

6. Конгруенції з невідомою

6.1. Алгебричні конгруенції та їх розв'язки

Нехай $f(x) = a_0x^m + \dots + a_{m-1}x + a_m$, $a_0 \neq 0$, – многочлен із цілими коефіцієнтами. Конгруенція вигляду

$$a_0x^m + \dots + a_{m-1}x + a_m \equiv 0 \pmod{n} \quad (6.1)$$

називається *алгебричною конгруенцією* (з невідомою x) степеня m за модулем n .

Ціле число b_0 називається *розв'язком конгруенції* (6.1), якщо число a конгруенція $f(b_0) \equiv 0 \pmod{n}$ є правильною.

Якщо b_0 є розв'язком конгруенції (6.1) і $b_1 \equiv b_0 \pmod{n}$, то за теоремою 5.5 число b_1 також буде розв'язком цієї конгруенції. Отже, всі елементи класу лишків $\bar{b}_0 \pmod{n}$ одночасно або є, або не є розв'язками (6.1). Тому природно називати розв'язком конгруенції (6.1) не тільки число b_0 , а й весь клас лишків $\bar{b}_0 \pmod{n}$.

Якщо в (6.1) коефіцієнти a_0, \dots, a_{m-1}, a_m замінити конгруентними їм за модулем n коефіцієнтами $\bar{a}_0, \dots, \bar{a}_{m-1}, \bar{a}_m$ (тобто $a_0 \equiv \bar{a}_0 \pmod{n}$, $\dots, a_m \equiv \bar{a}_m \pmod{n}$), то за теоремою 5.5 число b_0 буде розв'язком конгруенції

$$\bar{a}_0x^m + \dots + \bar{a}_{m-1}x + \bar{a}_m \equiv 0 \pmod{n}$$

тоді й лише тоді, коли b_0 є розв'язком (6.1). Отже, при заміні коефіцієнтів конгруентними множина розв'язків конгруенції (6.1) не змінюється. Це означає, що коефіцієнти в (6.1) також природно розглядати за модулем n , тобто як класи лишків. Тоді конгруенція (6.1) перетворюється в рівняння

$$\bar{a}_0x^m + \dots + \bar{a}_{m-1}x + \bar{a}_m = \bar{0} \quad (6.2)$$

над кільцем \mathbb{Z}_n лишків за модулем n . Корисно якомога раніше навчитись вільно переходити від конгруенції (6.1) до рівняння (6.2) і навпаки.

На конгруенцію (6.1) і рівняння (6.2) зручно дивитися як на різні способи запису одного й того ж. Це робить погляд на розв'язки конгруенції (6.1) як на класи лишків (тобто як на елементи кільця \mathbb{Z}_n) єдино прийнятним. Тому далі під розв'язками конгруенції (6.1) ми розумітимо саме розв'язки–класи лишків.

Але зовсім відмовитись від розв'язків–чисел теж незручно (це починяється є корисним при розв'язуванні конкретних конгруенцій), тому ми називатимемо їх частковими розв'язками конгруенції (6.1).

Інколи під алгебричними конгруенціями розуміють конгруенції вигляду

$$f(x) \equiv g(x) \pmod{n}, \quad (6.3)$$

де $f(x)$ і $g(x)$ – многочлени з цілими коефіцієнтами. Зрозуміло, що такі конгруенції завжди можна звести до вигляду (6.1).

Конгруенція (6.3) називається *сумісною*, якщо вона має хоча б один розв'язок. У протилежному разі вона називається *несумісною*.

Дві конгруенції за одним і тим же модулем називаються *еквівалентними* або *рівносильними*, якщо вони мають одні і ті ж розв'язки. Наприклад, будуть рівносильними конгруенції $x^3 + x^2 \equiv 0 \pmod{3}$ і $x^2 + x \equiv 0 \pmod{3}$ (розв'язками обох є класи $\bar{0}$ і $\bar{2}$). У той же час конгруенції $x^3 + x^2 \equiv 0 \pmod{3}$ і $x^3 + x \equiv 0 \pmod{3}$ не рівносильні (клас лишків $\bar{2}$ є розв'язком першої конгруенції, але не є розв'язком другої).

Із конгруенціями за різними модулями ситуація трохи складніша. Множини їх розв'язків, як правило, порівнювати не можна, бо коли $m \neq n$, то множини класів лишків \mathbb{Z}_m і \mathbb{Z}_n не мають спільних елементів. У той же час, як випливає з теореми 5.9(а), для будь-якого цілого числа x конгруенції $2x \equiv 4 \pmod{10}$ і $x \equiv 2 \pmod{5}$ виконуються чи не виконуються одночасно. Тому такі конгруенції природно вважати еквівалентними.

Щоб охопити випадок різних модулів, дві конгруенції будемо називати еквівалентними, якщо вони мають одинакові множини часткових розв'язків. Зрозуміло, що для однакових модулів це означення збігається з попереднім.

6.2. Лінійні конгруенції

Теорема 6.1. (a) *Лінійна конгруенція*

$$ax \equiv b \pmod{n} \quad (6.4)$$

сумісна тоді й лише тоді, коли b ділиться на найбільший спільний дільник чисел a і n .

(b) *Якщо конгруенція (6.4) сумісна, то вона має рівно d розв'язків за модулем n .*

Доведення. (a) Нехай x_0 – частковий розв'язок конгруенції (6.4). Тоді $ax_0 - b$ ділиться на n , тобто $ax_0 - b = kn$ для деякого цілого числа k . У

правій частині рівності $b = ax_0 - kn$ кожен доданок ділиться на d , тому і b ділиться на d .

Навпаки, нехай b ділиться на d . Тоді b має вигляд $b = b_0d$. За наслідком 1 теореми 1.5 число d можна записати у вигляді $d = ka + mn$. Тому $b = b_0d = b_0ka + b_0mn$. Оскільки число $ab_0k - b = -b_0mn$ ділиться на n , то $ab_0k \equiv b \pmod{n}$ і b_0k є частковим розв'язком (6.4). Отже, конгруенція (6.4) є сумісною.

(b) Нехай конгруенція (6.4) сумісна. За доведеним вище число b ділиться на d , і ми можемо записати: $a = a_0d$, $b = b_0d$, $n = n_0d$. Конгруенція (6.4) набуває вигляду $a_0dx \equiv b_0d \pmod{n_0d}$ і за теоремою 5.9(а) рівносильна конгруенції

$$a_0x \equiv b_0 \pmod{n_0}. \quad (6.5)$$

За твердженням 1.3 числа a_0 і n_0 взаємно прості. Тому клас лишків $a_0 \pmod{n_0}$ є оборотним і існує таке число c_0 , що $a_0c_0 \equiv 1 \pmod{n_0}$. Але тоді (6.5) рівносильна конгруенції

$$x \equiv c_0b_0 \pmod{n_0}. \quad (6.6)$$

Справді, (6.6) одержується з (6.5) множенням обох частин на c_0 , а (6.5) із (6.6) – множенням обох частин на a_0 .

Залишилось показати, що клас лишків $\overline{c_0b_0} \pmod{n_0}$ при переході до модуля n розпадається на d класів. Позначимо $r = c_0b_0 \pmod{n_0}$. Тоді $0 \leq r < n_0$. Клас лишків $\overline{t} \pmod{n}$ буде розв'язком конгруенції (6.4) тоді й лише тоді, коли t буде частковим розв'язком конгруенції (6.4), або, що те саме, частковим розв'язком рівносильної (6.4) конгруенції (6.5). Останнє еквівалентне тому, що t при діленні на n_0 дає в остачі r . t можна вибрати з множини $\{0, 1, 2, \dots, n-1 = n_0d-1\}$. Але з цієї множини остачу r при діленні на n_0 дають лише числа $r, n_0+r, 2n_0+r, \dots, (d-1)n_0+r$. Отже, конгруенція (6.4) має рівно d розв'язків $\overline{r} \pmod{n}$, $(n_0+r) \pmod{n}, \dots, (d-1)n_0+r \pmod{n}$. \square

Правильність конгруенції $ax_0 \equiv b \pmod{n}$ рівносильна існуванню такого цілого числа k , що $ax_0 - kn = b$. На пару $(x_0, -k)$ можна дивитись як на розв'язок лінійного діофантового рівняння

$$ax + ny = b. \quad (6.7)$$

Навпаки, кожен розв'язок (x_0, y_0) діофантового рівняння (6.7) дає частковий розв'язок x_0 конгруенції (6.4), бо $ax_0 - b = -ny_0$ ділиться на n . Тому конгруенцію (6.4) можна розглядати як діофантове рівняння

(6.7), в якому нас цікавить лише перша, “іксова”, компонента розв’язку. Це пояснює, чому критерій сумісності лінійної конгруенції (6.4) (теорема 6.1(a)) збігається з критерієм сумісності лінійного діофантового рівняння (6.7) (теорема 1.11).

Із доведення теореми 6.1(b) випливає, що розв’язання лінійної конгруенції (6.4) зводиться до випадку, коли a і b взаємно прості: якщо (6.4) сумісна, то можна розділити a , b і n на найбільший спільний дільник $d = (a, n)$ і перейти до конгруенції (6.5).

Нехай тепер a і n взаємно прості. Тоді за теоремою 6.1 конгруенція (6.4) сумісна і має єдиний розв’язок. Якщо n маленьке, то цей розв’язок можна знайти, перебираючи елементи із \mathbb{Z}_n , поки не натрапимо на розв’язок. Для великих n потрібні менш наїvnі методи.

(a) *Розв’язування за допомогою алгоритму Евкліда.* Від конгруенції (6.4) переходимо до лінійного діофантового рівняння (6.7) і розв’язуємо його методом, описаним після теореми 1.12 (зразком є задача 1.24). “Іксова” компонента розв’язку рівняння (6.7) дає розв’язок конгруенції (6.4).

Задача 6.1. Розв’язати за допомогою алгоритму Евкліда конгруенцію

$$128x \equiv 238 \pmod{94}. \quad (6.8)$$

Розв’язання. НСД(128, 94)=2 і $2|238$. Тому конгруенція (6.8) сумісна. Розділимо модуль і обидва коефіцієнти на 2. Одержано рівносильну (6.8) конгруенцію $64x \equiv 119 \pmod{47}$. Зручно перейти до лишків за модулем 47:

$$17x \equiv 25 \pmod{47}. \quad (6.9)$$

Розглянемо лінійне діофантове рівняння

$$17x + 47y = 25. \quad (6.10)$$

За допомогою алгоритму Евкліда шукаємо зображення $1 = 17k + 47m$:

$$47 = 2 \cdot 17 + 13, \quad 17 = 1 \cdot 13 + 4, \quad 13 = 3 \cdot 4 + 1. \quad (6.11)$$

Тому $1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 13) = 4 \cdot 13 - 3 \cdot 17 = 4 \cdot (47 - 2 \cdot 17) - 3 \cdot 17 = 4 \cdot 47 - 11 \cdot 17$. Рівність $25 = -25 \cdot 11 \cdot 17 + 25 \cdot 4 \cdot 47$ дає частковий розв’язок $x_0 = -25 \cdot 11 = -275$, $y_0 = 25 \cdot 4 = 100$ рівняння (6.10). Число $x_0 = -275$ буде і частковим розв’язком конгруенції (6.9). Тому єдиним розв’язком (6.9) буде клас лишків $\bar{x}_0 \pmod{47} = (-275) \pmod{47} = \bar{7} \pmod{47}$.

При переході до модуля 94 цей клас лишків розпадається на 2 класи: $\bar{7} \bmod 94$ і $(\bar{7} + \bar{47}) \bmod 94 = \bar{54} \bmod 94$. Отже, конгруенція (6.8) має 2 розв'язки: $\bar{7} \bmod 94$ і $\bar{54} \bmod 94$. \square

(b) *Розв'язування за допомогою ланцюгових дробів.* Як і в попередньому методі, спочатку переходимо до діофантового рівняння (6.7). Потім методом, описаним у наслідку 3 з твердження 4.2 (зразком є задача 4.3) знаходимо частковий розв'язок (x_0, y_0) рівняння (6.7). “Іксова” компонента x_0 цього розв'язку буде частковим розв'язком конгруенції (6.4). Повним розв'язком буде клас лишків $\bar{x}_0 \bmod n$.

Задача 6.2. Розв'язати конгруенцію (6.8) із задачі 6.1 за допомогою ланцюгових дробів.

Розв'язання. Перший крок – перехід до діофантового рівняння (6.10) – такий же, як у розв'язанні задачі 6.1. Тому почнемо одразу з рівняння (6.10). Із рівностей (6.11) випливає, що $\frac{17}{47} = [0; 2, 1, 3, 4]$. За наслідком 3 з твердження 4.2 рівняння (6.10) має частковий розв'язок (x_0, y_0) , компонента x_0 якого дорівнює $x_0 = (-1)^3 Q_3 \cdot 25$. За стандартною схемою обчислюємо Q_3 :

k	–	–	0	1	2	3
q_k	–	–	0	2	1	3
Q_k	1	0	1	2	3	11

Отже, конгруенція (6.9) має частковий розв'язок $x_0 = (-1)^3 \cdot 11 \cdot 25 = -275$. Далі треба дослівно повторити завершальну частину міркувань із розв'язання задачі 6.1. \square

(c) *Розв'язання за допомогою теореми Ойлера.* Якщо a і n взаємно прості, то за теоремою Ойлера $a^{\varphi(n)} \equiv 1 \pmod{n}$. Помножимо обидві частини конгруенції (6.4) на $a^{\varphi(n)-1}$:

$$a^{\varphi(n)-1} \cdot ax \equiv a^{\varphi(n)-1} \cdot b \pmod{n}.$$

Але $a^{\varphi(n)-1} \cdot ax \equiv a^{\varphi(n)} \cdot x \equiv 1 \cdot x \equiv x \pmod{n}$, тому $x \equiv a^{\varphi(n)-1}b \pmod{n}$.

Задача 6.3. Розв'язати за допомогою теореми Ойлера конгруенцію (6.8) із задачі 6.1.

Розв'язання. Як і в розв'язанні задачі 6.1, переходимо спочатку до конгруенції (6.9). $\varphi(47) = 46$, тому $x \equiv 17^{46-1} \cdot 25 = 17^{45} \cdot 25 \pmod{47}$. Але $17^{45} \cdot 25 = ((17^2)^2)^{11} \cdot 17 \cdot 25 = (289^2)^{11} \cdot 425 \equiv (7^2)^{11} \cdot 2 \equiv 2^{11} \cdot 2 = 4096 \equiv 7$

(mod 47). Отже, розв'язком конгруенції (6.9) є клас лишків $\bar{7} \pmod{47}$. Перехід до модуля 94 повторює завершальні міркування із розв'язання задачі 6.1. \square

6.3. Системи лінійних конгруенцій

Ми будемо розглядати лише системи лінійних конгруенцій від однієї невідомої, тобто системи вигляду

$$\left\{ \begin{array}{l} a_1x \equiv b_1 \pmod{n_1}, \\ a_2x \equiv b_2 \pmod{n_2}, \\ \dots \dots \\ a_mx \equiv b_m \pmod{n_m}. \end{array} \right. \quad (6.12)$$

Якщо якась із конгруенцій

$$a_kx \equiv b_k \pmod{n_k} \quad (6.13)$$

цієї системи несумісна, то і вся система, очевидно, несумісна. Якщо ж конгруенція (6.13) сумісна, то за теоремою 6.1 b_k ділиться на найбільший спільний дільник d_k чисел a_k і n_k , і можна замінити (6.13) рівносильною їй конгруенцією

$$a'_kx \equiv b_k \pmod{n'_k}, \text{ де } a'_k = \frac{a_k}{d_k}, b'_k = \frac{b_k}{d_k}, n'_k = \frac{n_k}{d_k}.$$

Зауважимо, що числа a'_k і n'_k взаємно прости.

Таким чином, систему (6.12) можна замінити рівносильною їй системою

$$\left\{ \begin{array}{l} a'_1x \equiv b'_1 \pmod{n'_1}, \\ a'_2x \equiv b'_2 \pmod{n'_2}, \\ \dots \dots \\ a'_m x \equiv b'_m \pmod{n'_m}, \end{array} \right. \quad (6.14)$$

в якій кожний коефіцієнт a'_k взаємно пристий з відповідним модулем n'_k . Але тоді для кожного k існує таке число c_k , що $a'_k \cdot c_k \equiv 1 \pmod{n'_k}$. Наприклад, можна взяти $c_k = (a'_k)^{\varphi(n'_k)-1}$.

Домноживши кожну з конгруенцій системи (6.14) на відповідний множник c_k , одержимо рівносильну систему

$$\left\{ \begin{array}{l} x \equiv b'_1 c_1 \pmod{n'_1}, \\ x \equiv b'_2 c_2 \pmod{n'_2}, \\ \dots \dots \\ x \equiv b'_m c_m \pmod{n'_m}. \end{array} \right.$$

Тому в подальших міркуваннях можна обмежитись лише системами вигляду

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \dots \dots \\ x \equiv b_m \pmod{n_m}. \end{array} \right. \quad (6.15)$$

Теорема 6.2. Якщо система (6.15) сумісна, то її розв'язки утворюють клас лишків за модулем числа НСК(n_1, n_2, \dots, n_m).

Доведення. Для $m = 1$ це тривіально. Розглянемо випадок $m = 2$. Припустимо, що система

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2} \end{array} \right. \quad (6.16)$$

сумісна, і нехай $n = \text{НСК}(n_1, n_2)$, а x_0 – частковий розв'язок цієї системи. Тоді кожен елемент x_1 із класу лишків $\bar{x}_0 \pmod{n}$ також буде розв'язком. Справді, x_1 має вигляд $x_1 = x_0 + kn$. Тому число $x_1 - b_1 = (x_0 + kn) - b_1 = (x_0 - b_1) + kn$ ділиться на n_1 , бо кожен із двох доданків правої частини ділиться на n_1 . Отже, x_1 задовільняє першу конгруенцію з (6.16). Аналогічно доводиться, що x_1 задовільняє і другу конгруенцію.

Навпаки, якщо x_2 – інший частковий розв'язок системи (6.16), то число $x_0 - x_2 = (x_0 - b_1) - (x_2 - b_1)$ ділиться на n_1 , бо кожний з двох доданків правої частини ділиться на n_1 . Аналогічно доводиться, що $x_0 - x_2$ ділиться на n_2 . Тому $x_0 - x_2$ є спільним кратним чисел n_1 і n_2 і ділиться на їх найменше спільне кратне n . Отже, $x_0 \equiv x_2 \pmod{n}$), тобто $x_2 \in \bar{x}_0 \pmod{n}$.

Таким чином, розв'язки системи (6.16) утворюють клас лишків $\bar{x}_0 \pmod{n}$. Для $m = 2$ теорема доведена.

Для довільного m тепер можна доводити за індукцією. Припустимо, що $m > 2$ і для всіх систем меншого розміру теорема вже доведена. Нехай $\acute{n} = \text{НСК}(n_1, n_2, \dots, n_{m-1})$. Тоді, за припущенням індукції, система

$$\left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \dots \dots \\ x \equiv b_{m-1} \pmod{n_{m-1}} \end{array} \right.$$

рівносильна одній конгруенції вигляду

$$x \equiv \acute{b} \pmod{\acute{n}},$$

а початкова система (6.15) – системі

$$\begin{cases} x \equiv b \pmod{n}, \\ x \equiv b_m \pmod{n_m}. \end{cases}$$

Як уже доведено, ця система рівносильна конгруенції вигляду $x \equiv b \pmod{n}$, де $n = \text{HCK}(n, n_m)$. Але $\text{HCK}(n, n_m) = \text{HCK}(\text{HCK}(n_1, n_2, \dots, n_{m-1}), n_m) = \text{HCK}(n_1, n_2, \dots, n_{m-1}, n_m)$. Отже, система (6.15) рівносильна конгруенції $x \equiv b \pmod{\text{HCK}(n_1, n_2, \dots, n_m)}$, тобто розв'язки системи (6.15) утворюють один клас лишків за модулем числа $\text{HCK}(n_1, n_2, \dots, n_m)$. \square

Розглянемо детальніше випадок, коли в системі (6.15) модулі n_1, n_2, \dots, n_m попарно взаємно прості.

Лема 6.1. *Нехай n_1 і n_2 взаємно прості і $1 = k_1 n_1 + k_2 n_2$. Тоді число $k_2 n_2$ буде розв'язком системи*

$$\begin{cases} x \equiv 1 \pmod{n_1}, \\ x \equiv 0 \pmod{n_2}. \end{cases}$$

Доведення. Із рівності $k_2 n_2 - 1 = -k_1 n_1$ випливає, що число $k_2 n_2$ задовольняє першу конгруенцію. Перевірка другої конгруенції тривіальна. \square

Зауважимо, що для взаємно простих чисел n_1 і n_2 зображення $1 = k_1 n_1 + k_2 n_2$ можна знайти за допомогою алгоритму Евкліда, тому лема має конструктивний характер.

Нехай числа n_1, n_2, \dots, n_m попарно взаємно прості. Тоді для кожного k , $1 \leq k \leq n$, числа n_k і $t_k = \frac{n_1 n_2 \dots n_m}{n_k}$ взаємно прості. Позначимо через B_k той розв'язок системи конгруенцій

$$\begin{cases} x \equiv 1 \pmod{n_k}, \\ x \equiv 0 \pmod{t_k}, \end{cases}$$

який будується за допомогою леми 6.1.

Теорема 6.3 (Китайська теорема про остачі). *Якщо модулі n_1, n_2, \dots, n_m попарно взаємно прості, то множина розв'язків системи конгруенцій*

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ x \equiv b_2 \pmod{n_2}, \\ \vdots \quad \vdots \quad \vdots \\ x \equiv b_m \pmod{n_m} \end{cases} \quad (6.17)$$

збігається з класом лишків

$$\overline{b_1B_1 + b_2B_2 + \dots + b_mB_m} \pmod{n_1n_2\dots n_m}.$$

Зокрема, система вигляду (6.17) із попарно взаємно простими модулями завжди сумісна.

Доведення. Зауважимо, що $t_k = \frac{n_1n_2\dots n_m}{n_k}$ ділиться на кожне з чисел $n_1, \dots, n_{k-1}, n_{k+1}, \dots, n_m$. Тому за теоремою 5.9(с) з конгруенції $B_k \equiv 0 \pmod{t_k}$ випливає, що для кожного $i \neq k$ виконується конгруенція $B_k \equiv 0 \pmod{n_i}$. Крім того, $B_k \equiv 1 \pmod{n_k}$. Але тоді для кожного k , $1 \leq k \leq m$, $b_1B_1 + \dots + b_{k-1}B_{k-1} + b_kB_k + b_{k+1}B_{k+1} + \dots + b_mB_m \equiv b_1 \cdot 0 + \dots + b_{k-1} \cdot 0 + b_k \cdot 1 + b_{k+1} \cdot 0 + \dots + b_m \cdot 0 \equiv b_k \pmod{n_k}$. Отже, система (6.17) сумісна і число $b_1B_1 + b_2B_2 + \dots + b_mB_m$ є її розв'язком. За теоремою 6.2 множина розв'язків системи (6.17) утворює клас лишків за модулем числа НСК(n_1, n_2, \dots, n_m). Але числа (n_1, n_2, \dots, n_m) попарно взаємно прості, тому $\text{НСК}(n_1, n_2, \dots, n_m) = n_1n_2\dots n_m$. Таким чином, множиною розв'язків системи (6.17) є клас лишків

$$\overline{b_1B_1 + b_2B_2 + \dots + b_mB_m} \pmod{n_1n_2\dots n_m}. \quad \square$$

Задачі, які зводяться до систем лінійних конгруенцій, китайські математики розв'язували ще майже 2 тисячі років тому, причому методом, описаним у доведенні теореми 6.3. Коли їх твори стали відомими в Європі, за цим методом закріпилась назва “китайський”.

Задача 6.4 (“задача Фібоначчі”). Знайти число, яке ділиться на 7, а при діленні на кожнє з чисел 2, 3, 4, 5 і 6 дає в остачі 1.

Розв'язання. Позначимо це число через x . Тоді задача зводиться до системи конгруенцій

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{2}, \\ x \equiv 1 \pmod{3}, \\ x \equiv 1 \pmod{4}, \\ x \equiv 1 \pmod{5}, \\ x \equiv 1 \pmod{6}, \\ x \equiv 0 \pmod{7}. \end{array} \right. \quad (6.18)$$

Одразу скористатись теоремою 6.3 не можна, бо модулі не є попарно взаємно простими. Тому спочатку перетворимо систему (6.18).

$x - 1$ ділиться на 6 тоді й лише тоді, коли ділиться і на 2, і на 3. Тому конгруенція $x \equiv 1 \pmod{6}$ рівносильна системі

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 1 \pmod{3}, \end{cases}$$

і передостанню конгруенцію з (6.18) можна вилучити. Крім того, з подільності 4 на 2 випливає (за теоремою 5.9(c)), що конгруенція $x \equiv 1 \pmod{2}$ є наслідком з $x \equiv 1 \pmod{4}$, тому першу конгруенцію теж можна вилучити. Остаточно одержуємо систему

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 1 \pmod{4}, \\ x \equiv 1 \pmod{5}, \\ x \equiv 0 \pmod{7} \end{cases} \quad (6.19)$$

із попарно взаємно простими модулями. У позначеннях теореми 6.3 $n_1 = 3$, $t_1 = 140$, $n_2 = 4$, $t_2 = 105$, $n_3 = 5$, $t_3 = 84$, $n_4 = 7$, $t_4 = 60$. Для системи

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 0 \pmod{140} \end{cases}$$

маємо: $1 = 47 \cdot 3 - 140$, тому $B_1 = -140$. Для системи

$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 0 \pmod{105} \end{cases}$$

маємо: $1 = 105 - 26 \cdot 4$, тому $B_2 = 105$. Для системи

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 0 \pmod{84} \end{cases}$$

маємо: $1 = 17 \cdot 5 - 84$, тому $B_3 = -84$. B_4 шукати не треба, бо воно буде виступати з нульовим коефіцієнтом. За теоремою 6.3 розв'язки системи (6.19) мають вигляд:

$$\begin{aligned} x &\equiv (1 \cdot B_1 + 1 \cdot B_2 + 1 \cdot B_3 + 0 \cdot B_4) \pmod{3 \cdot 4 \cdot 5 \cdot 7} \equiv \\ &\equiv -119 \pmod{420} \equiv 301 \pmod{420}. \end{aligned}$$

Зокрема, найменшим натуральним розв'язком задачі Фібоначчі буде число 301. \square

Задача 6.5. Розв'язати систему конгруенцій

$$\begin{cases} x \equiv 13 \pmod{21}, \\ x \equiv 7 \pmod{22}, \\ x \equiv 9 \pmod{23}. \end{cases} \quad (6.20)$$

Розв'язання. У позначеннях теореми 6.3 $n_1 = 21$, $t_1 = 506$, $n_2 = 22$, $t_2 = 483$, $n_3 = 23$, $t_3 = 462$. Розглянемо систему

$$\begin{cases} x \equiv 1 \pmod{21}, \\ x \equiv 0 \pmod{506}. \end{cases}$$

Застосуємо до чисел 506 і 21 алгоритм Евкліда. Маємо: $506 = 24 \cdot 21 + 2$, $21 = 10 \cdot 2 + 1$. Звідси $1 = 21 - 10 \cdot 2 = 21 - 10 \cdot (506 - 24 \cdot 21) = 241 \cdot 21 - 10 \cdot 506$. Тому $B_1 = -10 \cdot 506 = -5060$. Для системи

$$\begin{cases} x \equiv 1 \pmod{22}, \\ x \equiv 0 \pmod{483} \end{cases}$$

маємо: $483 = 21 \cdot 22 + 21$, $22 = 1 \cdot 21 + 1$. Звідси $1 = 22 - 1 \cdot 21 = 22 - 1 \cdot (483 - 21 \cdot 22) = 22 \cdot 22 - 483$ і $B_2 = -483$. Для системи

$$\begin{cases} x \equiv 1 \pmod{23}, \\ x \equiv 0 \pmod{462} \end{cases}$$

маємо: $462 = 20 \cdot 23 + 2$, $23 = 11 \cdot 2 + 1$. Звідси $1 = 23 - 11 \cdot 2 = 23 - 11 \cdot (462 - 20 \cdot 23) = 221 \cdot 23 - 11 \cdot 462$ і $B_3 = -11 \cdot 462 = -5082$. Тому розв'язки системи (6.20) мають вигляд: $x \equiv (-13 \cdot 5060 - 7 \cdot 483 - 9 \cdot 5082) \pmod{21 \cdot 22 \cdot 23} \equiv -114899 \pmod{10626} \equiv 1987 \pmod{10626}$. \square

Задача 6.6. Розв'язати систему конгруенцій

$$\begin{cases} 15x \equiv 24 \pmod{51}, \\ 28x \equiv 24 \pmod{72}, \\ 30x \equiv 24 \pmod{46}. \end{cases}$$

Розв'язання. Виконаємо спочатку необхідні спрощення. За теоремою 5.9 у першій конгруенції коефіцієнти ї модуль можна розділити на 3, у другій – на 4 і в третій – на 2. Одержано рівносильну початковій систему

$$\begin{cases} 5x \equiv 8 \pmod{17}, \\ 7x \equiv 6 \pmod{18}, \\ 15x \equiv 12 \pmod{23}, \end{cases}$$

в якій коефіцієнти при x взаємно прості з відповідними модулями, а модулі попарно взаємно прості. $\varphi(17) = 16$ і $5^{15} = (5^3)^5 = 125^5 \equiv 6^5 = 7776 \equiv 7 \pmod{17}$, тому перша конгруенція зводиться до вигляду $x \equiv 8 \cdot 7 = 56 \equiv 5 \pmod{17}$. Аналогічно для другої конгруенції: $\varphi(18) = 6$, $7^5 = 16807 \equiv 13 \pmod{18}$, $x \equiv 6 \cdot 13 = 78 \equiv 6 \pmod{18}$, і для третьої: $\varphi(23) = 22$, $15^{21} = (15^4)^5 \cdot 15 \equiv 2^5 \cdot 15 = 480 \equiv 20 \pmod{23}$, $x \equiv 12 \cdot 20 = 240 \equiv 10 \pmod{23}$. Таким чином, початкова система зводиться до системи

$$\begin{cases} x \equiv 5 \pmod{17}, \\ x \equiv 6 \pmod{18}, \\ x \equiv 10 \pmod{23}, \end{cases}$$

яка вже задовольняє умови теореми 6.3. Маємо: $n_1 = 17$, $t_1 = 414$, $n_2 = 18$, $t_2 = 391$, $n_3 = 23$, $t_3 = 306$. Для системи

$$\begin{cases} x \equiv 1 \pmod{17}, \\ x \equiv 0 \pmod{414} \end{cases}$$

із рівностей $414 = 24 \cdot 17 + 6$, $17 = 3 \cdot 6 - 1$ знаходимо: $1 = 3 \cdot 414 - 73 \cdot 17$, звідки $B_1 = 3 \cdot 414 = 1242$. Для системи

$$\begin{cases} x \equiv 1 \pmod{18}, \\ x \equiv 0 \pmod{391} \end{cases}$$

із рівностей $391 = 21 \cdot 18 + 13$, $18 = 1 \cdot 13 + 5$, $13 = 2 \cdot 5 + 3$, $5 = 2 \cdot 3 - 1$ знаходимо: $1 = 7 \cdot 391 - 152 \cdot 18$, звідки $B_2 = 7 \cdot 391 = 2737$. Нарешті для системи

$$\begin{cases} x \equiv 1 \pmod{23}, \\ x \equiv 0 \pmod{306} \end{cases}$$

із рівностей $306 = 13 \cdot 23 + 7$, $23 = 3 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$ знаходимо: $1 = 10 \cdot 306 - 133 \cdot 23$, звідки $B_3 = 10 \cdot 306 = 3060$. Тому розв'язки початкової системи мають вигляд: $x \equiv 5 \cdot 1242 + 6 \cdot 2737 + 10 \cdot 3060 \pmod{17 \cdot 18 \cdot 23} \equiv 53232 \pmod{7038} \equiv 3966 \pmod{7038}$. \square

Задача 6.7. Для яких значень параметра a система конгруенцій

$$\begin{cases} x \equiv 5 \pmod{6}, \\ x \equiv 8 \pmod{15}, \\ x \equiv a \pmod{10} \end{cases} \quad (6.21)$$

буде сумісною?

Розв'язання. $x - 5$ ділиться на 6 тоді й лише тоді, коли воно ділиться на 2 і 3. Тому конгруенція $x \equiv 5 \pmod{6}$ рівносильна системі

$$\begin{cases} x \equiv 5 \equiv 1 \pmod{2}, \\ x \equiv 5 \equiv 2 \pmod{3}. \end{cases}$$

Аналогічно другу конгруенцію з (6.21) можна замінити системою

$$\begin{cases} x \equiv 8 \equiv 3 \pmod{5}, \\ x \equiv 8 \equiv 2 \pmod{3}, \end{cases}$$

а третю – системою

$$\begin{cases} x \equiv a \pmod{2}, \\ x \equiv a \pmod{5}. \end{cases}$$

Отже, початкова система (6.21) рівносильна системі

$$\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv a \pmod{2}, \\ x \equiv a \pmod{5}. \end{cases} \quad (6.22)$$

Порівнюючи в (6.22) першу конгруенцію з четвертою, а третю – з п'ятою, бачимо, що для сумісності цієї системи необхідно (а з китайської теореми про остатці випливає, що й достатньо), щоб параметр a задовільняв систему

$$\begin{cases} a \equiv 1 \pmod{2}, \\ a \equiv 3 \pmod{5}. \end{cases}$$

Очевидно, що $a = 3$ останню систему задовільняє. Тому за теоремою 6.2 загальний розв'язок цієї системи має вигляд $a \equiv 3 \pmod{10}$. Отже, початкова система (6.21) сумісна тоді й тільки тоді, коли $a \equiv 3 \pmod{10}$. \square

6.4. Задачі для самостійного розв'язування

1. Розв'язати за допомогою алгоритму Евкліда лінійні конгруенції:
 - (a) $59x \equiv 17 \pmod{71}$; (b) $91x \equiv 29 \pmod{109}$;
 - (c) $38x \equiv 68 \pmod{83}$; (d) $44x \equiv 71 \pmod{97}$;
 - (e) $119x \equiv 17 \pmod{125}$; (f) $83x \equiv 25 \pmod{112}$.

2. Розв'язати за допомогою ланцюгових дробів лінійні конгруенції:

- (a) $72x \equiv 30 \pmod{85}$; (b) $104x \equiv 42 \pmod{122}$;
- (c) $51x \equiv 71 \pmod{98}$; (d) $57x \equiv 84 \pmod{110}$;
- (e) $106x \equiv 30 \pmod{138}$; (f) $96x \equiv 38 \pmod{125}$.

3. Розв'язати за допомогою теореми Ойлера лінійні конгруенції:

- (a) $25x \equiv 14 \pmod{36}$; (b) $27x \equiv 16 \pmod{50}$;
- (c) $21x \equiv 33 \pmod{40}$; (d) $11x \equiv 19 \pmod{54}$;
- (e) $35x \equiv 19 \pmod{48}$; (f) $15x \equiv 23 \pmod{56}$.

4. До числа 456 додати справа три цифри x , y і z так, щоб число $\overline{456xyz}$ ділилось

- (a) на 7, 8 і 9; (b) на 8, 9 і 10; (c) на 9, 10 і 11;
- (d) на 10, 11 і 12; (e) на 12, 13 і 14; (f) на 14, 15 і 16.

5. Розв'язати системи лінійних конгруенцій:

$$(a) \begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 5 \pmod{8}, \\ x \equiv 7 \pmod{11}; \end{cases} \quad (b) \begin{cases} x \equiv 2 \pmod{4}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{7}, \\ x \equiv 5 \pmod{9}; \end{cases}$$

$$(c) \begin{cases} x \equiv 7 \pmod{8}, \\ x \equiv 5 \pmod{9}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 1 \pmod{11}; \end{cases} \quad (d) \begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 2 \pmod{9}, \\ x \equiv 2 \pmod{10}, \\ x \equiv 2 \pmod{11}. \end{cases}$$

6. Розв'язати системи лінійних конгруенцій:

$$(a) \begin{cases} x \equiv 7 \pmod{15}, \\ x \equiv 4 \pmod{32}, \\ x \equiv 19 \pmod{23}; \end{cases} \quad (b) \begin{cases} x \equiv 13 \pmod{16}, \\ x \equiv 2 \pmod{25}, \\ x \equiv 11 \pmod{27}; \end{cases}$$

$$(c) \begin{cases} x \equiv 14 \pmod{18}, \\ x \equiv 5 \pmod{25}, \\ x \equiv 21 \pmod{41}; \end{cases} \quad (d) \begin{cases} x \equiv 12 \pmod{17}, \\ x \equiv 11 \pmod{21}, \\ x \equiv 10 \pmod{29}. \end{cases}$$

7. Розв'язати системи лінійних конгруенцій:

$$(a) \begin{cases} 20x \equiv 12 \pmod{56}, \\ 20x \equiv 34 \pmod{54}, \\ 24x \equiv 21 \pmod{57}; \end{cases} \quad (b) \begin{cases} 21x \equiv 15 \pmod{45}, \\ 27x \equiv 33 \pmod{48}, \\ 22x \equiv 18 \pmod{46}; \end{cases}$$

$$(c) \quad \begin{cases} 20x \equiv 32 \pmod{52}, \\ 15x \equiv 27 \pmod{54}, \\ 16x \equiv 14 \pmod{50}; \end{cases} \quad (d) \quad \begin{cases} 24x \equiv 8 \pmod{68}, \\ 21x \equiv 33 \pmod{60}, \\ 16x \equiv 42 \pmod{66}. \end{cases}$$

8. Знайти найменше натуральне число, яке при діленні на m, n і k дає відповідно остаті a, b і c :

- (a) $m = 12, n = 13, k = 14, a = 5, b = 6, c = 7;$
- (b) $m = 10, n = 12, k = 15, a = 9, b = 5, c = 14;$
- (c) $m = 14, n = 16, k = 20, a = 10, b = 6, c = 2;$
- (d) $m = 15, n = 16, k = 18, a = 13, b = 5, c = 7.$

9. Для яких значень параметра a система конгруенцій

$$(a) \quad \begin{cases} x \equiv 11 \pmod{24}, \\ x \equiv 7 \pmod{10}, \\ x \equiv 5 \pmod{22}, \\ x \equiv a \pmod{30}; \end{cases} \quad (b) \quad \begin{cases} x \equiv 10 \pmod{35}, \\ x \equiv 8 \pmod{18}, \\ x \equiv 6 \pmod{20}, \\ x \equiv a \pmod{42}; \end{cases}$$

$$(c) \quad \begin{cases} x \equiv 5 \pmod{28}, \\ x \equiv 17 \pmod{20}, \\ x \equiv 7 \pmod{30}, \\ x \equiv a \pmod{70}; \end{cases} \quad (d) \quad \begin{cases} x \equiv 7 \pmod{18}, \\ x \equiv 7 \pmod{27}, \\ x \equiv 7 \pmod{40}, \\ x \equiv a \pmod{60}. \end{cases}$$

буде сумісною?

10. Обчислити:

- (a) $n \bmod 60$, якщо $n \bmod 20 = 7$ і $n \bmod 42 = 19$;
- (b) $n \bmod 70$, якщо $n \bmod 30 = 13$ і $n \bmod 84 = 25$;
- (c) $n \bmod 105$, якщо $n \bmod 45 = 17$ і $n \bmod 70 = 32$;
- (d) $n \bmod 84$, якщо $n \bmod 60 = 27$ і $n \bmod 70 = 37$.