

е) $P_{p^k}(a) = P_{2p^k}(a)$, якщо a — непарне число, $a \nmid p$, $k \in \mathbb{N}$; зокрема, довільний непарний первісний корінь g за модулем p^k є ним і за модулем $2p^k$.

17.19. Довести, що:

а) первісний корінь за модулем $m > 2$ завжди є квадратичним нелишком за модулем m ;

б) $P_{a^{m-1}}(a) = m$, якщо $a, m \in \mathbb{N}$ і $a > 1$;

в) $\varphi(a^m - 1) \equiv 0 \pmod{m}$, якщо $a, m \in \mathbb{N}$ і $a > 1$;

г) $P_m(a) = [P_{p_1^{a_1}}(a), P_{p_2^{a_2}}(a), \dots, P_{p_s^{a_s}}(a)]$, якщо $(a, m) = 1$ і $m = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ — канонічний розклад числа m ;

д) $P_{p^k}(a) = d$, якщо $a^d \equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbb{N}$, $k > 1$, і $(a, p^k) = 1$;

е) $P_{p^k}(a) = p^d$, якщо $a^d \not\equiv 1 \pmod{p^k}$, де $d = P_{p^{k-1}}(a)$, p — просте число, $k \in \mathbb{N}$, $k > 1$, і $(a, p^k) = 1$;

ж) $P_{5929}(16) = 1155$;

ж) число a є первісним коренем за модулем m тоді і тільки тоді, коли клас лішків $K_a^{(m)}$ є твірним елементом мультиплікативної групи кільця Z_m .

§ 18. Індекси за простим модулем. Двочленні конгруенції за простим модулем; таблиці індексів із застосуванням

Література

- [1] — § 19, с. 201—204;
- [2] — § 19, с. 204—207;
- [3] — гл. 12, § 5, с. 416—420;
- [10] — гл. VI, § 4, с. 90—92;
- [11] — гл. 19, гл. 20, с. 163—172;
- [12] — гл. IV, § 3, 4, с. 136—146;
- [13] — § 31, 32, с. 144—152.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай g — первісний корінь за простим модулем p , $a \in \mathbb{Z}$ і $(a, p) = 1$. Ціле невід'ємне число γ називається індексом числа a за модулем p при основі g , якщо

$$g^\gamma \equiv a \pmod{p}. \quad (1)$$

Взагалі, довільне значення x , яке задовольняє конгруенцію

$$b^x \equiv d \pmod{m}, \quad (2)$$

називається індексом числа d за модулем m при основі b і позначається

$$x \equiv \text{ind}_b d \pmod{m}. \quad (3)$$

При цьому m може бути й складеним числом, проте

$$(d, m) = (b, m) = 1.$$

Означення індексу можна записати ще так:

$$b^{\text{ind}_b d} \equiv d \pmod{m}. \quad (4)$$

Користуючись цим означенням, складають таблицю індексів за даною основою і модулем. Таблиці індексів за кожним простим модулем p (не дуже великим) містять дві таблиці: одна — знаходження індексу за числом, а друга — знаходження числа за індексом (таблиця антиіндексів).

Основні властивості індексів

1°. Усі індекси числа a за простим модулем p утворюють клас чисел за модулем $p - 1$. Точніше, якщо γ і γ^l — індекси числа a за модулем p (при будь-якій тій самій основі), то

$$\gamma \equiv \gamma^l \pmod{p-1};$$

2°. Для того щоб $a \equiv b \pmod{p}$, необхідно і достатньо, щоб $\text{ind}_g a \equiv \text{ind}_g b \pmod{p-1}$;

Якщо значення чисел або індексів виходять за можні таблиць, то ці дві властивості дають змогу переходити до найменших невід'ємних лишків: для чисел — за модулем p , для індексів — за модулем $p - 1$.

$$3^\circ. \text{ind}_g 1 \equiv 0 \pmod{p-1};$$

$$4^\circ. \text{ind}_g g \equiv 1 \pmod{p-1};$$

$$5^\circ. \text{ind}_g(a_1 a_2 \dots a_s) \equiv \text{ind}_g a_1 + \text{ind}_g a_2 + \dots + \text{ind}_g a_s \pmod{p-1};$$

$$6^\circ. \text{ind}_g a^n \equiv n \text{ind}_g a \pmod{p-1};$$

$$7^\circ. \text{ Якщо } a \mid b, \text{ то } \text{ind}_g \frac{a}{b} = \text{ind}_g a - \text{ind}_g b \pmod{p-1}.$$

Зазначимо, що перехід від конгруенції між числами до конгруенції іхніх індексів називається **індексацією**, а зворотний перехід — **потенціюванням**.

Якщо задано двочленну конгруенцію n -го степеня за простим модулем

$$ax^n \equiv b \pmod{p}, \quad (a, p) = 1, \quad n \in \mathbb{N}, \quad (5)$$

то її розв'язок знаходить з конгруенції

$$n \text{ind } x \equiv \text{ind } b - \text{ind } a \pmod{p-1}. \quad (6)$$

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Складти таблиці індексів та антиіндексів за модулем 23.

Розв'язання. Знайдемо один з первісних коренів за модулем 23 (найчастіше це найменший з первісних коренів). Перевіряючи безпосередньо, дістанемо, що число 5 є одним з первісних коренів за модулем 23, причому найменшим з них. Справді,

$$\varphi(23) = 22 \text{ і } 5^2 \not\equiv 1 \pmod{23}, \quad 5^{11} \not\equiv 1 \pmod{23}, \quad \text{а } 5^{22} \equiv 1 \pmod{23}.$$

Отже, $\delta_{23}(5) = 22$, тому 5 є первісний корінь за модулем 23. Візьмемо його за основу таблиці індексів і знайдемо найменші невід'ємні лишки степенів

$$5^0, 5^1, 5^2, \dots, 5^{22}$$

за модулем 23:

$$\begin{array}{llll} 5^0 \equiv 1 \pmod{23}, & 5^8 \equiv 16 \pmod{23}, & 5^{16} \equiv 3 \pmod{23}, \\ 5^1 \equiv 5 \pmod{23}, & 5^9 \equiv 11 \pmod{23}, & 5^{17} \equiv 15 \pmod{23}, \\ 5^2 \equiv 2 \pmod{23}, & 5^{10} \equiv 9 \pmod{23}, & 5^{18} \equiv 6 \pmod{23}, \\ 5^3 \equiv 10 \pmod{23}, & 5^{11} \equiv 22 \pmod{23}, & 5^{19} \equiv 7 \pmod{23}, \\ 5^4 \equiv 4 \pmod{23}, & 5^{12} \equiv 18 \pmod{23}, & 5^{20} \equiv 12 \pmod{23}, \\ 5^5 \equiv 20 \pmod{23}, & 5^{13} \equiv 21 \pmod{23}, & 5^{21} \equiv 14 \pmod{23}, \\ 5^6 \equiv 8 \pmod{23}, & 5^{14} \equiv 13 \pmod{23}, & \\ 5^7 \equiv 17 \pmod{23}, & 5^{15} \equiv 19 \pmod{23}, & \end{array}$$

Отже, $\text{ind}_5 1 = 0$, $\text{ind}_5 5 = 1$, $\text{ind}_5 2 = 2$, $\text{ind}_5 10 = 3$, $\text{ind}_5 4 = 0$, $\text{ind}_5 20 = 5, \dots$

Складаємо таблицю індексів за модулем 23 з основовою 5 (табл. 14).

Таблиця 14

| N | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|-----|---|----|----|----|----|----|----|----|----|----|
| 0 | | 0 | 2 | 16 | 4 | 1 | 18 | 19 | 6 | 10 |
| 1 | 3 | 9 | 20 | 14 | 21 | 17 | 8 | 7 | 12 | 15 |
| 2 | 5 | 13 | 11 | | | | | | | |

Тут номер рядка означає число десятків, а номер стовпця — число одиниць заданого числа. На перетині певного рядка і стовпця знаходиться відповідний індекс. Так, індекс числа 18 знайдемо на перетині рядка з номером 1 і стовпця з номером 8, тобто $\text{ind}_5 18 = 12$.

Щоб побудувати таблиці антиіндексів, використаємо таблицю індексів. Маємо (табл. 15):

Таблиця 15

| I | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|-----|----|----|----|----|----|----|---|----|----|----|
| 0 | 1 | 5 | 2 | 10 | 4 | 20 | 8 | 17 | 16 | 11 |
| 1 | 9 | 22 | 18 | 21 | 13 | 19 | 3 | 15 | 6 | 7 |
| 2 | 12 | 14 | | | | | | | | |

Зauważення. Оскільки вибір основи для складання таблиць індексів за даним модулем є довільним, то в різних підручниках і посібниках такі таблиці не не завжди збігаються. Проте це не впливає на остаточний результат при розв'язуванні задач за допомогою індексів. У таблицях індексів, які наведено в кінці цього посібника, вказано основу g , а також канонічний розклад числа $p - 1$ для даного простого модуля p .

2. Розв'язати конгруенцію

$$17x^{18} \equiv 22 \pmod{23}. \quad (1)$$

Розв'язання. Беремо індекси від обох частин конгруенції

$$\text{ind } 17 + 18 \text{ ind } x \equiv \text{ind } 22 \pmod{22}.$$

За табл. 14 маємо

$$\text{ind } 17 = 7, \text{ ind } 22 = 11$$

І тому

$$7 + 18 \text{ ind } x \equiv 11 \pmod{22},$$

або

$$18 \text{ ind } x \equiv 4 \pmod{22}. \quad (2)$$

Дістали лінійну конгруенцію відносно $\text{ind } x$. Розв'яземо її. Оскільки $(18, 22) = 2$ і $4 \nmid 2$, то ця конгруенція має дві розв'язки. Знайдемо їх штучним способом. Скоротимо спочатку обидві частини і модуль на 2:

$$9 \text{ ind } x \equiv 2 \pmod{11}.$$

Додамо до правої частини число -11 :

$$9 \text{ ind } x \equiv -9 \pmod{11}.$$

Скоротимо обидві частини на 9:

$$\text{ind } x \equiv -1 \pmod{11}.$$

Звідси дістаємо два розв'язки конгруенції (2):

$$\text{ind } x \equiv 10, 21 \pmod{22}.$$

За табл. 15 знаходимо відповідні два значення невідомого x :

$$x \equiv 9, 14 \pmod{23}.$$

Зauważення

1. Зрозуміло, що розв'язування конгруенцій за допомогою індексів можливе для довільного модуля, якщо тільки є відповідні таблиці індексів.

2. При індексуванні конгруенції за модулем m відбувається перехід до конгруенції за модулем $\varphi(m)$, а при потенціюванні конгруенції за модулем $\varphi(m)$ — перехід до конгруенції за модулем m .

Задачі

18.1. Скласти таблиці індексів за модулем p з основою g , якщо

- a) $p = 3, g = 2$; д) $p = 7, g = 5$;
- б) $p = 5, g = 2$; е) $p = 11, g = 2$;
- в) $p = 5, g = 3$; є) $p = 13, g = 2$;
- г) $p = 7, g = 3$; ж) $p = 29, g = 2$.

18.2. Скласти таблицю індексів за складеним модулем $m = 27$ з основою $g = 5$.

18.3. Нехай g — первісний корінь за модулем m . Довести, що:

а) конгруенція $b \equiv c \pmod{m}$ виконується тоді і тільки тоді, коли $\text{ind}_g b \equiv \text{ind}_g c \pmod{\varphi(m)}$ (тут $(b, m) = 1$);

б) $\text{ind}_m a = \text{ind}_{2m} a$, якщо $m = p^\alpha$, p — просте непарне число, $(a, 2p) = 1$.

18.4. Нехай g і t — два первісних корені за простим модулем p . Довести, що:

- а) $\text{ind}_g a \equiv \text{ind}_t a \cdot \text{ind}_t g \pmod{(p-1)}$;
- б) $\text{ind}_g a \equiv \text{ind}_g a \cdot \text{ind}_t g \pmod{(p-1)}$;
- в) $\text{ind}_g g \cdot \text{ind}_t t \equiv 1 \pmod{(p-1)}$;
- г) $\text{ind}_g a \equiv \text{ind}_t a (\text{ind}_t g)^{\varphi(p-1)-1} \pmod{(p-1)}$

(формула переходу від системи індексів з основою t до системи індексів з основою g).

18.5. Розв'язати лінійні конгруенції:

- а) $7x \equiv 23 \pmod{17}$; е) $125x \equiv 7 \pmod{79}$;
- б) $5x \equiv 13 \pmod{27}$; є) $65x \equiv 38 \pmod{83}$;
- в) $8x \equiv -11 \pmod{37}$; ж) $23x \equiv 9 \pmod{97}$;
- г) $47x \equiv 23 \pmod{73}$; з) $37x \equiv 5 \pmod{221}$.
- д) $53x \equiv 37 \pmod{79}$;

18.6. Розв'язати конгруенції другого степеня:

- а) $x^2 \equiv 15 \pmod{17}$; ж) $x^2 \equiv 40 \pmod{83}$;
- б) $x^2 \equiv 10 \pmod{27}$; з) $3x^2 - 5x - 2 \equiv 0 \pmod{11}$;
- в) $x^2 \equiv 47 \pmod{53}$; к) $2x^2 - 7x + 28 \equiv 0 \pmod{43}$;
- г) $x^2 \equiv 58 \pmod{61}$; л) $3x^2 - 8x + 44 \equiv 0 \pmod{47}$;
- д) $x^2 \equiv 59 \pmod{67}$; м) $x^2 \equiv 29 \pmod{59^2}$;
- е) $x^2 \equiv -28 \pmod{67}$; н) $x^2 \equiv 61 \pmod{73^2}$.
- є) $x^2 \equiv 54 \pmod{71}$;

18.7. Довести, що:

а) конгруенція $x^n \equiv a \pmod{m}$, $(a, m) = 1$ має тоді і тільки тоді розв'язки, коли $\text{ind}_a d : d$, де $d = (n, \varphi(m))$. Якщо конгруенція має розв'язки, то їх всього d ;

б) конгруенція $x^n \equiv a \pmod{p}$, де p — просте непарне число, має розв'язки тоді і тільки тоді, коли

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \text{ де } d = (n, p-1);$$

в) число a тоді і тільки тоді є квадратичним лишком за модулем непарного простого числа p , коли за цим модулем $\text{ind} a$ — число парне;

г) порядок $\delta = P_m(a)$ визначається рівністю $(\text{ind} a, \varphi(m)) = \frac{\varphi(m)}{\delta}$. Зокрема, належність числа a до первісних коренів за модулем m визначається рівністю $(\text{ind} a, \varphi(m)) = 1$;

д) користуючись властивостями індексів, можна встановити справедливість теореми Вільсона;

е) для простого числа p виду $2^n + 1$, де $n > 3$, число 3 є первісним коренем;

ж) індекс числа — 1 за простим непарним модулем p при будь-якій основі дорівнює $\frac{p-1}{2}$.

18.8. Скільки розв'язків мають такі конгруенції:

- | | |
|------------------------------------|-----------------------------------|
| а) $x^{15} \equiv 6 \pmod{37}$; | е) $x^5 \equiv 3 \pmod{71}$; |
| б) $x^{16} \equiv 10 \pmod{37}$; | ж) $x^{21} \equiv 5 \pmod{71}$; |
| в) $3x^3 \equiv 2 \pmod{37}$; | з) $x^{15} \equiv 46 \pmod{97}$; |
| г) $7x^7 \equiv 11 \pmod{41}$; | к) $x^{55} \equiv 17 \pmod{97}$; |
| д) $3x^{12} \equiv 31 \pmod{41}$; | л) $x^{60} \equiv 79 \pmod{97}$? |
| е) $5x^{30} \equiv 37 \pmod{41}$; | |

18.9. Розв'язати такі двочленні конгруенції:

- | | |
|-----------------------------------|-----------------------------------|
| а) $x^{10} \equiv 33 \pmod{37}$; | е) $x^{27} \equiv 39 \pmod{43}$; |
| б) $x^3 \equiv 34 \pmod{41}$; | ж) $x^{35} \equiv 17 \pmod{67}$; |
| в) $x^8 \equiv 31 \pmod{41}$; | ж) $x^{30} \equiv 14 \pmod{67}$; |
| г) $x^{12} \equiv 37 \pmod{41}$; | з) $x^{12} \equiv 27 \pmod{83}$; |
| д) $x^6 \equiv 37 \pmod{43}$; | к) $x^{48} \equiv 2 \pmod{97}$. |

18.10. Розв'язати такі двочленні конгруенції:

- | | |
|----------------------------------|-------------------------------------|
| а) $3x^3 \equiv 4 \pmod{7}$; | е) $23x^5 \equiv 15 \pmod{73}$; |
| б) $2x^8 \equiv 5 \pmod{13}$; | ж) $37x^6 \equiv 69 \pmod{73}$; |
| в) $15x^4 \equiv 17 \pmod{23}$; | з) $37x^{15} \equiv 62 \pmod{73}$; |
| г) $27x^5 \equiv 25 \pmod{31}$; | к) $44x^{21} \equiv 53 \pmod{73}$; |
| д) $13x^3 \equiv 24 \pmod{37}$; | л) $27x^{30} \equiv 41 \pmod{79}$. |
| е) $37x^8 \equiv 59 \pmod{61}$; | |

18.11. Розв'язати конгруенції:

- | | |
|--|--|
| а) $5x^{11} + 19 \equiv 0 \pmod{29}$; | д) $7x^{13} + 23 \equiv 0 \pmod{47}$; |
| б) $25x^7 + 7 \equiv 0 \pmod{31}$; | е) $x^7 + 27 \equiv 0 \pmod{53}$; |
| в) $17x^5 + 3 \equiv 0 \pmod{37}$; | ж) $x^{11} + 36 \equiv 0 \pmod{71}$. |
| г) $8x^9 + 17 \equiv 0 \pmod{41}$; | |

18.12. Знайти найменше натуральне число x , яке задовольняє такі конгруенції:

- | | |
|---------------------------------|---------------------------------|
| а) $8^x \equiv 1 \pmod{13}$; | д) $24^x \equiv 1 \pmod{31}$; |
| б) $27^x \equiv 1 \pmod{17}$; | е) $32^x \equiv 15 \pmod{37}$; |
| в) $5^x \equiv 17 \pmod{31}$; | ж) $23^x \equiv 37 \pmod{41}$; |
| г) $11^x \equiv 17 \pmod{31}$; | ж) $13^x \equiv 25 \pmod{43}$; |

- з) $16^x \equiv 11 \pmod{53}$; л) $44^x \equiv 19 \pmod{71}$;
 к) $2^x \equiv 7 \pmod{67}$; м) $18^x \equiv 53 \pmod{79}$.

18.13. Розв'язати двочленні показникові конгруенції:

- а) $3 \cdot 8^x \equiv 7 \pmod{23}$; г) $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$;
 б) $12^{7x} \equiv 15 \pmod{31}$; д) $25^{5x} \equiv 47 \pmod{61}$;
 в) $21^{3x} \equiv 21^5 \pmod{29}$; е) $6 \cdot 11^x \equiv 56 \pmod{61}$.

18.14. Розв'язати конгруенції:

- а) $13 \cdot 7^{5x} + 1 \equiv 0 \pmod{67}$;
 б) $7 \cdot 5^x + 1 \equiv 0 \pmod{73}$;
 в) $11 \cdot 5^{3x} + 70 \equiv 0 \pmod{79}$;
 г) $8 \cdot 7^x + 4 \equiv 0 \pmod{83}$.

18.15. Знайти порядок числа a за модулем m , якщо:

- а) $a = 6, m = 7$; д) $a = 27, m = 47$;
 б) $a = 6, m = 23$; е) $a = 13, m = 53$;
 в) $a = 7, m = 29$; є) $a = 10, m = 1739$.
 г) $a = 18, m = 41$; ж) $a = 32, m = 4331$.

18.16. Знаючи, що за простим модулем p $\text{ind}_g(a) \equiv b \pmod{p-1}$), знайти за цим модулем $\text{ind}_g a$, якщо:

- а) $p = 47, g = 5, a = 34, b = 34, t = 10$;
 б) $p = 73, g = 5, a = 54, b = 26, t = 11$;
 в) $p = 71, g = 7, a = 66, b = 63, t = 13$;
 г) $p = 71, g = 7, a = 56, b = 19, t = 11$.

18.17. Чи є первісними коренями за модулем 59 такі числа:

- а) 2; б) 3; в) 6; г) 8; д) 12; е) 13; є) 14; ж) 19?

18.18. Знаючи, що 2 є первісний корінь за модулями 101 і 163, розв'язати конгруенції:

- а) $3 \cdot 5^x \equiv 4 \cdot 3^{2x+1} \pmod{101}$;
 б) $2^x \equiv 3 \cdot 5^{3x} \pmod{163}$.

18.19. Користуючись критерієм Ейлера та застосовуючи властивості індексів, з'ясувати, які з чисел 15, 16, 17, 18, 19, 20 є квадратичними лишками за такими модулями: а) 23; б) 29; в) 41; г) 59; д) 79; е) 89.

18.20. Серед чисел зведененої системи лишків за модулем p знайти ті, порядок яких дорівнює числу r , якщо:

- а) $p = 43, r = 6$; в) $p = 61, r = 10$;
 б) $p = 43, r = 42$; г) $p = 61, r = 60$.

§ 19. Арифметичні застосування теорії конгруенцій

Література

- [1] — § 20, с. 205—210;
- [2] — § 20, с. 207—213;
- [3] — гл. 12, § 6, с. 421—429;
- [10] — гл. ХХІІІ, с. 201—209;
- [12] — гл. V, с. 147—160;
- [14] — § 33—36, с. 154—169.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорія конгруенцій має ряд арифметичних застосувань. Основними з них є:

- 1) виведення ознак подільності;
- 2) обчислення остач при діленні;