

к) $a^{10} - a^6 - a^4 + 1 \equiv 0 \pmod{35}$, $(a, 35) = 1$.

13.11. Нехай p — просте число. Довести, що:

а) $a^p \equiv b^p \pmod{p^2}$, якщо $a^p \equiv b^p \pmod{p}$;

б) $a^{1+2+\dots+(p-1)} + 1 \equiv 0 \pmod{p}$ або $a^{1+2+\dots+(p-1)} - 1 \equiv 0 \pmod{p}$, якщо $p > 2$,

$(a, p) = 1$;

в) $a^{1+2+\dots+(p-1)} + 1 \equiv 0 \pmod{p}$ і $a^{1+2+\dots+(p-1)} - 1 \equiv 0 \pmod{p}$, якщо $p = 2$;

$(a, 2) = 1$;

г) $1^{k(p-1)} + 2^{k(p-1)} + \dots + (p-1)^{k(p-1)} \equiv -1 \pmod{p}$;

д) $a^p \equiv \pm 1 \pmod{p^2}$, якщо $a^p \equiv \pm 1 \pmod{p}$;

е) $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$, якщо q — просте число і $p \neq q$;

ж) $8p^2 + 1$ є простим числом, якщо $p = 3$;

ж) $p = 3$, якщо $5^p + 1 \equiv 0 \pmod{p^2}$;

з) $4p + 1$ є складеним числом, якщо $p > 3$, а $2p + 1$ — простим числом;

к) $qa^p + pa^q \equiv a(p+q) \pmod{pq}$, якщо q — просте число, $(a, p) = 1$, $(a, q) = 1$.

13.12. Знайти остаточу від ділення:

а) a^{100} на 125, $a \in \mathbb{Z}$;

б) $2^{\varphi(m)-1}$ на число m , якщо воно непарне і $m > 1$;

в) $4^{\varphi(m)-1}$ на число m , якщо воно непарне і $m > 1$.

13.13. Довести, що:

а) $a_1^5 + a_2^5 + \dots + a_n^5 \equiv 0 \pmod{30}$, якщо $a_1 + a_2 + \dots + a_n \equiv 0 \pmod{30}$, $a_1, a_2, \dots, a_n \in \mathbb{Z}$;

б) $a^{100n+1} \equiv a \pmod{1000}$, якщо $n \in \mathbb{N}$, $(a, 10) = 1$;

в) $n^2 \equiv 1 \pmod{24}$, якщо $(n, 6) = 1$;

г) $a^{6m} + a^{6n} \equiv 0 \pmod{7}$ тоді і тільки тоді, коли $a \equiv 1, 2, 4, 5 \pmod{7}$,

д) $(a-1)a(a+2) \equiv 0 \pmod{504}$, якщо a є кубом деякого цілого числа.

§ 14. Конгруенції першого степеня з одним невідомим та застосування їх

Література

[1] — § 17, с. 175—180;

[2] — § 17, с. 179—183;

[3] — гл. 12, § 4, с. 409—411;

[10] — гл. IV, § 2, 3, с. 54—58;

[12] — гл. III, § 2, 4, 5, с. 64—68, 79—87;

[14] — § 21, 22, с. 85—94.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Конгруенцію з одним невідомим за модулем m називають конгруенцією виду

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{m}, \quad (1)$$

ліва частина якої містить многочлен з цілими коефіцієнтами. Якщо $a_n \neq 0$, то n називається степенем конгруенції.

Розв'язком конгруенції (1) називають клас лишків за модулем m , кожне число якого задоволяє цю конгруенцію.

Якщо a — число, яке задовольняє конгруенцію (1), то записують $x \equiv a \pmod{m}$, або $x = K_a^{(m)}$, де $0 \leq a < m$.

Конгруенції з одним невідомим називають рівносильними, якщо множини їхніх розв'язків збігаються.

Операції, які не порушують множину розв'язків конгруенцій (у подальшому називатимемо їхніми елементарними перетвореннями):

а) додавання до обох частин конгруенції будь-якого многочлена з цілими коефіцієнтами;

б) додавання до однієї частини конгруенції многочлена з коефіцієнтами, кратними модулю;

в) множення (ділення) обох частин конгруенції на число, яке взаємно просте з модулем (яке є іхнім спільним дільником);

г) множення обох частин конгруенції та їхнього модуля на натуральне число.

Конгруенція

$$ax \equiv b \pmod{m}, \quad (2)$$

де a не $\equiv m$, називається конгруенцією 1-го степеня з одним невідомим.

Якщо $(a, m) = 1$, то конгруенція (2) має єдиний розв'язок.

Якщо $(a, m) = d$, $d > 1$ і $b \equiv d$, то конгруенція (2) має d розв'язків.

Якщо $(a, m) = d$, $d > 1$ і $b \not\equiv d$, то конгруенція (2) не має розв'язків.

Найбільш поширеними способами розв'язування конгруенції 1-го степеня є такі:

I. Способ спроб. Підстановка в конгруенцію (2) чисел повної системи лишків за модулем m (доцільно брати повну систему найменших за абсолютною величиною лишків). Цей спосіб використовується при невеликих модулях.

II. Штучний спосіб. Зведення даної конгруенції за допомогою елементарних перетворень до рівносильної їй конгруенції з коефіцієнтом при x , який дорівнює 1.

III. Способ Ейлера: Розв'язок знаходить за формулою

$$x \equiv ba^{\varphi(m)-1} \pmod{m}, \quad (3)$$

де $\varphi(m)$ — функція Ейлера.

IV. Застосування ланцюгових дробів. Розв'язок знаходить за формулою

$$x \equiv (-1)^n P_{n-1} b \pmod{m}, \quad (4)$$

де P_{n-1} — чисельник передостаннього підхідного дробу у розкладі $\frac{m}{a}$ в ланцюговий дріб.

V. Застосування класів лишків. Розв'язок знаходить за формулою

$$x = K_b^{(m)} (K_a^{(m)})^{-1}, \quad (5)$$

де $(K_a^{(m)})^{-1}$ — клас лишків, обернений до класу лишків $K_a^{(m)}$.

Зauważення

1. Формулі (3) — (5) справедливі тільки при $(a, m) = 1$. Тому розв'язування конгруенції (2) будь-яким способом треба починати з відшукання (a, m) .

2. Число x_0 (клас лишків $K_{x_0}^{(m)}$) вважається розв'язком конгруенції (2), якщо x_0 задовільняє (2) і $0 \leq x_0 < m$.

За допомогою конгруенцій першого степеня з одним невідомим можна розв'язувати невизначені рівняння першого степеня з двома невідомими (див. § 5).

Якщо x_0 — розв'язок конгруенції (2), то $\left\{ x_0, \frac{b - ax_0}{m} \right\}$ є розв'язком невизначеного рівняння першого степеня з двома невідомими

$$ax + my = b. \quad (6)$$

Якщо $\{x_0, y_0\}$ — деякий розв'язок рівняння (6), то множину розв'язків цього рівняння знаходить за формулами

$$x' = x_0 + \frac{m}{d} t, \quad y' = y_0 - \frac{a}{d} t, \quad (7)$$

де t — довільне ціле число, а $d = (a, m)$.

Якщо числа m_1, m_2, \dots, m_k попарно взаємно прості, то система з одним невідомим

$$\begin{aligned}x &\equiv c_1 \pmod{m_1}, \\x &\equiv c_2 \pmod{m_2}, \\&\dots \quad \dots \quad \dots \\x &\equiv c_k \pmod{m_k}\end{aligned}\tag{8}$$

має єдиний розв'язок

$$x \equiv x_0 \pmod{M},\tag{9}$$

де

$$M = m_1 m_2 \dots m_k, \quad x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \dots + M_k y_k c_k,$$

причому числа M_i і y_i визначають з таких умов:

$$M_i = \frac{M}{m_i}, \quad M_i y_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, \dots, k.$$

У загальному випадку, коли числа m_1, m_2, \dots, m_k можуть не бути попарно взаємно простими, систему (8) розв'язують ще так: з першої конгруенції системи (8) знаходять

$$x = c_1 + m_1 t_1, \quad \text{де } t_1 \in \mathbb{Z}. \tag{10}$$

Це значення x підставляють у другу конгруенцію системи (8) і розв'язують її відносно t_1 . Значення t_1 підставляють у рівність (10) і здобуте значення x підставляють у третю конгруенцію системи (8) і т. д. Зрозуміло, що на якомусь кроці можна дістати конгруенцію, яка не має розв'язків. Тоді вся система несумісна.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Користуючись способом спроб, розв'язати конгруенцію

$$2x \equiv 5 \pmod{9}.$$

Розв'язання. Спочатку знаходимо $(2, 9) = 1$. Отже, задана конгруенція має єдиний розв'язок. Випробуємо лишики з повної системи абсолютно найменших лишиків за модулем 9, тобто числа $0, \pm 1, \pm 2, \pm 3, \pm 4$. Маємо:

$$\begin{aligned}2 \cdot 0 &= 0 \not\equiv 5 \pmod{9}, \\2 \cdot 1 &= 2 \not\equiv 5 \pmod{9}, \\2(-1) &= -2 \not\equiv 5 \pmod{9}, \\2 \cdot 2 &= 4 \not\equiv 5 \pmod{9}, \\2(-2) &= -4 \equiv 5 \pmod{9}.\end{aligned}$$

Отже, число -4 задовільняє конгруенцію. Запишемо загальний розв'язок, який відповідає цьому окремому розв'язку. Оскільки $-4 \in K_5^{(9)}$, то

$$x \equiv 5 \pmod{9}, \quad \text{або } x = K_5^{(9)}.$$

Процес випробування можна вже припинити, оскільки довели, що конгруенція має єдиний розв'язок.

2. Користуючись штучним способом, розв'язати конгруенцію

$$27x \equiv 47 \pmod{38}.$$

Розв'язання. Знаходимо $(27, 38) = 1$. Отже, задана конгруенція має єдиний розв'язок. Додамо до правої частини конгруенції число -38 , яке кратне модулю. Дістаємо

$$27x \equiv 9 \pmod{38}.$$

Поділимо обидві частини цієї конгруенції на 9:

$$3x \equiv 1 \pmod{38}.$$

Додамо до правої частини модуль:

$$3x \equiv 39 \pmod{38}.$$

Поділімо обидві частини останньої конгруенції на 3:

$$x \equiv 13 \pmod{38}.$$

Це і є розв'язок заданої конгруенції.

Зауваження. Відомо, що коли $(a, m) = 1$, то для будь-якого цілого числа b існують такі цілі числа s і t , що $0 < s < a$ і $b + sm = at$. Отже, розв'язком конгруенції $ax \equiv b \pmod{m}$, де $(a, m) = 1$ є $x \equiv t \pmod{m}$, і тому будь-яку конгруенцію першого степеня з одним невідомим можна розв'язати штучним способом. Справді, якщо конгруенція має розв'язки, то досить розглянути випадок, коли $(a, m) = 1$. Тоді конгруенцію $ax \equiv b \pmod{m}$ послідовно замінюють еквівалентними їй конгруенціями:

$$ax \equiv b \pm m \pmod{m}, \quad ax \equiv b \pm 2m \pmod{m}, \dots,$$

поки не дістануть конгруенцію, в якій ліву і праву частини можна скоротити на a .

3. Користуючись способом Ейлера, розв'язати конгруенцію

$$27x \equiv 24 \pmod{102}.$$

Розв'язання. Знаходимо $(27, 102) = 3$. Задана конгруенція має три розв'язки, оскільки $24 \div 3$. Поділімо обидві частини і модуль заданої конгруенції на 3:

$$9x \equiv 8 \pmod{34}.$$

Оскільки тут $a = 9$, $m = 34$, $b = 8$, то за формулою (3) маємо

$$x \equiv ba^{\varphi(m)-1} \pmod{m},$$

або

$$x \equiv 8 \cdot 9^{\varphi(34)-1} \pmod{34}.$$

Тепер знайдемо $\varphi(34)$. Оскільки $34 = 2 \cdot 17$, то

$$\varphi(34) = 2 \cdot 17 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{17}\right) = 16.$$

Тоді $x \equiv 8 \cdot 9^{16} \pmod{34}$. Число $8 \cdot 9^{16}$ замінимо найменшим невід'ємним лишком за модулем 34. Дістаємо

$$x \equiv 8 \cdot 9^{16} \equiv 8 \cdot 3^{30} \equiv 8 \cdot 3^{16} \equiv 8 \cdot (2187)^2 \equiv 8 \cdot 11^2 \equiv 16 \pmod{34}.$$

Отже, $x \equiv 16 \pmod{34}$ є розв'язок конгруенції $9x \equiv 8 \pmod{34}$. Тоді конгруенція $27x \equiv 24 \pmod{102}$ має розв'язки:

$$x \equiv 16 \pmod{102},$$

$$x \equiv 50 \pmod{102},$$

$$x \equiv 84 \pmod{102},$$

або коротше

$$x \equiv 16; 50; 84 \pmod{102}.$$

Зауваження. Недоліком способу Ейлера є те, що при великому $\varphi(m)$ знаходження найменшого невід'ємного лишку того класу чисел за модулем m , до якого належить число $ba^{\varphi(m)-1}$, стає громіздким.

4. Використовуючи ланцюгові дроби, розв'язати конгруенцію

$$220x \equiv 28 \pmod{348}.$$

Розв'язання. Знаходимо $(220, 348) = 4$. Оскільки $28 \div 4$, то задана конгруенція має чотири розв'язки. Поділімо обидві частини і модуль заданої конгруенції на 4:

$$55x \equiv 7 \pmod{87}.$$

Розв'яжемо цю конгруенцію за допомогою ланцюгових дробів. Розкладемо $\frac{87}{55}$ у ланцюговий дріб і обчислимо його підхідні дроби. Дістанемо таблицю елементів q_i і чисельників P_i (табл. 13).

Таблиця 13

t	-1	0	1	2	3	4	5	6
q_t		1	1	1	2	1	1	4
P_t	1	1	2	3	8	11	19	87

Отже, $n = 6$, $P_{n-1} = 19$. Оскільки $b = 7$, $m = 87$, то за формулою (4)

$$x \equiv (-1)^n P_{n-1} b \pmod{m}.$$

Отже,

$$x \equiv (-1)^6 19 \cdot 7 \equiv 133 \equiv 46 \pmod{87}$$

є розв'язком конгруенції $55x \equiv 7 \pmod{87}$. Тоді задана конгруенція має розв'язки

$$x = 46; 133; 220; 307 \pmod{348}.$$

Зауваження. Перш ніж застосувати цей спосіб, слід спочатку (якщо це необхідно), використовуючи властивості конгруенцій, зробити коефіцієнт при невідомому невід'ємним і меншим за модулем.

Б. Застосовуючи класи лишків, розв'язати конгруенцію

$$37x \equiv 25 \pmod{107}.$$

Розв'язання. Знаходимо $(37, 107) = 1$. Отже, задана конгруенція має єдиний розв'язок. Запишемо конгруенцію у вигляді

$$K_{37}^{(107)} K_x^{(107)} = K_{25}^{(107)}.$$

Знайдемо $(K_{37}^{(107)})^{-1}$ — клас лишків за модулем 107, обернений до класу $K_{37}^{(107)}$.

Для цього застосуємо до чисел 107 і 37 алгоритм ділення з остачею. Матимемо

$$107 = 37 \cdot 2 + 33,$$

$$37 = 33 \cdot 1 + 4,$$

$$33 = 4 \cdot 8 + 1.$$

Розглядаючи цей процес знизу вверх, виразимо 1 через числа 107 і 33:

$$1 = 33 - 4 \cdot 8 = 33 - (37 - 33 \cdot 1) \cdot 8 = 33 \cdot 9 + 37(-8) =$$

$$= (107 - 37 \cdot 2) \cdot 9 + 37(-8) = 107 \cdot 9 + 37(-26).$$

Отже, $1 = 107 \cdot 9 + 37(-26)$. Це означає, що $(K_{37}^{(107)})^{-1} = K_{-26}^{(107)}$, тобто

$$(K_{37}^{(107)})^{-1} = K_{-26+107}^{(107)} = K_{81}^{(107)}.$$

Тоді за формулою (5) маємо

$$x \equiv K_b^{(m)} (K_a^{(m)})^{-1}, \text{ або } x = K_{25}^{(107)} \cdot K_{81}^{(107)} = K_{2025}^{(107)} = K_{99}^{(107)}.$$

Отже, $x = K_{99}^{(107)}$ є розв'язком заданої конгруенції, тобто $x \equiv 99 \pmod{107}$.

Зауваження. Процес розв'язування конгруенції першого степеня з одним невідомим будь-яким способом слід закінчувати перевіркою.

Б. Розв'язати в цілих числах невизначене рівняння $27x + 38y = 47$.

Розв'язання. Оскільки число y повинно бути цілим, то різниця $27x - 47$ має ділитися на 38. Дістаємо

$$27x \equiv 47 \pmod{38}.$$

Розв'яжемо цю конгруенцію. Знаходимо $(27, 38) = 1$. Отже, конгруенція має єдиний розв'язок. Застосуємо штучний спосіб. Додамо до правої частини число -38 , яке кратне модулю:

$$27x \equiv 9 \pmod{38}.$$

Поділимо обидві частини цієї конгруенції на 9:

$$3x \equiv 1 \pmod{38}.$$

Додамо до правої частини модуль:

$$3x \equiv 39 \pmod{38}.$$

Поділимо обидві частини на 3:

$$x \equiv 13 \pmod{38}.$$

Отже, $x \equiv 13 \pmod{38}$ є розв'язком конгруенції $27x \equiv 47 \pmod{38}$. Тоді

$$\left\{ 13, \frac{47 - 27 \cdot 13}{38} \right\} = \{13, -8\}$$

є окремим розв'язком заданого рівняння. Загальний розв'язок заданого рівняння дістаємо за формулами (7):

$$x' = x_0 + \frac{m}{d} t, \quad y' = y_0 - \frac{a}{d} t,$$

де $x_0 = 13$, $y_0 = -8$, $m = 38$, $a = 27$, $d = 1$. Отже,

$$\{x' = 13 + 38t, \quad y' = -8 - 27t\} -$$

загальний розв'язок заданого невизначеного рівняння, де t — довільне ціле число.

7. Розв'язати систему конгруенцій

$$\begin{cases} 3x \equiv 11 \pmod{17}, \\ 15x \equiv 35 \pmod{13}, \\ 21x \equiv 33 \pmod{30}. \end{cases}$$

Розв'язання. Розв'язуючи кожну конгруенцію, замінимо задану систему еквівалентною її системою конгруенцій:

$$\begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 3 \pmod{10}. \end{cases}$$

Оскільки модулі конгруенцій попарно взаємно прості, то можна використати формулу (9). Знаходимо:

$$M = 17 \cdot 13 \cdot 10 = 2210,$$

$$M_1 = \frac{2210}{17} = 130,$$

$$M_2 = \frac{2210}{13} = 170,$$

$$M_3 = \frac{2210}{10} = 221.$$

Розв'яжемо такі конгруенції:

$$130y_1 \equiv 1 \pmod{17}, \quad 170y_2 \equiv 1 \pmod{13}, \quad 221y_3 \equiv 1 \pmod{10}.$$

$$y_1 = 14, \quad y_2 = 1, \quad y_3 = 1.$$

Згідно з формuloю (9), дістанемо

$$x = x_0 + 130 \cdot 14 \cdot 15 + 170 \cdot 1 \cdot 11 + 221 \cdot 1 \cdot 3 = 29833 \equiv 1103 \pmod{2210}.$$

Зауваження. 1. Якщо деяка з конгруенцій системи має кілька розв'язків, то їх слід об'єднати і записати як один розв'язок за меншим модулем, бо в противному разі треба буде розв'язувати стільки систем, скільки розв'язків має конгруенція.

2. Розв'язки системи конгруенцій можуть мати різні форми запису. Так, якщо розв'язки третьої конгруенції з прикладу 7 ми записали б у вигляді $x \equiv 3, 13, 23 \pmod{30}$, то довелося б розв'язувати такі три системи конгруенцій:

$$\begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 3 \pmod{30}; \end{cases} \quad \begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 13 \pmod{30}; \end{cases} \quad \begin{cases} x \equiv 15 \pmod{17}, \\ x \equiv 11 \pmod{13}, \\ x \equiv 23 \pmod{30}. \end{cases}$$

Дістали б три розв'язки:

$$x \equiv 5523 \pmod{6630}, \quad x \equiv 3313 \pmod{6630}, \quad x \equiv 1103 \pmod{6630}.$$

Зазначимо, що множина чисел, які визначаються цими розв'язками, збігається з множиною чисел, що визначаються одним розв'язком, здобутим раніше,

$$x \equiv 1103 \pmod{2210}.$$

8. Розв'язати систему конгруенцій

$$\begin{cases} 2x \equiv 19 \pmod{15}, \\ 3x \equiv 41 \pmod{20}, \\ 6x \equiv 37 \pmod{35}. \end{cases}$$

Розв'язання. Розв'язуючи кожну конгруенцію, замінимо задану систему еквівалентною її системою конгруенцій:

$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}, \\ x \equiv 12 \pmod{35}. \end{cases}$$

З першої конгруенції маємо $x = 2 + 15t$, де $t \in \mathbb{Z}$. Щоб визначити t , підставимо значення x у другу конгруенцію:

$$2 + 15t \equiv 7 \pmod{20}.$$

Звідси $t \equiv 3 \pmod{4}$, або $t = 3 + 4s$, де $s \in \mathbb{Z}$. Тоді

$$x = 2 + 15t = 2 + 15(3 + 4s) = 47 + 60s,$$

причому x задовільняє вже перші дві конгруенції системи. Серед чисел x вибираємо такі, які б задовільняли й третю конгруенцію. Для цього знайдемо з умови

$$47 + 60s \equiv 12 \pmod{35}.$$

Звідси $s \equiv 0 \pmod{7}$, тобто $s = 7k$, де $k \in \mathbb{Z}$. Маємо $x = 47 + 60s = 47 + 60 \cdot 7k = 47 + 420k$. Отже, $x \equiv 47 \pmod{420}$ — розв'язок заданої системи.

Задачі

14.1. За способом спроб розв'язати такі конгруенції:

- | | |
|------------------------------|-------------------------------|
| a) $2x \equiv 1 \pmod{3}$; | д) $4x \equiv 6 \pmod{10}$; |
| б) $8x \equiv 3 \pmod{4}$; | е) $12x \equiv 1 \pmod{7}$; |
| в) $6x \equiv 7 \pmod{5}$; | ж) $5x \equiv 7 \pmod{11}$; |
| г) $3x \equiv 22 \pmod{7}$; | ж) $8x \equiv 16 \pmod{12}$. |

14.2. За штучним способом розв'язати такі конгруенції:

- | | |
|---------------------------------|--------------------------------|
| а) $7x \equiv 8 \pmod{13}$; | д) $16x \equiv 50 \pmod{23}$; |
| б) $6x \equiv 11 \pmod{14}$; | е) $25x \equiv 1 \pmod{37}$; |
| в) $8x \equiv 10 \pmod{14}$; | ж) $17x \equiv 23 \pmod{41}$; |
| г) $11x \equiv -32 \pmod{27}$; | ж) $32x \equiv 43 \pmod{51}$. |

14.3. За способом Ейлера розв'язати такі конгруенції:

- | | |
|-------------------------------|--------------------------------|
| а) $5x \equiv 7 \pmod{13}$; | д) $27x \equiv 11 \pmod{34}$; |
| б) $29x \equiv 3 \pmod{12}$; | е) $24x \equiv 1 \pmod{15}$; |
| в) $5x \equiv 26 \pmod{12}$; | ж) $15x \equiv 23 \pmod{22}$; |
| г) $8x \equiv 17 \pmod{19}$; | ж) $12x \equiv 51 \pmod{39}$. |

14.4. Застосовуючи ланцюгові дроби, розв'язати такі конгруенції:

- | | |
|----------------------------------|--------------------------------------|
| а) $15x \equiv 37 \pmod{98}$; | е) $192x \equiv 9 \pmod{327}$; |
| б) $32x \equiv 182 \pmod{119}$; | ж) $365x \equiv 50 \pmod{395}$; |
| в) $105x \equiv 72 \pmod{147}$; | з) $-639x \equiv 177 \pmod{924}$; |
| г) $97x \equiv 53 \pmod{169}$; | к) $1296x \equiv 1105 \pmod{2413}$; |
| д) $-50x \equiv 67 \pmod{177}$; | л) $1215x \equiv 560 \pmod{2755}$; |
| е) $69x \equiv 393 \pmod{201}$; | м) $1919x \equiv 1717 \pmod{4009}$. |

14.5. Застосовуючи класи лишків, розв'язати такі конгруенції:

- а) $21x \equiv 17 \pmod{23}$; д) $28x \equiv 33 \pmod{35}$;
б) $5x \equiv 7 \pmod{24}$; е) $12x \equiv 24 \pmod{30}$;
в) $17x \equiv 19 \pmod{24}$; ж) $9x \equiv 18 \pmod{41}$;
г) $13x \equiv -1 \pmod{30}$; ж) $11x \equiv 31 \pmod{50}$.

14.6. Розв'язати штучним способом конгруенції задач 14.3 і 14.5.

14.7. Розв'язати такі конгруенції:

- а) $(a+b)x \equiv a^2 + b^2 \pmod{ab}$, $(a, b) = 1$;
б) $(a^2 + b^2)x \equiv a - b \pmod{ab}$, $(a, b) = 1$;
в) $(a+b)^2 x \equiv a^2 - b^2 \pmod{ab}$, $(a, b) = 1$;
г) $(a-b)x \equiv a^2 + b^2 \pmod{ab}$, $(a, b) = 1$;
д) $2x \equiv 1 + p \pmod{p}$, де p — просте непарне число;
е) $(m-1)x \equiv 1 \pmod{m}$;
ж) $(m+1)^2 x \equiv a \pmod{m}$;
ж) $ax \equiv 1 \pmod{p}$, де p — просте число і $(a, p) = 1$.

14.8. Скласти конгруенцію першого степеня з одним невідомим за модулем 15 так, щоб вона мала:

- а) єдиний розв'язок;
б) 3 або 5 розв'язків;
в) 2, 4, 6, 14 розв'язків.

14.9. Розв'язати в цілих числах невизначені рівняння:

- а) $2x + 3y = 4$; ж) $17x - 16y = 31$;
б) $4x - 3y = 2$; з) $91x - 28y = 35$;
в) $3x + 4y = 13$; к) $17x - 39y = 26$;
г) $5x + 4y = 3$; л) $50x - 42y = 34$;
д) $3x + 8y = 5$; м) $47x - 105y = 4$;
е) $17x + 13y = 1$; н) $47x - 111y = 89$.
ж) $23x + 15y = 19$;

14.10. Розв'язати системи конгруенцій:

- а) $\begin{cases} 3x \equiv 5 \pmod{7}, \\ 2x \equiv 1 \pmod{5}; \end{cases}$ д) $\begin{cases} x \equiv b_1 \pmod{13}, \\ x \equiv b_2 \pmod{17}; \end{cases}$
б) $\begin{cases} 3x \equiv 1 \pmod{20}, \\ 2x \equiv 3 \pmod{15}; \end{cases}$ е) $\begin{cases} 3x + 4y \equiv 29 \pmod{143}, \\ 2x - 9y \equiv 59 \pmod{143}; \end{cases}$
в) $\begin{cases} 3x \equiv 1 \pmod{5}, \\ 5x \equiv 4 \pmod{7}; \end{cases}$ ж) $\begin{cases} x + 2y \equiv 0 \pmod{5}, \\ 3x + 2y \equiv 2 \pmod{5}; \end{cases}$
г) $\begin{cases} 14x \equiv 12 \pmod{18}, \\ x \equiv 5 \pmod{25}; \end{cases}$ ж) $\begin{cases} 5x - y \equiv 3 \pmod{6}, \\ 2x + 2y \equiv 5 \pmod{6}. \end{cases}$

14.11. Розв'язати системи конгруенцій:

- | | |
|--|---|
| a) $\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod{15}; \end{cases}$ | e) $\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{20}, \\ x \equiv 12 \pmod{35}; \end{cases}$ |
| b) $\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}; \end{cases}$ | ж) $\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 1 \pmod{12}; \\ x \equiv 7 \pmod{14}; \end{cases}$ |
| v) $\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 6 \pmod{9}; \end{cases}$ | з) $\begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 4 \pmod{11}, \\ x \equiv 6 \pmod{17}; \end{cases}$ |
| г) $\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{9}, \\ x \equiv 11 \pmod{15}; \end{cases}$ | к) $\begin{cases} x \equiv b_1 \pmod{25}, \\ x \equiv b_2 \pmod{27}, \\ x \equiv b_3 \pmod{59}; \end{cases}$ |
| д) $\begin{cases} x \equiv 4 \pmod{7}, \\ x \equiv 9 \pmod{13}, \\ x \equiv 1 \pmod{17}; \end{cases}$ | л) $\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 2 \pmod{7}, \\ x \equiv 9 \pmod{11}, \\ x \equiv 3 \pmod{13}. \end{cases}$ |
| е) $\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv 2 \pmod{8}, \\ x \equiv 2 \pmod{11}; \end{cases}$ | |

14.12. Розв'язати системи конгруенцій:

- | | |
|---|---|
| a) $\begin{cases} 3x \equiv 1 \pmod{10}, \\ 4x \equiv 3 \pmod{5}, \\ 2x \equiv 7 \pmod{9}; \end{cases}$ | д) $\begin{cases} 3x \equiv 7 \pmod{10}, \\ 2x \equiv 5 \pmod{15}, \\ 7x \equiv 5 \pmod{12}; \end{cases}$ |
| б) $\begin{cases} 2x \equiv 3 \pmod{5}, \\ 3x \equiv 5 \pmod{7}, \\ 3x \equiv 3 \pmod{9}; \end{cases}$ | е) $\begin{cases} 5x \equiv 3 \pmod{9}, \\ 4x \equiv 7 \pmod{13}, \\ 8x \equiv 4 \pmod{14}, \\ x \equiv 2 \pmod{17}; \end{cases}$ |
| в) $\begin{cases} 4x \equiv 1 \pmod{9}, \\ 5x \equiv 3 \pmod{7}, \\ 4x \equiv 5 \pmod{12}; \end{cases}$ | е) $\begin{cases} 2x \equiv 7 \pmod{13}, \\ 5x \equiv 8 \pmod{17}, \\ 14x \equiv 35 \pmod{19}, \\ 3x \equiv 7 \pmod{31}. \end{cases}$ |
| г) $\begin{cases} 7x \equiv 3 \pmod{11}, \\ 3x \equiv 2 \pmod{5}, \\ 15x \equiv 5 \pmod{35}; \end{cases}$ | |

14.13. Знайти точки з цілими координатами, які лежать на прямих $4x - 7y = 9$, $2x + 9y = 15$ і $5x - 13y = 12$ на одному перпендикулярі до осі абсцис.

14.14. При яких значеннях a мають розв'язки такі системи:

$$\begin{array}{ll} \text{а)} & \begin{cases} x \equiv a \pmod{6}, \\ x \equiv 1 \pmod{10}, \\ x \equiv 2 \pmod{21}, \\ x \equiv 3 \pmod{11}; \end{cases} \\ & \text{в)} \quad \begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}; \end{cases} \\ \text{б)} & \begin{cases} 2x \equiv a \pmod{4}, \\ 3x \equiv 4 \pmod{10}; \end{cases} \\ & \text{г)} \quad \begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod{15}, \\ x \equiv a \pmod{8}? \end{cases} \end{array}$$

14.15. Знайти хоча б одне значення m , при якому несумісною є система

$$\begin{cases} x \equiv 3 \pmod{6}, \\ x \equiv 7 \pmod{m}. \end{cases}$$

14.16. Скільки точок з цілими координатами лежать на прямій $8x - 13y + 6 = 0$ між прямими $x = -100$ і $x = 150$?

14.17. Довести, що всередині прямокутника, обмеженого прямими $x = -2$, $x = 5$ і $y = -1$, $y = 2$, на прямій $3x - 7y = 1$ не має жодної точки з цілими координатами.

14.18. Скільки точок з цілими координатами лежать на заданих прямих між точками з абсцисами a_1 і a_2 :

- а) $10x - 11y = 15$, $a_1 = -30$, $a_2 = 50$;
- б) $31x - 47y = 23$, $a_1 = 23$, $a_2 = -50$;
- в) $101x - 39y = 89$, $a_1 = 0$, $a_2 = 100$;
- г) $8x - 13y + 6 = 0$, $a_1 = -100$, $a_2 = 150$;
- д) $7x + 29y = 584$, $a_1 = -20$, $a_2 = 160$;
- е) $90x - 74y = 50$, $a_1 = -100$, $a_2 = 200$?

14.19. Нехай точки A і B мають цілі координати $A(x_1, y_1)$, $B(x_2, y_2)$. Довести, що на відрізку AB число внутрішніх точок з цілими координатами дорівнює $d - 1$, де

$$d = (y_1 - y_2, x_1 - x_2).$$

14.20. Через скільки точок з цілими координатами проходять сторони трикутника з вершинами:

- а) $A(2, 3)$, $B(7, 8)$, $C(13, 5)$;
- б) $A(2, 1)$, $B(20, 7)$, $C(8, 15)$?

14.21. Знайти відстань r між сусідніми точками з цілими координатами, які лежать на прямій $ax + by = c$, $(a, b) = 1$.

14.22. При якій умові дріб $\frac{c}{ab}$ можна подати у вигляді суми двох дробів із знаменниками a і b ($a, b, c \in \mathbb{Z}$)?

14.23. Відгадати день народження, якщо сума добутків числа місяця на 12 і номера місяця на 31 дорівнює 339. У чому суть відгадування?

14.24. Для перевезення зерна є мішки по 60 і 80 кг. Скільки таких мішків потрібно для перевезення 440 кг зерна?

14.25. На будівництво газопроводу на трасу завдовжки 283 м було доставлено труби, довжина яких 5 і 7 м. Скільки труб доставили?

14.26. Скільки квитків по 30 і 50 коп. можна купити на 14 крб. 90 коп.?

§ 15. Конгруенції вищих степенів з одним невідомим

Література

- [1] — § 18, с. 180—184;
- [2] — § 18, с. 183—187;
- [3] — гл. 12, § 4, с. 411—413;
- [5] — гл. VIII, § 4, с. 297—316;
- [10] — гл. IV, § 4, 5, с. 58—63;
- [11] — гл. 15, § 1, гл. 16, с. 126—131, с. 135—139;
- [12] — гл. III, § 6, 7, с. 87—101;
- [14] — § 24, 25, с. 94—105.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Якщо m_1, m_2, \dots, m_s — попарно взаємно прості числа, то конгруенція

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \equiv 0 \pmod{m_1m_2 \dots m_s} \quad (1)$$

еквівалентна системі конгруенцій

$$\left. \begin{aligned} f(x) &\equiv 0 \pmod{m_1}, \\ f(x) &\equiv 0 \pmod{m_2}, \\ &\dots \dots \dots \\ f(x) &\equiv 0 \pmod{m_s}. \end{aligned} \right\} \quad (2)$$

Число розв'язків конгруенції (1) дорівнює $k_1k_2 \dots k_s$, де k_1, k_2, \dots, k_s дорівнює відповідно числу розв'язків кожної з конгруенцій (2). Отже, треба розв'язати конгруенцію виду

$$f(x) \equiv 0 \pmod{p^a}, \quad (3)$$

де p — просте число, $a \in \mathbb{N}$.

Будь-який розв'язок

$$x \equiv a \pmod{p} \quad (4)$$

конгруенції

$$f(x) \equiv 0 \pmod{p} \quad (5)$$

при умові, що $f'(a) \neq p$, є одним з розв'язків конгруенції (3).

Якщо $f'(a) \equiv p$, то розв'язок (4) або не дає жодного розв'язку для (3), або дає кілька розв'язків.

Нехай $x \equiv a \pmod{p^{k-1}}$ — розв'язок конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$. Тоді число $x = a + p^{k-1}t$, $t \in \mathbb{Z}$, є розв'язком конгруенції $f(x) \equiv 0 \pmod{p^k}$ тоді і тільки тоді, коли відповідне значення t задоволяє конгруенцію

$$f'(a)t \equiv -\frac{f(a)}{p^{k-1}} \pmod{p}. \quad (6)$$

Якщо конгруенція (6) не має розв'язків, то в класі розв'язків $x \equiv a \pmod{p^{k-1}}$ конгруенції $f(x) \equiv 0 \pmod{p^{k-1}}$ немає жодного розв'язку конгруенції $f(x) \equiv 0 \pmod{p^k}$.