

7. Конгруенції вищих степенів

7.1. Конгруенції вищих степенів за простим модулем

Перейдемо тепер від конгруенцій першого степеня з однією невідомою до конгруенцій більш високих степенів. Почнемо з детального розгляду випадку простого модуля. Надалі в цьому параграфі буква p завжди позначатиме просте число. Загальний вигляд конгруенції n -го степеня за модулем числа p такий:

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{p}, \quad a_0, \dots, a_n \in \mathbb{Z}, \quad p \nmid a_0. \quad (7.1)$$

Але якщо $p \nmid a_0$, то існує таке $\alpha \in \mathbb{N}$, що $\alpha a_0 \equiv 1 \pmod{p}$. Тому після множення конгруенції (7.1) на α і заміни αa_0 на 1 матимемо конгруенцію

$$x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n \equiv 0 \pmod{p}, \quad (7.2)$$

яка рівносильна конгруенції (7.1). Тому, не обмежуючи загальності, в разі потреби можна вважати, що старший коефіцієнт конгруенції дорівнює 1.

Наприклад, перейдемо від конгруенції $11x^3 + 14x^2 - 9x + 12 \equiv 0 \pmod{41}$ до рівносильної їй конгруенції зі старшим коефіцієнтом 1. Для цього спочатку знаходимо розв'язок $y \equiv 15 \pmod{41}$ конгруенції $11y \equiv 1 \pmod{41}$. Тоді початкова конгруенція рівносильна конгруенції $11 \cdot 15x^3 + 14 \cdot 15x^2 - 9 \cdot 15x + 12 \cdot 15 \equiv 0 \pmod{41}$, тобто конгруенції $x^3 + 5x^2 - 12x + 16 \equiv 0 \pmod{41}$. Позначивши многочлен у лівій частині (7.1) або (7.2) через $f(x)$, записуватимемо відповідну конгруенцію у компактнішій формі

$$f(x) \equiv 0 \pmod{p}. \quad (7.3)$$

Твердження 7.1. За простим модулем p кожна конгруенція степеня, більшого або рівного p , еквівалентна деякій конгруенції степеня, меншого за p .

Доведення. Нехай в конгруенції (7.3) многочлен $f(x)$ має степінь більший або рівний p . Поділимо $f(x)$ на многочлен $x^p - x$ з остачею: $f(x) = (x^p - x)g(x) + r(x)$, де $g(x)$ – частка від ділення, а $r(x)$ – остача. Згідно з теоремою Ферма $x^p - x \equiv 0 \pmod{p}$, тому конгруенція (7.3) рівносильна конгруенції $r(x) \equiv 0 \pmod{p}$. Але степінь остачі $r(x)$ є меншим за степінь многочлена $x^p - x$, тобто меншим за p . \square

Приклад. Замінимо конгруенцію $x^{17} + 2x^7 + 5x^5 + x^2 - 3 \equiv 0 \pmod{7}$ рівносильною конгруенцією степеня, меншого за 7. Для цього можна або поділити $x^{17} + 2x^7 + 5x^5 + x^2 - 3$ на $x^7 - x$ з остачею, або (що насправді те саме) скористатися теоремою Ойлера, тобто тим, що $x^{\varphi(p)} \equiv 1 \pmod{p}$. Тоді матимемо: $x^{17} \equiv x^{17-2 \cdot 6} \equiv x^5 \pmod{7}$, $x^7 \equiv x \pmod{7}$. Таким чином, вихідна конгруенція рівносильна конгруенції $6x^5 + x^2 + 2x - 3 \equiv 0 \pmod{7}$.

Теорема 7.1 (Декарт). *Нехай $f(x) \equiv 0 \pmod{p}$ – довільна конгруенція степеня n . Тоді для кожного цілого числа x_0 існує такий многочлен $g(x)$ степеня $n-1$ з цілими коефіцієнтами, що $f(x) \equiv (x - x_0)g(x) + f(x_0) \pmod{p}$.*

Доведення. У кільці $\mathbb{Z}[x]$ многочленів від змінної x з цілими коефіцієнтами залишається справедливою теорема про ділення з остачею, хоча і в децьо послабленій формі: для довільного многочлена $u(x) \in \mathbb{Z}[x]$ і довільного многочлена $v(x) \in \mathbb{Z}[x]$ зі старшим коефіцієнтом 1 існують, причому однозначно визначені, такі многочлени $q(x)$ і $r(x)$, що $u(x) = v(x)q(x) + r(x)$ і степінь многочлена $r(x)$ менший за степінь многочлена $v(x)$ (або $r(x)$ є нульовим многочленом). Застосовуючи цю теорему до многочленів $f(x)$ і $x - x_0$, одержуємо рівність

$$f(x) = (x - x_0)g(x) + r(x), \quad (7.4)$$

а позаяк степінь остачі $r(x)$ має бути меншим за степінь многочлена $x - x_0$, то $r(x)$ є многочленом нульового степеня, тобто деякою константою $c \in \mathbb{Z}$. Очевидно також, що степінь многочлена $g(x)$ дорівнює $n-1$. Підставляючи в рівність (7.4) замість x число x_0 , одержимо: $f(x_0) = (x_0 - x_0)g(x_0) + c = c$. Тому $f(x) = (x - x_0)g(x) + f(x_0)$ і погодів $f(x) \equiv (x - x_0)g(x) + f(x_0) \pmod{p}$. \square

Наслідок 1 (Теорема Безу). *Конгруенція (7.3) має розв'язок $x \equiv x_0 \pmod{p}$ тоді й тільки тоді, коли її ліва частина $f(x)$ ділиться на $x - x_0$ за модулем p (тобто існує такий многочлен $g(x)$ степеня, меншого за степінь $f(x)$, що $f(x) \equiv (x - x_0)g(x) \pmod{p}$).*

Доведення. Якщо $x \equiv x_0 \pmod{p}$ є розв'язком конгруенції (7.3), то $f(x_0) \equiv x_0 \pmod{p}$ і за теоремою Декарта $f(x) \equiv (x - x_0)g(x) + f(x_0) \pmod{p}$ тобто $f(x)$ ділиться на $x - x_0$ за модулем p . У зворотний бік доведення очевидне. \square

Зауважимо, що в доведенні обох теорем простота модуля p не використовувалась, тому вони будуть правильними для довільного модуля.

Теорема 7.2. *Конгруенція (7.3) степеня n за простим модулем p має не більше ніж n різних за модулем p розв'язків. Якщо вона має рівно n різних розв'язків, то її ліва частина розкладається за модулем p на n лінійних множників.*

Доведення. Скористаємося методом математичної індукції. Для $n = 1$ маємо конгруенцію $a_0x + a_1 \equiv 0 \pmod{p}$, яка рівносильна певній конгруенції вигляду $x + b_1 \equiv 0 \pmod{p}$. Але тоді $x \equiv -b_1 \pmod{p}$ є єдиним її розв'язком, а в лівій частині маємо один лінійний множник.

Припустимо тепер, що теорема справджується для всіх конгруенцій степеня $n - 1$, і розглянемо конгруенцію $f(x) \equiv 0 \pmod{p}$ степеня n . Якщо вона не має розв'язків, то твердження теореми виконується. Якщо ж вона має розв'язок, наприклад, x_0 , то за теоремою Безу

$$f(x) \equiv (x - x_0)g(x) \pmod{p}, \quad (7.5)$$

причому степінь многочлена $g(x)$ дорівнює $n - 1$. Оскільки число p — просте, то всі розв'язки конгруенції $f(x) \equiv 0 \pmod{p}$ містяться серед розв'язків конгруенцій $x - x_0 \equiv 0 \pmod{p}$ і $g(x) \equiv 0 \pmod{p}$. Перша з них за модулем p має рівно один розв'язок, а друга, за припущенням індукції, не більше ніж $n - 1$ різних розв'язків. Тому початкова конгруенція має не більше ніж n різних розв'язків.

Якщо вона має n різних розв'язків, то конгруенція $g(x) \equiv 0 \pmod{p}$ має $n - 1$ різних розв'язків, і, за припущенням індукції, $g(x)$ розкладається на $n - 1$ лінійних множників. Тоді з (7.5) випливає, що $f(x)$ розкладається на n лінійних множників. \square

Зауважимо, що для складених модулів теорема 7.2 не виконується. Так, конгруенція $x^2 - 1 \equiv 0 \pmod{8}$ має аж 4 різні розв'язки: $x_1 \equiv 1 \pmod{8}$, $x_2 \equiv 3 \pmod{8}$, $x_3 \equiv 5 \pmod{8}$, $x_4 \equiv 7 \pmod{8}$.

Наслідок 1. *Якщо для многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ степеня n конгруенція*

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{p} \quad (7.6)$$

має більше ніж n різних за модулем p розв'язків, то всі коефіцієнти многочлена $f(x)$ діляться на p .

Доведення. Припустимо, що не всі коефіцієнти многочлена $f(x)$ діляться на p . Тоді, викинувши з лівої частини конгруенції (7.6) всі одночлени з коефіцієнтами, кратними p , одержимо рівносильну початковій конгруенцію степеня $\leq n$. За умовою вона має більше ніж n різних за модулем p розв'язків, що суперечить теоремі 7.2. \square

Задача 7.1. Нехай конгруенція $a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{p}$ має n різних за модулем p розв'язків $x \equiv x_1, x_2, \dots, x_n \pmod{p}$ і нехай $S_1 = x_1 + x_2 + \dots + x_n$, $S_2 = x_1x_1 + x_1x_3 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n$, \dots , $S_n = x_1x_2 \dots x_n$. Довести, що

$$a_1 \equiv -a_0S_1 \pmod{p}, \quad a_2 \equiv a_0S_2 \pmod{p}, \quad a_3 \equiv -a_0S_3 \pmod{p}, \quad \dots, \\ a_n \equiv (-1)^n a_0S_n \pmod{p}.$$

Розв'язання. Очевидно, що

$$a_0(x-x_1)(x-x_2) \dots (x-x_n) = a_0(x^n - S_1x^{n-1} + S_2x^{n-2} - \dots + (-1)^n S_n).$$

Розглянемо конгруенцію

$$a_0x^n + a_1x^{n-1} + \dots + a_n - a_0(x-x_1)(x-x_2) \dots (x-x_n) \equiv 0 \pmod{p}.$$

Степінь цієї конгруенції менший за n , але вона має принаймні n різних розв'язків $x \equiv x_1, x_2, \dots, x_n \pmod{p}$. З наслідку 1 випливає, що всі її коефіцієнти кратні p . А це рівносильно конгруенціям, які треба було довести. \square

Наслідок 2. Нехай число p — просте.

(a) Конгруенція $x^{p-1} - 1 \equiv 0 \pmod{p}$ має рівно $p-1$ розв'язок, а саме $\overline{1}, \overline{2}, \dots, \overline{p-1}$.

(b) Для кожного натурального дільника d числа p конгруенція

$$x^d - 1 \equiv 0 \pmod{p} \tag{7.8}$$

має рівно d різних розв'язків.

Доведення. (a) Це безпосередньо випливає з теореми Ферма.

(b) Нехай $d \mid (p-1)$ і $p-1 = d \cdot k$. Тоді конгруенцію (7.7), яка згідно з пунктом (a) має $p-1$ різних розв'язків, можна записати у вигляді $(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1) \equiv 0 \pmod{p}$. Але тоді кожен

із розв'язків має бути або розв'язком конгруенції $x^d - 1 \equiv 0 \pmod{p}$, або розв'язком конгруенції $x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 \equiv 0 \pmod{p}$. За теоремою 7.2 остання не може мати більше ніж $d(k-1)$ розв'язків. Отже, конгруенція $x^d - 1 \equiv 0 \pmod{p}$ повинна мати не менше ніж d розв'язків. Оскільки за тією ж теоремою більше ніж d розв'язків вона мати не може, то вона має рівно d різних розв'язків. \square

Зауважимо, що з наслідку 2(a) теореми 7.2 і теореми Безу випливає, що $x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}$. Підставивши сюди $x = 0$, матимемо $-1 \equiv (-1)(-2)\cdots(-p+1) \pmod{p}$ або $(p-1)! \equiv -1 \pmod{p}$, тобто теорему Вільсона.

Наслідок 3. Конгруенція

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1} x + b_n \equiv 0 \pmod{p}, \quad (7.9)$$

де $n \leq p$ і $b_n \not\equiv 0 \pmod{p}$, має n різних за модулем p розв'язків тоді й лише тоді, коли всі коефіцієнти остачі від ділення $x^{p-1} - 1$ на $f(x)$ будуть кратними p .

Доведення. За вже згадуваною теоремою про ділення з остачею в кільці $\mathbb{Z}[x]$ існують такі многочлени $g(x)$ і $r(x)$ з цілыми коефіцієнтами, що $x^{p-1} - 1 = f(x)g(x) + r(x)$ і степінь остачі $r(x)$ є меншим за n .

Необхідність. Нехай конгруенція (7.9) має n різних розв'язків і x_0 — один із них. Із умови $b_n \not\equiv 0 \pmod{p}$ випливає, що $x_0 \not\equiv 0 \pmod{p}$. Тоді за теоремою Ферма $x_0^{p-1} - 1 \equiv 0 \pmod{p}$, так що $r(x_0) \equiv (x_0^{p-1} - 1) - f(x_0)g(x_0) \equiv 0 \pmod{p}$. Таким чином, кожен із розв'язків конгруенції (7.9) є одночасно і розв'язком конгруенції $r(x_0) \equiv 0 \pmod{p}$, степінь якої є меншим за n . Тому, згідно з наслідком 1, усі коефіцієнти остачі $r(x)$ діляться на p .

Достатність. Нехай усі коефіцієнти остачі $r(x)$ діляться на p , а s і t — кількості розв'язків конгруенцій

$$f(x_0) \equiv 0 \pmod{p} \quad (7.10)$$

i

$$g(x_0) \equiv 0 \pmod{p} \quad (7.11)$$

відповідно. Тоді кожен розв'язок x_0 конгруенції $x^{p-1} - 1 \equiv 0 \pmod{p}$ (яка за наслідком 2(a) з теореми 7.2 має $p-1$ різних розв'язків) є розв'язком або конгруенції (7.10), або конгруенції (7.11), бо $0 \equiv r(x_0) = x_0^{p-1} - 1 - f(x_0)g(x_0) \equiv -f(x_0)g(x_0) \pmod{p}$. Тому $s+t \geq p-1$, звідки

$s \geq p-1-t$. З іншого боку, степінь многочлена $g(x)$ дорівнює $p-1-n$, тому за теоремою 7.2 конгруенція (7.11) не може мати більше ніж $p-1-n$ розв'язків, тобто $t \leq p-1-n$. Отже, $s \geq p-1-(p-1-n) = n$. Але за тією ж теоремою конгруенція (7.10) не може мати більше ніж n розв'язків. Отже, $s = n$, що й вимагалося. \square

Задача 7.2. Нехай натуральні числа n і a взаємно прості і $n < p$. Довести, що двочленна конгруенція $x^n - a \equiv 0 \pmod{p}$ має n різних розв'язків тоді й лише тоді, коли $n|(p-1)$ і $a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$.

Розв'язання. За наслідком 3 конгруенція $x^n - a \equiv 0 \pmod{p}$ має n різних розв'язків тоді й лише тоді, коли всі коефіцієнти остачі від ділення $x^{p-1}-1$ на x^n-a є кратними p . Знайдемо цю остачу. Із рівності $x^{p-1}-1 = (x^n-a)(x^{p-1-n}+ax^{p-1-2n}+a^2x^{p-1-3n}+\dots+a^{k-1}x^{p-1-kn})+(a^kx^{p-1-kn}-1)$ випливає, що остача дорівнює $a^kx^{p-1-kn}-1$, де $k = \left[\frac{p-1}{n} \right]$.

Якщо $p-1-kn > 0$, то коефіцієнти a^k та 1 остачі не кратні p , тому конгруенція $x^n - a \equiv 0 \pmod{p}$ не може мати n розв'язків. Таким чином, $p-1-kn = 0$, $k = \frac{p-1}{n}$, $n|(p-1)$ і $r(x) = a^k - 1$. Отже, всі коефіцієнти остачі діляться на p тоді й лише тоді, коли $p|(a^k - 1)$, тобто коли $a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$. \square

Задача 7.3. З'ясувати, скільки розв'язків має конгруенція: (a) $x^4 \equiv 3 \pmod{13}$, (б) $x^6 \equiv 3 \pmod{7}$, і знайти ці розв'язки.

Розв'язання. (a) За попередньою задачею для $p = 13$, $n = 4$, $a = 3$ маємо $4 | (13-1)$ і $3^{\frac{13-1}{4}} = 3^3 \equiv 1 \pmod{13}$, тому конгруенція $x^4 \equiv 3 \pmod{13}$ має 4 різні розв'язки. Послідовно перебираючи числа ± 1 , ± 2 , ± 3 , знаходимо: $x_1 \equiv 2 \pmod{13}$, $x_2 \equiv -2 \equiv 11 \pmod{13}$, $x_3 \equiv 3 \pmod{13}$, $x_4 \equiv -3 \equiv 10 \pmod{13}$ (оскільки всі 4 розв'язки вже знайдено, то перебирати далі числа ± 4 , ± 5 , ± 6 не потрібно).

(б) Числа $p = 7$, $n = 6$, $a = 3$ не задовольняють умову попередньої задачі, бо $3^{\frac{7-1}{6}} = 3^{\frac{6}{6}} = 3 \not\equiv 1 \pmod{7}$. Тому конгруенція $x^6 \equiv 3 \pmod{7}$ має менше 6 розв'язків. Послідовно перебираючи числа ± 1 , ± 2 , ± 3 , перевірюємося, що вона взагалі не має розв'язків. \square

Природно постає задача знаходження розв'язків довільної конгруенції (7.1) n -го степеня. Загальних простих методів розв'язання цієї задачі нема, однак процедуру перебору можна суттєво спростити, якщо дотримуватись такої послідовності дій:

1 крок: замінююмо всі коефіцієнти в лівій частині конгруенції (7.1) відповідними елементами із системи найменших невід'ємних лишків за модулем p .

2 крок: використовуючи твердження 7.1 або теорему Ферма, понижуємо степінь конгруенції, щоб він став менший за p , і в разі необхідності ще раз повторюємо 1 крок.

3 крок: безпосереднім випробуванням елементів системи найменших невід'ємних лишків $0, 1, 2, \dots, p-1$ (інколи зручніше брати елементи системи $0, \pm 1, \dots, \pm(p-1)/2$) знаходимо розв'язки конгруенції, що вийшла після попереднього кроку. Вони і будуть розв'язками вихідної конгруенції (7.1).

Проілюструємо цей метод на прикладі.

Задача 7.4. Розв'язати конгруенцію $7x^{10} + 3x^3 - 12x + 1 \equiv 0 \pmod{5}$.

Розв'язання. Після першого кроку отримуємо конгруенцію $2x^{10} + 3x^3 + 3x + 1 \equiv 0 \pmod{5}$. Оскільки за теоремою Ферма $x^5 \equiv x \pmod{5}$, то після другого кроку отримуємо конгруенцію $2x^{10-2\cdot4} + 3x^3 + 3x + 1 = 3x^3 + 2x^2 + 3x + 1 \equiv 0 \pmod{5}$. Безпосередня перевірка: $3 \cdot 0^3 + 2 \cdot 0^2 + 3 \cdot 0 + 1 \not\equiv 0 \pmod{5}$, $3 \cdot 1^3 + 2 \cdot 1^2 + 3 \cdot 1 + 1 \not\equiv 0 \pmod{5}$, $3 \cdot 2^3 + 2 \cdot 2^2 + 3 \cdot 2 + 1 \not\equiv 0 \pmod{5}$, $3 \cdot 3^3 + 2 \cdot 3^2 + 3 \cdot 3 + 1 \not\equiv 0 \pmod{5}$, $3 \cdot 4^3 + 2 \cdot 4^2 + 3 \cdot 4 + 1 \not\equiv 0 \pmod{5}$ показує, що остання конгруенція розв'язків не має. \square

Задача 7.5. Розв'язати конгруенцію $2x^4 + x^3 - 3x^2 - 2x - 2 \equiv 0 \pmod{11}$.

Розв'язання. Цю конгруенцію можна розв'язувати аналогічно попередній. Однак у даному випадку є ефективніший метод — за допомогою розкладу многочлена $f(x) = 2x^4 + x^3 - 3x^2 - 2x - 2$ на множники над полем \mathbb{Z}_{11} (на жаль, у загальному випадку процедура розкладу многочлена з коефіцієнтами зі скінченного поля на множники вимагає надзвичайно громіздких обчислень, і досі невідомо, чи існують алгоритми, які могли б зменшити об'єм обчислень до розумних меж). Випробовуючи маленькі за абсолютною величиною лишки, швидко знаходимо один із розв'язків: $x \equiv 2 \pmod{11}$. Звідси знаходимо: $f(x) \equiv 2(x-2)(x^3 - 3x^2 - 2x - 5) \pmod{11}$. Але $3^3 - 3 \cdot 3^2 - 2 \cdot 3 - 5 \equiv 0 \pmod{11}$, тому можна виділити ще один множник: $f(x) \equiv 2(x-2)(x-3)(x^2 - 2) \pmod{11}$. Далі легко пересвідчитись, що конгруенція $x^2 - 2 \equiv 0 \pmod{11}$ вже розв'язків не має. Отже, розв'язками вихідної конгруенції є $x_1 \equiv 2 \pmod{11}$ і $x_2 \equiv 3 \pmod{11}$. \square

Деякі з тверджень, що розглядалися в цьому параграфі, можна легко узагальнити на випадок конгруенцій з кількома невідомими вигляду

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p}, \quad (7.12)$$

де $f(x_1, \dots, x_n)$ – многочлен із цілыми коєфіцієнтами. Безпосереднім узагальненням твердження 7.1 є

Твердження 7.2. Якщо в ліву частину конгруенції (7.12) деякі невідомі входять зі степенями, не меншими за p , то (7.12) можна замінити рівносильною їй конгруенцією, в якій степінь кожного невідомого не перевищує $p - 1$.

Доведення майже повністю повторює доведення твердження 7.1, тому залишаємо його читачеві як вправу.

Твердження 7.3. Нехай в конгруенції (7.12) степінь кожного невідомого не перевищує $p - 1$. Якщо цю конгруенцію задоволює будь-який набір x_1, \dots, x_n цілих чисел, то всі коєфіцієнти многочлена $f(x_1, \dots, x_n)$ діляться на p .

Доведення легко проводиться природною індукцією за кількістю невідомих. Базою індукції слугує наслідок 1 з теореми 7.2. Деталі доведення залишаємо читачеві як вправу.

Теорема 7.3 (Шевальє). Нехай $f(x_1, \dots, x_n)$ – многочлен із цілими коєфіцієнтами, вільний член якого ділиться на просте число p . Якщо степінь цього многочлена менший за кількість невідомих, то конгруенція $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$ крім тривіального розв'язку $(0, \dots, 0)$ має ще хоча б один нетривіальний розв'язок.

Доведення. Нехай степінь многочлена $f(x_1, \dots, x_n)$ дорівнює s . За умовою $s < n$. Розглянемо конгруенцію

$$(f(x_1, \dots, x_n))^{p-1} \equiv 1 - (1 - x_1^{p-1}) \cdots (1 - x_n^{p-1}) \pmod{p}. \quad (7.13)$$

Згідно з твердженням 7.2 її можна замінити рівносильною конгруенцією

$$F(x_1, \dots, x_n) \equiv 1 - (1 - x_1^{p-1}) \cdots (1 - x_n^{p-1}) \pmod{p}, \quad (7.14)$$

де степінь кожного невідомого в лівій частині не перевищує $p - 1$. З іншого боку, степінь многочлена $F(x_1, \dots, x_n)$ не перевищує степеня многочлена $(f(x_1, \dots, x_n))^{p-1}$, тобто $s(p - 1)$, а тому менший за $n(p - 1)$.

Старшим членом конгруенції (7.14) є $(-1)^{n+1}x_1^{p-1}\cdots x_n^{p-1}$, який не може скоротитись за модулем p з деяким одночленом із лівої частини (7.14), бо його степінь більший за степінь лівої частини. Коефіцієнт $(-1)^{n+1}$ при цьому старшому членові не ділиться на p , тому за твердженням 7.3 існує такий набір $(\alpha_1, \dots, \alpha_n)$ цілих чисел, що

$$(f(\alpha_1, \dots, \alpha_n))^{p-1} \not\equiv 1 - (1 - \alpha_1^{p-1}) \cdots (1 - \alpha_n^{p-1}) \pmod{p}. \quad (7.15)$$

Набір $(\alpha_1, \dots, \alpha_n)$ не може збігатися за модулем p з набором $(0, \dots, 0)$, бо останній задовільняє конгруенцію (7.13). Тому для деякого k $p \nmid \alpha_k$ і за теоремою Ферма $1 - \alpha_k^{p-1} \equiv 0 \pmod{p}$. Тоді з (7.15) випливає, що $(f(\alpha_1, \dots, \alpha_n))^{p-1} \not\equiv 1 \pmod{p}$. Останнє, знову ж таки за теоремою Ферма, можливе лише тоді, коли $f(\alpha_1, \dots, \alpha_n) \equiv 0 \pmod{p}$. Таким чином, $(\alpha_1, \dots, \alpha_n)$ є відмінним від $(0, \dots, 0)$ розв'язком конгруенції $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$. \square

Приклад. Для довільних цілих чисел a, b, c, d конгруенція $ax^2 + by^2 + cz^2 + du^2 \equiv 0 \pmod{p}$ має розв'язок (x_0, y_0, z_0, u_0) , в якому хоча б одне з чисел x_0, y_0, z_0, u_0 не ділиться на p .

7.2. Конгруенції вищих степенів за складеним модулем

У цьому параграфі ми розглянемо способи зведення конгруенцій вищих степенів за складеним модулем до конгруенцій за простими модулями. Основною підставою для такого зведення є наступна

Теорема 7.4. *Нехай $m = m_1 \cdots m_k$, де всі множники m_i попарно взаємно прості. Тоді конгруенція*

$$f(x) \equiv 0 \pmod{m}, \quad (7.16)$$

де $f(x)$ – довільний многочлен із цілими коефіцієнтами, рівносильна системі конгруенцій

$$\begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ \vdots \\ f(x) \equiv 0 \pmod{m_k}, \end{cases} \quad (7.17)$$

а кількість розв'язків конгруенції (7.16) дорівнює добуткові кількості розв'язків кожної з конгруенцій (7.17).

Доведення. З означення розв'язків системи конгруенцій випливає, що розв'язками системи (7.17) є класи лишків за модулем НСК(m_1, \dots, m_k). Але НСК(m_1, \dots, m_k) = m , бо модулі m_i попарно взаємно прості. Якщо клас лишків $a \pmod{m}$ задовольняє систему (7.17), то $m_1|f(a), \dots, m_k|f(a)$. Але тоді $m|f(a)$, тобто $f(a) \equiv 0 \pmod{m}$ і клас $a \pmod{m}$ є розв'язком конгруенції (7.16). Навпаки, якщо клас $a \pmod{m}$ задовольняє (7.16), то $m|f(a)$, звідки $m_1|f(a), \dots, m_k|f(a)$ і $f(a) \equiv 0 \pmod{m_1}, \dots, f(a) \equiv 0 \pmod{m_k}$, тобто $a \pmod{m}$ є розв'язком системи (7.17).

Доведемо тепер, що кількість розв'язків конгруенції (7.16) дорівнює $l_1 l_2 \cdots l_k$, де l_i — кількість розв'язків конгруенції $f(x) \equiv 0 \pmod{m_i}$. Справді, якщо хоча б одне з чисел l_i дорівнює 0, то система (7.17) несумісна. Але тоді, за щою доведеним, і конгруенція (7.16) не матиме розв'язків. Нехай тепер $a_1 \pmod{m_1}, \dots, a_k \pmod{m_k}$ — один із розв'язків конгруенції $f(x) \equiv 0 \pmod{m_1}, \dots, f(x) \equiv 0 \pmod{m_k}$. Оскільки модулі m_i попарно взаємно прості, то за китайською теоремою про остачі (теорема 6.3) система

$$\begin{cases} a \equiv a_1 \pmod{m_1}, \\ \vdots \\ a \equiv a_k \pmod{m_k} \end{cases}$$

однозначно визначає клас лишків $a \pmod{m}$, який буде розв'язком системи (7.17). Навпаки, клас лишків $a \pmod{m}$ однозначно визначає набір $(a_1 \pmod{m_1}, \dots, a_k \pmod{m_k})$ класів лишків за модулями m_1, \dots, m_k , причому якщо $a \pmod{m}$ є розв'язком системи (7.17), то кожен із класів $a_i \pmod{m_i}$ є розв'язком відповідної конгруенції $f(x) \equiv 0 \pmod{m_i}$. Таким чином, між розв'язками системи (7.17) і наборами розв'язків конгруенцій $f(x) \equiv 0 \pmod{m_1}, \dots, f(x) \equiv 0 \pmod{m_k}$ існує взаємно однозначна відповідність. Тому система (7.17) має $l_1 l_2 \cdots l_k$ розв'язків. Оскільки конгруенція (7.16) рівносильна системі (7.17), то друга частина теореми також доведена. \square

Наслідок 1. *Нехай $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ — канонічний розклад числа m . Тоді конгруенція (7.16) рівносильна системі*

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \vdots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{cases} \quad (7.18)$$

Задача 7.6. Розв'язати конгруенцію $x^4 - 31x^3 - 7x + 22 \equiv 0 \pmod{30}$.

Розв'язання. $30 = 2 \cdot 3 \cdot 5$, тому дана конгруенція еквівалентна системі

$$\begin{cases} x^4 - 31x^3 - 7x + 22 \equiv 0 \pmod{2}, \\ x^4 - 31x^3 - 7x + 22 \equiv 0 \pmod{3}, \\ x^4 - 31x^3 - 7x + 22 \equiv 0 \pmod{5}. \end{cases}$$

Після спрощень отримуємо систему:

$$\begin{cases} x \equiv 0 \pmod{2}, \\ x^2 + x + 1 \equiv 0 \pmod{3}, \\ x^4 + 4x^3 + 3x + 2 \equiv 0 \pmod{5}. \end{cases}$$

Шляхом випробовувань найменших лишків знаходимо розв'язки кожної з конгруенцій останньої системи: розв'язком першої конгруенції є $x \equiv 0 \pmod{2}$, другої — $x \equiv 1 \pmod{3}$, третя має два розв'язки — $x \equiv 1 \pmod{5}$ і $x \equiv 3 \pmod{5}$. Отже, маємо дві системи:

$$\begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv 1 \pmod{3}, \\ x \equiv 1 \pmod{5}, \end{cases} \quad \text{та} \quad \begin{cases} x \equiv 0 \pmod{2}, \\ x \equiv 1 \pmod{3}, \\ x \equiv 3 \pmod{5}. \end{cases}$$

Щоб розв'язати їх за допомогою китайської теореми про остачі, розв'яжемо спочатку допоміжні конгруенції $\frac{30}{2} \cdot y_1 \equiv 1 \pmod{2}$, $\frac{30}{3} \cdot y_2 \equiv 1 \pmod{3}$ і $\frac{30}{5} \cdot y_3 \equiv 1 \pmod{5}$. Отримуємо: $y_1 \equiv 1 \pmod{2}$, $y_2 \equiv 1 \pmod{3}$ і $y_3 \equiv 1 \pmod{5}$. Тепер уже легко знаходиться розв'язок першої конгруенції

$$x_1 \equiv \frac{30}{2} \cdot y_1 \cdot 0 + \frac{30}{3} \cdot y_2 \cdot 1 + \frac{30}{5} \cdot y_3 \cdot 1 = 15 \cdot 1 \cdot 0 + 10 \cdot 1 \cdot 1 + 6 \cdot 1 \cdot 1 = 16 \pmod{30}$$

і другої

$$x_2 \equiv \frac{30}{2} \cdot y_1 \cdot 0 + \frac{30}{3} \cdot y_2 \cdot 1 + \frac{30}{5} \cdot y_3 \cdot 31 = 15 \cdot 1 \cdot 0 + 10 \cdot 1 \cdot 1 + 6 \cdot 1 \cdot 3 = 28 \pmod{30}.$$

Отже, початкова конгруенція має 2 розв'язки: $x_1 \equiv 16 \pmod{30}$ і $x_2 \equiv 28 \pmod{30}$. \square

Таким чином, дослідження і знаходження розв'язків конгруенції $f(x) \equiv 0 \pmod{m}$, де $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ — канонічний розклад числа m , зводиться до дослідження і розв'язання конгруенцій вигляду

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{7.19}$$

де p — просте число. Розв'язки останньої конгруенції, очевидно, слід шукати серед розв'язків конгруенції

$$f(x) \equiv 0 \pmod{p}. \quad (7.20)$$

Нехай $x \equiv a_1 \pmod{p}$ — довільний розв'язок конгруенції (7.20). Тоді x можна записати у вигляді $x = a_1 + pt_1$, $t_1 \in \mathbb{Z}$. Підставимо це значення x у конгруенцію $f(x) \equiv 0 \pmod{p^2}$, попередньо розкладавши многочлен $f(a_1 + pt_1)$ у ряд Тейлора за степенями pt_1 :

$$\begin{aligned} f(a_1 + pt_1) &= f(a_1) + \frac{f'(a_1)}{1!}(pt_1) + \frac{f^{(2)}(a_1)}{2!}(pt_1)^2 + \cdots + \\ &+ \frac{f^{(s)}(a_1)}{s!}(pt_1)^s + \cdots \equiv f(a_1) + f'(a_1)pt_1 \pmod{p^2} \end{aligned}$$

(це можна робити, оскільки, як легко пересвідчитись, усі коефіцієнти $\frac{f^{(s)}(a_1)}{s!}$ є цілими числами). Одержануємо конгруенцію $f(a_1) + f'(a_1)pt_1 \equiv 0 \pmod{p^2}$. Оскільки $f(a_1) \equiv 0 \pmod{p}$, то $p | f(a_1)$, тому можемо переходити до конгруенції

$$\frac{f(a_1)}{p} + f'(a_1)t_1 \equiv 0 \pmod{p}. \quad (7.21)$$

Далі розглянемо два можливі випадки. I випадок: $p \nmid f'(a_1)$. Тоді конгруенція (7.21) має єдиний розв'язок $t_1 \equiv r_1 \pmod{p}$, тобто $t_1 = r_1 + pt_2$, $t_2 \in \mathbb{Z}$, а x можна записати у вигляді $x = a_1 + pr_1 + p^2t_2 = a_2 + p^2t_2$, де $a_2 = a_1 + pr_1$. Підставимо отримане значення в конгруенцію $f(x) \equiv 0 \pmod{p^3}$, знову попередньо розкладавши многочлен $f(a_2 + p^2t_2)$ у ряд Тейлора за степенями p^2t_2 . Аналогічно попередньому отримаємо $f(a_2) + f'(a_2)p^2t_2 \equiv 0 \pmod{p^3}$ або

$$\frac{f(a_2)}{p^2} + f'(a_2)t_2 \equiv 0 \pmod{p}, \quad (7.22)$$

оскільки $f(a_2) \equiv 0 \pmod{p^2}$, тобто $p^2 | f(a_2)$. $p \nmid f'(a_2)$, бо за побудовою $a_2 \equiv a_1 \pmod{p}$ і $f'(a_2) \equiv f'(a_1) \pmod{p}$. Тому конгруенція (7.22) має єдиний розв'язок $t_2 \equiv r_2 \pmod{p}$, тобто $t_2 = r_2 + pt_3$, $t_3 \in \mathbb{Z}$, а вираз для x набуває вигляду $x = a_2 + p^2r_2 + p^3t_3 = a_3 + p^3t_3$, де $a_3 = a_2 + p^2r_2$.

Продовжуючи аналогічним чином далі, одержимо, що кожний розв'язок $x \equiv a_1 \pmod{p}$ конгруенції (7.20) за умови $p \nmid f'(a_1)$ визначає

один розв'язок вигляду $x \equiv a_1 + a_2p + a_3p^2 + \cdots + a_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$ конгруенції (7.19).

II випадок: $p \mid f'(a_1)$. Тоді якщо $p \nmid \frac{f(a_1)}{p}$, тобто якщо $p^2 \nmid f(a_1)$, то серед чисел $x \equiv a_1 \pmod{p}$ немає жодного, яке б було розв'язком конгруенції $f(x) \equiv 0 \pmod{p^2}$, а тим самим і конгруенції (7.19). Якщо ж $p^2 \mid f(a_1)$, то очевидно, що всі числа $x \equiv a_1 \pmod{p}$ є розв'язками і конгруенції $f(x) \equiv 0 \pmod{p^2}$. Продовжуючи цей процес далі, матимемо: якщо $p \mid f'(a_1)$ і

$$x \equiv a_i \pmod{p^i} \quad (7.23)$$

— розв'язок конгруенції $f(x) \equiv 0 \pmod{p^i}$, то у випадку $p^{i+1} \nmid f(a_1)$ серед чисел (7.23) немає жодного розв'язку конгруенції $f(x) \equiv 0 \pmod{p^{i+1}}$, а у випадку $p^{i+1} \mid f(a_1)$ всі числа (7.23) є її розв'язками.

Задача 7.7. Розв'язати конгруенцію: (a) $4x^3 - 11x + 17 \equiv 0 \pmod{81}$; (б) $x^3 + 3x^2 - 5x + 11 \equiv 0 \pmod{25}$; (в) $x^3 + 3x^2 - 5x + 11 \equiv 0 \pmod{125}$.

Розв'язання. (a) Спочатку розглянемо конгруенцію $f(x) = 4x^3 - 11x + 17 \equiv 0 \pmod{3}$. Після спрощень дістанемо рівносильну їй конгруенцію $x^3 + x + 2 \equiv 0 \pmod{3}$. Перебираючи лишки за модулем числа 3, знаходимо розв'язок останньої конгруенції: $x \equiv 2 \pmod{3}$ або $x = 2 + 3t_1, t_1 \in \mathbb{Z}$. Оскільки $f(2) = 27, f'(2) = 37$ і $3 \nmid f'(2)$, то конгруенція $\frac{f(2)}{3} + f'(2)t_1 \equiv 0 \pmod{3}$ набуває вигляду $9 + 37t_1 \equiv 0 \pmod{3}$, звідки знаходимо $t_1 \equiv 0 \pmod{3}$ або $t_1 = 3t_2, t_2 \in \mathbb{Z}$. Отже, тепер маємо $x = 2 + 3^2t_2, t_2 \in \mathbb{Z}$. Тоді складаємо конгруенцію $\frac{f(2)}{3^2} + f'(2)t_2 \equiv 0 \pmod{3}$ і одержуємо: $t_2 \equiv 0 \pmod{3}$ або $t_2 = 3t_3, x = 2 + 3^3t_3, t_3 \in \mathbb{Z}$. Далі розглядаємо конгруенцію $\frac{f(2)}{3^3} + f'(2)t_3 \equiv 0 \pmod{3}$ і знаходимо: $t_3 \equiv 2 \pmod{3}$, звідки $t_3 = 2 + 3t_4$ і $x = 2 + 3^3(2 + 3t_4) = 56 + 3^4t_4, t_4 \in \mathbb{Z}$. Позаяк $3^4 = 81$, то $x \equiv 56 \pmod{81}$ буде єдиним розв'язком конгруенції $4x^3 - 11x + 17 \equiv 0 \pmod{81}$.

(б) Аналогічно пункту (a) починаємо із розгляду конгруенції $f(x) = x^3 + 3x^2 - 5x + 11 \equiv 0 \pmod{5}$ або рівносильної їй $x^3 + 3x^2 + 1 \equiv 0 \pmod{5}$. Підбором знаходимо розв'язки останньої: $x \equiv 1 \pmod{5}$ та $x \equiv 3 \pmod{5}$. Для $x \equiv 1 \pmod{5}$, тобто для $x = 1 + 5t_1, t_1 \in \mathbb{Z}$, складаємо конгруенцію $\frac{f(1)}{5} + f'(1)t_1 \equiv 0 \pmod{5}$. Оскільки $f(1) = 10, f'(1) = 4$, то одержуємо: $2 + 4t_1 \equiv 0 \pmod{5}$, або $1 + 2t_1 \equiv 0 \pmod{5}$, звідки $t_1 \equiv 2 \pmod{5}$ і $t_1 = 2 + 5t_2, x = 11 + 5^2t_2, t_2 \in \mathbb{Z}$. Отже, $x \equiv 11 \pmod{25}$.

Для $x \equiv 3 \pmod{5}$, тобто для $x = 3 + 5t_1, t_1 \in \mathbb{Z}$, маємо: $f(3) = 50, f'(3) = 40$. Таким чином, $5 \mid f'(3)$ і $5^2 \mid f(3)$, тому всі числа вигляду

$x \equiv 3 \pmod{5}$ є розв'язками і конгруенції $f(x) \equiv 0 \pmod{25}$. Але за модулем 25 ці числа утворюють 5 класів лишків: $3 \pmod{25}$, $8 \pmod{25}$, $13 \pmod{25}$, $18 \pmod{25}$, $23 \pmod{25}$.

Таким чином, розв'язками вихідної конгруенції є такі класи лишків: $3 \pmod{25}$, $8 \pmod{25}$, $11 \pmod{25}$, $13 \pmod{25}$, $18 \pmod{25}$, $23 \pmod{25}$.

(б) Використаємо результати, одержані в попередньому пункті. Розв'язками конгруенції $f(x) = x^3 + 3x^2 - 5x + 11 \equiv 0 \pmod{5}$ є $x \equiv 1 \pmod{5}$ та $x \equiv 3 \pmod{5}$. Розв'язок $x \equiv 1 \pmod{5}$ приводить до розв'язку $x \equiv 11 \pmod{25}$ конгруенції $\frac{f(1)}{5} + f'(1)t_1 \equiv 0 \pmod{5}$. Далі розв'язуємо конгруенцію $\frac{f(11)}{5^2} + f'(11)t_2 \equiv 0 \pmod{5}$ або еквівалентну їй $1 + 4t_2 \equiv 0 \pmod{5}$, одержуємо: $t_2 \equiv 1 \pmod{5}$, тобто $t_2 = 1 + 5t_3$ і $x = 36 + 5^3t_3$, $t_3 \in \mathbb{Z}$, що дає один розв'язок $x \equiv 36 \pmod{125}$ вихідної конгруенції.

Щодо чисел вигляду $x \equiv 3 \pmod{5}$, то в попередньому пункті довоєно, що всі вони є розв'язками і конгруенції $f(x) \equiv 0 \pmod{25}$. Але $5^3 \nmid f(3)$, тому розв'язків конгруенції $f(x) \equiv 0 \pmod{5^3}$ серед цих чисел уже не буде. Таким чином, вихідна конгруенція має єдиний розв'язок $x \equiv 36 \pmod{125}$. \square

7.3. Задачі для самостійного розв'язування

1. Розв'язати конгруенцію, попередньо понизивши її степінь: а) $6x^{10} - 11x + 2 \equiv 0 \pmod{5}$; б) $x^5 - 8x^4 + 9x^2 - x + 12 \equiv 0 \pmod{3}$; в) $x^7 - x^6 + 7x^2 - 3 \equiv 0 \pmod{5}$; г) $x^7 - 6 \equiv 0 \pmod{5}$; д) $3x^7 - 2x^6 + 2x^2 + 11 \equiv 0 \pmod{5}$.
2. Розв'язати конгруенцію, попередньо розкладавши ліву частину на множники: а) $x^3 + 4x^2 - 3 \equiv 0 \pmod{5}$; б) $x^4 + x + 4 \equiv 0 \pmod{11}$; в) $x^4 - 7x^3 + 12x^2 + 21x + 23 \equiv 0 \pmod{7}$; г) $x^4 - 2x^2 + 3x + 4 \equiv 0 \pmod{7}$.
3. З'ясувати, які з наступних конгруенцій вигляду $x^n \equiv a \pmod{p}$ мають n розв'язків, і знайти ці розв'язки: а) $x^3 \equiv 1 \pmod{7}$; б) $x^2 \equiv 2 \pmod{5}$; в) $x^5 \equiv 10 \pmod{11}$; г) $x^4 \equiv 5 \pmod{11}$.
4. Довести, що при $a \not\equiv 0 \pmod{7}$ та $b \not\equiv 0 \pmod{7}$ конгруенція $x^3 + ax + b \equiv 0 \pmod{7}$ не має розв'язків.
5. Довести, що для кожного простого модуля p має місце конгруенція $x^{5p+1} \equiv x^6 \pmod{p}$.

6. Нехай числа a і m взаємно прості, а $x_0 \pmod{m}$ — фіксований розв'язок конгруенції $x^n \equiv a \pmod{m}$. Доведіть, що $t \pmod{m}$ буде розв'язком конгруенції $x^n \equiv a \pmod{m}$ тоді й лише тоді, коли його можна подати у вигляді добутку $x_0 \pmod{m}$ на деякий розв'язок конгруенції $y^n \equiv 1 \pmod{m}$.
7. Розв'язати конгруенцію: а) $2x^4 + 4x^2 - 7x - 6 \equiv 0 \pmod{15}$; б) $6x^3 - 9x^2 + 23x - 10 \equiv 0 \pmod{30}$; в) $x^5 - 3x^4 + 8x^3 + 9x^2 + 4x + 12 \equiv 0 \pmod{42}$; г) $x^6 + x^4 + 2x^3 - x^2 - x + 2 \equiv 0 \pmod{66}$.
8. Розв'язати конгруенцію: а) $x^4 - 3x^3 - 2x^2 - 7x + 11 \equiv 0 \pmod{125}$; б) $x^4 + 3x^3 - 2x^2 - 10 \equiv 0 \pmod{343}$; в) $9x^2 + 29x + 62 \equiv 0 \pmod{64}$; г) $x^3 + 3x^2 - 5x + 16 \equiv 0 \pmod{625}$.