Міністерство освіти і науки України
Миколаївський національний університет
імені В.О. Сухомлинського

В. М. ДАРМОСЮК
О. Ю. ПАРХОМЕНКО

Алгебра та теорія чисел: конгруенції та їх застосування

(завдання для самостійної роботи та методичні вказівки щодо їх виконання)

Посібник для самостійної та дистанційної роботи студентів закладів вищої освіти

Миколаїв
2021

УДК 511.2

Автори:
Дармосюк В.М., Пархоменко О.Ю.

Рецензенти:

Лисенков Е. А.	доктор фізико-математичних наук, доцент кафедри інтелектуальних інформаційних систем Чорноморського національного університету імені Петра Могили
Бойчук О. В.	кандидат фізико-математичних наук, старший викладач кафедри вищої та прикладної математики Миколаївського національного аграрного університету

Посібник для самостійної та дистанційної роботи студентів закладів вищої освіти

Рекомендовано вченою радою Миколаївського національного університету імені В.О. Сухомлинського (протокол №19 від 31.05.2021 р.)

Посібник присвячено вивченню одних із основних понять алгебри та теорії чисел: конгруенції першого порядку, системи конгруенцій, конгруенції вищих порядків.
Мета посібника – допомогти студентам у формуванні їх математичного мислення, оволодінні теоретичними знаннями і практичними навичками розв’язування задач, необхідних в подальшій навчальній та професійній діяльності. Наведені типові завдання для самоперевірки знань студентів з метою підготовки до семестрового контролю з курсу “Алгебра та теорія чисел”.

Дармосюк В. М.
Алгебра та теорія чисел: конгруенції та їх застосування (завдання для самостійної роботи та методичні вказівки до їх виконання)/ В. М. Дармосюк, О. Ю. Пархоменко: посібник для самостійної та дистанційної роботи студентів. – Миколаїв: Миколаївський національний університет ім. В.О. Сухомлинського, 2021– 152 с.

ЗМІСТ

ПЕРЕДМОВА

Курс алгебри та теорії чисел відноситься до нормативної частини циклу професійної підготовки майбутнього фахівця в галузі природничо-математичних наук. Посібник містить матеріали для організації самостійної та дистанційної роботи студентів при вивченні теми «Конгруенції та їх застосування», яка є обов’язковою до вивчення при підготовці фахівців за спеціальностями 014.04 Середня освіта (Математика) та 014.08 Середня освіта (Фізика).

В посібнику наведено короткі теоретичні відомості, завдання для індивідуальної самостійної роботи, які спрямовані на вдосконалення вмінь та навичок студентів з даної теми, а також показують практичне завстосування теорії чисел та її медодів. Авторами розроблено методичні вказівки до виконання завдань, в яких детально пояснюється хід розв’язку кожної задачі. Це важливо при організації дистанційної або самостійної роботи студентів, які завдяки такому підходу мають змогу самостійно вивчити матеріал, дослідити методичні прийоми розв’язання задач та виконати індивідуальні завдання. Також в посібнику містяться тестові питання з даної теми та питання для самоконтролю, які допоможуть при підготовці студентів до поточного та підсумкового контролю знань.

Посібник «Алгебра та теорія чисел: конгруенції та їх застосування (завдання для самостійної роботи та методичні вказівки до їх виконання)» пройшов апробацію на механіко-математичному факультеті Миколаївського національного університету імені В. О. Сухомлинського та одержав позитивну оцінку як у студентів фізико-математичних спеціальностей факультету, так і викладачів кафедри фізики та математики.

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Конгруенції та їх властивості

Означення 1. Числа a і b називаються конгруентними за модулем m, якщо остачі при діленні їх на число m рівні між собою, тобто $a = mq + r,\ b = mq_1 + r$ і $0 \le r \le m$.

Записують це так: $a \equiv b \pmod m$.

Теорема 1. Для того щоб числа a і b були конгруентні за модулем m, необхідно і достатньо, щоб різниця $a - b$ ділилася на m, або що теж саме, $a = b + mt$, де $t -$довільне ціле число.

Властивості конгруенцій при незмінному модулі:

1. Конгруенції за тим самим модулем можна почлено додавати.

$$a_1 \equiv b_1 \pmod m \wedge \ldots \wedge a_k \equiv b_k \pmod m \Rightarrow$$

$$\Rightarrow a_1 = b_1 + mt_1 \wedge \ldots a_k = b_k + mt_k \Rightarrow$$

$$a_1 + \ldots + a_k = (b_1 + \ldots + b_k) + m(t_1 + \ldots + t_k) \Rightarrow$$

$$\Rightarrow a_1 + \ldots + a_k \equiv b_1 + \ldots + b_k \pmod m.$$

2. Конгруенції за тим самим модулем можна почлено віднімати.

$$a_1 \equiv b_1 \pmod m \wedge a_2 \equiv b_2 \pmod m \Rightarrow a_1 = b_1 + mt_1 \wedge a_2 = b_2 + mt_2 \Rightarrow$$

$$a_1 - a_2 = b_1 - b_2 + m(t_1 - t_2) \Rightarrow a_1 - a_2 \equiv b_1 - b_2 \pmod m.$$

3. До обох частин конгруенції можна додати будь-яке ціле число, тобто з конгруенції $a \equiv b \pmod m$ випливає $a + c \equiv b + c \pmod m$, де c – довільне ціле число.

4. З однієї частини конгруенції можна переносити доданок з протилежним знаком, тобто з $a+b\equiv c\pmod m$ випливає

$$a\equiv c-b\pmod m.$$

5. До будь-якої частини конгруенції можна додати або відняти довільне ціле число, кратне модулю, тобто з конгруенції $a\equiv b\pmod m$ випливає $a+km\equiv b\pmod m$ або $a\equiv b+km\pmod m$.

6. Конгруенції за одним модулем можна почлено перемножити.

$$a_1\equiv b_1\pmod m\wedge\ldots\wedge a_k\equiv b_k\pmod m\Rightarrow a_1=b_1+mt_1\wedge\ldots\wedge a_k=b_k+mt_k\Rightarrow$$

$$a_1a_2\cdots a_k=b_1b_2\cdots b_k+mt\Rightarrow a_1a_2\cdots a_k\equiv b_1b_2\cdots b_k\pmod m.$$

Висновок. Конгруенцію можна піднести до будь-якого натурального степеня n.

$$a^n\equiv b^n\pmod m.$$

7. Обидві частини конгруенції можна помножити на те саме ціле число, тобто при $a\equiv b\pmod m$ і k цілому справедлива конгруенція $ak\equiv bk\pmod m$.

8. Обидві частини конгруенції можна поділити на їх спільний дільник d , якщо він взаємно простий з модулем m.

9. Якщо у виразі

$$f(a_1,a_2,\ldots,a_k)=\sum Aa_1^{n_1}a_2^{n_2}\ldots a_k^{n_k}$$

всі коефіцієнти A і числа $a_1,a_2,\ldots,a_k$ замінити на конгруентні їм за модулем m коефіцієнти B і числа $b_1,b_2,\ldots,b_k$ відповідно, то новий вираз

$$g(b_1,b_2,\ldots,b_k)=\sum Bb_1^{n_1},b_2^{n_2},\ldots,b_k^{n_k}$$

буде конгруентній за модулем m до заданого

$$f(a_1, a_2, \ldots, a_k) \equiv g(b_1, b_2, \ldots, b_k) \pmod{m}.$$

Наслідок 1. Якщо $a_i \equiv b_i \pmod{m}, i = 1, 2, ..., k,$ то

$$f(a_1, a_2, \ldots, a_k) \equiv f(b_1, b_2, \ldots, b_k) \pmod{m}.$$

Наслідок 2. Якщо в многочлені з цілими коефіцієнтами

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \tag{1}$$

заданому на множині цілих чисел **Z,** всі коефіцієнти a_i замінити коефіцієнтами b_i, конгруентними з a_i за модулем m, то дістанемо многочлен

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0,$$

конгруентний з многочленом $f(x)$, тобто

$$\forall_{x \in Z} f(x) \equiv g(x) \pmod{m}.$$

Наслідок 3. Якщо $x \equiv y \pmod{m}$, то для многочлена (1) справедлива конгруенція

$$f(x) \equiv g(x) \pmod{m}.$$

Властивості конгруенцій за різними модулями:

10. Обидві частини конгруенції і модуль можна множити на те саме ціле число.

11. Обидві частини конгруенції і модуль можна скоротити на спільний дільник.

12. Якщо конгруенція $a \equiv b \pmod{m}$ має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.

13. Якщо конгруенція має місце за модулем m, число d – дільник m, то вона має місце і за модулем d .

14. Якщо одна частина конгруенції і модуль ділиться на число d , то й друга частина конгруенція ділиться на це число.

15. Якщо $a \equiv b \pmod{m}$, то НСД чисел a, m і b, m рівні між собою:

$$(a,m)=(b,m).$$

1.2. Класи лишків

Відношення конгруентності ділить кільце K на класи чисел, конгруентних між собою за даним модулем – класи лишків.

Два цілих числа a і b тоді і тільки тоді належить до одного класу за модулем m, коли вони конгруентні за цим модулем.

Означення 2. Лишком класу за модулем m називається будь-яке число цього класу.

$$K_a^{(m)} = K_{a+mt}^{(m)}$$

Теорема 2. Кожний клас лишків $K_a^{(m)}$ за модулем m розпадається на d $(d \geq 1)$ класів лишків за модулем dm а саме:

$$\left\{K_a^{(dm)}, K_{a+m}^{(dm)}, K_{a+2m}^{(dm)}, ..., K_{a+(d-1)m}^{(dm)}\right\}.$$

У фактор-множині **Z**/m класів лишків за даним модулем m вводяться операції додавання і множення, погоджені з операціями додавання й множення в кільці цілих чисел, а саме:

Означення 3. Сумою класів $K_a^{(m)}$ і $K_b^{(m)}$називається такий клас $K_{a+b}^{(m)}$, який містить у собі число $a+b$.

Означення 4. Добутком класів $K_a^{(m)}$ і $K_b^{(m)}$ називається такий клас $K_{ab}^{(m)}$, який містить у собі число ab.

$$K_a^{(m)} + K_b^{(m)} = K_{a+b}^{(m)};\ K_a^{(m)} \cdot K_b^{(m)} = K_{ab}^{(m)}.$$

Теорема 3. Сукупність всіх класів чисел за модулем m. Утворює комутативне кільце відносно операцій додавання та множення класів.

Як відомо, в довільному кільці справедливе твердження: якщо в добутку двох або кількох елементів кільця хоча б один із співмножників є нуль, то й добуток дорівнює нулю. Обернене твердження виконується не завжди. Якщо $ab = 0$, але ні $a \neq 0$, ні $b \neq 0$; у цьому разі a і b називають *дільниками нуля*, а саме кільце – *кільцем з дільниками нуля*.

Теорема 4. Якщо m – складене число, то Z/m є комутативне кільце з дільниками нуля. Якщо ж m – просте число, то Z/m – поле.

Означення 5. Система лишків, утворена з m чисел, узятих по одному з кожного класу, називається повною системою лишків за модулем m.

Будь-які m чисел, які попарно не конгруентні між собою за модулем m, утворюють повну систему лишків за цим модулем.

Найчастіше за повну систему лишків за модулем m беруть найменші невід'ємні лишки $0,1,2,...,m-1$ або абсолютно найменші лишки.

Теорема 5. Якщо $(a,m)=1$, b- довільне ціле число, а x – пробігає ПСЛ за модулем m, то й лінійна форма $ax+b$ також пробігає ПСЛ за модулем m.

Означення 6. Найбільшим спільним дільником класу $K_a^{(m)}$ називається найбільший спільний дільник чисел a і m. Якщо $(a,m)=1$, то $K_a^{(m)}$ називається взаємно простим з модулем m.

Означення 7. Система лишків, узятих по одному з кожного класу, взаємно простого з модулем, називається зведеною системою лишків.

1.3. Функція Ейлера та її властивості

Означення 8. Функцією Ейлера $\varphi(m)$ називається функція, визначена на множині натуральних чисел; значення $\varphi(m)$ є кількість невід‘ємних чисел, менших за m і взаємно простих з m.

Теорема 6. Якщо $(a,m)=1,$ x пробігає ЗСЛ за модулем m, то лінійна форма $y = ax$ також пробігає ЗСЛ за модулем m.

Означення 9. Числова функція $f(n)$, визначена на множині натуральних чисел, називається мультиплікативною, якщо для кожного n $f(n)\neq 0$ і для будь-яких взаємно простих натуральних чисел n і m

$$f(nm)=f(n)\cdot f(m)$$

Мультиплікативні функції мають такі властивості:

1) Якщо $f(n)$ – мультиплікативна функція, то $f(1)=1$.

2) Якщо $f(n)$ – мультиплікативна функція і числа $n_1, n_2, \dots, n_k$ попарно взаємно прості, то

$$f(n_1\cdot n_2\cdot \ldots \cdot n_k)=f(n_1)\cdot f(n_2)\cdot \ldots \cdot f(n_k).$$

3) Добуток мультиплікативних функцій є мультиплікативна функція.

Властивості функції Ейлера $\varphi(m)$

Теорема 7. Функція Ейлера $\varphi(m)$ мультиплікативна.

Теорема 8. Якщо p – просте число, а k – натуральне число, то

$$\varphi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right).$$

Теорема 9. Якщо канонічний розклад числа m має вигляд

$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s},$$

то

$$\varphi(m) = m\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right).$$

Теорема 10. Сума значень функції Ейлера для всіх дільників d_i числа m дорівнює m :

$$\sum_i \varphi(d_i) = m.$$

Теорема 11.(**Ейлера**). Якщо m – натуральне число і $m > 1, \left(a, m\right) = 1,$ то

$$a^{\varphi(m)} \equiv 1\left(\operatorname{mod} m\right).$$

Теорема 12 (Ферма). При простому p і a, якщо $\left(a, p\right) = 1$, то

$$a^{p-1} \equiv 1\left(\operatorname{mod} p\right).$$

Наслідок. Якщо число p просте, то для будь-якого цілого числа a має місце конгруенція

$$a^p \equiv a\left(\operatorname{mod} p\right).$$

1.4. Конгруенції першого степеня та способи їх розв'язання

Означення 10. Конгруенціями з одним невідомим за модулем m називаються конгруенції виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m},$$

де в лівій частині міститься многочлен з цілими коефіцієнтами.

Якщо a_n не ділиться на число m, то n називається степенем конгруенції; при $a_n \vdots m$ старший член $a_n x^n \equiv 0 \pmod{m}$ і його можна відкинути.

Означення 11. Розв’язком конгруенції $f(x) \equiv 0 \pmod{m}$ називається клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію.

Оскільки класів чисел за модулем m є m, то конгруенція може мати лише скінченну кількість розв’язків або може не мати їх зовсім.

Щоб знайти розв’язки, досить підставити в конгруенцію замість невідомого х числа з різних класів за модулем m. Для цього можна перебрати ПСЛ з найменших невід’ємних лишків, а ще краще – повну систему абсолютно найменших лишків.

Означення 12. Конгруенції називаються рівносильними (еквівалентними), якщо множини їх розв‘язків збігаються.

Щоб побудувати рівносильні конгруенції, над заданою конгруенцією проводять операції, які ґрунтуються на властивостях конгруенцій, розглянутих раніше. До операцій, які не порушують множину розв‘язків конгруенцій, належать такі:

а) Додавання до обох частин конгруенції будь-якого многочлені $g(x)$ з цілими коефіцієнтами.

б) Додавання до однієї з частин конгруенції многочлена з коефіцієнтами, кратними нулю.

в) Множення обох частин конгруенції на число, взаємно просте з модулем.

г) Множення обох частин конгруенції і модуля на те саме додатне число.

Конгруенції 1-го степеня мають вигляд $a_1x + a_0 \equiv 0 \pmod m$. Якщо перенесемо вільний член у праву частину конгруенції і змінимо позначення коефіцієнтів, то дістанемо

$$ax \equiv b \pmod m.$$

При розв‘язуванні таких конгруенцій розглядають два випадки: $(a,m)=1$ і $(a,m)=d>1$.

Теорема 13. Якщо $(a,m)=1$, то конгруенція $ax \equiv b \pmod m$ має єдиний розв‘язок.

Теорема 14. Якщо $(a,m)=d>1$ і $b \vdots d$, то конгруенція $ax \equiv b \pmod m$ має d розв‘язків.

Теорема 15. Якщо $(a,m)=d>0$ і число b не ділиться на d, то конгруенція $ax \equiv b \pmod m$ не має розв‘язків.

Розглянемо деякі, найбільш поширені способи розв’язування конгруенцій 1-го степеня:

а) Підстановка в конгруенцію чисел ПСЛ. Цей спосіб використовують при невеликих модулях. При великих модулях підстановку лишків ПСЛ проводять на заключному етапі побудови рівносильних конгруенцій.

б) Зведення конгруенцій 1-го степеня до рівносильної їй конгруенції з коефіцієнтом при x, рівному 1. Цей спосіб полягає в проведенні ряду рівносильних перетворень заданої конгруенції за допомогою операцій, які ґрунтуються на властивостях конгруенцій, розглянутих раніше і не порушують множину розв'язків конгруенції.

в) Спосіб Ейлера. Нехай треба розв'язати конгруенцію $ax \equiv b(\bmod m)$, якщо $(a,m)=1$. Помножаючи цю конгруенцію на $a^{\varphi(m)-1}$, дістанемо еквівалентну конгруенцію:

$$a^{\varphi(m)} \cdot x \equiv b \cdot a^{\varphi(m)-1} (\bmod m)$$

$$x \equiv b \cdot a^{\varphi(m)-1} (\bmod m).$$

г) Розв'язування конгруенцій 1-го степеня за допомогою неперервних дробів.

Нехай дано конгруенцію

$$ax \equiv b(\bmod m),$$

де $(a,m)=1$. Розкладемо $\frac{m}{a}$ в ланцюговий дріб. Якщо $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_n}{Q_n}=\frac{m}{a}$ є останні підхідні дроби, то маємо рівність:

$$P_n \cdot Q_{n-1} - P_{n-1} \cdot Q_n = (-1)^{n-1},$$

$$mQ_{n-1} - P_{n-1}a = (-1)^{n-1}.$$

Враховуючи, що перший член кратний модулю m, дістанемо далі

$$-P_{n-1}a \equiv (-1)^{n-1} (\bmod m),$$

$$a(-1)^n P_{n-1} \equiv 1(\bmod m)$$

$$a(-1)^n P_{n-1}b \equiv b(\bmod m).$$

$$x \equiv (-1)^n P_{n-1} b \pmod m,$$

Зауваження: Перш ніж застосувати цей спосіб, слід спочатку (якщо це необхідно), використовуючи властивості конгруенцій, зробити коефіцієнт при невідомому невід'ємним і меншим за модуль.

1.5. Системи конгруенцій першого степеня

Розглянемо систему конгруенцій першого степеня, але з різними модулями:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}; \quad (a_1, m_1) = 1, \\ a_2 x \equiv b_2 \pmod{m_2}; \quad (a_2, m_2) = 1, \\ \dots\dots\dots\dots\dots\dots\dots \\ a_k x \equiv b_k \pmod{m_k}; \quad (a_k, m_k) = 1 \end{cases}. \tag{2}$$

Розв'язати систему конгруенцій з одним невідомим – означає знайти такі цілі значення невідомого x, які задовольняли б усі конгруенції цієї системи

Дві системи конгруенцій з невідомим x називають рівнозначними (або еквівалентними), якщо їх задовольняють ті самі значення невідомого x. Якщо $x \equiv \alpha$ за деяким модулем задовольняють систему (2), то весь цей клас чисел вважатимемо за один розв'язок цієї системи. Якщо ця система має хоча б один розв'язок, то вона називається сумісною.

Зауважимо, що, розв'язуючи окремо кожну з конгруенцій (2), матимемо систему, еквівалентну заданій:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots\dots\dots\dots\dots \\ x \equiv c_k \pmod{m_k}. \end{cases} \tag{3}$$

Отже, досить уміти розв'язувати систему конгруенцій (3).

Неважко показати, що коли система (3) сумісна, то вона має єдиний розв'язок за модулем M, що дорівнює найменшому спільному кратному чисел $m_1, m_2, \ldots, m_k$.

Теорема 16. Якщо модулі $m_1, m_2, \ldots, m_k$ попарно взаємно прості, то система конгруенцій (2) має єдиний розв'язок:

$$x \equiv x_0 \left(\operatorname{mod} m_1 m_2 \ldots m_k\right),$$

де

$$x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \ldots + M_k y_k c_k,$$

Причому числа M_i і y_i визначаються з умов:

$$M_i = \frac{m_1 m_2 \ldots m_k}{m_i} = \frac{M}{m_i},\ M_i y_i \equiv 1\left(\operatorname{mod} m_i\right) \left(i = 1, 2, \ldots, k\right)$$

У загальному випадку, коли модулі $m_1, m_2, \ldots, m_k$ можуть і не бути попарно взаємно простими, систему (3) можна розв'язати так.

З першої конгруенції системи (3) випливає, що всі значення x які його задовольняють, матимуть форму $x = c_1 + m_1 t_1$, де t_1 пробігає всі цілі числа. Щоб вибрати з них значення x , які б задовольняли й другу конгруенцію, визначимо t_1 з умови, що

$$c_1 + m_1 t_1 \equiv c_2 \left(\operatorname{mod} m_2\right),$$

або

$$m_1 t_1 \equiv c_2 - c_1 \left(\operatorname{mod} m_2\right).$$

Ця конгруенція першого степеня щодо t_1 матиме розв'язки, якщо $c_2 - c_1$ ділиться на $\left(m_1, m_2\right)$; інакше ця остання конгруенція не має розв'язків, а значить система (3) несумісна. Нехай $c_2 - c_1$ ділиться на (m_1, m_2). Розв'язуючи цю конгруенцію, дістанемо:

$$t_1 \equiv t_1' \left(\bmod \frac{m_2}{(m_1, m_2)} \right).$$

Тоді сукупність усіх значень t_1, що задовольняють другу конгруенцію, буде:

$$t_1 = t_1' + \frac{m_2}{(m_1, m_2)} t_2,$$

де t_2 пробігає всі цілі числа. Звідси дістанемо:

$$x = c_1 + m_1 t_1' + \frac{m_1 m_2}{(m_1, m_2)} t_2 = y_2 + [m_1, m_2] t_2, \tag{4}$$

де $y_2 = c_1 + m_1 t_1$ задовольнятимуть перші дві конгруенції. Тепер з чисел (4), аналогічно, виберемо ті, які задовольнятимуть третю конгруенцію. Так знову, або прийдемо до конгруенції відносно t_2, яка не має розв'язків, а значить система (3) несумісна, або знайдемо, що значення

$$x = y_3 + [m_1, m_2, m_3] t_3,$$

де t_3 ціле, або

$$x \equiv y_3 \left(\bmod [m_1, m_2, m_3] \right).$$

Задовольнятимуть перші три конгруенції і т.д. Якщо така система (3) сумісна, то, зрештою прийдемо до єдиного розв'язку цієї системи за модулем

$$[m_1, m_2, \ldots, m_k].$$

Зауваження. Якщо в системі (1) $(a_i, m_i) = d_i > 1$ для деяких $i = 1, 2, \ldots, k$ і b_i ділиться на d_i, тоді i-та конгруенція системи (2) матиме d_i розв'язків, і ми дістанемо кілька систем конгруенцій виду (3); тому система (2) матиме декілька розв'язків. Для складання систем виду (3) треба кожен розв'язок однієї конгруенції системи (2) скомбінувати з кожним розв'язком решти конгруенцій цієї системи.

1.6. Невизначене рівняння першого степеня

Означення 13. Діофантовим рівнянням 1-го степеня з n невідомими називається рівняння виду

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{5}$$

де всі коефіцієнти і невідомі – цілі числа і хоча б одне $a_i \neq 0$.

Означення 14. Розв'язком діофантового рівняння (5) називається сукупність цілих чисел $\left(x_1', x_2', \ldots, x_n'\right)$, яка задовольняє цьому рівнянню.

Теорема 17. Якщо коефіцієнти $a_1, a_2, \ldots, a_n$ діофантового рівняння

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$$

взаємно прості числа, то воно має розв'язки на множині цілих чисел.

Теорема 18. Нехай d – найбільший спільний дільник коефіцієнтів $a_1, a_2, \ldots, a_n$. Діофантове рівняння (5) має розв'язок тоді і тільки тоді, коли $d \mid b$. Число розв'язків такого рівняння або дорівнює нулю, або нескінченності.

Теорема 19. Якщо x_0 є розв'язком конгруенції $ax \equiv c \left(\mathrm{mod}\, b\right)$, то сукупність $\left(x_0, \dfrac{c - ax_0}{b}\right)$ буде розв'язком діофантового рівняння

$$ax + by = c.$$

Теорема 20. Нехай d – найбільший спільний дільник a і b, де $a \neq 0$, $b \neq 0, d \mid c$ і (x_0, y_0) – один із розв'язків діофантового рівняння:

$$ax + by = c \tag{6}$$

Тоді множина розв'язків рівняння (6) в цілих числах співпадає з множиною сукупностей (x', y'), де

$$x' = x_0 - \frac{b}{d}t,\ y' = y_0 + \frac{a}{d}t,$$

а t – довільне ціле число.

1.7. Конгруенції n – го степеня за простим модулем

Припустимо, що задано конгруенцію:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p \qquad (7),$$

де $a_n \not\equiv 0 \pmod p$ і p – просте число.

Теорема 21. Конгруенцію (7) завжди можна замінити еквівалентною конгруенцією того самого степеня з старшим коефіцієнтом, що дорівнює одиниці.

$$x^n + b_1 x^{n-1} + \ldots + b_{n-1}x + b_n \equiv 0 \pmod p, \text{ де } b_i \equiv a_i \alpha \pmod p.$$

Теорема 22. Якщо степінь конгруенції (7) не менший від модуля конгруенції, то вона еквівалентна деякій конгруенції степеня не вище $p-1$ (за тим самим модулем).

$$f(x) = (x^p - x)\cdot q(x) + r(x),$$

$$f(x) \equiv 0 \pmod p \text{ і } r(x) \equiv 0 \pmod p$$

Розглянемо методику розв'язування конгруенцій n – го степеня виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \qquad (8)$$

де p – просте число. За допомогою операцій, які приводять до рівносильних конгруенцій, можна побудувати рівносильну до (8) конгруенцію степеня, не вище $p-1$, з коефіцієнтами, які є найменшими невід'ємними або абсолютно найменшими лишками ПСЛ за модулем p.

Побудову такої конгруенції можна провести в такому порядку.

а) Замінити всі коефіцієнти a_i многочлена $f(x)$ відповідними їм найменшими невід'ємними або абсолютно найменшими лишками з ПСЛ за модулем p.

б) Зробити коефіцієнт при старшому члені конгруенції рівним одиниці.

в) Понизити степінь конгруенції.

Якщо степінь $n \geq p$, то конгруенцію (8) можна замінити рівносильною їй конгруенцією степеня, не вищого $p-1$. За наслідком теореми Ферма для будь-якого цілого числа x і простого p

$$x^p \equiv x \pmod{p},$$

або

$$x^p - x \equiv 0 \pmod{p}. \qquad (9)$$

З другого боку, ділячи многочлен $f(x)$ на $x^p - x$, дістанемо

$$f(x) = (x^p - x)g(x) + r(x).$$

Враховуючи це, на основі конгруенції (9) матимемо

$$f(x) = (x^p - x)g(x) + r(x) \equiv r(x) \pmod{p},$$

тобто

$$f(x) \equiv r(x) (\bmod p).$$

На основі теореми Ейлера

$$x^{p-1} \equiv 1 (\bmod p).$$

Тому

$$x^n = x^{(p-1)k+m} = x^{(p-1)k} \cdot x^m \equiv 1 \cdot x^m (\bmod p),$$

тобто $x^n \equiv x^m (\bmod p)$.

Число розв'язків конгруенції n-го степеня

Теорема 23. Конгруенція n – го степеня за простим модулем може мати не більш як n розв'язків.

Означення 15. Якщо всі коефіцієнти многочлена $f(x)$ є кратними модуля m, то конгруенція

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (\bmod m)$$

називається тотожною конгруенцією.

Теорема 24. Якщо конгруенція n-го степеня $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (\bmod p)$ має $n+1$ розв'язків, то всі її коефіцієнти кратні модулю, тобто ця конгруенція тотожна.

Теорема 25. Якщо α_1 – який-небудь розв'язок конгруенції (7), то має місце тотожна конгруенція:

$$f(x) \equiv (x - \alpha_1) f_1(x) (\bmod p),$$

де $f_1(x)$ – многочлен степеня, на одиницю нижчого від степеня многочлена $f(x)$. Старший коефіцієнт многочлена $f_1(x)$ збігається із старшим коефіцієнтом даного многочлена $f(x)$.

Висновок. Конгруенція (7) має корінь $x=\alpha_1$ тоді і тільки тоді, коли ліва її частина $f(x)$ ділиться на $x-\alpha_1$ за даним модулем p.

Теорема 26. Якщо $\alpha_1, \alpha_2, ..., \alpha_k$ $(k \le n)$ є різні розв'язки конгруенції (7), то має місце тотожна конгруенція:

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k) f_k(x) (\operatorname{mod} p),$$

де степінь $f_k(x)$ дорівнює $n-k$ і старші коефіцієнти $f(x)$ і $f_k(x)$ однакові.

Висновок. Якщо конгруенція (8) n-го степеня за простим модулем p (n можна вважати не більшим за $p-1$) має n різних розв'язків $\alpha_1, \alpha_2, ..., \alpha_n$, то справедлива тотожна конгруенція:

$$f(x) \equiv a_n (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)(\operatorname{mod} p).$$

Теорема 27 (Вільсона). Якщо p – просте число, то

$$(p-1)!+1 \equiv 0 (\operatorname{mod} p).$$

1.8. Зведення конгруенції за складеним модулем до системи конгруенцій за простими модулями

Теорема 28. Якщо $m_1, m_2, ..., m_k$ – попарно взаємно прості числа, то конгруенція

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \equiv 0 (\operatorname{mod} m_1 m_2 ... m_k) \quad (9)$$

еквівалентна системі конгруенцій:

$$\begin{cases} f(x) \equiv 0 (\operatorname{mod} m_1), \\ f(x) \equiv 0 (\operatorname{mod} m_2), \\ \qquad .... \\ f(x) \equiv 0 (\operatorname{mod} m_k). \end{cases} \quad (10)$$

При цьому, позначаючи через

$$S_1, S_2, ..., S_k.$$

Числа розв'язків окремих конгруенцій (10) за відповідними модулями і через S – число розв’язків конгруенції (9), матимемо:

$$S = S_1 S_2 \cdots S_k.$$

Висновок 1. Якщо хоч одна з конгруенцій системи (10) не має розв'язків, то й задана конгруенція (9) також не матиме розв'язків.

Висновок 2. Дослідження і розв'язування конгруенції

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

де $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ – канонічний розклад модуля m, зводиться до дослідження і розв'язування конгруенцій: $f(x) \equiv 0 \left(\operatorname{mod} p_i^{\alpha_i}\right)$ $(i = 1, 2, ..., k)$. Це випливає з того, що числа $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_k^{\alpha_k}$ попарно взаємно прості.

Отже, все зводиться до того, що доводиться окремо досліджувати і розв'язувати конгруенції виду

$$f(x) \equiv 0 \left(\operatorname{mod} p^{\alpha}\right), \tag{11}$$

де p – просте число, α – ціле додатне число. Зауважимо, що всякий розв'язок конгруенції буде розв'язком конгруенції

$$f(x) \equiv 0 \pmod{p}. \tag{12}$$

Очевидно, якщо конгруенція (12) не має розв'язків, то й конгруенція (11) розв'язків не матиме. Справді, якщо $f(x)$ не ділиться на p, то $f(x)$ і поготів не ділитиметься на p^{α}, тобто

$$f(x) \not\equiv 0 \left(\operatorname{mod} p^{\alpha}\right)$$

ні при якому цілому x.

Теорема 29. Всякий розв'язок

$$x \equiv x_1 \pmod p$$

конгруенції (12) при умові, що $f'(x_1)$ не ділиться на p, дає один єдиний розв'язок конгруенції (11)

$$f(x) \equiv 0 \pmod{p^2}. \tag{13}$$

Зауваження. Якщо $f'(x_1)$ ділиться на p і $f(x_1)$ не ділиться на p^2, то це означає, що яке б не було t_1

$$f(x_1 + pt_1) \not\equiv 0 \pmod{p^2}$$

і конгруенція (13), а, значить, конгруенція (11) не має розв'язків для розглядуваного $x \equiv x_1 \pmod p$. Якщо ж $f(x_1)$ ділиться на p^2, тобто $f(x_1) \equiv 0 \pmod{p^2}$, то x_1 буде вже розв'язком конгруенції $f(x) \equiv 0 \pmod{p^2}$.

Означення 16. Якщо конгруенція $x^n \equiv a \pmod p$ має розв'язок, то a називається лишком степеня n за простим модулем p, якщо ні, – то нелишком степеня n за модулем p.

$$x^2 \equiv a \pmod p,\ (a, p) = 1,\ p > 2.$$

Теорема 30. Якщо a – квадратичний лишок за модулем p, $(a, p) = 1,\ p > 2$, то квадратна конгруенція

$$x^2 \equiv a \pmod p$$

має два розв'язки.

Теорема 31. Для будь-якого простого числа $p > 2$ половина лишків ЗСЛ є квадратичними лишками, а половина – квадратичними нелишками.

Терема 32. (Критерій Ейлера). При простому $p > 2$ число a є квадратичним лишком за модулем p тоді і тільки тоді, коли

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

і квадратичним нелишком тоді і тільки тоді, коли

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Означення 17. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається для всіх цілих чисел a, які не діляться на просте число $p > 2$ рівністю

$$\left(\frac{a}{p}\right) = \begin{cases} +1, \textit{ якщо } a \textit{ є квадратичним лишком за модулем } p, \\ -1, \textit{ якщо } a \textit{ є квадратичним нелишком за модулем } p. \end{cases}$$

Використовуючи критерій Ейлера, очевидно, маємо

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Властивості символу Лежандра

1. Якщо $a \equiv a_1 \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

2. $\left(\frac{a^2}{p}\right) = 1$.

3. $\left(\frac{1}{p}\right) = 1$

4. $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$

5. $\left(\dfrac{a_1 \cdot a_2 \cdot \ldots \cdot a_k}{p}\right) = \left(\dfrac{a_1}{p}\right) \cdot \left(\dfrac{a_2}{p}\right) \cdot \ldots \cdot \left(\dfrac{a_k}{p}\right)$.

Наслідок 1. $\left(\dfrac{a \cdot b^2}{p}\right) = \left(\dfrac{a}{p}\right)$.

Наслідок 2. $\left(\dfrac{a^n}{p}\right) = \left(\dfrac{a}{p}\right)^n$.

Наслідок 3. Якщо число a не ділиться на просте число $p > 2$ і в канонічному розкладі на добуток простих множників має вигляд

$$a = q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots \cdot q_k^{l_k},$$

то

$$\left(\frac{q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots \cdot q_k^{l_k}}{p}\right) = \left(\frac{q_1}{p}\right)^{l_1} \cdot \left(\frac{q_2}{p}\right)^{l_2} \cdot \ldots \cdot \left(\frac{q_k}{p}\right)^{l_k}$$

6. $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

7. Закон взаємності квадратичних лишків:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right).$$

1.9. Розв'язування квадратичних конгруенцій

Найпростішим випадком конгруенції вищого степеня з одним невідомим є конгруенція другого степеня:

$$a_1 y^2 + a_2 y + a_3 \equiv 0 \pmod{m},\ a \not\equiv 0 \pmod{m}.$$

Її завжди можна звести до двочленної конгруенції виду

$$x^2 \equiv a \pmod{n},$$

де $a = a_2^2 - 4a_1a_3$, $x = 2a_1y + a_2$, $n = 4am$.

Для цього слід обидві частини і модуль конгруенції помножити на $4a$ і зробити відповідні перетворення.

Критерій Ейлера і символ Лежандра дають можливість встановити, чи є число a квадратичним лишком за модулем p, чи має розв'язки квадратна конгруенція

$$x^2 \equiv a \pmod{p} \tag{14}$$

При малих p цю конгруенцію розв'язують методом проб, при великих p необхідно встановити, чи має ця конгруенція розв'язок, тобто чи є a квадратичним лишком. Тоді за критерієм Ейлера маємо

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Якщо число p має вигляд $p = 4k + 3$, то

$$a^{\frac{p-1}{2}} = a^{2k+1} \equiv 1 \pmod{p}.$$

Помноживши на a обидві частини конгруенції, матимемо

$$a^{2k+2} \equiv a \pmod{p},$$

або

$$\left(a^{k+1}\right)^2 \equiv a \pmod{p}.$$

Очевидно, $x \equiv \pm a^{k+1} \pmod{p}$ дає нам класи чисел $K_{a^{k+1}}^{(p)}$ і $K_{-a^{k+1}}^{(p)}$, які є розв'язками конгруенції (14).

Конгруенції 2-го степеня за складеним модулем

Конгруенція другого степеня за складеним модулем:

$$x^2 \equiv a \pmod{m}, \text{ де } m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \ (a, m) = 1$$

еквівалентна системі конгруенцій

$$\begin{cases} x^2 \equiv a\left(\operatorname{mod} 2^{\alpha}\right), \\ x^2 \equiv a\left(\operatorname{mod} p_1^{\alpha_1}\right), \\ \dots\dots\dots\dots\dots\dots, \\ x^2 \equiv a\left(\operatorname{mod} p_k^{\alpha_k}\right). \end{cases}$$

Розглянемо конгруенції виду

$$x^2 \equiv a\left(\operatorname{mod} p^{\alpha}\right);\ \left(a, p\right) = 1, \tag{15}$$

де $\alpha > 1$ – ціле число, а p – просте непарне число.

Теорема 33. Конгруенція (15) має два розв‘язки або не має жодного залежно від того, чи буде число a квадратичним лишком або нелишком за модулем p, тобто чи буде відповідно $\left(\dfrac{a}{p}\right) = +1$ або $\left(\dfrac{a}{p}\right) = -1$.

Зауваження. Неважко побачити, що коли $x \equiv x_0\left(\operatorname{mod} p^{\alpha}\right)$ є один розв‘язок конгруенції (15), то другим її розв‘язком буде $-x_0$.

Розглянемо конгруенцію

$$x^2 \equiv a\left(\operatorname{mod} 2^{\alpha}\right);\ \alpha > 0,\ \left(a, 2\right) = 1. \tag{16}$$

Теорема 34. 1) Конгруенція (16) завжди має один розв‘язок при $\alpha = 1;$ 2) два розв‘язки – при $\alpha = 2,$ і $a \equiv 1\left(\operatorname{mod} 4\right)$ і жодного при $\alpha = 2$ і $a \equiv 3\left(\operatorname{mod} 4\right);$ 3) при $\alpha \geq 3$ конгруенція (16) має розв‘язки тільки при $a \equiv 1\left(\operatorname{mod} 8\right)$ і при цьому чотири різних розв‘язки; два з них неодмінно задовольняють і конгруенцію

$$x^2 \equiv a\left(\operatorname{mod} 2^{\alpha+1}\right).$$

Теорема 35. Конгруенція

$$x^2 \equiv a \pmod{m};\ m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k};\ (a, m) = 1 \qquad (17)$$

має розв‘язок тоді і тільки тоді, коли

$$\left(\frac{a}{p_1}\right) = +1,\ \left(\frac{a}{p_2}\right) = +1,\ \dots,\ \left(\frac{a}{p_k}\right) = +1;$$

$$a \equiv 1 \pmod{4} \text{ при } \alpha = 2,$$

$$a \equiv 1 \pmod{8} \text{ при } \alpha \geq 3.$$

Якщо жодну з цих умов не порушено, то кількість розв‘язків буде

$$2^k \text{ при } \alpha = 0;\ 1,$$

$$2^{k+1} \text{ при } \alpha = 2,$$

$$2^{k+2} \text{ при } \alpha \geq 3.$$

Зауваження. Якщо m – непарне і конгруенція (17) має розв‘язки, то символ Якобі

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k} = +1,$$

бо всі $\left(\frac{a}{p_i}\right) = +1$. Ця умова необхідна для розв‘язності конгруенції (17), але не достатня, бо з $\left(\frac{a}{m}\right) = +1$ не виходить, що всі $\left(\frac{a}{p_i}\right) = +1$. У зв‘язку з цим можемо зауважити, що застосування символу Якобі та його властивостей лише прискорює обчислення символу Лежандра.

Розглянемо множину цілих додатних степенів числа a:

$$a, a^2, a^3, a^4, \dots \qquad (18)$$

з точки зору їх конгруентності за деяким модулем $m>1$, вважаючи, що $(a,m)=1$. За теоремою Ейлера маємо:

$$a^{\varphi(m)}\equiv 1(\bmod m),$$

і, отже,

$$a^{\varphi(m)\cdot k}\equiv 1(\bmod m),\ \underset{k\in Z}{\forall} k>0.$$

Таким чином, серед степенів (18) числа a знайдеться нескінченна кількість чисел, конгруентних з 1 за модулем m.

Означення 18. Найменше натуральне число δ, для якого справедлива конгруенція $a^{\delta}\equiv 1(\bmod m)$, називається показником, до якого належить число a, за модулем m. $\left[\delta=P_m(a),\ \delta\le\varphi(m)\right]$. Якщо $\delta=\varphi(m)$, число a називається первісним коренем за модулем m.

Теорема 36. Якщо $a_1\equiv a_2(\bmod m)$, то числа a_1 і a_2 належать до того самого показника за цим модулем.

Наслідок. Усі числа одного класу $K_a^{(m)}$ належать тому самому показнику δ за модулем m.

1.10. Властивості показників за модулем

1. Якщо $(a,m)=1$ і δ – показник, до якого належить число a за модулем m, то серед степенів

$$1=a^0,\ a,\ a^2,a^3,\dots,a^{\delta-1}$$

немає чисел, конгруентних між собою за модулем m.

Наслідок. Якщо a – первісний корінь за модулем m, тобто $\delta=\varphi(m)$, то множина степенів

$$1 = a^0,\ a,\ a^2, a^3, \dots, a^{\varphi(m)-1}$$

є ЗСЛ за модулем m.

2. Якщо $\delta = P_m(a)$, то

$$\left[a^{k_1} \equiv a^{k_2} \pmod{m}\right] \Leftrightarrow \left[k_1 \equiv k_2 \pmod{\delta}\right].$$

Наслідок 1. Якщо число a належить до показника δ за модулем m і $a^k \equiv 1 \pmod{m}$, то $k \,\vdots\, \delta$.

Наслідок 2. Показник δ, до якого належить число a за модулем m , є дільником числа $\varphi(m)$.

Теорема 37. Якщо число a_1 належить до показника δ_1 за модулем m, а число a_2 – до показника δ_2 за модулем m і $(\delta_1, \delta_2) = 1$, то добуток чисел $a_1 \cdot a_2$ належить до добутку показників $\delta_1 \cdot \delta_2$ за модулем m.

Наслідок. Якщо числа $a_1, a_2, \ldots, a_n$ належать за модулем m відповідно до показників $\delta_1, \delta_2, \ldots, \delta_n$, які попарно взаємно прості між собою, то

$$P_m(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = P_m(a_1) \cdot P_m(a_2) \cdot \ldots \cdot P_m(a_n) = \delta_1 \delta_2 \ldots \delta_n$$

тобто показник, до якого належить добуток чисел $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ за модулем m, дорівнює добутку показників, до яких належать числа $a_1, a_2, \ldots, a_n$ за модулем m.

1.11. Існування первісних коренів

Теорема 38. За будь-яким простим модулем p існує хоча б один первісний корінь.

Теорема 39. Якщо існує хоч одне число, яке належить до показника δ за модулем p, то всього класів таких чисел є $\varphi(\delta)$.

Наслідок 1. Первісних коренів за модулем p існує $p-1$.

Наслідок 2. Якщо a – первісний корінь за модулем p, то інші первісні корені слід шукати серед степенів $a^2, a^3, ..., a^{p-1}$ – вони мають вигляд a^k, де $(k, p-1)=1$ і $k \le p-1$.

Теорема 40. Якщо $p-1 = q_1^{k_1} \cdot q_2^{k_2} \cdot \ldots \cdot q_s^{k_s}$ – канонічний розклад числа $p-1$, то для того щоб число a було первісним коренем за модулем p, достатньо, щоб виконувались умови:

$$a^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$$

для всіх $i = 1, 2, ..., s$.

ЗСЛ за модулем p можна подати сукупністю чисел – найменших невід‘ємних лишків

$$1, 2, 3, 4, ..., p-1. \tag{19}$$

ЗСЛ можна подати й інакше – за допомгою степенів якогось первісного кореня за модулем p. Якщо q є первісний корінь за модулем p [$(p, q)=1$], то степені

$$q, q^2, q^3, ..., q^{n-1} \tag{20}$$

є також сукупністю $p-1$ чисел, неконгруентних між собою за модулем p (властивість 1 показників за модулем). Тому ці числа є також представниками різних класів лишків за модулем p і утворюють ЗСЛ за модулем p. Кожне число з (19) конгруентне деякому числу з (20). Звідси кожний клас лишків ЗСЛ за модулем p можна подати якимсь числом виду q^{γ}. Тим самим кожному класу лишків $K_a^{(p)}$ ЗСЛ можна поставити у відповідність показник степеня γ числа q^{γ}, який і називається індексом класу $K_a^{(p)}$ при основі q.

Означення 19. Індексом числа a за модулем p (або класу $K_a^{(p)}$) при основі q називається таке ціле невід‘мне число γ, що

$$q^{\gamma} \equiv a \pmod{p}.$$

Позначають індекс $\gamma = \operatorname{ind}_q a$ за модулем p.

Основні властивості індексів

1. Числа $\gamma' \geq 0$ є індексами числа a за модулем p при основі q тоді і тільки тоді, коли

$$\gamma' \equiv \gamma \pmod{p-1},\text{ де } \gamma = \operatorname{ind}_q a \text{ за модулем } p.$$

2. Для того щоб

$$a \equiv b \pmod{p},$$

необхідно і достатньо, щоб виконувалася конгруенція

$$\operatorname{ind}_q a \equiv \operatorname{ind}_q b \pmod{p-1}.$$

3. $\operatorname{ind}_q 1 \equiv 0 \pmod{p-1}$.

4. $\operatorname{ind}_q q \equiv 1 \pmod{p-1}$.

5. Індекс добутку чисел за модулем p при основі q конгруентний за модулем $p-1$ сумі індексів окремих множників при основі q, тобто

$$\operatorname{ind}_q (a_1 a_2 \ldots a_n) \equiv \operatorname{ind}_q a_1 + \operatorname{ind}_q a_2 + \ldots + \operatorname{ind}_q a_n \pmod{p-1}.$$

6. $\operatorname{ind}_q a^n \equiv n \operatorname{ind}_q a \pmod{p-1}$.

7. Якщо $a \overline{\vdots}\, b$, то $\operatorname{ind}_q \dfrac{a}{b} \equiv \operatorname{ind}_q a - \operatorname{ind}_q b \pmod{p-1}$.

Зауважимо, що перехід від конгруенції між числами до конгруенції їх індексів називається *індексацією*, а зворотний перехід – *потенціюванням*.

1.12. Розв‘язування двочленних конгруенцій n-го степеня за допомогою індексів

В загальному вигляді двочленні конгруенції можна записати так:

$$ax^n \equiv b \pmod p, \text{ де } (a,p)=1 \tag{21}$$

і n – натуральне число.

Якщо провести індексацію цієї конгруенції при однаковій основі, то дістанемо конгруенцію $\operatorname{ind}\left(ax^n\right) \equiv \operatorname{ind} b \pmod{p-1}$, або, що те ж саме,

$$\operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1}. \tag{22}$$

Конгруенції (21) і (22) еквівалентні. Якщо позначити

$$\operatorname{ind} b - \operatorname{ind} a = c,\ \operatorname{ind} x = y.$$

то конгруенція (21) має вигляд

$$ny \equiv c \pmod{p-1}.$$

Тим самим від конгруенції n-го степеня (21) за допомогою індексації ми прийшли до конгруенції (22) першого степеня. Розв‘язавши її і взявши величину $y = \operatorname{ind} x$, знайдемо x за відповідними таблицями (Додаток 2).

1.13. Арифметичні застосування теорії конгруенцій

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

1) виведення ознак подільності;

2) обчислення остач при діленні;

3) перевірка результатів арифметичних дій;

4) визначення довжини періоду при перетворенні звичайного дробу в десятковий.

Обчислення остач при діленні на дане число

Нехай треба знайти невід‘ємну остачу x від ділення деякого числа N на натуральне число m; через те що дане число N і шукана остача x належить одному і тому самому класу чисел за модулем m, то ця задача зводиться до знаходження найменшого невід‘ємного лишку x того самого класу чисел, до якого належить N за модулем m, тому

$$N \equiv x \pmod{m},$$

де

$$0 \le x \le m .$$

Найчастіше N є степенем якого-небудь цілого числа або степенем многочлена від цілих чисел. Останній випадок зводиться до першого, а саме коли $N = a^k$. У цьому разі завжди можна вважати, що $0 \le a < m$; далі, якщо $(a, m) = 1$, то за теоремою Ейлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, і тому в конгруенції $a^k \equiv x \pmod{m}$, k можна замінити числом r, яке є остачею від ділення k на $\varphi(m)$.

Зауваження. Якщо для модуля m є таблиця індексів, то для обчислення остач від ділення на m добутків кількох співмножників і, зокрема, натуральних степенів, можна застосувати індекси. А саме, щоб знайти остачу x від ділення добутку $a_1 a_2 ... a_n$ на m, де всі a_i взаємно прості з m, запишемо

$$x \equiv a_1 a_2 ... a_n \left(\operatorname{mod} m \right), \text{ де } 0 \le x < m.$$

Звідси $$\operatorname{ind} x \equiv \operatorname{ind} a_1 + \operatorname{ind} a_2 + ... + \operatorname{ind} a_n \left(\operatorname{mod} \varphi(m) \right).$$

За таблицею індексів знайдемо $s = \operatorname{ind} a_1 + \operatorname{ind} a_2 + ... + \operatorname{ind} a_n$,

звідки $$\operatorname{ind} x \equiv s \left(\operatorname{mod} \varphi(m) \right).$$

Далі знаходимо число, індекс якого дорівнює s, тобто таке r, що

$$\operatorname{ind} x \equiv \operatorname{ind} r \left(\operatorname{mod} \varphi(m) \right), \text{ звідки } x \equiv r \left(\operatorname{mod} m \right).$$

Зокрема, якщо $a_1 = a_2 = ... = a_n = a$, ми дістанемо прийом для обчислення остачі від ділення на модуль m числа a^k.

Якщо $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, то , щоб знайти остачу від ділення на m добутку або степеня, можна знайти остачі $r_1, r_2, ..., r_k$ при діленні на модулі $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_k^{\alpha_k}$, а потім розв‘язати систему конгруенцій

$$\begin{cases} x \equiv r_1 \left(\operatorname{mod} p_1^{\alpha_1} \right), \\ x \equiv r_2 \left(\operatorname{mod} p_2^{\alpha_2} \right), \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv r_k \left(\operatorname{mod} p_k^{\alpha_k} \right). \end{cases}$$

Встановлення ознак подільності за допомогою конгруенцій

Ознакою подільності натурального числа N на натуральне число m називається необхідна і достатня умова подільності N на m, застосування якої потребує меншого числа дій, ніж процес ділення.

Одним із способів знаходження ознак подільності, основаних на конгруентності чисел, є спосіб Паскаля. Нехай деяке натуральне число N при основі числення g має вигляд

$$N = p_n g^n + p_{n-1} g^{n-1} + \ldots + p_1 g + p_0,$$

де коефіцієнти p_k є натуральні числа, які задовольняють нерівності $0 \le p_k < g$. Позначимо через r_k остачу від ділення числа g^k на m, тобто $g^k \equiv r_k \pmod{m}$, і побудуємо число $b = f(N)$ за таким правилом:

$$b = f(N) = p_n r_n + p_{n-1} r_{n-1} + \ldots + p_1 r_1 + p_0.$$

Отже, $N \equiv b \pmod{m}$.Оскільки $b < N$, то дістанемо ознаку Паскаля подільності чисел:

Якщо число $b = p_n r_n + p_{n-1} r_{n-1} + \ldots + p_1 r_1 + p_0$ ділиться на число m, то ділиться на нього і число $N = p_n g^n + p_{n-1} g^{n-1} + \ldots + p_1 g + p_0$.

Якщо ж b на число m не ділиться, то не ділиться на m і число N .

Ознаку подільності Паскаля можна сформулювати так:

Для того щоб число N, записане в довільній g-ічній системі числення у вигляді $N = p_n g^n + p_{n-1} g^{n-1} + \ldots + p_1 g + p_0$ ділилося на m, необхідно і достатньо, щоб число $b = p_n r_n + p_{n-1} r_{n-1} + \ldots + p_1 r_1 + p_0$ ділилося на m (тут p_i – цифри числа N, а r_i – абсолютно найменші лишки відповідних степенів g_i за модулем m, $i = 1, 2, 3, \ldots, n$).

Наслідок 1. Нехай m – дільник числа $g - 1$. Для того, щоб число, записане в g-ічній системі числення, ділилося на m, необхідно і достатньо, щоб сума його цифр ділилася на m .

Наслідок 2. Нехай m – дільник числа $g+1$. Для того, щоб число, записане в g-ічній системі числення, ділилося на m, необхідно і достатньо, щоб різниця між сумами цифр на парних і непарних місцях ділилася на m.

Наслідок 3. Нехай m – дільник числа g^k. Для того, щоб число, записане в g-ічній системі числення, ділилося на m, необхідно і достатньо, щоб число, записане останніми k цифрами даного числа, ділилося на m.

За допомогою цієї ознаки можна встановити зручні конкретні ознаки подільності чисел, записаних у звичайній для нас десятковій системі числення.

Перетворення звичайного дробу в систематичний
і визначення довжини періоду систематичного дробу

Розглядаючи питання про перетворення звичайного дробу в десятковий, з арифметики нам відомо, що звичайні дроби перетворюються або в скінченні, або в нескінченні періодичні десяткові дроби. При цьому звичайний дріб $\frac{a}{b}$ перетворюється в скінченний десятковий дріб тоді і тільки тоді, коли канонічний розклад знаменника має вигляд $2^{\alpha}5^{\beta}$, тобто не містить ніяких простих множників, крім 2 і 5. Для спрощення вважатимемо $\frac{a}{b}$ нескоротним правильним дробом. (Якщо він неправильний, то можна спочатку виділити цілу частину). Звичайні нескоротні правильні дроби виду

$\frac{a}{2^{\alpha}\cdot 5^{\beta}}$ перетворюються в скінченні десяткові дроби з числом десяткових знаків, яке дорівнює найбільшому з чисел α або β.

Отже, нескоротний дріб виду $\frac{a}{c\cdot 2^{\alpha}\cdot 5^{\beta}}$, де c відмінне від 2 і 5, в скінченний десятковий дріб не перетворюється.

Теорема 41. Якщо канонічний розклад знаменника b нескоротного дробу $\frac{a}{b}$ не містить у собі множників 2 і 5, то цей дріб перетворюється в чистий періодичний десятковий дріб; при цьому число цифр у періоді дорівнює показнику δ, до якого належить число 10, за модулем b.

Зауваження. З конгруенції $10^{\delta}\equiv 1\pmod{b}$ випливає, що $10^{\delta}-1\equiv$ $\equiv 0\pmod{b}$, або $\underbrace{999...9}_{\delta\ \text{цифр}}\equiv 0\pmod{b}$.

Іншими словами, число $999...9$, що складається з δ дев‘яток, – найменше з можливих чисел такої структури, яке ділиться на b. Це дає можливість легко знаходити число δ. Для цього треба послідовно ділити на b числа 9, 99, 999, 9999, … і т. д., аж поки таке ділення не відбудеться. Кількість дев‘яток у такому числі і дорівнює числу δ.

Теорема 42. Якщо канонічний розклад знаменника b нескоротного дробу $\frac{a}{b}$ має вигляд $b=2^{\alpha}\cdot 5^{\beta}\cdot c$, де $(c,10)=1$, то цей дріб перетворюється у мішаний періодичний дріб; число цифр до періоду дорівнює γ, де γ – найбільше з чисел α і β; число цифр періоду дорівнює δ, де δ – показник, якому належить число 10 за модулем c.

Перевірка результатів арифметичних дій

За допомогою конгруенцій можна вказати необхідні ознаки правильності і достатні ознаки неправильності результатів виконання арифметичних дій додавання, віднімання та множення цілих чисел.

Результат дій додавання, віднімання і множення є ціла раціональна функція компонент, а тому, якщо замість даних чисел взяти найменші додатні або найменші за абсолютною величиною лишки цих чисел за яким-небудь модулем, то результат дій над цими лишками повинен бути конгруентний за тим же модулем найменшому лишку результату, який перевіряємо.

Якщо конгруенція не має змісту, то одержаний результат невірний. За модуль зручніше брати число, найменші лишки за яким легко обчислювати (наприклад, для десяткової системи числення – 9 та 11 або 5). У випадку 9 можна брати замість найменших лишків просто суму цифр, у випадку 11 – різницю між сумами цифр, які стоять на парних і непарних місцях (рахуючи справа наліво).

Зауважимо, що неправильність відповідної конгруенції гарантує неправильність виконання дій. Правильність відповідної конгруенції лиш підтверджує, але не гарантує правильність результату. Перевіркою за допомогою 9 або 11 не можна виявити помилку стосовно числа кратного 9 або 11 відповідно. Тому краще перевіряти одночасно числами 9 і 11. В цьому випадку можлива помилка на число, кратне 99, але ймовірність такої помилки дуже мала.

Результат ділення перевіряють за допомогою множення (ділене дорівнює дільнику, помноженому на частку плюс остача). Взагалі, слід мати на увазі, що додержання контролю при неправильних обчисленнях пов‘язане принаймні з двократною помилкою в обчисленнях, тому треба визнати контроль (навіть одним числом) ефективним.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ З ТЕМИ:

«Конгруенції першого порядку, системи конгруенцій»

Варіант 1

1. Визначити остачу від ділення: 66^{17} на 7.
2. Розв'язати конгруенцію $12x \equiv 15(\bmod 35)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби;
3. Дослідити та розв'язати конгруенцію: $15x \equiv 21(\bmod 18)$
4. Скільки точок з цілими координатами лежить на прямій $37x + 11y = 1$ між точками з абсцисами $x_1 = -20$ та $x_2 = 15$?
5. Розв'язати задачу: Для перевезення зерна є мішки по 60 та 80 кг. Скільки треба таких мішків для перевезення 440 кг зерна ?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 17 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_7^{(17)}$;
   г) клас, обернений до класу $K_{11}^{(17)}$.
8. Знайти найменше натуральне число, яке при діленні на 13, 15 та 11 дає відповідно остачі 2, 11, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 6x \equiv 1(\bmod 11), \\ 5x \equiv 2(\bmod 6), \\ x \equiv a(\bmod 22). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + x_2 - x_3 + 4x_4 \equiv 1 \\ 2x_1 - x_2 + x_3 - 3x_4 \equiv 2 \\ 3x_1 + 2x_2 + x_3 - x_4 \equiv -3 \\ x_1 - 2x_2 - 3x_3 + x_4 \equiv 0 \end{array}\right\} (\bmod 19)$$

Варіант 2

1. Визначити остачу від ділення: 11^{802} на 1000.
2. Розв'язати конгруенцію $7x \equiv 11 (\mathrm{mod}\, 15)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $78x \equiv 42 (\mathrm{mod}\, 51)$
4. Скільки точок з цілими координатами лежить на прямій $673x + 103y = 1$ між точками з абсцисами $x_1 = -150$ та $x_2 = 120$?
5. Розв'язати задачу: Скільки квитків вартістю 30 та 50 коп. можна купити на 14 грн. 90 коп.?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 18 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{10}^{(18)}$;
   г) клас, обернений до класу $K_{13}^{(18)}$.
8. Знайти найменше натуральне число, яке при діленні на 9, 11 та 13 дає відповідно остачі 2, 7, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 5 (\mathrm{mod}\, 21), \\ 3x \equiv 8 (\mathrm{mod}\, 10), \\ x \equiv a (\mathrm{mod}\, 6). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - x_2 + 3x_3 - x_4 \equiv 0 \\ 2x_1 + x_2 + x_3 - 3x_4 \equiv 1 \\ 2x_1 - x_2 - 4x_3 + 6x_4 \equiv -3 \\ x_1 + 3x_2 + x_3 - x_4 \equiv -1 \end{array}\right\} (\mathrm{mod}\, 23)$$

Варіант 3

1. Визначити остачу від ділення: 19^{2402} на 14.
2. Розв'язати конгруенцію $15x \equiv 7 (\bmod 16)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $375x \equiv 195 (\bmod 50)$
4. Скільки точок з цілими координатами лежить на прямій $52x + 23y = 1$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Розв'язати задачу: Для купівлі стільців вартістю 140 грн. і табуреток вартістю 60 грн. дитячий садок виділив 3300 грн. Скільки можна купити стільців і табуреток, щоб повність використати виділену суму грошей?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 19 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_5^{(19)}$;
   г) клас, обернений до класу $K_{14}^{(19)}$.
8. Знайти найменше натуральне число, яке при діленні на 7, 9 та 11 дає відповідно остачі 2, 3, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 5 (\bmod 10), \\ 2x \equiv 1 (\bmod 21), \\ x \equiv a (\bmod 14). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - x_2 - 3x_3 - 4x_4 \equiv 1 \\ x_1 + 5x_2 + 3x_3 - x_4 \equiv -1 \\ 3x_1 + x_2 + 2x_3 - 2x_4 \equiv 0 \\ x_1 - 2x_2 + x_3 + x_4 \equiv 2 \end{array}\right\} (\bmod 31)$$

Варіант 4

1. Визначити остачу від ділення: 1967^{1968} на 11.
2. Розв'язати конгруенцію $11x \equiv 15 (\bmod 24)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $10x \equiv 25 (\bmod 35)$.
4. Скільки точок з цілими координатами лежить на прямій $253x + 1001y = 22$ між точками з абсцисами $x_1 = -100$ та $x_2 = 110$?
5. Розв'язати задачу: Туристичне бюро, яке має в своєму розпорядженні двадцяти трьох місткі автобуси та шести місткі легкові автомобілі, організує екскурсійну поїздку для 310 туристів. Скільки машин одного і другого типу слід виділити для екскурсантів при умові, що у виділених автомобілях не повинно залишатися вільних місць?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 55 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{15}^{(55)}$;
   г) клас, обернений до класу $K_{9}^{(55)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 5 та 7 дає відповідно остачі 2, 1, 3.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 2 (\bmod 10), \\ 2x \equiv 1 (\bmod 33), \\ x \equiv a (\bmod 22). \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + 6x_2 - 4x_3 + 2x_4 \equiv 1 \\ 3x_1 + 9x_2 + x_3 - 3x_4 \equiv -2 \\ x_1 + 8x_2 + x_3 + 4x_4 \equiv 3 \\ 2x_1 + 4x_2 - 7x_3 + x_4 \equiv 4 \end{array}\right\} (\bmod 19)$$

Варіант 5

1. Визначити остачу від ділення: 109^{345} на 14.
2. Розв'язати конгруенцію $27x \equiv 11(\mathrm{mod}\,106)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $42x \equiv 105(\mathrm{mod}\,245)$
4. Скільки точок з цілими координатами лежить на прямій $23x + 49y = 53$ між точками з абсцисами $x_1 = -20$ та $x_2 = 80$?
5. Розв'язати задачу: Шахова база парку культури і відпочинку придбала необхідну кількість комплектів шашок та шахів на 620 грн. Комплект шахів коштує 46 грн., а шашок – 19 грн. Скільки комплектів шахів і шашок було закуплено базою?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 21 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{15}^{(21)}$;
   г) клас, обернений до класу $K_{17}^{(21)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 7 та 9 дає відповідно остачі 2, 3, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 2(\mathrm{mod}\,22), \\ 5x \equiv 4(\mathrm{mod}\,21), \\ x \equiv a(\mathrm{mod}\,14). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + x_2 - 4x_3 + 4x_4 \equiv 1 \\ x_1 - 3x_2 - 7x_3 + 3x_4 \equiv -4 \\ 2x_1 - 5x_2 + x_3 + 3x_4 \equiv 3 \\ 3x_1 + x_2 - 2x_3 - 2x_4 \equiv 1 \end{array}\right\}(\mathrm{mod}\,23)$$

Варіант 6

1. Визначити остачу від ділення: 293^{275} на 48.
2. Розв'язати конгруенцію $27x \equiv 16(\mathrm{mod}\,58)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $12x \equiv 16(\mathrm{mod}\,28)$
4. Скільки точок з цілими координатами лежить на прямій $42x + 31y = 67$ між точками з абсцисами $x_1 = -10$ та $x_2 = 60$?
5. Розв'язати задачу: Знайти два натуральних числа, кожне з яких не перевищує 200, таких, щоб різниця між ними дорівнювала 11, зменшуване кратне 9, а від'ємник кратний 17.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 22 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(22)}$;
   г) клас, обернений до класу $K_{13}^{(22)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 7 та 8 дає відповідно остачі 2, 3, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 4(\mathrm{mod}\,14), \\ 2x \equiv 3(\mathrm{mod}\,15), \\ x \equiv a(\mathrm{mod}\,35). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + 2x_2 - x_3 - 3x_4 \equiv 1 \\ 2x_1 - 2x_2 + x_3 - x_4 \equiv 3 \\ -x_1 + x_2 + 4x_3 - 3x_4 \equiv 0 \\ x_1 - 5x_2 + 2x_3 + 2x_4 \equiv 2 \end{array}\right\}(\mathrm{mod}\,37)$$

Варіант 7

1. Визначити остачу від ділення: 117^{53} на 11.
2. Розв'язати конгруенцію $39x \equiv 19(\mathrm{mod}\,53)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $98x \equiv 70(\mathrm{mod}\,42)$
4. Скільки точок з цілими координатами лежить на прямій $35x - 37y = 12$ між точками з абсцисами $x_1 = -100$ та $x_2 = 25$?
5. Розв'язати задачу: Скільки треба взяти банок місткістю $0,55$ л. та $0,8$ л., для розлиття 12 л. рідини так, щоб всі взяті банки були заповнені.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 23 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{11}^{(23)}$;
   г) клас, обернений до класу $K_{13}^{(23)}$.
8. Знайти найменше натуральне число, яке при діленні на 6, 7 та 11 дає відповідно остачі 2, 5, 7.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 7(\mathrm{mod}\,15), \\ 5x \equiv 1(\mathrm{mod}\,14), \\ x \equiv a(\mathrm{mod}\,21). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - 3x_2 - 3x_3 - 2x_4 \equiv 1 \\ x_1 - 4x_2 - 2x_3 + x_4 \equiv -3 \\ 2x_1 - x_2 - x_3 + 3x_4 \equiv 0 \\ 2x_1 + x_2 + 2x_3 + 2x_4 \equiv 4 \end{array}\right\} (\mathrm{mod}\,17)$$

Варіант 8

1. Визначити остачу від ділення: $5^{80}+7^{100}$ на 13.
2. Розв'язати конгруенцію $13x\equiv 93(\mathrm{mod}\,111)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $183x\equiv 93(\mathrm{mod}\,111)$
4. Скільки точок з цілими координатами лежить на прямій $7x-12y=15$ між точками з абсцисами $x_1=-50$ та $x_2=10$?
5. Розв'язати задачу: Для проведення естафети з бігу необхідно розділити дистанцію в 6,7 км на відрізки розміром 175 м для жінок та 300 м для чоловіків. Із скількох спортсменів, як чоловіків так і жінок, повинні складатися команди, які приймають участь у естафеті?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 24 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{15}^{(24)}$;
   г) клас, обернений до класу $K_{19}^{(24)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 6 та 7 дає відповідно остачі 2, 3, 4.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 4x\equiv 1(\mathrm{mod}\,15), \\ 3x\equiv 8(\mathrm{mod}\,26), \\ x\equiv a(\mathrm{mod}\,6). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1+x_2+4x_3-2x_4\equiv 1 \\ 2x_1-x_2+x_3-2x_4\equiv -3 \\ 3x_1-3x_2+x_3+4x_4\equiv -1 \\ x_1+2x_2+2x_3+x_4\equiv 2 \end{array}\right\}(\mathrm{mod}\,23)$$

Варіант 9

1. Визначити остачу від ділення: 11^{1841} на 7.
2. Розв’язати конгруенцію $121x \equiv 7 (\mathrm{mod}\, 13)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв’язати конгруенцію: $30x \equiv 18 (\mathrm{mod}\, 102)$
4. Скільки точок з цілими координатами лежить на прямій $8x - 13y = 63$ між точками з абсцисами $x_1 = -15$ та $x_2 = 40$?
5. Розв’язати задачу: В населений пункт, з яким встановлено лише авіаційне сполучення, необхідно доставити 150 контейнерів вантажу. Відправник має в розпорядженні транспортні літаки вантажопідйомністю відповідно 8 та 13 контейнерів. Скільки необхідно взяти літаків одного і другого типу, щоб перевезти вказаний вантаж одним рейсом? Вагопідйомність кожного літака повинна бути використана повністю.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 25 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{21}^{(25)}$;
   г) клас, обернений до класу $K_{23}^{(25)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 4 та 5 дає відповідно остачі 2, 1, 3.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 8 (\mathrm{mod}\, 26), \\ 5x \equiv 2 (\mathrm{mod}\, 6), \\ x \equiv a (\mathrm{mod}\, 15). \end{cases}$$

   буде сумісною?

10. Дослідити і розв’язати систему конгруенцій:

$$\left.\begin{aligned} x_1 - 6x_2 + 2x_3 - 3x_4 &\equiv 1 \\ 2x_1 - x_2 + x_3 - 4x_4 &\equiv -1 \\ x_1 + x_2 + 4x_3 - 7x_4 &\equiv 3 \\ 2x_1 - 7x_2 + x_3 + x_4 &\equiv 0 \end{aligned}\right\} (\mathrm{mod}\, 41)$$

Варіант 10

1. Визначити остачу від ділення: 22^{3242} на 14.
2. Розв'язати конгруенцію $19x \equiv 4 (\bmod 25)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $24x \equiv 14 (\bmod 26)$
4. Скільки точок з цілими координатами лежить на прямій $39x - 22y = 10$ між точками з абсцисами $x_1 = -10$ та $x_2 = 30$?
5. Розв'язати задачу: На обробку кожної з деталей типу А та В токар затрачує відповідно 41 та 14 хв. Скільки деталей типу А та В обробе токар протягом шестигодинного робочого дня? Робочий час повинен бути використаний повністю.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 26 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{20}^{(26)}$;
   г) клас, обернений до класу $K_{11}^{(26)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 8 та 11 дає відповідно остачі 2, 4, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 2 (\bmod 10), \\ 5x \equiv 4 (\bmod 21), \\ x \equiv a (\bmod 6). \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + 5x_2 + 3x_3 - 2x_4 \equiv 1 \\ x_1 - x_2 + 2x_3 + x_4 \equiv -3 \\ 3x_1 + x_2 - x_3 - 3x_4 \equiv 2 \\ 2x_1 - 2x_2 + 3x_3 + x_4 \equiv 2 \end{array}\right\} (\bmod 29)$$

Варіант 11

1. Визначити остачу від ділення: 34^{3741} на 26.
2. Розв'язати конгруенцію $14x \equiv 9 \pmod{37}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $114x \equiv 42 \pmod{87}$
4. Скільки точок з цілими координатами лежить на прямій $122x + 129y = 2$ між точками з абсцисами $x_1 = -10$ та $x_2 = 100$?
5. Розв'язати задачу: Розкласти число 1500 на два додатних доданки, один з яких кратний 11, а другий – 17.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 27 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_7^{(27)}$;
   г) клас, обернений до класу $K_{17}^{(27)}$.
8. Знайти найменше натуральне число, яке при діленні на 4, 5 та 7 дає відповідно остачі 2, 3, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 7x \equiv 13 \pmod{15}, \\ 5x \equiv 3 \pmod{22}, \\ x \equiv a \pmod{10}. \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{aligned} x_1 - 2x_2 + x_3 + 6x_4 &\equiv 1 \\ 3x_1 + x_2 - 3x_3 + 7x_4 &\equiv 0 \\ -x_1 + 3x_2 + 4x_3 - 2x_4 &\equiv 2 \\ x_1 - x_2 + 2x_3 - x_4 &\equiv -1 \end{aligned}\right\} \pmod{23}$$

Варіант 12

1. Визначити остачу від ділення: 178^{2741} на 222.
2. Розв'язати конгруенцію $39x \equiv 5 (\mathrm{mod}\, 11)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $14x \equiv 22 (\mathrm{mod}\, 36)$
4. Скільки точок з цілими координатами лежить на прямій $3x + 4y = 13$ між точками з абсцисами $x_1 = -20$ та $x_2 = 2$?
5. Розв'язати задачу: Товарні вагони з вантажем типу А та В мають вагу відповідно 27 та 43 т. Скільки вагонів з вантажем типу А та В необхідно для формування товарного потягу вагою 1800 т?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 28 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{23}^{(28)}$;
   г) клас, обернений до класу $K_{11}^{(28)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 6 та 7 дає відповідно остачі 3, 2, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 5 (\mathrm{mod}\, 15), \\ 3x \equiv 5 (\mathrm{mod}\, 22), \\ x \equiv a (\mathrm{mod}\, 33). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - 3x_2 - x_3 + 4x_4 \equiv 1 \\ -x_1 + 2x_2 - 2x_3 - 3x_4 \equiv -4 \\ 2x_1 - 2x_2 + x_3 + 2x_4 \equiv -2 \\ x_1 - 4x_2 + 7x_3 + 3x_4 \equiv 0 \end{array}\right\} (\mathrm{mod}\, 17)$$

Варіант 13

1. Визначити остачу від ділення: 12^{2751} на 10.
2. Розв'язати конгруенцію $9x \equiv 2(\mathrm{mod}\,14)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $39x \equiv 84(\mathrm{mod}\,93)$
4. Скільки точок з цілими координатами лежить на прямій $45x - 37y = 25$ між точками з абсцисами $x_1 = -25$ та $x_2 = 100$?
5. Розв'язати задачу: В наявності є резистори 1,2 та 1,7 Ом опору. Необхідно скласти послідовно з'єднаний ланцюг опором 11,1 Ом. Скільки резисторів одного і другого типу необхідно взяти?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 29 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(29)}$;
   г) клас, обернений до класу $K_{11}^{(29)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 8 та 11 дає відповідно остачі 2, 6, 7.
9. При яких значеннях параметра a система конгруенцій
$$\begin{cases} 8x \equiv 1(\mathrm{mod}\,15), \\ 3x \equiv 8(\mathrm{mod}\,22), \\ x \equiv a(\mathrm{mod}\,33). \end{cases}$$
   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:
$$\left.\begin{array}{l} x_1 + 2x_2 + x_3 - x_4 \equiv 1 \\ 3x_1 - x_2 + 2x_3 + 2x_4 \equiv -4 \\ x_1 + 4x_2 - 3x_3 + x_4 \equiv 2 \\ 2x_1 + 2x_2 + x_3 + x_4 \equiv 0 \end{array}\right\} (\mathrm{mod}\,37)$$

Варіант 14

1. Визначити остачу від ділення: 12^{2751} на 5.
2. Розв'язати конгруенцію $21x \equiv 10 (\mathrm{mod}\, 25)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $15x \equiv 21 (\mathrm{mod}\, 6)$
4. Скільки точок з цілими координатами лежить на прямій $42x + 31y = 67$ між точками з абсцисами $x_1 = -10$ та $x_2 = 50$?
5. Розв'язати задачу: Скільки книжок можна купити по 3 і 5 гривень маючи в розпорядженні 200 гривень, так, щоб використати всі гроші?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 30 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{27}^{(30)}$;
   г) клас, обернений до класу $K_{23}^{(30)}$.
8. Знайти найменше натуральне число, яке при діленні на 6, 7 та 13 дає відповідно остачі 4, 3, 11.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 8 (\mathrm{mod}\, 10), \\ 2x \equiv 5 (\mathrm{mod}\, 33), \\ x \equiv a (\mathrm{mod}\, 22). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{l} x_1 + 6x_2 - 2x_3 - x_4 \equiv 1 \\ x_1 - x_2 + 5x_3 + 2x_4 \equiv -3 \\ 3x_1 + 2x_2 - x_3 + 4x_4 \equiv 0 \\ x_1 + 3x_2 + 3x_3 - x_4 \equiv 2 \end{array}\right\} (\mathrm{mod}\, 19)$$

Варіант 15

1. Визначити остачу від ділення: $5^{50}+7^{50}$ на 12.
2. Розв'язати конгруенцію $19x\equiv 4(\mathrm{mod}\,25)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $20x\equiv 35(\mathrm{mod}\,45)$
4. Скільки точок з цілими координатами лежить на прямій $237x+44y=1$ між точками з абсцисами $x_1=-40$ та $x_2=105$?
5. Розв'язати задачу: Будують водопровід довжиною 105 м, мають труби довжиною 3 м і 4,5 м. Скільки необхідно поставити одних і других труб.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 31 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{28}^{(31)}$;
   г) клас, обернений до класу $K_{29}^{(31)}$.
8. Знайти найменше натуральне число, яке при діленні на 4, 9 та 11 дає відповідно остачі 3, 7, 9.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x\equiv 7(\mathrm{mod}15), \\ 11x\equiv 8(\mathrm{mod}14), \\ x\equiv a(\mathrm{mod}10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{l} x_1+5x_2+x_3+2x_4\equiv 1 \\ 3x_1+x_2-3x_3-x_4\equiv 3 \\ 3x_1-2x_2-x_3+2x_4\equiv -3 \\ x_1+4x_2+3x_3-x_4\equiv 2 \end{array}\right\}(\mathrm{mod}17)$$

Варіант 16

1. Визначити остачу від ділення: $5^{70}+13^{100}$ на 18.
2. Розв'язати конгруенцію $37x \equiv 16(\mathrm{mod}\,11)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $1215x \equiv 560(\mathrm{mod}\,2755)$
4. Скільки точок з цілими координатами лежить на прямій $7x-19y=23$ між точками з абсцисами $x_1=-20$ та $x_2=50$?
5. Розв'язати задачу: На станцію прибуло 350 т вугілля. В вагонах було по 15 і 20 т вугілля. Скільки вагонів було по 15 т і скільки по 20 т?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 32 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(32)}$;
   г) клас, обернений до класу $K_{11}^{(32)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 7 та 8 дає відповідно остачі 3, 6, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 3(\mathrm{mod}\,35), \\ 5x \equiv 3(\mathrm{mod}\,22), \\ x \equiv a(\mathrm{mod}\,10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{aligned} x_1-7x_2+2x_3+x_4 &\equiv 1 \\ 3x_1+2x_2-6x_3-2x_4 &\equiv 0 \\ 2x_1-3x_2+x_3-4x_4 &\equiv -1 \\ x_1-6x_2-3x_3+3x_4 &\equiv 1 \end{aligned}\right\}(\mathrm{mod}\,37)$$

Варіант 17

1. Визначити остачу від ділення: 439^{291} на 60.
2. Розв'язати конгруенцію $8x \equiv 17 (\operatorname{mod} 23)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $45x \equiv 21 (\operatorname{mod} 132)$
4. Скільки точок з цілими координатами лежить на прямій $12x - 7y = 29$ між точками з абсцисами $x_1 = -10$ та $x_2 = 5$?
5. Розв'язати задачу: На побудову газопроводу для траси довжиною 283 м поставили труби, довжина яких 5 і 7 м. Скільки труб поставили?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 33 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{28}^{(33)}$;
   г) клас, обернений до класу $K_{29}^{(33)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 6 та 7 дає відповідно остачі 4, 5, 2.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 1 (\operatorname{mod} 35), \\ 3x \equiv 5 (\operatorname{mod} 22), \\ x \equiv a (\operatorname{mod} 10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{aligned} x_1 + x_2 + x_3 - 2x_4 &\equiv 1 \\ x_1 + 5x_2 - 3x_3 + x_4 &\equiv 3 \\ 2x_1 - 2x_2 - x_3 + 3x_4 &\equiv 4 \\ x_1 + 3x_2 + 2x_3 - 2x_4 &\equiv 2 \end{aligned}\right\} (\operatorname{mod} 31)$$

Варіант 18

1. Визначити остачу від ділення: 383^{175} на 45.
2. Розв'язати конгруенцію $64x \equiv 5(\mathrm{mod}\,17)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $21x \equiv 35(\mathrm{mod}\,77)$
4. Скільки точок з цілими координатами лежить на прямій $3x + 8y = 5$ між точками з абсцисами $x_1 = -20$ та $x_2 = 5$?
5. Розв'язати задачу: Скільки поштових марок вартістю 30 та 40 коп. можна купити на 5 гривень?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 34 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{31}^{(34)}$;
   г) клас, обернений до класу $K_{29}^{(34)}$.
8. Знайти найменше натуральне число, яке при діленні на 7, 9 та 10 дає відповідно остачі 5, 7, 3.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 13(\mathrm{mod}\,35), \\ 5x \equiv 8(\mathrm{mod}\,22), \\ x \equiv a(\mathrm{mod}\,10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - x_2 + 3x_3 + 5x_4 \equiv 0 \\ 4x_1 - 3x_2 + 7x_3 + 3x_4 \equiv 1 \\ -x_1 - x_2 + 2x_3 - x_4 \equiv 2 \\ x_1 + 4x_2 - x_3 + 2x_4 \equiv 5 \end{array}\right\} (\mathrm{mod}\,13)$$

Варіант 19

1. Визначити остачу від ділення: 178^{52} на 11.
2. Розв'язати конгруенцію $73x \equiv 39 \pmod{28}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $21x \equiv 33 \pmod{45}$
4. Скільки точок з цілими координатами лежить на прямій $17x - 25y = 117$ між точками з абсцисами $x_1 = -50$ та $x_2 = 20$?
5. Розв'язати задачу: Маємо 77 метрів тканини. На юбку необхідно 3 м, а на сорочку – 2 м. Скільки і чого можна пошити з цієї тканини?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 35 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{27}^{(35)}$;
   г) клас, обернений до класу $K_{33}^{(35)}$.
8. Знайти найменше натуральне число, яке при діленні на 4, 5 та 9 дає відповідно остачі 2, 3, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 4x \equiv 3 \pmod{15}, \\ 7x \equiv 6 \pmod{22}, \\ x \equiv a \pmod{10}. \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - 3x_2 + x_3 - x_4 \equiv 1 \\ 2x_1 + x_2 - 4x_3 - 6x_4 \equiv -3 \\ 3x_1 - 4x_2 + 2x_3 - 4x_4 \equiv -2 \\ x_1 + 2x_2 + 3x_3 + 3x_4 \equiv 0 \end{array}\right\} \pmod{29}$$

Варіант 20

1. Визначити остачу від ділення: $12^{1231}+14^{4324}$ на 13.
2. Розв'язати конгруенцію $65x\equiv 7(\mathrm{mod}\,71)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $28x\equiv 40(\mathrm{mod}\,44)$
4. Скільки точок з цілими координатами лежить на прямій $7x-19y=23$ між точками з абсцисами $x_1=-10$ та $x_2=30$?
5. Розв'язати задачу: Будують водопровід довжиною 169 м; мають труби довжиною 3 і 4 м. Скільки необхідно поставити одних і других труб.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 36 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{25}^{(36)}$;
   г) клас, обернений до класу $K_{29}^{(36)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 10 та 11 дає відповідно остачі 2, 7, 8.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases}3x\equiv 7(\mathrm{mod}14),\\ 7x\equiv 6(\mathrm{mod}15),\\ x\equiv a(\mathrm{mod}10).\end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r}x_1-2x_2+7x_3+2x_4\equiv 1\\ x_1+3x_2+4x_3+x_4\equiv -3\\ 2x_1-x_2+5x_3-x_4\equiv 0\\ -x_1+4x_2-x_3+3x_4\equiv -2\end{array}\right\}(\mathrm{mod}\,37)$$

Варіант 21

1. Визначити остачу від ділення: 13^{2751} на 10.
2. Розв'язати конгруенцію $5x \equiv 7 \pmod{21}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $48x \equiv 12 \pmod{174}$
4. Скільки точок з цілими координатами лежить на прямій $25x + 18y = 11$ між точками з абсцисами $x_1 = -10$ та $x_2 = 25$?
5. Розв'язати задачу: В населений пункт, з яким встановлено лише річковий зв'язок, необхідно доставити 170 контейнерів. Відправник має в розпорядженні транспортні кораблі вантажністю відповідно 14 та 19 контейнерів. Скільки необхідно кораблів одного і другого типів, щоб перевезти вказаний вантаж одним рейсом? Вантажність кожного корабля повинна бути повністю використана.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 37 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(37)}$;
   г) клас, обернений до класу $K_{31}^{(37)}$.
8. Знайти найменше натуральне число, яке при діленні на 6, 7 та 11 дає відповідно остачі 2, 5, 1.
9. При яких значеннях параметра a система конгруенцій
$$\begin{cases} 8x \equiv 1 \pmod{15}, \\ 7x \equiv 2 \pmod{26}, \\ x \equiv a \pmod{15}. \end{cases}$$
   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:
$$\left.\begin{aligned} x_1 - 3x_2 - 4x_3 + x_4 &\equiv 1 \\ 2x_1 - 4x_2 + x_3 - 3x_4 &\equiv 2 \\ 2x_1 + x_2 + x_3 + 4x_4 &\equiv 2 \\ x_1 - 4x_2 + 7x_3 - 2x_4 &\equiv 0 \end{aligned}\right\} \pmod{41}$$

Варіант 22

1. Визначити остачу від ділення: 46^{921} на 21.
2. Розв'язати конгруенцію $7x \equiv 12 (\mathrm{mod} 15)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $87x \equiv 9 (\mathrm{mod} 21)$
4. Скільки точок з цілими координатами лежить на прямій $15x - 7y = 19$ між точками з абсцисами $x_1 = -45$ та $x_2 = 30$?
5. Розв'язати задачу: Для настилання підлоги завширшки 4,5 м є дошки завширшки 12 і 17 см. Скільки треба взяти дошок того і другого розміру, якщо вважати, що довжина кімнати і довжина дошок однакові і дошки кладуться вздовж кімнати.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 38 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(38)}$;
   г) клас, обернений до класу $K_{13}^{(38)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 5 та 7 дає відповідно остачі 1, 4, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 7 (\mathrm{mod} 15), \\ 5x \equiv 4 (\mathrm{mod} 26), \\ x \equiv a (\mathrm{mod} 10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - x_2 + 4x_3 + 4x_4 \equiv 1 \\ -x_1 - 2x_2 + 3x_3 + x_4 \equiv 3 \\ x_1 + 4x_2 - x_3 + 6x_4 \equiv 0 \\ 2x_1 - x_2 x + 3_3 x - 2_4 \equiv 1 \end{array}\right\} (\mathrm{mod} 23)$$

Варіант 23

1. Визначити остачу від ділення: 51^{1995} на 13.
2. Розв'язати конгруенцію $139x \equiv 7(\mathrm{mod}\,8)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $8x \equiv 52(\mathrm{mod}\,22)$
4. Скільки точок з цілими координатами лежить на прямій $25x + 18y = 20$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Розв'язати задачу: Число 700 розкласти на суму таких двох цілих чисел, щоб одне з них ділилося на 7, а друге – на 13.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 39 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{27}^{(39)}$;
   г) клас, обернений до класу $K_{31}^{(39)}$.
8. Знайти найменше натуральне число, яке при діленні на 10, 11 та 13 дає відповідно остачі 7, 8, 2.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 4x \equiv 5(\mathrm{mod}\,15), \\ 17x \equiv 8(\mathrm{mod}\,26), \\ x \equiv a(\mathrm{mod}\,10). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1+2x_2 - x_3 + 3x_4 \equiv 1 \\ 2x_1-x_2 + 2x_3 - x_4 \equiv -1 \\ 3x_1+x_2 + 4x_3 + 4x_4 \equiv 1 \\ 2x_1+2x_2 + x_3 + x_4 \equiv 0 \end{array}\right\}(\mathrm{mod}\,17)$$

Варіант 24

1. Визначити остачу від ділення: 439^{291} на 60.
2. Розв'язати конгруенцію $37x \equiv 28 \pmod{24}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $213x \equiv 111 \pmod{360}$
4. Скільки точок з цілими координатами лежить на прямій $53x + 17y = 25$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Розв'язати задачу: Скільки треба взяти банок місткістю 0,48 і 0,23 л, щоб розлити 13 л рідини, при умові що всі банки будуть наповнені?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 40 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{17}^{(40)}$;
   г) клас, обернений до класу $K_{21}^{(40)}$.
8. Знайти найменше натуральне число, яке при діленні на 9, 10 та 11 дає відповідно остачі 6, 7, 3.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 5x \equiv 4 \pmod{21}, \\ 17x \equiv 8 \pmod{26}, \\ x \equiv a \pmod{39}. \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - 3x_2 + 3x_3 + 2x_4 \equiv 1 \\ x_1 - 2x_2 - 3x_3 - 3x_4 \equiv -4 \\ 2x_1 + x_2 + x_3 + 3x_4 \equiv 0 \\ 2x_1 + 4x_2 + 6x_3 + 4x_4 \equiv -1 \end{array}\right\} \pmod{23}$$

Варіант 25

1. Визначити остачу від ділення: 23^{78} на 11.
2. Розв'язати конгруенцію $8x \equiv 15 (\bmod 29)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $105x \equiv 75 (\bmod 125)$
4. Скільки точок з цілими координатами лежить на прямій $11x + 13y = 80$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Розв'язати задачу: Маємо 47 метрів тканини. На юбку необхідно 4 м, а на сорочку – 3 м. Скільки і чого можна пошити з цієї тканини?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 41 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{28}^{(41)}$;
   г) клас, обернений до класу $K_{37}^{(41)}$.
8. Знайти найменше натуральне число, яке при діленні на 11, 12 та 13 дає відповідно остачі 9, 11, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 1 (\bmod 10), \\ 11x \equiv 5 (\bmod 39), \\ x \equiv a (\bmod 6). \end{cases}$$

   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + x_2 - 2x_3 - 3x_4 \equiv 1 \\ 3x_1 + 3x_2 - 4x_3 - 2x_4 \equiv 2 \\ x_1 - x_2 + 2x_3 + 3x_4 \equiv -2 \\ x_1 + 2x_2 - x_3 + 4x_4 \equiv 3 \end{array}\right\} (\bmod 19)$$

Варіант 26

1. Визначити остачу від ділення: 14^{245} на 90.
2. Розв'язати конгруенцію $17x \equiv 3 \pmod{2}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $112x \equiv 52 \pmod{94}$
4. Скільки точок з цілими координатами лежить на прямій $12x + 11y = 13$ між точками з абсцисами $x_1 = -50$ та $x_2 = 30$?
5. Розв'язати задачу: Число 455 розкласти на суму двох таких додатних чисел, щоб одне з них було кратне 25, а друге – 17.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 42 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{37}^{(42)}$;
   г) клас, обернений до класу $K_{11}^{(42)}$.
8. Знайти найменше натуральне число, яке при діленні на 7, 12 та 13 дає відповідно остачі 4, 5, 2.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 1 \pmod{14}, \\ 4x \equiv 5 \pmod{39}, \\ x \equiv a \pmod{21}. \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{aligned} x_1 - 3x_2 + 4x_3 - 2x_4 &\equiv 1 \\ x_1 + 2x_2 + 3x_3 + 5x_4 &\equiv 0 \\ 3x_1 - x_2 + 5x_3 - x_4 &\equiv -3 \\ 2x_1 - 2x_2 - x_3 - x_4 &\equiv 2 \end{aligned}\right\} \pmod{19}$$

Варіант 27

1. Визначити остачу від ділення: 17^{2001} на 1000.
2. Розв'язати конгруенцію $11x \equiv 5 (\bmod 9)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $120x \equiv 6 (\bmod 51)$
4. Скільки точок з цілими координатами лежить на прямій $15x + 14y = 60$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Скільки треба взяти банок місткістю 0,7 і 0,3 л, щоб розлити 11 л рідини, при умові що всі банки будуть наповнені?
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 43 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{20}^{(43)}$;
   г) клас, обернений до класу $K_{19}^{(43)}$.
8. Знайти найменше натуральне число, яке при діленні на 3, 7 та 13 дає відповідно остачі 5, 2, 4.
9. При яких значеннях параметра a система конгруенцій
$$\begin{cases} 13x \equiv 5 (\bmod 21), \\ 3x \equiv 4 (\bmod 26), \\ x \equiv a (\bmod 14). \end{cases}$$
   буде сумісною?
10. Дослідити і розв'язати систему конгруенцій:
$$\left.\begin{array}{r} x_1 + 4x_2 + x_3 + x_4 \equiv 1 \\ 2x_1 - 2x_2 - x_3 + 4x_4 \equiv 0 \\ x_1 - 3x_2 + 2x_3 + 2x_4 - 1 \equiv \\ 2x_1 + 2x_2 - 3x_3 - 2x_4 \equiv -2 \end{array}\right\} (\bmod 31)$$

Варіант 28

1. Визначити остачу від ділення: 317^{259} на 15.
2. Розв'язати конгруенцію $11x \equiv 12(\mathrm{mod}\,13)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $34x \equiv 8(\mathrm{mod}\,22)$
4. Скільки точок з цілими координатами лежить на прямій $7x + 13y = 30$ між точками з абсцисами $x_1 = -20$ та $x_2 = 30$?
5. Розв'язати задачу: Для настилання підлоги завширшки 3,5 м є дошки завширшки 11 і 15 см. Скільки треба взяти дошок того і другого розміру, якщо вважати, що довжина кімнати і довжина дошок однакові і дошки кладуться вздовж кімнати.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 50 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{45}^{(50)}$;
   г) клас, обернений до класу $K_{39}^{(50)}$.
8. Знайти найменше натуральне число, яке при діленні на 8, 9 та 11 дає відповідно остачі 4, 3, 6.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 1(\mathrm{mod}\,14), \\ 2x \equiv 5(\mathrm{mod}\,39), \\ x \equiv a(\mathrm{mod}\,21). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - x_2 + 2x_3 - 4x_4 \equiv 1 \\ x_1 - 5x_2 + 5x_3 + 2x_4 \equiv -1 \\ 2x_1 + 2x_2 + x_3 - 4x_4 \equiv 3 \\ x_1 - 4x_2 + x_3 + x_4 \equiv 1 \end{array}\right\}(\mathrm{mod}\,17)$$

Варіант 29

1. Визначити остачу від ділення: 7^{332} на 100.
2. Розв'язати конгруенцію $7x \equiv 13 \pmod{5}$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $38x \equiv 10 \pmod{24}$
4. Скільки точок з цілими координатами лежить на прямій $10x + 7y = 13$ між точками з абсцисами $x_1 = -15$ та $x_2 = 25$?
5. Розв'язати задачу: Будують водопровід довжиною 150 м; мають труби довжиною 5 і 4 м. Скільки необхідно поставити одних і других труб.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 51 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{44}^{(51)}$;
   г) клас, обернений до класу $K_{25}^{(51)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 9 та 11 дає відповідно остачі 2, 4, 7.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 2 \pmod{10}, \\ 7x \equiv 3 \pmod{39}, \\ x \equiv a \pmod{15}. \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 - 3x_2 + 6x_3 - x_4 \equiv 1 \\ 3x_1 - x_2 + x_3 - x_4 \equiv -2 \\ 2x_1 + x_2 + 7x_3 + 2x_4 \equiv -1 \\ x_1 + 2x_2 + 2x_3 - 5x_4 \equiv 0 \end{array}\right\} \pmod{37}$$

Варіант 30

1. Визначити остачу від ділення: 3^{157} на 100.
2. Розв'язати конгруенцію $17x \equiv 3(\mathrm{mod}\,5)$ двома способами:
   а) за теоремою Ейлера;
   б) використовуючи ланцюгові дроби.
3. Дослідити та розв'язати конгруенцію: $33x \equiv 9(\mathrm{mod}\,123)$
4. Скільки точок з цілими координатами лежить на прямій $8x + 9y = 13$ між точками з абсцисами $x_1 = -25$ та $x_2 = 30$?
5. Розв'язати задачу: Число 400 розкласти на суму двох таких додатних чисел, щоб одне з них було кратне 5, а друге – 23.
6. Обчислити на який день тижня припадав ваш день народження.
7. У множині класів лишків за модулем 53 знайти:
   а) усі дільники нуля;
   б) усі дільники одиниці;
   в) клас, протилежний класу $K_{36}^{(53)}$;
   г) клас, обернений до класу $K_{45}^{(53)}$.
8. Знайти найменше натуральне число, яке при діленні на 5, 8 та 9 дає відповідно остачі 3, 6, 5.
9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 3x \equiv 5(\mathrm{mod}\,22), \\ 13x \equiv 4(\mathrm{mod}\,35), \\ x \equiv a(\mathrm{mod}\,14). \end{cases}$$

   буде сумісною?

10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1+x_2+x_3-5x_4 \equiv 1 \\ 3x_1-2x_2-2x_3-2x_4 \equiv 0 \\ 2x_1+2x_2+3x_3-4x_4 \equiv 1 \\ 2x_1-x_2-x_3-3x_4 \equiv 2 \end{array}\right\}(\mathrm{mod}\,13)$$

МЕТОДИЧНІ ВКАЗІВКИ ДО РОЗВ'ЯЗАННЯ ЗАВДАНЬ З ТЕМИ:

«Конгруенції першого порядку, системи конгруенцій»

Завдання 1.1. Знайти остачу від ділення 2598^{33} на 17.

Розв'язання. Оскільки 17 – просте число і $(2598,17)=1$, то за формулою $a^{p-1}\equiv 1(\mathrm{mod}\,p)$ маємо $2598^{16}\equiv 1(\mathrm{mod}\,17)$. Підносячи до квадрата обидві частини конгруенції, далі маємо $2598^{32}\equiv 1(\mathrm{mod}\,17)$. Крім того, $2598\equiv 14(\mathrm{mod}\,17)$. Далі дістаємо

$$2598^{32}\equiv 1(\mathrm{mod}\,17)\wedge 2598\equiv 14(\mathrm{mod}\,17)\Rightarrow 2598^{33}\equiv 14(\mathrm{mod}\,17).$$

Отже, остача дорівнює 14.

Відповідь: 14.

Завдання 1.2. Довести, що $2^{2^5}+1$ ділиться націло на 641.

Розв'язання. Оскільки $2^5=32$, то треба довести, що $2^{32}+1\equiv 0(\mathrm{mod}\,641)$.

Маємо:

$$2^{10}=1024\equiv 383(\mathrm{mod}\,641),$$

$$2^{15}=2^{10}\cdot 2^5=383\cdot 32=12256\equiv 77(\mathrm{mod}\,641),$$

$$2^{30}=(2^{15})^2=77^2=5929\equiv 160(\mathrm{mod}\,641).$$

Тому $2^{32}+1=2^{30}\cdot 4+1=160\cdot 4+1=641\equiv 0(\mathrm{mod}\,641)$.

Завдання 2. Розв'язати конгруенцію $15x\equiv 23(\mathrm{mod}\,22)$ двома способами:

а) за теоремою Ейлера;

б) використовуючи ланцюгові дроби.

Розв'язання.

а) Користуючись способом Ейлера, розв‘яжемо конгруенцію

$$15x\equiv 23(\mathrm{mod}\,22).$$

Знаходимо $(15,22)=1$. Задана конгруенція має 1 розв‘язок. Оскільки $a=15$, $m=22$, $b=23$, то за формулою $x\equiv ba^{\varphi(m)-1}\pmod m$ маємо $x\equiv 23\cdot 15^{\varphi(22)-1}\pmod{22}$.

Знайдемо $\varphi(22)$. Оскільки $22=2\cdot 11$, то

$$\varphi(22)=2\cdot 11\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{11}\right)=10.$$

Тоді $x\equiv 23\cdot 15^{10-1}\pmod{22}$. Число $23\cdot 15^9$ замінимо найменшим невід‘ємним лишком за модулем 22. Дістанемо

$$x\equiv 23\cdot 15^9\equiv 23\cdot(3375)^3\equiv 23\cdot 9^3\equiv 23\cdot 3\equiv 3\pmod{22}.$$

Отже, $x\equiv 3\pmod{22}$ є розв‘язок конгруенції $15x\equiv 23\pmod{22}$.

Зауваження. Недоліком способу Ейлера є те, що при великому $\varphi(m)$ знаходження найменшого невід‘ємного лишку того класу чисел за модулем m, до якого належить число $ba^{\varphi(m)}$, стає громіздким.

Відповідь: $x\equiv 3\pmod{22}$

б) Використовуючи ланцюгові дроби, розв‘яжемо конгруенцію

$$15x\equiv 23\pmod{22}.$$

Розкладемо $\frac{22}{15}$ у ланцюговий дріб і обчислимо його підхідні дроби. Дістанемо таблицю елементів q_k і чисельників P_k.

k	-1	0	1	2
q_k		1	2	7
P_k	1	1	3	22

Отже, $n=2$, $P_{n-1}=3$. Оскільки $b=23$, $m=22$, то за формулою

$$x\equiv(-1)^n P_{n-1}b\pmod m.$$

Отже,

$$x\equiv(-1)^2\cdot 3\cdot 23\equiv 69\equiv 3\pmod{22}.$$

є розв‘язком конгруенції $15x\equiv 23\pmod{22}$.

Відповідь: $x\equiv 3\pmod{22}$

Завдання 3. Розв‘язати конгруенцію $8x \equiv 16 \pmod{12}$.

Розв‘язання. Маємо $(8,12)=4$ і $16 \vdots 4$, тому дана конгруенція має 4 розв’язки. Скорочуючи обидві частини конгруенції і модуль на 4, дістанемо конгруенцію:

$$2x \equiv 4 \pmod{3}.$$

За елементарними перетвореннями поділимо обидві частини конгруенції на 2 (їх спільний дільник), матимемо:

$$x \equiv 2 \pmod{3}.$$

Звідси задана конгруенція матиме чотири таких розв‘язки: $x \equiv 2,\ 5,\ 8,\ 11 \pmod{12}$. Тут кожний розв‘язок, згідно з теоремою [Якщо $(a,m)=d>1$, і b ділиться на d, то конгруенція $ax \equiv b \pmod{m}$ має d розв‘язків виду $x \equiv x_0,\ x_0+m_1,\ x_0+2m_1,\ \ldots,\ x_0+(d-1)m_1 \pmod{m}$; якщо ж у цьому випадку b не ділиться на d, то конгруенція $ax \equiv b \pmod{m}$ розв‘язків не має.] В даному прикладі кожний розв‘язок, згідно вказаної теореми, виходить з попереднього додаванням $m_1 = \dfrac{m}{d} = 3$.

Відповідь: $x \equiv 2,\ 5,\ 8,\ 11 \pmod{12}$

Завдання 4. Розв‘язати в цілих числах невизначене рівняння

$$53x + 47y = 11.$$

Розв‘язання. Оскільки число y повинно бути цілим, то різниця $53x-11$ має ділитися на 47. Дістаємо

$$53x \equiv 11 \pmod{47}.$$

Розв‘яжемо цю конгруенцію. Знаходимо $(53,47)=1$. Отже, конгруенція має єдиний розв‘язок. Застосуємо штучний спосіб. Додамо до правої частини число $-329=(-47)\cdot 7$, яке кратне модулю:

$$53x \equiv 11+(-47)\cdot 7 \pmod{47},$$

$$53x \equiv -318 \pmod{47},$$

$$x \equiv -6 \pmod{47}.$$

Отже, $x \equiv -6 \pmod{47}$ є розв’язком конгруенції $53x \equiv 11 \pmod{47}$. Тоді

$$\left\{-6;\ \frac{11-53\cdot(-6)}{47}\right\} = \{-6;\ 7\}$$

є окремим розв’язком заданого рівняння. Загальний розв‘язок заданого рівняння дістаємо за формулами:

$$x' = x_0 + \frac{m}{d}t,\ y' = y_0 - \frac{a}{d}t,$$

де $x_0 = -6,\ y_0 = 7,\ m = 47,\ a = 53,\ d = 1$. Отже,

$$\{x' = -6 + 47t,\ y' = 7 - 53t\} -$$

загальний розв‘язок заданого невизначеного рівняння, де $t -$ довільне ціле число.

Відповідь: $x' = -6 + 47t,\ y' = 7 - 53t$.

Завдання 5. Необхідно прокласти трасу газопроводу довжиною 450 метрів. В наявності є труби двох розмірів: довжиною 9 і 13 м. Скільки труб одного і іншого розмірів потрібно взяти, щоб прокласти трасу? Труби розрізати не можна, кількість швів повинна бути мінімальною.

Розв‘язання. Нехай x та y – кількість труб довжиною 9 м і 13 м відповідно. Отримаємо рівняння $9x + 13y = 450$. Оскільки $(9,13) = 1$, це рівняння має розв’язки. Щоб їх знайти, замінимо рівняння конгруенцією $9x \equiv 450(\mathrm{mod}13)$. З цієї конгруенції знаходимо $x \equiv 11(\mathrm{mod}13)$. Якщо взяти $x_0 = 11$, то для знаходження y_0 маємо рівняння $9 \cdot 11 + 13y_0 = 450$, звідки $y_0 = 27$. Отримаємо частинний розв’язок: $x_0 = 11,\ y_0 = 27$.

Знаходимо всі розв’язки рівняння в цілих числах $x = 11 + 13t$, $y = 27 - 9t$, де $t = 0;\pm1;\pm2;\pm3,...$. Знаходимо цілі значення t, при яких $x \geq 0, y \geq 0$:

$$\begin{cases} 11 + 13t \geq 0 \\ 27 - 9t \geq 0 \end{cases},\ -\frac{11}{13} \leq t \leq 3,$$ тобто цілі значення $t = 0;1;2;3$.

Складемо таблицю:

t	0	1	2	3
x	11	24	37	50
y	27	18	9	0
$x+y$	38	42	46	50

З таблиці видно, що задача має чотири розв’язки. Мінімальна кількість швів буде якщо взяти 11 дев’ятиметрових труб та 27 тринадцяти метрових труб.

Відповідь: 11 дев'ятиметрових труб та 27 тринадцяти метрових труб.

Завдання 6. Обчислити на який день тижня припало 20 грудня 1980 року.

Розв'язання. Конгруенції використовують для опису дискретних періодичних явищ. Так, наприклад, за допомогою теорії конгруенцій можна визначити день тижня, що припадає на зазначену дату. Детальний вивід формули та її обґрунтування див. в [1]. Формула для дня тижня, який припадає на a-й день b - го місяця $(100k+l)$-го року, записується у вигляді $\left(5k+l+a+\left[\frac{k}{4}\right]+\left[\frac{l}{4}\right]+\left[\frac{13b-1}{5}\right]\right)\bmod 7$. Зауважимо, що в наведеній формулі першим роком місяця вважається березень.

Для того щоб скористатися даною формулою ми дату 20 грудня 1980 року запишемо як 20-й день 10-го місяця 1980-го року. Тоді $(95+80+20+4+20+25)\bmod 7=6$.

Отже, 20 грудня 1980 року була субота.

Відповідь: субота.

Завдання 8. У множині класів лишків за модулем 20 знайти:

а) усі дільники нуля;

б) усі дільники одиниці;

в) клас, протилежний до класу $K_{11}^{(20)}$;

г) клас, обернений до класу $K_7^{(20)}$.

Розв'язання. а) Оскільки дільником нуля є кожен клас $K_a^{(20)}$, для якого знайдеться такий клас $K_x^{(20)}$, що $K_a^{(20)}\cdot K_x^{(20)}=K_0^{(20)}$, де $K_a^{(20)}\neq K_0^{(20)}\neq K_x^{(20)}$, тобто такий клас $K_x^{(20)}$, що $ax \vdots 20$, де $1\le a,\ x\le 19$, то фактично дільниками нуля є всі ті класи $K_a^{(20)}$, в яких представник a не взаємно простий з 20. Отже, дільниками нуля є такі класи: $K_2^{(20)}, K_4^{(20)}, K_5^{(20)}, K_6^{(20)}, K_{10}^{(20)}, K_{12}^{(20)}, K_{14}^{(20)}, K_{16}^{(20)}, K_{15}^{(20)}, K_8^{(20)}, K_{18}^{(20)}$.

б) Аналогічні міркування для дільників одиниці показують, що дільниками одиниці є всі ті класи $K_a^{(20)}$, в яких представник a взаємно простий з 20. Справді, якщо $(a,20)=1$, то знайдуться такі цілі числа U

і V, що $a\cdot U+20\cdot V=1$. Тоді $K_{aU+20V}=K_1$, проте $K_{aU+20V}=K_{aU}+K_{20V}$, а $K_{20V}=K_0$, $K_{aU}=K_a\cdot K_U$. Отже, $K_a\cdot K_U=K_1$. Звідси, зокрема, $\left(K_a\right)^{-1}=K_U$, тобто ми вивели формулу для знаходження класу, оберненого до класу K_a, якщо $(a,20)=1$. Випишемо дільники одиниці:

$$K_1^{(20)},K_3^{(20)},K_7^{(20)},K_9^{(20)},K_{11}^{(20)},K_{13}^{(20)},K_{17}^{(20)},K_{19}^{(20)}.$$

в) Знайдемо, такий клас $K_x^{(20)}$, що $K_{11}^{(20)}+K_x^{(20)}=K_0^{(20)}$. Оскільки $K_{11}^{(20)}+K_x^{(20)}=K_{11+x}^{(20)}$, то шукатимемо таке ціле число x, що $11+x\,\vdots\,20$. Найменшим таким числом є 9. Отже, $x=9$ і тому $-K_9^{(20)}=K_{11}^{(20)}$.

г) Для знаходження класу $\left(K_a^{(m)}\right)^{-1}$, оберненого до класу $K_a^{(m)}$, існує ще один спосіб. Нехай $(a,m)=1$, у противному разі клас $K_a^{(m)}$ взагалі не має оберненого. Нехай P_{n-1} – чисельник передостаннього підхідного дробу $\dfrac{P_{n-1}}{Q_{n-1}}$ для числа $\dfrac{m}{a}$, $\dfrac{m}{a}=\dfrac{P_n}{Q_n}$. Оскільки $\dfrac{m}{a}$ – нескоротний дріб, то $m=P_n$, $a=Q_n$. За однією з властивостей підхідних дробів маємо

$$\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^{n-1}}{Q_{n-1}Q_n}.$$

Отже,

$$\frac{m}{a}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^{n-1}}{Q_{n-1}\cdot a}.$$

Звідси $Q_{n-1}\cdot m-a\cdot P_{n-1}=(-1)^{n-1}$.

Тоді $a\cdot(-1)^n P_{n-1}\equiv 1(\operatorname{mod} m)$.

Згідно з цією конгруенцією, клас $K_{(-1)^{n-1}P_{n-1}}^{(m)}$ є оберненим до класу $K_a^{(m)}$.

Отже, $\left(K_a^{(m)}\right)^{-1}=K_{(-1)^n P_{n-1}}^{(m)}$.

Для розглянутого прикладу маємо таблицю, де $m=20$, $a=7$, $n=2$, $P_{n-1}=P_1=3$. Тоді

$$\left(K_7^{(m)}\right)^{-1}=K_{(-1)^2\cdot 3}^{(20)}=K_3^{(20)}.$$

k	-1	0	1	2
q_k	$-$	2	1	6
P_k	1	2	3	20
Q_k	0	1	1	7

Знайдемо такий клас $K_U^{(20)}$, що $K_7^{(20)} \cdot K_U^{(20)} = K_1^{(20)}$. Оскільки $(7,20)=1$, то, згідно з пунктом б), цей клас можна знайти, знайшовши спочатку за допомогою алгоритму Евкліда число U. До чисел 7 і 20 застосуємо алгоритм Евкліда. Маємо:

$$20 = 7\cdot 2 + 6,$$
$$7 = 6\cdot 1 + 1.$$

Звідси

$$6 = 20 - 7\cdot 2,$$
$$1 = 7 - 6\cdot 1.$$

Тоді $1 = 7 - 6\cdot 1 = 7 - (20 - 7\cdot 2) = 7\cdot 3 - 20 = 7\cdot 3 + (-1)\cdot 20$.

Отже, $U = 3$, а $K_U^{(20)} = K_3^{(20)}$.

Оскільки $K_3^{(20)} \cdot K_7^{(20)} = K_1^{(20)}$, то $K_3^{(20)}$ є оберненим до класу $K_7^{(20)}$.

Зауваження:

1. У подальшому, знайшовши дільники нуля (дільники одиниці), говоритимемо, що відмінні від дільників нуля і самого нуля елементи є дільниками одиниці (відмінні від дільників одиниці і від нуля елементи є дільниками нуля).

2. У пунктах а) і б), не обмежуючись тільки переліком дільників нуля та одиниці, можна виписати відповідні конкретні пари. У розгорнутому прикладі такими парами відповідно є:

$$K_2^{(20)} \text{ і } K_{10}^{(20)},\ K_4^{(20)} \text{ і } K_5^{(20)},\ K_4^{(20)} \text{ і } K_{15}^{(20)} \text{ і т. д.}$$
$$K_3^{(20)} \text{ і } K_7^{(20)},\ K_{13}^{(20)} \text{ і } K_{17}^{(20)}.$$

3. Клас $K_U^{(m)}$, обернений до класу $K_a^{(m)}$, можна іноді швидко знаходити усно, підбираючи таке число U, щоб добуток $a\cdot U$ при діленні на m давав остачу 1. Так для класу $K_7^{(20)}$ класи $K_1^{(20)}$, $K_9^{(20)}$, $K_{11}^{(20)}$, $K_{13}^{(20)}$, $K_{17}^{(20)}$, $K_{19}^{(20)}$ не підійшли б, оскільки числа $1\cdot 7 = 7$, $9\cdot 7 = 63$, $11\cdot 7 = 77$, $13\cdot 7 = 91$, $17\cdot 7 = 119$, $19\cdot 7 = 133$ при діленні на 20 дають остачу, відмінну від 1. При цьому, звичайно, дільники нуля $K_2^{(20)}$, $K_4^{(20)}$, $K_5^{(20)}$, $K_6^{(20)}$, $K_8^{(20)}$, $K_{10}^{(20)}$, $K_{12}^{(20)}$, $K_{14}^{(20)}$, $K_{15}^{(20)}$, $K_{16}^{(20)}$, $K_{18}^{(20)}$ не випробовуються, бо вони вже дільниками одиниці не можуть бути. Оскільки $9\cdot 9 = 81$, $11\cdot 11 = 121$, $19\cdot 19 = 361$, то $\left(K_9^{(20)}\right)^{-1} = K_9^{(20)}$,

$\left(K_{11}^{(20)}\right)^{-1} = K_{11}^{(20)}$, $\left(K_{19}^{(20)}\right)^{-1} = K_{19}^{(20)}$, тобто $K_{9}^{(20)}$, $K_{11}^{(20)}$ і $K_{19}^{(20)}$ є оберненими до себе.

Завдання 8. Знайти найменше натуральне число, яке при діленні на 10, 13 та 17 дає відповідно остачі 3, 11, 15.

Розв'язання. Позначимо шукане число через x, тоді задача зводиться до розв'язання конгруенції:

$$\begin{cases} x \equiv 3(\bmod 10), \\ x \equiv 11(\bmod 13), \\ x \equiv 15(\bmod 17). \end{cases}$$

Оскільки модулі конгруенцій попарно взаємно прості, то можна використати формулу $x \equiv c_0 \left(\bmod M\right)$, де

$$M = m_1 \cdot m_2 \cdot \ldots \cdot m_k,\ x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \ldots + M_k y_k c_k,$$

причому числа M_i і y_i визначають з таких умов:

$$M_i = \frac{M}{m_i},\ M_i y_i \equiv 1\left(\bmod m_i\right),\ i = 1, 2, \ldots, k.$$

Знаходимо: $M = 10 \cdot 13 \cdot 17 = 2210$,

$$M_1 = \frac{2210}{10} = 221,\ M_2 = \frac{2210}{13} = 170,\ M_3 = \frac{2210}{17} = 130.$$

Розв'яжемо такі конгруенції:

$$221 y_1 \equiv 1(\bmod 10),\ 170 y_2 \equiv 1(\bmod 13),\ 130 y_3 \equiv 1(\bmod 17).$$

$$y_1 = 1,\ y_2 = 1,\ y_3 = 14.$$

Згідно з формулою, дістанемо розв'язок даної системи

$$x = x_0 = 211 \cdot 1 \cdot 3 + 170 \cdot 1 \cdot 11 + 130 \cdot 14 \cdot 15 = 29833 \equiv 1103\left(\bmod 2210\right).$$

Звідси випливає, що найменшим натуральним числом, яке задовольняє умову задачі є 1103.

Відповідь: 1103.

Завдання 9. При яких значеннях параметра a система конгруенцій

$$\begin{cases} 2x \equiv 7(\bmod 15) \\ x \equiv 5(\bmod 14) \\ x \equiv a(\bmod 21) \end{cases}$$

буде сумісною?

Розв'язання. Оскільки конгруенція $2x \equiv 7(\mathrm{mod}15)$ еквівалентна конгруенції $x \equiv 11(\mathrm{mod}15)$, то систему можна записати таким чином

$$\begin{cases} x \equiv 11(\mathrm{mod}\,15) \\ x \equiv 5(\mathrm{mod}\,14) \\ x \equiv a(\mathrm{mod}\,21) \end{cases}.$$

Оскільки $x - 11$ ділиться на 15 тоді і тільки тоді, коли воно ділиться на 3 і на 5. Тому конгруенція $x \equiv 11(\mathrm{mod}15)$ рівносильна системі

$$\begin{cases} x \equiv 11 \equiv 2(\mathrm{mod}\,3) \\ x \equiv 11 \equiv 1(\mathrm{mod}\,5) \end{cases}.$$

Аналогічно конгруенцію $x \equiv 5(\mathrm{mod}14)$ можна замінити системою

$$\begin{cases} x \equiv 5 \equiv 1(\mathrm{mod}\,2) \\ x \equiv 5(\mathrm{mod}\,7) \end{cases},$$

а третю – системою

$$\begin{cases} x \equiv a(\mathrm{mod}\,3) \\ x \equiv a(\mathrm{mod}\,7) \end{cases}.$$

Отже, початкова система рівносильна системі:

$$\begin{cases} x \equiv 2(\mathrm{mod}\,3) \\ x \equiv 1(\mathrm{mod}\,5) \\ x \equiv 1(\mathrm{mod}\,2) \\ x \equiv 5(\mathrm{mod}\,7) \\ x \equiv a(\mathrm{mod}\,3) \\ x \equiv a(\mathrm{mod}\,7) \end{cases}$$

Порівнюючи першу конгруенцію з п'ятою, четверту з шостою, бачимо що для сумісності цієї системи необхідно, щоб параметр a задовольняв систему:

$$\begin{cases} a \equiv 2(\mathrm{mod}\,3) \\ a \equiv 5(\mathrm{mod}\,7) \end{cases}$$

З першої конгруенції виражаємо $a = 2 + 3t_1$, де t_1 – ціле число. Щоб визначити t_2, підставимо значення x у другу конгруенцію; тоді матимемо:

$$3t_1 \equiv 3\left(\mathrm{mod}\,7\right)$$

або, скорочуючи на 3, знайдемо:

$$t_1 \equiv 1(\mathrm{mod}\,7).$$

Звідси $t_1 = 1 + 7t_2$, де t_2 – будь-яке ціле число. Тепер

$$a = 2 + 3t_1 = 2 + 3(1 + 7t_2) = 5 + 21t_2.$$

Тому загальний розв'язок даної системи: $a \equiv 5(\mathrm{mod}\,21)$.

Отже, початкова система сумісна тоді і тільки тоді, коли $a \equiv 5(\mathrm{mod}\,21)$.

Відповідь: $a \equiv 5(\mathrm{mod}\,21)$

Завдання 10. Дослідити і розв'язати систему конгруенцій:

$$\left.\begin{array}{r} x_1 + x_2 + 2x_3 + 3x_4 \equiv 1 \\ 3x_1 - x_2 - x_3 - 2x_4 \equiv -4 \\ 2x_1 + 3x_2 - x_3 - x_4 \equiv -6 \\ x_1 + 2x_2 + 3x_3 - x_4 \equiv 0 \end{array}\right\}(\mathrm{mod}\,31)$$

Розв'язання. При простому модулі p на систему конгруенцій першого степеня з кількома невідомими $a_{i1}x_1 + \ldots + a_{in}x_n \equiv b_i(\mathrm{mod}\,p)$ $(i = 1,2,\ldots,m)$, де a_{ij}, b_i – цілі числа, можна поширити всі результати загальної теорії лінійних рівнянь. Якщо через A_{ij} позначити клас, лишком якого є a_{ij}, і через B_i – клас з лишком b_i, то системі конгруенцій відповідатиме система лінійних рівнянь:

$$A_{i1}X_1 + \ldots + A_{in}X_n \equiv B_i \ \ (i = 1,2,\ldots,m),$$

де $X_1, X_2, \ldots, X_n$ – класи, лишками яких є невідомі $x_1, x_2, \ldots, x_n$.

$Dx_i \equiv D_i(\mathrm{mod}\,p)$, де D – основний визначник системи D_i – визначник, який утворюється із основного визначника системи заміною i-го стовпчика стовпчиком вільних членів.

Обчисливши відповідні визначники отримуємо систему:

$$\left.\begin{array}{r} 165x_1 \equiv -153 \\ 129x_2 \equiv -153 \\ -156x_3 \equiv -153 \\ -45x_4 \equiv -153 \end{array}\right\}(\mathrm{mod}\,31).$$

Розв'язавши відповідні конгруенції маємо:

$$\left.\begin{array}{r} -153x_1 \equiv 165 \\ -153x_2 \equiv 129 \\ -153x_3 \equiv -156 \\ -153x_4 \equiv -45 \end{array}\right\}(\mathrm{mod}\,31), \quad \left.\begin{array}{r} 2x_1 \equiv 10 \\ 2x_2 \equiv 5 \\ 2x_3 \equiv 30 \\ 2x_4 \equiv 74 \end{array}\right\}(\mathrm{mod}\,31), \quad \left.\begin{array}{r} x_1 \equiv 5 \\ x_2 \equiv 18 \\ x_3 \equiv 15 \\ x_4 \equiv 24 \end{array}\right\}(\mathrm{mod}\,31).$$

Відповідь: $x_1 \equiv 5$, $x_2 \equiv 18$, $x_3 \equiv 15$, $x_4 \equiv 24(\mathrm{mod}\,31)$.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ З ТЕМИ

«Конгруенції вищих порядків»

Варіант 1

1. Чи проходить через точки з цілими координатами парабола

$$113y = x^2 - 69?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 14 \pmod{31}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 17 \pmod{64}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 135 \pmod{243}$$

5. Розв‘язати конгруенцію:

$$2x^2 - 7x + 5 \equiv 0 (\bmod 11)$$

6. Розв‘язати конгруенцію:

$$x^2 + 7x - 8 \equiv 0 (\bmod 15)$$

7. Розв‘язати конгруенцію:

$$4x^9 + 3x^8 - 5x^7 - 4x^3 - 3x^2 + 9x - 3 \equiv 0 (\bmod 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1$, $b = 110$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$18 \cdot 12^{3x} + 27 \equiv 0 (\bmod 61)?$$

10. Розв‘язати конгруенцію:

$$14x^7 + 36 \equiv 0 (\bmod 61)$$

Варіант 2

1. Чи проходить через точки з цілими координатами парабола

$$197y = x^2 - 88\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 8 \pmod{31}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 137 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 706 \pmod{625}$$

5. Розв‘язати конгруенцію:

$$3x^2 + 7x + 4 \equiv 0 \pmod{17}$$

6. Розв‘язати конгруенцію:

$$2x^2 - 12x + 1 \equiv 0 \pmod{33}$$

7. Розв‘язати конгруенцію:

$$5x^8 + 2x^7 - 3x^6 + 2x^5 - 5x^4 - 2x^3 - 3x^2 - 5x + 4 \equiv 0 \pmod{5}$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=130$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$32 \cdot 11^{4x} + 18 \equiv 0 \pmod{53}\,?$$

10. Розв‘язати конгруенцію:

$$7x^{11} + 13 \equiv 0 \pmod{53}$$

Варіант 3

1. Чи проходить через точки з цілими координатами парабола

$$271y = x^2 - 41?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 13 \pmod{29}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 41 \pmod{32}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 29 \pmod{343}$$

5. Розв‘язати конгруенцію:

$$3x^2 + 7x + 8 \equiv 0 (\mathrm{mod}\, 11)$$

6. Розв‘язати конгруенцію:

$$3x^2 - 5x + 2 \equiv 0 (\mathrm{mod}\ 21)$$

7. Розв‘язати конгруенцію:

$$4x^{10} + 3x^9 - 2x^8 - 5x^7 - 4x^4 - 3x^3 - x^2 - 3x + 1 \equiv 0 (\mathrm{mod}\, 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 105$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$8 \cdot 5^{2x} + 27 \equiv 0 (\mathrm{mod}\, 59)\,?$$

10. Розв‘язати конгруенцію:

$$14x^{26} + 14 \equiv 0 (\mathrm{mod}\, 53)\,.$$

Варіант 4

1. Чи проходить через точки з цілими координатами парабола

$$337y = x^2 - 27\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 20 \pmod{29}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 57 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 15 \pmod{243}$$

5. Розв‘язати конгруенцію:

$$3x^2 + 4x + 7 \equiv 0 (\bmod 31)$$

6. Розв‘язати конгруенцію:

$$x^2 + 5x + 6 \equiv 0 (\bmod 49)$$

7. Розв‘язати конгруенцію:

$$6x^{13} - 3x^{12} - 2x^{11} - 6x^3 + 3x^2 + 7x + 2 \equiv 0 (\bmod 11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 210$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$5 \cdot 6^{3x} + 56 \equiv 0 (\bmod 71)\,?$$

10. Розв‘язати конгруенцію:

$$8x^{17} + 3 \equiv 0 (\bmod 13)$$

Варіант 5

1. Чи проходить через точки з цілими координатами парабола

$$127y = x^2 - 17\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 13 \pmod{17}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -151 \pmod{512}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 79 \pmod{625}$$

5. Розв‘язати конгруенцію:

$$12x^2 + 8x - 15 \equiv 0 \pmod{47}$$

6. Розв‘язати конгруенцію:

$$x^2 + 9x - 2 \equiv 0 \pmod{25}$$

7. Розв‘язати конгруенцію:

$$3x^9 + x^8 + 2x^7 - 3x^2 + 2x + 4 \equiv 0 \pmod{7}$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=220$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$59 \cdot 7^{2x} + 52 \equiv 0 \pmod{73}\,?$$

10. Розв‘язати конгруенцію:

$$13x^4 + 16 \equiv 0 \pmod{17}$$

Варіант 6

1. Чи проходить через точки з цілими координатами парабола

$$367y = x^2 - 40?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 22 \pmod{29}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 153 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 8 \pmod{343}$$

5. Розв‘язати конгруенцію:

$$5x^2 + x + 4 \equiv 0 (\bmod 13)$$

6. Розв‘язати конгруенцію:

$$3x^2 - 8x - 9 \equiv 0 (\bmod 49)$$

7. Розв‘язати конгруенцію:

$$2x^8 + x^7 - 3x^6 + x^5 - 2x^4 - x^3 + 4x^2 + x + 1 \equiv 0 (\bmod 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 230$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$46 \cdot 13^{8x} + 51 \equiv 0 (\bmod 97)?$$

10. Розв‘язати конгруенцію:

$$5x^{12} + 28 \equiv 0 (\bmod 83)$$

Варіант 7

1. Чи проходить через точки з цілими координатами парабола

$$103y = x^2 - 30\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 10 \pmod{31}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 153 \pmod{256}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 22 \pmod{243}$$

5. Розв‘язати конгруенцію:

$$4x^2 - 11x - 3 \equiv 0 (\bmod 23)$$

6. Розв‘язати конгруенцію:

$$x^2 - 3x + 7 \equiv 0 (\bmod 25)$$

7. Розв‘язати конгруенцію:

$$x^{15} + 2x^{14} + 5x^{13} - x^3 - 2x^2 - 11x + 5 \equiv 0 (\bmod 13)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 120$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$17 \cdot 2^{7x} + 42 \equiv 0 (\bmod 83)\,?$$

10. Розв‘язати конгруенцію:

$$13x^7 + 24 \equiv 0 (\bmod 31)$$

Варіант 8

1. Чи проходить через точки з цілими координатами парабола

$$173y = x^2 - 37\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 5 \pmod{19}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 337 \pmod{512}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 352 \pmod{2197}$$

5. Розв‘язати конгруенцію:

$$3x^2 + x - 2 \equiv 0 (\mathrm{mod}\,17)$$

6. Розв‘язати конгруенцію:

$$3x^2 - 8x - 18 \equiv 0 (\mathrm{mod}\,121)$$

7. Розв‘язати конгруенцію:

$$x^{101} + 3x^{15} + x^{11} - 3x^5 + 9x^2 + 10x - 5 \equiv 0 (\mathrm{mod}\,11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\dfrac{a}{b}$, де $(a,b) = 1,\ b = 440$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$19 \cdot 20^{6x} + 13 \equiv 0 (\mathrm{mod}\,59)\,?$$

10. Розв‘язати конгруенцію:

$$18x^7 + 24 \equiv 0 (\mathrm{mod}\,31)$$

Варіант 9

1. Чи проходить через точки з цілими координатами парабола

$$131y = x^2 - 38?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 2 \pmod 7$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 33 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 101 \pmod{2197}$$

5. Розв‘язати конгруенцію:

$$3x^2 + 10x + 10 \equiv 0 \pmod{23}$$

6. Розв‘язати конгруенцію:

$$x^2 + 4x + 7 \equiv 0 \pmod{12}$$

7. Розв‘язати конгруенцію:

$$2x^{35} - 17x^{15} + 13x^8 - 3x^5 + 12x + 5 \equiv 0 \pmod{11}$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1$, $b=270$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$17 \cdot 11^{7x} + 22 \equiv 0 \pmod{37}?$$

10. Розв‘язати конгруенцію:

$$32x^4 + 14 \equiv 0 \pmod{53}$$

Варіант 10

1. Чи проходить через точки з цілими координатами парабола

$$379y = x^2 - 51?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 7 \pmod{19}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 329 \pmod{512}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 11 \pmod{343}$$

5. Розв‘язати конгруенцію:

$$5x^2 - 2x + 6 \equiv 0 (\mathrm{mod}\, 31)$$

6. Розв‘язати конгруенцію:

$$x^2 - 9x + 4 \equiv 0 (\mathrm{mod}\, 20)$$

7. Розв‘язати конгруенцію:

$$x^7 + x^6 + 2x^5 - 3x^4 - 4x^3 + 2x^2 + 3x + 2 \equiv 0 (\mathrm{mod}\, 11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 550$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$42 \cdot 8^{3x} + 22 \equiv 0 (\mathrm{mod}\, 47)?$$

10. Розв‘язати конгруенцію:

$$22x^{16} + 4 \equiv 0 (\mathrm{mod}\, 61)$$

Варіант 11

1. Чи проходить через точки з цілими координатами парабола

$$653y = x^2 - 47\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 28\left(\operatorname{mod} 31\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 113\left(\operatorname{mod} 256\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv -18\left(\operatorname{mod} 243\right)$$

5. Розв‘язати конгруенцію:

$$6x^2 + 14x - 19 \equiv 0(\operatorname{mod} 11)$$

6. Розв‘язати конгруенцію:

$$3x^2 - 2x + 5 \equiv 0(\operatorname{mod} 75)$$

7. Розв‘язати конгруенцію:

$$6x^{13} - 3x^{12} - 2x^{11} - 6x^3 + 3x^2 + 7x + 2 \equiv 0(\operatorname{mod} 11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 55$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$33 \cdot 3^{7x} + 26 \equiv 0(\operatorname{mod} 59)\,?$$

10. Розв‘язати конгруенцію:

$$8x^6 + 15 \equiv 0(\operatorname{mod} 31)$$

Варіант 12

1. Чи проходить через точки з цілими координатами парабола

$$151y = x^2 - 20\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 20 \pmod{31}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 177 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 15 \pmod{343}$$

5. Розв‘язати конгруенцію:

$$2x^2 - 17x + 8 \equiv 0 (\mathrm{mod}\, 19)$$

6. Розв‘язати конгруенцію:

$$x^2 + 16x + 4 \equiv 0 (\mathrm{mod}\, 21)$$

7. Розв‘язати конгруенцію:

$$x^6 - 3x^5 - 2x^4 - 2x^3 - 2x^2 + 3x - 2 \equiv 0 (\mathrm{mod}\, 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 505$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$11 \cdot 7^{5x} + 24 \equiv 0 (\mathrm{mod}\, 53)\,?$$

10. Розв‘язати конгруенцію:

$$27x^7 + 17 \equiv 0 (\mathrm{mod}\, 43)$$

Варіант 13

1. Чи проходить через точки з цілими координатами парабола

$$173y = x^2 - 26?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 7\left(\mathrm{mod}\,31\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 281\left(\mathrm{mod}\,512\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 51\left(\mathrm{mod}\,625\right)$$

5. Розв‘язати конгруенцію:

$$4x^2 - 18x - 13 \equiv 0(\mathrm{mod}\,13)$$

6. Розв‘язати конгруенцію:

$$x^2 + 8x + 12 \equiv 0(\mathrm{mod}\,45)$$

7. Розв‘язати конгруенцію:

$$4x^8 + 5x^7 - 3x^6 + x^5 - 3x^3 + x^2 + x - 5 \equiv 0(\mathrm{mod}\,7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\dfrac{a}{b}$, де $(a,b)=1,\ b=540$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$33 \cdot 3^{7x} + 26 \equiv 0(\mathrm{mod}\,59)?$$

10. Розв‘язати конгруенцію:

$$11x^{11} + 57 \equiv 0(\mathrm{mod}\,23)$$

Варіант 14

1. Чи проходить через точки з цілими координатами парабола

$$181y = x^2 - 15\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 3 \pmod{13}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 65 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 177 \pmod{243}$$

5. Розв‘язати конгруенцію:

$$3x^2 - 16x + 13 \equiv 0 (\bmod 19)$$

6. Розв‘язати конгруенцію:

$$3x^2 + x + 8 \equiv 0 (\bmod 20)$$

7. Розв‘язати конгруенцію:

$$x^{10} - 2x^7 - x^4 + 7x + 4 \equiv 0 (\bmod 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1$, $b=99$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$32 \cdot 3^{9x} + 17 \equiv 0 (\bmod 61)\,?$$

10. Розв‘язати конгруенцію:

$$20x^4 + 13 \equiv 0 (\bmod 29)$$

Варіант 15

1. Чи проходить через точки з цілими координатами парабола

$$479y = x^2 - 23\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 11\left(\mathrm{mod}\,19\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 137\left(\mathrm{mod}\,256\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 23\left(\mathrm{mod}\,2197\right)$$

5. Розв‘язати конгруенцію:

$$7x^2 + 24x - 9 \equiv 0(\mathrm{mod}\,11)$$

6. Розв‘язати конгруенцію:

$$x^2 - x = 12 \equiv 0(\mathrm{mod}\,81)$$

7. Розв‘язати конгруенцію:

$$x^9 + x^8 + x^7 - x^3 - x^2 - 5x - 3 \equiv 0(\mathrm{mod}\,7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 909$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$17 \cdot 10^{7x} + 19 \equiv 0(\mathrm{mod}\,83)\,?$$

10. Розв‘язати конгруенцію:

$$9x^5 + 14 \equiv 0(\mathrm{mod}\,31)$$

Варіант 16

1. Чи проходить через точки з цілими координатами парабола

$$419y = x^2 - 39?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 5\pmod{31}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -15\pmod{64}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 35\pmod{2197}$$

5. Розв‘язати конгруенцію:

$$2x^2 - 4x - 9 \equiv 0(\mathrm{mod}\,7)$$

6. Розв‘язати конгруенцію:

$$3x^2 - 2x + 9 \equiv 0(\mathrm{mod}\,125)$$

7. Розв‘язати конгруенцію:

$$9x^{20} + 7x^{15} - 4x^{10} + 46x^2 - 52x + 16 \equiv 0(\mathrm{mod}\,11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 990$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$31 \cdot 13^{4x} + 8 \equiv 0(\mathrm{mod}\,53)?$$

10. Розв‘язати конгруенцію:

$$14x^7 + 6 \equiv 0(\mathrm{mod}\,29)$$

Варіант 17

1. Чи проходить через точки з цілими координатами парабола

$$433y = x^2 - 47\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 12\left(\bmod 13\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -263\left(\bmod 512\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 8\left(\bmod 243\right)$$

5. Розв‘язати конгруенцію:

$$4x^2 + 2x - 3 \equiv 0 (\bmod 17)$$

6. Розв‘язати конгруенцію:

$$3x^2 + x + 5 \equiv 0 (\bmod 343)$$

7. Розв‘язати конгруенцію:

$$3x^8 + x^6 - x^4 + x^5 - 2x^3 + 4x^2 + x + 1 \equiv 0 (\bmod 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\dfrac{a}{b}$, де $(a,b) = 1$, $b = 740$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$20 \cdot 5^{6x} + 18 \equiv 0 (\bmod 59)\,?$$

10. Розв‘язати конгруенцію:

$$36x^3 + 37 \equiv 0 (\bmod 79)$$

Варіант 18

1. Чи проходить через точки з цілими координатами парабола

$$499y = x^2 - 46\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 1\pmod{7}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 73\pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 17\pmod{2197}$$

5. Розв‘язати конгруенцію:

$$5x^2 + 2x + 25 \equiv 0 (\bmod 7)$$

6. Розв‘язати конгруенцію:

$$x^2 - 6x + 8 \equiv 0 (\bmod 343)$$

7. Розв‘язати конгруенцію:

$$5x^7 + 3x^6 - 4x^5 + 3x^4 - 2x^3 + x^2 + x + 1 \equiv 0 (\bmod 11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=48$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$12\cdot 7^{5x} + 19 \equiv 0 (\bmod 53)\,?$$

10. Розв‘язати конгруенцію:

$$13x^7 + 4 \equiv 0 (\bmod 73)$$

Варіант 19

1. Чи проходить через точки з цілими координатами парабола

$$283y = x^2 - 90\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 19\left(\bmod 31\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -39\left(\bmod 64\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 18\left(\bmod 343\right)$$

5. Розв‘язати конгруенцію:

$$2x^2 - 3x + 6 \equiv 0 (\bmod 11)$$

6. Розв‘язати конгруенцію:

$$x^2 - 4x - 2 \equiv 0 (\bmod 125)$$

7. Розв‘язати конгруенцію:

$$3x^{33} + 16x^{14} + 13x^9 + 5x^2 + 3x - 1 \equiv 0 (\bmod 11)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 480$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$16 \cdot 5^{7x} + 9 \equiv 0 (\bmod 41)\,?$$

10. Розв‘язати конгруенцію:

$$33x^{13} + 17 \equiv 0 (\bmod 59)$$

Варіант 20

1. Чи проходить через точки з цілими координатами парабола

$$347y = x^2 - 13?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 5\left(\bmod 11\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 241\left(\bmod 512\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 31\left(\bmod 625\right)$$

5. Розв‘язати конгруенцію:

$$3x^2 - 7x + 4 \equiv 0 (\bmod 31)$$

6. Розв‘язати конгруенцію:

$$x^2 + 5x - 3 \equiv 0 (\bmod 27)$$

7. Розв‘язати конгруенцію:

$$x^{12} + x^{11} - 2x^8 + 3x^6 + 5x^4 - 3x^3 + 2x^2 - x + 5 \equiv 0 (\bmod 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=82$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$28 \cdot 8^{3x} + 17 \equiv 0 (\bmod 67)?$$

10. Розв‘язати конгруенцію:

$$28x^4 + 17 \equiv 0 (\bmod 53).$$

Варіант 21

1. Чи проходить через точки з цілими координатами парабола

$$379y = x^2 - 22\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 17\left(\mathrm{mod}\,19\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -47\left(\mathrm{mod}\,128\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 40\left(\mathrm{mod}\,2197\right)$$

5. Розв‘язати конгруенцію:

$$x^2 - 8x - 33 \equiv 0(\mathrm{mod}\,23)$$

6. Розв‘язати конгруенцію:

$$2x^2 + 5x - 3 \equiv 0(\mathrm{mod}\,44)$$

7. Розв‘язати конгруенцію:

$$x^7 + 3x^6 + x^5 - x^3 - 3x^2 - 4x + 4 \equiv 0(\mathrm{mod}\,5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 820$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$23 \cdot 8^{5x} + 17 \equiv 0(\mathrm{mod}\,67)\,?$$

10. Розв‘язати конгруенцію:

$$14x^{17} + 5 \equiv 0(\mathrm{mod}\,89)$$

Варіант 22

1. Чи проходить через точки з цілими координатами парабола

$$401y = x^2 - 35\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 8\left(\bmod 17\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 193\left(\bmod 256\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 22\left(\bmod 343\right)$$

5. Розв‘язати конгруенцію:

$$x^2 - 4x - 21 \equiv 0(\bmod 7)$$

6. Розв‘язати конгруенцію:

$$x^2 + 5x + 6 \equiv 0(\bmod 21)$$

7. Розв‘язати конгруенцію:

$$x^{10} +^{8} + x^7 - x^4 - x^2 + 4x - 3 \equiv 0(\bmod 7)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\dfrac{a}{b}$, де $(a,b)=1,\ b=135$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$15 \cdot 7^{4x} + 19 \equiv 0(\bmod 43)\,?$$

10. Розв‘язати конгруенцію:

$$22x^4 + 8 \equiv 0(\bmod 89)$$

Варіант 23

1. Чи проходить через точки з цілими координатами парабола

$$349y = x^2 - 22?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 10 \pmod{13}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 89 \pmod{128}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 24 \pmod{625}$$

5. Розв‘язати конгруенцію:

$$3x^2 - 5x - 2 \equiv 0 (\bmod 11)$$

6. Розв‘язати конгруенцію:

$$x^2 + 13x - 6 \equiv 0 (\bmod 441)$$

7. Розв‘язати конгруенцію:

$$x^7 + 2x^6 + x^5 - x^3 - 2x^2 - 4x + 2 \equiv 0 (\bmod 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1$, $b = 175$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$31 \cdot 7^{6x} + 6 \equiv 0 (\bmod 37)?$$

10. Розв‘язати конгруенцію:

$$8x^8 + 9 \equiv 0 (\bmod 17)$$

Варіант 24

1. Чи проходить через точки з цілими координатами парабола

$$373y = x^2 - 24\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 6\left(\bmod 19\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 33\left(\bmod 64\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 11\left(\bmod 243\right)$$

5. Розв‘язати конгруенцію:

$$2x^2 - 7x + 28 \equiv 0(\bmod 43)$$

6. Розв‘язати конгруенцію:

$$x^2 + 9x - 2 \equiv 0(\bmod 275)$$

7. Розв‘язати конгруенцію:

$$x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0(\bmod 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=225$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$14\cdot 6^{9x} + 52 \equiv 0(\bmod 67)\,?$$

10. Розв‘язати конгруенцію:

$$24x^3 + 7 \equiv 0(\bmod 29)$$

Варіант 25

1. Чи проходить через точки з цілими координатами парабола

$$197y = x^2 - 41?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 5\pmod{29}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 137\pmod{256}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 23\pmod{343}$$

5. Розв‘язати конгруенцію:

$$3x^2 - 8x + 44 \equiv 0(\mathrm{mod}\,47)$$

6. Розв‘язати конгруенцію:

$$x^2 + 3x - 13 \equiv 0(\mathrm{mod}\,15)$$

7. Розв‘язати конгруенцію:

$$x^5 - 7x^4 + 9x^2 - x + 13 \equiv 0(\mathrm{mod}\,3)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\dfrac{a}{b}$, де $(a,b) = 1,\ b = 45$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$61 \cdot 6^{11x} + 12 \equiv 0(\mathrm{mod}\,73)?$$

10. Розв‘язати конгруенцію:

$$71x^{11} + 27 \equiv 0(\mathrm{mod}\,97)$$

Варіант 26

1. Чи проходить через точки з цілими координатами парабола

$$271y = x^2 - 45?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 3\left(\bmod 11\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 97\left(\bmod 128\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 42\left(\bmod 2197\right)$$

5. Розв‘язати конгруенцію:

$$3x^2 + 5x - 7 \equiv 0(\bmod 29)$$

6. Розв‘язати конгруенцію:

$$x^2 + 9x - 1 \equiv 0(\bmod 63)$$

7. Розв‘язати конгруенцію:

$$x^7 - x^6 + 5x^2 - 3 \equiv 0(\bmod 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=264$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$35 \cdot 8^{4x} + 13 \equiv 0(\bmod 79)?$$

10. Розв‘язати конгруенцію:

$$45x^3 + 15 \equiv 0(\bmod 83)$$

Варіант 27

1. Чи проходить через точки з цілими координатами парабола

$$643y = x^2 - 10?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 2 \pmod{17}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 17 \pmod{64}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 19 \pmod{625}$$

5. Розв‘язати конгруенцію:

$$5x^2 - 12x - 7 \equiv 0 (\mathrm{mod}\, 23)$$

6. Розв‘язати конгруенцію:

$$3x^2 + 2x - 6 \equiv 0 (\mathrm{mod}\, 45)$$

7. Розв‘язати конгруенцію:

$$x^5 - 2x^3 + x^2 - 2 \equiv 0 (\mathrm{mod}\, 3)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 1650$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$41 \cdot 7^{12x} + 56 \equiv 0 (\mathrm{mod}\, 89)?$$

10. Розв‘язати конгруенцію:

$$9x^3 + 18 \equiv 0 (\mathrm{mod}\, 43)$$

Варіант 28

1. Чи проходить через точки з цілими координатами парабола

$$241y = x^2 - 10\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 6\left(\operatorname{mod} 29\right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 105\left(\operatorname{mod} 512\right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 55\left(\operatorname{mod} 2197\right)$$

5. Розв‘язати конгруенцію:

$$8x^2 - 5x - 4 \equiv 0(\operatorname{mod} 53)$$

6. Розв‘язати конгруенцію:

$$5x^2 - 2x + 5 \equiv 0(\operatorname{mod} 24)$$

7. Розв‘язати конгруенцію:

$$3x^7 - 2x^6 + 2x^2 + 13 \equiv 0(\operatorname{mod} 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 4500$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$15 \cdot 8^{4x} + 16 \equiv 0(\operatorname{mod} 31)\,?$$

10. Розв‘язати конгруенцію:

$$14x^7 + 26 \equiv 0(\operatorname{mod} 47)$$

Варіант 29

1. Чи проходить через точки з цілими координатами парабола

$$233y = x^2 - 28\,?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 16 \pmod{29}$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv 57 \pmod{256}$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 18 \pmod{243}$$

5. Розв‘язати конгруенцію:

$$5x^2 - 11x + 16 \equiv 0 (\operatorname{mod} 41)$$

6. Розв‘язати конгруенцію:

$$x^2 + 7x - 8 \equiv 0 (\operatorname{mod} 25)$$

7. Розв‘язати конгруенцію:

$$4x^7 - 2x^3 + 8 \equiv 0 (\operatorname{mod} 5)$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=3300$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$17 \cdot 7^{3x} + 62 \equiv 0 (\operatorname{mod} 79)\,?$$

10. Розв‘язати конгруенцію:

$$16x^6 + 13 \equiv 0 (\operatorname{mod} 17)$$

Варіант 30

1. Чи проходить через точки з цілими координатами парабола

$$229y = x^2 - 74?$$

2. Розв‘язати конгруенцію:

$$x^2 \equiv 15 \left(\mathrm{mod}\, 17 \right)$$

3. Розв‘язати конгруенцію:

$$x^2 \equiv -55 \left(\mathrm{mod}\, 64 \right)$$

4. Розв‘язати конгруенцію:

$$x^2 \equiv 21 \left(\mathrm{mod}\, 625 \right)$$

5. Розв‘язати конгруенцію:

$$5x^2 - 4x - 1 \equiv 0 (\mathrm{mod}\, 143)$$

6. Розв‘язати конгруенцію:

$$2x^2 + 4x - 3 \equiv 0 (\mathrm{mod}\, 45)$$

7. Розв‘язати конгруенцію:

$$x^{15} - 2x^7 + 3x^3 + 2x^2 - 7 \equiv 0 (\mathrm{mod}\, 11).$$

8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b) = 1,\ b = 2200$. Навести приклад.

9. При якому найменшому натуральному x виконується рівність

$$18 \cdot 9^{7x} + 57 \equiv 0 (\mathrm{mod}\, 73)?$$

10. Розв‘язати конгруенцію:

$$21x^{11} + 19 \equiv 0 (\mathrm{mod}\, 29)$$

МЕТОДИЧНІ ВКАЗІВКИ ДО РОЗВ'ЯЗАННЯ ЗАВДАНЬ З ТЕМИ:

«Конгруенції вищих порядків»

Завдання 1. Чи проходить через точки з цілими координатами парабола $643y = x^2 - 904$?

Розв'язання. Знайдемо цілі значення x при яких $x^2 - 904$ націло ділиться на 643. Тобто потрібно з'ясувати чи матиме розв'язки конгруенція $x^2 \equiv 904 \pmod{643}$. За властивостями конгруенцій $x^2 \equiv 904 \pmod{643} \equiv 261 \pmod{643}$.

Конгруенція $x^2 \equiv a \pmod{p}$; $(a, p) = 1$ має два розв'язки або не має жодного залежно від того, чи буде число a квадратичним лишком або нелишком за модулем p, тобто чи буде відповідно $\left(\dfrac{a}{p}\right) = +1$ або $\left(\dfrac{a}{p}\right) = -1$.

Знайдемо символ Лежандра $\left(\dfrac{261}{643}\right)$. Оскільки $261 = 3^2 \cdot 29$, а 643 – просте число, то, згідно з властивістю символа Лежандра

$$\left(\frac{261}{643}\right) = \left(\frac{3^2 \cdot 29}{643}\right) = \left(\frac{29}{643}\right).$$

Обчислимо символ Лежандра $\left(\dfrac{29}{643}\right)$. Оскільки 29 і 643 – різні прості непарні числа, то внаслідок закону взаємності дістаємо

$$\left(\frac{29}{643}\right)=\left(\frac{643}{29}\right)\cdot(-1)^{\frac{643-1}{2}\cdot\frac{29-1}{2}}=\left(\frac{643}{29}\right).$$

Застосовуючи далі властивості символу Лежандра маємо

$$\left(\frac{643}{29}\right)=\left(\frac{5}{29}\right)=\left(\frac{29}{5}\right)\cdot(-1)^{\frac{29-1}{2}\cdot\frac{5-1}{2}}=\left(\frac{4}{5}\right)=\left(\frac{2^2}{5}\right)=1.$$

Дана конгруенція має два розв‘язки.

Отже, дана парабола проходить через дві точки з цілими координатами.

Відповідь: дана парабола проходить через дві точки з цілими координатами.

Завдання 2. Розв‘язати конгруенцію $x^2 \equiv 13 \pmod{23}$

Розв'язання. Розглянемо найпростішу квадратну двочленну конгруенцію

$$x^2 \equiv a \pmod{p},\ (a, p)=1,\ p>2.$$

Знайдемо всі квадратичні лишки і нелишки за модулем $p=23$. Множина чисел

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

являє собою ЗСЛ за модулем $p=23$. Якщо цю множину чисел розглянути з точки зору можливості існування розв'язків квадратної конгруенції, то частина цих чисел множини є квадратичними лишками, а частина їх – квадратичними нелишками.

Враховуючи, що

$$\begin{array}{lll}
1^2 \equiv 1(\bmod 23), & 9^2 \equiv 12(\bmod 23), & 16^2 \equiv 3(\bmod 23) \\
2^2 \equiv 4(\bmod 23), & 10^2 \equiv 8(\bmod 23), & 17^2 \equiv 13(\bmod 23), \\
3^2 \equiv 9(\bmod 23), & 11^2 \equiv 6(\bmod 23), & 18^2 \equiv 2(\bmod 23), \\
4^2 \equiv 16(\bmod 23), & 12^2 \equiv 6(\bmod 23), & 19^2 \equiv 16(\bmod 23), \\
5^2 \equiv 2(\bmod 23), & 13^2 \equiv 8(\bmod 23), & 20^2 \equiv 9(\bmod 23), \\
6^2 \equiv 13(\bmod 23), & 14^2 \equiv 12(\bmod 23), & 21^2 \equiv 4(\bmod 23), \\
7^2 \equiv 3(\bmod 23),\ ' & 15^2 \equiv 18(\bmod 23), & 22^2 \equiv 1(\bmod 23). \\
8^2 \equiv 18(\bmod 23), & &
\end{array}$$

Бачимо, що квадратичними лишками за модулем 23 є числа: $1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$, а числа $5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22$ є квадратичними нелишками за модулем $p = 23$.

Відповідно до сказаного конгруенцію $x^2 \equiv 13(\bmod 23)$ задовольняють числа $x = 6$ і $x = 17$, і тому вона має два розв'язки: $K_6^{(23)}$ і $K_{17}^{(23)}$

Відповідь: $x \equiv 6(\bmod 23)$, $x \equiv 13(\bmod 23)$

Завдання 3. Розв‘язати конгруенцію $x^2 \equiv 681(\bmod 1024)$

Розв‘язання. Для конгруенції $x^2 \equiv a\left(\bmod 2^{\alpha}\right)$, $(a, 2) = 1$, необхідними умовами існування розв'язків є $a \equiv 1(\bmod 4)$ при $\alpha = 2$, $a \equiv 1(\bmod 8)$ при $\alpha \geq 3$.

Якщо ці умови виконуються, то існує один розв'язок при $\alpha = 1$; два розв'язки при $\alpha = 2$ і чотири розв'язки при $\alpha \geq 3$.

У даному прикладі маємо:

$$a = 681 \equiv 1(\bmod 8),$$

отже, розв‘язків буде чотири. Для їх знаходження розглянемо конгруенції

$$x^2 \equiv 681 \equiv 1 \pmod{8},$$

$$x^2 \equiv 681 \equiv 9 \pmod{16},$$

$$x^2 \equiv 681 \equiv 9 \pmod{32},$$

$$x^2 \equiv 681 \equiv 41 \pmod{64},$$

$$x^2 \equiv 681 \equiv 41 \pmod{128},$$

$$x^2 \equiv 681 \equiv 169 \pmod{256},$$

$$x^2 \equiv 681 \equiv 169 \pmod{512},$$

$$x^2 \equiv 681 \pmod{1024}.$$

Розв‘язки першої конгруенції будуть 1, 3, 5, 7; з них, наприклад, 3 задовольняє другу конгруенцію. Решта розв‘язків другої конгруенції є: $3+2^3$, -3, $-3-2^3$, тобто розв‘язки другої конгруенції будуть 3, 5, 11, 13. З них, наприклад, 3 задовольняє третю конгруенцію; решта її розв‘язків буде: $3+2^4$, -3, $-3-2^4$, тобто 3, 13, 19, 29 є всі розв‘язки третьої конгруенції. З цих розв‘язків, наприклад, 13 задовольняє четверту конгруенцію, а решта її розв‘язків буде: $13+2^5$, -13, $-13-2^5$ Отже, 13, 19, 45, 51 будуть розв‘язками четвертої конгруенції. Далі, по аналогії з попереднім розв‘язуванням, знаходимо розв‘язки п‘ятої, шостої, сьомої та восьмої конгруенцій.

Для конгруенції $x^2 \equiv 681 \equiv 41 \pmod{128}$ розв‘язками будуть:

$13,\ 13+2^6,\ -13,\ -13-2^6,$

тобто числа 13, 51, 77, 115 становитимуть всі розв‘язки конгруенції $x^2 \equiv 681 \equiv 41 \pmod{128}$.

Для конгруенції $x^2 \equiv 681 \equiv 169 \pmod{256}$ розв‘язками будуть 13, $13+2^7$, -13, $-13-2^7$, тобто числа 13, 115, 141, 243 є розв‘язками конгруенції $x^2 \equiv 681 \equiv 169 \pmod{256}$.

Для конгруенції $x^2 \equiv 681 \equiv 169 \pmod{512}$ розв‘язками будуть 13, $13+2^8$, -13, $-13-2^8$, тобто числа 13, 243, 269, 499 є розв‘язками конгруенції $x^2 \equiv 681 \equiv 169 \pmod{512}$.

Для конгруенції $x^2 \equiv 681 \pmod{1024}$ розв‘язками будуть 243, $243+2^9$, -243, $-243-2^9$, тобто числа 243, 269, 755, 781 є розв‘язками конгруенції $x^2 \equiv 681 \pmod{1024}$.

Отже, маємо всі розв‘язки даної конгруенції:

$$x \equiv 243, 269, 755, 781 \pmod{1024}.$$

Зауваження. Дану конгруенцію не обов‘язково було починати розв‘язувати з конгруенції $x^2 \equiv 681 \equiv 1 \pmod 8$; краще починати з конгруенції за модулем 2^α, для якої нам відомо хоч один розв‘язок x_α, решта три будуть:

$$-x_\alpha,\ x_\alpha + 2^{\alpha-1},\ -x_\alpha - 2^{\alpha-1}.$$

Відповідь: $x \equiv 243, 269, 755, 781 \pmod{1024}$.

Завдання 4. Розв‘язати конгруенцію $x^2 \equiv 3 \pmod{11^3}$.

Розв‘язання. Якщо x_0 задовольняє конгруенцію за простим модулем $p > 2$: $x^2 \equiv a \pmod p$, де $p \overline{\vdots}\, a$,

$$\left.\begin{array}{l} P_k = x_0^k + C_k^2 x_0^{k-2} a + C_k^4 x_0^{k-4} a^2 + \ldots \\ Q_k = C_k^1 x_0^{k-1} + C_k^3 x_0^{k-3} a + C_k^5 x_0^{k-5} a^2 + \ldots\ (k \ge 1) \end{array}\right\},$$

то $p \,\overline{\vdots}\, Q_k$ і розв‘язок конгруенції

$$x^2 \equiv a\left(\operatorname{mod} p^k\right)$$

має вигляд $x \equiv \pm P_k y_k \left(\operatorname{mod} p^k\right)$, де y_k – розв‘язок конгруенції $Q_k y \equiv 1\left(\operatorname{mod} p^k\right)$.

Конгруенція $x^2 \equiv 3(\operatorname{mod} 11)$ має розв‘язок $x \equiv 5(\operatorname{mod} 11)$.

Взявши $x_0 = 5$, $a = 3$, обчислимо:

$$P_3 = 5^3 + 3\cdot 5\cdot 3 = 170,\ Q_3 = 3\cdot 5^2 + 3 = 78.$$

Розв‘язуючи конгруенцію $78y \equiv 1(\operatorname{mod} 1331)$, знаходимо $y_3 = 529$, тому $x \equiv \pm 170\cdot 529 \equiv \pm 753(\operatorname{mod} 1331)$.

***Відповідь**:* $x \equiv \pm 753(\operatorname{mod} 1331)$.

Завдання 5. Розв‘язати конгруенцію $5x^2 - 9x - 2 \equiv 0(\operatorname{mod} 43)$.

Розв‘язання. Для простого модуля старший коефіцієнт взаємно простий з ним. Тоді процес зведення заданої конгруенції до двочленної можна скоротити і навіть залишити модуль незмінним. Так як $(4a, m) = (4\cdot 5, 43) = 1$, то модуль конгруенції можна не множити на $4a$. Помножаючи обидві частини конгруенції на 20 за модулем 43, дістаємо

$$100x^2 - 180x - 40 \equiv 0(\operatorname{mod} 43),$$

або

$$(10x - 9)^2 - 121 \equiv 0(\operatorname{mod} 43),$$

$$(10x - 9)^2 \equiv 121(\operatorname{mod} 43).$$

Позначимо $10x-9=y$ і тоді буде $y^2 \equiv 121 \pmod{43}$. Остання конгруенція має два розв‘язки: $y \equiv 11 \pmod{43}$, $y \equiv -11 \pmod{43}$.

Отже, квадратна конгруенція $5x^2-9x-2 \equiv 0 \pmod{43}$ має розв‘язки тоді, коли мають розв‘язки конгруенції: $10x-9 \equiv 11 \pmod{43}$ і $10x-9 \equiv -11 \pmod{43}$. Розв‘язуючи дві останні конгруенції, матимемо:

$$x \equiv 2 \pmod{43} \text{ і } x \equiv 17 \pmod{43}.$$

Тоді задана конгруенція має розв‘язки $x \equiv 2;17 \pmod{43}$.

Відповідь: $x \equiv 2;17 \pmod{43}$

Завдання 6. Розв'язати конгруенцію $x^2+5x+4 \equiv 0 \pmod{22}$.

Розв‘язання. Конгруенцію $x^2+5x+4 \equiv 0 \pmod{22}$ замінюємо системою за простими модулями

$$\begin{cases} x^2+5x+4 \equiv 0 \pmod{2}, \\ x^2+5x+4 \equiv 0 \pmod{11}. \end{cases}$$

Спочатку розв‘язуємо конгруенцію $x^2+5x+4 \equiv 0 \pmod{2}$. Застосуємо елементарні перетворення над конгруенціями до виразу зліва $x^2+5x+4 \equiv x^2+x \equiv 0 \pmod{2}$. Конгруенція $x^2+x \equiv 0 \pmod{2}$ має розв‘язки $x \equiv 0;1 \pmod{2}$.

Далі розв‘язуємо конгруенцію $x^2+5x+4 \equiv 0 \pmod{11}$. Помножаючи обидві частини конгруенції на 4 за модулем 11, дістаємо

$$4x^2+20x+16 \equiv 0 \pmod{11},$$

$$(2x+5)^2-9 \equiv 0 \pmod{11},$$

$$(2x+5)^2 \equiv 9 \pmod{11}.$$

$$x \equiv -4;\ -1 \pmod{11}.$$

Тепер складаємо системи конгруенцій за модулями 2 і 11.

$$\text{а)}\begin{cases} x \equiv \ \ 0 \pmod 2, \\ x \equiv -4 \pmod{11}. \end{cases} \text{б)}\begin{cases} x \equiv \ \ 0 \pmod 2, \\ x \equiv -1 \pmod{11}. \end{cases}$$

$$\text{в)}\begin{cases} x \equiv \ \ 1 \pmod 2, \\ x \equiv -4 \pmod{11}. \end{cases} \text{г)}\begin{cases} x \equiv \ \ 1 \pmod 2, \\ x \equiv -1 \pmod{11}. \end{cases}$$

Розв‘яжемо систему а): $x = 0 + 2t_1 = 2t_1$, $2t_1 \equiv -4 \pmod{11}$, $t_1 \equiv -2 \pmod{11}$, $t_1 = -2 + 11t,\ t \in Z$. Отже, $x = 2t_1 = 2(-2+11t) = -4 + 22t,\ t \in Z$.

Система конгруенцій б) має розв‘язок: $x = 0 + 2t_1 = 2t_1$, $2t_1 \equiv -1 \pmod{11}$, $2t_1 \equiv -1 + 11 \equiv 10 \pmod{11}$, $t_1 \equiv 5 \pmod{11}$, $t_1 = 5 + 11t,\ t \in Z$. Отже, $x = 2t_1 = 2(5+11t) = 10 + 22t,\ t \in Z$.

Розмірковуючи аналогічно, знаходимо розв‘язки систем в) $x = 7 + 22t$, $t \in Z$ і г) $x = -1 + 22t$, $t \in Z$.

Відповідь: $x \equiv -4;\ -1;\ 7;\ 10 \pmod{22}$.

Завдання 7. а) Розв'язати конгруенцію

$$f(x) = x^4 + 3x^3 + 2x + 6 \equiv 0 \pmod{63}.$$

Розв‘язання. Маємо: $63 = 3^2 \cdot 7$; тому така конгруенція еквівалентна системі конгруенцій:

$$\begin{cases} f(x) \equiv 0 \pmod{3^2}, \\ f(x) \equiv 0 \pmod 7. \end{cases}$$

Розв'язуємо окремо кожну з конгруенцій. Безпосереднім випробуванням переконуємось, що розв'язком конгруенції

$$f(x) \equiv 0 \pmod 7$$

буде $x \equiv 4 \pmod 7$. Тепер розв'язуємо конгруенцію

$$f(x) \equiv 0 \left(\bmod 3^2\right).$$

Для цього спочатку треба розв'язати конгруенцію $f(x) \equiv 0 \pmod 3$, яку можна переписати так:

$$x^4 + 2x \equiv 0 \pmod 3.$$

Ця конгруенція має, очевидно, розв'язки: $x \equiv 0, 1 \pmod 3$. З розв'язку $x \equiv 0 \pmod 3$ дістанемо, що $x = 3t_1$, де t_1 – ціле. Підставляючи це значення x в конгруенцію

$$f(x) \equiv 0 \pmod 9,$$

маємо

$$6 + 3t_1 \cdot 2 \equiv 0 \pmod 9;$$

тут $f(0) = 6,\ f'(0) = 2$; або, скорочуючи обидві частини конгруенції і модуль на 3, дістанемо: $2 + 2t_1 \equiv 0 \pmod 3$, звідки $t_1 \equiv 2 \pmod 3$, $t_1 = 2 + 3t$. Отже,

$$x = 3t_1 = 6 + 9t,$$

або

$$x \equiv 6 \pmod 9$$

буде розв'язком конгруенції $f(x) \equiv 0 \pmod 9$.

Аналогічно шукатимемо інший розв'язок конгруенції $f(x) \equiv 0 \pmod{9}$. Маємо: $x = 1 + 3t_1'$. Підставляючи в конгруенцію і розкладаючи в ряд Тейлора за степенями $x - 1 = 3t_1'$, дістанемо:

$$12 + 3t_1' \cdot 15 \equiv 0 \pmod{9}.$$

Тут $f'(1) = 15$ ділиться на 3, але $f(1) = 12$ не ділиться на 3^2 і знайдена конгруенція відносно t_1' розв'язків не має, отже, конгруенція $f(x) \equiv 0 \pmod{9}$ не має розв'язків для $x = 1 + 3t_1'$, або для $x \equiv 1 \pmod{3}$.

Отже, конгруенція $f(x) \equiv 0 \pmod{7}$ має один розв'язок $x \equiv 4 \pmod{7}$ і конгруенція $f(x) \equiv 0 \pmod{9}$ також має один розв'язок $x \equiv 6 \pmod{9}$.

Розв'язуючи тепер спільно конгруенції $x \equiv 4 \pmod{7}$ і $x \equiv 6 \pmod{9}$, дістанемо їхній спільний розв'язок:

$$x \equiv 60 \equiv -3 \pmod{63}.$$

Це і буде єдиним розв'язком цієї конгруенції.

Відповідь: $x \equiv -3 \pmod{63}$

б) Розв‘язати конгруенцію

$$x^{10} + x^8 + x^7 - x^4 - x^2 + 4x - 3 \equiv 0 \pmod{7}.$$

Розв‘язання. Замінимо цю конгруенцію еквівалентною їй конгруенцією степеня не вище 6 за тим самим модулем 7. Поділимо $f(x)$ на $x^7 - x$. Дістанемо

$$f(x) = (x^7 - x)(x^3 + x + 1) + 5x - 3.$$

Розв‘яжемо конгруенцію $5x-3\equiv 0(\bmod 7)$. Штучним способом знаходимо:

$$5x\equiv 3(\bmod 7),$$

$$5x\equiv 3+7(\bmod 7),$$

$$x\equiv 2(\bmod 7).$$

Отже, дана конгруенція має єдиний розв‘язок $x\equiv 2(\bmod 7)$.

Зауваження. Замість того, щоб ділити $f(x)$ на x^p-x, можна було б замінити x^s $(p-1\le s\le n)$ на x^r, де $r-$ остача від ділення s на $p-1$, причому, якщо s ділиться на $p-1$, то покладемо $r=p-1$.

Відповідь: $x\equiv 2(\bmod 7)$.

в) Розв‘язати конгруенцію

$$4x^9+3x^8-5x^7-4x^3-3x^2+9x-3\equiv 0(\bmod 7).$$

Розв’язання. Так як степінь многочлена $f(x)$ більший модуля, застосувавши вище вказане зауваження, одержимо: $x^9\equiv x^3(\bmod 7)$, $x^8\equiv x^2(\bmod 7)$, $x^7\equiv x(\bmod 7)$. Тоді дана конгруенція буде еквівалентна такій:

$$4x^3+3x^2-5x-4x^3-3x^2+2x-3\equiv 0(\bmod 7),$$

$$-3x-3\equiv 0(\bmod 7),$$

$$-x\equiv 1(\bmod 7),$$

$$x\equiv 6(\bmod 7).$$

Отже, розв‘язок даної конгруенції $x\in K_6^{(7)}$.

Завдання 8. Вказати число цифр у періоді та число цифр до періоду в мішаному періодичному дробі $\frac{a}{b}$, де $(a,b)=1,\ b=140.$

Розв'язання. Відомо, що якщо $\frac{a}{b}$ – нескоротний дріб і $b=2^{\alpha}5^{\beta}\cdot b_1$, де $(b_1,10)=1$, то цей дріб перетворюється у мішаний періодичний десятковий дріб; число цифр у періоді дробу дорівнює δ, де δ – показник, якому належить 10 за модулем b_1; число цифр до періоду дорівнює γ; де γ – найбільше з чисел α та β .

За умовою задачі $b=140=2^2\cdot5\cdot7$, маємо $\gamma=2$. Знайдемо δ, тобто показник, до якого належить 10 за модулем 7. Маємо: $\varphi(7)=6$, можливі значення δ шукаємо серед чисел $1,2,3,6$; $10^1\equiv3, 10^2\equiv9, 10^3\equiv-1, 10^6\equiv1(\bmod 7)$. Отже, $\delta=6$.

Зауваження: δ можна знайти ще й так: ділимо 9 на b_1, потім 99 на b_1 і т.д., поки не дістанемо в остачі нуль. Число дев'яток у цьому діленні, а отже, й число цифр частки, дорівнюватимуть шуканому показнику δ.

Таким чином усі дроби виду $\frac{a}{140}$, де $(a,140)=1$, перетворюються в мішані періодичні дроби з числом цифр у періоді, яке дорівнює 6, і з числом цифр до періоду, яке дорівнює 2. Так, наприклад, безпосередньо переконуємося, що $\frac{123}{140}=0,87(857142)$.

Відповідь: число цифр у періоді рівне 6; число цифр до періоду рівне 2.

Завдання 9. При якому найменшому натуральному x виконується рівність $8\cdot 7^x+4\equiv 0\pmod{83}$.

Розв'язання. Перетворимо вираз, який стоїть в лівій частині конгруенції за властивостями конгруенцій.

$$8\cdot 7^x\equiv -4\pmod{83},$$

$$8\cdot 7^x\equiv 79\pmod{83}$$

Візьмемо індекси від обох частин конгруенції

$$\text{ind}8+x\text{ind}7\equiv \text{ind}79\pmod{82}.$$

За таблицями індексів (Додаток 2) маємо

$$\text{ind}8=3,\ \text{ind}7=8, \text{ind}79=43$$

і тому

$$3+8x\equiv 43\pmod{82},$$

$$8x\equiv 40\pmod{82},\ (8,82)=2.$$

Оскільки 40 ділиться на 2, то конгруенція має два розв'язки.

$$x\equiv 5,46\pmod{82}.$$

Отже, найменшим натуральним розв'язком даної конгруенції є число 5.

Відповідь: 5.

Завдання 10. Розв'язати конгруенцію $7x^6-94\equiv 0\pmod{83}$.

Розв'язання. Перетворимо вираз, який стоїть в лівій частині конгруенції за властивостями конгруенцій.

$$7x^6\equiv 11\pmod{83}.$$

Візьмемо індекси від обох частин конгруенції

$$\mathrm{ind}7+6\mathrm{ind}x \equiv \mathrm{ind}11 \pmod{82}.$$

За таблицями індексів (Додаток 2) маємо

$$\mathrm{ind}7=8,\ \mathrm{ind}11=24$$

і тому

$$8+6\mathrm{ind}x \equiv 24 \pmod{82},$$

$$6\mathrm{ind}x \equiv 16 \pmod{82},\ (6,82)=2.$$

Оскільки 24 ділиться на 2, то конгруенція має два розв’язки.

$$\mathrm{ind}x \equiv 30, 71 \pmod{82}.$$

Виконавши потенціювання останньої конгруенції, одержуємо

$$x \equiv 40, 43 \pmod{83}.$$

Відповідь: $x \equiv 40, 43 \pmod{83}$.

ТЕСТОВІ ПИТАННЯ

1. Числа a і b називаються конгруентними за модулем m, якщо

a) остачі при діленні їх на число m рівні між собою
b) остачі при діленні їх на число m нерівні між собою
c) якщо їх добуток кратний числу m
d) якщо $a+b$ ділилася на m

2. Яка необхідна і достатня умова конгруентності двох чисел за модулем m?

a) різниця $a-b$ ділилася на m
b) добуток ab ділилася на m
c) сума $a+b$ ділилася на m
d) кожне з чисел ділилася на m

3. Обрати невірне твердження:

a) конгруенції за тим самим модулем можна почлено додавати.
b) конгруенції за тим самим модулем можна почлено віднімати.
c) конгруенції за тим самим модулем можна почлено множити.
d) до однієї з частин конгруенції можна додати довільне ціле число

4. Обрати вірне твердження:

a) з однієї частини конгруенції можна переносити доданок з протилежним знаком
b) будь-яку частину конгруенції можна помножити на довільне ціле число
c) до будь-якої частини конгруенції можна додати або відняти довільне ціле число
d) обидві частини конгруенції можна поділити на їх спільний дільник d

5. Якщо конгруенція $a \equiv b \pmod{m}$ має місце за кількома модулями, то вона має місце і за модулем, який дорівнює

a) спільному найменшому кратному цих модулів
b) спільному найбільшому дільнику цих модулів
c) добутку цих модулів
d) різниці цих модулів

6. Якщо p – просте число, а k – натуральне число, то

a) $\varphi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right)$

b) $\varphi\left(p^k\right) = p^k\left(1 + \frac{1}{p}\right)$

c) $\varphi\left(p^k\right) = p\left(1 - \frac{1}{p}\right)$

d) $\varphi\left(p^k\right) = p$

7. Виберіть твердження, яке є визначенням функції Ейлера:

a) Функцією Ейлера $\varphi(m)$ називається функція, визначена на множині натуральних чисел; значення $\varphi(m)$ є кількість невід‘ємних чисел, більших за m і взаємно простих з m;

b) Функцією Ейлера $\varphi(m)$ називається функція, визначена на множині натуральних чисел; значення $\varphi(m)$ є кількість додатних чисел, взаємно простих з m;

c) Функцією Ейлера $\varphi(m)$ називається функція, визначена на множині натуральних чисел; значення $\varphi(m)$ є кількість натуральних чисел, менших за m і взаємно простих з m;

d) Функцією Ейлера $\varphi(m)$ називається функція, визначена на множині цілих чисел; значення $\varphi(m)$ є кількість невід‘ємних чисел, менших за m і взаємно простих з m.

8. Зведена система лишків за модулем 8 включає класи:

a) $K_0^{(8)}, K_2^{(8)}, K_4^{(8)}, K_6^{(8)}$

b) $K_0^{(8)}, K_1^{(8)}, K_2^{(8)}, K_3^{(8)}, K_4^{(8)}, K_5^{(8)}, K_6^{(8)}, K_7^{(8)}$

c) $K_1^{(8)}, K_3^{(8)}, K_5^{(8)}, K_7^{(8)}$

d) $K_0^{(8)}, K_1^{(8)}$

9. Оберіть невірне твердження

a) Якщо одна частина конгруенції і модуль ділиться на число d, то й друга частина конгруенція ділиться на це число.

b) Якщо $a \equiv b(\operatorname{mod} m)$, то НСД чисел a, m і b, m рівні між собою.

c) Якщо конгруенція $a \equiv b \pmod{m}$ має місце за кількома модулями, то вона має місце і за модулем, який дорівнює сумі цих модулів.
d) Якщо конгруенція має місце за модулем m, число d – дільник m, то вона має місце і за модулем d.

10. $K_a^{(m)}$ **називається взаємно простим з модулем** m**, якщо**

a) $(a,m) = a$
b) $(a,m) = m$
c) $(a,m) = p$, де p просте число
d) $(a,m) = 1$

11. Обрати операцію, яка порушить множину розв‘язків конгруенцій:

a) множення обох частин конгруенції і модуля на те саме додатне число
b) додавання до обох частин конгруенції будь-якого многочлені з цілими коефіцієнтами
c) додавання до однієї з частин конгруенції многочлена з коефіцієнтами, кратними нулю
d) множення однієї з частин конгруенції на число, кратне модулю

12. Конгруенція виду $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}$**, де в лівій частині міститься многочлен з цілими коефіцієнтами називається**

a) конгруенцією з одним невідомим за модулем m
b) конгруенцією з одним невідомим за модулем n
c) конгруенцією з m невідомим за модулем n
d) конгруенцією з n невідомим за модулем m

13. Розв'язком конгруенції $f(x) \equiv 0 \pmod{m}$ **називається**

a) клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію
b) числа взаємнопрості з m, кожне з яких задовольняє цю конгруенцію
c) числа кратні m, кожне з яких задовольняє цю конгруенцію
d) коефіцієнти $f(x)$

14. Якщо $(a,m)=1$, то конгруенція $ax \equiv b \pmod m$

a) має єдиний розв‘язок
b) має безліч розв’язки
c) не має жодного розв’язку
d) має m розв’язків

15. Якщо $(a,m)=d>1$ і $b \vdots d$, то конгруенція $ax \equiv b \pmod m$

a) має d розв‘язків
b) має безліч розв’язки
c) не має жодного розв’язку
d) має єдиний розв‘язок

16. Якщо $(a,m)=d>0$ і число b не ділиться на d, то конгруенція $ax \equiv b \pmod m$

a) не має розв‘язків
b) має d розв‘язків
c) має безліч розв’язки
d) має єдиний розв‘язок

17. Обрати пропущену частину виразу: «Якщо модулі $m_1, m_2, \ldots, m_k$ попарно взаємно прості і система $\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k \pmod{m_k}. \end{cases}$ **сумісна, то вона має єдиний розв'язок за модулем M, що дорівнює ______________________________ чисел $m_1, m_2, \ldots, m_k$.»**

a) найменшому спільному кратному
b) найменшому з чисел
c) найбільшому з чисел
d) добутку

18. Якщо модулі $m_1, m_2, \ldots, m_k$ попарно взаємно прості, то система конгруенцій $\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k \pmod{m_k}. \end{cases}$

a) має єдиний розв'язок

b) не має розв‘язків
c) має d розв‘язків
d) має безліч розв’язки

19. Розв’язуючи конгруенцію $ax \equiv b \pmod{m}$, де $(a,m)=1$, способом Ейлера потрібно помножити цю конгруенцію на

a) $a^{\varphi(m)-1}$
b) $a^{\varphi(m)}$
c) $a^{\varphi(m)+1}$
d) $\varphi(m)$

20. Розв’язуючи конгруенцію $ax \equiv b \pmod{m}$, де $(a,m)=1$ за допомогою неперервних дробів в ланцюговий дріб розкладаємо

a) $\frac{m}{a}$
b) $\frac{m}{b}$
c) $\frac{a}{m}$
d) $\frac{b}{m}$

21. Конгруенція *n*-го степеня за простим модулем може мати

a) не більш як n розв'язків
b) не більш як $2n$ розв'язків
c) тільки один розвязок
d) не менше як n розв'язків

22. Якщо конгруенція $x^n \equiv a \pmod{p}$ має розв'язок, то a називається

a) лишком степеня n за простим модулем p
b) нелишком степеня n за модулем p
c) розв’язком рівняння
d) кратністю кореня

23. Виберіть вірне твердження для квадратичних конгруенцій

a) або мають два розв'язки, або не мають їх зовсім
b) завжди мають розв’язки

c) завжди не мають розв'язків
d) завжди мають один розв'язок

24. Якщо a - квадратичний лишок за модулем p, $(a,p)=1,\ p>2$, то квадратна конгруенція $x^2 \equiv a \pmod p$

a) має два розв'язки
b) не має розв'язків
c) має тільки один розв'язок
d) має хоча б один розв'язок

25. При простому $p>2$ число a є квадратичним лишком за модулем p тоді і тільки тоді, коли

a) $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

b) $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

c) $a^{\frac{p}{2}} \equiv -1 \pmod p$

d) $a^{\frac{p}{2}} \equiv 1 \pmod p$

26. Які значення може приймати символ Лежандра

a) 1; -1
b) 0; 1
c) 0; -1
d) будь-яке натуральне число

27. Вибрати, яка із наведених властивостей символа Лежандра $\left(\frac{a}{p}\right)$ записана невірно

a) якщо $a \equiv a_1 \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

b) $\left(\frac{a^2}{p}\right) = -1$.

c) $\left(\frac{1}{p}\right) = 1$

d) $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}}$

28. Якщо $x \equiv x_0 \left(\mathrm{mod}\, p^{\alpha}\right)$ **є один розв‘язок конгруенції** $x^2 \equiv a\left(\mathrm{mod}\, p^{\alpha}\right)$; $\left(a, p\right) = 1$**, то другим її розв‘язком буде**

a) $-x_0$
b) 1
c) 0
d) ${x_0}^2$

29. Конгруенція $x^2 \equiv a\left(\mathrm{mod}\, 2^{\alpha}\right)$; $\alpha > 0$, $\left(a, 2\right) = 1$ **завжди має один розв‘язок при**

a) $\alpha = 1$
b) $\alpha = 2$ і $a \equiv 1\left(\mathrm{mod}\, 4\right)$
c) $\alpha = 2$ і $a \equiv 3\left(\mathrm{mod}\, 4\right)$
d) $\alpha \geq 3$

30. Якщо p **– просте число, то**

a) $\left(p-1\right)!+1 \equiv 0\left(\mathrm{mod}\, p\right)$
b) $\left(p+1\right)!-1 \equiv 0\left(\mathrm{mod}\, p\right)$
c) $p!+1 \equiv 0\left(\mathrm{mod}\, p\right)$
d) $p! \equiv 0\left(\mathrm{mod}\, p\right)$

31. Для яких чисел не справджується теорема Ейлера:

a) $a = 2, m = 9$
b) $a = 2, m = 15$
c) $a = 3, m = 4$
d) $a = 3, m = 9$

32. Для яких чисел справджується теорема Ейлера:

a) $a = 2, m = 9$
b) $a = 2, m = 16$
c) $a = 3, m = 24$
d) $a = 3, m = 9$

33. Яке з тверджень відповідає конгруенції $ax \equiv b(\mathrm{mod}\, 21)$**, де** $(a, 21) = 1$**:**

a) має сім розв’язків
b) розв’язків не має

c) має три розв'язки
d) має один розвязок

34. Яке з тверджень відповідає конгруенції $ax \equiv b(\bmod 21)$, де $(a,21)=7$, b ділиться на 7:

a) має сім розв'язків
b) розв'язків не має
c) має три розв'язки
d) має один розвязок

35. Яка з конгруенцій має один розв'язок:

a) $2x \equiv 8(\bmod 14)$
b) $5x \equiv 10(\bmod 15)$
c) $13x \equiv 5(\bmod 14)$
d) $3x \equiv 6(\bmod 12)$

36. Записати у вигляді конгруенції умову: -352 при діленні на 31 дає остачу рівну 20.

a) $352 \equiv 20(\bmod 31)$
b) $352 \equiv 31(\bmod 20)$
c) $-352 \equiv 31(\bmod 20)$
d) $-352 \equiv 20(\bmod 31)$

37. Записати у вигляді конгруенції умову: 20 остача від ділення 389 на 41.

a) $389 \equiv 41(\bmod 20)$
b) $41 \equiv 20(\bmod 389)$
c) $20 \equiv 41(\bmod 389)$
d) $389 \equiv 20(\bmod 41)$

38. Записати у вигляді конгруенції умову: число N має вигляд $10k+3$

a) $N \equiv 10(\bmod 3)$
b) $3 \equiv N(\bmod 10)$
c) $N \equiv 3(\bmod 10)$
d) $10 \equiv 3(\bmod N)$

39. Записати у вигляді конгруенції умову: число N парне

a) $N \equiv 2 (\mathrm{mod}\, 3)$
b) $2 \equiv 0 (\mathrm{mod}\, N)$
c) $N \equiv 1 (\mathrm{mod}\, 2)$
d) $N \equiv 0 (\mathrm{mod}\, 2)$

40. Записати у вигляді конгруенції умову: число N непарне

a) $N \equiv 2 (\mathrm{mod}\, 3)$
b) $2 \equiv 0 (\mathrm{mod}\, N)$
c) $N \equiv 1 (\mathrm{mod}\, 2)$
d) $N \equiv 0 (\mathrm{mod}\, 2)$

41. Записати у вигляді конгруенції умову: число N має вигляд $8k-5$

a) $N \equiv 5 (\mathrm{mod}\, 8)$
b) $-5 \equiv N (\mathrm{mod}\, 8)$
c) $N \equiv -5 (\mathrm{mod}\, 8)$
d) $8 \equiv 5 (\mathrm{mod}\, N)$

42. Конгруенція $100 \equiv 9 (\mathrm{mod}\, 13)$ описує умову:

a) число 100 кратне 13
b) 100 остача при діленні 13 на 8
c) 9 остача при діленні 100 на 13
d) 13 остача при діленні 100 на 9

43. При якому значенні b конгруенція $4x \equiv 18 (\mathrm{mod}\, b)$ має два розвязки:

a) $b = 9$
b) $b = 13$
c) $b = 44$
d) $b = 42$

44. Щоб знайти k останніх цифр числа a, досить знайти остачу від ділення цього числа на

a) k
b) 10^2
c) 10^k
d) 10^a

45. Скільки розв'язків має конгруенція $13x \equiv 4 \pmod{24}$

a) безліч
b) один
c) два
d) чотири

46. Скільки розв'язків має конгруенція $105x \equiv 75 \pmod{125}$

a) один
b) два
c) чотири
d) п'ять

47. Скільки розв'язків має система конгруенцій $\begin{cases} x \equiv 1 \pmod{11}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 2 \pmod{8}. \end{cases}$

a) безліч
b) один
c) два
d) жодного

48. Скільки розв'язків має конгруенція $x^2 \equiv a \pmod{11}$ **при** $a = 1, 3, 4, 5, 9 \pmod{11}$

a) безліч
b) один
c) два
d) жодного

49. Скільки розв'язків має конгруенція $x^2 \equiv a \pmod{11}$ **при** $a = 2, 6, 7, 8, 10 \pmod{11}$

a) безліч
b) один
c) два
d) жодного

50. Яка з конгруенцій має два розв'язки

a) $x^2 \equiv 2 \pmod{11}$
b) $x^2 \equiv 13 \pmod{17}$
c) $x^2 \equiv 3 \pmod{5}$
d) $x^2 \equiv 6 \pmod{7}$

51. Яка з конгруенцій не має розв'язків

a) $x^2 \equiv 2 \pmod{11}$

b) $x^2 \equiv 13 \pmod{17}$

c) $x^2 \equiv 4 \pmod{5}$

d) $x^2 \equiv 2 \pmod{7}$

52. Скіль точок з цілими координатами належать параболі $17y = x^2 - 13$

a) одна
b) жодної
c) дві
d) інша відповідь

53. Обрати параболу, яка не проходить через точки з цілими координатами

a) $17y = x^2 - 13$

b) $17y = x^2 - 14$

c) $17y = x^2 - 15$

d) $17y = x^2 - 16$

54. Яка з двочлених конгруенцій відповідає конгруенції $2x^2 + 4x - 1 \equiv 0 \pmod{5}$

a) $(x+1)^2 \equiv 4 \pmod{5}$

b) $(x-1)^2 \equiv 1 \pmod{5}$

c) $(x+1)^2 \equiv 0 \pmod{5}$

d) $(x-1)^2 \equiv 4 \pmod{5}$

55. Обрати конгруенцію еквівалентну конгруенції $28x^9 + 29x^8 - 26x^7 + 20x^4 - 17x + 23 \equiv 0 \pmod{3}$

a) $4x^2 + x + 2 \equiv 0 \pmod{3}$

b) $20x^4 - 17x + 23 \equiv 0 \pmod{3}$

c) $2x^4 + x + 2 \equiv 0 \pmod{3}$

d) $x^2 + 2 \equiv 0 \pmod{3}$

56. Знайти порядок $P_{15}(2)$ числа 2 за модулем 15

a) 1
b) 2
c) 4
d) 8

57. Якщо система $\begin{cases} x \equiv c_1 (\bmod 3) \\ x \equiv c_2 (\bmod 5) \\ x \equiv c_3 (\bmod 7) \\ x \equiv c_4 (\bmod 4) \end{cases}$ **сумісна, то вона має**

a) безліч розвязків
b) єдиний розвязок за модулем 420
c) єдиний розвязок за модулем 210
d) єдиний розвязок за модулем 105

58. Розвязком якої систем може бути $x \equiv b (\bmod 462)$

a) $\begin{cases} x \equiv c_1 (\bmod 3) \\ x \equiv c_2 (\bmod 5) \\ x \equiv c_3 (\bmod 7) \\ x \equiv c_4 (\bmod 4) \end{cases}$

b) $\begin{cases} x \equiv c_1 (\bmod 13) \\ x \equiv c_2 (\bmod 5) \\ x \equiv c_3 (\bmod 17) \\ x \equiv c_4 (\bmod 14) \end{cases}$

c) $\begin{cases} x \equiv c_1 (\bmod 2) \\ x \equiv c_2 (\bmod 3) \\ x \equiv c_3 (\bmod 7) \\ x \equiv c_4 (\bmod 11) \end{cases}$

d) $\begin{cases} x \equiv c_1 (\bmod 5) \\ x \equiv c_2 (\bmod 9) \\ x \equiv c_3 (\bmod 14) \\ x \equiv c_4 (\bmod 23) \end{cases}$

59. Обрати систему, які еквівалентна конгруенція $x \equiv b (\bmod 210)$

a) $\begin{cases} x \equiv c_1 (\bmod 3) \\ x \equiv c_2 (\bmod 5) \\ x \equiv c_3 (\bmod 7) \\ x \equiv c_4 (\bmod 4) \end{cases}$

b) $\begin{cases} x \equiv b(\mathrm{mod}\,10) \\ x \equiv b(\mathrm{mod}\,22) \end{cases}$

c) $\begin{cases} x \equiv b(\mathrm{mod}\,2) \\ x \equiv b(\mathrm{mod}\,3) \\ x \equiv b(\mathrm{mod}\,5) \\ x \equiv b(\mathrm{mod}\,17) \end{cases}$

d) $\begin{cases} x \equiv b(\mathrm{mod}\,2) \\ x \equiv b(\mathrm{mod}\,3) \\ x \equiv b(\mathrm{mod}\,5) \\ x \equiv b(\mathrm{mod}\,7) \end{cases}$

60. Обрати конгруенцію, яка відповідає даній $17x^{18} \equiv 22(\mathrm{mod}\,23)$

a) $ind17 + ind18 + indx \equiv ind22(\mathrm{mod}\,22)$

b) $ind17 + 18indx \equiv ind22$

c) $ind17 + xind18 \equiv ind22(\mathrm{mod}\,22)$

d) $ind17 + 18indx \equiv ind22(\mathrm{mod}\,22)$

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які числа називаються конгруентними?
2. Якій рівності еквівалентна конгруенція?
3. Що означає запис $a \equiv b \pmod{m}$?
4. Яка необхідна і достатня умова конгруентності двох чисел за модулем m?
5. Сформулювати властивості конгруенцій, аналогічні властивостям рівностей.
6. Сформулювати властивості конгруенцій, відмінні від властивостей рівностей.
7. Сформулювати правило скорочення конгруенцій.
8. Записати по кілька чисел, що належать до кожного класу за модулем 7.
9. Яка умова є необхідною і достатньою для того, щоб числа належали до того самого класу за модулем m?
10. За яких умов числа a і $-a$ належать до одного і того ж класу лишків за модулем m?
11. Яке означення операцій „додавання” класів?
12. Яке означення операцій „множення” класів?
13. Що розуміють під словами: множина містить дільники нуля?
14. Наведіть приклад кільця класів чисел з дільниками нуля.
15. Як дістати повну систему лишків за модулем m?
16. Напишіть повну систему абсолютно найменших, найменших невід‘ємних лишків і довільних лишків за модулем 6.
17. До яких класів лишків за модулем 10 належать усі прості числа $p > 3$? Записати загальний вигляд у вигляді рівності і у вигляді конгруенції.
18. Сформулюйте основні властивості повної системи лишків.
19. Нехай x пробігає повну систему найменших невід‘ємних лишків за модулем 8.

20. Що називається зведеною системою лишків за модулем $m = 5$?
21. Сформулюйте основні властивості зведеної системи лишків.
22. Якими елементами відрізняється зведена система лишків за простим модулем p від повної системи лишків за цим модулем?
23. Запишіть зведену систему найменших невід‘ємних лишків і довільну зведену систему лишків за модулем 12.
24. Скільком класам лишків за модулем 21 належать лишки із одного класу за модулем 7?
25. Чи пробігає вираз $ax + b$, де $(a, m) = 1$, зведену систему лишків за модулем m при умові, що x пробігає зведену систему лишків?
26. Як зрозуміти, що для кожного класу чисел, взаємно простих з модулем, існує обернений клас?
27. Нехай $m = 20$; знайти: а) $\overline{7} \cdot \overline{19}$; б) $\overline{8} \cdot \overline{9}$; в) клас, протилежний до класу $\overline{13}$; г) класи, які є дільниками нуля.
28. Які з класів лишків $\overline{6}, \overline{7}, \overline{8}, \overline{10}$ за модулем 15 є оборотними? Якщо такі класи існують, знайти їм обернені.
29. Чи може бути добуток двох необоротних класів лишків стати оборотним?
30. Чи може бути добуток оборотного класу лишків на необоротний клас лишків?
31. Чи утворює сукупність усіх класів чисел за модулем групу відносно множення класів?
32. Чи утворює сукупність усіх класів чисел за модулем групу відносно додавання класів?
33. Дайте визначення функції Ейлера.
34. Яка числова функція називається мультиплікативною?
35. Які вдастивості має мультиплікативна функція?
36. Які властивості має функція Ейлера?
37. Сформулюйте теореми Ейлера і Ферма.
38. Перевірте справедливість теореми Ейлера на числовому прикладі $a = 5$, $m = 12$.

39. Дайте означення алгебраїчної конгруенції $n-$го степеня з одним невідомим.
40. Яке число називається розв'язком конгруенції?
41. Які конгруенції називаються еквівалентними?
42. Які конгруенції не вважаються рівними?
43. Чи завжди при множенні обох частин конгруенції на ціле число дістанемо еквівалентну конгруенцію?
44. Чи дістанемо еквівалентні конгруенції при множенні обох частин конгруенції і модуля на ціле число?
45. При якій умові розв'язується конгруенція першого степеня з одним невідомим?
46. Скільки розв'язків має конгруенція $ax \equiv b \left(\mathrm{mod}\, m\right)$, якщо вона розв'язна?
47. Як знайти усі розв'язки конгруенції $ax \equiv b \left(\mathrm{mod}\, m\right)$ при умові $\left(a,m\right)=d>1$, коли відомо один розв'язок цієї конгруенції?
48. Написати формулу для знаходження розв'язків конгруенції першого степеня способом Ейлера.
49. Написати формулу для знаходження розв'язків конгруенції першого степеня, яка ґрунтується на застосуванні неперервних дробів, і пояснити зміст букв, що входять до неї.
50. Чи утворює поле сукупність усіх класів чисел за складеним модулем? Чому?
51. Яким конгруенціям еквівалентне рівняння $ax+by=c$?
52. Дайте означення розв'язку системи конгруенцій першого степеня з одним невідомим?
53. Які системи конгруенцій називаються еквівалентними?
54. За яким модулем визначають розв'язок системи конгруенцій $\begin{cases} x \equiv c_1 \left(\mathrm{mod}\, m_1\right), \\ x \equiv c_2 \left(\mathrm{mod}\, m_2\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k \left(\mathrm{mod}\, m_k\right). \end{cases}$?

55. Напишіть формулу для розв'язування системи конгруенцій $\begin{cases} x \equiv c_1 \left(\bmod m_1\right), \\ x \equiv c_2 \left(\bmod m_2\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k \left(\bmod m_k\right). \end{cases}$, якщо модулі попарно взаємно прості. Поясніть зміст букв, які входять до формули.

56. Чи застосовний другий спосіб для розв'язування системи конгруенцій, якщо модулі попарно взаємно прості?

57. Як з розв'язків першої конгруенції системи $\begin{cases} x \equiv c_1 \left(\bmod m_1\right), \\ x \equiv c_2 \left(\bmod m_2\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k \left(\bmod m_k\right). \end{cases}$ знайти числа, які задовольняють другу систему?

58. Чи може система конгруенцій першого степеня з одним невідомим не мати розв'язків або мати більш як один розв'язок? У якому випадку?

59. Дайте визначення діофантового рівняння першого степеня з n невідомими.

60. Що можна сказати про розв’язки діофантового рівняння $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$, якщо коефіцієнти $a_1, a_2, \ldots, a_n$ взаємно прості числа.

61. За якої умови діофантове рівняння $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$, у якого d – найбільший спільний дільник коефіцієнтів $a_1, a_2, \ldots, a_n$,. має розв'язок?

62. Як треба перетворити конгруенцію $f(x) \equiv 0 \left(\bmod p\right)$, щоб старший коефіцієнт дорівнював одиниці? Чи завжди є таке α, що $a_n\alpha \equiv 1 \left(\bmod p\right)$? Чому?

63. Як застосувати теорему Ферма, щоб перетворити конгруенцію за простим модулем p у еквівалентну конгруенцію з степенем, меншим від p?

64. Яка необхідна і достатня умова того, щоб конгруенція $f(x) \equiv 0 \left(\bmod p\right)$ мала корінь $x = \alpha_1$?

65. Що можна сказати про число розв'язків конгруенції n -го степеня за простим модулем?
66. Сформулювати умову, необхідну і достатню для того, щоб натуральне число p було простим.
67. При якій умові конгруенція $f(x) \equiv 0 \left(\operatorname{mod} m_1 \cdot m_2 \cdot \ldots \cdot m_k \right)$, де $m_1, m_2, ..., m_k$ – попарно взаємно прості, не має розв'язків?
68. Які конгруенції випливають з розв'язку конгруенції за складеним модулем?
69. Відомо, що конгруенція $f(x) \equiv 0 \left(\operatorname{mod} p^2 \right)$ має розв'язок. Чи можна твердити, що конгруенція $f(x) \equiv 0 \left(\operatorname{mod} p \right)$ також має розв'язок? Чи справедливе обернене твердження?
70. Дайте означення показника, до якого належить число a за модулем m.
71. З якої теореми випливає існування показника, до якого належить a за модулем m, якщо $(a, m) = 1$?
72. Перелічіть основні властивості показників.
73. Серед чисел якого виду міститься показник, до якого належить число a за модулем m?
74. Яке число a називається первісним коренем за модулем m?
75. Чи достатньо конгруенції $a^{\varphi(m)} \equiv 1 \left(\operatorname{mod} m \right)$ для того, щоб число a було – первісним коренем за модулем m?
76. Чому числа ряду $1 = a^0, a, a^2, ..., a^{\varphi(m)-1}$ не конгруентні між собою за модулем m, якщо a – первісний корінь?
77. Які числа належать показнику δ за простим модулем p, коли відомо що a належить показнику δ за цим модулем?
78. Якому показнику належить первісний корінь за модулем p? $p = 43$?
79. Чому дорівнює число первісних коренів за модулем p?
80. $K_4^{(11)}$ має порядок 5. Знайти всі інші класи лишків за модулем 11, які також мають порядок 5.

81. Скільки існує класів лишків порядку δ за простим модулем p?
82. Чи може існувати клас лишків порядку 7 за модулем 26?
83. Скільки може бути класів лишків порядку 9 за модулем 37?
84. Якщо g – первісний корінь за простим модулем p, то чи утворюють числа $g^0, g, g^2, ..., g^{p-1}$ зведену систему лишків за цим модулем? У чому переваги цієї зведеної системи лишків над будь-якою іншою?
85. Яке число називається індексом числа a за простим модулем p при основі g?
86. На підставі яких міркувань можна твердити, що всяке число a, взаємно просте з p, має єдиний індекс γ' менший від p?
87. Знаючи один індекс γ числа a за модулем p, назвати всі індекси цього числа a. За яким модулем вони утворюють клас чисел?
88. Назвіть основні властивості індексів.
89. Що являють собою таблиці індексів для даного простого числа p?
90. Чи можна побудувати таблиці індексів для складеного модуля m?
91. До розв‘язування якої конгруенції першого степеня зводиться розв‘язування конгруенції $ax^n \equiv b \pmod{p}$, де $(a, p) = 1$?
92. Скільки розв‘язків має конгруенція $ax^n \equiv b \pmod{p}$ і при якій умові?
93. Яке число називається лишком степеня n за простим модулем p?
94. Яка умова буде необхідною і достатньою для того, щоб a було лишком степеня n за простим модулем p?
95. Скільки розв‘язків має конгруенція $a \cdot c^x \equiv b \pmod{p}$ і при якій умові?
96. Як застосувати властивості і таблицю індексів для обчислення остач від ділення на просте число p ?
97. В чому суть процесів індексування та потенціювання конгруенції.
98. Як знайти довжину періоду при перетворенні звичайного дробу в десятковий?

99. На якому твердженні ґрунтується перевірка арифметичних дій за допомогою конгруенцій?

100. Сформулювати необхідну умову перевірки результатів дій додавання, віднімання і множення числами 9 і 11.

ДОДАТКИ

Додаток 1. Таблиця простих чисел, які не перевищують 5000

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379
383	389	397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541	547	557	563	569	571
577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941	947	953	967	971	977
983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187
1193	1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399	1409	1423	1427
1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613
1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867
1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087
2089	2099	2111	2113	2129	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287	2293	2297	2309	2311	2333
2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557
2579	2591	2593	2609	2617	2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741	2749	2753	2767	2777	2789
2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037
3041	3049	3061	3067	3079	3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271	3299	3301	3307
3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539
3541	3547	3557	3559	3571	3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727	3733	3739	3761	3767	3769
3779	3793	3797	3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989	4001	4003	4007	4013	4019
4021	4027	4049	4051	4057	4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231	4241	4243	4253	4259	4261
4271	4273	4283	4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493	4507	4513	4517	4519	4523
4547	4549	4561	4567	4583	4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751	4759	4783	4787	4789	4793
4799	4801	4813	4817	4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999						

Додаток 2. Таблиці первісних коренів та індексів

Просте число 3

Первісні корені: 2

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Просте число 5

Первісні корені: 2, 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Просте число 7

Первісні корені: 3, 5

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Просте число 11

Первісні корені: 2, 6, 7, 8

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6

Просте число 13

Первісні корені: 2, 6, 7, 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6				10	10	10	10

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7					10	10	10	10

Просте число 17

Первісні корені: 3, 5, 6, 7, 11, 12, 14

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Просте число 19

Первісні корені:2, 3, 10, 14, 15

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Просте число 23

Первісні корені: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21

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

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

Просте число 29

Первісні корені:2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Просте число 31

Первісні корені: 3, 11, 12, 13, 17, 21, 22, 24

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*24*	*1*	*18*	*20*	*25*	*28*	*12*	*2*
1	*14*	*23*	*19*	*11*	*22*	*21*	*6*	*7*	*26*	*4*
2	*8*	*29*	*17*	*27*	*13*	*10*	*5*	*2*	*16*	*9*
3	*15*									

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*3*	*9*	*27*	*19*	*26*	*16*	*17*	*20*	*29*
1	*25*	*13*	*8*	*24*	*10*	*30*	*28*	*22*	*4*	*12*
2	*5*	*15*	*14*	*11*	*2*	*6*	*18*	*23*	*7*	*21*

Просте число 37

Первісні корені: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*1*	*26*	*2*	*23*	*27*	*32*	*3*	*16*
1	*24*	*30*	*28*	*11*	*33*	*13*	*4*	*7*	*17*	*35*
2	*25*	*22*	*31*	*15*	*29*	*10*	*12*	*6*	*34*	*21*
3	*14*	*9*	*5*	*20*	*8*	*19*	*18*			

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*2*	*4*	*8*	*16*	*32*	*27*	*17*	*34*	*31*
1	*25*	*13*	*26*	*15*	*30*	*23*	*9*	*18*	*36*	*35*
2	*33*	*29*	*21*	*5*	*10*	*20*	*3*	*6*	*12*	*24*
3	*11*	*22*	*7*	*14*	*28*	*19*				

Просте число 41

Первісні корені: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*26*	*15*	*12*	*22*	*1*	*39*	*38*	*30*
1	*8*	*3*	*27*	*31*	*25*	*37*	*24*	*33*	*16*	*9*
2	*34*	*14*	*29*	*36*	*13*	*4*	*11*	*5*	*11*	*7*
3	*23*	*28*	*10*	*18*	*19*	*21*	*2*	*32*	*35*	*6*
4	*20*									

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*6*	*36*	*11*	*25*	*27*	*39*	*29*	*10*	*19*
1	*32*	*28*	*4*	*24*	*21*	*3*	*18*	*26*	*33*	*34*
2	*40*	*35*	*5*	*30*	*16*	*14*	*2*	*12*	*31*	*22*
3	*9*	*13*	*37*	*17*	*20*	*38*	*23*	*15*	*8*	*7*

Просте число 43

Первісні корені: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*27*	*1*	*12*	*25*	*28*	*35*	*39*	*2*
1	*10*	*30*	*13*	*32*	*20*	*26*	*24*	*38*	*29*	*19*
2	*37*	*36*	*15*	*16*	*40*	*8*	*17*	*3*	*5*	*41*
3	*11*	*34*	*9*	*31*	*23*	*18*	*14*	*7*	*4*	*33*
4	*22*	*6*	*21*							

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*3*	*9*	*27*	*38*	*28*	*41*	*37*	*25*	*32*
1	*10*	*30*	*4*	*12*	*36*	*22*	*23*	*26*	*35*	*19*
2	*14*	*42*	*40*	*34*	*16*	*5*	*15*	*2*	*6*	*18*
3	*11*	*33*	*13*	*39*	*31*	*7*	*21*	*20*	*17*	*8*
4	*24*	*29*								

Просте число 47

Первісні корені: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 39, 40, 41, 43, 44, 45

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*18*	*20*	*36*	*1*	*38*	*32*	*8*	*40*
1	*19*	*7*	*10*	*11*	*4*	*21*	*26*	*16*	*12*	*45*
2	*37*	*6*	*25*	*5*	*28*	*2*	*29*	*14*	*22*	*35*
3	*39*	*3*	*44*	*27*	*34*	*33*	*30*	*42*	*17*	*31*
4	*9*	*15*	*24*	*13*	*43*	*41*	*23*			

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*5*	*25*	*31*	*14*	*23*	*21*	*11*	*8*	*40*
1	*12*	*13*	*18*	*43*	*27*	*41*	*17*	*38*	*2*	*10*
2	*3*	*15*	*28*	*46*	*42*	*22*	*16*	*33*	*24*	*26*
3	*36*	*39*	*7*	*35*	*34*	*29*	*4*	*20*	*6*	*30*
4	*9*	*45*	*37*	*44*	*32*	*19*				

Просте число 53

Первісні корені: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*1*	*17*	*2*	*47*	*18*	*14*	*3*	*34*
1	*48*	*6*	*19*	*24*	*15*	*12*	*4*	*10*	*35*	*37*
2	*49*	*31*	*7*	*39*	*20*	*42*	*25*	*51*	*16*	*46*
3	*13*	*33*	*5*	*23*	*11*	*9*	*36*	*30*	*38*	*41*
4	*50*	*45*	*32*	*22*	*8*	*29*	*40*	*44*	*21*	*28*
5	*43*	*27*	*26*							

I	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*2*	*4*	*8*	*16*	*32*	*11*	*22*	*44*	*35*
1	*17*	*34*	*15*	*30*	*7*	*14*	*28*	*3*	*6*	*12*
2	*24*	*48*	*43*	*33*	*13*	*26*	*52*	*51*	*49*	*45*
3	*37*	*21*	*42*	*31*	*9*	*18*	*36*	*19*	*38*	*23*
4	*46*	*39*	*25*	*50*	*47*	*41*	*29*	*5*	*10*	*20*
5	*40*	*27*								

Просте число 59

Первісні корені: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Просте число 61

Первісні корені: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	32	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Просте число 67

Первісні корені: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Просте число 71

Первісні корені: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	36
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Просте число 73

Первісні корені: 5, 11, 13, 14, 15, 20, 26, 28, 29,31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Просте число 79

Первісні корені: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53,54, 59, 60, 63, 66, 68, 70, 74, 75,77

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	8	65	37
2	32	17	51	74	64	34	23	9	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Просте число 83

Первісні корені: 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	36	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Просте число 89

Первісні корені: 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	64	11	33	10	30		

Просте число 97

Первісні корені: 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	33
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

СПИСОК ЛІТЕРАТУРИ

1. Безущак О.О., Ганюшкін О.Г. Елементи теорії чисел. – К.: Видавничо-поліграфічний центр «Київський університет», 2003.
2. Бородін О.І. Теорія чисел.-К.: Вища школа. Головне вид-во, 1970.
3. Завало С.Т. та ін. Алгебра і теорія чисел, Ч.2. – К.: Вища школа. Головне вид-во, 1976.
4. Завало С.Т. та ін. Алгебра і теорія чисел: Практикум.Ч.2. – К.: Вища школа. Головне вид-во, 1986.
5. Оглобліна О.І., Сушко Ю.В., Шрамко Ю.В. Елементи теорії чисел. – Суми : Сумський державний університет, 2015.
6. Практикум з алгебри і теорії чисел/ Гудивок П.М., Кирилюк О.А., Погоріляк Є. Я., Тилищак О.А., Юрченко Н.В. – Ужгород: Видавництво УжНУ «Говерла», 2008.