

к) $K_{ap-1}^{(p)} = K_1^{(p)}$, де p — просте число, a не ділиться на p .

12.13. Об'єднанням яких класів лишків є класи лишків:

а) $K_1^{(6)}, K_3^{(6)}, K_5^{(6)}$ за модулем 48;

б) $K_1^{(13)}, K_3^{(13)}, K_5^{(13)}, K_7^{(13)}$ за модулем 52;

в) $K_2^{(10)}, K_3^{(10)}, K_5^{(10)}, K_9^{(10)}$ за модулем 30.

13.14. Знайти класи лишків, обернені до таких класів:

а) $K_2^{(3)}$; б) $K_3^{(4)}$; в) $K_3^{(5)}$; г) $K_5^{(7)}$;

д) $K_7^{(8)}$; е) $K_5^{(9)}$; е) $K_7^{(10)}$; ж) $K_5^{(11)}$;

з) $K_{57}^{(61)}$; к) $K_{196}^{(501)}$; л) $K_{190}^{(501)}$; м) $K_{233}^{(1498)}$; и) $K_{501}^{(1993)}$.

§ 13. Теореми Ейлера і Ферма

Література

[1] — § 16, с. 174—175;

[2] — § 16, с. 178—179;

[3] — гл. 12, § 3, с. 408—409;

[10] — гл. 3, § 6;

[11] — гл. 2, с. 96—106;

[12] — гл. II, § 5, с. 57—60;

[14] — § 19, с. 79—80.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорема Ейлера. Якщо $m > 1$ і $(a, m) = 1$, то

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

Теорема Ферма (мала теорема Ферма). Якщо число p просте і $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$.

Наслідок. Якщо p — просте число, a — будь-яке ціле число, то $a^p \equiv a \pmod{p}$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти остаточу від ділення: а) 223^{2123} на 52; б) 264^{1020} на 138.

Розв'язання. а) Якщо треба знайти остаточу від ділення a^s на m , де $(s, m) = 1$ і $s > \varphi(m)$, то s можна подати у вигляді (за теоремою про ділення остаточою): $s = \varphi(m)q + r$, де $0 < r < \varphi(m)$. Оскільки $a^{\varphi(m)} \equiv 1 \pmod{m}$, то

$$a^s = a^{\varphi(m)q+r} = (a^{\varphi(m)})^q \cdot a^r \equiv a^r \pmod{m},$$

де a^r може бути значно меншим, ніж a^s .

У цьому разі маємо

$$52 = 2^2 \cdot 13, \quad \varphi(52) = 2^2 \cdot 13 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) = 24,$$

$$223 = 52 \cdot 4 + 15, \quad 2123 = 24 \cdot 88 + 11.$$

Тоді

$$223^{2123} = (52 \cdot 4 + 15)^{24 \cdot 88 + 11} \equiv 15^{11} = 15^9 \cdot 15^2 = (15^3)^3 \cdot 225 \equiv \\ \equiv (3375)^3 \cdot 17 \equiv (-5)^3 \cdot 17 \Rightarrow (-125) \cdot 17 \equiv (-21) \cdot 17 = -357 \equiv 7 \pmod{52}.$$

Отже, 223^{2123} при діленні на 52 дає остаточу 7.

б) Якщо $(a, m) \neq 1$ і $(a^s, m) = d > 1$, то знаходимо спочатку таке найменше k , що $a^k \equiv d$. Тоді $a^k = a_1d$, $m = m_1d$, де вже $(a, m_1) = 1$. Позначимо через x остаточу від ділення a^s на m . Тоді

$$x \equiv a^s = a^{s-k} \cdot a^k = a^{s-k} \cdot a_1d \pmod{m_1, d}.$$

Звідси $x = x_1 d$, де

$$x_1 \equiv a^{s-k} a_1 \pmod{m_1}.$$

Тепер x_1 знайдемо як добуток остач від ділення a^{s-k} і a_1 на m_1 . Оскільки $(a, m_1) = 1$, то остатчу від ділення a^{s-k} на m_1 можна знайти за теоремою Ейлера.

Маємо $(264, 138) = 6$. Якщо $x \equiv 264^{1020} \pmod{138}$, то $x \equiv 6x_1$. Оскільки $264 \equiv -126 \pmod{138}$, то $264^{1020} \equiv 126^{1020} \pmod{138}$. Найменшим k таким, що $126^k \equiv 6$, є 1. Тоді $a_1 \equiv 126 : 6 \equiv 21$, $m_1 \equiv 138 : 6 \equiv 23$ і $x_1 \equiv 21 \cdot 126 \pmod{23}$. Оскільки $\varphi(23) = 22$ і $1019 \equiv 22 \cdot 46 + 7$, то

$$\begin{aligned} x_1 &\equiv 21 \cdot 11^{1019} \equiv 21 \cdot 11^{22 \cdot 46 + 7} \equiv 21 \cdot (11^{22})^{46} \cdot 11^7 \equiv \\ &\equiv 21 \cdot 11^7 \equiv (-2) \cdot 11 \cdot 11^6 \equiv -22 \cdot 11^6 \equiv 11^6 \equiv (121)^3 \equiv \\ &\equiv 6^3 = 36 \cdot 6 \equiv (-10) \cdot 6 \equiv -60 \equiv 9 \pmod{23}. \end{aligned}$$

Тоді $x = 9 \cdot 6 = 54$. Отже, 264^{1020} при діленні на 138 дає остатчу 54.

2. Знайти останнії дві цифри числа 243^{402} .

Розв'язання. Досить знайти остатчу від ділення 243^{402} на 100. Маємо $243^{402} \equiv 43^{402} \pmod{100}$.

Оскільки $(43, 100) = 1$, а

$$\varphi(100) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40,$$

то $43^{40} \equiv 1 \pmod{100}$. Оскільки $402 = 40 \cdot 10 + 2$, то

$$43^{402} \equiv 43^{40 \cdot 10 + 2} \equiv 43^2 \equiv 1849 \equiv 49 \pmod{100}.$$

Отже, останніми двома цифрами числа 243^{402} є 4 і 9.

Зауваження. Щоб знайти k останніх цифр числа a , досить знайти остатчу від ділення цього числа на 10^k .

3. Довести, що $13^{176} - 1 \equiv 89$.

Розв'язання. Оскільки $13^{176} - 1 = (13^{88})^2 - 1 = (13^{88} - 1)(13^{88} + 1)$, а 89 — просте число, то досить показати, що на 89 ділиться хоч один з множників $13^{88} - 1$ чи $13^{88} + 1$. Згідно з малою теоремою Ферма,

$$13^{88} \equiv 1 \pmod{89},$$

звідки $13^{88} - 1 \equiv 89$. Отже, $13^{176} - 1 \equiv 89$.

Задачі

13.1. Чи справджується теорема Ейлера для таких чисел:

- | | |
|-------------------------|-------------------------|
| а) $a = 2$, $m = 9$; | е) $a = 4$, $m = 9$; |
| б) $a = 2$, $m = 15$; | е) $a = 5$, $m = 24$; |
| в) $a = 3$, $m = 4$; | ж) $a = 2$, $m = 33$; |
| г) $a = 3$, $m = 9$; | з) $a = 3$, $m = 24$? |
| д) $a = 3$, $m = 16$; | |

13.2. Чи справджується мала теорема Ферма для таких чисел:

- | | |
|-------------------------|-------------------------|
| а) $a = 2$, $p = 3$; | е) $a = 5$, $p = 3$; |
| б) $a = 2$, $p = 5$; | е) $a = 5$, $p = 7$; |
| в) $a = 3$, $p = 2$; | ж) $a = 4$, $p = 3$; |
| г) $a = 10$, $p = 5$; | з) $a = 4$, $p = 5$; |
| д) $a = 5$, $p = 2$; | к) $a = 14$, $p = 7$? |

13.3. Користуючись теоремою Ейлера, знайти остаточу від ділення:

- а) 7^{67} на 12; е) 293^{275} на 48;
б) 109^{345} на 14; е) 439^{291} на 60;
в) 197^{157} на 35; ж) 527^{144} на 65;
г) 356^{273} на 39; з) 353^{160} на 75;
д) 383^{175} на 45; к) 485^{84} на 129.

13.4. Користуючись малою теоремою Ферма, знайти остаточу від ділення:

- а) 93^{253} на 7; д) 2598^{33} на 17;
б) 5008^{10000} на 5, 7, 11, 13; е) 230^{347} на 37;
в) 42^{50} на 17; е) 71^{50} на 67;
г) 20^{59} на 17; ж) 512^{402} на 101.

13.5. Знайти остаточу від ділення:

- а) 45^{83} на 24; г) 204^{41} на 111;
б) 6^{76} на 26; д) 460^{150} на 425.
в) 96^{113} на 92;

13.6. Знайти остаточу від ділення:

- а) $7^{100} + 8^{100}$ на 5; е) $15^{60} + 20^{30}$ на 13;
б) $10^{100} + 40^{100}$ на 7; е) $5^{70} + 7^{50}$ на 12;
в) $3^{100} + 4^{100}$ на 7; ж) $3^{500} + 7^{500}$ на 101;
г) $5^{50} + 25^{70}$ на 9; з) $(12 \cdot 371^{56} + 145)^{28}$ на 111;
д) $25^{80} + 40^{80}$ на 11; к) $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

13.7. Знайти дві останні цифри числа:

- а) 3^{100} ; д) 17^{900} ; з) 2^{100} ;
б) 3^{219} ; е) 19^{882} ; к) 2^{153} ;
в) 11^{243} ; е) 903^{1294} ; л) 102^{54} .
г) 13^{219} ; ж) 573^{1931} ;

13.8. Розв'язати ті з задач 11.9 і 11.16, до яких можна застосувати теореми Ейлера і Ферма.

13.9. Довести, що:

- а) $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$;
б) $2^{19(73-1)} \equiv 1 \pmod{19 \cdot 73}$;
в) $5^{17 \cdot 19} \equiv 23 \pmod{17 \cdot 19}$;
г) $2^{1093 \cdot 1092} \equiv 1 \pmod{1093^2}$;
д) $2^{73 \cdot 37-1} \equiv 1 \pmod{73 \cdot 37}$.

13.10. Довести, що:

- а) $a^7 - a : 42$;
б) $a^{11} - a : 66$;
в) $a^{21} - a^3 : 27$;
г) $a^{42} - a^2 : 100$;
д) $a^{103} - a^3 : 125$;
е) $a^{12} - b^{12} : 65$, якщо $(a, 65) = (b, 65) = 1$;
ж) $a^{560} - 1 : 561$, $(a, 561) = 1$;
з) $a^{561} - a : 11$;

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 $a_n \not\equiv 0 \pmod{m}$, то n називається степенем конгруенції.

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

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