Міністерство освіти і науки України
Сумський державний педагогічний університет
імені А. С. Макаренка

ЛУКАШОВА Т.Д., ДРУШЛЯК М.Г.

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

ЧАСТИНА І

Суми-2022

УДК 512.12(075.3)
Л 89

Рекомендовано вченою радою Сумського державного педагогічного університету імені А.С. Макаренка, протокол №4 від 28 листопада 2022 р.

Рецензенти:
О.О. Пипка – доктор фізико-математичних наук, професор, завідувач кафедри геометрії та алгебри Дніпровського національного університету імені Олеся Гончара;
Семко М.М. – доктор фізико-математичних наук, професор кафедри кібернетики та прикладної математики Державного податкового університету

Лукашова Т. Д. , Друшляк М. Г.
М 89 Алгебра і теорія чисел: навчальний посібник для студентів спеціальності 014 «Середня освіта. Математика». Ч.І. – Суми: СумДПУ ім. А.С. Макаренка, 2022. – 123 с.

Посібник складено відповідно до програми курсу «Алгебра і теорія чисел» спеціальності 014 «Середня освіта. Математика» педагогічних університетів.

Посібник містить теоретичний матеріал з основних розділів курсу теорії чисел та теорії груп, а також приклади розв’язування типових задач. Наведено завдання для індивідуальної роботи та для тестової перевірки знань.

Для студентів спеціальності «Середня освіта. Математика» денної та заочної форм навчання.

УДК 512.12(075.3)

ЗМІСТ

ВСТУП

Головною метою курсу «Алгебра і теорія чисел» є формування у студентів погляду на сучасну алгебру як на науку про системи об’єктів довільної природи, в яких встановлено операції, що за своїми властивостями більш або менш подібні до додавання і множення чисел; вивчення та розв’язання задач, що виникають у цих системах, а також виховання алгебраїчної культури та формування наукового світогляду, які необхідні майбутньому вчителю математики для глибокого розуміння цілей та завдань шкільного курсу математики, спеціальних факультативних курсів, для забезпечення міжпредметних зв’язків та проведення наукових досліджень.

Курс алгебри і теорії чисел дає наукове обґрунтування таких понять як: *група, кільце, поле, подільність, конгруенція, многочлен,* що лежать в основі багатьох математичних теорій та безпосередньо стосуються фундаментальних курсів математичного аналізу, дискретної математики, теорії ймовірностей, топології та математичного програмування.

У результаті вивчення дисципліни *студенти повинні*:

знати: предмет та об’єкти вивчення сучасної алгебри і теорії чисел; основні поняття теорії алгебраїчних систем, зокрема, теорії груп, кілець та полів; теорії подільності у кільцях, теорії конгруенцій, алгебри многочленів від однієї та кількох змінних; ключові теоретичні положення курсу; основні методи розв’язання типових задач;

вміти: розв’язувати основні типи задач, передбачені програмою; аналізувати доведення теорем, вказувати необхідні та достатні умови; доводити ключові положення курсу.

Посібник призначений для викладачів та студентів спеціальності 014 «Середня освіта. Математика» денної та заочної форм навчання.

В посібнику будуть використовуватись загальноприйняті терміни та позначення. Зокрема, для числових множин будуть використовуватися наступні символи:

$N = \{1, 2, 3, \dots, n, \dots\}$ – множина цілих чисел;

$Z = \{\dots, -m, \dots, -2, -1, 0, 1, 2, \dots, m, \dots\}$ – множина цілих чисел (її можна також означити як об'єднання $Z = N \cup \{0\} \cup N^{-}$);

$Q = \left\{\frac{m}{n}, m \in Z, n \in N\right\}$ – множина раціональних чисел;

I – множина ірраціональних чисел (тобто, чисел, які не можна подати у вигляді $\frac{m}{n}$, де $m \in Z, n \in N$);

$R = Q \cup I$ – множина дійсних чисел;

$C = \{a + bi, a, b \in R,\ i^2 = -1\}$ – множина комплексних чисел.

Для вказаних числових множин має місце включення

$$N \subset Z \subset Q \subset R \subset C.$$

1. ТЕОРІЯ ПОДІЛЬНОСТІ У КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

1.1. Відношення подільності в кільці цілих чисел

Означення 1.1. *Нехай* $a, b \in Z$. *Говорять, що* a *ділиться націло на* b (*або* b *ділить* a), *якщо існує таке ціле число* q, *що* $a = bq$.

При цьому a називають *діленим* або *кратним* числа b, b – *дільником* числа a, q – *часткою* відповідно. Для запису твердження «a ділиться на b» використовується позначення $a \vdots b$ (відповідно, запис $b|a$ означає, що b є дільником a).

Наприклад, $-10 \vdots 5$, оскільки $-10 = 5 \cdot (-2)$ (тут $q = -2 \in Z$). Відповідно, $10 \,\dot{\vdots}\, 3$, бо не існує такого цілого числа q, що $10 = 3 \cdot q$.

Зауважимо, що при $b \neq 0$ число q визначається однозначно. Справді, нехай $a \vdots b$. Припустимо, що існують цілі числа q_1 та q_2 такі, що $a = b \cdot q_1$ і $a = b \cdot q_2$. Віднімаючи від першої рівності другу, одержимо: $0 = b \cdot (q_1 - q_2)$. Оскільки, Z не містить дільників нуля, тобто відмінних від нуля чисел, які в добутку дають 0 і $b \neq 0$, то $q_1 - q_2 = 0$, тобто $q_1 = q_2$. Отже, частка від ділення у даному випадку єдина.

Властивості подільності

1. $\forall a \in Z \;\; a \vdots a$ (рефлексивність).

▻ Справді, $a = a \cdot 1$, де $q = 1$.◅

2. $\forall a \in Z \;\; a \vdots 1, a \vdots (-1), a \vdots (-a)$.

3. $\forall a \in Z \;\; 0 \vdots a$.

▻ Справді, $0 = a \cdot 0$, де $q = 0$. ◅

4. $a \vdots 0 \;\Leftrightarrow a = 0$.

▻ *Необхідність.* Нехай $a \vdots 0$, тоді $a = 0 \cdot q$, звідки $a = 0$.
Доведення *достатності* випливає з властивості 3. ◅

5. Якщо $a \vdots b$ і $b \vdots c$, то $a \vdots c$ (транзитивність).

▻ Оскільки $a \vdots b$ і $b \vdots c$, то існують такі $q_1, q_2 \in Z$, що $a = b \cdot q_1$ і $b = c \cdot q_2$. Тоді $a = (c \cdot q_2) \cdot q_1 = c \cdot q$, де $q \in Z$, тобто $a \vdots c$. ◅

6. Якщо $a \vdots b \wedge b \vdots a$, то $a = \pm b$. Зокрема,

$$\forall a, b \in N\ (a \vdots b \wedge b \vdots a\ \Rightarrow a = b).$$

$\triangleright$ Нехай $a \vdots b$ і $b \vdots a$. Тоді $a = b \cdot q_1$ і $b = a \cdot q_2$, де $q_1, q_2 \in Z$. Якщо при цьому $a = 0$, то й $b = 0$ і властивість доведено.

Нехай $a \neq 0$. Тоді $a = b \cdot q_1 = aq_2q_1$, звідки $q_1q_2 = 1$ і $q_1 = q_2 = 1$ або $q_1 = q_2 = -1$. Отже, $a = \pm b$.$\triangleleft$

7. Якщо $a \vdots b \wedge c \vdots b$, то $(a \pm c) \vdots b$.

$\triangleright$ З умов $a \vdots b$ і $c \vdots b$ випливає, що існують такі $q_1, q_2 \in Z$, що $a = b \cdot q_1$ і $c = b \cdot q_2$. Тоді $a \pm c = b(q_1 \pm q_2) = b \cdot q$, де $q = q_1 \pm q_2 \in Z$, тобто $(a \pm c) \vdots b$. $\triangleright$

Твердження, обернене до властивості 7, місця не має: алгебраїчна сума $(5 \pm 4) \vdots 3$, але жоден з доданків на 3 не ділиться.

8. Якщо $a_1 \vdots b \wedge a_2 \vdots b \wedge \ldots \wedge a_n \vdots b$, то $(a_1 \pm a_2 \pm \cdots \pm a_n) \vdots b$.

9. Якщо $a \vdots b$, то $ac \vdots b$ для довільного $c \in Z$.

$\triangleright$ З умови $a \vdots b$ випливає, що для деякого цілого $q \in Z$ має місце рівність $a = b \cdot q$. Тоді для довільного $c \in Z$ маємо $ac = b \cdot (qc)$, причому $qc \in Z$, тобто $ac \vdots b$. $\triangleright$

10. Якщо $a \vdots b$, то $a^n \vdots b^n$ і $a^n \vdots b$, де $n \in N$.

$\triangleright$ Оскільки $a \vdots b$, то існує таке ціле число q, що $a = b \cdot q$. Для довільного $n \in N$: $a^n = b^n \cdot q^n$, де $q^n \in Z$, тобто $a^n \vdots b^n$. $\triangleright$

11. Якщо $a_1 \vdots b \wedge a_2 \vdots b \wedge \ldots \wedge a_n \vdots b$, то $(a_1c_1 \pm a_2c_2 \pm \cdots \pm a_nc_n) \vdots b$.

12. Якщо $(a \pm c) \vdots b$ і $a \vdots b$, то $c \vdots b$.

$\triangleright$ З умов $(a \pm c) \vdots b$ та $a \vdots b$ випливає, що $a \pm c = b \cdot q$ і $a = b \cdot q_1$, де $q, q_1 \in Z$. Підставимо значення a в попередню рівність:

$$\pm c = b \cdot q - b \cdot q_1 = b(q - q_1),$$

де $(q - q_1) \in Z$, тобто $c \vdots b$. $\triangleright$

Приклад 1.1. Довести, що для довільного натурального числа n

$$(n^3 + 3n^2 + 2n) \vdots 6.$$

Розв'язання

Спосіб 1. Розкладемо даний вираз на множники:

$$n^3+3n^2+2n=n^3+n^2+2n^2+2n=n^2(n+1)+2n(n+1)=$$

$$=(n+1)(n^2+2n)=n(n+1)(n+2)$$

Отже, вказаний вираз є добутком трьох послідовних натуральних чисел. Оскільки кожне друге натуральне число дялиться на 2, а кожне третє – на 3, то вказаний вираз ділиться на $2\cdot 3=6$. Отже, $(n^3+3n^2+2n)\vdots 6$

Спосіб 2. Доведемо твердження із використанням методу математичної індукції.

1. Перевіримо, чи ділиться даний вираз на 6 при $n=1$:

$$1+3+2=6\vdots 3.$$

2. Припустимо, що при $n=k$ твердження виконується, тобто

$$(k^3+3k^2+2k)\vdots 6.$$

3. Доведемо, що при $n=k+1$ подільність виконується, тобто

$$((k+1)^3+3(k+1)^2+2(k+1))\vdots 6.$$

Маємо:

$$(k+1)^3+3(k+1)^2+2(k+1)=$$

$$=k^3+3k^2+3k+1+3k^2+6k+3+2k+2=$$

$$=(k^3+3k^2+2k)+3k^2+9k+6=$$

$$=(k^3+3k^2+2k)+3(k^2+3k+2)=$$

$$=(k^3+3k^2+2k)+3(k+1)(k+2)$$

Вираз (k^3+3k^2+2k) ділиться на 6 за індуктивним припущенням. Вираз у других дужках, очевидно, ділиться на 2 (бо кожне друге натуральне число парне), отже, другий доданок ділиться на 6, а значить, сума також ділиться на 3. За принципом математичної індукції дане твердження має місце для довільного натурального *n.*

1.2. Ділення з остачею. Теорема про ділення з остачею

Як зазначалося раніше, в кільці Z ділення націло виконується не завжди, тому виникає потреба так узагальнити поняття ділення, щоб воно виконувалося для будь-яких чисел a та b.

Означення 1.2. *Нехай* $a \in Z, b \in N$. *Розділити* a *на* b *з остачею означає представити* a *у вигляді*

$$a = bq + r, \quad 0 \le r < b, \quad r, q \in Z.$$

При цьому a *називають діленим;* b *– дільником,* q *– неповною часткою, а* r *– остачею.*

Зауважимо, що $a \vdots b$ тоді і тільки тоді, коли $r = 0$.

Приклад 1.2. Знайти r та q якщо:

1) $a = 5, b = 2$: $\quad 5 = 2q + r \Rightarrow q = 2, r = 1;$
2) $a = 2, b = 5$: $\quad 2 = 5q + r \Rightarrow q = 0, r = 2.$

Означення 1.2 можна узагальнити для будь-яких цілих чисел a і $b \neq 0$ наступним чином.

Означення 1.3. *Нехай* $a, b \in Z$ і $b \neq 0$. *Розділити* a *на* b *з остачею означає представити* a *у вигляді*

$$a = bq + r, \quad 0 \le r < |b|, \quad r, q \in Z.$$

Приклад 1.3. Для $a = -2, b = -5$ маємо:

$$-2 = (-5) \cdot 1 + 3, q = 1, r = 3.$$

Теорема 1.1 *(про ділення з остачею). Для довільних цілих чисел* a *та* b $(b \neq 0)$ *існує і до того ж єдина пара чисел* q *та* r*, які задовольняють рівність:*

$$a = bq + r, \quad 0 \le r < |b|, \quad r, q \in Z.$$

Доведення. **Випадок 1**. Нехай $b > 0$. Тоді $|b| = b$. Розглянемо функцію $y = bx$. Оскільки $b > 0$, то функція $y = bx$ зростаюча й існує таке $q \in Z$, що

$$bq \le a < b(q + 1).$$

Тоді $0 \le a - bq < b$. Позначимо $a - bq = r$. Тоді $0 \le r < b$.

Доведемо єдиність представлення (тобто, єдиність r та q у цьому випадку). Справді, нехай існують цілі числа q_1 та r_1 і $0 \le r_1 < b$. Тоді $a = bq + r$ та $a = bq_1 + r_1$. Прирівнюючи праві частини цих ріностей, одержимо: $bq + r = bq_1 + r_1$, звідки

$$b(q - q_1) = r_1 - r.$$

Але тоді, з одного боку, $(r_1 - r) \vdots b$, а з іншого, $0 \le |r_1 - r| < b$. Це можливо лише за умови $|r_1 - r| = 0$, тобто при $r_1 = r$. Але у такому випадку $b(q - q_1) = 0$ і оскільки $b > 0$, то $q - q_1 = 0$, звідки $q = q_1$, що й треба було довести. Єдиність доведено.

Випадок 2. Нехай $b < 0$. Позначимо $b_1 = -b > 0$ і за доведенням вище для чисел a та b_1 існує одна і лише одна пара цілих чисел q_1 та r_1 таких, що $a = b_1 q_1 + r_1$, де $0 \le r_1 < b_1$.

Тоді $a = b_1 q_1 + r_1 = (-b_1)(-q_1) + r_1 = bq + r$, де $q = -q_1$, $r = r_1$, $b_1 = |b|$. Теорему доведено.

Приклад 1.4. Знайти неповну частку q і остачу r від ділення цього числа a на ціле число b, якщо:

1) a=17, b=5;
2) a=5, b=17;
3) a=17, b=–5;
4) a=–17, b=5;
5) a=5, b=–17;
6) a=–5, b=–17;
7) a=–5, b=17;
8) a=–17, b=–5.

Розв'язання

Для відшукання q та r знайдемо найбільше ціле число k, яке кратне b і не перевищує a. Тоді неповну q дістанемо як частку від ділення k на b, а остачу r знайдемо як різницю між a на k.

a	17	5	17	-17
b	5	17	-5	5
$a=bq+r$	17=5·3+2	5=17·0+5	17=(-5)(-3)+2	-17=5·(-4)+3

a	5	-5	-5	-17
b	-17	-17	17	-5
$a=bq+r$	5=(-17)·0+5	-5=(-17)·1+12	-5=17·(-1)+12	-17=(-5)·4+3

1.3. Найбільший спільний дільник (НСД) двох чисел. Алгоритм Евкліда. Властивості НСД двох чисел

Означення 1.4. *Ціле число* δ *називається спільним дільником чисел* a *і* b*, якщо* $a \vdots \delta$ *і* $b \vdots \delta$.

Означення 1.5. *Натуральне число* d *називається найбільшим спільним дільником (НСД) чисел* a *і* b*, якщо* d *є спільним дільником цих чисел і ділиться на будь-який інший спільний дільник* δ *чисел* a *і* b.

Позначення: $d = (a, b)$.

Очевидно, що НСД чисел a *і* b є найбільшим натуральним дільником цих чисел.

Теорема 1.2. *Якщо НСД* d *цілих чисел* a *і* b *існує, то він визначається однозначно.*

Доведення. Нехай d і d_1 – найбільші спільні дільники цілих чисел a і b. Оскільки $d = (a, b)$, то $d \vdots d_1$ і $d = d_1 k,\ k \in N$, Аналогічно, $d_1 = (a, b)$, тому $d_1 \vdots d$ і $d_1 = dt,\ t \in N$.

З цих рівностей випливає, що $d = dkt$, звідки $kt = 1$. Оскільки $k \in N$ і $t \in N$, то $t = k = 1$ і $d = d_1$. Теорему доведено.

В той же час, однозначність найбільшого спільного дільника двох цілих чисел не гарантує його існування. У зв'язку з цим опишемо спосіб знаходження НСД, запропонований Евклідом.

Лема 1.1. *Нехай* a, b *– цілі числа,* $b > 0$. *Якщо* $a \vdots b$, *то* $(a, b) = b$.

Доведення. Оскільки $a \vdots b$ і $b \vdots b$, то b – спільний дільник чисел a і b. Навпаки, якщо c – довільний спільний дільник чисел a і b, то він є дільником b. Отже, за означенням $(a, b) = b$.

Зокрема, якщо $a \vdots b$ і $b \neq 0$, то $(a, b) = |b|$.

Лема 1.2. *Якщо* $a = bq + r$, *де* a, b, r *– відмінні від нуля цілі числа, то* $(a, b) = (b, r)$.

Доведення. Нехай $d = (a, b)$ і $d_1 = (b, r)$. Тоді $a \vdots d$ і $b \vdots d$, то $a - bq = r \vdots d$ і d – спільний дільник b і r, отже $d_1 \vdots d$.

Оскільки $d_1 = (b, r)$, то $b \vdots d_1$ і $b \vdots r$, а значить $bq + r = a \vdots d_1$, то d_1 – спільний дільник b і a. Тоді $d \vdots d_1$. Оскільки d і d_1– натуральні числа, то $d = d_1$. Лему доведено.

Для доведення існування НСД двох чисел $a \ i \ b$ застосовують спосіб, запропонований Евклідом. Цей спосіб називається *алгоритмом Евкліда.*

Алгоритм Евкліда

Нехай a і b – цілі числа, причому $0 < b < a$. Поділимо a на b з остачею:

$$a = bq_0 + r_1, 0 \le r_1 < b.$$

Якщо $r_1 = 0$, то $a \vdots b$ і за лемою 1.1 $(a, b) = b$.

Нехай $0 < r_1 < b$. Розділимо b з остачею на r_1:

$$b = q_1 r_1 + r_2, 0 \le r_2 < r_1.$$

Якщо $r_2 = 0$, то $b \vdots r_1$ і за лемами 1.1 та 1.2 $(a, b) = (b, r_1) = r_1$.

Нехай $0 < r_2 < r_1$. Ділимо з остачею r_1 на r_2 і т.д. Процес вважається закінченим, якщо отримаємо остачу, що дорівнює 0. Дійсно, остачі r_1, r_2... за означенням є цілими додатними числами і задовольняє умову: $b > r_2 > r_1 > 0$. Але таких остач може бути не більше ніж b. Отже, через кілька кроків отримаємо, що

$$b > r_2 > r_1 > \cdots > r_{n-1} > r_n > 0, \text{ але } r_{n+1} = 0.$$

Запишемо отримані рівності:

$$a = bq_0 + r_1, 0 < r_1 < b$$
$$b = q_1 r_1 + r_2, 0 < r_2 < r_1$$
$$r_1 = q_2 r_2 + r_3, 0 < r_3 < r_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = q_{n-1} r_{n-1} + r_n, 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_n r_n, \ r_{n+1} = 0.$$

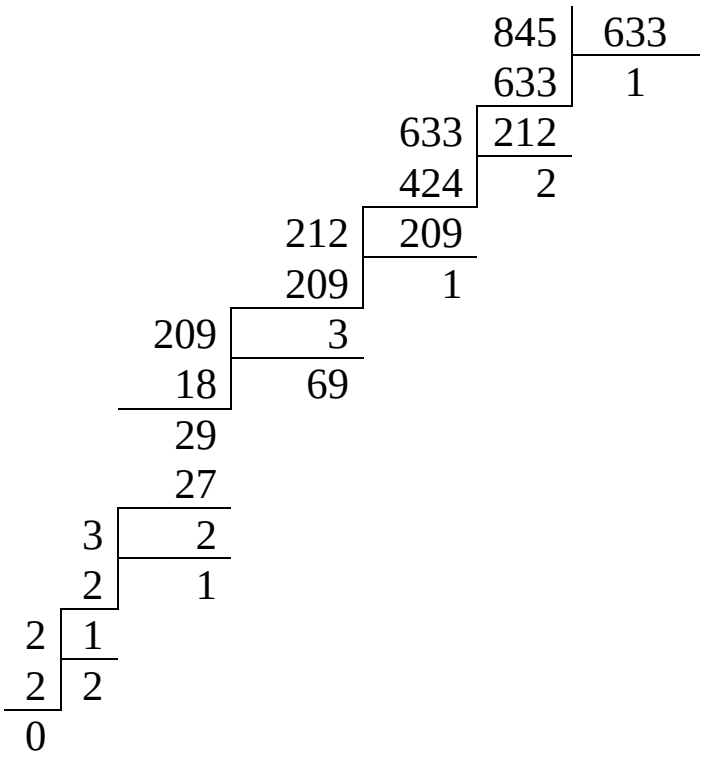
Тоді $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = r_n > 0$, а r_{n+1}=0.

Теорема 1.3. *Для будь-яких цілих чисел a і b, одночасно не рівних 0, найбільший спільний дільник завжди існує і дорівнює останній відмінній від нуля остачі в алгоритмі Евкліда.*

Приклад 1.5. Знайти НСД чисел 845 і –633.

Розв'язання

Зрозуміло, що $(845,-633)=(845,633)$. Виконаємо послідовно ділення більшого числа на менше, меншого – на отриману остачу і так далі.



Отже, $(845,-633)=(845,633)=1$.

Властивості НСД двох чисел

1. $\forall a.b\in\mathbb{N}\ (a,b)=(-a,b)=(a,-b)=(-a,-b)$.

2. *Якщо кожне з цілих чисел* a *і* b *помножити на натуральне число* m*, то їх НСД також помножиться на* m*, тобто*

$$(ma,mb)=m(a,b).$$

▷ Помножимо кожну з рівностей в алгоритмі Евкліда на m:

$$am=bmq_0+r_1m,$$
$$bm=r_1mq_1+r_2m,$$
$$r_1m=r_2mq_2+r_3m,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2}m=r_{n-1}mq_{n-1}+r_nm,$$
$$r_{n-1}m=r_nmq_{n-1}.$$

Маємо алгоритм Евкліда для чисел am та bm. Остання відмінна від 0 остача дорівнює $r_n m$, отже, $(am, bm) = r_n m = m(a, b)$.◁

3. *Якщо кожне з двох чисел a і b поділити на їх спільний дільник $c > 0$, то НСД цих чисел також поділиться на c, тобто*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}.$$

▻ За властивістю 2 $(a, b) = \left(\frac{a}{c} \cdot c, \frac{b}{c} \cdot c\right) = c\left(\frac{a}{c}, \frac{b}{c}\right)$ і $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}$.◁

4. *Натуральний спільний дільник d цілих чисел a і b є їх НСД тоді і тільки тоді, коли* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

▻ *Необхідність.* Нехай $d = (a, b)$. Тоді за попередньою властивістю $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d} = 1$.

Достатність. Нехай $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. За властивістю 1

$$(a, b) = \left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) = d \cdot \left(\frac{a}{d}, \frac{b}{d}\right) = d.$$◁

5. *Якщо d – найбільший спільний дільник цілих чисел a і b, то існують цілі числа x і y такі, що $d = ax + by$* (відповідне зображення називається *лінійним представленням НСД чисел a і b*).

▻ З алгоритму Евкліда маємо:

$$r_1 = a - bq_0,$$
$$r_2 = b - r_1 q_1,$$
$$r_3 = r_1 - r_2 q_2,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-4} = r_{n-1} - r_{n-3} q_{n-3},$$
$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-2},$$
$$r_n = r_{n-2} - r_{n-1} q_{n-1}.$$

Тоді $d = r_{n-2} \cdot 1 + r_{n-1} \cdot (-q_{n-1})$. Підставимо в цю рівність значення $r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$, тоді

$$d = r_{n-2} + (r_{n-3} - r_{n-2} q_{n-2}) \cdot (-q_{n-1}) =$$
$$= r_{n-2}(1 + q_{n-2} q_{n-1}) + r_{n-3} \cdot (-q_{n-1}).$$

Послідовно підставляючи замість $r_{n-2}, r_{n-3}, \dots, r_3, r_2, r_1$ їх значення, отримаємо: $d = ax + by$, де x і y – деякі цілі числа. ◅

6. *Нехай $a_1, a_2, \dots, a_n$ – цілі числа, відмінні від нуля. Тоді їх НСД визначається рекурентно з рівності*

$$(a_1, a_2, \dots, a_n) = ((\dots(a_1, a_2), a_3) \dots, a_n).$$

▻ Введемо позначення. Нехай $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$,…, $(d_{n-2}, a_{n-1}) = d_{n-1}$, $(d_{n-1}, a_n) = d_n$. Покажемо, що

$$(a_1, a_2, \dots, a_n) = (d_{n-1}, a_n).$$

Для $n = 2$, тобто для двох чисел, твердження справедливе. Припустимо, що воно справедливе для $(n-1)$ числа і покажемо, що воно справедливе для n чисел.

Нехай $(a_1, a_2, \dots, a_{n-1}, a_n) = d$. Тоді $a_i \vdots d$ для $\forall i = 1,2, \dots, n$. Значить $d_{n-1} \vdots d$ і $a_n \vdots d$, а отже, $d_n \vdots d$. З іншого боку, оскільки $(d_{n-1}, a_n) = d_n$,то $d_{n-1} \vdots d_n$ і $a_n \vdots d_n$, значить $a_i \vdots d_n$ для $\forall i = 1,2, \dots, n$. Тоді $d \vdots d_n$. З умов $d_n \vdots d$ і $d \vdots d_n$ для натуральних чисел d та d_n маємо $d_n = d$. ◅

Приклад 1.6. Знайти НСД чисел 1920, 450, 985, користуючись алгоритмом Евкліда.

Розв'язання

Для знаходження НСД трьох чисел знайдемо НСД двох чисел $d_1 = (1920,450)$, а потім НСД третього числа і d_1: $d = (985, d_1)$.

1920	450
1800	4

450	120
360	3

120	90
90	1

90	30
90	3
0	

985	30
90	32

85	
60	

30	25
25	1

25	5
25	5
0	

Отже, $d_1 = (1920,450) = 30$, $d = (985, d_1) = 5$.

Приклад 1.7. Знайти лінійне представлення НСД чисел a=845 і b=633.

Розв'язання

$$a = b \cdot 1 + 212 \qquad 212 = a - b$$
$$b = 212 \cdot 2 + 209 \qquad 209 = b - 2 \cdot 212$$
$$212 = 209 \cdot 1 + 3 \qquad 3 = 212 - 209 \cdot 1$$
$$209 = 3 \cdot 69 + 2 \qquad 2 = 209 - 3 \cdot 69$$
$$3 = 2 \cdot 1 + 1 \qquad d = 3 - 2 \cdot 1$$
$$d = 1$$
$$d = 3 - 2 \cdot 1 = 3 - 1(209 - 3 \cdot 69) = 70 \cdot 3 - 1 \cdot 209$$
$$= 70(212 - 209 \cdot 1) - 209 =$$
$$= 70 \cdot 212 - 71 \cdot 209 = 70 \cdot 212 - 71(b - 2 \cdot 212) =$$
$$= -71b + 212 \cdot 212 =$$
$$= -71b + 212(a - b) = 212a - 283b = a \cdot 212 + (-283) \cdot b$$
$$x = 212, y = 283.$$

Взаємно прості числа

Означення 1.7. *Цілі числа* a *і* b *називаються взаємно простими, якщо їх НСД дорівнює* 1.

1. (*Критерій взаємної простоти двох цілих чисел). Для того, щоб числа* a *і* b *були взаємно простими, необхідно і достатньо, щоб існували такі цілі числа* x *та* y*, що* $ax + by = 1$.

◅ *Необхідність*. Нехай $(a, b) = 1$, тоді за властивістю 5 НСД існують такі цілі числа x і y, що $ax + by = 1$.

Достатність. Нехай існують такі цілі числа x та y, що $ax + by = 1$ і нехай $d = (a, b)$. Тоді $a \vdots d$ і $b \vdots d$, значить $ax \vdots d$ і $by \vdots d$, отже, $ax + by = 1 \vdots d$. Це можливо лише, коли $d = 1$, тобто числа a і b взаємно прості. ▻

2. Якщо $(a, b) = 1$, то $(a^n, b^m) = 1$

3. Якщо $(a, b) = 1, \forall c \in N, \forall n \in N \cup \{0\}$, то $(a^n c, b) = (c, b)$.

4. Якщо $ab \vdots c$ і $(b, c) = 1$, то $a \vdots c$.

◅ Оскільки $(b,c)=1$, то за властивістю 1 існують такі цілі числа x та y, що $bx+cy=1$. Помножимо цю рівність на a:

$$abx+acy=a,$$

при цьому $abx \vdots c$, $acy \vdots c$, отже, $abx+acy=a \vdots c$.▻

5. Якщо $a \vdots b$ і $a \vdots c$ і $(b,c)=1$, то $a \vdots bc$.

◅ Оскільки $a \vdots b$ і $a \vdots c$, то $a=bt,\ a=cs,\ t,s \in Z$, отримаємо $bt=cs,\ bt \vdots c$. Оскільки $(b,c)=1$, то $t \vdots c$ і $t=cm,\ m \in Z$. Звідси $a=bt=bcm$, тобто $a \vdots bc$.▻

6. Якщо $(a,c)=1$, $(b,c)=1$, то $(ab,c)=1$.

◅ Оскільки $(a,c)=1$, то існують числа $x,y \in Z$ такі, що$ax+cy=1$. Помножимо обидві частини рівності на b: $abx+bcy=b$.

Нехай $d=(ab,c)$. Тоді $ab \vdots d$ і $c \vdots d$, а значить, $abx+bcy=b$. Таким чином, d – спільний дільник b і c, а оскільки $(b,c)=1$, то $1 \vdots d$. В силу того, що $d>0$, маємо $d=1$. Отже, $(ab,c)=1$.▻

Означення 1.7. *Числа $a_1,a_2,\ldots,a_n$ називаються попарно взаємно простими , якщо будь-які два з них є взаємно простими*

1.4. Найменше спільне кратне (НСК) двох чисел. Властивості НСК. Теорема про зв'язок НСК та НСД

Означення 1.8. *Ціле число M називається спільним кратним (СК) чисел a і b, якщо воно ділиться на кожне з цих чисел.*

Означення 1.9. *Натуральне число m називається найменшим спільним кратним (НСК) чисел a і b, якщо воно є їх спільним кратним і ділить будь-яке інше спільне кратне.*

Позначення: $m=[a,b]$.

Теорема 1.4. $\forall a,b \in N \quad [a,b]=\frac{ab}{(a,b)}$.

Доведення. Позначимо $d=\text{НСД}(a,b)$ і $M=\text{СК}(a,b)$. Тоді $a=da_1;\quad b=db_1$, причому $(a_1,b_1)=1$ за властивістю 3 НСД.

З іншого боку, $M=a\cdot k,\quad M=b\cdot k',$ для деяких $k,k' \in N$.

Розглянемо дріб $\frac{M}{b} = \frac{ak}{db_1} = \frac{a_1 k}{b_1}$. Оскільки $M \vdots b$, то $\frac{M}{b} \in Z$. Враховуючи, що $(a_1, b_1) = 1$, маємо $k \vdots b_1$, звідки $k = b_1 t$, $t \in Z$. Підставимо це значення у дріб $\frac{M}{b}$:

$$\frac{M}{b} = \frac{a_1 k}{b_1} = \frac{a_1 b_1 t}{b_1} = a_1 t = \frac{a_1 dt}{d} = \frac{at}{d}.$$

Тобто, довільне спільне кратне заданих чисел визначається з рівності $M = \frac{bat}{d}$. Число M буде найменшим, якщо $t = 1$. Отже, найменше спільне кратне чисел a і b дорівнює $m = \frac{ab}{d}$. Теорему доведено.

Властивості НСК двох чисел

1. $\forall a. b \in \mathbb{N}$ $[a, b] = [-a, b] = [a, -b] = [-a, -b]$

2. $\forall a, b, m \in N$ $[ma, mb] = m[a, b]$

$\triangleright$ $[ma, mb] = \frac{ma \cdot mb}{(ma, mb)} = \frac{ma \cdot mb}{m(a, b)} = m \cdot [a, b]. \triangleleft$

3. $\forall a. b \in \mathbb{N}\ [a, b] = ab \Leftrightarrow (a, b) = 1.$

4. *Для будь-яких цілих чисел a і b їх НСК визначається однозначно.*

$\triangleright$ Нехай m і m_1 – НСК цілих чисел a і b. Оскільки $m = [a, b]$, то $m_1 \vdots m$. Оскільки $m_1 = [a, b]$, то $m \vdots m_1$. Враховуючи, що $m \in \mathbb{N}$ і $m_1 \in \mathbb{N}$, маємо $m_1 = m. \triangleleft$

5. *Нехай a і b – цілі числа, $a > 0$. Якщо $a \vdots b$, то $[a, b] = a$.*

6. *Нехай $a_1, a_2, \ldots, a_n$ – цілі числа, відмінні від нуля. Тоді* $[a_1, a_2, \ldots, a_n] = \big[[a_1, a_2, \ldots, a_{n-1}], a_n\big]$.

$\triangleright$ Нехай $[a_1, a_2] = m_2$, $[m_2, a_3] = m_3$, …, $[m_{n-2}, a_{n-1}] = m_{n-1}$, $[m_{n-1}, a_n] = m_n$. Покажемо, що $[a_1, a_2, \ldots, a_n] = [m_{n-1}, a_n] = m_n$.

Для $n = 2$, тобто для двох чисел a_1 і a_2 твердження справедливе.

Нехай воно має місце для $(n - 1)$ числа. Покажемо, що воно справедливе для n чисел. Справді, $m_n \vdots a_1$ і $m_n \vdots m_{n-1}$. Але за

припущенням $m_{n-1} = [a_1, a_2, \ldots, a_{n-1}]$ і тому $m_{n-1} \vdots a_1$, $m_{n-1} \vdots a_2, \ldots, m_{n-1} \vdots a_{n-1}$. Отже, m_n ділиться на кожне з чисел $a_1, a_2, \ldots, a_n$ і тому є їх спільним кратним.

Нехай M – спільне кратне чисел $a_1, a_2, \ldots, a_n$. Тоді M ділиться на $a_1, a_2, \ldots, a_{n-1}$, а отже, і на їх НСК m_{n-1}. Оскільки M ділиться на m_{n-1} і a_n, то воно ділиться й на $[m_{n-1}, a_n] = m_n$. Це означає, що $m_n = [a_1, a_2, \ldots, a_n]$.◅

Приклад 1.8. Знайти НСК чисел 1920, 450, 985.

Розв'язання

НСК трьох чисел знайдемо наступним чином: знайдемо НСК чисел 1920 та 985, а потім НСК третього числа і [1920, 450]. За результатами прикладу 1.6 НСД перших двох чисел $d_1 = (1920{,}450) = 30$. Тому [1920, 450]=$\frac{450 \cdot 1920}{30} = 28800$.

Знайдемо тепер НСК 28800 та 985:

$$[28800, 985] = \frac{28800 \cdot 985}{5} = 5673600.$$

1.5. Прості та складені числа, їх властивості. Теорема Евкліда

Натуральні числа залежно від кількості їх натуральних дільників можна розділити на 3 групи:

1) перша група складається з одиниці, яка має один натуральний дільник;
2) другу групу складають числа, які мають рівно два різних натуральних дільники. Це, наприклад, числа 2,3,5,7,…;
3) третю групу складають числа, що мають більше, ніж два натуральних дільники.

Означення 1.9. *Натуральне число називається* ***простим****, якщо воно має рівно два натуральних дільники. Відповідно, число, що має більше двох натуральних дільників, називається* ***складеним****.*

Одиниця не відноситься ні до простих, ні до складених чисел.

Властивості простих чисел

1. *Якщо* p *– просте число,* $a \in N, \quad p \vdots a \Rightarrow a = p \vee a = 1.$

2. *Якщо* p, q *– прості числа,* $p \neq q$*, то* $(p^n, q^m) = 1, \quad m, n \in N.$

3. $\forall a \in N, p$ *– просте число або* $a \vdots p \vee (a, p) = 1.$

4. *Якщо* $ab \vdots p, p$ *– просте число, то або* $a \vdots p$ *або* $b \vdots p.$

5. *Найменший неодиничний дільник натурального числа* n *є числом простим.*

◅ Якщо n – просте число, то властивість очевидна. Якщо n – число складене і n_1 – найменший неодиничний дільник, то $n = n_1 m$. Припустимо, що n_1 складене, тоді існує число $n_2 \neq 1$, що є його власним дільником. Тоді n_2 – менший за n_1 дільник n, що суперечить умові. ▻

6. *Найменший простий дільник складеного числа не перевищує кореня квадратного з цього числа.*

◅ Нехай a – складене число і p – його найменший дільник. За властивістю 5 p – просте число. Оскільки $a = pa_1$ і $p \le a$, то $a = pa_1 \ge p \cdot p = p^2$. Отже, $a \ge p^2 \Leftrightarrow p \le \sqrt{a}$. ▻

7. *Якщо кожне просте число, що не перевищує* $\sqrt{a}, a \in N$*, не є дільником a, то a – просте число.*

Теорема 1.5 (*теорема Евкліда*). *Множина простих чисел нескінченна.*

Доведення. Припустимо супротивне. Нехай множина простих чисел скінченна і складається з чисел

$$\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_k.$$

Розглянемо їх добуток $q = \mathrm{p}_1 \mathrm{p}_2 \ldots \mathrm{p}_k + 1$. Оскільки $q > 1$ і $p_i > 1$, то q не може бути простим, а значить є складеним. Але в такому випадку воно має прості дільники, тобто існує таке p_i, що $q \vdots \mathrm{p}_i$. Маємо протиріччя з побудовою числа q. Отже, припущення неправильне і простих чисел нескінченна кількість.

Решето Ератосфена

Грецький математик Ератосфен (III ст. до н.е.) знайшов досить простий спосіб знаходження усіх простих чисел, що не перевищують даного натурального числа n. Алгоритм даного процесу наступний:

1) виписуємо підряд всі числа натурального ряду від 2 до n;
2) викреслюємо всі числа, що діляться на 2, окрім 2;
3) викреслюємо всі числа, що діляться на 3, окрім 3, і т.д.;
4) викреслюємо всі числа, що діляться на прості числа, які не перевищують $\sqrt{n}$, крім нього.

Всі числа, що залишилися невикресленими, є простими.

Приклад 1.9. Знайти всі прості числа від 1 до 30.

Розв'язання

Випишемо натуральні числа від 2 до 30:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~,
11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~,
~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~.

Оскільки $\sqrt{30} \approx 5{,}6$, то будемо працювати з простими числами 2, 3, 5. Беремо просте число 2 і викреслюємо всі парні числа, крім 2; потім викреслюємо всі числа, кратні 3, окрім 3; викреслюємо всі числа, кратні 5, крім 5. Всі числа, що залишаються, є простими: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

1.6. Основна теорема арифметики

Теорема 1.6. *Довільне, відмінне від одиниці натуральне число є або простим або його можна подати і до того ж єдиним способом у вигляді добутку простих множників з точністю до порядку слідування співмножників.*

Доведення. *Існування.* Нехай $n \in N$, $n \neq 1$.

Якщо n – просте число, то твердження теореми очевидне.

Нехай n – число складене. Позначимо через p_1 його найменший простий дільник. Тоді $n = p_1 \cdot n_1, (n_1 < n)$.

Якщо n_1 – просте, то остання рівність і є розклад. В противному випадку позначимо p_2 – його найменший простий дільник, тоді

$$n_1 = p_2 < n_2, \text{ де } n_2 < n_1 \text{ і } n = p_1 p_2 \cdot n_2.$$

Продовжуючи процес далі, одержимо спадну і обмежену знизу послідовність натуральних чисел: $n > n_1 > n_2 > \cdots \geq 1$. Оскільки, усі такі послідовності є скінченими, через декілька кроків одержимо розклад:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k. \qquad \textbf{(1.1)}$$

Єдиність. Припустимо, що разом з вказаним представленням існує інше представлення числа n у добуток простих чисел:

$$n = q_1 \cdot q_2 \cdot \ldots \cdot q_s .$$

Покажимо спочатку, що $k = s$. Для цього прирівняємо праві частини рівностей:

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

Оскільки ліва частина рівності ділиться на p_1, то і права теж має ділитися на p_1. За властивістю 4 простих чисел принаймні одне з чисел q_i ділиться на p_1. Нехай, наприклад, $q_1 \vdots p_1$. За властивостями простих чисел $q_1 = p_1$. Скоротимо останню рівність на p_1:

$$p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_s.$$

Нехай $k < s$. Тоді, використовуючи наведене міркування k разів, та скорочуючи останню рівність на $p_i,\ i = 1 \div k$, одержимо

$$q_{k+1} \cdot \ldots \cdot q_s = 1,$$

що неможливо.

Отже, припущення неправильне. Аналогічно, неважко довести, що неможливим є випадок $k < s$ і тому $k = s$.

З доведення випливає, що при відповідній перенумерації $p_1 = q_1,\ p_2 = q_2, \ldots, p_k = q_k$, тобто, отриманий розклад єдиний. Теорему доведено.

Зберемо в рівності (1.1) однакові прості множники у степені. Тоді такий добуток можна подати у вигляді:

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k} \qquad \textbf{(1.2)}$$

де p_i – прості числа, $p_i \neq p_j$ і $i \neq j$, $m_i \in N$. Представлення (1.2) називається ***канонічним розкладом числа n.***

Наслідок. *Якщо* $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$ *– канонічний розклад n, то будь-який дільник цього числа можна подати у вигляді:*

$$d = p_1^{l_1} \cdot p_2^{l_1} \cdot \ldots \cdot p_k^{l_k}, \text{ де } m_i \geq l_i \geq 0.$$

Наслідок. *Якщо* $n_1 = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$ *і* $n_2 = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_k^{l_k}$ *де* $m_i \geq 0,\ l_i \geq 0$, *то*

$$(n_1, n_2) = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}, \text{ де } s_i = min\{m_i, l_i\}, 1 \leq i \leq k;$$

$$[n_1, n_2] = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_k^{t_k}, \text{ де } t_i = max\{m_i, l_i\}, 1 \leq i \leq k.$$

Тобто, щоб знайти НСД двох (або кількох) чисел, треба з їх канонічних представлень виписати добуток спільних простих множників у найменших степенях. Відповідно, для знаходження НСК двох або кількох чисел, слід виписати усі прості множники у найбільших степенях.

Приклад 1.10. Знайти НСД чисел 1920, 985, 450, користуючись канонічним розкладом числа. Знайти їх НСК.

Розв'язання

Знайдемо канонічний розклад кожного з чисел:

$$1920 = 2^7 \cdot 3 \cdot 5,\ 985 = 5 \cdot 197,\ 450 = 2 \cdot 3^2 \cdot 5^2.$$

За наслідком 1.2 маємо:

$$(1920,985,450) = 5,\ [1920,985,450] = 2^7 \cdot 3^2 \cdot 5 \cdot 197.$$

1.7. Розподіл простих чисел в натуральному ряді

Існує загальна тенденція до зменшення кількості простих чисел, які входять у відрізок $[a, a+h]$ довжини h із збільшенням a при заданому h. Але незважаючи на неї, можна вказати відрізки однієї й тієї ж самої довжини з порівняного малою і порівняно великою кількістю простих чисел. Взагалі, існують як завгодно довгі відрізки натурального ряду, що зовсім не містять простих чисел. Зокрема,

відрізок довжини n, що не містить жодного простого числа може бути наступним:

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n,\ \ (n+1)!+(n+1).$$

У той же час, для довільного натурального n інтервал $[n, 2n]$ містить хоча б одне просте число. Більш того, існують такі прості числа (3 і 5, 5 і 7, 11 і 13, 17 і 19 і т.д.), різниця між якими дорівнює 2. Їх називають *простими числами-близнюками*. Пари простих чисел-близнюків зустрічаються й серед досить великих чисел, але питання про нескінченність множини таких пар й досі залишається відкритим.

Функцію, що визначає кількість чисел, які не перевищують дійсного числа $x > 1$, позначають $\pi(x)$. Відомо, що для достатньо великих x має місце наближена рівність $\pi(x) \approx \frac{x}{\ln x}$

Теорема 1.7 (*нерівність Чебишова*). *Для всіх дійсних* $x \geq 2$ *можна вказати такі дві додатні сталі* a *і* b $(a < b)$, *що*

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}.$$

Було встановлено, що $a \approx 0{,}92129$ і $b \approx 1{,}10555$.

Окрім того, існує й інше наближення $\pi(x)$ за допомогою так званого *інтегрального логарифма*

$$\pi(x) \approx Li(x) = \int_2^x \frac{dx}{\ln x},$$

яке було встановлено Гауссом.

Теорема 1.8. (*Діріхле*). *Будь-яка арифметична прогресія, перший член і різниця якої – взаємно прості натуральні числа, містить нескінчену кількість простих чисел.*

Зокрема, нескінченну кількість простих чисел містить прогресія із загальним членом $3 + 4t,\ t \in N$.

1.8. Числові функції. Ціла і дробова частини числа.

Означення 1.10. *Функція, визначена на множині натуральних чисел (або її підмножинах), називається* ***числовою***.

Приклад 1.11. Числовими є наступні функції:

$y = sin\, x$, $y = [x]$, $y = \pi(x)$ (кількість простих чисел, що не перевищують x), $x \in \mathbb{R}$; $y=n^k$, $y = n!$, $y = \frac{1}{n}, n \in N$.

Ціла та дробова частини числа

Означення 1.11. ***Цілою частиною дійсного числа*** x *називається найбільше ціле число, що не перевищує його.*

Позначення: $y=[x]$

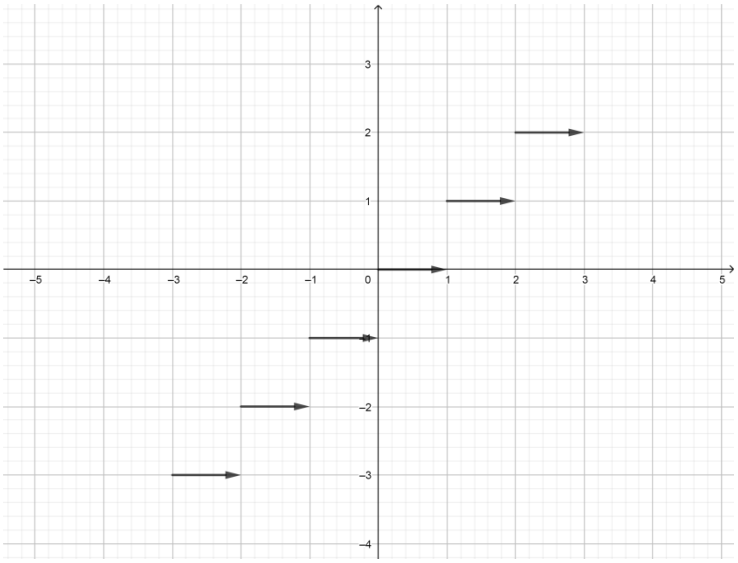


Рис. 1. Графік функції $y=[x]$

Властивості цілої частини числа

1. $\forall m \in Z\ [m] = m$

2. $\forall a \in R, m \in N\ [a + m] = [a] + m,$

3. $\forall x \in R\ [x] \leq x < [x] + 1$

4. $\forall x, y \in R\ [x] = [y] \Rightarrow -1 < x - y < 1$

5. $\forall x, y \in R\ [x + y] \geq [x] + [y]$

6. Кількість натуральних чисел, що не перевищують даного додатного цілого числа a і діляться націло на n, дорівнює $\left[\frac{a}{n}\right]$.

7. Показник степеня α, з яким просте число p входить в канонічний розклад числа $n!$ дорівнює

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right], \text{ де } n \geq p^k \text{ і } n \leq p^{k+1}$$

▻ Розглянемо число $n! = 1 \cdot 2 \cdot 3 \ldots \cdot n$. В цьому добутку на p буде ділитися $\left[\frac{n}{p}\right]$ чисел (за властивістю 6). При цьому деякі з них ділитимуться на p^2, їх кількість дорівнює $\left[\frac{n}{p^2}\right]$, на p^3 діляться $\left[\frac{n}{p^3}\right]$ чисел і т.д. Тому показник α дорівнює кількості чисел від 1 до n, що діляться на $p, p^2, p^3, \ldots$, що і доводить дану властивість.◅

Приклад 1.12. Знайти показник степеня, з яким просте число 7 входить до канонічного розкладу числа $2021!$

Розв'язання

$$k = \left[\frac{2021}{7}\right] + \left[\frac{2021}{7^2}\right] + \left[\frac{2021}{7^3}\right] = 288 + 41 + 5 = 333.$$

Означення 1.12. ***Дробовою частиною*** (*мантисою*) ***числа*** x називають різницю між числом та його цілою частиною:

$$\{x\} = x - [x].$$

Приклад 1.13. $\{2\} = 0$, $\{2{,}7\} = 0{,}7$, $\{-3{,}9\} = 0{,}1$, $\left\{-4\frac{5}{9}\right\} = \frac{4}{9}$.

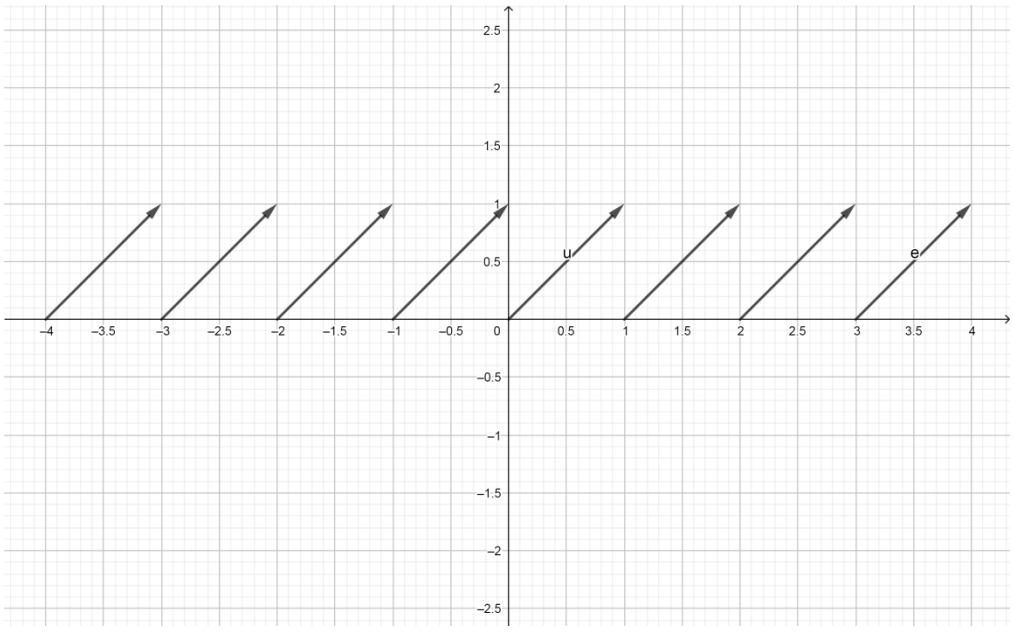


Рис. 2. Графік функції $y=\{x\}$

Властивості дробової частини числа

1. $\forall x \in R \;\; 0 \leq \{x\} < 1.$

2. $\forall m \in Z \;\; \{m\} = 0,$

3. $\forall x \in R [x] = \{x\} \Leftrightarrow x = 0$

4. $\forall x \in R \; \forall m \in Z: \{x + m\} = \{x\}.$

5. $\forall x, y \in R \;\; \{x + y\} = \{x\} + \{y\}$, якщо $\{x\} + \{y\} < 1$
$\{x + y\} = \{x\} + \{y\} - 1$, якщо $\{x\} + \{y\} \geq 1.$

Приклад 1.14. Побудувати графік функції $y = [x] \cdot x.$

Розв'язання

Побудуємо графік, враховуючи проміжки «сталості» цілої частини:

x	$[-3; -2)$	$[-2; -1)$	$[-1; 0)$	$[0; 1)$	$[1; 2)$	$[2; 3)$
y	$-3x$	$-2x$	$-x$	0	x	$2x$

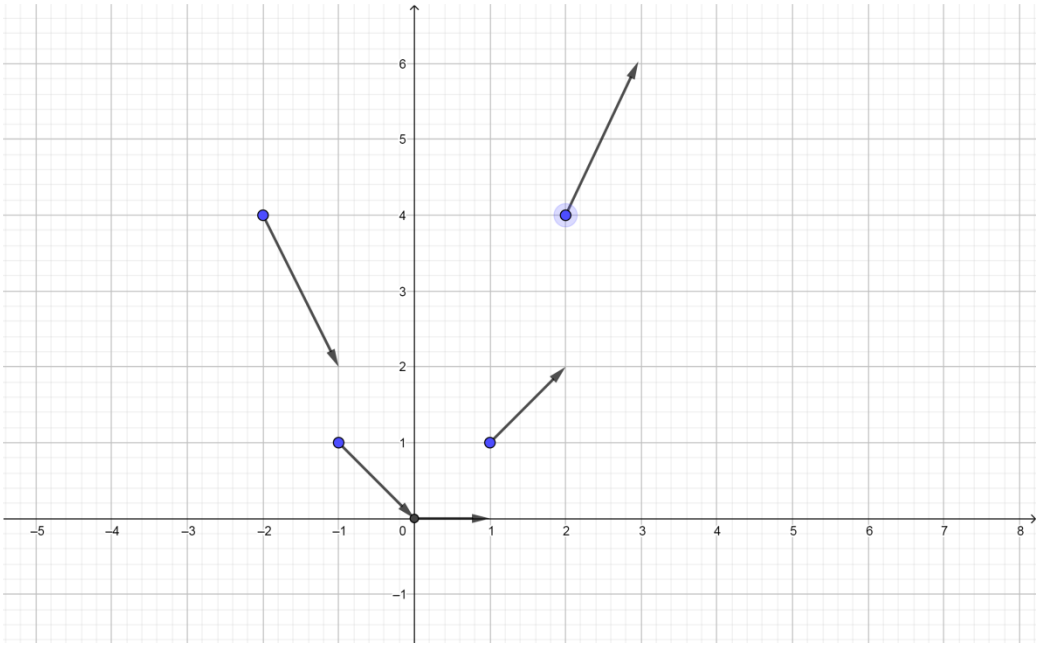


Рис. 3. Графік функції $y=[x]x$

Приклад 1.15. Розв'язати рівняння:

1) $\left[\frac{x-3}{2}\right] = \frac{2x-1}{3}$ 2) $[x - 2] = \left[\frac{x+1}{2}\right].$

Розв'язання

1) Оскільки $\left[\frac{x-3}{2}\right] \in Z$, то $\frac{2x-1}{3} \in Z$. Нехай $\frac{2x-1}{3} = t$, тоді $t \in Z$,

$$2x - 1 = 3t \text{ і } x = \frac{3t-1}{2}.$$

Маємо:

$$\left[\frac{x-3}{2}\right] = \left[\frac{\frac{3t+1}{2}-3}{2}\right] = \left[\frac{3t+1-6}{4}\right] = \left[\frac{3t-5}{4}\right],$$

звідки $\left[\frac{3t-5}{4}\right] = t$. За означенням цілої частини $t \leq \frac{3t-5}{4} < t + 1$, тому

$$4t \leq 3t - 5 < 4t + 4,$$

$$4t + 5 \leq 3t < 4t + 9$$

$$\begin{cases} 4t + 5 \leq 3t \\ 4t + 9 > 3t \end{cases}, \quad \begin{cases} t \leq -5 \\ t > -9 \end{cases}, \quad t \in (-9,-5].$$

Отже, $t \in \{-8,-7,-6,-5\}$. Оскільки $x = \frac{3t-1}{2}$, то $x \in \{-12{,}5; -11, -9{,}5; -8\}$.

Відповідь: $x \in \{-12{,}5; -11,-9{,}5;-8\}$

2) $[x - 2] = \left[\frac{x+1}{2}\right]$.

Нехай $[x - 2] = k \in Z$, тоді $\left[\frac{x+1}{2}\right] = k \in Z$. Отже,

$$\begin{cases} k \leq x - 2 < k + 1 \\ k \leq \frac{x+1}{2} < k + 1 \end{cases}, \begin{cases} k + 2 \leq x < k + 3 \\ 2k - 1 \leq x < 2k + 1 \end{cases}$$

$$\begin{cases} k + 2 < 2k + 1 \\ 2k - 1 < k + 3 \end{cases} \begin{cases} k > 1 \\ k < 4 \end{cases}.$$

Отже, $k \in (1; 4)$, де $k \in Z$, і тому $k \in \{2; 3\}$.

При $k = 2$ маємо $\begin{cases} 2 \leq x - 2 < 3 \\ 2 \leq \frac{x+1}{2} < 3 \end{cases}, \begin{cases} 4 \leq x < 5 \\ 4 \leq x < 5 \end{cases}$, тобто, $x \in [4; 5)$.

Відповідно, при $k = 3$: $\begin{cases} 5 \leq x < 6 \\ 5 \leq x < 7 \end{cases}$, тобто, $x \in [5; 6)$.

Відповідь: $x \in [4; 5) \cup [5; 6)$.

1.9. Мультиплікативні функції. Властивості. Сума й кількість дільників числа. Функція Ейлера

Означення 1.13. *Числова функція* $f(n)$ *називається* ***мультиплікативною,*** *якщо:*

1. $f(n) \not\equiv 0$

2. $\forall m,n \in N\ (m,n) = 1 \Longrightarrow f(nm) = f(n)f(m)$.

Приклад 1.16.

1. Функція $f(n) = n!$ – не мультиплікативна, бо для взаємно простих чисел $n = 2$ та $m = 3$ умова 2 означення не виконується:

$$f(nm) = (2\cdot 3)! \neq 2!\,3! = f(n)f(m).$$

2. Функція $f(n) = n^k$, де k – фіксоване натуральне число, – мультиплікативна, оскільки

$$\forall m,n \in N(m,n) = 1\colon f(mn) = (mn)^k = m^k n^k = f(m)f(n).$$

Властивості мультиплікативних функцій

1. Якщо $f(n)$ *– мультиплікативна, то* $f(1) = 1$.

▷ За пунктом 1 означення існує таке n_0, що $f(n_0) \neq 0$. Тоді за означенням мультиплікативної функції $f(n_0) = f(1 \cdot n_0) = f(1)f(n_0)$ (бо 1 і n_0 взаємно прості). Отже,

$$f(n_0)f(1) = f(n_0) \text{ і тому } f(1) = 1. \triangleleft$$

2. *Добуток двох мультиплікативних функції є мультиплікативною функцією.*

▷ Позначимо $f(n) = f_1(n) \cdot f_2(n)$ і доведемо, що $f(n)$ також мультиплікативна. Перевіримо означення:

1) За властивістю 1 маємо: $f_1(1) = f_2(1) = 1$, тому

$$f(1) = f_1(1)f_2(1) \text{ і } f(n) \not\equiv 0$$

2) Нехай $(m,n) = 1$. Тоді

$$f(mn) = f_1(mn) \cdot f_2(mn) = f_1(m) \cdot f_1(n) \cdot f_2(m) \cdot f_2(n)$$
$$= \underbrace{f_1(m)f_2(m)}_{f(m)} \cdot \underbrace{f_1(n)f_2(n)}_{f(n)} = f(m) \cdot f(n). \triangleleft$$

3. *Якщо* $f(n)-$ *мультиплікативна функція і* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *– канонічний розклад числа* n*, то сума значень даної функції від усіх дільників* d числа n *дорівнює*:

$$\sum_{d|n} f(d) = (1 + f(p_1) + f(p_1^2) + \cdots . + f(p_1^{\alpha_1})) \cdot (1 + f(p_2) + f(p_2^2) + \cdots + (f(p_2^{\alpha_2})) \ldots . (1 + f(p_k) + \cdots + f(p_k^{\alpha_k})) \quad \textbf{(1.3)}$$

▻ Після розкриття дужок у правій частині одержимо добутки виду:

$$f(p_1^{\beta 1}) \cdot f(p_2^{\beta 2}) \cdot \ldots \cdot f(p_k^{\beta k}),\ 0 \le \beta_i \le \alpha_i \quad \textbf{(1.4)}$$

Враховуючи, що функція $f(n)$ мультиплікативна і $(p_i^{\beta i}, p_j^{\beta j}) = 1$ при $i \neq j$, вираз (1.4) можна записати у вигляді $f(p_1^{\beta 1} \cdot p_2^{\beta_2} \ldots . \cdot p_k^{\beta_k})$.

Оскільки $p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots . \cdot p_k^{\beta k}$ – дільник числа n і $0 \le \beta_i \le \alpha_i$, то в правій частині стоятиме сума чисел виду $f(d)$, де $d-$ довільний дільник n, що й доводить властивість. ◅

Підставимо в формулу (1.3) $f(n) = n^m$. Одержимо:

$$\sum_{d|n} d^m = (1 + p_1^m + p_1^{2m} + \ldots + p_1^{\alpha_1 m}) \ldots (1 + p_k^m + p_k^{2m} + \ldots + p_k^{m\alpha_k}) \quad \textbf{(1.5)}$$

При $m = 1$ будемо мати:

$$\sum_{d|n} d = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdot \ldots \cdot (1 + p_k + p_k^{\alpha} + \ldots + p_k^{\alpha_k}).$$

Тобто,

$$\sum_{d|n} d = \frac{{p_1}^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{{p_k}^{\alpha_k+1} - 1}{p_k - 1} = S(n)$$

$-$ сума дільників числа n. Остаточно

$$\boxed{S(n) = \frac{{p_1}^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{{p_k}^{\alpha_k+1} - 1}{p_k - 1}}$$

$-$ ***сума дільників числа*** n.

Покладемо в (1.5) $m = 0$:

$$\sum_{d|n} 1 = \underbrace{(1+1+\ldots+1)}_{\alpha_1+1} \cdot \underbrace{(1+1+1+\ldots+1)}_{\alpha_2+1} \cdot \ldots \cdot \underbrace{(1+1+1+\ldots+1)}_{\alpha_k+1}$$

$\sum_{d|n} 1 = \tau(n) -$ ***кількість дільників числа*** n

$$\boxed{\tau(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)}$$

Функція Ейлера

Означення 1.14. *Функція, яка визначає кількість натуральних чисел, що не перевищують даного числа* $n \in N$ *і взаємно прості з ним, називається* ***функцією Ейлера****.*

Позначення: $\varphi(n)$.

Приклад 1.17. $\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6.$

Властивості функції Ейлера

1. *Якщо* p *– просте число, то* $\varphi(p) = p - 1$

▷ Від 1 до p числами, взаємно простими з p будуть числа: 1, 2, 3,..., $p-1$. Отже, $\varphi(p) = p - 1$. ◁

2. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ або $\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{\mathrm{p}}\right)$

▷ Випишемо числа від 1 до p^α, компонуючи їх у групи по p чисел у кожній:

$$1,2,3,\ldots,p$$
$$(p-1)(p+2)\ldots(p+p)$$
$$(2p+1)(2p+2)\ldots 3p$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$(p^\alpha - p + 1)(p^\alpha - p + 2),\ldots,p^\alpha$$

Зрозуміло, що кількість таких груп дорівнює $\frac{p^\alpha}{p} = p^{\alpha-1}$. У кожній групі лише останнє число буде ділитися на p, тому за властивістю подільності усі інші числа у кожній групі будуть взаємно прості з p, а відтак і з p^α. Їх кількість $(p-1)$ штук в групі, отже

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1). \text{ ◁}$$

3. *Функція Ейлера є числовою мультиплікативною, тобто*

$$\forall m,n \in N\colon\ (m,n)=1,\ \varphi(mn)=\varphi(m)\varphi(n)$$

4. *Якщо* $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ *– канонічний розклад числа* n*, то*

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)$$

▻ Застосуємо попередню властивість:

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

$$=p_1^{\alpha_1}\left(1-\tfrac{1}{p_1}\right)\dots p_k^{\alpha_1}\left(1-\tfrac{1}{p_k}\right)=n\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\dots\left(1-\tfrac{1}{p_n}\right).\ \triangleleft$$

5. $\sum_{d|n}\varphi(d)=n.$

Доведення. Оскільки є мультиплікативною, то за формулою (1.3) основної властивості мультиплікативних функцій, маємо:

$$\sum_{d|n}\varphi(n)=\prod_{i=1}^{k}\left(1+\varphi(p_i)+\varphi(p_i^2)+\dots+\varphi(p_i^{\alpha_i})\right)=$$

$$=\prod_{i=1}^{k}\left(1+p_i-1+p_i^2-p_i+\dots+p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=\prod_{i=1}^{k}p_i^{\alpha_i}=n.$$

6. *Значення* $\varphi(n)$ *при* $n>2$ *є числом парним.*

Приклад 1.18. Обчислити значення функцій $s(n)$, $\tau(n)$ та $\varphi(n)$ для $n=324$.

Розв'язання

Якщо $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots\cdot p_k^{\alpha_k}$, то сума натуральних дільників числа n дорівнює

$$s(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\dots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1},$$

кількість натуральних дільників:

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1),$$

кількість натуральних дільників взаємно простих з n, які не перевищують n:

$$\varphi(n)=n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\dots(1-\tfrac{1}{p_k}).$$

Знайдемо канонічний розклад числа 324: $324=2^2\cdot3^4$. Тоді

$$s(324) = \frac{2^{2+1}-1}{2-1} \cdot \frac{3^{4+1}-1}{3-1} = 7 \cdot 121 = 847,$$
$$\tau(324) = (2+1)(4+1) = 15,$$
$$\varphi(324) = 324(1-\frac{1}{2})(1-\frac{1}{3}) = 324 \cdot \frac{2}{3} \cdot \frac{1}{2} = 108.$$

1.10. Системні числа, дії над ними

Спосіб найменування та запису чисел називається ***системою числення*** або ***нумерацією***. У кожній системі числення числа записують за допомогою певних знаків (символів), які називають ***цифрами***.

В непозиційній системі числення кожна цифра завжди позначає одне й те саме число незалежно від її місця (позиції) в записі числа. Прикладами непозиційних систем є римська та старослов'янська нумерації.

В позиційних системах значення кожної цифри визначається не лише самою цифрою, а й позицією, яку вона займає в записі числа.

Нехай g – деяке число фіксоване натуральне число, $g > 1$.

Означення 1.15. *Представлення натурального числа a у вигляді*

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0, \qquad \textbf{(1.6)}$$

де $a_i \in \mathbb{N} \cup \{0\}, a_n \neq 0,\ 0 \leq a_i < g,$ називається ***записом числа a у системі числення з основою g.***

Символи $a_n, a_{n-1}, \dots, a_1, a_0$ називають ***цифрами*** числа a в системі числення з основою g.

Скорочено зображення (1.6) записують у вигляді:

$$a = (\overline{a_n a_{n-1} \dots a_1 a_0})_g.$$

Теорема 1.8. *Кожне натуральне число a можна записати і до того ж єдиним способом у вигляді*

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

де $a_i (i = 0, \dots, n)$ *– деякі невід'ємні цілі числа, менші від g, $a_n \neq 0$.*

Доведення. Доведемо можливість подання a у вигляді (1.6) методом математичної індукції. Нехай $a = 1$. Тоді $a_n = a_0 = 1 < g$, тобто потрібне зображення існує.

Припустимо, що для числа $b < a$ зображення виду (1.6) існує і доведемо, що відповідний запис можливий для числа a.

Розділимо a на g з остачею:

$$a = bg + r, \text{де } 0 \le r < g, \qquad \textbf{(1.7)}$$

причому числа r та b визначаються однозначно за теоремою про ділення з остачею. Оскільки $0 \le r < g$, можемо вважати, що $r = a_0$.

Оскільки $b < a$, то за індуктивним припущенням

$$b = a_n g^{n-1} + a_{n-1} g^{n-2} + \cdots + a_2 g + a_1,$$

причому $0 \le a_i < g$. Підставивши отриманий розклад числа b в (1.7), дістанемо:

$$a = bg + a_0 = g(a_n g^{n-1} + a_{n-1} g^{n-2} + \cdots + a_2 g + a_1) + a_0 =$$
$$= a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0.$$

Однозначність представлення (1.7) випливає з єдиності остачі та неповної частки. Теорему доведено.

Зрозуміло, що для запису натуральних чисел в позиційній системі числення з основою потрібно рівно g цифр:

$$0,1,2,\ldots,(g-1).$$

Найпоширенішою у наш час є десяткова позиційна система числення, основа якої $g = 10$**.** Окрім того, широко використовуються двійкова та 16-вова системи числення.

При виконанні ***арифметичних операцій*** над числами, записаними в g-овій системі числення, користуємося правилами додавання, віднімання, множення «стовпцем», ділення «кутом».

Нехай $a = (a_k a_{k-1} \ldots a_1 a_0)_g$, $b = (b_s b_{s-1} \ldots b_1 b_0)_g$ і $k \ge s$. Тоді

$$a + b = (a_k g^k + \cdots + a_1 g + a_0) + (b_s g^s + \cdots + b_1 g + b_0) =$$
$$= a_k g^k + \cdots + a_{s+1} g^{s+1} + (a_s + b_s) g^s + \cdots +$$
$$+ (a_1 + b_1) g + (a_0 + b_0).$$

При цьому деякі із чисел $a_0 + b_0, a_1 + b_1, \ldots, a_s + b_s$можуть бути більшими або рівними g. Якщо $a_m + b_m \geq g$ $(0 \leq m \leq s)$, то суму цифр в m-му розряді $a_m + b_m = g + r_m$, $0 \leq r_m \leq g$ замінюємо на r_m та переносимо одиницю в наступний розряд.

$$a + b = c_k g^k + c_{k-1} g^{k-1} + \cdots + c_s g^s + \cdots + c_1 g + c_0,$$

$$a + b = (c_k c_{k-1} \ldots c_1 c_0)_g.$$

Приклад 1.19. Скласти таблиці додавання і множення цифр у 8-ковій системі числення. Виконати дії над числами.

Розв'язання

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

$$+\ \begin{array}{r} 23451_8 \\ 15254_8 \\ \hline 40725_8 \end{array}$$

×	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	10	12	14	16
3	3	6	11	14	17	22	25
4	4	10	14	20	24	30	34
5	5	12	17	24	31	36	43
6	6	14	22	30	36	44	52
7	7	17	25	34	43	52	61

$$\begin{array}{r} \times\ 451_8 \\ 54_8 \\ \hline 2244_8 \\ +\ \underline{2715_8} \\ 31414_8 \end{array}$$

Переведення цілих чисел з однієї позиційної системи числення в іншу

1. Щоб число $a = (a_n a_{n-1} \ldots a_1 a_0)_g$, записане в g–овій системі числення, перевести в 10-ву систему числення, треба представити його у вигляді суми

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

та виконати дії за правилами 10-вої системи.

2. Щоб перевести число a, записане в 10-вій системі числення, в g-ову систему, треба послідовно ділити дане число, отриману неповну частку від ділення і наступні неповні частки на g. Цифрами даного числа в g-овій системі числення є отримані остачі від ділення, записані у зворотному порядку.

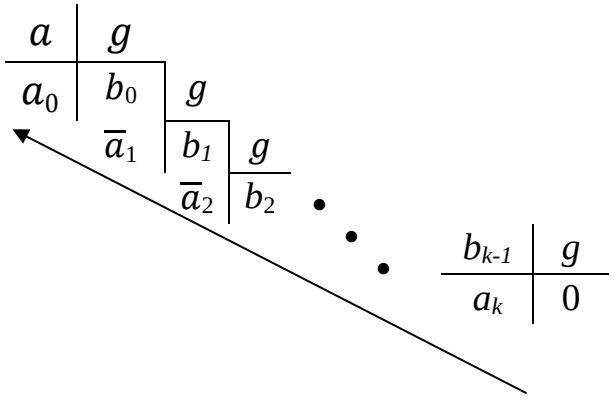
Справді, при першому діленні a на g, отримаємо в остачі a_0:

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0 =$$
$$= g(\underbrace{a_n g^{n-1} + a_{n-1} g^{n-2} + \cdots + a_1}_{b_0}) + a_0 = b_0 g + a_0.$$

Далі будемо ділити на g число b_0:

$$b_0 = a_n g^{n-1} + a_{n-1} g^{n-2} + \cdots + a_1 =$$
$$= g(\underbrace{a_n g^{n-2} + a_{n-1} g^{n-3} + \cdots + a_2}_{b_1}) + a_1 = b_1 g + a_1.$$

Продовжуючи далі, ділимо b_1 на g і т.д. до тих пір, поки відповідна неповна частка не буде рівна нулю.



3. Щоб число a, записане в g_1-овій системі числення, записати в g_2-овій системі, треба перейти спочатку від запису числа в g_1-вій системі до запису в десятковій системі, а вже потім отримане число з десяткової системи перевести в g_2-ову.

$$a_{g_1} \rightarrow x_{10} \rightarrow y_{g_2}.$$

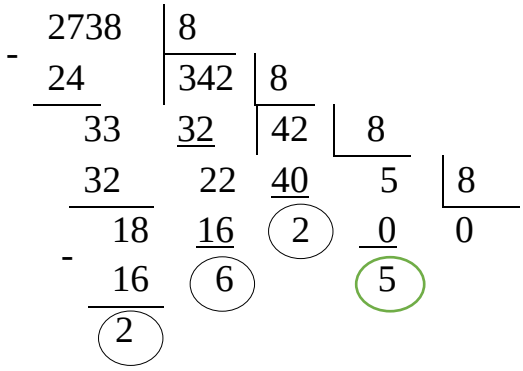
Приклад 1.20. Записати число 1736_8 у десятковій системі числення.

Розв'язання

$$1736_8 = 6 + 3 \cdot 8 + 7 \cdot 8^2 + 1 \cdot 8^3 = 990_{10}.$$

Приклад 1.21. Записати число 2738_{10} у вісімковій системі числення.

Розв'язання



Отже, $2738_{10}=5268_{8}$.

2. ТЕОРІЯ КОНГРУЕНЦІЙ У КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

2.1. Числові конгруенції в кільці цілих чисел

Означення 2.1. *Цілі числа a і b називають конгруентними по модулю $m \in N$, якщо їх різниця ділиться на m,* тобто $(a-b) \vdots m$.

Позначення: $a \equiv b(mod\ \ m)$.

Приклад 2.1. 1) $47 \equiv 22(mod\ 5)$, оскільки $(47-22) \vdots 5$

2) $5 \not\equiv 28(mod\ 3)$, оскільки $(5-28) \ddot{\vdots} 3$.

Теорема 2.1. *$\forall a, b \in Z, m \in N$ наступні умови еквівалентні:*

1) *числа a і b дають однакові остачі при діленні на m, тобто*

$$a = mq_1 + r;\ \ b = mq_2 + r, \quad 0 \le r < m.$$

2) $(a-b) \vdots m$

3) *a відрізняється від b на ціле кратне m:* $a = mq + b, q \in Z$.

Доведення. Доведемо, що з першої умови слідує друга, з другої – третя, а з третьої – перша.

1 ⇒ 2. Нехай виконується умова 1):

$$\begin{array}{l} a = mq_1 + r \\ \underline{b = mq_2 + r} \end{array}$$

Тоді $a - b = m(\underbrace{q_1 - q_2}_{q \in Z}) \Rightarrow (a-b) \vdots m.$

2 ⇒ 3. Нехай $(a-b) \vdots m$, тоді за означенням подільності

$$a - b = mq,\ \ q \in Z, \text{звідки } a = mq + b$$

3 ⇒ 1. Припустимо, що умова $a = mq + b, q \in Z$ виконується, але числа a і b дають різні остачі від ділення на m, тобто

$$a = mq_1 + r_1;\ \ b = mq_2 + r_2, \quad r_1 \ne r_2, \quad 0 \le r < m.$$

Віднімемо почленно від першої рівності другу. Отримаємо:

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

Оскільки $r_1 - r_2 < m$ і $r_1 \ne r_2$, то $(r_1 - r_2) \ddot{\vdots} m$. Тоді $(a-b) \ddot{\vdots} m$, що суперечить умові 3. Отже, припущення неправильне і $r_1 = r_2$.

Теорему доведено.

Таким чином, умови 1) – 3) теореми з різних сторін характеризують конгруентність чисел a і b по модулю m і кожна з цих умов може бути покладена в означення конгруентності цих чисел по вказаному модулю.

Властивості числових конгруенцій

1. $\forall a \in Z\ a \equiv a(mod\, m)$ (відношення конгруентності *рефлексивне*;

2. $\forall a, b \in Z\ a \equiv b(mod\, m) \Rightarrow b \equiv a(mod\ \ m)$ (відношення конгруентності *симетричне*);

3. $\forall a, b, c \in Z\ a \equiv b(mod\, m);\ \ b \equiv c(mod\ \ m) \Rightarrow a \equiv c(mod\, m)$ (відношення конгруентності *транзитивне*).

◅ Оскільки $a \equiv b(mod\, m)$ і $b \equiv c(mod\ \ m)$, то $a = b + mt$ і $b = c + mq$, де $t, q \in Z$.

Отже,

$a = c + mq + mt$ або $a = c + m\underbrace{(q + t)}_{q' \in Z} \Rightarrow a \equiv c(mod\, m)$. ◅

Отже, відношення конгруентності є *відношенням еквіваленції*, тому множина Z розбивається на класи еквівалентності, які попарно не перетинаються і в сукупності вичерпують Z. В кожному класі містяться числа конгруентні між собою по модулю m.

4. *Кожне число конгруентне зі своєю остачею при діленні на* m:

якщо $a = mq + r, q \in Z$, то $a \equiv r(mod\ \ m)$.

◅ Нехай $a = mq + r$, де $q \in Z, 0 \leq r < m$. Тоді $a - r = mq$, і $a \equiv r(mod\ \ m)$ за означенням. ◅

5. *Якщо конгруенція має місце по модулю* m*, то вона має місце і по модулю, що є дільником числа* m.

$$a \equiv b(mod\, m) \Rightarrow a \equiv b(mod\ \ d);\ \ d|m,\ d \in N$$

◅ З умови випливає, що $(a - b) \vdots m$, оскільки $d|m \Rightarrow m \vdots d$. В силу транзитивності подільності $(a - b) \vdots d \Rightarrow a \equiv b(mod\, d)$. ◅

6. *Якщо конгруенція має місце по модулям* $m_1, m_2, \ldots, m_k$, *то вона має місце і по модулю, що дорівнює НСК цих чисел.*

$$\left.\begin{array}{l} a \equiv b(\mathrm{mod}\, m_1) \\ a \equiv b(\mathrm{mod}\ m_2) \\ \ldots\ldots \\ a \equiv b(\mathrm{mod}\, m_k) \end{array}\right| \Rightarrow a \equiv b\left(\mathrm{mod}\,\left[m_1, m_2, \ldots, m_k\right]\right)$$

◅ Нехай

$$\left.\begin{array}{l} a \equiv b(\mathrm{mod}\ m_1) \\ a \equiv b(\mathrm{mod}\ m_2) \\ \ldots\ldots \\ a \equiv b(\mathrm{mod}\ m_k) \end{array}\right| \qquad \textbf{(2.1)}$$

і $m = [m_1, m_2, \ldots, m_k]$ – найменше спільне кратне чисел $m_1, m_2, \ldots, m_k$.

З системи (2.1) випливає, що різниця чисел $a - b$ ділиться на числа $m_1, m_2, \ldots, m_k$. Але в цьому випадку вона повинна ділитися і на їх НСК m. Отже, $a - b = mt$, тобто $a \equiv b(mod\ \ m)$, що й треба було довести. ◅

7. *Дві конгруенції за одним і тим же модулем можна почленно додавати, віднімати та множити*

$$a \equiv b(mod\, m)\ \wedge c \equiv d(mod\, m) \Rightarrow$$

$$a \pm c \equiv b \pm d(mod\, m)\ \wedge\ a \cdot c \equiv b \cdot d(mod\, m)$$

◅ З умови випливає, що $a = b + mt$ і $c = d + mq, t, q \in Z$. Додамо ці рівності почленно: $a + c = b + d + m\underbrace{(t + q)}_{q' \in Z}$, звідки

$$a + b \equiv b + d(mod\, m)$$

Аналогічно, перемножимо рівності:

$$a \cdot c = b \cdot d + bmq + dmt + m^2 tq = bd + mk, k \in Z \Leftrightarrow$$

$$ac \equiv bd(mod\, m). \blacktriangleleft$$

8. *До лівої і правої частин конгруенції можна додати одне й те саме ціле число*

$$a \equiv b(mod\, m\ ) \Rightarrow a + c \equiv b + c(mod\, m).$$

◅ Справді, оскільки $a = b + mt,$ то $a + c = b + c + mt.$ Отже,

$$a + c = b(mod\, m).$$ ◅

9. *До будь-якої частини конгруенції можна додати (відняти) ціле число, кратне модулю, тобто*

$$a \equiv b(mod\, m) \Rightarrow a + mq \equiv b(mod\, m) \text{ і } a \equiv b + mq(mod\, m)$$

◅ За умовою $a \equiv b(mod\, m)$. Окрім того, $mq \equiv 0(mod\, m)$. Додамо ці конгруенції почленно: $a + mq \equiv b(mod\, m)$. Аналогічно, з конгруенцій $a \equiv b(mod\, m)$ і $0 \equiv mq(mod\, m)$ випливає, що

$$a \equiv b + mq(mod\, m).$$ ◅

10. *З однієї частини конгруенції в іншу можна перенести ціле число, змінивши його знак на протилежний*:

$$a + c \equiv b(mod\, m) \Leftrightarrow a \equiv b - c(mod\, m)$$

◅ Оскільки, $a + c \equiv b(mod\, m)$, то $a + c = b + mq \Rightarrow a = b - c + mq \Rightarrow a \equiv b - c(mod\, m)$. Навпаки аналогічно. ◅

11.*Обидві частини конгруенції можна піднести до одного і того ж натурального степеня:*

$$a \equiv b(mod\, m) \Rightarrow \mathrm{a}^n \equiv b^n(mod\, m), n \in N.$$

12. *Обидві частини конгруенції можна множити на одне й те саме ціле число*

$$a \equiv b(mod\, m),\ c \in Z \Rightarrow ac \equiv bc(mod\, m).$$

◅ Справедливість твердження випливає з властивості 7 та рефлексивності відношення конгруентності:

$$a \equiv b(mod\, m) \wedge c \equiv c(mod\, m) \Rightarrow ac \equiv bc(mod\, m).$$

13. *Обидві частини конгруенції і модуль можна помножити на одне й те саме натуральне число*:

$$a \equiv b(mod\, m),\ n \in Z \Rightarrow an \equiv bn(mod\, mn)$$

◅ Справді, з умови $a \equiv b(mod\, m)$ випливає, що $a = b + mq$. Тоді $an = bn + (m \cdot n)q$ і $an \equiv bn(mod\, mn)$. ◅

14. *Обидві частини конгруенції можна скоротити на їх спільний дільник, якщо він взаємно простий з модулем.*

◅ Позначимо $d = (a, b)$. Тоді $a = a_1 d, b = b_1 d$. Оскільки $a \equiv b(mod\, m)$, то $a = b + mt$. Тоді $a_1 d = b_1 d + mt$ і $(a_1 - b_1)d = mt$. Права частина останньої рівності ділиться на m, тому на m ділиться і ліва частина. Оскільки $(m, d) = 1$, то $(a_1 - b_1) \vdots m$, звідки $a_1 - b_1 = ms$ і $a_1 = b_1 + ms$. Отже, $a_1 \equiv b_1(mod\, m)$, що й треба було довести. ◅

15. *Обидві частини конгруенції і модуль можна скоротити на їх натуральний спільний дільник:*

$$ak \equiv bk(mod\, mk), k \in N \Rightarrow a \equiv b(mod\, m)$$

◅ Оскільки, $ak \equiv bk(mod\, m\, k), k \in N$, то $ak = bk + (mk)t \Rightarrow a = b + mt$ і $a \equiv b(mod\, m)$. ◅

16. *Якщо одна з частин конгруенції і модуль діляться на деяке число, то й інша частина конгруенції ділиться на це число*

$$a \equiv b(mod\, m) \wedge a \vdots k \wedge m \vdots k \Rightarrow b \vdots k$$

◅ Оскільки, $a = b + mt$, то $b = \underset{\vdots k}{a} - \underset{\vdots k}{mt}$. Оскільки права частина ділиться на k, то і $b \vdots k$. ◅

17. *Якщо* $a \equiv b(mod\, m) \Rightarrow$ НСД$(a, m) =$ НСД(b, m).

◅ З умови випливає, що $a = b + mt$, і оскільки a ділиться на будь-який спільний дільник d чисел b і m, то d є спільним дільником чисел a і m. Навпаки, число b ділиться на будь-який спільний дільник d чисел a і m, тому d є спільним дільником чисел b і m. Таким чином, спільні дільники чисел a і m є ті ж самі, що й чисел b і m. Зокрема, повинні збігатися і найбільші спільні дільники, тобто $(a, m) = (b, m)$. ◅

18. *Нехай задано многочлен*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \forall a_i \in Z, a_n \neq 0$$

Якщо $a \equiv b(mod\, m)$, *то* $f(a) \equiv f(b)(mod\, m)$.

◅ З умови та властивостей 1 та 7 випливає, що

$$a_0 \equiv a_0 (mod\, m)$$
$$a_1 a \equiv a_1 b (mod\, m)$$
$$a_2 a^2 \equiv a_2 b^2 (mod\, m)$$
$$\ldots\ldots\ldots$$
$$a_{n-1} a^{n-1} \equiv a_{n-1} b^{n-1} (mod\, m)$$
$$a_n a^n \equiv a_n b^n (mod\, m)$$

Додаючи усі конгруенції одержимо

$$a_0 + a_1 a + \cdots + a_{n-1} a^{n-1} + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + .. + a_n b^n (mod\, m)$$

Тобто,

$$f(a) \equiv f(b) (mod\, m). \lhd$$

Властивості конгруенцій дозволяють досить швидко доводити подільність чисел, знаходити остачі від ділення та встановити ознаки подільності.

Приклад 2.2. Довести, що $(7^{2n} + 15) \vdots 8, \forall n \in N$.

Розв'язання

Оскільки $7 \equiv -1 (mod\, 8)$, то $7^2 \equiv (-1)^2 \equiv 1 (mod\, 8)$. Піднесемо останню конгруенцію до степеня n:

$$7^{2n} \equiv 1^{2n} \equiv 1 (mod\, 8).$$

Знайдемо тепер, з яким числом по модулю 8 конгруентне 15:

$$15 \equiv -1 (mod\, 8).$$

Додаючи почленно отримані конгруентності, одержимо:

$$7^{2n} + 15 \equiv 1 - 1 \equiv 0 (mod\, 8).$$

Оскільки число конгруентне зі своєю остачею при діленні на m, то $(7^{2n} + 15) \vdots 8$.

Застосування конгруенцій до встановлення ознак подільності. Загальна ознака подільності Паскаля

Нехай $a = \overline{a_n a_{n-1} \ldots a_1 a_0}$ – систематичний запис натурального числа a, тобто $a = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10 a_1 + a_0$.

Якщо потрібно встановити ознаку подільності довільного числа a на деяке $m \in N$, слід знайти остачі, що дають числа

$10, 10^2, \ldots, 10^{n-1}, 10^n$ на m (або замінити їх конгруентними по модулю m числами). Наприклад,

$$10 \equiv r_1 (mod\, m)$$
$$10^2 \equiv r_2 (mod\, m)$$
$$\ldots.$$
$$10^n \equiv r_n (mod\, m).$$

Помножимо кожну конгруенцію на $a_1, a_2, \ldots, a_n$ відповідно, та додамо їх почленно. Одержимо:

$$10a_1 + 10a_2^2 + \ldots + 10^n a_n = a_1 r_1 + a_2 r_2 + \ldots + a_n r_n (mod\, m).$$

Звідси

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^n a_n \equiv$$
$$\equiv a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_n r_n (mod\, m)$$

Останнє відношення свідчить про те, що при діленні на m число a дає ту ж саму остачу, що і $a_0 + a_1 r_1 + \ldots + a_n r_n$. Зокрема,

$$a \vdots m \Leftrightarrow a_0 + a_1 r_1 + \ldots + a_n r_n \vdots m.$$

Приклад 2.3. Сформулювати ознаки подільності на 11 та на 7.

Розв'язання

Нехай a – довільне натуральне число

$$a \equiv 10^n a_n + \ldots + 10^2 a_2 + 10a_1 + a_0.$$

Оскільки

$$10 \equiv -1 (mod\, 11)$$
$$10^2 \equiv 1 (mod\, 11)$$
$$10^3 \equiv -1 (mod\, 11)$$
$$\ldots..$$
$$10^n \equiv (-1)^n (mod\, 11),$$

то, помноживши кожну з конгруенцій на $a_1, a_2, \ldots, a_n$ відповідно, та додавши їх почленно, одержимо

$$a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots + 10^n a_n \equiv$$
$$\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n (mod\, 11).$$

Отже, ознака подільності на 11 формулюється наступним чином:

$$a = a_n \ldots a_1 a_0 \vdots 11 \Leftrightarrow (a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n) \vdots 11.$$

Визначимо тепер умови, за яких число ділиться на 7.
Аналогічно, маємо:

$$10 \equiv 3(mod\ 7)$$
$$10^2 \equiv 2(mod\ 7)$$
$$10^3 \equiv -2(mod\ 7)$$
$$10^4 \equiv 4(mod\ 1\ 1)$$
$$10^5 \equiv -2(mod\ 7).$$

Отже,

$$(\ldots a_5 a_4 a_3 a_2 a_0) \vdots 7 \Leftrightarrow (a_0 + 3a_1 + 2a_2 - 2a_3 + 4a_4 - 2a_5 + ..) \vdots 7.$$

2.2. Класи лишків. Повна та зведена системи лишків

Як зазначалося вище, будь-яке ціле число по модулю m конгруентне зі своєю остачею: $a \equiv r(mod\, m)$, де r – остача від ділення на m. Оскільки при діленні на m можливо m різних остач:

$$0,1,2,..,\ (m-1),$$

то цілі числа можна розбити на m класів залежно від того, з якою з цих остач буде конгруентне те чи інше ціле число при діленні на m.

Позначимо ці класи

$$\overline{0} = \{mk | k \in Z\} = \{\ldots, -m, 0, m, 2m, \ldots\}$$
$$\overline{1} = \{mk + 1\} = \{\ldots, -m + 1,\ 1,\ m + 1,\ 2m + 1, ..\}$$
$$\overline{2} = \{mk + 2\} = \{\ldots, -m + 2,\ 2,\ m + 2,\ 2m + 2, \ldots\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\overline{m-1} = \{mk + m-1\} = \{\ldots, -1,\ m-1,\ 2m-1,\ \ldots\}$$

Вказані класи не перетинаються і вичерпують множину Z. Їх називають ***класами рівноостанніх чисел*** або ***класами лишків*** по модулю m. Зрозуміло, що будь-яке ціле число належить одному і тільки одному класу. Числа одного класу конгруентне між собою по модулю m. Числа різних класів – не конгруентні. Разом з кожним числом a класу лишків $\overline{a}$ належать числа виду $a + mt, t \in Z$, тобто клас має нескінченне число елементів. Всі числа одного класу є рівноправними, тобто кожен клас визначається будь-яким своїм представником.

Довільне $a \in Z$, що належить класу лишків $\overline{a}$ називається ***лишком по модулю*** т.

Означення 2.2. *Система лишків, що містить по одному і тільки одному лишку з кожного класу називається повною системою лишків по модулю* m (ПСЛ_m).

Зрозуміло, що ПСЛ_m містить рівно m елементів.

Приклад 2.4. Знайти ПСЛ_5

$$\overline{0} = \{5k | k \in Z\} = \{\dots, -5, 0, 5, 10, \dots\}$$
$$\overline{1} = \{5k + 1\} = \{\dots, -4,\ 1,\ 6,\ 11, \dots\}$$
$$\overline{2} = \{5k + 2\} = \{\dots, -3,\ 2,\ 7,\ 12, \dots\}$$
$$\overline{3} = \{5k + 3\} = \{\dots, -2,\ 3,\ 8,\ 13, \dots\}$$
$$\overline{4} = \{5k + 4\} = \{\dots, -1,\ 4,\ 9,\ 14 \dots\}$$

$\text{ПСЛ}_5 = \{0,1,2,3,4\}$ або $\text{ПСЛ}_5 = \{-5, -4, 2, 8, 14\}$.

Виділяють наступні ПСЛ_m:

- повну систему найменших невід'ємних лишків по модулю т:
$$\{0,1,2, \dots, m-1\}$$
- повну систему найменших додатних лишків:
$$\{0,1,2, \dots, m-1, m\}$$
- систему лишків, найменших за абсолютною величиною: $\left\{0,1,2, \dots, \frac{m-1}{2}\right\}$, якщо т –непарне; $\left\{0,1,2, \dots, \frac{m}{2}\right\}$, якщо $m -$ парне.

Властивості ПСЛ_m

1. Будь-яка ПСЛ_m містить m елементів.

2. Будь-яка сукупність m штук попарно не конгруентних між собою цілих чисел утворює ПСЛ_m.

⊲Оскільки числа не конгруентні вони належать різних класам лишків. Враховуючи, що їх кількість т у даній сукупності будуть представники усіх класів лишків. ⊲

3. Якщо $\{x_1, x_2, \dots, x_m\} - \text{ПСЛ}_m$ і $(a, m) = 1$, то сукупність

$$\{ax_1 + b, ax_2 + b, \dots, ax_m + b\} \qquad \textbf{(2.2)}$$

$\forall b \in Z$ також утворює ПСЛ_m.

◅ В системі (2.2) міститься m чисел, тому враховуючи попередню властивість достатньо показати, що числа цієї системи попарно не конгруентні.

Припустимо супротивне, нехай, наприклад,

$$ax_i + b \equiv bx_j + b(mod\, m), \quad i \neq j.$$

Тоді $ax_i \equiv ax_j(mod\, m)$. Оскільки $(a, m) = 1$, то останню конгруенцію можна скоротити на a: $x_i \equiv x_j(mod\, m)$, що суперечить умові. Отже, (2.2) – ПСЛ$_m$. ◅

Виберемо у будь-якій ПСЛ$_m$ всі лишки взаємно прості з модулем. Нехай x міститься в ПСЛ$_m$ і $(x, m) = 1$, тоді для довільного $y \in \overline{x},\ y = x + mk$ і тому $(y, m) = (x, m) = 1$. Отже, кожен елемент класу лишків $\overline{x}$ буде взаємно простим з m.

Означення 2.3. *Клас лишків $\overline{x}$ називається взаємно простим з модулем m, якщо $(x, m) = 1$.*

Означення 2.4. *Сукупність попарно не конгруентних між собою цілих чисел по модулю m, взятих з усіх класів лишків, що є взаємно простими з m, називаються* ***зведеною системою лишків*** (ЗСЛ$_m$) *по модулю m.*

Іншими словами, ЗСЛ$_m$ – це сукупність не конгруентних між собою цілих чисел, кожне з яких є взаємно простим з модулем.

Властивості ЗСЛ$_m$

1. Будь-яка ЗСЛ$_m$ містить $\varphi(m)$ елементів.

◅ Справді, кількість класів лишків по модулю m, що є взаємно-простими з m дорівнює кількості натуральних чисел, що не перевищують m і взаємно прості з ним, тобто дорівнює $\varphi(m)$. ◅

2. Будь-яка сукупність цілих чисел, що містить $\varphi(m)$ елементів, які не конгруентні між собою і взаємно прості з модулем утворює ЗСЛ$_m$.

3. Якщо $\{x_1, x_2, \dots x_{\varphi(m)}\} - $ ЗСЛ$_m$ і $a \in Z, \quad (a, m) = 1,$ то сукупність

$$\{ax_1, ax_2, \dots, ax_{\varphi(m)}\} \qquad \textbf{(2.3)}$$

також утворює $ЗСЛ_m$.

◅ Оскільки система (2.3) містить $\varphi(m)$ чисел, достатньо показати, що вони попарно не конгруентні і взаємно прості з m. Припустимо, що для деяких $i \neq j$ $ax_i \equiv ax_j(mod\, m)$. Скоротимо останню конгруенцію на a, де $(a,m) = 1$: $x_i \equiv x_j(mod\, m)$. Маємо протиріччя.

Оскільки за умовою $(x_i, m) = 1$ і $(a,m) = 1$, то $(ax_i, m) = 1$. Отже, (2.3) – $ЗСЛ_m$. ◅

Приклад 2.5. Побудувати яку-небудь повну та зведену системи лишків по модулю 6.

Розв'язання

Оскільки $\varphi(6) = 2$, то у $ЗСЛ_6$ буде два елементи, взаємно прості з 6. Відберемо їх з повної системи лишків по модулю 6:

$$ПСЛ_6 = \{0,1,2,3,4,5\}.$$

Зрозуміло, що взаємно простими з 6 будуть 1 та 5. Отже, $ЗСЛ_6 = \{1,5\}$.

2.3. Теорема Ейлера і мала теорема Ферма

Теорема 2.1. (*Ейлера*). *Якщо* $a \in Z, m \in N$ *і* $(a,m) = 1$, *то*

$$a^{\varphi(m)} \equiv 1(mod\, m).$$

Доведення. Візьмемо зведену систему найменших невід'ємних лишків по модулю т: $\{x_1, x_2, \ldots x_{\phi(m)}\}$ і $(a,m) = 1$. Тоді за властивістю 3 сукупність $\{ax_1, ax_2, \ldots, ax_{\phi(m)}\}$ також утворюватиме $ЗСЛ_т$. Замінимо кожен з цих лишків найменшим невід'ємним:

$$\begin{gathered} ax_1 \equiv x_1'(mod\, m) \\ ax_2 \equiv x_2'(mod\, m) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ ax'_{\varphi(m)} \equiv x'_{\varphi(m)}(mod\, m) \end{gathered} \qquad \textbf{(2.4)}$$

де всі x_i' містяться в межах $0 \leq x_i' < m$, тобто $\{x_1', \ldots, x'_{\varphi(m)}\}$ утворює зведену систему найменших невід'ємних лишків по модулю m.

Помножимо конгруенції з (2.4) почленно

$$a^{\varphi(m)}x_1x_2\dots x_{\varphi(m)} \equiv x_1'x_2'\dots x_{\varphi(m)}'(mod\, m).$$

Враховуючи, що $x_1', x_2', \dots, x_{\varphi(m)}'$ – перестановка чисел $x_1, x_2, \dots, x_{\varphi(m)}$, робимо висновок, що добутки цих чисел рівні. Скорочуючи останню конгруенцію на ці добутки одержимо

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

(скорочення правомірне, бо $(x_i, m) = 1$ і $(x_1x_2\dots x_{\varphi(m)}, m) = 1$). ◅

Наслідком з теореми Ейлера є мала теорема Ферма.

Теорема 2.3(*мала теорема Ферма*). *Якщо p – просте число і $a \in Z$, причому $a \vdots p$, то*

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

Для доведення достатньо згадати, що $\phi(p) = p - 1$.

Наслідок. *Для довільного цілого a простого числа p виконується*

$$(a^p - a) \vdots p.$$

Доведення. Якщо $(a, p) = 1$, то за теоремою Ферма $a^{p-1} \equiv 1(mod\, p)$. Звідси $a^p \equiv a(mod\, p)$ і $(a^p - a) \vdots p$. Нехай $(a, p) \neq 1$, тоді $a \vdots p \Rightarrow (a^p - a) \vdots p$. ◅

Теореми Ейлера і Ферма значно спрощують знаходження остач від ділення на задане число.

Приклад 2.6. Довести, що $(7 \cdot 3^{100} + 4 \cdot 5^{200})$ ділиться на 11.

Розв'язання

Оскільки $(3,11) = 1$, то за теоремою Ферма $3^{11-1} \equiv 1(mod\, 11)$. Отже,

$$3^{100} \equiv 1(mod\, 11)$$
$$\underline{7 \cdot 3^{100} \equiv 7(mod\, 11)}$$

Оскільки $(5,11) = 1$, то

$$5^{10} \equiv 1(mod\, 11)$$
$$5^{200} \equiv 1(mod\, 11)$$
$$\underline{4 \cdot 5^{200} \equiv 4(mod\, 11)}$$

Додаючи почленно підкреслені конгруенції отримаємо:

$$4 \cdot 5^{200} + 7 \cdot 3^{100} \equiv 4 + 7 \equiv 0(mod\ 11)$$

Отже, $(7 \cdot 3^{100} + 4 \cdot 5^{2000}) \vdots 11$.

Приклад 2.7. Знайти дві останні цифри числа 47^{81}.

Розв'язання

Дві останні цифри числа можна знайти як остачу від ділення даного числа на $m = 100$. Оскільки $(47,100) = 1$, то за теоремою Ейлера $47^{\varphi(100)} \equiv 1(mod\ 100)$. Знайдемо $\varphi(100)$:

$\varphi(100) = \varphi(25 \cdot 4) = \varphi(25) \cdot \varphi(4) = 2 \cdot (5^2 - 5) = 40.$

Отже,

$$47^{40} \equiv 1(mod\ 100)$$
$$47^{80} \equiv 1(mod\ 100)$$
$$47^{81} \equiv 47(mod\ 100)$$

Відповідь: 47.

Приклад 2.8. Використовуючи теорему Ейлера, знайти остачу від ділення $6(14^{150} + 341^{291})$ на 45.

Розв'язання

Оскільки $(14,45) = 1$, то $14^{\varphi(45)} \equiv 1(mod\ 45)$, де

$$\varphi(45) = 45 \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 24.$$

Тоді $14^{24} \equiv 1(mod\ 45)$ і $(14^{24})^6 = 14^{144} \equiv 1(mod\ 45)$,

$14^2 = 196 \equiv 16(mod\ 45)$, $14^4 \equiv 16^2 \equiv 256 \equiv 31 \equiv -14(mod\ 45)$,

$$14^6 \equiv (-14) \cdot 16 \equiv -224 \equiv 1(mod\ 45).$$

Отже, $14^{150} \equiv 1(mod\ 45)$.

Аналогічно, оскільки $(341,45) = 1$, то $341^{24} \equiv 1(mod\ 45)$ і $341^{288} \equiv 1(mod\ 45)$. Далі

$$341 = -19(mod\ 45),\ 341^2 \equiv (-19)^2 \equiv 361 \equiv 1(mod\ 45),$$
$$341^3 \equiv -19 \cdot 1(mod\ 45).$$

Отже, $341^{291} \equiv -19(mod\ 45)$. Остаточно,

$$6(14^{150} + 341^{291}) \equiv 6(1 - 19) \equiv -108 \equiv -18 \equiv 27(mod\ 45).$$

Отже, остача від ділення $6(14^{150} + 341^{291})$ на 45 дорівнює 27.

Відповідь: 27.

2.4. Конгруенції першого степеня з одним невідомим

Означення 2.5. Конгруенція виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (mod\, m), \quad \textbf{(2.5)}$$

де $a_i \in Z$ називається ***конгруенцією зі змінною x степеня*** *n.*

Розв'язком конгруенції (2.5) називають довільне ціле значення x_0 змінної x, що задовольняє дану конгруенцію (тобто, перетворює її на правильну числову конгруенцію).

Зрозуміло, що разом зі значенням x_0 конгруенцію (2.5) задовольнятиме й довільний елемент з класу лишків $\overline{x_0}$ по модулю m. Отже, має місце означення.

Означення 2.6. *Розв'язком конгруенції* (2.5) називається клас лишків $\overline{x_0}$ по модулю m, кожен елемент якого задовольняє дану конгруенцію.

З цього випливає, що конгруенція (2.5) за модулем m не може мати більше, ніж m розв'язків.

Дві конгруенції зі змінною називають ***рівносильними,*** якщо їх множини розв'язків за вказаним модулем збігаються.

Наступні перетворення зберігають множину розв'язків конгруенції (2.5) і дозволяють замінити її рівносильною, більш простого виду.

Рівносильні перетворення конгруенцій зі змінною

1) додавання до обох частин конгруенції цілого числа або виразу з цілими коефіцієнтами;

2) додавання до будь-якої частини конгруенції виразу від x з коефіцієнтами, що цілими кратними модуля;

3) перенесення виразів з однієї частини конгруенції в іншу зі зміною знаку на протилежний;

4) множення обох частин конгруенції на ціле число, взаємно просте з модулем;

5) ділення обох частин конгруенції на їх спільний дільник, що є числом, взаємно простим з модулем;

6) множення обох частин конгруенції і модуля на натуральне число;

7) ділення обох частин конгруенції і модуля на їх натуральний спільний дільник.

Означення 2.7. *Лінійною називають конгруенцію виду:*

$$ax \equiv b(mod\, m),\ a, b \in Z, m \in N \qquad \textbf{(2.6)}$$

Теорема 2.4. (*про існування та число розв'язків лінійної конгруенції*) *Нехай задано лінійну конгруенцію*

$$ax \equiv b(mod\, m).$$

Тоді справедливі наступні умови:

1) *якщо* $(a, m) = 1$, *то задана конгруенція має єдиний розв'язок*

$$x_0 = a^{\varphi(m)-1} b(mod\, m);$$

2) *якщо* $(a, m) = d > 1 \wedge b \,\overline{\vdots}\, d$, *то конгруенція розв'язків не має;*

3) *якщо* $(a, m) = d > 1 \wedge b \vdots d$, *то конгруенція має* d *розв'язків:*

$$x \equiv x_0(mod\, m),$$

$$x \equiv x_0 + \frac{m}{d}\ (mod\, m),$$

$$x \equiv x_0 + \frac{2m}{d}\ (mod\, m), \ldots$$

$$x \equiv x_0 + \frac{m(d-1)}{d}\ (mod\, m)$$

де x_0 *– розв'язок конгруенції*

$$\frac{a}{d}x \equiv \frac{b}{d}\left(mod\, \frac{m}{d}\right).$$

Доведення: 1) Оскільки $(a, m) = 1$, то за теоремою Ейлера

$$a^{\varphi(m)} \equiv 1(mod\, m).$$

Домножимо обидві частини конгруенції $ax \equiv b(mod\, m)$ на $a^{\varphi(m)-1}$. Одержимо:

$$aa^{\varphi(m)-1}x \equiv a^{\varphi(m)-1}b(mod\, m),$$

звідки

$$a^{\varphi(m)}x \equiv a^{\varphi(m)-1}b(mod\, m)$$

і $x \equiv a^{\varphi(m)-1}b(mod\, m)$. Отже, розв'язком даної конгруенції є клас лишків $x \equiv a^{\varphi(m)-1}b(mod\, m)$.

Припустимо, що дана конгруенція має інший розв'язок по модулю m: $x \equiv x_1(mod\, m)$ і $x_0 \not\equiv x_1(mod\, m)$. Тоді $ax_0 \equiv b(mod\, m)$ і $ax_1 \equiv b(mod\, m)$ – правильні числові конгруенції. В силу транзитивності відношення конгруентності одержимо

$$ax_0 \equiv ax_1(mod\, m).$$

Враховуючи, що $(a, m) = 1$, скоротимо останню конгруентність на a. Одержимо $x_0 \equiv x_1(mod\, m)$. Суперечність. Отже, розв'язок єдиний.

2) Нехай $(a, m) = d > 1, b \vdots d$. Запишемо конгруенцію (2.6) у вигляді рівності: $\underbrace{ax - mt}_{\vdots d} = \underset{\vdots d}{b}$. Маємо суперечність. Отже, у цьому випадку конгруенція (2.6) розв'язків не має.

3) Нехай $(a, m) = d > 1, b \vdots d$ Розділимо обидві частини і модуль конгруенції (2.6) на d.

$$\frac{a}{d}x = \frac{b}{d}(mod\, \frac{m}{d}) \qquad \textbf{(2.7)}$$

Покажемо, що (2.6) і (2.7) рівносильні і мають однакові розв'язки по модулю m. Справді, якщо α – розв'язок (2.6), то

$$a\alpha \equiv b(mod\, m) \Leftrightarrow \frac{a}{d}\alpha \equiv \frac{b}{d}\left(mod\, \frac{m}{d}\right),$$

тобто, $\alpha -$ розв'язок (2.7).

Нехай тепер β – розв'язок (2.7). Тоді

$$\frac{a}{d}\beta \equiv \frac{b}{d}\left(mod\, \frac{m}{d}\right) \Rightarrow a\beta \equiv b(mod\, m).$$

Отже, $\beta -$ розв'язок (2.6). Оскільки $(\frac{a}{d}, \frac{m}{d}) = \frac{(a,m)}{d} = 1$, то за пунктом 1) теореми конгруенція (2.7) має єдиний розв'язок $x \equiv x_0\ (mod\, \frac{m}{d})$, де x_0 можна взяти як найменший невід'ємний лишок по модулю $\frac{m}{d}$. Тоді числа

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d} \ldots x_0 + (d-1)\frac{m}{d} \qquad \textbf{(2.8)}$$

є розв'язками конгруенції (2.7), а значить і конгруенції (2.6). Покажемо, що числа (2.8) попарно не конгруентні по модулю m. Припустимо супротивне: нехай якісь з цих чисел конгруентні по модулю m:

$$x_0 + \frac{lm}{d} \equiv x_0 + \frac{km}{d} (mod\, m), l, k \in \{0,1, \dots, d-1\}, l < k.$$

Тоді $\frac{m}{d}(l-k) \equiv 0(mod\, m)$. Скоротимо обидві частини конгруенції і модуль на $\frac{m}{d}$: $(l-k) \equiv 0(mod\, d)$, тобто $(l-k) \vdots d$.

З іншого боку, враховуючи, що $|l-k| < d$, дістанемо $l-k=0$, тобто $l=k$. Отже числа ряду (2.8) не конгруентні між собою по модулю m і є різними розв'язками (2.6). Припустимо, що конгруенція (2.6) має ще якийсь розв'язок x_0', що не належить (2.8). Тоді

$$ax_0' \equiv b(mod\, m) \Rightarrow \frac{a}{d}x_0' = \frac{b}{d}\left(mod\, \frac{m}{d}\right)$$

За доведеним остання конгруенція має один розв'язок, тому $x_0' = x_0 + \frac{m}{d}t,\ t \in Z$. Нехай $t = dq + r, 0 \le r < d$. Тоді

$$x_0' = x_0 + \frac{m(dq+r)}{d} = x_0 + mq + \frac{mq}{d} \equiv x_0 + \frac{mr}{d} (mod\, m)$$

Отже, всі числа (2.8) вичерпують розв'язки конгруенції (2.6). Теорему доведено.

Способи розв'язування лінійних конгруенцій

1) ***спосіб перебору*** повної системи лишків по модулю m.

Недолік: при великих значеннях модуля доводиться перебирати велику кількість чисел.

Приклад 2.8. Способом спроб розв'язати конгруенцію

$$3x \equiv 1(mod\ 5).$$

Розв'язання

Оскільки (3,5)=1, то задана конгруенція має один розв'язок. Запишемо повну систему лишків по модулю 5: ПСЛ$_5$={0,1,2,-1,-2} та підставимо замість x числа з цієї системи:

$$3 \cdot 0 \not\equiv 1(\text{mod}\, 5)$$

$$3 \cdot 1 \not\equiv 1(\text{mod}\, 5)$$

$$3 \cdot 2 \equiv 1(\mathrm{mod}\,5),$$

отже значення 2 задовольняє дану конгруенцію.

Відповідь: $x \equiv 2(\mathrm{mod}\,5)$.

2) ***спосіб рівносильних перетворень*** (штучний спосіб).

Використовуючи вказані вище перетворення, ліву чи праву частини конгруенції змінюють так, щоб їх можна було скоротити на коефіцієнт при невідомому. Для цього, як правило, до будь-якої частини конгруенції додають вираз, кратний модулю.

Приклад 2.9. Розв'язати конгруенції:

а) $29x \equiv 23(\mathrm{mod}\ 25)$

б) $18x \equiv 42(\mathrm{mod}\,24)$.

Розв'язання

а) Оскільки $(29,25) = 1$, то дана конгруенція має єдиний розв'язок. Додамо до лівої частини вираз $(-25x)$, а до правої 25, кратні модулю Одержимо:

$$4x \equiv 48(mod\,25).$$

Поділимо обидві частини останньої конгруенції на 4 (перетворення не змінює множину розв'язків конгруенції, бо 4 і 25 взаємно прості):

$$x \equiv 12(mod\,25).$$

Отже, $x \equiv 12(mod\,25)$ – розв'язок даної конгруенції.

б) Оскільки $(18,24) = 6$ і $42 \vdots 6$, то конгруенція має 6 розв'язків. Поділимо обидві частини конгруенції і модуль на 6:

$$3x \equiv 7(mod\,4).$$

Далі $3x \equiv 3(mod\,4)$ і $x \equiv 1(mod\,4)$.

Цей розв'язок дає 6 розв'язків за модулем 24:

$$x_1 \equiv 1(mod\,24),$$

$$x_2 \equiv (1 + \tfrac{24}{6})(mod\,24) \equiv 5(mod\,24),$$

$$x_3 \equiv (5 + \tfrac{24}{6})(mod\,24) \equiv 9(mod\,24),$$

$$x_4 \equiv (9 + \frac{24}{6})(mod\,24) \equiv 13(mod\,24)$$

$$x_5 \equiv (13 + \frac{24}{6})(mod\ 24) \equiv 17(mod\ 24),$$

$$x_6 \equiv (17 + \frac{24}{6})(mod\ 24) \equiv 21(mod\ 24).$$

Відповідь: а) $x \equiv 12(\mathrm{mod}\ 25)$, б) $x \equiv 1(mod\ 24)$, $x \equiv 5(mod\ 24)$, $x \equiv 9(mod\ 24)$, $x \equiv 13(mod\ 24)$, $x \equiv 17(mod\ 24)$, $x \equiv 21(mod\ 24)$.

3) ***Спосіб Ейлера***.

Якщо в конгруенції $(a, m) = 1$ то розв'язок можна шукати у вигляді $x \equiv ba^{\varphi(m)-1}(mod\ m)$ (пункт 1 теореми).

Недоліком є те, що відповідь доводиться спрощувати.

Приклад 2.10. Розв'язати способом Ейлера конгруенцію $5x \equiv 20(mod 12)$.

Розв'язання

Оскільки (5,12)=1, то конгруенція має один розв'язок.

За теоремою Ейлера $5^{\varphi(12)} \equiv 1(mod\ 12)$, тому

$$x \equiv 20 \cdot 5^{\varphi(12)-1}(mod\ 12),$$

де $\varphi(12) = \varphi(2^2 3) = \varphi(2^2)\ \varphi(3) = 2 \cdot 2 = 4$. Тоді

$$x \equiv 20 \cdot 5^{4-1}(mod\ 12) \equiv 20 \cdot 5^3(mod\ 12).$$

Спростимо праву частину отриманої конгруенції:

$$5^2 = 25 \equiv 1(mod\ 12),$$

$$5^3 \equiv 5(mod\ 12),$$

$$20 \equiv 8(mod\ 12),$$

$$20 \cdot 5^3 \equiv 8 \cdot 5(mod\ 12) \equiv 40(mod\ 12) \equiv 4(mod\ 12).$$

Відповідь. $x \equiv 4(mod\ 12)$.

2.5. Застосування лінійних конгруенцій до розв'язування невизначених рівнянь першого степеня з двома невідомими

Означення 2.8. *Рівняння виду*

$$ax + by = c, \qquad (2.9)$$

де $a, b, c \in Z$, називається невизначеним рівнянням першого степеня з двома невідомими.

Якщо при цьому

1) $(a,b)=d>1 \wedge c \overline{\vdots} d$, то рівняння (2.9) цілих розв'язків не матиме.

2) $(a,b)=d>1 \wedge c \vdots d$, то обидві частини рівняння можна скоротити на d. В результаті чого отримаємо рівняння $a_1x+b_1y=c_1$, де $(a_1,b_1)=1$.

3) Нехай $(a,b)=1$. Перетворимо рівняння наступним чином

$$ax-c=-by. \qquad \textbf{(2.10)}$$

Оскільки права частина рівності ділиться на b, то і ліва кратна b, отже

$$ax-c\equiv 0(mod\, b),$$

$$ax\equiv c(mod\, b).$$

Оскільки, $(a,b)=1$, то остання конгруенція матиме єдиний розв'язок $x\equiv x_0(mod\, b)$ або $x=x_0+bt, \quad t\in Z$.

Підставляючи його у (6) знайдемо відповідне значення y:

$$y=\frac{c-ax}{b}=\frac{c-a(x_0+bt)}{b}=\frac{c-ax_0}{b}-at=y_0-at, \quad t\in Z,$$

y_0- частинний розв'язок.

Отже, $\begin{cases}x=x_0+bt\\ y=y_0-at, \quad t\in Z\end{cases}$.

Приклад 2.10. Розв'язати в цілих числах рівняння

$$17x-15y=22.$$

Розв'язання

Оскільки $(17,15)=1$, то дане рівняння має розв'язки.Запишемо його у вигляді

$$17x-22=15y$$

Тоді

$$17x\equiv 22(mod\, 15),$$

$$2x\equiv 22(mod\, 15)$$

$$x\equiv 11(mod\, 15)$$

$$x=11+15t, \quad t\in Z$$

$$y = \frac{17x - 22}{19} = \frac{17(11 + 15t) - 22}{150} = \frac{17 \cdot 11 + 17 \cdot 15t - 22}{15}$$
$$= \frac{11 \cdot 15 + 17 \cdot 15t}{15} = 11 + 17t.$$

Відповідь: $\begin{cases} x = 11 + 15t \\ y = 11 + 17t \end{cases}, t \in Z.$

2.6. Системи лінійних конгруенцій

Під системою лінійних конгруенцій розуміють систему, яка складається з лінійних конгруенцій:

$$\begin{cases} a_1 x \equiv b_1 (\mathrm{mod}\, m_1) \\ a_2 x \equiv b_2 (\mathrm{mod}\, m_2) \\ \ldots\ldots\ldots\ldots \\ a_n x \equiv b_n (\mathrm{mod}\, m_n) \end{cases} \quad \textbf{(2.11)}$$

Очевидно, що якщо одна з конгруенцій цієї системи не матиме розв'язків, то система буде несумісною.

Один зі способів розв'язування систем конгруенцій полягає у послідовному знаходженні розв'язку однієї (наприклад, першої) конгруенції, підстановці його в 2-гу конгруенцію і т.д. Розв'язок системи прийнято записувати по модулю, що є найменшим спільних кратних усіх модулів: $[m_1, m_2, \ldots, m_n]$.

1)Якщо $(a_1,\ m_1) = d_1 \neq 1$ і $b_1 \vdots d_1$, то перша конгруенція розв'язків не має, тому й задана система розв'язків не має.

2)Якщо$(a_1, m_1) = 1$, то отримаємо розв'язок

$$x \equiv x_1\ (mod\ m_1),$$
$$x = x_1 + m_1 y,\ y \in Z \quad \textbf{(2.12)}$$

3)підставляємо цей розв'язок в другу конгруенцію системи. Отримана конгруенція може або не мати розв'язків (і тоді задана система також розв'язків не має), або мати розв'язок

$$y \equiv y_1 (mod\ m_2),$$
$$y = y_1 + m_2 z,\ z \in Z. \quad \textbf{(2.13)}$$

4) підставимо значення y з (2.13) у (2.12):

$$x = x_1 + m_1(y_1 + m_2 z) = x_1 + m_1 y_1 + m_1 m_2 z,\ z \in Z.$$

5) продовжуючи далі, в результаті отримаємо розв'язок системи

$$x \equiv x_k\ (mod\ m_1 m_2 \dots m_n)$$

Приклад 2.11. Розв'язати систему

$$\begin{cases} 5x \equiv 2(mod\ 6) \\ 2x \equiv 4(mod\ 10) \end{cases}$$

Розв'язання

1) $5x \equiv 2(mod\ 6)$

Оскільки $(5,6) = 1$, то дана конгруенція має один розв'язок. Додамо до лівої частини вираз $-6x$, кратний модулю:

$$-x \equiv 2(mod\ 6),$$
$$x \equiv -2(mod\ 6)$$
$$x = -2 + 6t.$$

2) Підставимо значення у другу конгруенцію

$$2x \equiv 4(mod\ 10)$$
$$2(-2 + 6t) \equiv 4(mod\ 10)$$
$$-4 + 12t \equiv 4(mod\ 10)$$
$$12t \equiv 8(mod\ 10)$$

Маємо $(12,10) = 2\ i\ \ 8 : 2$, отже буде два розв'язки по модулю 10. Скоротимо обидві частини конгруенції і модуль на 2.

$$6t \equiv 4(mod\ 5)$$
$$t \equiv 4(mod\ 5)$$

Отже, $t = 4 + 5t_1, \quad t_1 \in Z$

$$x = -2 + 6t = -2 + 6(4 + 5t_1) = 22 + 30t_1$$

Відповідь. $x = 22 + 30t_1, \quad t_1 \in Z.$

2.7. Конгруенції вищих степенів за простим модулем

Означення 2.9. *Конгруенцію виду*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (mod\, p) \qquad \textbf{(2.14),}$$

де p *– просте число,* $p \neq 2$*, в якій* $a_n \overline{\vdots}\, p$*, називають* ***конгруенцією степеня n по модулю p***.

Наступні перетворення не змінюють множини розв'язків конгруенцій і дозволяють записати їх у більш простому вигляді.

Рівносильні перетворення конгруенцій

1) заміна коефіцієнтів $a_0, a_1, \ldots, a_n$ конгруентими їм абсолютно найменшими або найменшими невід'ємними лишками $b_0, b_1, \ldots, b_n$ по модулю p.

2) пониження степеня конгруенції.

В основі останнього перетворення лежить наступна теорема.

Теорема 2.5. *Конгруенція*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (mod\ p),$$

де p *– просте число рівносильна конгруенції*

$$r(x) \equiv 0 (mod\, p) \qquad \textbf{(2.15)}$$

де $r(x)$ *– многочлен степеня* $0 \leq$ ст. $r(x) \leq p - 1$*, який є остачею при діленнілівої частини конгруенції на многочлен* $x^p - x$.

Доведення. Розділимо $f(x)$ на $(x^p - x)$ з остачею. Одержимо

$$f(x) = (x^p - x)q(x) + r(x), \qquad \textbf{(2.16)}$$

причому $r(x) = 0$ або ст $r(x) \leq p - 1$. Нехай α – розв'язок конгруенції (2.14), тоді

$$f(\alpha) = (\alpha^p - \alpha)q(\alpha) + r(\alpha) \equiv 0 (mod\, p) \qquad \textbf{(2.17)}$$

За наслідком з теореми Ферма $(\alpha^p - \alpha) \vdots p$, тому $r(\alpha) \equiv 0 (mod\, p)$, отже α – розв'язок (2.15).

Навпаки, нехай α – розв'язок конгруенції (2.15). Тоді $r(\alpha) \equiv 0\ (mod\ p)$. Піднімаючись вгору по співвідношенням (2.17) і (2.16) одержимо, що α – розв'язок (2.14). ⊲

Теорема 2.6. *Будь-яка конгруенція степеня* n *по простому модулю має не більше* n *розв'язків.*

Доведення. Нехай маємо конгруенцію

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(mod\ p),\ (a_n, p) = 1.$$

Проведемо доведення методом математичної індукції.

При $n = 1$, $a_1 x + a_0 \equiv 0(mod\ p)$, $a_1 x = -a_0(mod\ p)$. Оскільки $(a_1, p) = 1$, то конгруенція має один розв'язок.

Припустимо, що твердження теореми справедливе при $n-1 \geq 1$.

Доведемо його справедливість для n. Якщо конгруенція (2.14) розв'язків не має, то твердження справедливе, оскільки дана конгруенція має не більше ніж n розв'язків. Нехай (2.14) має розв'язки і α_1 – один з них. Тоді

$$f(\alpha_1) = a_n\alpha^n + \cdot_1\cdot + a_0 \equiv 0(mod\ p) \qquad \textbf{(2.18)}$$

Віднімемо від (2.14) конгруенцію (2.18):

$$a_n(x^n - \alpha^n) + \cdots + a_1(x - \alpha_1) \equiv 0(mod\ p)$$

$$(x - \alpha_1)(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \equiv 0(mod\ p).$$

Якщо конгруенція

$$b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \equiv 0(mod\ p) \qquad \textbf{(2.19)}$$

розв'язків не має, то теорему доведено. Якщо ж конгруенція (2.19) має розв'язки, то за індуктивним припущенням їх не більше, ніж $(n-1)$. Додавши до них розв'язок α_1, дістанемо, що конгруенція (2.14) має не більше, ніж n розв'язків. ⊲

Наслідок. *Якщо конгруенція* (2.14) *за простим модулем має більше* n *розв'язків, то всі коефіцієнти* a_i *діляться на* p $(0 \leq i \leq n)$.

Для розв'язання конгруенції вищих степенів за простим модулем використовують наступний алгоритм:

– зменшують коефіцієнти так, щоб за абсолютною величиною вони були меншими за модуль.

– понижують степінь конгруенції (до степеня не вищого за $p-1$).

– використовують рівносильні перетворення і розкладають ліву частину на множники або перебирають $ПСЛ_p$.

Приклад 2.12. Спростити конгруенцію та розв'язати її способом підбору: $x^7 + 2x^6 + x^5 + 4x^4 - 2x^2 - 4x + 3 \equiv 0\ (mod\ 5)$.

Розв'язання

Спосіб 1. За теоремою 2.5 конгруенція $f(x) \equiv 0(mod\, p)$, де p – просте число, рівносильна конгруенції $r(x) \equiv 0(mod\, p)$, де $r(x)$ – остача від ділення многочлена $f(x)$ на $(x^p - x)$.

Розділимо многочлен

$$f(x) = x^7 + 2x^6 + x^5 + 4x^4 - 2x^2 - 4x + 3$$

на $(x^5 - x)$.

$$\begin{array}{l|l}
x^7+2x^6+x^5+4x^4-2x^2-4x+3 & x^5-x \\
\cline{2-2}
x^7 \qquad\qquad -x^3 & x^2+2x+1 \\
\cline{1-1}
2x^6+x^5+4x^4+x^3-2x^2-4x+3 & \\
2x^6 \qquad\qquad -2x^2 & \\
\cline{1-1}
x^5+4x^4+x^3-4x+3 & \\
x^5 \qquad\quad -x & \\
\cline{1-1}
4x^4+x^3-3x+3 &
\end{array}$$

Отже, $r(x) = 4x^4 + x^3 - 3x + 3$.

Замінимо початкову конгруенцію на конгруенцію

$$4x^4 + x^3 - 3x + 3 \equiv 0(mod\ 5)$$

та розв'яжемо останню способом підбору. Для цього запишемо повну систему найменших за абсолютною величиною лишків за модулем 5: $ПСЛ_5 = \{-2,-1,0,1,2\}$. Перевіряємо:

$$r(-2) = 64 - 8 + 6 + 3 = 65 \equiv 0(mod\ 5),$$
$$r(-1) = 4 - 1 + 3 + 3 = 9 \not\equiv 0(mod\ 5),$$
$$r(0) = 3 \not\equiv 0(mod\ 5),$$

$$r(1) = 4 + 1 - 3 + 3 = 5 \equiv 0(mod\,5),$$
$$r(2) = 64 + 8 - 6 + 3 = 69 \not\equiv 0(mod\,5).$$

Отже, розв'язками конгруенції є $x \equiv -2(mod\,5)$ та $x \equiv 1(mod\,5)$.

Спосіб 2. За наслідком з теореми Ферма $x^p \equiv x(mod\,p)$.

Тоді

$$x^5 \equiv x(mod\,5),$$
$$x^6 \equiv x^2(mod\,5),$$
$$x^7 \equiv x^3(mod\,5).$$

Отже, початкова конгруенція рівносильна конгруенції

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

Розв'язуючи останню конгруенцію способом підбору, отримаємо розв'язки: $x \equiv -2(mod\,5)$ та $x \equiv 1(mod\,5)$.

Відповідь: $x \equiv -2(mod\,5)$ та $x \equiv 1(mod\,5)$.

Приклад 2.13. Спростити конгруенцію та розв'язати її:

$$23x^{11} + 12x^6 + 15x^3 - 45 \equiv 0(mod\,5).$$

Розв'язання

Замінимо коефіцієнти конгруентними числами по модулю 5:

$$-2x^{11} + 2x^6 \equiv 0(mod\,5)$$

Оскільки $(2,5) = 1$, то останню конгруенцію можна скоротити на 2:

$$x^7 - x^6 \equiv 0(mod\,5).$$

За наслідком з теореми Ферма:

$$x^5 \equiv x(mod\,5).$$

Отже,

$$x^6 \equiv x^2(mod\,5)$$
$$x^{11} \equiv x^3(mod\,5).$$

Замінюючи степені у початковій конгруенції, одержимо:

$$x^3 - x^2 \equiv 0(mod\,5).$$

Перебираючи повну систему лишків $ПСЛ_5 = \{0, \pm 1, \pm 2\}$, знаходимо розв'язки: $x \equiv 0(mod\,5),\ x \equiv 1(mod\,5)$.

Відповідь: $x \equiv 0(mod\,5),\ x \equiv 1(mod\,5)$.

2.8. Конгруенції другого степеня за простим модулем. Квадратичні лишки і нелишки. Критерій Ейлера

Розглянемо конгруенцію:

$$Ay^2 + By + C \equiv 0(mod\ p),$$

де p – просте число, $p \neq 2$, $A \vdots p$.

Помножимо обидві конгруенції на $4A$ і виділимо у лівій частині повний квадрат:

$$4A^2y^2 + 4ABy + 4AC \equiv 0(mod\ p),$$

$$4A^2y^2 + 4ABy + B^2 - B^2 + 4AC \equiv 0(mod\ p),$$

$$(2Ay + B)^2 + \underbrace{4AC - B^2}_{-a} \equiv 0(mod\ p),$$

Позначимо $2ay+b=x$, $b^2-4ac=-a$, дістанемо двочленну конгруенцію

$$x^2 \equiv a(mod\ p), \qquad \textbf{(2.20)}$$

де p – просте число, $p \neq 2$.

Конгруенція (2.20), в якій $(a, p) = 1$ називається *двочленною конгруенцією другого степеня***.**

Приклад 2.14. Звести конгруенцію другого степеня до двочленної і розв'язати її, використовуючи зведену систему лишків:

$$4x^2 - 11x - 8 \equiv 0(mod 13).$$

Розв'язання

Домножимо обидві частини конгруенції на 4α, де α визначимо з умови $4\alpha \equiv 1(mod\ 13)$. Тоді

$4\alpha \equiv 1+13\cdot3(mod\ 13)$, $4\alpha \equiv 40\ (mod\ 13)$ і $\alpha \equiv 10\ (mod\ 13)$.

Домножимо вихідну конгруенцію на 10:

$$40x^2 - 110x - 80 \equiv 0(mod\ 13),$$

$$x^2 - 6x - 2 \equiv 0(mod\ 13).$$

Виділимо повний квадрат у лівій частині конгруенції

$$x^2 - 6x + 9 - 9 - 2 \equiv 0(mod\ 13),$$

$$(x^2 - 3)^2 \equiv 11(mod\ 13).$$

Позначимо $x-3=y$, тоді $y^2 \equiv 11(mod\ 13)$. Розв'язки останньої

шукаємо у зведеній системі лишків по модулю 13. Неважко переконатись, що жодне число цієї системи не задовольняє останню конгруенцію і тому вихідна конгруенція також не має розв'язків.

Означення 2.8. *Якщо конгруенція* $x^2 \equiv a(mod\ p)$, p *– просте число,* $p \neq 2$, (a, p)=1, *то* a *називають* ***квадратичним лишком по модулю*** p. *Відповідно, якщо вказана конгруенція не має розв'язків, то* a *називають* ***квадратичним нелишком по модулю*** p.

Теорема 2.7. *Якщо* a *– квадратичний лишок по модулю* p, *то конгруенція* (2.20) *має два розв'язки.*

Доведення. Нехай a – квадратичний лишок, тоді за означенням конгруенція (2.20) має деякий розв'язок α.

$$\alpha^2 \equiv a(mod\ p).$$

Очевидно, що розв'язком (2.20) буде також число $(-\alpha)$, бо

$$(-\alpha)^2 = \alpha^2 \equiv a(mod\ p).$$

Покажемо, що α і $(-\alpha)$ належать різним класам лишків по модулю p. Припустимо супротивне. Нехай $\alpha \equiv -\alpha(mod\ p)$, тоді

$$2\alpha \equiv 0(mod\ p).$$

Оскільки за умовою $(2, p)$=1, то $\alpha \equiv 0(mod\ p)$ і $a \equiv 0(mod\ p)$, що неможливо. Отже, конгруенція (2.20) має два різні розв'язки: $x \equiv \alpha(mod\ p)$ та $x \equiv -\alpha(mod\ p)$. За теоремою 2.6 конгруенція (2.20) має не більше двох розв'язків. Отже, таких розв'язків буде в точності два. ⊲

Теорема 2.8. *В будь-якій* ЗСЛ *по модулю* p *половина чисел є лишками, а половина – нелишками по модулю* p.

Доведення. Розглянемо $ЗСЛ_p$ найменших за абсолютною системою лишків:

$$ЗСЛ_p = \left\{-\frac{(p-1)}{2}; -\frac{(p-1)}{2} + 1; \dots; -1; 1; 2; \dots; -\frac{(p-1)}{2}\right\}.$$

Серед них квадратичними лишками будуть лише ті числа, які конгруентні з числами

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2. \qquad \textbf{(2.21)}$$

В послідовності (2.21) міститься $\frac{(p-1)}{2}$ чисел. Покажемо, що вони попарно не конгруентні по модулю p. Припустимо супротивне.

Нехай в (2.21) числа k^2 і l^2 такі, що $k^2 \equiv l^2(mod\, p)$. Тоді конгруенція $x^2 \equiv a(mod\, p)$, буде мати чотири розв'язки:

$$x \equiv \pm k(mod\, p) \text{ і } x \equiv \pm l(mod\, p),$$

оскільки $a \equiv k^2 \equiv l^2(mod\, p)$. Проте конгруенція другого степеня не може мати більше ніж два розв'язки, тому в послідовності (2.21) буде $\frac{p-1}{2}$ чисел, а значить і квадратичних лишків буде стільки ж. ⊲

Приклад 2.15. Знайти квадратичні лишки і нелишки по модулю 11.

Розв'язання

Запишемо ЗСЛ$_{11}$={1,2,3,4,5,6,7,8,9,10}.

За попередньою теоремою квадратичних лишків та нелишків по модулю 11 буде порівну, по $\frac{11-1}{2} = 5$. Перевіримо кожне число з ЗСЛ$_{11}$:

$$1^2 \equiv 1(mod\ 11),$$
$$2^2 \equiv 4(mod\ 11),$$
$$3^2 \equiv 9(mod\ 11),$$
$$4^2 \equiv 5(mod\ 11),$$
$$5^2 \equiv 3(mod\ 11).$$

Отже, квадратичними лишками по модулю є: 1, 3, 4, 5, 9, а квадратичними нелишками відповідно будуть: 2, 6, 7, 8, 10.

Теорема 2.9 (критерій Ейлера). *Число a є квадратичним лишком по модулю p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1(mod\, p)$, і квадратичним нелишком по цьому модулю, тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1(mod\, p)$.*

Доведення. Оскільки (a, p)=1, то за теоремою Ферма $a^{p-1} \equiv 1(mod\, p)$ або $(a^{p-1}-1) \vdots\ p$. Враховуючи, що число $(p-1)$ парне, $(a^{p-1}-1)$ можна подати у вигляді:

$$(a^{p-1}-1) = (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1).$$

Покажемо, що обидва числа $(a^{\frac{p-1}{2}}-1)$ і $(a^{\frac{p-1}{2}}+1)$ не можуть ділитися на p. Справді, в іншому випадку їх різниця також ділилася б на p:

$$(a^{\frac{p-1}{2}}-1)-(a^{\frac{p-1}{2}}+1)=2\vdots\ p,$$

що неможливо за вибором p. Отже,

$$(a^{\frac{p-1}{2}}-1)\equiv 0(mod\ p) \text{ або } (a^{\frac{p-1}{2}}+1)\equiv 0(mod\ p),$$

тобто $a^{\frac{p-1}{2}}\equiv 1(mod\ p)$ або $a^{\frac{p-1}{2}}\equiv -1(mod\ p)$ і має місце лише одна з цих умов.

Нехай a – квадратичний лишок по модулю p, тоді існує таке $x_0\in Z$, що $x_0^2\equiv a(mod\ p)$. Тоді

$$(x_0^2)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}(mod\ p)$$

або

$$a^{\frac{p-1}{2}}\equiv (x_0^2)^{\frac{p-1}{2}}\equiv x_0^{p-1}\equiv 1(mod\ p).$$

Враховуючи, що по модулю p в зведеній системі буде $\frac{p-1}{2}$ квадратичних лишків, то всі вони будуть розв‘язками останньої конгруенції. Більше розв’язків остання конгруенція мати не може, бо її степінь $\frac{p-1}{2}$.

Отже, якщо a – квадратичний лишок, то $a^{\frac{p-1}{2}}\equiv 1(mod\ p)$. З цього також випливає, що квадратичні нелишки вичерпують розв’язки конгруенції $a^{\frac{p-1}{2}}\equiv -1(mod\ p)$. ◅

Приклад 2.16. З’ясувати, скільки розв’язків має конгруенція

$$x^2\equiv 3(mod\ 13).$$

Розв’язання.

Застосуємо критерій Ейлера і з’ясуємо, з яким числом конгруентне $a^{\frac{p-1}{2}}$ по модулю p:

$$3^{\frac{13-1}{2}}=3^6=3^3\cdot 3^3\equiv 1\cdot 1\equiv 1(mod\ 13).$$

Отже, число 3 є квадратичним лишком по модулю 13 і задана конгруенція має 2 розв’язки. Очевидно, ними є $x\equiv\pm 4(mod\ 13)$.

2.9. Символ Лежандра, його властивості і застосування

При великих значеннях p застосування критерію Ейлера стає практично незручним, тому використовують метод, заснований на властивостях символа Лежандра.

Означення 2.9. *Нехай* (a, p)=1. *Символом Лежандра* $\left(\frac{a}{p}\right)$ («a *по відношенню до* p») *називається*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{якщо } a - \text{квадратичний лишокпо модулю } p \\ -1, \text{ якщо } a - \text{квадратичний нелишок по модулю } p \end{cases}$$

Приймаючи до уваги критерій Ейлера, маємо

$$\left(\frac{a}{\mathrm{p}}\right) \equiv a^{\frac{\mathrm{p}-1}{2}} (mod\, p)$$

Властивості символа Лежандра

1. Якщо $a \equiv b(mod\, p)$, то $\left(\frac{a}{\mathrm{p}}\right) = \left(\frac{b}{\mathrm{p}}\right)$.

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

◅ Доведення властивості випливає з означення та критерію Ейлера.

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

◅ Справді, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\, p)$ і $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} (mod\, p)$. Тому

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} (mod\, p) \equiv (ab)^{\frac{p-1}{2}} (mod\, p) \equiv \left(\frac{ab}{p}\right)$$

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

◅ Випливає з властивості 3.

5. $\left(\frac{1}{p}\right) = 1$

◅ Випливає з властивості 4.

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

7. (*Квадратичний закон взаємності лишків). Якщо* p *і* q *– прості непарні числа, то* $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Приклад 2.17. З'ясувати, скільки розв'язків має конгруенція

$$x^2 \equiv 13(mod\ 17).$$

Розв'язання.

Запишемо символ Лежандра: $\left(\frac{a}{p}\right) = \left(\frac{13}{17}\right)$. Застосуємо властивість 1) і замінимо 13 числом –4, конгруентним по модулю 17, а потім застосуємо властивості 3), 4) і 2):

$$\left(\frac{13}{17}\right) = \left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{4}{17}\right) = (-1)^{\frac{17-1}{2}} = (-1)^8 = 1.$$

Отже, дана конгруенція має два розв'язки.

Приклад 2.18. З'ясувати, чи проходить через точки з цілими координатами парабола $53y = x^2 - 210$.

Розв'язання

Парабола $53y = x^2 - 210$ проходить через точки з цілими координатами, якщо конгруенція $x^2 \equiv 210(mod\ 53)$ має розв'язки, і не проходить через точки з цілими координатами, якщо ця конгруенція не має розв'язків.

Конгруенція $x^2 \equiv 210(mod\ 53)$ має два розв'язки або не має жодного, якщо 210 є квадратичним лишком або, відповідно, нелишком по модулю 53.

Обчислимо символ Лежандра $\left(\frac{210}{53}\right)$.

Оскільки $210 \equiv 51(mod\ 53)$, то $\left(\frac{210}{53}\right) = \left(\frac{51}{53}\right)$. Далі маємо:

$$\left(\frac{51}{53}\right) = \left(\frac{17}{53}\right)\left(\frac{3}{53}\right) = (-1)^{\frac{17-1}{2}\cdot\frac{53-1}{2}}\left(\frac{53}{17}\right)(-1)^{\frac{3-1}{2}\cdot\frac{53-1}{2}}\left(\frac{53}{3}\right) =$$

$$= (-1)^{208}\left(\frac{53}{17}\right)(-1)^{26}\left(\frac{53}{3}\right) = \left(\frac{53}{17}\right)\left(\frac{53}{3}\right) = \left(\frac{2}{17}\right)\left(\frac{2}{3}\right) =$$

$$= (-1)^{\frac{17^2-1}{8}}(-1)^{\frac{3^2-1}{8}} = (-1)^{36}(-1) = -1$$

Отже, задана парабола не проходить через точки з цілими координатами.

2.10. Показник числа за даним модулем. Первісні корені, їх існування та властивості

Нехай $a \in Z$, $m \in N$ і $(a,m)=1$. За теоремою Ейлера $a^{\varphi(m)} \equiv 1(mod\ m)$, тому існують числа $x \in N$ такі, що

$$a^x \equiv 1(mod\ m)$$

(одним з них є, наприклад, $\varphi(m)$).

Означення 2.10. *Найменше натуральне число δ, для якого виконується умова*

$$a^\delta \equiv 1(mod\ m)$$

називається ***показником числа a за модулем m.***

Показник числа ***a*** за модулем ***m*** позначають $P_m(a)$.

Якщо $(a,m) \neq 1$, то число a не має показника по модулю m.

Приклад 2.19. Знайти $P_m(a)$, якщо:

1) a =2, m=3,

2) a=4, m=9,

3) a=5, m=11.

Розв'язання

1) a=2, m=3: $2^1 \equiv -1(mod\ 3)$, тому $2^2 \equiv 1(mod\ 3)$ і $P_3(2)$=2.

2) a=4, m=9: $4^1 \not\equiv 1(mod\ 9)$, $4^2 \equiv -2 \not\equiv 1(mod\ 9)$, $4^3 \equiv -8 \equiv 1(mod\ 9)$ і $P_9(4)$=3.

3) a=5, m=11: $5^1 \not\equiv 1(mod\ 11)$, $5^2 \equiv 3(mod\ 11)$, $5^3 \equiv 15 \equiv 4(mod\ 11)$, $5^4 \equiv 9(mod\ 11)$, $5^5 \equiv 45(mod\ 11) \equiv 1(mod\ 11)$ і $P_{11}(5)$=5.

Теорема 2.10. *Якщо $a \equiv b(mod\ m)$, то a і b мають однакові показники за модулем m, тобто $P_m(a) = P_m(b)$.*

Доведення. Нехай $a \equiv b(mod\ m)$ і $P_m(a) = \delta$, $P_m(b) = \beta$. Тоді δ і β – найменші натуральні числа такі, що

$$a^\delta \equiv 1(mod\ m),\ b^\beta \equiv 1(mod\ m).$$

За умовою $a \equiv b(mod\ m)$. Піднесемо до степеня δ:

$$a^\delta \equiv b^\delta(mod\ m) \text{ і } b^\delta \equiv 1(mod\ m).$$

Оскільки β – найменше натуральне з такою властивістю, то

$\delta \geq \beta$. Піднесемо тепер початкову конгруенцію до степеня β:

$$a^{\beta} \equiv b^{\beta} (mod\ m) \text{ і } a^{\beta} \equiv 1 (mod\ m),$$

$\beta \leq \delta$. Отже, $\delta = \beta$.

Наслідок. *Всі числа одного і того ж класу лишків мають за модулем m однакові показники.*

Отже, може можна вважати, що увесь клас лишків належить даному показнику.

Означення 2.11. *Клас чисел має показник δ за модулем m, якщо представник цього класу має показник δ за модулем m.*

Отже, якщо $P_m(a) = \delta$, то $P_m(\bar{a}) = \delta$.

Властивості показників

1. Якщо $P_m(a) = \delta$, то числа

$$a^0 = 1,\ a, a^2, \ldots a^{\delta - 1}$$

попарно не конгруентні між собою за модулем m.

◅ Припустимо супротивне, нехай $a^k \equiv a^l (mod\ m)$ при $k \neq l$, $0 \leq k \leq \delta - 1$, $0 \leq l \leq \delta - 1$ і $k > l$. Поділимо обидві частини конгруенції на a^l:

$$a^{k-l} \equiv 1 (mod\ m),\ 0 < k - l < \delta,$$

що неможливо, бо δ – найменше натуральне з такою властивістю. Отже, $a^k \not\equiv a^l (mod\ m)$.

2. Якщо $P_m(a) = \delta$, то конгруенція

$$a^{\alpha} \equiv a^{\beta} (mod\ m),$$

де α, β – деякі цілі невід'ємні числа, має місце тоді і тільки тоді, коли $\alpha \equiv \beta (mod\ \delta)$.

◅ *Необхідність*. Нехай $P_m(a) = \delta$ і $a^{\alpha} \equiv a^{\beta} (mod\ m)$, $\alpha \geq \beta$. Тоді $a^{\alpha - \beta} \equiv 1 (mod\ m)$. Поділимо $\alpha - \beta$ на δ: $\alpha - \beta = \delta q + r$, $0 \leq r < \delta$. Тоді

$$a^{\alpha - \beta} = a^{\delta q + r} = (a^{\delta})^q a^r \equiv a^r (mod\ m) \equiv 1 (mod\ m).$$

Це можливо лише за умови $r = 0$. Отже, $\alpha - \beta = \delta q$ і $\alpha \equiv \beta (mod\ \delta)$.

Достатність. Нехай $P_m(a) = \delta$ і $\alpha \equiv \beta (mod\ \delta)$. Тоді $\alpha = \beta + \delta k$, $k \in Z$. Тоді

$$a^{\alpha} = a^{\beta + \delta k} = a^{\beta} (a^{\delta})^k \equiv a^{\beta} (mod\ m),$$

тобто $a^{\alpha} \equiv a^{\beta}(mod\ m)$.

3. Якщо $P_m(a)=\delta$ і $a^n \equiv 1(mod\ m)$, то $n \vdots \delta$ і навпаки.

◅ Оскільки $P_m(a)=\delta$, то $a^{\delta} \equiv 1(mod\ m)$. За властивістю 2

$$n \equiv \delta(mod\ \delta), \text{ тобто } n \vdots \delta.$$

Навпаки, нехай $n \vdots \delta$, тоді $n = \delta k$ і з умови $a^{\delta} \equiv 1(mod\, m)$ випливає, що $(a^{\delta})^k = a^n \equiv 1(mod\, m)$.

4. Якщо $P_m(a) = \delta$, то $\varphi(m) \vdots \delta$.

◅ За теоремою Ейлера $a^{\varphi(m)} \equiv 1(mod\ m)$. За властивістю 3 $\varphi(m) \vdots \delta$.

З останньої властивості випливає, що показник числа за модулем m міститься серед дільників $\varphi(m)$.

Приклад 2.20. Знайти $P_m(a)$, якщо a=2, m=11.

Розв'язання

Маємо $\varphi(11)=10$, тому показник числа 5 слід шукати серед дільників числа 10: 1,2,5,10:

$2^1 \not\equiv 1(mod\ 11)$, $2^2 \equiv 4 \not\equiv 1\ (mod\ 11)$,

$2^5 \equiv 32 \equiv -1 \not\equiv 1(mod\ 11)$, $2^{10} \equiv 1(mod\ 11)$.

Отже, $P_{11}(2)=10$.

Означення 2.12. *Число a називають* первісним коренем *за модулем m, якщо* $P_m(a) = \varphi(m)$.

Теорема 2.11. *Якщо a – первісний корінь за модулем m, то числа*

$$a^0 = 1, a, a^2, \dots, a^{\varphi(m)-1} \qquad (\mathbf{2.22})$$

утворюють ЗСЛ$_m$.

Доведення. Кількість членів у послідовності (2.22) дорівнює $\varphi(m)$. За властивістю 1 вони попарно не конгруентні за модулем m. Оскільки (a,m)=1, то і (a^k, m)=1 для всіх k=0,1,2,…, $\varphi(m)-1$. Відомо, що сукупності цілих чисел з такими ознаками ці числа утворюють ЗСЛ$_m$. Теорему доведено.

Теорема 2.12 *(про число первісних коренів за простим*

модулем). Існує точно $\varphi(p-1)$ *первісних коренів за модулем* p.

Доведення. Нехай a – первісний корінь по модулю p, тобто $P_p(a) = \varphi(p) = p-1$. За теоремою 2.11 числа

$$\{a^0, a^1, .., a^{p-2}\}$$

утворюють ЗСЛp, і кожне з них є розв'язком конгруенції $x^{p-1} \equiv 1(mod\, p)$ за теоремою Ферма. Як відомо, остання конгруенція має не більш, ніж $p-1$ розв'язок.

Знайдемо, скільки з чисел вказаної послідовності мають показник $(p-1)$. Нехай a^k – одне з чисел вказаного ряду, яке має показник δ, тоді $(a^k)^\delta \equiv 1(mod\, p)$. З іншого боку, оскільки $P_p(a) = p-1$, то $a^{p-1} \equiv 1(mod\, p)$, і за властивістю 3 $(k\delta) \vdots (p-1)$. При цьому можливі два випадки:

1) $(k, p-1) = 1$, тоді $\delta \vdots (p-1)$ і $\delta = l(p-1)$. Враховуючи, що δ – найменший натуральний розв'язок конгруенції

$$(a^k)^\delta \equiv 1(mod\, p),$$

одержимо $a^{k\delta} = a^{kl(p-1)} \equiv 1(mod\, p)$. З іншого боку, за теоремою Ферма $(a^k)^{p-1} \equiv 1(mod\, p)$. Отже, $l = 1$ і a^k має показником $(p-1)$.

2) Нехай $(k, p-1) \neq 1$. В цьому випадку нескладно довести, що a^k матиме показник менший, ніж $(p-1)$.

Таким чином, у вказаній послідовності показник $(p-1)$ будуть мати числа a^k, де k взаємно просте з $p-1$ і $k < p-1$. Це означає, що їх кількість дорівнює $\varphi(p-1)$, що й треба було показати.

Приклад 2.21. Знайти первісні корені за модулем 17.

Розв'язання

Будемо шукати первісні корені за модулем 17 серед чисел ЗСЛ$_{17}$:

$$\{1,2,3,4,5,6,7, 8,–8,–7, –6,–5,–4,–3,–2,–1\}.$$

Число первісних коренів за модулем 17 дорівнює

$$\varphi(p-1)=\varphi(16)=8$$

Оскільки показники числа містяться серед дільників $\varphi(17)=16$, то будемо перевіряти лише ті степені, що є дільниками 16 (тобто, 1,2,4,8,16):

$2^4 = 16 \equiv -1 \not\equiv 1 \ (mod\ 17)$, $2^8 \equiv 1 (mod\ 17)$, але $8 < \varphi(17) = 16$.

Отже, 2 не є первісним коренем.

Далі маємо:

$3^2 = 9 \not\equiv 1 \ (mod\ 17)$, $3^3 \equiv 27 \equiv 10 \not\equiv 1 \ (mod 17)$, $3^4 = 30 \equiv -4 \not\equiv 1 (mod\ 17)$, $3^8 \equiv 16 \equiv -1 \not\equiv 1 \ (mod\ 17)$, $3^{16} \equiv 1 (mod\ 17)$.

Отже, 3 є первісним коренем. З доведення теореми 3 випливає, що первісними коренями будуть також числа виду 3^k, де $(k, 16) = 1$, $k < 16$. Такими числами є: $3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}$ і 3^{15}. При цьому

$$3^3 \equiv 10 (mod\ 17),\ 3^5 \equiv 5 (mod\ 17),\ 3^7 \equiv 11 (mod\ 17),$$

$3^9 \equiv 14 (mod\ 17)$, $3^{11} \equiv 7 (mod\ 17)$, $3^{13} \equiv 12 (mod\ 17)$, $3^{15} \equiv 6 (mod 17)$.

Відповідь: первісними коренями по модулю 17 є: 5, 6, 7, 10, 11, 12, 14.

Зауваження. Якщо існує хоча б одне число, що має показник δ по модулю m, то кількість класів лишків, які мають цей же показник дорівнює $\varphi(\delta)$**.**

Приклад 2.22. Знайти порядки усіх класів лишків за модулем 9. Вказати класи, представники яких є первісними коренями.

Розв'язання

Порядок класу лишків дорівнює порядку будь-якого представника цього класу лишків за модулем 9. Представники класів лишків за модулем 9 містяться в зведеній системі лишків:

$$ЗСЛ_9 = \{1, -1, 2, -2, 4, -4, \}.$$

Оскільки $\varphi(9) = 9(1 - \frac{1}{3}) = 6$, порядки δ потрібно шукати серед дільників $\varphi(9)$, тобто $\delta \in \{1,2,3,6\}$.

Оскільки $1^1 \equiv 1 (mod\ 9)$, то $P_9(1) = 1 = P_9(\overline{1})$;

$(-1)^2 \equiv 1 (mod\ 9)$, то $P_9(-1) = 2 = P_9(\overline{-1})$;

$2^3 \equiv -1 (mod\ 9)$, $2^6 \equiv 1 (mod\ 9)$, то $P_9(2) = 6 = P_9(\overline{2})$ і довільний представник класу $\overline{2}$ є первісним коренем за модулем 9.

Аналогічно, $(-2)^3 \equiv 1 (mod\ 9)$, тому $P_9(-2) = P_9(\overline{-2}) = 3$;

$4^2 \equiv -2 (mod\ 9)$, $4^3 \equiv 1 (mod\ 9)$, отже, $P_9(4) = P_9(\overline{4}) = 3$.

Нарешті, $(-4)^3 \equiv -1 (mod\ 9)$, $(-4)^6 \equiv 1 (mod\ 9)$, звідки

$P_9(4) = P_9(\overline{-4}) = 6$. Отже, довільний представник класу $\overline{-4}$ є первісним коренем за модулем 9.

Відповідь: $P_9(\overline{1}) = 1,\ P_9(\overline{2}) = 6, P_9(\overline{4}) = 3, P_9(\overline{-4}) = 6, P_9(\overline{-2}) = 3, P_9(\overline{-1}) = 2$. Класи, елементи яких є первісними коренями – це $\overline{-4}$ та $\overline{2}$.

2.11. Індекси за простим модулем та їх застосування

Нехай p – просте число $p \neq 2$ і g – первісний корінь по модулю p. Тоді за теоремою 3 послідовність

$$\{q^0, q^1, \ldots, q^{p-2}\} \qquad \textbf{(2.23)}$$

утворює ЗСЛ$_p$. Якщо $a \in Z$ $(a, p) = 1$, то a буде конгруентним з одним із чисел (2.23) тобто $a \equiv g^{\gamma}(mod\ p)$.

Означення 2.13. *Нехай* $(g,\ p) = 1$, число γ *називають індексом числа* a *за основою* g *і модулем* p, *якщо* $g^{\gamma} \equiv a\ (mod\ p)$.

Позначення: $\gamma = ind_g a$ (індекс a за основою g по модулю p)

Властивості індексів по модулю p за основою g

1. *Якщо* $a \equiv b(mod\ p)$, *то* $ind_g a \equiv ind_g b(mod\ p - 1)$ *і навпаки.*

◅ Нехай $\gamma = ind_g a$, тобто $g^{\gamma} \equiv a(mod\ p)$. Оскільки $a \equiv b(mod\ p)$ і відношення конгруентності транзитивне, то $g^{\gamma} \equiv b(mod\ p)$ і $ind_g b = \gamma$.

Навпаки, нехай $\gamma = ind_g a$ і $\gamma' = ind_g b$ і $\gamma' \equiv \gamma\ (mod\ p - 1)$. Тоді $\gamma' = \gamma + (p-1)k, k \in Z$. Враховуючу малу теорему Ферма, будемо мати

$$b \equiv g^{\gamma'} \equiv g^{\gamma + (p-1)k} \equiv g^{\gamma} g^{(p-1)k} \equiv g^{\gamma} \equiv a(mod\ p).$$

Отже, $a \equiv b(mod\ p)$.

2. Якщо γ і γ' – індекси числа a за основою g і модулем p то

$$\gamma \equiv \gamma'(mod\ p - 1).$$

◅ Нехай $\gamma = ind_g\ a$ і $\gamma' = ind_g\ a$, тобто $g^{\gamma} \equiv a(mod\ p)$ і $g^{\gamma'} \equiv a(mod\ p)$. Тоді $g^{\gamma} \equiv g^{\gamma'}\ (mod\ p)$ і $\gamma \geq \gamma$. Поділимо обидві частини конгруенції на $g^{\gamma'}$: $g^{\gamma - \gamma'} \equiv 1(mod\ p)$ і $\gamma - \gamma' \vdots (p-1)$, звідки

$$\gamma \equiv \gamma'(mod\ p - 1).$$

3. *Якщо* $(a, p) = 1, (b, p) = 1$, *то*

$$ind_g(ab) \equiv ind_g a + ind_g b \ (mod\ p - 1).$$

◅ Нехай $\gamma_1 = ind_g a$ і $\gamma_2 = ind_g b$, тоді $g^{\gamma_1} \equiv a(mod\ p)$ і $g^{\gamma_2} \equiv b(mod\ p)$. Перемножимо конгруенції почленно:

$$g^{\gamma_1}\, g^{\gamma_2} \equiv ab(mod\ p), \quad g^{\gamma_1 + \gamma_2} \equiv ab(mod\ p),$$

Отже, $ind_g(ab) = \gamma_1 + \gamma_2 = ind_g a + ind_g b$.

4. $ind_g a^n \equiv n\ ind_g a\ (mod\ p - 1),\ n \in N$.

5. Якщо $a \vdots b$, то $ind_g \frac{a}{b} \equiv ind_g a - ind_g b (mod\ p - 1)$.

6. $ind_g g \equiv 1 (mod\ p - 1)$.

7. $ind_g 1 \equiv 0 (mod\ p - 1)$

Приклад 2.23. Скласти таблицю індексів за модулем 19.

Розв'язання

Знайдемо один із первісних коренів за модулем 19. Оскільки $\varphi(19)=18$, то будемо перевіряти лише ті степені, що мають показником дільник 18 (тобто, 2,3,6 , 9 і 18):

$2^2 \equiv 4(mod\ 19),\ 2^3 \equiv 8(mod\ 19),\ 2^6 \equiv 7(mod\ 19),$

$2^9 \equiv -1(mod\ 19),\ 2^{18} \equiv 1(mod\ 19).$

Отже, 2 – первісний корінь за модулем 19. Візьмемо його за основу таблиці індексів і знайдемо найменші невід'ємні лишки степенів $2^0, 2^1, \dots, 2^{18}$ за модулем 19.

$2^0 \equiv 1(mod\ 19),\ ind_2 1 = 0,$

$2^1 \equiv 2(mod\ 19),\ ind_2 2 = 1,$

$2^2 \equiv 4(mod\ 19),\ ind_2 4 = 2,$

$2^3 \equiv 8(mod\ 19),\ ind_2 8 = 3,$

$2^4 \equiv 16(mod\ 19),\ ind_2 16 = 4,$

$2^5 = 32 \equiv 13(mod\ 19),\ ind_2 13 = 5,$

$2^6 \equiv 26(mod\ 19) \equiv 7(mod\ 19),\ ind_2 7 = 6,$

$2^7 \equiv 14(mod\ 19)$, $ind_2 14 = 7$,

$2^8 \equiv 28(mod\ 19) \equiv 9(mod\ 19)$, $ind_2 9 = 8$,

$2^9 \equiv 18(mod\ 19)$, $ind_2 18 = 9$,

$2^{10} \equiv 36(mod\ 19) \equiv 17(mod\ 19)$, $ind_2 17 = 10$,

$2^{11} \equiv 34(mod\ 19) \equiv 15(mod\ 19)$, $ind_2 15 = 11$,

$2^{12} \equiv 30(mod\ 19) \equiv 11(mod\ 19)$, $ind_2 11 = 12$,

$2^{13} \equiv 22(mod\ 19) \equiv 3(mod\ 19)$, $ind_2 3 = 13$,

$2^{14} \equiv 6(mod\ 19)$, $ind_2 6 = 14$,

$2^{15} \equiv 12(mod\ 19)$, $ind_2 12 = 15$,

$2^{16} \equiv 24(mod\ 19) \equiv 5(mod\ 19)$, $ind_2 5 = 16$,

$2^{17} \equiv 10(mod\ 19)$, $ind_2 10 = 17$,

$2^{18} \equiv 20(mod\ 19) \equiv 1(mod\ 19)$, $ind_2 1 = 18$.

		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Індекси	**0**		0	1	13	2	16	14	6	3	8
	1	17	12	15	5	6	11	4	10	9	

Розв’язування двочленних конгруенцій за допомогою індексів

Конгруенція виду

$$ax^n \equiv b\ (mod\ p),$$

де (a,p)=1, $n \in N$ називається *двочленною конгруенцією* n*-го степеня за простим модулем.*

Застосуємо властивості індексів до цієї конгруенції та проіндексуємо обидві її частини:

$$ind\ a + n \cdot ind\ x \equiv ind\ b\ (mod\ p{-}1)$$

$$n \cdot ind\ x \equiv c(mod\ p{-}1), \quad \text{де } c = ind\ b - ind\ a.$$

Отже, розв’язування цієї конгруенції зводиться до розв’язуванняконгруенції першого степеня відносно $ind\ x$.

Приклад 2.24. Розв’язати конгруенцію, використовуючи індекси:

1) $5x^{12} \equiv 8(mod\ 19)$

2) $7x^{14} \equiv 9(mod\ 19)$.

Розв'язання

3) Проіндексуємо обидві частини конгруенції $5x^{12} \equiv 8(mod\ 19)$ (модуль замінимо на $p-1$):

$$ind\ 5 + 12ind\ x \equiv ind\ 8(mod\ 18).$$

За таблицею індексів: $16 + 12ind\ x \equiv 3(mod\ 18)$,

$$12ind\ x \equiv -13(mod\ 18),$$

$$12ind\ x \equiv 5(mod\ 18).$$

Оскільки (12,18) = 6, $5 \ \vdots\ 6$, то конгруенція розв'язків не має.

2) $7x^{14} \equiv 9(mod\ 19)$.

Проіндексуємо обидві частини конгруенції:

$$ind\ 7 + 14ind\ x \equiv ind\ 9(mod\ 18),$$

$$6 + 14ind\ x \equiv 8(mod\ 18),$$

$$14ind\ x \equiv 2(mod\ 18).$$

Оскільки (14,18) = 2 і $2 \vdots 2$, то конгруенція має два розв'язки. Поділимо обидві частини конгруенції та модуль на 2:

$$7ind\ x \equiv 1(mod\ 9),$$

$$7ind\ x \equiv -35(mod\ 9),$$

$$ind\ x \equiv -5(mod\ 9).$$

Отже, розв'язками конгруенції будуть

$$ind\ x \equiv 4(mod\ 18) \text{ і } ind\ x \equiv 4+9 \equiv 13(mod\ 18).$$

За таблицею індексів знайдемо числа, які мають індекси 4 і 13 по модулю 19: $x \equiv 3(mod\ 19)$ та $x \equiv 16(mod\ 19)$ (перехід від індексів до чисел називають *потенціюванням*).

Розв'язування показникових конгруенцій

Нехай маємо конгруенцію $a^x \equiv b(mod\ p)$. Перейдемо до індексів:

$$x \cdot ind\ a \equiv ind\ b(mod\ p).$$

Отримали конгруенцію першого степеня з одним невідомим.

Приклад 2.25. Розв'язати конгруенцію: $5^x \equiv 17(mod\ 19)$.

Розв'язання

Проіндексуємо обидві частини конгруенції:

$$x \cdot ind\ 5 \equiv ind\ 17(mod\ 18),\ 16x \equiv 10(mod\ 18).$$

Оскільки (16,18)=2 і 10 ⋮ 2, то конгруенція має два розв'язки.

$$8x \equiv 5(mod\ 9),\ -x \equiv 5(mod\ 9),\ x \equiv -5 \equiv 4(mod\ 9).$$

Отже, $x \equiv 4(mod\ 18)$ і $x \equiv 13(mod\ 18)$.

Оскільки (23,30) = 1, то конгруенція має один розв'язок:

$$23x \equiv -23(mod\ 30),$$

$$x \equiv -1(mod\ 30),\ \text{або}\ x \equiv 29(mod\ 30).$$

3. ЕЛЕМЕНТИ ТЕОРІЇ ГРУП

3.1. Алгебраїчні операції та алгебраїчні системи

Нехай A – будь-яка непорожня множина, $A \times A = A^2 = \{(a,b) | a,b \in A\}$ – прямий добуток множини A самої на себе (декартів квадрат).

Означення 3.1. *Функція* $A \times A \xrightarrow{f} A$ *називається бінарною алгебраїчною операцією, заданою на множині A.*

Отже, на множині A задана бінарна алгебраїчна операція, якщо кожній парі (a,b) її елементів ставиться у відповідність деякий третій однозначно визначений елемент з цієї ж множини. При цьому результат бінарної алгебраїчної операції f записуватимемо не у вигляді $f(a,b)$, а у вигляді afb. Такий запис добре узгоджується з позначеннями арифметичних операцій: ми пишемо 3+5=8, а не +(3,5)=8. Крім цього, у загальному випадку саму операцію позначатимемо символом «$*$».

Прикладами алгебраїчних операцій є: додавання і множення натуральних, цілих, раціональних, дійсних і комплексних чисел, многочленів, алгебраїчних дробів, матриць; об’єднання і перетин множин; знаходження найбільшого спільного дільника і найменшого спільного кратного двох натуральних чисел; композиція відображень деякої множини на себе.

З іншого боку, віднімання натуральних чисел, ділення цілих чисел, ділення многочленів, скалярний добуток векторів не є бінарними алгебраїчними операціями.

Зауваження. Якщо на множині A задана алгебраїчна операція «$*$», то вона повинна виконуватись для *кожної пари елементів* множини A. При цьому множину A називають *замкненою* відносно операції «$*$», а саму операцію інколи називають *внутрішньою* бінарною алгебраїчною операцією, заданою на множині A. Таке виділення операцій особливо корисно тоді, коли поряд з внутрішніми операціями розглядаються і так звані зовнішні операції.

Означення 3.2. *Множина A, на якій задано хоча б одну алгебраїчну операцію називається алгебраїчною системою.*

Найважливішими алгебраїчними системами є: напівгрупи, групи, кільця, поля, лінійні простори, модулі над кільцями, алгебри.

3.2. Групоїди, напівгрупи, моноїди, групи

Нехай G – деяка непорожня множина, на якій задана бінарна алгебраїчна операція «$*$».

Означення 3.3. *Множина G, на якій задано бінарну алгебраїчну операцію* «$*$» *називається групоїдом.*

Цей групоїд позначатимемо $(G;*)$. Наприклад, $(N;+)$ – групоїд натуральних чисел відносно додавання.

Означення 3.4. *Групоїд* $(G;*)$ *називається напівгрупою, якщо операція* «$*$» *асоціативна:*

$\forall\, a,b,c \in G\left(a*\left(b*c\right)=\left(a*b\right)*c\right)$.

Прикладами напівгруп є групоїди $(N;+)$, $(N;\cdot)$, $(Z;+)$.

Приклад 3.1. Довести, що групоїд $(R;*)$, де $a*b=a+b-ab$ для довільних дійсних чисел, є напівгрупою.

Розв'язання

Доведемо, що для довільних дійсних чисел a,b,c виконується рівність $a*\left(b*c\right)=\left(a*b\right)*c$ За означенням операції «$*$» маємо:

$a*(b*c)=a*(b+c-bc)=a+b+c-bc-a(b+c-bc)=a+b+c-bc-ab-ac+abc$

$\left(a*b\right)*c=\left(a+b-ab\right)*c=a+b-ab+c-\left(a+b-ab\right)c=a+b+c-ab-ac-bc+abc$

Отже, $a*\left(b*c\right)=\left(a*b\right)*c$ і $(R;*)$ – напівгрупа.

Приклад 3.2. Довести, що групоїд $(N;*)$, де $a*b=a^b$ для довільних натуральних чисел, є неасоціативним.

Розв'язання

Справді, маємо:

$$a*(b*c)=a*b^c=a^{b^c},\ \left(a*b\right)*c=\left(a^b\right)^c=a^{bc}.$$

Але $a^{b^c} \neq a^{bc}$ у загальному випадку. Наприклад, при a=2, b=2, c=3 одержимо $2^{2^3} = 2^8 \neq 2^{2\cdot 3} = 2^6$. Отже, цей групоїд не є напівгрупою.

Означення 3.5. *Елемент e групоїда називається нейтральним, якщо він задовольняє умову:*

$$\forall a \in G(a * e = e * a = a).$$

Нейтральний елемент e групоїда називають *нульовим* елементом, якщо операція «$*$» є додаванням, і *одиничним* елементом, якщо «$*$» є множенням.

Наприклад, якщо M_n – множина усіх квадратних матриць порядку n з дійсними елементами, то нейтральним елементом напівгрупи $(M_n;+)$ буде нульова квадратна матриця порядку n, а нейтральним елементом напівгрупи $(M_n;\cdot)$ буде одинична матриця порядку n.

Означення 3.6. *Напівгрупа $(G; *)$ з нейтральним елементом називається моноїдом.*

Приклад 3.3. Довести, що (Z;$*$) є моноїдом, якщо $a * b = a + b - 3$ для довільних цілих чисел a і b.

Розв'язання

Безпосередньо з означення випливає, що «$*$» є бінарною алгебраїчною операцією на Z. Покажемо, що вона асоціативна. Справді,

$(a * b) * c = (a + b - 3) * c = a + b - 3 + c - 3 = a + (b + c - 3) - 3 = a * (b * c)$.

Знайдемо нейтральний елемент. Маємо $a * e = a + e - 3 = a$, звідки $e - 3 = 0$, e = 3 – нейтральний елемент. Отже, (Z;$*$) – моноїд.

Теорема 3.1. *Якщо групоїд $(G; *)$ містить нейтральний елемент, то він лише один.*

Доведення. Нехай e_1 і e_2 – два нейтральні елементи групоїда $(G; *)$. Тоді $e_1 = e_1 * e_2 = e_2$ і теорему доведено.

Означення 3.6. *Моноїд $(G;*)$ з нейтральним елементом e, елементи якого задовольняють умову*

$$\forall a \in G\ \exists x \in G(a * x = x * a = e)$$

називається групою.

Елемент x, про який йдеться в означенні, називається *симетричним* до елемента a. При додаванні його називають *протилежним*, а при множенні – *оберненим* елементом до елемента a і позначають відповідно $(-a)$ та a^{-1}.

Теорема 3.2. *У групі $(G;*)$ кожен елемент має лише один симетричний елемент.*

Доведення. Нехай $a * x_1 = x_1 * a = e$ і $a * x_2 = x_2 * a = e$. Тоді $x_1 = x_1 * e = x_1 * (a * x_2) = (x_1 * a) * x_2 = e * x_2 = x_2$.

Теорему доведено.

Об'єднуючи означення 2.1–2.5, одержимо наступне означення групи.

Означення 3.7. *Алгебраїчна система* $(G;*)$ *називається групою, якщо виконуються наступні умови (аксіоми):*

1) $\forall a,b \in G\ \exists! c \in G(a * b = c)$;
2) $\forall a,b,c \in G(a * (b * c) = (a * b) * c)$;
3) $\exists e \in G\ \forall a \in G\ (a * e = e * a = a)$;
4) $\forall a \in G\ \exists x \in G(a * x = x * a = e)$.

Якщо крім аксіом 1)-4) виконується аксіома

5) $\forall a,b \in G\ (a * b = b * a)$,

то група називається *комутативною* або *абелевою* – на честь видатного норвезького математика Н. Г. Абеля.

Якщо множина G нескінченна, то група $(G;*)$ називається *нескінченною*; якщо множина G скінченна, то група $(G;*)$ називається *скінченною*. Число елементів групи називається її *порядком* і позначається $|G|$. Запис $|G| = \infty$ означає, що група нескінченна, а запис $|G| < \infty$ означає, що група скінченна.

Якщо за текстом зрозуміло, яка операція розглядається у групі $(G;*)$, то знак «$*$» опускають і говорять просто: «група G».

Групи з операцією додавання називаються *адитивними*, а з операцією множення – *мультиплікативними*.

Усі наступні теоретичні міркування для зручності будемо проводити для груп з операцією множення, тобто для мультиплікативних груп.

Добуток n елементів групи, кожен з яких дорівнює елементу a, називається n-м *степенем елемента* a і позначається a^n. При цьому очевидно, що $a^0 = e$, $a^n = (a^{-n})^{-1}$, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Якщо $a^k = e$ для деякого числа $k \in N$, виберемо серед усіх натуральних чисел з цією умовою найменше і позначимо його n. Число n називають ***порядком елемента a*** і позначають $|a| = n$. Якщо $a^k \neq e$ для будь-якого натурального числа k, то a називають ***елементом нескінченного порядку***. При цьому записують $|a| = \infty$.

Зауваження. В адитивних групах порядком елемента a називають найменше натуральне число n, що задовольняє умову

$$n \cdot a = \theta,$$

де θ – нульовий елемент групи. Якщо такого $n \in N$ не існує, то говорять, що елемент a має нескінченний порядок.

Якщо порядки всіх елементів групи скінченні, то група називається *періодичною*. Якщо порядки всіх неодиничних елементів групи нескінченні, то група називається *групою без скруту*. Група називається *мішаною*, якщо вона містить неодиничні елементи як скінченного так і нескінченного порядків.

Перейдемо до розгляду прикладів груп.

Приклад 3.4. Алгебраїчні системи $(Z;+)$, $(Q;+)$, $(R;+)$, $(C;+)$ є нескінченними абелевими групами без скруту.

Розв'язання

Справді, виконання аксіом групи означення 2.6 випливає з відомих властивостей додавання чисел. Окрім того, для довільного числа $a \neq 0$ не існує такого натурального n, що $n \cdot a = 0$. Отже, $|a| = \infty$ і кожна з вказаних систем є групою без скруту.

Приклад 3.5. Алгебраїчні системи $(Q\backslash\{0\};\cdot)$, $(R\backslash\{0\};\cdot)$, $(C\backslash\{0\};\cdot)$ є нескінченними мішаними абелевими групами.

Елементом порядку 2 в кожній з цих груп є число –1, бо $(-1)^2=1$. Прикладом елемента нескінченного порядку в кожній з цих груп є число 0,3, бо $(0,3)^n \neq 1$ для будь-якого числа $n \in N$.

Алгебраїчна система $(Z\backslash\{0\},\cdot)$– моноїд, але не група, бо якщо $a \in Z$ і $|a| \neq 1$, то $a^{-1} \notin Z$.

Приклад 3.6. Алгебраїчні системи $(\{1,-1\},\cdot)$, $(\{1,-1,i,-i\},\cdot)$ – скінченні абелеві групи порядків 2 і 4 відповідно. Перша з них є групою коренів другого, а друга – коренів четвертого степеня з одиниці. Неважко переконатись, що $|1| = 1$, $|-1| = 2, |i| = |-i| = 4$.

Приклад 3.7. Множина C_n всіх коренів n-го степеня з одиниці є мультиплікативною абелевою групою порядку n. Справді, відомо, що корені n-го степеня з одиниці обчислюються за формулою

$$\varepsilon_k = cos\frac{2\pi k}{n} + i\, sin\frac{2\pi k}{n},\ k=0,1,\ldots,n-1.$$

При цьому $\varepsilon_k = \varepsilon_1^k$, добуток будь-яких двох коренів n-го степеня з 1 є коренем n-го степеня з одиниці, $\varepsilon_k^{-1} = \varepsilon_{n-k}$, бо $\varepsilon_{n-k} = \varepsilon_1^{n-k}$ і $\varepsilon_k\varepsilon_{n-k} = \varepsilon_1^k\varepsilon_1^{n-k} = \varepsilon_1^n = 1$. Виконання асоціативного та комутативного законів множення для множини C_n гарантується їх виконанням для всіх комплексних чисел. Отже, $(C_n;\cdot)$ – абелева група порядку n.

Приклад 3.8. Нехай $Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ – множина класів лишків по модулю n $(n \in N)$, $\bar{a} = \{a + nt | t \in Z\}$. Сумою класів $\bar{a}$ та $\bar{b}$ назвемо клас лишків по модулю n, що містить число $a + b$:

$$\forall \bar{a}, \bar{b} \in Z_n\left(\bar{a} + \bar{b} = \overline{a+b}\right).$$

Довести, що $(Z_n; +)$ – абелева група порядку n.

Розв'язання

Алгебраїчність додавання класів випливає з означення. Перевірка асоціативності та комутативності додавання класів виконується безпосередньо і зводиться до перевірки відповідних властивостей цілих чисел. Нульовим елементом у Z_n є клас $\bar{0}$, бо для довільного класу

лишків $\bar{a} \in Z_n$ виконується $\bar{0} + \bar{a} = \overline{0 + a} = \bar{a}$. Протилежним до класу $\bar{a}$ є клас лишків $\overline{n - a}$:

$$\overline{a} + \overline{n - a} = \overline{a + (n - a)} = \overline{n} = \overline{0}.$$

Отже, $(Z_n; +)$ – абелева група.

Приклад 3.9. Позначимо $GL_n(R)$ множину всіх невироджених матриць порядку n з дійсним елементами. Тоді $(GL_n(R), \cdot)$ – нескінченна неабелева мішана група.

Розв'язання

Оскільки визначник добутку двох матриць дорівнює добутку їх визначників, то множина $GL_n(R)$ замкнена відносно множення. Крім того, множення матриць асоціативне, некомутативне, кожна невироджена матриця має собі обернену і множині $GL_n(R)$ належить одинична матриця порядку n. Отже, $GL_n(R)$ – нескінченна мультиплікативна неабелева група.

Покажемо, що вона мішана, тобто містить неодиничні елементи скінченного і нескінченного порядків. Справді, матриця n-го порядку

$$\mathrm{A} = \begin{pmatrix} -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

задовольняє умову $A^2=E$ і тому (як елемент групи $GL_n(R)$) є елементом другого порядку, а матриця

$$\mathrm{B} = \begin{pmatrix} 5 & 0 & \dots & 0 & 0 \\ 0 & 5 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 5 \end{pmatrix}$$

задовольняє умову $B^n \neq E$ для будь-якого натурального числа n і тому є елементом нескінченного порядку групи $GL_n(R)$.

Групу $GL_n(R)$ називають *загальною лінійною (матричною)* групою степеня n над полем дійсних чисел R.

3.3. Групи підстановок

Означення 3.8. *Взаємно однозначне відображення скінченної множини, що містить n елементів, на себе називається підстановкою n-го степеня.*

Можна вважати, що підстановка *n*-го степеня відображає на себе множину {1, 2,..., *n*} перших *n* натуральних чисел.

Одна з форм запису підстановок – таблична. Таблиця має два рядки: у верхньому рядку записуються числа від 1 до *n* в натуральному порядку, а в нижньому рядку під кожним числом записують його образ при дії даної підстановки. Запис

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & \text{п} \\ \varphi(1) & \varphi(2) & \dots & \varphi(\text{п}) \end{pmatrix}$$

є записом підстановки (відображення) ϕ:

$$\begin{matrix} 1 & 2 & \dots & \text{п} \\ \downarrow & \downarrow & \dots & \downarrow \\ \varphi(1) & \varphi(2) & \dots & \varphi(\text{п}) \end{matrix}$$

При цьому говорять, що 1 переходить у $\varphi(1)$, 2 – у $\varphi(2)$ і т.д. Оскільки φ – взаємно однозначне відображення, то

$$\{\varphi(1), \varphi(2), \dots, \varphi(\text{п})\} = \{1, 2, \dots, \text{п}\}.$$

Множину всіх підстановок *n*-го степеня позначають S_n, а її елементи – малими грецькими літерами $\alpha, \beta, \gamma, \dots$ Тотожну підстановку позначають ε.

Кількість підстановок n-го степеня дорівнює n!

Композицію підстановок, тобто їх послідовне виконання, називатимемо *множенням підстановок*, а результат множення – *добутком підстановок*.

Приклад 3.10. Знайти добутки $\alpha\beta$ і $\beta\alpha$, якщо

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Розв'язання

За означенням добутку маємо:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Цей приклад показує, що $\alpha\beta \neq \beta\alpha$, тобто множення підстановок не комутативне.

Теорема 3.3. *Множина S_n всіх підстановок n-го степеня утворює мультиплікативну групу порядку $n!$. Ця група неабелева при $n \geq 3$.*

Доведення. З означення добутку підстановок випливає, що операція множення підстановок асоціативна і замкнена на множині S_n.

Одиничним елементом є тотожна підстановка

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & \text{п} \\ 1 & 2 & \dots & \text{п} \end{pmatrix},$$

бо $\alpha\varepsilon = \varepsilon\alpha = \alpha$ для будь-якої підстановки $\alpha \in S_n$.

Оберненою до підстановки $\alpha \in S_n$, яка переводить число i в число j, буде підстановка $\alpha^{-1} \in S_n$, яка переводить число j в число i. Формально α^{-1}можна записати як підстановку, верхній рядок якої є нижнім рядком підстановки α, а нижній – верхнім рядком α.

Отже, $(S_n; \cdot)$ – група порядку $n!$. Оскільки

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

то S_n – неабелева група при $\text{п} \geq 3$. Група $(S_n; \cdot)$ називається *симетричною групою підстановок n-го степеня.*

Приклад 3.11. Записати усі підстановки 3-го степеня та скласти для них таблицю Келі.

Розв'язання

Випишемо підстановки третього степеня (тобто, елементи симетричної групи S_3):

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Заповнимо таблицю множення для групи S_3, яка називається *квадратом Келі*. Для заповнення таблиці перший множник беремо з лівого стовпця, а другий – з верхнього рядка. Результат множення записується на їх перетині.

Наприклад, $\beta \cdot \delta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \gamma.$

	ε	α	β	γ	δ	τ
ε	ε	α	β	γ	δ	τ
α	α	ε	δ	τ	β	γ
β	β	τ	ε	δ	γ	α
γ	γ	δ	τ	ε	α	β
δ	δ	γ	α	β	τ	ε
τ	τ	β	γ	α	ε	δ

3.4. Підгрупи групи. Критерій підгрупи

Означення 3.9. *Підмножина H групи G. називається підгрупою цієї групи, якщо H є групою відносно операції, яка визначена в групі G.*

Запис $H \leq G$ означає, що H – підгрупа групи G.

У будь-якій групі G. її підгрупами є сама група G. та підмножина, що містить лише один нейтральний елемент (одинична підгрупа). Всі інші підгрупи групи G, якщо вони існують, називаються *нетривіальними підгрупами* групи G. Нетривіальна або одинична підгрупа називається *власною підгрупою* групи (у цьому випадку записують $H < G$).

Теорема 3.4. ***(Критерій підгрупи).*** *Підмножина H мультиплікативної групи G тоді і тільки тоді є її підгрупою, коли H замкнена відносно множення та взяття обернених елементів.*

Доведення. Необхідність умов теореми очевидна. Доведемо їх достатність. Якщо H містить добутки своїх елементів та їх обернені елементи, то одиничний елемент $\mathrm{e} = \mathrm{a} \cdot \mathrm{a}^{-1} \in \mathrm{H}$, де $\mathrm{a} \in \mathrm{H}$. Асоціативний закон для елементів множини H виконується, бо H – підмножина групи G. Теорему доведено.

Зауваження. У випадку, коли група адитивна, критерієм підгрупи буде замкненість підмножини відносно додавання та взяття протилежних елементів.

Розглянемо приклади підгруп у групах.

Приклад 3.12. 1) **(***Z*; +) < (*Q*; +) < (*R*; +) < (*C*; +).

2) Нехай $mZ = \{mk \mid k \in Z\}$, де $m \in N$. Тоді (*mZ*; +)<**(***Z*;+).

3) (*Q*\{0}; ·)<(*R*\{0}; ·)<(C\{0}; ·)

Зауваження. Група ({-1,1}; ·) не є підгрупою групи (*Z*;+), бо хоча $\{-1,1\} \subset Z$, проте операції у цих групах різні.

Теорема 3.5. *Перетин будь-якої множини підгруп групи G є підгрупою групи G.*

Доведення. Нехай $S = \{H_i | i \in I\}$ – довільна множина підгруп групи *G*. Позначимо *H* перетин всіх підгруп з множини *S*. Якщо елементи $x \in H, y \in H,$ то вони належать будь-якій підгрупі з множини *S*. Тому *xy* та x^{-1} теж належать усім підгрупам з множини *S*. Значить, $xy \in H$, $x^{-1} \in H$. Отже, *H* –підгрупа групи *G*. Теорему доведено.

3.5. Циклічні групи і підгрупи. Властивості циклічних груп

Нехай *G* – довільна мультиплікативна група і g – будь-який елемент цієї групи. Позначимо $\langle g \rangle$ множину всіх цілих степенів цього елемента, тобто

$$\langle g \rangle = \{g^k | k \in Z\} = \{\dots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \dots\}.$$

Покажемо, що $\langle g \rangle$ – підгрупа групи *G*. Справді, якщо g^m, g^k – довільні елементи з $\langle g \rangle$, то

$$g^m g^k = g^{m+k} \in \langle g \rangle, (g^m)^{-1} = g^{-m} \in \langle g \rangle.$$

За критерієм підгрупи $\langle g \rangle \leq G$. Її називають *циклічною підгрупою, породженою елементом g.*

Означення 3.10. *Підгрупа H мультиплікативної групи G називається циклічною підгрупою, породженою елементом g, якщо будь-який елемент з H є цілим степенем елемента g, тобто H=*$\langle g \rangle$*. Якщо при цьому H=G, то циклічною називають саму групу G.*

Елемент g, що породжує циклічну групу $\langle g \rangle$, називають також *твірним елементом* цієї групи.

Зрозуміло, що будь-яка циклічна група є абелевою, але не кожна абелева група є циклічною. Наприклад, група $(R\backslash\{0\}, \cdot)$ – абелева, але не циклічна.

Якщо порядок твірного елемента g циклічної групи нескінченний, то $\langle g\rangle$ – нескінченна циклічна група.

Нехай $|g| = n$ і g^m – довільний елемент групи $\langle g\rangle$. Розділимо m на n з остачею:

$$m = nq + r,\ r = 0,1,2,..,(n-1)$$

Тоді $g^m = g^{nq+r} = (g^n)^q g^r = g^r$, де $r = 0,1,2,..,(n-1)$. Отже, у цьому випадку циклічна група $\langle g\rangle$ містить n елементів:

$$\langle g\rangle = \{g^0 = e, g, g^2, \dots g^{n-1}\}.$$

Зауваження. У випадку операції додавання циклічна група (підгрупа) складається з цілих кратних твірного елемента, тобто

$$\langle g\rangle = \{kg | k \in Z\} = \{\dots, -2g, -g, 0, g, 2g, \dots\}.$$

Розглянемо два основних приклади циклічних груп.

Приклад 3.13. Група $(Z; +)$ – циклічна, оскільки будь-яке ціле число є кратним 1 або –1. Ніяким іншим числом адитивна група цілих чисел не породжується. Отже, $Z = \langle 1\rangle = \langle -1\rangle$

Приклад 3.14. Група $(C_n;\cdot)$ коренів n-го степеня з одиниці циклічна. Справді, всі корені n-го степеня з одиниці обчислюються за формулою

$$\varepsilon_k = cos\frac{2\pi k}{n} + i\, sin\frac{2\pi k}{n},\ k = 0, 1,\dots, n-1.$$

Оскільки $\varepsilon^k = \varepsilon_1^k$ за формулою Муавра, то $C_n = \langle \varepsilon_1\rangle$ – циклічна група з твірним елементом ε_1. У ролі твірного елемента цієї групи може бути будь-яке $\varepsilon_т$ при умові $(m, n) = 1$.

Приклад 3.15. Адитивна група $Z_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ класів лишків по модулю n $(n \in N)$ циклічна з твіним елементом $\bar{1}$, бо всі її елементи є цілі кратні $\bar{1}$:

$Z_n = \langle \bar{1}\rangle = \{k \cdot \bar{1} |\ k \in Z\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Теорема 3.6. *Будь-яка підгрупа циклічної групи циклічна.*

Доведення. Нехай $G=\langle g\rangle$– циклічна група і H – її підгрупа. Якщо H – одинична підгрупа, то вона циклічна, $H=\langle e\rangle$. Тому припустимо, що H містить неодиничні елементи. Кожний з них є деяким степенем елемента g. Нехай $g^m \in H$. Тоді $g^{-m} \in H$. Одне з чисел m, $-m$ є натуральним. Серед усіх натуральних степенів елемента g, що належать H, виберемо степінь з найменшим натуральним показником. Позначимо його g^k. Нехай g^s – довільний елемент підгрупи H. Розділимо s на k з остачею:

$$s = kq + r, \qquad 0 \le r < k.$$

Тоді

$$g^s = g^{kq+r} = (g^k)^q \cdot g^r.$$

Звідси $g^r = g^s(g^k)^{-q} \in H$. За вибором числа k маємо r=0 і тому $g^s = (g^k)^q$. Отже, $H=\langle g^k\rangle$ – циклічна підгрупа і теорему доведено.

3.6. Ізоморфізми груп

Означення 3.11. *Взаємно однозначне відображення φ групи $(G;*)$ на групу $(H;\circ)$ називається ізоморфним відображенням або ізоморфізмом групи G на групу H, якщо виконується умова:*

$$\forall g_1, g_2 \in G \quad (\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)).$$

Іншими словами, ϕ є *ізоморфним відображенням* групи $(G;*)$ *на* групу $(H;\circ)$, якщо:

1) кожний елемент $h \in H$ має пробраз $g \in G$, тобто $h = \phi(g)$;

2) різні елементи групи G мають різні образи в H і навпаки, тобто

$$\forall g_1, g_2 \in G\big(g_1 \neq g_2 \Leftrightarrow \phi(g_1) \neq \phi(g_2)\big),$$

3) відображення ϕ «зберігає» операцію, тобто

$$\forall g_1, g_2 \in G\ (\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2))..$$

Ізоморфізми групи G на себе називають *автоморфізмами.*

Властивості ізоморфізмів груп

Якщо φ – ізоморфізм групи G на групу H, то:

1) $\varphi(e) = e'$ *– одиничний елемент групи H, де e – одиниця групи G;*

2) $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

3) *обернене відображення* $\varphi^{-1}: H \mapsto G$ *також є ізоморфізмом.*

Доведення. 1) Справді, з умови збереження операції випливає, що $\varphi(e) \circ \varphi(g) = \varphi(e * g) = \varphi(g)$. Отже, $\varphi(e)$ – одиниця групи H.

Означення 3.12. *Групи* G *і* H *називаються ізоморфними (запис* $G \cong H$*), якщо існує ізоморфне відображення однієї групи на іншу.*

Кожна група ізоморфна сама собі: для доведення досить взяти тотожне відображення групи на себе. Отже, відношення ізоморфізму груп рефлексивне. Це відношення також є симетричним: якщо $G \cong H$, то $H \cong G$; і транзитивним: якщо $G \cong H$ і $H \cong K$, то $G \cong K$. Таким чином, відношення ізоморфізму груп є відношенням еквівалентності на множині всіх груп і розбиває цю множину на класи ізоморфних груп.

Групи одного класу можуть відрізнятись одна від одної природою своїх елементів, назвою операції та символікою для її позначення. Проте, з точки зору властивостей операцій, вони однакові: все, що доведено для однієї групи на основі властивостей її операції без використання конкретної природи її елементів, автоматично переноситься на всі групи, що їй ізоморфні. Тим самим алгебраїчна операція виділяється в якості безпосереднього об'єкта вивчення.

Наступні твердження ілюструють роль ізоморфізмів у теорії груп.

Теорема 3.7. *Будь-яка нескінченна циклічна група* $\langle g \rangle$ *ізоморфна адитивній групі (Z; +).*

Доведення. Функція $\varphi(g^n) = n$ є взаємно однозначним відображенням множини $\langle g \rangle$ на множину Z цілих чисел. Рівності

$$\varphi(g^{\text{п}} g^{\text{т}}) = \varphi(g^{\text{п}+\text{т}}) = \text{п} + \text{т} = \varphi(g^{\text{п}}) + \varphi(g^{\text{т}})$$

показують, що це відображення є ізоморфізмом. Теорему доведено.

Теорема 3.8. *Будь-яка циклічна група* $\langle g \rangle$ *порядку n ізоморфна адитивній групі* Z_n *класів лишків по модулю n.*

Доведення. Нехай $\langle g \rangle = \{g^0 = e, g, g^2, \ldots, g^{n-1}\}$ – циклічна група порядку n, $Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ – множина класів лишків по

модулю n $(n \in N)$. Функція $\varphi(g^k) = \bar{k}$ є взаємно однозначним відображенням множини $\langle g \rangle$ на множину Z_n=$\langle \bar{1} \rangle$. Рівності

$$\varphi(g^k \cdot g^m) = \varphi(g^{k+m}) = \overline{k+m} = \bar{k} + \bar{m} = \varphi(g^k) \cdot \varphi(g^m)$$

показують, що це відображення є ізоморфізмом. Теорему доведено.

Отже, *усі циклічні групи одного й того ж порядку (скінченного чи нескінченного) ізоморфні*. Тобто, адитивною групою цілих чисел та мультиплікативною групою коренів з одиниці фактично вичерпуються усі циклічні групи.

3.7. Суміжні класи. Теорема Лагранжа

Нехай *A* і *B* – підмножини мультиплікативної групи *G*.

Означення 3.13. *Добутком підмножини A на підмножину B називається підмножина AB елементів групи G, кожний з яких є добутком дякого елемента підмножини A на деякий елемент підмножини B:*

$$AB = \{x | \, x = ab, a \in A, b \in B\}.$$

Можна довести, що добуток двох підгруп групи *G* не завжди є підгрупою (відповідний приклад можна знайти серед підгруп симетричної групи S_3).

Зокрема, для підгрупи *H* маємо $H \cdot H = H$. Справді, для будь-яких елементів $a, b \in H$ їх добуток $ab \in H$ і тому $H \cdot H \subseteq H$. З іншого боку $a = a \cdot 1 \in H \cdot H$ і тому $H \subseteq H \cdot H$. Отже, $H \cdot H = H$.

Інший важливий випадок добутку двох підмножин групи отримаємо тоді, коли одна з підмножин містить лише один елемент, а друга є підгрупою. Нехай $g \in G$ і $H \leq G$.

Означення 3.14. *Множина* $gH = \{gh | \, h \in H\}$ *називається лівостороннім суміжним класом групи G за підгрупою H. Множина* $Hg = \{hg | \, h \in H\}$ *називається правостороннім суміжним класом групи G за підгрупою H. Кожний елемент класу (лівостороннього чи правостороннього) називається представником цього класу.*

Теорема 3.9. *Нехай H – підгрупа групи G. Тоді:*

1) $\forall g \in G \; (g \in gH)$.

2) *Якщо* $g \in H$, *то* $H = H$.

3) *Суміжний клас* gH *є підгрупою групи G тоді і тільки тоді, коли* $g \in H$.

4) *Якщо підгрупа H – скінченна, то* $|gH| = |H|$.

Аналогічні твердження мають місце й для правосторонніх суміжних класів.

Доведення. 1) Справедливість твердження 1 випливає з означення суміжного класу.

2) Нехай $g \in H$ і gh – довільний елемент з gH. Тоді $gh \in H$, бо H – підгрупа. Отже, $gH \subseteq H$.

Позначимо h_1 – довільний елемент з H. Тоді

$$h_1 = g(g^{-1}h_1) = gh \in gH,$$

де $h = g^{-1}h_1 \in H$. Отже, $H \subseteq gH$. Враховуючи попереднє включення, маємо $gH = H$.

3) Нехай $gH \leq G$. Тоді, очевидно, $e \in gH$ і $e = gh$ для деякого елемента $h \in H$. Звідси $g = h^{=1} \in H$, що й треба довести.

Навпаки: нехай $g \in H$. Тоді за твердженням 2) $gH = H$– підгрупа групи *G*.

4) Розглянемо відображення $h \mapsto gh,\ h \in H$. Неважко переконатись, що воно взаємно однозначне. Тому $|gH| = |H|$.

Теорему доведено.

Теорема 3.10. *Будь-які два лівосторонні суміжні класи групи G за підгрупою H або збігаються, або не мають спільних елементів.*

Доведення. Нехай xH і yH – два суміжних класи групи G за підгрупою H *і* $xH \cap yH \neq \varnothing$. Візьмемо елемент $g \in xH \cap yH$. Тоді $g \in xH$, $g \in yH$ і тому $g = xh_1$, $g = yh_2$, де h_1,$h_2 \in$ H. Отримаємо

$$gH = (xh_1)H = x(h_1H) = xH,\ \ gH = (yh_2)H = y(h_2H) = yH.$$

Отже, $xH = yH$ і теорему доведено.

Доведена теорема показує, що вся група G розпадається на лівосторонні (правосторонні) суміжні класи групи G за підгрупою H.

$$G = H \cup g_1H \cup g_2H \cup \ldots\ \ (G = H \cup Hg_1 \cup Hg_2 \cup \ldots)$$

Це розбиття групи G на класи називається ***лівостороннім (правостороннім) розкладом групи G за підгрупою H.***

Звернемо також увагу на те, Що в адитивних групах запис ліво(право)сторонніх суміжних класів наступний: $g + H$ та $H + g$ відповідно.

Кожне розбиття множини на класи, що не перетинаються, визначає на цій множині деяке відношення еквівалентності: два елементи множини еквівалентні, якщо вони належать одному і тому ж класу. Отже, суміжні класи групи G за підгрупою H є *класами еквівалентності.*

Теорема 3.11. *Два лівосторонні суміжні класи aH і bH групи G за підгрупою H рівні тоді і тільки тоді, коли* $a^{-1}b \in H$.

Два правосторонні суміжні класи Ha і Hb групи G за підгрупою H рівні тоді і тільки тоді, коли $ab^{-1} \in H$.

Таким чином, два елементи a і b групи G еквівалентні (запис: a~b) тоді і тільки тоді, коли $a^{-1}b \in H$ (ліва суміжність) або $ab^{-1} \in H$ (права суміжність) для деякої підгрупи H групи G.

В будь-якій абелевій групі лівосторонні і правосторонні суміжні класи за даною підгрупою збігаються. У таких випадках говорять просто про суміжні класи за тією чи іншою підгрупою.

Розглянемо приклади розкладу групи за підгрупою.

Приклад 3.16. Суміжними класами адитивної групи Z цілих чисел за підгрупою $4Z$ цілих чисел, кратних 4 є:

$$4Z,\ 1+4Z,\ 2+4Z,\ 3+4Z.$$

Приклад 3.17. Записати лівосторонній і правосторонній розклади групи S_3 за підгрупою $\langle\alpha\rangle$ порядку 2 і підгрупою $\langle\delta\rangle$ порядку 3.

Розв'язання

Лівосторонні класи за підгрупою $\langle\alpha\rangle$:

$$\langle\alpha\rangle=\{\varepsilon, \alpha\},\ \beta\langle\alpha\rangle=\{\beta, \tau\},\ \gamma\langle\alpha\rangle=\{\gamma, \delta\}.$$

Отже, лівостороннім розкладом групи S_3 за підгрупою$\langle\alpha\rangle$ є:

$$S_3 = \langle\alpha\rangle \cup \beta\langle\alpha\rangle \cup \gamma\langle\alpha\rangle = \{\varepsilon, \alpha\} \cup \{\beta, \tau\} \cup \{\gamma, \delta\}.$$

Правосторонні класи за підгрупою $\langle\alpha\rangle$:

$$\langle\alpha\rangle=\{\varepsilon, \alpha\},\ \langle\alpha\rangle\beta=\{\beta, \delta\},\ \langle\alpha\rangle\gamma=\{\gamma, \tau\}.$$

Запишемо правосторонній розклад групи S_3 за підгрупою $\langle\alpha\rangle$:

$$S_3 = \langle\alpha\rangle \cup \langle\alpha\rangle\beta \cup \langle\alpha\rangle\gamma = \{\varepsilon, \alpha\} \cup \{\beta, \delta\} \cup \{\gamma, \tau\}$$

Лівосторонні класи за підгрупою $\langle\delta\rangle$:

$$\langle\delta\rangle=\{\varepsilon,\delta,\tau\},\ \ \alpha\langle\delta\rangle=\{\alpha,\beta,\gamma\}$$

Правосторонні класи за підгрупою $\langle\delta\rangle$:

$$\langle\delta\rangle=\{\varepsilon,\delta,\tau\},\ \langle\delta\rangle\alpha =\{\alpha,\gamma,\beta\}.$$

Запишемо лівосторонні та правосторонні розклади групи S_3 за підгрупою $\langle\delta\rangle$:

$$S_3 = \langle\delta\rangle \cup \alpha\langle\delta\rangle = \{\varepsilon, \delta, \tau\} \cup \{\alpha, \beta, \gamma\}$$

$$S_3 = \langle\delta\rangle \cup \langle\delta\rangle\alpha = \{\varepsilon, \delta, \tau\} \cup \{\alpha, \beta, \gamma\}$$

Отже, в неабелевих групах існують підгрупи, для яких лівосторонні суміжні класи збігаються з відповідними правосторонніми суміжними класами (тут це суміжні класи за підгрупою $\langle\delta\rangle$).

Очевидно, у кожній групі G між множинами лівосторонніх і правосторонніх суміжних класів за підгрупою H можна встановити взаємно однозначну відповідність, наприклад так: $gH \leftrightarrow Hg$. Це дозволяє ввести нове поняття.

Означення 3.15. *Кількість суміжних класів (лівосторонніх або правосторонніх) групи G за підгрупою H називається індексом підгрупи H у групі G. Якщо ця кількість нескінченна, то говорять, що підгрупа H має нескінченний індекс.*

Індекс підгрупи H у групі G позначається |G : H |.

Приклад 3.18. 1) Індекс підгрупи $4Z$ чисел кратних 4 у групі Z цілих чисел дорівнює 4, бо є всього 4 різних суміжних класи за цією підгрупою (див. приклад 3.16).

2) $|S_3 : \langle\alpha\rangle| = 3,\ |S_3 : \langle\delta\rangle| = 2$ (приклад 3.17)

Теорема 3.12. ***(Лагранжа)*** *Якщо H – підгрупа скінченної групи G, то добуток порядку підгрупи H на її індекс у групі G дорівнює порядку групи G:*

$$|G| = |H| \cdot |G : H|.$$

Доведення. Оскільки кожний суміжний клас gH містить стільки ж елементів, скільки їх у підгрупі H, а різні суміжні класи не мають спільних елементів, то порядок групи G можна підрахувати шляхом

множення числа елементів у суміжному класі на кількість класів, тобто

$$|G| = |H| \cdot |G:H|$$

Теорему доведено.

З цієї теореми випливає кілька важливих наслідків.

Наслідок. *Порядок і індекс підгрупи скінченної групи є дільниками порядка групи.*

Наслідок. *Порядок будь-якого елемента скінченної групи є дільником порядка групи.*

Доведення. Нехай елемент $g \in G$ і $|G| < \infty$.Тоді $|g| = |\langle g \rangle|$ і тому $|G|$ ділиться на $|g|$ за попереднім наслідком.

Наслідок. *Будь-яка група G простого порядку циклічна.*

Доведення. Візьмемо довільний неодиничний елемент групи G. За першим наслідком з теореми Лагранжа порядок циклічної підгрупи $\langle g \rangle$ є відмінним від 1 дільником простого числа $|G|$. Це можливо лише за умови $|G|=|\langle g \rangle|$. Тому $G = \langle g \rangle$ – циклічна група.

Наслідок. *Число 6 є найменшим серед порядків неабелевих груп.*

Доведення. Пересвідчимося в тому, що будь-яка група абелева, якщо її порядок менше 6. Це очевидно для груп порядків 1, 2, 3, 5, бо вони циклічні за попереднім наслідком.

Покажемо, що будь-яка група G порядку 4 абелева. Якщо $g \in G$ і $|g| = 4$, то $G = \langle g \rangle$ – циклічна група і тому абелева. Припустимо, що G не містить елементів порядку 4. Оскільки порядки елементів групи є дільниками порядку групи, то вона містить одиницю e і 3 елементи порядку 2. Нехай $|a| = |b| = 2$. Звідси $ab \neq a$, $ab \neq b$, але $ab = ba$, бо інакше група G містила б не менше 5 елементів. Отже, $G = \{e, a, b, ab\}$ і G – абелева група.

Серед груп порядку 6 є неабелева (приклад –група S_3).

3.8. Нормальні підгрупи. Фактор-групи

Як було зазначено вище, групи можуть мати підгрупи, лівосторонні та правосторонні розклади за якими різні, так і підгрупи,

лівосторонні і правосторонні розклади за якими збігаються. Останні з названих підгруп відіграють у теорії груп особливу роль.

Означення 3.16. *Підгрупа H групи G називається нормальною підгрупою, якщо для будь-якого елемента $g \in G$ виконується умова*

$$gH = Hg.$$

У математичній літературі для нормальних підгруп вживаються також терміни «нормальний дільник» або «інваріантна підгрупа». Якщо підгрупа H нормальна у групі G, то це записують так: $H \lhd G$.

Нормальна в групі G підгрупа H є нормальною в усіх підгрупах, які її містять, тобто якщо $H \leq K \leq G$ і $H \lhd G$, то $H \lhd K$. Проте, з умов $H \lhd K$ і $K \lhd G$ зовсім не випливає, що $H \lhd G$.

Теорема 3.13. *Підгрупа H групи G нормальна в G тоді і тільки тоді, коли вона збігається з усіма своїми спряженими підгрупами, тобто*

$$H \lhd G \Leftrightarrow \forall g \in G \quad (g^{-1}Hg = H).$$

Доведення. З рівності $gH=Hg$ маємо $H=g^{-1}Hg$, що й треба довести.

Теорема 3.14. ***(Критерій нормальності підгрупи)*** *Підгрупа H групи G нормальна в G тоді і тільки тоді, коли разом з кожним своїм елементом вона містить усі елементи,* ***спряжені*** *з ним у групі G, тобто*

$$\forall g \in G \; \forall h \in H \; g^{-1}hg \in H.$$

Доведення. Нехай $H \lhd G$. Тоді для будь-якого елемента $g \in G$ за означенням $gH=Hg$. Звідси $g^{-1}Hg = H$ і тому $g^{-1}hg \in H$ для кожного елемента $h \in H$.

Навпаки, нехай $g^{-1}hg \in H$ для будь-яких елементів $g \in G$ і $h \in H$. Тоді $g^{-1}hg = h_1 \in H$. Звідси $hg = gh_1$ і тому $Hg \subseteq gH$.

Аналогічно $(g^{-1})^{-1}hg^{-1} = h_2$, $gh = h_2g$ і $gH \subseteq Hg$. Отже, $gH = Hg$, тобто $H \lhd G$ і теорему доведено.

Розглянемо приклади нормальних підгруп у групах.

Приклад 3.19. У кожній групі G сама група G та її одинична підгрупа E – нормальні підгрупи. Якщо група не містить інших

нормальних підгруп, то вона називається *простою групою*. До простих груп відносяться, зокрема, усі циклічні групи простого порядку.

Приклад 3.20. В симетричній групі S_3, підстановок третього степеня підгрупа $\langle\delta\rangle$ порядку 3 нормальна, бо лівосторонній і правосторонній розклади групи S_3 за підгрупою $\langle\delta\rangle$ збігаються, а підгрупа $\langle\alpha\rangle$ не є нормальною, бо не задовольняє означенню нормальної підгрупи (див. приклад 3.17).

Приклад 3.21. В групі $GL_n(R)$ невироджених матриць порядку n з дійсними елементами підгрупа $SL_n(R)$ матриць, визначник яких дорівнює 1, нормальна.

Це випливає з того, що для будь-яких матриць $X \in GL_n(R)$, $A \in SL_n(R)$ за теоремою про визначник добутку матриць маємо

$$|X^{-1}AX| = |X^{-1}| \cdot |A| \cdot |X| = |X^{-1}| \cdot |X| \cdot |A| = |A| = 1$$

і тому $X^{-1}AX \in SL_n(R)$. За критерієм нормальності

$$SL_n(R) \lhd GL_n(R).$$

Виняткова роль нормальних підгруп у групах пояснюється тим, з кожною такою підгрупою можна пов'язати нову групу, елементами якої будуть суміжні класи.

Нехай H $\lhd G$. Тоді:

1) $\forall g_1, g_2 \in G \ \ (g_1H \cdot g_2H = g_1g_2H)$
2) $\forall g_1, g_2, g_3 \in G \ \ ((g_1H \cdot g_2H) \cdot g_3H = g_1H \cdot (g_2H \cdot g_3H))$
3) $\forall g \in G \ \ (gH \cdot H = H \cdot gH = gH)$
4) $\forall g \in G \ \ (gH \cdot g^{-1}H = g^{-1}H \cdot gH = H)$

Отже, має місце наступне твердження.

Теорема 3.15. *Множина суміжних класів групи G за нормальною підгрупою H є групою відносно множення суміжних класів.*

Ця група називається *фактор-групою групи* G за нормальною підгрупою H і позначається G/H. Роль одиниці у фактор-групі G/H відіграє H, а оберненим до суміжного класу gH є клас $g^{-1}H$.

Розглянемо деякі властивості фактор-груп.

Теорема 3.16. *Порядок довільної фактор-групи G/H скінченної групи G є дільником порядку групи G.*

Доведення. Число елементів фактор-групи G/H дорівнює індексу $|G:H|$. Далі залишилось застосувати теорему Лагранжа.

Теорема 3.17. *Будь-яка фактор-група абелевої групи G абелева.*

Доведення. Нехай G – абелева група і $H \lhd G$. Оскільки $xy=yx$ для будь-яких елементів $x, y \in G$, то

$$xyH = xH \cdot yH = yxH = yH \cdot xH,$$

що і треба було довести.

Теорема 3.18. *Будь-яка фактор-група циклічної групи циклічна.*

Доведення. Нехай $G=\langle g\rangle$ – циклічна група і $H \lhd G$. Візьмемо будь-який елемент xH фактор-групи G/H. Тоді $x = g^k$ для деякого цілого числа k. Отже, $xH = g^kH = (gH)^k$ і тому $G/H=\langle gH\rangle$ – циклічна група. Теорему доведено.

Приклад 3.21. Адитивна група Z цілих чисел циклічна: $Z=\langle 1\rangle$. Її підгрупа $4Z$ цілих чисел, кратних 4, нормальна в Z. Тому фактор-група $Z/4Z=\{4Z, 1+4Z, 2+4Z, 3+4Z\}$ також циклічна:

$$Z/4Z = \langle 1 + 4Z\rangle \cong Z_4.$$

3.9. Гомоморфізми груп

Поняття нормальної підгрупи і фактор-групи тісно пов’язані з наступним узагальненням поняття ізоморфізму груп.

Означення 3.17. *Однозначне відображення φ групи $(G; *)$ на групу $(H; \circ)$ називається гомоморфним відображенням або гомоморфізмом G на G_1, якщо виконується умова*

$$\forall g_1, g_2 \in G\ (\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)).$$

Якщо існує гомоморфне відображення групи G на групу H то говорять, що група G *гомоморфна* групі H (запис $G \cong H$).

Порівнюючи означення ізоморфізму та гомоморфізму груп, помічаємо, що кожний ізоморфізм є гомоморфізмом, а гомоморфізм φ

тоді і тільки тоді є ізоморфізмом, коли φ – взаємно однозначне відображення однієї групи на іншу.

Приклад 3.22. Довести, що групи $(Z;+)$ і $(C_2;\cdot)$ гомоморфні.

Розв'язання

Розглянемо функцію $\varphi: Z \mapsto C_2 = \{1, -1\}$, що діє на множині цілих чисел Z за правилом:

$$\varphi(n) = \begin{cases} 1, \text{ якщо } n = 2k,\ k \in Z \\ -1, \text{ якщо } n = 2k+1,\ k \in Z \end{cases}.$$

Ця функція є однозначним відображенням множини Z на множину $C_2=\{-1, 1\}$. Оскільки

$$\varphi(n+m) = \varphi(n)\varphi(m)$$

для будь-яких цілих чисел, то відображення φ – гомоморфізм. Отже, $Z \simeq C_2$.

Приклад 3.23. Довести, що групи $GL_n(R)$ і $(R \setminus \{0\},\cdot)$ гомоморфні.

Розв'язання

Розглянемо відображення, яке кожній матриці $A \in GL_n(R)$ зіставляє її визначник $|A|$:

$$\varphi(A) = |A|.$$

Оскільки кожне дійсне число $a \neq 0$ має при цьому відображенні прообраз, наприклад, матрицю

$$\begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

то різним дійсним числам відповідають різні матриці. Отже, φ – однозначне відображення групи $GL_n(R)$ ***на*** групу $R \setminus \{0\}$. Крім того, для будь-яких матриць $A, B \in GL_n(R)$ мають місце рівності

$$\varphi(A \cdot B) = |A \cdot B| = |A| \cdot |B| = \varphi(A) \cdot \varphi(B).$$

Отже, φ – гомоморфізм групи $GL_n(R)$ на групу $R \setminus \{0\}$.

Теорема 3.19. (*Властивості гомоморфізмів груп***)** *Якщо φ – гомоморфізм групи G в H, e та x – відповідно одиничний та довільний елементи групи G, то:*

1) $\varphi(e) = e'$ – *одиничний елемент групи H;*
2) $\varphi(x^{-1}) = (\varphi(x))^{-1}$.
3) *образ* $\varphi(G)$ *групи G є підгрупою групи H.*

Доведення. 1) Нехай y' – довільний елемент групи H. Тоді в групі G існує його прообраз y. Отже,

$$y' = (y) = \varphi(y \cdot e) = \varphi(y)\varphi(e) = y' \cdot \varphi(e).$$

Звідси $\varphi(e) = e'$– одиничний елемент групи H.

2) Використовуючи доведену рівність $\varphi(\mathrm{e}) = e'$ маємо:

$$e' = \varphi(e) = \varphi(x \cdot x^{-1}) = \varphi(x)\varphi(x^{-1}).$$

Звідси $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

4) Нехай x' та y' – довільні елементи з множини $\varphi(G)$. Тоді $x' = \varphi(x), y' = \varphi(y)$, де $x, y \in G$. Оскільки $x'y' = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(G)$, $(x')^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1}) \in \varphi(G)$, то за критерієм підгрупи $\varphi(G)$ – підгрупа в H.

Теорема 3.20. *Будь-яку групу G можна гомоморфно відобразити на її фактор-групу* G/H.

Доведення. Очевидно, що відображення $\phi(g) = gH$ групи G на фактор-групу G/H є однозначним. Оскільки

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H \cdot g_2 H = \phi(g_1) \cdot \phi(g_2),$$

то ϕ зберігає операцію і є гомоморфізмом. Теорему доведено.

Гомоморфізм групи G на її фактор-групу називається *природним гомоморфізмом.* Далі буде показано, що всі групи, на які задана група може гомоморфно відобразитись, з точністю до ізоморфізму вичерпуються її фактор-групами.

Означення 3.18. *Ядром гомоморфізму* φ *групи G на групу H називається повний прообраз* e' *одиниці групи H, тобто множина тих елементів групи G, які відображаються на одиницю* e' *групи H.*

Теорема 3.21. *Нормальні підгрупи групи G і тільки вони є ядрами її гомоморфізмів.*

Доведення. Спочатку доведемо, що ядро K деякого гомоморфізму φ групи G на групу H є нормальною підгрупою групи G. Візьмемо будь-які елементи $x, y \in K$. Тоді за умовою $\varphi(x) = \varphi(y) = \mathrm{e}'$, де e' – одиниця групи H. Звідси

$$\varphi(xy) = \varphi(x)\varphi(y) = e'e' = e'.$$

Отже, $xy \in K$. Одиничний елемент $e \in G$ також належить до K, бо $\varphi(e) = e'$. Якщо $x \in K$, то $x^{-1} \in K$, бо

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = (e')^{-1} = e'.$$

Підсумовуючи, робимо висновок, що ядро K є підгрупою.

Покажемо, що $K \lhd G$. Для цього застосуємо критерій нормальності підгрупи. Нехай $g \in G,\ x \in K$, тоді:

$$\varphi(g^{-1}xg) = (\varphi(g))^{-1}\varphi(x)\varphi(g) = (\varphi(g))^{-1}e'\varphi(g) = e'.$$

Це означає, що $g^{-1}xg \in K$ і $K \lhd G$.

Доведемо тепер, що кожна нормальна підгрупа H групи G є ядром деякого гомоморфізму φ групи G. Справді, візьмемо фактор-групу G/H і розглянемо відображення $\varphi(g) = gH$ групи G на групу G/H. За теоремою 3.20 це відображення є гомоморфізмом. Одиничним елементом групи G/H є елемент H. Якщо $\varphi(x) = xH = H$, то $x \in H$.

Навпаки, для будь-якого елемента $h \in$ H його образ $\varphi(h) = hH = H$. Отже, ядро досліджуваного гомоморфізму збігається з нормальною підгрупою H. Теорему доведено.

Теорема 3.22. ***(Основна теорема про гомоморфізми)*** *Якщо φ – гомоморфізм групи G на групу H з ядром K, то $\varphi(G) = H \cong G/K$. При цьому гомоморфізм φ рівносильний послідовному виконанню природного гомоморфізму $\sigma: G \to G/K$, а потім деякого ізоморфізму $\tau: G/K \to H$.*

ІНДИВІДУАЛЬНІ РОБОТИ

Індивідуальна робота №1

Завдання 1. Довести, що для довільного натурального числа n:

1) $(n^4+6n^3+11n^2+6n)\vdots 24$;
   $(11^{n+2}+12^{2n+1})\vdots 133$.
2) $(n^5-5n^3+4n)\vdots 120$;
   $(3^{2n+3}+40n-27)\vdots 64$.
3) $(10^{n+1}-9n-10)\vdots 81$;
   $(n^7-n)\vdots 42$.
4) $(10^n-4^n+3n)\vdots 9$;
   $(n+1)(n+2)...(n+n)\vdots 2^n$.
5) $(2^{2n-1}-9n^2+21n-14)\vdots 27$;
   $(n^9-n^5)\vdots 10$.
6) $(n^4-2n^3-n^2+2n)\vdots 12$;
   $(6^{2n}-1)\vdots 35$.
7) $(n^5-15n^4-6n)\vdots 5$;
   $(7^{n+2}+8^{2n+1})\vdots 57$.
8) $(n^3+3n^2+2n)\vdots 3$;
   $(3^{3n+2}+5\cdot 2^{3n+1})\vdots 19$.
9) $(n^5+4n+5)\vdots 5$;
   $(3^{2n+2}-8n-9)\vdots 16$.
10) $(n^5-10n^3+9n)\vdots 10$;
    $(5^{2n+1}+2^{n+4}+2^{n+1})\vdots 23$.

Завдання 2. Довести подільність:

1) $(26^{26}-14^{14})\vdots 10$;
2) $(26^{30}-1)\vdots 5$;
3) $(8\cdot 23^{23}-71\cdot 32^{32})\vdots 10$;
4) $(3^{10}+3^5+1)\vdots 13$;
5) $(43^{43}-17^{17})\vdots 10$;
6) $(2^{18}+3^{18})\vdots 13$;
7) $(11^{10}-1)\vdots 100$;
8) $(17^{72}-1)\vdots 10$;
9) $(2+2^2+2^3+...+2^{100})\vdots 3$;
10) $(8^{100}-10+7!)\vdots 9$.

Завдання 3. Довести, що число є складеним:

1) $(n^4+4n^2-5), n>1$
3) $(n^4+4), n\neq\pm1$;4)
   $(4n^4+5n^2+1), n\in N$;
5) $(n^4+n^2+1), n>1$;
6) $(n^3+n-2), n>2$;
2) $(2^{30}-1)$;
7) $(2n^3-n^2+3), n>1$
8) $(n^8+4), n\neq\pm1$;
9) $(n^4+324), n\in N$;
10) $(n^8+n^4+1), n>1$.

Завдання 4.

1) Знайти найменше натуральне число, що ділиться на 41, а при діленні на 39 дає остачу 24.

2) При діленні числа a на 9 неповна частка дорівнює 8. Знайти найбільше значення a.

3)Число a при діленні на 2 дає остачу 1, а при діленні на 3 остачу 2. Яку остачу дає a при діленні на 6?

4) Знайти найбільше натуральне число, що ділиться націло на 21, а при діленні на 15 дає в остачі 12.

5) Знайти всі натуральні числа, при діленні яких на 9 число, отримане у частці, на 1 більше за остачу.

6) Число a при діленні на 3 дає остачу 2, а при діленні на 4 остачу 3. Яку остачу дає a при діленні на 12?

7) Число a при діленні на 12 дає остачу 9. Яку остачу дає a при діленні на 6?

8)Число a при діленні на 9 дає остачу 1. Яку остачу дає $2a$ при діленні на 6?

9) Знайти усі натуральні числа при діленні яких на 7 часка удвічі більша за остачу.

10) Число a при діленні на 5 дає в остачі 1. Яку остачу дасть a^2 пр и діленні на 5?

Завдання 5. Знайти просте число p, щоб одночасно були простими числа:

1) $p+2$, $p+4$;
2) $2p+7$, $5p+2$;
3) p^2-1;
4) $8p^2+1$;
5) p^2+14;
6) $p+10$, $p+14$;
7) $p+14$, $p+16$;
8) $2p+1$, $4p+1$;
9) $p+4$, $p+14$;
10) $4p^2+5$.

Завдання 6. Довести, що вказані числа одночасно простими бути не можуть:

1) $m+5$ та $m+10$, $m \in N$;
2) m, $m+2$ та $m+5$, $m \in N$;
3) $m+2$ та $m+7$, $m \in N$;
4) $2^m - 1$ та $2^m + 1, m > 2$;
5) m, $m+3$ та $m+6$, $m \in N$;
6) $m+3$ та $m+10$, $m \in N$;
7) $m+2$ та $m+7$, $m \in N$;
8) m та $m+7$, $m \in N$;
9) $7m+1$ та m, $m \in N$;
10) 2^m+1 та $2^m + 4$, $m \in N$.

Завдання 7. Знайти n послідовних складених чисел, якщо:

1) $n = 11$;
2) $n = 12$;

3) $n = 13$;
4) $n = 9$;
5) $n = 15$;
6) $n = 17$;
7) $n = 14$;
8) $n = 10$;
9) $n = 16$;
10) $n = 18$.

Завдання 8. Довести, що для довільних цілих чисел n і m виконуються наступні рівності:

1) $(n,m)=(n+2m, 3n+5m)$;
2) $(n,m)=(4n+3m, 5n+4m)$;
3) $(n,m)=(3n+5m, 8n+13m)$;
4) $(n,m)=(2n+3m, 3n+4m)$;
5) $(n,m)=(7n+5m, 4n+3m)$;
6) $(n,m)=(2n+3m, 3n+5m)$;
7) $(n,m)=(n+7m, n+6m)$;
8) $(n,m)=(2n+5m, 7n+17m)$;
9) $(n,m)=(7n+3m, 5n+2m)$;
10) $(n,m)=(7n+3m, 9n+4m)$.

Завдання 9.

1) Знайти усі натуральні значення n, при яких дріб $\frac{11n+9}{4n+3}$ нескоротний.

2) Довести, що для будь-якого $n \in N$ дріб $\frac{21n+4}{14n+3}$ нескоротний.

3) Знайти усі натуральні числа n, при яких дріб $\frac{6n+4}{9n+5}$ нескоротний

4) Знайти усі значення $n \in N$, при яких дріб $\frac{5n+2}{7n+5}$ є скоротним.

5) Визначити, при яких значеннях $n \in N$ дріб $\frac{2n+2}{5n+3}$ скоротний.

6) Довести, що для будь-якого $n \in N$ дріб $\frac{3n+1}{12n+5}$ нескоротний.

7) Визначити, при яких значеннях $n \in N$ дріб $\frac{15n+6}{18n+4}$ нескоротний.

8) Визначити, при яких значеннях $n \in N$ дріб $\frac{14n+5}{10n+3}$ є скоротним.

9) Визначити, при яких значеннях $n \in N$ дріб $\frac{3n+7}{5n+12}$ є скоротним.

10)Довести, що для будь-якого $n \in N$ дріб $\frac{5n-1}{10n+3}$ нескоротний.

Завдання 10. Знайти натуральні числа n і m, якщо:

1) $\begin{cases} n+m=12, \\ (n,m)=2 \end{cases}$;

2) $\begin{cases} nm=48, \\ (n,m)=2 \end{cases}$;

3) $\begin{cases} n+m=168, \\ (n,m)=24 \end{cases}$;

4) $\begin{cases} nm=720, \\ (n,m)=4 \end{cases}$;

5) $\begin{cases} n^2+m^2=52, \\ (n,m)=2 \end{cases}$;

6) $\begin{cases} n^2+m^2=45, \\ (n,m)=3 \end{cases}$;

7) $\begin{cases} \frac{m}{n}=\frac{5}{7}, \\ (n,m)=4 \end{cases}$

8) $\begin{cases} \frac{m}{n}=\frac{11}{7}, \\ (n,m)=45 \end{cases}$

9) $\begin{cases} [n,m]=36, \\ (n,m)=6 \end{cases}$

10) $\begin{cases} [n,m]=24, \\ nm=48 \end{cases}$

Завдання 11. Знайти натуральне число n, якщо:

1) $n \vdots 12, \tau(n)=14$;

2) $n=pq^2$ та $\sigma(n)=39$.

3) $n=p^k, \sigma(n)=15$, p – просте число;

4) n має лише два прості дільники і $\tau(n)=12, \sigma(n)=28$;

5) n – найменше, для якого $\tau(n)=100$;

6) n – найменше, для якого $\tau(n)=12$;

7) $\tau(n)=6$;

8) $\tau(n)=5, \sigma(n)=31$,

9) n має лише два прості дільники і $\tau(n)=12, \sigma(n)=465$;

10) n – найменше, для якого $\sigma(n)=28$.

Завдання 12. Визначити, скількома нулями закінчується число n та з'ясувати, чи ділиться воно на 2^{1000}:

1) n=2007!;

2) n=1998!;

3) n=2000!;

4) n=1990!;

5) n=1999!;

6) n=1991!;

7) n=2005!;

8) n=1997!;

9) n=2009!;

10) n=1994!.

Завдання 13. Побудувати графіки функцій $\tau(n), \sigma(n), \varphi(n)$:

1) $1 \le n \le 16, n \in N$;

2) $6 \le n \le 22, n \in N$;

3) $10 \le n \le 26, n \in N$;
4) $3 \le n \le 19, n \in N$;
5) $7 \le n \le 23, n \in N$;
6) $5 \le n \le 21, n \in N$;
7) $4 \le n \le 17, n \in N$;
8) $8 \le n \le 24, n \in N$;
9) $9 \le n \le 25, n \in N$;
10) $2 \le n \le 18, n \in N$.

Завдання 14. Побудувати графіки функцій:

1) $y = \left[\frac{1}{x}\right]$; $y = \{x^2\}$;
2) $y = \frac{[x]}{x}$; $y = \{x+1\} - 1$;
3) $y = [x^2]$, $y = \frac{\{x\}}{[x]}$
4) $y = [x] + x$, $y = \frac{[x]}{x^2}$
5) $y = \frac{x^2}{[x]} + 2$; $y = \{x\} + x$;
6) $y = [x] + 2$; $y = \left\{\frac{1}{x}\right\}$
7) $y = \{x\}[x]$; $y = \left\{\frac{x}{2}\right\}$;
8) $y = \frac{x^2}{[x]} + 2$; $y = \{x\} + x$;
9) $y = 2[x^2]$; $y = \{x^2 - 1\}$;
10) $y = \frac{x}{[x]} + 1$; $y = \{2x\}$.

Завдання 15. Знайти кількість натуральних чисел, що:

1) не перевищують 10000 і не діляться ні на 6, ні на 9;
2) менші за 1000 і взаємно прості з 36;
3) менші за 1000 і не діляться ні на 2, ні на 5, але діляться на 3.
4) не перевищують 1000 і не діляться ні на 3, ні на 5, ні на 10.
5) менші за 1000 і не діляться ні на 5, ні на 6, але діляться на 4.
6) не більші за 1000, діляться на 36, але не діляться на 5;
7) менші за 1000 і не діляться ні на 5, ні на 7, ні на 15;
8) менші за 1000 і взаємно прості з 15;
9) не більші за 1000, діляться на 18, але не діляться на 7;
10) менші за 1000 і не діляться ні на 3, ні на 7, але діляться на 2.

Завдання 16. Знайти натуральне число *n*, якщо

1) $\varphi(n) = 378, n = 3^k 7^m, k, m \in N$;
2) $\varphi(n) = 440, n = 2^k 11^m, k, m \in N$;
3) $\varphi(n) = 120, n = p^k q^m, k, m \in N$, p,q – різні прості числа;
4) $\varphi(n) = 294, n = 7^m, m \in N$;
5) $\varphi(n) = 946, n = 3^k \cdot 13^m, k, m \in N$.

6) $\varphi(n)=6p^{k-2}$, $n=p^k$, $k\in N$ p – просте число;

7) $\varphi(n)=1680, n=5^k7^m11, k,m\in N$;

8) $\varphi(n)=252, n=p^2q^2$, p,q – різні прості числа;

9) $\varphi(n)=289, n=pq, p-q=2$, p,q – різні прості числа;

10) $\varphi(n)=36, n=p^3q^2$, p,q – різні прості числа.

Завдання 17. Розв'язати рівняння:

1) $\left[x^2-4\right]=2;$

2) $\left[x^2\right]=x+2;$

3) $\left[x+1\right]=\left[\frac{x-1}{2}\right];$

4) $\left[x^2\right]=x;$

5) $\left[x^2\right]=2x+3;$

6) $\left[x+3\right]=\frac{x-2}{2};$

7) $\left[x^3\right]=2-x;$

8) $\left[2x^2+x\right]=5-2x;$

9) $\left[x\right]=\frac{2x}{3};$

10) $\left\lfloor x^{2008}\right\rfloor+\left\lfloor x^{2007}\right\rfloor+\ldots\left[x\right]=\{x\}-1;$

Завдання 18. Знайти значення функції $\tau(n^3)$, якщо:

1) $\tau(n)=6$;

2) $\tau(n^2)=27$ і n має лише два прості дільники;

3) $\tau(n)=12$ і n має три прості дільники;

4) $\tau(n^2)=165$ і n має три прості дільники;

5) $\tau(n^4)=35$ і n має лише два прості дільники;

6) $\tau(n)=10$;

7) $\tau(n^2)=21$ і n має лише два прості дільники;

8) $\tau(n^2)=9$ і n має лише два прості дільники;

9) $\tau(n^2)=27$ і n має три прості дільники;

10) $\tau(n^2)=15$ і n має два прості дільники.

Завдання 19. Знайти основу системи числення g, якщо:

1) $401_g=265_7$;

2) $502_g=151_9$

3) $364_g=3001_4$;

4) $100_g=34_7$;

5) $103_g=151_6$;

6) $324_g=10022_3$;

7) $541_g=2014_6$;

8) $236_g=1240_5$;

9) $203_g=53_{10}$;

10) $106_g=153_7$

Завдання 20. Перевести з однієї системи числення в іншу:

1) $2042_5 \to x_9, x_3$;
2) $21211_3 \to x_6, x_2$;
3) $2786_9 \to x_5, x_{12}$;
4) $101111_2 \to x_9, x_6$;
5) $8762_9 \to x_7, x_3$;
6) $1234_6 \to x_8, x_3$;
7) $2467_8 \to x_9, x_6$;
8) $1045_6 \to x_7, x_3$;
9) $11221_3 \to x_8, x_2$;
10) $13231_4 \to x_7, x_3$.

Завдання 21. Виконати дії:

1) $(351_6 \cdot 14_6 - 1153_6 : 31_6 - 150_6) : 25_6$;
2) $(215_8 + 532_8) \cdot 16_8 - (11031_8 - 527_8) : 32_8$;
3) $3215_7 \cdot 24_7 - 11461_7 : 25_7 + 1532_7 - 115047_7$;
4) $(4123_8 - 4221_8) \cdot 11_8 + (1222_8 + 772_8) : 3_8$;
5) $(3333_4 + 2222_4) \cdot 12_4 - (231020_4 + 3333311_4) : 23_4$;
6) $(351_7 \cdot 14_7 - 1144_7 : 65_7 - 150_7)$;
7) $(215_9 + 532_9) \cdot 16_9 - (11071_9 - 526_9) : 337_9$;
8) $3215_6 \cdot 24_6 - 3531_6 : 205_6 + 1532_6 - 15041_6$;
9) $(4123_5 - 4221_5) \cdot 11_5 + (1222_5 + 443_5) : 20_5$;
10) $(1111_3 + 2222_3) \cdot 12_3 - (21020_3 + 111112_3) : 101_3$;

Індивідуальна робота №2

Завдання 1. Використовуючи теореми Ейлера та Ферма, знайти остачі від ділення:

1) $\left(7 \cdot 45^{90} + 5 \cdot 54^{30}\right)^{100}$ на 11;
2) $8 \cdot 10^{100} + 11^{200}$ на 17;
3) $13 \cdot 115^{47} + 15 \cdot 114^{48}$ на 17;
4) $5 \cdot 2^{1101} - 3^{101}$ на 101;
5) $7 \cdot 315^{41} + 6^{320}$ на 11;
6) $\left(2005^{2009} + 2009^{2005}\right)^{2000}$ на 13;
7) $2^{1600} + 3^{3200} + 5^{480}$ на 17;
8) $3 \cdot 513^{111} + 7 \cdot 49^{320}$ на 1;
9) $35\left(41^{100} + 5 \cdot 142^{200}\right)$ на 21.
10) $6\left(14^{150} + 341^{291}\right)$ на 45.

Завдання 2. Знайти дві останні цифри числа:

1) 23^{130};
2) 13^{159}:
3) 42^{555};
4) 1007^{1008};
5) 67^{444};
6) 98^{999};
7) 989^{989};
8) 2008^{200};
9) 2009^{2012};
10) 2010^{211}.

Завдання 3. Розв’язати конгруенції:

1) $27x \equiv 59 \pmod{41}$; $32x \equiv 36 \pmod{28}$;
2) $25x \equiv 108 \pmod{29}$; $24x \equiv 12 \pmod{60}$;
3) $18x \equiv 12 \pmod{42}$; $28x \equiv 5 \pmod{31}$;
4) $10x \equiv 7 \pmod{17}$; $24x \equiv 32 \pmod{60}$;
5) $22x \equiv 8 \pmod{29}$; $21x \equiv 33 \pmod{54}$;
6) $12x \equiv 83 \pmod{29}$; $18x \equiv 42 \pmod{24}$;
7) $43x \equiv 214 \pmod{48}$; $33x \equiv 9 \pmod{54}$;
8) $32x \equiv 30 \pmod{39}$; $24x \equiv 48 \pmod{33}$;
9) $29x \equiv 23 \pmod{25}$; $14x \equiv 49 \pmod{21}$;
10) $23x \equiv 15 \pmod{47}$; $45x \equiv 27 \pmod{63}$;

Завдання 4. Знайти кількість точок з цілими координатами, які лежать на заданих прямих між точками з абсцисами n та m:

1) $17x - 16y = 35$, $m = -10$, $n = 25$;
2) $10x - 11y = 15$, $m = -30$, $n = 50$;
3) $31x - 47y = 23$, $m = -23$, $n = 20$;
4) $17x + 13y = 1$, $m = -20$, $n = 15$;
5) $101x - 39y = 89$, $m = 0$, $n = 50$;
6) $3x + 19y = 5$, $m = -7$, $n = 41$;
7) $8x + 13y + 6 = 0$, $m = -100$, $n = -50$;
8) $5x + 4y = 13$, $m = 10$, $n = 35$;
9) $23x + 15y = 19$, $m = -20$, $n = 25$;
10) $7x + 29y = 532$, $m = -20$, $n = 40$.

Завдання 5. Розв’язати системи конгруенцій:

1) $\begin{cases} 2x \equiv 5 \pmod{7} \\ 3x \equiv 2 \pmod{8} \\ x \equiv 1 \pmod{5} \end{cases}$;

2) $\begin{cases} 2x \equiv 3 \pmod{5} \\ 3x \equiv 5 \pmod{7} \\ 3x \equiv 3 \pmod{9} \end{cases}$;

3) $\begin{cases} 4x \equiv 10 \pmod{5} \\ 4x \equiv 1 \pmod{3} \\ 2x \equiv 6 \pmod{7} \end{cases}$;

4) $\begin{cases} 4x \equiv 1 \pmod{9} \\ 5x \equiv 3 \pmod{7} \\ 4x \equiv 12 \pmod{10} \end{cases}$;

5) $\begin{cases} 7x \equiv 3 \pmod{11} \\ 3x \equiv 2 \pmod{5} \\ 15x \equiv 5 \pmod{35} \end{cases}$;

6) $\begin{cases} 5x \equiv 3 \pmod{6} \\ 4x \equiv 7 \pmod{13} \\ 2x \equiv 11 \pmod{3} \end{cases}$;

7) $\begin{cases} 3x \equiv 7 (\mathrm{mod}\, 10) \\ 2x \equiv 5 (\mathrm{mod}\, 13) \\ 7x \equiv 5 (\mathrm{mod}\, 12) \end{cases}$;

8) $\begin{cases} 2x \equiv 7 (\mathrm{mod}\, 13) \\ 5x \equiv 8 (\mathrm{mod}\, 7) \\ 3x \equiv 7 (\mathrm{mod}\, 11) \end{cases}$;

9) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 12) \\ 2x \equiv 1 (\mathrm{mod}\, 7) \\ 3x \equiv 14 (\mathrm{mod}\, 5) \end{cases}$;

10) $\begin{cases} 5x \equiv 3 (\mathrm{mod}\, 9) \\ 4x \equiv 7 (\mathrm{mod}\, 13) \\ 8x \equiv 4 (\mathrm{mod}\, 14) \end{cases}$

Завдання 6. Спростити конгруенції та розв'язати їх способом підбору:

1) $6x^{15} - 12x^{10} + 9x^7 + 16 \equiv 0 \pmod 5$;
2) $13x^{23} - 30x^{22} - 2x^{13} + 1 \equiv 0 \pmod{11}$;
3) $6x^{13} - 3x^{12} - 2x^{11} - 6x^3 + 3x^2 + 7x + 2 \equiv 0 \pmod 7$;
4) $x^{13} - x^{11} + x^9 - x^7 + x^5 + x^3 + x + 1 \equiv 0 \pmod 5$;
5) $x^{14} - x^{13} - 12x^2 + 2x - 1 \equiv 0 \pmod{13}$;
6) $6x^{18} + 18x^{15} + 3x^4 - 8x^3 + x^2 + 3 \equiv 0 \pmod{11}$;
7) $10x^{42} - 5x^{30} + 10x^{18} + 9x^{12} + 4 \equiv 0 \pmod 7$;
8) $x^7 - 3x^6 + x^5 - 15x^4 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod 5$;
9) $75x^{13} - 62x^{12} - 53x^{11} - 24x^6 + 13x - 27 \equiv 0 \pmod 7$;
10) $x^7 + 2x^6 + x^5 + 4x^3 - 2x^2 - 4x + 2 \equiv 0 \pmod 5$.

Завдання 7. З'ясувати, чи проходять через точки з цілими координатами наступні параболи:

1) $23x = y^2 - 149$;
2) $43y = x^2 - 412$;
3) $47y = x^2 + 7$;
4) $73y = x^2 - 37$;
5) $83x = y^2 - 134$;
6) $43y = x^2 - 412$;
7) $53y = x^2 + 131$;
8) $73y = 142 - x^2$;
9) $53y = x^2 - 210$;
10) $151x = y^2 - 76$.

Завдання 8. Знайти порядки усіх класів лишків по модулю m. Вказати класи, представники яких є первісними коренями.

1) $m = 11$;
2) $m = 15$;
3) $m = 14$;
4) $m = 18$;
5) $m = 24$;
6) $m = 12$;
7) $m = 21$;
8) $m = 20$;
9) $m = 16$;
10) $m = 17$.

Завдання 9. Розв'язати конгруенції, використовуючи індекси:

1) $8x^9 + 17 \equiv 0 \pmod{23}$;
2) $15x^4 \equiv 17 \pmod{23}$;
$24^{2x} \equiv 1 \pmod{31}$;
$11 \cdot 5^{3x} \equiv 9 \pmod{79}$;

3) $27x^5 \equiv 25 \pmod{31}$;
4) $13x^3 \equiv 24 \pmod{37}$;
5) $37x^8 \equiv 59 \pmod{61}$;
6) $23x^5 \equiv 15 \pmod{73}$;
7) $25x^7 + 7 \equiv 0 \pmod{31}$;
8) $7x^{13} \equiv 24 \pmod{47}$;
9) $25x^7 \equiv 24 \pmod{73}$;
10) $5x^{11} + 36 \equiv 0 \pmod{71}$;

$8 \cdot 7^x + 4 \equiv 0 \pmod{83}$;
$7 \cdot 5^x \equiv 14 \pmod{73}$;
$15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{61}$;
$12 \cdot 5^x \equiv 7 \pmod{31}$;
$25^{5x} \equiv 47 \pmod{61}$;
$6 \cdot 11^x \equiv 56 \pmod{61}$;
$8 \cdot 5^{2x} + 9 \equiv 0 \pmod{53}$;
$7 \cdot 11^{3x} + 50 \equiv 0 \pmod{79}$;

Завдання 10. З'ясувати, чи утворюють підгрупи мультиплікативної групи $GL_3(R)$ наступні множини. Якщо так, з'ясувати, чи будуть ці підгрупи абелевими.

1) Множина діагональних матриць $D_3(R)=$
$\left\{\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \middle| a,b,c \in R, abc \neq 0\right\}$;

2) Множина матриць $M_3(R)=\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \middle| a,b,c \in R, a \neq 0\right\}$;

3) Множина матриць $T_3(R)=\left\{\begin{pmatrix} a & 0 & 0 \\ d & b & 0 \\ g & k & c \end{pmatrix} \middle| a,b,c,d,f,g,k \in R, abc \neq 0\right\}$;

4) Множина S матриць третього порядку, визначник яких рівний 1 або -1 ;

5) Множина матриць $L_3(R)=\left\{\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \middle| a,b,c \in R\right\}$;

6) Множина матриць $F_3(R)=\left\{\begin{pmatrix} a & 0 & 0 \\ b & a & 0 \\ c & b & a \end{pmatrix} \middle| a,b,c \in R, a \neq 0\right\}$;

7) Множина матриць $UT_3(R)=\left\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c, \in R\right\}$;

8) Множина матриць $I_3(R)=\left\{\begin{pmatrix} a & d & f \\ 0 & b & k \\ 0 & 0 & c \end{pmatrix} \middle| a,b,c,d,k,f \in R, abc \neq 0\right\}$;

9) Множина матриць 3-го порядку, визначник яких рівний 1;

10) Множина матриць $K_3(R)=\left\{\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \middle| a \in R, a \neq 0 \right\}$.

Завдання 11. У групі підстановок S_6 вказати циклічну підгрупу $<a>$, породжену елементом a. Знайти порядки усіх елементів групи $<a>$ та усі її підгрупи. Знайти лівосторонній та правосторонній розклади групи $<a>$ за підгрупою $<b>$.

1) $a=\begin{pmatrix}123456\\654132\end{pmatrix}, b=\begin{pmatrix}123456\\546213\end{pmatrix}$

2) $a=\begin{pmatrix}123456\\234561\end{pmatrix}, b=\begin{pmatrix}123456\\456123\end{pmatrix}$;

3) $a=\begin{pmatrix}123456\\465321\end{pmatrix}, b=\begin{pmatrix}123456\\546213\end{pmatrix}$

4) $a=\begin{pmatrix}123456\\612345\end{pmatrix}, b=\begin{pmatrix}123456\\456123\end{pmatrix}$;

5) $a=\begin{pmatrix}123456\\654231\end{pmatrix}, b=\begin{pmatrix}123456\\132546\end{pmatrix}$;

6) $a=\begin{pmatrix}123456\\645321\end{pmatrix}, b=\begin{pmatrix}123456\\132546\end{pmatrix}$;

7) $a=\begin{pmatrix}123456\\654312\end{pmatrix}, b=\begin{pmatrix}123456\\213465\end{pmatrix}$

8) $a=\begin{pmatrix}123456\\234561\end{pmatrix}, b=\begin{pmatrix}123456\\345612\end{pmatrix}$

9) $a=\begin{pmatrix}123456\\652341\end{pmatrix}, b=\begin{pmatrix}123456\\145236\end{pmatrix}$

10) $a=\begin{pmatrix}123456\\612345\end{pmatrix}, b=\begin{pmatrix}123456\\561234\end{pmatrix}$

ПИТАННЯ ДО ЕКЗАМЕНУ

1. Відношення подільності в кільці цілих чисел. Властивості подільності.
2. Ділення з остачею. Теорема про ділення з остачею.
3. НСД двох чисел. Алгоритм Евкліда. Властивості НСД двох чисел.
4. НСК двох чисел. Властивості НСК. Теорема про зв'язок НСК з НСД.
5. Взаємно прості числа, їх властивості.
6. Прості та складені числа. Властивості простих чисел. Теорема Евкліда.
7. Основна теорема арифметики. Наслідки з неї.
8. Решето Ератосфена.Розподіл простих чисел у натуральному ряді.
9. Числові функції. Ціла та дробова частини числа, приклади, властивості, графіки.
10. Мультиплікативні функції. Властивості. Сума й кількість дільників числа
11. Функція Ейлера. Властивості. Приклади.
12. Мультиплікативність функції Ейлера.
13. Числові конгруенції (означення, ознаки).
14. Властивості числових конгруенцій.
15. Класи лишків. Повна та зведена системи лишків. Властивості.
16. Теорема Ейлера. Мала теорема Ферма.
17. Конгруенції з невідомою величиною. Класи розв'язків конгруенцій з невідомою величиною.Рівносильність конгруенцій.
18. Конгруенції першого степеня з одним невідомим. Дослідження та способи розв'язання.
19. Застосування лінійних конгруенцій до розв'язування невизначених рівнянь першого степеня з двома невідомими. Системи конгруенцій.
20. Конгруенції вищих степенів за простим модулем. Число розв'язків конгруенції n-го степеня за простим модулем.
21. Конгруенції другого степеня за простим модулем. Квадратичні лишки й нелишки. Критерій Ейлера.

22. Символ Лежандра, його властивості і застосування.
23. Показник числа та класу лишків за даним модулем, властивості показників.
24. Первісні корені. Теорема про число класів первісних коренів за простим модулем.
25. Індекси, їх властивості та застосування.
26. Арифметичні застосування конгруенції (встановлення ознак подільності, перевірка результатів арифметичних дій, перетворення звичайного дробу у десятковий).
27. Означення та приклади груп. Порядок групи й порядок елемента.
28. Групи підстановок.
29. Підгрупи, приклади, властивості. Критерій підгрупи.
30. Циклічні групи та підгрупи, приклади.
31. Ізоморфізм груп. Ізоморфізм циклічних груп.
32. Суміжні класи. Ліво- і правосторонній розклад групи за підгрупою. Індекс підгрупи в групі.
33. Теорема Лагранжа та наслідки з неї.
34. Нормальні підгрупи. Критерій нормальності підгрупи у групі. Приклади нормальних підгруп.
35. Фактор-групи. Властивості фактор-груп абелевих та циклічних підгруп.
36. Гомоморфізми груп. Властивості гомоморфізмів.
37. Ядра гомоморфізмів груп. Теорема про природний гомоморфізм груп.

ТЕСТИ

Тест № 1

1. Вкажіть правильну відповідь ($a, q \in Z$):

A. Якщо $a = 6q - 3$, то остача при діленні a на q дорівнює (-3).
B. Якщо $a = 6q - 2$, то остача при діленні a на q дорівнює 2.
C. Якщо $a = 6q + 3$, то остача при діленні a на q дорівнює 3.
D. Якщо $a = 6q - 2$, то остача при діленні a на q дорівнює (-2).
E. Правильна відповідь відсутня.

2. Вкажіть правильну відповідь:

A. НСД чисел 252 та 468 дорівнює 2.
B. НСД чисел 252 та 468 дорівнює 36.
C. Числа 252 та 468 взаємно прості.
D. НСД чисел 252 та 468 дорівнює 3.
E. Правильна відповідь відсутня.

3. Найбільше ціле число, яке при діленні на 13 дає неповну частку 17, дорівнює:

A. 241.
B. 233.
C. Не існує.
D. 344.
E. Правильна відповідь відсутня.

4. Відомо, що $12 \equiv a(\mathrm{mod}\,10)$, $a \in Z$. Тоді:

A. $12 = 10a + r$, $0 \le r < 10$.
B. $a \vdots 2$.
C. $a \equiv 2(\mathrm{mod}\,10)$.
D. $12 = 10k + 2$, $k \in Z$.
E. Правильна відповідь відсутня.

5. Які з наступних чисел є простими:

A. 17.
B. 1.
C. 21.
D. 29.
E. Правильна відповідь відсутня.

6. Канонічний розклад числа 160:

A. $2^4 \cdot 5$.
B. $2^5 \cdot 3 \cdot 5$.
C. $2^5 \cdot 5$.
D. $2^4 \cdot 3 \cdot 5$.
E. Правильна відповідь відсутня.

7. Обчислити $\varphi(32)$:

A. 16
B. 8
C. 31
D. 4
E. Правильна відповідь відсутня.

8. Зведена система лишків за модулем 9 містить:

A. 4 елемента.
B. 9 елементів.
C. 6 елементів.
D. 2 елементи.
E. Правильна відповідь відсутня.

9. Який вигляд мають елементи класу лишків $\overline{6}$ за модулем 9 (вкажіть усі можливі відповіді):

A. $6+9k,\ k \in Z$.
B. $-3+9k,\ k \in Z$.
C. $-6+9k,\ k \in Z$.
D. $6-9k,\ k \in Z$.
E. Правильна відповідь відсутня.

10. Скільки розв'язків має конгруенція $3x \equiv 8(\mathrm{mod}\,6)$:

A. Один розв'язок.
B. Три розв'язки.
C. Два розв'язки.
D. Жодного розв'язку.
E. Правильна відповідь відсутня.

11. Яку остачу має число –29 при діленні на 5:

A. -1.

B. 4.
C. 1.
D. -4.
E. Правильна відповідь відсутня.

12. Розв'язком конгруенції $5x \equiv 1(\mathrm{mod}\, 7)$ є:

A. 3.
B. $3+7k,\ k \in Z$.
C. $x \equiv 3(\mathrm{mod}\, 7)$.
D. Клас чисел, які при діленні на 7 дають остачу 3.
E. Правильна відповідь відсутня.

13. Число a є квадратичним лишком за модулем p, $(a, p)=1$, якщо:

A. $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$.
B. $\left(\frac{a}{p}\right)=1$.
C. $x^2 \equiv a(\mathrm{mod}\ p)$ має розв'язок.
D. $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$.
E. Правильна відповідь відсутня.

14. Скільки розв'язків може мати конгруенція $x^2 \equiv a(\mathrm{mod}\ p)$, $(a, p)=1$:

A. Жодного розв'язку.
B. Один розв'язок.
C. Безліч розв'язків.
D. Два розв'язки.
E. Правильна відповідь відсутня.

15. Які з чисел складають повну систему лишків за модулем 5:

A. 0,1,2,3,4,5.
B. $0,\pm 1,\pm 2$.
C. 1,2,3,4.
D. $\pm 1,\pm 2$.
E. Правильна відповідь відсутня.

16. Числа a та b є конгруентними за модулем p, якщо:

A. $(a-b) \vdots p$.
B. a та b при діленні на p дають однакові остачі.
C. $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.
D. a та b входять в один клас лишків за модулем p.
E. Правильна відповідь відсутня.

17. Які з чисел утворюють зведену систему лишків за модулем 5:

A. 0,1,2,3,4,5.
B. 0,2,3,4.
C. 1,2,3,4.
D. 1,2,3,4,5.
E. Правильна відповідь відсутня.

18. Яку остачу дає число 2^{106} при діленні на 7:

A. 1.
B. 0.
C. 2.
D. -2.
E. Правильна відповідь відсутня.

19. Число 71_5 в десятковій системі числення має зображення:

A. 40.
B. 36.
C. 180.
D. 71.
E. Правильна відповідь відсутня.

20. Скільки існує простих парних чисел:

A. Два.
B. Безліч.
C. Жодного.
D. Одне.
E. Правильна відповідь відсутня.

21. Знайти x, якщо $201_x = 41_8$:

A. 2.
B. 4.
C. 6.
D. 8.
E. Правильна відповідь відсутня.

22. Обчислити $\{-1{,}4\}$:

A. 0,4.
B. -0,4.
C. 0,6.
D. -0,6.
E. Правильна відповідь відсутня.

23. Конгруенція $8x \equiv 10(\mathrm{mod}\,14)$ рівносильна наступній конгруенції:

A. $4x \equiv 5(\mathrm{mod}\,14)$.
B. $4x \equiv 5(\mathrm{mod}\,7)$.
C. $4x \equiv 10(\mathrm{mod}\,14)$.
D. $4x \equiv 10(\mathrm{mod}\,7)$.
E. Правильна відповідь відсутня.

24. Запис $\gamma = ind_g a$ означає, що:

A. $g \equiv a^{\gamma}(\mathrm{mod}\ p)$.
B. $a \equiv g^{\gamma}(\mathrm{mod}\ p)$.
C. $\gamma \equiv a(\mathrm{mod}\ p)$.
D. $\gamma \equiv g(\mathrm{mod}\ p)$.
E. Правильна відповідь відсутня.

25. Конгруенція $3x^5 \equiv 4(\mathrm{mod}\,11)$ рівносильна конгруенції:

A. $5ind\,3x \equiv ind\,4(\mathrm{mod}\,10)$.
B. $ind\,3 + 5indx \equiv ind\,4(\mathrm{mod}\,10)$.
C. $ind\,3 + 5indx \equiv ind\,4(\mathrm{mod}\,11)$.
D. $ind\,3 + 5indx \equiv 4(\mathrm{mod}\,11)$.
E. Правильна відповідь відсутня.

ЛІТЕРАТУРА

Основна

1. Бородін О.І. Теорія чисел. К.: Вища школа, 1970. 276 с.
2. Завало С.Т., Костарчук В.М., Хацет Б.І. Алгебра і теорія чисел. К.: Вища школа, ч. 2, 1974. 408 с.
3. Грибанов В.У., Титов П.И. Сборник упражнений по теории чисел. М.: Просвещение, 1964. 164 с.
4. Завало С.Т. та ін. Алгебра і теорія чисел. Практикум. Ч. ІІ. К.: Вища школа, 1986. 264 с.
5. Завало С.Т. та ін. Алгебра і теорія чисел. Практикум. Ч. І. К.: Вища школа, 1983. 232 с.
6. Лиман Ф.М., Лукашова Т.Д. Елементи теорії груп, кілець та полів: Навч. посібн. – Суми: Видавництво «МакДен», 2013. – 208 с.
7. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел. К.:НПУ імені М.П. Драгоманова, 2006. Ч.І. 400 с.
8. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. М.: Наука, 1977. 416 с.

Додаткова:

9. Бухштаб А.А. Теорія чисел. М.: Высшая школа, 1967. 384 с.
10. Виноградов И.М. Основы теории чисел. М.: Наука, 1965. 168 с.
11. Завало С.Т. Курс алгебри. К.: Вища школа, 1985. 504 с.
12. Курош А.Г. Курс высшей алгебры. М.: Наука, 1971. 432 с.
9. Куликов Л.Я. Алгебра и теория чисел. М.: Высшая школа, 1979. 560с.