

5. Конгруенції і кільця класів лишків

5.1. Конгруенції

Зафіксуємо натуральне число $n \geq 1$. Будемо говорити, що цілі числа a і b *конгруентні* (або порівняльні) *за модулем числа n* (і писатимемо $a \equiv b \pmod{n}$), якщо різниця $a - b$ ділиться на n . Наприклад, $27 \equiv -7 \pmod{10}$, бо $27 - (-7) = 34 = 2 \cdot 17$. Довільні два непарних числа конгруентні за модулем 2, бо їх різниця є парним числом. Якщо у двох натуральних чисел одна й та ж остання цифра, то вони конгруентні за модулем 10.

Вирази $27 \equiv -7 \pmod{17}$, $347 \equiv 217 \pmod{10}$, $a \equiv b \pmod{n}$ та їм подібні називаються *конгруенціями*.

Теорема 5.1 (критерій конгруентності). $a \equiv b \pmod{n}$ тоді й лише тоді, коли a і b при діленні на n дають однакові остачі.

Доведення. Розділимо a і b на n з остачею: $a = q_1 n + r_1$, $b = q_2 n + r_2$. Тоді $a - b = (q_1 - q_2)n + (r_1 - r_2)$. Перший доданок у правій частині ділиться на n . Тому подільність $a - b$ на n рівносильна подільності на n другого доданку $r_1 - r_2$. Але $n > r_1 \geq r_1 - r_2 \geq -r_2 > -n$. Єдине число з проміжку $(-n, n)$, яке ділиться на n , це 0. Отже, подільність $a - b$ на n рівносильна умові $r_1 - r_2 = 0$, тобто $r_1 = r_2$. \square

Наслідок 1. Якщо остача від ділення a на n дорівнює r , то $a \equiv r \pmod{n}$.

Із цього наслідку стає зрозумілим позначення $a \pmod{n}$ для остачі від ділення a на n .

Наслідок 2. Для фіксованого n відношення конгруентності $a \equiv b \pmod{n}$ на множині \mathbb{Z} цілих чисел є відношенням еквівалентності.

Доведення. За теоремою 5.1 це відношення збігається з відношенням “ a і b мають однакові остачі при діленні на n ”, рефлексивність, симетричність і транзитивність якого очевидні. \square

Кожне відношення еквівалентності на множині визначає розбиття цієї множини на класи еквівалентності. Для відношення $a \equiv b \pmod{n}$ на множині \mathbb{Z} класи еквівалентності називаються *класами лишків за модулем n* . Клас лишків, який містить число a , будемо позначати через \bar{a} або $\bar{a} \pmod{n}$, якщо треба вказати і число n .

Задача 5.1. Розбити множину чисел 13, 41, 9, 88, 117, 36, 95, 1999, 146, 207 на класи попарно конгруентних за модулем 5.

Розв'язання. Остачі від ділення на 5 дорівнюють відповідно 3, 1, 4, 3, 2, 1, 0, 4, 1, 2. Тому дана множина розпадається на такі класи попарно конгруентних чисел: {13, 88}, {41, 36, 146}, {9, 1999}, {117, 207}, {95}. \square

Неважко підрахувати кількість класів лишків за модулем n . Справді, з теореми 5.1 випливає, що різні остачі від ділення на n потрапляють у різні класи, а з наслідку 1 – що кожен клас містить якусь остаточу. Отже, клас лишків однозначно характеризується тією єдиною остаточею від ділення на n , яку він містить. Тому класів буде стільки ж, скільки остач, тобто n . Множину $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$ всіх класів лишків за модулем n звичайно позначають \mathbb{Z}_n .

Наприклад, за модулем 3 маємо 3 класи лишків: $\overline{0} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ (всі числа, які при діленні на 3 дають в остатці 0), $\overline{1} = \{\dots, -5, -2, 1, 4, 7, \dots\}$ (остача 1) і $\overline{2} = \{\dots, -4, -1, 2, 5, 8, \dots\}$ (остача 2).

Твердження про характеризацію класу лишків остаточею від ділення на n можна дещо узагальнити.

Вправа 5.1. Довести, що $\bar{a} \pmod n = \{a + kn : k \in \mathbb{Z}\}$.

Задача 5.2. Довести, що з конгруенції $7a - 13b + 8c \equiv 0 \pmod{15}$ випливає конгруенція $11a + b + 4c \equiv 0 \pmod{15}$.

Розв'язання. Позначимо $A = 7a - 13b + 8c$, $B = 11a + b + 4c$. Треба довести, що з подільності A на 15 випливає подільність B на 15. Маємо: $2A + B = 25a - 25b + 20c = 5 \cdot (5a - 5b + 4c)$. Тому $B = (2A + B) - 2A$ ділиться на 5. Крім того, $2A - B = 3a - 27b + 12c = 3 \cdot (a - 9b + c)$. Тому $B = 2A - (2A - B)$ ділиться на 3. Числа 5 і 3 взаємно прості. Тому B ділиться і на їх добуток $5 \cdot 3 = 15$. \square

Задача 5.3. Довести, що для кожного цілого числа a виконується конгруенція $a^5 \equiv a \pmod{30}$.

Розв'язання. Треба довести, що $a^5 - a$ ділиться на 30. Із розкладу $a^5 - a = a(a^4 - 1) = a(a^2 - 1)(a^2 + 1) = (a - 1)a(a + 1)(a^2 + 1)$ випливає, що $a^5 - a$ ділиться на 2 (бо з двох послідовних цілих чисел $a - 1$ і a одне обов'язково є парним) і на 3 (бо з трьох послідовних цілих чисел $a - 1$, a і $a + 1$ одне обов'язково ділиться на 3). Якщо при діленні a на 5 остача дорівнює 1, 0 або 4, то на 5 ділиться відповідно множник $a - 1$, a або $a + 1$. Якщо остача дорівнює 2, то a має вигляд $a = 5k + 2$ і

$a^2 + 1 = (5k+2)^2 + 1 = 25k^2 + 20k + 5$ ділиться на 5. Аналогічно у випадку остачі 3 маємо: $a^2 + 1 = (5k+3)^2 + 1 = 25k^2 + 30k + 10 = 5 \cdot (5k^2 + 6k + 2)$. Отже, $a^5 - a$ завжди ділиться на кожне з простих чисел 2, 3 і 5, а тому ділиться і на їх добуток $2 \cdot 3 \cdot 5 = 30$. \square

Задача 5.4. Довести, що для взаємно простого з 6 числа n виконується конгруенція $n^2 \equiv 1 \pmod{24}$.

Розв'язання. Щоб довести, що $n^2 - 1$ ділиться на 24, досить показати, що $n^2 - 1 = (n-1)(n+1)$ ділиться на 8 і на 3. За умовою n непарне і не ділиться на 3. Тому один із множників $n-1$ або $n+1$ ділиться на 3, бо з трьох послідовних чисел $n-1$, n і $n+1$ одне обов'язково ділиться на 3. Крім того, $n-1$ і $n+1$ – послідовні парні числа, тому одне з них має ділитись на 4. Отже, добуток $(n-1)(n+1)$ ділиться на $2 \cdot 4 = 8$. \square

5.2. Арифметика конгруенцій

Теорема 5.2 (про додавання конгруенцій). Якщо $a_1 \equiv b_1 \pmod{n}$ і $a_2 \equiv b_2 \pmod{n}$, то $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.

Доведення. $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$. Але за умовою кожний з двох доданків правої частини ділиться на n . Тому й ліва частина ділиться на n . \square

Наслідок 1. До обох частин конгруенції можна додати одне й те ж число.

Доведення. Додати до обох частин конгруенції $a \equiv b \pmod{n}$ число $b - c$ – це все одно, що додати конгруенцію $c \equiv c \pmod{n}$. \square

Наслідок 2. Будь-який з доданків можна перенести на інший бік конгруенції, змінивши знак доданку на протилежний.

Доведення. Перенести в конгруенції $a + b \equiv c \pmod{n}$ на інший бік доданок c – це все одно, що додати конгруенцію $-b \equiv -b \pmod{n}$. \square

Задача 5.5. Довести, що жодне натуральне число вигляду $4k + 3$ не можна подати у вигляді суми двох квадратів.

Розв'язання. Припустимо, що $4k + 3 = a^2 + b^2$. Тоді

$$a^2 + b^2 \equiv 4k + 3 \equiv 3 \pmod{n}. \quad (5.1)$$

Із рівностей $(2m)^2 = 4m^2$ і $(2m+1)^2 = 4m^2 + 4m + 1$ випливає, що квадрат числа може бути порівняльним за модулем 4 лише з 0 або з 1. Але тоді або $a^2 + b^2 \equiv 0 \pmod{n}$, або $a^2 + b^2 \equiv 1 \pmod{n}$, або $a^2 + b^2 \equiv 2 \pmod{n}$. Кожна з цих конгруенцій суперечить конгруенції (5.1), тому рівність $4k + 3 = a^2 + b^2$ неможлива. \square

Теорема 5.3 (про множення конгруенцій). Якщо $a_1 \equiv b_1 \pmod{n}$ і $a_2 \equiv b_2 \pmod{n}$, то $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Доведення. Використаємо стандартний трюк із додаванням і відніманням одного й того ж члена: $a_1 a_2 - b_1 b_2 = a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2$. Права частина ділиться на n , бо за умовою множники $a_2 - b_2$ і $a_1 - b_1$ кратні n . Тому й ліва частина ділиться на n . \square

Наслідок 1. Обидві частини конгруенції можна помножити на одне й те ж число.

Доведення. Помножити обидві частини на число c – це все одно, що помножити на конгруенцію $c \equiv c \pmod{n}$. \square

Наслідок 2. Обидві частини конгруенції можна піднести до одного й того ж натурального степеня k .

Доведення. Піднести обидві частини конгруенції $a \equiv b \pmod{n}$ до степеня k – це все одно, що перемножити k конгруенцій $a \equiv b \pmod{n}, \dots, a \equiv b \pmod{n}$. \square

Задача 5.6. Довести, що $2^{2^5} + 1$ ділиться на 641.

Розв'язання. Оскільки $2^5 = 32$, то треба довести, що $2^{32} + 1 \equiv 0 \pmod{641}$. Маємо: $2^{10} = 1024 \equiv 383 \pmod{641}$, $2^{15} = 2^{10} \cdot 2^5 = 383 \cdot 32 = 12256 \equiv 77 \pmod{641}$, $2^{30} = (2^{15})^2 = 77^2 = 5929 \equiv 160 \pmod{641}$. Тому $2^{32} + 1 = 2^{30} \cdot 4 + 1 = 160 \cdot 4 + 1 = 641 \equiv 0 \pmod{641}$. \square

Цікава історія цієї задачі. У середині ХVІІ ст. славетний французький математик Ферма висловив переконання, що всі числа вигляду $2^{2^k} + 1$ є простими. Це справді так для $k = 0, 1, 2, 3, 4$ (відповідні прості числа – це 3, 5, 17, 257 і 65537). У 1739 р. не менш славетний швейцарський математик Ойлер спростував гіпотезу Ферма, довівши, що $2^{2^5} + 1$ ділиться на 641 (головна трудність зовсім не в перевірці самого факту подільності. Набагато важче цей дільник знайти, адже менших за 641 дільників числа $2^{2^5} + 1$ не має).

Задача 5.7. Знайти остачу від ділення числа $5 \cdot 11 \cdot 19 \cdot 29 \cdot 101 \cdot 197$ на 13.

Розв'язання. $19 \equiv 6 \pmod{13}$, $29 \equiv 3 \pmod{13}$, $101 \equiv 10 \pmod{13}$, $197 \equiv 2 \pmod{13}$. Тому $5 \cdot 11 \cdot 19 \cdot 29 \cdot 101 \cdot 197 \equiv 5 \cdot 11 \cdot 6 \cdot 3 \cdot 10 \cdot 2 = 55 \cdot 18 \cdot 20 = 3 \cdot 5 \cdot 7 = 105 \equiv 1 \pmod{13}$. Отже, шукана остача дорівнює 1. \square

Задача 5.8. Знайти дві останні цифри числа 3^{100} .

Розв'язання. Якщо $n = \overline{a_k \dots a_1 a_0}$, то число $\overline{a_1 a_0}$ є остачею від ділення n на 100. Маємо: $3^5 = 243 \equiv 43 \pmod{100}$, $3^{10} = (3^5)^2 = 43^2 = 1849 \equiv 49 \pmod{100}$, $3^{20} = (3^{10})^2 = 49^2 = 2401 \equiv 1 \pmod{100}$, $3^{100} = (3^{20})^5 = 1^5 \equiv 1 \pmod{100}$. Отже, останніми цифрами будуть 01. \square

Теорема 5.4 (про скорочення конгруенції на спільний множник).

Якщо $ac \equiv bc \pmod{n}$ і c взаємно просте з n , то $a \equiv b \pmod{n}$.

Доведення. За умовою $ac - bc = (a - b)c$ ділиться на n . Із взаємної простоти n і c і твердження 1.2(b) випливає, що $n | a - b$. \square

Зауваження. Вимога в теоремі 5.4 взаємної простоти чисел n і c дуже суттєва. У протилежному разі скорочення на спільний множник може привести до помилки. Наприклад, $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$, але $2 \neq 4 \pmod{6}$; $3 \cdot 2 \equiv 9 \cdot 2 \pmod{12}$, але $3 \neq 9 \pmod{12}$.

Теорема 5.5. Якщо $f(x_1, \dots, x_k)$ – многочлен від змінних x_1, \dots, x_k з цілими коефіцієнтами і $a_1 \equiv b_1 \pmod{n}, \dots, a_k \equiv b_k \pmod{n}$, то $f(a_1, \dots, a_k) \equiv f(b_1, \dots, b_k) \pmod{n}$.

Доведення. Для одночлена $ax_1^{m_1} \dots x_k^{m_k}$ це випливає з теореми 5.3, а для довільних многочленів (які є сумами одночленів) треба ще скористатись теоремою 5.2. \square

Теореми 5.2 і 5.3 дозволяють природним чином визначити додавання і множення класів лишків за модулем n : *сумою* класів \bar{a} і \bar{b} назовемо клас $\bar{a} + \bar{b}$, а їх *добутком* – клас \bar{ab} . Із теореми 5.2 випливає, що результат додавання $\bar{a} + \bar{b}$ не залежить від вибору представників a і b класів \bar{a} і \bar{b} . Справді, якщо \bar{a} і \bar{b} – інші представники, то $a \equiv \bar{a} \pmod{n}$, $b \equiv \bar{b} \pmod{n}$ і $a + b \equiv \bar{a} + \bar{b} \pmod{n}$. Тому $a + b$ і $\bar{a} + \bar{b}$ лежать в одному класі лишків, тобто $\bar{a} + \bar{b} = \bar{a} + \bar{b}$. Коректність означення дій множення доводиться аналогічно.

Для прикладу наведемо таблиці додавання і множення класів лишків за модулем 6:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$						
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Додавання і множення класів лишків своїми властивостями дуже нагадує додавання і множення звичайних цілих чисел.

Теорема 5.6. *Множина \mathbb{Z}_n класів лишків за модулем n утворює відносно додавання $\bar{a} + \bar{b} := \overline{a+b}$ і множення $\bar{a} \cdot \bar{b} := \overline{ab}$ комутативне кільце з одиницею.*

Доведення зводиться до чесної перевірки всіх аксіом кільця. Наприклад, з рівності $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}$ випливає, що одиницею кільця \mathbb{Z}_n буде клас лишків $\bar{1}$, який містить звичайну одиницю 1. Дистрибутивний закон випливає з рівностей

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} = \overline{a \cdot (b + c)} = \overline{ab} + \overline{ac} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

(у третьій рівності ми скористалися дистрибутивним законом для цілих чисел). Решта аксіом перевіряється аналогічно. \square

За означенням класів лишків рівність $\bar{a} = \bar{b}$ в кільці \mathbb{Z}_n рівносильна конгруенції $a \equiv b \pmod{n}$. Корисно якомога раніше навчитись вільно переходити від рівностей в \mathbb{Z}_n до конгруенцій за модулем n і навпаки.

Клас лишків \bar{a} з кільця \mathbb{Z}_n називається *оборотним*, якщо існує такий клас $\bar{b} \in \mathbb{Z}_n$, що $\bar{a} \cdot \bar{b} = 1$. Тоді клас \bar{b} називають *оберненим до \bar{a}* . У курсі алгебри доводиться, що в кільці кожний елемент має не більше одного оберненого. Тому обернений до \bar{a} клас лишків \bar{b} (якщо він існує) визначений однозначно, і ми будемо писати $\bar{b} = \bar{a}^{-1}$.

Із таблиці множення для \mathbb{Z}_6 видно, що далеко не кожний клас лишків оборотний (в \mathbb{Z}_6 такими будуть лише $\bar{1}$ і $\bar{5}$).

Теорема 5.7 (критерій оборотності в кільці класів лишків). *Клас лишків $\bar{a} \in \mathbb{Z}_n$ оборотний тоді й лише тоді, коли a і n взаємно прості.*

Доведення. Необхідність. Нехай клас лишків \bar{a} оборотний і $\bar{a} \cdot \bar{b} = \bar{1}$. Тоді $a\bar{b} = \bar{1}$ і $a\bar{b} \equiv 1 \pmod{n}$, тобто $a\bar{b} - 1 = kn$ для деякого цілого числа n . Із рівності $1 = ab - kn$ і теореми 1.6 випливає, що числа a і n – взаємно прості.

Достатність. Якщо a і n взаємно прості, то за тільки що згаданою теоремою 1.6 існують такі числа b і m , що $1 = ab + mn$. Але тоді

$$\bar{1} = \overline{ab + mn} = \overline{ab} + \overline{mn} = \bar{a} \cdot \bar{b} + \bar{m} \cdot \bar{n} = \bar{a} \cdot \bar{b} + \bar{m} \cdot \bar{0} = \bar{a} \cdot \bar{b} + \bar{0} = \bar{a} \cdot \bar{b},$$

тобо $n \equiv 0 \pmod{n}$ і $\bar{n} = \bar{0}$. Отже, клас лишків \bar{a} є оборотним. \square

Наслідок 1. У кільці класів лишків \mathbb{Z}_n добуток оборотних елементів також буде оборотним елементом.

В алгебрі доводиться, що в будь-якому кільці добуток оборотних елементів є оборотним. Незалежне доведення для кільця \mathbb{Z}_n випливає з теореми 5.7 і того, що добуток двох чисел, взаємно простих з n , теж буде взаємно простим з n (тврдження 1.2(a)).

Із теореми 5.7 і рівності $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ випливає, що кількість оборотних елементів у кільці \mathbb{Z}_n дорівнює числу елементів множини $\{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$, взаємно простих з числом n , тобто значенню $\varphi(n)$ функції Ойлера. Таким чином, маємо

Наслідок 2. Кільце \mathbb{Z}_n має $\varphi(n)$ оборотних елементів.

Теорема 5.8. Кільце \mathbb{Z}_n буде полем тоді й лише тоді, коли число n є простим.

Доведення. За означенням комутативне кільце з одиницею є полем, якщо всі ненульові елементи кільця оборотні. Із наслідку 2 теореми 5.7 випливає, що необхідно і достатньо умовою цього є виконання рівності

$$\varphi(n) = n - 1. \quad (5.2)$$

Якщо канонічний розклад числа n має вигляд $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, то за формулою для $\varphi(n)$ з теореми 2.6 маємо:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right) \leq n \left(1 - \frac{1}{p_1}\right) = n - \frac{n}{p_1} \leq n - 1. \quad (5.3)$$

Рівність (5.2) виконується тоді й лише тоді, коли в (5.3) скрізь будуть рівності. Останнє буде в тому і тільки в тому випадку, коли $m = 1$ і $\frac{n}{p_1} - 1$, тобто коли $n = p_1$. Отже, \mathbb{Z}_n є полем тоді й лише тоді, коли n – просте число. \square

Для оборотного класу лишків \bar{b} добуток $\bar{a} \cdot \bar{b}^{-1}$ записують також у вигляді \bar{a}/\bar{b} і говорять про ділення \bar{a} на \bar{b} .

Твердження 5.1. Якщо $b|a$ і клас \bar{b} є оборотним елементом кільця \mathbb{Z}_n , то $\frac{\bar{a}}{\bar{b}} = \overline{\left(\frac{a}{b}\right)}$.

Доведення. Нехай $a = cb$. Тоді $\bar{a} = \bar{c} \cdot \bar{b}$, звідки

$$\frac{\bar{a}}{\bar{b}} = \bar{a} \cdot \bar{b}^{-1} = \bar{c} \cdot \bar{b} \cdot \bar{b}^{-1} = \bar{c} \cdot \bar{1} = \bar{c} = \overline{\left(\frac{a}{b}\right)}. \quad \square$$

Задача 5.9. Довести, що для простого числа p і біноміального коефіцієнта $\binom{p-1}{k}$ виконується конгруенція

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}. \quad (5.4)$$

Розв'язання. Для $k = 0$ конгруенція (5.4) виконується: $\binom{p-1}{0} = 1 = (-1)^0$. Нехай тепер $0 < k \leq p-1$. Запишемо очевидні конгруенції $p-1 \equiv -1 \pmod{p}$, $p-2 \equiv -2 \pmod{p}$, \dots , $p-k \equiv -k \pmod{p}$. Перемноживши їх, дістанемо: $(p-1)(p-2)\dots(p-k) \equiv (-1)^k 1 \cdot 2 \cdot \dots \cdot k \pmod{p}$, або, після переходу до класів лишків за модулем p ,

$$\overline{(p-1)(p-2)\dots(p-k)} = \overline{(-1)^k} \cdot \overline{1 \cdot 2 \cdot \dots \cdot k}. \quad (5.5)$$

Клас $\overline{1 \cdot 2 \cdot \dots \cdot k}$ є оборотним у кільці \mathbb{Z}_n , бо $k \leq p-1$ і добуток $1 \cdot 2 \cdot \dots \cdot k$ взаємно простий з p . Крім того, число

$$\binom{p-1}{k} = \frac{(p-1)(p-2)\dots(p-k)}{1 \cdot 2 \cdot \dots \cdot k}$$

— ціле, тому $1 \cdot 2 \cdot \dots \cdot k | (p-1)(p-2)\dots(p-k)$. Використовуючи твердження 5.1 і рівність (5.5), одержуємо:

$$\overline{\binom{p-1}{k}} = \overline{\frac{(p-1)(p-2)\dots(p-k)}{1 \cdot 2 \cdot \dots \cdot k}} = \overline{(-1)^k},$$

що рівносильно конгруенції (5.4). \square

Якщо n маленьке, то для оборотного елемента $\bar{a} \in \mathbb{Z}_n$ знайти обернений можна за допомогою простого перебору всіх елементів із \mathbb{Z}_n . Для

великих n бажано мати якийсь кращий метод. Один із способів обчислення оберненого елемента \bar{a}^{-1} підказує доведення теореми 5.7. Справді, з цього доведення випливає, що ми знатимемо елемент $\bar{b} = \bar{a}^{-1}$, якщо будемо мати розклад $1 = ab + tn$. А такий розклад можна знайти за допомогою алгоритма Евкліда. Відповідну процедуру описано в п. 2.7.

Задача 5.10. Знайти число a , якщо $a^{36} \equiv 68 \pmod{83}$ і $a^{37} \equiv 40 \pmod{83}$.

Розв'язання. У кільці лишків \mathbb{Z}_{83} дані умови перепишуться як $\bar{a}^{36} = \bar{68}$ і $\bar{a}^{37} = \bar{40}$. Звідси

$$\bar{a} = \frac{\bar{a}^{37}}{\bar{a}^{36}} = \frac{\bar{40}}{\bar{68}}.$$

Елемент $\bar{68}^{-1}$ шукаємо за допомогою алгоритма Евкліда. Маємо: $83 = 1 \cdot 68 + 15$, $68 = 4 \cdot 15 + 8$, $15 = 1 \cdot 8 + 7$, $8 = 1 \cdot 7 + 1$. Звідси $1 = 1 \cdot 8 - 1 \cdot 7 = 1 \cdot 8 - 1(1 \cdot 15 - 1 \cdot 8) = 2 \cdot 8 - 1 \cdot 15 = 2(1 \cdot 68 - 4 \cdot 15) - 1 \cdot 15 = 2 \cdot 68 - 9 \cdot 15 = 2 \cdot 68 - 9(1 \cdot 83 - 1 \cdot 68) = 11 \cdot 68 - 9 \cdot 83$. Тому $68^{-1} = \bar{11}$ і $\bar{a} = \bar{40} \cdot \bar{68}^{-1} = \bar{40} \cdot \bar{11} = \bar{40} \cdot \bar{11} = \bar{440} = \bar{25}$. Отже, $a \equiv 25 \pmod{83}$. \square

Завершимо параграф властивостями конгруенцій, пов'язаними зі зміною модуля.

Теорема 5.9. (a) Для кожного натурального числа k конгруенції $a \equiv b \pmod{n}$ і $ak \equiv bk \pmod{nk}$ рівносильні.

(b) Якщо $a \equiv b \pmod{n_1}$, ..., $a \equiv b \pmod{n_k}$, то для найменшого спільного кратного n чисел n_1, \dots, n_k виконується конгруенція $a \equiv b \pmod{n}$.

(c) Якщо $a \equiv b \pmod{n}$ і d ділить n , то $a \equiv b \pmod{d}$.

Доведення. (a) Очевидно, що число $ak - bk = (a - b)k$ ділиться на nk тоді і тільки тоді, коли $a - b$ ділиться на k .

(b) Якщо $a - b$ ділиться на кожне з чисел n_1, \dots, n_k , то $a - b$ є їх спільним кратним. А тому $a - b$ ділиться на їх найменше спільне кратне n .

(c) Якщо число $a - b$ ділиться на n , то воно ділиться і на кожен дільник числа n . \square

Задача 5.11. Знайти всі k , для яких виконується конгруенція

$$3^{100} \equiv 1 \pmod{10^k}. \quad (5.6)$$

Розв'язання. Для $k = 3$ маємо: $3^{10} = 59049 \equiv 49 \pmod{1000}$, $3^{20} = 49^2 = 2401 \equiv 401 \pmod{1000}$, $3^{50} = 3^{20} \cdot 3^{20} \cdot 3^{10} = 401 \cdot 401 \cdot 49 = 801 \cdot 49 \equiv 249 \pmod{1000}$, $3^{100} = 249^2 = 62001 \equiv 1 \pmod{1000}$. Отже, для $k = 3$ конгруенція (5.6) виконується. За теоремою 5.9(c) вона буде виконуватися і для $k = 1, k = 2$. Для $k = 4$ маємо: $3^{10} = 59049 = 9049 \equiv 49 \pmod{10^4}$, $3^{20} = 9049^2 \equiv 4401 \pmod{10^4}$, $3^{50} = 3^{20} \cdot 3^{20} \cdot 3^{10} = 4401 \cdot 4401 \cdot 9049 \equiv 249 \pmod{10^4}$, $3^{100} = 249^2 = 62001 = 2001 \neq 1 \pmod{10^4}$. Отже, для $k = 4$ конгруенція (5.6) вже не виконується. Із теореми 5.9(c) випливає, що вона не буде виконуватися і для всіх $k > 4$. \square

5.3. Системи лишків

Набір цілих чисел називається *повною системою лишків за модулем n* , якщо він містить рівно по одному представнику з кожного класу лишків за модулем n . Зокрема, такий набір повинен містити рівно n елементів.

Іншими словами, набір a_1, \dots, a_n є повною системою лишків за модулем n , якщо класи лишків $\bar{a}_1, \dots, \bar{a}_n$ всі різні. Звідси і з теореми 5.1 випливає такий критерій повноти системи лишків.

Твердження 5.2. Числа a_1, a_2, \dots, a_n утворюють повну систему лишків за модулем n тоді й лише тоді, коли остачі r_1, r_2, \dots, r_n від ділення цих чисел на n попарно різні.

Приклади.

- Числа 7, 2, 149, -213 , 48, 34 утворюють повну систему лишків за модулем 6, бо остачі від ділення цих чисел на 6 дорівнюють відповідно 1, 2, 3, 0, 4, 4.
- Числа 1, 12, 123, 1234, ..., 123456789, 1234567890 утворюють повну систему лишків за модулем 10.
- Стандартним прикладом повної системи лишків за модулем n є набір $0, 1, 2, \dots, n-1$ остатів від ділення на n . Цей набір називається *системою найменших невід'ємних лишків*.
- Іншим стандартним прикладом є набір усіх цілих чисел із проміжку $(-\frac{n}{2}, \frac{n}{2}]$, так звана *система абсолютно найменших лишків*.
- Для будь-якого цілого числа a набір $a, a+1, \dots, a+n-1$ є повною системою лишків за модулем n .

Задача 5.12. Чи утворюють повну систему лишків за модулем 5 числа $[\sqrt{2}], [2\sqrt{2}], [4\sqrt{2}], [8\sqrt{2}], [16\sqrt{2}]$?

Розв'язання. Із співвідношень $1^2 = 1 < 2 = (\sqrt{2})^2 < 4 = 2^2$, $2^2 = 4 < 8 = (2\sqrt{2})^2 < 9 = 3^2$, $5^2 = 25 < 32 = (4\sqrt{2})^2 < 36 = 6^2$, $11^2 = 121 < 128 = (8\sqrt{2})^2 < 144 = 12^2$, $22^2 = 484 < 512 = (16\sqrt{2})^2 < 529 = 23^2$ випливає, що $[\sqrt{2}] = 1$, $[2\sqrt{2}] = 2$, $[4\sqrt{2}] = 5$, $[8\sqrt{2}] = 11$, $[16\sqrt{2}] = 22$. Остачі від ділення на 5 дорівнюють відповідно 1, 2, 0, 1 і 2. Серед них є однакові, тому дані числа повну систему лишків не утворюють. \square

Набір цілих чисел називається *зведеногою системою лишків за модулем n* , якщо всі числа з набору взаємно прості з n і він містить рівно по одному представнику з кожного оборотного класу лишків за модулем n . Із наслідку 2 теореми 5.7 випливає, що такий набір повинен містити рівно $\varphi(n)$ елементів.

Для зведеної системи лишків можна сформулювати критерій, аналогічний твердженню 5.2.

Твердження 5.3. Числа $a_1, a_2, \dots, a_{\varphi(n)}$ утворюють зведену систему лишків за модулем n тоді й лише тоді, коли остачі $r_1, r_2, \dots, r_{\varphi(n)}$ від ділення цих чисел на n попарно різні і взаємно прості з n .

Приклади.

- (a) Числа 5 і 25 утворюють зведену систему лишків за модулем 6.
- (b) Числа 11, -97 , 97 і -11 утворюють зведену систему лишків за модулем 10.
- (c) Множина $1, 2, 3, \dots, p - 1$ ненульових остач від ділення на просте число p утворює зведену систему лишків за модулем p .

Задача 5.13. Скільки чисел містить зведенна система лишків за модулем $10!$?

Розв'язання. $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, тому зведенна система лишків містить $\varphi(10!) = (2 - 1)(3 - 1)(5 - 1)(7 - 1) \cdot 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^0 = 829440$ чисел. \square

Задача 5.14. Нехай числа t і n взаємно прості, а числа a і b пробігають зведені системи лишків за модулями t і n відповідно. Довести, що сума $an + bt$ пробігає зведену систему лишків за модулем tn .

Розв'язання. Доведемо, що кожне число $an + bm$ буде взаємно просте з mn . Припустимо, що це не так. Тоді $an + bm$ не буде взаємно просте принаймні з одним із множників m або n . Нехай $an + bm$ не взаємно просте з m і нехай $d \neq 1$ – спільний дільник цих чисел. Із подільності $d|an + bm$ і $d|m$ випливає $d|an$. За означенням зведені системи лишків a взаємно просте з числом m , тому a взаємно просте і з його дільником d . Але тоді, за твердженням 1.2(b), $d|n$, що суперечить взаємній простоті чисел m і n .

Далі покажемо, що коли суми $a_1n + b_1m$ і $a_2n + b_2m$ розрізняються хоча б одним коефіцієнтом, то вони дають різні остачі при діленні на mn . Справді, нехай, наприклад, $a_1 \neq a_2$ і $a_1n + b_1m \equiv a_2n + b_2m \pmod{mn}$. Тоді з подільності числа $(a_1n + b_1m) - (a_2n + b_2m) = (a_1 - a_2)n + (b_1 - b_2)m$ на mn і числа $(b_1 - b_2)m$ на m випливає подільність на m числа $(a_1 - a_2)n$. Але m і n взаємно прості, тому $m|a_1 - a_2$. Останнє суперечить умові, що a пробігає зведену систему лишків за модулем m .

Отже, всі суми $an + bm$ взаємно прості з mn і дають при діленні на mn різні остачі. Для коефіцієнта a маємо $\varphi(m)$ можливостей, а для b – $\varphi(n)$. Тому всього сум буде $\varphi(m)\varphi(n)$. Але за теоремою 2.5, із взаємної простоти чисел m і n випливає, що $\varphi(m)\varphi(n) = \varphi(mn)$. Таким чином, усі умови твердження 5.3 виконані і суми $an + bm$ утворюють зведену систему лишків за модулем mn . \square

Задача 5.15. Для яких n зведена система лишків за модулем n містить рівно 6 чисел?

Розв'язання. Нехай $n = p_1^{k_1} \dots p_m^{k_m}$. Тоді має виконуватись рівність $\varphi(n) = (p_1 - 1) \dots (p_m - 1)p_1^{k_1-1} \dots p_m^{k_m-1} = 6$. Тому n не може ділитись на 5 (бо тоді $\varphi(n)$ ділилось би на $5 - 1 = 4$) і на жодне з простих чисел, більших за 7 (бо тоді $\varphi(n)$ було б більше 6). Отже, n має вигляд $n = 2^\alpha 3^\beta 7^\gamma$, причому $\alpha \leq 2$, $\beta \leq 2$, $\gamma \leq 1$. Із розгляду можливих випадків знаходимо, що n може бути одним із чисел 7, 9, 14, 18. \square

5.4. Теорема Ойлера

Теорема 5.10 (Ойлер). Якщо число a взаємно просте з n , то

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad (5.7)$$

Доведення. Нехай $a_1, a_2, \dots, a_{\varphi(n)}$ – довільна зведені система лишків за модулем n . Тоді $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(n)}$ – не всі оборотні класи лишків за модулем n . Розглянемо класи $\bar{a}_1\bar{a}, \bar{a}_2\bar{a}, \dots, \bar{a}_{\varphi(n)}\bar{a}$. Всі вони оборотні (за

наслідком 1 теореми 5.7) і різні (бо з рівності $\bar{a}_k\bar{a} = \bar{a}_j\bar{a}$ випливає рівність $\bar{a}_k\bar{a} \cdot \bar{a}^{-1} = \bar{a}_j\bar{a} \cdot \bar{a}^{-1}$, тобто $\bar{a}_k = \bar{a}_j$). Тому $\bar{a}_1\bar{a}, \bar{a}_2\bar{a}, \dots, \bar{a}_{\varphi(n)}\bar{a}$ – це ті ж самі класи $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(n)}$, тільки, можливо, в іншому порядку. Але тоді $\bar{a}_1\bar{a} \cdot \bar{a}_2\bar{a} \cdots \bar{a}_{\varphi(n)}\bar{a} = \bar{a}_1 \cdot \bar{a}_2 \cdots \bar{a}_{\varphi(n)}$, звідки $\bar{a}_1\bar{a}_2 \cdots \bar{a}_{\varphi(n)}\bar{a}^{\varphi(n)} = \bar{a}_1\bar{a}_2 \cdots \bar{a}_{\varphi(n)}$ або $a_1a_2 \cdots a_{\varphi(n)} \cdot a^{\varphi(n)} \equiv a_1a_2 \cdots a_{\varphi(n)} \pmod{n}$. Після скорочення на числа $a_1, a_2, \dots, a_{\varphi(n)}$ (а це можна робити, бо вони взаємно прості з n) остання конгруенція набуває вигляду $a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

Для знайомих із початками теорії груп зауважимо, що теорема Ойлера є частковим випадком відомої теореми Лагранжа про порядок елемента скінченної групи. Справді, за наслідком 2 теореми 5.7 група обертових елементів кільця \mathbb{Z}_n має порядок $\varphi(n)$. Але тоді за теоремою Лагранжа для кожного обертового елемента \bar{a} має виконуватись рівність $\bar{a}^{\varphi(n)} = \bar{1}$, яка рівносильна конгруенції (5.7).

Важливим частковим випадком теореми Ойлера є сформульована століттям раніше

Теорема 5.11 (Ферма). Якщо a не ділиться на просте число p , то

$$a^{p-1} \equiv 1 \pmod{p}. \quad (5.8)$$

Доведення. Якщо p – просте і a не ділиться на p , то a взаємно просте з p . Крім того, $\varphi(p) = p - 1$. Тому конгруенція (5.7) набуває вигляду (5.8). \square

Домноживши обидві частини (5.8) на a , одержимо конгруенцію

$$a^p \equiv a \pmod{p}, \quad (5.9)$$

яка справедлива і для чисел, подільних на p (в останньому випадку обидві частини (5.9) конгруентні 0). Навпаки, з конгруенції (5.9) випливає теорема Ферма: якщо a не ділиться на p , то в (5.9) на a можна скоротити.

Теореми Ферма і Ойлера часто формулюють у термінах подільності:

Теорема 5.12 (Ферма, I варіант). Якщо a не ділиться на просте число p , то $a^{p-1} - 1$ ділиться на p .

Теорема 5.13 (Ферма, II варіант). Якщо число p – просте, то для кожного a число $a^p - a$ ділиться на p .

Теорема 5.14 (Ойлер). Якщо число a взаємно просте з n , то $a^{\varphi(n)} - 1$ ділиться на n .

Задача 5.16. Знайти остаточу від ділення 293^{275} на 48.

Розв'язання. Зауважимо, що число $293 \bmod 48 = 5$ взаємно просте із 48. Тому для обчислення 293^{275} можна скористатись теоремою Ойлера. Оскільки $\varphi(48) = \varphi(2^4 \cdot 3) = (2-1)(3-1) \cdot 2^4 = 16$ і $275 \bmod 16 = 3$, то $293^{275} = 5^{275} = 5^{16k+3} = (5^{16})^k \cdot 5^3 = 1^k \cdot 5^3 = 125 \equiv 29 \pmod{48}$. Отже, остаточа від ділення 293^{275} на 48 дорівнює 29. \square

Задача 5.17. Знайти дві останні цифри числа 2^{100} .

Розв'язання. Задача рівносильна знаходженню остаточі r від ділення 2^{100} на 100. Із подільності на 4 кожного з чисел 2^{100} і 100 випливає її подільність на 4 остаточі r . Тому r має вигляд $r = 4k$. Скорочуючи в конгруенції $2^{100} \equiv 4k \pmod{100}$ обидва члени її модуль на 4 (за теоремою 5.9(c) це вільно робити), одержуємо: $2^{98} \equiv k \pmod{25}$. Тепер 2 і 25 взаємно прости і можна скористатись теоремою Ойлера: $2^{98} = 2^{4 \cdot 20 + 18} = 2^{4 \cdot \varphi(25) + 18} = (2^{\varphi(25)})^4 \cdot 2^{18} = 1^4 \cdot 2^{18} = 2^{18} = (2^9)^2 = (512)^2 = 12^2 = 144 \equiv 19 \pmod{25}$. Отже, $k = 19$ і $r = 4 \cdot 19 = 76$ – дві останні цифри числа 2^{100} . \square

Задача 5.18. Обчислити $2^{\varphi(m)-1} \pmod{m}$, якщо m – непарне число.

Розв'язання. Нехай $m = 2k + 1$. Число $a = 2^{\varphi(m)-1} \pmod{m}$ належить множині $\{0, 1, 2, \dots, 2k\}$. За теоремою Ойлера $2a = 2 \cdot 2^{\varphi(m)-1} = 2^{\varphi(m)} \equiv 1 \pmod{m}$. Тому $2a$ має бути одним із чисел 1, $(2k+1)+1$, $2 \cdot (2k+1)+1$, Але $2a \neq 1$ і $2a \leq 2 \cdot 2k = 4k$. Лишається лише одна можливість: $2a = (2k+1)+1 = 2k+2$ і $a = k+1 = \frac{m+1}{2}$. \square

Задача 5.19. Довести, що добуток трьох послідовних цілих чисел, середнє з яких є точним кубом, завжди ділиться на 504.

Розв'язання. $504 = 7 \cdot 8 \cdot 9$. Множники 7, 8 і 9 попарно взаємно прости, тому досить довести, що добуток $(n^3 - 1)n^3(n^3 + 1)$ ділиться на кожен з них. Добуток $(n^3 - 1)n^3(n^3 + 1) = (n^7 - n)n^2$ завжди ділиться на 7, бо, за теоремою Ферма, $n^7 - n$ ділиться на 7.

Якщо n – парне, то $8|n^4$. Якщо ж n – непарне, то в розкладі $(n^3 - 1)n^3(n^3 + 1) = (n-1)(n+1)(n^2 + n + 1)n^3(n^2 - n + 1)$ множники $n-1$ і $n+1$ є послідовними парними числами. Тому один із них обов'язково ділиться на 4, а весь добуток – на 8.

Якщо n кратне 3, то $9|n^3$. У протилежному разі n і 3 взаємно прості і за теоремою Ойлера добуток $(n^3 - 1)(n^3 + 1) = n^6 - 1 = n^{\varphi(9)} - 1$ ділиться на 9. \square

Задача 5.20. Нехай p і q – різні прості числа. Довести, що конгруенція

$$a^{p+q-2} + 1 \equiv a^{p-1} + a^{q-1} \pmod{pq} \quad (5.10)$$

виконується тоді й лише тоді, коли число a взаємно просте з pq .

Розв'язання. Нехай a взаємно просте з pq . Тоді a взаємно просте з кожним із множників p і q . За теоремою Ферма число

$$a^{p+q-2} + 1 - a^{p-1} - a^{q-1} = a^{p-1}(a^{q-1} - 1) + (1 - a^{q-1}) = (a^{q-1} - 1)(a^{p-1} - 1)$$

ділиться на кожне з чисел p і q , а тому ділиться і на їх добуток pq . Отже, у випадку $(a, pq) = 1$ конгруенція (5.10) виконується.

Нехай тепер a не взаємно просте з pq . Тоді a ділиться без остачі на p або q . Якщо a ділиться на p , то число $a^{p+q-2} + 1 - a^{p-1} - a^{q-1}$ при діленні на p дає в остачі 1. Тому воно не може ділитись на pq . Аналогічно розглядається випадок $q|a$. Отже, у випадку $(a, pq) \neq 1$ конгруенція (5.10) не виконується. \square

Задача 5.21. Довести, що для простого числа $p > 3$ хоча б одне з чисел $2p + 1$ і $4p + 1$ є складеним.

Розв'язання. Якщо число $2p + 1$ складене, то доводити нічого. Припустимо, що воно просте. Тоді кожне з чисел p і $2p + 1$ взаємно просте з 3 і за теоремою Ферма $3|p^2 - 1$ і $3|(2p + 1)^2 - 1$. Із рівності $4p + 1 = ((2p + 1)^2 - 1) - 4(p^2 - 1) - 3$ тепер випливає, що $4p + 1$ ділиться на 3. За умовою $4p + 1 > 4 \cdot 3 > 3$, тому число $4p + 1$ – складене. \square

Задача 5.22. Для яких простих чисел p виконується умова $p|(2^p + 999)$?

Розв'язання. Очевидно, що $p \neq 2$. Тому p – непарне і за теоремою Ферма $2^{p-1} - 1$ ділиться на p . Із рівності $2^p + 999 = 2 \cdot (2^{p-1} - 1) + 1001$ тепер випливає, що на p ділиться число 1001. $1001 = 7 \cdot 11 \cdot 13$. Отже, p дорівнює одному з чисел 7, 11 або 13. \square

Теорема Ойлера дає ще один спосіб знаходження в кільці класів лішків \mathbb{Z}_n оберненого елемента, адже з рівностей $\bar{1} = \bar{a} \cdot \bar{a}^{-1} = \bar{a}^{\varphi(n)} = \bar{a} \cdot \bar{a}^{\varphi(n)-1}$ випливає, що $\bar{a}^{-1} = \bar{a}^{\varphi(n)-1}$.

Задача 5.23. Знайти $\overline{47}^{-1}$ у кільці \mathbb{Z}_{100} .

Розв'язання. $100 = 2^2 \cdot 5^2$, тому $\varphi(100) = (2-1)(95-1) \cdot 2 \cdot 5 = 40$ і $\overline{47}^{-1} = \overline{47}^{39}$. Маємо: $47^2 = 2209 \equiv 9 \pmod{100}$, $47^6 = (47^2)^3 = 9^3 = 729 \equiv 29 \pmod{100}$, $47^{12} = (47^6)^2 = 29^2 = 841 \equiv 41 \pmod{100}$, $47^{13} = 47^{12} \cdot 47 = 41 \cdot 47 = 1927 \equiv 27 \pmod{100}$, $47^{39} = (47^{13})^3 = 27^3 = 19683 \equiv 83 \pmod{100}$. Отже, $\overline{47}^{-1} = \overline{83}$. Справді, $47 \cdot 83 = 3901 \equiv 1 \pmod{100}$. \square

Чи не можна в теоремі Ойлера замінити $\varphi(n)$ меншим показником?
Відповідь на це дає

Теорема 5.15. Якщо $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ – канонічний розклад числа n і $m = \text{НСК}(\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \dots, \varphi(p_r^{k_r}))$, то $a^m \equiv 1 \pmod{n}$ для всіх a , взаємно простих з n .

Доведення. Позначимо $\varphi(p_1^{k_1}) = m_1, \dots, \varphi(p_r^{k_r}) = m_r$. Тоді m можна записати у вигляді $m = m_1 t_1 = \dots = m_r t_r$. Якщо a взаємно просте з n , то a взаємно просте з кожним із чисел $p_1^{k_1}, \dots, p_r^{k_r}$. За теоремою Ойлера $a^m = a^{m_1 t_1} = (a^{m_1})^{t_1} = 1^{t_1} \equiv 1 \pmod{p_1^{k_1}}, \dots, a^m = a^{m_r t_r} = (a^{m_r})^{t_r} = 1^{t_r} \equiv 1 \pmod{p_r^{k_r}}$. Таким чином, $a^m - 1$ ділиться на кожне з чисел $p_1^{k_1}, \dots, p_r^{k_r}$. Ці числа попарно взаємно прості, тому $a^m - 1$ ділиться на їх добуток n . Отже, $a^m \equiv 1 \pmod{n}$. \square

Можна довести, що показник m у теоремі 5.15 зменшити вже не можна. Точніше, завжди знайдеться взаємно просте з n число a , яке в жодному степені не конгруентне 1 за модулем n .

Для $n = 100$ теорема 5.15 дає показник $m = \text{НСК}(\varphi(2^2), \varphi(5^2)) = \text{НСК}(2, 20) = 20$. Тому в задачі 5.23 замість $\overline{47}^{39}$ можна було обчислювати $\overline{47}^{19}$. Справді, $47^{19} = 47^{13} \cdot 47^6 = 27 \cdot 29 = 783 \equiv 83 \pmod{100}$.

Задача 5.24. Довести, що для кожного взаємно простого з 32760 числа виконується конгруенція $a^{12} \equiv 1 \pmod{32760}$.

Розв'язання. $32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ і $\text{НСК}(\varphi(2^3), \varphi(3^2), \varphi(5), \varphi(7), \varphi(13)) = \text{НСК}(4, 6, 4, 6, 12) = 12$. Тому твердження задачі випливає з теореми 5.15. \square

Для порівняння одержаного результату з теоремою Ойлера зауважимо, що $\varphi(32760) = (2-1)(3-1)(5-1)(7-1)(13-1) \cdot 2^2 \cdot 3 = 6912$.

5.5. RSA – шифри

Не так давно теорема Ойлера знайшла несподіване й дуже практичне застосування. Використовуючи цю теорему, в 1977 р. троє американських математиків – Р.Райвест, А.Шамір та Л.Адлеман – запропонували першу, і донині найпопулярнішу, криптографічну систему з відкритим ключем (сама ідея таких систем була сформульована роком раніше теж американськими математиками У.Діффі та М.Геллманом).

У класичних криптографічних системах, добре знаних із детективів і серіалів про шпигунів, спосіб шифрування тримається в глибокій таємниці, бо інакше секретне повідомлення зможуть розшифрувати й ті, від кого власне воно засекречується. А в системах з відкритим ключем, винахід яких став у криптографії справжнім переворотом, тримати в таємниці спосіб шифрування (чи так званий ключ шифру) немає жодної потреби. Він є доступним для всіх, відкритим, що й пояснює назву таких систем. Все одно знання ключа жодним чином не допомагає в розшифруванні секретних повідомлень.

Запропонований Райвестом з колегами спосіб шифрування, названий на честь винахідників *RSA*-шифром, виглядає так. Вибираються два випадкові великі, десь до ста цифр кожне, прості числа p і q . Обчислюються $n = pq$ і $\varphi(n) = (p - 1)(q - 1)$. Далі вибирається випадкове число $k < \varphi(n)$, взаємно просте з $\varphi(n)$. Тоді за модулем $\varphi(n)$ клас \bar{k} буде оборотним, тобто існує таке число l , що $kl \equiv 1 \pmod{\varphi(n)}$. l можна знайти за допомогою алгоритму Евкліда (відповідну процедуру описано після теореми 5.7). Числа n і k визначають спосіб шифрування. Вони не засекречуються і утворюють так званий відкритий ключ, доступний всім зацікавленим особам і організаціям. Проте прості множники p і q не розголошуються. Потрібне для дешифрування число l також тримається в таємниці. Саме повідомлення записується у цифровій формі (кодування будь-якої інформації – текстової, музичної, візуальної і т.д. – у цифровому вигляді стало нині дуже поширеним явищем. Наприклад, саме в такому вигляді зберігається інформація в пам'яті ЕОМ).

Для шифрування повідомлення розбивається на блоки M_1, M_2, \dots довжини t . Число t вибирається так, щоб виконувалась нерівність $10^m < n$ (вважаємо, що повідомлення записується за допомогою звичайних цифр 0, 1, 2, ..., 9). Тоді блоки повідомлення можна розглядати як елементи кільця \mathbb{Z}_n . Шифрування блоку M полягає в заміні M блоком $E(M) = M^k \pmod{n}$. За наявності сучасних комп'ютерів такі обчислення не є занадто обтяжливими.

Процедура дешифрування схожа: ми заміняємо блок $E(M)$ блоком $(E(M))^l \bmod n$.

Число l вибиралось так, що для певного t виконується рівність $kl = t \cdot \varphi(n) + 1$. Тому за теоремою Ойлера $(E(M))^l = (M^k)^l = M^{kl} = M^{t \cdot \varphi(n)+1} = (M^{\varphi(n)})^t \cdot M = 1^t \cdot M \equiv M \pmod{n}$. Таким чином, після дешифрування одержимо початкове повідомлення.

Хоча попередні викладки формально є законними лише для блоків M , взаємно простих з n , конгруенція

$$M^{kl} \equiv M \pmod{n} \quad (5.11)$$

насправді виконується для всіх блоків. Для $M = 0$ це очевидно. Залишилось розглянути випадок, коли $0 < M < n$ і M не взаємно просте з pq . Тоді M ділиться або на p , або на q , але не на p і q одночасно. Припустимо, що $p|M$ (випадок $q|M$ розглядається аналогічно). Тоді M має вигляд $M = M_0p$ і число $M^{kl} - M = M_0^{kl}p^{kl} - M_0p$ ділиться на p . З іншого боку, $q \nmid M$. Тому за теоремою Ферма $M^{kl} = M^{t \cdot \varphi(n)+1} = M^{t(p-1)(q-1)+1} = (M^{q-1})^{t(p-1)} \cdot M = 1^{t(p-1)} \cdot M \equiv M \pmod{q}$. Отже, $M^{kl} - M$ ділиться і на q . Таким чином, $M^{kl} - M$ ділиться на $p \cdot q = n$, що й доводить конгруенцію 5.11.

Проблема надійності RSA–шифру зводиться до питання: чи можна дешифрувати криптоважт $E(M)$, тобто розв'язати конгруенцію $X^k \equiv E(M) \pmod{n}$, не знаючи наперед числа l ? Крім піднесення правої частини до степеня l математики знають сьогодні фактично єдиний загальний метод розв'язання таких конгруенцій. Це – різні варіанти пе ребору всіх можливостей для X . Але звичайно довжину t блоку вибирають у межах $100 \div 200$, тому перебір вимагає розгляду $10^{100} \div 10^{200}$ можливостей, що робить його абсолютно нереальним.

Таким чином, на сьогодні проблема зламання RSA–шифру вирається в задачу: як знайти l за відомими числами n і k ? Якби був знаний розклад $n = pq$, то l можна було б обчислити так, як описано вище. Виявляється, що й навпаки, знаючи числа n , k і l , можна порівняно легко знайти розклад $n = pq$. Отже, знаходження числа l вимагає приблизно стільки ж часу і зусиль, як і знаходження розкладу $n = pq$ (говорять, що ці задачі обчислювально еквівалентні).

Вправа 5.2. Як знайти прості множники p і q , якщо відомі іх добуток $n = pq$ і значення функції Ойлера $\varphi(n)$?

Вважається, що без відкриття принципово нових дуже швидких методів факторизації чисел (саме існування яких є вельми проблематичним),

чним) знаходження розкладу $n = pq$ у випадку, коли кожен із множників має до 100 цифр, є нереальним навіть за допомогою гіпотетичних машин майбутнього. Для RSA-шифрів це означає, що ймовірність обчислити за реальний час значення $\varphi(n) = (p-1)(q-1)$ (і потім знайти таємний ключ l) настільки мала, що її можна не брати до уваги. Тому RSA-шифри вважаються дуже надійними.

5.6. Теорема Вільсона

Теорема 5.16 (Вільсон). (a) Для кожного простого числа p виконується конгруенція

$$(p-1)! \equiv -1 \pmod{p}. \quad (5.12)$$

(b) Для кожного складеного числа n виконується конгруенція

$$(n-1)! \equiv 0 \pmod{n}.$$

Доведення. (a) $1! = 1 \equiv -1 \pmod{2}$ і $2! = 2 \equiv -1 \pmod{3}$, тому для $p = 2$ і $p = 3$ конгруенція (5.12) виконується.

Нехай тепер $p > 3$. Якщо число a належить проміжку $(0, p)$, то a взаємно просте з p , а тому, за теоремою 5.7, клас \bar{a} є оборотним. Отже, для кожного a з проміжку $(0, p)$ існує таке b з цього ж проміжку, що

$$ab \equiv 1 \pmod{p}. \quad (5.13)$$

З'ясуємо, чи може виконуватись рівність $a = b$. У цьому випадку конгруенція (5.13) набуває вигляду $a^2 \equiv 1 \pmod{p}$. Тому $a^2 - 1 = (a-1)(a+1)$ ділиться на p . Оскільки p – просте число, то на p має ділитись один із множників $a-1$ або $a+1$. У першому випадку $a \equiv 1 \pmod{p}$, а в другому – $a \equiv -1 \pmod{p}$. Отже, коли $a \neq \pm 1 \pmod{p}$, то $b \neq a$. Тому всі числа з множини $\{2, 3, 4, \dots, p-3, p-2\}$ можна розбити на такі пари (a, b) , що $ab \equiv 1 \pmod{p}$. Випишемо для кожної пари відповідну конгруенцію, а потім перемножимо всі отримані конгруенції. З одного боку одержимо добуток усіх чисел від 2 до $p-2$, а з іншого – добуток одиниць. Таким чином, $2 \cdot 3 \cdot \dots \cdot (p-3) \cdot (p-2) \equiv 1 \pmod{p}$. Домноживши останню конгруенцію на $p-1 \equiv -1 \pmod{p}$, одержимо (5.12).

(b) Це легко перевірити для $n = 4$, тому можна вважати, що $n \geq 6$. Якщо n розкладається в добуток $n = km$, де $1 < k < m < n$, то k і m входять множниками в $(n-1)!$, а тому $(n-1)!$ ділиться на $km = n$ і

$(n-1)! \equiv 0 \pmod{n}$. У протилежному разі n має вигляд $n = q^2$, де $q \geq 4$. Але тоді добуток $(n-1)!$ містить множники q і $2q$, і знову $(n-1)! \equiv 0 \pmod{n}$. \square

5.7. Застосування конгруенцій

(a) *Ознаки подільності.* Зафіксуємо натуральне число n . Послідовність лишків

$$a_0 = 1, \quad a_1 \equiv 10 \pmod{n}, \quad a_2 \equiv 10^2 \pmod{n}, \dots, \quad a_k \equiv 10^k \pmod{n}, \dots \quad (5.14)$$

є періодичною. Справді, члени цієї послідовності належать скінченній множині

$\{0, 1, 2, \dots, n-1\}$, тому серед її членів обов'язково є одинакові. Крім того, з рівності $10^{k+1} = 10^k \cdot 10$ випливає рівність $a_{k+1} \equiv 10a_k \pmod{n}$, тобто кожний наступний член послідовності (5.14) однозначно визначається попереднім. Тому з рівності $a_k = a_m$ випливає рівність $a_{k+1} = a_{m+1}$, з якої, у свою чергу, рівність $a_{k+2} = a_{m+2}$ і т.д. Отже, фрагмент $a_k, a_{k+1}, \dots, a_{m-1}$ буде періодично повторюватись.

Якщо період послідовності (5.14) не дуже довгий, на підставі конгруенції

$$\overline{a_k \dots a_2 a_1 a_0} \equiv a_0 \pmod{n} + a_1 10 \pmod{n} + \dots + a_k 10^k \pmod{n}$$

за модулем n можна сформулювати корисну для великих чисел ознакоу подільності на n . Покажемо на прикладах, як це робиться.

1) $n = 8$. Послідовність (5.14) набуває вигляду

$$1, 10 \pmod{8} = 2, \quad 10^2 \pmod{8} = 4, \quad 10^3 \pmod{8} = 0, \quad 0, \quad 0, \quad \dots.$$

Отже, остача від ділення на 8 числа $\overline{a_k \dots a_2 a_1 a_0}$ дорівнює остачі від ділення на 8 числа $a_0 + 2a_1 + 4a_2$. Зокрема, числа $\overline{a_k \dots a_2 a_1 a_0}$ і $a_0 + 2a_1 + 4a_2$ діляться чи не діляться на 8 одночасно.

Спостереження, що $10^3 \pmod{8} = 0$, дозволяє сформулювати ознакоу подільності на 8 трохи в іншому вигляді. Із рівностей $\overline{a_k \dots a_2 a_1 a_0} \pmod{8} = (a_k \cdot 10^k + \dots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0) \pmod{8} = 0 + \dots + 0 + a_2 \cdot 10^2 \pmod{8} + a_1 \cdot 10 \pmod{8} + a_0 \pmod{8} = (a_2 \cdot 10^2 + a_1 \cdot 10 + a_0) \pmod{8} = \overline{a_2 a_1 a_0} \pmod{8}$ випливає, що число $\overline{a_k \dots a_2 a_1 a_0}$ ділиться на 8 тоді й лише тоді, коли на 8 ділиться число $\overline{a_2 a_1 a_0}$, утворене трьома останніми цифрами.

2) $n = 9$. Послідовність (5.14) набуває вигляду

$$1, 10 \bmod 9 = 1, 10^2 \bmod 9 = 1, 1, 1, \dots .$$

Отже, остача від ділення на 9 числа $\overline{a_k \dots a_2 a_1 a_0}$ дорівнює остачі від ділення на 9 числа $a_0 + a_1 + \dots + a_k$, тобто сумі цифр початкового числа.

3) $n = 7$. Послідовність (5.14) набуває вигляду

$$1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, \dots .$$

Отже, остача від ділення на 7 числа $\overline{a_k \dots a_2 a_1 a_0}$ дорівнює остачі від ділення на 7 числа

$$a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + 3a_7 + \dots . \quad (5.15)$$

Цю ознаку можна переформулювати трохи інакше.

I спосіб. Перейшовши до від'ємних лишків, можна замінити 6, 4 і 5 меншими за абсолютною величиною числами $-1, -3$ та -2 і замість (5.15) розглядати простіше власновану суму $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 - \dots$

II спосіб. Із конгруенції $10^3 \equiv -1 \pmod{7}$ випливає, що

$$\begin{aligned} \overline{a_k \dots a_3 a_2 a_1 a_0} &= \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} \cdot 10^3 + \overline{a_8 a_7 a_6} \cdot 10^6 + \dots \equiv \\ &\equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \overline{a_1 a_{10} a_9} + \dots \pmod{7}. \end{aligned}$$

Остання сума будується так: розбиваємо початкове число, починаючи справа, на блоки по 3 цифри. Потім обчислюємо суму одержаних 3-цифрових чисел, чергуючи знаки “+” і “-”. Ця сума дає при діленні на 7 таку ж остачу, як і початкове число.

Для числа $a = 27318281828459045$ відповідна сума дорівнює $045 - 459 + 828 - 281 + 318 - 27 = 424$. Але $424 \bmod 7 = 4$, тому число a при діленні на 7 дає в остачі 4.

4) $n = 37$. Послідовність (5.14) набуває вигляду

$$1, 10, 26, 1, 10, 26, 1, 10, 26, 1, \dots .$$

Отже, остача від ділення на 37 числа $\overline{a_k \dots a_2 a_1 a_0}$ збігається з остачею від ділення на 37 числа $a_0 + 10a_1 + 26a_2 + a_3 + 10a_4 + 26a_5 + a_6 + \dots$.

Аналогічно попередньому прикладу зручно скористатись конгруенцією $10^3 \equiv 1 \pmod{37}$. Одержано:

$$\overline{a_k \dots a_3 a_2 a_1 a_0} = \overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} \cdot 10^3 + \overline{a_8 a_7 a_6} \cdot 10^6 + \dots \equiv$$

$$\overline{a_2a_1a_0} + \overline{a_5a_4a_3} + \overline{a_8a_7a_6} + \dots \pmod{37}.$$

На відміну від попереднього прикладу, чергувати знаки тепер не потрібно.

Для того самого числа a відповідна сума тепер дорівнює $045 + 459 + 828 + 281 + 318 + 27 = 1958$. Але $1958 \pmod{37} = 34$, тому остача від ділення a на 37 дорівнює 34.

(b) *Перевірка правильності обчислень.* Найпростішим способом перевірки правильності арифметичних обчислень є контроль за парністю аргументів і результату: сума $a + b$ є парною тоді й лише тоді, коли доданки a і b однакової парності, а добуток ab є непарним лише в разі, коли обидва множники – непарні.

Фактично для перевірки за парністю ми переходимо до лишків за модулем 2: замість рівності $a + b = c$ перевіряємо конгруенцію $a \pmod{2} + b \pmod{2} = c \pmod{2}$, а замість рівності $ab = c$ – конгруенцію $a \pmod{2} \times b \pmod{2} = c \pmod{2}$.

На жаль, контроль за парністю є малоефективним. Парність числа залежить лише від останньої цифри, а інших цифр результату такий контроль не зачіпає. Однак дуже привабливою є головна ідея цього методу: заміна для контролю великих аргументів малими числами – лишками аргументів за модулем фіксованого числа. Тому природним узагальненням перевірки на парність є такий метод контролю правильності обчислень:

вибираємо не дуже велике число n так, щоб лишок $a \pmod{n}$ залежав від усіх цифр числа a . Після цього правильність рівностей $a + b = c$, $ab = c$ та ім подібних контролюємо справдженням конгруенцій $a \pmod{n} + b \pmod{n} = c \pmod{n}$, $a \pmod{n} \cdot b \pmod{n} = c \pmod{n}$ і т.д. Найчастіше вибирають $n = 9$. Як доведено в попередньому пункті, $\overline{a_k \dots a_1 a_0} \equiv a_k + \dots + a_1 + a_0 \pmod{9}$, тому лишок $a \pmod{9}$ справді залежить від усіх цифр числа a . А з іншого боку, цей лишок легко обчислюється навіть для дуже великих чисел.

Таким чином, якщо $a = \overline{a_k \dots a_1 a_0}$, $b = \overline{b_l \dots b_1 b_0}$ і $c = \overline{c_m \dots c_1 c_0}$, то для контролю рівності $a + b = c$ перевіряється правильність конгруенції

$$(a_k + \dots + a_1 + a_0) + (b_l + \dots + b_1 + b_0) \equiv (c_m + \dots + c_1 + c_0) \pmod{9},$$

а для контролю рівності $ab = c$ – правильність конгруенції

$$(a_k + \dots + a_1 + a_0) \cdot (b_l + \dots + b_1 + b_0) \equiv (c_m + \dots + c_1 + c_0) \pmod{9}. \quad (5.16)$$

Вправа 5.3. З'ясуйте, чи можна сформулювати аналогічні правила для контролю віднімання і ділення.

Якщо $x \equiv y \pmod{9}$, то $x - y$ ділиться на 9, тобто x і y розрізняються на число, кратне 9. Тому конгруенцію (5.16) для перевірки правильності рівності $ab = c$ можна переформулювати у вигляді правила:

сума цифр добутку двох чисел повинна відрізнятись від добутку сум цифр кожного із множників на число, кратне 9.

Вправа 5.4. Сформулюйте аналогічне правило для перевірки правильності додавання.

У такій формі ці правила були відомі ще в ранньому Середньовіччі під назвою “правила дев’яток” або “правила викидання дев’яток”. Остання назва прояснює, як могли виникнути ці правила (адже поняття конгруенції з’явилось лише у XVIII ст., та й то в неявному вигляді. Явно конгруенції з’являються лише в Гауса, на межі XVIII і XIX ст.). Коли при додаванні відбувається переповнення розряду і перенос одициці в наступний розряд, то цифра наступного розряду збільшується на 1, а сума цифр даного розряду зменшується на 10 (при додаванні на рахівниці це безпосередньо видно). Отже, сума цифр зменшується на 9, тобто відбувається “викидання дев’ятки”.

Якщо помилково в результаті є лише одна цифра, то контроль “за модулем 9” таку помилку майже завжди виявляє (точніше, не саму помилку, а лише факт її наявності). Повз контроль може проскочити лише заміна цифри 0 на 9 або навпаки. У загальному випадку помилка залишиться непоміченою, якщо хибний результат відрізняється від правильного на число, кратне 9.

Значно рідше, ніж контроль “за модулем 9”, використовується контроль “за модулем 11”. Оскільки $10 \equiv -1 \pmod{11}$, то

$$\overline{a_k \dots a_1 a_0} \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^k a_k \pmod{11}.$$

Отже, і в цьому випадку лишок $a \pmod{11}$ обчислюється легко і залежить від усіх цифр числа. При контролі “за модулем 11” помилка залишиться непоміченою, якщо хибний результат відрізняється від правильного на число, кратне 11.

Можна застосовувати контроль і за більшими модулями, наприклад, за модулями 99 чи 101. Надійність контролю при цьому, звичайно, посилюється. Але за підвищення надійності доводиться платити: сама процедура контролю стає складнішою.

(c) *Перевірка простоти числа.* Щоб встановити складність даного числа n , зовсім не обов’язково шукати його дільники. Один із найпростіших методів спирається на теорему Ферма: беремо число $1 < a < n$

і обчислюємо за допомогою алгоритму Евкліда найбільший спільний дільник d чисел a і n . Якщо $d > 1$, то маємо нетривіальний дільник числа n і воно не є простим. У випадку $d = 1$ обчислюємо ще $a^{n-1} \pmod{n}$. Якщо $a^{n-1} \pmod{n} \neq 1$, то з теореми Ферма випливає, що n є складеним.

Наприклад, нехай $n = 8023$. На роль a візьмемо взаємно просте з n число 2. Обчислюючи кожного разу за модулем 8023 квадрат попереднього числа, матимемо: $2^{2^0} = 2$, $2^{2^1} = 4$, $2^{2^2} = 16$, $2^{2^3} = 256$, $2^{2^4} = 1352$, $2^{2^5} = 6683$, $2^{2^6} = 6471$, $2^{2^7} = 1804$, $2^{2^8} = 5101$, $2^{2^9} = 1612$, $2^{2^{10}} = 7115$, $2^{2^{11}} = 6118$, $2^{2^{12}} = 2629$. Тоді з рівності $8023 = 1111101010110_2$ випливає конгруенція $2^{8023} = 2629 \cdot 6118 \cdot 7115 \cdot 1612 \cdot 5101 \cdot 6471 \cdot 1352 \cdot 16 \cdot 4 \equiv 7796 \pmod{8023}$. Отже, 8023 не є простим числом (насправді $8023 = 71 \cdot 113$).

На сучасних комп'ютерах така перевірка робиться надзвичайно швидко навіть для чисел, які мають десятки або й сотні цифр. Зокрема, саме в такий спосіб було доведено непростоту багатьох чисел Ферма $2^{2^k} + 1$. Однак цей метод не дає жодної інформації про дільники числа. Тому для більшості тих чисел Ферма, складеність яких уже доведена, досі не відомо жодного простого дільника.

Якщо ж $a^{n-1} \pmod{n} = 1$, то нічого певного про простоту числа n сказати не можна. Ця рівність інколи може виконуватись і для складених чисел. Наприклад, $2^{20} = 1048576 = 341 \cdot 3075 + 1 \equiv 1 \pmod{341}$, тому $2^{340} = (2^{20})^{17} \equiv 1 \pmod{341}$. Але число $341 = 11 \cdot 31$ не є простим.

У межах $1 < n \leq 1000$ є ще 2 складених числа, для яких виконується рівність $2^{n-1} \pmod{n} = 1$. Це $561 = 3 \cdot 11 \cdot 17$ і $645 = 3 \cdot 5 \cdot 43$.

Для спрощення простоти числа в непевних випадках може бути корисним

Твердження 5.4. Якщо $a^{n-1} \equiv 1 \pmod{n}$, але для кожного власного дільника t числа $n - 1$ $a^m \neq 1 \pmod{n}$, то число n – просте.

Доведення. Якщо $a^{n-1} \equiv 1 \pmod{n}$, то a і n взаємно прості. Тому до a можна застосувати теорему Ойлера і $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Припустимо, що число n – не просте. Тоді $\varphi(n) < n - 1$. Зобразимо найбільший спільний дільник d чисел $n - 1$ і $\varphi(n)$ у вигляді $d = k\varphi(n) + m(n - 1)$. Тоді $a^d = a^{k\varphi(n)+m(n-1)} = (a^{\varphi(n)})^k \cdot (a^{n-1})^m \equiv 1 \pmod{n}$. Але $d \leq \varphi(n) < n - 1$, тому d є власним дільником числа $n - 1$. Одержані суперечності доводить твердження. \square

Вправа 5.5. Довести, що в твердженні 5.4 умову $a^m \neq 1 \pmod{n}$ досить перевірити лише для показників вигляду $m_1 = \frac{n-1}{p_1}, \dots, m_k =$

$\frac{n-1}{p_k}$, де p_1, \dots, p_k – всі прості дільники числа $n - 1$.

Якщо

$$a^{n-1} \bmod n = 1, \quad (5.17)$$

але умови твердження 5.4 спрвдити не можна (наприклад, ми не знаємо простих дільників числа $n - 1$), то варто перевірити виконання цієї рівності для якогось іншого значення a . Якщо ж і кілька наступних перевірок не спростують гіпотезу про простоту числа n , то для перевірки простоти слід застосувати більш складні методи, які вже дадуть однозначну відповідь (проте такі методи вимагають значно більше зусиль і часу).

Обмежитись лише перевіркою рівності (5.17), хай і для дуже багатьох значень a , не можна. Існують такі складені числа n (вони називаються *числами Кармайкла*), що рівність (5.17) виконується для всіх a , взаємно простих з n . Найменшим з таких чисел є $561 = 3 \cdot 11 \cdot 17$. Нещодавно, у 1994 р., доведено, що чисел Кармайкла є безліч.

(d) *Визначення дня тижня*. Остача від ділення на дане число n змінюється дискретно і періодично повторюється. Тому не дивно, що конгруенції з успіхом використовуються для опису дискретних періодичних явищ. Одне з таких застосувань – формула для визначення дня тижня, що припадає на зазначену дату.

Оскільки в найближчі тисячу–другу років розходження між григоріанським і астрономічним календарями не перевищуватиме доби і до виходу цього посібника з друку реформа календаря не передбачається, далі ми дотримуємося григоріанського календаря.

Проблема визначення дня тижня викликана різною кількістю днів у роках (звичайних і високосних) і місяцях. Наш календар походить від римлян, а в них рік починається з березня. Тому для них було природно у високосний рік приєднувати додатковий день до останнього місяця – лютого.

Принагідно зауважимо, що і в наших предків новий рік святкувався весною. Про це свідчать численні новорічні щедрівки, приурочені до початку весняних польових робіт (“сію, вію, посіваю . . .”), в яких говориться про приліт ластівоньки тощо.

Ще одна неприємність пов’язана з переносом початку року з березня на січень (автори не знають, хто до цього причетний). Після такої, з дозволу сказати, реформи додатковий день у високосний рік представав бути останнім днем року. Це значно ускладнює рахунки. Щоб не завдавати собі й читачам зайвих клопотів, ми повернемось до традицій

римлян і предків: вважатимемо, що рік починається з березня. Точніше, вважатимемо березень, квітень, ..., грудень відповідно 1-м, 2-м, ..., 10-м місяцем року, а січень і лютий – 11-м і 12-м місяцями попереднього року. Так, 9 серпня 1999 р. буде рахуватись 9-м днем 6-го місяця 2001 р., а 13 лютого 2001 р. – 13-м днем 12-го місяця 2000 р. Цей перерахунок дат не є складним, зате дозволить одержати для підрахунку дня тижня зовсім просту формулу.

Отже, нам треба встановити, який день тижня припадає на a -й день b -го місяця n -го року. Номер n року записуватимемо у вигляді $n = 100k + l$, де k – кількість століть, що минула, а l – номер року в поточному столітті. Дні тижня також занумеруємо: понеділок – 1-й, вівторок – 2-й, ..., неділя – 7-й.

Дні тижня періодично повторюються, тому далі зручно міркувати за модулем числа 7, зокрема, вважати неділю 0-м днем тижня.

Розберемось спочатку з днем тижня, який припадає на перший день року (нагадаємо, що ми домовились починати рік із 1 березня). Нехай m_0 – номер дня тижня, який припав на 1 березня 0 року н.е., тобто 1-го року до н.е. Якби не було високосних років і всі роки мали по 365 днів, то з конгруенції $365 \equiv 1 \pmod{7}$ випливало б, що номер m_n дня тижня, який припадає на 1 березня n -го року, дорівнював би $m_n = (m_0 + n) \pmod{7} = (m_0 + 100k + l) \pmod{7}$. Але кожний 4-й рік є високосним. Поправка на додатковий день для кожного високосного року становить

$$\left[\frac{n}{4} \right] = \left[\frac{100k + l}{4} \right] = 25k + \left[\frac{l}{4} \right]. \quad (5.18)$$

Із поправкою (5.18) ми трохи переборшили, бо “круглі” роки – 100-й, 200-й, ... – не високосні. Тому від (5.18) треба відняти кількість “круглих” років, тобто k . Але “дуже круглі” роки – 400-й, 800-й, ... – все-таки високосні, тому треба ще додати $\left[\frac{k}{4} \right]$. Остаточно отримуємо:

$$m_n = \left(m_0 + 100k + l + 25k + \left[\frac{l}{4} \right] - k + \left[\frac{k}{4} \right] \right) \pmod{7} = \\ \left(m_0 + 124k + l + \left[\frac{k}{4} \right] + \left[\frac{l}{4} \right] \right) \pmod{7} = \left(m_0 + 5k + l + \left[\frac{k}{4} \right] + \left[\frac{l}{4} \right] \right) \pmod{7}. \quad (5.19)$$

Щоб узнати константу m_0 , не обов’язково звертатись до колекціонерів стародавніх календариків. Досить застосувати (5.19), наприклад, до 1

березня 2003 р., яке припало на суботу. Матимемо:

$$m_{2003} = 6 \equiv \left(m_0 + 5 \cdot 20 + 3 + \left[\frac{20}{4} \right] + \left[\frac{3}{4} \right] \right) \bmod 7 =$$

$$(m_0 + 108) \bmod 7 = (m_0 + 3) \bmod 7.$$

Отже, $6 \equiv m_0 + 3 \pmod{7}$ і $m_0 \equiv 3 \pmod{7}$. Таким чином, формула (5.19) набуває вигляду

$$m_n = \left(3 + 5k + l + \left[\frac{k}{4} \right] + \left[\frac{l}{4} \right] \right) \bmod 7. \quad (5.20)$$

Якби всі місяці містили ціле число тижнів (наприклад, були по 28 або 35 днів), то кожного року перші дні всіх місяців припадали б на один і той же день тижня. А для a -го дня місяця треба було б додати до формули (5.20) $a - 1$. Однак різна і неузгоджена з тривалістю тижня тривалість місяців призводить до того, що для кожного місяця потрібна ще своя додаткова поправка. Для березня вона, очевидно, нульова, але для квітня поправка дорівнює 3 (бо в березні були ще 3 додаткові дні до 4 повних тижнів), для травня — 5 (квітень додав ще 2 дні) і т.д. Підсумкова таблиця поправок виглядатиме так (нагадаємо, що нумерація місяців починається з березня):

N місяця	1	2	3	4	5	6	7	8	9	10	11	12
загальна кількість	0	3	5	8	10	13	16	18	21	23	26	29
додаткових днів	0	3	5	8	10	13	16	18	21	23	26	29

Хоча поправка зі збільшенням номера місяця зростає не зовсім регулярно, все-таки її ріст більш-менш рівномірний. За 11 місяців поправка зростає на 29 днів, тому в середньому за місяць вона зростає на $\frac{29}{11}$. Отже, певним наближенням до поправки для b -го місяця буде вираз

$$\frac{29}{11}(b - 1). \quad (5.21)$$

Можна спробувати пошукати точний вираз для поправки, замінивши (5.21) чимось на кшталт

$$\left[A + \frac{29}{11}(b - 1) \right]. \quad (5.22)$$

Справді, якщо покласти в (5.22) $A = \frac{4}{11}$, то значення виразу

$$\left[\frac{4}{11} + \frac{29}{11}(b - 1) \right] = -2 + \left[\frac{29b - 3}{11} \right] \quad (5.23)$$

для відповідних b будуть точно збігатися зі значеннями в нижньому рядку таблиці поправок.

Основна ідея побудови формул (5.23) дуже проста: будуємо для поправок деяке лінійне наближення $A + B(b - 1)$, а потім переходимо до цілої частини $[A + B(b - 1)]$. Вибираючи коефіцієнт B близьким до $\frac{29}{11}$ і підбираючи відповідне A , можна побудувати для місячних поправок багато інших формул, подібних до (5.23). Найпростішою з них є

$$\left[\frac{2}{5} + \frac{13}{5}(b - 1) \right] = -2 + \left[\frac{13b - 1}{5} \right].$$

Вправа 5.6. Довести, що місячні поправки можна задавати формулою $\left[\frac{5}{13} + \frac{34}{13}(b - 1) \right]$.

Таким чином, остаточно формулу для дня тижня, який припадає на a -й день b -го місяця $(100k + l)$ -го року, можна записати у вигляді

$$\begin{aligned} & \left(3 + 5k + l + \left[\frac{k}{4} \right] + \left[\frac{l}{4} \right] + (a - 1) + \left(-2 + \left[\frac{13b - 1}{5} \right] \right) \right) \bmod 7 = \\ & \left(5k + l + a + \left[\frac{k}{4} \right] + \left[\frac{l}{4} \right] + \left[\frac{13b - 1}{5} \right] \right) \bmod 7. \end{aligned} \quad (5.24)$$

Задача 5.25. Обчислити, на який день тижня припадав перший день третього тисячоліття.

Розв'язання. Перший день третього тисячоліття – це 1 січня 2001 р. Щоб скористатись формулою (5.24), треба цю дату записати як 1-й день 11-го місяця 2000-го року. Тоді

$$\left(5 \cdot 20 + 0 + 1 + \left[\frac{20}{4} \right] + \left[\frac{0}{4} \right] + \left[\frac{13 \cdot 11 - 1}{5} \right] \right) \bmod 7 = (101 + 5 + 28) \bmod 7 = 1.$$

Отже, перший день третього тисячоліття припадав на понеділок. \square

5.8. Задачі для самостійного розв'язування

1. Розбити множину простих чисел, менших 50, на класи попарно конгруентних за модулем 7.
2. Довести, що з першої конгруенції випливає друга:
 - (a) $27a - 10b + 14c \equiv 0 \pmod{33}$, $-6a + b - 8c \equiv 0 \pmod{33}$;

- (b) $29a + 8b + 22c \equiv 0 \pmod{21}$, $a + b - 13c \equiv 0 \pmod{21}$;
- (c) $9a - 2b + 17c \equiv 0 \pmod{15}$, $-3a + 4b - 4c \equiv 0 \pmod{15}$;
- (d) $33a + 31b + 50c \equiv 0 \pmod{35}$, $12a + 24b + 15c \equiv 0 \pmod{35}$.
3. Довести, що наступні конгруенції рівносильні:
- (a) $15a + 7b \equiv 0 \pmod{17}$ і $10a - b \equiv 0 \pmod{17}$;
 - (b) $12a + b \equiv 0 \pmod{19}$ і $2a - 3b \equiv 0 \pmod{19}$;
 - (c) $6a - b \equiv 0 \pmod{19}$ і $a + 2b \equiv 0 \pmod{19}$;
 - (d) $11a + 3b \equiv 0 \pmod{23}$ і $3a + 5b \equiv 0 \pmod{23}$.
4. Довести, що для кожного цілого числа a виконується конгруенція $a^7 \equiv a \pmod{42}$.
5. Довести, що для кожного натурального числа $k > 1$ виконується конгруенція $2^{2^k} \equiv 6 \pmod{10}$.
6. Довести, що сума 5 послідовних квадратів не може бути точним квадратом.
7. Довести, що для кожного простого числа p з конгруенції $a \equiv b \pmod{p^n}$ випливає конгруенція $a^p \equiv b^p \pmod{p^{n+1}}$.
8. Для кожного оборотного елемента кільця \mathbb{Z}_n знайти обернений:
- (a) $n = 9$; (b) $n = 12$; (c) $n = 14$; (d) $n = 16$; (e) $n = 15$.
9. Для кожного з класів $\overline{25}, \overline{26}, \overline{27}, \overline{28}, \overline{29}, \overline{30}$ знайти в кільці \mathbb{Z}_{61} обернений клас.
10. Обчислити в кільці \mathbb{Z}_{65} :
- (a) $\frac{\overline{41}}{\overline{21}}$; (b) $\frac{\overline{15}}{\overline{49}}$; (c) $\frac{\overline{24}}{\overline{27}}$; (d) $\frac{\overline{19}}{\overline{33}}$; (e) $\frac{\overline{28}}{\overline{29}}$.
11. Знайти остаточу від ділення:
- (a) 66^{17} на 7; (b) 117^{53} на 11; (c) 113^{74} на 24; (d) 219^{133} на 15.
12. Знайти остаточу від ділення:
- (a) $5^{70} + 7^{50}$ на 12; (b) $5^{50} + 13^{100}$ на 18; (c) $12^{100} + 20^{100}$ на 15; (d) $8^{120} + 25^{220}$ на 14.
13. Знайти дві останні цифри числа:
- (a) 243^{402} ; (b) 156^{382} ; (c) 3^{5^7} ; (d) $17^{17^{17}}$; (e) $7^{7^{7^7}}$.

14. Знайти число a , якщо:
- $a^{18} \equiv 7 \pmod{48}$, $a^{35} \equiv 35 \pmod{48}$;
 - $a^{50} \equiv 49 \pmod{60}$, $a^{35} \equiv 37 \pmod{60}$;
 - $a^{15} \equiv 43 \pmod{50}$, $a^{36} \equiv 21 \pmod{50}$;
 - $a^{15} \equiv 26 \pmod{45}$, $a^{40} \equiv 31 \pmod{45}$.
15. Чи утворюють повну систему лишків за модулем 8 числа:
- 71, 193, 314, 431, 547, 660, 771, 880;
 - 2, 147, -29, -700, 391, 98, -111, -250 ?
16. Чи утворюють повну систему лишків за модулем 5 числа:
- $[\sqrt{2}], [3\sqrt{2}], [5\sqrt{2}], [7\sqrt{2}], [9\sqrt{2}]$;
 - $[2\sqrt{3}], [3\sqrt{3}], [4\sqrt{3}], [5\sqrt{3}], [6\sqrt{3}]$;
 - $[5 \sin \frac{\pi}{3}], [10 \sin \frac{\pi}{3}], [15 \sin \frac{\pi}{3}], [20 \sin \frac{\pi}{3}], [25 \sin \frac{\pi}{3}]$;
 - $[e], [e^2], [e^3], [e^4], [e^5]$?
17. Чи утворюють повну систему лишків за модулем 13 числа:
- $2^1, 2^2, 2^3, \dots, 2^{12}, 2^{13}$; (b) 1, 11, 111, ..., 11...1 (13 одиниць);
 - 0, 1, 3, $3^2, \dots, 3^{10}, 3^{11}$; (d) $1!, 2!, 3!, \dots, 13!$?
18. Чи утворюють зведену систему лишків за модулем 18 числа:
- 755, 529, 989, 133, 757, 281; (b) -13, -23, -61, -29, -73, -35 ?
19. Чи утворюють зведену систему лишків за модулем 11 числа:
- $2^1, 2^2, 2^3, \dots, 2^{10}$; (b) 1, 10, 100, ..., 1000 000 000;
 - $1!, 2!, 3!, \dots, 10!$; (d) $1^3, 2^3, 3^3, \dots, 10^3$?
20. Довести, що коли числа m і n взаємно прості і коефіцієнт a пробігає повну систему лишків за модулем n , то для кожного цілого числа b сума $am + b$ також пробігає повну систему лишків за модулем n .
21. Довести, що коли a і n взаємно прості, то числа $1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (n-1) \cdot a, n \cdot a$ утворюють повну систему лишків за модулем n .
22. Нехай m і n взаємно прості, а коефіцієнти a і b пробігають повні системи лишків за модулями m і n відповідно. Довести, що сума $an + bm$ пробігає повну систему лишків за модулем mn .

23. Нехай a і b взаємно прості і числа $a_1, a_2, \dots, a_{\varphi(n)}$ утворюють зведену систему лішків за модулем n . Довести, що числа $aa_1, aa_2, \dots, aa_{\varphi(n)}$ також утворюють зведену систему лішків за модулем n .
24. Скільки лішків містить зведенна система лішків за модулем:
 (a) $12!$; (b) 2162160 ; (c) 2924207 ; (d) 833833 ?
25. Для яких натуральних чисел n зведенна система лішків за модулем n містить:
 (a) 4; (b) 8; (c) 10; (d) 14; (e) 16 елементів?
26. Нехай $n = kd$ і a_1, a_2, \dots, a_n – повна система лішків за модулем n . Скількома способами можна вибрати з цієї системи повну систему лішків за модулем d ?
27. Довести, що коли
 (a) $n = 130$; (b) $n = 210$; (c) $n = 42$; (d) $n = 90$; (e) $n = 84$,
 то для кожного взаємно простого з n числа a виконується конгруенція $a^{50} \equiv a^2 \pmod{n}$.
28. Довести такі конгруенції:
 (a) $2^{341} \equiv 2 \pmod{341}$; (b) $2^{561} \equiv 2 \pmod{561}$;
 (c) $2^{645} \equiv 2 \pmod{645}$; (d) $2^{1105} \equiv 2 \pmod{1105}$;
 (e) $2^{1387} \equiv 2 \pmod{1387}$; (f) $2^{1729} \equiv 2 \pmod{1729}$;
 (g) $2^{2465} \equiv 2 \pmod{2465}$; (h) $2^{2821} \equiv 2 \pmod{2821}$.
29. Довести, що для кожного взаємно простого з 14364 числа a виконується конгруенція $a^{18} \equiv 1 \pmod{14364}$.
30. Довести, що для кожного взаємно простого з 85932 числа a виконується конгруенція $a^{30} \equiv 1 \pmod{85932}$.
31. Довести, що для кожного взаємно простого з 69090840 числа a виконується конгруенція $a^{36} \equiv 1 \pmod{69090840}$.
32. З'ясувати, яких значень може набувати:
 (a) $a^{100} \pmod{125}$; (b) $a^{128} \pmod{128}$; (c) $a^{108} \pmod{81}$.
33. Для $n = 2k + 1$ довести конгруенцію: $4^{\varphi(n)-1} \equiv k^2 \pmod{n}$.

34. Нехай p і q – різні прості числа. Довести конгруенцію: $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
35. Довести, що для кожного взаємно простого з 10 числа n знайдеться число вигляду $\overline{aaa\dots aa}$, яке ділиться на n .
36. Довести, що для кожного непарного n число $2^{n!} - 1$ ділиться на n .
37. Знайти всі прості числа p , для яких $p|(2^p + 2000)$.
38. Довести, що для кожного натурального n число $2^{2^{6n-4}} + 3$ ділиться на 19.
39. За допомогою теореми Ойлера обчислити \bar{a}^{-1} в кільці \mathbb{Z}_n :
- (a) $a = 35, n = 48$; (b) $a = 35, n = 54$; (c) $a = 49, n = 60$;
 - (d) $a = 25, n = 84$; (e) $a = 27, n = 70$; (f) $a = 55, n = 72$.
40. Довести, що:
- (a) $100!30! + 1$ ділиться на 131; (b) $800!800! + 1$ ділиться на 1601;
 - (c) $1001!1001! - 1$ ділиться на 2003; (d) $1000!1002! + 1$ ділиться на 2003.
41. Для чисел, записаних у десятковій системі, сформулювати ознаки подільності на:
- (a) 13; (b) 41; (c) 73; (d) 137.
42. Довести, що числа p і $p + 2$ одночасно будуть простими тоді й лише тоді, коли виконується конгруенція $4 \cdot ((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$.
43. Знайти остаточу від ділення числа $2 + 2^2 + 2^3 + \dots + 2^n$ на:
- (a) 3; (b) 4; (c) 5; (d) 6; (e) 7.