

Розділ III. ТЕОРІЯ КОНГРУЕНЦІЙ З АРИФМЕТИЧНИМИ ЗАСТОСУВАННЯМИ

§ 11. Конгруенції в кільці цілих чисел та їхні найпростіші властивості

Література

- [1] — § 15, с. 162—167;
- [2] — § 15, с. 166—169;
- [3] — гл. 12, § 1, с. 397—399;
- [10] — гл. III, § 1—3, с. 41—44;
- [11] — гл. 7, с. 72—77;
- [12] — гл. II, § 1, с. 36—43;
- [14] — § 15, с. 66—71.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Серед багатьох означень конгруентності двох цілих чисел a і b за модулем m розглянемо три.

Означення 1. Цілі числа a і b називають конгруентними за модулем m , де m — ціле число, якщо їхня різниця $a - b$ ділиться на m . Позначення:

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

Якщо a і b не конгруентні за модулем m , то пишуть

$$a \not\equiv b \pmod{m}.$$

Означення 2. Цілі числа a і b називають конгруентними за модулем m , де $m \in \mathbb{Z}$, якщо вони при діленні на m дають однакові остачі.

Означення 3. Цілі числа a і b називають конгруентними за модулем m , де $m \in \mathbb{Z}$, якщо існує таке ціле число q , що $a = b + mq$.

Означення 1, 2, 3 рівносильні.

Основні властивості конгруенцій

1°. Відношення конгруентності за даним модулем є бінарне відношення еквівалентності на множині цілих чисел. Класи еквівалентності називають класами лишків за даним модулем;

2°. Конгруенції за одним модулем можна почленно додавати, віднімати і множити;

3°. До обох частин конгруенції можна додати будь-яке ціле число (це дає змогу переносити будь-який доданок з однієї сторони в другу з протилежним знаком);

4°. До будь-якої частини конгруенції можна додати довільне ціле число, кратне модулю;

5°. Обидві частини конгруенції можна помножити на те саме ціле число;

6°. Обидві частини конгруенції можна поділити на їхній спільний дільник, якщо він взаємно простий з модулем;

7°. Якщо у виразі

$$f(a_1, a_2, \dots, a_k) = \sum A a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$$

усі коефіцієнти A і числа a_1, a_2, \dots, a_k замінити на конгруентні їм за модулем m коефіцієнти B і числа b_1, b_2, \dots, b_k відповідно, то вираз

$$g(b_1, b_2, \dots, b_k) = \sum B b_1^{n_1} b_2^{n_2} \dots b_k^{n_k}$$

буде конгруентний заданому за модулем m :

$$f(a_1, a_2, \dots, a_k) \equiv g(b_1, b_2, \dots, b_k) \pmod{m}$$

8°. Обидві частини конгруенції і модуль можна множити на те саме ціле число.

9°. Обидві частини конгруенції і модуль можна скорочувати на їхній спільний дільник.

10°. Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.

11°. Якщо конгруенція має місце за модулем m , то вона має місце за модулем d , де d — довільний дільник числа m .

12°. Якщо одна частина конгруенції і модуль ділиться на деяке число, то й друга частина конгруенції ділиться на те саме число.

13°. Якщо $a \equiv b \pmod{m}$, то $(a, m) = (b, m)$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Чи конгруентні числа 78, 210 і 346 з числом 27 за модулем 11?

Розв'язання. Віднімемо від даних чисел число 27. Дістанемо 51, 183 і 319. З них тільки 319 ділиться на 11, а тому тільки 346 конгруентне 27 за модулем 11, тобто $346 \equiv 27 \pmod{11}$.

2. Довести, що коли $100a + 10b + c \equiv 0 \pmod{21}$, то $a - 2b + 4c \equiv 0 \pmod{21}$, $a, b, c \in \mathbb{Z}$.

Розв'язання. Нехай $100a + 10b + c \equiv 0 \pmod{21}$. Помноживши обидві частини цієї конгруенції на 4, матимемо

$$400a + 40b + 4c \equiv 0 \pmod{21}. \quad (1)$$

При цьому мають місце конгруенції:

$$400a \equiv a \pmod{21}, \text{ бо } 400a - a = 399a \equiv 0 \pmod{21}, \quad (2)$$

$$40b \equiv -2b \pmod{21}, \text{ бо } 40b - (-2b) = 42b \equiv 0 \pmod{21}, \quad (3)$$

$$4c \equiv 4c \pmod{21}, \text{ бо } 4c - 4c = 0 \pmod{21}. \quad (4)$$

Додавши почленно ці конгруенції, дістанемо

$$400a + 40b + 4c \equiv a - 2b + 4c \pmod{21}. \quad (5)$$

Беручи до уваги конгруенцію (1), матимемо

$$a - 2b + 4c \equiv 0 \pmod{21}.$$

3. Знайти остатчу від ділення $1532^5 - 1$ на 9.

Розв'язання. Зрозуміло, що нерационально знаходити число $1532^5 - 1$, а потім остатчу від ділення цього числа на 9. Слід скористатися властивостями конгруенцій за модулем 9. Нам треба знайти таке ціле невід'ємне число x , що $x \equiv 1532^5 - 1 \pmod{9}$ і $x < 9$. Оскільки $1530 \equiv 0 \pmod{9}$, то $1532^5 \equiv (1532 - 1530)^5 \pmod{9}$, тобто $1532^5 \equiv 2^5 \pmod{9}$. Проте $2^5 = 32 \equiv 5 \pmod{9}$. Отже, $1532^5 \equiv 5 \pmod{9}$. Віднімемо почленно від цієї конгруенції конгруенцію $1 \equiv 1 \pmod{9}$. Матимемо $1532^5 - 1 \equiv 4 \pmod{9}$. Оскільки $0 < 4 < 9$, то $x = 4$. Отже, число $1532^5 - 1$ при діленні на 9 дає остатчу 4.

4. Довести, що числа виду $3^{2^{4n+1}} + 2$, $n \in \mathbb{N}$ є складеними.

Розв'язання. Оскільки $4 \equiv -1 \pmod{5}$, то $2^{4n+1} \equiv 2 \cdot 4^{2n} \equiv 2 \pmod{5}$.

Тоді число 2^{4n+1} має вид $5k + 2$, де $k \in \mathbb{N}$, а тому $3^{2^{4n+1}} + 2 \equiv 3^{5k+2} + 2$.

Оскільки $243 \equiv 1 \pmod{11}$, а $3^5 = 243$, то $3^{5k+2} + 2 \equiv 9 \cdot 243^k + 2 \equiv 0 \pmod{11}$. Отже, $3^{2^{4n+1}} + 2 \equiv 2 \pmod{11}$. Беручи до уваги нерівність $3^{2^{4n+1}} + 2 > 11$, маємо, що $3^{2^{4n+1}} + 2$ є складене число.

Задачі

11.1. Серед чисел a_1, a_2, \dots, a_n знайти всі пари різних чисел, конгруентних за модулем m , якщо:

- а) $a_1 = 216, a_2 = 134, a_3 = 214, a_4 = 303, a_5 = 21, m = 5$;
- б) $a_1 = 135, a_2 = 106, a_3 = 181, a_4 = 225, a_5 = 167, a_6 = 452, m = 15$;

- в) $a_1 = 217, a_2 = 42, a_3 = 182, a_4 = 241, m = 12$.

11.2. Які з чисел a, b, c конгруентні числу d за модулем m , якщо:

- а) $a = 137, b = 343, c = 633, d = 13, m = 31$;
- б) $a = 217, b = 201, c = 186, d = 11, m = 19$;
- в) $a = 234, b = 634, c = 104, d = 9, m = 25$.

11.3. Довести, що:

- а) означення 1—3 еквівалентні між собою;

- б) властивості 1—13 справедливі;

в) якщо у многочлені з цілими коефіцієнтами $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, який задано на множині цілих чисел \mathbb{Z} , усі коефіцієнти a_i замінити на коефіцієнти b_i , конгруентні a_i за модулем m , то дістанемо многочлен $g(x) = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$, конгруентний многочлену $f(x)$, тобто $f(x) \equiv g(x) \pmod{m}$;

г) якщо $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ — многочлен від одного аргументу x з цілими коефіцієнтами і $x \equiv x' \pmod{m}$, то $f(x) \equiv f(x') \pmod{m}$;

- д) $n^2 - 1 \equiv 0 \pmod{8}$, якщо n — непарне число;

- е) $a \equiv r \pmod{m}$, де r — остача від ділення a на m .

- е) $a \equiv b \pmod{\frac{m}{(x, m)}}$, якщо $ax \equiv bx \pmod{m}$;

ж) якщо $ac \equiv bd \pmod{m}$, $a \equiv b \pmod{m}$ і $(a, m) = 1$, то $c \equiv d \pmod{m}$.

11.4. Записати у вигляді конгруенцій такі умови:

- а) -38 і -3 дають при діленні на 7 одинакові остачі;

- б) при діленні на 8 число 53 дає остачу 5 ;

- в) $a+2$ ділиться на 5 ;

- г) $a^2 - b^2$ ділиться на $a - b$ ($a \neq b$);

- д) знайти остачу r від ділення -73 на 8 ;

- е) 20 є остача від ділення числа 389 на 41 ;

- е) числа 219 і 129 дають неоднакові остачі при діленні на 7 .

11.5. Охарактеризувати конгруенціями числа n , якщо:

- а) n — парне число;

- б) n — непарне число;

- в) n має вид $4k + 1$, $k \in \mathbb{Z}$;

- г) n має вид $5k + 3$, $k \in \mathbb{Z}$;

- д) n має вид $7k - 2$, $k \in \mathbb{Z}$;

- е) n має вид $-3 + 8k$, $k \in \mathbb{Z}$.

11.6. Довести, що:

- а) $121 \equiv 13145 \pmod{2}$;

- б) $121347 \equiv 92817 \pmod{10}$;

- в) $31 \equiv -9 \pmod{10}$;

- г) $(m-1)^2 \equiv 1 \pmod{m}$;

- д) $2m + 1 \equiv (m + 1)^2 \pmod{m}$;
 е) $26^{30} - 1 \equiv 0 \pmod{5 \cdot 7 \cdot 11 \cdot 31}$;
 є) $26^{15} + 1 \equiv 0 \pmod{3 \cdot 7 \cdot 31}$;
 ж) $26^{26} \equiv 14^{14} \pmod{10}$;
 з) $17^{72} \equiv 1 \pmod{10}$;
 к) $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$;
 л) $3^{14} \equiv -1 \pmod{29}$;
 м) $11 \cdot 13 \cdot 18 \cdot 19 \cdot 2322 \equiv 6 \pmod{7}$.

11.7. Довести, що:

- а) $5^{1812} \not\equiv 1964 \pmod{25}$;
 б) $7^{103} \not\equiv 3 \pmod{27}$;
 в) $4^{1965} \not\equiv 25 \pmod{10}$;
 г) $30 \cdot 17 \not\equiv 81 \cdot 19 \pmod{6}$;
 д) $11^{207} \not\equiv 6 \pmod{27}$;
 е) $6^{89} \not\equiv 7 \pmod{16}$;
 є) $13^{25} \not\equiv 5 \pmod{30}$;
 ж) $7^{101} \not\equiv 3 \pmod{35}$;
 з) $8^{107} \not\equiv 7 \pmod{14}$;
 к) $26^{15} - 1 \not\equiv 0 \pmod{5 \cdot 7}$;
 л) $7^{100} \not\equiv 3 \pmod{125}$;
 м) $(2n + 1)(2m + 1) \not\equiv 2k \pmod{6}$, $n, m, k \in \mathbb{Z}$.

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

- а) $(a + b)^p \equiv a^p + b^p \pmod{p}$, $a, b \in \mathbb{Z}$;
 б) $C_{p-1}^k \equiv (-1)^k \pmod{p}$;
 в) $C_{p-2}^k \equiv (-1)^k (k+1) \pmod{p}$;
 г) $a^p \equiv b^p \pmod{p^{n+1}}$, якщо $a \equiv b \pmod{p^n}$;
 д) $1^{2k+1} + 2^{2k+1} + 3^{2k+1} + \dots + (p-1)^{2k+1} \equiv 0 \pmod{p}$, де $p > 2$;
 е) $p^{p+2} + (p+2)^p \equiv 0 \pmod{2p+2}$, якщо $p > 2$;
 є) числа $-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -1, 0, 1, \dots, \frac{p-3}{2}, \frac{p-1}{2}$

попарно неконгруентні між собою за модулем p , $p > 2$.

11.9. Знайти остаточу від ділення:

- а) 15^{231} на 14;
 б) $15^{231} + 2$ на 16;
 в) $1532^5 - 1$ на 9;
 г) $12^{1231} + 14^{4324}$ на 13;
 д) 208^{208} на 23;
 е) $215783 - 7$ на 25;
 є) $379821 + 5$ на 17;
 ж) $10^{2732} + 10$ на 22;
 з) $18^{2815} - 3$ на 14;
 к) $2^{100} + 5^{200}$ на 29;
 л) $13^{1054} - 23 \cdot 16^{285} + 22^{17}$ на 15;
 м) $29^{2929} - 34^{3434} + 29 \cdot 41 \cdot 6^{231} - 24 \cdot 17^{120}$ на 31;
 н) a на 73, якщо $a^{100} \equiv 2 \pmod{73}$ і $a^{101} \equiv 69 \pmod{73}$. Як зміниться відповідь, якщо a ділити на 79 і $a^{25} \equiv 3 \pmod{79}$, $a^{26} \equiv 29 \pmod{79}$, $(a, 79) = 1$?

11.10.. Довести, що:

- | | |
|--------------------------------|-----------------------------------|
| a) $a - b - c \vdash 2$, | якщо $a + b - c \vdash 2$; |
| б) $18a + 5b \vdash 19$, | якщо $11a + 2b \vdash 19$; |
| в) $2a + 7b \vdash 17$, | якщо $a - 5b \vdash 17$; |
| г) $4a + 23b \vdash 16$, | якщо $12a - 7b \vdash 16$; |
| д) $10a + 7b \vdash 19$, | якщо $a - 5b \vdash 19$; |
| е) $11a - b + 2c \vdash 21$, | якщо $16a - 11b + c \vdash 21$; |
| ж) $a - 7b \vdash 31$, | якщо $6a - 11b \vdash 31$; |
| з) $5a + b \vdash 17$, | якщо $15a + 3b \vdash 17$; |
| к) $a - 4b + 41c \vdash 199$, | якщо $50a - b + 60c \vdash 388$. |

11.11. Довести, що при будь-якому натуральному n :

- | |
|--|
| а) $2^{3n} \equiv -1 \pmod{3^{n+1}}$; |
| б) $10^n + 17 \equiv 0 \pmod{3}$; |
| в) $3^{4n+3} \equiv 17 \pmod{10}$; |
| г) $24^{2n+1} \cdot 21^{n+2} \equiv 3^{n+2} \cdot 17^{2n+1} \pmod{19}$; |
| д) $48^{3n+1} + 16^{3n+1} + 1 \equiv 0 \pmod{13}$; |
| е) $2^{3^{4n+1}} + 3$ — складене число; |
| ж) $(m-1)^{m^n} \equiv -1 \pmod{m^{n+1}}$, де $m > 1$ — непарне число; |
| з) $3^{n+4} \equiv -1 \pmod{10}$, якщо $3^n \equiv -1 \pmod{10}$; |
| к) $2^{5n} \equiv 1 \pmod{31}$; |
| л) $3 \cdot 10^n + 24 \equiv 0 \pmod{54}$. |

11.12. Довести, що задані рівняння не мають розв'язків у натуральних числах:

- | | |
|-------------------------|---------------------------|
| а) $2^x + 7^y = 19^z$; | в) $24^x + 36^y = 61^z$; |
| б) $2^x + 5^y = 19^z$; | г) $20^x + 50^y = 71^z$. |

11.13. Довести, що при будь-яких цілих a , b і невід'ємному n :

- | |
|---|
| а) $(11a + 5)^{2n+1} + (11b + 6)^{2n+1} \equiv 0 \pmod{11}$; |
| б) $(13a + 3)^{3n+2} + (13b - 4)^{3n+2} + 1 \equiv 0 \pmod{13}$; |
| в) $9^{3n+1} + 3^{3n+1} + 1 \equiv 0 \pmod{13}$. |

11.14. Знайти такі натуральні k , l , m , щоб при будь-якому цілому a справдіжувалися такі конгруенції:

- | |
|---|
| а) $a^{3k} + a^{3l+1} + a^{3m+2} \equiv 0 \pmod{a^2 + a + 1}$; |
| б) $a^{3k} - a^{3l+1} + a^{3m+2} \equiv 0 \pmod{a^2 - a + 1}$; |
| в) $a^{3k} + a^{3l+1} + a^{3m+2} \equiv 0 \pmod{a^4 + a^2 + 1}$. |

11.15. Знайти останню цифру чисел:

- | |
|--|
| а) 2^{34} ; |
| б) 9^{9^9} ; |
| в) $(\dots ((7^7)^7)^7)^7$ — піднесення до степеня повторюється 1000 раз; |
| г) $7^{(7 \dots (7^{71}) \dots)}$ — піднесення до степеня повторюється 1000 раз. |

11.16. Знайти останні дві цифри чисел:

- а) 2^{999} ; д) 203^{203203} ;
 б) 3^{999} ; е) $14^{14^{14}}$;
 в) 2^{341} ; ж) 9^{9^9} ;
 г) 289^{289} ; ж) 7^{9^9} .

11.17. Нехай $F_n = 2^{2^n} + 1$ — число Ферма, де $n = 0, 1, 2, \dots$
Довести, що:

- а) $F_5 = 6411$;
 б) число F_n закінчується цифрою 7 при всіх n , крім $n=0$
і $n=1$.

§ 12. Класи лишків, повна і зведені системи лишків за даним модулем

Література

- [1] — § 15, с. 166—168, § 16, с. 168—170;
 [2] — § 15, с. 169—171, § 16, с. 171—173;
 [3] — гл. 12, § 2, 3, с. 399—404;
 [10] — гл. III, § 4, 5, с. 45—46;
 [11] — гл. 8, 9, с. 77—92;
 [12] — гл. II, § 2, 3, с. 43—51;
 [13] — § 16—18, с. 66—78.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Відношення конгруентності за даним модулем m є бінарним відношенням еквівалентності на множині цілих чисел Z . Класи еквівалентностей називають **класами лишків за даним модулем**. **Лишком** (або представником) класу за модулем m називають будь-яке число цього класу. Кільце цілих чисел Z розкладається на m класів лишків. До класу лишків, який містить число a , належать усі цілі числа x виду $x = a + mt$, де $t \in Z$. Цей клас позначатимемо символом $K_a^{(m)}$, причому, якщо йдеться тільки про класи лишків за тим самим модулем m , то можна писати K_a . Число a називають **представником класу лишків** $K_a^{(m)}$.

Представником класу лишків $K_a^{(m)}$ може бути будь-який елемент цього класу, тобто $K_a^{(m)} = K_b^{(m)}$, якщо $b \in K_a^{(m)}$. Якщо $K_a^{(m)} \cap K_b^{(m)} \neq \emptyset$, то $K_a^{(m)} = K_b^{(m)}$. Якщо $d > 1$, то $K_a^{(m)} = K_a^{(dm)} \cup K_{(a+m)}^{(dm)} \cup K_{(a+2m)}^{(dm)} \cup \dots \cup K_{(a+(d-1)m)}^{(dm)}$:

$$K_a^{(m)} + K_b^{(m)} = K_{a+b}^{(m)}, \quad K_a^{(m)} K_b^{(m)} = K_{ab}^{(m)}.$$

Множина всіх класів лишків за модулем m відносно додавання класів утворює комутативну групу, її називають **групою класів лишків**.

Множина класів лишків кільца цілих чисел за даним модулем m утворює комутативне кільце з одиницею, його позначають Z_m .

Якщо m — складене число, то в Z_m є дільники нуля, причому, якщо $m = m_1 m_2$, то зокрема,

$$K_{m_1}^{(m)} K_{m_2}^{(m)} = K_{\phi}^{(m)}, \text{ де } K_{m_1}^{(m)} \neq K_{\phi}^{(m)} \text{ і } K_{m_2}^{(m)} \neq K_{\phi}^{(m)}.$$

Якщо m — просте число, то Z_m — скінченне поле.

Повною системою лишків за модулем m називають будь-яку систему лишків, утворену з m чисел, взятих по одному з кожного класу лишків.

Існують такі основні повні системи лишків:

¹ Це було доведено ще Л. Ейлером (1707—1783).