi(n) - n - 1 = -\left(p + \frac{n}{p}\right) \Rightarrow \varphi(n) - n - 1 = -\left(\frac{p^2 + n}{p}\right) \Rightarrow p(\varphi(n) - n - 1) = -p^2 - n \Rightarrow$$

$p^2 - p(n + 1 - \varphi(n)) + n = 0$.

Звідси числа p і q – це розв'язки рівнянь

$$p^2 - p(n + 1 - \varphi(n)) + n = 0 \text{ і } q = \frac{n}{p}.$$

Теореми Ейлера та Ферма

Теореми Ейлера та Ферма відіграють важливу роль в асиметричних криптографічних системах.

Теорема 1 (Ейлера).

Для будь-яких взаємно простих чисел a та m ($m \in N, m > 1$) справедливе порівняння

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m) \qquad (5.4)$$

Доведення. Нагадаємо, що $\varphi(m)$ дорівнює числу додатних цілих значень, менших m і взаємно простих з m. Розглянемо множину таких цілих чисел, пронумерувавши їх у такий спосіб

$$L = \{x_1, x_2, \ldots, x_{\varphi(m)}\}.$$

Тепер помножимо кожен елемент множини L на a за модулем m

$$L' = \{(ax_1 \bmod m), (ax_2 \bmod m), \ldots, (ax_{\varphi(m)} \bmod m)\}.$$

Наведена множина L' представляє перестановку елементів множини L з таких причин:

по-перше, оскільки a, як і x_i, є взаємно простим з m, ax_i теж повинно бути взаємно простим з m. Таким чином, всі елементи L' є цілими числами, меншими m і взаємно простими з m;

по-друге, у множині L' немає повторень. Відповідно до властивостей порівнянь, якщо $ax_1 \bmod m = ax_i \bmod m$, то $x_1 = x_i$. Тому

$$\prod_{i=1}^{\varphi(m)} ax_i \bmod m = \prod_{i=1}^{\varphi(m)} x_i,$$

$$\prod_{i=1}^{\varphi(m)} ax_i \equiv \prod_{i=1}^{\varphi(m)} x_i (\bmod m),$$

$$a^{\varphi(m)} + \left[\prod_{i-1}^{\varphi(m)} x_i\right] \equiv \prod_{i-1}^{\varphi(m)} x_i (\bmod m),$$

$$a^{\varphi(m)} \equiv 1 (\bmod m).$$

Теорема доведена.■

Теорема 2 (Ферма).

Якщо p – просте число, і a є додатним цілим числом, що не ділиться на p, то

$$a^{p-1} \equiv 1 (\bmod p). \qquad (5.5)$$

Ця теорема – окремий випадок теореми Ейлера, бо якщо p – просте, то $\varphi(p) = p - 1$ і тоді із формули (5.4) стає логічною формула (5.5).

Інколи формулі (5.5) надають іншого вигляду, помноживши обидві частини на a, а саме: $a^p \equiv a (\bmod p)$.

Приклад 5. Записати а) теорему Ферма при $p = 7$ і $a = 2$;

б) теорему Ейлера при $m = 12$ і $a = 5$.

Розв'язання.

а) $2^6 = 64 \equiv 1 (\bmod 7)$;

б) $\varphi(12) = \varphi(3 \cdot 2^2) = \varphi(3) \cdot \varphi(2^2) = (3-1) \cdot 4\left(1 - \frac{1}{2}\right) = 4$, $5^4 = 625 \equiv 1 (\bmod 12)$.

Приклад 6. Довести, що $3^{100} \equiv 1 (\bmod 1000)$.

Розв'язання.

НСК(8, 125)=1000. Знайдемо значення функції Ейлера при $n = 8$ і $n = 125$:

$\varphi(8) = \varphi(2^3) = 8(1 - \frac{1}{2}) = 4$ і $\varphi(125) = \varphi(5^3) = 125\left(1 - \frac{1}{5}\right) = 100$.

За теоремою Ейлера $3^4 = 3^{\varphi(8)} \equiv 1 (\bmod 8)$ і $3^{100} = 3^{\varphi(125)} \equiv 1 (\bmod 125)$.

Перше порівняння піднесемо до степеня 25, тобто $3^{100} \equiv 1 (\bmod 8)$. Якщо порівняння справедливі за модулями 8 і 125, то вони справедливі і за найменшим спільним кратним даних модулів (властивість порівнянь). Отже, $3^{100} \equiv 1 (\bmod 1000)$.

Приклад 7. Обчислити $2^{5432675}(\text{mod}13)$.

Розв'язання.

Узагальнимо задачу так: за умови, що число a не ділиться на число p, обчислимо значення $a^k(\text{mod}\,p)$. Розділимо k на $(p-1)$ з остачею:
$k=(p-1)q+r,\ 0<r<p-1,\ q>0$.

Тоді, використовуючи теорему Ферма, отримаємо:

$$a^k(\text{mod}\,p)=a^{(p-1)q+r}(\text{mod}\,p)=(a^{p-1})^q a^r(\text{mod}\,p)\equiv 1^q a^r(\text{mod}\,p)=a^r(\text{mod}\,p).$$

За умовою прикладу $5432675:(13-1)=452722\cdot 12+11$, тоді $2^{5432675}(\text{mod}13)\equiv 2^{11}(\text{mod}13)=(2^5)^2\cdot 2(\text{mod}13)=(32)^2\cdot 2(\text{mod}13)\equiv(6)^2\cdot 2(\text{mod}13)=$
$=72(\text{mod}13)\equiv 7(\text{mod}13)$.

Приклад 8. Знайти остачу від ділення 485^{84} на 129.

Розв'язання.

$\varphi(129)=\varphi(3\cdot 43)=129\left(1-\frac{1}{3}\right)\left(1-\frac{1}{43}\right)=84$. НСД(485, 129)=1.

На основі теореми Ейлера $485^{84}=485^{\varphi(129)}\equiv 1(\text{mod}129)$ приходимо до висновку, що остача від ділення дорівнює одиниці.

Приклад 9. Довести, що при НСД$(a,35)$=1 справедливе порівняння $a^{10}-a^6-a^4+1\equiv 0(\text{mod}35)$.

Розв'язання.

Згідно з теоремою Ферма $a^4\equiv 1(\text{mod}5)$ і $a^6\equiv 1(\text{mod}7)\Rightarrow a^4-1=5t_1$ і $a^6-1=7t_2$, де $t_1=0,\pm 1,\pm 2,\ldots;\ t_2=0,\pm 1,\pm 2,\ldots$.

Помножимо почленно знайдені рівності: $(a^4-1)(a^6-1)=35t_1t_2$. Матимемо $a^{10}-a^6-a^4+1=35t_1t_2$, або $a^{10}-a^6-a^4+1=35t$, де $t=0,\pm 1,\pm 2,\ldots$.

Отже, маємо $a^{10}-a^6-a^4+1\equiv 0(\text{mod}35)$.

Узагальненою функцією Ейлера $L(m)$ називається функція, що визначена для всіх натуральних значень m при $m=1$ $L(1)=1$; при $m>1$ $L(1)=M$, де M – найменше спільне кратне чисел $p_1^{\alpha_1-1}(p_1-1);\ p_2^{\alpha_2-1}(p_2-1);\ \ldots;\ p_s^{\alpha_s-1}(p_s-1)$, де $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ – канонічне розкладання числа m.

Приклад 10. Обчислити $L(360)$.

Розв'язання.

Канонічне розкладання числа $360=2^3\cdot 3^2\cdot 5$. Тоді

$p_1^{\alpha_1-1}(p_1-1)=2^{3-1}(2-1)=4;$

$p_2^{\alpha_2-1}(p_2-1)=3^{2-1}(3-1)=6;$

$p_3^{\alpha_3-1}(p_3-1)=5^{1-1}(5-1)=4.$

НСК(4, 6, 4)=12 $\Rightarrow L(360)=12$.

При $m=p^{\alpha}$ функції $L(m)$ та $\varphi(m)$, очевидно, збігаються.

Теорема 3. Узагальнення теореми Ейлера.

При будь-якому модулі m і НСД(a,m)=1 має місце порівняння $a^{L(m)}\equiv 1(\mathrm{mod}\, m)$.

Доведення. Нехай $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ – канонічне розкладання числа m. За теоремою Ейлера $a^{p_i^{\alpha_i-1}(p_i-1)}\equiv 1(\mathrm{mod}\, p_i^{\alpha_i})$, де $i=1,2,\ldots,s$. Піднесемо обидві частини цього порівняння до цілого степеня $\frac{L(m)}{p_i^{\alpha_i-1}(p_i-1)}$: $a^{L(m)}\equiv 1(\mathrm{mod}\, p_i^{\alpha_i})$.

З порівнянності $a^{L(m)}$ і одиниці за модулями $p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ відповідно до властивості порівнянь випливає порівнянність цих чисел за модулем m, тобто $a^{L(m)}\equiv 1(\mathrm{mod}\, m)$.■

Приклад 11. Дев'ята степінь однозначного числа n закінчується цифрою 7. Знайти це число.

Розв'язання.

Так як дев'ята степінь числа n закінчується цифрою 7, то лишок від ділення числа n^9 на 10 повинен дорівнювати 7, що рівносильно порівнянню $n^9\equiv 7(\mathrm{mod}10)$.

Так як НСД(7, 10)=1, то НСД(n, 10)=1. Використавши теорему Ейлера, отримаємо: $n^{\varphi(10)}\equiv 1(\mathrm{mod}10)\Rightarrow n^4\equiv 1(\mathrm{mod}10)$.

Піднесемо обидві частини порівняння до квадрату. Отримаємо $n^8\equiv 1(\mathrm{mod}10)$. Тоді з порівняння $n^9\equiv 7(\mathrm{mod}10)$ отримаємо $n\equiv 7(\mathrm{mod}10)$. Отже, $n=7$.

Приклад 12. Довести, що $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18}\equiv -1(\mathrm{mod}7)$.

Розв'язання.

Використаємо малу теорему Ферма. Якщо НСД(a,p)=1, то $a^{p-1}\equiv 1(\mathrm{mod}\, p)$. Числа 1, 2, 3, 4, 5, 6 взаємно прості з числом 7. За даною теоремою $a^6\equiv 1(\mathrm{mod}7)$, де $a=1,2,3,4,5,6$. Піднесемо дане порівняння до третього степеня, отримаємо: $a^{18}\equiv 1(\mathrm{mod}7)$. Додаючи почленно дане порівняння при $a=1,2,3,4,5,6$, маємо: $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18}\equiv 6\equiv -1(\mathrm{mod}7)$.

Зауваження. Розв'язання буде значно простішим, якщо показник степеня є непарне число. Нехай потрібно довести, що $1^{11}+2^{11}+3^{11}+4^{11}\equiv 0(\mathrm{mod}5)$.

В лівій частині порівняння в якості основи фігурує зведена система найменших додатних лишків по модулю 5. У випадку непарних показників, використовуючи систему абсолютно найменших лишків по модулю 5, отримаємо: $1^{11}+2^{11}+3^{11}+4^{11}\equiv 1^{11}+2^{11}+(-2)^{11}+(-1)^{11}\equiv 0(\mathrm{mod}5)$.

Приклад 13. Знайти остачу від ділення числа 7^{402} на 101.

Розв'язання.

101 – просте число. Числа 7 і 101 взаємно прості, тому з малої теореми Ферма слідує, що

$7^{100} \equiv 1(\mathrm{mod}101)$.

Піднесемо дане порівняння до четвертого степеня. Отримаємо:

$7^{400} \equiv 1(\mathrm{mod}101)$.

Крім того, $7^2 \equiv 49(\mathrm{mod}101)$. Перемножимо ці порівняння:

$7^{402} \equiv 49(\mathrm{mod}101)$.

З останнього порівняння слідує, що шуканим лишком буде число 49.

Приклад 14. Знайти останні дві цифри числа 243^{402}.

Розв'язання.

Очевидно, що достатньо знайти лишок, отриманий при діленні числа 243^{402} на 100.

$243^{402} \equiv 43^{402}(\mathrm{mod}100)$.

Так як НСД(43, 100)=1, то

$43^{\varphi(100)} \equiv 1(\mathrm{mod}100) \Rightarrow 43^{40} \equiv 1(\mathrm{mod}100)$.

Піднесемо останнє порівняння почленно до десятого степеня:

$43^{400} \equiv 1(\mathrm{mod}100)$.

Візьмемо порівняння $43^2 \equiv 49(\mathrm{mod}100)$ і перемножимо почленно з останнім порівнянням, отримаємо:

$43^{402} \equiv 49(\mathrm{mod}100)$.

Отже, шуканий лишок дорівнює 49.

Приклад 15. Перевірити, що $(73^{12} - 1)$ ділиться на 105.

Розв'язання.

Канонічний розклад числа $105 = 3 \cdot 5 \cdot 7$.

Так як НСД(73, 3)=НСД(73, 5)=НСД(73, 7)=1 і 73 – просте число, застосуємо малу теорему Ферма до числа 73 по модулям 3, 5, 7. Отримаємо порівняння:

$73^2 \equiv 1(\mathrm{mod}3)$, $73^4 \equiv 1(\mathrm{mod}5)$, $73^6 \equiv 1(\mathrm{mod}7)$.

Піднесемо обидві частини порівнянь до відповідних степенів, отримаємо порівняння:

$73^{12} \equiv 1(\mathrm{mod}3)$, $73^{12} \equiv 1(\mathrm{mod}5)$, $73^{12} \equiv 1(\mathrm{mod}7)$.

Використаємо властивість: Якщо $a \equiv b(\mathrm{mod}m_1)$, $a \equiv b(\mathrm{mod}m_2)$ і m – найменше спільне кратне модулів m_1 і m_2, то $a \equiv b(\mathrm{mod}m)$. Отже,

$73^{12} \equiv 1(\mathrm{mod}105) \Rightarrow (73^{12} - 1) \vdots 105$.

Приклад 16. Показати, що число $(13^{176} - 1)$ ділиться на 89.

Розв'язання.

Скористаємось формулою розкладання різниці квадратів:

$13^{176}-1=(13^{88}-1)(13^{88}+1)$.

Якщо хоча б один із співмножників правої частини даної рівності ділиться на 89, то дане число ділиться на 89.

Так як 89 – просте число і НСД(13, 89)=1, то, використавши малу теорему Ферма, бачимо, що справедливе порівняння: $13^{88}\equiv 1(\mathrm{mod}89)$. Отже, так як $(13^{88}-1)\vdots 89$, то $(13^{176}-1)\vdots 89$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Записати значення функції Ейлера для чисел 28, 101, 225.
2. Для числа $n=p_1^{\alpha_1}\times p_2^{\alpha_2}\times\ldots\times p_s^{\alpha_s}$ обчислити функцію Ейлера $\varphi(n)$.

a. $n=2^6\cdot 7^2\cdot 11^2\cdot 37$;

b. $n=3^7\cdot 5^2\cdot 7\cdot 71$;

c. $n=2^6\cdot 5^3\cdot 101$.

4. Знайти останні дві цифри числа 582^{302}.

12.6 Практична робота №6

Тема: Дії над класами лишків за модулем. Повна і зведена система лишків.

Мета: Розглянути розподіл чисел у класах за даним модулем, а також властивості класів за даним модулем, дати визначення повній і зведеній системам лишків.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Дії над класами за модулем

Розподіл чисел у класах за даним модулем. На множині цілих чисел визначимо бінарне відношення, поклавши $a\sim b$, якщо $a\equiv b(\mathrm{mod}m)$. Таке бінарне відношення є відношенням еквівалентності, бо рефлексивне, симетричне і транзитивне.

До того ж зазначене відношення "$\equiv(\mathrm{mod}m)$" розбиває множину всіх цілих чисел на неперетинні класи еквівалентності $\bar{0},\bar{1},\bar{2},\ldots,\overline{m-1}$, які називаються ***класами лишків за модулем*** m, а будь-яке число класу – ***лишком класу (представником класу)***. Клас лишків за модулем m, що містить число a, позначатимемо $\bar{a}$. Він являє собою множину чисел x, які є порівнянними з числом a за модулем m, тобто задовольняють умову $x\equiv a(\mathrm{mod}m)$. Отже,

$$r=\bar{0}=\{\ldots,-2m,-m,0,m,2m,3m,\ldots\}$$
$$r=\bar{1}=\{\ldots,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}$$
……
$$r=\overline{m-1}=\{\ldots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,\ldots\}$$

Наприклад, за модулем 10 число 73 належить до класу $\overline{13}$, а число –17 до класу $\bar{3}$, бо $73\equiv 13(\mathrm{mod}10),\ -17\equiv 3(\mathrm{mod}10)$.

З означення класу лишків випливає, що числам класу відповідає одна й та ж остача r від ділення на модуль, тому дістанемо числа класу, коли у виразі $r+mt$ змінна t пробігатиме всі цілі числа. Лишок, обчислений при $t=0$, рівний самій остачі r, називають ***найменшим невід'ємним лишком***.

Властивості класів за даним модулем.

1) Усі лишки одного й того ж класу порівнянні один з одним за модулем m, тоді як лишки інших класів – ні.

2) Кожен клас лишків містить нескінченну множину чисел. Кількість класів за модулем m скінченна і дорівнює m. Кожне ціле число можна порівняти за модулем m тільки з одним із чисел $0,1,2,\ldots,m-1$. Наприклад за модулем 6 можна назвати всього 6 класів, а саме:

$$\bar{0}=\{\ldots,-12,-6,0,6,12,18,\ldots\},\ \bar{1}=\{\ldots,-11,-5,1,7,13,19,\ldots\},$$
$$\bar{2}=\{\ldots,-10,-4,2,8,14,20,\ldots\},\ \bar{3}=\{\ldots,-9,-3,3,9,15,21,\ldots\},$$
$$\bar{4}=\{\ldots,-8,-2,4,10,16,22,\ldots\},\ \bar{5}=\{\ldots,-7,-1,5,11,17,23,\ldots\},$$

3) Якщо два класи мають принаймні одне спільне число, то вони збігаються.

4) Усі лишки одного класу $\bar{a}$ за модулем m мають з числом m однаковий найбільший спільний дільник.

Повна і зведена система лишків

Повною системою лишків за модулем m називається будь-яка система з m чисел, узятих по одному з кожного класу лишків за цим модулем. Наприклад, числа –12, –11, 2, 15, 22, 5 утворюють повну систему лишків за модулем 6. Очевидно, для будь-якого модуля m повну систему лишків утворюють числа $\{0,1,2,\ldots,m-1\}$. Класи лишків за модулем m, представники яких взаємно прості з числом m, називаються ***зведеними***, а будь-яка система чисел, узятих по одному з кожного зведеного класу, називається ***зведеною системою лишків***. Таким чином зведена система лишків складається з тих чисел повної системи лишків, що взаємно прості з модулем (звичайно їх вибирають з повної системи найменших невід'ємних лишків). Так зведена система лишків за модулем 6 містить два числа 1 і 5. Якщо модуль m – просте число, то до зведеної системи лишків увійде вся множина чисел $\{0,1,2,\ldots,m-1\}$.

Зауваження. Якщо $\mathrm{НСД}(a,m)=1$ і x пробігає повну систему лишків за модулем m, то вираз $ax+b$, де b – будь-яке ціле, також пробігає повну систему лишків за тим же модулем.

Приклад 1. Задана сукупність чисел (9, 2, 16, 20, 27, 39, 46, 85). Чи можна розглядати дану сукупність як повну систему лишків по модулю 8?

Розв'язання.

У відповідності з визначенням повної системи лишків по модулю m сукупність відповідних чисел при діленні на m повинна давати в остачі числа: $0,1,2,3,4,\ldots,m-1.$

Легко встановити, виконуючи послідовно ділення чисел даної сукупності на число 8, що остачі дорівнюють числам: $1,2,0,4,3,7,6,5.$

Отже, дану сукупність чисел можна розглядати як повну систему лишків по модулю 8.

Приклад 2. Задана сукупність чисел (9, 2, 16, 20, 27, 39, 46, 86). Здійснити таку заміну чисел цієї сукупності, щоб її можна було прийняти як повну систему лишків по модулю 8.

Розв'язання.

Порівнюючи дану послідовність з послідовністю у прикладі 1, помічаємо, що вони відрізняються лише останнім числом, і тепер вже два числа (46 і 86) дають в остачі при діленні на 8 число 6. Щоб отримати потрібну сукупність, необхідно замінити одне з чисел, наприклад число 86, на будь-яке інше число, яке дає в остачі при діленні на число 8 число 5 (наприклад, 85).

Приклад 3. Написати повні системи абсолютно найменших лишків по модулям 7 і 8.

Розв'язання.

Якщо модуль m – непарне число, то в шуканій системі лишків допустиме найбільше по абсолютному значенню число $\frac{m-1}{2}$; якщо модуль m – парне число, то в шуканій системі лишків допустиме найбільше по абсолютному значенню число $\frac{m}{2}$. Шуканими повними системами абсолютно найменших лишків будуть системи:

(–3, –2, –1, 0, 1, 2, 3), якщо модуль дорівнює 7;

(–3, –2, –1, 0, 1, 2, 3, 4) чи (–4, –3, –2, –1, 0, 1, 2, 3), якщо модуль дорівнює 8.

Приклад 4. Задана повна система лишків (9, 2, 16, 20, 27, 39, 46, 85) по модулю 8. Вибрати з цих чисел ті, які входять у зведену систему лишків по модулю 8.

Розв'язання.

У відповідності до визначення, з даної сукупності потрібно вибрати всі числа, які взаємно прості з модулем. Тому зведена система лишків по модулю 8 буде мати вигляд: (9, 27, 39, 85).

Зауваження. Зведена система лишків по модулю m містить $\varphi(m)$ чисел; $\varphi(8)=4$, тобто шукана система повинна містити чотири числа.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Перевірити, чи становить задана сукупність чисел (85, 46, 39, 27, 20, 16, 2, 9) повну систему лишків за модулем 8.
2. Із скількох елементів складається абсолютно найменша система лишків за модулем 13? Назвіть ці елементи.
3. Доведіть, що задані конгруенції НЕ мають місця:
   a. $6^{89} \equiv 13 (\mathrm{mod} 16)$;
   b. $21^{138} \equiv 31 (\mathrm{mod} 49)$;
   c. $8^{107} \equiv 7 (\mathrm{mod} 35)$.

12.7 Практична робота №7

Тема: Базові означення з теорії поля. Операції арифметики в класах лишків.

Мета: Дати визначення таким поняттям: група, півгрупа, поле, кільце. Ввести операції арифметики в класах лишків та розглянути властивості арифметики в класах лишків.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Базові означення з теорії поля

Абелева (комутативна) **група** – це множина F, на якій визначена одна бінарна операція $(\bullet)$ з такими властивостями для $\forall a, b \in F$:

1. $\exists c \in F : a \bullet b = c$ – замкненість,
2. $a \bullet b = b \bullet a$ – комутативність,
3. $\exists c \in F : a \bullet b \bullet c = (b \bullet a) \bullet c = a \bullet (b \bullet c)$ – асоціативність,
4. $\exists e \in F : a \bullet e = e \bullet a = a$ – існування нейтрального елемента,
5. $\exists a^{-1} \in F : a \bullet a^{-1} = e$ – існування для кожного елемента a множини F оберненого елемента.

Півгрупа відрізняється від групи тим, що не для кожного ненульового елемента множини існує обернений елемент.

Поле – це множина, на якій визначені дві бінарні операції – адитивна (“+”, або “додавання”) та мультиплікативна (“×”, або “множення”) – на таких підставах:

a) за адитивною операцією множина створює абелеву групу;
a) за мультиплікативною операцією всі ненульові елементи множини створюють абелеву групу;
b) виконується дистрибутивний закон.

Кільце відрізняється від поля тим, що за мультиплікативною операцією множина створює півгрупу.

Операції арифметики в класах лишків

Кільця Z_m лишків за модулем m. Для кожного натурального m через Z_m позначимо множину чисел $Z_m = \{0,1,2,\ldots,m-1\}$, що являють собою повну систему найменших невід'ємних лишків за модулем m, і утворюють множину класів лишків за модулем $\bar{0},\bar{1},\bar{2},\ldots,\overline{m-1}$.

На зазначеній множині введемо дві операції, які відповідно назвемо *додаванням* та *множенням класів лишків за модулем*, і позначимо їх "+" та "×". Для цих операцій покладемо:

$\bar{a}+\bar{b}=\overline{a+b}$, якщо $a+b<m$,

$\bar{a}+\bar{b}=\overline{a+b-m}$, якщо $a+b\geq m$,

$\bar{a}\cdot\bar{b}=\bar{r}$, де $a\cdot b=mq+r,\ 0\leq r<m$.

Згідно з означенням, сумою і добутком класів $\bar{a}$ та $\bar{b}$ будуть відповідно класи чисел, які містять числа $a+b$ та ab. Клас лишків $\overline{-a}$ називають ***протилежним класу*** $\bar{a}$. На множині $Z_m=\{0,1,2,\ldots,m-1\}$ $\overline{-a}=\overline{m-a}$.

Додавання та множення класів зручно задавати за допомогою таблиць Келі. Так, табл. 1 визначає додавання класів $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ за модулем 4, а табл. 2 – їх множення. (*Примітка:* у першому рядку і першому стовпці таблиць записані представники класів, сума та добутки класів також визначені своїми представниками).

Таблиця 1

Представник класу	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Таблиця 2

Представник класу	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Відзначимо такі факти:

1) Множина класів $\bar{0},\bar{1},\bar{2},\ldots,\overline{m-1}$ лишків за модулем m (і відповідно множина чисел $Z_m=\{0,1,2,\ldots,m-1\}$) із введеною операцією додавання класів утворює скінченну ***абелеву адитивну групу порядку*** m, бо, по-перше, додаванню класів характерні властивості замкненості, комутативності та асоціативності, а, по-друге, роль нульового елемента групи виконує клас $\bar{0}$, елементами якого є числа, кратні m, і для кожного класу $\bar{a}$ існує протилежний клас $\overline{-a}$. Абелева адитивна група класів лишків за модулем m позначається Z_m.

2) Множина $Z_m=\{0,1,2,\ldots,m-1\}$ лишків за модулем m з операціями додавання $a+b\equiv(a+b)(\mathrm{mod}m)$ та множення $a\cdot b\equiv(ab)(\mathrm{mod}m)$ утворює

скінченне ***комутативне кільце лишків за модулем*** m ***з одиницею***. Дійсно, для множини $Z_m = \{0,1,2,\ldots,m-1\}$ виконуються всі умови, що визначають комутативне кільце: вона являє собою адитивну групу. Операція множення елементів – замкнена, комутативна, асоціативна та дистрибутивна (ці властивості походять з властивостей порівнянь та властивостей комутативного кільця цілих чисел). *У кільці лишків за модулем* m *можуть бути дільники нуля тоді і тільки тоді, коли* m *– складене число*. Дійсно, якщо $a \cdot b = 0$, то $a \cdot b \equiv 0 (\mathrm{mod} m)$, що неможливо за умови, що m – просте число та $a \neq 0$ або $b \neq 0$. Це, наприклад, обумовлює появу результату $\bar{2} \cdot \bar{2} = \bar{0}$ у таблиці Келі для кільця Z_4. *Кільце класів за простим модулем не містить дільників нуля.*

3) Нехай $Z_m = \{0,1,2,\ldots,m-1\}$ – кільце лишків за модулем m. Елемент кільця $a^{-1} \in Z_m$ називається ***оберненим*** до елемента $a \in Z_m$ у кільці Z_m, а саме число a – ***оборотним***, якщо виконується рівність $a \cdot a^{-1} \equiv 1 (\mathrm{mod} m)$ або $1 \equiv a \cdot a^{-1} (\mathrm{mod} m)$. Множина елементів у Z_m, для яких у цьому кільці існують обернені елементи відносно множення, утворює ***мультиплікативну групу*** (позначають Z_m^*).

Теорема 1.

Елементами групи Z_m^* будуть тільки взаємно прості за модулем m елементи a кільця Z_m.

Доведення. Найбільший спільний дільник взаємно простих чисел дорівнює одиниці, тобто $\mathrm{НСД}(a,m) = 1$. Тоді існують такі цілі числа α та β, що $\alpha a + \beta m = 1$. Звідси $\alpha a \equiv 1 (\mathrm{mod} m)$ і $a^{-1} \equiv \alpha (\mathrm{mod} m)$ – обернений елемент до елемента a у кільці Z_m. Якщо ж допустити протилежне, що у кільці Z_m $a \cdot a^{-1} \equiv 1$, остача від ділення добутку $a \cdot a^{-1}$ на m дорівнює одиниці, тобто $a \cdot a^{-1} = qm + 1$. Таким чином, кожен спільний дільник чисел a та m ділить також одиницю, звідки $\mathrm{НСД}(a,m) = 1$.■

Порядок групи Z_m^* дорівнює кількості чисел, менших за m, які взаємно прості з m. Так, $Z_8^* = \{1,3,5,7\}$, $|Z_8^*| = 4$.

Визначення. Для простого модуля p кільце Z_p ***є полем***, тобто $Z_p^* = Z_p \setminus \{0\}$ – поле, бо тоді умова $\mathrm{НСД}(a,p) = 1$ рівнозначна умові, коли p не ділить a, що справедливо для всіх натуральних чисел, менших за p. Це обумовлює існування нескінченної кількості різних скінченних полів лишків за простим модулем: поля Z_2 лише двома елементами, а також полів $Z_3, Z_5, Z_7, \ldots$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Зробити розгорнутий конспект на тему: “Властивості арифметики в класах лишків”.

12.8 Практична робота №8

Тема: Одномодульна арифметика: додавання за модулем, віднімання за модулем, множення за модулем, ділення за модулем.

Мета: Розглянути операції додавання, віднімання, множення та ділення за модулем, отримати навики розв'язування завдань з даної теми.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай a, b і m – цілі додатні числа, m – модуль, $0 \le a \le m-1$, $0 \le b \le m-1$.

Додавання за модулем m

$a + b \equiv c(\mathrm{mod} m)$,

де $$c = \begin{cases} a+b, & якщо\ a+b < m; \\ a+b-m, & якщо\ a+b > m. \end{cases}$$

Приклад 1.

Додати за модулем $m = 11$ числа $a = 4$ і $b = 5$.

Розв'язання.

$a + b = 4 + 5 = 9 < 11$, отже $4 + 5 \equiv 9(\mathrm{mod}11)$.

Приклад 2.

Додати за модулем $m = 11$ числа $a = 6$ і $b = 9$.

Розв'язання.

$a + b = 6 + 9 = 15 > 11$, отже $6 + 9 \equiv 15(\mathrm{mod}11) \equiv (15 - 11)(\mathrm{mod}11) \equiv 4(\mathrm{mod}11)$.

Віднімання за модулем m

$a - b \equiv r(\mathrm{mod} m)$,

де $$r = \begin{cases} a-b, & якщо\ a-b \ge 0; \\ a-b+m, & якщо\ a-b < 0. \end{cases}$$

Приклад 3.

Відняти за модулем $m = 11$ числа $a = 8$ і $b = 5$.

Розв'язання.

$a - b = 8 - 5 = 3 > 0$, отже $8 - 5 \equiv 3(\mathrm{mod}11)$.

Приклад 4.

Додати за модулем $m = 11$ числа $a = 6$ і $b = 9$.

Розв'язання.

$a - b = 6 - 9 = -3 < 0$, отже $6 - 9 \equiv -3(\mathrm{mod}11) \equiv (-3 + 11)(\mathrm{mod}11) \equiv 8(\mathrm{mod}11)$.

Множення за модулем m

$a \cdot b \equiv d(\mathrm{mod} m)$,

де $$d = a \cdot b - \left]\frac{a \cdot b}{m}\right[\cdot m,$$

$\left] \right[$ – означають цілу частину числа.

Приклад 5.

Помножити за модулем $m = 11$ числа $a = 8$ і $b = 5$.

Розв'язання.

$d = 8 \cdot 5 - \left]\frac{8 \cdot 5}{11}\right[\cdot 11 = 40 - 3 \cdot 11 = 40 - 33 = 7$. Отже, $8 \cdot 5 \equiv 7(\mathrm{mod} 11)$.

Ділення за модулем m

$\frac{a}{b} \equiv q(\mathrm{mod} m)$,

де $$q \equiv a \cdot h(\mathrm{mod} m),$$

$h \equiv \frac{1}{b}(\mathrm{mod} m)$ – ***мультиплікативне обернене числа*** b ***за модулем*** m.

Якщо $\mathrm{НСД}(b, m) = 1$, то існує таке h, що $b \cdot h \equiv 1(\mathrm{mod} m)$.

Для обчислення мультиплікативного оберненого використовують розширений алгоритм Евкліда.

Крок 1: $(x_1, x_2, x_3) := (1, 0, m)$; $(y_1, y_2, y_3) := (0, 1, b)$.

Крок 2: якщо $y_3 = 0$, то $x_3 = \mathrm{НСД}(b, m)$ $\Rightarrow$ немає мультиплікативного оберненого $\Rightarrow$ кінець.

Крок 3: якщо $y_3 = 1$, то $x_3 = \mathrm{НСД}(b, m)$; $y_2 = h(\mathrm{mod} m)$ $\Rightarrow$ кінець.

Крок 4: $g = \left]\frac{x_3}{y_3}\right[$.

Крок 5: $(t_1, t_2, t_3) := (x_1 - g \cdot y_1,\ x_2 - g \cdot y_2,\ x_3 - g \cdot y_3)$.

Крок 6: $(x_1, x_2, x_3) := (y_1, y_2, y_3)$.

Крок 7: $(y_1, y_2, y_3) := (t_1, t_2, t_3)$.

Крок 8: перейти до кроку 2.

Приклад 6.

Обчислити мультиплікативне обернене числа $b = 4$ за модулем $m = 13$.

Розв'язання.

g	x_1	x_2	x_3	y_1	y_2	y_3	t_1	t_2	t_3
-	1	0	13	0	1	4	-	-	-
3							1	-3	1
	0	1	4	1	-3	1			

Оскільки $y_3 = 1$, то $y_2 = h(\mathrm{mod} m)$. Отже, $\frac{1}{4}(\mathrm{mod}13) \equiv -3(\mathrm{mod}13) \equiv 10(\mathrm{mod}13)$.

Перевірка: $4 \cdot 10(\mathrm{mod}13) \equiv 40(\mathrm{mod}13) \equiv 1(\mathrm{mod}13)$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Курсова робота, розділ 1, пункти 1.2, 1.3, 1.4.

Самостійна робота. Модуль
Варіант №1

1. Задана сукупність чисел (100, 56, 24, 111, 61, 95). Чи можна розглядати дану сукупність як повну систему лишків за модулем 6?
2. Чому дорівнює Функція Ейлера $\varphi(378)$?
3. Сформулювати теорему Ферма.
4. Записати теорему Ейлера при $m = 15,\ a = 8$.
5. Дев'ята степінь однозначного числа n закінчується цифрою 3. Знайти це число.

Варіант №1

1. Задана сукупність чисел (100, 56, 24, 111, 61, 95). Чи можна розглядати дану сукупність як повну систему лишків за модулем 6?
2. Чому дорівнює Функція Ейлера $\varphi(378)$?
3. Сформулювати теорему Ферма.
4. Записати теорему Ейлера при $m = 15,\ a = 8$.
5. Дев'ята степінь однозначного числа n закінчується цифрою 3. Знайти це число.

Варіант №2

1. Задана сукупність чисел (30, 99, 171, 69, 35, 25, 75). Чи можна розглядати дану сукупність як повну систему лишків за модулем 7?
2. Чому дорівнює Функція Ейлера $\varphi(245)$?
3. Сформулювати теорему Ейлера.
4. Записати теорему Ейлера при $m = 18,\ a = 7$.

5. Дев'ята степінь однозначного числа n закінчується цифрою 9. Знайти це число.

Варіант №2

1. Задана сукупність чисел (30, 99, 171, 69, 35, 25, 75). Чи можна розглядати дану сукупність як повну систему лишків за модулем 7?
2. Чому дорівнює Функція Ейлера $\varphi(245)$?
3. Сформулювати теорему Ейлера.
4. Записати теорему Ейлера при $m=18,\ a=7$.
5. Дев'ята степінь однозначного числа n закінчується цифрою 9. Знайти це число.

12.9 Практична робота №9

Тема: Алгебраїчні порівняння: основні поняття. Умови існування розв'язку порівнянь першого степеня. Способи розв'язання алгебраїчних порівнянь першого степеня.

Мета: Розглянути способи розв'язання конгруенцій першого степеня, пригадати розкладання дробу у скінченний ланцюговий дріб, отримати навички розв'язання алгебраїчних порівнянь першого степеня.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Алгебраїчні порівняння: основні поняття

Якщо $f(x_1,x_2,...,x_n)$ – многочлен від n змінних з цілими коефіцієнтами, то порівняння вигляду

$$f(x_1,x_2,...,x_n)=0(\mathrm{mod}\,m) \qquad (9.1)$$

називається ***алгебраїчним порівнянням з n змінними***.

Розв'язок порівняння $f(x_1,x_2,...,x_n)=0(\mathrm{mod}\,m)$ – будь-який набір $a_1,a_2,...,a_n$ таких цілих значень невідомих $x_1,x_2,...,x_n$, що число $f(a_1,a_2,...,a_n)$ буде порівнянним з нулем за модулем m. Якщо цілі числа розв'язку $a_i,\ i=1,2,...,n$ належать відповідно до класів лишків $\overline{a_i}$ за модулем m, то будь-який інший набір чисел a_i^*, які належать до тих же класів лишків, тобто $a_i^*\in\overline{a_i}$, також буде розв'язком порівняння (9.1). Тому *розв'язком порівняння прийнято називати і сам набір класів лишків, представниками яких є числа* $a_1,a_2,...,a_n$. При такій домовленості порівняння (9.1) має стільки розв'язків, скільки лишків повної системи його задовольняє.

Алгебраїчним порівнянням з однією змінною x називається порівняння вигляду

$$c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n = 0(\mathrm{mod}\, m) \qquad (9.2)$$

або скорочено $f(x) = 0(\mathrm{mod}\, m)$, де $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$ – многочлен з цілими коефіцієнтами, що залежить від однієї змінної x.

Найвищий степінь невідомого у такому порівнянні називають ***степенем порівняння***. Якщо якесь число a задовольняє зазначене порівняння, то й увесь клас лишків $\overline{a}$ задовольнятиме таке порівняння, тому ***розв'язком (коренем)*** порівняння (9.2) вважають клас лишків $\overline{a}$ за модулем m. Кількість класів за даним модулем скінченна, адже саме за модулем лишків існує m класів: $\overline{a_0}, \overline{a_1}, \ldots, \overline{a_{m-1}}$. Отже, щоб розв'язати порівняння (9.2), можна взяти будь-яку повну систему лишків $x_1, x_2, \ldots, x_m$ за модулем m, обчислити $f(x_1), f(x_2), \ldots, f(x_m)$ та відібрати ті значення x_i, при яких $f(x_i)$ ділиться на m. Відповідні класи лишків, представниками яких є x_i, дадуть усі розв'язки (корені) порівняння.

Зауваження 1. Якщо порівняння має декілька розв'язків $x_1, x_2, \ldots, x_s$, то інколи їх записують у вигляді $x \equiv x_1, x_2, \ldots, x_s (\mathrm{mod}\, m)$.

Зауваження 2. ***Порівняння*** $f(x) = 0(\mathrm{mod}\, m)$ ***та*** $g(x) = 0(\mathrm{mod}\, m)$ ***називаються еквівалентними***, якщо множина чисел, що задовольняє одне з них, збігається з множиною чисел, які задовольняють інше.

Приклад 1. Розв'язати порівняння

а) $x^3 - 2x + 6 \equiv 0(\mathrm{mod}11)$; б) $x^4 + 2x^3 + 6 \equiv 0(\mathrm{mod}8)$.

Розв'язання.

а) запишемо повну систему найменших за абсолютною величиною лишків за модулем 11: –5, –4, –3, –2, –1, 0, 1, 2, 3, 4, 5. Порівняння задовольнить тільки число 5, бо

$$5^3 - 2 \cdot 5 + 6 = 121 \text{ і } 121 \equiv 0(\mathrm{mod}11).$$

Корені порівняння запишемо як $x \equiv 5(\mathrm{mod}11)$. Жодне інше число з системи лишків не задовольнить порівняння, наприклад, при $x = 2$

$$2^3 - 2 \cdot 2 + 6 = 10 \not\equiv 0(\mathrm{mod}11)$$

б) у повній системі лишків –3, –2, –1, 0, 1, 2, 3, 4 жодне число не задовольняє порівняння, і тому воно не має розв'язків.

На перший погляд, задача розв'язання порівнянь $f(x) = 0(\mathrm{mod}\, m)$ простіша за розв'язок рівнянь в алгебрі, проте, при великих модулях розв'язання порівнянь шляхом випробувань представників класів лишків за модулем m – досить громіздка робота.

Розглянемо способи, що дадуть змогу визначати кількість розв'язків порівняння та знаходити їх за допомогою як найменшої кількості операцій.

Умови існування розв'язку порівнянь першого степеня

Загальний вигляд порівняння першого степеня такий

$$ax \equiv b(\mathrm{mod}\, m), \tag{9.3}$$

де a, b – цілі задані коефіцієнти.

Нехай НСД$(a,m) = d$ – найбільший спільний дільник чисел a і m. Тоді:

- якщо коефіцієнт b не ділиться на d, то порівняння $ax \equiv b(\mathrm{mod}\, m)$ не матиме розв'язку;
- за умови, що число b кратне d, порівняння $ax \equiv b(\mathrm{mod}\, m)$ має рівно d розв'язків, а саме: $x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$, де x_0 – розв'язок порівняння $\frac{a}{d}x \equiv \frac{b}{d}(\mathrm{mod}\frac{m}{d})$;
- якщо НСД$(a,m) = 1$, тобто числа a і m взаємно прості, то порівняння $ax \equiv b(\mathrm{mod}\, m)$ має тільки один розв'язок $x = x_0(\mathrm{mod}\, m)$, причому порівняння задовольняє клас розв'язків $x = x_0 + mt,\ t = 0, \pm 1, \pm 2$.

Способи розв'язування порівнянь першого степеня

Існує декілька способів розв'язування порівнянь першого степеня вигляду $ax \equiv b(\mathrm{mod}\, m)$ при НСД$(a,m) = 1$. Зокрема, розв'язування порівнянь за допомогою:

– *випробування лишків повної системи за модулем* m;

– *теореми Ейлера* $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, де НСД$(a,m) = 1$. Для цього почленно помножимо порівняння $ax \equiv b(\mathrm{mod}\, m)$ на $a^{\varphi(m)-1}$:

$$a \cdot a^{\varphi(m)-1} \cdot x \equiv b \cdot a^{\varphi(m)-1}(\mathrm{mod}\, m) \Rightarrow a^{\varphi(m)} \cdot x \equiv b \cdot a^{\varphi(m)-1}(\mathrm{mod}\, m) \Rightarrow x \equiv b \cdot a^{\varphi(m)-1}(\mathrm{mod}\, m)$$

Приклад 2. Розв'язати порівняння $7x \equiv 5(\mathrm{mod}9)$.

Розв'язання.

$$a = 7;\ b = 5;\ m = 9;\ \text{НСД}(7,9) = 1;\ \varphi(9) = \varphi(3^2) = 9(1 - \frac{1}{3}) = 6;\ \varphi(9) - 1 = 5;$$

$$x \equiv 5 \cdot 7^5(\mathrm{mod}9) = 5 \cdot 49^2 \cdot 7(\mathrm{mod}9) = 5 \cdot (5 \cdot 9 + 4)^2 \cdot 7(\mathrm{mod}9) \equiv$$

$$\equiv 5 \cdot 4^2 \cdot 7(\mathrm{mod}9) = 560(\mathrm{mod}9) = (62 \cdot 9 + 2)(\mathrm{mod}9) \equiv 2(\mathrm{mod}9)$$

Остаточно $x \equiv 2(\mathrm{mod}9)$.

Напевно, при великому m розв'язування порівнянь за допомогою методу випробувань або теореми Ейлера – доволі нелегка обчислювальна задача.

Скористаємося властивістю скінченних ланцюгових дробів. Дійсно, нехай $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_{k-1}}{q_{k-1}}, \frac{p_k}{q_k} = \frac{m}{a}$ – послідовність підхідних дробів розкладання дробу $\frac{m}{a}$ на ланцюговий дріб і НСД$(a,m) = 1$. За властивістю підхідних дробів

НСД$(p_k, q_k) = 1$ і тому $\frac{p_k}{q_k} = \frac{m}{a}$ являє собою рівність двох нескоротних дробів, отже, $p_k = m$ і $q_k = a$. У рекурентній формулі $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ для чисельників і знаменників підхідних дробів замінимо $p_k = m$ та $q_k = a$: $mq_{k-1} - ap_{k-1} = (-1)^{k-1}$. Звідси $ap_{k-1} = (-1)^k + mq_{k-1}$ або $ap_{k-1} = (-1)^k (\mathrm{mod} m)$. Помноживши останнє порівняння на $(-1)^k b$, дістанемо $a((-1)^k bp_{k-1}) \equiv b(\mathrm{mod} m)$.

Таким чином, число $x \equiv (-1)^k bp_{k-1} (\mathrm{mod} m)$.

Приклад 3. Розв'язати порівняння $31x \equiv 19(\mathrm{mod} 83)$.

Розв'язання.

$a = 31;\ b = 19;\ m = 83;\ $ НСД$(31,83) = 1$.

Розкладемо дріб $\frac{83}{31}$ на ланцюговий дріб:

$$\frac{83}{31} = 2\frac{21}{31} = 2 + \frac{21}{31} = 2 + \frac{1}{\frac{31}{21}} = 2 + \frac{1}{1\frac{10}{21}} = 2 + \frac{1}{1 + \frac{10}{21}} = 2 + \frac{1}{1 + \frac{1}{\frac{21}{10}}} = 2 + \frac{1}{1 + \frac{1}{2\frac{1}{10}}} =$$

$$= 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{10}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{10}{1}}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{10}}}.$$

Отже, маємо ланцюжок неповних часток $\frac{83}{31} = [2,1,2,10]$. Це розкладання дасть таку таблицю частинних знаменників a_k ланцюгового дробу та чисельників p_k підхідних дробів:

k	0	1	2	3	4
a_k	–	2	1	2	10
p_k	1	2	3	8	–
q_k	0	1	1	3	–

Чисельники p_k підхідних дробів визначаються з формул:

$$\frac{p_1}{q_1} = a_1 = 2,\quad \frac{p_2}{q_{21}} = a_1 + \frac{1}{a_2} = 2 + \frac{1}{1} = 3,\quad \frac{p_3}{q_3} = a_1 + \frac{1}{a_2 + \frac{1}{a_3}} = 2 + \frac{1}{1 + \frac{1}{2}} = \frac{8}{3},$$

p_0 і q_0 покладемо відповідно рівними 1 і 0.

Тут $k = 3,\ p_{k-1} = 8$. Тоді $x \equiv (-1)^3 \cdot 19 \cdot 8(\mathrm{mod} 83) = -152(\mathrm{mod} 83) \equiv 14(\mathrm{mod} 83)$ – шуканий розв'язок.

Розглянемо нижченаведену теорему при невеликих значеннях a.

Теорема 1.

Якщо НСД$(a,m)=1$ і $(b+km)\vdots a$, то розв'язком порівняння $ax\equiv b(\mathrm{mod}\,m)$ стає $x\equiv\dfrac{b+km}{a}(\mathrm{mod}\,m)$.

Доведення. $a\left(\dfrac{b+km}{a}\right)=b+km\equiv b(\mathrm{mod}\,m)$.

За означеною теоремою порівняння $ax\equiv b(\mathrm{mod}\,m)$ послідовно замінюють еквівалентними порівняннями $ax\equiv b\pm m(\mathrm{mod}\,m)$, $ax\equiv b\pm 2m(\mathrm{mod}\,m)$, $ax\equiv b\pm 3m(\mathrm{mod}\,m),\ldots$, поки не отримають таке, в якому ліву та праву частини можна скоротити на a. При цьому кількість випробувань буде не більша за a.■

Приклад 4. Розв'язати порівняння $3x\equiv 20(\mathrm{mod}161)$.

Розв'язання.

$a=3;\ b=20;\ m=161;$ НСД$(3,161)=1$.

При такому значенні a число k можна вибрати серед чисел –1, 0, 1. У даному випадку $(20-161)\vdots 3$, а відтак порівняння $3x\equiv 20(\mathrm{mod}161)$ еквівалентне порівнянню $3x\equiv -141(\mathrm{mod}161)$ і, тоді $x\equiv -47(\mathrm{mod}161)\equiv 114(\mathrm{mod}161)$.

Розглянемо приклад, в якому у порівнянні $ax\equiv b(\mathrm{mod}\,m)$ число b кратне НСД$(a,m)=d$.

Приклад 5. Розв'язати порівняння $15x\equiv 21(\mathrm{mod}18)$.

Розв'язання.

$a=15;\ b=21;\ m=18;\ d=$НСД$(15,18)=3$.

Скоротимо обидві частини на $d=3$. Отримаємо $5x\equiv 7(\mathrm{mod}6)$. Звідси

$$5x\equiv 1(\mathrm{mod}6),\ 5x\equiv(4\cdot 6+1)(\mathrm{mod}6)=25(\mathrm{mod}6)\Rightarrow x\equiv 5(\mathrm{mod}6),$$
$$x\equiv(5+6)(\mathrm{mod}6)=11(\mathrm{mod}6);\ x\equiv(5+12)(\mathrm{mod}6)=17(\mathrm{mod}6);$$

Використаємо розширений евклідів алгоритм. Нехай у порівнянні (9.3) НСД$(a,m)=1$. Якби (9.3) було звичайним лінійним рівнянням $ax=b$, то для визначення його кореня слід b поділити на a. Використаємо цю ідею для розв'язання порівняння. За умови розширеного евклідового алгоритму визначимо обернений елемент a^{-1} до елемента a за модулем m, тобто $a\cdot a^{-1}\equiv 1(\mathrm{mod}\,m)$. Помноживши обидві частини порівняння (9.3) на a^{-1}, дістанемо $x:\ a^{-1}ax\equiv a^{-1}b(\mathrm{mod}\,m)\Rightarrow x\equiv a^{-1}b(\mathrm{mod}\,m)$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розкласти у неперервний дріб $\dfrac{151}{13}$. Розкладання подати у вигляді схеми:

k	0	1	2	3	…
a_k					
p_k					
q_k					

Записати отримані підхідні дроби.

2. Записати дріб через ланцюжок неповних часток: a. $\frac{179}{19}$; b. $\frac{53}{7}$ c. $\frac{105}{38}$.

3. Розв'язати конгруенцію $15x \equiv 25(\mathrm{mod}17)$, використавши властивості конгруенцій.

4. Розв'язати конгруенцію $256x \equiv 179(\mathrm{mod}337)$, використавши підхідні дроби.

12.10 Практична робота №10

Тема: Системи порівнянь першого степеня.

Мета: Розглянути, за яких вимог система порівнянь першого степеня буде мати розв'язки, навчитися розв'язувати системи порівнянь першого степеня.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Визначення. *Системою порівнянь* називають систему вигляду

$$\begin{cases} f_1(x) \equiv 0(\mathrm{mod}\, m_1), \\ f_2(x) \equiv 0(\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ f_n(x) \equiv 0(\mathrm{mod}\, m_n) \end{cases} \qquad (10.1)$$

де $f_1(x), f_2(x), \ldots, f_n(x)$ – задані многочлени з цілими коефіцієнтами. Нехай M – найменше спільне кратне всіх модулів $m_1, m_2, \ldots, m_n$.

Визначення. *Розв'язком системи (10.1)* буде клас чисел за модулем M, що містить числа, які задовольняють кожне порівняння системи. Так, у системі

$$\begin{cases} x^2 - 3x + 2 \equiv 0(\mathrm{mod}6), \\ 2x^2 + x + 2 \equiv 0(\mathrm{mod}4) \end{cases}$$

$m_1 = 6;\ m_2 = 4;\quad M = \mathrm{НСК}(m_1, m_2) = 12$. У повній системі найменших за абсолютною величиною лишків за модулем 12 обидва порівняння системи задовольняють числа ± 2. Тому розв'язки системи – це два класи за модулем 12, тобто $x = \pm 2(\mathrm{mod}12)$.

Система порівнянь першого степеня складається з n порівнянь із одним і тим же невідомим, але з різними модулями:

$$\begin{cases} a_1 x \equiv b_1 (\mathrm{mod}\, m_1), \\ a_2 x \equiv b_2 (\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ a_n x \equiv b_n (\mathrm{mod}\, m_n) \end{cases} \qquad (10.2)$$

де $\text{НСД}(a_1, m_1) = 1$; $\text{НСД}(a_2, m_2) = 1$; …; $\text{НСД}(a_n, m_n) = 1$.

Кожне порівняння у системі (10.2) можна розв'язати окремо, тобто спочатку записати порівняння у вигляді

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_n (\mathrm{mod}\, m_n) \end{cases} \qquad (10.3)$$

Якщо хоч одне з порівнянь наведеної системи не має розв'язків, то система несумісна.

Теорема 1.

Нехай $d = \text{НСД}(m_1, m_2)$ – найбільший спільний дільник чисел m_1 і m_2, а $M = \text{НСК}(m_1, m_2)$ – їх найменше спільне кратне. Система двох порівнянь

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2) \end{cases} \qquad (10.4)$$

має розв'язок

$$x \equiv x_0 (\mathrm{mod}\, M) \qquad (10.5)$$

тільки за умови, що $c_2 \equiv c_1 (\mathrm{mod}\, d)$.

Доведення. Перше порівняння системи свідчить, що $x = c_1 + m_1 t,\ t = 0, \pm 1, \pm 2, \ldots$. Підставимо цей вираз замість x у друге порівняння:

$$c_1 + m_1 t \equiv c_2 (\mathrm{mod}\, m_2) \text{ або } m_1 t \equiv c_2 - c_1 (\mathrm{mod}\, m_2). \qquad (10.6)$$

Останнє порівняння має розв'язок t тільки за умови, що $(c_2 - c_1) \vdots d$, де $d = \text{НСД}(m_1, m_2)$. Загальний розв'язок порівняння має вигляд $t = t_0 + k\frac{m_2}{d}$, де t_0 – який-небудь частинний розв'язок порівняння (10.6), $k = 0, \pm 1, \pm 2, \ldots$. Підставимо це значення t у формулу $x = c_1 + m_1 t$: $x = c_1 + m_1 t_0 + \frac{m_1 m_2}{d} k$, але $\frac{m_1 m_2}{d} = M$. Позначивши $c_1 + m_1 t_0 = x_0$, дістанемо загальний розв'язок системи $x \equiv x_0 (\mathrm{mod}\, M)$.■

Наслідок. Якщо m_1 і m_2 – взаємно прості числа, то $d = 1$ і система (10.4) завжди має єдиний розв'язок.

Приклад 1. Розв'язати систему порівнянь

$$\begin{cases} x \equiv 9 (\mathrm{mod}\, 34), \\ x \equiv 4 (\mathrm{mod}\, 19). \end{cases}$$

Розв'язання.

Система має розв'язки, бо НСД $(34,19)=1$. Знайдемо $x = 9 + 34t \equiv 4 (\mathrm{mod}\, 19)$, $t = 0, \pm 1, \pm 2, \ldots$. Тоді

$$34t \equiv -5 (\mathrm{mod}\, 19) \Rightarrow 15t \equiv -5 (\mathrm{mod}\, 19) \Rightarrow 3t \equiv -1 (\mathrm{mod}\, 19) \equiv 18 (\mathrm{mod}\, 19) \Rightarrow$$

$$\Rightarrow t \equiv 6 (\mathrm{mod}\, 19) \Rightarrow t = 6 + 19k, \ k = 0, \pm 1, \pm 2, \ldots$$

Підставимо значення t у вираз для x:

$$x = 9 + 34(6 + 19k) = 213 + 646k \Rightarrow x \equiv 213 (\mathrm{mod}\, 646).$$

Якщо розв'язується система (10.3), що складається з n порівнянь, то спочатку можна розв'язати перші два з них і замінити їх у системі (10.3) виразом (10.5). Далі взяти здобуте порівняння і третє з системи та розв'язати їх і т.д. З кожним таким кроком кількість порівнянь у системі зменшується і наприкінці дістанемо одне порівняння вигляду (10.5), де M – найменше спільне кратне всіх модулів.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Скільки розв'язків має система конгруенцій?

a. $\begin{cases} x \equiv 48 (\mathrm{mod}\, 85), \\ x \equiv 14 (\mathrm{mod}\, 51). \end{cases}$

b. $\begin{cases} x \equiv 48 (\mathrm{mod}\, 203), \\ x \equiv 24 (\mathrm{mod}\, 119). \end{cases}$

2. Розв'язати систему конгруенцій, попередньо спростивши її.

a. $\begin{cases} 913x \equiv 132 (\mathrm{mod}\, 23), \\ 138x \equiv 245 (\mathrm{mod}\, 11), \\ 457x \equiv 623 (\mathrm{mod}\, 17). \end{cases}$

b. $\begin{cases} 253x \equiv 429 (\mathrm{mod}\, 17), \\ 338x \equiv 545 (\mathrm{mod}\, 19), \\ 579x \equiv 741 (\mathrm{mod}\, 13). \end{cases}$

12.11 Практична робота №11

Тема: Китайська теорема про лишки.

Мета: Отримати відповідь про існування та структуру розв'язку системи порівнянь першого степеня.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Китайська теорема про лишки

Нехай в системі

$$\begin{cases} x \equiv c_1 (\mathrm{mod} m_1), \\ x \equiv c_2 (\mathrm{mod} m_2), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_n (\mathrm{mod} m_n) \end{cases} \qquad (11.1)$$

модулі $m_1, m_2, \ldots, m_n$ – попарно взаємно прості; M – найменше спільне кратне чисел $m_1, m_2, \ldots, m_n$; числа $y_1, y_2, \ldots, y_n$ підібрані так, що виконуються порівняння $\frac{M}{m_1} y_1 \equiv 1 (\mathrm{mod} m_1), \frac{M}{m_2} y_2 \equiv 1 (\mathrm{mod} m_2), \ldots, \frac{M}{m_n} y_n \equiv 1 (\mathrm{mod} m_n)$. Тоді система (11.1) матиме єдиний розв'язок $x \equiv x_0 (\mathrm{mod} M)$, де $x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \ldots + \frac{M}{m_n} y_n c_n$.

Доведення. Позначимо $M_i = \frac{M}{m_i}$, $i = 1, 2, \ldots, n$. Для кожного M_i визначимо число y_i таке, що $\frac{M}{m_i} y_i \equiv 1 (\mathrm{mod} m_i)$. Домножимо обидві частини і модуль першої конгруенції на M_1, другої – на M_2 і т.д. Одержимо:

$$xM_1 \equiv c_1 M_1 (\mathrm{mod} M)$$

$$xM_2 \equiv c_1 M_2 (\mathrm{mod} M)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$xM_n \equiv c_1 M_n (\mathrm{mod} M)$$

Домножимо ліву і праву частини першої конгруенції на y_1, другої – на y_2 і т.д., і одержані таким чином конгруенції за модулем M почленно додамо.

Одержимо:

$$x(M_1 y_1 + \ldots + M_n y_n) \equiv c_1 M_1 y_1 + \ldots + c_n M_n y_n (\mathrm{mod} M). \qquad (11.2)$$

Доведемо, що коефіцієнт при x конгруентний 1 за модулем M. Дійсно, $M_1 y_1 + \ldots + M_n y_n \equiv 1 (\mathrm{mod} m_1)$, оскільки всі доданки, крім першого, діляться на m_1, а перший доданок конгруентний 1 за модулем m_1 в силу визначення y_1. Аналогічно,

$$M_1 y_1 + \ldots + M_n y_n \equiv 1 (\mathrm{mod} m_2)$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$M_1y_1+\dots+M_ny_n\equiv 1(\mathrm{mod}\,m_n)$$

За властивістю конгруенцій, маємо $M_1y_1+\dots+M_ny_n\equiv 1(\mathrm{mod}\,M)$.

Повертаючись до конгруенції (11.2), одержуємо: $x\equiv c_1M_1y_1+\dots+c_nM_ny_n(\mathrm{mod}\,M)$, який буде розв'язком системи (11.1).

Доведемо єдиність розв'язку за модулем M. Дійсно, нехай x_1 та x_2 – два розв'язки системи (11.1), тобто

$$\begin{array}{ll} x_1\equiv c_1(\mathrm{mod}\,m_1) & x_2\equiv c_1(\mathrm{mod}\,m_1)\\ x_1\equiv c_2(\mathrm{mod}\,m_2) & x_2\equiv c_2(\mathrm{mod}\,m_2)\\ \dots\dots\dots\dots\dots & \dots\dots\dots\dots\dots\\ x_1\equiv c_n(\mathrm{mod}\,m_n) & x_2\equiv c_n(\mathrm{mod}\,m_n) \end{array} \quad \text{і} \quad .$$

Звідки маємо:

$$\begin{array}{l} x_1\equiv x_2(\mathrm{mod}\,m_1)\\ x_1\equiv x_2(\mathrm{mod}\,m_2)\\ \dots\dots\dots\dots\dots\\ x_1\equiv x_2(\mathrm{mod}\,m_n) \end{array}$$

За властивістю конгруенцій, одержуємо $x_1\equiv x_2(\mathrm{mod}\,M)$, що і треба було довести.■

Приклад 1. Розв'язати систему порівнянь

$$\begin{cases} x\equiv 6(\mathrm{mod}17)\\ x\equiv 4(\mathrm{mod}11)\\ x\equiv -3(\mathrm{mod}8) \end{cases}$$

Розв'язання.

Усі модулі взаємно прості. $M=\mathrm{НСК}(17,11,8)=1496$ – найменше спільне кратне модулів. За китайською теоремою про лишки знайдемо:

$$11\cdot 8\cdot y_1\equiv 1(\mathrm{mod}17)\Rightarrow 3y_1\equiv 1(\mathrm{mod}17)\Rightarrow y_1=6,$$
$$17\cdot 8\cdot y_2\equiv 1(\mathrm{mod}11)\Rightarrow 4y_2\equiv 1(\mathrm{mod}11)\Rightarrow y_2=3,$$
$$17\cdot 11\cdot y_3\equiv 1(\mathrm{mod}8)\Rightarrow 3y_3\equiv 1(\mathrm{mod}8)\Rightarrow y_3=3,$$
$$x=11\cdot 8\cdot 6\cdot 6+17\cdot 8\cdot 3\cdot 4+17\cdot 11\cdot 3\cdot(-3)=3117,$$
$$x=3117(\mathrm{mod}1496)\equiv 125(\mathrm{mod}1496).$$

Приклад 2. Розв'язати систему конгруенцій

$$\begin{cases} x \equiv 16(\mathrm{mod}13) \\ x \equiv 128(\mathrm{mod}5) \\ x \equiv 82(\mathrm{mod}3) \\ x \equiv 55(\mathrm{mod}7) \end{cases}$$

Розв'язання.

Спершу спростимо систему:

$$\begin{cases} x \equiv 16(\mathrm{mod}13) \\ x \equiv 128(\mathrm{mod}5) \\ x \equiv 82(\mathrm{mod}3) \\ x \equiv 55(\mathrm{mod}7) \end{cases} \Rightarrow \begin{cases} x \equiv 3(\mathrm{mod}13) \\ x \equiv -2(\mathrm{mod}5) \\ x \equiv 1(\mathrm{mod}3) \\ x \equiv -1(\mathrm{mod}7) \end{cases}.$$

Побудуємо систему чисел M_i:

$M_1 = 5 \cdot 3 \cdot 7 = 105;\ M_2 = 13 \cdot 3 \cdot 7 = 273;\ M_3 = 13 \cdot 5 \cdot 7 = 455;\ M_4 = 13 \cdot 5 \cdot 3 = 195.$

Знайдемо обернені значення до M_i, $i = \overline{1,4}$:

$105M_1^{-1} \equiv 1(\mathrm{mod}13):\ 105 = 13 \cdot 8 + 1,\ 105 \equiv 1(\mathrm{mod}13) \Rightarrow M_1^{-1} \equiv 1(\mathrm{mod}13).$

$273M_2^{-1} \equiv 1(\mathrm{mod}5):\ 273 \cdot 2 = 546 = 545 + 1 \Rightarrow M_2^{-1} \equiv 2(\mathrm{mod}5).$

$455M_3^{-1} \equiv 1(\mathrm{mod}3):\ 455 \cdot 2 = 910 = 909 + 1 \Rightarrow M_3^{-1} \equiv 2(\mathrm{mod}3).$

$195M_4^{-1} \equiv 1(\mathrm{mod}7):\ 195 \cdot 6 = 1170 = 167 \cdot 7 + 1 \Rightarrow M_4^{-1} \equiv 6(\mathrm{mod}7) \equiv -1(\mathrm{mod}7).$

Будуємо розв'язок:

$x = 105 \cdot 1 \cdot 3 + 273 \cdot 2 \cdot (-2) + 455 \cdot 2 \cdot 1 + 195 \cdot (-1) \cdot (-1) = 315 - 1092 + 910 + 195 = 328$

Перевірка:

$328 = 25 \cdot 13 + 3;\quad 328 = 65 \cdot 5 + 3 = 66 \cdot 5 - 2;$

$328 = 109 \cdot 3 + 1;\quad 328 = 46 \cdot 7 + 6 = 47 \cdot 8 - 1.$

Система розв'язана правильно.

Отже, розв'язком системи є клас лишків $x = 328 + 13 \cdot 5 \cdot 3 \cdot 7 \cdot t$ за модулем, що дорівнює НСК чисел 13, 5, 3, 7.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Реалізація алгоритму китайської теореми про лишки на мові С++.
2. Знайти розв’язок системи порівнянь.

1	$\begin{cases} x \equiv 5 (\mod 7) \\ x \equiv 10 (\mod 11) \\ x \equiv 2 (\mod 9) \end{cases}$	11	$\begin{cases} x \equiv 3 (\mod 5) \\ x \equiv 2 (\mod 7) \\ x \equiv 0 (\mod 2) \end{cases}$	21	$\begin{cases} x \equiv 1 (\mod 3) \\ x \equiv 4 (\mod 5) \\ x \equiv 2 (\mod 4) \end{cases}$
2	$\begin{cases} x \equiv 5 (\mod 7) \\ x \equiv 4 (\mod 5) \\ x \equiv 1 (\mod 2) \end{cases}$	12	$\begin{cases} x \equiv 3 (\mod 5) \\ x \equiv 6 (\mod 7) \\ x \equiv 0 (\mod 2) \end{cases}$	22	$\begin{cases} x \equiv 1 (\mod 5) \\ x \equiv 6 (\mod 7) \\ x \equiv 0 (\mod 2) \end{cases}$
3	$\begin{cases} x \equiv 3 (\mod 7) \\ x \equiv 3 (\mod 5) \\ x \equiv 0 (\mod 2) \end{cases}$	13	$\begin{cases} x \equiv 1 (\mod 7) \\ x \equiv 2 (\mod 3) \\ x \equiv 3 (\mod 5) \end{cases}$	23	$\begin{cases} x \equiv 5 (\mod 7) \\ x \equiv 10 (\mod 11) \\ x \equiv 6 (\mod 9) \end{cases}$
4	$\begin{cases} x \equiv 2 (\mod 3) \\ x \equiv 2 (\mod 5) \\ x \equiv 0 (\mod 2) \end{cases}$	14	$\begin{cases} x \equiv 3 (\mod 7) \\ x \equiv 2 (\mod 3) \\ x \equiv 1 (\mod 5) \end{cases}$	24	$\begin{cases} x \equiv 2 (\mod 5) \\ x \equiv 1 (\mod 3) \\ x \equiv 0 (\mod 2) \end{cases}$
5	$\begin{cases} x \equiv 2 (\mod 3) \\ x \equiv 3 (\mod 5) \\ x \equiv 2 (\mod 4) \end{cases}$	15	$\begin{cases} x \equiv 5 (\mod 7) \\ x \equiv 2 (\mod 3) \\ x \equiv 1 (\mod 5) \end{cases}$	25	$\begin{cases} x \equiv 6 (\mod 7) \\ x \equiv 2 (\mod 3) \\ x \equiv 1 (\mod 5) \end{cases}$
6	$\begin{cases} x \equiv 2 (\mod 7) \\ x \equiv 1 (\mod 3) \\ x \equiv 1 (\mod 4) \end{cases}$	16	$\begin{cases} x \equiv 1 (\mod 5) \\ x \equiv 1 (\mod 3) \\ x \equiv 0 (\mod 2) \end{cases}$	26	$\begin{cases} x \equiv 2 (\mod 3) \\ x \equiv 4 (\mod 5) \\ x \equiv 0 (\mod 2) \end{cases}$
7	$\begin{cases} x \equiv 3 (\mod 5) \\ x \equiv 4 (\mod 7) \\ x \equiv 0 (\mod 2) \end{cases}$	17	$\begin{cases} x \equiv 1 (\mod 7) \\ x \equiv 1 (\mod 3) \\ x \equiv 1 (\mod 5) \end{cases}$	27	$\begin{cases} x \equiv 1 (\mod 5) \\ x \equiv 3 (\mod 7) \\ x \equiv 0 (\mod 2) \end{cases}$
8	$\begin{cases} x \equiv 3 (\mod 5) \\ x \equiv 3 (\mod 7) \\ x \equiv 4 (\mod 6) \end{cases}$	18	$\begin{cases} x \equiv 1 (\mod 5) \\ x \equiv 1 (\mod 3) \\ x \equiv 0 (\mod 2) \end{cases}$	28	$\begin{cases} x \equiv 4 (\mod 5) \\ x \equiv 1 (\mod 7) \\ x \equiv 2 (\mod 6) \end{cases}$
9	$\begin{cases} x \equiv 3 (\mod 7) \\ x \equiv 2 (\mod 5) \\ x \equiv 1 (\mod 2) \end{cases}$	19	$\begin{cases} x \equiv 4 (\mod 5) \\ x \equiv 3 (\mod 7) \\ x \equiv 0 (\mod 6) \end{cases}$	29	$\begin{cases} x \equiv 5 (\mod 7) \\ x \equiv 1 (\mod 5) \\ x \equiv 0 (\mod 2) \end{cases}$
10	$\begin{cases} x \equiv 4 (\mod 5) \\ x \equiv 5 (\mod 7) \\ x \equiv 1 (\mod 2) \end{cases}$	20	$\begin{cases} x \equiv 2 (\mod 3) \\ x \equiv 4 (\mod 5) \\ x \equiv 0 (\mod 2) \end{cases}$	30	$\begin{cases} x \equiv 3 (\mod 5) \\ x \equiv 2 (\mod 3) \\ x \equiv 1 (\mod 4) \end{cases}$

Відповіді

№	x	z_i	M_i
1	362(mod 693)	5, 4, 4,	99, 63, 77,
2	19(mod 70)	4, 1, 1,	10, 14, 35,
3	38(mod 70)	1, 2, 6,	10, 14, 35,
4	2(mod 30)	2, 2, 6,	10, 6, 15,
5	38(mod 60)	1, 4, 6,	20, 12, 15,
6	37(mod 84)	6, 4, 1,	12, 28, 21,
7	18(mod 70)	2, 6, 6,	14, 10, 35,
8	178(mod 210)	4, 5, 2,	42, 30, 35,
9	17(mod 70)	1, 3, 1,	10, 14, 35,
10	19(mod 70)	1, 4, 1,	14, 10, 35,
11	58(mod 70)	2, 3, 6,	14, 10, 35,
12	48(mod 70)	2, 2, 6,	14, 10, 35,
13	8(mod 105)	1, 4, 3,	15, 35, 21,
14	101(mod 105)	3, 1, 6,	15, 35, 21,
15	26(mod 105)	5, 4, 6,	15, 35, 21,
16	16(mod 30)	1, 4, 2,	6, 10, 15,
17	1(mod 105)	1, 2, 6,	15, 35, 21,
18	16(mod 30)	1, 1, 6,	6, 10, 15,
19	24(mod 210)	2, 5, 6,	42, 30, 35,
20	14(mod 30)	2, 4, 6,	10, 6, 15,
21	34(mod 60)	2, 2, 2,	20, 12, 15,
22	6(mod 70)	4, 2, 6,	14, 10, 35,
23	285(mod 693)	5, 4, 3,	99, 63, 77,
24	22(mod 30)	2, 4, 6,	6, 10, 15,
25	41(mod 105)	6, 1, 6,	15, 35, 21,
26	14(mod 30)	2, 4, 6,	10, 6, 15,
27	66(mod 70)	4, 1, 6,	14, 10, 35,
28	134(mod 210)	2, 4, 4,	42, 30, 35,
29	26(mod 70)	4, 4, 6,	10, 14, 35,
30	53(mod 60)	4, 1, 3,	12, 20, 15,

12.12 Практична робота №12

Тема: Алгебраїчні порівняння вищих степенів за простим модулем. Алгебраїчні порівняння вищих степенів за складеним модулем.

Мета: Розглянути загальні теореми, які стосуються конгруенцій n-го степеня за простим модулем p та складеним модулем. Навчитися розв'язувати порівняння n-го степеня.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Алгебраїчні порівняння вищих степенів за простим модулем

Загальний вигляд алгебраїчного порівняння n-го степеня такий:

$$c_0x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_{n-1}x + c_n = 0(\mathrm{mod}\, p) \qquad (12.1)$$

або скорочено

$$f(x) = 0(\mathrm{mod}\, p), \qquad (12.2)$$

де p – просте число, $f(x) = c_0x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_{n-1}x + c_n$ – многочлен однієї змінної x з цілими коефіцієнтами.

Наведемо загальні теореми щодо розв'язку таких порівнянь.

Теорема 1.

Якщо у порівнянні (12.1) старший коефіцієнт c_0 не ділиться на p, то порівняння можна замінити еквівалентним порівнянням

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_{n-1}x + b_n = 0(\mathrm{mod}\, p),$$

в якому коефіцієнт при старшому члені дорівнює одиниці.

Приклад 1. Замінити порівняння $27x^3 + 14x^2 - 10x + 13 \equiv 0(\mathrm{mod}59)$ еквівалентним порівнянням з коефіцієнтом при старшому члені, рівним одиниці.

Розв'язання.

НСД$(27,59) = 1$. Порівняння $27y_0 \equiv 1(\mathrm{mod}59)$ має розв'язок $y_0 = 35$. Задане порівняння еквівалентне

$$x^3 + 14 \cdot 35x^2 - 10 \cdot 35x + 13 \cdot 35 \equiv 0(\mathrm{mod}59)$$

або

$$x^3 + 18x^2 + 4x - 17 \equiv 0(\mathrm{mod}59).$$

Теорема 2.

Якщо $f(x)$ і $g(x)$ – многочлени з цілими коефіцієнтами, то порівняння за простим модулем

$$f(x) = 0(\mathrm{mod}\, p) \qquad (12.3)$$

та

$$f(x) - (x^p - x) \cdot g(x) = 0(\mathrm{mod}\, p) \qquad (12.4)$$

будуть еквівалентними.

Доведення. Нехай $f(x_0)=0(\mathrm{mod}\,p)$, p – просте число. Оскільки при будь-якому x_0 згідно з теоремою Ферма $x_0^p-x_0\equiv 0(\mathrm{mod}\,p)$, то коли x_0 задовольняє порівняння (12.4), маємо $f(x_0)-(x_0^p-x_0)\cdot g(x_0)=0(\mathrm{mod}\,p)$ і, таким чином, порівняння (12.3) і (12.4) еквівалентні.■

Теорема 3.

Порівняння $f(x)=0(\mathrm{mod}\,p)$, степінь якого більший за простий модуль p або рівний йому, можна замінити еквівалентним порівнянням, степінь якого менший за p.

Доведення. Розділимо $f(x)$ на x^p-x. На основі алгоритму ділення $(x^p-x)\cdot g(x)+r(x)\equiv 0(\mathrm{mod}\,p)$, де степінь остачі $r(x)$ менший за p. Відповідно до теореми Ферма $x_0^p-x_0\equiv 0(\mathrm{mod}\,p)$ і тоді залишиться $r(x)\equiv 0(\mathrm{mod}\,p)$. Отже, знайшли порівняння нижчого степеня, еквівалентне даному.■

Наведена теорема подає загальний підхід до розв'язання алгебраїчних порівнянь, степінь яких більший за простий модуль p або рівний йому.

Приклад 2. Розв'язати порівняння

$$x^7+2x^6+x^5-x^3-2x^2-4x+2\equiv 0(\mathrm{mod}5)$$

Розв'язання.

$p=5<7=n$. Розділивши многочлен на $x^p-x=x^5-x$, маємо $(x^2+2x+1)(x^5-x)+(-3x+2)\equiv 0(\mathrm{mod}5)$.

Отже, $-3x+2\equiv 0(\mathrm{mod}5)\Rightarrow 3x\equiv 2(\mathrm{mod}5)\Rightarrow 3x\equiv 12(\mathrm{mod}5)\Rightarrow x\equiv 4(\mathrm{mod}5)$.

Теорема 4.

Порівняння степеня n за простим модулем p з коефіцієнтом при старшому степені, що не ділиться на p, може мати не більше n розв'язків.

Для складених модулів ця теорема несправедлива.

Наслідок. Якщо деякі числа $\alpha_1,\alpha_2,\ldots,\alpha_n$ становлять розв'язок порівняння $f(x)\equiv 0(\mathrm{mod}\,p)$ n-го степеня, то це порівняння еквівалентне порівнянню $c_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)\equiv 0(\mathrm{mod}\,p)$.

Алгебраїчні порівняння вищих степенів за складеним модулем.

Теорема 5. Якщо $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ – канонічне розкладання модуля m на множники, то алгебраїчне порівняння n-го степеня за складеним модулем

$$f(x)\equiv 0(\mathrm{mod}m) \tag{12.5}$$

еквівалентне системі порівнянь

$$\begin{cases} f(x)\equiv 0(\mathrm{mod}\,p_1^{\alpha_1}),\\ f(x)\equiv 0(\mathrm{mod}\,p_2^{\alpha_2}),\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ f(x)\equiv 0(\mathrm{mod}\,p_s^{\alpha_s}), \end{cases} \tag{12.6}$$

Розглянемо два випадки розв'язання порівняння (12.5).

Перший випадок. Модуль порівняння (12.5) має лише прості множники $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. Якщо відповідна система (12.6) у цьому разі сумісна, то порівняння $f(x) \equiv 0(\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s})$ налічує розв'язки, кількість яких дорівнює добутку кількостей розв'язків кожного порівняння системи (12.6). Розв'язуючи систему, спочатку розв'яжемо кожне порівняння окремо, а потім знайдені розв'язки скомбінуємо між собою.

Приклад 3. Розв'язати порівняння

$$x^7 + 3x^6 + 2x^5 - x^3 - 3x^2 + 5x - 1 \equiv 0(\mathrm{mod}15)$$

Розв'язання.

Перший випадок.

Задане порівняння $f(x) \equiv 0(\mathrm{mod}5 \cdot 3)$ замінимо системою за простими модулями.

$$\begin{cases} x^7 + 3x^6 + 2x^5 - x^3 - 3x^2 + 5x - 1 \equiv 0(\mathrm{mod}5), \\ x^7 + 3x^6 + 2x^5 - x^3 - 3x^2 + 5x - 1 \equiv 0(\mathrm{mod}3) \end{cases}$$

Тепер розв'яжемо кожне порівняння окремо.

1) $x^7 + 3x^6 + 2x^5 - x^3 - 3x^2 + 5x - 1 \equiv 0(\mathrm{mod}5)$

Згідно з теоремою 3 маємо $(x^2 + 3x + 2)(x^5 - x) + 7x - 1 \equiv 0(\mathrm{mod}5)$, звідки $7x - 1 \equiv 0(\mathrm{mod}5) \Rightarrow 7x \equiv 1(\mathrm{mod}5) \Rightarrow 2x \equiv 1(\mathrm{mod}5) \Rightarrow 2x \equiv 6(\mathrm{mod}5) \Rightarrow x \equiv 3(\mathrm{mod}5)$;

2) $x^7 + 3x^6 + 2x^5 - x^3 - 3x^2 + 5x - 1 \equiv 0(\mathrm{mod}3) \Rightarrow x^7 + 2x^5 - x^3 + 2x - 1 \equiv 0(\mathrm{mod}3)$

Згідно з теоремою 3 маємо $(x^4 + 3x^2 + 2)(x^3 - x) + 4x - 1 \equiv 0(\mathrm{mod}3)$, звідки $4x - 1 \equiv 0(\mathrm{mod}3) \Rightarrow 4x \equiv 1(\mathrm{mod}3) \Rightarrow x \equiv 1(\mathrm{mod}3)$.

Після цього складемо і розв'яжемо систему порівнянь $\begin{cases} x \equiv 3(\mathrm{mod}5), \\ x \equiv 1(\mathrm{mod}3) \end{cases}$.

$x = 3 + 5t;\ 3 + 5t \equiv 1(\mathrm{mod}3);\ t \equiv -1(\mathrm{mod}3) \equiv 2(\mathrm{mod}3);\ t = 2 + 3k;\ x = 3 + 5(2 + 3k);$ $x = 13 + 15k$, де $t, k = 0, \pm 1, \pm 2, \ldots$. Остаточно $x \equiv 13(\mathrm{mod}15)$.

Другий випадок. Модуль порівняння (12.5) має вигляд $m = p^{\alpha}$, де p – просте число. Спочатку розв'яжемо порівняння за простим модулем $f(x) = 0(\mathrm{mod}\, p)$. Припустимо, що його розв'язок $x = x_0 + pt$, де $t = 0, \pm 1, \pm 2, \ldots$. Розкладемо функцію $f(x_0 + pt)$ у ряд Тейлора:

$$f(x_0 + pt) = f(x_0) + \frac{f'(x_0)}{1!} pt + \frac{f''(x_0)}{2!} p^2 t^2 + \ldots$$

Усі члени даного ряду, починаючи з третього, діляться на p^2. Отже, порівняння матиме місце при $f(x_0) + f'(x_0) pt = 0(\mathrm{mod}\, p^2)$.

Значення $f(x_0)$ ділиться на p, бо x_0 – розв'язок порівняння за модулем p. Зі знайденого порівняння легко визначити t за умови, що $f'(x_0)$ не ділиться на p:

$$\frac{f(x_0)}{p} + f'(x_0)t = 0(\mathrm{mod}\, p).$$

Розв'язком останнього порівняння буде $t \equiv x'(\mathrm{mod}\, p) \Rightarrow t = x' + pk$, де $k = 0, \pm 1, \pm 2, \ldots$. Тоді $x = x_0 + p(x' + pk) = x_0 + px' + p^2k = x_0' + p^2k$, де $x_0' = x_0 + px'$. У результаті $x \equiv x_0'(\mathrm{mod}\, p^2)$. Тепер підставимо це значення на місце x в даний многочлен і знову розкладемо $f(x_0' + p^2k)$ у ряд Тейлора:

$$f(x_0' + p^2t) = f(x_0') + \frac{f'(x_0')}{1!}p^2k + \frac{f''(x_0')}{2!}p^4k^2 + \ldots$$

Усі члени ряду, починаючи з третього, діляться на p^3. На цій основі весь многочлен ділиться на p^3 тоді, коли вираз $f(x_0') + f'(x_0')p^2k$ ділиться на p^3.

Отже, запишемо порівняння $f(x_0') + f'(x_0')p^2k = 0(\mathrm{mod}\, p^3)$, $\frac{f(x_0')}{p^2} + f'(x_0')k = 0(\mathrm{mod}\, p)$ відносно k. Припустимо, що $k = x'' + pl$, де $l = 0, \pm 1, \pm 2, \ldots$. Підставивши це значення у вираз для x, дістанемо загальний розв'язок за модулем p^3: $x = x_0' + p^2(x'' + pl) = x_0' + p^2x'' + p^3l = x_0'' + p^3l$, де $x_0'' = x_0' + p^2x''$.

Продовжуючи, дійдемо порівняння за модулем p^α, тобто дістанемо розв'язок вихідного порівняння за цим модулем.

Приклад 4. Розв'язати порівняння

$$x^5 + 2x^4 + 3x^3 + x^2 + x + 1 \equiv 0(\mathrm{mod}\, 27)$$

Розв'язання.

Модуль $27 = 3^3$. Спочатку розв'яжемо порівняння за модулем 3:

$$x^5 + 2x^4 + 3x^3 + x^2 + x + 1 \equiv 0(\mathrm{mod}\, 3) \Rightarrow$$

$$\Rightarrow (x^2 + 2x + 4)(x^3 - x) + (3x^2 + 5x + 1) \equiv 0(\mathrm{mod}\, 3),$$

$$(3x^2 + 5x + 1) \equiv 0(\mathrm{mod}\, 3),\ (2x + 1) \equiv 0(\mathrm{mod}\, 3),\ 2x \equiv -1(\mathrm{mod}\, 3),\ 2x \equiv 2(\mathrm{mod}\, 3),$$

$$x \equiv 1(\mathrm{mod}\, 3),\ x = 1 + 3t, \text{ де } t = 0, \pm 1, \pm 2, \ldots .$$

Тепер розкладемо функцію в ряд Тейлора для $x = 1 + 3t$:

$$f(1 + 3t) = f(1) + \frac{f'(1)}{1!}3t + \frac{f''(1)}{2!}9t^2 + \frac{f'''(1)}{3!}27t^3 + \ldots$$

Усі члени ряду, починаючи з третього, діляться на 9 і на цій основі запишемо нове порівняння, яке розв'яжемо відносно t:

$$f(1) + f'(1)3t \equiv 0(\mathrm{mod}\, 3),$$

$$f(1) = 9,\ f'(1) = (5x^4 + 8x^3 + 9x^2 + 2x + 1)\Big|_{x=1} = 25,$$

$$9 + 25 \cdot 3t \equiv 0(\mathrm{mod}\, 3),\ 3 + 25t \equiv 0(\mathrm{mod}\, 3),\ 0 + 25t \equiv 0(\mathrm{mod}\, 3),\ t \equiv 0(\mathrm{mod}\, 3),\ t = 3k,$$

$$x = 1 + 9k\ \ (k = 0, \pm 1, \pm 2, \ldots).$$

Складемо порівняння за модулем 27 і розв'яжемо відносно k:

$$f(1)+f'(1)9k\equiv 0(\mathrm{mod}27),$$

$$9+25\cdot 3t\equiv 0(\mathrm{mod}27),\ 9+25\cdot 9k\equiv 0(\mathrm{mod}3),\ 1+25k\equiv 0(\mathrm{mod}3),\ 25+25k\equiv 0(\mathrm{mod}3),$$

$$1+k\equiv 0(\mathrm{mod}3),\ k\equiv -1(\mathrm{mod}3)\equiv 2(\mathrm{mod}3),\ k=2+3l\ \ (l=0,\pm 1,\pm 2,\ldots).$$

Далі визначимо значення x, яке задовольняє основне порівняння за модулем 27.

$$x=1+9k=1+9(2+3l)=1+18+27l=19+27l.$$

Отже, розв'язок порівняння $x=19\ (\mathrm{mod}27)$.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розв'язати конгруенцію за складеним модулем.

1	$x^4-3x^3+2x^2-5x-10\equiv 0(\mathrm{mod}343)$
2	$6x^3-7x-11\equiv 0(\mathrm{mod}125)$
3	$x^4+4x^3+2x^2+x+12\equiv 0(\mathrm{mod}625)$
4	$9x^2+29x+62\equiv 0(\mathrm{mod}32)$
5	$x^3+3x^2-5x+16\equiv 0(\mathrm{mod}125)$
6	$x^5-5x^4-5x^3+25x^2+4x-20\equiv 0(\mathrm{mod}147)$
7	$x^5+3x^4-7x^3+4x^2+4x-10\equiv 0(\mathrm{mod}175)$
8	$x^4-4x^3+2x^2+x+6\equiv 0(\mathrm{mod}135)$
9	$4x^3+7x^2-7x-10\equiv 0(\mathrm{mod}225)$
10	$31x^4+57x^3+96x+191\equiv 0(\mathrm{mod}225)$
11	$2x^4+7x^2-3x-32\equiv 0(\mathrm{mod}208)$
12	$x^4-3x^3+x^2+5x+24\equiv 0(\mathrm{mod}441)$
13	$x^3-4x^2-3x+6\equiv 0(\mathrm{mod}343)$
14	$x^4-3x^3+2x^2-5x-10\equiv 0(\mathrm{mod}175)$
15	$6x^3-7x-11\equiv 0(\mathrm{mod}605)$
16	$x^4+4x^3+2x^2+x+12\equiv 0(\mathrm{mod}1325)$
17	$9x^2+29x+62\equiv 0(\mathrm{mod}196)$
18	$x^3+3x^2-5x+16\equiv 0(\mathrm{mod}225)$
19	$x^5-5x^4-5x^3+25x^2+4x-20\equiv 0(\mathrm{mod}245)$
20	$x^5+3x^4-7x^3+4x^2+4x-10\equiv 0(\mathrm{mod}392)$
21	$x^4-4x^3+2x^2+x+6\equiv 0(\mathrm{mod}275)$
22	$4x^3+7x^2-7x-10\equiv 0(\mathrm{mod}200)$
23	$31x^4+57x^3+96x+191\equiv 0(\mathrm{mod}243)$

24	$2x^4 + 7x^2 - 3x - 32 \equiv 0 (\mathrm{mod} 1225)$
25	$x^4 - 3x^3 + x^2 + 5x + 24 \equiv 0 (\mathrm{mod} 675)$
26	$x^3 - 4x^2 - 3x + 6 \equiv 0 (\mathrm{mod} 482)$
27	$x^4 - 3x^3 + 2x^2 - 5x - 10 \equiv 0 (\mathrm{mod} 1323)$
28	$6x^4 + 7x + 35 \equiv 0 (\mathrm{mod} 675)$
29	$11x^4 - 17x + 125 \equiv 0 (\mathrm{mod} 1225)$
30	$x^5 - 3x^3 + 2x - 14 \equiv 0 (\mathrm{mod} 343)$

ПРИКЛАДИ

Приклад 1. Розв'язати порівняння:

а) $5x \equiv 2 \pmod 8$;

б) $7x \equiv 2 \pmod{13}$.

Розв'язок.

а) Так як (5, 8) = 1, то порівняння має єдиний розв'язок. Знайдемо його за допомогою формули

$$x \equiv b\, a^{\varphi(m)-1} \pmod m .$$

Тоді

$$x \equiv 2 * 5^{\varphi(8)-1}.$$

Відповідь: $x \equiv 2 \pmod *$.

б) Так як (7, 13) = 1, то порівняння

$$7x \equiv 2 \pmod{13}$$

має єдиний розв'язок.

Розв'яжемо це порівняння методом проб, заснованим на властивості повної системи лишків, заставляючи x у формі $7x$ пробігати послідовно значення 0, 1, 2, … , 12.

Встановлюємо, що значення x, які рівні 0, 1, 2, 3, не задовольняють даному порівнянню. Так як порівняння має єдиний розв'язок, то процес знаходження розв'язку закінчений. Порівнянню задовольняє цілий клас чисел за даним модулем; отже, розв'язок порівняння отримуємо у вигляді:

$$x \equiv 4 \pmod{13}.$$

Зауваження. Відмітимо, що метод розв'язку порівняння, заснований на застосуванні теореми Ейлера і малої теореми Ферма, не можна віднести до раціональних методів порівнянь.

В деяких вправах результат може бути отриманий швидше, якщо використовувати штучний прийом, заснований на наступній властивості порівняння: до будь-якої частини порівняння добавити число, кратне модулю. Пояснимо це на прикладах.

а) $5x \equiv 2 \pmod 8$.

Добавимо до правої частини порівняння число 8, рівне модулю, отримаємо:

$$5x \equiv 10 \pmod 8;$$

Поділивши обидві частини порівняння на число 5, взаємно просте з модулем 8, приходимо до результату:

$$x \equiv 2 \pmod 8.$$

б) $7x \equiv 2 \pmod{13}$.

Добавимо до правої частини порівняння число $26 = 13*2$

$$7x \equiv 28 \pmod{13}.$$

Так як $(7, 13) = 1$, то після ділення обох частин порівняння на 7, отримаємо:

$$x \equiv 4 \pmod{13}.$$

Приклад 2. Розв'язати порівняння $115x \equiv 85 \pmod{355}$.

Розв'язок. Так як $(115, 355) = 5$ і 85 ділиться на 5, то дане порівняння має 5 розв'язків.

Скорочуємо обидві частини і модуль на 5:

$$23x \equiv 17 \pmod{71}.$$

Отримане порівняння має єдиний розв'язок:

$$x \equiv 10 \pmod{73},$$

так як

$$23x \equiv 230 \pmod{71}.$$

Отже, дане порівняння має наступні розв'язки:

$$x \equiv 10 \pmod{355},$$
$$x \equiv 81 \pmod{355},$$
$$x \equiv 152 \pmod{355},$$
$$x \equiv 223 \pmod{355},$$
$$x \equiv 294 \pmod{355}.$$

Приклад 3. Знайти числа, які при діленні на 7, 13, 17 дають в залишку відповідно 4, 9 і 1.

Розв'язок. Шукані числа повинні задовольняти системі порівнянь:

$$\begin{cases} x \equiv 4 \pmod 7, & (1) \\ x \equiv 9 \pmod{13}, & (2) \\ x \equiv 1 \pmod{17}. & (3) \end{cases}$$

Так як модулі порівнянь попарно взаємно прості, то ця система має єдиний розв'язок за модулем $M = 7*13*17$.

Перше порівняння має єдиний розв'язок:

$$x = 7t + 4.$$

Підставимо в порівняння (2) замість x вираз $7t + 4$.

Отримаємо:

$$7t + 4 \equiv 9 \pmod{13},$$
$$7t \equiv 5 \pmod{13}.$$

Так як $(7, 13) = 1$, то останнє порівняння має єдиний розв'язок

$t \equiv 10 \pmod{13}$, тобто $t = 10 + 13u$.

Звідки $x = 7(10 + 13u) + 4 = 91u + 74$.

Знайдемо ті значення u, при яких x буде задовольняти і порівнянню (3).

Маємо: $91u + 74 \equiv 1 \pmod{17}$ або $6u \equiv 12 \pmod{17}$.

Звідки $u \equiv 2 \pmod{17}$, отже, $u = 2 + 17k$. І так,

$x = 91(2 + 17k) + 74 = 256 + 1547k$ або $x \equiv 256 \pmod{1547}$.

Приклад 4. Розв'язати систему порівнянь:

$$\begin{cases} 3x \equiv 5 \pmod 7, \\ 2x \equiv 3 \pmod 5, \\ 3x \equiv 3 \pmod 9. \end{cases}$$

Розв'язок. Так як модулі цих порівнянь попарно взаємно прості числа, то дана система має розв'язок за модулем, що є добутком даних модулів, тобто за модулем 315. Звертаючись до коефіцієнтів при невідомому і відповідним модулям, для першого порівняння маємо (3, 7) = 1, для другого (2, 5) = 1, для третього (3, 9) = 3 і, таким чином, перше і друге порівняння мають єдиний розв'язок, третє – 3 розв'язки. Легко установити, що розв'язок даної системи зводиться до розв'язку трьох систем:

$$\begin{cases} x \equiv 4 \pmod 7, \\ x \equiv 4 \pmod 5, \\ x \equiv 1 \pmod 9; \end{cases} \qquad \begin{cases} x \equiv 4 \pmod 7, \\ x \equiv 4 \pmod 5, \\ x \equiv 4 \pmod 9; \end{cases} \qquad \begin{cases} x \equiv 4 \pmod 7, \\ x \equiv 4 \pmod 5, \\ x \equiv 7 \pmod 9. \end{cases}$$

Далі можна знайти усі розв'язки даної системи, розв'язуючи кожну із отриманих трьох систем порівнянь (див. розв'язок попереднього прикладу). Отримаємо наступні розв'язки:

$x \equiv 4 \pmod{315}$, $x \equiv 109 \pmod{315}$, $x \equiv 214 \pmod{315}$.

Розв'язок даної системи можна здійснити значно простіше, а саме: розв'язуючи перше і друге із даних порівнянь, отримаємо:

$x \equiv 4 \pmod 7$, $x \equiv 4 \pmod 5$.

Відмітимо, що ліві і праві частини порівнянь однакові, тому скористаємося властивістю: якщо порівняння має місце за декількома модулями, то це порівняння має місце за модулем, що є найменшим загальним кратним даних модулів, тобто, система двох розглянутих порівнянь рівнозначна порівнянню

$$x \equiv 4 \pmod{35}.$$

Далі можна, знайшовши розв'язок третього порівняння

$x \equiv 1 \pmod 9$, $x \equiv 4 \pmod 9$, $x \equiv 7 \pmod 9$,

перейти до наступних систем:

$$\begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 1 \pmod 9; \end{cases} \qquad \begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 4 \pmod 9; \end{cases} \qquad \begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 7 \pmod 9. \end{cases}$$

Розв'язок кожної із цих систем не визиває труднощів. Відмітимо, система порівнянь

$$\begin{cases} x \equiv 4 (\mathrm{mod}\, 35), \\ x \equiv 4 (\mathrm{mod}\, 9) \end{cases}$$

зразу дає розв'язок

$$x \equiv 4 \ (\mathrm{mod}\ 315).$$

Можна поступити інакше: до вище отриманого розв'язку перших двох порівнянь у вигляді

$$x \equiv 4 \ (\mathrm{mod}\ 35)$$

приєднаємо третє із даних порівнянь

$$3x \equiv 3 \ (\mathrm{mod}\ 9)$$

і, помітивши, що шуканий розв'язок даної системи повинен бути отриманий за модулем 315, послідовно будемо мати:

$x = 35k + 4$, $3\,(35k + 4) \equiv 3 \ (\mathrm{mod}\ 9)$, $105\,k \equiv 0 \ (\mathrm{mod}\ 9)$,

$$6\,k \equiv 0 \ (\mathrm{mod}\ 9).$$

Останнє порівняння має три розв'язки за модулем 9, а саме:

$k \equiv 0 \ (\mathrm{mod}\ 9)$, $k \equiv 3 \ (\mathrm{mod}\ 9)$, $k \equiv 6 \ (\mathrm{mod}\ 9)$.

Отримаємо

$$x = 35 * 9u + 4 = 315u + 4,$$
$$x = 35\,(9u + 3) + 4 = 315u + 109,$$
$$x = 35\,(9u + 6) + 4 = 315u + 214$$

або відповідно

$x \equiv 4 \ (\mathrm{mod}\ 315)$, $x \equiv 109 \ (\mathrm{mod}\ 315)$, $x \equiv 214 \ (\mathrm{mod}\ 315)$.

Зупинимося ще на одному прийомі розв'язку системи порівнянь.

Приклад 5. Розв'язати систему порівнянь:

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 25). \end{cases}$$

Розв'язок. Відмітимо, що дані модулі, тобто, числа 15 і 25 не є взаємно простими. В цьому випадку необхідно спочатку переконатися в існуванні розв'язків.

Якщо задана система порівнянь:

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ x \equiv c_2 (\mathrm{mod}\, m_2). \end{cases}$$

де $(m_1, m_2) = a > 1$, то ця система буде мати розв'язок при умові:

$$c_1 \equiv c_2 \ (\mathrm{mod}\ a).$$

Повертаючись до даної системи порівнянь, маємо:

(15, 25), $2 \equiv 7 \ (\mathrm{mod}\ 5)$, тобто дана система сумісна.

Із першого порівняння отримаємо:

$$x \equiv 15t + 2;$$

підставивши це значення у друге порівняння, приходимо до порівняння

$$15t + 2 \equiv 7 \ (\mathrm{mod}\ 25),$$

тобто

$$15t \equiv 5 \pmod{25}.$$

Після скорочення обох частин порівняння і модуля на 5 отримаємо:

$$3t \equiv 1 \pmod 5),$$
$$3t \equiv 6 \pmod 5),$$
$$t \equiv 2 \pmod 5),$$
$$t = 5k + 2;$$

тепер знаходження розв'язку даної системи порівнянь не визиває складності:

$$x = 15t + 2 = 15 (5k + 2) + 2 = 75k + 32,$$
$$x \equiv 32 \pmod{75}.$$

Знайдений розв'язок є єдиним, що виходить із єдиності розв'язку кожного із порівнянь даної системи.

Правильність отриманого розв'язку може бути легко перевірена його підстановкою в кожне із порівнянь даної системи.

Зауваження. Розглянемо прийом розв'язку, який, на наш погляд, є раціональним в цілому ряду випадків.

Дана система порівнянь:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}, \\ a_2 x \equiv b_2 \pmod{m_2}, \end{cases} \qquad (1)$$

де $(m_1 m_2) = (a_1, m_1) = (a_2, m_2) = 1$. Цю систему замінимо еквівалентною їй системою:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \end{cases} \qquad (2)$$

де перше і друге із порівнянь системи (2) являються відповідно розв'язками першого і другого порівнянь системи (1).

Від системи (2) перейдемо до системи

$$\begin{cases} m_2 x \equiv m_2 c_1 \pmod{m_1 * m_2}, \\ m_1 x \equiv m_1 c_2 \pmod{m_1 * m_2}. \end{cases} \qquad (3)$$

Покажемо еквівалентність системи порівнянь (2) і системи порівнянь (3).

Нехай x_1 - будь-який розв'язок системи порівнянь (2) за модулем $m_1 * m_2$. Тоді справедлива наступна система порівнянь:

$$\begin{cases} x_1 \equiv c_1 \pmod{m_1}, \\ x_1 \equiv c_2 \pmod{m_2}, \end{cases}$$

яка після перемноження обох частин порівнянь і модулів відповідно на m_2 і m_1 приводить до справедливих порівнянь:

$$\begin{cases} m_2 x_1 \equiv m_2 c_1 \pmod{m_1 * m_2}, \\ m_1 x_1 \equiv m_1 c_2 \pmod{m_1 * m_2}, \end{cases}$$

звідки x_1 - розв'язок системи порівнянь (3) за модулем $m_1 * m_2$. Обернено, якщо x_2 - будь-який розв'язок системи порівнянь (3) за модулем $m_1 * m_2$, то справедлива наступна система порівнянь:

$$\begin{cases} m_2\, x_2 \equiv m_2\, c_1 \,(\mathrm{mod}\, m_1 * m_2), \\ m_1\, x_2 \equiv m_1\, c_2 \,(\mathrm{mod}\, m_1 * m_2). \end{cases}$$

Отже,

$$\begin{cases} x_2 \equiv c_1 \,(\mathrm{mod}\, m_1), \\ x_2 \equiv c_2 \,(\mathrm{mod}\, m_2) \end{cases}$$

і x_2 - розв'язок системи порівнянь (2) за модулем $m_1 m_2$,

Таким чином, системи порівнянь (2) і (3) еквівалентні, а так як система порівнянь (2) має єдиний розв'язок за модулем $m_1 * m_2$, то і система порівнянь (3) також має єдиний розв'язок.

При розв'язуванні системи порівнянь розглянутим способом у випадку попарно взаємно простих модулів немає необхідності заміняти систему (1) системою (2).

Приклад. Розв'язати систему порівнянь:

$$\begin{cases} 3x \equiv 5 \,(\mathrm{mod}\, 7), \\ 2x \equiv 1 \,(\mathrm{mod}\, 5). \end{cases}$$

Розв'язок: Так як (3, 7) = (2, 5) = 1, то кожне із порівнянь має єдиний розв'язок; (7, 5) = 1 і, отже, дана система має єдиний розв'язок за модулем 35.

Від даної системи переходимо до системи порівнянь

$$\begin{cases} 15x \equiv 25 \,(\mathrm{mod}\, 35), \\ 14x \equiv 7 \,(\mathrm{mod}\, 35) \end{cases}$$

і, віднімаючи із першого порівняння друге, отримуємо шуканий розв'язок:

$$x \equiv 18 \,(\mathrm{mod}\, 35).$$

Застосуємо розглянутий прийом до деяких розв'язаних вище задач.

Приклад. Розв'язати систему порівнянь:

$$\begin{cases} 3x \equiv 5 \,(\mathrm{mod}\, 7), \\ 2\,x \equiv 3 \,(\mathrm{mod}\, 5), \\ 3x \equiv 3 \,(\mathrm{mod}\, 9). \end{cases}$$

Розв'язок: Як встановлено вище, система сумісна і має три розв'язки за модулем 315. Отримаємо систему:

$$\begin{cases} 135x \equiv 225 \,(\mathrm{mod}\, 315), \\ 126x \equiv 189 \,(\mathrm{mod}\, 315), \\ 105x \equiv 105 \,(\mathrm{mod}\, 315). \end{cases}$$

Перші два порівняння дають

$$9x \equiv 36 \,(\mathrm{mod}\, 315).$$

Перемножуючи обидві частини порівняння на 11, де (11, 315) = 1, маємо:

$$99x \equiv 396 \,(\mathrm{mod}\, 315),$$

Віднімаючи отримане порівняння із порівняння

$$105x \equiv 105 \,(\mathrm{mod}\, 315),$$

приходимо до порівняння:

$$6x \equiv 24 \,(\mathrm{mod}\, 315),$$

а так як $(2, 315) = 1$, то отримуємо:

$$3x \equiv 12 (\mathrm{mod}\, 315).$$

Знайдені розв'язки:

$$x \equiv 4 (\mathrm{mod}\, 315), \quad x \equiv 109 (\mathrm{mod}\, 315), \quad x \equiv 214 (\mathrm{mod}\, 315).$$

Приклад. Розв'язати систему порівнянь:

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 25). \end{cases}$$

Розв'язок: Вище було установлено, що дана система має єдиний розв'язок за модулем 75.

Переходимо до системи порівнянь:

$$\begin{cases} 5x \equiv 10 (\mathrm{mod}\, 75), \\ 3x \equiv 21 (\mathrm{mod}\, 75), \end{cases}$$

Звідки

$$2x \equiv -11 (\mathrm{mod}\, 75),$$
$$2x \equiv 64 (\mathrm{mod}\, 75),$$

так як $(2, 75) = 1$, то

$$x \equiv 32 (\mathrm{mod}\, 75)$$

являється шуканим розв'язком.

Приклад 6. Розв'язати порівняння $17x \equiv 7 (\mathrm{mod}\, 30)$.

Розв'язок. Модулем порівняння є складене число 30, канонічним розкладанням якого буде: $30 = 2*3*5$. Отже, розв'язок даного порівняння можна привести до розв'язку системи:

$$\begin{cases} 17x \equiv 7 (\mathrm{mod}\, 2), \\ 17x \equiv 7 (\mathrm{mod}\, 3), \\ 17x \equiv 7 (mos 5). \end{cases} \qquad (1)$$

Розв'язок останньої системи пропонуємо знайти читачу. Розв'язком буде $x \equiv 11 (\mathrm{mod}\, 30)$. Рекомендуємо читачу розв'язати дане порівняння, не приводячи його до системи порівнянь.

Приклад 7. За допомогою критерію Ейлера серед чисел 3, 5, 7 і 9 знайти квадратичні лишки за модулем 13.

Розв'язок. Бачимо, що кожне із даних чисел взаємно просте з модулем, а тому критерій Ейлера можна застосувати.

Як відомо, якщо $(a, p) = 1$ і $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$, то a - квадратичний лишок за модулем p.

В даному прикладі маємо:

$$3^6 = (27)^2 \equiv 1 (\mathrm{mod} 13);$$
$$5^6 = (25)^3 \equiv (-1)^3 \equiv -1 (\mathrm{mod} 13);$$
$$7^6 = (49)^3 \equiv (-3)^3 \equiv -1 (\mathrm{mod} 13);$$
$$9^6 \equiv (-4)^6 \equiv 16^3 \equiv 3^3 \equiv 1 (\mathrm{mod} 13).$$

Отже, числа 3 і 9 являються квадратичними лишками, а 5 і 7 – квадратичними нелишками за модулем 13.

Приклад 8. Показати, що непарне число, взаємно просте з числом 10, піднесене до тридцятого степеня, може закінчуватися лише цифрами 1 і 9.

Розв'язок. Якщо x – шукане число, то розв'язок зведеться до знаходження числа a в якості найменшого невід'ємного лишка за модулем 10 в порівнянні

$$x^{30} \equiv a \pmod{10},$$

де $(x, 10) = 1$ (за умовою задачі), $(a, 10) = 1$ (за властивістю порівнянь).

Так як $(x, 10) = 1$, $\varphi(10) = 4$, то на підставі теореми Ейлера справедливе порівняння

$$x^4 \equiv 1 \pmod{10}.$$

Якщо звести обидві частини до сьомого степеня, отримаємо порівняння:

$$x^{28} \equiv 1 \pmod{10}.$$

На підставі останнього порівняння і порівняння

$$x^{30} \equiv a \pmod{10}$$

приходимо до порівняння

$$x^2 \equiv a \pmod{10},$$

де $(a, 10) = 1$.

Залишається знайти квадратичні лишки за модулем 10, якими являються числа 1, 9, в чому можна переконатися, перевіривши, що із порівнянь

$$x^2 \equiv 1 \pmod{10},$$
$$x^2 \equiv 9 \pmod{10},$$
$$x^2 \equiv 3 \pmod{10},$$
$$x^2 \equiv 7 \pmod{10}$$

тільки перших два мають розв'язок відповідно:

$$x \equiv 1;\ 9 \pmod{10},$$
$$x \equiv 3;\ 7 \pmod{10}.$$

Приклад 9. Розв'язати порівняння:

$$5x^2 + x - 4 \equiv 0 \pmod{11}.$$

Розв'язок. Перемножимо обидві частини порівняння на число 20, де $(20, 11) = 1$, отримаємо порівняння:

$$100x^2 + 20x - 80 \equiv 0 \pmod{11}$$

або

$$(10x + 1)^2 \equiv 81 \pmod{11}.$$

Позначимо $10x + 1$ через z. Отже, $z^2 \equiv 81 \pmod{11}$ або $z^2 \equiv 4 \pmod{11}$.

Розв'яжемо це порівняння методом проб. Перевіряючи числа 0, 1, 2, …, 10, бачимо, що порівняння має розв'язок: $z = 2$ і $z = 9$, тобто задовольняється при $z = 2 + 11t$ і $z = 9 + 11t$.

Так як z = 10x, то $x = \frac{z-1}{10}$, тобто

$$x_1 \equiv \frac{11t+1}{10}, \qquad x_2 \equiv \frac{11t+8}{10};$$

При $t = 9$ маємо $x_1 = 10$ і при $t = 2$ отримуємо $x_2 = 3$.

Отже, це порівняння має розв'язки 3 і 10, тобто , йому задовольняють цілі числа виду: $x = 3 + 11t$, $x = 10 + 11t$.

Відповідь:

$$x \equiv 3 (\mathrm{mod} 11),$$
$$x \equiv 10 (\mathrm{mod} 11).$$

Приходячи до необхідності розв'язку порівняння

$$z^2 \equiv 81 (\mathrm{mod} 11),$$

отримуємо очевидний розв'язок $z \equiv 9 (\mathrm{mod} 11)$, а на підставі однієї із властивостей двочленних порівнянь отримуємо другий розв'язок $z \equiv 11 - 9 (\mathrm{mod} 11)$, тобто, $z \equiv 2 (\mathrm{mod} 11)$.

Далі, як вказано вище.

Цілочисельні розв'язки лінійних рівнянь

Розглянемо деякі положення теорії чисел, які є більшою мірою алгеброю. Почнемо із знаходження розв'язків рівнянь алгебри. Використовуючи алгоритм Евкліда, можна знайти цілочисельні розв'язки рівняння $ax + by = c$, якщо вони існують. Наведене нижче твердження було раніше доведене і наводиться тут ще раз для зручності викладення.

Теорема

Рівняння $ax + by = c$, де a, b і c - цілі числа, має цілочисельний розв'язок (тобто існують цілі числа x і y такі, що $ax - by = c$) тоді і тільки тоді, коли c ділиться на НСД(a, b). Якщо c ділиться на НСД(a, b), то розв'язком рівняння а $ax - by = c$ є пара чисел

$$x_0 = \frac{uc}{\text{НСД}(a,b)}, \quad y_0 = \frac{vc}{\text{НСД}(a,b)},$$

де u і v - будь-який розв'язок рівняння НСД(a, b) = $au+bv$.

Приклад 1

Знайти розв'язок рівняння $85x + 34y = 51$. Розв'язок має вигляд

$$x_0 = \frac{uc}{\text{НСД}(a,b)} = \frac{1*51}{17}, \quad y_0 = \frac{vc}{\text{НСД}(a,b)} = \frac{(-2)*51}{17}.$$

Для перевірки обчислимо

$$ax_0 + by_0 = 85 \cdot 3 + 34 \cdot (-6) = 255 + (-204) = 51.$$

Інший спосіб побудови розв'язку полягає у безпосередньому використанні рівняння $au + bv$ = НСД(a, b). Оскільки

$au + bv$ = НСД(a, b) або $a \cdot (1) + b \cdot (-2) = 17$,

то, помноживши на 3, одержуємо $a \cdot (3) + b \cdot (-6) = 51$. Помічаючи, що при $x = 5$ і $y = -11$ $85 \cdot 5 + 34 \cdot (-11) = 425 + (-374) = 51$,
приходимо до висновку, що може існувати більше одного розв'язку.

Приклад 2

Розв'язати рівняння $252x + 580y = 20$

НСД(252,580) = 4 і (252)(-23) + (580)(10) = 4. Помноживши кожен доданок на 5, одержуємо (252)(-115) + (580)(50) = 20.
Отже, $x = -115$ і $y = 50$ є розв'язком.
Тепер у нас є можливість визначати, чи існує розв'язок, і знаходити частковий розв'язок для рівняння $ax + by = c$, якщо розв'язок існує. Теорема, наведена нижче, дає можливість знаходити всі розв'язки рівняння.

Теорема

Якщо a і b - ненульові цілі числа і (x_0,y_0) - розв'язок рівняння $ax + by = c$,
тоді будь-який інший розв'язок (x,y) має вигляд

$$x = x_0 + \frac{b}{d}\,t, \quad y = y_0 \frac{a}{d}\,t,$$

де t - довільне ціле число, а d = НСД(a,b).

Доведення

Якщо (x,y) і (x_0,y_0) є розв'язками рівняння

$ax + by = c$, то $ax + by = ax_0 + by_0$.

Тому $ax - ax_0 = by_0 - by$ і $a(x - x_0) = b(y_0 - y)$.

Поділивши обидві частини співвідношення на d = НСД(a,b), маємо $\frac{a}{d}\ (x - x_0) = \frac{b}{d}\ (y_0 - y)$.

Оскільки НСД $(\frac{a}{d}, \frac{b}{d}) = 1$, одержуємо, що $\frac{a}{d}\ (y_0 - y)$ і $\frac{b}{d}\ (x - x_0)$,

скажемо, $x - x_0 = u$ $(\frac{b}{d})$ і $y_0 - y = v$ $(\frac{a}{d})$.

Тоді, $(\frac{a}{d})\ u\ (\frac{b}{d}) = (\frac{b}{d})\ v\ (\frac{a}{d})$ і звідси після скорочення $u = v$.

Поклавши $t = u = v$, одержуємо $x = x_0 + t$ і $y = y_0 - t$.

Розв'язки конгруенцій

Вище розглядалися рівняння виду $ax + by = c$, що мають як розв'язки цілі числа x і y. У окремому випадку $b = 0$ можна знаходити розв'язки рівняння $ax \equiv c$. Тепер шукатимемо розв'язки конгруенцій $ax \equiv c \pmod n$ у тому значенні, що треба знайти таке ціле число x, при якому ціле число ax конгруентно c по модулю n. Або, на мові класів еквівалентності, для класів еквівалентності $[a]$ і $[c]$ по

модулю n, знайти клас еквівалентності $[x]$ такий, що $[a] \otimes [x] = [c]$, де ця рівність означає рівність множин.

Використовуючи таблицю множення для Z_5 ,

$[a] \otimes [x]$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

можна знайти розв'язки конгруенції $3x \equiv 1 (\text{mod } 5)$, розглядаючи (по модулю 5) $[3] \otimes [x] = [1]$.

Аналіз таблиці множення показує, що $[x] = [2]$ буде розв'язком, оскільки $[3] \otimes [2] = [1]$. Тому можна покласти $x = 2$. Оскільки $[2] = \{..., -8, -3, 2, 7, 12,...\}$, відзначаємо, що кожне число з сукупності $x = -3$, $x = 7$ і $x = -8$ є тим значенням x, яке задовольняє $3x \equiv 1 (\text{mod } 5)$.

Теорема

а) Якщо $a \equiv b$ (mod n) і $c \equiv d$ (mod n), то $a + c \equiv b+d$ (mod n) і $ac = bd$ (mod n).
б) Якщо $ac \equiv be$ (mod n) і НОД(c,n)$\equiv$ 1, то $a \equiv b$ (mod n).
в) Якщо $a \equiv b$ (mod n), то $am \equiv bm$ (mod n) для всіх цілих додатних чисел m.
г) Якщо $a \equiv b$ (mod mn), то $a \equiv b$(mod m) і $a \equiv b$(mod n).
д) Для c=0 співвідношення $ac \equiv be$ (mod n) має місце тоді і тільки тоді, коли $a \equiv b$(mod).
е) Якщо $a \equiv b$(mod m), $a \equiv b$ (mod n) і НСД(m,n)= 1, то $a \equiv b$ (mod mn).

Доведення

Також згідно цій теоремі, розв'язок має вигляд $x_0 = \frac{u*c}{\text{НСД}\,(a,m)}$, $y_0 = \frac{t*m}{\text{НСД}\,(a,m)}$, де u і v вибрані таким чином, що $au + mv$ = НСД(a, m). За вище наведеною теоремою всі розв'язки мають вигляд

$$x = x_0 = \frac{t*m}{\text{НСД}\,(a,m)},$$

де t - довільне ціле число. У даному випадку необхідний розв'язок тільки для x. Таким чином, всі цілочисельні розв'язки $ax \equiv c$ (mod m) мають вигляд

$$x = x_0 = \frac{t*m}{\text{НСД}\,(a,m)},$$

де t - будь-яке ціле число.

Наступна теорема надає різні розв'язки конгруенцій $ax \equiv c$ (mod m). Оскільки існує скінченне число класів еквівалентності по модулю m, може

існувати тільки скінченне число різних розв'язків по модулю m. Всі вони дані в наведеній нижче теоремі. Доведення теореми проведіть самостійно.

Теорема

Якщо НСД(a,m) | c ,то $ax \equiv c \pmod m$ має скінченне число різних розв'язків по модулю m. Ці розв'язки мають вигляд

$$x_0 = \frac{t*m}{\text{НСД}\ (a,m)}$$

по модулю

$$m = [[x_0 + \frac{t*m}{\text{НСД}\ (a,m)}]]_m$$

для t = 1,2,3,..., НСД(a,m), де для x_0 існує таке y_0, що (x_0, y_0) є розв'язком рівняння $ax + my = c$.

Приклад 1

Внаслідок того, що НСД(35,84) = 7 і 7 | 14, конгруенція $35\text{-}x \equiv 14 \pmod{84}$ має в точності 7 різних розв'язків по модулю 84, які мають вигляд

$$x_0 + \frac{84 \cdot t}{7} = x_0 + 12 \cdot t$$

де t = 1,2,3,..., 7 і (x_0,y_0) є розв'язком $35x + 84y = 14$, яке рівносильне $5x + 12y = 2$. Перевірка дає у якості розв'язку $x_0 = -2$ і $y_0 = 1$. Сім різних розв'язків по модулю 84 мають наступний вигляд.

t	$x_0 + 12t$
1	$-2 + 12 \cdot 1 = 10$
2	$-2 + 12 \cdot 2 = 22$
3	$-2 + 12 \cdot 3 = 34$
4	$-2 + 12 \cdot 4 = 46$
5	$-2 + 12 \cdot 5 = 58$
6	$-2 + 12 \cdot 6 = 70$
7	$-2 + 12 \cdot 7 = 82$

Приклад 2

Коли НСД(a,m) = 1, існує єдиний розв'язок конгруенції $ax \equiv c \pmod m$. Наприклад, розглянемо конгруенцію $6x \equiv 7 \pmod{55}$, НОД(6,55) = 1, і, очевидно, 1 ділить 7. Тому існує тільки один розв'язок по модулю 55, який має вигляд

$$x_0 + \frac{t*m}{\text{НСД}(6,55)} = x_0 + \frac{1*55}{1} = x_0 + 55 \equiv x_0 \pmod{55},$$

де (x_0, y_0) - розв'язок рівняння $ax + my = c$ або $6x + 55y = 7$. Для знаходження x_0 і y_0 проведемо перебір з поверненням по алгоритму Евкліда, як показано у прикладах, наведених вище, одержуючи при цьому
$6(-9) + 55(1) = 1 = \text{НОД}(6, 55)$.
Помноживши кожен доданок на 7, одержуємо $6(-63) + 55(7) = 7$,
так що $x_0 = -63$ і $x = -63 + 55 = -8$.

Приклад 3

Розв'язати конгруенцію $623x \equiv -406 \pmod{84}$. Число 623 більше, ніж модуль конгруенції 84, а -406 є від'ємним. Оскільки розшукуються розв'язки за модулем 84, обираємо цілі числа у діапазоні 0, 1, 2, ..., 83, оскільки вони є можливими лишками при діленні на 84 і простими представниками класів еквівалентності, породжених конгруенцією за модулем 84. Використовуючи алгоритм ділення, одержуємо $623 = 84 \cdot 7 + 35$, так що $623 \equiv 35 \pmod{84}$;
$-406 = 84(-5) + 14$, так що $-406 \equiv 14 \pmod{84}$.
Таким чином, $35x \equiv 14 \pmod{84}$ рівносильне початковому $623x \equiv -406 \pmod{84}$. Розв'язок конгруенції $35x \equiv 14 \pmod{84}$ було знайдено у попередньому прикладі.

Теорема

Якщо $a \equiv b \pmod{n_1}$, $a \equiv b \pmod{n_2}$, ..., $a \equiv b \pmod{n_k}$ = НСК($n_1, n_2, \ldots, n_k$), то $a \equiv b \pmod{n}$, і обернено.

Практична робота №13

Тема: Первісні (примітивні) корені.
Мета: Розглянути загальні визначення і теореми про порядок числа та первісні корені, властивості показника δ, дослідити існування первісних коренів за елементарними модулями, навчитися знаходити первісні корені за елементарними модулями.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

За простим модулем p *зведена* система лишків складається із усіх лишків *повної* системи, окрім лишка 0. Кількість лишків зведеної системи за модулем p становить $\varphi(p) = p - 1$. За складеним модулем m зведені системи лишків мають у собі $\varphi(m)$ лишків повної системи, взаємно простих з m.

Загальні визначення і теореми про порядок числа та первісні корені

Візьмемо за модуль довільне ціле число m.

Для будь-якого цілого a із зведеної системи лишків за модулем m ($a \in Z_{\varphi(m)}$) існує хоча б одне додатне ціле число k, таке, що $a^k \equiv 1 (\mathrm{mod} m)$. Наприклад, $k = \varphi(m)$ – за теоремою Ейлера.

Визначення. Якщо для даного числа a існує декілька таких чисел $k_1, k_2, \ldots, k_s$, то найменше з них $\delta = \min(k_1, k_2, \ldots, k_s)$ називається *показником*, якому a належить за модулем m або *порядком числа* a за модулем m. Позначається це число так:

$$\delta = ord(a)_m, \ a \in Z_{\varphi(m)}. \qquad (13.1)$$

У разі, коли $(a, m) \neq 1$, тобто a належить до повної системи лишків за модулем m і не належить зведеній системі, порядок числа a за модулем m будемо визначати, як нескінченний:

$$ord(a) = \infty, \ a \in Z_m, \ (a, m) \neq 1. \qquad (13.2)$$

Властивості показника $\delta = ord(a)_m$

Теорема 1.

Якщо δ є порядком числа a за модулем m, то числа $a^0 = 1, a^1, \ldots, a^{\delta - 1}$ за цим самим модулем неконгруентні.

Доведення. Дійсно, якщо $a^l \equiv a^k (\mathrm{mod} m),\ 0 < k < l < \delta$, то $a^{l-k} \equiv 1(\mathrm{mod} m),\ l-k < \delta$, що суперечить визначенню δ (1).■

Теорема 2.

Якщо $\delta = ord(a)_m$, то необхідною і достатньою умовою $a^k \equiv a^l (\mathrm{mod} m)$ є $k \equiv l(\mathrm{mod}\,\delta)$, зокрема (якщо $l = 0$), $a^k \equiv 1(\mathrm{mod} m) \Leftrightarrow \delta | k$.

Теорема 3.

Нехай a за модулем m має порядок δ. Тоді $\varphi(m)$ ділиться на δ.

Таким чином, порядок довільного цілого числа a за модулем m є дільником функції Ейлера $\varphi(m)$ модуля m. Найбільшим із дільників є сама функція Ейлера $\varphi(m)$.

Приклад 1. Визначимо, до якого показника належить кожне число із зведеної системи за модулем 7.

Розв'язання.

Зведена система найменших додатних лишків для $\mathrm{mod}\,7: 1,2,3,4,5,6$.

Число 1 конгруентне саме до себе (рефлексивність), тобто порядок числа 1 за модулем 7 буде $1 - ord(1)_7 = 1$.

Розглянемо інші лишки.

Число 2:

$2^1 = 2;\ 2^2 = 4;\ 2^3 = 8 \equiv 1(\mathrm{mod}\,7);\ 2^4 = 16 \equiv 2(\mathrm{mod}\,7);$

$2^5 = 32 \equiv 4(\mathrm{mod}\,7);\ 2^6 = 64 \equiv 1(\mathrm{mod}\,7).$

Для лишка 2 отримали два степеня, в яких число 2 конгруентне 1 за модулем 7 – це $k_1 = 3,\ k_2 = 6;\ \min(3,6) = 3$. Тобто, число 2 за модулем 7 належить показнику 3 або $ord(2)_7 = 3$.

Примітка. $\varphi(7) = 6$, тобто $k_2 = 6$ в отриманій множині є значенням функції Ейлера для модуля 7. Порядок числа 2 за модулем 7 менший, ніж функція Ейлера, і є її дільником.

Число 3:

$3^1 = 3;\ 3^2 = 9 \equiv 2(\mathrm{mod}\,7);\ 3^3 = 27 \equiv 6(\mathrm{mod}\,7);\ 3^4 = 81 \equiv 4(\mathrm{mod}\,7);$

$2^5 = 243 \equiv 5(\mathrm{mod}\,7);\ 3^6 = 729 \equiv 1(\mathrm{mod}\,7).$

Для лишка 3 отримали тільки один степінь – $6 = \varphi(7)$, в якому 3 конгруентне 1 за модулем 7. Число 3 за модулем 7 належить показнику 6, або $ord(3)_7 = 6 = \varphi(7)$.

Число 4:

$4^1 = 4;\ 4^2 = 16 \equiv 2(\mathrm{mod}\,7);\ 4^3 = 64 \equiv 1(\mathrm{mod}\,7);\ 4^4 = 256 \equiv 4(\mathrm{mod}\,7);$

$4^5 = 1024 \equiv 2(\mathrm{mod}\,7);\ 4^6 = 4096 \equiv 1(\mathrm{mod}\,7).$

Для лишка 4 отримали два степеня, в яких 4 конгруентне 1 за модулем 7 – це $k_1 = 3,\ k_2 = 6;\ \min(3,6) = 3$. Тобто, число 4, як і число 2, за модулем 7 належить

показнику 3 або $ord(4)_7 = 3$. Порядок числа 4 за модулем 7 менший, ніж функція Ейлера, і є її дільником.

Число 5:

$5^1 = 5;\ 5^2 = 25 \equiv 4(\mathrm{mod}7);\ 5^3 = 125 \equiv 6(\mathrm{mod}7);\ 5^4 = 625 \equiv 2(\mathrm{mod}7);$

$5^5 = 3125 \equiv 3(\mathrm{mod}7);\ 5^6 = 15625 \equiv 1(\mathrm{mod}7).$

Для лишка 5 отримали тільки один степінь – $6 = \varphi(7)$, в якому 5 конгруентне 1 за модулем 7. Число 5 за модулем 7 належить показнику 6, або $ord(5)_7 = 6 = \varphi(7)$.

Число 6:

$6^1 = 6;\ 6^2 = 36 \equiv 1(\mathrm{mod}7);\ 6^3 = 216 \equiv 6(\mathrm{mod}7);\ 6^4 = 1296 \equiv 1(\mathrm{mod}7);$

$6^5 = 7776 \equiv 6(\mathrm{mod}7);\ 6^6 = 46656 \equiv 1(\mathrm{mod}7).$

Для лишка 6 отримали три степеня, в яких 6 конгруентне 1 за модулем 7 – це $k_1 = 2,\ k_2 = 4,\ k_3 = 6;\ \min(2,4,6) = 2$. Тобто число 6 за модулем 7 належить показнику 2, або $ord(6)_7 = 2$. Порядок числа 6 за модулем 7 менший, ніж функція Ейлера, і є її дільником.

Відповідь: за модулем 7 у зведеній системі найменших додатних лишків два лишки – 3 і 5 мають порядок, який співпадає із значенням функції Ейлера, а саме: $ord(3)_7 = ord(5)_7 = 6$. Числа 2, 4, 6 мають порядок, менший за функцію Ейлера: $ord(2)_7 = 3,\ ord(4)_7 = 3,\ ord(6)_7 = 2$. Усі отримані порядки є дільниками функції Ейлера для числа 7.

Визначення. Числа a, порядок яких дорівнює $\varphi(m)$ (тобто, $\delta = \varphi(m)$, якщо такі числа існують), називаються *первісними коренями* за модулем m.

Дослідження існування первісних коренів за елементарними модулями

Визначення. Будемо називати модулі $p, p^\alpha, 2p^\alpha, 2^\alpha\ (\alpha \geq 2)$ елементарними модулями.

Елементарні модулі p^α та $2p^\alpha$

Нехай p – просте непарне число, $\alpha > 1$. Доведемо існування первісних коренів за модулями p^α та $2p^\alpha$, розглянувши попередньо три допоміжні теореми.

Теорема 4.

Якщо $ab = ord(x)_m$, то $b = ord(x^a)_m$.

Теорема 5.

Якщо $a = ord(x)_m,\ b = ord(y)_m,\ (a,b) = 1$, то $ab = ord(xy)_m$.

Теорема 6.

Існують первісні корені за модулем p.

Доведення. Нехай $\Delta = \{\delta_1, \delta_2, ..., \delta_r\}$ – множина всіх різних показників, яким належать числа $1, 2, ..., (p-1)$ за модулем p.■

Нехай $\tau = НСК(\delta_1, \delta_2, ..., \delta_r)$ і $\tau = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot ... \cdot q_k^{\alpha_k}$ – його канонічне подання.

Кожен множник $q_s^{\alpha_s}$ цього подання ділить хоча б одне число δ_j з множини Δ, відповідно це число може бути подано у вигляді: $\delta_j = t_j \cdot q_s^{\alpha_s}$, $t_j \in Z$. Нехай a_j – одне з тих чисел множини $1,2,...,(p-1)$, які належать показнику δ_j. Згідно з теоремою 1 число $n_j = a_j^{t_j}$ належить показнику $q_s^{\alpha_s}$. Згідно з теоремою 2 добуток $g = n_1 \cdot n_2 \cdot ... \cdot n_k$ належить показнику $\tau = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot ... \cdot q_k^{\alpha_k}$. Отже, згідно з теоремою 3 τ ділить $\varphi(p) = p-1$, тобто $\tau \le p-1$.

Але оскільки числа з множини Δ ділять $\tau = НСК(\delta_1, \delta_2, ..., \delta_r)$, всі числа $1,2,...,(p-1)$ є розв'язками конгруенції $x^\tau \equiv 1 (\mathrm{mod}\, p)$. Отже, будемо мати $p-1 \le \tau$. Звідси, $\tau = p-1$, та $g = n_1 \cdot n_2 \cdot ... \cdot n_k$ – первісний корінь.

Теорема 7.

Нехай g – первісний корінь за модулем p $(p \ge 3)$, тобто $ord(g)_p = p-1$. Згідно з властивостями конгруенцій $(g + p \cdot t)^{p-1} = p \cdot q + 1$, $t, q \in Z$. Серед множини чисел t можна зазначити таке, для якого $(p, q) = 1$. Для такого t число $g + p \cdot t$ буде первісним коренем за модулем p^α для будь-яких $\alpha > 1$.

Теорема 8 (узагальнення для модуля p^α).

Степінь p^α простого непарного числа p завжди має первісні корені. Кількість таких коренів дорівнює $\varphi(\varphi(p^\alpha))$. Кожний первісний корінь g модуля p породжує $\varphi(p^{\alpha-1})$ неконгруентних між собою первісних коренів за модулем p^α. Первісний корінь g модуля p буде первісним коренем модуля p^α тільки в тому випадку, коли число $g^{p-1} - 1$ ділиться на p і не ділиться на p^2.

Висновки з теорем 7, 8.

Висновок 1. Якщо g – первісний корінь за простим непарним модулем p, то або g, або $g + pt$, $t \in Z$ є первісним коренем за модулем p^2.

Висновок 2. Якщо g – первісний корінь за модулем p^2 (p – просте непарне число), то g є первісним коренем за модулем p^α, $\forall \alpha > 2$.

Теорема 9.

Нехай $\alpha \ge 1$ та g – первісний корінь за модулем p^α. Непарне g_0 з двох чисел g та $g + p^\alpha$ буде первісним коренем за модулем $2p^\alpha$.

Елементарний модуль 2^α

Нехай $\alpha = 1$, тоді $2^\alpha = 2$. Маємо $\varphi(2) = 1$. Зведена система лишків за модулем 2 дорівнює $\{1\}$. Цей лишок є первісним коренем за модулем 2.

Нехай $\alpha = 2$, тоді $2^\alpha = 4$. Маємо $\varphi(4) = 2$. Зведена система лишків за модулем 4 має вигляд $\{\pm 1\}$. Первісними коренями за модулем 4 будуть обидва лишка, оскільки $(\pm 1)^2 = 1 (\mathrm{mod}\, 4)$.

Для $\alpha \ge 3$ справедливою буде теорема 10.

Теорема 10.
Для довільного числа a, такого, що $(2,a)=1$, і довільного степеня $\alpha \geq 3$ порядок числа a за модулем 2^α не перевищує $2^{\alpha-2}$, тобто $ord(a)_{2^\alpha} \leq 2^{\alpha-2}$.

Наслідок із теореми 10.
Оскільки $\varphi(2^\alpha)=2^{\alpha-1}$ і порядок довільного непарного числа для усіх модулів 2^α, $\alpha \geq 3$ менший, ніж $\varphi(2^\alpha)=2^{\alpha-1}$, робимо висновок, що за модулем типу 2^α, $\alpha \geq 3$ первісних коренів немає.

Теорема 11.
Первісні корені за модулем m існують тоді і тільки тоді, коли $m=p^\alpha$; $m=2p^\alpha$ (p – просте непарне, α – довільне ціле), а також $m=2$; $m=4$.

Знаходження первісних коренів за елементарними модулями

Первісні корені за модулями p^α та $2p^\alpha$, де p – просте непарне число і $\alpha \geq 0$, можна знайти, користуючись загальною теоремою 12.

Теорема 12.
Нехай $\Phi=\varphi(m)$ та $\{q_1,q_2,...,q_k\}$ – різні нетривіальні прості дільники числа Φ. Для того щоб число g, взаємно просте з m, було первісним коренем за модулем m, необхідно та достатньо, щоб g не задовольняло ні одну з конгруенцій

$$g^{\frac{\Phi}{q_1}} \equiv 1(\mathrm{mod}\, m);\ g^{\frac{\Phi}{q_2}} \equiv 1(\mathrm{mod}\, m);\ g^{\frac{\Phi}{q_3}} \equiv 1(\mathrm{mod}\, m);\ ...;\ g^{\frac{\Phi}{q_k}} \equiv 1(\mathrm{mod}\, m). \qquad (13.3)$$

Доведення. Дійсно, якщо g є первісним коренем за модулем m, то тим самим він не може задовольняти ні одну з конгруенцій (13.3).
Нехай це не так. Тоді існує хоча б один нетривіальний простий дільник q_i, $i \in [1,k]$, такий, що $\Phi = q_i \cdot \delta$ і $g^\delta \equiv 1(\mathrm{mod}\, m)$, $\delta < \Phi$. А це є протиріччям первісності кореня g за модулем m.
Отже, для перевірки g на первісність за модулем m досить перевірити невиконання усіх конгруенцій із (13.3).■

Приклад 2. Знайти найменший первісний корінь за модулем $m=41$.

Розв'язання.
Маємо $\Phi=\varphi(41)=40=2^3\cdot 5$. Нетривіальними простими дільниками функції Ейлера будуть $q_1=2$, $q_2=5$. Отже, для того щоб довільне число g, $(g,41)=1$, було первісним коренем за модулем 41, необхідно і достатньо, щоб це число не задовольняло жодну з конгруенцій:

$$g^{\frac{40}{2}} = g^{20} \equiv 1(\mathrm{mod}\, 41);\ g^{\frac{40}{5}} = g^{8} \equiv 1(\mathrm{mod}\, 41).$$

Перевіримо декілька перших чисел з повної системи найменших додатних лишків за модулем 41 на статус «первісний корінь». Нехай $g=2$, $g=3$, $g=4$, $g=5$, $g=6$, $g=7$.

1. $g=2$, $2^{20}=1024^2=(41\cdot 25-1)^2\equiv 1(\mathrm{mod}\,41)$ – перша конгруенція із двох виконується, отже, порушується умова теореми, і відповідно 2 не є первісним коренем за модулем 41.

2. $g=3$, $3^{20}=81^5=(41\cdot 2-1)^5\equiv -1(\mathrm{mod}\,41)$, – перша конгруенція не виконується.

$3^8=(41\cdot 2-1)^2\equiv 1(\mathrm{mod}\,41)$ – друга конгруенція з двох виконується, отже, 3 не є первісним коренем за модулем 41.

3. $g=4$, $4^{20}=\underbrace{2^{40}\equiv 1}_{\text{теорема Ферма}}\ (\mathrm{mod}\,41)$, – перша конгруенція з двох виконується, отже, 4 не є первісним коренем за модулем 41.

4. $g=5$, $5^{20}=5^{3\cdot 6+2}=125^6\cdot 25=(41\cdot 3+2)^6(41-16)\equiv 2^6(-16)(\mathrm{mod}\,41)\equiv$

$\equiv 2^5\cdot 9=4\cdot 72\equiv 4\cdot(-10)=-40\equiv 1(\mathrm{mod}\,41)$ – перша конгруенція з двох виконується, отже, 5 не є первісним коренем за модулем 41.

5. $g=6$, $6^{20}=3^{20}\cdot 2^{20}\equiv(-1)\cdot 1\equiv -1(\mathrm{mod}\,41)$ – перша конгруенція не виконується.

$6^8=3^8\cdot 2^8\equiv 1\cdot 256\equiv 1\cdot 10(\mathrm{mod}\,41)$ – друга конгруенція не виконується. Обидві конгруенції з умови теореми не виконуються, тобто число 6 є первісним коренем за модулем 41, найменший степінь у якому число 6 конгруентне 1 за модулем 41 є $\varphi(41)=40$.

6. $g=7$, $7^{20}=49^{10}\equiv 8^{10}=2^{30}=(-1)^3\equiv -1(\mathrm{mod}\,41)$ – перша конгруенція не виконується.

$7^8=49^4\equiv 8^4=2^{12}\equiv(-1)\cdot 4(\mathrm{mod}\,41)$ – друга конгруенція не виконується. Обидві конгруенції з умови теореми не виконуються, тобто число 7 є первісним коренем за модулем 41.

Відповідь: найменшим первісним коренем за модулем 41 є лишок 6.

Приклад 3. Знайти первісні корені за модулем $m=1681$.

Розв'язання.

Модуль $m=41^2=1681$. Первісний корінь можна було б знайти, користуючись загальною теоремою. Знайдемо його іншим способом, використовуючи теорему 8.

Згідно з цією теоремою модуль $m=41^2$ має $\varphi\left(\varphi\left(p^\alpha\right)\right)=\varphi\left(\varphi\left(41^2\right)\right)=\varphi(41\cdot 40)=40\cdot 4\cdot 4=640$ первісних коренів. Із прикладу 2 відомо, що найменший первісний корінь за модулем 41 дорівнює 6. Він породжує $\varphi\left(p^{\alpha-1}\right)=\varphi(41)=40$ первісних коренів (згідно з теоремою 8).

Для первісного кореня 6 виконується конгруенція $6^{40}\equiv 1(\mathrm{mod}\,41)$, або $6^{40}=1+41q,\ \forall q\in Z$.

Оскільки $6^{40}-1$ не ділиться на 41^2 (перевірити самостійно), то це приводить до досить великих чисел і тому має сенс скористатися теоремою 7 безпосередньо.

Використовуючи властивості конгруенцій, запишемо $(6+41t)^{40}=1+41q$. Піднесемо обидві частини рівності до степеня 41 і праву частину розкладемо за біномом Ньютона:

$$(6+41t)^{40\cdot 41}=(1+41q)^{41}=1+C_{41}^{1}41q+C_{41}^{2}41^{2}q^{2}+\ldots+41^{2}41^{39}q^{41}.$$

З урахуванням того, що $C_{41}^{1}=41$, маємо

$$(6+41t)^{40\cdot 41}=1+41^{2}\left(q+C_{41}^{2}q^{2}+\ldots+41^{39}q^{41}\right).$$

Вираз $\left(q+C_{41}^{2}q^{2}+\ldots+41^{39}q^{41}\right)$ є суперпозицією цілих чисел, тобто число ціле. Позначимо його через u, отримаємо $(6+41t)^{40\cdot 41}=1+41^{2}\cdot u$.

Зауважимо, що $40\cdot 41=\varphi\left(41^{2}\right)$, тоді отриманий вираз набирає вигляду $(6+41t)^{\varphi\left(41^{2}\right)}=1+41^{2}\cdot u$ або $(6+41t)^{\varphi\left(41^{2}\right)}=1(\mathrm{mod}\,41^{2})$.

Тобто за модулем 41^{2} усі неконгруентні між собою числа вигляду $6+41t$ будуть первісними коренями, які породжуються первісним коренем 6 за модулем 41. Їх 40, найменший отримаємо для $t=0$, тобто найменший первісний корінь за модулем $41^{2}=1681$ є 6, як і за модулем 41. Наступні первісні корені за модулем 1681 будуємо так: $6+41\cdot 1=47$; $6+41\cdot 2=88$; $6+41\cdot 3=129$ і т. д. Останнім первісним коренем модуля $m=41^{2}$ буде число $6+41\cdot 39=1605$.

З урахуванням теореми 8 (висновок 2) можна стверджувати, що клас лишків $6+mt$ буде найменшим первісним коренем і для модулів $m=41^{\alpha}$, $\forall\alpha\geq 2$.

Приклад 3. Знайти первісний корінь за модулем $m=3362$.

Розв'язання.

Модуль $m=3362=2\cdot 1681=2\cdot 41^{2}$. Первісний корінь і тут можна було б знайти, використовуючи загальну теорему 8. Знайдемо його простіше, використовуючи теорему 9.

Із прикладу 3 відомо, що первісний корінь за модулем $m=1681=41^{2}$ це 6. Первісним коренем за модулем 3362 може бути непарне число із двох чисел $g=6$ та $g+p^{\alpha}=6+41^{2}$, тобто число 6+1681=1687.

Відповідь: первісним коренем за модулем 3362 є число 1687.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Знайти порядок числа: a за модулем m, якщо:
   а) a =2, m = 5;
   б) a = 4, m = 5;
   в) a = 5, m =8;
   г) a = 10, m=13;
   д) a = 4, m = 15;
   е) a = 2, m= 15;
   є) a = 2, m= 17;
   ж) a = 7, m = 20;

з) a = 7, m = 22;

к) a = 6, m = 39.

2. Знайти всі первісні корені за такими модулями:

а) 11; 5. 12. 18. б)13; 5. 12. 19. в) 15; 5. 12. 26. г) 19; 5. 12. 21. д) 49; 5. 12. 22.

3. Знайти число первісних коренів і найменший з них за такими модулями:

а) 10; 5. 12. 18. б) 18; 5. 12. 25. в) 15; 5. 12. 20. г) 31; 5. 12. 27.

4. Знайти найменший первісний корінь за такими модулями:

а) 7;

б) 17;

в) 23;

г) 41;

д) 53;

е) 50.

5. Знаючи, що 3 є первісним коренем за модулем 29, знайти решту первісних коренів за цим модулем.

6. Знаючи, що 2 задовольняє порівнянню $x^8 \equiv 1 (\mathrm{mod} 17)$, знайти всі розв'язки цього порівняння.

7. Знаючи, що $P_{29}(4)=14$, знайти решту чисел, які мають порядок 14 за модулем 29.

8. Знаючи, що $P_{29}(12)=4,\ \ P_{29}(23)=7,$ знайти $P_{29}(15).$

9. Знаючи, що 2 є первісний корінь за модулем 131, знайти всі розв'зки порівняння $x^3 \equiv 16 (\mathrm{mod} 131).$

10. Нехай p - просте непарне число. Довести, що:

а) серед первісних коренів за модулем p не може бути квадратів;

б) $\left|\frac{a}{p}\right|=-1,$ якщо a – первісний корінь за модулем p;

в) добуток двох первісних коренів за модулем p не є первісним коренем за цим модулем.

г) якщо $n > 1$, то існує тільки $\varphi(\varphi(p^n))$ різних первісних коренів за модулем p^n .

11. Довести, що $P_{5929}(16)=1155.$

12.14 Практична робота №14

Тема: Індекси.
Мета: Розглянути індекси та їх властивості за елементарними модулями, індекси за модулем 2^α та індекси за складеним модулем, навчитися будувати таблиці індексів та застосовувати індекси до розв'язання задач теорії чисел.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Індекси за елементарними модулями

Нехай p – просте непарне число, $\alpha \geq 1$, m – одне з чисел p^α та $p^{2\alpha}$, $\Phi = \varphi(m)$, g – первісний корінь за модулем m.

Теорема 1.
Якщо γ пробігає повну систему найменших додатних лишків за модулем Φ, $\gamma = \{0,1,2,\ldots,\Phi-1\}$, то g^γ пробігає зведену систему лишків за модулем m, $g^\gamma = \{0,1,2,\ldots,m-1\}$.

Доведення. Дійсно, згідно з теоремою 1 практичної роботи №13 із зміною $\gamma = \{0,1,2,\ldots,\Phi-1\}$ g^γ пробігає Φ чисел, взаємно простих з m, та неконгруентних між собою за модулем m.■
Розглянемо ціле число a, таке, що $(a,m)=1$.

Визначення. Якщо $a \equiv g^\gamma (\mathrm{mod} m)$, $\gamma \geq 0$, то γ називається індексом числа a з основою g за модулем m і позначається символом $\gamma = ind_g a$.

Індекс числа a з основою g за модулем m є аналогом логарифма числа a з основою g. Тобто індекс γ за модулем m є таким степенем, до якого треба піднести число g, щоб отримати число, яке належить класу лишків $a + m \cdot t$.

З урахуванням теореми 1 будь-яке a, взаємно просте з m, має певний єдиний індекс γ' серед чисел повної системи лишків за модулем Φ, $\gamma = \{0,1,2,\ldots,\Phi-1\}$.

Якщо γ' відоме, то можна визначити і всі індекси числа a для основи g. Відповідно до теореми 3 практичної роботи №13 це будуть усі невід'ємні числа класу $\gamma = \gamma' + \Phi \cdot t$.

Безпосередньо з означення індексу випливає, що числа a, створені як g^γ, з даним індексом γ утворюють клас чисел із зведеної системи лишків за модулем m.

Властивості індексів

Властивості індексів схожі на властивості логарифмів. Для спрощення написання властивостей вважаємо, що основа індексів – це первісний корінь g.

1. $ind(ab) = ind\, a + ind\, b (\mathrm{mod}\Phi)$.

2. $ind\, a^n \equiv n \cdot ind\, a (\mathrm{mod}\Phi)$.

Дійсно,

$a \equiv g^{ind\, a} (\mathrm{mod} m);\ b \equiv g^{ind\, b} (\mathrm{mod} m);\ a \cdot b \equiv g^{ind\, a} \cdot g^{ind\, b} (\mathrm{mod} m) \equiv g^{ind\, a + ind\, b} (\mathrm{mod} m)$.

З іншого боку $a \cdot b \equiv g^{ind\,(ab)} (\mathrm{mod} m)$.

Отже, $g^{ind\,(ab)} \equiv g^{ind\, a + ind\, b} (\mathrm{mod} m) \Rightarrow ind\,(ab) \equiv ind\, a + ind\, b (\mathrm{mod}\Phi)$,

або $ind\,(ab) \equiv ind\, a + ind\, b + \Phi \cdot t,\ \forall t \in Z$.

Властивості можна поширити на довільну кількість множників. Якщо множників n і всі вони дорівнюють a, отримуємо властивість 2.

Оскільки індекси, як і логарифми з певною основою, мають значне практичне застосування, для них складені таблиці індексів за певним модулем. Для кожного простого модуля p складені дві таблиці. Перша – для знаходження індексу за певним числом, друга – для знаходження числа за певним індексом. Таблиці містять найменші додатні лишки чисел (зведена система) та їх найменші індекси (повна система) за модулями p та $\Phi = \varphi(p) = p - 1$ відповідно.

За основу індексів стандартно обирають найменший первісний корінь.

Приклад 1. Побудуємо таблиці індексів за модулем $p = 41$.

Розв'язання.

Знайдемо всі степені числа 7 за модулем 41, коли індекс пробігає повну систему найменших додатних лишків.

$\mathrm{mod}\, 41$

$7^0 \equiv 1$	$7^8 \equiv 37$	$7^{16} \equiv 16$	$7^{24} \equiv 18$	$7^{32} \equiv 10$
$7^1 \equiv 7$	$7^9 \equiv 13$	$7^{17} \equiv 30$	$7^{25} \equiv 3$	$7^{33} \equiv 29$
$7^2 \equiv 8$	$7^{10} \equiv 9$	$7^{18} \equiv 5$	$7^{26} \equiv 21$	$7^{34} \equiv 39$
$7^3 \equiv 15$	$7^{11} \equiv 22$	$7^{19} \equiv 35$	$7^{27} \equiv 24$	$7^{35} \equiv 27$
$7^4 \equiv 23$	$7^{12} \equiv 31$	$7^{20} \equiv 40$	$7^{28} \equiv 4$	$7^{36} \equiv 25$
$7^5 \equiv 38$	$7^{13} \equiv 12$	$7^{21} \equiv 34$	$7^{29} \equiv 28$	$7^{37} \equiv 11$
$7^6 \equiv 20$	$7^{14} \equiv 2$	$7^{22} \equiv 33$	$7^{30} \equiv 32$	$7^{38} \equiv 36$
$7^7 \equiv 17$	$7^{15} \equiv 14$	$7^{23} \equiv 26$	$7^{31} \equiv 19$	$7^{39} \equiv 6$

$7^{40} \equiv 1$ є підтвердженням первісності кореня $g_2 = 7$.

Легко помітити, що степенями числа 7 за простим модулем 41 є зведена система найменших додатних лишків, що підтверджує істинність теореми 1.

Будуємо таблиці.

$p = 41;\ \Phi = p - 1 = 40 = 2^3 \cdot 5,\ g = 7$. У заголовному стовпці таблиці кожний рядок визначає кількість десятків даного числа, у заголовному рядку – кількість одиниць. На перетині обраних рядка і стовпця стоїть результуюче число.

Спочатку побудуємо таблицю, з якої можна знайти індекс за певним числом (табл. 1).

Таблиця 1

a	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
0		0	14	25	28	**18**	39	1	2	10
1	32	37	13	9	15	3	16	7	24	31
2	6	26	11	4	27	36	23	35	29	33
3	17	12	30	22	21	19	38	**8**	5	34
4	20									

Нехай виникла необхідність знайти індекс числа 37 з основою 7 за модулем 41. Десятків 3, обираємо рядок **3**, одиниць 7, обираємо стовпчик **7**. На перетині стоїть число **8**. Отже, індекс числа 37 з основою 7 за модулем 41 є 8. Число 7, піднесене до 8-го степеня, дасть клас лишків, до якого належить найменший додатний лишок 37: $37 \equiv 7^8 (\mathrm{mod}\, 41)$.

Знайдемо індекс числа 5: десятків немає, беремо рядок **0**, одиниць 5 – стовпчик **5**. На перетині стоїть число **18**, отже $5 \equiv 7^{18} (\mathrm{mod}\, 41)$.

Тепер побудуємо таблицю, в якій за відомим індексом можна знайти число (табл. 2).

Таблиця 2

ind	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
0	1	7	8	15	23	38	20	17	37	13
1	9	22	31	12	2	14	16	**30**	5	35
2	40	34	33	26	18	3	21	24	4	28
3	32	19	10	29	39	27	25	11	36	6
4	1									

Знайдемо число, у якого індекс з основою 7 за модулем 41 є 17. Обираємо рядок **1** і стовпчик **7**. Отримали, що $7^{17} \equiv 30 (\mathrm{mod}\, 41)$.

Наслідки з теорем про індекси

Нехай p – просте непарне число, $\alpha \geq 1$, m – одне з чисел p^α та $p^{2\alpha}$, $\Phi = \varphi(m)$, числа a, n – деякі цілі числа, такі, що $(n, \Phi) = d$, $(a, m) = 1$ відповідно.

Наслідок 1.

Конгруенція $x^n \equiv a (\mathrm{mod}\, m)$ має розв'язок тоді і тільки тоді, коли $d \mid ind\, a$. Число a за таких умов буде лишком степеня n за модулем m і конгруенція матиме d розв'язків.

Наслідок 2.

У зведеній системі лишків за модулем m кількість лишків степеня n становить $\frac{\Phi}{d}$.

Приклад 2. Розглянемо декілька степеневих конгруенцій за модулем 41 і проаналізуємо їх розв'язання за допомогою індексів з основою 7.

Розв'язання.

а) Розглянемо конгруенцію $x^8 \equiv 23(\mathrm{mod}\,41)$.

Маємо $\Phi = \varphi(41) = 40,\ n = 8,\ (8,40) = 8$. Із таблиці 1 індексів за модулем 41 знаходимо індекс числа 23.

$ind_7 23 = 4$ – не ділиться на 8, отже, дана конгруенція не розв'язується з основою 7.

б) Розглянемо конгруенцію $x^8 \equiv 37(\mathrm{mod}\,41)$.

Маємо $\Phi = \varphi(41) = 40,\ n = 8,\ (8,40) = 8$. Із таблиці 1 знаходимо індекс числа 37.

$ind_7 37 = 8$ – ділиться на $d = 8$, отже, конгруенція така, що розв'язується і має вісім розв'язків.

Знайдемо їх. Спершу індексуємо вихідну конгруенцію з основою 7: $8 \cdot ind_7 x \equiv 8(\mathrm{mod}\,40)$.

Скоротимо конгруенцію на 8, отримаємо $ind_7 x \equiv 1(\mathrm{mod}\,5)$.

Отже, індекси з основою 7, неконгруентні за модулем 40, будуть такими: $ind_7 x \equiv 1,6,11,16,21,26,31,36$.

Цим індексам відповідають вісім неконгруентних за модулем 41 значень x із таблиці 2: $x \equiv 7,20,22,16,34,21,19,25(\mathrm{mod}\,41)$.

Упорядкувавши ці значення, отримаємо вісім розв'язків вихідної конгруенції із зведеної системи найменших додатних лишків за модулем 41: $x \equiv 7,16,19,20,21,22,25,34(\mathrm{mod}\,41)$, або із зведеної системи абсолютно найменших лишків за модулем 41: $x \equiv \pm 7, \pm 16, \pm 19, \pm 20(\mathrm{mod}\,41)$.

Перевірка.

Розв'язок перевіряємо в таблиці 1. Через парність степеня $37 \equiv -7(\mathrm{mod}\,41)$ теж є розв'язком.

Для $x \equiv \pm 16(\mathrm{mod}\,41)$ маємо:

$$(\pm 16)^8 \equiv 256^4 \equiv 10^4 \equiv 100^2 \equiv 18^2 \equiv 81 \cdot 4 \equiv -4 \equiv 37(\mathrm{mod}\,41).$$

Отже, $(\pm 16)^8 \equiv 37(\mathrm{mod}\,41)$, $x \equiv \pm 16(\mathrm{mod}\,41)$ – розв'язки.

Для $x \equiv \pm 19(\mathrm{mod}\,41)$ маємо:

$$(\pm 19)^8 \equiv 361^4 \equiv (-8)^4 \equiv 64^2 \equiv (-18)^2 \equiv 81 \cdot 4 \equiv -4 \equiv 37(\mathrm{mod}\,41).$$

Отже, $(\pm 19)^8 \equiv 37(\mathrm{mod}\,41)$, $x \equiv \pm 19(\mathrm{mod}\,41)$ – розв'язки.

Для $x \equiv \pm 20(\mathrm{mod}\,41)$ маємо:

$$(\pm 20)^8 \equiv x(\mathrm{mod}\,41) \Rightarrow 400^4 \equiv (-10)^4 \equiv 37(\mathrm{mod}\,41).$$

Отже, $(\pm 20)^8 \equiv 37(\mathrm{mod}\,41)$, $x \equiv \pm 20(\mathrm{mod}\,41)$ – розв'язки.

Відповідь: $x \equiv \pm 7, \pm 16, \pm 19, \pm 20(\mathrm{mod}\,41)$.

Приклад 3. Розглянемо числа, індекси яких з основою 7 кратні $d = 4$ (табл. 2):

ind_7	0	4	8	12	16	20	24	28	32	36
Число	1	23	37	31	16	40	18	4	10	25

Розв'язання.

Після впорядкування чисел другого рядка отримаємо ряд 1, 4, 10, 16, 18, 23, 25, 31, 37, 40.

Ці числа є біквадратичними лишками (або усі лишки довільного степеня $n = 4,12,16,\ldots,36$, де $(n,40) = 4$) серед найменших додатних лишків за модулем 41. Кількість чисел такого ряду $\frac{\Phi}{d} = \frac{\varphi(41)}{4} = \frac{40}{4} = 10$.

Наслідок 3.

Число a є лишком степеня n за модулем m тоді і тільки тоді, коли $a^{\frac{\Phi}{d}} \equiv 1(\mathrm{mod}\, m),\ d = (\Phi, n)$.

Приклад 4. У теоремі 12 практичної роботи №12 умовою первісності кореня для числа g за модулем m є невиконання конгруенції $g^{\frac{\Phi}{q}} \equiv 1(\mathrm{mod}\, m)$, $\forall q : \{q \in Z, q \neq 1, q \neq \Phi, q | \Phi\}$. Ця умова означає, що первісний корінь g є нелишком степеня q за модулем m. Отже, у разі невиконання конгруенції $g^{\frac{\Phi}{2}} \equiv 1(\mathrm{mod}\, m)$ число g є квадратичним нелишком за модулем m.

Наслідок 4.

1) Якщо $ord(a)_m = \delta$, то $(ind\, a, \Phi) = \frac{\Phi}{\delta}$. Зокрема, у випадку, коли число g є первісним коренем за модулем m, то $(ind\, g, \Phi) = 1$.

2) У зведеній системі лишків за модулем m кількість чисел, які належать показнику δ, є $\varphi(\delta)$.

У відповідності до останнього твердження кількість первісних коренів за модулем m дорівнює $\varphi(\Phi) = \varphi(\varphi(m))$.

Приклад 5. У зведеній системі лишків за модулем 41 числами, які належать показнику 10, є числа a з умовою $(ind\, a, \varphi(41)) = (ind\, a, 40) = \frac{40}{10} = 4$, тобто числа, які відповідають у таблиці 2 індексам 4, 12, 28, 36. Це будуть числа 23, 31, 4, 25 або в ранжованому вигляді – 4, 23, 25, 31.

Кількість чисел чотири, що відповідає $\varphi(10) = 4$.

Приклад 6. У зведеній системі лишків за модулем 41 первісними коренями є такі числа g, для яких виконується умова $(ind\, g, \Phi) = (ind\, g, 40) = 1$. Такими індексами будуть 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.

За таблицею 2 знайдемо відповідні до індексів числа 7, 15, 17, 13, 22, 12, 30, 35, 34, 26, 24, 28, 19, 29, 11, 6, або у ранжованому вигляді 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Кількість первісних коренів становить 16, що збігається з $\varphi(40) = 2^2 \cdot 4 = 16$.

Індекси за модулем 2^α

У теоремі 10 практичної роботи №13 доведено, що $ord_{2^\alpha} a \le 2^{\alpha-2}$, $(a,2)=1$, $\alpha \ge 3$, тобто первісні корені існують тільки для чисел за модулями 2 і 4 (за модулем
2 – $g=1$, за модулем 4 – $g_1=1$, $g_2=3$). Отже, індекси за модулем 2^α, $\alpha \ge 3$ у вищенаведеному визначенні не існують. Але теорію індексів можна поширити і для індексів такого типу, дещо ускладнивши міркування та розглянувши декілька додаткових теорем.

По-перше, впевнимося, що числа, які належать показнику $2^{\alpha-2}$ за модулем 2^α, $\alpha \ge 3$, існують. Таким числом, наприклад, буде 5. Розглянемо теорему.

Теорема 2.

Для будь-якого цілого $\alpha \ge 2$ виконується рівність $5^{2^{\alpha-2}} = 1 + 2^\alpha t_\alpha$, де $t_\alpha = 2k+1$ – непарне.

Теорема 3.

Для $\alpha \ge 2$ два числа вигляду $(-1)^u 5^v$ та $(-1)^{u'} 5^{v'}$ конгруентні за модулем 2^α тоді і тільки тоді, коли виконуються такі дві конгруенції:

$$u \equiv u' (\mathrm{mod}\, 2) \text{ та } v \equiv v' (\mathrm{mod}\, 2^{\alpha-2}).$$

Теорема 4.

За модулем 2^α, $\alpha \ge 2$, будь-яке просте непарне число конгруентне одному і тільки одному числу із системи чисел $-5^{2^{\alpha-2}}, \ldots, -5^2, -5, 5, 5^2, \ldots, 5^{2^{\alpha-2}}$.

Маючи систему степенів числа 5, яка створює зведену систему лишків, можемо визначити поняття індексу за модулем 2^α, $\alpha \ge 3$.

Визначення. Індексом непарного числа a за модулем 2^α, $\alpha \ge 3$, називається пара чисел (u,v), $v \ge 0$, для якої виконується конгруенція $(-1)^u 5^v \equiv a (\mathrm{mod}\, 2^\alpha)$.

Іноді таку пару у відповідності до загальної теорії індексів позначають $ind\, a = (u,v)$, $v \ge 0$.

Із теореми 4 випливає, що будь-яке непарне число a має свій індекс за модулем 2^α.

Визначення. Дві пари (u,v), $v \ge 0$ та (u',v'), $v' \ge 0$, називаються конгруентними за подвійним модулем (m,n), якщо одночасно виконуються дві конгруенції $u \equiv u' (\mathrm{mod}\, m)$ та $v \equiv v' (\mathrm{mod}\, n)$.

Конгруентність пар чисел за подвійним модулем позначають так: $(u,v) \equiv (u',v') (\mathrm{mod}(m,n))$.

Для конгруенції за подвійним модулем виконується очевидна властивість транзитивності конгруенцій.

У термінах конгруенції за подвійним модулем теорему 3 можна подати у вигляді теореми 3 а.

Теорема 3 а.

Для $\alpha \geq 3$ $a \equiv b(\mathrm{mod}\, 2^{\alpha})$ тоді і тільки тоді, коли $ind\, a \equiv ind\, b\left(\mathrm{mod}(2, 2^{\alpha-2})\right)$, зокрема, якщо для довільного числа a за модулем 2^{α}, $\alpha \geq 3$ $ind\, a = (u, v)$, $v \geq 0$ та $ind\, a = (u', v')$, $v' \geq 0$, то $(u, v) \equiv (u', v')\left(\mathrm{mod}(2, 2^{\alpha-2})\right)$.

Визначення. Сумою індексів $(u_1, v_1) + \ldots + (u_n, v_n)$ називається індекс $(u_1 + u_2 + \ldots + u_n, v_1 + v_2 + \ldots + v_n)$.

Теорема 5.

Для модуля 2^{α}, $\alpha \geq 3$ індекс добутку непарних чисел є конгруентним сумі індексів множників за подвійним модулем $(2, 2^{\alpha-2})$.

Якщо $a_1 = a_2 = \ldots = a_n$, то згідно з теоремою 5, можемо записати

$$ind\, a^n \equiv n \cdot (u, v)\left(\mathrm{mod}(2, 2^{\alpha-2})\right),$$

або

$$ind\, a^n \equiv n \cdot ind\, a\left(\mathrm{mod}(2, 2^{\alpha-2})\right).$$

Таблиці індексів для модулів типу 2^{α}, $\alpha \geq 3$ складаються з двох рядків:

- перший рядок – непарне число;
- другий рядок – пара (u, v), яка є індексом даного числа за модулем 2^{α}, $\alpha \geq 3$, тобто пара, яка подає дане непарне число у вигляді $(-1)^u 5^v (\mathrm{mod}\, 2^{\alpha})$.

Приклад 7. Скласти таблицю індексів за модулем 64.

Розв'язання.

Число $64 = 2^6$, тобто модуль типу 2^{α}, $\alpha = 6 > 3$. Нам треба знайти всі пари (u, v), такі, що $u = \{0,1\}$, v пробігає повну систему лишків за модулем $2^{\alpha-2} = 2^4 = 16$ $(v = 0,1,2,\ldots,15)$, а числа $(-1)^u 5^v$ – зведену систему лишків за модулем $2^{\alpha} = 2^6 = 64$. Кількість класів у зведеній системі буде $\varphi(2^6) = 2^5 = 32$.

Маємо:

$$\pm 5^0 \equiv \pm 1; \quad \pm 5^1 \equiv \pm 5; \quad \pm 5^2 \equiv \pm 25; \quad \pm 5^3 \equiv \pm 61;$$
$$\pm 5^4 \equiv \pm 49; \quad \pm 5^5 \equiv \pm 53; \quad \pm 5^6 \equiv \pm 9; \quad \pm 5^7 \equiv \pm 45;$$
$$\pm 5^8 \equiv \pm 33; \quad \pm 5^9 \equiv \pm 37; \quad \pm 5^{10} \equiv \pm 57; \quad \pm 5^{11} \equiv \pm 29;$$
$$\pm 5^{12} \equiv \pm 17; \quad \pm 5^{13} \equiv \pm 21; \quad \pm 5^{14} \equiv \pm 41; \quad \pm 5^{15} \equiv \pm 13.$$

Враховуючи, що знак «+» відповідає $u = 0$, а знак «–» – $u = 1$, та перетворивши від'ємні лишки на відповідні додатні, можемо записати таблицю індексів (табл. 3).

Таблиця 3

N	a	$ind\ a$	N	a	$ind\ a$	N	a	$ind\ a$	N	a	$ind\ a$
1	1	(0,0)	9	17	(0,12)	17	33	(0,8)	25	49	(0,4)
2	3	(1,3)	10	19	(1,7)	18	35	(1,11)	26	51	(1,15)
3	5	(0,1)	11	21	(0,13)	19	37	(0,9)	27	53	(0,5)
4	7	(1,10)	12	23	(1,14)	20	39	(1,2)	28	55	(1,6)
5	9	(0,6)	13	25	(0,2)	21	41	(0,14)	29	57	(0,10)
6	11	(1,5)	14	27	(1,9)	22	43	(1,13)	30	59	(1,1)
7	13	(0,15)	15	29	(0,11)	23	45	(0,7)	31	61	(0,3)
8	15	(1,4)	16	31	(1,8)	24	47	(1,12)	32	63	(1,0)

Індекси за складеним модулем

Узагальнимо попередню теорію для модулів, які мають більш складну структуру.

Визначення. Нехай $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ – канонічне подання числа m, a – довільне ціле число. Введемо такі позначення: $\Phi = 2,\ \Phi_0 = 2^{\alpha-2},\ \Phi_s = \varphi\left(p_s^{\alpha_s}\right)$, де g_s – найменший первісний корінь за модулем $p_s^{\alpha_s}$.

Якщо

$$\begin{cases} a \equiv (-1)^u 5^v \left(\mathrm{mod}\, 2^{\alpha}\right); \\ a \equiv g_1^{\gamma_1} \left(\mathrm{mod}\, p_1^{\alpha_1}\right); \\ \ldots\ldots\ldots\ldots\ldots\ldots; \\ a \equiv g_k^{\gamma_k} \left(\mathrm{mod}\, p_k^{\alpha_k}\right), \end{cases} \qquad (14.1)$$

то система $\{u, v, \gamma_1, \gamma_2, \ldots, \gamma_k\}$ називається системою індексів числа a за модулем m.

Із такого визначення випливає, що u, v – система індексів числа a за модулем 2^{α}, а $\{\gamma_1, \gamma_2, \ldots, \gamma_k\}$ – індекси числа a за модулями $p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Отже, відповідно до теорем 3, За та теореми 1 число a, взаємно просте з $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, має єдину систему індексів $\{u, v, \gamma_1, \gamma_2, \ldots, \gamma_k\}$ за модулем $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Будь-яка інша система $\{u', v', \gamma_1', \gamma_2', \ldots, \gamma_k'\}$ за цим самим модулем буде складатися з індексів, конгруентних до $\{\gamma_1, \gamma_2, \ldots, \gamma_k\}$ за модулями $\Phi, \Phi_0, \Phi_1, \ldots, \Phi_k$, тобто

$$u \equiv u' (\mathrm{mod}\, \Phi),\ v \equiv v' (\mathrm{mod}\, \Phi_0),\ \gamma_1 \equiv \gamma_1' (\mathrm{mod}\, \Phi_1), \ldots,\ \gamma_k \equiv \gamma_r' (\mathrm{mod}\, \Phi_k).$$

Числа a із заданою системою індексів $\{u', v', \gamma_1', \gamma_2', ..., \gamma_k'\}$ можуть бути однозначно визначені із системи (14.1) і утворюють клас чисел за модулем $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$.

Побудова таблиць індексів. Застосування індексів до розв'язання задач теорії чисел

Приклад 8. Побудувати таблицю індексів за модулем 27.

Розв'язання.

Модуль $m = 27 = 3^3$, $p = 3$, $\alpha = 3$, $\Phi = \varphi(3^3) = 3^2 \cdot 2 = 18$, тобто у зведеній системі лишків за модулем 27 є 18 чисел.

Знайдемо первісний корінь за модулем 27.

Оскільки $27 = 3^3$, то за основу беремо первісний корінь за модулем 3, тобто $g = 2$ або $g = 2 + 3t$, наприклад, $g = 5$.

Перевіряємо найменший первісний корінь.

$2^{3-1} - 1 = 3$ – ділиться на $p = 3$ і не ділиться на $p^2 = 9$, отже, відповідно до теорем 7 і 8 практичної роботи №13 $g = 2$ є первісним коренем за модулем $3^2 = 9$ і відповідно за модулем $3^3 = 27$.

Знаходимо значення степенів γ із повної системи лишків за модулем $\Phi = 18$ для первісного кореня $g = 2$.

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8;\ 2^4 = 16;\ 2^5 = 32 \equiv 5;\ 2^6 \equiv 10;\ 2^7 \equiv 20;\ 2^8 \equiv 13;\ 2^9 \equiv 26;$

$2^{10} \equiv 25;\ 2^{11} \equiv 23;\ 2^{12} \equiv 19;\ 2^{13} \equiv 11;\ 2^{14} \equiv 22;\ 2^{15} \equiv 17;\ 2^{16} \equiv 7;\ 2^{17} \equiv 14 (\mathrm{mod}\, 27).$

Будуємо таблицю індексів для чисел a зведеної системи за модулем $m = 27 = 3^3$ і основою $g = 2$.

Таблиця 4

a	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25	26
$Ind\, a$	0	1	2	5	16	3	6	13	8	17	4	15	12	7	14	11	10	9

Відповідь: таблиця 4 є таблицею індексів для чисел a зведеної системи за модулем $m = 27 = 3^3$ і основою $g = 2$.

Приклад 9. Побудувати таблицю індексів для модуля 18.

Розв'язання.

Модуль $m = 18 = 2 \cdot 3^3$ типу $m = 2p^{\alpha}$. Відповідно до теореми 9 практичної роботи №13 непарний із двох первісних коренів g та $g + p^{\alpha}$ за модулем p^{α} є первісним і за модулем $m = 2p^{\alpha}$.

Для цієї задачі первісним коренем за модулем $3^2 = 9$ краще взяти непарний первісний корінь $g = 2 + 3 = 5$, породжений первісним коренем $g = 2$ за модулем 3 (теорема 8 практичної роботи №13).

Зведені системи за модулями 9 і 18 нараховують за $\Phi = \varphi(18) = \varphi(9) = 6$ лишків. Для модуля 9 це лишки 1, 2, 4, 5, 7, 8. Для модуля 18 лишками є 1, 5, 7, 11, 13,

17. Повна система лишків за модулем $\Phi = \varphi(18) = \varphi(9) = 6$ нараховує шість лишків 0, 1, 2, 3, 4, 5, які є індексами чисел зведених систем за модулями 9 та 18. Будуємо таблицю 5 індексів для модуля 9 за основою $g = 2$.

$$5^0 = 1;\ 5^1 = 5;\ 5^2 \equiv 7;\ 5^3 \equiv 8;\ 5^4 \equiv 4;\ 5^5 \equiv 2.$$

Таблиця 5

a	1	2	4	5	7	8
$Ind\, a$	0	5	4	1	2	3

Тепер побудуємо таблицю індексів за модулем 18 з урахуванням того, що зведену систему найменших лишків (ЗСНЛ) за модулем $2p^\alpha$ складають лишки класів за модулем p^α, взаємно прості з $2p^\alpha$ (теорема 9, практична робота №13). Тобто лишки 1, 5, 7 входять як до ЗСНЛ за модулем 9, так і до ЗСНЛ за модулем 18 і мають однакові індекси за цими модулями. При цьому лишки 2, 4 та 8 входять до ЗСНЛ за модулем 9, але через те, що мають спільний дільник із модулем 18, до ЗСНЛ за цим модулем не входять.

Замість цих лишків обираємо представників класів $2+9t,\ 4+9t,\ 8+9t$ за модулем 9, взаємно простих із 18:

- замість 2 беремо наступний лишок класу $2+9=11$, він взаємно простий з модулем 18 і входить до його ЗСНЛ;
- замість 4 беремо $4+9=13$;
- замість 8 беремо $8+9=17$.

У цей самий час індекси для цих лишків залишаються такі самі, оскільки індекс лишка є індексом класу за певним модулем (теорема 1).

Спираючись на попереднє, таблицю 6 індексів за модулем 18 будуємо з використанням таблиці індексів за модулем 9 (табл. 5).

Таблиця 6

a	1	5	7	11	13	17
$Ind\, a$	0	1	2	5	4	3

Приклад 10. Побудувати таблицю індексів для модуля 72.

Розв'язання.

Модуль $m = 72 = 2^3 \cdot 3^2$ типу $m = 2^\alpha p_1^{\alpha_1}$, тобто довільний складений модуль.

Зведена система лишків складається з $\varphi(2^3 3^2) = 2^2 \cdot 6 = 24$ класів лишків, взаємно простих із модулем 72.

В цьому випадку кожне число з ЗСНЛ подається системою (14.1)

$$\begin{cases} a \equiv (-1)^u 5^v \pmod{2^3}, \\ a \equiv g_1^{\gamma_1} \pmod{3^2}, \end{cases}$$

тобто індексами чисел з ЗСНЛ за модулем 72 виступають системи індексів $\{u, v, \gamma_1\}$.

Побудуємо таблицю індексів за модулем 2^3:

Лишків у ЗСНЛ за модулем 2^3 буде $\Phi_0 = \varphi(2^3) = 2^2 = 4$. Кожний лишок ЗСНЛ за таким модулем подається у вигляді $(-1)^u 5^v$. Степені u пробігають повну систему додатних лишків за модулем 2, тобто набирають значень 0, 1 або $\{0,1\}$. Степені v пробігають всі значення повної системи лишків за модулем $2^{\alpha-2} = 2^{3-2} = 2$, тобто теж $v \in \{0,1\}$. Отримаємо числа ЗСНЛ за модулем 2^3.

$(u,v) = (0,0) \Rightarrow a = (-1)^0 5^0 = 1;$

$(u,v) = (0,1) \Rightarrow a = (-1)^0 5^1 = 5;$

$(u,v) = (1,0) \Rightarrow a = (-1)^1 5^0 = -1 \equiv 7 \left(\mathrm{mod}\, 2^3\right);$

$(u,v) = (1,1) \Rightarrow a = (-1)^1 5^1 = -5 \equiv 3 \left(\mathrm{mod}\, 2^3\right).$

Таблиця індексів за модулем 8 буде мати такий вигляд:

Таблиця 7

a	1	3	5	7
u	0	1	0	1
v	0	1	1	0

Таблицю індексів для модуля $9 = 3^2$ беремо із попереднього прикладу (таблиця 5).

Будуємо таблицю індексів за модулем 72. ЗСНЛ за модулем 72 складається з 24 лишків. Це числа {1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71}.

Для побудови таблиці індексів за модулем 72 будемо визначати пару індексів (u,v) із таблиці 7 індексів за модулем 8 відповідно до того, якому класу за модулем 8 належить лишок ЗСНЛ за модулем 72. Індекс γ_1 визначається з таблиці 5 індексів за модулем 9 (для первісного кореня $g = 5$) за таким самим принципом. Наприклад, для числа 47, яке належить до ЗСНЛ за модулем 72, буде виконуватись

$$47 \equiv 7(\mathrm{mod}8) \underset{табл.7}{\Rightarrow} (u,v) \equiv (1,0)\left(\mathrm{mod}(2,2)\right);$$

$$47 \equiv 2(\mathrm{mod}9) \underset{табл.5}{\Rightarrow} \gamma_1 \equiv 5\left(\mathrm{mod}\,\varphi(9) = 6\right).$$

Отже, система індексів для числа 47 за модулем 72 буде мати вигляд $ind\,47 = \{u,v,\gamma_1\} = \{1,0,5\}$.

Таблиця індексів за модулем 72 має такий вигляд:

Таблиця 8

a	1	5	7	11	13	17	19	23	25	29	31	35
u	0	0	1	1	0	0	1	1	0	0	1	1
v	0	1	0	1	1	0	1	0	0	1	0	1
γ_1	0	1	2	5	4	3	0	1	2	5	4	3
a	37	41	43	47	49	53	55	59	61	65	67	71
u	0	0	1	1	0	0	1	1	0	0	1	1
v	1	0	1	0	0	1	0	1	1	0	1	0
γ_1	0	1	2	5	4	3	0	1	2	5	4	3

Перевірка.

Перевіримо, чи отримаємо заданий лишок із системи (14.1). Розглянемо лишок 43. Для цього лишка індексом буде система індексів $\{1,1,2\}$, тобто ми повинні отримати цей лишок із системи

$$\begin{cases} a \equiv (-1)^1 5^1 (\mathrm{mod}8), \\ a \equiv 5^2 (\mathrm{mod}9). \end{cases}$$

У другій конгруенції 5 взятий нами первісний корінь за модулем 9 для побудови таблиці індексів.

Розв'яжемо систему. Оскільки $(8,9)=1$, то розв'язок у системи буде єдиний. Із першої конгруенції a запишемо так: $a=-5+8t$. Підставляємо у другу конгруенцію, шукаємо відповідне t:

$$-5+8t \equiv 25(\mathrm{mod}9) \Rightarrow 8t \equiv 30(\mathrm{mod}9) \Rightarrow 8t \equiv 3(\mathrm{mod}9) \Rightarrow 8t \equiv 3+45(\mathrm{mod}9) \Rightarrow t = 6+9t_1$$

Підставляємо у вираз для a:

$$a = -5+8(6+9t_1) = -5+48+72t_1 \equiv 43(\mathrm{mod}72).$$

У результаті розв'язання системи конгруенцій, яка визначає задану систему індексів за модулем 72, дійсно отримали лишок 43.

Приклад 11. Побудувати таблицю індексів для модуля 21.

Розв'язання.

Модуль $m=21=3\cdot 7$ типу $m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}$, де $\alpha_1=\alpha_2=1$, тобто довільний складений модуль, індексується системою індексів $\{\gamma_1,\gamma_2\}$, де γ_1 пробігає повну систему лишків за модулем $\Phi_1=\varphi(3)=2$, тобто $\gamma_1\in\{0,1\}$, а γ_2 пробігає повну систему лишків за модулем $\Phi_2=\varphi(7)=6$, тобто $\gamma_1\in\{0,1,2,3,4,5\}$.

Первісний корінь за модулем 3 є $g=2$, найменший первісний корінь за модулем 7 є 3, оскільки

$$\Phi_2 = 6 = 2\cdot 3;\ 2^{\frac{6}{2}} = 8 \equiv 1(\mathrm{mod}7) \Rightarrow ord_7 2 = 3 < \varphi(7);\ 3^{\frac{6}{2}} = 27 \equiv 6(\mathrm{mod}7);$$

$$3^{\frac{6}{3}} = 9 \equiv 2(\mathrm{mod}7).$$

Кількість лишків у ЗСНЛ за модулем 3 буде 2, за модулем 7 буде 6, за модулем 21 буде $\Phi_1\Phi_2 = \varphi(3)\varphi(7) = 12$. ЗСНЛ за модулем 21 {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}.

Будуємо таблицю індексів за модулем 3.

Таблиця 9

a	1	2
$ind\, a = \gamma_1$	0	1

Будуємо таблицю індексів за модулем 7.

Таблиця 10

a	1	2	3	4	5	6
$ind\, a = \gamma_2$	0	2	1	4	5	3

Складаємо таблицю індексів за модулем 21, використовуючи таблиці 9 та 10. Систему індексів визначаємо з названих таблиць за належністю лишка з ЗСНЛ за модулем 72 до класів лишків за модулями 3 та 7.

Таблиця 11

a	1	2	4	5	8	10	11	13	16	17	19	20
γ_1	0	1	0	1	1	0	1	0	0	1	0	1
γ_2	0	2	4	5	0	1	4	6	2	1	5	3

Перевірка.

Перевіримо, чи отримаємо заданий лишок із системи (14.1). Розглянемо лишок 11. Система індексів для нього $\{1,4\}$. Складаємо систему

$$\begin{cases} a \equiv 2^1 (\mathrm{mod}\, 3), \\ a \equiv 3^4 (\mathrm{mod}\, 7) \end{cases} \Rightarrow \begin{cases} a \equiv 2 (\mathrm{mod}\, 3), \\ a \equiv 4 (\mathrm{mod}\, 7). \end{cases}$$

$(3,7) = 1$, розв'язок єдиний. Із першої конгруенції $a = 2 + 3t$. Підставляємо у другу, визначаємо t:

$2 + 3t \equiv 4 (\mathrm{mod}\, 7) \Rightarrow 3t \equiv 2 (\mathrm{mod}\, 7) \Rightarrow 3t \equiv 9 (\mathrm{mod}\, 7) \Rightarrow t \equiv 3 (\mathrm{mod}\, 7) \Rightarrow t = 3 + 7t_1$

Підставляємо у вираз для а:

$a = 2 + 3(3 + 7t_1) = 11 + 21t_1 \equiv 11 (\mathrm{mod}\, 21)$.

За результатами розв'язання системи отримали дійсно лишок 11 із ЗСНЛ за модулем 21.

Індекси можна застосовувати для знаходження залишку від ділення на модуль m добутку декількох множників, зокрема – степенів чисел.

Маючи таблицю індексів за модулем m для обчислення залишку від ділення добутку чисел $a_1 a_2 \cdot \ldots \cdot a_n$, $(a_i, m) = 1, i = \overline{1,n}$, позначаємо залишок через r і записуємо конгруенцію $r \equiv a_1 a_2 \cdot \ldots \cdot a_n (\mathrm{mod}\, m)$.

Індексуємо її:

$$ind\, r \equiv ind\, a_1 + ind\, a_2 + \ldots + ind\, a_n (\mathrm{mod}\, \varphi(m)).$$

Індекси чисел $a_1, a_2, ..., a_n$ беремо з таблиці індексів за модулем m, знаходимо суму індексів $c \equiv ind\, a_1 + ... + ind\, a_n$ і отримуємо конгруенцію

$$ind\, r = c \pmod{\varphi(m)}.$$

Із таблиці індексів знаходимо число b, індекс якого дорівнює c. Остаточно маємо $r = b \pmod{m}$.

Приклад 12. Знайти залишок від ділення числа $37^{20} \cdot 23^{12}$ на 61.

Розв'язання.

Складаємо конгруенцію $37^{20} \cdot 23^{12} \equiv r \pmod{61}$. Зауважимо, що $(37, 61) = 1$; $(23, 61) = 1$. Індексуємо конгруенцію $20 ind\, 37 + 12 ind\, 23 \equiv ind\, r \pmod{60}$.

З таблиці індексів за модулем 61 та основою $g = 2$ знаходимо, що $ind\, 37 \equiv 39 \pmod{60}$; $ind\, 23 \equiv 57 \pmod{60}$. Підставляємо в конгруенцію індексів. $20 \cdot 39 + 12 \cdot 57 = 780 + 684 = 1464 \equiv 24 \pmod{60}$, тобто $ind\, r \equiv 24 \pmod{60}$.

Із таблиці індексів за модулем 61 та основою $g = 2$ знаходимо, що індексу 24 відповідає лишок 20, отже, $ind\, r \equiv ind\, 20 \pmod{60}$, або $r \equiv 20 \pmod{61}$.

Відповідь: залишок від ділення числа $37^{20} \cdot 23^{12}$ на 61 дорівнює 20.

У випадку, коли необхідно знайти залишок від ділення добутку чисел на модуль $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, знаходимо залишки від ділення заданого числа на модулі $p_i^{\alpha_i}$, $i = \overline{1, n}$ і далі розв'язуємо систему

$$\begin{cases} r_1 \equiv b_1 \pmod{p_1^{\alpha_1}}; \\ r_2 \equiv b_2 \pmod{p_2^{\alpha_2}}; \\ \ldots\ldots\ldots\ldots\ldots \\ r_k \equiv b_k \pmod{p_k^{\alpha_k}}. \end{cases}$$

Якщо модуль $m = 2 p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, то відносимо множник 2 до будь-якого множника (наприклад, до першого) і знаходимо залишки за модулями $2 p_1^{\alpha_1}$, $p_i^{\alpha_i}$, $i = \overline{2, n}$, і далі розв'язуємо систему.

У випадку, коли до модуля входить множником число 2^{α}, $\alpha > 2$, в деяких випадках (у разі незначних степенів α) легше шукати залишок від ділення на таке число іншими способами, тобто без індексування. Але можна застосовувати і систему індексів $(u, v, \gamma_1, ..., \gamma_k)$.

Приклад 13. Знайти залишок від ділення числа $37^{20} \cdot 23^{12}$ на 4392.

Розв'язання.

Модуль $4392 = 61 \cdot 72 = 2^3 3^2 61$, $\alpha = 3 > 1$, $\alpha_1 = 2$, $\alpha_2 = 1$. Індекси чисел за даним модулем розглядаються за модулем $\varphi(2^3 3^2 61) = 4 \cdot 6 \cdot 60 = 1440$.

Складемо конгруенцію $37^{20} \cdot 23^{12} \equiv r \pmod{72 \cdot 61}$. Індексуємо $20 ind\, 37 + 12 ind\, 23 \equiv ind\, r \pmod{24 \cdot 60}$.

У таблиці індексів за модулем 72 (табл. 8) знайдемо систему індексів для лишків 37 і 23. Для 37 маємо систему індексів $(u,v,\gamma_1)=(0,1,0)$, для 24 маємо систему індексів $(u,v,\gamma_1)=(1,0,1)$. З прикладу 12 маємо індекси 37 та 23 за модулем 61 $ind\,37\equiv 39,\ ind\,23\equiv 57$. Позначимо ці індекси через γ_2 і додамо в систему індексів вихідного числа, розглядаючи їх за модулем 1440.

Підставимо системи індексів 37 та 23 до конгруенції $20(0,1,0,39)+12(1,0,1,57)\equiv ind\,r(\mathrm{mod}24\cdot 60)$.

Виконаємо дії.

$(0,20,0,780)+(12,0,12,684)\equiv ind\,r(\mathrm{mod}24\cdot 60)$;

$(12,20,12,1464)\equiv ind\,r(\mathrm{mod}24\cdot 60)$.

Отримали систему індексів залишку від ділення вихідного числа на модуль $72\cdot 61$ $\{u,v,\gamma_1,\gamma_2\}=\{12,20,12,1464\}$.

Пару (u,v) ми розглядаємо за подвійним модулем $(\Phi,\Phi_0)=(2,2^{\alpha-2})=(2,2^{3-2})=(2,2)$.

Отже, $(12,20)\equiv(0,0)(\mathrm{mod}(2,2))$.

$\gamma_1=12$ розглядається за модулем $\Phi_1=\varphi(3^2)=6$, отже, $\gamma_1=12\equiv 0(\mathrm{mod}6)$.

Насамкінець $\gamma_2=1464$ розглядається за модулем $\Phi_2=\varphi(61)=60$, $\gamma_1=1464\equiv 24(\mathrm{mod}60)$.

Отримуємо спрощену конгруенцію індексів $(0,0,0,24)\equiv ind\,r(\mathrm{mod}24\cdot 60)$.

Запишемо відповідну систему конгруенцій чисел, яка відповідає даній конгруенції індексів. Згадаємо, що за модулем 2^α ЗСНЛ створюється парою $(-1)^u 5^v$, для модуля 3^2 за первісний корінь брався лишок 5, а для модуля 61 – лишок 2. Маємо

$$\begin{cases} r\equiv(-1)^0 5^0(\mathrm{mod}8),\\ r\equiv 5^0(\mathrm{mod}9),\\ r\equiv 2^{24}(\mathrm{mod}61). \end{cases}$$

Із таблиці індексів для модуля 61 з первісним коренем $g=2$ беремо значення лишка з індексом 24. Для третьої конгруенції системи можна записати $r\equiv 20(\mathrm{mod}61)$ (приклад 12).

Система набуває вигляду

$$\begin{cases} r\equiv 1(\mathrm{mod}8),\\ r\equiv 1(\mathrm{mod}9),\\ r\equiv 2^{24}(\mathrm{mod}61). \end{cases} \Rightarrow \begin{cases} r\equiv 1(\mathrm{mod}72),\\ r\equiv 20(\mathrm{mod}61). \end{cases}$$

Із першої конгруенції маємо $r=1+72t$, підставляємо цей вираз у другу конгруенцію.

$1+72t \equiv 20(\mathrm{mod}61) \Rightarrow 72t \equiv 19(\mathrm{mod}61) \Rightarrow 11t \equiv 19(\mathrm{mod}61) \Rightarrow -50t \equiv 80(\mathrm{mod}61) \Rightarrow$
$\Rightarrow 5t \equiv -8(\mathrm{mod}61) \Rightarrow 5t \equiv -130(\mathrm{mod}61) \Rightarrow t \equiv -26(\mathrm{mod}61) \Rightarrow t \equiv 35(\mathrm{mod}61)$ або
$t = 35 + 61t_1$

Підставляємо в рівняння для залишку $r = 1+72(35+61t_1) = 1+2520+4392t_1$ або $r \equiv 2521(\mathrm{mod}4392)$.

Відповідь: залишок від ділення числа $37^{20} \cdot 23^{12}$ на 4392 дорівнює 2521.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Знайти залишок від ділення добутку степенів чисел $N = a^k b^l$ на складений модуль m, попередньо побудувавши необхідну для розв'язання частину таблиці індексів для даного модуля.

№	Вихідні дані	№	Вихідні дані
1	$N = 37^{11}23^{19},\ m = 88$	2	$N = 51^{13}43^{15},\ m = 104$
3	$N = 29^{31}53^{23},\ m = 136$	4	$N = 37^{29}59^{11},\ m = 152$
5	$N = 43^{17}51^{35},\ m = 184$	6	$N = 37^{29}61^{31},\ m = 66$
7	$N = 57^{23}41^{19},\ m = 78$	8	$N = 47^{37}67^{13},\ m = 102$
9	$N = 47^{29}63^{31},\ m = 114$	10	$N = 57^{37}63^{41},\ m = 138$
11	$N = 37^{29}59^{11},\ m = 99$	12	$N = 37^{11}23^{19},\ m = 117$
13	$N = 51^{13}43^{15},\ m = 153$	14	$N = 29^{31}53^{23},\ m = 171$
15	$N = 37^{29}59^{11},\ m = 207$	16	$N = 57^{23}41^{19},\ m = 110$
17	$N = 37^{29}61^{31},\ m = 130$	18	$N = 47^{29}63^{31},\ m = 170$
19	$N = 23^{23}63^{19},\ m = 190$	20	$N = 43^{17}47^{31},\ m = 230$
21	$N = 43^{29}51^{31},\ m = 275$	22	$N = 47^{29}63^{31},\ m = 325$
23	$N = 23^{23}63^{19},\ m = 425$	24	$N = 57^{23}41^{19},\ m = 475$
25	$N = 37^{29}59^{11},\ m = 575$	26	$N = 37^{11}23^{19},\ m = 144$

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Виноградов И.М. Основы теории чисел, Изд. 9-е, перераб., М.: Наука, 1981.- 180 с.

2. Лидл Р., Нидерайтер Г. Конечные поля: В 2-х т. Пер. с англ.- М.: Мир, 1988.- 822 с.

3. Хассе Г. Лекции по теории чисел. Перевод с немецкого В.В. Демьянова под редакцией И.Р. Шафаревича. – М.: Изд-во Ин. литературы, 1953.- 520 с.

4. Коблиц Н. Курс теории чисел и криптографии. Перевод с английского М.А. Михайловой и В.Е. Тараканова под редакцией А.М. Зубкова.- М.: Научное изд-во "ТВП", 2001.- 269 с.

5. Криптографічні перетворювання: навчально-методичні матеріали до самостійної роботи для студентів спеціальностей 6.160.100 і 7.160.100 "Захист інформації в комп'ютерних системах та мережах". Частина 1. Основи теорії чисел / Укл.: Ю.Г. Лега, А.Д. Кожухівський, О.А. Кожухівська, В.А. Лужецький.-Черкаси: ЧДТУ, 2008.- 32 с.

6. W.R. Alford, A.Granville and C.Pomerance. There are many Carmichael numbers, Ann. Math. 140 (1994), 703-722.

7. D. Shanks. Class number, a theory of factorization and genera. In Proc, Symposium Pure Mathematics, vol.20, pp. 415-440. American Mathematical Society, 1970.

8. Вербицький О.В. Вступ до криптології.- Львів: Видавництво науково-технічної Літератури, 1998.- 247 с.

9. Шнайер Б. Прикладная криптография / Пер. с англ.- М.: Триумф, 2003.- 815 с.

10. Математичні основи криптогафії. Навч. посібник / Г.В. Кузнецов, В.В. Фомичов, С.О Сушков, Л.Я. Фомичова.- Дніпропетровськ: Національний гірничий університет, 2004.- Ч.1.- 391 с.

11.Горбенко Ю.І., Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія: за заг. ред. І.Д. Горбенко. – Харків : Форт, 2015. – 959 с.

12. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. (ЛК №23). Харків, ХНУРЕ, 2012 р.

13. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

14. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010, 593 с.

15. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: монографія.- Харків: Видавництво "Форт", 2012.- 870 с.

16. Yu. Manin. Computable and uncomputable (in Russian). - Moscow, Sovetskoye Radio. - 1980. - l4-38 pp.

17. R. Feynman. Simulating physics with computers. - International Journal of Theoretical Physics 21, 6&7, - 1982. - 467-488 pp.

18. E. Reiffel, W. Polak. Fundamentals of quantum calculations. - ACM Computing Surveys, V. 12, №3, - September 2000. — 5-62 pp.

19.Браунштейн С. Л. Квантові обчислення: навчальне керівництво. –

Encyclopedia of Applied Physics, Update, W1LEY-VCH. - 1999, - 35 p.
20. P. W. Shor. Algorithm for quantum computation: Discrete log and factoring. – In Proceedings of the 35th Annual Symposium on Foundations of Compute Science, - November 1994. - 124-134 pp.
21. Стин. Квантові обчислення. - Іжевськ: Регулярна й хаотична динаміка, - 2000. - 100 с.
22. B. Omer. Simualtion of Quantum Computers. - Vienna: Technical University of Vienna. - 1996. – 23 p.