Міністерство освіти і науки України
Сумський державний університет

О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко

ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ

Навчальний посібник

Рекомендовано вченою радою Сумського державного університету

Суми
Сумський державний університет
2015

УДК 511.1(075.8)
ББК 22.13я73
О-37

Рецензенти:

К. Г. Малютін – доктор фізико-математичних наук, професор кафедри прикладної та обчислювальної математики Сумського державного університету;

В. Д. Погребний – кандидат фізико-математичних наук, доцент кафедри вищої математики Сумського державного педагогічного університету ім. А. С. Макаренка

Рекомендовано до видання вченою радою
Сумського державного університету
як навчальний посібник
(протокол № 11 від 11 червня 2015 року)

Оглобліна О. І.

О-37 Елементи теорії чисел : навч. посіб. / О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. – Суми : Сумський державний університет, 2015. – 186 с.

ISBN 978-966-657-584-8

У навчальному посібнику розглянуті арифметичні основи теорії цілих чисел та теорія конгруенцій. Весь викладений теоретичний матеріал підкріплений великою кількістю прикладів розв'язування задач. Посібник може бути використаний як для аудиторного вивчення матеріалу, так і для самостійної підготовки, оскільки містить тестові та інші завдання в кількості, достатній для забезпечення індивідуальної роботи кожного студента.

Посібник підготовлений для студентів вищих навчальних закладів III–IV рівнів акредитації спеціальностей, пов'язаних із математикою, інформатикою та безпекою інформації.

УДК 511.1(075.8)
ББК 22.13я73

ISBN 978-966-657-584-8

Навчальне видання

Оглобліна Олена Іванівна,
Сушко Тетяна Сергіївна,
Шрамко Юрій Вікторович

ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ

Навчальний посібник

Художнє оформлення обкладинки Р. С. Приходченка
Редактор Н. В. Лисогуб
Комп'ютерне верстання Н. О. Молдаванової

Формат 60×84/16. Ум. друк. арк. 10,93. Обл.-вид. арк. 8,12. Тираж 300 пр. Зам. №

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.2007.

ЗМІСТ

С.

ПЕРЕДМОВА

Посібник побудований за матеріалами курсу «Застосування теорії чисел у криптографії», що викладався в Сумському державному університеті упродовж п’яти років студентам спеціальностей «Інформатика» та «Прикладна математика», та містить базові розділи теорії чисел, необхідні для подальшого вивчення методів криптографії та криптології.

У розділах 1, 2 наведені арифметичні основи алгебри цілих чисел: подільність цілих чисел та деякі важливі функції теорії чисел. У розділах 3–7 розглядається алгебра конгруенцій.

Розділи посібника містять питання для самоперевірки, тести та індивідуальні завдання для виконання самостійної контрольної роботи за матеріалами кожного розділу. У додатках до посібника наведені відповіді до тестових завдань, таблиці індексів, таблиці простих чисел та їх найменших первісних коренів.

Посібник може бути використаний як для аудиторного, так і для самостійного вивчення матеріалу курсу «Елементи теорії чисел», окремих розділів курсів «Алгебра та геометрія» і «Дискретна математика» та як допоміжний матеріал у рамках вивчення курсів «Криптологія» і «Захист інформації».

РОЗДІЛ 1 ПОДІЛЬНІСТЬ ЦІЛИХ ЧИСЕЛ

1.1 Основні поняття та теореми

Теорія чисел розглядає властивості цілих чисел, тобто чисел класу $Z = 0, \pm 1, \pm 2...$. Сума та добуток цілих чисел є цілими числами, але про результат ділення двох цілих чисел такого стверджувати вже не можна.

Означення 1.1 Для довільних цілих чисел a і b визначається, що b ділить a (a ділиться на b), якщо існує таке ціле число q, для якого виконується рівність

$$a = b \cdot q. \tag{1.1}$$

Позначається цей факт так: $b \mid a$. При цьому b називається *дільником* a, число a за таких умов називається *кратним* b.

Означення 1.2 Власним дільником a називається будь-який додатний дільник a, що не дорівнює a. Нетривіальним дільником a називається будь-який додатний дільник a, який не дорівнює 1 та a.

Означення 1.3 Простим числом є ціле число, яке має дільники тільки 1 та a. Ціле число, яке має хоча б один нетривіальний дільник, називається *складеним* числом.

Властивості подільності цілих чисел

1. Якщо $b \mid a$ і c – будь-яке додатне ціле число, то $b \mid a \cdot c$.

2. Якщо $b \mid a$ та $c \mid b$, то $c \mid a$.

3. Якщо $b \mid a$ та $b \mid c$, то $b \mid a + c$.

У з а г а л ь н е н н я

Якщо у рівності $k + l + ... + n = p + q + ... + s$ про всі числа, крім одного, відомо, що вони кратні числу b, то і це останнє є кратним b.

Теорема 1.1 (про ділення із залишком)

Будь-яке ціле число a єдиним способом подається за допомогою додатного цілого числа b рівністю

$$a = b \cdot q + r, \quad 0 \le r < b, \tag{1.2}$$

де q – неповна частка; r – залишок.

Очевидно, що за умови $r = 0$, q є повною часткою, а $b \mid a$.

Якщо просте число p є неоднократним дільником довільного цілого числа a (число a ділиться на p α-разів, α – ціле невід'ємне число), то цей факт будемо позначати так: $p^{\alpha} \mid a$. У цьому випадку $p^{\alpha} \mid a$, а $p^{\alpha+1} \nmid a$.

1.2 Найбільший спільний дільник

Не нехтуючи загальною теорією, у подальшому будемо розглядати тільки додатні дільники чисел.

Означення 1.4 Будь-яке ціле d_i, яке одночасно ділить числа $a, b, ..., l$, має назву спільного дільника цих чисел. Найбільший із всіх дільників має назву найбільшого спільного дільника (НСД) і позначається

$$d = (a, b, ..., l). \tag{1.3}$$

Означення 1.5 Якщо $(a, b, ..., l) = 1$, то числа $a, b, ..., l$ взаємно прості. Якщо кожне число із наведеного набору є взаємно простим із кожним іншим числом цього набору, то ці числа попарно прості. Попарно прості числа є одночасно і взаємно простими, але не навпаки.

Приклад 1.1

Числа 6, 10, 15 взаємно прості, оскільки $(6,10,15) = 1$, але вони не попарно прості. Числа 7, 13, 23 – попарно прості,

оскільки $(7,13)=(7,23)=(13,23)=1$ і одночасно вони взаємно прості.

Властивості НСД двох цілих чисел a і b

1. Якщо $b \mid a$, то $(a,b)=b$ і кількість дільників у чисел a та b дорівнює кількості дільників b.

2. Якщо $a=bq+r$, то кількість дільників a дорівнює кількості спільних дільників b та r, зокрема $(a,b)=(b,r)$ (за теоремою 1.1).

3. Якщо $a_0=cq_0+r_0,\ a_1=cq_1+r_1,...,\ a_n=cq_n+r_n \Rightarrow$ $\Rightarrow (a_0,\ a_1,...,a_n,\ c)=(c,\ r_0,\ r_1,...,r_n)$.

Алгоритм Евкліда для знаходження НСД двох чисел a і b

Цей алгоритм ґрунтується на попередніх твердженнях. Розглянемо a та b, причому $a \geq b$. Тоді можна записати обмежений ланцюжок ділень із залишком:

$$
\begin{aligned}
&a=bq_0+r_1; \quad 0<r_1<b\\
&b=r_1q_1+r_2; \quad 0<r_2<r_1\\
&r_1=r_2q_2+r_3; \quad 0<r_3<r_2\\
&.....\\
&r_{n-2}=r_{n-1}q_{n-1}+r_n; \qquad 0<r_m<r_{m-1}\\
&r_{n-1}=r_nq_n
\end{aligned}
$$

Останнє ділення – ділення без залишку, тобто $r_n \mid r_{n-1}$.

Досліджуючи цей ланцюжок з останнього ділення уверх, отримаємо:

$$r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow (r_{n-2},r_{n-1})=r_n;$$

$$r_n \mid r_{n-2} \Rightarrow r_n \mid r_{n-3} \Rightarrow (r_{n-3},r_{n-2})=(r_{n-2},r_{n-1})=r_n;$$

.....

$$r_n \mid r_1 \Rightarrow r_n \mid b \Rightarrow (b, r_1) = ... = r_n;$$

$$r_n \mid b \Rightarrow r_n \mid a \Rightarrow (a, b) = ... = r_n.$$

Отже, сукупність дільників a і b дорівнює сукупності дільників їхнього НСД.

НСД a та b дорівнює *останньому ненульовому залишку* в ланцюжку ділень за алгоритмом Евкліда.

Теорема 1.2 (узагальнення алгоритму Евкліда)

Спільний дільник двох довільних цілих чисел $d = (a, b)$ можна єдиним способом подати лінійною комбінацією цих чисел:

$$d = ax + by, \quad x, y \in Z,\ x \neq 0,\ y \neq \text{ одночасно.}$$

Доведення теореми випливає з алгоритму Евкліда, якщо всі залишки, починаючи з $r_n = d$, поступово виразити через попередні залишки, а потім і через a та b.■

Приклад 1.2

Знайти НСД $a = 648$ та $b = 261$.

►Шукаємо НСД

$\frac{648}{261}$: $648 = 261 \cdot 2 + 126,\ a = bq_0 + r_1,\ r_1 = 126,\ 0 < 126 < 261,$

$\frac{261}{126}$: $261 = 126 \cdot 2 + 9,\ b = r_1 q_1 + r_2,\ r_2 = 9,\ 0 < 9 < 126,$

$\frac{126}{9}$: $126 = 9 \cdot 14 + 0,\ r_3 = 0.$

Останній ненульовий залишок – $r_2 = 9$.

Отже, $(648, 261) = 9$.◄

Приклад 1.3

Знайти $x, y:\ d = ax + by$.

►Шукаємо подання НСД лінійною комбінацією:

$d = r_2 = b - r_1 q_1;\ r_1 = a - bq_0 \Rightarrow$

$\Rightarrow d = b - (a - bq_0) q_1 = a(-q_1) + b(1 + q_0 q_1) =$

$= -2a + (1+4)b = -2a + 5b$

Отже, $x = -2,\ y = 5$.◄

Деякі властивості НСД

1. Якщо $(a,b) \Rightarrow \forall m \in Z : (am, bm) = m(a,b)$.

2. Якщо $\delta \mid a,\ \delta \mid b,\ \forall \delta \in Z \Rightarrow \left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{\delta}$, зокрема $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \frac{(a,b)}{(a,b)} = 1$, тобто два будь-яких цілих числа, поділених на НСД цих чисел, є взаємно простими числами.

3. Якщо $(a,b) = 1 \Rightarrow (ca, b) = (c, b)$.

4. Якщо $(a,b) = 1.\ b \mid ac \Rightarrow b \mid c$.

5. Якщо $a_1, a_2, ..., a_m$ взаємно прості з кожним із $b_1, b_2, ..., b_n$, то добуток $a_1 \cdot a_2 \cdot ... \cdot a_m$ взаємно простий із добутком $b_1 \cdot b_2 \cdot ... \cdot b_n$.

1.3 Найменше спільне кратне

Означення 1.6 Дані числа $a_1, a_2, ..., a_m$. 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 $a=a_1d,\ b=b_1d$ і $(a_1,b_1)=1$ (властивості НСД, 2.) Нехай M – деяке кратне a та b, тобто $M=ka$ і $\frac{M}{b}=\frac{ka}{b}=\frac{ka_1d}{b_1d}=\frac{ka_1}{b_1}\in Z$. Оскільки $(a_1,b_1)=1$, то k повинно ділитися на b_1, тобто $k=b_1t$. Для СК буде правильною формула

$$M=ka=ak=ab_1t=\frac{ab_1d}{d}t=\frac{a\cdot b}{d}t.$$

Найменше значення СК буде за умови, що $t=1$, тобто для НСК виконується формула

$$m=\frac{ab}{(a,b)}, \text{ тоді } M=m\cdot t. \qquad (1.4)$$

Теорема 1.3

Сукупність спільних кратних чисел a та b дорівнює сукупності кратних для їхнього НСК.

Теорема 1.4

НСК a та b дорівнює відношенню добутку цих чисел до їхнього НСД.

1.4 Прості числа

Базові вислови для простих чисел

1. Число 1 має тільки один додатний дільник – самого себе. Одиниця стоїть осторонь у ряду натуральних чисел.

2. Найменший дільник, що не дорівнює 1, для будь-якого цілого числа є числом простим. Дійсно, візьмемо число a і його найменший дільник $q\neq 1$. Припустимо, що $q=q_1\cdot r,\ q_1\le q,\ r\le q$. Тоді a ділиться на q_1 і на r, тобто a має дільник, менший за q, що суперечить вихідному припущенню.

3. Найменший дільник, що не дорівнює 1, для будь-якого складеного цілого числа a не перевищує значення $\sqrt{a}$. Дійсно, нехай $a = q \cdot c$. Оскільки q – найменший дільник, то $c \geq q$. Отже $ac \geq q^2 c$, $a \geq q^2$, або $q \leq \sqrt{a}$.

4. Простих чисел нескінченно багато (*теорема Ейлера*).

5. Найпростішим методом вибору простих чисел, що не перевищують даного числа N, є метод «*Решето Ератосфена*».

Алгоритм методу

а) Обираємо перше просте число $p_1 = 2$.

б) Викреслюємо всі цілі числа з інтервалу $(2, N)$, кратні 2.

в) Обираємо наступне найменше просте число $p_2 = 3$.

г) Викреслюємо всі цілі числа з інтервалу $(3, N)$, кратні 3.

ґ) Повторюємо процес із наступним $p_3 = 5$.

д) Обираючи чергове p_k, звертаємо увагу на те, що кандидатів на викреслення необхідно розглядати з $p_k{}^2$, оскільки до цього числа всі складені викреслені, як такі, що кратні простим числам, меншим за p_k.

е) Викреслення можна зупинити, коли p_k перевищить $\sqrt{N}$. Усі кратні числа на той час будуть викреслені.

1.5 Розкладання цілого числа на прості множники

Базові вислови для складених чисел

1. Довільне ціле a або взаємно просте з даним простим числом $p < a$, або ділиться на нього.

2. Якщо добуток декількох множників ділиться на просте число p, то хоча б один із множників теж ділиться на p.

3. Фундаментальна теорема арифметики. Довільне ціле число можна розкласти на добуток простих множників єдиним способом (враховуючи комутативність множення)

$$a = p_1 \cdot p_2 \cdot ... \cdot p_n .$$

У наведеному розкладанні деякі з множників можуть повторюватися не один раз. Позначивши через $p_1, p_2, ..., p_k$ тільки різні множники, а через $\alpha_1, \alpha_2, ..., \alpha_k$ відповідні кратності входження множників до числа a, запишемо *канонічне розкладання* довільного цілого числа a на множники:

$$a = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_k}^{\alpha_k} . \qquad (1.5)$$

Нехай $a = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_k}^{\alpha_k}$ – канонічне розкладання довільного цілого числа a. Тоді усі дільники цього числа можна подати у канонічному вигляді:

$$d = {p_1}^{\beta_1} \cdot {p_2}^{\beta_2} \cdot ... \cdot {p_k}^{\beta_k}, \text{ де } 0 \le \beta_i \le \alpha_i, \ \ i = \overline{1,k} . \qquad (1.6)$$

У відповідності до вищенаведеної формули кількість дільників τ довільного цілого числа a можна знайти так:

$$\tau = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1). \qquad (1.7)$$

Розглянемо канонічне розкладання m довільних цілих:

$$a_i = {p_{i1}}^{\alpha_{i1}} \cdot {p_{i2}}^{\alpha_{i2}} \cdot ... \cdot {p_{ik}}^{\alpha_{ik}}, \quad i = \overline{1,m} .$$

Тоді **НСД** цих чисел у канонічному вигляді матиме вигляд

$$d = p_{i1}^{\min\limits_{i=1,m}(\alpha_{i1})} \cdot p_{i2}^{\min\limits_{i=1,m}(\alpha_{i2})} \cdot \ldots \cdot p_{ik}^{\min\limits_{i=1,m}(\alpha_{ik})}, \quad i = \overline{1,m},$$

а **НСК**

$$m = p_{i1}^{\max\limits_{i=1,m}(\alpha_{i1})} \cdot p_{i2}^{\max\limits_{i=1,m}(\alpha_{i2})} \cdot \ldots \cdot p_{ik}^{\max\limits_{i=1,m}(\alpha_{ik})}, \quad i = \overline{1,m}.$$

Сукупність спільних дільників декількох цілих чисел збігається з кількістю дільників їхнього НСД.

НСК декількох взаємно простих чисел дорівнює їх добутку, а сукупність кратних декількох чисел дорівнює сукупності кратних їхнього НСК.

Приклад 1.4

Побудувати канонічну форму чисел 12348 та 867, знайти їх НСД та НСК.

►Число 12348 за ознаками ділення ділиться на $4(2^2)$ і на 9 (3^2).

$12348 = 3087 \cdot 2^2 = 2^2 \cdot 3^2 \cdot 343 = 2^2 \cdot 3^2 \cdot 7^3$ – канонічне розкладання першого числа. Дільників у першого числа буде $\tau = (2+1)(2+1)(3+1) = 36$.

$867 = 3 \cdot 17^2$ – канонічне розкладання другого числа. Дільників у другого числа буде $\tau = (1+1)(2+1) = 6$: 1, 3, 17, 289, 51 та 867.

НСД – $d = (12348, 867) = 2^{\min(2,0)} 3^{\min(2,1)} 7^{\min(3,0)} 17^{\min(0,2)} = 3$.

НСК – $m = 2^{\max(2,0)} 3^{\max(2,1)} 7^{\max(3,0)} 17^{\max(0,2)} = 2^2 3^2 7^3 17^2 =$
$= 4235364$.◄

1.6 Ознаки подільності чисел

Загальні принципи

Будь-яке ціле $(n+1)$-значне число можна подати у десятковій системі так:

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0;$$

$$0 \le a_i \le 9; \quad i = \overline{0,n}.$$

Застосовують ще один запис числа N як послідовності цифр:

$$N = \overline{a_n a_{n-1} ... a_2 a_1 a_o}; \quad 0 \le a_i \le 9; \quad i = \overline{0,n}.$$

Вирішити питання подільності числа N на будь-яке інше число k можна, розглянувши послідовність залишків від ділення степенів основи числення на k:

$$r_0 = a_0 - k \cdot q_0; \quad r_1 = 10 - k \cdot q_1;$$

$$r_2 = 10^2 - k \cdot q_2; ...; r_n = 10^n - k \cdot q_n \ ,$$

де q_i – відповідні неповні частки ділення 10^i, $i = \overline{0,n}$ на k. Очевидно, що залишки r_i, $i = \overline{0,n}$ не перевищують числа k за значенням. Кількість різних цілих залишків менша за k.

Згідно з властивостями такої послідовності залишків щодо k можна вивести відповідне правило подільності цілих чисел на число k.

Ознаки подільності цілого числа N на число k

а) Подільність N на $k = 2$:

$$N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0.$$

Очевидно, що в такому записі числа всі доданки, крім останнього, діляться на 2. Таким чином, для подільності N на 2 необхідно, щоб остання цифра a_0 числа N ділилася на 2 (була парною).

б) Подільність N ***на*** $k=3$ ***та*** $k=9$:

$$N=\left(\underset{n}{99...9}+1\right)a_n+\left(\underset{n-1}{99...9}+1\right)a_{n-1}+...$$

$$...+\left(99+1\right)a_2+\left(9+1\right)a_1+a_0=$$

$$=\left(\underset{n}{9...9}\,a_n+\underset{n-1}{9...9}\,a_{n-1}+...+99a_2+9a_1\right)+$$

$$+\left(a_n+a_{n-1}+...+a_2+a_1+a_0\right).$$

Перший доданок ділиться на 3 та на 9, отже, для подільності N на 3 або на 9 необхідно, щоб сума цифр числа N ділилася на 3 або на 9 відповідно.

в) Подільність N ***на*** $k=4$:

$$N=\left(10^n a_n+10^{n-1}a_{n-1}+...+10^2 a_2+8a_1\right)+\left(2a_1+a_0\right).$$

Отже, для подільності N на 4 необхідно, щоб $2a_1+a_0$ ділилося на 4.

Наприклад, 183 546 976 ділиться на 4, оскільки $7\cdot 2+6=20$, 20 ділиться на 4.

г) Подільність N ***на*** $k=5$:

$$N=10^n a_n+10^{n-1}a_{n-1}+...+10^2 a_2+10a_1+a_0.$$

Усі доданки, крім останнього, діляться на 5, отже, для подільності N на 5 необхідно, щоб остання цифра числа a_0 ділилася на 5.

д) Подільність N ***на*** $k=8$:

$$N=\left(10^n a_n+10^{n-1}a_{n-1}+...+96a_2+8a_1\right)+\left(4a_2+2a_1+a_0\right).$$

Отже, для подільності N на 8 необхідно, щоб число $4a_2+2a_1+a_0$ ділилося на 8.

Відома й інша ознака подільності на 8. Для того щоб все число $N=\overline{a_n a_{n-1}...a_2 a_1 a_o}$ ділилося на 8, необхідно, щоб число $\overline{a_2 a_1 a_0}$ ділилося на 8.

Для визначення подільності на 8 тризначного числа зручно розглянути його у такому вигляді:

$$10\left(10a_2+a_1\right)+a_0=8\left(10a_2+a_1\right)+2\left(10a_2+a_1\right)+a_0.$$

Якщо $2\left(10a_2+a_1\right)+a_0$ ділиться на 8, то і все число ділиться на 8.

Такий спосіб можна застосовувати до чисел, які отримуємо під час перевірки на подільність до того часу, поки подільність не стане очевидною.

Приклад 1.5

Дослідити число 195 347 839 на подільність на 8.

►Визначимо, чи ділиться 839 на 8:

$$839=10\cdot 83+9 \underset{10\leftrightarrow 2}{\Rightarrow} 2\cdot 83+9=175=10\cdot 17+5 \underset{10\leftrightarrow 2}{\Rightarrow}$$

$$\underset{10\leftrightarrow 2}{\Rightarrow} 2\cdot 17+5=39 \Rightarrow 10\cdot 3+9 \underset{10\leftrightarrow 2}{\Rightarrow}$$

$$\underset{10\leftrightarrow 2}{\Rightarrow} 6+9=15=10\cdot 1+5 \underset{10\leftrightarrow 2}{\Rightarrow} 2+5=7.$$

За ознакою число 839 не ділиться на 8 без залишка. Залишок має значення 7. Отже, вихідне число $N=195347839$ при діленні на 8 має залишок 7.

Дійсно, $\dfrac{195347839}{8}=24418479\dfrac{7}{8}$.◄

е) Подільність N на $k=7$:

Для формулювання ознаки подільності на 7 дослідимо послідовність залишків від ділення степенів числа 10 на 7:

$$10=7\cdot 1+3,\ q_1=1,\ r_1=3;$$

$$10^2=100=7\cdot 14+2,\ q_2=14,\ \ r_2=2;$$

$$10^3=1000=7\cdot 142+6,\ \ q_3=142,\ \ r_3=6,$$

або $10^3 = 1000 = 7 \cdot 143 - 1, \quad q_3 = 143, \; r_3 = -1;$

$10^4 = 10000 = 7 \cdot 1428 + 4, \; q_4 = 1428, \; r_4 = 4;$

$10^5 = 100000 = 7 \cdot 14285 + 5, \quad q_5 = 14285, \; r_5 = 5;$

$10^6 = 1000000 = 7 \cdot 142857 + 1, \quad r_6 = 1$.

Після r_6 значення залишків будуть повторюватися, починаючи з $r_1 = 3$. Тим самим отримана послідовність вміщує у собі усі можливі ненульові залишки від ділення довільного степеня числа 10 на 7.

На увагу заслуговують два залишка – залишок від ділення на 7 числа $10^3 \;\; r_3 = -1$ і залишок від ділення на 7 числа $10^6 \;\; r_6 = 1$.

Якщо цифрову послідовність довільного натурального числа $N = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$ розбити на трійки, починаючи з наймолодших позицій, то число набере вигляду

$$N = \ldots + 10^6 a_8 a_7 a_6 + 10^3 a_5 a_4 a_3 + a_2 a_1 a_0 = \ldots + (7 \cdot q_6 + 1) a_8 a_7 a_6 +$$

$$+ (7 \cdot q_3 - 1) a_5 a_4 a_3 + a_2 a_1 a_0 =$$

$$= 7 \cdot N_1 + \ldots + a_8 a_7 a_6 - a_5 a_4 a_3 + a_2 a_1 a_0,$$

де $7 \cdot N_1$ – доданок усіх елементів розкладання числа, які мають у собі множник 7; $\ldots + a_8 a_7 a_6 - a_5 a_4 a_3 + a_2 a_1 a_0$ – сума залишків від ділення числа 10^{3k}, $k \in N$ на 7.

З такого подання числа можна вивести ознаку ділення на 7.

Для того, щоб дізнатись, чи ділиться конкретне число N на 7 без залишка, необхідно попередньо числову послідовність заданого числа розбити на трійки, починаючи з правого краю, пронумерувати трійки, скласти отримані тризначні числа з непарними номерами окремо, з парними – окремо. Далі від суми тризначних чисел із

непарними номерами відняти суму тризначних чисел із парними номерами.

Якщо отримане число ділиться на 7, то вихідне число ділиться на 7.

Якщо отримане число при діленні на 7 має ненульовий залишок, то такий залишок буде мати і вихідне число.

Приклад 1.6

Перевірити, чи ділиться на 7 число 24 135 897 155.

►Розбиваючи число на трійки, починаючи з правого краю, маємо цифри 155, 897, 135, 24. Трійки з непарними номерами 1, 3 – 155 і 135, з парними номерами 2, 4 – 897 і 24. Додаємо окремо трійки з парними і непарними номерами. 155+135=290 – сума трійок із непарними номерами; 897+24=921 – сума трійок із парними номерами, різниця цих сум $290-921=-631$ – число, яке на 7 не ділиться і має залишок $r=-1$ або $r=6$. Отже, вихідне число має залишок від ділення на 7 теж 6 (або –1).

Дійсно, $\frac{24135897155}{7}=3447985307\frac{6}{7}$,

або $\frac{24135897155}{7}=3447985308-\frac{1}{7}$.◄

є) Подільність N ***на*** $k=13$ (ознака аналогічна до ознаки подільності числа на $k=7$). Перевірте самостійно: знайдіть залишки від ділення на 13 чисел 10^3 та 10^6. Порівняйте із залишками від ділення на 7.

Приклад 1.7

Перевірити, чи ділиться на 13 число $N=24135\,897162$.

►Розбиваючи число на трійки, починаючи з правого краю, маємо такі цифри: 162, 897, 135, 24. Трійки з непарними номерами 1, 3 – 162 і 135, з парними номерами 2, 4 – 897 і 24. Додаємо окремо трійки з парними і непарними

номерами. 162+135=297 – сума трійок із непарними номерами; 897+24=921 – сума трійок із парними номерами, різниця цих сум $297-921=-624$. Число 624 на 13 ділиться.

Отже, вихідне число 24 135 897 162 ділиться на 13. $\frac{24135897162}{13}=\boldsymbol{1856607474}$. ◄

ж) Подільність N на числа вигляду $10k\pm1$

Прикладом таких чисел можуть бути числа $19=10\cdot2-1$, $31=10\cdot3+1$, $29=10\cdot3-1$ та ін.

Для визначення ознаки подільності цілого числа $N=\overline{a_n a_{n-1}\ldots a_2 a_1 a_0}$ на $10k\pm1$ подамо вихідне число у такий спосіб: $N=10A+a_0$, $A=\overline{a_n a_{n-1}\ldots a_2 a_1}$.

Якщо число N ділиться на $10k\pm1$, то можна записати: $10A+a_0=(10k\pm1)\cdot q$, де $q\in Z$ – повна частка.

Не порушуючи співвідношення і з метою виділення у лівій частині отриманої рівності частини, що ділиться на $10k\pm1$, множимо її на k з урахуванням, що $(10k+1,k)=1$:

$$k(10A+a_0)=(10k\pm1)\cdot q\cdot k;\quad q\cdot k=q_1\in Z,$$

$$10kA+ka_0=(10k\pm1)\cdot q_1,$$

$$10kA\pm A\mp A+ka_0=(10k\pm1)\cdot q_1,$$

$$A(10k\pm1)\mp A+ka_0=(10k\pm1)\cdot q_1.$$

В останній рівності права частина ділиться на $10k\pm1$, перший доданок у лівій частині – $A(10k\pm1)$ – також ділиться на $10k\pm1$. Отже, з урахуванням властивостей подільності цілих чисел число лівої частини буде ділитися

на $10k \pm 1$ тільки в тому разі, коли $\mp A + ka_0$ ділиться на це число.

Отриману умову подільності можна записати так:

1. Довільне число $N = 10A + a_0$, $A = \overline{a_n a_{n-1} \ldots a_2 a_1}$ ділиться на число $10k + 1$**,** якщо $A - ka_0$ ділиться на це число.

2. Довільне число $N = 10A + a_0$, $A = \overline{a_n a_{n-1} \ldots a_2 a_1}$ ділиться на число $10k - 1$**,** якщо $A + ka_0$ ділиться на це число.

Приклад 1.8

Запишіть умову подільності довільного числа N на число 19.

►Число $19 = 10 \cdot 2 - 1$. Тут $k = 2$, число 19 відповідає умові **2**, тобто довільне число $N = 10A + a_0$, $A = \overline{a_n a_{n-1} \ldots a_2 a_1}$ ділиться на число 19, якщо число $A + 2a_0$ ділиться на 19.◄

Приклад 1.9

Перевірити, чи ділиться число $N = 12\,345687$ на 19.

►Число $N = 12345687;\ A = 1234568,\ a_0 = 7,$

$A + 2a_0 = 1234568 + 14 = 1234582.$

Отримали велике число $N_1 = 1234582$, яке теж необхідно дослідити на подільність на 19, а саме:

$A = 123458,\ a_0 = 2,\ A + 2a_0 = 123458 + 4 = 123462.$

Отримане число завелике, його подільність на 19 не очевидна. Робимо ще один крок:

$A = 12346,\ a_0 = 2,\ \ A + 2a_0 = 12346 + 4 = 12350.$

Процес виконується до того моменту, поки не стане очевидно, що отримане число або ділиться на 19, або не ділиться на нього.

$A=1235,\ a_0=0,\quad A+2a_0=1235+0=1235;$

$A=123,\ a_0=5,\quad A+2a_0=123+10=133;$

$A=13,\ a_0=3,\quad A+2a_0=13+6=19.$

Остання сума ділиться на 19, отже, вихідне число ділиться на 19.

Висновок: число 12 345 687 ділиться на 19. Дійсно, $\frac{12345687}{19}=649773$. ◄

1.7 Неперервні дроби

Будь-яке дійсне число $\alpha\in R$ можна подати як неперервний дріб.

Нехай q_1 – найбільше ціле число, $q_1\le\alpha$. Тоді довільне неціле число $\alpha\in R$ можна подати так: $\alpha=q_1+\frac{1}{\alpha_2},\ \alpha_2>1.$

Відповідно $\alpha_2,\alpha_3,...\alpha_{s-1}\in R$, якщо вони не цілі, їх можна подати як

$$\alpha_2=q_2+\frac{1}{\alpha_3},\quad \alpha_3>1,$$

$$\alpha_3=q_3+\frac{1}{\alpha_4},\quad \alpha_4>1,$$

$$.....$$

$$\alpha_{s-1}=q_{s-1}+\frac{1}{\alpha_s},\quad \alpha_s>1,$$

або $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots\ldots}}$

$$\vdots$$

$$\ldots\ldots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}$$

Якщо α – ірраціональне число, то таке подання буде **нескінченним**.

Якщо ж $\alpha = \frac{a}{b} \in Q$, то неперервний дріб буде скінченний і розкладання можна отримати за допомогою алгоритму Евкліда:

$$a = bq_1 + r_1;\ \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}},$$

$$b = r_1 q_2 + r_2;\ \frac{b}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}},$$

$$r_1 = r_2 q_3 + r_3;\ \frac{r_1}{r_2} = q_3 + \frac{1}{\frac{r_2}{r_3}},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} q_n + r_n;\ \frac{r_{n-2}}{r_{n-1}} = q_n + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_{n+1};\ \frac{r_{n-1}}{r_n} = q_{n+1}.$$

Тоді $\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... \\ \vdots \\ ... + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}$.

Зробимо позначення:

$$\delta_1 = q_1; \quad \delta_2 = q_1 + \frac{1}{q_2}; \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}; ....;$$

$$\delta_s = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... \\ \vdots \\ ..... + \cfrac{1}{q_{s-1} + \cfrac{1}{q_s}}}}.$$

Такі дроби мають назву **підхідні дроби**.

Щоб скласти алгоритм обчислення будь-якого підхіднго дробу δ_i, позначимо $P_0 = 1,\ Q_0 = 0$ та $\frac{a}{b} = \frac{P_s}{Q_s}$. Зауважимо, що у кожному підхідному дробу δ_s досить q_{s-1} замінити на $q_{s-1} + \frac{1}{q_s}$. Тоді

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 \cdot q_2 + 1}{q_2} = \frac{P_1 q_2 + P_0}{1 \cdot q_2 + 0} = \frac{P_1 \cdot q_2 + P_0}{Q_1 \cdot q_2 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_2 q_3 P_1 + P_1 + P_0 q_3}{q_2 q_3 Q_1 + Q_1 + Q_0 q_3} =$$

$$= \frac{q_3 \left(P_1 q_2 + P_0\right) + P_1}{q_3 \left(Q_1 q_2 + Q_0\right) + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1},$$

.....

$$\delta_s = \frac{q_s \cdot P_{s-1} + P_{s-2}}{q_s \cdot Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s}.$$

Отже, для обчислення будь-якого δ_i, $i > 1$ нам необхідно обчислити

$$P_i = q_i \cdot P_{i-1} + P_{i-2} \text{ та } Q_i = q_i \cdot Q_{i-1} + Q_{i-2}.$$

Зручно використовувати схему

i	*0*	*1*	*2*	....	*i-2*	*i-1*	*i*	...	*n-1*	*n*
q_i		q_1	q_2	....	q_{i-2}	q_{i-1}	q_i	....	q_{n-1}	q_n
P_i	1	q_1	P_2	....	P_{i-2}	P_{i-1}	P_i	....	P_{n-1}	*a*
Q_i	0	1	Q_2	....	Q_{i-2}	Q_{i-1}	Q_i	....	Q_{n-1}	*b*

Останні 2 рядки використовуються лише у випадку, коли дріб $\alpha = \frac{a}{b}$ не є скорочуваним.

Приклад 1.10

Розкласти у неперервний дріб $\frac{151}{13}$.

►Дріб такий, що не скорочується. Розкладемо за алгоритмом Евкліда:

$151 = 13 \cdot 11 + 8, \quad q_1 = 11,$

$13 = 8 \cdot 1 + 5, \quad q_2 = 1,$

$8 = 5 \cdot 1 + 3, \quad q_3 = 1,$

$5 = 3 \cdot 1 + 2, \quad q_4 = 1,$

$3 = 2 \cdot 1 + 1, \quad q_5 = 1,$

$2 = 1 \cdot 2, \quad q_6 = 2.$

Отже, $\frac{151}{13} = 11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}}}$.

Розкладання подамо у вигляді схеми.

i	0	1	2	3	4	5	6
q_i		11	1	1	1	1	2
P_i	1	11	12	23	35	58	151
Q_i	0	1	1	2	3	5	13

Тобто дріб $\frac{151}{13}$ має такі підхідні дроби:

$$\delta_1 = \frac{P_1}{Q_1} = 11; \delta_2 = \frac{P_2}{Q_2} = 12; \delta_3 = \frac{P_3}{Q_3} = \frac{23}{2} = 11\frac{1}{2};$$

$$\delta_4 = \frac{P_4}{Q_4} = \frac{35}{3} = 11\frac{2}{3}; \delta_5 = \frac{P_5}{Q_5} = \frac{58}{5} = 11\frac{3}{5}.$$

Якщо проаналізувати схему, можна помітити, що задане число розміщене між двома сусідніми підхідними дробами.◀

Властивості схеми розкладання

1. Для усіх $i > 0$ маємо: $P_i Q_{i-1} - Q_i P_{i-1} = (-1)^i$.

Дійсно, $i = 1$:

$$P_1 Q_0 - Q_1 P_0 = q_1 \cdot 0 - 1 \cdot 1 = -1 = (-1)^1.$$

$i = 2$:

$$P_2 Q_1 - Q_2 P_1 = (q_2 P_1 + P_0) Q_1 - (Q_1 q_2 + Q_0) P_1 =$$
$$= q_2 (P_1 Q_1 - P_1 Q_1) - (P_1 Q_0 - P_0 Q_1) = 0 - (-1) = (-1)^2.$$

і т. д.

2. Для усіх $i > 1$ маємо $\delta_i - \delta_{i-1} = \dfrac{(-1)^i}{Q_i Q_{i-1}}$.

Дійсно, $\delta_i - \delta_{i-1} = \dfrac{P_i}{Q_i} - \dfrac{P_{i-1}}{Q_{i-1}} = \dfrac{P_i Q_{i-1} - P_{i-1} Q_i}{Q_i Q_{i-1}} = \dfrac{(-1)^i}{Q_i Q_{i-1}}$.

3. Для усіх $1 < i < n$ раціональний нескорочуваний дріб $\alpha = \dfrac{a}{b}$ із додатним знаменником завжди розміщений між δ_{i-1} та δ_i, ближче до δ_i.

Питання для самоперевірки до розділу 1

1. Дати визначення простого числа, складеного числа, неповної частки, залишку.
2. Сформулювати основні властивості подільності чисел.
3. Сформулювати теорему про ділення із залишком.

4. У чому полягає різниця між *взаємно простими* і *попарно простими* числами?

5. Дати визначення спільного дільника довільного набору цілих чисел a, b, c, d.

6. Дати означення НСД (a,b).

7. Спираючись на властивості подільності чисел, довести, що якщо числа a,b можна зв'язати рівністю $a = b \cdot q + r$, то $(a,b) = (b,r)$.

8. Сформулювати алгоритм Евкліда для знаходження (a,b).

9. Відомо, що a – довільне число, а p – просте число. Які можливі варіанти (a,p)?

10. Дати визначення НСК $[a,b]$. Який існує зв'язок між (a,b) та $[a,b]$?

11. Яке обмеження існує на найменший дільник числа a?

12. Сформулювати теорему про єдиність канонічного розкладання довільного цілого числа a на прості множники.

13. Що таке неперервний дріб?

14. Довести, що неперервний дріб для раціонального числа завжди має скінченну довжину. Чи правильно це для ірраціональних чисел? Обґрунтуйте свою думку.

15. Що таке підхідний дріб? Якщо взяти два сусідніх підхідних дроби, то де буде розміщене вихідне число?

16. Сформулюйте самостійно схему обчислення підхідних дробів для довільного нескорочуваного раціонального дробу.

17. Які властивості мають підхідні дроби?

18. Використовуючи схему розкладання раціонального числа на неперервні дроби, знайти для двох чисел 197 та 23 розв'язок рівняння $197x + 23y = 1$.

Тест до розділу 1

Для відповіді на питання із блоків 1–7 позначте один правильний варіант.

Для відповіді на питання із блоків 8–9 впишіть числові значення, які вважатимете правильними.

Перевірити правильність відповідей можна за допомогою Додатку А «Таблиці відповідей до тестів».

Блок 1			
1. Власний дільник числа a – це			
A	будь-яке додатне число $b \le a$, таке, що $a = b \cdot q$	**B**	будь-яке додатне ціле число $b < a$, таке, що $a = b \cdot q$
C	будь-яке додатне ціле число $b \le a$, таке, що $a = b \cdot q$	**D**	будь-яке додатне ціле число $b \le a$, таке, що $a = b \cdot q + r$
2. Нетривіальний дільник числа a – це			
A	будь-яке додатне число $1 < b < a$, таке, що $a = b \cdot q$	**B**	будь-яке додатне ціле число $1 < b < a$, таке, що $a = b \cdot q$
C	будь-яке додатне ціле число $1 \le b \le a$, таке, що $a = b \cdot q$	**D**	будь-яке число $b < a$ таке, що $a = b \cdot q + r$
3. Просте число – це			
A	ціле число, яке має тільки нетривіальні дільники	**B**	ціле число, яке має тільки тривіальні дільники
C	ціле число, яке не має дільників	**D**	ціле число $p = 2k + 1$

Блок 2			
1. Чи ділиться число b на 13, якщо відомо, що $169 = 52 + 26k + b, \ \forall k \in Z$			
A	Про кожну складову виразу, крім b, відомо, що він ділиться на 13. Отже, за властивістю 4 подільності чисел заданий вираз ділиться на 13	**B**	Так, оскільки 169 ділиться на 13
		C	Ні, оскільки невідоме значення k
		D	Результат визначити не можливо, оскільки невідоме значення k
2. Чи ділиться число b на 29, якщо відомо, що $116 = 87 + 29k - b, \ \forall k \in Z$			
A	Про кожну складову виразу, крім b, відомо, що вона ділиться на 29. Отже, за властивістю 4 подільності чисел заданий вираз ділиться на 29	**B**	Так, оскільки 116 ділиться на 29
		C	Ні, оскільки невідоме значення k
		D	Результат визначити не можливо, оскільки невідоме значення k
3. Чи ділиться число b на 19, якщо відомо, що $190 = 95 + 76k + b, \ \forall k \in Z$			
A	Про кожну складову виразу, крім b, відомо, що вона ділиться на 19. Отже, за властивістю 4 подільності чисел заданий вираз ділиться на 19	**B**	Так, оскільки 190 ділиться на 19
		C	Ні, оскільки невідоме значення k
		D	Результат визначити не можливо, оскільки невідоме значення k

Блок 3			
1. НСК набору чисел $(a_1, a_2, ..., a_k)$ – це			
A	найменше число, яке	**B**	найбільше число, яке

Блок 3			
	ділить кожне число з набору		ділить кожне число з набору
C	найменше число, яке ділиться на кожне число з набору	**D**	найбільше число, яке ділиться на кожне число з набору
2. Якщо $b \mid a_1,\ b \mid a_2,\ b \mid a_3$, то			
A	b є НСД набору чисел (a_1, a_2, a_3)	**B**	b є НСК набору чисел (a_1, a_2, a_3)
C	b є НСК набору чисел (a_1, a_2, a_3, b)	**D**	b є НСД набору чисел (a_1, a_2, a_3, b)
3. НСД набору чисел $(a_1, a_2, ..., a_k)$ – це			
A	найбільше число, яке ділиться на кожне число з набору	**B**	найменше число, яке ділиться на кожне число з набору
C	найменше число, яке ділить кожне число з набору	**D**	найбільше число, яке ділить кожне число з набору

Блок 4			
1. $(a,b) = 31, [a,b] = 238$. Чому дорівнює ab			
A	31	**B**	238
C	7378	**D**	3689
2. $ab = 333960, [a,b] = 968$. Чому дорівнює (a,b)			
A	345	**B**	690
C	333960	**D**	968
3. $a = 2 \cdot 3^3 13^2 29^3$; $b = 2^5 7^3 13 \cdot 17$. Чому дорівнює (a,b)			
A	338	**B**	26
C	2873	**D**	91936

Блок 5			
1. Числа 7, 13, 36, 25, 31			
A	попарно прості	**B**	не мають спільних дільників
C	мають нетривіальний спільний дільник	**D**	складені
2. Числа 7, 14, 35, 98, 133			
A	взаємно прості	**B**	попарно прості
C	складені	**D**	мають нетривіальний спільний дільник
3. Числа 24, 13, 18, 10, 35			
A	попарно прості	**B**	взаємно прості
C	мають нетривіальний спільний дільник	**D**	складені

Блок 6			
1. $(a,b)=31$, $[a,b]=403$. Чому дорівнює ab			
A	12533	**B**	13
C	12493	**D**	12 103
2. $a=2\cdot3^3 13^2 29^3$; $b=2^5 7^3 13\cdot17$. Чому дорівнює (a,b)			
A	$2^5\cdot3^3\cdot7^3\cdot13^2\cdot17\cdot29^3$	**B**	$2\cdot13$
C	$2\cdot3\cdot7\cdot13\cdot17\cdot29$	**D**	$2\cdot13^2$
3. $(a,b)=6$, $[a,b]=1260$. Чому дорівнює $a\cdot b$			
A	210	**B**	3720
C	1260	**D**	7560

Блок 7			
1. Записати дріб $\frac{a}{b}=\frac{53}{7}$ через ланцюжок неповних часток.			
A	$[7,1,1,5]$	**B**	$[7,1,1,3]$
C	$[7,1,1]$	**D**	$[7,1,2,1,3]$
2. Записати дріб $\frac{a}{b}=\frac{37}{13}$ через ланцюжок неповних часток			
A	$[2,1,5,5]$	**B**	$[2,1,5]$
C	$[2,1,1,5]$	**D**	$[2,1,1,3]$
3. Записати дріб $\frac{a}{b}=\frac{179}{19}$ через ланцюжок неповних часток			
A	$[9,2,2,1,2]$	**B**	$[9,2,2,1]$
C	$[9,2,2,2,2]$	**D**	$[9,2,2,1,3]$

Блок 8		
1.	Маємо неперервний дріб $\frac{a}{b}=[3,1,1,2,5]$. Заповніть порожні клітинки таблиці підхідних дробів	I 0 1 2 3 4 5 q_i 3 1 1 2 5 P_i 1 3 4 7 Q_i 0 1 1 2
2.	Маємо неперервний дріб $\frac{a}{b}=[1,3,1,1,15]$. Заповніть порожні клітинки таблиці підхідних дробів	I 0 1 2 3 4 5 q_i 1 3 1 1 15 P_i 4 5 9 140 Q_i 3 4 7 109

Блок 8

3. Маємо неперервний дріб $\frac{a}{b}=[5,1,1,1,7]$.

Заповніть порожні клітинки таблиці підхідних дробів

I	0	1	2	3	4	5
q_i		5	1	1	1	7
P_i	1			11	17	130
Q_i	0			2	3	23

Блок 9

1. Маємо таблицю неперервних дробів.

I	0	1	2	3	4	5
q_i		20	5	1	1	2
P_i	1	20	101	121	222	565
Q_i	0	1	5	6	11	28

Записати розв'язок рівняння $565x+28y=1$

***x*=____;**
***y*= ____.**

2. Маємо таблицю неперервних дробів.

I	0	1	2	3	4
q_i		11	3	1	5
P_i	1	11	34	45	259
Q_i	0	1	3	4	23

Записати розв'язок рівняння $135x+102y=3$

***x*=____;**
***y*= ____.**

<table>
<tr><th colspan="3">Блок 9</th></tr>
<tr><td>3.</td><td>Маємо таблицю неперервних дробів.
<table>
<tr><td>I</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>q_i</td><td></td><td>15</td><td>7</td><td>1</td><td>3</td></tr>
<tr><td>P_i</td><td>1</td><td>15</td><td>106</td><td>121</td><td>469</td></tr>
<tr><td>Q_i</td><td>0</td><td>1</td><td>7</td><td>8</td><td>31</td></tr>
</table>
Записати розв’язок рівняння
$938x + 62y = 2$</td><td>x=____;
y= ____.</td></tr>
</table>

Індивідуальні завдання до розділу 1

Завдання 1.1 Використовуючи алгоритм Евкліда, знайти НСД та НСК двох чисел.

Вихідні дані			
1.	1232, 1672	16.	7 650, 25 245
2.	5 427, 32 877	17.	25 245, 129 591
3.	29 719, 76 501	18.	46 550, 37 730
4.	738 089, 3 082 607	19.	138 285, 356 405
5.	12 870, 7 650	20.	24 789, 35 286
6.	24 700, 33 250	21.	1 359, 8 211
7.	35 574, 192 423	22.	12 606, 6494
8.	36 372, 147 220	23.	469 459, 579 203
9.	213 239, 512 525	24.	3 327 449, 6 314 153
10.	354 295, 543 440	25.	3 640, 14 300

Вихідні дані			
11.	1 329, 2 136	26.	56 595, 82 467
12.	5 894, 3 437	27.	10 140, 92 274
13.	162 891, 32 176	28.	1 403, 1 058
14.	179 370 199, 4 345 121	29.	72 348, 5 632
15.	41 382, 103 818	30.	32 893, 72 568

Завдання 1.2 Використовуючи третю властивість НСД, знайти НСД трьох чисел.

Вихідні дані			
1.	529, 1 541, 1 817	16.	67 283, 122 433, 221 703
2.	549 493, 863 489, 2 133 125	17.	738 089, 3 082 607, 28 303 937
3.	1 767, 2 223, 11 913	18.	476, 1 258, 21 114
4.	3 445, 4 225, 5 915	19.	572, 5 746, 1 118
5.	19 074, 13 566, 8 211	20.	1 073, 3 683, 34 481
6.	1 012, 1 474, 4 598	21.	988, 2 014, 42 598
7.	2 585, 7 975, 13 915	22.	874, 1 518, 20 142
8.	2 227, 9 911, 952	23.	1 253, 252, 406
9.	2 743, 3 587, 6 963	24.	4 345, 6 523, 10 967
10.	7 683, 5 161, 12 909	25.	5 174, 12 337, 13 403
11.	10 047, 6 749, 16 881	26.	6 766, 16 133, 17 527

Вихідні дані			
12.	11 229, 7 543, 18 867	27.	7 562, 18 031, 19 589
13.	13 593, 9 131, 22 839	28.	9 154, 21 827, 23 713
14.	17 139, 11 513, 28 797	29.	11 542, 27 521, 29 899
15.	18 321, 12 307, 30 783	30.	12 338, 29 419, 31 961

Завдання 1.3 Використовуючи ознаки подільності чисел, дослідити, чи ділиться число a на число m.

$m=35$		$m=39$		$m=55$	
1.	*a=351645*	6.	*a=437931*	11.	*a=747615*
2.	*a=236215*	7.	*a=294177*	12.	*a=502205*
3.	*a=590835*	8.	*a=735813*	13.	*a=1256145*
4.	*a=236810*	9.	*a=294918*	14.	*a=503470*
5.	*a=564655*	10.	*a=703209*	15.	*a=1200485*
$m=31$		$m=91$		$m=29$	
16.	*a=238173*	21.	*a=1559649*	26.	*a=394197*
17.	*a=159991*	22.	*a=1047683*	27.	*a=264799*
18.	*a=400179*	23.	*a=2620527*	28.	*a=662331*
19.	*a=160394*	24.	*a=1050322*	29.	*a=265466*
20.	*a=382447*	25.	*a=2504411*	30.	*a=632983*

Завдання 1.4 Раціональне число a/b задане ланцюжком неповних часток. Побудувати відповідне

найменше раціональне число a/b і знайти розв'язок рівняння $ax+by=1$.

Примітка. Для кожного варіанта у таблиці наведений ланцюжок неповних часток

Вихідні дані					
1.	[2,1,3,4,1,2]	11.	[2,1,1,6,8]	21.	[0,3,1,2,7,1]
2.	[1,1,2,4,5]	12.	[0,3,4,3,2,3]	22.	[3,1,1,1,5]
3.	[2,1,3,4,2,9]	13.	[13,1,4,2,5]	23.	[0,4,1,3,2,5]
4.	[22,3,1,4,7]	14.	[2,1,30,2,3]	24.	[1,24,3,4,5]
5.	[1,25,1,2,3,1,1]	15.	[11,2,3,5,1,1]	25.	[31,5,2,3,1,5]
6.	[1,25,1,2,3,1,1]	16.	[1,13,1,2,5,1,1]	26.	[2,8,1,2,3,1,2]
7.	[2,7,2,1,1,1,4]	17.	[3,7,2,5,1,1,2]	27.	[2,41,2,3,1]
8.	[2,17,1,5,1]	18.	[3,19,1,1,3]	28.	[2,1,1,3,5,1,1]
9.	[2,11,3,19,1,1,3]	19.	[5,9,3,11,1,1,2]	29.	[21,1,3,7,1,1,3]
10.	[2,23,1,2,3,1,2]	20.	[3,29,1,1,2,2]	30.	[1,47,1,1,2,1,2]

РОЗДІЛ 2 НАЙВАЖЛИВІШІ ФУНКЦІЇ В ТЕОРІЇ ЧИСЕЛ

2.1 Функції виділення цілої та дробової частин числа

Означення 2.1 Функція виділення цілої частини дійсного числа x повертає найбільше ціле число, яке не перевищує x:

$$\left[x\right] = N; \quad x = N + q; \quad N \in Z; \; 0 < q < 1. \tag{2.1}$$

Наприклад, $\left[-100\right] = -100; \; \left[45,9\right] = 45; \; \left[-5,1\right] = -6.$

Означення 2.2 Функція виділення дробової частини дійсного числа x повертає різницю між числом x та його цілою частиною $\left[x\right]$:

$$\left\{x\right\} = x - \left[x\right] = q; \qquad 0 < q < 1. \tag{2.2}$$

Наприклад, $\left\{-100\right\} = 0; \; \left\{45,9\right\} = 0,9; \; \left\{-5,1\right\} = 0,9.$

Приклад 2.1

Визначити степінь α простого числа p, з яким це число входить до числа $n!$.

►Застосуємо функцію виділення цілої частини.

У числі $n!$ множників, які кратні p, буде $\left[\frac{n}{p}\right]$. Серед них множників, кратних p^2, буде $\left[\frac{n}{p^2}\right]$ і т. д. доти, поки $p^k \le n$, а $p^{k+1} > n$. Отже, загальна кількість входжень p до $n!$ буде такою:

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + \left[\frac{n}{p^k}\right].\blacktriangleleft$$

Приклад 2.2

Знайти, з яким степенем число $p = 2$ входить до числа 11!

► $\alpha = \left[\frac{11}{2}\right] + \left[\frac{11}{4}\right] + \left[\frac{11}{8}\right] = 5 + 2 + 1 = 8.$

Дійсно,

$11! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 =$

$= 1 \cdot 2^1 \cdot 3 \cdot 2^2 \cdot 5 \cdot \left(2^1 \cdot 3\right) \cdot 7 \cdot 2^3 \cdot 9 \cdot \left(2^1 \cdot 5\right) \cdot 11.$

Порахувавши усі степені 2, матимемо $1 + 2 + 1 + 3 + 1 = 8$.◄

2.2 Мультиплікативні функції

Означення 2.3

Функція $f(a)$ називається мультиплікативною, якщо для неї виконуються дві умови:

1) $f(a)$ визначена для усіх $a = 0,1,2...$ і хоча б для одного a_0 $f(a_0) = 0$;

2) для будь-яких a_1, a_2 : $(a_1, a_2) = 1$ виконується: $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$.

Наприклад, a^r, де $r \in R$.

Властивості мультиплікативних функцій

1. Для будь-якої мультиплікативної функції $f(1) = 1$.

Доведення. $\forall a \in N$ виконується $(a,1) = 1$, тоді $f(a) = f(a \cdot 1) = f(a) \cdot f(1) \Rightarrow f(1) = 1$.■

Якщо розглянути $a_1, a_2, ..., a_k$ попарно простих чисел, то $f(a_1 \cdot a_2 \cdot ... \cdot a_k) = f(a_1) \cdot f(a_2) \cdot ... \cdot f(a_k)$, зокрема

$$f\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right) \cdot f\left(p_2^{\alpha_2}\right) \cdot ... \cdot f\left(p_k^{\alpha_k}\right).$$

Наприклад, задамо мультиплікативну функцію так: $f(1)=1,\ f(p^{\alpha})=2,\ \forall\alpha>0$. Тоді для довільного цілого числа $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k},\quad \alpha_i>0,\ i=\overline{1,k}$ матимемо

$$f\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right)=f\left(p_1^{\alpha_1}\right)\cdot f\left(p_2^{\alpha_2}\right)\cdot\ldots\cdot a\left(p_k^{\alpha_k}\right)=2^k.$$

Звідси, наприклад,

$$f(1)=1,\ f(2)=2,\ f(7)=2,\ f(9)=f\left(3^2\right)=2,$$

$$f(14)=f(2\cdot 7)=f(2)\,f(7)=4.$$

2. Добуток двох мультиплікативних функцій є функцією мультиплікативною.

Доведення. $f(a)=f_1(a)f_2(a)$ – задана функція.

$$f(a_1,a_2)=f_1(a_1\cdot a_2)\,f_2(a_1\cdot a_2)=$$

$$=f_1(a_1)\,f_1(a_2)\,f_2(a_1)\,f_2(a_2)=$$

$$=\left(f_1(a_1)\,f_2(a_1)\right)\left(f_1(a_2)\,f_2(a_2)\right)=f(a_1)\,f(a_2).\blacksquare$$

3. Нехай $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ – довільне ціле число, $f(a)$ – довільна мультиплікативна функція, $D\,|\,a$ – множина усіх дільників a вигляду $d=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_k^{\beta_k}$, $0\le\beta_i\le\alpha_i,\ i=\overline{1,k}$. Тоді

$$\sum_{D|a}f(d)=\left(1+f(p_1)+f\left(p_1^2\right)+\ldots+f\left(p_1^{\alpha_1}\right)\right)\times$$

$$\times\left(1+f(p_2)+f\left(p_2^2\right)+\ldots+f\left(p_2^{\alpha_2}\right)\right)\cdot\ldots\times$$

$$\times\left(1+f(p_k)+f\left(p_k^2\right)+\ldots+f\left(p_k^{\alpha_k}\right)\right).$$

Доведення. Для доведення необхідно перемножити усі дужки, тоді отримаємо суму усіх дільників:

$$f\left(p_1^{\beta_1}\right)f\left(p_2^{\beta_2}\right)\cdot\ldots\cdot f\left(p_k^{\beta_k}\right)=f\left(p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_k^{\beta_k}\right)=f(d),$$

$0 \le \beta_i \le \alpha_i$. ■

Визначимо кількість дільників числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$. Уведемо мультиплікативну функцію $f(a) = 1$. Розглянемо для цієї функції 3-тю властивість мультиплікативних функцій:

Ліва частина: $\sum_{D|a} f(d) = \sum_{D|a} 1 = 1 + 1 + 1 ...$ – кількість дільників числа a.

Права частина: $(1+\alpha_1)(1+\alpha_2)...(1+\alpha_k)$.

Отже, кількість дільників числа a дорівнює добутку степенів усіх простих чисел, що входять до канонічного розкладання числа, збільшених на 1. Позначимо функцію визначення кількості дільників числа як $\tau(a)$. Тоді

$$\tau(a) = (1+\alpha_1)(1+\alpha_2)...(1+\alpha_k), \qquad (2.3)$$

де $\tau(a)$ – мультиплікативна функція, для якої кількість дільників числа $a = p^{\alpha}$ за умови, що $\alpha > 0$, p – просте число, дорівнює $\tau(p^{\alpha}) = (\alpha + 1)$.

Приклад 2.3

Знайти кількість дільників чисел $a_1 = 27440 \cdot 19$, $a_2 = 84$.

►Спочатку запишемо числа в канонічному вигляді, а потім застосуємо формулу (2.3).

$a_1 = 27440 \cdot 19 = 2^4 \cdot 5^1 \cdot 7^3 \cdot 19^1$, $\tau(a_1) = 5 \cdot 2 \cdot 4 \cdot 2 = 80$,

$a_2 = 84 = 2^2 \cdot 3^1 \cdot 7^1$, $\tau(a_2) = 3 \cdot 2 \cdot 2 = 12$.◄

Запишемо суму дільників числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$.

Для цього введемо мультиплікативну функцію $f(a) = a$ і підставимо її у властивість 3. Матимемо

$$\sum_{D|a} d = \left(1 + p_1 + p_1^{\,2} + ... + p_1^{\,\alpha_1}\right)\left(1 + p_2 + p_2^{\,2} + ... + p_2^{\,\alpha_2}\right)\cdot ...\times$$
$$\times\left(1 + p_k + p_k^{\,2} + ... + p_k^{\,\alpha_k}\right).$$

Ліворуч у формулі стоїть сума усіх дільників числа a. Позначимо цю суму $S(a)$. Праворуч у дужках маємо суми геометричних прогресій із знаменниками $p_1, p_2, ..., p_k$. Використовуючи формулу суми геометричної прогресії для $n = \alpha_i + 1,\ \left(i = \overline{1,k}\right)$ членів, отримаємо

$$S(a) = \frac{1 - p_1^{\,\alpha_1+1}}{1 - p_1} \cdot \frac{1 - p_2^{\,\alpha_2+1}}{1 - p_2} \cdot ... \cdot \frac{1 - p_k^{\,\alpha_k+1}}{1 - p_k}, \text{ або}$$

$$S\left(p_1^{\,\alpha_1} \cdot p_2^{\,\alpha_2} \cdot ... \cdot p_k^{\,\alpha_k}\right) =$$

$$= \frac{p_1^{\,\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\,\alpha_2+1} - 1}{p_2 - 1} \cdot ... \cdot \frac{p_k^{\,\alpha_k+1} - 1}{p_k - 1}.$$

$S(a)$ – мультиплікативна функція, для якої за умови, що $\alpha > 0$, сума дільників числа $a = p^{\alpha}$ дорівнює

$$S\left(p^{\alpha}\right) = \frac{p^{\alpha+1} - 1}{p - 1}. \qquad (2.4)$$

Приклад 2.4

Знайти суму дільників чисел $a_1 = 27440 \cdot 19$, $a_2 = 84$.

►З прикладу 2.3 маємо $a_1 = 2^4 \cdot 5^1 \cdot 7^3 \cdot 19^1$, $a_2 = 2^2 \cdot 3^1 \cdot 7^1$.

Згідно з (2.4) запишемо

$$S(a_1) = S\left(2^4 \cdot 5 \cdot 7^3 \cdot 19\right) = \frac{2^5 - 1}{1} \cdot \frac{5^2 - 1}{4} \cdot \frac{7^4 - 1}{6} \cdot \frac{19^2 - 1}{18} =$$
$$= 1488000.$$

$$S(a_2) = S\left(2^2 \cdot 3 \cdot 7\right) = \frac{2^3 - 1}{1} \cdot \frac{3^2 - 1}{2} \cdot \frac{7^2 - 1}{6} = \frac{5 \cdot 8 \cdot 48}{12} = 160 . \blacktriangleleft$$

З функцією суми дільників числа a – $S(a)$ пов'язаний певний якісний аналіз числа a.

Сума власних додатних дільників числа a може бути:

1) менша, ніж саме число a, число a у цьому разі має назву **„недостатнє число"**;

2) більша, ніж саме число a, тоді a – **„надлишкове число"**;

3) в окремих випадках – дорівнює самому числу a.

Із самим числом a повна сума додатних дільників числа a буде в цьому випадку дорівнювати $2a$.

Означення 2.4 Числа, для яких $S(a) = 2a$, мають назву „досконалі числа".

Для досконалих чисел справедлива теорема.

Теорема 2.1

Число a буде досконалим тоді і тільки тоді, коли воно має вигляд

$a = 2^{k-1}\left(2^k - 1\right);\ k \geq 2;\ \left(2^k - 1\right)$ – просте число.

У теорії чисел доведено, що число $\left(2^k - 1\right)$ буде простим тільки, коли k є простим числом. Числа $\left(2^k - 1\right)$ в теорії чисел мають назву **прості числа Мерсенна**. Кожне число Мерсенна відповідає новому досконалому парному числу.

Приклад 2.5

Визначити, чи є число $a = 8128$ досконалим.

►Візьмемо $k=7$ $P=2^7-1=127$ – просте число Мерсенна.

$a=2^6\left(2^7-1\right)=2^6\cdot 127=\boldsymbol{8128}$.

Згідно з (2.4) обчислимо кількість додатних дільників числа a:

$$S(a)=\frac{2^7-1}{2-1}\cdot\frac{127^2-1}{126}=\frac{127\cdot\left(127^2-1\right)}{126}=$$

$$=\frac{127\cdot(127-1)(127+1)}{126}=127\cdot 128=2\cdot 2^6\cdot 127=2a.$$

Таким чином, число $a=8128$ є досконалим числом, оскільки $S(8128)=2\cdot 8128$, або $S(a)=2a$.◄

Інколи розглядаються в теорії чисел і так звані **„дружні числа”**.

Означення 2.5 Дружніми числами називається пара чисел a та b, якщо

$$S(a)=b \;\;\&\;\; S(b)=a,$$

тобто сума додатних дільників числа a дорівнює b, і сума додатних дільників числа b дорівнює a.

2.3 Функція Ейлера

Означення 2.6 Функція Ейлера – це функція, що визначає для довільного цілого додатного числа a кількість чисел із ряду цілих $0\le b_i\le a-1$, взаємно простих з числом a, тобто таких, що $(a,b_i)=1$. Позначається функція Ейлера $\varphi(a)$.

Приклад 2.6

Записати значення функції Ейлера для чисел $a=\overline{1,5}$ та числа 13.

► $\varphi(1)=1$ – за означенням.

$a=2,\ \varphi(2)=1$ – перед 2 є одне просте число – 1.

$a=3,\ \varphi(3)=2$ – взаємно прості з 3 – 1,2.

$a=4,\ \varphi(4)=2$ – взаємно прості з 4 – 1,3.

$a=5,\ \varphi(3)=4$ – взаємно прості з 5 – 1,2,3,4.

$a=13,\ \varphi(13)=12$ – оскільки 13 – просте, то увесь ряд чисел до цього числа є взаємно простим із ним.◄

Розглянемо канонічне подання довільного цілого $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$. Для довільного цілого функція Ейлера буде мати вигляд

$$\varphi(a)=\varphi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right)=a\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right),$$

або

$$\varphi(a)=\left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)\ldots\left(p_k^{\alpha_k}-p_k^{\alpha_k-1}\right), \quad (2.5)$$

зокрема

1) для $a=p$ – простого числа – $\varphi(p)=p^1-p^0=p-1$.

2) для $a=p^\alpha$ – степені простого числа –

$$\varphi(p)=p^\alpha\left(1-\frac{1}{p}\right)=p^\alpha-p^{\alpha-1}. \quad (2.6)$$

Функція Ейлера є мультиплікативною функцією.

Приклад 2.7

Записати значення функції Ейлера для чисел 28, 101, 225.

► $\varphi(28)=\varphi(2^2)\varphi(7)=(2^2-2)(7-1)=12$.

Числами, взаємно простими з числом 28, будуть числа $(1,3,5,9,11,13,15,17,19,23,25,27)$.

$\varphi(101)=100;\ \ \varphi(225)=(3^2-3)(5^2-5)=6\cdot 20=120$.◄

Питання для самоперевірки до розділу 2

1. Дати визначення функцій виділення цілої та дробової частин дійсного числа α, тобто $[\alpha]$ і $\{\alpha\}$.

2. Записати функції $[\alpha]$ і $\{\alpha\}$ для чисел 25.45; 200; 34.98; -20.89; -145.04; 0.07; -0.07.

3. Яка кількість натуральних чисел, таких, що діляться на 7, розміщена на проміжках $[1, 137]$; $[37, 396]$?

4. Дати визначення мультиплікативної функції. Навести приклади.

5. Дати визначення функцій $\tau(a)$, $S(a)$.

6. Обчислити кількість і суму дільників для чисел 13, 81, 91, 100, 8712.

7. Дати визначення недостатнього числа, надлишкового числа, досконалого числа. Навести приклади.

8. Які числа мають назву простих чисел Мерсенна?

9. Перевірити, чи є число 2096128 досконалим.

10. Дати визначення функції Ейлера.

11. Обчислити функцію Ейлера для чисел із питання 6.

12. Перевірити властивість 2 функції Ейлера для числа $a=6084$.

13. Скільки чисел в інтервалі від 1 до 120 є невзаємно простими з числом 30?

Тест до розділу 2

Для відповіді на питання з блоку 1 позначте один правильний варіант.

Для відповіді на питання з блоку 2 позначте кілька правильних варіантів.

Для відповіді на питання з блоків 3–6 впишіть числові значення, які вважаєте правильними.

Перевірити правильність відповідей можна за допомогою Додатку А «Таблиці відповідей до тестів».

Блок 1			
1. Зазначити, в якому степені входить число 7 до числа 431!			
A	у 61-му степені	**B**	у 70-му степені
C	у 0-му степені	**D**	у 75-му степені
2. Визначити, скількома нулями закінчується число 121!			
A	24	**B**	28
C	0	**D**	31
3. Зазначити, в якому степені входить число 2 до числа 63!			
A	у 60-му степені	**B**	у 57-му степені
C	у 13-му степені	**D**	у 31-му степені

Блок 2			
1. Зазначити, які властивості мають мультиплікативні функції $f(a)$, якщо $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, $p_i -$ прості числа			
A	$f(0) = 1$	**B**	$f(1) = 1$
C	$\forall a_i : f(a_1 \cdot a_2 \cdot ... \cdot a_k) = = \sum_{i=1}^{k} f(a_i)$	**D**	$\forall a_i : f(a_1 \cdot a_2 \cdot ... \cdot a_k) = = \prod_{i=1,k} f(a_i)$

Блок 2			
E	$\forall a_i : (a_1,...,a_k)=1 \Rightarrow$ $\Rightarrow f(a_1 \cdot ... \cdot a_k)=\prod_{i=1,k} f(a_i)$	**F**	$\sum_{D\mid a} f(d)=\prod_{i=1,k} f\left(p_i^{\alpha_i}\right)$
G	$\sum_{D\mid a} f(d)=\prod_{i=1,k}\left[\sum_{s=0}^{\alpha_i} f\left(p_i^{s}\right)\right]$		
2. У наведеному переліку функцій відмітити мультиплікативні функції, якщо $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ...\cdot p_k^{\alpha_k}$, p_i – прості числа			
A	$f(a)=\log_2(a)$	**B**	$f(a)=a^r$
C	$f(a)=(a+c)^r$, $c\in Z$	**D**	$f(a)=e^a$
E	$f(a)=$ $=a\left(1+\frac{1}{p_1}\right)\cdot ...\cdot\left(1+\frac{1}{p_k}\right)$	**F**	$f(a)=$ $=(1+\alpha_1)(1+\alpha_2)...(1+\alpha_k)$
G	$f(a)=\frac{1-p_1^{\alpha_1+1}}{1-p_1}\cdot\frac{1-p_2^{\alpha_2+1}}{1-p_2}\cdot ...\cdot\frac{1-p_k^{\alpha_k+1}}{1-p_k}$		

Блок 3		
№	*Питання*	*Впишіть відповіді*
1.	Обчислити кількість дільників числа $a=3^{11}\cdot 7^2\cdot 13^5\cdot 43^7$	$\tau(a)=$_____
2.	Обчислити кількість дільників числа $a=2^6\cdot 5^7\cdot 13^2\cdot 37^3$	$\tau(a)=$_____
3.	Обчислити кількість дільників числа $a=2^{17}\cdot 5^4\cdot 19^2\cdot 47$	$\tau(a)=$_____

Блок 4		
№	*Питання*	*Впишіть відповіді*
1.	Знайти суму дільників числа $a = 2^5 \cdot 7^2 \cdot 11$	$S(a) =$_____
2.	Знайти суму дільників числа $a = 3^2 \cdot 5^3 \cdot 13$	$S(a) =$_____
3.	Знайти суму дільників числа $a = 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$	$S(a) =$_____

Блок 5		
№	*Питання*	*Впишіть відповіді*
1.	Побудувати досконале число для $k = 5$	$a =$_____
2.	Побудувати досконале число для $k = 11$	$a =$_____
3.	Побудувати досконале число для $k = 13$	$a =$_____

Блок 6		
№	*Питання*	*Впишіть відповіді*
1.	Знайти кількість чисел, менших за число $a = 2^5 \cdot 7^2 \cdot 11$ і взаємно простих із ним	$\varphi(a) =$_____
2.	Знайти кількість чисел, менших за число $a = 3^2 \cdot 5^3 \cdot 13$ і взаємно простих із ним	$\varphi(a) =$_____

Блок 6		
3.	Знайти кількість чисел, менших за число $a = 2^3 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$ і взаємно простих із ним	$\varphi(a) =$_____

Індивідуальні завдання до розділу 2

Завдання 2.1 Оберіть умову завдання і вихідні дані до нього згідно з номером свого варіанта.

В якому степені числа a і b входять до числа $N = n!$			
1.	$a = 3, b = 5, N = 337!$	8.	$a = 3, b = 5, N = 931!$
2.	$a = 2, b = 7, N = 234!$	9.	$a = 2, b = 7, N = 491!$
3.	$a = 2, b = 11, N = 381!$	10.	$a = 3, b = 11, N = 834!$
4.	$a = 3, b = 11, N = 534!$	11.	$a = 2, b = 11, N = 745!$
5.	$a = 5, b = 7, N = 625!$	12.	$a = 5, b = 11, N = 652!$
6.	$a = 2, b = 13, N = 271!$	13.	$a = 7, b = 11, N = 734!$
7.	$a = 5, b = 13, N = 234!$	14.	$a = 3, b = 7, N = 439!$

Скількома нулями закінчується число $N = n!$			
15.	$N = 356!$	23.	$N = 957!$
16.	$N = 428!$	24.	$N = 367!$
17.	$N = 295!$	25.	$N = 841!$
18.	$N = 295!$	26.	$N = 791!$
19.	$N = 650!$	27.	$N = 399!$
20.	$N = 728!$	28.	$N = 923!$
21.	$N = 534!$	29.	$N = 847!$
22.	$N = 749!$	30.	$N = 537!$

Завдання 2.2 Для числа $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ обчислити три мультиплікативні функції:

1) кількість дільників $\tau(a)$;

2) суму дільників $S(a)$;

3) функцію Ейлера $\varphi(a)$.

Вихідні дані			
1.	$a = 2^8 \cdot 3^3 \cdot 13 \cdot 17$	16.	$a = 2^5 5^2 \cdot 7 \cdot 61$
2.	$a = 5^4 \cdot 7^2 \cdot 19$	17.	$a = 3^5 \cdot 7^2 \cdot 11^2 \cdot 79$
3.	$a = 2^3 \cdot 3^4 \cdot 5^3 \cdot 31$	18.	$a = 2^6 \cdot 3^4 \cdot 5^3 \cdot 41$
4.	$a = 2^3 \cdot 3^7 \cdot 7^2 \cdot 59$	19.	$a = 2^7 \cdot 3^2 \cdot 7^2 \cdot 97$
5.	$a = 2^5 \cdot 5^2 \cdot 31 \cdot 43$	20.	$a = 2^9 \cdot 3^4 \cdot 11^2 \cdot 41$
6.	$a = 5^4 \cdot 7^3 \cdot 19 \cdot 41$	21.	$a = 3^7 \cdot 7^3 \cdot 17 \cdot 19$
7.	$a = 3^2 \cdot 5^2 \cdot 11^2 \cdot 23$	22.	$a = 2^6 \cdot 3^5 \cdot 5 \cdot 17$
8.	$a = 2^6 \cdot 3^4 \cdot 5^3 \cdot 41$	23.	$a = 5^2 \cdot 7^3 \cdot 29$
9.	$a = 3^7 \cdot 5^2 \cdot 103$	24.	$a = 3^3 \cdot 7^6 \cdot 17 \cdot 23$
10.	$a = 2^5 \cdot 3^4 \cdot 7^2 \cdot 71$	25.	$a = 3^8 \cdot 11^2 \cdot 19 \cdot 23$
11.	$a = 3^5 \cdot 5^3 \cdot 11 \cdot 13$	26.	$a = 2^6 \cdot 7^2 \cdot 11^2 \cdot 37$
12.	$a = 2^9 \cdot 3^7 \cdot 5^2 \cdot 29$	27.	$a = 3^7 \cdot 5^2 \cdot 7 \cdot 71$
13.	$a = 3^5 \cdot 7^2 \cdot 37 \cdot 41$	28.	$a = 2^6 \cdot 5^3 \cdot 101$
14.	$a = 5^5 \cdot 7^2 \cdot 13 \cdot 43$	29.	$a = 3^3 \cdot 7^2 \cdot 101$
15.	$a = 2^8 \cdot 7^2 \cdot 23 \cdot 53$	30.	$a = 2^9 \cdot 3^4 \cdot 5^3 \cdot 53$

РОЗДІЛ 3 КОНГРУЕНЦІЇ ТА ЇХ ВЛАСТИВОСТІ

3.1 Основні поняття та теореми

Розглянемо ділення із залишком цілих чисел на деяке певне ціле число m, яке будемо називати *модулем*. Подання довільного цілого через неповну частку та залишок розглядалося в п. 1.1: $a = m \cdot q + r, \quad 0 \le r < m$. Серед множини цілих чисел, знайдуться такі, які діленням на модуль m дадуть різні неповні частки і *однаковий залишок*.

Приклад 3.1

Записати ряд чисел, ділення яких на число 7 дає залишок 1.

►За умовою модулем буде число $m = 7$, тоді ряд чисел можна записати так:

$15 = 7 \cdot 2 + 1;\ \ 22 = 7 \cdot 3 + 1;\ \ 50 = 7 \cdot 7 + 1;\ \ 7778 = 7 \cdot 1111 + 1.$◄

Означення 3.1 Числа, які від ділення на модуль m дають рівні залишки r, називаються рівнозалишковими, або конгруентними (порівнянними) за модулем m.

Конгруенція чисел a і b за модулем m записується так:

$$a \equiv b \pmod{m}. \tag{3.1}$$

Читаємо: «Число a конгруентне числу b за модулем m».

Еквівалентними до запису (3.1) конгруенції чисел a і b за модулем m є:

1) $a = mt + b,\ t \in Z$ – тобто a складає конгруенцію із своїм залишком від ділення на модуль.

2) $m \mid a - b$.

Приклад 3.2

Згідно з прикладом 3.1 можемо записати

$15 \equiv 22 \equiv 50 \equiv 7778 \equiv 1 (\mathrm{mod}\, 7)$.

Ділення будь-якого натурального числа можна подати у два способи, наприклад:

$15 = 7 \cdot 2 + 1$, або $15 = 7 \cdot 3 - 6$.

Це відповідає двом поданням через конгруенції:

$15 \equiv 1 (\mathrm{mod}\, 7)$, $15 \equiv -6 (\mathrm{mod}\, 7) = 1 - 7 (\mathrm{mod}\, 7)$. ◄

У загальному випадку будь-яке число можна подати через конгруенцію так

$$a \equiv b (\mathrm{mod}\, m) \text{ або } a \equiv b - m (\mathrm{mod}\, m). \qquad (3.2)$$

Таким чином, поняття конгруенції можна подовжити на цілі від'ємні числа, тобто $b \in Z$.

Властивості конгруенцій

Закони рівностей, які виконуються для конгруенцій

- *Рефлективність* – $a \equiv a (\mathrm{mod}\, m)$.
- *Симетричність* – якщо $a \equiv b (\mathrm{mod}\, m)$, то $b \equiv a (\mathrm{mod}\, m)$.
- *Транзитивність* – якщо $a \equiv b (\mathrm{mod}\, m)$, $b \equiv c (\mathrm{mod}\, m)$, то $a \equiv c (\mathrm{mod}\, m)$.

Інші властивості конгруенцій, що відповідають властивостям рівностей

1. *Додавання конгруенцій.*

$$a \equiv b (\mathrm{mod}\, m);\ c \equiv d (\mathrm{mod}\, m) \Rightarrow a + c \equiv b + d (\mathrm{mod}\, m).$$

Дійсно, $a = m \cdot q_1 + b$, $c = m \cdot q_2 + d$. Додамо ці дві рівності, отримаємо

$$a + c = m \cdot (q_1 + q_2) + b + d, \quad (q_1 + q_2) \in Z,$$

отже, $a + c \equiv b + d (\mathrm{mod}\, m)$.

Властивість поширюється на довільну кількість конгруенцій.

2. Доданок із будь-якого боку конгруенції можна перенести в інший бік із зміною знака:

$$a+b\equiv c\left(\operatorname{mod} m\right)\Rightarrow a\equiv c-b\left(\operatorname{mod} m\right).$$

Дійсно, розглядаючи за законом рефлективності конгруенцію $-b=-b\left(\operatorname{mod} m\right)$, додамо її до вихідної $a+b\equiv c\left(\operatorname{mod} m\right)$, тоді отримаємо $a\equiv c-b\left(\operatorname{mod} m\right)$.

3. Оскільки $mt\equiv 0\left(\operatorname{mod} m\right)$, $t\in Z$, то до кожної з частин конгруенції можна додати будь-яке число, кратне модулю:

$$a\equiv b\left(\operatorname{mod} m\right)\Rightarrow a+mt\equiv b+mt\left(\operatorname{mod} m\right).$$

4. *Множення конгруенцій*

$$a\equiv b\left(\operatorname{mod} m\right);\ c\equiv d\left(\operatorname{mod} m\right)\Rightarrow a=mt+b;\ c=mq+d\Rightarrow$$

$$\Rightarrow ac=m^2tq+mtd+mqb+bd,$$

$$ac=m\left(mtq+qb+td\right)+bd;\ \ mtq+qb+td=t_1\in Z\Rightarrow$$

$$\Rightarrow ac=mt_1+bd\Rightarrow ac\equiv bd\left(\operatorname{mod} m\right).$$

Властивість поширюється на довільну кількість конгруенцій.

5. *Піднесення конгруенції до степеня*

$$\text{Якщо } a\equiv b\left(\operatorname{mod} m\right)\Rightarrow a^n\equiv b^n\left(\operatorname{mod} m\right).$$

6. *Множення конгруенції* на число k

Правильним є $k\equiv k\left(\operatorname{mod} m\right)$, отже, за властивістю 5 маємо $ka\equiv kb\left(\operatorname{mod} m\right)$.

7. У з а г а л ь н е н н я. Якщо у виразі полінома від k змінних із сталими коефіцієнтами

$S = \sum A_{\alpha_1,\ldots,\alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ замінити $A_{\alpha_1,\ldots,\alpha_k}$ на $B_{\alpha_1,\ldots,\alpha_k}$, порівнянним $A_{\alpha_1,\ldots,\alpha_k}$ за модулем m і змінні $x_i \ \left(i = \overline{1,k}\right)$ замінити на порівнянні з ними за модулем m змінні $y_i \ \left(i = \overline{1,k}\right)$, то новий вираз полінома S буде порівнянним із вихідним виразом за модулем m:

$$S = \sum A_{\alpha_1,\ldots,\alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv \sum B_{\alpha_1,\ldots,\alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \left(\operatorname{mod} m\right).$$

Для доведення використовуються властивості 1–6.

Зокрема, для полінома n-го степеня від однієї змінної:

$$a_i \equiv b_i \left(\operatorname{mod} m\right), \ \ x_i \equiv y_i \left(\operatorname{mod} m\right), \left(i = \overline{0,n}\right) \Rightarrow$$

$$\Rightarrow \sum_{i=0}^{n} a_i x^{n-i} \equiv \sum_{i=0}^{n} b_i y^{n-i} \left(\operatorname{mod} m\right).$$

8. Обидві частини конгруенції можна поділити на спільний дільник d, якщо $\left(m,d\right)=1$:

$$a \equiv b \left(\operatorname{mod} m\right), \ \ d \mid a, \ \ d \mid b, \ \ \left(d,m\right)=1 \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \left(\operatorname{mod} m\right).$$

Властивості, що належать тільки конгруенціям

1. Обидві частини конгруенції і модуль можна помножити на одне й те саме число:

$$a \equiv b \left(\operatorname{mod} m\right) \Rightarrow \left(a = mt + b\right) \cdot k \Rightarrow$$

$$\Rightarrow ka = kmt + kb \Rightarrow ka \equiv kb \left(\operatorname{mod} km\right).$$

2. Обидві частини конгруенції і модуль можна розділити на будь-який їх спільний множник d:

$$a \equiv b \left(\operatorname{mod} m\right); \ a = a_1 d; \ b = b_1 d, \ m = m_1 d \Rightarrow$$

$$\Rightarrow \left(a_1 d = m_1 dt + b_1 d\right) \cdot \frac{1}{d} \Rightarrow a_1 \equiv b_1 \left(\operatorname{mod} m_1\right).$$

3. Якщо a та b можуть бути конгруентними за декількома модулями $m_1, m_2, ..., m_n$, то конгруенція a і b правильна і за модулем, що дорівнює НСК модулів $m_1, m_2, ..., m_n$.

Оскільки число $a - b$ ділиться на кожний із модулів $m_1, m_2, ..., m_n$, то воно повинно ділитися і на НСК цих модулів, тобто $a - b \equiv 0 \left(\operatorname{mod} M\right) \Rightarrow \quad a \equiv b \left(\operatorname{mod} M\right)$, $M = НСК\left(m_1, m_2, ..., m_n\right)$.

4. Якщо одна з частин конгруенції і модуль діляться на деяке число, то й інша частина ділиться на це число. $a \equiv b (\operatorname{mod} m),\ a = mt + b,\ c \mid a,\ c \mid m \Rightarrow c \mid b$ (за третьою властивістю подільності).

5. Якщо $a \equiv b \left(\operatorname{mod} m\right) \Rightarrow \left(a, m\right) = \left(b, m\right)$.

3.2 Повна та зведена системи лишків

3.2.1 Повна система лишків

Усі числа, які мають однаковий залишок r від ділення на деякий модуль m, створюють клас чисел за модулем m. Усі числа цього класу можна отримати з формули ділення числа із залишком $a = m \cdot q + r$, якщо надавати неповній частці q усіх значень з множини цілих чисел.

k різним залишкам від ділення за модулем m $(k < m)$ відповідатимуть k різних класів. Модуль m залишками може мати числа $0, 1, 2, ..., m - 1$. Отже, *кількість таких класів* за довільним цілим модулем m становить m.

Означення 3.2 Кожне число з певного класу має назву *лишку щодо усіх інших чисел класу*. Якщо $q=0$, то лишок r є *найменшим додатним лишком*.

Означення 3.3 Найменший лишок за абсолютною величиною називається *абсолютно найменшим лишком* і позначається δ.

Приклад 3.3

Записати класи чисел за модулем 7 та абсолютно найменші лишки за модулем 7.

►Візьмемо за модуль число $m=7$. Тоді найменшими додатними лишками будуть числа $1, 2, 3, 4, 5, 6$. Для кожного з них можна записати клас чисел за модулем 7:

$a_1 = 7\cdot q_1 + 1 \Rightarrow a_1 \equiv 1 \pmod 7$,

$a_2 = 7\cdot q_2 + 2 \Rightarrow a_2 \equiv 2 \pmod 7$,

$a_3 = 7\cdot q_3 + 3 \Rightarrow a_3 \equiv 3 \pmod 7$,

$a_4 = 7\cdot q_4 + 4 \Rightarrow a_4 \equiv 4 \pmod 7$,

$a_5 = 7\cdot q_5 + 5 \Rightarrow a_5 \equiv 5 \pmod 7$,

$a_6 = 7\cdot q_6 + 6 \Rightarrow a_6 \equiv 6 \pmod 7$.

При цьому, створюючи відповідний клас i, $\left(i=\overline{1,6}\right)$, неповна частка q_i пробігає всю множину цілих чисел.

Абсолютно найменшими лишками за модулем 7 будуть числа $-3, -2, -1, 0, 1, 2, 3$.

Якщо порівняти їх із найменшими додатними лишками, можна помітити, що для лишків $r < \frac{m}{2} = \frac{7}{2}$ $\delta = r$, а для $r > \frac{m}{2} = \frac{7}{2}$ $\delta = r - m$.◄

Для побудови множини абсолютно наменших лишків δ за будь-яким модулем m керуються таким: якщо $r < \frac{m}{2}$, то $\delta = r$; якщо $r > \frac{m}{2}$, то $\delta = r - m$.

Зокрема, якщо модуль m є парним числом, то для $r = \frac{m}{2}$ можна за абсолютно найменший лишок брати або $\frac{m}{2}$, або $-\frac{m}{2}$.

Якщо з кожного класу лишків узяти по одному числу, то будемо мати *повну систему лишків*. Кількість повної системи лишків за модулем m є m. Звернемо увагу на те, що числа з двох різних класів *неконгруентні, оскільки мають різні залишки від ділення на модуль*.

Найменші додатні лишки $0, 1, ..., m-1$ складають *повну систему*.

Абсолютно найменші лишки $-\frac{m-1}{2},...,-1, 0, 1,..., \frac{m-1}{2}$ для m непарного і $-\frac{m}{2},...,-1,0,1,..., \frac{m}{2}$ для m парного теж складають *повну систему лишків*.

У з а г а л ь н е н н я

1. Будь-які m чисел, які попарно неконгруентні за модулем m, складають повну систему лишків за цим модулем.

2. Якщо $(a,m)=1$ і у виразі $ax+b,\ b \in Z$ x пробігає усі значення повної системи лишків за модулем m, то $ax+b$ теж набирає усіх значень повної системи лишків.

Приклад 3.4

Перевірити, чи становить задана сукупність чисел $(9,2,16,20,27,39,46,85)$ повну систему лишків за модулем 8.

►Повною системою лишків за модулем 8, складеною з найменших додатних лишків, є $(0,1,2,3,4,5,6,7)$. Необхідно впевнитися, що ця сукупність чисел становить конгруенції за модулем 8, такі, що входять до повної системи.

$$9 \equiv 1 \bmod(8),\ 2 \equiv 2 \bmod(8),\ 16 \equiv 0 \bmod(8),\ 20 \equiv 4 \bmod(8),$$

$$27 \equiv 3 \bmod(8),\ 39 \equiv 7 \bmod(8),\ 46 \equiv 6 \bmod(8),\ 85 \equiv 5 \bmod(8).$$

Задана сукупність чисел конгруентна лишкам із повної системи, але розміщеним у іншому порядку. Отже, вихідна система є повною системою лишків.◄

3.2.2 Зведена система лишків

Згідно із властивістю лишків числа одного й того самого класу лишків за модулем m мають з m однаковий НСД:

$$a = m \cdot q_1 + r,\ \ b = m \cdot q_2 + r,\ \ (a,m) = (b,m).$$

Серед множини класів лишків за певним модулем m розглянемо такі класи лишків, у яких $(m \cdot q_i + r, m) = 1$, тобто класи взаємно прості з модулем m. Якщо взяти з кожного такого класу по числу, то складеться *зведена система лишків за модулем* m. Як правило, зведену систему лишків виділяють із найменшої додатної системи лишків або з абсолютно найменшої системи лишків.

Оскільки кількість чисел від 0 до m взаємно простих із m визначається функцією Ейлера $\varphi(m)$, то відповідно і кількість чисел у зведеній системі, і кількість класів, що

відповідають зведеній системі, визначаються функцією Ейлера

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right), \qquad (3.3)$$

де $p_1, p_2, ..., p_k$ – прості числа з канонічного розкладання m.

Приклад 3.5

1) $m = 130 = 2\cdot 5\cdot 13$, $\varphi(130) = (2-1)(5-1)(13-1) = 48$, отже, зведена система лишків за модулем 130 складається із 48 чисел, взаємно простих із 130;

2) $m = 16 = 2^4$, $\varphi(16) = 2^4 - 2^3 = 8$, отже, зведена система лишків за модулем 16 складається з 8 чисел, взаємно простих із 16. Ці числа такі: $1, 3, 5, 7, 9, 11, 13, 15$. Вони і становлять зведену систему лишків для числа 16.◄

У з а г а л ь н е н н я

1. Будь-які $\varphi(m)$ чисел, попарно неконгруентні за модулем m та взаємно прості з модулем, *створюють зведену систему лишків.*

2. Якщо $(a,m) = 1$ і x пробігає усі значення зведеної системи лишків за модулем m, то ax теж набирає всіх значень зведеної системи лишків.

3.3 Системи лишків як структури теорії груп

Базові означення з теорії поля

Як відомо з вищої алгебри, абелева (комутативна) **група** – це множина F, на якій визначена одна бінарна операція $(\bullet)$ з такими властивостями $\forall a, b \in F$:

1. $\exists c \in F:\ a \bullet b = c$ – замкненість,
2. $a \bullet b = b \bullet a$ – комутативність,

3. $\forall c \in F:\ a \bullet b \bullet c = (b \bullet a) \bullet c = a \bullet (b \bullet c)$ – 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:

а) за адитивною операцією множина створює абелеву групу;

б) за мультиплікативною операцією всі ненульові елементи множини створюють абелеву групу;

в) виконується дистрибутивний закон.

Кільце відрізняється від поля тим, що за мультиплікативною операцією множина створює півгрупу.

Тепер розглянемо повну систему лишків (наприклад, повну систему найменших додатних лишків) за модулем m, яка створює m попарно не конгруентних класів. Позначимо цю систему

$$(r_1, r_2, ..., r_m),\ 0 \le r_i \le m-1,\ r_i \ne r_j (\mathrm{mod}\, m).$$

На такій системі, враховуючи усі вище наведені властивості, можна розглянути дві бінарні операції: додавання та множення.

Додавання (адитивна операція). Оскільки конгруенції можна додавати без зміни модуля, то результат додавання лишків з різних класів повної системи належатиме до цієї самої системи.

Для операції додавання лишків виконуються такі властивості:

1. $\forall i,\ j=\overline{1,m}:\ r_i+r_j\equiv r_j+r_i(\mathrm{mod}\,m)$ – комутативність;
2. $\forall i,\ j,k=\overline{1,m}:r_i+r_j+r_k\equiv(r_j+r_i)+r_k\equiv r_i+(r_j+r_k)(\mathrm{mod}\,m)$ – асоціативність;
3. $\forall r_i\ \ \exists\ 0+mt\ \ (t\in Z):\ r_i+mt\equiv r_i(\mathrm{mod}\,m)$ – клас, що є нейтральним елементом із додавання;
4. $\forall r_i\ \ \exists\ (-r_i+mt)\ (t\in Z):\ r_i-r_i+mt\equiv 0(\mathrm{mod}\,m)$ – клас, що є оберненим елементом із додавання.

Висновок. Повна система лишків створює абелеву групу із додавання.

Множення (мультиплікативна операція). Оскільки конгруенції можна перемножувати без зміни модуля, то результат множення лишків із різних класів повної системи належатиме до повної системи лишків за тим самим модулем.

Для операції множення лишків виконуються такі властивості, $\forall i,\ j,k=\overline{1,m}$:

1. $r_i\cdot r_j\equiv r_j\cdot r_i\,(\mathrm{mod}\,m)$ – комутативність;
2. $r_i\cdot(r_j+r_k)\equiv r_i\cdot r_j+r_i\cdot r_k\,(\mathrm{mod}\,m)$ – дистрибутивність для лівого множника;
3. $(r_j+r_k)\cdot r_i\equiv r_i\cdot r_j+r_i\cdot r_k\,(\mathrm{mod}\,m)$ – дистрибутивність для правого множника.

Висновок. Повна система лишків створює півгрупу із множення.

Оскільки ніяких обмежень на значення модуля m при цьому не накладалося, то робимо висновок про те, що повна система лишків за будь-яким модулем m з операціями додавання та множення створює кільце.

Для визначення повної системи лишків як поля не вистачає доведення існування єдиного нейтрального

елемента із множення (одиниці) та єдиного оберненого елемента із множення до будь-якого елемента з повної системи лишків, тобто елемента, для якого виконується рівність

$$r_i \cdot x \equiv 1 (\mathrm{mod}\, m).$$

У випадку, коли модулем є *просте число* p, існування одиничного елемента щодо множення для *повної системи лишків* доводить мала теорема Ферма.

Теорема 3.1 (мала теорема Ферма)

Розглядаються цілі додатні числа: довільне ціле a та просте число p. Якщо $(a, p) = 1$, то завжди виконується

$$p \mid a^p - a. \tag{3.4}$$

Якщо записати (3.4) у термінах модульної арифметики, то мала теорема Ферма набирає вигляду

$$a^p - a \equiv 0 (\mathrm{mod}\, p), \tag{3.5}$$

або, використовуючи властивості конгруенцій,

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \tag{3.6}$$

Якщо модуль m є складеним числом, для повної системи лишків, одиничний елемент визначити не можна, але теорема Ейлера доводить існування єдиної одиниці за множенням для *зведеної системи лишків* для довільного цілого модуля.

Теорема 3.2 (теорема Ейлера – узагальнення малої теореми Ферма)

Для двох довільних цілих додатних чисел a та $m > 1$, таких, що $(a, m) = 1$, виконується

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m), \tag{3.7}$$

де $\varphi(m)$ – функція Ейлера, кількість чисел, менших за m і взаємно простих із ним.

Якщо $m = p$ – просте число, то функція Ейлера буде $\varphi(p) = p - 1$, а теорема Ейлера набирає вигляду

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p), \tag{3.8}$$

що відповідає малій теоремі Ферма. Тобто теорема Ейлера поширює результат теореми Ферма на будь-який складний цілий модуль.

Висновки

1. *Одиниця з множення* існує і єдина для повної системи лишків за простим модулем p.

2. За складеним модулем m *одиниця з множення* існує лише на класах *зведеної системи лишків*.

Для існування та єдиності оберненого елемента необхідно спочатку розібратися з конгруенціями, які мають одну невідому величину та методами їх розв'язання (див. розділ 4).

Питання для самоперевірки до розділу 3

1. Сформулюйте умову конгруентності двох чисел a і b.
2. Згадайте основні властивості конгруенцій.
3. Доведіть, що задані конгруенції НЕ мають місця: $6^{89} \equiv 13 (\mathrm{mod} 16)$; $21^{138} \equiv 31 (\mathrm{mod}\, 49)$; $8^{107} \equiv 7 (\mathrm{mod}\, 35)$.
4. У чому полягають необхідна і достатня умови для того, щоб два числа a і b належали до одного класу за модулем m.
5. Дайте визначення лишку за певним модулем, найменшої додатної системи лишків, абсолютно найменшої системи лишків, зведеної системи лишків за певним модулем.

6. Із скількох елементів складається абсолютно найменша система лишків за модулем 13? Назвіть ці елементи.
7. Чи складає система лишків (6, 18, 39, 92, 155) повну систему лишків за модулем 5?
8. Із скількох елементів складається зведена система найменших додатних лишків за модулем 24? Назвіть ці елементи.
9. Сформулюйте малу теорему Ферма.
10. Сформулюйте теорему Ейлера.
11. Чи є комутативними операції додавання та множення в найменшій додатній системі лишків за певним модулем?
12. Яка величина в найменшій додатній системі лишків за певним модулем є нейтральним елементом за додаванням?
13. Чи існує єдиний обернений елемент за додаванням до кожного елемента найменшої додатної системи лишків за певним модулем?
14. Яка величина в найменшій додатній системі лишків за простим модулем є нейтральним елементом за множенням? Яка теорема присвячена цьому питанню?
15. Яку алгебраїчну структуру створює повна система лишків за певним модулем?

Індивідуальні завдання до розділу 3

Завдання 3.1 Знайдіть залишок від ділення.

Вихідні дані			
1.	66^{17} на 7	16.	12^{2751} на 5
2.	178^{52} на 11	17.	11^{1201} на 1000
3.	293^{275} на 48	18.	7^{114} на 100
4.	$5^{50}+13^{100}$ на 18	19.	17^{2001} на 1000

5.	34^{3741} на 26	20.	109^{345} на 14
6.	17^{78} на 100	21.	$5^{70}+7^{50}$ на 12
7.	$2^{100}+3^{100}$ на 5	22.	22^{2342} на 14
8.	1967^{1968} на 11	23.	7^{1199} на 1000
9.	66^{17} на 7	24.	11^{203} на 100
10.	11^{1841} на 7	25.	19^{2402} на 100
11.	178^{2741} на 22	26.	439^{291} на 60
12.	19^{79} на 100	27.	$5^{80}+7^{100}$ на 13
13.	11^{802} на 1000	28.	12^{2751} на 10
14.	383^{175} на 45	29.	3^{157} на 100
15.	117^{53} на 11	30.	7^{332} на 100

РОЗДІЛ 4 КОНГРУЕНЦІЇ З ОДНИМ НЕВІДОМИМ

4.1 Основні відомості

Означення 4.1 Алгебраїчною конгруенцією з одним невідомим називається конгруенція виду

$$\begin{array}{l} f(x) \equiv 0 (\mathrm{mod}\, m), \quad \forall m \in Z, \\ f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \end{array}, \tag{4.1}$$

Означення 4.2. Якщо a_n не ділиться на m, то n називається степенем конгруенції.

Означення 4.3. Розв'язати конгруенцію, означає знайти усі такі x_i, які задовольняють конгруенцію.

Означення 4.4. Дві конгруенції з одним невідомим називаються еквівалентними, якщо всякий розв'язок x однієї конгруенції є розв'язком іншої.

Теорема 4.1

Якщо $x = x_1$ задовольняє конгруенцію (4.1), то довільне число, яке належить до того самого класу лишків за модулем m, що й число x_1, також задовольняє цю конгруенцію, тобто розв'язком буде весь клас чисел $x \equiv x_1 (\mathrm{mod}\, m)$.

Доведення. Твердження теореми безпосередньо випливає з властивостей конгруенцій. Справді, нехай x_2 – будь-яке число, що належить до того самого класу лишків за модулем m, що й x_1; тоді $x_2 \equiv x_1 (\mathrm{mod}\, m)$. За умовою x_1 є розв'язком конгруенції (4.1), тобто має місце тотожна конгруенція $f(x_1) \equiv 0 (\mathrm{mod}\, m)$, але тоді згідно із властивістю 7 конгруенцій матиме місце й конгруенція $f(x_2) \equiv 0 (\mathrm{mod}\, m)$, тобто x_2 також буде розв'язком

конгруенції. Оскільки x_2 – будь-яке число класу $x \equiv x_1 (\mathrm{mod}\, m)$, то весь цей клас задовольнятиме дану конгруенцію.■

Усі розв'язки конгруенції (4.1), що належать до одного класу чисел за модулем m, беруть за **один розв'язок** даної конгруенції. При цьому конгруенція (4.1) має стільки розв'язків, скільки класів чисел її задовольняють.

Приклад 4.1

Розв'язати конгруенцію

$141x^5 - 126x^3 + 196x^2 - 111x + 36 \equiv 0 (\mathrm{mod}\, 7)$.

►Використовуючи властивості конгруенцій, можна спростити дану конгруенцію, враховуючи, що

$141 \equiv 1 (\mathrm{mod}\, 7)$, $-126 \equiv 0 (\mathrm{mod}\, 7)$, $196 \equiv 0 \,\mathrm{mod}(7)$,

$-111 \equiv -6 (\mathrm{mod}\, 7) \equiv 1 \,\mathrm{mod}(7)$, $36 \equiv 1 (\mathrm{mod}\, 7)$.

Конгруенція матиме вигляд $x^5 + x + 1 \equiv 0 (\mathrm{mod}\, 7)$.

Розв'язки будемо обирати з повної системи абсолютно найменших лишків за модулем 7:

$(-3, -2, -1, 0, 1, 2, 3)$.

Легко побачити, що $0, \pm 1$ не є коренями конгруенції. Перевіримо інші значення, використавши схему Горнера, кожний раз зводячи отримані числа до лишків за даним модулем з повної системи абсолютно найменших лишків:

	1	0	0	0	1	1
2	1	2	4≡-3	8≡1	3	7≡0
-2	1	0	4≡-3	0	3≠0 (mod7)	
3	1	-2	-2	2	2≠0 (mod7)	
-3	1	-1	0	1	0	

Із схеми Горнера видно, що конгруенція має два корені з повної системи абсолютно найменших лишків $x_1 = 2,\ x_2 = -3$. Отже, розв'язками цієї конгруенції є два класи:

$x_1 = 7q + 2,\ \left(x_1 \equiv 2 \left(\mathrm{mod}\, 7\right)\right),$

$x_2 = 7q - 3,\ \left(x_2 \equiv -3 \left(\mathrm{mod}\, 7\right)\right).$

Якщо розглянути розв'язки у повній системі найменших додатних лишків, то розв'язок буде такий:

$x_1 = 7q + 2,\ \left(x_1 \equiv 2 \left(\mathrm{mod}\, 7\right)\right),$

$x_2 = 7q + 4,\ \left(x_2 \equiv 4 \left(\mathrm{mod}\, 7\right)\right).$◄

Теорема 4.2

Якщо обидві частини конгруенції (4.1) помножити на ціле число k, взаємно просте з модулем m, то дістанемо конгруенцію, еквівалентну даній.

Доведення. Припустимо, що $x \equiv \alpha \left(\mathrm{mod}\, m\right)$ є деяким розв'язком конгруенції (4.1), тоді $f\left(\alpha\right) \equiv 0 \left(\mathrm{mod}\, m\right)$.

Помножимо обидві частини цієї конгруенції на k, отримаємо $kf\left(\alpha\right) \equiv 0 \left(\mathrm{mod}\, m\right)$. Отже, α є розв'язком і для конгруенції $kf\left(x\right) \equiv 0 \left(\mathrm{mod}\, m\right)$.

В інший бік: якщо α є розв'язком конгруенції $kf\left(x\right) \equiv 0 \left(\mathrm{mod}\, m\right)$, тобто $kf\left(\alpha\right) \equiv 0 \left(\mathrm{mod}\, m\right)$, тоді обидві частини конгруенції можна скоротити на k, не змінюючи модуля, оскільки $\left(k, m\right) = 1$, отже, $f\left(\alpha\right) \equiv 0 \left(\mathrm{mod}\, m\right)$, тобто α є розв'язком конгруенції (4.1), що і доводить наше твердження.■

Зауваження. При розв'язуванні конгруенцій із невідомою величиною можна, не змінюючи модуля, скорочувати обидві частини конгруенції тільки на такий їх спільний дільник, який є взаємно простим із модулем (див. властивість 8, п.3.1).

4.2 Конгруенції першого степеня та методи розв'язання

Конгруенції 1-го степеня мають вигляд

$$ax+b\equiv 0\left(\operatorname{mod} m\right) \text{ або } ax\equiv b\left(\operatorname{mod} m\right). \qquad (4.2)$$

Дослідимо наявність розв'язків у такій конгруенції.

По-перше, розглянемо ситуацію, коли $(a,m)=1.$

Якщо x набирає по черзі всі значення повної системи лишків за модулем m, то і ax теж набирає значення повної системи лишків із точністю до порядку наступності. Отже, x, який є конгруентним до b, є тільки один.

Висновок. За умови, що $(a,m)=1,$ конгруенція $ax\equiv b\left(\operatorname{mod} m\right)$ має **єдиний** розв'язок.

По-друге, розглянемо конгруенцію $ax\equiv b\left(\operatorname{mod} m\right)$ за умови $(a,m)=d>1.$ $ax\equiv b\left(\operatorname{mod} m\right)\Rightarrow ax=b+mt$. Отже, якщо $d\mid a,\ d\mid m\Rightarrow d\mid b$, тоді складові конгруенції можна подати так: $a=a_1d,\ b=b_1d,\ m=m_1d,\ (a_1,m_1)=(b_1,m_1)=1.$ Отже, за властивістю конгруенцій таку конгруенцію можна скоротити на d. Отримаємо конгруенцію $a_1x\equiv b_1\left(\operatorname{mod} m_1\right).$ Із попереднього така конгруенція має єдиний розв'язок $x\equiv x_1\left(\operatorname{mod} m_1\right)$, або $x=m_1t+x_1$. Але якщо розглянути повну систему лишків для модуля $m=dm_1$, можна помітити, що у інтервал $[0,m]$ потрапляють такі розв'язки:

$$x_1,\ x_1+m_1,\ x_1+2m_1,...,x_1+(d-1)m_1,$$

тобто кількість таких розв'язків – d. Ці розв'язки неконгруентні між собою за модулем m, і, у свою чергу, кожний з них створює свій клас лишків.

Висновок. За умови, що $(a,m)=d>1$ конгруенція має хоча б один розв'язок, якщо $d\mid b$. Цих розв'язків є

рівно d (d класів). Перший із розв'язків знаходиться із скороченої на d конгруенції, інші обчислюються як

$$x_2 = x_1 + m_1, ..., x_d = x_1 + (d-1)m_1. \quad (4.3)$$

4.2.1 Використання функції Ейлера

Розглянемо конгруенцію $ax \equiv b(\mathrm{mod}\, m)$, $(a,m)=1$. За теоремою Ейлера в разі, якщо $(a,m)=1$, $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, або, використовуючи рефлективність, $1 \equiv a^{\varphi(m)}(\mathrm{mod}\, m)$.

Перемножимо дві конгруенції: $ax \equiv ba^{\varphi(m)}(\mathrm{mod}\, m)$, або $x \equiv ba^{\varphi(m)-1}(\mathrm{mod}\, m)$.

Розв'язок знайдений, але розв'язання за цим методом доволі часто буває нераціональним через необхідність підносити числа до значних степенів.

4.2.2 Використання властивостей конгруенцій

Застосування цього методу проілюструємо на прикладах 4.2 та 4.3.

Приклад 4.2

Розв'язати конгруенцію $15x \equiv 25(\mathrm{mod}\, 17)$.

►По-перше, розглянемо НСД 15 та 17: $(15,17)=1$, отже, конгруенція має єдиний розв'язок. Спростимо конгруенцію за властивостями: 25 і 15 мають спільний множник 5, який є взаємно простим із модулем 17. Отже, використовуючи властивості конгруенції, можемо поділити конгруенцію на 5: $3x \equiv 5(\mathrm{mod}\, 17)$. Число 5 відповідає абсолютно найменшому лишку -12, який є кратний числу 3, отже, $3x \equiv -12(\mathrm{mod}\, 17)$ скоротимо на 3: $x \equiv -4(\mathrm{mod}\, 17)$. Отже, конгруенція має єдиний розв'язок із повної системи абсолютно найменших лишків за модулем

17, або розв'язок з повної системи найменших додатних лишків $x=-4+17=13$.◄

Приклад 4.3

Розв'язати конгруенцію $5x\equiv 8^{125}-6^{29}(\mathrm{mod}\,7)$.

►$(5,7)=1$ – розв'язок 1. У конгруенції складові можна заміняти відповідними лишками з мінімальних систем (згідно з узагальненням властивостей конгруенції). Отже, $8^{125}-6^{29}\equiv 1^{125}-(-1)^{29}(\mathrm{mod}\,7)$.

Вихідна конгруенція зміниться так:

$5x\equiv 2(\mathrm{mod}\,7)$, $-2x\equiv 2(\mathrm{mod}\,7)$.

Відповідь: $x\equiv -1(\mathrm{mod}\,7)$ або $x\equiv 6(\mathrm{mod}\,7)$.◄

4.2.3 Використання підхідних дробів

Розглянемо випадок $ax\equiv b(\mathrm{mod}\,m)$, $(a,m)=1$.

Розкладемо у неперервний дріб відношення $\dfrac{m}{a}=q_1+\dfrac{1}{q_2+\ldots+\dfrac{1}{q_n}}$.

Будемо мати набір $q_1,q_2,\ldots,q_n$. За відомою схемою побудуємо підхідні дроби $\delta_i=\dfrac{P_i}{Q_i}$. Розглянемо два останніх підхідних дроби:

$$\delta_{n-1}=\frac{P_{n-1}}{Q_{n-1}},\ \delta_n=\frac{P_n}{Q_n}=\frac{m}{a}.$$

Із властивостей підхідних дробів відомо, що

$$P_nQ_{n-1}-Q_nP_{n-1}=(-1)^n,\ \text{отже}\ mQ_{n-1}-aP_{n-1}=(-1)^n.$$

Враховуючи, що Q_{n-1} – це ціле число, можна mQ_{n-1} вважати за модульний період, який можна відкинути. Тобто маємо $aP_{n-1} = (-1)^{n-1} \bmod(m)$. Помножимо ліву і праву частини на число $(-1)^n b$:

$$a(-1)^{n-1} bP_{n-1} \equiv b(\bmod m).$$

Отже, розв'язок конгруенції $x \equiv (-1)^n P_{n-1} b(\bmod m)$.

Приклад 4.4

Розв'язати конгруенцію $256x \equiv 179(\bmod 337)$.

► $(256,337) = 1$ – розв'язок єдиний.

Розкладемо відношення $\frac{337}{256}$ у неперервний дріб:

$\frac{337}{256} = 1 + \frac{81}{256}$; $q_1 = 1$;

$\frac{256}{81} = 3 + \frac{13}{81}$; $q_2 = 3$;

$\frac{81}{13} = 6 + \frac{3}{13}$; $q_3 = 6$;

$\frac{13}{3} = 4 + \frac{1}{3}$; $q_4 = 4$;

$\frac{3}{1} = 3$; $q_5 = 3$.

Будуємо схему.

i	***0***	***1***	***2***	***3***	***4***	***5***
q_i		1	3	6	4	3
P_i	1	1	4	25	104	337
Q_i	0	1	3	19	79	256

За схемою маємо

$n=5,\ P_{n-1}=P_4=104,\ b=179\Rightarrow$

$\Rightarrow x=(-1)^4\,104\cdot 179 \pmod{337};\quad \frac{104\cdot 179}{337}=55+\frac{81}{337}.$

Отже, $x\equiv 81 \pmod{337}$. ◄

4.2.4 Розв'язання конгруенцій окремих типів

Розглянемо розв'язання конгруенцій типу $2^k x\equiv b \pmod{m}$, $(2,m)=(2,b)=1$.

Еквівалентним записом до заданої конгруенції є $2^k x=b+mt$. Обираючи $t=1$ або $t=-1$, отримуємо $b\pm m\equiv 0 \pmod{2^s}$. Чим більший степінь 2, тим краще. Нехай δ – найбільший степінь 2, такий, що $2^\delta \mid b\pm a$.

Якщо $\delta > k$, маємо

$$x=\frac{b\pm m}{2^k} \pmod{m}.$$

Якщо $\delta < k$, то скорочуємо конгруенцію на 2^δ та повторюємо процедуру для еквівалентної конгруенції

$$2^{k-\delta}x=\frac{b\pm m}{2^\delta} \pmod{m}.$$

Приклад 4.5

Розв'язати конгруенцію $256x\equiv 179 \pmod{337}$.

►Число $256=2^8$, отже, можна вихідну конгруенцію подати так: $2^8 x\equiv 179 \pmod{337}$.

Обчислимо

$b+m=179+337=516=2^2 129\Rightarrow b+m\equiv 0 \pmod{4}$,

$b-m=179-337=-158=-2\cdot 79\Rightarrow b-m\equiv 0 \pmod{2}$.

Обираємо $b+m=516$. Найбільший степінь 2, який ділить $b+m$, є $2<8$, отже, переходимо до еквівалентної конгруенції:

а) $2^6 x \equiv 129 (\mathrm{mod}\, 337)$,

$b+m=129+337=466=2\cdot 233,$

$b-m=129-337=-208=-16\cdot 13=-2^4\cdot 13.$

Обираємо $b-m=-2^4\cdot 13$, $\delta=4<6$, отже, переходимо до еквівалентної конгруенції:

б) $2^2 x \equiv -13 (\mathrm{mod}\, 337)$,

$b+m=-13+337=324=4\cdot 81=2^2\cdot 81,$

$b-m=-350=-2\cdot 175.$

Обираємо $b+m=2^2 81$, $\delta=2=k=2$, отже,

$$x=\frac{b+m}{2^2}\,\mathrm{mod}\,(m)=\frac{2^2 81}{2^2}\,\mathrm{mod}\,(337)=81(\mathrm{mod}\, 337).$$

Відповідь: $x=81(\mathrm{mod}\, 337)$ – розв'язок збігається із попереднім. ◄

4.3 Обернений елемент за множенням

Отримавши правила для розв'язання конгруенцій із одним невідомим, можемо дати відповідь на питання: для яких елементів повної системи лишків за довільним модулем m існує обернений елемент з множення?

Щоб дати відповідь на це питання, треба розглянути розв'язання конгруенції

$$ax \equiv 1 (\mathrm{mod}\, m).$$

Виходячи з вимог існування розв'язку такої конгруенції – $(a,m)=1$, оскільки права частина конгруенції дорівнює 1. Якщо за a взяти елементи повної системи лишків (як базу для всіх класів чисел за модулем m), то очевидно, що конгруенція не завжди буде мати розв'язок.

Наприклад, $m=15$, $a=5$. Отже, з повної системи треба відкинути всі елементи, кратні модулю. Отримаємо зведену систему лишків із кількістю $\varphi(m)$ елементів. Для будь-якого елемента зведеної системи за модулем m обернений елемент буде розв'язком конгруенції $ax \equiv 1 (\mathrm{mod}\, m)$:

$$x \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m). \qquad (4.4)$$

Позначимо обернений елемент через a^{-1}.

Отже, для складеного модуля m обернений елемент існує **тільки для його зведеної системи лишків** і для будь-якого елемента a з класу зведеної системи лишків дорівнює

$$a^{-1} \equiv a^{\varphi(m)-1} (\mathrm{mod}\, m). \qquad (4.5)$$

Якщо модуль є простим числом p, то зведена система лишків для нього збігається з повною системою лишків.

Отже, для будь-якого елемента повної системи лишків за простим модулем p обернений елемент заданий та єдиний:

$$a^{-1} \equiv a^{p-2} (\mathrm{mod}\, p). \qquad (4.6)$$

Висновки

1. Повна система лишків за простим модулем p за операцією множення створює *абелеву групу*.

2. Повна система лишків за простим модулем p з заданими на ній операціями додавання і множення створює *поле*. Оскільки кількість елементів у повній системі лишків скінченна, то такі поля теж скінченні і мають назву *полів Галуа*.

4.4 Системи конгруенцій з одним невідомим

Розглянемо систему конгруенцій за різними модулями

$$\begin{cases} a_1 x \equiv b_1 (\bmod m_1), & (a_1, m_1) = 1, \\ a_2 x \equiv b_2 (\bmod m_2), & (a_2, m_2) = 1, \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ a_k x \equiv b_k (\bmod m_k), & (a_k, m_k) = 1 \end{cases} \tag{4.7}$$

з одним невідомим. Будемо вважати також, що модулі $m_1, m_2, ..., m_k$ попарно прості.

Означення 4.5. Розв'язком системи конгруенцій із одним невідомим називається таке ціле число α, яке задовольняє всі конгруенції даної системи (4.7).

По-перше, систему (4.7) можна спростити. Оскільки $(a_i, m_i) = 1, \ i = \overline{1,k}$, то для a_i існує обернений елемент $a_i^{-1}: \ a_i \cdot a_i^{-1} \equiv 1 (\bmod m_i)$. Помноживши кожне рівняння системи на свій обернений елемент, перейдемо до системи, еквівалентної даній:

$$\begin{cases} x \equiv c_1 (\bmod m_1), \\ \ldots \ \ldots \ \ldots \ \ldots \\ x \equiv c_k (\bmod m_k). \end{cases} \tag{4.8}$$

Отже, розв'язавши систему (4.7), ми тим самим знайдемо розв'язок системи (4.8).

Відповідь про існування та структуру розв'язку системи (4.8) дає наступна теорема.

Теорема 4.3 (Китайська теорема про залишки)

Нехай дані k попарно простих чисел $m_1, m_2, ..., m_k$ та чисел $c_1, c_2, ..., c_k$, таких, що $0 \le c_i \le m_i - 1, \quad i = \overline{1,k}$. Тоді

існує таке єдине ціле число α, у якого залишок від ділення на m_i становить c_i (тобто $\alpha \equiv c_i (\mathrm{mod}\, m_i)$).

Доведення. Доводити будемо побудовою числа α. Позначимо через M НСК усіх модулів. Оскільки вони попарно прості, то $M = m_1 m_2 ... m_k$. Далі побудуємо систему чисел

$$M_i = \frac{M}{m_i} = \frac{m_1 m_2 ... m_i ... m_k}{m_i} = m_1 m_2 ... m_{i-1} m_{i+1} ... m_k, \ i = \overline{1,k}.$$

Кожне M_i є взаємно простим із числом m_i, тому для нього існує обернений елемент

$$M_i^{-1} \equiv M_i^{\varphi(m_i)-1} \mathrm{mod}(m_i).$$

Побудуємо число $\alpha = \sum_{i=1}^{k} M_i M_i^{-1} c_i$.

Тоді розв'язком системи (4.8) буде клас лишків, що задовольняє конгруенцію

$$x \equiv \alpha (\mathrm{mod}\, M).$$

Дійсно, підставимо α у першу конгруенцію системи (4.7), матимемо

$$M_1 M_1^{-1} c_1 + M_2 M_2^{-1} c_2 + ... + M_k M_k^{-1} c_k \equiv c_1 (\mathrm{mod}\, m_1).$$

Усі доданки, починаючи з другого, діляться на m_1, оскільки цей модуль наявний у M_i як множник. Тому всі ці доданки конгруентні 0 за модулем m_1. Добуток $M_1 M_1^{-1} \equiv 1 (\mathrm{mod}\, m_1)$ за побудовою, $(M_1, m_1) = 1$. Залишається тотожна конгруенція $c_1 \equiv c_1 (\mathrm{mod}\, m_1)$.

У другому рівнянні неконгруентний 0 за модулем m_2 тільки доданок $M_2 M_2^{-1} c_2$. Отже, α є розв'язком для другої конгруенції і т. д.

Розв'язок підійде кожній конгруенції завдяки своїй структурі.

В и с н о в о к . Розв'язок системи (4.8) існує, і це є клас чисел $x = \alpha + Mt, \quad t \in Z$.■

Приклад 4.6

Розв'язати систему конгруенцій

$$\begin{cases} x \equiv 16 \pmod{13}, \\ x \equiv 128 \pmod{5}, \\ x \equiv 82 \pmod{3}, \\ x \equiv 55 \pmod{7}. \end{cases}$$

►Спершу спростимо систему:

$$\begin{cases} x \equiv 3 \pmod{13}, \\ x \equiv -2 \pmod{5}, \\ x \equiv 1 \pmod{3}, \\ x \equiv -1 \pmod{7}. \end{cases}$$

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 $M_i,\ i = 1,2,3,4$:

$105M_1^{-1} \equiv 1 \bmod(13):\ 105 = 13 \cdot 8 + 1,\ \ 105 \equiv 1 \pmod{13} \Rightarrow,$

$\Rightarrow M_1^{-1} \equiv 1 \pmod{13}.$

$273M_2^{-1} \equiv 1 \bmod(5):\ 273 \cdot 2 = 546 = 545 + 1 \Rightarrow$

$\Rightarrow M_2^{-1} \equiv 2 \pmod{5}.$

$455M_3^{-1} \equiv 1 \bmod(3):\ 455 \cdot 2 = 910 = 909 + 1 \Rightarrow$

$\Rightarrow M_3^{-1} \equiv 2 \pmod{3}.$

$195M_4^{-1} \equiv 1 \bmod(7):\ 195 \cdot 6 = 1170 = 167 \cdot 7 + 1 \Rightarrow$

$M_4^{-1} \equiv 6 \pmod 7 \equiv -1 \pmod 7.$

Будуємо розв'язок:

$$\alpha = 105 \cdot 1 \cdot 3 + 273 \cdot 2 \cdot (-2) + 455 \cdot 2 \cdot 1 + 195 \cdot (-1) \cdot (-1) =$$

$$= 315 - 1092 + 910 + 195 = 328.$$

Перевірка:

$328 = 25 \cdot 13 + 3;\ 328 = 65 \cdot 5 + 3 = 66 \cdot 5 - 2;$

$328 = 109 \cdot 3 + 1;\ 328 = 46 \cdot 7 + 6 = 47 \cdot 8 - 1.$

Система розв'язана правильно.

Відповідь: 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.◄

Якщо у системі (4.7) для будь-якої конгруенції $a_i x \equiv b_i \pmod{m_i}$ $(a_i, m_i) = d > 1,\ d \mid b_i$, то, скорочуючи конгруенцію на d, переходимо до конгруенції $\frac{a_i}{d} x \equiv \frac{b_i}{d} \left(\bmod \frac{m_i}{d} \right)$ і вже цю конгруенцію підставляємо в систему. Якщо для нової системи збереглася попарна простота модулів, то вона має єдиний розв'язок згідно з китайською теоремою про залишки (теорема 4.3). Але в цьому випадку i-та конгруенція має d розв'язків:

$$x \equiv c_i + t_j \frac{m_i}{d} \pmod{m_i}, \quad t_j = \overline{0, (d-1)},$$

отже, необхідно розглянути відповідно d систем, в кожній із яких на $i-$му місці буде стояти відповідний розв'язок конгруенції.

Якщо модулі системи конгруенцій не є попарно простими, тобто $(m_i, m_j) = d > 1$, то для розв'язання системи треба додатково досліджувати існування розв'язку. Якщо він є, то це буде розв'язок за модулем, що дорівнює НСК модулів системи:

$$x \equiv \alpha \left(\operatorname{mod} \text{НСК}\left(m_1, m_2, ..., m_k \right) \right).$$

Розглянемо для прикладу систему із двох конгруенцій. Будемо вважати, що її можна звести до вигляду

$$\begin{cases} x \equiv c_1 \left(\operatorname{mod} m_1 \right), \\ x \equiv c_2 \left(\operatorname{mod} m_2 \right). \end{cases}$$

Нехай $\left(m_1, m_2 \right) = d > 1$, $m_1 = m_1' \cdot d$, $m_2 = m_2' \cdot d$, $\left(m_1', m_2' \right) = 1$. Будемо розв'язувати систему методом підстановки. Із першої конгруенції можна записати

$$x = c_1 + m_1' dt .$$

Розв'язок повинен задовольняти і другу конгруенцію. Підставимо x у другу конгруенцію, отримаємо

$$c_1 + m_1' dt \equiv c_2 \left(\operatorname{mod} m_2' d \right), \quad m_1' dt \equiv c_2 - c_1 \left(\operatorname{mod} m_2' d \right).$$

Отже, виникла умова: якщо $d \mid c_2 - c_1$, то друга конгруенція має розв'язок. В іншому випадку – ні.

Нехай умова виконується. Тоді розглядаємо конгруенцію $m_1' t \equiv \frac{c_2 - c_1}{d} \left(\operatorname{mod} m_2' \right)$. Розв'язком її буде конгруенція $t = \frac{c_2 - c_1}{d} \left(m_1' \right)^{-1} \left(\operatorname{mod} m_2' \right)$. Розв'язок можна подати так:

$$t = \frac{c_2 - c_1}{d} \left(m_1' \right)^{-1} + m_2' t_1 .$$

Підставимо значення t у вираз для x:

$$x = c_1 + m_1' dt = c_1 + m_1' d \left(\frac{c_2 - c_1}{d} \left(m_1' \right)^{-1} + m_2' t_2 \right) =$$

$$= c_1 + m_1'\left(c_2 - c_1\right)\left(m_1'\right)^{-1} + m_1\frac{m_2}{d}t_2 =$$

$$= c_1 + m_1'\left(m_1'\right)^{-1}\left(c_2 - c_1\right) + \frac{m_1 m_2}{d}t_2 .$$

Позначимо $c_1 + m_1'\left(m_1'\right)^{-1}\left(c_2 - c_1\right) = x_1$, $\frac{m_1 m_2}{d} = M$. Тоді розв'язок системи матиме вигляд

$$x \equiv x_1 \left(\mathrm{mod}\, M\right).$$

Висновки

1. Система із двох рівнянь вигляду

$$\begin{cases} x \equiv c_1 \left(\mathrm{mod}\, m_1\right), \\ x \equiv c_2 \left(\mathrm{mod}\, m_2\right), \end{cases}$$

у випадку, якщо $\left(m_1, m_2\right) = d > 1$, матиме розв'язок лише за умови, що $d \mid c_2 - c_1$. В іншому випадку система несумісна. Якщо умова виконана і розв'язок є, він буде знайдений за модулем, який дорівнює НСК m_1 та m_2.

2. Якщо система складається з $k > 2$ конгруенцій за модулями, що мають НСД>1, то перевірку необхідно проводити поступово. У випадку, коли з'ясується в ході розв'язку, що хоча б одна з отриманих конгруенцій розв'язку не має, то і вся система буде несумісною. Якщо розв'язок є, то це буде конгруенція за модулем, що дорівнює НСК усіх модулів.

Питання для самоперевірки до розділу 4

1. Дати визначення алгебраїчної конгруенції з одним невідомим, степеня конгруенції, розв'язку конгруенції.
2. Дати визначення конгруенції першого степеня з одним невідомим. Яка структура є розв'язком конгруенції?
3. За яких умов конгруенція $ax \equiv b \pmod{m}$ має єдиний розв'язок, декілька розв'язків, не має розв'язків?
4. Які конгруенції називаються еквівалентними?
5. Які ви знаєте методи розв'язання конгруенцій першого степеня з одним невідомим?
6. Чи існує єдиний обернений елемент за множенням до кожного елемента найменшої додатної системи лишків за простим модулем? На базі якої теореми можна знайти відповідь на це питання?
7. Яку алгебраїчну структуру створює повна система лишків за простим модулем? Чиїм ім'ям названа ця структура?
8. Дайте визначення розв'язку системи конгруенцій першого порядку з одним невідомим.
9. Сформулюйте Китайську теорему про залишки.
10. За яких умов система конгруенцій розпадається на ряд систем?
11. За яких умов система із двох конгруенцій не матиме розв'язку?

Тест до розділу 4

Для відповіді на питання оберіть один правильний варіант із запропонованих.

Перевірити правильність відповідей можна за допомогою Додатку А «Таблиці відповідей до тестів».

Блок 1			
1.	Скільки розв'язків має конгруенція $26x \equiv 49 (\mathbf{mod}\ 169)$	**A**	Один
		B	13
		C	Жодного
2.	Скільки розв'язків має конгруенція $221x \equiv 68 (\mathbf{mod}\ 391)$	**A**	Один
		B	17
		C	Жодного
3.	Скільки розв'язків має конгруенція $251x \equiv 121 (\mathbf{mod}\ 319)$	**A**	Один
		B	11
		C	Жодного
4.	Скільки розв'язків має конгруенція $91x \equiv 26 (\mathbf{mod}\ 169)$	**A**	Один
		B	13
		C	Жодного
5.	Скільки розв'язків має конгруенція $101x \equiv 26 (\mathbf{mod}\ 169)$	**A**	Один
		B	13
		C	Жодного
6.	Скільки розв'язків має конгруенція $108x \equiv 25 (\mathbf{mod}\ 171)$	**A**	Один
		B	9
		C	Жодного

Блок 2			
1.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 48 (\mathrm{mod}\, 85), \\ x \equiv 14 (\mathrm{mod}\, 51) \end{cases}$	**A**	Один
		B	17
		C	Жодного

Блок 2			
2.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 48 \pmod{85}, \\ x \equiv 34 \pmod{51} \end{cases}$	**A**	Один
		B	7
		C	Жодного
3.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 98 \pmod{143}, \\ x \equiv 72 \pmod{91} \end{cases}$	**A**	Один
		B	7
		C	Жодного
4.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 48 \pmod{203}, \\ x \equiv 13 \pmod{119} \end{cases}$	**A**	Один
		B	7
		C	Жодного
5.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 48 \pmod{203}, \\ x \equiv 24 \pmod{119} \end{cases}$	**A**	Один
		B	7
		C	Жодного
6.	Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 84 \pmod{115}, \\ x \equiv 38 \pmod{161} \end{cases}$	**A**	Один
		B	23
		C	Жодного

Індивідуальні завдання до розділу 4

Завдання 4.1 Знайти обернений елемент для числа a за модулем m.

Вихідні дані			
1.	$a = 142, m = 439$	16.	$a = 37, m = 107$
2.	$a = 221, m = 367$	17.	$a = 93, m = 133$
3.	$a = 97, m = 323$	18.	$a = 91, m = 323$
4.	$a = 97, m = 433$	19.	$a = 47, m = 311$

5.	$a=64, m=743$	20.	$a=93, m=531$
6.	$a=137, m=932$	21.	$a=37, m=217$
7.	$a=41, m=101$	22.	$a=23, m=691$
8.	$a=101, m=931$	23.	$a=137, m=837$
9.	$a=113, m=923$	24.	$a=67, m=691$
10.	$a=71, m=531$	25.	$a=128, m=1025$
11.	$a=95, m=308$	26.	$a=113, m=311$
12.	$a=31, m=142$	27.	$a=137, m=323$
13.	$a=103, m=1031$	28.	$a=59, m=311$
14.	$a=89, m=323$	29.	$a=64, m=531$
15.	$a=83, m=323$	30.	$a=29, m=531$

Завдання 4.2 Розв'язати систему конгруенцій, попередньо спростивши її.

1. $\begin{cases} 913x \equiv 132 \pmod{17}, \\ 138x \equiv 245 \pmod{19}, \\ 457x \equiv 623 \pmod{13}. \end{cases}$

2. $\begin{cases} 913x \equiv 132 \pmod{23}, \\ 138x \equiv 245 \pmod{11}, \\ 457x \equiv 623 \pmod{17}. \end{cases}$

3. $\begin{cases} 913x \equiv 132 \pmod{29}, \\ 138x \equiv 245 \pmod{17}, \\ 457x \equiv 623 \pmod{23}. \end{cases}$

4. $\begin{cases} 253x \equiv 429 \pmod{17}, \\ 338x \equiv 545 \pmod{19}, \\ 579x \equiv 741 \pmod{13}. \end{cases}$

5. $\begin{cases} 253x \equiv 429 \pmod{31}, \\ 338x \equiv 545 \pmod{23}, \\ 579x \equiv 741 \pmod{19}. \end{cases}$

6. $\begin{cases} 253x \equiv 429 \pmod{37}, \\ 338x \equiv 545 \pmod{29}, \\ 579x \equiv 741 \pmod{23}. \end{cases}$

7. $\begin{cases} 353x \equiv 529 \pmod{17}, \\ 138x \equiv 945 \pmod{19}, \\ 279x \equiv 241 \pmod{13}. \end{cases}$

8. $\begin{cases} 353x \equiv 529 \pmod{31}, \\ 137x \equiv 945 \pmod{23}, \\ 279x \equiv 241 \pmod{17}. \end{cases}$

9. $\begin{cases} 353x \equiv 529 \pmod{37}, \\ 137x \equiv 945 \pmod{17}, \\ 279x \equiv 241 \pmod{23}. \end{cases}$

10. $\begin{cases} 347x \equiv 519 \pmod{17}, \\ 438x \equiv 345 \pmod{29}, \\ 271x \equiv 541 \pmod{37}. \end{cases}$

11. $\begin{cases} 347x \equiv 519 \pmod{31}, \\ 438x \equiv 327 \pmod{23}, \\ 271x \equiv 541 \pmod{19}. \end{cases}$

12. $\begin{cases} 347x \equiv 519 \pmod{37}, \\ 438x \equiv 327 \pmod{17}, \\ 271x \equiv 541 \pmod{23}. \end{cases}$

13. $\begin{cases} 547x \equiv 219 \pmod{17}, \\ 639x \equiv 175 \pmod{29}, \\ 371x \equiv 341 \pmod{37}. \end{cases}$

14. $\begin{cases} 547x \equiv 219 \pmod{31}, \\ 638x \equiv 145 \pmod{23}, \\ 371x \equiv 341 \pmod{19}. \end{cases}$

15. $\begin{cases} 547x \equiv 219 \pmod{37}, \\ 638x \equiv 145 \pmod{17}, \\ 371x \equiv 341 \pmod{23}. \end{cases}$

16. $\begin{cases} 747x \equiv 319 \pmod{17}, \\ 838x \equiv 195 \pmod{29}, \\ 571x \equiv 241 \pmod{37}. \end{cases}$

17. $\begin{cases} 747x \equiv 319 \pmod{31}, \\ 838x \equiv 195 \pmod{23}, \\ 571x \equiv 241 \pmod{19}. \end{cases}$

18. $\begin{cases} 747x \equiv 319 \pmod{37}, \\ 838x \equiv 195 \pmod{17}, \\ 571x \equiv 241 \pmod{23}. \end{cases}$

19. $\begin{cases} 437x \equiv 719 \pmod{17}, \\ 925x \equiv 395 \pmod{29}, \\ 771x \equiv 225 \pmod{37}. \end{cases}$

20. $\begin{cases} 437x \equiv 719 \pmod{31}, \\ 925x \equiv 395 \pmod{23}, \\ 771x \equiv 225 \pmod{41}. \end{cases}$

21. $\begin{cases} 437x \equiv 719 \pmod{37}, \\ 925x \equiv 395 \pmod{17}, \\ 771x \equiv 225 \pmod{23}. \end{cases}$

22. $\begin{cases} 333x \equiv 579 \pmod{17}, \\ 1025x \equiv 495 \pmod{29}, \\ 797x \equiv 245 \pmod{37}. \end{cases}$

23. $\begin{cases} 333x \equiv 579 \pmod{31}, \\ 1025x \equiv 495 \pmod{23}, \\ 797x \equiv 245 \pmod{41}. \end{cases}$

24. $\begin{cases} 337x \equiv 525 \pmod{37}, \\ 1025x \equiv 495 \pmod{17}, \\ 797x \equiv 245 \pmod{23}. \end{cases}$

25. $\begin{cases} 733x \equiv 571 \pmod{17}, \\ 625x \equiv 405 \pmod{29}, \\ 707x \equiv 295 \pmod{37}. \end{cases}$

26. $\begin{cases} 733x \equiv 571 \pmod{31}, \\ 625x \equiv 405 \pmod{23}, \\ 707x \equiv 295 \pmod{19}. \end{cases}$

27. $\begin{cases} 733x \equiv 571 \pmod{37}, \\ 625x \equiv 405 \pmod{17}, \\ 707x \equiv 295 \pmod{23}. \end{cases}$

28. $\begin{cases} 398x \equiv 171 \pmod{17}, \\ 925x \equiv 605 \pmod{29}, \\ 507x \equiv 395 \pmod{37}. \end{cases}$

29. $\begin{cases} 398x \equiv 171 \pmod{31}, \\ 925x \equiv 605 \pmod{19}, \\ 507x \equiv 395 \pmod{11}. \end{cases}$

30. $\begin{cases} 398x \equiv 171 \pmod{11}, \\ 925x \equiv 605 \pmod{13}, \\ 507x \equiv 395 \pmod{41}. \end{cases}$

РОЗДІЛ 5 КОНГРУЕНЦІЇ ВИЩИХ СТЕПЕНІВ

5.1 Конгруенції *n*-го степеня за простим модулем

Розглянемо загальні теореми, які стосуються конгруенцій *n*-го степеня за простим модулем p. Припустимо, що задано конгруенцію

$$\begin{aligned} &f(x) \equiv 0 \pmod{p}, \\ &f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \end{aligned} \tag{5.1}$$

де p – просте число і a_0 не ділиться на p.

Теорема 5.1

Конгруенцію (5.1) завжди можна замінити на еквівалентну їй:

$$f(x) \equiv 0 \pmod{p}, \quad f(x) = x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n.$$

Доведення. Справді, через те, що p – просте і a_0 не ділиться на p, завжди існує єдине число, обернене до a_0: $a_0 a_0^{-1} \equiv 1 \pmod{p}$, $a_0^{-1} \equiv a_0^{p-2} \pmod{p}$. Помноживши конгруенцію (5.1) на a_0^{-1}, отримаємо еквівалентну конгруенцію із старшим коефіцієнтом $b_0 \equiv 1 \pmod{p}$.■

Теорема 5.2

Якщо степінь конгруенції (5.1) не менший від модуля конгруенції, то вона еквівалентна деякій конгруенції степеня не вище за $p-1$ (за тим самим модулем). Тобто якщо у (5.1) $n \geq p$, то

$$\begin{aligned} &a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv \\ &\equiv b_0 x^{p-1} + b_1 x^{p-2} + \ldots + b_{p-2} x + b_{p-1} \equiv 0 \pmod{p}. \end{aligned} \tag{5.2}$$

Доведення. Поділимо $f(x)$ на $x^p - x$. Частку від ділення позначимо через $Q(x)$, залишок – через $R(x)$. Тоді на підставі алгоритму ділення із залишком дістанемо

$$f(x) = (x^p - x)Q(x) + R(x),$$

де $Q(x)$ – поліном степеня $n - p$; $R(x)$ – поліном степеня не більшого за $p - 1$. Коефіцієнти $Q(x)$, $R(x)$ – цілі числа. За теоремою Ферма якщо p – просте число, то $x^p - x \equiv 0 (\mathrm{mod}\, p)$ для будь-якого цілого x. Отже, отримаємо еквівалентну конгруенцію $f(x) \equiv R(x) (\mathrm{mod}\, p)$.■

Висновок. Конгруенції $f(x) \equiv 0 (\mathrm{mod}\, p)$ та $R(x) \equiv 0 (\mathrm{mod}\, p)$ мають *однакові корені*.

Частинні випадки:

1. $(x^p - x) | f(x)$. Тоді $R(x) \equiv 0 (\mathrm{mod}\, p)$ – тотожна, $0 \equiv 0 (\mathrm{mod}\, p)$, тобто виконується для будь-якого x.

2. $R(x) \equiv b_{p-1} (\mathrm{mod}\, p)$ – поліном нульового степеня. Якщо b_{p-1} не ділиться на p, то дана конгруенція не має розв'язків, оскільки вона зводиться до неправильної конгруенції $b_{p-1} \equiv 0 (\mathrm{mod}\, p)$.

Наслідок із малої теореми Ферма

Якщо $(a, p) = 1$, $n \equiv m (\mathrm{mod}\, p-1)$, то

$$a^n \equiv a^m (\mathrm{mod}\, p). \qquad (5.3)$$

Доведення. Дійсно, нехай $n > m$, $n = m + q(p-1)$. За малою теоремою Ферма $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Піднесемо цю конгруенцію до степеня q: $a^{(p-1)q} \equiv 1 (\mathrm{mod}\, p)$. Помножимо отриману конгруенцію і конгруенцію $a^m \equiv a^m (\mathrm{mod}\, p)$, дістанемо

$$a^{(p-1)q+m} \equiv a^m (\mathrm{mod}\ p), \text{ або } a^n \equiv a^m (\mathrm{mod}\ p).\blacksquare$$

Приклад 5.1

Знайти конгруенцію степеня не вище 4, еквівалентну заданій $f(x) = x^{17} + 2x^{11} + 3x^8 - 4x^7 + 2x - 3 \equiv 0 (\mathrm{mod}\, 5)$.

►Поділимо $f(x)$ на $x^5 - x$. Для полегшення ділення використаємо наслідок з малої теореми Ферма (5.3), а саме $a^{p-1} \equiv 1 (\mathrm{mod}\ p),\ (a, p) = 1$. За допомогою цього наслідку можна зменшити степені вихідного полінома, взявши замість даних степенів їх залишки за модулем 4:

$17 \equiv 1 (\mathrm{mod}\, 4); 11 \equiv 3 (\mathrm{mod}\, 4); 8 \equiv 0 (\mathrm{mod}\, 4); 7 \equiv 3 (\mathrm{mod}\, 4)$.

Отримаємо $R(x) = x^1 + 2x^3 + 3x^0 - 4x^3 + 2x - 3 \equiv 0 (\mathrm{mod}\, 5)$, або $-2x^3 + 3x \equiv 0 \,\mathrm{mod}(5)$, або, замінивши лишок -2 на лишок 3(mod5), отримаємо: $3x^3 + 3x \equiv 0 \,\mathrm{mod}(5)$, остаточно $x^3 + x \equiv 0 \,\mathrm{mod}(5)$.

Розв'язки останньої конгруенції $x_1 \equiv 2 (\mathrm{mod}\, 5)$, $x_2 \equiv 3 (\mathrm{mod}\, 5)$ будуть також розв'язками і вихідної конгруенції.◄

Теорема 5.3

Якщо α_1 – деякий розв'язок конгруенції n-го степеня $f(x) \equiv 0 (\mathrm{mod}\ p)$, то має місце тотожна конгруенція

$$f(x) \equiv (x - \alpha_1) f_1(x) (\mathrm{mod}\ p), \qquad (5.4)$$

де $f_1(x)$ – поліном $(n-1)$-го степеня. Старший коефіцієнт полінома $f_1(x)$ збігається із старшим коефіцієнтом вихідного полінома $f(x)$.

Доведення. Поділимо $f(x)$ на $(x-\alpha_1)$ і частку позначимо як $f_1(x)$, а залишок – $R(x)$, тоді

$$(x-\alpha_1)f_1(x)+R(x)\equiv 0(\mathrm{mod}\ p).$$

За теоремою Безу $R(x)=f(\alpha_1)$, але оскільки α_1 – розв'язок конгруенції, то $f(\alpha_1)\equiv 0(\mathrm{mod}\ p)$, отже, справедливою буде конгруенція

$$(x-\alpha_1)f_1(x)\equiv 0(\mathrm{mod}\ p).$$

За таких умов говорять про подільність $f(x)$ на $(x-\alpha_1)$ за модулем p. І, очевидно, навпаки, якщо $f(x)$ ділиться на $(x-\alpha_1)$ із нульовим залишком за модулем p, тобто $R(x)\equiv 0\,\mathrm{mod}(p)$, то, використовуючи теорему Безу, можна стверджувати, що $f(\alpha_1)=R(x)\equiv 0(\mathrm{mod}\ p)$, звідки випливає, що α_1 – розв'язок конгруенції.■

Висновок. Конгруенція (5.1) має корінь $x=\alpha_1$ тоді і тільки тоді, коли $x-\alpha_1$ ділить $f(x)$ за модулем p.

Зауваження. Теорема 5.3 і висновок із неї справедливі і для складеного модуля m.

Теорема 5.4

Якщо $\alpha_1,\alpha_2,...,\alpha_k;\ (k\le n)$ є різні корені конгруенції (5.1), то її можна подати у вигляді

$$f(x)=(x-\alpha_1)(x-\alpha_2)..(x-\alpha_k)f_k(x)\equiv 0\,\mathrm{mod}(p), \qquad (5.5)$$

де $f_k(x)$ – такий поліном степеня, не вище $n-k$, що не має коренів за модулем p, старші коефіцієнти у $f(x)$ та $f_k(x)$ збігаються.

Доведення. Розглянемо $f_1(x)$ з (5.4). Нехай α_2 – деякий його корінь. Тоді $f_1(x)$ можна подати за формулою (5.4):

$$f_1(x) \equiv (x-\alpha_2) f_2(x) (\mathrm{mod}\ p),$$

де $f_2(x)$ – поліном степеня, не вищого за $n-2$.

Підставимо $f_1(x)$ у (5.4). Отримаємо

$$f(x) = (x-\alpha_1)(x-\alpha_2) f_2(x) \equiv 0 \bmod(p).$$

Якщо $\alpha_2 = \alpha_1$, то корінь α_1 – кратний.

З іншого боку, розглянемо $\alpha_2 \neq \alpha_1$ таке число, що

$$(\alpha_2 - \alpha_1) f_1(\alpha_2) \equiv 0 (\mathrm{mod}\ p).$$

Добуток двох або декількох чисел ділиться на просте число p тоді і тільки тоді, коли на p ділиться принаймні один із множників добутку. За умовою α_1 та α_2 не збігаються $\alpha_1 \neq \alpha_2 (\mathrm{mod}\ p)$. Тому, $(\alpha_2 - \alpha_1)$ не ділиться на p, і, отже, на p ділиться $f_1(x)$

$$f_1(\alpha_2) \equiv 0 (\mathrm{mod}\ p).$$

Останнє означає, що α_2 – корінь конгруенції $f_1(x) \equiv 0 (\mathrm{mod}\ p)$ і для нього справедливим є подання

$$(x-\alpha_2) f_2(x) \equiv 0 (\mathrm{mod}\ p).$$

Підставимо останній вираз у (5.4):

$$(x-\alpha_1)(x-\alpha_2) f_2(x) \equiv 0 (\mathrm{mod}\ p).$$

Так поступово можна прийти до полінома $f_k(x)$, $k \leq n$, який не має коренів за даним модулем p. Якщо

конгруенція (5.1) має n коренів, то $f_k(x) = f_0(x) = a_0$, де a_0 – старший коефіцієнт конгруенції (5.1).■

В и с н о в о к. Якщо конгруенція (5.1) n-го степеня за простим модулем p (можна вважати $n \le p$) має n різних розв'язків $\alpha_1, \alpha_2, ..., \alpha_n$, то поліном $f(x)$ можна розкласти на n лінійних множників типу $(x - \alpha_i)$, $i = \overline{1,n}$ та множник a_0, а саме:

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \equiv 0 (\mathrm{mod}\ p). \qquad (5.6)$$

Приклад 5.2

Розкласти конгруенцію за даним модулем

$x^4 + x^3 - x^2 + x - 2 \equiv 0 (\mathrm{mod}\, 5)$.

►По-перше, можна понизити степінь конгруенції, оскільки щодо степеня конгруенції за наслідком із малої теореми Ферма можна записати: $4 \equiv 0 (\mathrm{mod}(5-1))$.

Таким чином, отримаємо еквівалентну конгруенцію $x^3 - x^2 + x - 1 \equiv 0 (\mathrm{mod}\, 5)$.

Знайдемо корені еквівалентної конгруенції із повної системи абсолютно найменших лишків $(-2, -1, 0, 1, 2)$.

Підстановкою з'ясовуємо, що коренями конгруенції будуть $x \equiv \{-2, 1, 2\}$. Очевидно, що ці корені є коренями й вихідної конгруенції.

Застосуємо для розкладання вихідного полінома за модулем 5 схему Горнера.

	1	1	-1	1	-2
-2	1	-1	1	-1	0
1	1	0	1	0	
2	1	2	0		

Із останнього рядка отримаємо конгруенцію першого степеня $x+2\equiv 0(\mathrm{mod}\,5)$.

Її розв'язок $x\equiv -2(\mathrm{mod}\,5)$ співпадає із першим коренем. Отже, маємо для вихідного полінома однократні корені $x_1\equiv 1(\mathrm{mod}\,5)$, $x_2\equiv 1(\mathrm{mod}\,5)$ і корінь кратності 2 $x_{3,4}\equiv -2(\mathrm{mod}\,5)$.

Відповідь: задана конгруенція розкладається так:
$(x+2)^2(x-1)(x-2)\equiv 0(\mathrm{mod}\,5)$.◄

5.2 Кількість коренів конгруенції *n*-го степеня

Теорема 5.5

Конгруенція n-го степеня за простим модулем не може мати більш ніж n різних розв'язків.

Доведення. Нехай β – деякий розв'язок, відмінний від $\alpha_1,\alpha_2,...,\alpha_n$, тобто

$$\beta\neq\alpha_i\,(\mathrm{mod}\,p),\ i=\overline{1,n}.$$

Підставимо в (5.6) β замість x:

$$a_0(\beta-\alpha_1)(\beta-\alpha_2)...(\beta-\alpha_n)\equiv 0(\mathrm{mod}\,p). \qquad (5.7)$$

Оскільки модуль простий, отже, хоча б один із множників повинен ділитися на модуль p. Лінійні множники не діляться на модуль за припущенням. Старший коефіцієнт конгруенції теж не ділиться на модуль, оскільки інакше степінь конгруенції був би нижчим. Отже, доходимо висновку, що конгруенція (5.7) неможлива.

Отже, β не може бути коренем і не збігатися хоча б з одним значенням із набору $\alpha_1,\alpha_2,...,\alpha_n$.■

Необхідно зауважити, що, по-перше, ця теорема не підтверджує взагалі наявності розв'язків конгруенції n-го степеня за простим модулем p і, по-друге, для складених модулів вона не виконується.

Наприклад, у конгруенції першого степеня $16x \equiv 32 (\mathrm{mod}\, 48)$ НСД $(a, m) = (16, 48) = 16$, $16 \mid 32$. Отже, конгруенція має шістнадцять розв'язків.

Висновок. Конгруенція $f(x) \equiv 0 (\mathrm{mod}\, p)$,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,\ n < p,$$

має більше ніж n розв'язків тоді і тільки тоді, коли вона тотожна, тобто коли всі її коефіцієнти діляться на p.

Дійсно, якщо коефіцієнти заданої конгруенції діляться на p, то конгруенція виконується при будь-якому значенні x з повної системи лишків, тобто вона тотожна, кількість її розв'язків, що дорівнює p, буде більше ніж n.

5.3 Конгруенції *n*-го степеня за складеним модулем

Розглянемо конгруенцію

$$f(x) \equiv 0 (\mathrm{mod}\, m),\ f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n. \quad (5.8)$$

Якщо в (5.8) $m = m_1 m_2 \cdot \ldots \cdot m_k$, $(m_i, m_j) = 1$, $\forall i \neq j$, $i, j = \overline{1, k}$, то конгруенція рівносильна системі

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, m_1); \\ f(x) \equiv 0 (\mathrm{mod}\, m_2); \\ \quad \ldots \\ f(x) \equiv 0 (\mathrm{mod}\, m_k). \end{cases}$$

Якщо позначити через T_i кількість розв'язків i-ї конгруенції системи, то загальна кількість розв'язків вихідної конгруенції дорівнюватиме

$$T = T_1 \cdot T_2 \cdot ... \cdot T_k . \qquad (5.9)$$

Справедливість цього твердження випливає із властивостей конгруенцій. Зокрема, якщо конгруенція виконується за модулем m, то вона виконується і за будь-яким дільником m.

Приклад 5.3

Розв'язати конгруенцію $x^4 + 2x^3 + 8x + 9 \equiv 0 (\mathrm{mod}\, 35)$.

►Число $35 = 5 \cdot 7$, отже, модуль складений і задана конгруенція відповідає системі:

$$\begin{cases} x^4 + 2x^3 + 8x + 9 \equiv 0 (\mathrm{mod}\, 5), \\ x^4 + 2x^3 + 8x + 9 \equiv 0 (\mathrm{mod}\, 7). \end{cases}$$

Після спрощення система матиме вигляд:

$$\begin{cases} x^0 + 2x^3 + 3x - 1 \equiv 0 (\mathrm{mod}\, 5), \\ x^4 + 2x^3 + x + 2 \equiv 0 (\mathrm{mod}\, 7). \end{cases}$$

Перша конгруенція

$2x^2 + 3 \equiv 0 (\mathrm{mod}\, 5)$; $2x^2 - 2 \equiv 0 (\mathrm{mod}\, 5)$; $x^2 \equiv 1 (\mathrm{mod}\, 5)$.

Розв'язки першої конгруенції $x_1 \equiv 1 (\mathrm{mod}\, 5)$; $x_2 \equiv 4 (\mathrm{mod}\, 5)$.

Друга конгруенція

$x^4 + 2x^3 + x + 2 \equiv 0 (\mathrm{mod}\, 7)$.

Шукаємо розв'язки серед повної системи абсолютно найменших лишків $(-3, -2, -1, 0, 1, 2, 3)$: 0, 1 – не розв'язки, $x_1 \equiv -1 (\mathrm{mod}\, 7)$ – розв'язок. Інші розв'язки шукаємо за схемою Горнера.

Знайдемо ще два – $x_2 \equiv -2 (\mathrm{mod}\, 7)$, $x_3 \equiv 3 (\mathrm{mod}\, 7)$.

Отже, маємо два розв'язки першої конгруенції і три розв'язки другої. Загалом система, а отже, і вихідна конгруенція має $T = 2 \cdot 3 = 6$ розв'язків. Для того щоб їх знайти, необхідно розглянути шість систем вигляду

$$\begin{cases} x \equiv b_1 \pmod 5, \ b_1 \in (1, 4), \\ x \equiv b_2 \pmod 7, \ b_2 \in (-2, -1, 3). \end{cases}$$

Але ми можемо розв'язати цю систему у загальному вигляді і, маючи її загальний розв'язок, підставити потрібні значення b_1, b_2:

$$x \equiv b_1 \pmod 5 \Rightarrow x = b_1 + 5t \qquad (*)$$

Підставимо x у друге рівняння системи

$b_1 + 5t \equiv b_2 \pmod 7 \Rightarrow 5t \equiv b_2 - b_1 \pmod 7$;

$5^{-1} \equiv 3 \pmod 7 \Rightarrow t \equiv 3(b_2 - b_1) \pmod 7$.

Отже, $t = 3(b_2 - b_1) + 7t_1$.

Підставимо t в (*):

$x = b_1 + 5(3(b_2 - b_1) + 7t_1) = b_1 + 15b_2 - 15b_1 + 35t_2 =$

$= -14b_1 + 15b_2 + 35t_1$, або $x \equiv 21b_1 + 15b_2 \pmod{35}$ – загальна формула розв'язку.

Залишилося тільки по черзі підставити у неї значення $b_1 = (1, 4)$, $b_2 = (-2, -1, 3)$.

Отже, $x \equiv 26, 6, 31, 19, 34, 24 \pmod{35}$. ◄

Тепер розглянемо конгруенцію (5.8) за умови, що $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$,

$$f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right). \qquad (5.10)$$

Розв'язання такої конгруенції зводиться до розв'язання конгруенцій вигляду

$$f(x) \equiv 0 (\mathrm{mod}\ p^{\alpha}). \qquad (5.11)$$

Розв'язання конгруенції (5.11) зводиться до розв'язання конгруенції

$$f(x) \equiv 0 (\mathrm{mod}\ p).$$

Для доведення цього факту пригадаємо ряд Тейлора для розкладання полінома в околі точки x_0:

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \ldots +$$
$$+ \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n.$$

Розглянемо конгруенцію (5.11). Її розв'язок $x \equiv x_1 (\mathrm{mod}\ p)$, що еквівалентно запису

$$x = x_1 + pt_1, \quad t \in Z, \qquad (5.12)$$

підставимо у конгруенцію $f(x) \equiv 0 (\mathrm{mod}\ p^2)$. Розкладемо $f(x)$ у ряд Тейлора в околі точки x_1

$$f(x_1 + pt_1) = f(x_1) + \frac{f'(x_1)}{1!}(x_1 + pt_1 - x_1) +$$
$$+ \frac{f''(x_1)}{2!}(x_1 + pt_1 - x_1)^2 + \ldots + \frac{f^{(n)}(x_1)}{n!}(x_1 + pt_1 - x_1)^n$$

або

$$f(x_1 + pt_1) = f(x_1) + \frac{f'(x_1)}{1!} pt_1 +$$
$$+ \frac{f''(x_1)}{2!} p^2 t_1^{\,2} + \ldots + \frac{f^{(n)}(x_1)}{n!} p^n t_1^{\,n} \equiv 0 (\mathrm{mod}\ p^2).$$

Відкинемо усі складові, кратні p^2, тоді матимемо

$$f(x_1) + f'(x_1)pt_1 \equiv 0 (\mathrm{mod}\ p^2).$$

Оскільки x_1 є розв'язком (5.11), то $p \mid f(x)$, отже, конгруенцію можна скоротити

$$\frac{f(x_1)}{p} + f'(x_1)t_1 \equiv 0 (\mathrm{mod}\ p)$$

або

$$f'(x_1)t_1 \equiv -\frac{f(x_1)}{p} (\mathrm{mod}\ p).$$

Розглянемо випадок, коли $f'(x_1)$ не ділиться на p.

Знайдемо розв'язок цієї конгруенції. Позначимо його $t_1 \equiv u_1 (\mathrm{mod}\ p)$. Отже, $t_1 = u_1 + pt_2$. Підставимо значення t у (5.12) і отримаємо

$$x = x_1 + p(u_1 + pt_2) = x_1 + pu_1 + p^2 t_2, \quad t_2 \in Z.$$

Якщо позначити $x_1 + pu_1 = x_2$, то матимемо

$$x \equiv x_2 (\mathrm{mod}\ p^2), \text{ або } x \equiv x_2 + p^2 t_2. \qquad (5.13)$$

Підставляємо цей розв'язок у конгруенцію $f(x) \equiv 0 (\mathrm{mod}\ p^3)$. Розкладаємо в ряд Тейлора в околі x_2, відкидаємо всі складові, кратні p^3, і отримуємо:

$$f(x_2) + f'(x_2)p^2 t_2 \equiv 0 (\mathrm{mod}\ p^3).$$

Зауважимо, що оскільки $x_1 \equiv x_2 (\mathrm{mod}\ p)$, то $f'(x_1) \equiv f'(x_2) (\mathrm{mod}\ p)$ і $f'(x_2)$ не ділиться на p^2, а $f(x_2)$ – ділиться. Скоротимо конгруенцію на p^2, матимемо

$$\frac{f(x_2)}{p^2} + f'(x_2)t_2 \equiv 0 \pmod{p}.$$

Розв'язок $t_2 = u_2 + pt_3$ підставимо в (5.13):

$$x = x_2 + p^2(u_2 + pt_3) = (x_2 + p^2 u_2) + p^3 t_3,$$
$$x_2 + p^2 u_2 = x_3 \Rightarrow x \equiv x_3 \pmod{p^3}.$$

Продовжуючи описану процедуру, знайдемо нарешті конгруенцію $x \equiv x_\alpha \pmod{p^\alpha}$, що є розв'язком конгруенції (5.11).

В и с н о в о к . Будь-який розв'язок $x \equiv x_1 \pmod{p}$ конгруенції $f(x) \equiv 0 \pmod{p}$ за умови, що $f'(x_1)$ не ділиться на p, дає єдиний розв'язок конгруенції (5.11).

Приклад 5.5

Розв'язати конгруенцію $x^4 + 7x + 4 \equiv 0 \pmod{27}$.

► Маємо $x^4 + 7x + 4 \equiv 0 \pmod{3^3}$. Отже, спочатку шукаємо розв'язок конгруенції $x^4 + 7x + 4 \equiv 0 \pmod{3}$.

По-перше, спростимо її $x^0 + x + 1 \equiv 0 \pmod{3}$ або $x \equiv -2 \pmod{3}$.

Маємо розв'язок $x \equiv 1 \pmod{3}$, $x = 1 + 3t_1$. Підставимо отриманий x у конгруенцію $x^4 + 7x + 4 \equiv 0 \pmod{9}$.

$f(1) = 1^4 + 7 + 4 = 12 \equiv 3 \pmod{9}$;

$f'(x) = 4x^3 + 7$; $f'(1) = 11 \equiv 2 \pmod{9}$ – не ділиться на $p = 3$.

$f(1) + f'(1) \cdot 3t_1 \equiv 0 \pmod{9}$. Поділимо конгруенцію на $p = 3$:

$$\frac{f(1)}{3} + f'(1)t_1 \equiv 0 \pmod 3 \Rightarrow$$

$$\Rightarrow 1 + 2t_1 \equiv 0 \pmod 3, \quad 2t_1 \equiv -1 \pmod 3;$$

$$t_1 \equiv 1 \pmod 3;\ t_1 = 1 + 3t_2.$$

Підставимо значення t_1 у формулу для x: $x = 1 + 3t_1 = 1 + 3(1 + 3t_2) = 4 + 9t_2$. Отже, знайшли розв'язок $x \equiv 4 \pmod 9$. Вираз $x = 4 + 9t_2$ підставимо у конгруенцію $x^4 + 7x + 4 \equiv 0 \pmod{27}$.

$$f(4) = 256 + 7 \cdot 4 + 4 = 288 \equiv 18 \pmod{27};$$

$$f'(x) = 4x^3 + 7;$$

$$f'(4) = 4 \cdot 4^3 + 7 = 263 \equiv 20 \pmod{27}.$$

$$f(4) + f'(4) \cdot 9t_2 \equiv (\mathrm{mod}\, 27).$$

Поділимо конгруенцію на $p^2 = 9$:

$$\frac{f(4)}{9} + f'(4)t_2 \equiv 0 \pmod 3 \Rightarrow$$

$$\Rightarrow 2 + 20t_2 \equiv 0 \pmod 3,\ 2t_2 \equiv -2 \pmod 3;$$

$$t_2 \equiv -1 \pmod 3;\ t_2 = 2 + 3t_3.$$

$$x = 4 + 9t_2 = 4 + 9(2 + 3t_3) = 22 + 27t_3 \Rightarrow x \equiv 22 \pmod{27}.$$

Отже розв'язком конгруенції $x^4 + 7x + 4 \equiv 0 \pmod{27}$ є клас чисел $x = 22 + 27t$. Розв'язок єдиний.◀

Питання для самоперевірки до розділу 5

1. Який загальний вигляд має конгруенція n-го степеня з одним невідомим за довільним модулем m? Яка умова накладається на коефіцієнт a_0 біля старшого степеня змінної x?
2. Чи можна конгруенцію n-го степеня з одним невідомим за простим модулем p в разі довільного коефіцієнта a_0 біля старшого степеня змінної x звести до еквівалентної конгруенції зі старшим коефіцієнтом $a_0=1$?
3. На якій теоремі базується метод зниження степеня конгруенції за простим модулем p? На яку величину можна знизити степінь конгруенції за простим модулем?
4. Яке число називається коренем конгруенції n-го степеня з одним невідомим?
5. Скільки коренів можуть мати конгруенції n-го степеня з одним невідомим за простим модулем p, якщо $(a_0,p)=1$?
6. Елементи якої системи становлять множину коренів конгруенції n-го степеня з одним невідомим за простим модулем p, якщо всі коефіцієнти конгруенції діляться на модуль p?
7. Для конгруенції $6x^{132}+129x^{34}-336\equiv 0\pmod 3$ назвіть усі розв'язки.
8. Як можна розкласти праву частину конгруенції n-го степеня з одним невідомим за простим модулем p, якщо $\alpha_1,\alpha_2,...,\alpha_k;\ (k\le n)$ є коренями цієї конгруенції?
9. Якою структурою можна замінити конгруенцію n-го степеня з одним невідомим за складеним модулем m?
10. Нехай модуль конгруенції $m=p_1\cdot p_2\cdot\ldots\cdot p_k$. Відомо, що за модулем p_1 ця конгруенція має T_1 розв'язків, за модулем p_2 – T_2 розв'язків, …, за модулем p_k – T_k розв'язків. Скільки розв'язків має конгруенція за модулем $m=p_1\cdot p_2\cdot\ldots\cdot p_k$?
11. До якої конгруенції зводиться розв'язок конгруенції n-го степеня з одним невідомим за модулем p^α?

12. На якій множині значень змінної x поліном з правої частини конгруенції за модулем p^α розкладається у ряд Тейлора для отримання розв'язку за модулем підвищеного степеня? В околі якої точки x відбувається розкладання?
13. Яка умова накладається на похідну функції з правої частини конгруенції n-го степеня з одним невідомим для того, щоб розв'язок конгруенції за модулем підвищеного степеня існував?
14. За яких умов кількість розв'язків конгруенції n-го степеня з одним невідомим за модулем p^α буде меншою за кількість розв'язків цієї конгруенції за простим модулем p?

Індивідуальні завдання до розділу 5

Завдання 5.1 Розв'язати конгруенцію за складеним модулем.

1. $x^4 - 3x^3 + 2x^2 - 5x - 10 \equiv 0 \pmod{343}$.
2. $6x^3 - 7x - 11 \equiv 0 \pmod{125}$.
3. $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 \pmod{625}$.
4. $9x^2 + 29x + 62 \equiv 0 \pmod{32}$.
5. $x^3 + 3x^2 - 5x + 16 \equiv 0 \pmod{125}$.
6. $x^5 - 5x^4 - 5x^3 + 25x^2 + 4x - 20 \equiv 0 \pmod{147}$.
7. $x^5 + 3x^4 - 7x^3 + 4x^2 + 4x - 10 \equiv 0 \pmod{175}$.
8. $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{135}$.
9. $4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{225}$.
10. $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{225}$.
11. $2x^4 + 7x^2 - 3x - 32 \equiv 0 \pmod{208}$.

12. $x^4 - 3x^3 + x^2 + 5x + 24 \equiv 0 \pmod{441}$.
13. $x^3 - 4x^2 - 3x + 6 \equiv 0 \pmod{343}$.
14. $x^4 - 3x^3 + 2x^2 - 5x - 10 \equiv 0 \pmod{175}$.
15. $6x^3 - 7x - 11 \equiv 0 \pmod{605}$.
16. $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 \pmod{1325}$.
17. $9x^2 + 29x + 62 \equiv 0 \pmod{196}$.
18. $x^3 + 3x^2 - 5x + 16 \equiv 0 \pmod{225}$.
19. $x^5 - 5x^4 - 5x^3 + 25x^2 + 4x - 20 \equiv 0 \pmod{245}$.
20. $x^5 + 3x^4 - 7x^3 + 4x^2 + 4x - 10 \equiv 0 \pmod{392}$.
21. $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{275}$.
22. $4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{200}$.
23. $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{243}$.
24. $2x^4 + 7x^2 - 3x - 32 \equiv 0 \pmod{1225}$.
25. $x^4 - 3x^3 + x^2 + 5x + 24 \equiv 0 \pmod{675}$.
26. $x^3 - 4x^2 - 3x + 6 \equiv 0 \pmod{482}$.
27. $x^4 - 3x^3 + 2x^2 - 5x - 10 \equiv 0 \pmod{1323}$.
28. $6x^4 + 7x + 35 \equiv 0 \pmod{675}$.
29. $11x^4 - 17x + 125 \equiv 0 \pmod{1225}$.
30. $x^5 - 3x^3 + 2x - 14 \equiv 0 \pmod{343}$.

РОЗДІЛ 6 КОНГРУЕНЦІЇ ДРУГОГО СТЕПЕНЯ

6.1 Загальні положення

Загальний вигляд конгруенції 2-го степеня

$$ax^2 + bx + c \equiv 0 \pmod{m}. \qquad (6.1)$$

Теорема 6.1

Конгруенцію (6.1) завжди можна звести до конгруенції вигляду

$$y^2 \equiv C \pmod{4am}. \qquad (6.2)$$

Доведення. Дійсно, за властивостями конгруенцій, які відповідають зміні модуля конгруенції, можемо помножити усі складові конгруенції на множник $4a$:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}.$$

Виділимо ліворуч повний квадрат:

$$(2ax+b)^2 - b^2 + 4ac \equiv 0 \pmod{4am} \Rightarrow$$

$$\Rightarrow (2ax+b)^2 \equiv b^2 - 4ac \pmod{4am}.$$

Позначимо $2ax + b = y,\ \ b^2 - 4ac = C$, отримаємо вираз (6.2).■

Якщо конгруенція (6.2) має розв'язок $y \equiv y_1 \pmod{4am}$, то можна знайти розв'язок $x \equiv \dfrac{y-b}{2a} \pmod{m}$ за умови, що $2a \mid (y-b)$. Тобто за виконання додаткової умови розв'язок (6.2) є розв'язком (6.1). Якщо (6.2) не має розв'язку, то (6.1) теж не має розв'язку.

Наслідок з теореми 6.1

Якщо модуль є складеним числом $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, то розв'язання конгруенції (6.2) зводиться до розв'язання системи конгруенцій вигляду

$$\begin{cases} y^2 \equiv C \bmod \left(p_1^{\alpha_1} \right), \\ y^2 \equiv C \bmod \left(p_2^{\alpha_2} \right), \\ \quad \cdots \\ y^2 \equiv C \bmod \left(p_k^{\alpha_k} \right), \end{cases}$$

де p – просте число.

Розглянемо розв'язання (6.2) у випадках:

а) модуль $p > 2$ – просте непарне число в першому степені;

б) модуль p^{α} – просте непарне число в степені $\alpha > 1$;

в) модуль $p = 2$.

6.2 Конгруенція за простим непарним модулем

Розглянемо конгруенцію

$$x^2 \equiv a \left(\bmod p \right). \tag{6.3}$$

Якщо $a \equiv 0 \left(\bmod p \right)$, то (6.3) має один розв'язок.

Теорема 6.2 (критерій Ейлера)

Якщо a в конгруенції (6.3) не ділиться на p, тобто $\left(a, p \right) = 1$, то відповідна конгруенція має два різних розв'язки, якщо

$$a^{\frac{p-1}{2}} \equiv 1 \left(\bmod p \right),$$

або зовсім не має розв'язків, якщо

$$a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p).$$

Доведення. Розглянемо конгруенцію (6.3) за простим непарним модулем p.

Оскільки $(a, p) = 1$, то за малою теоремою Ферма (теорема 3.1) $a^{p-1} - 1 \equiv 0 (\mathrm{mod}\, p)$. Оскільки в нашому випадку $p-1$ завжди парне, то справедливим буде подання

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\mathrm{mod}\, p).$$

Якщо добуток ділиться на просте число, отже, обов'язково хоча б один із множників ділиться на це число. Одночасно числа $\left(a^{\frac{p-1}{2}} - 1\right)$ та $\left(a^{\frac{p-1}{2}} + 1\right)$ на p ділитися не можуть, оскільки їхня різниця дорівнює 2 і не ділиться на p. Отже, можливі два випадки:

$$a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p) \text{ або } a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p).$$

Тепер згадаємо, що коли (6.3) має розв'язок, то існує x (та $-x$), такий, що $(-x)^2 \equiv x^2 \equiv a (\mathrm{mod}\, p)$, причому, оскільки $(a, p) = 1$, то і $(\pm x, p) = 1$. Для таких конгруенцій за властивостями можливе піднесення до цілого степеня. Піднесемо конгруенцію до степеня $\frac{p-1}{2}$, отримаємо

$$x^{p-1} \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

За малою теоремою Ферма (теорема 3.1) з урахуванням $(x, p)=1$ маємо $x^{p-1} \equiv 1 (\mathrm{mod}\, p)$, отже, виходячи з існування розв'язку x конгруенції (6.3), отримали

$$a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p).$$

Висновки

1. Якщо (6.3) має розв'язки, то для неї виконується конгруенція $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$. Коренів конгруенція має рівно два класи, створені на лишках x та $-x$ із повної системи абсолютно найменших лишків (або x та $p-x$ з повної системи найменших додатних лишків) модуля p, оскільки $(-x)^2 = x^2 \equiv a (\mathrm{mod}\, p)$.

Очевидно, що x та $-x$ різні, тобто неконгруентні між собою, інакше б виконувалася конгруенція $2x \equiv 0 (\mathrm{mod}\, p)$, тобто x ділився б на p, а це суперечить вихідній конгруенції. Більше коренів бути не може за теоремою про кількість коренів конгруенції із простим модулем.

2. Відповідно інший випадок – $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$ – виконується тільки для таких a, для яких конгруенція (6.3) не має розв'язку.

Тепер прояснимо питання кількості чисел a, для яких конгруенція (6.3) буде мати розв'язки. Очевидно, що a належить до класів, створених на повних системах абсолютно найменших або найменших додатних лишків без нуля. Для простого модуля p таких класів $p-1$. Але вище було зазначено, що x та $-x$ (або x та $p-x$) дають однакові квадрати, тобто $(-x)^2 = x^2 \equiv a (\mathrm{mod}\, p)$. Отже, будемо мати чисел, для яких конгруенція (6.3) має розв'язок, рівно половину з кількості елементів у повній

системі лишків без нуля, тобто рівно $\frac{p-1}{2}$ лишки з повної системи лишків відповідають (6.3), а інша половина – ні. Нагадаємо, що p – непарне, отже, $\frac{p-1}{2}$ – ціле число.

Приклад 6.1

Розглянемо повну систему абсолютно найменших лишків для чисел 5 та 7 і з'ясуємо, для яких лишків конгруенція (6.3) буде мати розв'язок, а для яких ні.

►В дужках будемо подавати відповідні лишки з повної системи найменших лишків.

Розглянемо число $p=5$, повна система абсолютно найменших лишків без нуля: $-2,-1,1,2$ $(1,2,3,4)$.

Відповідні квадрати:

$(\pm 2)^2 = 4 \equiv -1 (\mathrm{mod}\, 5)$, $(\pm 1)^2 = 1 \equiv 1 (\mathrm{mod}\, 5)$,

$\left((1)^2 = 1 \equiv 1 (\mathrm{mod}\, 5),\ (2)^2 = 4 \equiv 4 (\mathrm{mod}\, 5),\right)$,

$(3)^2 = 9 \equiv 4 (\mathrm{mod}\, 5)$, $(4)^2 = 16 \equiv 1 (\mathrm{mod}\, 5)$.

Отже, якщо в (6.3) модуль дорівнює 5, а права частина $a \equiv \pm 1 (\mathrm{mod}\, 5)$ $(a \equiv 1,4 (\mathrm{mod}\, 5))$, то конгруенція розв'язок має. Для $a \equiv \pm 2 (\mathrm{mod}\, 5)$ $(a \equiv 2,3 (\mathrm{mod}\, 5))$ розв'язків немає. Тобто для $\frac{5-1}{2} = 2$ лишків розв'язок є, для 2 – немає.

Розглянемо число $p=7$, повна система абсолютно найменших лишків без нуля: $-3,-2,-1,1,2,3$ $(1,2,3,4,5,6)$.

Відповідні квадрати:

$(\pm 3)^2 = 9 \equiv 2 (\mathrm{mod}\, 7)$, $(\pm 2)^2 = 4 \equiv -3 (\mathrm{mod}\, 7)$,

$(\pm 1)^2 = 1 \equiv 1 (\mathrm{mod}\, 7)$,

$\left((1)^2 = 1 \equiv 1 (\mathrm{mod}\, 7),\ (2)^2 = 4 \equiv 4 (\mathrm{mod}\, 7),\right.$

$(3)^2 = 9 \equiv 2 (\mathrm{mod}\, 7)$, $(4)^2 = 16 \equiv 2 (\mathrm{mod}\, 7)$,

$(5)^2 = 25 \equiv 4 (\mathrm{mod}\, 7)$, $(6)^2 = 36 \equiv 1 (\mathrm{mod}\, 7)\big)$.

Отже, якщо в (6.3) модуль дорівнює 7, а права частина $a \equiv 1, 2, -3 (\mathrm{mod}\, 7)$ $\big(a \equiv 1, 2, 4 (\mathrm{mod}\, 7)\big)$, то конгруенція розв'язок має. Для $a \equiv -1, -2, 3 (\mathrm{mod}\, 7)$ $\big(a \equiv 3, 5, 6 (\mathrm{mod}\, 5)\big)$ розв'язків немає. Тобто для $\frac{7-1}{2} = 3$ лишків розв'язок є, для 3 – немає. ◄

Висновок

Серед повної системи лишків для простого непарного модуля p $\frac{p-1}{2}$ елементів відповідає конгруенції (6.3) і $\frac{p-1}{2}$ елементів не відповідає їй. Для таких елементів, що відповідають (6.3), виконується конгруенція $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$. Для інших – конгруенція $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$.

Означення 6.1. Значення a, для якого конгруенція (6.3) має розв'язок, називається *квадратичним лишком модуля* p.

Означення 6.2. Якщо для деякого a конгруенція (6.3) розв'язку не має, то a називається *квадратичним нелишком модуля* p.

Наслідок із теореми 6.2 (з критерію Ейлера)

У повній системі лишків простого непарного модуля p кількість лишків завжди дорівнює кількості нелишків, а саме $\frac{p-1}{2}$.

Теорема 6.3 (теорема Ейлера)

Добуток двох лишків або двох нелишків за модулем p є лишком. Добуток лишка на нелишок за модулем p є нелишком.

Д о в е д е н н я . З критерію Ейлера (теореми 6.2) маємо

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p},\ b^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p},$$

$$(ab)^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Знак „+” буде за умови, що знаки біля 1 однакові, знак „–” оберемо, якщо знаки біля 1 різні.■

6.3 Символ Лежандра

Розглянемо конгруенцію (6.3).

Означення 6.3. Якщо p простий непарний модуль і $(a, p) = 1$, то символом Лежандра називається величина:

$\left(\frac{a}{p}\right) = 1$, якщо a – квадратичний лишок за модулем p,

і

$\left(\frac{a}{p}\right) = -1$, якщо a – квадратичний нелишок за модулем p.

Тобто, враховуючи критерій Ейлера,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \qquad (6.4)$$

Критерій Ейлера дає одразу і формулу обчислення символу Лежандра, але для великих p, a обчислення є досить складними. Наведемо властивості символу Лежандра, які значно спрощують процес обчислення даного показника і відповідно визначення наявності розв’язків (6.3).

Властивості символу Лежандра

1. Якщо $a \equiv b(\mathrm{mod}\ p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

Як наслідок, $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$; $\left(\frac{a^2}{p}\right) = 1$; $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Властивість **2** зводить обчислення символу Лежандра $\left(\frac{a}{p}\right)$ за простим непарним модулем p до обчислення символів $\left(\frac{1}{p}\right), \left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)$, якщо $q \neq p$ – просте непарне число.

3. $\left(\frac{1}{p}\right) = 1$.

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

Якщо взяти до уваги, що для усіх простих чисел $p = 4k+1$ величина $\frac{p-1}{2}$ парна, а для $p = 4k+3$, або $p = 4k-1$ – непарна, то таку властивість можна прокоментувати так: для всіх модулів типу $p = 4k+1$ число -1 є квадратичним лишком, а для модулів типу $p = 4k+3$, або $p = 4k-1$ – квадратичним нелишком.

Наприклад, -1 за модулем 29 є квадратичним лишком, оскільки $29 = 7 \cdot 4 + 1$, а для модуля 3 – квадратичним нелишком, оскільки $3 = 4 \cdot 1 - 1$.

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

Якщо розглянути просте непарне число за модулем 8, то будемо мати для нього один із таких виглядів:

$p=8k+1;\ p=8k+3;$

$p=8k+5\ (або\ p=8k-3);$

$p=8k+7(або\ p=8k-1).$

Якщо розглянути степінь $\frac{p^2-1}{8}$ для цих видів, то матимемо

$p=8k\pm1$:

$\frac{64k^2+16k+1-1}{8}=8k^2+2k$,

$\frac{64k^2-6k+1-1}{8}=8k^2-2k$ – парні степені;

$p=8k\pm3$:

$\frac{64k^2+48k+9-1}{8}=8k^2+6k+1,$

$\frac{64k^2-48k+9-1}{8}=8k^2-6k+1$ – непарні степені.

Тобто властивість **5** можна подати інакше.

Для чисел $p=8k\pm1$ символ Лежандра $\left(\frac{2}{p}\right)=1$, 2 є лишком за модулем $p=8k\pm1$.

Для чисел $p=8k\pm3$ символ Лежандра $\left(\frac{2}{p}\right)=-1$, 2 є нелишком за модулем $p=8k\pm3$.

6. Закон взаємності двох простих непарних чисел.

Якщо p та q два різних непарних простих числа, то для них виконується співвідношення

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

Число q, як і число p, подається за модулем 4 або як $4k+1$, або $4k+3$. У першому випадку $\frac{q-1}{2}$ буде парним степенем, у другому – непарним. Добуток степенів $\frac{p-1}{2}\cdot\frac{q-1}{2}$ буде парним, якщо хоч один із множників парний.

Отже, якщо хоча б одне із чисел p або q має вигляд $4k+1$, то $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$.

Якщо обидва числа мають вигляд $4k+3$, то

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right).$$

Приклад 6.2

Дослідити, чи має розв'язки конгруенція

$x^2\equiv 438(\mathrm{mod}\,593)$.

►Спочатку спростимо конгруенцію $x^2\equiv -155(\mathrm{mod}\,593)$.

Розкладемо $a=-155=(-1)\cdot 5\cdot 31$.

Для визначення наявності розв'язків обчислимо символ Лежандра

$$\left(\frac{-155}{593}\right)=\left(\frac{-1}{593}\right)\left(\frac{5}{593}\right)\left(\frac{31}{593}\right)$$

1) $593=148\cdot 4+1$, тобто $\left(\frac{-1}{593}\right)=(-1)^{1482}=1$.

2) $(5,593)=1,\ 593=148\cdot 4+1,\ 5=4\cdot 1+1\Rightarrow$

$\Rightarrow\left(\frac{5}{593}\right)=\left(\frac{593}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right),\ \ 3=8\cdot 0+3,$ отже, 2 є нелишком за модулем 3, $\left(\frac{2}{3}\right)=(-1)^1=-1.$

3) $(31,593)=1,\ 593=4\cdot 148+1\Rightarrow$

$\Rightarrow\left(\frac{31}{593}\right)=\left(\frac{593}{31}\right)=\left(\frac{4}{31}\right)=\left(\frac{2^2}{593}\right)=1.$

4) $\left(\frac{-155}{593}\right)=1\cdot(-1)\cdot 1=-1.$

Відповідь: конгруенція $x^2\equiv 438(\mathrm{mod}\,593)$ розв'язків не має.◄

Приклад 6.3

Дослідити, чи має розв'язки конгруенція $x^2\equiv 2021(\mathrm{mod}\,1231).$

►Спочатку спростимо конгруенцію: $x^2\equiv 792(\mathrm{mod}\,1231).$

Розкладемо $a=792=8\cdot 9\cdot 11=2^3\cdot 3^2\cdot 11.$

Для визначення наявності розв'язків обчислимо символ Лежандра

$$\left(\frac{2^3\cdot 3^2\cdot 11}{1231}\right)=\left(\frac{2}{1231}\right)\left(\frac{11}{1231}\right).$$

1) $1231=153\cdot 8-1,$ тобто $\left(\frac{2}{1231}\right)=1.$

2) $11=2\cdot 4+3,\ 1231=4\cdot 307+3\Rightarrow$

$\Rightarrow\left(\frac{11}{1231}\right)=-\left(\frac{1231}{11}\right)=-\left(\frac{-1}{11}\right)=1.$

3) $\left(\frac{2^3\cdot 3^2\cdot 11}{1231}\right)=1\cdot 1=1.$

Відповідь: конгруенція $x^2\equiv 792(\mathrm{mod}1231)$ має два розв'язки. ◄

6.4 Символ Якобі

Якобі узагальнив символ Лежандра на випадок, коли модуль конгруенції P є непарним числом, яке складене з простих чисел, тобто $P=p_1p_2...p_k$, p_i можуть повторюватися.

Означення 6.5. Символом Якобі називається показник

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)...\left(\frac{a}{p_k}\right), \tag{6.5}$$

де $\left(\frac{a}{p_1}\right),\left(\frac{a}{p_2}\right),...,\left(\frac{a}{p_k}\right)$ – є звичайними символами Лежандра.

Нехай $a=q_1q_2...q_m$ – розкладання числа a на прості множники. Тоді за властивостями символу Лежандра

$$\left(\frac{a}{p_1}\right)=\left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)...\left(\frac{q_m}{p_1}\right),$$

$$\left(\frac{a}{p_2}\right)=\left(\frac{q_1}{p_2}\right)\left(\frac{q_2}{p_2}\right)...\left(\frac{q_m}{p_2}\right);...;\left(\frac{a}{p_k}\right)=\left(\frac{q_1}{p_k}\right)\left(\frac{q_2}{p_k}\right)...\left(\frac{q_m}{p_k}\right),$$

тобто

$$\left(\frac{a}{P}\right)=\prod_{\substack{i=1,m\\ j=1,k}}\left(\frac{q_i}{p_j}\right). \tag{6.6}$$

Теорема 6.4

Символ Якобі має всі властивості символу Лежандра.

Приклад 6.4

Обчислити символ Якобі $\left(\frac{853}{1409}\right)$.

► $853 = 4 \cdot 213 + 1 \Rightarrow \left(\frac{853}{1409}\right) = \left(\frac{1409}{853}\right) = \left(\frac{556}{853}\right) =$

$\left(\frac{2^2 \cdot 139}{853}\right) = \left(\frac{139}{853}\right) = \left(\frac{853}{139}\right) = \left(\frac{853}{139}\right) = \left(\frac{19}{139}\right).$

$19 = 4 \cdot 4 + 3;\ 139 = 4 \cdot 34 + 3 \Rightarrow \left(\frac{19}{139}\right) =$

$= -\left(\frac{139}{19}\right) = -\left(\frac{6}{19}\right) = -\left(\frac{2}{19}\right)\left(\frac{3}{19}\right).$

$19 = 8 \cdot 2 + 3 \Rightarrow \left(\frac{2}{19}\right) = -1;\ 3 = 4 \cdot 0 + 3 \Rightarrow$

$\Rightarrow \left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = -1.$

$\left(\frac{853}{1409}\right) = (-1) \cdot (-1) \cdot (-1) = -1.$

Відповідь: $\left(\frac{853}{1409}\right) = -1.$ ◄

Питання для самоперевірки до розділу 6

1. Дайте визначення квадратичної конгруенції за довільним модулем.
2. Зазначте, в якому випадку квадратична конгруенція має єдиний нульовий розв'язок.
3. Назвіть спосіб розв'язання квадратичної конгруенції за складеним модулем.
4. Назвіть критерій Ейлера про наявність розв'язків конгруенції $x^2 \equiv a \pmod{p}$.
5. Дайте визначення лишка і нелишка за модулем p.
6. Назвіть наслідок із критерію Ейлера (із теореми 6.2) про наявність розв'язку квадратичної конгруенції.
7. Назвіть теорему Ейлера про добутки лишків і нелишків за певним простим модулем.
8. Назвіть 6 властивостей символу Лежандра.
9. За допомогою символу Лежандра з'ясуйте, чи є лишком 139 за модулем 5, якщо так, знайдіть розв'язок квадратичної конгруенції $x^2 \equiv 139 \pmod{5}$.
10. За допомогою символу Лежандра з'ясуйте, чи є лишком 98 за модулем 5, якщо так, знайдіть розв'язок квадратичної конгруенції $x^2 \equiv 98 \pmod{5}$.
11. Які лишки з повної системи найменших додатних лишків за модулем 7 $a = \{0,1,2,3,4,5,6\}$ є лишками для квадратичної конгруенції $x^2 \equiv a \pmod{7}$? Скільки таких лишків?
12. Дайте визначення символу Якобі за складеним модулем $P = p_1 p_2 ... p_k$.
13. Обчисліть символ Якобі для 393 за модулем 455.

Індивідуальні завдання до розділу 6

Завдання 6.1 Використовуючи символ Лежандра, зробити висновок про існування розв'язку конгруенції $ax^2 \equiv 0 \pmod{p}$.

Варіант	a	p	Варіант	a	p
1	221492250	29	16	19775250	19
2	576416412	41	17	5965164	41
3	17570858256	23	18	151954704	23
4	230783189	29	19	162084013	37
5	65447200	53	20	86442400	53
6	199938375	37	21	57580875	13
7	75719259	31	22	107545347	11
8	16472429225	43	23	114536275	57
9	13098765472	47	24	368322656	19
10	268372625	23	25	180758875	23
11	3479237307	59	26	45151570233	19
12	60061375	37	27	12720125	47
13	618566641	23	28	842682841	67
14	6618763525	43	29	1681419025	43
15	4235178717	47	30	1397919600	53

РОЗДІЛ 7 ПЕРВІСНІ КОРЕНІ ТА ІНДЕКСИ

У цьому розділі викладені теоретичні основи дискретного логарифмування, на яких базуються деякі тести на простоту числа та алгоритми побудови великих простих чисел.

Розглянуто зведені системи лишків за модулем m. Нагадуємо, що 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.

7.1 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).

Означення 7.1 Якщо для даного числа a існує декілька таких чисел $k_1, k_2, ..., k_s$, то найменше з них $\delta = \min(k_1, k_2, ..., k_s)$ називається *показником*, якому a належить за модулем m або *порядком числа* a за модулем m. Позначається це число так:

$$\delta = ord(a)_m, \ a \in Z_{\varphi(m)}. \tag{7.1}$$

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:

$$ord\,(a)=\infty,\ a\in Z_m,\ (a,m)\neq 1. \qquad (7.2)$$

Властивості показника $\delta = ord(a)_m$

Теорема 7.1

Якщо δ є порядком числа a за модулем m, то числа $a^0=1, a^1, ..., a^{\delta-1}$ за цим самим модулем неконгруентні.

Доведення

Дійсно, якщо $a^l \equiv a^k \pmod m$, $0<k<l<\delta$, то $a^{l-k}\equiv 1 \pmod m$, $l-k<\delta$, що суперечить визначенню δ (7.1).■

Теорема 7.2

Якщо $\delta = ord\,(a)_m$, то необхідною і достатньою умовою $a^k \equiv a^l \pmod m$ є $k \equiv l \pmod \delta$, зокрема (якщо $l=0$), $a^k \equiv 1 \pmod m \Leftrightarrow \delta \mid k$.

Доведення

а) Необхідність: $a^k \equiv a^l \pmod m$.

Нехай r і r_1 є найменшими додатними лишками чисел k і l за модулем δ; тоді з теореми про ділення із залишком маємо $k=\delta\cdot q+r$; $l=\delta\cdot t+r_1$ $q,t\in Z$, $0\le r<\delta$, $0\le r_1<\delta$. Використовуючи те, що $a^\delta \equiv 1 \pmod m$, робимо висновки:

$$a^k = a^{\delta\cdot q+r} = \left(a^\delta\right)^q a^r \equiv a^r \pmod m,$$

$$a^l = a^{\delta\cdot t+r_1} = \left(a^\delta\right)^t a^{r_1} \equiv a^{r_1} \pmod m,$$

$$a^k \equiv a^l \pmod m \Rightarrow a^r \equiv a^{r_1} \pmod m,$$

$r,\ r_1 < \delta \Rightarrow r \equiv r_1 \pmod\delta \Rightarrow k \equiv l \pmod\delta$, що і потрібно було довести.

б) Достатність: $k \equiv l \pmod\delta$.

Із визначення конгруенції можемо записати $k = l + \delta \cdot t$. Тоді $a^k = a^{l+\delta\cdot t} = a^l \left(a^\delta\right)^t$. Враховуючи, що $a^\delta \equiv 1 \pmod m$, можна записати $a^k = a^{l+\delta\cdot t} = a^l \left(a^\delta\right)^t \equiv a^l \pmod m$. Тобто з $k \equiv l \pmod\delta$ випливає $a^k \equiv a^l \pmod m$, що і потрібно було довести.■

Теорема 7.3

Нехай a за модулем m має порядок δ. Тоді $\varphi(m)$ ділиться на δ.

Доведення. Нехай $\delta = ord(a)_m$. З теореми Ейлера маємо $a^{\varphi(m)} \equiv 1 \pmod m$, $1 = a^0$, $a^{\varphi(m)} \equiv a^0 \pmod m$. За теоремою 7.2 $\varphi(m) \equiv 0 \pmod\delta$, отже, $\delta \mid \varphi(m)$, що і потрібно було довести.■

Таким чином, порядок довільного цілого числа a за модулем m є дільником функції Ейлера модуля m $\varphi(m)$. Найбільшим із дільників є сама функція Ейлера $\varphi(m)$.

Приклад 7.1

Визначимо, до якого показника належить кожне число із зведеної системи за модулем 7.

►Зведена система найменших додатних лишків для $\mod 7$: $1, 2, 3, 4, 5, 6$.

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:

$2^1 = 2;\ 2^2 = 4;\ \underline{2^3 = 8 \equiv 1 (\mathrm{mod}\, 7)};\ 2^4 = 16 \equiv 2 (\mathrm{mod}\, 7);$

$2^5 = 32 \equiv 4 (\mathrm{mod}\, 7);\ \underline{2^6 = 64 \equiv 1 (\mathrm{mod}\, 7)}.$

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:

$3^1 = 3;\ 3^2 = 9 \equiv 2 (\mathrm{mod}\, 7);\ 3^3 = 27 \equiv 6 (\mathrm{mod}\, 7);$

$3^4 = 81 \equiv 4 (\mathrm{mod}\, 7);$

$3^5 = 243 \equiv 5 (\mathrm{mod}\, 7);\ \underline{3^6 = 729 \equiv 1 (\mathrm{mod}\, 7)}.$

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:

$4^1 = 4;\ 4^2 = 16 \equiv 2 (\mathrm{mod}\, 7);\ \underline{4^3 = 64 \equiv 1 (\mathrm{mod}\, 7)};$

$4^4 = 256 \equiv 4 (\mathrm{mod}\, 7);$

$4^5 = 1024 \equiv 2 (\mathrm{mod}\, 7);\ \underline{4^6 = 4096 \equiv 1 (\mathrm{mod}\, 7)}.$

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:

$5^1 = 5;\ \ 5^2 = 25 \equiv 4 \pmod 7;\ \ 5^3 = 125 \equiv 6 \pmod 7;$

$5^4 = 625 \equiv 2 \pmod 7;$

$5^5 = 3125 \equiv 3 \pmod 7;\ 5^6 = 15625 \equiv 1 \pmod 7.$

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:

$6^1 = 6;\ \ 6^2 = 36 \equiv 1 \pmod 7;\ \ 6^3 = 216 \equiv 6 \pmod 7;$

$6^4 = 1296 \equiv 1 \pmod 7;\ \ 6^5 = 7776 \equiv 6 \pmod 7;$

$6^6 = 46656 \equiv 1 \pmod 7.$

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.◄

Означення 7.2 Числа a, порядок яких дорівнює $\varphi(m)$ (тобто $\delta = \varphi(m)$, якщо такі існують), називаються первісними коренями за модулем m.

7.2 Дослідження існування первісних коренів за елементарними модулями

Означення 7.3 Будемо називати модулі p, p^α, $2p^\alpha$, 2^α $(\alpha \geq 2)$ 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 $2p^\alpha$, довівши попередньо три допоміжні теореми.

Теорема 7.4

Якщо $ab = ord(x)_m$, то $b = ord(x^a)_m$.

Доведення. Дійсно, нехай x^a належить показнику δ ($\delta = ord\left(x^a\right)_m$). Тоді за означенням $\left(x^a\right)^\delta \equiv 1 (\mathrm{mod}\, m)$, звідки $x^{a\delta} \equiv 1 (\mathrm{mod}\, m)$; отже, $ab \mid a\delta$ (за теоремою 7.2 та з умови даної теореми), тобто $b \mid \delta \Rightarrow b \leq \delta$.

З іншого боку, за умовою теореми $x^{ab} \equiv 1 (\mathrm{mod}\, m)$, звідси $\left(x^a\right)^b \equiv 1 (\mathrm{mod}\, m)$. Отже, $\delta \mid b \Rightarrow \delta \leq b$ (за теоремою 7.2 та припущенням $\delta = ord\left(x^a\right)_m$).

З обох міркувань випливає, що $b = \delta$, тобто $b = ord\left(x^a\right)_m$, що і потрібно було довести.■

Теорема 7.5

Якщо $a = ord(x)_m$, $b = ord(y)_m$, $(a,b) = 1$, то $ab = ord(xy)_m$.

Доведення. Дійсно, нехай xy належить показнику δ $(\delta = ord(xy)_m)$. Тоді $(xy)^{\delta} \equiv 1 (\mathrm{mod}\, m)$. Піднесемо останню конгруенцію до степеня b. Маємо $x^{b\delta} y^{b\delta} \equiv 1 (\mathrm{mod}\, m)$. Оскільки за умовою теореми $y^b \equiv 1 (\mathrm{mod}\, m)$, то $x^{b\delta} \equiv 1 (\mathrm{mod}\, m)$. За умовою теореми $a = ord(x)_m$. Отже, $a \mid b\delta$ (за теоремою 7.2), оскільки $(a,b) = 1 \Rightarrow a \mid \delta$.

Піднесемо тепер конгруенцію $(xy)^{\delta} \equiv 1 (\mathrm{mod}\, m)$ до степеня a і використаємо припущення, аналогічні попереднім.

Маємо $x^{a\delta} y^{a\delta} \equiv 1 (\mathrm{mod}\, m) \Rightarrow y^{a\delta} \equiv 1 (\mathrm{mod}\, m) \Rightarrow b \mid \delta$.

Отримали, що $ab \mid \delta \Rightarrow ab \le \delta$.

З іншого боку, якщо теорема справедлива і $(xy)^{ab} \equiv 1 (\mathrm{mod}\, m)$, то із припущення $\delta = ord(xy)_m$ та теореми 7.2 випливає, що $\delta \mid ab \Rightarrow \delta \le ab$.

Отже $\delta = ab$, тобто $ab = ord(xy)_m$, що і потрібно було довести.■

Теорема 7.6

Існують первісні корені за модулем p.

Доведення. Нехай $\Delta = \{\delta_1, \delta_2, ..., \delta_r\}$ – множина всіх різних показників, яким належать числа $1, 2, \ldots, (p-1)$ 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 $1,2,\ldots,(p-1)$, які належать показнику δ_j. Згідно з теоремою 7.1 число $n_j = a_j^{t_j}$ належить показнику $q_s^{\alpha_s}$. Згідно з теоремою 7.2 добуток $g = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ належить показнику $\tau = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$. Отже, згідно з теоремою 7.3 τ ділить $\varphi(p) = p-1$, тобто $\tau \le p-1$.

Але оскільки числа з множини Δ ділять $\tau = НСК(\delta_1, \delta_2, \ldots, \delta_r)$, всі числа $1,2,\ldots,(p-1)$ є розв'язками конгруенції $x^{\tau} \equiv 1 \pmod p$. Отже, будемо мати $p-1 \le \tau$. Звідси, $\tau = p-1$, та $g = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ – первісний корінь.■

Теорема 7.7

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 $\alpha > 1$.

Доведення

Дійсно, якщо $g^{p-1} \equiv 1 \pmod p \Rightarrow g^{p-1} = p \cdot s + 1$, $s \in Z$.

$(g + p \cdot t)^{p-1} = g^{p-1} + p \cdot Q(g,t)$, де $Q(g,t)$ – поліном від g та t, тобто суперпозиція цілих чисел, тобто ціле число.

$$g^{p-1} + p \cdot Q(g,t) = 1 + p \cdot s + p \cdot Q(g,t) = 1 + p(s + Q(g,t)).$$

Позначимо $s+Q(g,t)=q$, $q\in Z$. Отримаємо $(g+p\cdot t)^{p-1}=1+p\cdot q$.

Якщо в останній рівності t пробігає повну систему лишків за модулем p, то одночасно з ним і q пробігає цю саму систему. Тому можна вибрати таке t, щоб $(q,p)=1$. Припустивши, що t саме таке і враховуючи, що в розкладанні бінома Ньютона $C_p^{\,1}=C_p^{\,p-1}=p$, виводимо індуктивний ланцюжок

- $(g+p\cdot t)^{p-1}=1+p\cdot q$ піднесемо до степеня p, маємо

$$(g+pt)^{(p-1)p}=(1+pq)^p=$$
$$=1+C_p^{\,1}pq+C_p^{\,2}p^2q^2+\ldots+C_p^{\,p-1}p^{p-1}q^{p-1}+p^pq^p=$$
$$=1+p^2\cdot q_1,\quad \text{тобто}\quad (g+pt)^{(p-1)p}\equiv 1\left(\mathrm{mod}\,p^2\right),\quad \text{з}$$

урахуванням $p(p-1)=\varphi(p^2)$ маємо

$$(g+pt)^{\varphi(p^2)}\equiv 1\left(\mathrm{mod}\,p^2\right).$$

- $(g+pt)^{(p-1)p}=1+q^2\cdot u_1$ піднесемо до степеня p, маємо

$$(g+p\cdot t)^{(p-1)p^2}=1+p^3\cdot q_2,$$

тобто $(g+pt)^{(p-1)p^2}\equiv 1\left(\mathrm{mod}\,p^3\right)$, з урахуванням $p^2(p-1)=\varphi(p^3)$ маємо

$$(g+pt)^{\varphi(p^3)}\equiv 1\left(\mathrm{mod}\,p^3\right),$$

……

• $\left(g+p\cdot t\right)^{(p-1)p^{\alpha-2}}=1+p^{\alpha-1}\cdot q_{\alpha-2}$ піднесемо до степеня p, маємо

$$\left(g+p\cdot t\right)^{(p-1)p^{\alpha-1}}=1+p^{\alpha}\cdot q_{\alpha-1},$$

тобто $\left(g+pt\right)^{(p-1)p^{\alpha-1}}\equiv 1\left(\mathrm{mod}\, p^{\alpha}\right)$, з урахуванням $p^{\alpha-1}\left(p-1\right)=\varphi\left(p^{\alpha}\right)$ маємо

$$\left(g+pt\right)^{\varphi\left(p^{\alpha}\right)}\equiv 1\left(\mathrm{mod}\, p^{\alpha}\right),$$

де всі $q_1, q_2,...q_{\alpha-1}$ також не діляться на p.

Розглянемо тепер порядок числа $g+pt$ за модулем p^{α}.

1) Нехай $g+pt$ належить показнику δ за модулем p^{α}, або $\delta=ord\left(g+pt\right)_{p^{\alpha}}$. Тоді згідно з теоремою 7.3 $\delta\,|\,p^{\alpha-1}\left(p-1\right)$.

2) $\left(g+pt\right)^{\delta}\equiv 1\left(\mathrm{mod}\, p^{\alpha}\right)$. Тоді $g^{\delta}\equiv 1\left(\mathrm{mod}\, p^{\alpha}\right)$, і відповідно $g^{\delta}\equiv 1\left(\mathrm{mod}\, p\right)$. Оскільки $ord\left(g\right)_p=p-1$, згідно з теоремою 7.3 $p-1|\delta$.

Згідно з 1), 2) показник δ має вигляд $\delta=p^{\lambda}\left(p-1\right)$, $0\le\lambda\le\alpha-1$. Але з індукції виведення співвідношення $\left(g+p\cdot t\right)^{(p-1)p^{\alpha-2}}=1+p^{\alpha-1}\cdot q_{\alpha-2}$, $\left(u_{\alpha\text{-}2},p\right)=1$ випливає, що $\left(g+pt\right)^{(p-1)p^{\lambda}}\equiv 1\left(\mathrm{mod}\, p^{\alpha}\right)$ буде справедливим для $\lambda=\alpha$-1 та порушуватиметься для $0\le\lambda<\alpha-1$.

Отже, число $g+pt$ належить показнику $\varphi\left(p^{\alpha}\right)=p^{\alpha-1}\left(p-1\right)$ за модулем p^{α}, тобто є первісним коренем за цим модулем, що і потрібно було довести.■

Теорема 7.8 (узагальнення для модуля p^α)

Степінь p^α простого непарного числа p завжди має первісні корені. Кількість таких коренів дорівнює $\varphi\left(\varphi\left(p^\alpha\right)\right)$. Кожний первісний корінь g модуля p породжує $\varphi\left(p^{\alpha-1}\right)$ неконгруентних між собою первісних коренів за модулем p^α. Первісний корінь g модуля p буде первісним коренем модуля p^α тільки в тому разі, коли число $g^{p-1}-1$ ділиться на p і не ділиться на p^2.

Висновки з теорем 7.7, 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 $p^\alpha,\ \ \forall\alpha>2$.

Теорема 7.9

Нехай $\alpha\geq 1$ та g – первісний корінь за модулем p^α. Непарне g_0 з двох чисел g та $g+p^\alpha$ буде первісним коренем за модулем $2p^\alpha$.

Доведення. Розглянемо функцію Ейлера для p^α та $2p^\alpha$:

$$\varphi\left(p^\alpha\right)=p^{\alpha-1}\left(p-1\right);\ \ \varphi\left(2p^\alpha\right)=\varphi\left(2\right)\varphi\left(p^\alpha\right)=$$

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

Отже, $\varphi\left(p^\alpha\right)=\varphi\left(2p^\alpha\right)$. Позначимо це значення $\Phi=\varphi\left(p^\alpha\right)=\varphi\left(2p^\alpha\right)$.

Розглянемо g та $g + p^{\alpha}$.

1) Нехай непарним буде g, тобто $g_0 = g$.

Розглянемо для конгруенцій $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$ та $g_0^{\,r} \equiv 1 \pmod{2p^{\alpha}}$ умови їх одночасного виконання.

Запишемо першу конгруенцію через рівність $g_0^{\,r} - 1 = p^{\alpha} \cdot t$. Оскільки g_0 є непарним, то $g_0^{\,r} - 1$ – парне число, отже, права частина рівності теж парне число. Оскільки p^{α} – непарне, то парним буде число $t = 2k$. Отже, першу рівність можна записати так:

$$g_0^{\,r} - 1 = p^{\alpha} \cdot 2k = 2p^{\alpha} \cdot k$$

або у визначеннях конгруенції

$$g_0^{\,r} \equiv 1 \pmod{2p^{\alpha}}.$$

Висновок. Якщо виконується конгруенція $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$, то виконується і $g_0^{\,r} \equiv 1 \pmod{2p^{\alpha}}$.

В інший бік. Друга конгруенція подається через рівність як $g_0^{\,r} - 1 = 2p^{\alpha} \cdot k$, $\forall k \in Z$. Позначимо $2k = t$, отримаємо $g_0^{\,r} - 1 = p^{\alpha} \cdot t$ або $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$.

Висновок. Якщо виконується конгруенція $g_0^{\,r} \equiv 1 \pmod{2p^{\alpha}}$, то виконується і $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$.

Підсумуємо висновки. Обидві конгруенції $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$ та $g_0^{\,r} \equiv 1 \pmod{2p^{\alpha}}$ виконуються одночасно.

Оскільки g_0 є первісним коренем за модулем p^{α}, то конгруенція $g_0^{\,r} \equiv 1 \pmod{p^{\alpha}}$ може виконуватися тільки для $r \geq \Phi$.

Оскільки конгруенції $g_0^{\,r} \equiv 1 \pmod{p^\alpha}$ та $g_0^{\,r} \equiv 1 \pmod{2p^\alpha}$ виконуються одночасно, то $g_0^{\,r} \equiv 1 \pmod{2p^\alpha}$ теж виконується тільки для $r \geq \Phi$, і g_0 є первісним коренем за модулем $2p^\alpha$.

2) У випадку, якщо $g = 2g_1$ – парне число, $g + p^\alpha$ буде непарним (через непарність p^α). Позначивши через g_0 число $g + p^\alpha$, можна провести ряд попередніх міркувань і дійти висновку, що для даного випадку первісним коренем за модулем $2p^\alpha$ буде саме $g + p^\alpha$. Таким чином, теорема 7.9 доведена.■

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 $(\pm 1)^2 = 1 \pmod 4$.

Для $\alpha \geq 3$ справедливою буде теорема 7.10.

Теорема 7.10

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 $ord(a)_{2^\alpha} \leq 2^{\alpha-2}$.

Доведення. Нехай $a = 1 + 2t$ – довільне непарне число. Проведемо доведення теореми індукцією за степенем α.

1) $\alpha = 3$. Порядок числа a за модулем $2^3 = 8$ згідно із твердженням теореми не перевищує $2^{3-2} = 2$. Перевіряємо

$$(1+2t)^2 = 1+4t+4t^2 = 1+4t(t+1) \equiv 1 \pmod{2^3}.$$

Візьмемо до уваги, що $t(t+1)$ є добутком двох чисел поспіль – парне число. Таким чином, твердження теореми виконується для $\alpha = 3$.

2) Припустимо, що твердження теореми виконується для довільного $\alpha \geq 3$, а саме:

$$a^{2^{\alpha-2}} = 1+2^{\alpha}t.$$

3) Доведемо справедливість твердження теореми для $\alpha+1$, $\alpha \geq 3$. Для цього піднесемо останню рівність до квадрата:

$$a^{2^{\alpha-1}} = 1+2^{\alpha+1}t+2^{2\alpha}t^2 = 1+2^{\alpha+1}t\left(1+2^{\alpha-1}t\right) \equiv 1 \pmod{2^{\alpha+1}},$$

отже твердження виконується і для $\alpha+1$, $\alpha \geq 3$. Теорема доведена.■

Наслідок із теореми 7.10

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.

Підсумовує все викладене в пункті 7.2 теорема 7.11.

Теорема 7.11

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 $m = 2$, $m = 4$.

7.3 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 7.12.

Теорема 7.12

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

$$\begin{aligned} &g^{\frac{\Phi}{q_1}} \equiv 1(\bmod m);\ g^{\frac{\Phi}{q_2}} \equiv 1(\bmod m);\\ &g^{\frac{\Phi}{q_3}} \equiv 1(\bmod m);...;\ g^{\frac{\Phi}{q_k}} \equiv 1(\bmod m). \end{aligned} \tag{7.3}$$

Доведення. Дійсно, якщо g є первісним коренем за модулем m, то тим самим він не може задовольняти ні одну з конгруенцій (7.3).

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 $g^{\delta} \equiv 1(\bmod m)$, $\delta < \Phi$. 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 (7.3).■

Приклад 7.2

Знайти найменший первісний корінь за модулем $m = 41$.

►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. $g=5$, $5^{20}=5^{3\cdot 6+2}=125^6\cdot 25=(41\cdot 3+2)^6(41-16)\equiv$

$\equiv 2^6(-16)(\mathrm{mod}\,41)\equiv 2^5\cdot 9=$

$=4\cdot 72\equiv 4\cdot(-10)=-40\equiv 1(\mathrm{mod}\,41)$ – перша конгруенція з двох виконується, отже, 5 не є первісним коренем за модулем 41.

5. $g=6$, $6^{20}=3^{20}\cdot 2^{20}\equiv(-1)1\equiv -1(\mathrm{mod}\,41)$ – перша конгруенція не виконується.

$6^8 \equiv 3^8 2^8 \equiv 1 \cdot 256 \equiv 1 \cdot 10 \pmod{41}$ – 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. $g = 7$, $7^{20} = 49^{10} \equiv 8^{10} = 2^{30} = (-1)^3 \equiv -1 \pmod{41}$ – перша конгруенція не виконується.

$7^8 = 49^4 \equiv 8^4 = 2^{12} \equiv (-1) \cdot 4 \pmod{41}$ – 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 7.3

Знайти первісні корені за модулем $m = 1681$.

►Модуль $m = 41^2 = 1681$. Первісний корінь і тут можна було б знайти, користуючись загальною теоремою. Але ми можемо знайти його, використовуючи теорему 7.8.

Згідно з цією теоремою модуль $m = 41^2$ має $\varphi\left(\varphi\left(41^2\right)\right) = \varphi(41 \cdot 40) = 40 \cdot 4 \cdot 4 = 640$ первісних коренів. Із прикладу 7.2 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 7.8).

Для первісного кореня 6 виконується конгруенція $6^{40} \equiv 1 \pmod{41}$, або $6^{40} = 1 + 41q, \quad \forall q \in Z$.

Оскільки $6^{40} - 1$ не ділиться на 41^2 (перевірити самостійно), то це приводить до досить великих чисел і тому має сенс скористатися теоремою 7.7 безпосередньо.

Використовуючи властивості конгруенцій, запишемо

$\left(6+41\cdot t\right)^{40}=1+41q$.

Піднесемо обидві частини рівності до степеня 41 і праву частину розкладемо за біномом Ньютона:

$\left(6+41\cdot t\right)^{40\cdot 41}=\left(1+41q\right)^{41}=$

$=1+C^{1}_{41}41q+C^{2}_{41}41^{2}q^{2}+...+41^{2}41^{39}q^{41}$.

З урахуванням того, що $C^{1}_{41}=41$, маємо

$\left(6+41\cdot t\right)^{40\cdot 41}=1+41^{2}\left(q+C^{2}_{41}q^{2}+...+41^{39}q^{41}\right)$.

Вираз $\left(q+C^{2}_{41}q^{2}+...+41^{39}q^{41}\right)$ є суперпозицією цілих чисел, тобто число ціле. Позначимо його через u, отримаємо

$\left(6+41\cdot t\right)^{40\cdot 41}=1+41^{2}\cdot u$.

Зауважимо, що $40\cdot 41=\varphi\left(41^{2}\right)$, тоді отриманий вираз набирає вигляду

$\left(6+41\cdot t\right)^{\varphi\left(41^{2}\right)}=1+41^{2}\cdot u$ або $\left(6+41\cdot t\right)^{\varphi\left(41^{2}\right)}\equiv 1\left(\mathrm{mod}\,41^{2}\right)$.

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 7.8 (висновок 2) можна стверджувати, що клас лишків $6+mt$ буде найменшим первісним коренем і для модулів $m=41^{\alpha}$, $\forall\alpha\geq 2$.◀

Приклад 7.4

Знайти первісний корінь за модулем $m = 3362$.

► Модуль $m = 3362 = 2 \cdot 1681 = 2 \cdot 41^2$. Первісний корінь і тут можна було б знайти, використовуючи загальну теорему 7.8, але ми знайдемо його простіше, використовуючи теорему 7.9.

Із прикладу 7.3 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. ◄

7.4 Індекси за елементарними модулями. Властивості індексів

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 7.13

Якщо γ пробігає повну систему найменших додатних лишків за модулем Φ, $\gamma = \{0,1,2,...,\Phi - 1\}$, то g^{γ} пробігає зведену систему лишків за модулем m, $g^{\gamma} = \{0, 1, 2,..., m-1\}$.

Доведення. Дійсно, згідно з теоремою 7.1 із зміною $\gamma = \{0,1,2,...,\Phi - 1\}$ g^{γ} пробігає Φ чисел, взаємно простих з m, та неконгруентних між собою за модулем m. ■

Розглянемо ціле число a, таке, що $(a,m) = 1$.

Означення 7.4 Якщо $a \equiv g^{\gamma} \pmod{m}$, $\gamma \geq 0$, 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 7.13 будь-яке a, взаємно просте з m, має певний єдиний індекс γ' серед чисел повної системи лишків за модулем Φ: $\gamma = \{0,1,2,...,\Phi - 1\}$.

Якщо γ' нам відоме, то ми можемо визначити і всі індекси числа a для основи g. Відповідно до теореми 7.3 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. $ind(ab) = ind\, a + ind\, b \pmod{\Phi}$.
2. $ind\, a^n \equiv n \cdot ind\, a \pmod{\Phi}$.

Дійсно,

$a \equiv g^{inda} \pmod{m}; b \equiv g^{indb} \pmod{m};$

$a \cdot b \equiv g^{inda} \cdot g^{indb} \pmod{m} \equiv g^{inda+indb} \pmod{m}.$

З іншого боку, $a \cdot b \equiv g^{ind(ab)} \pmod{m};$

Отже, $g^{ind(ab)} \equiv g^{inda+indb} \pmod{m} \Rightarrow$

$\Rightarrow ind\,(ab) \equiv ind\,a + ind\,b \pmod{\Phi}$, або

$ind\,(ab) = ind\,a + ind\,b + \Phi \cdot t,\ \forall t \in Z$.■

Властивість 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 7.5

Побудуємо таблиці індексів за модулем $p = 41$.

►У прикладі 7.2 ми знайшли перші два первісних корені за модулем 41 – $g_1 = 6$ та $g_2 = 7$. Оскільки таблиці індексів для основи 6 є серед стандартних таблиць, то візьмемо для демонстрації побудови за основу другий первісний корінь $g_2 = 7$.

Знайдемо всі степені числа 7 за модулем 41, коли індекс пробігає повну систему найменших додатних лишків.

$\pmod{41}$

$7^0 \equiv 1$	$7^8 \equiv 37$	$7^{16} \equiv 16$	$7^{24} \equiv 18$	$7^{32} \equiv 10$
$7^1 \equiv 7$	$7^9 \equiv 13$	$7^{17} \equiv 30$	$7^{25} \equiv 3$	$7^{33} \equiv 29$
$7^2 \equiv 8$	$7^{10} \equiv 9$	$7^{18} \equiv 5$	$7^{26} \equiv 21$	$7^{34} \equiv 39$

$7^3 \equiv 15$	$7^{11} \equiv 22$	$7^{19} \equiv 35$	$7^{27} \equiv 24$	$7^{35} \equiv 27$
$7^4 \equiv 23$	$7^{12} \equiv 31$	$7^{20} \equiv 40$	$7^{28} \equiv 4$	$7^{36} \equiv 25$
$7^5 \equiv 38$	$7^{13} \equiv 12$	$7^{21} \equiv 34$	$7^{29} \equiv 28$	$7^{37} \equiv 11$
$7^6 \equiv 20$	$7^{14} \equiv 2$	$7^{22} \equiv 33$	$7^{30} \equiv 32$	$7^{38} \equiv 36$
$7^7 \equiv 17$	$7^{15} \equiv 14$	$7^{23} \equiv 26$	$7^{31} \equiv 19$	$7^{39} \equiv 6$

$7^{40} \equiv 1$ 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 7.13.

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.7.1).

Таблиця 7.1

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: $37 \equiv 7^8 \pmod{41}$.

Знайдемо індекс числа 5: десятків немає, беремо рядок **0**, одиниць 5 – стовпчик **5**. На перетині стоїть число **18**, отже $5 \equiv 7^{18} \pmod{41}$.

Тепер побудуємо таблицю, в якій за відомим індексом можна знайти число (табл.7.2).

Таблиця 7.2

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 $7^{17} \equiv 30 \pmod{41}$. ◄

7.5 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 7.1

Конгруенція

$$x^n \equiv a \pmod{m} \tag{7.4}$$

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.

Доведення. Дійсно, якщо перейти до індексів, то індексування конгруенції $x^n \equiv a(\mathrm{mod}\, m)$ приведе до рівносильної конгруенції

$$n \cdot ind\, x \equiv ind\, a(\mathrm{mod}\, \Phi). \qquad (7.5)$$

Згідно із властивістю конгруенцій (п.3.1 *Властивості, що належать тільки конгруенціям*, властивість 4) остання має розв'язок тільки якщо $d \mid ind\, a$. Така конгруенція має d розв'язків (п.4.2). Тобто ми знайдемо d неконгруентних між собою за модулем Φ чисел $\varphi_1, \varphi_2, , \varphi_d$, які відповідають $ind\, x$ і є розв'язками конгруенції (7.5). Цим значенням індексів відповідають d неконгруентних між собою за модулем m чисел, які відповідають x і є розв'язками вихідної конгруенції (7.4).■

Наслідок 7.2

У зведеній системі лишків за модулем m кількість лишків степеня n становить $\frac{\Phi}{d}$.

Доведення. Дійсно, серед чисел $0,1,...,\Phi-1$, які є найменшими індексами лишків зведеної системи за модулем m, є $\frac{\Phi}{d}$ кратних d. Отже, твердження правильне.■

Приклад 7.6

Розглянемо декілька степеневих конгруенцій за модулем 41 і проаналізуємо їх розв'язання за допомогою індексів з основою 7.

►а) Розглянемо конгруенцію $x^8 \equiv 23(\mathrm{mod}\, 41)$.

Маємо $\Phi = \varphi(41) = 40$, $n = 8$, $(8,40) = 8$. Із таблиці 7.1 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 7.1 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 x 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 7.2:

$x \equiv 7, 20, 22, 16, 34, 21, 19, 25 (\mathrm{mod}\, 41)$.

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:

$x \equiv \pm 7, \pm 16, \pm 19, \pm 20 (\mathrm{mod}\, 41)$.

Виконаємо перевірку розв'язків.

Розв'язок $x \equiv 7 (\mathrm{mod}\, 41)$ перевіряємо в таблиці 7.1. Через парність степеня $34 \equiv -7 (\mathrm{mod}\, 41)$ теж є розв'язком.

Для $x \equiv \pm 16 (\mathrm{mod}\, 41)$ маємо:

$$(\pm 16)^8 \equiv 256^4 \equiv 10^4 \equiv 100^2 \equiv 18^2 \equiv 81 \cdot 4 \equiv -4 \equiv$$

$$\equiv 37 (\mathrm{mod}\, 41).$$

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:

$(\pm 19)^8 \equiv 361^4 \equiv (-8)^4 \equiv 64^2 \equiv (-18)^2 \equiv 81 \cdot 4 \equiv -4 \equiv$

$\equiv 37 (\mathrm{mod}\, 41)$.

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 7.7

Розглянемо числа, індекси яких з основою 7 кратні $d = 4$ (табл.7.2):

ind_7	0	4	8	12	16	20	24	28	32	36
Число	1	23	37	31	16	40	18	4	10	25

Після ранжування 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 7.3

Число a є лишком степеня n за модулем m тоді і тільки тоді, коли

$$a^{\frac{\Phi}{d}} \equiv 1(\mathrm{mod}\, m), \quad d = (\Phi, n). \tag{7.6}$$

Доведення. Дійсно, конгруенція $ind\, a \equiv 0(\mathrm{mod}\, d)$ рівносильна рівності $ind\, a = d \cdot t, \forall t \in Z$. Помножимо рівність на $\Phi = \varphi(m)$ і розділимо на d.

Отримаємо рівність $\frac{\Phi}{d} ind\, a = \Phi \cdot t, \forall t \in Z$, або конгруенцію $\frac{\Phi}{d} ind\, a \equiv 0(\mathrm{mod}\, \Phi)$, яка відповідає конгруенції (7.6).■

Приклад 7.8

У теоремі 7.12 умовою первісності кореня для числа g за модулем m є **не**виконання конгруенції $g^{\frac{\Phi}{q}} \equiv 1(\mathrm{mod}\, m)$, $\forall q : \{q \in Z, q \neq 1, q \neq \Phi, q \mid \Phi\}$. Ця умова означає, що первісний корінь g є нелишком степеня q за модулем m. Отже, у разі **не**виконання конгруенції $g^{\frac{\Phi}{2}} \equiv 1(\mathrm{mod}\, m)$ число g є квадратичним нелишком за модулем m (порівняйте з теоремою 2 пункту 6.2).

Наслідок 7.4

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 $\varphi(\Phi)=\varphi(\varphi(m))$.

Д о в е д е н н я

1) За означенням порядку числа a за модулем m δ є найменшим дільником $\Phi=\varphi(m)$, для якого виконується умова $a^{\delta}\equiv 1(\mathrm{mod}\, m)$.

Після індексування отримаємо

$\delta\cdot ind\, a\equiv 0(\mathrm{mod}\,\Phi)$ або $ind\, a\equiv 0\left(\mathrm{mod}\,\frac{\Phi}{\delta}\right)$.

Отже, отримали, що δ є найменшим дільником Φ, з яким $\frac{\Phi}{\delta}$ ділить число $ind\, a$. Відповідно саме число $\frac{\Phi}{\delta}$ буде найбільшим дільником, який ділить число $ind\, a$, тобто найбільшим спільним дільником між $ind\, a$ та Φ. *Пункт 1) доведений.*

2) Серед чисел $0,1,...,\Phi-1$, які є найменшими індексами лишків зведеної системи за модулем m, кратними $\frac{\Phi}{\delta}$, є числа вигляду $\frac{\Phi}{\delta}\cdot t$, $t=0,1,2,...,\delta-1$. Підставляючи ці числа в умову **1)**, отримаємо $\left(\frac{\Phi}{\delta}\cdot t,\Phi\right)=\frac{\Phi}{\delta}$. Згідно із властивостями НСД двох чисел скоротимо вираз на $\frac{\Phi}{\delta}$ і отримаємо взаємно прості числа – $(t,\delta)=1$. Чисел t, менших за δ, буде $\varphi(\delta)$. *Пункт 2) доведений.* ■

Приклад 7.9

У зведеній системі лишків за модулем 41 числами, які належать показнику 10, є числа a з умовою $\left(ind\, a, \varphi(41)\right) = \left(ind\, a, 40\right) = \frac{40}{10} = 4$, тобто числа, які відповідають у таблиці індексів 7.2 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 7.10

У зведеній системі лишків за модулем 41 первісними коренями є такі числа g, для яких виконується умова $\left(ind\, g, \Phi\right) = \left(ind\, g, 40\right) = 1$. Такими індексами будуть 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.

За таблицею 7.2 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 $\varphi(40) = 2^2 \cdot 4 = 16$.◄

7.6 Індекси за модулем 2^α

У теоремі 7.10 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}, $\alpha \geq 3$, існують. Таким числом, наприклад, буде 5. Розглянемо теорему.

Теорема 7.14

Для будь-якого цілого $\alpha \geq 2$ виконується рівність $5^{2^{\alpha-2}} = 1 + 2^{\alpha} t_{\alpha}$, де $t_{\alpha} = 2k+1$ – непарне.

Доведення. Доведення проведемо методом повної математичної індукції.

1) Перевіримо справедливість твердження при $\alpha = 2$, $\alpha = 3$:

$$\alpha = 2, \quad 5^{2^0} = 5 = 1 + 2^2 \cdot 1,$$

$$\alpha = 3, \; 5^{2^1} = 25 = 1 + 2^3 + 2^4 = 1 + 2^3 \cdot 3.$$

2) Припустимо, що рівність виконується для α:

$$5^{2^{\alpha-2}} = 1 + 2^{\alpha} t_{\alpha}, \quad t_{\alpha} = 2k+1. \qquad (*)$$

3) Доведемо рівність для $\alpha+1$. Для цього піднесемо до квадрата рівність (*), отримаємо

$$\left(5^{2^{\alpha-2}}\right)^2 = 5^{2^{\alpha-1}} = \left(1 + 2^{\alpha} t_{\alpha}\right)^2 = 1 + 2 \cdot 2^{\alpha} \cdot t_{\alpha} + 2^{2\alpha} \cdot t^2{}_{\alpha} =$$

$$= 1 + 2^{\alpha+1} \cdot t_{\alpha} \cdot \left(1 + 2^{\alpha-1} \cdot t_{\alpha}\right).$$

Позначимо $t_{\alpha+1} = t_{\alpha} \cdot \left(1 + 2^{\alpha-1} \cdot t_{\alpha}\right)$, t_{α} – непарне, $1 + 2^{\alpha-1} \cdot t_{\alpha}$ – непарне, тому і $t_{\alpha+1}$ – непарне число. Для $\alpha+1$ отримали $5^{2^{\alpha-1}} = 1 + 2^{\alpha+1} \cdot t_{\alpha+1}$.

Таким чином, припустивши справедливість рівності для α, ми довели справедливість рівності для $\alpha+1$.

Згідно з методом повної математичної індукції теорема доведена.■

У теоремі показано, що $ord_{2^\alpha} 5 = 2^{\alpha-2}$, тобто число 5 дійсно *належить* показнику $2^{\alpha-2}$ за модулем 2^α, $\alpha \geq 2$.

Розглянемо ще дві допоміжні теореми.

Теорема 7.15

Для $\alpha \geq 2$ 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:

$$u \equiv u' \pmod 2 \text{ та } v \equiv v' \pmod{2^{\alpha-2}}.$$

Доведення

Розглянемо конгруенцію $(-1)^u 5^v \equiv (-1)^{u'} 5^{v'} \pmod{2^\alpha}$. Якщо $(-1)^u \equiv (-1)^{u'} \pmod 2$, то $5^v \equiv 5^{v'} \pmod{2^\alpha}$. Оскільки 5 має порядок $2^{\alpha-2}$ за модулем 2^α, $\alpha \geq 2$, то у відповідності до теореми 7.2 $v \equiv v' \pmod{2^{\alpha-2}}$.

Якщо перша конгруенція не виконується, то друга неможлива для будь-яких v, v', оскільки тоді конгруенція набирає вигляду $5^v \equiv -5^{v'} \pmod{2^\alpha}$, і, зокрема, повинна б була виконуватися конгруенція $1 \equiv -1 \pmod 4$, що є неможливим.

Висновок. Конгруенція $(-1)^u 5^v \equiv (-1)^{u'} 5^{v'} \pmod{2^\alpha}$ виконується тільки тоді, коли обидві конгруенції з умови теореми виконуються **одночасно**.■

Теорема 7.16

За модулем 2^α, $\alpha \geq 2$, будь-яке просте непарне число конгруентне одному і тільки одному числу із системи чисел

$$-5^{2^{\alpha-2}}, \ldots, -5^2, -5, 5, 5^2, \ldots, 5^{2^{\alpha-2}}.$$

Доведення. Наведені числа мають вигляд $(-1)^u 5^v$, де $u=0$ або $u=1$, а v: $1 \le v \le 2^{\alpha-2}$. Згідно з теоремою 7.15 ці числа попарно неконгруентні, кількість цих чисел дорівнює $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha)$, що відповідає кількості непарних класів за модулем 2^α, тобто кожне з цих чисел конгруентне до одного певного класу непарних чисел за модулем 2^α. Отже, дана система чисел є зведеною системою лишків за модулем 2^α і будь-яке просте непарне число конгруентне тільки одному числу з цієї системи.■

Маючи систему степенів числа 5, яка створює зведену систему лишків, можемо визначити поняття індексу за модулем 2^α, $\alpha \ge 3$.

Означення 7.5 Індексом непарного числа a за модулем 2^α, $\alpha \ge 3$, називається пара чисел (u, v), $v \ge 0$, для якої виконується конгруенція $(-1)^u 5^v \equiv a \pmod{2^\alpha}$.

Іноді таку пару у відповідності до загальної теорії індексів позначають

$$inda = (u, v), \quad v \ge 0. \tag{7.7}$$

Із теореми 7.16 випливає, що будь-яке непарне число a має свій індекс за модулем 2^α.

Означення 7.6. 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

$$u \equiv u' \pmod{m} \text{ та } v \equiv v' \pmod{n}.$$

Конгруентність пар чисел за подвійним модулем будемо позначати так $(u,v) \equiv (u',v') \pmod{(m,n)}$.

Для конгруенції за подвійним модулем виконується очевидна властивість транзитивності конгруенцій.

У термінах конгруенції за подвійним модулем теорему 7.15 можна подати у вигляді теореми 7.15 а.

Теорема 7.15 а

Для $\alpha \geq 3$ $a \equiv b \left(\mathrm{mod}\, 2^{\alpha}\right)$ тоді і тільки тоді, коли $ind\, a \equiv ind\, b \left(\mathrm{mod}\left(2, 2^{\alpha-2}\right)\right)$, зокрема, якщо для довільного числа a за модулем 2^{α}, $\alpha \geq 3$ $inda = (u, v)$, $v \geq 0$ та $inda = (u', v')$, $v' \geq 0$, то $(u, v) \equiv (u', v') \left(\mathrm{mod}\left(2, 2^{\alpha-2}\right)\right)$.

Означення 7.7 Сумою індексів $(u_1, v_1) + ... + (u_n, v_n)$ називається індекс $(u_1 + u_2 + ... + u_n, v_1 + v_2 + ... + v_n)$.

Теорема 7.17

Для модуля 2^{α}, $\alpha \geq 3$ індекс добутку непарних чисел є конгруентним сумі індексів множників за подвійним модулем $\left(2, 2^{\alpha-2}\right)$.

Доведення. Розглянемо n непарних чисел $a_1, \ldots, a_n$. Кожне з цих чисел за теоремою 7.16 є конгруентним одному з чисел $-5^{2^{\alpha-2}}, \ldots, -5^2, -5, 5, 5^2, ..., 5^{2^{\alpha-2}}$, а саме:

$$a_1 \equiv (-1)^{u_1} 5^{v_1} \left(\mathrm{mod}\, 2^{\alpha}\right); a_2 \equiv (-1)^{u_2} 5^{v2} \left(\mathrm{mod}\, 2^{\alpha}\right); ...;$$

$$a_n \equiv (-1)^{u_n} 5^{v_n} \left(\mathrm{mod}\, 2^{\alpha}\right).$$

Перемноживши ці конгруенції, отримаємо

$$a_1 a_2 \cdot ... \cdot a_n \equiv (-1)^{u_1 + u_2 + ... + u_n} 5^{v_1 + v_2 + ... + v_n} \left(\mathrm{mod}\, 2^{\alpha}\right).$$

Позначимо індекс числа $a_1 a_2 \cdot ... \cdot a_n \left(\mathrm{mod}\, 2^{\alpha}\right)$ парою (u, v). Тоді $(u, v) \equiv (u_1 + ... + u_n, v_1 + ... + v_n) \left(\mathrm{mod}\left(2, 2^{\alpha-2}\right)\right)$.

За визначенням суми індексів (означення 7.7) останню конгруенцію можна переписати як

$$(u,v)\equiv(u_1,v_1)+(u_2,v_2)+...+(u_n,v_n)\left(\mathrm{mod}\left(2,2^{\alpha-2}\right)\right),$$

що і доводить теорему.■

Якщо $a_1=a_2=...=a_n$, то згідно з теоремою 7.17, можемо записати

$$inda^n\equiv n\cdot(u,v)\left(\mathrm{mod}\left(2,2^{\alpha-2}\right)\right),$$

або

$$inda^n\equiv n\cdot inda\left(\mathrm{mod}\left(2,2^{\alpha-2}\right)\right).$$

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 $(-1)^u 5^v\left(\mathrm{mod}\,2^\alpha\right)$.

Приклад 7.11

Скласти таблицю індексів за модулем 64.

►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 $2^{\alpha-2}=2^4=16$ $(v=0,1,2,...,15)$, а числа $(-1)^u 5^v$ – зведену систему лишків за модулем $2^\alpha=2^6=64$. Кількість класів у зведеній системі буде $\varphi\left(2^6\right)=2^5=32$.

Маємо:

$\pm 5^0 \equiv \pm 1;\ \pm 5^1 \equiv \pm 5;\ \pm 5^2 \equiv \pm 25;\ \pm 5^3 \equiv \pm 61;$

$\pm 5^4 \equiv \pm 49;\ \pm 5^5 \equiv \pm 53;\ \pm 5^6 \equiv \pm 9;\ \pm 5^7 \equiv \pm 45;$

$\pm 5^8 \equiv \pm 33;\ \pm 5^9 \equiv \pm 37;\ \pm 5^{10} \equiv \pm 57;\ \pm 5^{11} \equiv \pm 29;$

$\pm 5^{12} \equiv \pm 17;\ \pm 5^{13} \equiv \pm 21;\ \pm 5^{14} \equiv \pm 41;\ \pm 5^{15} \equiv \pm 13.$

Враховуючи, що знак «+» відповідає $u = 0$, а знак «-» – $u = 1$, та перетворивши від'ємні лишки на відповідні додатні, можемо записати таблицю індексів (табл.7.3).

Таблиця 7.3

N	*a*	*inda*	*N*	*a*	*inda*	*N*	*a*	*inda*	*N*	*a*	*inda*
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)

7.7 Індекси за складеним модулем

У пункті 7.2 було доведено існування первісних коренів за елементарними модулями типу p, p^α, $2p^\alpha$. Був наведений критерій відповідності первісного кореня за модулем p первісному кореню за модулем p^2, доведена теорема про те, що первісний корінь за модулем p^2 є первісним коренем за модулем p^α, $\alpha > 2$, і теорема про те, що непарний первісний корінь за модулем p^α, $\alpha > 2$, є одночасно первісним коренем за модулем $2p^\alpha$.

У пунктах 7.4 – 7.6 наведені визначення індексу числа за модулем та правила побудови таблиць індексів на базі

первісних коренів для елементарних модулів $p,\ p^{\alpha},\ 2p^{\alpha},\ 2^{\alpha}$.

Узагальнимо попередню теорію для модулів, які мають більш складну структуру.

Означення 7.8 Нехай $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ – 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

$$\begin{cases} a \equiv (-1)^u 5^v \left(\mathrm{mod}\, 2^{\alpha}\right); \\ a \equiv g_1^{\gamma_1} \left(\mathrm{mod}\, p_1^{\alpha_1}\right); \\ ...; \\ a \equiv g_k^{\gamma_k} \left(\mathrm{mod}\, p_k^{\alpha_k}\right), \end{cases} \tag{7.8}$$

то система $\{u, v, \gamma_1, \gamma_2, ..., \gamma_k\}$ називається системою індексів числа a за модулем m.

Із такого визначення випливає, що u,v – система індексів числа a за модулем 2^{α}, а $\{\gamma_1, \gamma_2, ..., \gamma_k\}$ – індекси числа a за модулями $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_k^{\alpha_k}$. Отже, відповідно до теорем 7.15, 7.15а та теореми 7.13 число a, взаємно просте з $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, має єдину систему індексів $\{u, v, \gamma_1, \gamma_2, ..., \gamma_k\}$ за модулем $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$. Будь-яка інша система $\{u', v', \gamma_1', \gamma_2', ..., \gamma_k'\}$ за цим самим модулем буде складатися з індексів, конгруентних до $\{\gamma_1, \gamma_2, ..., \gamma_k\}$ за модулями $\Phi, \Phi_0, \Phi_1, ..., \Phi_k$, тобто

$$u \equiv u' \pmod{\Phi},\ v \equiv v' \pmod{\Phi_0},$$
$$\gamma_1 \equiv \gamma_1' \pmod{\Phi_1}, ..., \gamma_k \equiv \gamma_r' \pmod{\Phi_k}.$$

Числа a із заданою системою індексів $\{u', v', \gamma_1', \gamma_2', ..., \gamma_k'\}$ можуть бути однозначно визначені із системи (7.8) і утворюють клас чисел за модулем $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ (п.4.4).

7.8 Побудова таблиць індексів. Застосування індексів до розв'язання задач теорії чисел

Приклад 7.12

Побудувати таблицю індексів за модулем 27.

► 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 7.7, 7.8 $g = 2$ 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 $g = 2$.

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8;\ 2^4 = 16;\ 2^5 = 32 \equiv 5;\ 2^6 \equiv 10;$

$2^7 \equiv 20;\ 2^8 \equiv 13;\ 2^9 \equiv 26;$

$2^{10} \equiv 25;\ 2^{11} \equiv 23;\ 2^{12} \equiv 19;\ 2^{13} \equiv 11;\ 2^{14} \equiv 22;\ 2^{15} \equiv 17;$

$2^{16} \equiv 7;\ 2^{17} \equiv 14 \pmod{27}.$

Будуємо таблицю індексів для чисел a зведеної системи за модулем $m = 27 = 3^3$ і основою $g = 2$.

Таблиця 7.4

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 7.4 є таблицею індексів для чисел a зведеної системи за модулем $m = 27 = 3^3$ і основою $g = 2$.◄

Приклад 7.13

Побудувати таблицю індексів для модуля 18.

►Модуль $m = 18 = 2 \cdot 3^2$ типу $m = 2p^\alpha$. Відповідно до теореми 7.9 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 7.8).

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 7.5 індексів для **модуля 9** за основою $g = 5$ (табл.7.5). $5^0 = 1;\ 5^1 = 5;\ 5^2 \equiv 7;\ 5^3 \equiv 8,\ 5^4 \equiv 4;\ 5^5 \equiv 2$.

Таблиця 7.5

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 7.9). 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 7.13).

Спираючись на попереднє, таблицю 7.6 індексів за **модулем 18** будуємо з використанням таблиці індексів за модулем 9 (табл.7.5).

Таблиця 7.6

a	1	5	7	11	13	17
Ind a	0	1	2	5	4	3

◄

Приклад 7.14

Побудувати таблицю індексів для модуля 72.

►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 $\varphi\left(2^3 3^2\right)=2^2 6=24$ класів лишків, взаємно простих із модулем 72.

Як було показано у п. 7.7 в цьому випадку кожне число з ЗСНЛ подається системою (7.8)

$$\begin{cases} a \equiv (-1)^u 5^v \pmod{2^3}, \\ a \equiv g_1^{\gamma_1} \pmod{3^2}, \end{cases}$$

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 $u \in \{0,1\}$. 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.

$(u,v) = (0,0) \Rightarrow a = (-1)^0 5^0 = 1;$

$(u,v) = (0,1) \Rightarrow a = (-1)^0 5^1 = 5;$

$(u,v) = (1,0) \Rightarrow a = (-1)^1 5^0 = -1 \equiv 7 \pmod{2^3};$

$(u,v) = (1,1) \Rightarrow a = (-1)^1 5^1 = -5 \equiv 3 \pmod{2^3}.$

Таблиця індексів за **модулем 8** буде мати такий вигляд (табл.7.7).

Таблиця 7.7

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 7.5).

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 7.7 індексів за модулем 8 відповідно до того, якому класу за модулем 8 належить лишок ЗСНЛ за модулем 72. Індекс γ_1 визначається з таблиці 7.5 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

$$47 \equiv 7 \pmod 8 \underset{табл\ 7.7}{\Rightarrow} (u,v) \equiv (1,0) \pmod{(2,2)};$$

$$47 \equiv 2 \pmod 9 \underset{табл\ 7.5}{\Rightarrow} \gamma_1 \equiv 5 \pmod{\varphi(9)=6}.$$

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 7.8

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 (7.8). Розглянемо лишок 43. Для цього лишка індексом буде

система індексів $\{1, 1, 2\}$, тобто ми повинні отримати цей лишок із системи

$$\begin{cases} a \equiv (-1)^1 5^1 \pmod 8, \\ a \equiv 5^2 \pmod 9. \end{cases}$$

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 (див. п. 4.4). Із першої конгруенції a запишемо так: $a=-5+8t$. Підставляємо у другу конгруенцію, шукаємо відповідне t:

$$-5+8t \equiv 25 \pmod 9; \quad 8t \equiv 30 \equiv 3 \pmod 9;$$

$$8t \equiv 3+45 \pmod 9; \; t = 6+9t_1.$$

Підставляємо у вираз для a:

$$a = -5+8(6+9t_1) = -5+48+72t_1 \equiv 43 \pmod{72}.$$

У результаті розв'язання системи конгруенцій, яка визначає задану систему індексів за модулем 72, дійсно отримали лишок 43.◄

Приклад 7.15

Побудувати таблицю індексів для модуля 21.

►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 $\gamma_2\in\{0,1,2,3,4,5\}$.

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** (табл. 7.9)

Таблиця 7.9

a	1	2
$inda = \gamma_1$	0	1

Будуємо таблицю індексів за **модулем 7** (табл. 7.10)

$3^0 = 1;\ 3^1 = 3;\ 3^2 = 9 \equiv 2;\ 3^3 \equiv 6;\ 3^4 \equiv 4;\ 3^5 \equiv 5.$

Таблиця 7.10

a	1	2	3	4	5	6
$inda = \gamma_2$	0	2	1	4	5	3

Складаємо таблицю індексів за **модулем 21** (табл. 7.11), використовуючи таблиці 7.9 та 7.10. Систему індексів визначаємо з названих таблиць за належністю лишка з ЗСНЛ за модулем 72 до класів лишків за модулями 3 та 7.

Таблиця 7.11

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 (7.8). Розглянемо лишок 11. Система індексів для нього $\{1,4\}$. Складаємо систему

$$\begin{cases} a \equiv 2^1 \pmod 3; \\ a \equiv 3^4 \pmod 7 \end{cases} \Rightarrow \begin{cases} a \equiv 2 \pmod 3; \\ a \equiv 4 \pmod 7. \end{cases}$$

$(3,7)=1$, розв'язок єдиний. Із першої конгруенції $a = 2+3t$. Підставляємо у другу, визначаємо t

$2+3t \equiv 4 \pmod 7;\ 3t \equiv 2 \pmod 7;\ 3t \equiv 9 \pmod 7;\ t = 3+7t_1.$

Підставляємо у вираз для a

$a = 2+3(3+7t_1) = 11+21t_1 \equiv 11 \pmod{21}.$

За результатами розв'язання системи отримали дійсно лишок 11 з 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

$$r \equiv a_1 a_2 \cdot \ldots \cdot a_n \pmod m.$$

Індексуємо її:

$$indr \equiv inda_1 + inda_2 + \ldots + inda_n \pmod{\varphi(m)}.$$

Індекси чисел $a_1, a_2, \ldots, a_n$ беремо з таблиці індексів за модулем m, знаходимо суму індексів $c = inda_1 + \ldots + inda_n$ і отримуємо конгруенцію

$$indr = c \pmod{\varphi(m)}.$$

Із таблиці індексів знаходимо число b, індекс якого дорівнює c. Остаточно маємо $r \equiv b \pmod m$.

Приклад 7.16

Знайти залишок від ділення числа $37^{20} \cdot 23^{12}$ на 61.

►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

$$\begin{cases} r_1 \equiv b_1 \left(\mathrm{mod}\ p_1^{\alpha_1}\right); \\ r_2 \equiv b_2 \left(\mathrm{mod}\ p_2^{\alpha_2}\right); \\ ..... \\ r_k \equiv b_k \left(\mathrm{mod}\ p_k^{\alpha_k}\right). \end{cases}$$

Якщо модуль $m = 2p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, то відносимо множник 2 до будь-якого множника (наприклад, до першого) і знаходимо залишки за модулями $2p_1^{\alpha_1}$, $p_i^{\alpha_i}$, $i = \overline{2,n}$ 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 залищок від ділення на таке число іншими способами, тобто без індексування. Але можна застосовувати і систему індексів $(u, v, \gamma_1, ..., \gamma_k)$.

Приклад 7.17

Знайти залишок від ділення числа $37^{20} \cdot 23^{12}$ на 4392.

► 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 $\varphi\left(2^3 3^2 61\right) = 4 \cdot 6 \cdot 60 = 1440$.

Складемо конгруенцію $37^{20} 23^{12} \equiv r \left(\mathrm{mod}\, 72 \cdot 61\right)$.

Індексуємо $20 ind 37 + 12 ind 23 \equiv indr \left(\mathrm{mod}\, 24 \cdot 60\right)$.

У таблиці індексів за модулем 72 (табл.7.8) 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 7.16 маємо індекси 37 та 23 за модулем 61 $ind 37 = 39$, $ind 23 = 57$. 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

$20(0,1,0,39) + 12(1,0,1,57) \equiv indr \left(\mathrm{mod}\, 24 \cdot 60\right)$.

Виконаємо дії.

$(0,20,0,780) + (12,0,12,684) \equiv indr \left(\mathrm{mod}\, 24 \cdot 60\right)$;

$(12,20,12,1464) \equiv indr \pmod{24 \cdot 60}$.

Отримали систему індексів залишку від ділення вихідного числа на модуль $72 \cdot 61$ $\{u, v, \gamma_1, \gamma_2\} = \{12,20,12,1464\}$.

Згадаємо, що 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 $\Phi_2 = \varphi(61) = 60$, $\gamma_2 = 1464 \equiv 24 (\mathrm{mod}\, 60)$.

Отримуємо спрощену конгруенцію індексів $(0,0,0,24) \equiv indr \pmod{24 \cdot 60}$.

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

$$\begin{cases} r \equiv (-1)^0 5^0 \pmod 8; \\ r \equiv 5^0 \pmod 9; \\ r \equiv 2^{24} \pmod{61}. \end{cases}$$

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 7.16).

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.

$1 + 72t \equiv 20 (\mathrm{mod}\, 61)$;

$11t \equiv 19;\ -50t \equiv 80;\ 5t \equiv -8;\ 5t \equiv -130;$

$t \equiv -26 \equiv 35 (\mathrm{mod}\, 61)$ 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. ◄

Питання для самоперевірки до розділу 7

1. Дайте визначення порядку числа a за модулем m. Для яких чисел дається це визначення?
2. Яка домовленість існує про порядок числа a за модулем у разі, коли $(a, m) \neq 1$?
3. За яких умов для певного модуля m будуть конгруентні між собою степені числа a.
4. Дайте визначення первісного кореня за модулем m.
5. За якими елементарними модулями існують первісні корені? Як визначити кількість первісних коренів за елементарними модулями?
6. Назвіть умови, за якими первісний корінь за модулем p буде первісним коренем за модулем p^2 та $p^\alpha, \alpha \geq 3$.
7. Скільки первісних коренів за модулем p^α породжує первісний корінь за модулем p?

8. Чи існують первісні корені за модулем 2^{α}? Поясніть свою відповідь.
9. Яка умова визначає лишок зведеної системи лишків за модулем m як первісний корінь?
10. До яких систем найменших додатних лишків і за якими модулями належать показники степенів і самі степені первісного кореня?
11. Дайте визначення індексу числа a за модулем m. Який аналог для дійсних чисел ви знаєте?
12. Яке число може бути основою індексування за певним модулем m?
13. Назвіть властивості індексів.
14. Сформулюйте умову розв'язання конгруенції $x^n \equiv a \pmod{m}$ із використанням теорії індексів. Скільки розв'язків має така конгруенція?
15. Чому дорівнює $\left(indg, \varphi(m)\right)$, якщо g є первісним коренем за модулем m.
16. Доведіть із використання теорії індексів теорему Ейлера про розв'язок квадратичної конгруенції.
17. Назвіть множину чисел, яка створює зведену систему лишків за модулем 2^{α}, $\alpha \geq 2$.
18. Дайте визначення індексу для непарного числа за модулем 2^{α}, $\alpha \geq 3$.
19. Дайте визначення конгруенції за подвійним модулем.
20. Чому дорівнює індекс добутку непарних чисел за модулем 2^{α}, $\alpha \geq 3$?
21. Дайте визначення системи індексів за модулем $m = 2^{\alpha} p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$.

22. За яких умов дві системи індексів $\{u, v, \gamma_1, ..., \gamma_k\}$ та $\{u', v', \gamma_1', ..., \gamma_k'\}$ будуть системами індексів непарного числа a за модулем $m = 2^{\alpha} p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$.

23. Яка система конгруенцій визначає певний лишок з таблиці індексів за модулем $m = 2^{\alpha} p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$? Чи визначена ця система? Чому?

Індивідуальні завдання до розділу 7

Знайти залишок від ділення добутка 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.	$N = 37^{11}23^{19};\ m = 144$

№	Вихідні дані	№	Вихідні дані
27.	$N = 51^{13}43^{15};\ m = 400$	28.	$N = 29^{31}53^{23};\ m = 784$
29.	$N = 61^{31}47^{23};\ m = 544$	30.	$N = 47^{37}67^{13};\ m = 736$

СПИСОК ЛІТЕРАТУРИ

1. Основы теории чисел / И. М. Виноградов. – Москва-Ижевск : НИЦ«Регулярная и хаотическая динамика», 2005. – 176 с.
2. Теория чисел. Элементарный курс / А. К. Сушкевич – Х. : Издательство ХГУ, 1954. – 204 с.
3. Теория чисел / А. А. Бухштаб. – изд. 2-е, испр. – М. : Просвещение, 1966.
4. Конспект лекцій з курсу «Застосування теорії чисел у криптографії» / укладач О. І. Оглобліна. – Суми : СумДУ, 2009.
5. Сборник упражений по теории чисел / В. У. Грибанов, П. И. Титов. – М. : Просвещение, 1964. – 144 с.
6. Задачник-практикум по алгебре и теории чисел / А. А. Кочева. – М. : Просвещение, 1984. – Ч. 3 – 40 с.
7. Задачник-практикум по теории чисел / В. А. Александров, С. М. Горшенин. – М. : Просвещение, 1972. – 80 с.
8. Методичні вказівки та контрольні завдання з дисципліни «Застосування теорії чисел у криптографії» для студентів спеціальностей «Інформатика» та «Прикладна математика» / укладач О. І. Оглобліна. – Суми : СумДУ, 2010.
9. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. :МЦНМО, 2003. – 328 с.
10. Курс теории чисел и криптографии / Н. Коблиц. – М. : Научное изд-во ТВП, 2001. – 254 с.
11. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. – М. : МЦНМО, 2002. – 104 с.

Додаток А
(обов'язковий)
Таблиці відповідей до тестів

Тест до розділу 1

Ном. питання ►	**Блок 1**			**Блок 2**		
Варіанти відповідей ▼	**1**	**2**	**3**	**1**	**2**	**3**
A				●	●	●
B	●	●	●			
C						
D						
Ном. питання ►	**Блок 3**			**Блок 4**		
Варіанти відповідей ▼	**1**	**2**	**3**	**1**	**2**	**3**
A					●	
B						●
C	●			●		
D		●	●			
Ном. питання ►	**Блок 5**			**Блок 6**		
Варіанти відповідей ▼	**1**	**2**	**3**	**1**	**2**	**3**
A						
B		●			●	
C	●			●		●
D			●			

Продовження додатка А

Ном.питання►	**1**	**2**	**3**
Блок 7	18 97 5 27	1 1 0 1	5 6 1 1
Блок 8	***x=-11, y=222***	***x=-3, y=4***	***x=8, y=-121***

Тест до розділу 2

Ном. питання ►	**Блок 1**			**Блок 2**	
Варіанти відповідей ▼	**1**	**2**	**3**	**1**	**2**
A					
B				●	●
C	●				
D		●	●		
E				●	●
F					●
G				●	●

Ном. питання ►	**1**	**2**	**3**
Блок 3	***1728***	***672***	***540***
Блок 4	***43092***	***28392***	***262080***
Блок 5	***496***	***2096128***	***33550336***
Блок 6	***6720***	***7200***	***17280***

Продовження додатка А

Тест до розділу 4

Ном. питання ►	**Блок 1**					
Варіанти відповідей ▼	**1**	**2**	**3**	**4**	**5**	**6**
A			●		●	
B		●		●		
C	●					●

Ном. питання ►	**Блок 2**					
Варіанти відповідей ▼	**1**	**2**	**3**	**4**	**5**	**6**
A	●		●	●		●
B						
C		●			●	

Додаток Б
(обов'язковий)
Таблиці індексів

p = 3, p-1 = 2, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

p = 5, p-1 = 2^2, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

p = 7, p-1 = 2·3, g = 3

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

p = 11, p-1 = 2·5, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

p = 13, p-1 = 2^2·3, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

p = 17, p-1 = 2^2·3, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

p = 19, p-1 = 2·3^2, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

p = 23, p-1 = 2·11, g = 5

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

p = 29, p-1 = 2^2·7, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

p = 31, p-1 = 2·3·5, g = 3

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

p = 37, p-1 = 22·32, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

p = 41, p-1 = 23·5, g = 6

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	9	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

p = 43, p-1 = 2·3·7, g = 3

N	0	1	2	3	4	5	6	7	8	9
0		0	27	I	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Продовження додатка Б

p = 47, p-1 = 2·23, g = 5

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	36	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

p = 53, p-1 = 22·13, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

p = 59, p-1 = 2·29, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

p = 61, p-1 = 22·3·5, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

p = 67, p-1 = 2·3·11, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

p = 71, p-1 = 2·5·7, g = 7

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

p = 73, p-1 = 23·32, g = 5

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

p = 79, p-1 = 2·3·13, g = 3

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

p = 83, p-1 = 2·41, g = 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

p = 89, p-1 = 23·11, g = 3

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Продовження додатка Б

p = 97, p-1 = $2^5 \cdot 3$, g = 5

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Додаток В

(обов'язковий)

Таблиця простих чисел $p < 4070$ та їх найменших первісних коренів g

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1 ЮЗ	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3

Продовження додатка В

p	g	p	g	p	g	p	g	p	g	p	g	p	g
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6