ЗБІРНИК
задач з теорії чисел

За редакцією І.О.Рокіцького

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів

Вінниця
2003

УДК 512 + 511
З – 41

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів (Лист Міністерства освіти і науки України № 14/18.2–931 від 29.04.2002 р.)
Рецензенти: доктор фізико-математичних наук, професор Панков О.А. і кандидат фізико-математичних наук, доцент Дереч В.Д.

Пропонований навчальний посібник є збірником задач з алгебри і теорії чисел. Він містить понад 1200 задач та вправ і охоплює повністю програму третього семестру з названої дисципліни для студентів фізико-математичних факультетів педагогічних університетів та інститутів.

Рекомендовано до друку Вченою радою Вінницького державного педагогічного університету ім.М.Коцюбинського, протокол № 7 від 28 березня 2001 року.

КОЛЕКТИВ АВТОРІВ: В.С.Гарвацький, В.Т.Кулик, І.О.Рокіцький, Р.І.Рокіцький, В.А.Ясінський

Збірник задач з теорії чисел. [Навчальний посібник для студентів фізико-математичного факультету] За редакцією І.О.Рокіцького, Вінниця, 2003 – 140с.
ISBN 966–527–071–О
Вінниця: ДОВ "Вінниця"

Зміст

Передмова

Впродовж багатьох років студенти фізико-математичних факультетів педагогічних університетів та інститутів на практичних заняттях з курсу "Алгебра і теорія чисел"широко використовують відомий посібник [7]. Однак в останній час він уже став бібліографічною рідкістю. Російськомовні видання подібних збірників [8–11] також малодоступні для українського студента. Тому виникла гостра необхідність у виданні україномовного збірника з цього курсу. Колектив авторів вирішив на першому етапі підготувати такий збірник з розділів, що охоплюють зміст теорії чисел.

При написанні цього збірника автори заклали ідею розподілу задач кожного з основних параграфів розділів за рубриками: задачі на ілюстрацію основних понять, задачі на техніку обчислень і перетворень, задачі на доведення, творчі задачі та олімпіадні задачі. Такий розподіл дозволить студенту при самостійній роботі поступово переходити від простих до складніших задач, керуючись самостійною оцінкою свого рівня підготовки. До більшості задач з перших двох рубрик у збірнику є відповіді. До задач з інших трьох рубрик іноді даються вказівки або розв'язки. Для їх розв'язування студент повинен добре володіти основними поняттями і теоремами теорії, проявити творче мислення, винахідливість та логічну стрункість в математичних доведеннях і перетвореннях. В окремих випадках такі задачі на дослідження можуть стати темами курсових робіт.

Кожен параграф розпочинається з посилання на літературу та коротких теоретичних відомостей, в яких читач може знайти означення понять і формулювання основних теорем необхідних для розв'язування задач.

У всіх трьох розділах є параграф "Вибрані задачі."До них включено задачі відомих математиків та з різних математичних олімпіад і конкурсів для учнів шкіл і студентів вищих навчальних закладів. Вони призначені для тих студентів, які хочуть зробити свої перші кроки в наукових дослідженнях. Тому до цих задач не дано вказівок і відповідей.

У збірнику в різних рубриках є ряд задач з різноманітних учнівських математичних олімпіад і конкурсів. Це допоможе вчителю математики в роботі з учнями в шкільному математичному гуртку.

Збірник містить у виді додатків таблиці простих чисел, найменших первісних коренів та індексів за основою, яка є найменшим первісним коренем, квадратів, грецький і літинський алфавіти. Поміщено також список основних позначень, які використовуються в книзі та предметний показчик.

Розділ 1

Теорія подільності в кільці цілих чисел

§ 1.1 Відношення подільності. Ділення з остачею

Література: [2] стор. 66–69; [3] стор. 141–146; [4] стор. 5–8; [6] стор. 3–6.

Теоретичні відомості

Якщо для цілих чисел a і b в кільці цілих чисел $\mathbb{Z}$ існує таке ціле число q, що $a = bq$, то кажуть, що a ділиться на b і цей факт позначають коротко так: $a \vdots b$. При цьому число a називають діленим (або кратним b), b – дільником a, q – часткою.

Відношення подільності на множині цілих чисел має такі властивості:

1. Число 0 ділиться на будь-яке ціле число.
2. Єдиним цілим числом яке ділиться на нуль є ціле число нуль.
3. Кожне ціле число ділиться на числа 1 і -1.
4. Відношення $\vdots$ має властивості рефлексивності і транзитивності;
5. Якщо $a \vdots b$, то $a \vdots (-b)$, $(-a) \vdots b$, $(-a) \vdots (-b)$.
6. Якщо $a \vdots b$, то $|a| \geqslant |b|$.
7. Якщо $a \vdots c$ і $b \vdots c$, то $(a \pm b) \vdots c$.
8. Якщо $a \vdots c$, то $(a \cdot b) \vdots c$.

9. Якщо $a \vdots c$ і $b \vdots c$, то $(m \cdot a \pm n \cdot b) \vdots c$.

Для будь-яких цілих чисел a і $b \neq 0$ існує єдина пара цілих чисел q і r така, що $a = bq + r$ і $0 \leqslant r < |b|$. При цьому число q називають неповною часткою, а r – остачею.

Ціле число a ділиться на ціле число $b \neq 0$ тоді і тільки тоді, коли остача від ділення a на b дорівнює нулю.

Задачі на ілюстрацію понять

1. Для заданих цілих чисел a та b знайти ціле число q таке, що $b \cdot q \leqslant a < b \cdot (q + 1)$:
   а) $a = -35, b = 21$; в) $a = 35, b = 21$;
   б) $a = -35, b = -21$; г) $a = 35, b = -21$.

2. При діленні цілого числа a на ціле число b утворилася неповна частка q і остача r, тобто $a = b \cdot q + r$ і $0 \leqslant r < |b|$. Знайти невідомі числа з цієї рівності, якщо:
   а) $a = 173, b = -21$; в) $a = -23, q = 13$; д) $a = -238, r = 17$;
   б) $q = 89, b = -8$; г) $r = 9, b = -36$; е) $q = 15, r = 11$.

3. Записати загальний вид усіх цілих чисел, які:
   а) діляться на 3; в) не діляться на -7;
   б) при діленні на 5 дають остачу 2; г) не діляться на 2 і 3.

Задачі на техніку обчислень та перетворень

4. Встановити, чи ділиться на 10 число $8 \cdot 23^{23} - 71 \cdot 32^{32}$.

5. Знайти остачу при діленні числа:
   а) 11^{10} на 100; в) $5^{5^5} + 1$ на 13;
   б) $5^{100} + 13^{10}$ на 11; г) 23^n на 7, де $n \in \mathbb{N}$.

6. Знайти найменше натуральне число, яке:
   а) ділиться на 11, а при діленні на 2,3,4,5 дає остачу 1;
   б) при діленні на 2,3,4,5,6 дає відповідно остачі 1,2,3,4,5.

7. Для довільного натурального числа n знайти остачу при діленні на 6 числа:
   а) $n^3 + 5n$; в) $n^3 + 3n^2 + 2n + 1$;
   б) $n^3 + 11n + 1$; г) $2n^3 + 3n^2 + 13n + 2$.

8. Знайти всі можливі остачі при діленні кубів цілих чисел на 9.

9. Знайти останню цифру числа:
   а) $3^{3^3}+8$; в) $8^{4n+1}-1$;
   б) $4^{2n+2}+1$; г) 2^{2^n}, де $n>1$.

10. Для довільного натурального числа n перевірити подільність:
   а) $(3^{4n-1}+3^{4n-2}+\cdots+3+1)$ на 40;
   б) $(11^{2n}+31^{2n}+38\cdot 11^n\cdot 31^n)$ на 40;
   в) $[(n+1)^{3n}-n^{2n}(n+3)^n]$ на $(3n+1)$;
   г) $(n^4+6n^3+11n^2+6n)$ на 24.

11. Знайти, при яких натуральних n:
   а) $(n^2+14)\vdots(n+2)$; в) $(n^3+7n+1)\vdots(n-2)$;
   б) $(n^2+1)\vdots(n+1)$; г) $(n^3+4n^2-3)\vdots(n+2)$.

12. Натуральні числа m і n такі, що $m>n$ та m при діленні на n дає таку ж відмінну від нуля остачу, як $m+n$ при діленні на $m-n$. Знайти відношення $m:n$.

Задачі на доведення

13. Довести, що:
   а) з трьох послідовних цілих чисел тільки одне ділиться на 3;
   б) з двох послідовних парних цілих чисел тільки одне ділиться на 4;
   в) добуток чотирьох послідовних цілих чисел ділиться на 24;
   г) добуток n послідовних цілих чисел ділиться на $n!$.

14. Довести, що:
   а) квадрат непарного цілого числа при діленні на 8 дає остачу 1;
   б) сума квадратів двох послідовних цілих чисел при діленні на 4 дає остачу 1;
   в) числа виду $3k+2, k\in\mathbb{Z}$ не можуть бути квадратами цілих чисел;
   г) сума квадратів двох непарних цілих чисел не може бути квадратом цілого числа;
   д) якщо натуральне число n не ділиться на 7, то (n^3-1) ділиться на 7 або (n^3+1) ділиться на 7;
   е) сума квадратів п'яти послідовних цілих чисел не може бути квадратом цілого числа;
   є) якщо остача від ділення деякого цілого числа на 9 є одне з чисел 2,3,5,6,8, то це число не може бути квадратом цілого числа;
   ж) якщо чисельник дробу є різниця квадратів двох непарних цілих

чисел, а знаменник – сума квадратів цих чисел, то такий дріб можна скоротити на 2, але не на 4.

15. Довести, що для довільних цілих чисел m і n:

а) $(n^3 - n) \vdots 6$; в) $(n^3 + 11n) \vdots 6$; д) $mn(m^4 - n^4) \vdots 30$;

б) $(n(n^2 + 5)) \vdots 6$; г) $(n^5 - n) \vdots 30$; е) $(n^7 - n) \vdots 7$.

16. Довести, що для довільного натурального числа n:

а) $(5^{2n} - 1) \vdots 24$; е) $(10^n + 18n - 1) \vdots 27$;

б) $(10^{3n} - 1) \vdots 27$; є) $(3^{2n+3} + 40n - 27) \vdots 64$;

в) $(15^n - 1) \vdots 7$; ж) $(94^n + 6n - 1) \vdots 9$;

г) $(3^{6n} - 2^{6n}) \vdots 35$; з) $(10^{n+1} - 9n - 10) \vdots 81$;

д) $(11^{n+2} + 12^{2n+1}) \vdots 133$; к) $(9^{n+1} - 8n - 9) \vdots 16$.

17. Довести, що з довільної множини, яка містить n цілих чисел, завжди можна вибрати декілька таких, що їх сума ділиться на n.

18. Довести, що для будь-яких цілих чисел m і n:

а) якщо $(m^2 + n^2) \vdots 3$, то $(m^2 + n^2) \vdots 9$;

б) якщо $(m^2 + n^2) \vdots 7$, то числа m і n діляться на 7.

Творчі задачі

19. Відомо, що довжини сторін та діагоналей прямокутника є натуральними числами. Що можна сказати про подільність площі цього прямокутника на числа 2, 3, 4, 5, 6, 7,8,9,10?

20. Для заданих натуральних чисел a, b, які не перевищують 9, описати множину всіх чисел $an + b$, які є квадратом натурального числа.

21. Встановити, для яких простих чисел p число $n^p - n$ ділиться на p при всіх $n \in \mathbb{N}$.

22. Знайти найменше натуральне число, яке при діленні на $2, 3, \ldots, k$ дає відповідно остачі $1, 2, \ldots, (k-1)$.

Задачі з олімпіад

23. Скільки є нескоротних дробів з чисельником 1997 менших, ніж $\frac{1}{1997}$ і більших, ніж $\frac{1}{1998}$?

24. Чи буде число $11\cdots155\cdots56$ (1998 одиниць та 1997 п'ятірок) квадратом цілого числа?

25. Було 4 аркуші паперу. Деякі з них розрізали на 8 частин, потім деякі з цих частин знову розрізали на 8 частин і т.д. Встановити, чи може на якомусь етапі загальна кількість аркушів стати рівною 2001.

26. Нехай $n \geqslant 2$ та дано многочлен $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + 1$ такий, що всі a_k – натуральні числа та $a_i = a_{n-i}$ для всіх $i = 1, 2, \ldots, n-1$. Довести, що існує нескінченна кількість різних пар натуральних чисел (k, l) таких, що $f(k)$ ділиться на l та $f(l)$ ділиться на k. (Різні пари відрізняються хоча б одною координатою.)

27. Знайти всі пари (a, b) натуральних чисел такі, що $a^2 + a + b$ ділиться на $ab^2 + b + 7$.

28. Довести, що з довільних 100 натуральних чисел можна вибрати декілька чисел так, щоб їх сума ділилася на 100.

29. Довести, що для будь-якого цілого $n > 1$ число $n^n - n^2 + n - 1$ ділиться на $(n-1)^2$.

30. Нехай $n \in \mathbb{N}$ ділиться на m^2. Довести, що $(1 + \frac{n}{m})^{n-1} - 1$ не ділиться на n.

31. Довести, що для будь-якого простого $p \geqslant 5$ чисельник нескоротного дробу, рівного $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$, ділиться: а) на число p; б) на число p^2.

32. Нехай $k_1, k_2, \ldots, k_n$ – довільна перестановка чисел $1, 2, \ldots, n$. Довести, що коли n є парним, то добуток $(k_1 - 1)(k_2 - 2)\cdots(k_n - n)$ є парним числом.

33. Довести, що для будь-якого цілого $n \geqslant 0$ число $1\underbrace{0\ldots0}_{3n+2}1\underbrace{0\ldots0}_{2n+2}$ ділиться на $1\underbrace{0\ldots0}_{n}1$.

34. Знайти всі цілі числа n, для яких число $n^2 + 19n + 99$ є квадратом цілого числа.

§ 1.2 Найбільший спільний дільник і найменше спільне кратне. Алгоритм Евкліда. Взаємно прості числа

Література: [1] стор. 72–78;[2] стор. 69–76; [3] стор. 372–389; [4] стор. 22–30.

Теоретичні відомості

Якщо кожне з цілих чисел $a_1, a_2, \ldots, a_n$ ділиться на число δ, то його називають їх спільним дільником. Найбільшим спільним дільником (НСД) цілих чисел $a_1, a_2, \ldots, a_n$ називається їх спільний дільник, який ділиться на кожний спільний дільник цих чисел.

Найбільший спільний дільник цілих чисел $a_1, a_2, \ldots, a_n$ визначається однозначно з точністю до знака. Його додатне значення позначають через $d = (a_1, a_2, \ldots, a_n)$.

Число d є найбільшим спільним дільником цілих чисел $a_1, a_2, \ldots, a_n$ тоді і тільки тоді, коли d є найбільший за величиною спільний дільник цих чисел.

Якщо $(a_1, a_2) = d_1$, $(d_1, a_3) = d_2$, $\ldots$, $(d_{n-2}, a_n) = d_{n-1}$, то $(a_1, a_2, \ldots, a_n) = d_{n-1}$.

Якщо ціле число a ділиться на b, то $(a, b) = b$.

Якщо $a = bq + r$ і $0 \leqslant r < |b|$, то $(a, b) = (b, r)$.

Нехай серед цілих чисел a і b хоча б одне є відмінним від нуля. Тоді послідовність ділень з остачею

$$\begin{array}{lcl}
a = bq_1 + r_1 & \text{і} & 0 < r_1 < |b|, \\
b = r_1 q_2 + r_2 & \text{і} & 0 < r_2 < r_1, \\
r_1 = r_2 q_3 + r_3 & \text{і} & 0 < r_3 < r_2, \\
\ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots \\
r_{n-2} = r_{n-1} q_n + r_n & \text{і} & 0 < r_n < r_{n-1}, \\
r_{n-1} = r_n q_{n+1} & &
\end{array}$$

називають алгоритмом Евкліда. При цьому $(a, b) = r_n$.

Тому $(a, b) = d$ тоді і тільки тоді, коли $(\exists x, y)(d = ax + by)$. Останню рівність називають лінійним поданням або зображенням НСД чисел a і b.

Якщо ціле число M ділиться на кожне з цілих чисел $a_1, a_2, \ldots, a_n$, то його називають їх спільним кратним. Найменшим спільним кратним (НСК) цілих чисел $a_1, a_2, \ldots, a_n$ називається їх спільне кратне, на яке ділиться кожне спільне кратне цих чисел.

Найменше спільне кратне цілих чисел $a_1, a_2, \ldots, a_n$ визначається однозначно з точністю до знака. Його додатне значення позначають через

$m = [a_1, a_2, \ldots, a_n]$.

Якщо $[a_1, a_2] = m_1$, $[m_1, a_3] = m_2$, $\ldots$, $[m_{n-2}, a_n] = m_{n-1}$, то $[a_1, a_2, \ldots, a_n] = m_{n-1}$.

Число m є найменшим спільним кратним цілих чисел $a_1, a_2, \ldots, a_n$ тоді і тільки тоді, коли m є найменшим за величиною додатним спільним кратним цих чисел.

Якщо $ab \neq 0$, то $[a, b] = \frac{ab}{(a,b)}$.

Цілі числа $a_1, a_2, \ldots, a_n$ називають взаємно простими, якщо $(a_1, a_2, \ldots, a_n) = 1$.

Взаємно прості числа мають такі властивості:

1. Цілі числа a і b взаємно прості тоді і тільки тоді, коли існують цілі числа u та v такі, що $au + bv = 1$;
2. Якщо $(a, b) = (a, c) = 1$, то $(a, bc) = 1$;
3. Якщо $ab \vdots c$ і $(a, c) = 1$, то $b \vdots c$;
4. Якщо $(a, b) = 1$, то $c \vdots ab$ тоді і тільки тоді, коли $c \vdots a$ і $c \vdots b$;
5. Якщо $(a, b) = 1$, то $(ac, b) = (c, b)$.

Задачі на ілюстрацію понять

1. Що можна сказати про НСД і НСК таких чисел:
   а) 0 і 0? б) 25 і 0? в) 0 і -12?

2. Що можна сказати про НСД і НСК двох та трьох довільних послідовних натуральних чисел?

3. Яка частка і остача утворюються при діленні НСК на НСД будь-яких двох натуральних чисел?

4. Перевірити виконання рівностей для будь-яких натуральних чисел a та b:
   а) $(a, b) = (a, a - b) = (a + b, a - b)$;
   б) $([a, b], (a, b)) = (a, b)$;
   в) $([a, b], ab) = [a, b]$;
   г) $[[a, b], (a, b)] = [a, b]$.

5. Перевірити, чи є взаємно простими такі числа:
   а) 341 і 256; б) n і $2n + 1$; в) $n - 1$ і $2n + 1$; г) $n + 1$ і $2n + 1$.

6. Чи може бути так щоб $(a, b) = 1$ і $(a^n, b) \neq 1$n>1?

Задачі на техніку обчислень та перетворень

7. Нехай $(a, b) = (m, n) = (b, n) = 1$. Встановити, чи може сума $\frac{a}{b} + \frac{m}{n}$ бути цілим числом, коли $|bn| \neq 1$.

8. Знайти НСД таких чисел:
   а) $a = -231, b = 546$; в) $a = 3763, b = 3337$;
   б) $a = 420, b = 630, c = 1155$; г) $a = 1023, b = 1518, c = 14883$.

9. Знайти всі можливі значення НСД натуральних чисел:
   а) $7n + 8$ і $6n + 5$; б) $8n + 5$ і $6n + 9$.

10. Знайти $(3m + 5n, 8m + 13n)$, якщо $(m, n) = 5$.

11. Знайти лінійне зображення НСД таких чисел:
   а) $a = 822, b = 1734$; в) $a = 903, b = -731$;
   б) $a = -826, b = 4373$; г) $a = 1445, b = 629$.

12. Знайти НСК таких чисел:
   а) $a = 252, b = 468$; в) $a = 28, b = 29, c = 30$;
   б) $a = -381, b = 178$; г) $a = 84, b = 147, c = 245$.

13. Розв'язати систему рівнянь в множині $\mathbb{N}$:
   а) $\begin{cases} ab = 720, \\ (a,b) = 4; \end{cases}$ в) $\begin{cases} a+b = 667, \\ [a,b] = 120(a,b); \end{cases}$
   б) $\begin{cases} (a,b) = 4, \\ [a,b] = 24; \end{cases}$ г) $\begin{cases} \frac{a}{(a,b)} + \frac{b}{(a,b)} = 7, \\ [a,b] = 120. \end{cases}$

14. Знайти при яких натуральних n є скоротним дріб:
   а) $\frac{8n+71}{5n+46}$; б) $\frac{3n-1}{4n-5}$; в) $\frac{12n-1}{4n+3}$; г) $\frac{8n-2}{-7n+4}$?

15. Знайти НСД всіх чисел виду $7^{n+2} + 8^{2n+1}$, де $n \in \mathbb{N}$ і $n < 2003$.

Задачі на доведення

16. Довести, що ірраціональним є число: а) $\sqrt[3]{3}$; б) $\sqrt[5]{5}$; в) $\sqrt[p]{p}$ для будь-якого простого числа p.

17. Довести, що для довільних натуральних m і n:
   а) $(m, n) = (7m + 5n, 4m + 3n)$; в) $([m, n], mn) = [m, n]$;
   б) $([m, n], (m, n)) = (m, n)$; г) $(\frac{[m,n]}{m}, \frac{[m,n]}{n}) = 1$.

18. Нехай натуральні числа m та n є взаємно простими. Довести, що:
   а) $(m + n, 2m + n) = 1$; г) $(2^m - 1, 2^n - 1) = 1$;
   б) $(m + n, mn) = 1$; д) $(2^{2^n} + 1, 2^{2^m} + 1) = 1$ при $n \neq m$;
   в) $(m - n, m) = 1$; е) $\frac{2m+n}{m(m+n)}$ - нескоротний дріб.

19. Довести, що коли натуральні числа $2^m - 1$ і $2^n - 1$ є взаємно простими то, числа m та n також є взаємно простими.

20. Довести, що $(2^{1986}-1, 2^{1983}-1) = 7$.

21. Дано взаємно прості натуральні числа n і $k (n > k)$.
Кожне з чисел множини $M = \{1; 2; 3; \cdots; (n-1)\}$ пофарбовано або в жовтий, або в блакитний колір, причому виконуються такі умови:
а) для кожного $i \in M$ числа i та $n-i$ пофарбовано в один колір;
б) для кожного $i \in M \setminus \{k\}$ числа i та $|k-i|$ пофарбовано в один колір.
Довести, що всі числа множини M пофарбовано в один колір.

22. Нехай $d = (a_1, a_2, \ldots, a_n)$. Довести, що існують цілі числа $k_1, k_2, \ldots, k_n$ такі, що $d = k_1a_1 + k_2a_2 + \cdots + k_na_n$.

23. Нехай $a_1, a_2, \ldots, a_n$ – цілі числа, з яких хоча б одне відмінне від нуля, та існують цілі числа $k_1, k_2, \ldots, k_n$ такі, що $d = k_1a_1 + k_2a_2 + \cdots + k_na_n$. Довести, що число d є найбільшим спільним дільником чисел $a_1, a_2, \ldots, a_n$.

24. Довести, що серед трьох послідовних цілих чисел завжди знайдеться число, яке взаємно просте з двома іншими.

Творчі задачі

25. Встановити можливість узагальнення задачі 9 на числа $kn+l$ і $mn+t$ для заданих натуральних чисел k, l, m, t.

26. Дослідити істинність твердження: серед n послідовних натуральних чисел завжди існує число, яке є взаємно простим зі всіма іншими з цих чисел.

27. Знайти необхідні і достатні умови для виконання рівності $(i, j) = (ik + jl, im + jn)$ для довільних натуральних чисел i, j, k, l, m, n.

28. Для довільних заданих натуральних чисел m, n, k дослідити $(m, m+n, m+2n, \cdots, m+kn)$ та $[m, m+n, m+2n, \cdots, m+kn]$.

29. Числова послідовність, в якій $u_1 = u_2 = 1$, а кожен наступний член, починаючи з третього, дорівнює сумі двох попередніх, тобто $u_{n+2} = u_{n+1} + u_n$, називається рядом Фібоначчі. Числа цього ряду:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \cdots$$

називають числами Фібоначчі.

Встановити істинність чи хибність таких тверджень для чисел Фібоначчі:

а) $u_{n+m} = u_{n-1}u_m + u_n u_{m+1}$;

б) $u_{n+1}^2 = u_n u_{n+2} + (-1)^n$;

в) якщо $n \vdots m$, то $u_n \vdots u_m$;

г) сусідні числа Фібоначчі завжди є взаємно простими;

д) $(u_n, u_m) = u_{(n,m)}$;

е) серед чисел Фібоначчі немає такого, яке ділиться на 2001.

Задачі з олімпіад

30. Знайти всі цілі значення x при яких вираз $\dfrac{7x+1}{3x+4}$ набуває цілих значень.

31. Нехай m, n - натуральні числа, причому m - непарне. Довести, що $(2^m - 1, 2^n + 1) = 1$.

32. До натуральних чисел a і b, $a > b$, застосовують алгоритм Евкліда для знаходження найбільшого спільного дільника цих чисел. Довести, що кількість кроків алгоритму (ділень з остачею) не перевищує $5p$, де p – кількість цифр в десятковому записі числа b.

33. Дано взаємно прості натуральні числа m та n. Знайти найбільший спільний дільник чисел $5^m + 7^m$ та $5^n + 7^n$.

34. Довести, що число $1979^2 + 2^{1979}$ взаємно просте з числом 1979.

35. Довести, що жодне з чисел Фібоначчі не є степенем числа 7.

36. Чи існують такі натуральні числа m і n, для яких виконується рівність:
    а) $\text{НСД}(m+n, mn) - \text{НСД}(m, n) = 2000$;
    б) $\text{НСД}(m+n, mn) - \text{НСД}(m, n) = 2001$?

37. Нехай p і q – взаємно прості числа. Ціле число n назвемо "гарним", якщо його можна подати у виді $px + qy$, де x і y – цілі невід'ємні числа, і "поганим" в протилежному випадку. Довести, що найбільшим "поганим" числом є $a = pq - p - q$, і завжди, якщо n – "гарне", то $a - n$ – "погане" і навпаки.

§ 1.3 Прості і складені числа. Канонічна форма натурального числа

Література: [1] стор. 89–93, 96–99; [2] стор. 86–91, 93–98; [3] стор. 364–371; [4] стор. 42–46.

Теоретичні відомості

Натуральне число $p > 1$ називають простим, якщо воно має тільки два натуральних дільники 1 і p та складеним, якщо воно має більше двох натуральних дільників. Таким чином, маємо розбиття множини натуральних чисел $\mathbb{N} = \{1\} \cup P \cup S$, де P – множина всіх простих чисел і S – множина всіх складених чисел.

Кожне натуральне число $n > 1$ ділиться хоча б на одне просте число.

Якщо n – натуральне число і p – просте число, то має місце одне з двох тверджень $n \vdots p$ або $(n, p) = 1$.

Якщо добуток двох або кількох натуральних чисел ділиться на просте число p, то хоча б один із співмножників ділиться на це число p.

Найменший простий дільник складеного натурального числа $n > 1$ не перевищує $\sqrt{n}$.

Основна теорема арифметики. Кожне натуральне число $n > 1$ є простим або може бути записаним у вигляді добутку простих чисел і притому єдиним способом, якщо не брати до уваги порядок розміщення множників.

Запис натурального числа $n > 1$ у вигляді $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, де $p_1, p_2, \ldots, p_k$ – попарно взаємно прості числа і α_i – натуральні числа, називається канонічною формою числа n.

Якщо натуральне число $n = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_1^{\alpha_k}$ записано у канонічній формі і $n \vdots c$, то $c = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_k^{\varepsilon_k}$, де $0 \leqslant \varepsilon_i \leqslant \alpha_i$ для всіх $0 \leqslant i \leqslant k$.

Нехай $a = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_1^{\alpha_k}$ і $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, де $\alpha_i, \beta_i \geqslant 0$. Такий запис іноді називають узагальненою канонічною формою. Тоді

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \quad \text{де} \quad \gamma_i = min\{\alpha_i, \beta_i\};$$
$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \quad \text{де} \quad \delta_i = max\{\alpha_i, \beta_i\}.$$

Задачі на ілюстрацію понять

1. Які з наступних натуральних чисел є простими або складеними: 101, 1111, 2121, 4327, 5432?

2. Знайти всі прості числа, які містяться між числами:
   а) 75 і 100; б) 150 і 175; в) 2550 і 2572.

3. Відомо, що при діленні з остачею простого числа p на 30 отримали $p = 30q + r, \quad 0 \leqslant r < 30$. Чи може бути число r складеним?

4. Вказати найменше складене число виду $n^2 - n + 11$, де $n \in \mathbb{N}$.

5. Якою може бути остача при діленні простого числа $p > 5$ на 6?

Задачі на техніку обчислень та перетворень

6. Знайти канонічний розклад числа n, якщо:
   а) $n = 496$; е) $n = 7^6 + 7^3 - 6$;
   б) $n = 1761$; є) $n = 5^6 + 5^3 - 2$;
   в) $n = 36125$; ж) $n = 2^{18} + 3^{18}$;
   г) $n = 5^4 + 5^3 - 6$; з) $n = 7^8 - 1$;
   д) $n = 536^2 - 241^2$; к) $n = 5^8 - 4$.

7. Скільки існує способів розкладу числа $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ в добуток двох взаємно простих множників?

8. Чи може сума $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p}$ бути цілим числом для деякого простого числа p?

9. Перевірити, чи можуть бути одночасно простими числа:
   а) $p, p + 5$ і $p + 10$; в) $p, p + 2$ і $p + 4$;
   б) $p, p + 2$ і $p + 5$; г) $p, p + 4$ і $p + 14$.

10. Знайти таке просте число p, щоб простими були також числа:
    а) $2p^2 + 1$; в) $2p + 1$ і $4p + 1$; д) $p + 9$ і $p + 15$;
    б) $p^2 + 8$; г) $8p^2 + 1$ і $8p^2 + 2p + 1$; е) $4p^2 + 1$ і $6p^2 + 1$.

11. Знайти всі цілі числа n, для яких число $|n^2 - 7n + 10|$ є простим.

12. Знайти прості числа p, для яких число $2p + 1$ є кубом натурального числа.

13. Ціле число a таке, що число $3a$ можна подати у вигляді $x^2 + 2y^2$, де x і y – цілі числа. Перевірити, що і число a можна подати в такому ж вигляді.

Задачі на доведення

14. Довести, що для складених натуральних чисел n числа Мерсенна $M_n = 2^n - 1$ є складеними.

15. Довести, що сума n послідовних непарних чисел при $n > 1$ є складеним числом.

16. Довести, що коли добуток двох взаємно простих натуральних чисел є квадратом натурального числа, то кожен із співмножників також є квадратом деякого натурального числа.

17. Довести, що число $2^{10} + 5^{12}$ є складеним.

18. Довести нескінченність множини простих чисел виду:
    а) $p = 3k + 1, k \in \mathbb{N}$; в) $p = 4k - 1, k \in \mathbb{N}$;
    б) $p = 3k + 8, k \in \mathbb{N}$; г) $p = 6k + 5, k \in \mathbb{N}$.

19. Пронумеруємо всі прості числа так: $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \cdots$. Довести, що
    а)$p_k \leqslant 2^{2^{k-1}}$, причому рівність виконується тільки при $k = 1$;
    б) $p_k > 2k$, де $k \geqslant 5$;
    в) $p_{k+1} < p_1 p_2 \cdots p_k, k > 1$;
    г) $p_1 p_2 \cdots p_k > n$, де $p_k \leqslant n$ і $n > 2$.

20. Довести, що коли число $F_n = 2^n + 1$ є простим (числа Ферма), то $n = 2^k$ для деякого невід'ємного цілого числа k.

21. Довести, що для будь-яких натуральних чисел m, n, k:
    а) $m \cdot n \cdot k \cdot (m, n, k) = [m, n, k] \cdot (m, n) \cdot (n, k) \cdot (m, k)$;
    б) $mnk = [m, n, k](mn, mk, nk)$;
    в) $(m, [n, k]) = [(a, b), (a, c)]$;
    г) $[m, (n, k)] = ([m, n], [m, k])$.

Творчі задачі

22. Встановити, якою може бути остача від ділення квадрата простого числа на 30.

23. Описати властивості множин остач від ділення квадрата простого числа $p > 5$ на числа $3 < m < 15$ відносно операції $\otimes$ множення остач ($r_1 \otimes r_2$ дорівнює остачі від ділення добутку $r_1 \cdot r_2$ на m).

24. Вивчити множину натуральних чисел виду $n^2 + n + 41$, де $n = 0, 1, 2, 3, \cdots$, на предмет встановлення їх простоти.

25. Описати множину всіх натуральних чисел a, для яких з того, що p і $p^2 + a$ є простими, слідує, що простим є число $p^3 + a$.

26. Дослідити, як часто в натуральному ряду зустрічаються прості числа виду $4n^2 + 1$.

27. Нехай p - просте число. Дослідити, для яких чисел $m, n \in \{1, 2, \cdots, 9\}$ число $mp + n$ є квадратом або кубом натурального числа.

Задачі з олімпіад

28. В сім'ї, що складається з п'яти осіб (тато, мати та троє дітей), помітили, що коли перемножити вік усіх членів сім'ї між собою, то отримаємо 1998. Який вік мають члени сім'ї, якщо тато старший за матір на 10 років?

29. Знайти всі пари (p, q) простих чисел такі, що число $2^p - 1$ ділиться на q і серед простих дільників числа $q - 1$ є лише числа 2,3,5 та 7.

30. Нехай p – просте число, більше 2. Знайдіть суму остач від ділення чисел $1^p, 2^p, \cdots, (p-1)^p$ на p^2.

31. Доведіть, що не існує простих чисел a, b, c, d для яких має місце рівність $a^2 + b^2 + c^2 + d^2 = abcd + 4$.

32. Послідовність $a_1, a_2, \ldots$ натуральних чисел така, що $a_{n+2} = a_{n+1}a_n + 1$ при всіх натуральних n. Довести, що при всіх $n > 10$ число $a_n - 22$ є складеним.

33. Розкласти число $989 \cdot 1001 \cdot 1007 + 320$ на прості множники.

34. Натуральні числа a, b і c такі, що $\frac{ab}{a-b} = c$. Відомо також, що числа a, b і c не мають спільного натурального дільника, більшого 1. Довести, що число $a - b$ є квадратом натурального числа.

35. Знайти всі четвірки чисел k, l, m, n, які задовольняють рівняння $k^l + k^m - k^n = 2000$.

36. Добуток деяких 48 натуральних чисел має рівно 10 різних простих дільники. Довести, що з цих чисел можна вибрати чотири, добуток яких є квадратом натурального числа.

§ 1.4 Системні числа

Література: [1] стор. 79–88; [2] стор. 76–86; [3] стор. 385–388.

Теоретичні відомості

Розрізняють непозиційні і позиційні системи числення.

Під непозиційною системою числення розуміють систему, в якій кожна цифра завжди позначає те саме число незалежно від її місця (позиції) в запису числа. Однією з них є римська система числення, яка до цих пір має застосування. У ній для запису чисел використовують сім цифр: цифра I означає одиницю, цифра V – п'ять, цифра X – десять, L – п'ятдесят, C – сто, D – п'ятсот, M – тисячу. Для запису чисел у цій системі застосовують принцип додавання і віднімання. Він полягає в тому, що:

1. коли менша цифра стоїть справа (після) від більшої, то вона додається до більшої, причому менша може повторюватися не більше трьох раз;

2. якщо менша цифра стоїть зліва (попереду) від більшої – то вона віднімається від більшої і повторення меншої цифри у цьому випадку не дозволяється.

Під позиційною системою числення розуміють систему, в якій значення кожної цифри визначається не тільки цифрою, а й позицією (місцем), яку вона займає в записі числа. З'ясуємо цю систему запису чисел детальніше.

Нехай g – деяке фіксоване число, більше від 1. Будемо називати його основою системи числення.

Кожне натуральне число m можна записати і притому єдиним способом у вигляді

$$m = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0,$$

де всі a_i – цілі невід'ємні числа, менші g і $a_n \neq 0$. Запис натурального числа m у такому вигляді називають систематичним записом з основою g. При цьому символи, якими позначають числа $a_n, a_{n-1}, \ldots, a_1, a_0$ називають цифрами числа m у системі числення з основою g (або: у g-ковій системі числення). У такій системі їх є g: $0, 1, 2, \ldots, g-1$. Скорочено вживають один із записів $m = \overline{a_n a_{n-1} \ldots a_1 a_0}_g = (a_n a_{n-1} \ldots a_1 a_0)_g = a_n a_{n-1} \ldots a_1 a_0{}_g$. Тоді $g = \overline{10}_g = (10)_g = 10_g$.

Кожне дробове додатне число $\frac{a}{b}$ можна записати і притому єдиним способом у вигляді

$$\frac{a}{b} = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0 + q_1 g^{-1} + q_2 g^{-2} + \cdots = \overline{a_n \ldots a_1 a_0, q_1 q_2 \ldots}_g,$$

де всі a_i, q_j – цілі невід'ємні числа, менші g і $a_n \neq 0$. Це систематичний запис додатних дробів з основою g і для нього додатково вжито знак –

кома. Застосовуючи знак мінус, можна записати у g-ковій системі числення всі раціональні числа.

Загальновживаною тепер є позиційна система числення з основою $g = 10$. Її називають десятковою позиційною системою і в цій системі основа числення не пишеться. Арифметичні операції додавання, віднімання, множення і ділення над числами записаними у g-ковій системі числення виконуються за тими ж правилами як і в десятковій системі числення з врахуванням таблиць додавання і множення одноцифрових чисел у g-ковій системі числення.

Потреби практики вимагають вміння переходити від однієї системи числення до іншої. Зокрема, електронно обчислювальні машини працюють у двійковій системі числення. Якщо число m записано у g-ковій системі числення і потрібно перейти до у s-кової системи числення, то поступають так:

1. записують число s у g-ковій системі числення;

2. виконують кілька ділень кутом числа m_g на число s_g і послідовно утворюваних часток на число s_g у g-ковій системі числення до тих пір, поки не дістанемо частку рівну нулю;

3. Знайдені остачі виражають цифрами у s-ковій системі числення і записують їх у зворотному порядку. Це і є записом числа m у s-ковій системі числення.

Перехід від g-кової системи числення до десяткової виконують ще й так. Кожну цифру числа m_g і основу g записують у десятковій системі числення і виконують відповідні обчислення у десятковій системі числення. Отриманий результат і є шуканим.

На практиці перехід від g-кової системи числення до s-кової системи числення зручніше виконувати так: спочатку перейти від g-кової системи числення до десяткової, а потім від десяткової до s-кової системи числення.

Задачі на ілюстрацію понять

1. Записати в римській нумерації числа: а) 326; б) 7940; в) 2654; г) 1097.

2. Записати в десятковій системі числення такі числа римської нумерації: а) XXIV; б) CLVII; в) DCCIXL; г) MIM; д) MMI; е) MDCXLVIII.

3. Чому дорівнює основа числення g, якщо в записі числа вжито найбільшу цифру цієї системи:
   а) 1025_g? в) 33333_g?
   б) $5(11)89_g$ г) $(10)11233_g$?

4. Чи вірно записані у відповідній системі числення такі числа:
   а) 3145_6; в) $5123(10)6_9$;
   б) 628547_8; г) $953(11)28_{12}$.

5. Записати в десятковій системі числення такі числа:
   а) мільярд; в) $11001,1111_2$;
   б) 33311_7; г) $437,321_8$.

6. Нехай дано число $m = \overline{a_1 a_2 \cdots a_n}_6$. Як зміниться величина цього числа, якщо до нього дописати справа нуль? два нулі? три нулі?

7. Записати скорочено числа у відповідній системі числення:
   а) $2 \cdot 4^5 + 3 \cdot 4^3 + 3 \cdot 4 + 2$; в) $5 \cdot 6^5 + 3 \cdot 6^3 + 2 \cdot 6^2 + 5$;
   б) $5^4 + 4 \cdot 5^3 + 5^2 + 3 \cdot 5 + 4$; г) $4 \cdot 10^7 + 2 \cdot 10^5 + 3 \cdot 10^4 + 10^2 + 1$.

8. Сказав Кащей Івану-Царевичу: "Жити тобі до завтрашнього ранку. Ранком з'явишся перед мої очі, я загадаю три цифри a, b, c. Ти - назвеш мені три числа: x, y, z. Вислухаю я тебе і скажу, чому дорівнює вираз $ax + by + cz$. Тоді відгадай, які a, b, c я загадав. Не відгадаєш-голову зніму. "Засмутився Іван-Царевич, пішов думу думати. Треба йому допомогти. Як?

9. Знайти невідомі цифри, позначені буквами, якщо має місце числова рівність $\overline{forty}_{10} + \overline{ten}_{10} + \overline{ten}_{10} = \overline{sixty}_{10}$ (різним буквам відповідають різні цифри).

10. Складіть таблиці додавання і множення в семірковій системі числення.

Задачі на техніку обчислень та перетворень

11. Обчислити:
   а) $231121_7 + 145621_7$; г) $454051_6 : 425_6$;
   б) $12312_6 - 23245_6$; д) $4,234_6 \cdot 1,54_6$;
   в) $4156_7 \cdot 562_7$; е) $2,435_8 : 0,52_8$.

12. Знайти значення числового виразу в десятковій системі числення:
   а) $232011_5 : 104_5 + 1234_5 \cdot 322_5 - 1022131_5$;
   б) $(563_8 + 217_8) \cdot 15_8 + (2365_8 - 636_8) : 17_8 - 15120_8$;
   в) $3215_7 \cdot 24_7 - 11461_7 : 25_7 + 1532_7 - 115044_7$;
   г) $[(351_6 \cdot 14_6 - 1153_6 : 31_6 - 150_6) : 205_6 + 3_6] : 5_6$.

13. Перевести з однієї системи числення в іншу:
   а) $33311_7 \to x_{12}$; в) $2786 \to x_8; x_2$; д) $4672510_9 \to x_3$;
   б) $32014_5 \to x_8$; г) $2012211_3 \to x_9$; е) $206315_7 \to x_5$.

14. Знайти x, y, z, якщо:
    а) $225_x = 89_{10}$; в) $37051_8 = x_6$; д) $\overline{xy}_4 = \overline{yx}_{10}$;
    б) $312_x - 1102_4 = 0$; г) $143_x + 105_x = 168_{10}$; е) $\overline{xyz}_{10} = \overline{zyx}_3$.

15. Знайти всі натуральні числа n такі, що перші цифри числа n^2 утворюють число n.

16. Розв'язати рівняння:
    а) $(\overline{xy}_{10})^2 = \overline{uvxy}_{10}$; б) $(\overline{xyz}_{10})^2 = \overline{uvtxyz}_{10}$.

Задачі на доведення

17. Нехай p - просте число, $p > 3$. Відомо, що для деякого натурального n число p^n містить 20 цифр. Довести, що серед них є принаймні 3 однакових цифри.

18. Довести, що число:
    а) 144 є квадратом натурального числа в системі числення з будь-якою основою $g > 4$;
    б) 1331 є кубом натурального числа в системі числення з будь-якою основою $g > 3$.

19. Довести, що:
    а) сума цифр квадрата будь-якого натурального числа не може дорівнювати 1997_{10}.
    б) число $11\cdots1$, яке містить в записі 3^n одиниць, ділиться на 3^n.

20. Довести, що в системі числення з будь-якою основою $g > 1$ числа $2(g-1)$ і $(g-1)^2$ записуються однаковими цифрами, але в зворотному порядку.

21. Довести, що в десятковій системі числення існує тільки одне чотирицифрове число, після піднесення якого до квадрату одержуємо число, в якого чотири останні цифри дають дане число.

22. Довести, що подільність суми $\overline{abc}_g + \overline{cba}_g$ на число g не залежить від середньої цифри.

Творчі задачі

23. Нехай маємо вагу з двома шальками і по одній гирі масою 1 грам, 3 грами, 9 грам, 27 грам і т.д. Чи можна за допомогою такого набору

гирь зважити 1 кілограм з точністю до 1 грама? Як зміниться ситуація, коли в наборі гирь будуть по одній гирі масою 1 грам, 5 грам, 25 грам, 125 грам і т.д.? Узагальніть цю задачу.

24. Число $\frac{1}{4}$ в десятковій системі числення записується скінченним десятковим дробом $0,25$, а в трійковій – нескінченним періодичним дробом $0,(02)$. Опишіть умови, при яких нескоротний звичайний дріб $\frac{p}{q}$ перетворюється в скінченний або нескінченний в системі числення за основою $g > 1$.

25. Вивчити можливість узагальнення задач 16 та 21 на більшу кількість цифр та інші системи числення.

26. Нехай $g = -4$. Розгляньте можливість подання раціонального числа у виді
$$\frac{a}{b} = a_n(-4)^n + \cdots + a_1(-4) + a_0 + a_{-1}(-4)^{-1} + \cdots.$$
Таку систему числення називають нега-четвірковою. Які її особливості?

27. Розгляньте систему числення за основою $g = 2i$ та установіть її зв'язок з з десятковою і нега-четвірковою системою числення. Зокрема, перевірте виконання рівностей:
$$\overline{(a_{2n}a_{2n-1}\cdots a_2a_1a_0)}_{2i} = \overline{(a_{2n}a_{2n-2}\cdots a_2a_0)}_{2i} + \overline{(a_{2n-1}a_{2n-3}\cdots a_1)}_{2i} = x + yi;$$
$$\overline{(a_{2n}a_{2n-1}\cdots a_2a_1a_0)}_{2i} = \overline{(a_{2n}a_{2n-2}\cdots a_2a_0)}_{-4} + 2i \cdot \overline{(a_{2n-1}a_{2n-3}\cdots a_1)}_{-4}.$$

Задачі з олімпіад

28. В десятизначному числі $m = \overline{a_1a_2\cdots a_{10}}$ цифра a_1 співпадає з кількістю одиниць в записі m, a_2 - з кількістю двійок, a_3 - трійок, ..., a_{10} - кількістю нулів. Знайти число m.

29. Довести, що останні цифри в послідовності чисел $1 \cdot 2 \cdot 3, 2 \cdot 3 \cdot 4, \cdots, (n-1) \cdot n \cdot (n+1)$ періодично повторюються.

30. Знайти всі натуральні числа $a = \overline{a_1a_2\cdots a_n}$ такі, що в десятковому записі $\overline{2a_1a_2\cdots a_n1} : \overline{1a_1a_2\cdots a_n2} = 21 : 12$.

31. Сума трьохзначних чисел $\overline{aab}, \overline{aba}, \overline{baa}$ в десятковому записі дорівнює 1998. Знайти усі трійки таких чисел.

32. Знайти чотири останні цифри числа: а) $1997 \cdot 5^{1998}$; б) $2001 \cdot 5^{1998}$ в його десятковому записі.

33. Довести, що число $11\cdots1$ (1998 одиниць) ділиться на 37.

34. Відомо, що число $\overline{a_1a_2a_3a_4a_5a_6}$ ділиться на 37. Встановити, чи ділиться на 37 число $\overline{a_2a_3a_4a_5a_6a_1}$.

35. Визначити, яку максимальну кількість трицифрових чисел можна утворити з цифр $1, 2, 3, 4, 5, 6, 7, 8$ так, щоб кожне з них не містило однакових цифр, та будь-які два з утворених чисел мали не більше однієї спільної цифри.

36. Шестизначне число записане різними цифрами ділиться на 37. Чи можна з цих цифр записати інше шестизначне число, яке також ділиться на 37?

37. Довести, що існує ціле число q таке, що в десятковому записі числа $q \cdot 2^{1000}$ немає жодного нуля.

38. Довести, що коли натуральне число m не закінчується нулем, то існує натуральне t, яке ділиться на m і таке, що в його десятковому записі немає жодного нуля.

39. Число y получають з натурального числа x деякою перестановкою його цифр. Довести, що для для будь-якого натурального x сума $x + y$ не може дорівнювати числу, яке записане 1967 дев'ятками.

40. Число y получають з натурального числа x деякою перестановкою його цифр.Відомо, що $x + y = 100\ldots00$ (200 нулів). Довести, що число x ділиться на 50.

41. Задано натуральне число k таке, що для будь-якого натуральногоn, яке ділиться на k, число $\overleftarrow{n}$ тоже ділиться на k ($\overleftarrow{n}$ – число, яке складається з тих самих цифр, що і n, але записаних у зворотному порядку). Довести, що число k є дільником числа 99.

42. Знайти найменше натуральне число, яке у десятковому записі починається з цифри 4 і зменшується в чотири рази від перестановки цієї цифри в кінець числа.

§ 1.5 Числові функції

Література: [1] стор. 93–95, 169–174; [2] стор. 92–93, 173–178; [3] стор. 368–369; [4] стор. 49–65;

Теоретичні відомості

Функцію f називають числовою, якщо множина $\mathbb{N}$ всіх натуральних чисел входить до її області визначення.

В теорії подільності цілих чисел знаходять застосування числові функції:

- τ – число натуральних дільників числа;
- σ – сума натуральних дільників числа;
- φ – функція Ейлера;
- E або [] – ант'є-функція або ціла частина числа;
- {} – дробова частина числа.

Значення функції Ейлера $\varphi(n)$ дорівнює кількості натуральних чисел, які не перевищують n і взаємно прості з ним.

Через $E(x)$ ($[x]$) позначають найбільше ціле число, яке не перевищує x.

Значення функції дробова частина числа обчислюється за формулою

$$\{x\} = x - [x].$$

Числова функція f називається мультиплікативною, якщо $f(n) \neq 0$ для кожного n і для будь-яких взаємно простих чисел m і n має місце рівність

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

Числові функції τ, σ і φ є мультиплікативними.

Мультиплікативні функції мають такі властивості:

1. $f(1) = 1$;

2. Добуток мультиплікативних функцій є мультиплікативною функцією;

3. Якщо числа $n_1, n_2, \ldots, n_k$ попарно взаємно прості і f – мультиплікативна функція, то $f(n_1 \cdot n_2 \cdots n_k) = f(n_1)f(n_2)\cdots f(n_k)$.

Якщо натуральне число $n = p_1^{\alpha_1} \cdot p_1^{\alpha_2} \cdots p_1^{\alpha_k}$ записано у канонічній формі, то $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$, $\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}-1}{p_k-1}$ і $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

Показник α простого числа p, яке входить до канонічного розкладу натурального числа $n!$, обчислюється за формулою

$$\alpha = E(\frac{n}{p}) + E(\frac{n}{p^2}) + \cdots + E(\frac{n}{p^k}) + \cdots.$$

Задачі на ілюстрацію понять

1. Знайти число і суму всіх натуральних дільників числа:
   а) 256; в) 998;
   б) 257; г) 989^2.

2. Знайти значення функції Ейлера для чисел 81, 256, 1331, 2041.

3. Знайти:
   а) $[1-\sqrt[3]{5}]$; в) $\{-1,3\}$;
   б) $[\sqrt{3}-1]$; г) x, якщо $[x]=-1$ і $\{x\}=0,75$.

4. Як обчислюються значення функцій τ, σ та φ для простих чисел?

5. Скільки є натуральних чисел, які менші за число p^3 і взаємно прості з ним для даного простого p.

6. Скільки є натуральних чисел, які менші за число 81 і взаємно прості з 6?

7. Натуральне число n ділиться на 2 і 9 і має 14 дільників. Знайти це число.

8. Скількома нулями закінчується число, яке дорівнює добутку всіх натуральних чисел від 1 до 2002 включно?

Задачі на техніку обчислень та перетворень

9. Знайти натуральне число n, якщо:
   а) n має тільки два простих дільники, $\tau(n)=12, \sigma(n)=1240$;
   б) n – найменше натуральне число, для якого $\tau(n)=18$;
   в) добуток всіх натуральних дільників числа n дорівнює $3^{30}\cdot 5^{40}$;
   г) $n=2^x5^y7^z; \tau(5n)=\tau(n)+8; \tau(7n)=\tau(n)+12; \tau(8n)=\tau(n)+18$.

10. Знайти кількість натуральних чисел, які менші від числа n і мають з ним найбільший спільний дільник d, якщо:
    а) $n=300, d=20$; в) $n=975, d=13$;
    б) $n=1072, d=8$; г) $n=1476, d=41$.

11. Нехай n - натуральне число. Знайти $\tau(n^3)$, якщо:
    а) $\tau(n^2)=15$ і n має тільки два простих дільники;
    б) $\tau(n^2)=105$ і n має тільки три простих дільники.

12. Розв'язати рівняння:
    а) $\varphi(x) = 12$; г) $\varphi(6^x) = 72$;
    б) $\varphi(x) = \frac{x}{2}$; д) $[3, 2x] = 1$;
    в) $\varphi(x) = \frac{x}{4}$; е) $[\frac{8m-m^2}{4}] = m, m \in \mathbb{Z}$.

13. Побудувати графіки функцій $y = \tau(x)$ і $y = \sigma(x)$, де $1 \leqslant x \leqslant 20$.

14. Побудувати графіки функцій:
    а) $y = 3[x]$; в) $y = \{x\} + 1$;
    б) $y = [3x]$; г) $y = [2x] + \{2x\} - 1$.

15. Знайти канонічний розклад чисел:
    а) $15!$; б) $30!$; в) $\frac{25!}{5!5!}$; г) $\frac{20!}{10!10!}$.

16. Скільки є натуральних чисел, які:
    а) кратні 786 і містяться між 10^6 і 10^7?
    б) менші від числа 1000 і не діляться ні на 5 , ні на 7?
    в) не більші від 12317 і взаємно прості з 1575?
    г) не більші від 1000 і не взаємно прості з 363?

Задачі на доведення

17. Довести, що добуток всіх натуральних дільників числа n дорівнює $n^{\frac{\tau(n)}{2}}$.

18. Довести, що:
    а) $[x + y] \geqslant [x] + [y]$; в) $\tau(mn) < \tau(m)\tau(n)$, якщо $(m, n) > 1$;
    б) $\varphi(4n) = 2\varphi(2n)$; г) $\varphi(mn) > \varphi(m)\varphi(n)$, якщо $(m, n) > 1$.

19. Натуральне число n називається досконалим, якщо $\sigma(n) = 2n$. Довести, що:
    а) 6, 28, 496, 8128 – досконалі числа;
    б) парне число n є досконалим тоді і тільки тоді, коли $n = 2^{k-1} \cdot (2^k - 1)$, де $k \geqslant 2$, а $p = 2^k - 1$ – просте число;
    в) довільне натуральне число з одним простим дільником не є досконалим;
    г) непарне натуральне число з двома простими дільниками не є досконалим.

20. Два натуральних числа m і n називаються дружніми, якщо $\sigma(n) = n + m = \sigma(m)$. Довести, що дружніми є такі пари чисел:
    а) 220 і 284; б) 1184 і 1210; в) 2620 і 2924; г) 18416 і 17296.

21. Довести формулу Гаусса: $\sum\limits_{n:d} \varphi(d) = n$.

22. Довести, що для будь-якого додатного дійсного числа x і натурального n виконується рівність $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

23. Довести, що $\tau(1) + \tau(2) + \cdots + \tau(n) = \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right]$.

Творчі задачі

24. Знайдіть необхідну і достатню умову того, щоб для даного натурального числа n число $\tau(n)$ було непарним.

25. Встановити, які значення може приймати числова функція $y = [x] - 2\left[\frac{x}{2}\right]$.

26. Вивести формулу для суми всіх чисел, які взаємно прості з натуральним числом n і менші від нього.

27. Перевірте, що для натурального числа $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ існує $\frac{1+\tau(n)}{2}$ різних розкладів на два множники. Чи існують формули для числа різних розкладів на три та більшу кількість множників.

28. Виведіть формулу для суми σ_k k-тих степенів всіх дільників числа $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, записаного в канонічній формі.

Задачі з олімпіад

29. Розв'зати рівняння: $[x] + \frac{1}{[x]} = \{x\} + \frac{1}{\{x\}}$.

30. Яких чисел більше серед цілих чисел від 1 до 1000000 включно:
    а) тих, що діляться на 11, але не діляться на 5, чи тих, що діляться на 12, але не діляться на 7?
    б) тих, що діляться на 13, але не діляться на 6, чи тих, що діляться на 15, але не діляться на 26?

31. Знайти всі натуральні числа k такі, що $\frac{\tau(n^2)}{\tau(n)} = k$ для деякого n.

32. Знайти всі натуральні числа n такі, що $\frac{n}{\tau(n)} = p$ для простого p.

33. Для будь-якого натурального числа n будується послідовність $n, \tau(n), \tau(\tau(n)), \cdots$, де $\tau(k)$ – кількість натуральних дільників числа k. Знайти всі такі n, для яких у відповідній послідовності немає квадратів цілих чисел.

§ 1.6 Скінченні ланцюгові дроби

Література: [1] стор. 99–111; [2] стор. 98–111; [3] стор. 380–385; [4] стор. 30–41.

Теоретичні відомості

Нехай $\frac{a}{b}$ – раціональне число та $b > 0$. Застосуємо до цілих чисел a і b алгоритм Евкліда:

$$\begin{array}{lll} a = bq_0 + r_1 & \text{і} & 0 < r_1 < |b|, \\ b = r_1q_1 + r_2 & \text{і} & 0 < r_2 < r_1, \\ r_1 = r_2q_2 + r_3 & \text{і} & 0 < r_3 < r_2, \\ \cdots\cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n & \text{і} & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_nq_n. & & \end{array}$$

З цих рівностей послідовно одержимо

$$\frac{a}{b} = q_0 + \frac{r_1}{b} = q_0 + \frac{1}{\frac{b}{r_1}} = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}} = \ldots = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Подання раціонального числа $\frac{a}{b}$ у останньому вигляді називають скінченним ланцюговим або неперервним дробом. Скорочено ланцюговий дріб записують у виді

$$\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n].$$

Число q_0 є цілою частиною дробу $\frac{a}{b}$, а $[0; q_1, q_2, \ldots, q_n]$ – його дробовою частиною. Всі неповні частки $q_1, q_2, \ldots, q_n$ є натуральними числами.

Кожне раціональне число можна подати у вигляді скінченного ланцюгового дробу і до того ж єдиним чином при умові, що $q_n > 1$.

Якщо $\frac{a}{b} = c$ є цілим числом, то $\frac{a}{b} = [c]$.

Дроби $\frac{P_0}{Q_0} = \frac{q_0}{1}$, $\frac{P_1}{Q_1} = q_0 + \frac{1}{q_1}$, $\frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}$, $\ldots$,

$$\frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_k}}}$$

називаються підхідними дробами даного ланцюгового дробу або відповідного йому числа $\frac{a}{b}$. При цьому $\frac{P_k}{Q_k}$ називається підхідним дробом k-го порядку. Якщо k – парне (непарне), то говорять, що підхідний дріб $\frac{P_k}{Q_k}$ парного (непарного) порядку. Очевидно, що $\frac{P_n}{Q_n} = \frac{a}{b}$.

Рекурентні формули для обчислення чисельників і знаменників підхідних дробів є такими:

$P_0 = q_0, \quad P_1 = q_0 q_1 + 1, \quad$ а при $s > 1 \quad P_s = P_{s-1} q_s + P_{s-2};$

$Q_0 = 1, \quad Q_1 = q_1, \quad$ а при $s > 1 \quad Q_s = Q_{s-1} q_s + Q_{s-2}.$

Усі обчислення зручно виконувати за схемою

k		0	1	2	...	n
q_k		q_0	q_1	q_2		q_n
P_k	1	q_0	$P_1 = q_0 q_1 + 1$	$P_2 = P_1 q_2 + P_0$		$P_n = P_{n-1} q_n + P_{n-2}$
Q_k	0	1	$Q_1 = q_1$	$Q_2 = Q_1 q_2 + Q_0$		$Q_n = Q_{n-1} q_n + Q_{n-2}$

Щоб обчислити P_s для $s = 1, 2, \ldots, n$ потрібно число q_s, яке стоїть над P_s, помножити на число P_{s-1}, яке передує P_s з цього самого ряду, і до добутку додати число P_{s-2}, яке стоїть в тому самому рядку і передує P_{s-1}. Аналогічно обчислюють і Q_s.

Підхідні дробі скінченого ланцюгового дробу мають такі властивості:

1. Чисельники і знаменники підхідних дробів є цілими числами; крім того знаменники є натуральними числами і утворюють зростаючу послідовність, починаючи з Q_1;

2. Якщо $s \geqslant 1$, то $P_s Q_{s-1} - P_{s-1} Q_s = (-1)^{s-1}$;

3. Кожен підхідний дрію нескоротний;

4. Якщо $s \geqslant 2$, то $P_s Q_{s-2} - P_{s-2} Q_s = (-1)^s q_s$;

5. Підхідні дроби парного порядку даного ланцюгового дробу утворюють зростаючу послідовність, а підхідні дроби непарного порядку – спадну послідовність;

6. Кожен підхідний дріб парного порядку даного ланцюгового дробу менший за будь-який підхідний дріб непарного порядку цього дробу;

7. Якщо $\frac{a}{b}$ – додатне раціональне число і $\frac{P_k}{Q_k}$ – підхідний дріб k-го порядку в розкладі $\frac{a}{b}$ в ланцюговий дріб, то

$$\left| \frac{a}{b} - \frac{P_k}{Q_k} \right| \leqslant \frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k^2}.$$

Якщо у рівнянні $ax + by = c$ з цілими коефіцієнтами і вільним членом числа a і b взаємно прості, то його загальний розв'язок у цілих числах можна подати у вигляді

$$x = (-1)^{n-1} \cdot c \cdot Q_{n-1} + bt, \quad y = (-1)^n \cdot c \cdot P_{n-1} - at,$$

де t – довільне ціле число, а P_{n-1} і Q_{n-1} – чисельник і знаменник передостаннього підхідного дробу розкладу числа $\frac{a}{b}$ у ланцюговий дріб.

Задачі на ілюстрацію понять

1. Чи є запис
   а) $[-1;2,1,3]$; в) $[-1;1,-1,2]$;
   б) $[0;1,2,3,1]$; г) $[0;1,6,2]$.
   поданням деякого числа у виді ланцюгового дробу?

2. Яким є ланцюговий дріб, якщо його передостанній підхідний дріб дорівнює $\frac{14}{9}$, а останній елемент $q_n = 2$?

3. Нехай для деякого ланцюгового дробу $[q_0;q_1,\cdots,q_n]$ маємо $\frac{P_k}{Q_k}: -2,-1,-\frac{3}{2},-\frac{7}{5}$. Знайдіть q_4.

4. Чи може дана послідовність чисел бути чисельниками послідовних підхідних дробів деякого ланцюгового дробу $[q_0;q_1,\cdots,q_n]$:
   а) 2, 3, 11, 47, 105; в) 2, -3, 11, 47, 105;
   б) -2, 3, 11, 47, 105; г) -2, -3, 11, 47, 105?

5. Чи може дана послідовність чисел бути знаменниками послідовних підхідних дробів деякого ланцюгового дробу $[q_0;q_1,\cdots,q_n]$:
   а) 1, 1, 4, 17, 38; в) 1, 1, 4, 4, 38;
   б) 1, -1, 4, 17, 38; г) -2, 1, 4, 17, 38?

6. Знайти похибку при заміні ланцюгового дробу $[4;3,1,2]$ кожним з його підхідних дробів та вказати яким є це наближення – з надвишком чи недостачею.

7. Встановити, який із ланцюгових дробів більший $[q_0;q_1,\cdots,q_n]$ чи $[q_0;q_1,\cdots,q_m]$, якщо $m > n$.

Задачі на техніку обчислень та перетворень

8. Наступні звичайні дроби подати у виді ланцюгових та знайти всі їхні підхідні дроби:
   а) $\frac{134}{217}$; в) $-\frac{99}{170}$; д) $-6\frac{28}{57}$; є) $\frac{83}{217}$;
   б) $\frac{2121}{1500}$; г) $-\frac{602}{367}$; е) $2\frac{314}{450}$; ж) $\frac{269}{170}$.

9. Подайте ланцюговий дріб у виді звичайного:
   а) [2;3,1,4]; в) [-3;1,2,1,1,5]; д) $[0;3,1,1,4,5]$;
   б) [0;4,1,2,5,6]; г) [-6;3,1,5,4,2]; е) $[0;1,2,1,1,4,5]$.

10. Порівняйте ланцюгові та підхідні дроби для раціональних чисел:
    а) $\frac{343}{226}$ і $\frac{226}{343}$; б) $-\frac{83}{217}$ і $-\frac{217}{83}$.

11. Поділити на 2 ланцюговий дріб:
    а) $[2;2,2,2]$; в) $[2;2,2,2,2,2]$;
    б) $[2;2,2,2,2]$; г) $[2;2,2,2,\cdots,2]$.

12. Розв'язати рівняння:
    а) $[q_0;2,3,4]=\frac{73}{30}$; в) $[-1;q_1,2,4]=-\frac{22}{31}$;
    б) $[2;1,2,q_3]=\frac{19}{7}$; г) $[0;2,3,4]=[0;x_1,x_2,\ldots,x_n]$.

13. Скоротити дроби:
    а) $\frac{1043}{3427}$; в) $-\frac{1872}{1560}$;
    б) $\frac{3587}{2743}$; г) $-\frac{3523}{1300}$.

14. Розв'язати рівняння в цілих числах:
    а) $119x+63y=34$; в) $23x+18y=5$;
    б) $12x+31y=170$; г) $74x+46y=30$.

15. Розв'язати рівняння в натуральних числах:
    а) $8x+13y=15$; в) $15x+28y=185$;
    б) $23x-42y=72$; г) $15x+35y=-5$.

16. Через які точки з цілими координатами проходять сторони трикутника з вершинами:
    а) $A(-1,1),B(1,3),C(2,2)$; в) $A(2,\frac{1}{2}),B(\frac{5}{2},8),C(13,5)$;
    б) $A(2,\frac{1}{2}),B(-1,7),C(3,15)$; г) $A(-2,-\frac{7}{2}),B(\frac{5}{2},-2),C(-\frac{1}{2},2)$;

17. При розрахунку зубчастої передачі від одного до іншого валу виявилося, що передаточне число (відношення зубців на валах) дорівнює $\frac{a}{b}$. Чи можна замінити це відношення дробом з меншими чисельниками і знаменниками так, щоб похибка не перевищувала α при:
    а) $\frac{a}{b}=\frac{355}{113}$ і $\alpha=0,002$? в) $\frac{a}{b}=\frac{73}{30}$ і $\alpha=0,001$?
    б) $\frac{a}{b}=\frac{587}{113}$ і $\alpha=0,001$? г) $\frac{a}{b}=\frac{648}{385}$ і $\alpha\in\{0,0005,0,0006\}$?

18. Чи можна подати дріб $\frac{100}{77}$ у виді суми двох додатних нескоротних дробів знаменники яких дорівнюють 7 та 11?

19. Для настилання підлоги в квадратній кімнаті з стороною 3 м є дошки шириною 11 см і 13 см та довжиною 3 м. Другі дошки на 20% дорожчі від перших. Скільки треба взяти дощок різної ширини для найекономнішого настилу?

20. За 30 монет однакової вартості купили 30 птахів трьох видів: перепелів, голубів та півнів. За кожних трьох перепелів заплатили 1 монету, за кожні два голуби також 1 монету і за кожного півня – по 2 монети. Скільки яких птахів було куплено?

21. Вивести формулу для запису ланцюгового дробу довжини n у виді звичайного:
    а) $[a; a, a, a, \cdots, a]$; в) $[a; b, a, b, \cdots, a]$;
    б) $[a; b, a, b, \cdots, b]$; г) $[a; b, b, b, \cdots, b]$.

Задачі на доведення

22. Довести, що коли в ланцюговому дробі довжини n всі неповні частки дорівнюють одиниці, то дріб дорівнює $\frac{u_{n+1}}{u_n}$, де u_{n+1} та u_n – числа Фібоначчі (дивись задачу 5.).

23. Довести властивості 1 – 7 підхідних дробів $\frac{P_k}{Q_k}$ даного ланцюгового дробу $[q_0; q_1, \cdots, q_n]$ (дивись теоретичні відомості до цього параграфа).

24. Нехай маємо рівняння $ax + by = c$ з цілими коефіцієнтами, $(a, b) = 1$ та $\frac{P_{n-1}}{Q_{n-1}}$ є передостаннім підхідним дробом розкладу числа $\frac{a}{b}$ у ланцюговий дріб. Довести, що:
    а) пара чисел $x_0 = (-1)^{n-1} c Q_{n-1}, \quad y_0 = (-1)^n c P_{n-1}$ є розв'язком цього рівняння;
    б) загальний розв'язок рівняння задають формули $x = x_0 + bt, \quad y = y_0 - at, \quad t \in \mathbb{Z}$.

Творчі задачі

25. Встановити, чи можуть члени кожної скінченної зростаючої послідовності натуральних чисел бути знаменниками послідовних підхідних дробів деякого ланцюгового дробу. Якщо це не так, то яким умовам повинні задовольняти такі послідовності?

26. Перевірити, чи виконуються нерівності із властивості 7 підхідних дробів для від'ємних раціональних чисел.

27. Нехай x – довільне дійсне число. Відомо, що $x = [x] + \{x\}$, де $0 \leqslant \{x\} < 1$. Якщо $\{x\} > 0$, то $\{x\} = \frac{1}{y}$, де $y > 1$, тобто $x = [x] + \frac{1}{y}$. Продовжуючи цей процес з числом y, ми для раціонального числа x, одержимо подання його у виді скінченного ланцюгового дробу.

Розглянути питання про можливість подання ірраціонального числа у виді нескінченного ланцюгового дробу (розгляньте, наприклад, число $\sqrt{2}$). Чи можуть серед них бути періодичні? Вивчити можливість такого узагальнення поняття підхідних дробів та їх властивості.

28. Встановити, чи існує залежність між раціональними числами, які зображені ланцюговими дробами $[q_0; q_1, \cdots, q_n]$ і $[kq_0; kq_1, \cdots, kq_n]$ для $k \in \mathbb{N}$.

29. Встановити зв'язок між поданнями у виді ланцюгових дробів для раціональних чисел $\frac{a}{b}$ та $\frac{b-a}{b}$.

30. Встановити залежності між ланцюговими і підхідними дробами для нескоротних раціональних чисел:
а) $\frac{p}{q}$ і $\frac{q}{p}$; б) $\frac{kp}{q}$ і $\frac{q}{p}$; в) $\frac{kp}{q}$ і $\frac{q}{lp}$; г) $\frac{kp}{q}$ і $\frac{lq}{p}$;

31. Створити теорію скінченних ланцюгових дробів для системи числення за основою g.

Задачі з олімпіад

32. Довести, що ірраціональне число можна подати у виді нескінченного періодичного (чистого або мішаного) ланцюгового дробу тоді і тільки тоді, коли воно є дійсним коренем квадратного рівняння з цілими коефіцієнтами.

33. Розв'язати рівняння $[0; x_1, x_2, \cdots, x_{2001}] = 1 - [0; 2, 3, 4, \cdots, 2001]$.

34. Розв'язати рівняння $[0; x_1, x_2, \cdots, x_n] = 1 - [0; 2, 3, 4, \cdots, n+1]$.

§ 1.7 Вибрані задачі

Двадцять перший математичний турнір міст, 1999

1. Нехай для цілих чисел a, b і c виконується умова: $a + b + c = 0$. Для кожної такої трійки обчислюють $d = a^{1999} + b^{1999} + c^{1999}$.
   а) Чи може $d = 2$?
   б) Чи може число d бути простим?

2. Довести, що існує нескінченна множина непарних натуральних чисел n, для яких число $2^n + n$ є складеним.

3. Декілька послідовних натуральних чисел записали в рядок так, що сума будь-якої трійки підряд записаних чисел ділиться на саме ліве число цієї трійки. Яка максимальна кількість чисел могла бути записаною, якщо останнє число послідовності є непарним?

4. Невтомні Фома і Ярема будують послідовність. Спочатку в послідовності одно натуральне число. Потім вони по черзі записують числа так: Фома записує число, додаючи до попереднього одну з його цифр, а Ярема - віднімаючи від попереднього одну з його цифр. Доведіть, що якесь число в цій послідовності повториться не менше 100 раз.

5. При яких n можна розставити натуральні числа від 1 до n по кругу так, щоб сума будь-яких двох сусідніх чисел ділилася на наступне за ними за годинниковою стрілкою число?

6. 100 гирок масою $1, 2, \cdots, 100$ грам розклали на дві шальки терезів так, що є рівновага. Довести, що можна забрати по 2 гирки з кожної шальки так, що рівновага не порушиться.

7. Розглянемо такі n, що набір гир масою $1, 2, \cdots, n$ грам можна розділити на дві частини, рівні за вагою. Чи вірне те, що для кожного такого n, більшого трьох, можна забрати по дві гирі з кожної частини так, що рівновага збережеться.

Задачі з московських математичних олімпіад

8. Довести, що $\tau(n) \leqslant 2\sqrt{n}$.

9. Суму цифр числа n позначимо через $S(n)$. Довести, що коли $S(n) = S(2n)$, то число n ділиться на 9.

10. Довести, що не існує цілих чисел a, b, c, d, які задовольняють рівностям:

$$\begin{cases} a \cdot b \cdot c \cdot d - a &= 1961, \\ a \cdot b \cdot c \cdot d - b &= 961, \\ a \cdot b \cdot c \cdot d - c &= 61, \\ a \cdot b \cdot c \cdot d - d &= 1. \end{cases}$$

11. Розглянемо суми цифр всіх чисел від 1 до 1 000 000 включно.В одержаних чисел знову розглянемо суми цифр, і так дальше, поки не отримаємо мільйон одноцифрових чисел. Яких чисел серед них більше – одиниць чи двійок?

12. Двохсотзначне число $89252525\ldots2525$ помножено на число $\overline{444x18y27}$ (x і y – невідомі цифри). Виявилося, що 53-я цифра отриманого числа (рахуючи справа) є 1, а 54-а – 0. Знайти x і y.

13. Довести, що кожне натуральне число є числом Фібоначчі або його можна подати у виді суми кількох різних чисел Фібоначчі.

14. Позначимо через $k(n)$ найменший номер k числа Фібоначчі u_k такий, що $u_k \vdots n$ і $u_{k+1} - 1 \vdots n$. Довести нерівність $k(n) \leqslant n^2$.

15. В якомусь році деяке число ні в один місяць не було неділею. Знайти це число.

16. Довести, що в послідовності u_n чисел Фібоначчі всі числа u_{5k} діляться на 5.

17. Знайти найбільше п'ятизначне число a, у якого четверта цифра більша п'ятої, третя більша суми четвертої і п'ятої, друга більша суми третьої, четвертої і п'ятої та п'ята цифра більша від суми решти.

18. Назвемо автобусний білет щасливим, якщо сума цифр його шестизначного номера ділиться на 7. Встановити, чи можуть бути два білети з послідовними номерами щасливими і, якщо так, то описати їх.

19. В кодовому замку є 3 кнопки з номерами 1, 2, 3. Про код, який відкриває замок відомо, що він тризначний. Замок відкривається, як иільки підряд і в правильному порядку натиснуті всі три цифри його коду. Яке найменше число раз потрібно натиснути на кнопки замка, щоб він відкрився?

20. В десятковому записі даного натурального числа n немає нулів. Якщо в ньому стоять рядом дві однакові цифри або два однакових двозначних числа, то їх дозволяється викреслити. Крім того, дозволяється також в будь-якому місці вставити дві однакові цифри або два однакових двозначних числа. Довести, що комбінуючи ці операції, можна з числа n отримати число, яке менше 10^9.

21. Натуральні числа m і n взаємно прості і $n < m$. Яке число більше $\left[1 \cdot \frac{m}{n}\right] + \left[2 \cdot \frac{m}{n}\right] + \cdots \left[n \cdot \frac{m}{n}\right]$ чи $\left[1 \cdot \frac{n}{m}\right] + \left[2 \cdot \frac{n}{m}\right] + \cdots + \left[m \cdot \frac{n}{m}\right]$?

22. Чи може число $n!$ закінчуватися цифрами $1976000\ldots000$?

23. Добуток деяких 1986 натуральних чисел має рівно 1985 різних простих дільників. Довести, що одне з цих чисел або добуток кілької з них є квадратом натурального числа.

24. Знайти найменше натуральне число, першою цифрою якого є 4 і яке зменшується у 4 рази від перестановки цієї цифри в кінець числа.

Задачі з різних олімпіад і математичних турнірів

25. Знайти суму цифр числа $123456789101112\ldots999998999999$. Скільки у цьому числі семірок?

26. Знайти найменше натуральне число $\overline{a_1 a_2 \ldots a_n}$, серед цифр якого у десятковому записі немає нулів, яке в сумі з числом $\overline{a_n \ldots a_2 a_1}$ дає число, цифри якого отримані перестановкою цифр даного числа.

27. Позначимо через $S(n)$ суму цифр числа n в десятковому записі. Довести, що існує нескінченно багато таких чисел n, що в записі n немає нулів і:
а) n ділиться на $S(n)$; б) n ділиться на $S(n) + 1$.

28. Знайти найменше натуральне число, сума цифр якого ділиться на 7, таке, що сума цифр наступного за ним числа також ділиться на 7.

29. Довести, що серед будь-яких 13 послідовних натуральних чисел знайдеться число з сумою цифр, яка ділиться на 7.

30. Довести, що існують безліч цілих чисел, які є точними квадратами і залишаються такими ж після дописування до них справа одиниці (в десятковому записі).

31. Числа x та y – цілі, причому число $6x + 11y$ ділиться на 31. Довести, що число $x + 7y$ також ділиться на 31.

32. Знайти всі натуральні числа n для яких число $n^3 + 3$ ділиться на $n + 3$.

33. В послідовності $\{u_n\} : u_1 = u_2 = 1, u_{n+2} = u_{n+1}^2 + u_n^2 (n \geqslant 1)$. Чи ділиться число u_{1986} на 7?

34. Ціле число a має властивість: число $3a$ можна подати у вигляді $x^2 + 2y^2$, де x та y – цілі чила. Довести, що і число a можна подати в такому вигляді.

35. Всі натуральні числа довільним чином розбиті на дві групи. Довести, що хоча б в одній з них знайдуться три числа, одне з яких є середнім арифметичним двох інших.

36. Довести, що найбільший спільний дільник цілих чисел m та $a - 1$ дорівнює найбільшому спільному дільнику чисел $a - 1$ та $\dfrac{a^m - 1}{a - 1}$.

37. Довести, що для будь-яких натуральних чисел m і n має місце рівність $(3^n - 2^n, 3^m - 2^m) = 3^{(m,n)} - 2^{(m,n)}$.

38. Натуральні числа a і b такі, що $a^2 + ab + 1$ ділиться на $b^2 + ab + 1$. Довести, що $a = b$.

39. Нехай n – натуральне число, а на дошці записані всі натуральні числа від n до $3n - 1$. Дозволяється стерти з дошки будь-які два числа a і $b (a \leqslant b)$ і записати замість них число $\frac{a}{2}$. Довести, що коли після серії таких операцій на дошці залишиться одне число, то воно буде менше за одиницю.

40. Довести, що число $3000 \ldots 01$ не є квадратом цілого числа.

41. Довести, що число $2^{58} + 1$ можна подати як добуток трьох натуральних чисел, більших 1.

42. Знайти всі цілі розв'язки рівняння:
    а) $\left[\frac{x+3}{x-4}\right] = \frac{x+2}{x-3}$; б) $\left\{\frac{3}{2}x - 1\right\} = -\frac{1}{6}x + \frac{2}{3}$.

43. Довести, що всі біноміальні коефіцієнти $C_n^1, C_n^2, \ldots, C_n^k, \ldots, C_n^{n-1}$ діляться на n тоді і тільки тоді, коли n – просте число.

44. Довести, що число $\frac{[2,4,\ldots,2n]}{C_{2n}^n}$ є цілим, і що $[2, 4, \ldots, 2n] = [n + 1, n + 2, \ldots, 2n]$.

45. Нехай p – просте число і $k \leqslant n$ – натуральні числа. Довести, що:
    а) $C_{np}^{nk} - C_n^k$ ділиться на p^2;
    б) $C_{np}^{nk} - C_n^k$ ділиться на p^3 при $p \geqslant 5$.

Задачі з шостої Соросовської олімпіади з математики

46. До натурального числа n додали 72 і в сумі отримали число, записане тими самими цифрами, що і число n, але в зворотному порядку. Знайти всі числа n, які задовольняють вказаній умові.

47. Нехай $p_1, p_2, \ldots, p_n$ – різні прості числа ($n \geqslant 2$). Із цих чисел складені всі можливі добутки, що містять парну кількість співмножників (усі співмножники – різні). Нехай S_n – сума всіх таких добутків. Наприклад, $S_4 = p_1p_2 + p_1p_3 + p_1p_4 + p_2p_3 + p_2p_4 + p_3p_4 + p_1p_2p_3p_4$. Довести, що $S_n + 1$ ділиться на 2^{n-2}.

48. Розв'язати рівняння $[x]\{x\} = 1999x$, де $[x]$ позначає найбільше ціле число, що не перевищує x, а $\{x\} = x - [x]$.

49. Знайти всі пари (p, q) простих натуральних чисел, для яких значення виразу $\frac{p}{q} + \frac{q+1}{p+1}$ є цілим числом.

50. Для простих чисел p, q і натуральних чисел n, k, r виконується рівність $p^{2k} + q^{2n} = r^2$. Довести, що число r є простим.

51. На дошці виписані 16 різних натуральних чисел, жодне з яких не перевищує 30. Довести, що серед виписаних чисел обов'язково знайдуться два взаємно простих.

52. Довести, що існує нескінченно багато натуральних чисел k, l, m, n, які задовольняють рівність

$$k^2 + l^2 + m^2 = n^{2001}.$$

53. На дошці записані всі п'ятицифрові числа, в записі кожного з яких цифри розташовані в строго зростаючому зліва направо порядку. Чи можна з кожного з них викреслити по одній цифрі так, щоб утворились всі чотирицифрові числа з такою ж властивістю?

54. Натуральні числа m і n такі, що сума дробів $\frac{m^n-1}{n-1}$ і $\frac{n^m-1}{m-1}$ є цілою. Довести, що кожен з вказаних дробів є цілим числом.

Розділ 2

Кільця

§ 2.1 Кільце та його найпростіші властивості. Підкільце

Література: [1] стор. 132–135; [2] стор. 133–137; [3] стор. 104–111.

Теоретичні відомості

Алгебра $(K; +, \cdot)$ з двома бінарними операціями (додавання і множення) називається *кільцем,* якщо операції мають властивості:

1. $(K; +)$ є абелевою групою.

2. $(K; \cdot)$ є півгрупою.

3. Операція множення дистрибутивна відносно операції додавання, тобто для будь-яких елементів a, b, c з K виконуються рівності

$a \cdot (b + c) = a \cdot b + a \cdot c$ і $(a + b) \cdot c = a \cdot c + b \cdot c$.

Кільце називається *комутативним*, якщо операція множення має властивість комутативності.

Кільце, яке містить тільки один нульовий елемент називається *нульовим*.

В кожному кільці визначається операція віднімання $-$, яка кожній впорядкованій парі (a, b) елементів кільця K ставить у відповідність розв'язок рівняння $b + x = a$.

Кільцем з одиницею називають ненульове кільце, яке містить нейтральний елемент відносно операції множення.

Елемент a кільця з одиницею K називають *оборотним*, якщо для нього існує в K обернений елемент a^{-1}. Множина K^* всіх оборотних елементів

кільця з одиницею K є групою відносно операції множення, заданої в K. Її називають *мультиплікативною групою кільця* K.

Комутативне кільце з одиницею, в якому для кожного ненульового елемента існує обернений елемент, називається *полем*.

Якщо в кільці K виконується рівність $a = bc$, то елемент b називають *лівим*, а елемент c – *правим дільником елемента* a. Якщо кільце K – комутативне, то елементи a, b називають *дільниками елемента* a і говорять, що *елемент* a *ділиться на елементи* b *і* c (короткий запис: $a \vdots b$, $a \vdots c$). При цьому c називають також *часткою від ділення* a *на* b (b є часткою від ділення a на c).

Якщо в кільці K елементи a і b ненульові і в той же час $a \cdot b = 0$, то їх називають *лівим і правим дільниками нуля* відповідно.

Елементи a і b комутативного кільця K з одиницею називаються *асоційованими*, якщо a ділиться на b і b ділиться на a.

Елементи a і b комутативного кільця K з одиницею є асоційованими тоді і тільки тоді, коли $a = bc$ і c є дільником одиниці в K.

Підмножина K_1 кільця K називається *підкільцем кільця* K, якщо K_1 є кільцем відносно операцій заданих в K. Підкільця K і $\{0\}$ кільця K називають *тривіальними*.

Непорожня підмножина K_1 кільця K є його підкільцем тоді і тільки тоді, коли вона разом з будь-якими своїми елементами a і b містить їх суму $a+b$, різницю $a-b$ і добуток $a \cdot b$ (іншими словами: замкнута відносно операцій додавання, віднімання і множення).

Кільце K називається *числовим*, якщо воно є підкільцем кільця комплексних чисел $\mathbb{C}$.

Задачі на ілюстрацію понять

1. Які з заданих числових множин утворюють кільце відносно операцій додавання і множення та містять одиницю:
   а) $\mathbb{Z}[-\sqrt{2}] = \{a - b\sqrt{2} | a, b \in \mathbb{Z}\}$;
   б) $\frac{1}{2}\mathbb{Q} = \{\frac{1}{2}q | q \in \mathbb{Q}\}$;
   в) $\mathbb{Z}[\sqrt{2}i] = \{a + b\sqrt{2}i | a, b \in \mathbb{Z}\}$;
   г) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} | a, b \in \mathbb{Z}\}$;
   д) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$;
   е) $5\mathbb{Z}[i] = \{a + bi | a, b \in 5\mathbb{Z}\}$;
   є) $\{\frac{a+bi\sqrt{3}}{2} | a, b -$ парні або непарні числа$\}$.

2. Які з заданих числових множин:
   а) $\{bi | b \in \mathbb{Q}\}$;
   б) $\{a + ai | a \in \mathbb{R}\}$;
   в) $\{a - bi | a, b \in 3\mathbb{Z}\}$;
   г) $\{a + bi | a, b \in \mathbb{R} \wedge ab > 0\}$;
   є підкільцями кільця комплексних чисел $\mathbb{C}$?

3. Знайти найменше числове кільце, яке містить числа $1, \sqrt{3}, \sqrt{5}$.

4. Перевірити, що множина $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ всіх остач від ділення на 8 є кільцем відносно операцій $\oplus$ та $\odot$ при яких $a \oplus b$ і $a \odot b$ дорівнюють остачі при діленні на 8 чисел $a+b$ та ab, відповідно. Знайти всі дільники нуля.

5. Навести приклади кілець, які не мають нетривіальних підкілець.

6. Навести приклади:
   а) нескінченного комутативного кільця без дільників нуля (числового і нечислового);
   б) нескінченного некомутативного кільця;
   в) скінченного кільця з дільниками нуля;
   г) скінченного кільця без дільників нуля;
   д) нескінченного комутативного кільця з дільниками нуля;
   е) комутативного кільця без одиниці;
   є) некомутативного кільця без одиниці;
   ж) скінченного некомутативного кільця.

7. Які числа є асоційованими елементами в кільцях: а) $\mathbb{Z}$; б) $\mathbb{C}$?

Задачі на техніку обчислень та перетворень

8. В кільцях з одиницею задач 1в, 1д, 1е знайти всі дільники одиниці.

9. Знайти всі пари асоційованих елементів в кільці $\mathbb{Z}[i]$.

10. Які з заданих множин матриць утворюють кільце відносно операцій додавання і множення:
    а) $\left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{N} \right\}$;
    б) $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$;
    в) $\left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \middle| a, b, c, d \in 2\mathbb{Z} \right\}$;
    г) $\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$;
    д) $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}$;
    е) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$;
    є) $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$;
    ж) $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$.
    Які з кілець комутативні? У кільцях з одиницею знайти всі дільники одиниці. Встановити наявність і вид дільників нуля.

11. Які з заданих множин дійсних функцій від однієї змінної, визначених на відрізку $[a, b]$, утворюють кільце відносно відомих операцій додавання і множення:

а) множина всіх неперервних функцій;
б) множина всіх непарних функцій;
в) множина всіх диференційовних функцій;
г) множина всіх обмежених функцій;
д) множина $\mathbb{Z}[x]$ всіх многочленів з цілими коефіцієнтами;
е) множина всіх многочленів не вище другого степеня?

Які з кілець комутативні? У кільцях з одиницею знайти всі дільники одиниці. Встановити наявність і вид дільників нуля.

12. Які з заданих множин пар цілих чисел утворюють кільце відносно операцій додавання і множення пар, які визначені так:
а) $(a,b)\oplus(c,d)=(ac,bd)$, $(a,b)\odot(c,d)=(a+c,b+d)$?
б) $(a,b)\oplus(c,d)=(a+c,b+d)$, $(a,b)\odot(c,d)=(ac+bd,bc+ad)$?
в) $(a,b)\oplus(c,d)=(a+c,b+d)$, $(a,b)\odot(c,d)=(ac,bd)$?
г) $(a,b)\oplus(c,d)=(a+c,b+d)$, $(a,b)\odot(c,d)=(ac-2bd,bc+ad)$?

Які з кілець комутативні? У кільцях з одиницею знайти всі дільники одиниці. Встановити наявність і вид дільників нуля.

13. Перевірити подільність чисел у відповідних кільцях:
а) $7+17\sqrt{2}$ на $3+4\sqrt{2}$ в кільці $\mathbb{Z}[\sqrt{2}]$;
б) $8+6i$ на $7+5i$ в кільці $\mathbb{Z}[i]$;
в) 8 на $2+2i\sqrt{3}$ в кільці $\mathbb{Z}[\sqrt{3}i]$;
г) $9+3\sqrt[3]{3}+2\sqrt[3]{9}$ на $2+\sqrt[3]{3}$ в кільці $\mathbb{Z}[\sqrt[3]{3}]$.

14. Розв'язати рівняння $AX=B$ та $YA=B$ в кільці $M(2,\mathbb{R})$, якщо:
а) $A=\begin{pmatrix}1&1\\2&2\end{pmatrix}$, $B=\begin{pmatrix}1&2\\3&4\end{pmatrix}$;
б) $A=\begin{pmatrix}1&1\\2&2\end{pmatrix}$, $B=\begin{pmatrix}4&4\\6&6\end{pmatrix}$;
в) $A=\begin{pmatrix}1&2\\3&4\end{pmatrix}$, $B=\begin{pmatrix}1&1\\2&2\end{pmatrix}$
г) $A=\begin{pmatrix}1&1\\2&2\end{pmatrix}$, $B=\begin{pmatrix}4&4\\8&8\end{pmatrix}$.

15. Описати будову всіх підкілець кільця $\mathbb{Z}$. Які з них містять одиницю?

Задачі на доведення

16. Нехай маємо кільця K і L з операціями $+$ і $\cdot$. На множині $K\times L$ визначені операції:

$$(a,b)\oplus(c,d)=(a+c,b+d);\qquad (a,b)\odot(c,d)=(a\cdot c,b\cdot d).$$

Довести, що $K \times L$ є кільцем (його називають прямим добутком кілець K і L)

17. Нехай p – просте число. Позначимо через $\mathbb{Q}_p$ множину всіх раціональних чисел, які можна подати у виді дробу з знаменником, який не ділиться на p. Довести, що:
    а) $\mathbb{Q}_p$ є підкільцем кільця раціональних чисел $\mathbb{Q}$ і містить 1;
    б) будь-який ненульовий елемент a з $\mathbb{Q}_p$ можна подати у виді $a = p^n\varepsilon$, де $n \in \mathbb{N} \cup \{0\}$, і ε є дільником одиниці в $\mathbb{Q}_p$.

18. Довести, що:
    а) перетин довільної непорожньої множини підкілець даного кільця є його підкільцем;
    б) множина K^* всіх дільників одиниці кільця K з одиницею є мультиплікативною групою цього кільця;
    в) у кільці K, яке містить n елементів, для кожного елемента a цього кільця виконується рівність $na = 0$;
    г) кільце $K = \{0, 1, a, b\}$ з визначальними співвідношеннями $a^2 = b, b^2 = a, ab = ba = 1, 1 + 1 = 0, 1 + a = b$ є полем;
    д) підмножина $K_1 = \{me | m \in \mathbb{Z}\}$ кільця K з одиницею e утворює підкільце;
    е) дільник одиниці кільця K з одиницею не може бути дільником нуля.

19. Довести, що коли в комутативному кільці K існує елемент a такий, що $aK = K$, то в K є одиниця і a є дільником одиниці.

20. Довести, що множина $\mathfrak{P}(M)$ всіх підмножин множини M є кільцем відносно операцій $\div$(симетрична різниця) та $\cap$.

21. Довести, що наступні множини є числовими кільцями:
    а) $D_2 = \{a_1 \cdot 2^{r_1} + a_2 \cdot 2^{r_2} + \cdots + a_n \cdot 2^{r_n} | n \in \mathbb{N} \wedge a_i \in \mathbb{Z} \wedge r_i \in \overline{\mathbb{Q}}\}$;
    б) $D_5 = \{a_1 \cdot 5^{r_1} + a_2 \cdot 5^{r_2} + \cdots + a_n \cdot 5^{r_n} | n \in \mathbb{N} \wedge a_i \in \mathbb{Z} \wedge r_i \in \overline{\mathbb{Q}}\}$;
    в) $D_6 = \{a_1 \cdot 6^{r_1} + a_2 \cdot 6^{r_2} + \cdots + a_n \cdot 6^{r_n} | n \in \mathbb{N} \wedge a_i \in \mathbb{Z} \wedge r_i \in \overline{\mathbb{Q}}\}$;
    г) $D_k = \{a_1 \cdot k^{r_1} + a_2 \cdot k^{r_2} + \cdots + a_n \cdot k^{r_n} | k, n \in \mathbb{N} \wedge a_i \in \mathbb{Z} \wedge r_i \in \overline{\mathbb{Q}}\}$,

    де $\overline{\mathbb{Q}} = \mathbb{Q}^+ \cup \{0\}$. Чи містять ці кільця одиницю?

22. Довести, що числа:
    а) $5 + 2\sqrt{3}$ та $4 - \sqrt{3}$ є асоційованими в кільці $\mathbb{Z}[\sqrt{3}]$;
    б) $1 + 2\sqrt{5}$ та $-8 + 3\sqrt{5}$ є асоційованими в кільці $\mathbb{Z}[\sqrt{5}]$;
    в) $25 - 17\sqrt{2}$ та $7 - \sqrt{2}$ є асоційованими в кільці $\mathbb{Z}[\sqrt{2}]$;
    г) $7 - 2i$ та $-2 - 7i$ є асоційованими в кільці $\mathbb{Z}[i]$.

23. Нехай K – скінченне кільце. Довести, що:
    а) коли K не містить дільників нуля, то воно є кільцем з одиницею, і всі його ненульові елементи оборотні, тобто $K^* = K \setminus \{0\}$;
    б) коли K містить одиницю, то кожний його елемент, який має односторонній обернений, є оборотним;
    в) коли K містить одиницю, то кожний його лівий дільник нуля є правим дільником нуля.

    Перевірити, чи будуть мати місце висновки тверджень б) і в), якщо в K немає одиниці.

24. Нехай кільце K містить одиницю і $x, y \in K$. Довести, що:
    а) коли $xy, yx \in K^*$, то $x, y \in K^*$;
    б) коли K не містить дільників нуля і $xy \in K^*$, то $x, y \in K^*$;
    в) коли K скінченне і $xy \in K^*$, то $x, y \in K^*$;
    г) без додаткових обмежень на кільце K з $xy \in K^*$ не обов'язково слідує $x, y \in K^*$.

Творчі задачі

25. Дослідити наявність дільників нуля в прямому добутку $K \times L$ кілець K та L (див. 2.13) в залежності від їх присутності в даних кільцях і навпаки.

26. Нехай K_1 підкільце кільця K. Встановити, які з наступних тверджень істинні:
    а) якщо K – кільце з одиницею, то K_1 – кільце з одиницею;
    б) якщо K_1 – кільце з одиницею, то K – кільце з одиницею;
    в) якщо K і K_1 – кільце з одиницею, то одиниця K співпадає з одиницею K_1;
    г) якщо K – кільце з дільниками нуля, то K_1 – кільце з дільниками нуля;
    д) якщо K_1 – кільце з дільниками нуля, то K – кільце з дільниками нуля;
    е) якщо $a \in K_1$ є дільником нуля в K_1, то a є дільником нуля в K;
    є) якщо $a \in K_1$ є дільником нуля в K, то a є дільником нуля в K_1;
    ж) якщо K_1 – кільце без дільників нуля, то K – кільце без дільників нуля.

27. Описати мультиплікативні групи $\mathbb{Z}^*[\sqrt{p}]$ для простих чисел $p = 2, 3, 7$.

Задачі з олімпіад

28. Описати мультиплікативну групу $\mathbb{Z}^*[\sqrt{5}]$.

§ 2.2 Область цілісності та поле часток. Подільність в області цілісності

Література: [1] стор. 136–141, 153–155 ; [2] стор. 137–141, 153–156; [3] стор. 439–444.

Теоретичні відомості

Комутативне кільце K з одиницею без дільників нуля називається *областю цілісності*.

Характеристикою кільця K з одиницею e називають найменше натуральне число n таке, що $ne = \underbrace{e+e+\cdots+e}_{n} = 0$; якщо такого натурального числа не існує, то говорять, що *кільце K має характеристику* 0.

Якщо кільце K має характеристику $p \neq 0$, то для кожного елемента $a \in K$ виконується рівність $pa = 0$.

Характеристикою будь-якої області цілісності є деяке просте число або нуль.

Якщо область цілісності K має характеристику 0, то для кожного ненульового елемента $a \in K$ і будь-якого натурального числа n маємо $na \neq 0$.

Для кожної області цілісності K існує поле P, яке містить K як підкільце. При цьому кожен елемент поля P дорівнює частці від ділення деяких двох елементів області цілісності K. Поле P називають *полем часток області цілісності K*.

У області цілісності K кожен елемент a має своїми дільниками всі дільники одиниці (елементи мультиплікативної групи K^*) та асоційовані з ним елементи. Їх називають тривіальними дільниками елемента a.

Відмінний від нуля і одиниці елемент a області цілісності K називають *простим (нерозкладним, незвідним)*, якщо його дільниками є тільки асоційовані з ним елементи та дільники одиниці (іншими словами: елемент a не має нетривіальних дільників).

Елемент a області цілісності K називають *складеним (розкладним, звідним)*, якщо серед його дільників є хоча б один відмінний від асоційованого з ним елемента та дільників одиниці (має нетривіальний дільник).

Елемент b області цілісності K, асоційований з простим елементом a, також є простим.

Елемент b області цілісності K називають спільним дільником елементів $a_1, a_2, \ldots, a_n$, якщо кожен з них ділиться на b. Найбільшим спільним дільником елементів $a_1, a_2, \ldots, a_n$ називають такий спільний дільник цих елементів, який ділиться на будь-який інший їхній спільний дільник.

Найбільший спільний дільник елементів $a_1, a_2, \ldots, a_n$ області цілісності K позначається символом $(a_1, a_2, \ldots, a_n)$ і визначається з точністю до множника, що є дільником одиниці.

Елементи a і b області цілісності K називають взаємно простими, якщо їх спільними дільниками є тільки дільники одиниці. Тоді пишуть $(a, b) = 1$.

Якщо b – простий елемент області цілісності K і $a \in K$, то $(a, b) = 1$ або $(a, b) = b$.

Задачі на ілюстрацію понять

1. Яку характеристику має числове кільце: а) $2\mathbb{Z}$; б) $\mathbb{Z}[i]$?
2. Якою є характеристика кільця $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ всіх остач від ділення на 8 (дивись задача № 4, § 2.1)
3. Навести приклад числового кільця, яке не є областю цілісності.
4. Чи є областю цілісності прямий добуток $(\mathbb{Q} \times \mathbb{R}; \oplus, \odot)$?
5. Чи є поле комплексних чисел полем часток кільця цілих гауссових чисел? Якщо це не так, то що є полем часток кільця $\mathbb{Z}[i]$?
6. Навести приклади простих і складених елементів в кільцях $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Q}$, $\mathbb{C}$.
7. Нехай K є підкільцем кільця L. Чи буде простий елемент в K простим в L і навпаки?
8. Чи має нетривіальні дільники число 13 з кільця $\mathbb{Z}[i]$?
9. Встановити простим чи складеним є число $3i$ в кільці $\mathbb{Z}[i]$.

Задачі на техніку обчислень та перетворень

10. На множині $\mathbb{Z}$ задано дві бінарні операції:
    а) $m * n = m + n + 1$, $m \circ n = mn + m + n$;
    б) $m * n = m + n + 5$, $m \circ n = mn + 5m + 5n + 20$.
    Встановити, чи є алгебра $(\mathbb{Z}; *, \circ)$ областю цілісності?
11. Знайти поля часток кілець $\mathbb{Z}[i\sqrt{3}]$ і $\mathbb{Z}[-\frac{1}{2} + \frac{i\sqrt{3}}{2}]$ та порівняти їх.
12. Знайти всі нетривіальні дільники числа 6 в кільці $\mathbb{Z}[i\sqrt{5}]$.
13. Встановити можливість розкладу на прості множники числа 2 в кільцях $\mathbb{Z}[i\sqrt{3}]$ та $\mathbb{Z}[i]$.

14. В кільці $\mathbb{Z}[i\sqrt{3}]$:
    а) знайти всі дільники числа 4;
    б) знайти всі спільні дільники чисел 4 і $2+2i\sqrt{3}$;
    в) встановити існування НСД чисел 4 і $2+2i\sqrt{3}$;
    г) довести, що число 4 неоднозначно розкладається на прості множники.

15. В кільцях з задачі 21(а-г) § 2.1 знайти елементи, які є складеними, але їх не можна розкласти на прості множники.

16. В кільцях $\mathbb{Z}[i\sqrt{5}]$ та $\mathbb{Z}[i\sqrt{17}]$ знайти числа, які неоднозначно розкладаються на прості множники.

17. Знайти кілька простих елементів в кільці $\mathbb{Q}_2$.

Задачі на доведення

18. Довести, що кільце $\mathbb{Z}[x]$ всіх многочленів від змінної x з цілими коефіцієнтами є областю цілісності.

19. Довести, що кільце $\mathbb{C}_{[a,b]}$ не є областю цілісності.

20. Довести, що елементи a, b області цілісності K асоційовані тоді і тільки тоді, коли існує дільник одиниці ε такий, що $a = b\varepsilon$.

21. Довести, що скінченна область цілісності є полем.

22. Довести, що характеристикою області цілісності є 0 або просте число.

23. Довести, що кожний асоційований до простого елемента в даній області цілісності також є простим.

24. Довести, що всі числа $a \in \mathbb{Z}[i]$ такі, що $|a|^2$ є простим числом, є простими елементами кільця $\mathbb{Z}[i]$.

25. Довести, що в області цілісності K кожний елемент, який має односторонній обернений є оборотним.

26. Довести, що $\mathbb{Q}[\sqrt{2}]$ є полем часток для кільця $\mathbb{Z}[\sqrt{2}]$.

27. Довести, що коли кільце K має характеристику $p \neq 0$, то для кожного елемента $a \in K$ виконується рівність $pa = 0$.

28. Нехай P є полем часток для області цілісності K. Довести, що характеристики P і K однакові.

29. Довести, що коли кільце K має характеристику 8, то воно містить підкільце, ізоморфне кільцю $\mathbb{Z}_8$.

30. Довести, що число елементів скінченного поля характеристики $p \neq 0$ є деяким натуральним степенем числа p.

Творчі задачі

31. Знайти необхідну і достатню умову того, щоб просте число $p \in \mathbb{Z}$ було простим елементом в кільці $\mathbb{Z}[i]$.

32. Нехай p - просте число. Встановити, які елементи є простими в кільці $\mathbb{Q}_p$ (дивись задачу 1.16).

33. Встановити, чи кожне складене число з кільця $\mathbb{Z}[\sqrt{n}](n \in \mathbb{N})$ має однозначний розклад на прості множники.

Задачі з олімпіад

34. Знайти всі прості елементи в кільці $\mathbb{Q}_2$.

35. Нехай K – комутативне кільце без одиниці. Елемент $a \in K$ називається складеним в K, якщо він ділиться на відмінний від себе елемент цього кільця. Опишіть множину складених чисел кільця $2\mathbb{Z}$. Чи має місце в цьому кільці аналог основної теореми арифметики?

36. Довести, що скінченне комутативне кільце без дільників нуля, яке містить більше одного елемента є областю цілісності.

37. Довести, що множина чисел виду $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, де $a, b, c \in \mathbb{Q}$, є областю цілісності. Знайти в ній елемент асоційований до елемента $1 - \sqrt[3]{2} + 2\sqrt[3]{4}$.

§ 2.3 Ідеали кільця. Конгруенції за ідеалом та фактор-кільце

Література: [1] стор. 141–147; [2] стор. 143–150; [3] стор. 430–433.

Теоретичні відомості

Непорожня підмножина I кільця K називається *лівим (правим) ідеалом кільця*, якщо виконуються умови:

1. Підмножина I замкнута відносно операцій додавання і віднімання;

2. $KI \subset I \quad (IK \subset I)$.

Підмножина I кільця K, яка є лівим і правим ідеалом, називається *двостороннім ідеалом* або *ідеалом кільця* K. У комутативному кільці кожен лівий і правий ідеали є двостороннім ідеалом.

Кожен лівий і правий ідеал кільця K є підкільцем кільця K.

Підмножини K і $\{0\}$ є ідеалами кільця K. Їх називають *одиничним і нульовим* відповідно та *тривіальними*.

Нехай K – комутативне кільце і $a \in K$. Множина всіх елементів виду $ka + na$ кільця K, де k – будь-який елемент цього кільця і n – будь-яке ціле число, є ідеалом K. Цей ідеал називають *головним ідеалом, породженим елементом* a і позначають (a) або $< a >$. Аналогічно визначають поняття головного ідеалу, породженого кількома елементами: $(a_1, a_2, \ldots, a_n) =< a_1, a_2, \ldots, a_n >= \sum_{i=1}^{n} k_i a_i + \sum_{j=1}^{s} n_j a_j$, де $k_i \in K$, $n_j \in \mathbb{Z}$.

Нехай U і V – ідеали кільця K. Множина $U + V = \{a + b | a \in U, b \in V\}$ називається *сумою ідеалів* U *і* V. Множина
$UV = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n | a_1, a_2, \ldots, a_n \in U, b_1, b_2, \ldots, b_n \in V, n \in \mathbb{N}\}$ називається *добутком ідеалів* U *і* V.

Перетин, сума і добуток ідеалів U і V кільця K є ідеалом кільця K.

Нехай I – ідеал кільця K. Елементи a і b кільця K називаються конгруентними за ідеалом I (за модулем I), якщо $a - b \in I$. Цей факт записують так: $a \equiv b \pmod{I}$. Якщо $I = (k)$, то пишуть $a \equiv b \pmod{k}$.

Відношення конгруентності між елементами кільця K за ідеалом I має такі властивості:

1. Відношення $\equiv$ є відношенням еквівалентності на множині K.

2. Клас еквівалентності з представником a має вид $\overline{a} = a + I$ і є суміжним класом адитивної групи K за її підгрупою I. Його називають класом лишків кільця K за ідеалом I з представником a.

3. Конгруенції можна почленно додавати, віднімати і множити.

Множину всіх класів лишків кільця K за ідеалом I позначають K/I. У цій множині визначаються операції додавання і множення так:

$$\overline{a}+\overline{b}=\overline{a+b}, \qquad \overline{a}\cdot\overline{b}=\overline{a\cdot b}.$$

Алгебра $(K/I;+,\cdot)$ є кільцем, яке називають фактор-кільцем або кільцем класів лишків кільця K за ідеалом I.

Задачі на ілюстрацію понять

1. Навести приклади лівих та правих ідеалів кільця $M(2,\mathbb{R})$.

2. Чи є лівим, правим та двостороннім ідеалом множина:

   а) $\{n|n\vdots 6 \wedge n\vdots 10\}$ в кільці $\mathbb{Z}$? б) $2\mathbb{Z}$ в кільці $\mathbb{Z}[i]$?

   в) $\left\{\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} | a\in\mathbb{Z}\right\}$ в кільці $M(2,\mathbb{Z})$?

   г) $\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} | a\in\mathbb{Q}\right\}$ в кільці $M(2,\mathbb{Q})$?

   д) $\left\{\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} | a\in\mathbb{R}\right\}$ в кільці $M(2,\mathbb{R})$?

   е) $\left\{\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} | a\in\mathbb{C}\right\}$ в кільці $M(2,\mathbb{C})$?

3. Які з чисел: $3-5i$, $4+6i$, $-15+9i$, $5-3i$ належать ідеалу $(3+5i)$ кільця $\mathbb{Z}[i]$? Які з них породжують цей ідеал?

4. При якій умові має місце рівність $n+(6)=5+(6)$, якщо $n\in\mathbb{Z}$?

5. Які з чисел: $-3+5i$, $7-8i$, $25+3i$, $-2+4i$, $1+i$, $1-i$, 123, $2+i$, $-2+3i$ є конгруентними за ідеалом (2) в кільці $\mathbb{Z}[i]$?

6. Скільки елементів містить фактор-кільце:
   а) $\mathbb{Z}/(0)$; б) $\mathbb{Z}/(1)$; в) $\mathbb{Z}/(4)$; $\mathbb{Z}[i]/(3)$?

7. Ідеал I області цілісності K називається простим, якщо K/I є областю цілісності. Наведіть приклади простих ідеалів в кільці $\mathbb{Z}$.

Задачі на техніку обчислень та перетворень

8. У кільці цілих чисел знайти ідеали:
   а) $(3,7)$; в) $(6,10)$; д) $(3,5,7)$;
   б) $(4,6)$; г) $(2,4,6)$; е) $(3,-6,9)$.

9. У кільці цілих чисел виконати такі дії над його ідеалами:
   а) $(3) \cap (5)$; г) $(4) \cap (8)$; є) $(6) \cap (8)$;
   б) $(3) \cdot (5)$; д) $(4) \cdot (8)$; ж) $(-6) \cdot (8)$;
   в) $(3) + (5)$; е) $(4) + (8)$; з) $(6) + (8)$.

10. На множині ідеалів $A = \{2\mathbb{Z}, 3\mathbb{Z}, -3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 8\mathbb{Z}, 12\mathbb{Z}\}$ кільця $\mathbb{Z}$ розглянути відношення включення $\subseteq$ та порівняти його з відношенням подільності на підмножині $B = \{2, 3, -3, 4, 6, 8, 12\}$ множини цілих чисел.

11. Які з рівностей мають місце в фактор-кільці $\mathbb{Z}[i]/(3)$:
   а) $1 + 2i + (3) = 1 - 2i + (3)$; г) $1 + 4i + (3) = 4 + i + (3)$;
   б) $1 + (3) = i + (3)$; д) $2 + i + (3) = 5 - 2i + (3)$;
   в) $3i + (3) = -1 + (3)$; е) $-1 - i + (3) = 2 + 2i + (3)$?

12. Побудувати фактор-кільця $\mathbb{Z}_4$, та $\mathbb{Z}_7$ і скласти таблиці Келі для додавання і множення. Знайти всі їх дільники нуля та мультиплікативні групи $\mathbb{Z}_4^*$ і $\mathbb{Z}_7^*$.

13. Розв'язати рівняння в кільці $\mathbb{Z}_6$:
   а) $\bar{3} + x = \bar{1}$); в) $\bar{5} \cdot x = \bar{2}$; д) $\bar{3} \cdot x = \bar{2}$; є) $\bar{2} \cdot x = \bar{3}$;
   б) $\bar{4} - x = \bar{5}$; г) $\bar{4} \cdot x = \bar{0}$; е) $\bar{5} \cdot x = \bar{0}$; ж) $\bar{4} \cdot x = \bar{5}$.

14. Побудувати фактор-кільце $\mathbb{Z}[i]/(3)$ та знайти $(\mathbb{Z}[i]/(3))^*$.

15. Скільки елементів містить фактор-кільце $\mathbb{Z}[i]/(5)$? Чи є воно полем?

16. У фактор-кільці $\mathbb{Z}[i]/(m)$ знайти всі дільники нуля і обернені елементи до a якщо:
   а) $m = 4, \quad a \in \{\bar{i}, \overline{2i}, \overline{1 - 2i}\}$;
   б) $m = 6i, \quad a \in \{\overline{2 + 5i}, \overline{4 + i}\}$.

17. Знайти всі ідеали кілець: а) $\mathbb{Z}_6$; б) $\mathbb{Z}_{16}$.

Задачі на доведення

18. Нехай K – кільце і $U = \{x | x \in K \wedge (\exists n \in \mathbb{Z}^+)(na = 0)\}$. Довести, що U є ідеалом кільця K.

19. Нехай K – комутативне кільце і $U = \{x | x \in K \wedge (\forall y \in K)(xy = 0)\}$. Довести, що:
   а) U є ідеалом кільця K;
   б) коли K містить одиницю, то $U = \{0\}$.
   Навести приклад комутативного кільця, для якого $U \neq \{0\}$.

20. Нехай K_1 – підкільце кільця K та I – ідеал кільця K. Довести, що $I_1 = K_1 \cap I$ є ідеалом кільця K_1.

21. Довести, що в будь-якому полі немає нетривіальних ідеалів.

22. Довести, що для ідеалів кільця цілих чисел умова $m\mathbb{Z} \subseteq n\mathbb{Z}$ виконується тоді і тільки тоді, коли $m \vdots n$.

23. Довести, що фактор-кільце K/I кільця K з одиницею за будь-яким його ідеалом I містить також одиничний елемент.

24. Нехай K є областю цілісності. Довести, що:
    а) коли $(\{a, b\}) = (d)$, то $a \in (d), b \in (d)$;
    б) коли $(\{a, b\}) = (d)$, то $(a, b) \vdots d$;
    в) коли $(\{a, b\}) = (d)$, то існують $x, y \in K$ такі, що $ax + by = d$;
    г) коли $(\{a, b\}) = (d), a \vdots c, b \vdots c$, то $d \vdots c$;
    д) коли $(\{a, b\}) = (d)$, то d і (a, b) є асоційованими;
    е) ненульовий елемент $a \in K \setminus K^*$, який не розкладається на прості множники, має хоч один нетривіальний дільник, який теж не розкладається на прості множники;
    є) за умови попереднього пункту для елемента $a \in K \setminus K^*$ в кільці K існує нескінченна послідовність елементів $a_1, a_2, \cdots, a_n, \cdots$, в якій кожний наступний елемент є нетривіальним дільником попереднього; при цьому $(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$, тобто, в K існує нескінченна послідовність ідеалів, в якій кожен наступний ідеал строго містить попередній.

25. Довести, що коли для елементів a, b, m області цілісності K має місце рівність $(a) \cap (b) = (m)$, то m є найменшим спільним кратним для a і b.

26. Довести, що в комутативному кільці K з одиницею:
    а) $a \vdots b$ тоді і тільки тоді, коли $(a) \subseteq (b)$, де $a, b \in K$;
    б) асоційовані елементи кільця породжують той самий головний ідеал;
    в) головний ідеал, породжений дільником e одиниці 1 кільця K співпадає з K, тобто $(e) = (1) = K$;
    г) головні ідеали, породжені елементами a і b рівні тоді і тільки тоді, коли a і b є асоційованими елементами і K – область цілісності.

27. Довести, що:
    а) $(2+\sqrt{3}) = \mathbb{Z}[\sqrt{3}]$; г) $(-i) = \mathbb{Z}[i]$;
    б) $(8+3\sqrt{7}) = \mathbb{Z}[\sqrt{7}]$; д) $(2i) = 2\mathbb{Z}[i]$;
    в) $(9-4\sqrt{5}) = \mathbb{Z}[\sqrt{5}]$; е) $(13+5\sqrt{7}) \subset (3+\sqrt{7})$ в $\mathbb{Z}[\sqrt{7}]$;

28. Довести, що деякого елемента a області цілісності K має місце рівність $(a) = K$ тоді і тільки тоді, коли $a \in K^*$.

29. Довести, що в області цілісності K з рівності $(a) \cap (b) = \{0\}$ випливає $a = 0$ або $b = 0$.

Творчі задачі

30. Для кожного натурального n опишіть множину всіх ідеалів кільця $M(n, \mathbb{R})$.

31. Нехай I_1, I_2 - ідеали кільця K, $I_1 + I_2 = \{x + y | x \in I_1, y \in I_2\}$ та $I_1 \cdot I_2 = \{\sigma x_i y_j | x_i \in I_1, y_j \in I_2\}$. Встановити зв'язки між множинами $I_1 \cdot I_2, I_1 \cup I_2, I_1 \cap I_2$ та $I_1 + I_2$. Знайти необхідну і достатню умову при якій має місце рівність $I_1 + I_2 = I_1 \cup I_2$.

32. Нехай I є ідеалом кільця K. Встановити, яке з тверджень істинне:
    а) якщо в кільці K є дільники нуля, то вони є в фактор-кільці K/I?
    б) якщо в фактор-кільці K/I є дільники нуля, то вони є в кільці K?
    Чи існують кільця та їх ідеали, в яких обидва твердження істинні?

33. Описати ідеали кільця $n\mathbb{Z}$.

Задачі з олімпіад

34. Нехай I є нетривіальним ідеалом кільця $C_{[a,b]}$. Довести, що для будь-яких $f_1, f_2, \cdots, f_n \in I$ існує точка $x_0 \in [a, b]$ така, що $f_i(x_0) = 0$ для всіх $1 \leqslant i \leqslant n$.

35. При яких натуральних n всі необоротні елементи кільця $\mathbb{Z}_n$ утворюють ідеал?

36. Довести, що множина I_s неперервних функцій, які перетворюються в 0 на фіксованій підмножині $S \subseteq [a, b]$, є ідеалом в кільці $C_{[a,b]}$. Чи вірно, що всякий ідеал цього кільця має вид I_s для деякої підмножини $S \subseteq [a, b]$?

§ 2.4 Гомоморфізми та ізоморфізми кілець

Література: [1] стор. 147–150; [2] стор. 150–153; [3] стор. 434–437.

Теоретичні відомості

Нехай $(K;+,\cdot)$ і $(K_1;\oplus,\odot)$ – кільця. Відображення f множини K на множину K_1 називають *гомоморфізмом кільця K на кільце K_1*, якщо виконуються умови:

1. $(\forall a,b\in K)(f(a+b)=a\oplus b)$ (читається: образ суми довільних двох елементів з кільця K дорівнює сумі їхніх образів);

2. $(\forall a,b\in K)(f(a\cdot b)=a\odot b)$ (читається: образ добутку довільних двох елементів з кільця K дорівнює добутку їхніх образів).

Якщо гомоморфізмом кільця K на кільце K_1 є взаємно однозначним відображенням (бієкцією), то його називають *ізоморфізмом*.

Відображення f множини K у множину K_1, яке задовольняє умовам 1 – 2 гомоморфізму називають *гомоморфізмом кільця K у кільце K_1*.

Гомоморфізм кільця K на кільце K_1 має такі властивості:

1. Образ нульового елемента першого кільця є нульовий елемент другого кільця.

2. Образ елемента $-a$ протилежного до даного елемента a кільця K, є елемент $-f(a)$, протилежний до образа $f(a)$ даного елемента.

3. Якщо в кільці K є одиничний елемент e, то його образ $f(e)$ є одиничним елементом кільця K_1; якщо в кільці K для елемента a існує обернений елемент a^{-1}, то $f(a^{-1})$ є оберненим елементом до елемента $f(a)$ в кільці K_1.

Нехай f є гомоморфізмом кільця K на кільце K_1. Множину всіх елементів кільця K, образами яких при гомоморфізмі f є нульовий елемент кільця K_1, називають *ядром гомоморфізму f* і позначають $Ker\,f$.

Ядро $Ker\,f$ будь-якого гомоморфізму f кільця K на кільце K_1 є ідеалом кільця K.

Теорема про гомоморфізми кілець. Якщо f є гомоморфізмом кільця K на кільце K_1, то фактор-кільце $K/Ker\,f$ і кільце K_1 ізоморфні.

Задачі на ілюстрацію понять

1. Задати гомоморфізм кільця $\mathbb{Z}$ на кільце $\mathbb{Z}_3$.

2. Чи можна задати гомоморфізм кільця $\mathbb{Z}_3$ на кільце $\mathbb{Z}_2$?

3. Чи можна задати гомоморфізм кільця $\mathbb{Z}_4$ на кільце $\mathbb{Z}_2$?

4. Наведіть приклади гомоморфізмів поля P на поле P_1 та поля P в поле $P_1 (P \neq P_1)$.

5. Перевірити, чи задовольняють умовам гомоморфізму кілець відображення:
   а) $f : \mathbb{Z} \to 5\mathbb{Z}$ при якому $f(n) = 5n$;
   б) $f : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{5}]$ при якому $f(a + b\sqrt{5}) = a - b\sqrt{5}$;
   в) $f : \mathbb{C} \to \mathbb{C}$ при якому $f(z) = z^2$;
   г) $f : M(2, \mathbb{R}) \to \mathbb{R}$ при якому $f(A) = |A|$.

Задачі на техніку обчислень та перетворень

6. Знайти всі ізоморфізми поля $\mathbb{C}$, при яких кожне дійсне число переходить само в себе.

7. Знайти всі ізоморфізми поля $\mathbb{Z}[\sqrt{2}]$, при яких кожне раціональне число переходить само в себе.

8. Нехай відображення f є гомоморфізмом кільця K у кільце K_1. Перевірити, що образ $f(K)$ кільця K є підкільцем кільця K_1.

9. Знайти всі гомоморфізми кілець:
   а) $\mathbb{Z}$ в $2\mathbb{Z}$; б) $2\mathbb{Z}$ в $2\mathbb{Z}$; в) $2\mathbb{Z}$ в $3\mathbb{Z}$; г) $\mathbb{Z}$ в $M_2(\mathbb{Z}_2)$.

10. Знайти всі гомоморфізми кільця цілих чисел в поле раціональних чисел.

11. Знайти з точністю до ізоморфізму всі скінченні кільця з чотирьох елементів, які містять 0 і 1.

12. На множині $M_3 = \{1, 2, 3\}$ визначити бінарні операції "*"і " $\circ$ " так, щоб одержана алгебра була ізоморфна кільцю $\mathbb{Z}_3$.

13. Перевірити, чи буде гомоморфізмом відображення $\varphi(f(x)) = f(c), c \in \mathbb{R}$ кільця K всіх дійсних функцій від однієї змінної, визначених на множині $\mathbb{R}$, на поле $(\mathbb{R}; +, \cdot)$?

Задачі на доведення

14. Нехай $(\mathbb{Z}; *, \circ)$ кільця з задач 10 а,б) в § 2.2. Довести, що відображення $f : \mathbb{Z} \to \mathbb{Z}$, які задано формулою:
   а) $f(n) = n + 1$; б) $f(n) = n + 5$
   є ізоморфізмом кільця $(\mathbb{Z}; *, \circ)$ на кільце $(\mathbb{Z}; +, \cdot)$ в обох випадках.

15. Довести, що ізоморфними є такі кільця:

а) $\mathbb{Q}[\sqrt{2}]$ і $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q}\right\}$;

б) $\mathbb{Z}[i]$ і $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$;

в) $\mathbb{Z}[\sqrt{3}i]$ і $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$;

г) $3\mathbb{Z}[i]$ і $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$.

tem Довести, що наступні кільця не ізоморфні:

а) $\mathbb{R}$ і $M(2, \mathbb{R})$; в) $\mathbb{Q}[\sqrt{2}]$ і $\mathbb{Q}[\sqrt{3}]$;

б) $\mathbb{Q}$ і $\mathbb{Q}[\sqrt{2}]$; г) $3\mathbb{Z}$ і $5\mathbb{Z}$.

16. Довести, що гомоморфний образ області цілісності не завжди є областю цілісності.

17. Довести, шо гомоморфізм двох кілець є їх ізоморфізмом тоді і тільки тоді, коли його ядро містить тільки нульовий елемент першого кільця.

18. Нехай φ є відображенням кільця $K = \left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$ на кільце цілих чисел $\mathbb{Z}$, причому $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b$. Довести, що φ – гомоморфізм і знайти його ядро.

19. Нехай φ є відображенням кільця $K = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q}\right\}$ діагональних матриць на кільце раціональних чисел $\mathbb{Q}$, причому $\varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = a$. Довести, що φ – гомоморфізм і знайти його ядро.

20. Нехай φ є відображенням кільця $C_{[-1,2]}$ на кільце дійсних чисел $\mathbb{R}$, причому $\varphi(f) = f(1)$ для будь-якої функції $f \in C_{[-1,2]}$. Довести, що φ – гомоморфізм і знайти його ядро.

21. Довести, що:
    а) будь-який I ідеал кільця K є ядром гомоморфізму при відображенні кільця K на фактор-кільце K/I;
    б) підмножина I кільця K є ядром гомоморфізму цього кільця на деяке кільце тоді і тільки тоді, коли I є ідеалом кільця K;
    в) будь-яке кільце, гомоморфне кільцю K, ізоморфне деякому фактор-кільцю цього кільця.

22. Нехай K – кільце з одиницею e і f відображення $\mathbb{Z}$ в K таке, що $f(m) = me$. Довести, що f є гоморфізмом кілець. Для яких кілець K відображення f є ін'єктивним?

23. Довести, що кільце нульової характеристики K містить підкільце, ізоморфне кільцю $\mathbb{Z}$.

24. Довести, що будь-яке поле нульової характеристики P містить підполе, ізоморфне полю $\mathbb{Q}$.

Творчі задачі

25. Знайти (з точністю до ізоморфізму) всі скінченні кільця, які містять pq елементів, де p і q – різні прості числа.

26. Чи можна на множині $\mathbb{N}$ задати бінарні операції $*$ і $\circ$ так, щоб алгебра $(\mathbb{N}; *, \circ)$ була ізоморфною кільцю цілих чисел $\mathbb{Z}$?

Задачі з олімпіад

27. Довести, що кільце K ненульової характеристики n, містить підкільце, ізоморфне кільцю $\mathbb{Z}/n$.

§ 2.5 Факторіальні кільця. Кільця головних ідеалів та евклідові кільця

Література: [1] стор. 155–161; [2] стор. 156–158; [3] стор. 445–452.

Теоретичні відомості

Кільце K називають *факторіальним*, якщо воно є областю цілісності і будь-який його елемент, відмінний від нуля і одиниці, однозначно (з точністю до дільників одиниці і порядку множників) розкладається на добуток простих множників.

Область цілісності K, в якій кожен ідеал є головним, називається *кільцем головних ідеалів*.

У кільці головних ідеалів K мають місце властивості найбільшого спільного дільника і взаємно простих елементів, які узагальнюють відповідні властивості для цілих чисел.

Елемент b кільця головних ідеалів K називають *спільним кратним* $a_1, a_2, \ldots, a_n$, якщо b ділиться на кожен з них. *Найменшим спільним кратним* елементів $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K називають таке спільне кратне цих елементів, на яке ділиться на будь-яке їхнє спільне кратне. Його позначають $[a_1, a_2, \ldots, a_n]$.

Будь-які два найменших спільних кратних елементів $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K, асоційовані між собою в K.

Для будь-яких елементів $a_1, a_2, \ldots, a_n$ кільця головних ідеалів K існує їх найменше спільне кратне і, якщо $m = [a_1, a_2, \ldots, a_n]$, то
$(m) = (a_1) \cap (a_2) \cap \cdots \cap (a_n)$.

Область цілісності K називається *евклідовим кільцем*, якщо існує відображення $\varphi : K \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ множини відмінних від нуля елементів області цілісності в множину цілих невід'ємних чисел, яке задовольняє умову: для будь-яких елементів $a, b \in K$ в K існують такі елементи q і r , що $a = bq + r$, причому $r = 0$ або $\varphi(r) < \varphi(b)$. При цьому число $\varphi(a)$ називають *нормою елемента* a.

Кожне евклідове кільце є кільцем головних ідеалів.

Кільця головних ідеалів і евклідові кільця є факторіальними.

Задачі на ілюстрацію понять

1. Навести приклади кілець в яких:
   а) розглядаються поняття простого і складеного елемента, НСД і НСК;

б) існують складені елементи, які не розкладаються в добуток простих;
в) складені елементи неоднозначно розкладаються в добуток простих;
г) всі складені елементи однозначно (з точністю до порядку множників і дільників одиниці) розкладаються в добуток простих;
д) не існує послідовності ідеалів, в якій кожний наступний строго включає попередній;
е) можна застосовувати алгоритм Евкліда для знаходження НСД.

2. До якого класу кілець належить довільне поле P?

3. Які з наступних тверджень про кільця є істинними:
   а) область цілісності є факторіальним кільцем;
   б) кільце головних ідеалів є факторіальним;
   в) евклідове кільце є факторіальним;
   г) кільце головних ідеалів є евклідовим?

Задачі на техніку обчислень та перетворень

4. В кільці $\mathbb{Z}[\sqrt{5}i]$ знайти НСД і НСК чисел 3 та $1 + i\sqrt{5}$.

5. Нехай K_1 є підкільцем області цілісності K, яке містить її одиницю. Чи може бути так, щоб:
   а) кільце K_1 було факторіальним, а K – ні;
   б) кільце K було евклідовим, а K_1 – ні;
   в) кільце K_1 було евклідовим, а K – ні;
   г) K було кільцем головних ідеалів, а K_1 – ні?

6. Перевірити, чи є кільцем головних ідеалів множина всіх раціональних чисел $\frac{m}{n}$ з непарним натуральним знаменником і цілим чисельником?

7. Перевірити, чи дані кільця є евклідовими:
   а) кільце $\mathbb{Z}[i]$ з нормою $\varphi(a + bi) = |a + bi|^2$;
   б) кільце $\mathbb{Z}[\sqrt{2}]$ з нормою $\varphi(a + b\sqrt{2}) = |a^2 - 2b^2|$;
   в) кільце $\mathbb{Z}[\sqrt{3}]$ з нормою $\varphi(a + b\sqrt{3}) = |a^2 - 3b^2|$;
   г) кільце $\mathbb{Z}[\sqrt{5}]$ з нормою $\varphi(a + b\sqrt{5}) = |a^2 - 5b^2|$?

8. Нехай $K \times L$ – прямий добуток кілець K і L. Яким він є, якщо:
   а) обидва кільця факторіальні;
   б) K і L є кільцями головних ідеалів;
   в) K і L є евклідовими кільцями;

9. Знайти твірні елементи даних ідеалів кільця цілих чисел $\mathbb{Z}$:
   а) $(4,6,8)+(10,15,20)$; в) $(m,n,k)+(l,s,t)$;
   б) $(2,4,8)\cap(5,15,20)$; г) $(m,n,k)\cap(l,s,t)$.

10. Знайти НСД і НСК таких цілих гауссових чисел:
   а) $6-17i$ та $18+i$; в) $5-5i$ та $7-i$;
   б) $4+3i$ та $3+i$; г) $3+7i$ та $11-3i$.

11. Знайти канонічний розклад цілих гауссових чисел:
   а) 5; в) $-90+180i$; д) $7+8i$;
   б) $5-5i$; г) $3+i$; е) 41.

Задачі на доведення

12. Довести, що в кільці $\mathbb{Z}[\sqrt{5}i]$:
   а) числа 2 та $1+i\sqrt{5}$ взаємно прості;
   б) для чисел 6 та $2+2i\sqrt{5}$ не існує найбільшого спільного дільника;
   в) порушується однозначність розкладу на прості множники;
   г) існують неголовні ідеали.

13. Довести, що в наступних кільцях порушується однозначність розкладу на прості множники: а) $\mathbb{Z}[\sqrt{3}i]$; б) $\mathbb{Z}[\sqrt{17}i]$; в) $\mathbb{Z}[\sqrt{19}i]$.

14. Нехай K є факторіальним кільцем, $a=\varepsilon_1 p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ та $b=\varepsilon_2 p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ – розклади його елементів на прості множники $p_1,p_2,\cdots,p_k$, де $\varepsilon_1,\varepsilon_2$ – дільники одиниці та α_i,β_j – цілі невід'ємні числа. Довести, що:
   а) a ділиться на c в K тоді і тільки тоді,коли $c=\varepsilon p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$, де $\varepsilon\in K^*$ і $0\leqslant\gamma_i\leqslant\alpha_i$;
   б) $(a,b)=\varepsilon p_1^{min\{\alpha_1,\beta_1\}}p_2^{min\{\alpha_2,\beta_2\}}\cdots p_k^{min\{\alpha_k,\beta_k\}}$, де $\varepsilon\in K^*$;
   в) $[a,b]=\varepsilon p_1^{max\{\alpha_1,\beta_1\}}p_2^{max\{\alpha_2,\beta_2\}}\cdots p_k^{max\{\alpha_k,\beta_k\}}$, де $\varepsilon\in K^*$;
   г) $(a,b)[a,b]$ і ab є асоційованими елементами в K.

15. Довести, що в будь-якому факторіальному кільці для довільних його елементів a,b мають місце твердження:
   а) якщо c ділиться на два взаємно простих елементи b і a, то c ділиться на їх добуток ab;
   б) якщо a і c взаємно прості та ab ділиться на c, то b ділиться на c;
   в) якщо a – простий елемент, то для будь-якого елемента b виконується одне з двох: $b\vdots a$ або $(a,b)=1$;
   г) якщо a і b – прості елементи, то виконується одне з двох: a і b асоційовані або $(a,b)=1$.

16. Нехай K є кільцем головних ідеалів. Довести, що:
    а) K є факторіальним кільцем;
    б) якщо добуток $a_1a_2\cdots a_s$ ділиться на простий елемент p, то хоча б один з співмножників a_i ділиться на p;
    в) в K не існує нескінченної послідовності ідеалів, в якій кожен наступний ідеал строго містить попередній.
    г) $(a,b)=d$ тоді і тільки тоді, коли $(d)=(a)+(b)$;
    д) $[a,b]=m$ тоді і тільки тоді, коли $(m)=(a)\cap(b)$.

17. Довести, що в кільці $\mathbb{Z}[x]$ є неголовні ідеали.

18. Нехай K є евклідовим кільцем та φ – його норма. Довести, що:
    а) для асоційованих елементів a і b має місце рівність $\varphi(a)=\varphi(b)$;
    б) коли a ділиться на b і $\varphi(a)=\varphi(b)$, то a і b асоційовані;
    в) $\varphi(a)=\varphi(1)$ тоді і тільки тоді, коли $a\in K^*$;
    г) K є кільцем головних ідеалів.

19. Довести, що у будь-якому ненульовому ідеалі I евклідового кільця K існує такий ненульовий елемент r, що $\varphi(r)\leqslant\varphi(c)$ для будь-якого ненульового елемента $c\in I$ і, при цьому $I=(r)$.

20. Довести що:
    а) ціле гауссове число є простим, якщо його норма є простим натуральним числом;
    б) будь-яке просте ціле гауссове число є дільником одного і тільки одного простого натурального числа;
    в) норма простого цілого гауссового числа є або простим натуральним числом, або квадратом простого натурального числа;
    г) усі прості натуральні числа виду $p=4n+3$ є простими цілими гауссовими числами.

Творчі задачі

21. Знайти необхідну і достатню умову, при якій просте натуральне число є нормою цілого гауссового числа.

22. Встановити, чи є кільце Q_p кільцем головних ідеалів для кожного простого числа $p\in\mathbb{Z}$ і описати будову всіх його ідеалів.

§ 2.6 Вибрані задачі

1. Нехай K – скінченне кільце. Довести, що:
   а) коли K не містить дільників нуля, то в ньому є одиниця і всі його ненульові елементи оборотні;
   б) коли K містить одиницю, то кожний його елемент, який оборотний зліва або справа є оборотним;
   в) коли K містить одиницю, то кожний його лівий дільник нуля є правим дільником нуля.

   Чи має місце твердження в) для кілець без одиниці?

2. Довести, що в кільці з одиницею і без дільників нуля кожний елемент, який має односторонній оберненений є оборотним.

3. Чи утворюють ідеал необоротні елементи кілець:
   а) $\mathbb{Z}$; б) $n\mathbb{Z}$; в) $\mathbb{Z}_n$?

4. Нетривіальний ідеал I кільця K називають максимальним, якщо для будь-якого ідеала U даного кільця такого, що $I \subseteq U \subseteq K$ виконується одна з рівностей $I = U$ або $U = K$. Знайти максимальні ідеали в кільцях: а) $\mathbb{Z}$; б) $n\mathbb{Z}$; в) $\mathbb{Z}_n$?

5. Нехай I –ідеал області цілісності K. Довести, що K/I є полем тоді і тільки тоді, коли I є максимальним.

6. Нехай K – кільце головних ідеалів, $a \in K$ і $a \neq 0$. Довести, що ідеал (a) є максимальним тоді і тільки тоді, коли a є простим елементом в K.

7. Нетривіальний ідеал I кільця K називають мінімальним, якщо для будь-якого ідеала U даного кільця такого, що $\{0\} \subseteq U \subseteq I$ виконується одна з рівностей $U = \{0\}$ або $U = I$. Довести, що кільце цілих чисел не містить мінімальних ідеалів.

8. Довести, що ідеал I комутативного кільця K є простим тоді і тільки тоді, коли I є ядром гомоморфізму K в деяке поле.

9. Нехай K – кільце головних ідеалів, $a \in K$ і $a \neq 0$. Довести, що ідеал (a) є максимальним тоді і тільки тоді, коли (a) є простим ідеалом в K. Чи є вірним це твердження для довільної області цілісності?

10. Нехай $C_{[0,1]}$ – кільце неперервних функцій на відрізку $[0,1]$, $I_c = \{f \in C | f(c) = 0, 0 \leqslant c \leqslant 1\}$. Довести, що:
    а) I_c – максимальний ідеал в $C_{[0,1]}$;
    б) кожний максимальний ідеал кільця $C_{[0,1]}$ має вид I_c для деякого числа $0 \leqslant c \leqslant 1\}$.

11. Довести, що кожне кільце K_1, яке включає кільце головних ідеалів K і міститься в його полі часток само є кільцем головних ідеалів.

12. Нехай K – комутативне кільце з одиницею. Довести, що:
    а) коли I_1 і I_2 – ідеали в K і $I_1 + I_2 = K$, то для будь-яких елементів $x_1, x_2 \in K$ існує елемент $x \in K$ такий, що $x - x_1 \in I_1, x - x_2 \in I_2$;
    б) коли $I_1, \ldots, I_n$ – ідеали в K і $I_i + I_j = K$ для всіх $i \neq j$, то для будь-яких $x_1, \ldots, x_n \in K$ елементів існує такий елемент $x \in K$ такий, що $x - x_1 \in I_1, \ldots, x - x_n \in I_n$.

13. Довести, що кільця $\mathbb{Z}_{mn}$ і $\mathbb{Z}_m \times \mathbb{Z}_n$ (§ 2.1, № 16) ізоморфні тоді і тільки тоді, коли m і n взаємно прості.

14. Довести, що кільце $\mathbb{Z}_{p_1 \ldots p_m}$, де $p_1, \ldots, p_m$ – різні прості числа, є прямим добутком полів.

15. Знайти всі прості елементи в кільці $\mathbb{Q}_p$.

16. Довести, що для відображення $f : \mathbb{Z}[-\frac{1}{2} + \frac{\sqrt{11}}{2}i] \to \mathbb{Z}$, яке задано рівністю $f(z) = |z|^2$, виконуються умови:
    а) $f(z_1 \cdot z_2) = f(z_1) f(z_2)$;
    б) $f(z) = 0$ тоді і тільки тоді, коли $z = 0$;
    в) z є дільником одиниці тоді і тільки тоді, коли $f(z) = 1$.

17. Знайти мультиплікативні групи кілець з попередніх двох задач.

18. Опишіть всі ідеали кільця $\mathbb{Z}_n$.

19. Нехай P_1 і P_2 –поля часток для областей цілісності K_1 і K_2 відповідно. Довести, що будь-який ізоморфізм $\varphi : K_1 \to K_2$ продовжується, і єдиним чином, до ізоморфізму $f : P_1 \to P_2$.

Розділ 3

Конгруенції

§ 3.1 Конгруенції в кільці цілих чисел та їх властивості

Література: [1] стор. 162–167;[2] стор. 166–169;[3] стор. 397–399; [4] стор. 68–72.

Теоретичні відомості

Нехай $m \in \mathbb{N}$. Цілі числа a і b називаються конгруентними за модулем m, якщо при діленні на m вони дають однакові остачі. Цей факт скорочено записують так: $a \equiv b \pmod{m}$

Цілі числа a і b є конгруентними за модулем m тоді і тільки тоді, коли:

а) їх різниця ділиться на m;

б) існує ціле число t таке, що $a = b + mt$.

Основні властивості конгруенцій:

1. Відношення конгруентності за модулем m на множині всіх цілих чисел є відношенням еквівалентності. Класи еквівалентності за цим відношенням називають класами лишків за даним модулем m.

2. Конгруенції за одним модулем можна почленно додавати, віднімати і множити.

3. До обох частин конгруенції можна додати будь-яке ціле число, а отже, переносити будь-який доданок з однієї частини в іншу з протилежним знаком.

4. До будь-якої частини конгруенції можна додати ціле число, кратне модулю.

5. Обидві частини конгруенції можна помножити на будь-яке ціле число.

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

7. Якщо $f(x) = a^n x^n + \cdots + a_1 x + a_0$ – многочлен з цілими коефіцієнтами і $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$.

8. Якщо у виразі

$$f(a_1, a_2, \ldots, a_k) = \sum_{j=1}^{n} A_j a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k}$$

усі коефіцієнти A_j і числа $a_1, a_2, \ldots, a_k$ замінити на конгруенті їм за модулем m коефіцієнти B_j і числа $b_1, b_2, \ldots, b_k$ відповідно, то отримаємо вираз

$$g(b_1, b_2, \ldots, b_k) = \sum_{j=1}^{n} B_j b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_k^{\alpha_k},$$

конгруентний заданому за модулем m, тобто

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

9. Обидві частини конгруенції і модуль можна помножити на будь-яке натуральне число.

10. Обидві частини конгруенції і модуль можна скоротити на їх спільний дільник.

11.Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який є їх найменшим спільним кратним.

12. Якщо конгруенція має місце за модулем m, то вона має місце і за кожним модулем d, який є дільником числа m.

13. Якщо одна частина конгруенції і модуль діляться на деяке число, то й друга частина конгруенції ділиться на те саме число.

Задачі на ілюстрацію понять

1. Записати у вигляді конгруенцій такі твердження:
   а) остача при діленні числа 81 на 13 дорівнює 3;
   б) число n є непарним;
   в) число n при діленні на 7 дає остачу 5;
   г) число $n^3 - 8$ ділиться на 3.

2. Сформулювати твердження, які записані мовою конгруенцій:
   а) $137 \equiv 5 \pmod{11}$;
   б) $256 \equiv 6 \pmod{2}$;
   в) $\overline{a_2 a_1 a_0}_{10} \equiv a_2 + a_1 + a_0 \pmod{3}$;
   г) $7^{29} \not\equiv 2 \pmod{5}$.

3. Серед чисел $a_1, a_2, \cdots, a_n$ знайти всі пари різних чисел, конгруентних за модулем m, якщо:
   а) $a_1 = 16, a_2 = 21, a_3 = 33, a_4 = 99, m = 4$;
   б) $a_1 = 231, a_2 = 119, a_3 = 220, a_4 = 283, a_5 = 301, m = 7$;
   в) $a_1 = 230, a_2 = 172, a_3 = 1001, a_4 = 953, m = 13$;
   г) $a_1 = 725, a_2 = 190, a_3 = 315, a_4 = 465, m = 15$.

4. Чи можуть числа виду $2^n - 1$ закінчуватися цифрою 0 для деякого натурального n?

5. Як записати наступні твердження за допомогою конгруенцій? Знайти множину значень x таких, що:
   а) вираз $x + 3$ кратний 5;
   б) вираз $2x + 3$ ділиться з остачею 2 на число 11;
   в) вираз $4x - 1$ ділиться з остачею 3 на число 13;
   г) вираз $2x - 1$ ділиться з остачею 1 на число 2.

Задачі на техніку обчислень та перетворень

6. Знайти остачу від ділення:
   а) 91^{2001} на 15; г) $43^{2000} + 6^{2000}$ на 41;
   б) 1532^{19} на 9; д) $2^{100} + 5^{200}$ на 29;
   в) $10^{2732} - 9$ на 22; е) $1999^{2000} + 2000^{2001}$ на 37.

7. Знайти останню цифру чисел:
   а) 3^{3^3}; в) 5^{5^5}; д) 7^{7^7};
   б) 4^{4^4}; г) 6^{6^6}; е) 8^{8^8}.

8. Знайти дві останні цифри чисел:
   а) 2^{999}; в) 289^{289}; д) 1999^{1999};
   б) 3^{999}; г) 2001^{2001}; е) 105^{105105}.

9. Нехай задано многочлен $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ з цілими коефіцієнтами та відомо, що число $f(14)$ закінчується цифрою 6. Якою цифрою закінчується число $f(54)$?

10. Знайти натуральні числа n при яких вираз $\frac{6^n - 1}{7}$ є цілим числом.

11. Дано дві конгруенції $a^9 \equiv 7 \pmod{31}$ і $a^{10} \equiv 4 \pmod{31}$, де $(a, 31) = 1$. Знайти остачу від ділення a на 31.

12. Знайти всі цілі розв'язки рівняння $2^x + 1 = 3^y$.

Задачі на доведення

13. Нехай p – просте число. Довести, що:
    а) $(a+b)^p \equiv a^p + b^p \pmod p$ для всіх цілих a, b;
    б) $C_{p-1}^k \equiv (-1)^k \pmod p$;
    в) $C_{p-2}^k \equiv (-1)^k (k+1) \pmod p$;
    г) $1 + 2^{2k+1} + 3^{2k+1} + \cdots (p-1)^{2k+1} \equiv 0 \pmod p$ для $p > 2$;
    д) $p^{p+2} + (p+2)^p \equiv 0 \pmod{2p+2}$ для $p > 2$;
    е) числа з множини $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{p-3}{2}, \frac{p-1}{2}\}$ попарно неконгруентні за модулем $p > 2$.

14. Довести, що для всіх цілих чисел a, b, c з подільності:
    а) $a + b - c$ на 2 слідує подільність $a - b - c$ на 2;
    б) $a - 5b$ на 17 слідує подільність $2a + 7b$ на 17;
    в) $12a - 7b$ на 16 слідує подільність $4a + 27b$ на 16;
    г) $11a + 2b$ на 19 слідує подільність $18a + 5b$ на 19;
    д) $16a - 11b + c$ на 21 слідує подільність $11a - b + 2c$ на 21;
    е) $5a - 11b$ на 31 слідує подільність $a + 4b$ на 31.

    Сформулюйте обернені твердження і перевірте їх виконання.

15. Довести, що для будь-якого натурального n:
    а) $100^n - 40 \equiv 0 \pmod 3$;
    б) $3^{4n+3} \equiv 37 \pmod{10}$;
    в) $9^{3n+1} + 3^{3n+1} + 1 \equiv 0 \pmod{13}$;
    г) $24^{2n+1} \cdot 21^{n+2} \equiv 3^{n+2} \cdot 17^{2n+1} \pmod{19}$;
    д) $48^{3n+1} + 16^{3n+1} \equiv 12 \pmod 1$;
    е) $3 \cdot 10^n + 24 \equiv 0 \pmod{54}$.

16. Довести, що для всіх цілих чисел a, b, c і будь-якого натурального n:
    а) $(11a+5)^{2n+1} + (11b+6)^{2n+1} \equiv 0 \pmod{11}$;
    б) $(13a+3)^{3n+2} + (13b-4)^{3n+2} \equiv 12 \pmod{13}$.

17. Довести, що коли $a \equiv b \pmod p$, то $a^p \equiv b^p \pmod{p^2}$, де p – просте число.

18. Довести, що коли має місце конгруенція $3a \equiv b \pmod{11}$, то справедлива також і конгруенція $4a \equiv 5b \pmod{11}$.

19. Довести, що $2^{3^n} \equiv -1 \pmod{3^{n+1}}$ для кожного $n \in \mathbb{N}$.

20. Довести, що задані рівняння не мають розв'язків у натуральних числах:
    а) $3^x + 9^y = 17^z$; в) $11^x - 6^y = 9^z$;
    б) $5^x + 7^y = 19^z$; г) $13^x - 22^y = 36^z$.

Творчі задачі

21. Встановити, якою цифрою закінчуються числа Ферма $F_n = 2^{2^n} + 1$, де $n \in \mathbb{N}$.

22. Встановити, при яких натуральних m, n, k число $a^{3m} - a^{3n+1} + a^{3k+2}$ ділиться на $a^2 - a + 1$ для будь-якого $a \in \mathbb{Z}$.

Задачі з олімпіад

23. Яких натуральних чисел більше на відрізку $[1; 10^{2001}]$: таких, що можна представити у вигляді $2x^2 - 3y^2 (x, y \in \mathbb{Z})$, чи таких, що можна представити у вигляді $10xy - x^2 - y^2 (x, y \in \mathbb{Z})$?

24. Згідно з григоріанським календарем, який було введено у жовтні 1582 року, роки, у яких число століть не ділиться на 4, не рахуються високосними хоч і діляться на 4 (це: $1700, 1800, 1900, 2100, 2200, \ldots$). Поставимо у відповідність кожному дню тижня число: неділі – 0, понеділку – 1, ... , суботі – 6, а кожному місяцю число: березню – 1, квітню – 2, травню – 3, ..., січню – 11, лютому – 12.

    Довести, що встановити яким днем тижня був або буде певний день d місяця m (дивись встановлену відповідність) у році $1600 \leqslant c \cdot 100 + k < 4000$ можна за формулою

$$x \equiv d + \left[\frac{1}{5}(13m - 1)\right] + k + \left[\frac{1}{4}k\right] + \left[\frac{1}{4}c\right] - 2c \pmod 7.$$

§ 3.2 Класи лишків. Повна і зведена система лишків. Теореми Ейлера і Ферма

Література: [1] стор. 166–170, 174–175; [2] стор. 169–173; [3] стор. 399–405, 408-409; [4] стор. 72–81.

Теоретичні відомості

Нехай на множині $\mathbb{Z}$ задано відношення конгруентності за модулем m. Відповідну йому фактор-множину будемо позначати через $\mathbb{Z}/m$ або коротше $\mathbb{Z}_m$. Вона містить m класів еквівалентності. Класи еквівалентності з цієї фактор-множини називають *класами лишків за модулем* m. Якщо елемент a є представником класу лишків, то такий клас позначають через $K_a^{(m)}$ або $\bar{a}$ (якщо з контексту відомий модуль m). Будь-яке число з довільного класу лишків називають *лишком за модулем* m.

У множині $\mathbb{Z}_m$ визначають операції додавання і множення класів лишків так:

$$K_a^{(m)} \oplus K_b^{(m)} = K_{a+b}^{(m)}, \qquad K_a^{(m)} \odot K_b^{(m)} = K_{a\cdot b}^{(m)}.$$

Алгебра $(\mathbb{Z}_m; \oplus, \odot)$ є комутативним кільцем з одиницею.

Алгебра $(\mathbb{Z}_m; \oplus, \odot)$ є полем тоді і тільки тоді, коли число m є простим.

Повною системою лишків (скорочено ПСЛ) за модулем m називають будь-яку систему лишків, взятих по одному з кожного класу лишків. Кожна повна система лишків містить m чисел. Розрізняють такі ПСЛ:

а) повна система найменших невід'ємних лишків;

б) повна система найменших за абсолютною величиною лишків;

в) повна система найменших додатних (натуральних) лишків.

Якщо $(a, m) = 1$, то клас $K_a^{(m)}$ називають *взаємно простим з модулем* m.

Зведеною системою лишків (скорочено ЗСЛ) за модулем m називають будь-яку систему лишків, взятих по одному з кожного класу лишків, взаємно простого з модулем m. Кожна зведена система лишків містить $\varphi(m)$ чисел. Для ЗСЛ розглядають такі ж системи, як і для ПСЛ.

Якщо $(a, m) = 1$, $b \in \mathbb{Z}$ та x пробігає повну систему лишків за модулем m, то вираз $ax + b$ також пробігає повну систему лишків за модулем m.

Якщо $(a, m) = 1$ та x пробігає зведену систему лишків за модулем m, то вираз ax також пробігає зведену систему лишків за модулем m.

Множина всіх класів лишків за модулем m, взаємно простих з m, утворює мультиплікативну групу в кільці $(\mathbb{Z}_m; \oplus, \odot)$. Позначимо її $\mathbb{Z}_m^*$.

Теорема Ейлера. Якщо $m > 1$ і $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

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

Наслідок. Для будь-якого простого числа p і довільного цілого числа a має місце конгруенція $a^p \equiv a \pmod{p}$.

Задачі на ілюстрацію понять

1. Замінити найменшим невід'ємним і найменшим за абсолютною величиною лишками такі числа:
   а) 28 за модулем 5; г) -337 за модулем 56;
   б) 231 за модулем 14; д) -4021 за модулем 91;
   в) 356 за модулем 27; е) -1239 за модулем 118.

2. Чи утворює повну систему лишків (надалі ПСЛ) множина чисел:
   а) -21,9,4,3,-8 за модулем 6;
   б) 25,-20,16,54,-21,26,37,-17 за модулем 8;
   в) 921,92,-18,28,-109,40,-22,-2,15 за модулем 9;
   г) -13,16,15,29,-35,21,73 за модулем 7;
   д) -1,-23,58,0,65,74,-17,91,82,-74 за модулем 10;
   е) -17,-13,38,14,22,49,11,61 за модулем 15?

3. Чи утворює зведену систему лишків (надалі ЗСЛ) множина чисел:
   а) 1,-1,5 за модулем 4;
   б) -7,17 за модулем 6;
   в) 25,-9,-6,72,52,-15 за модулем 7;
   г) 1,2,3,4,120,121,123,-1,-2,-3 за модулем 11;
   д) -10,17,84,-132 за модулем 12;
   е) -17,-13,38,14,22,49,11,61 за модулем 15?

4. Який зв'язок існує між класами лишків:
   а) за модулями 2 і 6; г) за модулями 3 і 8;
   б) за модулями 4 і 8; д) за модулями 5 і 9;
   в) за модулями 6 і 10; е) за модулями 7 і 14?

5. Чи можна застосувати теорему Ейлера до числа:
   а) 4 за модулем 8; г) 51 за модулем 14;
   б) 4 за модулем 11; д) 237 за модулем 111;
   в) 24 за модулем 27; е) 1093 за модулем 2237?

6. Чи можна застосувати теорему Ферма до чисел:
   а) 21 за модулем 53; г) 54 за модулем 17;
   б) 5 за модулем 91; д) 331 за модулем 158;
   в) 68 за модулем 17; е) 18 за модулем 2083?

7. Які з фактор-кілець утворюють поле:
   а) $\mathbb{Z}_8$; б) $\mathbb{Z}_{11}$; в) $\mathbb{Z}_{15}$; г) $\mathbb{Z}_{71}$?

8. Чому наступні фактор-кільця не утворюють поле:
   а) $\mathbb{Z}_6$; б) $\mathbb{Z}_{12}$; в) $\mathbb{Z}_{21}$; г) $\mathbb{Z}_{28}$?

Задачі на техніку обчислень та перетворень

9. Знайти повну систему найменших невід'ємних лишків за модулем:
   а) 8; б) 9; в) 14; г) 15.

10. Знайти повну систему найменших за абсолютною величиною лишків за модулем:
    а) 7; б) 10; в) 11; г) 19.

11. Знайти повну систему найменших натуральних лишків за модулем:
    а) 6; б) 12; в) 17; г) 18.

12. Знайти зведену систему найменших невід'ємних лишків за модулем:
    а) 8; б) 9; в) 10; г) 11.

13. Знайти зведену систему найменших за абсолютною величиною лишків за модулем:
    а) 12; б) 13; в) 14; г) 15.

14. Знайти зведену систему найменших натуральних лишків за модулем:
    а) 16; б) 17; в) 18; г) 19.

15. На які класи лишків розпадеться даний клас:
    а) $K_2^{(4)}$ за модулем 12; г) $K_4^{(12)}$ за модулем 6;
    б) $K_2^{(4)}$ за модулем 7; д) $K_5^{(11)}$ за модулем 22;
    в) $K_3^{(7)}$ за модулем 21; е) $K_4^{(12)}$ за модулем 36?

16. Знайти мультиплікативну групу фактор-кільця:
    а) $\mathbb{Z}_6$; б) $\mathbb{Z}_{15}$; в) $\mathbb{Z}_{20}$; г) $\mathbb{Z}_{23}$.

17. Яка з мультиплікативних груп $\mathbb{Z}_m^*$ є циклічною, якщо:
    а) $m = 8$; б) $m = 9$; в) $m = 10$; г) $m = 12$.
    Якщо група є циклічною, то знайти всі її твірні (первісні) елементи.

18. Розв'язати рівняння в кільці класів лишків $\mathbb{Z}_{20}$:
    а) $\overline{13}\bar{x} = \overline{18}$; б) $\overline{8}\bar{x} = \overline{5}$; в) $\overline{11}\bar{x} = \overline{8}$; г) $\overline{5}\bar{x} = \overline{8}$.

19. Розв'язати рівняння в полі класів лишків $\mathbb{Z}_{23}$:
    а) $\overline{12}\bar{x} = \bar{5}$; б) $\bar{5}\bar{x} = \overline{21}$; в) $\bar{2}\bar{x} = \overline{15}$; г) $\overline{13}\bar{x} = \bar{8}$.

20. Користуючись теоремою Ейлера, знайти остачу від ділення:
    а) 109^{345} на 14; в) 527^{144} на 65;
    б) 356^{273} на 39; г) 485^{84} на 129.

21. Користуючись теоремою Ферма, знайти остачу від ділення:
    а) 42^{50} на 17; в) 71^{50} на 67;
    б) 230^{347} на 37; г) 512^{402} на 101.

22. Знайти остачу від ділення:
    а) $7^{100} + 8^{100}$ на 5; в) $3^{500} + 7^{500}$ на 101;
    б) $5^{50} + 25^{70}$ на 9; г) $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

23. Знайти дві останні цифри числа:
    а) 3^{219}; б) 17^{900}; в) 903^{1294}; г) 102^{54}.

24. Знайти остачу від ділення:
    а) a^{100} на 125, якщо $a \in \mathbb{Z}$;
    б) $2^{\varphi(m)-1}$ на число m, якщо воно непарне і $m > 1$;
    в) $4^{\varphi(m)-1}$ на число m, якщо воно непарне і $m > 1$;
    г) $a^{10} - a^6 - A^4 + 2$ на 35, якщо $(a, 35) = 1$.

25. Знайти остачу від ділення на 561 числа:
    а) 4^{561}; б) 6^{561}; в) 15^{561}; г) 20^{561}.

Задачі на доведення

26. Довести, що числа $5^1, 5^2, 5^3, 5^4, 5^5, 5^6$ утворюють ЗСЛ за модулем 7.

27. Довести, що коли:
    а) x пробігає ПСЛ за модулем 10, то й x^5 пробігає ПСЛ за модулем 10;
    б) $(a, b) = 1$, x пробігає ПСЛ за модулем b, y пробігає ПСЛ за модулем a і c – будь-яке ціле число, то $ax + by + c$ пробігає ПСЛ за модулем ab.

28. Довести, що коли:
    а) x пробігає ЗСЛ за модулем 9, то й $7x^5$ пробігає ЗСЛ за модулем 9;
    б) $m \in \mathbb{Z}$, то числа $6m - 1, 6m + 1$ утворюють ЗСЛ за модулем 6;

29. Нехай $a_1, a_2, \cdots, a_{\varphi(m)}$ – зведена система найменших невід'ємних лишків за модулем m. Довести, що $a_1 + a_2 + \cdots + a_{\varphi(m)} = \frac{1}{2} m\varphi(m)$.

30. Довести, що групи $\mathbb{Z}_5^*$ і $\mathbb{Z}_6^*$ є циклічними.

31. Довести, що $2^{341} \equiv 2 \pmod{341}$.

32. Довести, що $2^{644} \equiv 1 \pmod{645}$.

33. Довести, що $2^{340n} \equiv 1 \pmod{341}$ для кожного натурального n.

34. Довести, що $a^{561} \equiv a \pmod{561}$ для будь-якого цілого a.

35. Довести, що $a^{13} \equiv a \pmod{2730}$ для будь-якого цілого a.

Творчі задачі

36. Встановити, при яких $2 \leqslant n \leqslant 20$ мультиплікативна група $\mathbb{Z}_n^*$ є циклічною.

37. Встановити, чи існують складені натуральні числа n, крім 561, такі, що $a^n \equiv a \pmod{n}$ для будь-якого цілого a.

Задачі з олімпіад

38. Знайти всі впорядковані пари (p, q) простих чисел p і q, для яких $(5^p - 2^p)(5^q - 2^q)$ ділиться на pq.

39. Нехай p і q – прості числа, $q > 5$ та $2^p + 3^p \equiv 0 \pmod{q}$. Довести, що $q > p$.

§ 3.3 Конгруенції першого степеня з одним невідомим та їх системи

Література: [1] стор. 175–180; [2] стор. 179–183; [3] стор. 409–411; [4] стор. 84–94.

Теоретичні відомості

Нехай $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ – многочлен з цілими коефіцієнтами від змінної x і ціле число $m > 1$.

Конгруенцію виду $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod m$ називають *конгруенцією з одним невідомим x за модулем m*. Якщо a_n не ділиться на m, то число n називається *степенем даної конгруенції*.

Розв'язком конгруенції називають клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію. Якщо число $0 \leqslant a < m$ задовольняє дану конгруенцію, то записують, що $x \equiv a \pmod m$ або $x = K_a^{(m)}$ є її розв'язком. Число розв'язків будь-якої конгруенції за модулем m не може перевищувати модуля.

Конгруенції з одним невідомим називають рівносильними, якщо множини їх розв'язків рівні.

Конгруенція $ax \equiv b \pmod m$, де a не ділиться на m, називається *конгруенцією першого степеня з одним невідомим*.

Якщо $(a, m) = 1$, то конгруенція першого степеня має єдиний розв'язок.

Якщо $(a, m) = d$, $d > 1$ і $b \vdots d$, то конгруенція першого степеня має d розв'язків.

Якщо $(a, m) = d$, $d > 1$ і b не ділиться на d, то конгруенція першого степеня не має розв'язків.

Основними способами розв'язування конгруенцій першого степеня є такі:

Спосіб спроб. Він полягає у підстановці ПСЛ за модулем m у конгруенцію і перевірці її виконання.

Спосіб рівносильних перетворень. Він полягає у виконанні над даною конгруенцією таких рівносильних перетворень, в результаті яких коефіцієнт біля x стає рівним 1.

Спосіб Ейлера. Розв'язок знаходять за формулою $x \equiv ba^{\varphi(m)-1} \pmod m$.

Спосіб застосування ланцюгових дробів. Розв'язок знаходять за формулою $x \equiv (-1)^n P_{n-1} b \pmod m$, де P_{n-1} – чисельник передостаннього підхідного дробу у розкладі числа $\frac{m}{a}$ у ланцюговий дріб.

Спосіб застосування класів лишків. Розв'язок знаходять за формулою $x = K_b^{(m)}(K_a^{(m)})^{-1}$ в групі $\mathbb{Z}_m^*$ всіх класів лишків за модулем m.

Нехай $\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots\dots\dots\dots\dots \\ x \equiv c_k \pmod{m_k} \end{cases}$ – система k конгруенцій, тобто потрібно знайти всі числа, які задовольняють кожну з заданих конгруенцій.

У загальному випадку її розв'язують так:

1. Розв'язок першої конгруенції записують у виді $x = c_1 + m_1 t$, де $t \in \mathbb{Z}$.
2. Серед знайдених розв'язків першої конгруенції шукають той, який задовольняє другу конгруенцію. Для цього підставляють знайдене значення x у другу конгруенцію $c_1 + m_1 t \equiv c_2 \pmod{m_2}$ і розв'язують її відносно змінної t. Якщо розв'язок існує, то його підставляють у наступну конгруенцію і процес продовжується до останньої конгруенції. Якщо ж отримана конгруенція не має розв'язків, то і вихідна система не має розв'язків.

У випадку, коли числа $m_1, m_2, \dots, m_k$ попарно взаємно прості і $M = m_1 \cdot m_2 \cdots m_k$, то система має єдиний розв'язок

$$x \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + \dots + m_k y_k c_k \pmod{M},$$

де числа M_i і y_i визначають з умов $M_i = \frac{M}{m_i}$, $M_i y_i \equiv 1 \pmod{m_i}$ для всіх $1 \leqslant i \leqslant k$.

Задачі на ілюстрацію понять

1. Які з наступних перетворень конгруенції з одним невідомим є рівносильними:
   а) перенесення доданку з однієї частини конгруенції в іншу без зміни знаку;
   б) множення обох частин конгруенції на ціле число, взаємно просте з модулем;
   в) скорочення обох частин конгруенції на їх спільний дільник;
   г) віднімання від будь-якої частини конгруенції числа, кратного модулю?

2. Скільки розв'язків має конгруенція:
   а) $14x \equiv 5 \pmod{61}$; в) $15x \equiv 48 \pmod{81}$;
   б) $18x \equiv 47 \pmod{81}$; г) $21x \equiv 49 \pmod{91}$?

3. Чи може конгруенція першого степеня за модулем 8 мати 5 розв'язків?

4. Скласти конгруенцію першого степеня за модулем 30 так, щоб вона:
   а) мала єдиний розв'зок;
   б) не мала розв'язків;
   в) мала 2, 5 або 6 розв'язків;
   г) мала 3, 15 або 16 розв'язків.

Задачі на техніку обчислень та перетворень

5. Розв'язати конгруенції способом перевірки ПСЛ:
   а) $6x \equiv 7 \pmod 5$; в) $4x \equiv 6 \pmod{10}$;
   б) $3x \equiv 22 \pmod 7$; г) $8x \equiv 16 \pmod{12}$.

6. Розв'язати конгруенції способом рівносильних перетворень:
   а) $8x \equiv 10 \pmod{14}$; в) $17x \equiv 23 \pmod{41}$;
   б) $16x \equiv 50 \pmod{23}$; г) $32x \equiv 43 \pmod{51}$.

7. Розв'язати конгруенції способом Ейлера:
   а) $29x \equiv 3 \pmod{12}$; в) $24x \equiv 1 \pmod{15}$;
   б) $27x \equiv 11 \pmod{34}$; г) $15x \equiv 23 \pmod{22}$.

8. Розв'язати конгруенції за допомогою ланцюгових дробів:
   а) $32x \equiv 182 \pmod{119}$; в) $-50x \equiv 67 \pmod{177}$;
   б) $105x \equiv 72 \pmod{147}$; г) $365x \equiv 50 \pmod{395}$.

9. Розв'язати конгруенції за допомогою класів лишків:
   а) $15x \equiv -1 \pmod{26}$; в) $37x \equiv 25 \pmod{107}$;
   б) $8x \equiv 36 \pmod{17}$; г) $11x \equiv 21 \pmod{30}$.

10. Розв'язати в цілих числах рівняння:
    а) $2x + 3y = 4$; в) $3x + 4y = 13$;
    б) $4x - 3y = 2$; г) $5x + 4y = 3$.

11. Розв'язати в натуральних числах рівняння:
    а) $23x + 15y = 19$; в) $91x - 28y = 35$;
    б) $17x - 16y = 31$; г) $5x - 3y = -1$.

12. Розв'язати систему конгруенцій:
    а) $\begin{cases} 3x \equiv 1 \pmod 5, \\ 5x \equiv 4 \pmod 7; \end{cases}$ в) $\begin{cases} x + 2y \equiv 0 \pmod 5, \\ 3x + 2y \equiv 2 \pmod 5; \end{cases}$
    б) $\begin{cases} x \equiv b_1 \pmod{13}, \\ x \equiv b_2 \pmod{17}; \end{cases}$ г) $\begin{cases} 5x - y \equiv 3 \pmod 6, \\ 2x + 2y \equiv 5 \pmod 6. \end{cases}$

13. Розв'язати систему конгруенцій:
    а) $\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod 5; \end{cases}$ в) $\begin{cases} 3x \equiv 1 \pmod{10}, \\ 4x \equiv 3 \pmod 5, \\ 2x \equiv 7 \pmod 9; \end{cases}$
    б) $\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv 2 \pmod 8, \\ x \equiv 2 \pmod{11}; \end{cases}$ г) $\begin{cases} 2x \equiv 3 \pmod 5, \\ 3x \equiv 5 \pmod 7, \\ 3x \equiv 3 \pmod 9. \end{cases}$

14. При яких натуральних a має розв'язки система конгруенцій:

а) $\begin{cases} x \equiv 1 \pmod{10}, \\ x \equiv 2 \pmod{21}, \\ x \equiv 3 \pmod{11}, \\ x \equiv a \pmod{6}; \end{cases}$ в) $\begin{cases} x \equiv 1 \pmod{15}, \\ x \equiv 11 \pmod{20}, \\ x \equiv 3 \pmod{11}, \\ x \equiv a \pmod{8}; \end{cases}$

б) $\begin{cases} 3x \equiv 4 \pmod{10}, \\ 2x \equiv a \pmod{4}; \end{cases}$ г) $\begin{cases} x \equiv 1 \pmod{18}; \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}? \end{cases}$

15. Скільки точок з цілими координатами лежать на заданій прямій між точками з абсцисами a_1 і a_2:
    а) $101x - 39y = 89, \quad a_1 = 0, \quad a_2 = 100;$
    б) $8x - 13y = -6, \quad a_1 = -100, \quad a_2 = 150;$
    в) $7x + 29y = 584, \quad a_1 = -20, \quad a_2 = 160;$
    г) $90x - 74y = 50, \quad a_1 = -100, \quad a_2 = 200?$

16. Через скільки точок з цілими координатами проходять сторони трикутника з вершинами:
    а) $A(2;3), B(7;8), C(13;5);$
    б) $A(2;1), B(20;7), C(8;15)?$

17. Відгадати день народження, якщо сума добутків числа місяця на 12 і номера місяця на 31 дорівнює 318. В чому суть відгадування?

18. На складі є в наявності труби довжиною 5 і 7 метрів. Яку кількість кожних труб кожного виду потрібно привезти для будівництва дільниці газопроводу довжиною 283 метри, щоб при їх зварюванні було найменше швів?

19. Знайти найменше натуральне число, яке ділиться на 7 і дає остачу 1 при діленні на 2, 3, 4, 5 і 6.

20. Дописати справа до числа 71 таке двоцифрове число, щоб отримане чотирицифрове число ділилося на 5 і 7.

21. Дописати справа до числа 71 таке двоцифрове число, щоб отримане чотирицифрове число при діленні на 11 давало остачу 3, а при діленні на 13 давало остачу 9.

22. Дописати справа до числа 629 таке трицифрове число, щоб отримане шестицифрове число ділилося на 5, 8 і 11.

23. Між числами 100 і 300 знайти всі натуральні числа, які при діленні на 3, 5 і 8 дають остачі 2, 3 і 4 відповідно.

Задачі на доведення

24. Довести, що всередині прямокутника, обмеженого прямими $x = -2$, $x = 5, y = -1$ і $y = 2$ на прямій $3x - 7y = 1$ немає жодної точки з цілими координатами.

25. Довести, що система конгруенцій

$$\begin{cases} x & \equiv 3 \pmod 6, \\ x & \equiv 7 \pmod m \end{cases}$$

є несумісною тоді і тільки тоді, коли $(6, m) > 2$.

Творчі задачі

26. Нехай на координатній площині xOy задано точки $A(a_1, a_2)$ і $B(b_1, b_2)$ з цілими координатами. Чи існує формула, яка дає можливість за координатами даних точок обчислити число всіх внутрішніх точок відрізка AB з цілими координатами?

27. Оцінити відстань між двома сусідніми точками з цілими координатами, які лежать на прямій $ax + by = c$, де $a, b, c \in \mathbb{Z}$.

28. Знайти умови, які потрібно накласти на число m, при яких система конгруенцій

$$\begin{cases} x & \equiv a \pmod b, \\ x & \equiv c \pmod m \end{cases}$$

є несумісною для заданих $a, b, c \in \mathbb{Z}$.

29. При якій умові звичайний дріб $\frac{m}{abc}$ можна подати у вигляді суми трьох дробів із знаменниками a, b і c?

30. Система m лінійних конгруенцій від n змінних $x_1, x_2, \ldots, x_n$ за модулем p у загальному виді записується так:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \pmod p, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \pmod p, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \equiv b_m \pmod p. \end{cases}$$

Створити теорію розв'язування таких систем конгруенцій.

§ 3.4 Конгруенції вищих степенів з одним невідомим

Література: [1] стор. 180–184;[2] стор. 183–187; [3] стор. 411–413; [4] стор. 95–105.

Теоретичні відомості

Нехай маємо конгруенцію

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

де p – просте число і a_n не ділиться на p. Дана конгруенція рівносильна конгруенції цього самого степеня з старшим коефіцієнтом рівним 1 за модулем p. Для цього слід домножити обидві частини конгруенції на число, яке є розв'язком конгруенції $a_n y \equiv 1 \pmod{p}$.

Оскільки, за наслідком з малої теореми Ферма, $x^p \equiv x \pmod{p}$, то дана конгруенція рівносильна конгруенції за модулем p, степінь якої не перевищує $p-1$. Для цього слід замінити кожний вираз x^s на x^r, де r – ненульова остача від ділення s на $p-1$. Якщо ж s ділиться на $p-1$, то вираз x^s замінюємо на вираз x^{p-1}.

Конгруенція n-го степеня за простим модулем p (тепер можна вважати, що $n < p$) має не більше як n розв'язків.

Нехай маємо конгруенції $f(x) \equiv 0 \pmod{p^k}$ і $f(x) \equiv 0 \pmod{p^{k+1}}$.

Якщо $x \equiv a \pmod{p^k}$ – розв'язок конгруенції $f(x) \equiv 0 \pmod{p^k}$, то число $x = a + p^k t, \quad t \in \mathbb{Z}$ є розв'язком конгруенції $f(x) \equiv 0 \pmod{p^{k+1}}$ тоді і тільки тоді, коли t є розв'язком конгруенції $f'(a) \cdot t \equiv -\frac{f(a)}{p^k} \pmod{p}$.

При цьому:

1. якщо остання конгруенція не має розв'язків (тобто $f'(a) \vdots p$ і $-\frac{f(a)}{p^k}$ не ділиться на p), то конгруенція $f(x) \equiv 0 \pmod{p^{k+1}}$ також немає жодного розв'язку;

2. якщо $f'(a) \vdots p$ і $-\frac{f(a)}{p^k} \vdots p$, то кожне число $x = a + p^k t, t \in \mathbb{Z}$ є розв'язком конгруенції $f(x) \equiv 0 \pmod{p^{k+1}}$;

3. якщо ж $f'(a)$ не ділиться на p, то остання конгруенція має єдиний розв'язок $t \equiv t_0 \pmod{p}$ і з класу розв'язків $x \equiv a \pmod{p^k}$ конгруенції $f(x) \equiv 0 \pmod{p^k}$ дістаємо єдиний розв'язок $x \equiv a + p^k t_0 \pmod{p^{k+1}}$ конгруенції $f(x) \equiv 0 \pmod{p^{k+1}}$.

Кожний розв'язок $x \equiv a \pmod{p}$ конгруенції $f(x) \equiv 0 \pmod{p}$ при умові, що $f'(a)$ не ділиться на p, дає один з розв'язків конгруенції $f(x) \equiv 0 \pmod{p^k}$.

Якщо $p_1, p_2, \ldots, p_s$ – різні прості числа, то конгруенція

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}}$$

рівносильна системі конгруенцій $\begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}}, \\ f(x) \equiv 0 \pmod{p_2^{k_2}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{p_s^{k_s}}. \end{cases}$

Якщо $k_1, k_2, \ldots, k_s$ числа розв'язків першої, другої, ..., s-ої конгруенцій системи відповідно, то дана конгруенція має $k_1 \cdot k_2 \cdot \ldots \cdot k_s$ розв'язків.

Задачі на ілюстрацію понять

1. Чи може конгруенція $3x^5 - 2x^3 + 4x - 1 \equiv 0 \pmod{11}$:
   а) мати 9 розв'язків; в) мати 1 розв'язок;
   б) мати 5 розв'язків; г) не мати розв'язків?

2. Знайти конгруенцію найменшого степеня, яка рівносильна заданій:
   а) $x^8 + 2x^7 + x^5 - x^4 - x + 3 \equiv 0 \pmod{5}$;
   б) $x^{16} + 3x^8 - 5x^7 - x^4 + 6x - 2 \equiv 0 \pmod{7}$;
   в) $6x^{18} + 18x^{15} + 3x^4 - 8x^3 + x^2 + 3 \equiv 0 \pmod{11}$;
   г) $x^{14} - x^{13} + 12x^2 + 2x + 1 \equiv 0 \pmod{13}$.

3. Як можна спростити розв'язування конгруенції $f(x) \equiv 0 \pmod{pq}$, де $f(x)$ – многочлен з цілими коефіцієнтами, а p і q – прості числа.

4. Чи можна задані конгруенції замінити на рівносильні їм того ж степеня та старшим коефіцієнтом, рівним одиниці:
   а) $15x^4 + 7x^3 - 3x - 2 \equiv 0 \pmod{3}$;
   б) $3x^3 - 5x^2 - 2 \equiv 0 \pmod{5}$;
   в) $27x^3 + 14x^2 - 10x + 13 \equiv 0 \pmod{7}$;
   г) $16x^4 - 23x^3 + 2x - 5 \equiv 0 \pmod{9}$?

5. Звести задані конгруенції шляхом рівносильних перетворень до найпростішого вигляду:
   а) $6x^4 + 17x^2 + 15x - 16 \equiv 0 \pmod{3}$;
   б) $27x^9 + 29x^8 - 26x^7 + 20x^4 - 17x + 23 \equiv 0 \pmod{3}$;
   в) $x^7 + 2x^6 + x^5 + 4x^3 - 2x^2 - 4x + 2 \equiv 0 \pmod{5}$;
   г) $34x^{10} - 29x^7 + 43x^4 - 19x + 37 \equiv 0 \pmod{5}$.

6. Скільки розв'язків має конгруенція:
   а) $x^3 \equiv 1 \pmod{7}$; в) $x^5 \equiv 10 \pmod{11}$;
   б) $x^4 \equiv 1 \pmod{11}$; г) $x^6 \equiv 2 \pmod{5}$?

Задачі на техніку обчислень та перетворень

7. Спростити задані конгруенції та розв'язати їх способом підстановки ПСЛ:
   а) $10x^{42} - 5x^{30} + 10x^{18} + 9x^{12} + 4 \equiv 0 \pmod 7$;
   б) $6x^{13} - 3x^{12} - 2x^{11} - 6x^3 + 3x^2 + 7x + 2 \equiv 0 \pmod{11}$;
   в) $120x^{91} + 14x^{15} + x^{11} - 3x^5 + 9x^2 - x + 6 \equiv 0 \pmod{11}$;
   г) $300x^{90} + 259x^{67} - 95x^{23} - 1 \equiv 0 \pmod{23}$.

8. Розв'язати конгруенції:
   а) $x^2 - 3x + 2 \equiv 0 \pmod 6$;
   б) $3x^3 - x^2 + 4x \equiv -2 \pmod{10}$;
   в) $3x^3 + 6x^2 + x \equiv -10 \pmod{15}$;
   г) $3x^2 + 7x \equiv -5 \pmod{34}$;
   д) $x^7 + x^2 \equiv 0 \pmod{35}$;
   е) $2x^2 - 7x \equiv -6 \pmod{55}$.

9. Розв'язати конгруенції:
   а) $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{25}$;
   б) $5x^3 + 3x + 1 \equiv 0 \pmod{25}$;
   в) $3x^3 - 5x^2 - 15 \equiv 0 \pmod{49}$;
   г) $x^2 + 3x + 5 \equiv 0 \pmod{121}$.

10. Розв'язати конгруенції:
    а) $4x^3 - 8x - 13 \equiv 0 \pmod{27}$;
    б) $x^4 + 7x + 4 \equiv 0 \pmod{27}$;
    в) $9x^2 + 29x + 62 \equiv 0 \pmod{64}$;
    г) $x^3 + 2x + 2 \equiv 0 \pmod{125}$.

11. Розв'язати конгруенції:
    а) $x^5 - 7x^4 + 11x^3 - 5x + 1 \equiv 0 \pmod{12}$;
    б) $x^2 - 3x + 23 \equiv 0 \pmod{63}$;
    в) $2x^3 - 5x - 32 \equiv 0 \pmod{175}$;
    г) $x^4 + 3x^3 + 2x + 6 \equiv 0 \pmod{45}$.

12. Скільки розв'язків має конгруенція:
    а) $x^6 \equiv 1 \pmod 7$;
    б) $x^{\varphi(20)} \equiv 1 \pmod{20}$;
    в) $x^9 \equiv 1 \pmod{19}$;
    г) $x^9 \equiv -1 \pmod{19}$?

13. Розкласти на множники за модулем 5 многочлен:
    а) $f(x) = x^3 - 2x + 1$; б) $f(x) = 3x^3 + 2x^2 - 2x - 3$.

14. Розкласти на множники за модулем 7 многочлен:
    а) $f(x) = 5x^3 + 4x^2 - 8x - 1$; б) $f(x) = 2x^3 + 5x^2 - 2x - 3$.

15. Розкласти на множники за модулем 11 многочлен:
    а) $f(x) = 6x^3 + 5x^2 - 2x - 9$; б) $f(x) = x^4 + x + 4$.

16. Розв'язати систему конгруенцій:

$$\begin{cases} x^4 + 2x + 1 & \equiv 0 \pmod 4, \\ x^3 + 3 & \equiv 0 \pmod{10}. \end{cases}$$

Задачі на доведення

17. Довести, що:
    а) коли p – просте число, то $2(p-3)! + 1 \equiv 0 \pmod p$;
    б) натуральне число $p > 2$ є простим тоді і тільки тоді, коли $(p-2)! \equiv 1 \pmod p$ (*критерій Лейбніца*);
    в) числа p і $p+2$ є простими тоді і тільки тоді, коли $4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$ (*теорема Клемента*);
    г) коли p – просте число і $p = 4n + 1$, то для будь-якого $n \in \mathbb{N}$ має місце конгруенція $[(2n)!]^2 + 1 \equiv 0 \pmod p$;
    д) коли p – просте число і $p = 4n + 3$, то для будь-якого $n \in \mathbb{N}$ має місце конгруенція $[(2n+1)!]^2 - 1 \equiv 0 \pmod p$;
    е) коли p – просте число і $a \in \mathbb{Z}$, то $a^p + (p-1)!a \equiv 0 \pmod p$.

18. Довести, що $x^{5p+1} \equiv x^6 \pmod p$, якщо p – просте число.

19. Довести *теорему Вільсона*: натуральне число $n > 1$ є простим тоді і тільки тоді, коли $(n-1)! + 1 \equiv 0 \pmod n$.

20. Довести, що коли p – просте число, то конгруенція $x^{p-1} \equiv 1 \pmod p$ має точно $p - 1$ розв'язок.

21. Довести, що коли p – просте число і d – натуральний дільник числа $p - 1$, то конгруенція $x^d \equiv 1 \pmod p$ має точно d розв'язків.

22. Довести, що конгруенція $x^n \equiv 1 \pmod p$ має n розв'язків, якщо p – просте число і $p \equiv 1 \pmod n$.

23. Довести, що коли $a \in \mathbb{Z}_p^*$ є елементом k-го порядку для простого p, то розв'язками рівняння $x^k \equiv 1 \pmod p$ є степені елемента a і тільки вони.

24. Довести, що конгруенція $x^2 + p \equiv 0 \pmod{p^2}$ не має розв'язків, якщо p – просте число.

25. Довести, що конгруенція

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p,$$

де p – просте число, має більш як n розв'язків тоді і тільки тоді, коли всі коефіцієнти в лівій частині діляться на p.

Творчі задачі

26. Знайти необхідну і достатню умову того, що конгруенція $x^n \equiv a \pmod{p}$, де p – просте число, $(a,p)=1$,і $n<p$, має тільки n розв'язків.

27. Яким умовам повинні задовольняти цілі числа a і b, щоб конгруенція $x^3+ax+b\equiv 0 \pmod{7}$, не мала 3 розв'язки?

28. Нехай маємо систему конгруенцій

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n\equiv b_1 \pmod{m},\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n\equiv b_2 \pmod{m},\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{n1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n\equiv b_n \pmod{m}. \end{cases}$$

При яких умовах до розв'язування цієї системи можна застосувати метод, аналогічний до методу Крамера для розв'язування систем лінійних рівнянь?

29. Описати метод знаходження розв'язків системи конгруенцій

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n\equiv b_1 \pmod{p^2},\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n\equiv b_2 \pmod{p^2},\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{m1}x_1+a_{m2}x_2+\ldots+a_{mn}x_n\equiv b_m \pmod{p^2} \end{cases}$$

для довільного простого числа p, з відомого розв'язку цієї ж системи за модулем p.

30. Узагальнити описаний в попередній задачі метод розв'язування системи конгруенцій шляхом переходу від модуля p^k до модуля p^{k+1}, де $k\in\mathbb{N}$.

§ 3.5 Квадратичні лишки. Символ Лежандра

Література: [1] стор. 184–192;[2] стор. 187–196; [4] стор. 105–120.

Теоретичні відомості

Розв'язування кожної конгруенції другого степеня можна звести до розв'язування двочленної конгруенції $x^2 \equiv a \pmod m$. Якщо ця конгруенція має хоча б один розв'язок, то число a називається *квадратичним лишком за модулем* m. В протилежному випадку число a називається *квадратичним нелишком за модулем* m.

Якщо $m = 2$, то парні числа є квадратичними лишками, а непарні – квадратичними нелишками за модулем 2. Тому надалі будемо розглядати $m > 2$.

Розв'язування конгруенції $x^2 \equiv a \pmod m$ за складеним модулем зводиться до розв'язування таких конгруенцій:

1. $x^2 \equiv a \pmod p$, де p – непарне просте число;
2. $x^2 \equiv a \pmod{p^k}$, де p – непарне просте число і $k > 1$;
3. $x^2 \equiv a \pmod{2^k}$, де $k > 1$.

Якщо $(a, p) > 1$, то перша конгруенція має єдиний розвязок $x \equiv 0 \pmod p$. Тому надалі розглянемо випадок, коли $(a, p) = 1$.

Для будь-якого непарного простого числа p половина лишків ЗСЛ за модулем p є квадратичними лишками, а інша половина – квадратичними нелишками.

Критерій Ейлера. Для будь-якого непарного простого числа p 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 за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Для ефектиного застосування критерію Ейлера при достатньо великих числах a і p розглядають поняття символ Лежандра.

Символ Лежандра визначається для всіх цілих чисел a, які не діляться на просте число $p > 2$ так:

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

Конгруенція $x^2 \equiv a \pmod{p^k}$, де p – непарне просте число, $(a, p) = 1$ і $k > 1$ має два розв'язки, якщо $\left(\frac{a}{p}\right) = 1$ і не має розв'язків, якщо $\left(\frac{a}{p}\right) = -1$.

Необхідними умовами існування розв'язків для конгруенції $x^2 \equiv a \pmod{2^k}$ є:

1. якщо $k = 2$, то $a \equiv 1 \pmod 4$;
2. якщо $k \geqslant 3$, то $a \equiv 1 \pmod 8$.

Якщо ці умови виконуються, то існує два розв'язки при $k = 2$ і чотири розв'язки при $k > 2$.

Нехай $m = 2^k \cdot p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$ – канонічний розклад числа m і $(a, m) = 1$.

Для того, щоб конгруенція

$$x^2 \equiv a \pmod{2^k \cdot p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}}$$

мала розв'язки необхідно і достатньо виконання умов:

1. $a \equiv 1 \pmod 4$ при $k = 2$;
2. $a \equiv 1 \pmod 8$ при $k > 2$;
3. $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \ldots = \left(\frac{a}{p_k}\right) = 1$.

Задачі на ілюстрацію понять

1. Які рівносильні перетворення конгруенції другого степеня

   $a_2x^2 + a_1x + a_0 \equiv 0 \pmod n, a_2 \not\vdots n$ потрібно виконати для того, щоб отримати двочленну конгруенцію $x^2 \equiv a \pmod m$?

2. Як звести розв'язування конгруенції $x^2 - 7 \equiv 0 \pmod{180}$ до розв'язування конгруенцій за меншими модулями?

3. Скільки існує квадратичних:
   а) лишків за модулем 19;
   б) нелишків за модулем 37?

4. Для яких цілих чисел a і p визначається символ Лежандра?

5. Чому дорівнює символ Лежандра $\left(\frac{a}{p}\right)$, якщо:
   а) $a = 4, \quad p = 7;$ в) $a = 12, \quad p = 7;$
   б) $a = 5, \quad p = 7;$ г) $a = 20, \quad p = 7$?

Задачі на техніку обчислень та перетворень

6. Розв'язати конгруенції:
   а) $3x^2 - 5x - 7 \equiv 0 \pmod 5$; в) $2x^2 + 5x - 1 \equiv 0 \pmod 7$;
   б) $2x^2 - 4x - 5 \equiv 0 \pmod 7$; г) $4x^2 - 7x \equiv 3 \pmod{11}$.

7. Розв'язати конгруенції, шляхом зведення їх до двочленних:
   а) $3x^2 + 6x + 1 \equiv 0 \pmod{10}$; г) $7x^2 + 15x - 11 \equiv 0 \pmod{23}$;
   б) $4x^2 + 3x + 3 \equiv 0 \pmod{15}$; д) $x^2 - 5x + 6 \equiv 0 \pmod{24}$;
   в) $6x^2 + 3x + 1 \equiv 0 \pmod{17}$; е) $12x^2 - 8x - 15 \equiv 0 \pmod{44}$.

8. Знайти всі квадратичні лишки за модулями:
   а) 7; б) 11; в) 13; г) 17; д) 23; е) 31.

9. Знайти всі квадратичні нелишки за модулями:
   а) 3; б) 11; в) 13; г) 19; д) 29; е) 37.

10. Обчислити символи Лежандра:
    а) $\left(\frac{12}{13}\right)$; б) $\left(\frac{19}{67}\right)$; в) $\left(\frac{56}{73}\right)$; г) $\left(\frac{68}{113}\right)$; д) $\left(\frac{219}{383}\right)$; е) $\left(\frac{283}{563}\right)$.

11. Скільки розв'язків має конгруенція:
    а) $x^2 \equiv 2 \pmod{31}$; в) $x^2 \equiv 579 \pmod{821}$;
    б) $x^2 \equiv 226 \pmod{563}$; г) $x^2 \equiv 3766 \pmod{5987}$?

12. Чи проходять через точки з цілими координатами такі параболи:
    а) $73y = x^2 - 37$; в) $11y = 5x^2 - 7$;
    б) $83y = x^2 - 34$; г) $443y = x^2 - 152$?

13. Розв'язати в цілих числах рівняння:
    а) $4x^2 - 5y - 6 = 0$; в) $x^2 - 10x - 11y + 5 = 0$;
    б) $5x^2 - 11y - 7 = 0$; г) $x^2 - 21x - 13y + 110 = 0$.

Задачі на доведення

14. Довести, що добуток:
    а) двох квадратичних лишків або нелишків є квадратичним лишком за модулем p.
    б) квадратичного лишку на нелишок є квадратичним нелишком за модулем p.

15. Довести властивості символу Лежандра:
    а) Якщо $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
    б) $\left(\frac{a^2}{p}\right) = 1$; $\left(\frac{1}{p}\right) = 1$; $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;
    в) $\left(\frac{ab\cdots}{c}p\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{c}{p}\right)$;
    г) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$; $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$; $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

16. Довести закон взаємності квадратичних лишків:
    якщо p і q – різні непарні прості числа, то

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

17. Довести, що $\left(\frac{-2}{p}\right) = (-1)^{\frac{p^2+4p-5}{8}}$.

18. Символ $\left(\frac{a}{m}\right)_J$ Якобі a відносно непарного числа $m > 2$ визначається для всіх цілих чисел a, взаємно простих з числом m, рівністю: якщо $m = p \cdot q \cdot \ldots \cdot r$ – розклад на прості множники (серед них можуть бути рівні), то

$$\left(\frac{a}{m}\right)_J \stackrel{df}{=} \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) \cdots \left(\frac{a}{r}\right).$$

Довести, що властивості а)-г) символу Лежандра (дивись № 15) виконуються для символу Якобі.

19. Довести, що рівняння $x^2 - 43y - 42 = 0$ не має розв'язків у цілих числах.

20. Довести, що при діленні добутку двох послідовних цілих чисел на число 13 остача ніколи не дорівнює 1.

21. Довести, що конгруенція $x^2 \equiv -1 \pmod{p}$ за простим модулем p має розв'язки тоді і тільки тоді, коли $p = 4m + 1$.

22. Довести, що конгруенція $x^2 \equiv -2 \pmod{p}$ за простим модулем p має розв'язки тоді і тільки тоді, коли $p = 8m + 1$ або $p = 8m + 3$.

23. Довести, що конгруенція $x^2 \equiv -3 \pmod{p}$ за простим модулем p має розв'язки тоді і тільки тоді, коли $p = 6m + 1$.

Творчі задачі

24. Скільки розв'язків може мати конгруенція $x^2 \equiv a \pmod{2^2 \cdot 5}$?

25. Скільки розв'язків може мати конгруенція $x^2 \equiv a \pmod{2^3 \cdot 5}$?

26. Описати необхідні і достатні умови існування розв'язку конгруенції $x^2 \equiv a \pmod{2^k}$.

27. Описати необхідні і достатні умови існування розв'язку конгруенції $x^2 \equiv a \pmod{3^k}$.

Задачі з олімпіад

28. Довести, що кожне просте число є дільником принаймні одного члена послідовності $a_n = n^6 - n^4 - 24n^2 - 36, n \in \mathbb{N}$.

§ 3.6 Показник числа і класу лишків за модулем. Первісні корені

Література: [1] стор. 193–201;[2] стор. 196–204; [3] стор. 413–416; [4] стор. 135–141.

Теоретичні відомості

Розглянемо довільну мультиплікативну групу $(G;\cdot)$. Відомо, що *порядком елемента* g мультиплікативної групи G називається найменше натуральне число k таке, що a^k є нейтральним елементом цієї групи. Крім того, елемент g циклічної мультиплікативної групи G називається *твірним або первісним,* якщо його порядок рівний порядку групи. В теорії чисел ці поняття трансформуються таким чином.

Нехай $m > 1$ – натуральне число. Розглянемо мультиплікативну групу $\mathbb{Z}_m^*$ всіх класів лишків за модулем m, взаємно простих з m, кільця $(\mathbb{Z}_m;\oplus,\odot)$ (§ 3.2.). Зауважимо, що ця група містить $\varphi(m)$ елементів і порядок кожного її елемента, за теоремою Лагранжа, є дільником порядку групи, тобто $\varphi(m)$. При окремих значеннях модуля вона є циклічною, тобто у ній є твірні (первісні) елементи.

Показником, до якого належить число a за модулем m або порядком числа a за модулем m, називають таке найменше натуральне число δ, що $a^\delta \equiv 1 \pmod m$. В такому випадку пишуть $\delta = P_m(a)$. Всі числа з одного класу лишків за модулем m мають однаковий показник за модулем m.

Для будь-якого числа a, взаємно простого з модулем m, показник завжди існує (слідує з теореми Ейлера) і він рівний порядку елемента $K_a^{(m)}$ мультиплікативної групи $\mathbb{Z}_m^*$.

Якщо $P_m(a) = \varphi(m)$, то число a називають *первісним коренем за модулем m.*

Показники числа за модулем мають такі властивості.

1. Якщо $\delta = P_m(a)$, то числа $1 = a^0, a^1, a^2, \ldots, a^{\delta-1}$ попарно неконгруенті за модулем m.

2. Якщо $P_m(a) = \varphi(m)$, то числа $1 = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$ утворюють ЗСЛ за модулем m.

3. Якщо $\delta = P_m(a)$, то $a^k \equiv a^l \pmod m$ тоді і тільки тоді, коли $k \equiv l \pmod \delta$. Як наслідок з цієї властивості отримуємо, що $a^k \equiv 1 \pmod m$ тоді і тільки тоді, коли $k \equiv 0 \pmod \delta$, тобто $k \vdots \delta$.

4. Якщо $(P_m(a), P_m(b)) = 1$, то $(P_m(ab) = P_m(a) \cdot P_m(b)$.

Якщо $\delta = P_m(a)$, то класи лишків $K_a^{(m)}, K_{a^2}^{(m)}, \ldots, K_{a^\delta}^{(m)}$ є різними розв'язками конгруенції $x^k \equiv 1 \pmod m$. Якщо m –просте число, то ці класи лишків вичерпують усі розв'язки даної конгруенції.

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

Якщо існує хоч одне число, яке належить до показника δ за простим модулем p, то всього класів таких чисел є $\varphi(\delta)$. Звідси закрема випливає, що за будь-яким простим модулем p існує $\varphi(p-1)$ первісних коренів.

Задачі на ілюстрацію понять

1. Який зв'язок існує в скінченній групі між порядком групи та порядком кожного її елемента?

2. Які порядки мають елементи мультиплікативної групи $\mathbb{Z}_8^*$?

3. Знайти числа, які є первісними коренями групи коренів 6-го степеня з одиниці.

4. Для яких натуральних a і m рівняння $a^x \equiv 1 \pmod m$ має розв'язок?

5. Які з заданої множини чисел належать до одного показника:
   а) -5, 2, 5, 13, 33, 41 за модулем 6;
   б) -13, -4, 2, 10, 45, 50, 119 за модулем 7;
   в) -11, -4, 7, 41, 50, 106 за модулем 9;
   г) -10, 1, 3, 7, 20, 29 за модулем 11?

6. Чи можуть існувати цілі числа a такі, що $P_{26}(a) = 7$?

7. Скільки первісних коренів є за модулем 29?

Задачі на техніку обчислень та перетворень

8. Знайти показник числа a за модулем m, якщо:
   а) $a = 4, m = 15$; в) $a = 7, m = 22$;
   б) $a = 2, m = 17$; г) $a = 5, m = 108$.

9. Знайти показники всіх класів лишків за модулем m, якщо:
   а) 11; б) 15; в) 19; г) 21.

10. Знайти показники чисел a, b, c, d за модулем m, якщо:
    а) $a = 7, b = 9, c = 12, d = 27; m = 13$;
    б) $a = 5, b = 8, c = 10, d = 16; m = 33$;
    в) $a = 10, b = 25, c = 50, d = 13; m = 39$;
    г) $a = 5, b = 15, c = 21, d = 35; m = 44$.

11. Знайти показник числа:
    а) 10 за модулем 37; в) m^2-1 замодулемm;
    б) 10 за модулем 39; г) m^3+1 за модулем m.

12. Знайти число первісних коренів за модулями:
    а) 21; б) 22; в) 23; г) 24.

13. Знайти найменший первісний корінь за модулями:
    а) 17; б) 23; в) 41; г) 53.

14. Відомо, що 2 є первісним коренем за модулем 13. Знайти всі інші первісні корені за цим модулем.

15. Знайти всі первісні корені за модулями:
    а) 11; б) 19; в) 29; г) 36.

16. Розв'язати конгруенції в множині натуральних чисел:
    а) $4^x \equiv 1 \pmod 3$; в) $2^x \equiv 1 \pmod{25}$;
    б) $5^x \equiv 1 \pmod 9$; г) $6^x \equiv 1 \pmod{49}$.

17. Знаючи, що 2 задовольняє конгруенцію $x^8 \equiv 1 \pmod{17}$, знайти всі розв'язки цієї конгруенції.

18. Відомо, що 2 є первісним коренем за модулем 131. Знайти всі розв'язки конгруенції $x^3 \equiv 16 \pmod{131}$.

19. Відомо, що $P_{29}(4)$. Знайти решту чисел, які мають показник 14 за модулем 29.

20. Знайти ті значення b, при яких має розв'язок конгруенція:
    а) $4^x \equiv b \pmod 9$; б) $5^x \equiv b \pmod 9$.

Задачі на доведення

21. Відомо, що 2 і 17 є первісними коренями за модулем 37. Довести, що $2^{18} \equiv -1 \pmod{37}$. Чи буде вірною конгруенція $17^{18} \equiv -1 \pmod{37}$?

22. Довести, що число a є первісним коренем за модулем m тоді і тільки тоді, коли клас лишків $K_a^{(m)}$ є твірним елементом групи $\mathbb{Z}_m^*$.

23. Довести, що за непарним простим модулем p існують первісні корені.

24. Довести, що за простим модулем p кожен дільник d числа $p-1$ є показником для $\varphi(d)$ класів лишків за цим модулем.

25. Нехай p –непарне просте число. Довести, що:
    а) серед первісних коренів за модулем p не може бути квадратів;
    б) коли a – первісний корінь за модулем p, то $\left(\frac{a}{p}\right) = 1$;
    в) коли a – первісний корінь за модулем p і $n \in \mathbb{N}$, то $\left(\frac{a^{2n+1}}{p}\right) = 1$;
    г) добуток двох первісних коренів за модулем p не є первісним коренем за цим модулем.
    д) коли p – просте число виду $4k+1$ і a – первісний корінь за модулем p, то $p-a$ також є первісним коренем за цим модулем;
    е) коли $P_p(a) = 2k$, то $a^k + 1$ ділиться на p.

26. Довести, що не існує первісних коренів за модулем m, якщо:
    а) $m = 36$;
    б) $m = 2^s, s \geqslant 3$;
    в) $m = 2^s p$, де $s > 1$ і p – непарне просте число;
    г) m – непарне складене число, яке ділиться хоча б на два різних простих множники.

27. Довести, що коли $P_m(a) = k$, то класи лишків $K_a^{(m)}, K_{a^2}^{(m)}, \cdots, K_{a^k}^{(m)}$ є різними розв'язками конгруенції $x^k \equiv 1 \pmod{m}$.

28. Довести, що первісний корінь за модулем $m > 2$ завжди є квадратичним нелишком за модулем m.

Творчі задачі

29. Вивчити питання про розв'язування конгруенцій виду $a^x \equiv b \pmod{m}$ для різних натуральних a, b, m.

Задачі з олімпіад

30. Нехай натуральні числа m та n такі, що 2^n+1 ділиться на 3^m. Довести, що y ділиться на 3^{m-1}.

§ 3.7 Індекси за простим модулем та їх застосування

Література: [1] стор. 201–204; [2] стор. 204–207; [3] стор. 416–420; [4] стор. 142–147.

Теоретичні відомості

Нехай g – первісний корінь за простим модулем p, $a \in \mathbb{Z}$ і $(a,p)=1$. Ціле невід'ємне число γ називається *індексом числа a за модулем p при основі g,* якщо

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

В такому випадку пишуть $\gamma = \operatorname{ind}_g a$.

Властивості індексів

1. Якщо $g^{\gamma_1} \equiv a \pmod{p}$ і $g^{\gamma_2} \equiv a \pmod{p}$, то $\gamma_1 \equiv \gamma_1 \pmod{(p-1)}$.
2. $a \equiv b \pmod{p}$ тоді і тільки тоді, коли $\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{(p-1)}$.
3. $\operatorname{ind}_g 1 \equiv 0 \pmod{(p-1)}$.
4. $\operatorname{ind}_g g \equiv 1 \pmod{(p-1)}$.
5. $\operatorname{ind}_g(a_1 a_2 \cdots a_k) \equiv (\operatorname{ind}_g a_1 + \operatorname{ind}_g a_2 + \cdots + \operatorname{ind}_g a_k) \pmod{(p-1)}$.
6. $\operatorname{ind}_g a^n \equiv n \cdot \operatorname{ind}_g a \pmod{(p-1)}$.

7. Якщо $a \vdots b$, то $\operatorname{ind}_g \frac{a}{b} \equiv (\operatorname{ind}_g a - \operatorname{ind}_g b) \pmod{(p-1)}$.

Перехід від конгруенції між числами до конгруенції між їх індексами називається *індексацією,* а зворотний перехід – *потенціюванням.* Для виконання цих переходів складають таблиці індексів і антиіндексів. Для окремих простих модулів та найменших первісних коренів такі таблиці є наведені у додатку 2 до збірника.

Двочленна конгруенція $ax^n \equiv b \pmod{p}$ n-го степеня за простим модулем p (тобто при $(a,p)=1$), рівносильна конгруенції першого степеня $n \cdot \operatorname{ind}_g x \equiv (\operatorname{ind}_g b - \operatorname{ind}_g a) \pmod{(p-1)}$, де g – довільний первісний корінь за простим модулем p.

Задачі на ілюстрацію понять

1. Нарисувати графіки відповідностей $y = \operatorname{ind}_3 x$ за модулем 7 між множинами:
   а) $\{0,1,2,3,4,5,6\}$ та $\{0,1,2,3,4,5\}$; в) $\mathbb{Z}$ та $\{0,1,2,3,4,5\}$;
   б) $\{1,2,3,4,5,6\}$ та $\{0,1,2,3,\cdots,10\}$; г) $\mathbb{Z}$ та $\mathbb{Z}^+$.

2. Чи можна визначити поняття індексу за складеним модулем?

3. Розв'язати у полі дійсних чисел різними відомими способами двочленне рівняння $5x^{47} - 6 = 0$.

4. Якими способами можна розв'язати двочленну конгруенцію $5x^{47} - 6 \equiv 0 \pmod{11}$?

5. Чи можна застосувати теорію індексів до розв'язування двочленної конгруенції $5x^4 - 6 \equiv 0 \pmod{21}$?

Задачі на техніку обчислень та перетворень

6. Скласти таблиці індексів за модулем p з основою g, якщо:
   а) $p = 5$, $q = 3$; в) $p = 13$, $q = 6$;
   б) $p = 11$, $q = 6$; г) $p = 29$, $q = 2$.

7. Розв'язати лінійні конгруенції за допомогою індексів:
   а) $8x \equiv -11 \pmod{37}$; в) $125x \equiv 7 \pmod{79}$;
   б) $47x \equiv 23 \pmod{73}$; г) $23x \equiv 9 \pmod{97}$.

8. Розв'язати конгруенції другого степеня за допомогою індексів:
   а) $x^2 \equiv 47 \pmod{53}$; в) $3x^2 - 5x - 2 \equiv 0 \pmod{11}$;
   б) $x^2 \equiv 59 \pmod{67}$; г) $3x^2 - 8x + 41 \equiv 0 \pmod{47}$.

9. Скільки розв'язків мають такі двочленні конгруенції:
   а) $x^{16} \equiv 10 \pmod{37}$; в) $x^{21} \equiv 5 \pmod{71}$;
   б) $7x^7 \equiv 11 \pmod{41}$; г) $x^{60} \equiv 79 \pmod{97}$?

10. Розв'язати двочленні конгруенції:
    а) $x^{10} \equiv 33 \pmod{37}$; д) $15x^4 \equiv 17 \pmod{23}$;
    б) $x^8 \equiv 31 \pmod{41}$; е) $23x^5 \equiv 15 \pmod{73}$;
    в) $x^{12} \equiv 37 \pmod{41}$; є) $27x^5 \equiv 25 \pmod{31}$;
    г) $x^{35} \equiv 17 \pmod{67}$; ж) $44x^{21} \equiv 53 \pmod{73}$.

11. Розв'язати конгруенції:
    а) $5x^{11} + 19 \equiv 0 \pmod{29}$; в) $7x^{13} + 23 \equiv 0 \pmod{47}$;
    б) $17x^5 + 3 \equiv 0 \pmod{37}$; г) $x^{11} + 36 \equiv 0 \pmod{71}$.

12. Знайти найменший натуральний розв'язок конгруенції:
    а) $27^x \equiv 1 \pmod{17}$; в) $32^x \equiv 15 \pmod{37}$;
    б) $11^x \equiv 17 \pmod{31}$; г) $16^x \equiv 11 \pmod{53}$.

13. Розв'язати двочленні показникові конгруенції:
    а) $3 \cdot 8^x \equiv 7 \pmod{23}$; в) $21^{3x} \equiv 21^5 \pmod{29}$;
    б) $12^{7x} \equiv 15 \pmod{31}$; г) $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$.

14. Розв'язати конгруенції:
    а) $13 \cdot 7^{5x} \equiv -1 \pmod{67}$; в) $11 \cdot 5^{3x} \equiv -70 \pmod{79}$;
    б) $7 \cdot 5^{x} \equiv -1 \pmod{73}$; г) $8 \cdot 7^{x} \equiv -4 \pmod{83}$.

15. Застосовуючи теорію індексів, знайти показник числа a за модулем p, якщо:
    а) $a = 6, \quad p = 23$; в) $a = 18, \quad p = 41$;
    б) $a = 7, \quad p = 29$; г) $a = 13, \quad p = 53$.

16. Застосовуючи теорію індексів, встановити, чи є первісними коренями за модулем 59 такі числа: а) 3; б) 6; в) 12; г) 14.

17. Серед чисел зведеної системи лишків за модулем p знайти ті, показник яких дорівнює числу r, якщо:
    а) $p = 43, \quad r = 6$; в) $p = 61, \quad r = 10$;
    б) $p = 43, \quad r = 42$; г) $p = 61, \quad r = 60$.

Задачі на доведення

18. Нехай g - первісний корінь за простим модулем p, та цілі числа a, b взаємно прості з p. Довести такі властивості індексів за модулем p при основі g:
    а) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{(p-1)}$;
    б) якщо a ділиться на b, то $\operatorname{ind}_g \frac{a}{b} \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{(p-1)}$.

19. Нехай g і t – два первісних корені за простим модулем p. Довести,що:
    а) $\operatorname{ind}_g a \equiv \operatorname{ind}_t a \cdot \operatorname{ind}_g t \pmod{(p-1)}$;
    б) $\operatorname{ind}_t a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_t g \pmod{(p-1)}$;
    в) $\operatorname{ind}_t g \cdot \operatorname{ind}_g t \equiv 1 \pmod{(p-1)}$;
    г) $\operatorname{ind}_g a \equiv \operatorname{ind}_t a \cdot (\operatorname{ind}_t g)^{\varphi(p-1)-1} \pmod{(p-1)}$.
    Останню конгруенцію називають формулою переходу від системи індексів з основою t до системи індексів з основою g.

20. Довести, що конгруенція $2^x \equiv 3 \cdot 5^{3x} \pmod{163}$ не має розв'язків.

21. Нехай маємо адитивну групу $\mathbb{Z}_{p-1}$ і мультиплікативну групу $\mathbb{Z}_p^*$ за простим модулем p. Довести, що вони ізоморфні і шуканим ізоморфізмом є відображення $f : \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ таке, що $f(\bar{a}) = \overline{\operatorname{ind}_g a}$, незалежно від вибору основи індексування g.

22. Довести, що:
    а) конгруенція $x^n \equiv a \pmod{p}$, де p – просте непарне число, має розв'язки тоді і тільки тоді, коли $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, де $d = (n, p-1)$;
    б) число a тоді і тільки тоді є квадратичним лишком за модулем непарного простого числа p, коли за цим модулем $\mathrm{ind}a$ – число парне;
    в) показник $\delta = P_m(a)$ визначається рівністю $(\mathrm{ind}a, \varphi(m)) = \frac{\varphi(m)}{\delta}$. Зокрема належність числа a до первісних коренів за модулем m визначається рівністю $(\mathrm{ind}a, \varphi(m)) = 1$;
    г) застосовуючи властивості індексів, можна довести теорему Вільсона (дивись §4, задача 19);
    д) для простого числа p виду $2^n + 1$, де $n > 3$, число 3 є первісним коренем;
    е) індекс числа -1 за простим непарним модулем p при будь-якій основі дорівнює $\frac{p-1}{2}$.

Творчі задачі

23. Визначити поняття індексу за складеним модулем і вивчити його властивості.

24. Нехай g – первісний корінь за модулем m і $(b, m) = 1$. Встановити, який зв'язок існує між конгруенціями $b \equiv c \pmod{m}$ та $\mathrm{ind}_g b \equiv \mathrm{ind}_g c \pmod{\varphi(m)}$.

25. Скласти таблицю індексів за складеним модулем 27 при основі 5 та застосувати її до розв'язування конгруенції $5x \equiv 13 \pmod{27}$.

26. Яким умовам повинні задовольняти цілі числа a, m та n, щоб конгруенція $x^n \equiv a \pmod{m}$ мала розв'язки?

§ 3.8 Арифметичні застосування конгруенцій

Література: [1] стор. 205–210; [2] стор. 207–213; [3] стор. 421–429; [4] стор. 151–162.

Теоретичні відомості

Теорія конгруенцій знаходить застосування в арифметиці при:

1. виведенні ознак подільності цілих чисел;
2. обчисленні остач при діленні цілих чисел (дивись § 3.1, 3.2);
3. перевірці результатів арифметичних дій;
4. визначенні довжини періоду при перетворенні звичайного дробу в десятковий.

Нехай натуральне число a записане у системі числення за основою g так:

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

та r_k абсолютно найменші лишки числа g^k за модулем m. Тоді *загальна ознака подільності Паскаля* записується так:

$$a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0 \equiv a_n r_n + a_{n-1} r_{n-1} + \cdots + a_1 r_1 + a_0 \pmod{m}.$$

Підставляючи сюди конкретні значення g і m, отримаємо різні ознаки подільності цілих чисел.

Для перевірки результатів арифметичних дій можна застосовувати властивість 8 з § 3.1. При цьому за модуль беруть числа 9 або 11 і тоді говорять про правила дев'ятки та одинадцяти відповідно.

Зокрема, правило дев'ятки формулюється так:

якщо у цілочисловому виразі всі числа замінити на їх остачі від ділення на 9, то отримаємо число конгруентне даному за модулем 9.

Зауважимо, що всі ці правила дають тільки необхідні, але не достатні умови вірності результату виконання дій.

При застосуванні цього правила для перевірки результату арифметичних дій слід знайти остачі від ділення результату і, отриманого в результаті заміни, значно меншого числа на 9. Якщо остачі різні, то в обчисленнях є допущена помилка. Якщо ж остачі однакові, то помилка може бути на число кратне 9. В такому випадку застосовують ще правило 11. Це дає кращий результат, оскільки помилка може бути кратною 99, що мало ймовірно.

Нарешті відомо, що нескоротний дріб виду $\frac{a}{2^\alpha \cdot 5^\beta \cdot c}$, де $c > 2$ і $c \neq 5$, у скінченний десятковий дріб не перетворюється.

Якщо $\frac{a}{b}$ – нескоротний дріб і $(b, 10) = 1$, то цей дріб перетворюється у чистий періодичний десятковий дріб. При цьому число цифр у періоді дорівнює $P_b(10)$ показнику числа 10 за модулем b.

Якщо $\frac{a}{b}$ – нескоротний дріб, $b = 2^\alpha \cdot 5^\beta \cdot b_1$ і $(b_1, 10) = 1$, то цей дріб перетворюється у мішаний періодичний десятковий дріб. При цьому число цифр до періоду дорівнює γ, де γ – більше з чисел α і β; число цифр у періоді дорівнює $P_{b_1}(10)$ показнику числа 10 за модулем b_1.

Задачі на ілюстрацію понять

1. Знайти ознаки подільності на 4, 8 і 11 в дванадцятковій системі числення.

2. Чому при перевірці за правилами "дев'ятки"і "одинадцяти"результатів арифметичних дій немає впевненості в остаточному результаті?

3. Яким може бути знаменник дробу $\frac{1}{q}$, який перетворюється у чистий періодичний десятковий дріб:
   а) з двома цифрами в періоді;
   б) з трьома цифрами в періоді?

4. Яким може бути знаменник дробу $\frac{1}{q}$, який перетворюється у мішаний періодичний десятковий дріб:
   а) з одною цифрою до періоду і двома цифрами в періоді;
   б) з двома цифрами до періоду і одною цифрою в періоді.

Задачі на техніку обчислень та перетворень

5. Встановити за допомогою ознак подільності, чи ділиться число a на m, якщо:
   а) $a = 973126, m = 13$; в) $a = 96736068, m = 44$;
   б) $a = 63364, m = 28$; г) $a = 2575163, m = 37$.

6. Знайти канонічний розклад числа:
   а) 244943325; в) 3058487;
   б) 90799; г) 282321246671737.

7. Знайти невідомі цифри числа, якщо відомо, що:
   а) $(13xy45z)_{10}$ ділиться на 792; в) $(x809y)_{10}$ ділиться на 55;
   б) $(7x36y5)_{10}$ ділиться на 1375; г) $(665xy)_{10}$ ділиться на 504.

8. Знайти остачу від ділення:
   а) 3989713 на 37; в) 53^{29} на 37;
   б) $125 \cdot 465$ на 61; г) 272^{1141} на 135.

9. За правилом "дев'ятки"перевірити правильність виконання арифметичних дій над цілими числами:
   а) $73416 \cdot 8539 = 626899224$; в) $5433153 : 4371 = 1243$;
   б) $24667 + 18625 = 42932$; г) $8740297 - 561245 = 8179052$.

10. За правилом "одинадцяти"перевірити правильність виконання арифметичних дій над цілими числами:
   а) $387912 - 203756 = 185146$; в) $437 \cdot 86 + 16384 = 54866$;
   б) $5839131309 : 67377 = 85847$; г) $(2708^2 - 8513874) \cdot 18 = 76181397$.

11. Знайти основу g системи числення, в якій мають місце дві ознаки подільності:
   а) число a ділиться на 5 тоді і тільки тоді, коли сума його цифр ділиться на 5;
   б) число a ділиться на 7 тоді і тільки тоді, коли на 7 ділиться число, записане двома його останніми цифрами.

12. Знайти довжину періоду при перетворенні звичайного нескоротного дробу у десятковий, якщо його знаменник дорівнює:
   а) 17; д) 43; з) 21; н) 91;
   б) 19; е) 59; к) 33; о) $11 \cdot 17$;
   в) 29; є) 67; л) 49; п) $13 \cdot 17$;
   г) 37; ж) 73; м) 77; р) $17 \cdot 23$.

13. Знайти кількість цифр до періоду і довжину періоду при перетворенні нескоротного звичайного дробу із знаменником b у десятковий, якщо:
   а) $b = 140$; д) $b = 540$; з) $b = 950$;
   б) $b = 220$; е) $b = 550$; к) $b = 1150$;
   в) $b = 450$; є) $b = 665$; л) $b = 2380$;
   г) $b = 528$; ж) $b = 816$; м) $b = 26500$.

14. Перетворити у звичайні такі періодичні дроби:
   а) 3,(27); б) 0,35(62); в) 11,12(31); г) 5,1(538).

Задачі на доведення

15. Довести, що:
   а) $14^{120} - 1$ ділиться на 45; в) $43^{23} + 23^{43}$ ділиться на 66;
   б) $13^{176} - 1$ ділиться на 89; г) $222^{555} + 555^{222}$ ділиться на 7.

16. Нехай $n \in \mathbb{N}$. Довести, що:
   а) $n^7 + 6n \vdots 7$; в) $3 \cdot 5^{2n+1} + 2^{3n+1} \vdots 17$;
   б) $10^n(9n - 1) + 1 \vdots 9$; г) $6^{2n+1} + 5^{n+2} \vdots 31$.

17. Довести, що:
    а) число $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18}+1$ ділиться на 7;
    б) число $7^{40}-5^{30}$ ділиться на 11;
    в) число $8^{80}+13^{90}$ ділиться на 17;
    г) число $13^{176}-1$ ділиться на 89.

18. Довести, що коли до будь-якого тризначного числа дописати справа це саме число, то утворене число ділиться на 7, 11, 13.

19. Довести, що сума, різниця, добуток і частка двох періодичних дробів є періодичним дробом.

20. Довести, що в 11-ковій системі числення:
    а) число a ділиться на 2, 3, 4, 6 та 12 тоді і тільки тоді, коли різниця між сумами цифр числа a, які стоять на парних і непарних місцях, ділиться на ці числа;
    б) число a ділиться на 2, 5 та 10 тоді і тільки тоді, коли сума цифр числа a ділиться на ці числа.

21. Довести, що для всіх $n>1$ сума $\frac{1}{n-1}+\frac{1}{n}+\frac{1}{n+1}$ перетворюється у мішаний десятковий періодичний дріб.

22. Довести, що коли 10 є первісним коренем за модулем m, то періоди всіх нескоротних дробів із знаменником m складатимуться з кругових перестановок однієї і тієї самої системи $k=\varphi(m)$ цифр.

Творчі задачі

23. Чи існує система числення, в якій ознаки подільності на числа $2,3,4,\cdots,n$ такі ж, як ознака подільності на 3 в десятковій системі числення?

24. Встановити залежність між цифрами чистого періодичного дробу з парним числом цифр у періоді, в який перетворюється звичайний дріб $\frac{1}{p}$ для простого числа $p>5$.

Задачі з олімпіад

25. Яким може бути знаменник дробу $\frac{1}{q}$, який перетворюється у мішаний періодичний десятковий дріб:
    а) з двома цифрами до періоду і двома цифрами в періоді;
    б) з двома цифрами до періоду і трьома цифрами в періоді.

§ 3.9 Вибрані задачі

Задачі з різних олімпіад і математичних турнірів

1. (ММО, 1986) Нехай d – натуральне число, причому $d \notin \{2, 5, 13\}$. Довести, що у множині $\{2, 5, 13, d\}$ можна вибрати такі два різні числа a та b, що $ab - 1$ не є квадратом цілого числа.

2. (ММО, 1996) Натуральні числа a і b є такими, що $15a+16b$ та $16a-15b$ – квадрати натуральних чисел. Яке найменше значення може приймати при цьому $\min\{15a + 16b, 16a - 15b\}$?

3. (Угорщина, 1980) Довести, що дріб $\frac{4}{n}$ при непарному n можна подати у вигляді $\frac{1}{a} + \frac{1}{b}$ тоді і тільки тоді, коли $n = m(4k - 1), m, k \in \mathbb{N}$.

4. (Австрія - Польща, 1980) Довести, що число n є сумою всіх дробів виду $\frac{1}{i_1 i_2 \cdots i_k}$, де $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$.

5. (США, 1975) Довести, що для будь-яких натуральних m, n число $\frac{(5m)!(5n)!}{m!n!(3m+n)!(m+3n)!}$ є натуральним.

6. (ФРН, 1978) Просте число p має таку властивість, що кожне число, яке утворюється із числа p перестановкою його цифр, також є простим. Довести, що десятковий запис числа p містить не більше, ніж три різні цифри.

7. Довести, що для будь-яких натуральних m, n число $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ є натуральним.

8. Довести, що конгруенція $x^2+x+1 \equiv 0 \pmod{(6m-1)}$ не має розв'язків для будь-якого натурального числа m.

9. У десятковому записі натурального числа a зустрічається кожна з цифр 1, 2, 3 та 4. Довести, що можна переставити цифри у числі a так, щоб число, яке при цьому утвориться, ділилося на 7.

10. Довести, що для будь-якого натурального числа $\overline{a_n \cdots a_1 a_0}$, взаємно простого з 10, існує натуральне число, куб якого має вигляд $\cdots \overline{a_n \cdots a_1 a_0}$.

11. Розв'язати в цілих числах рівняння:
    а) $1 + x + x^2 + x^3 = y^2$;
    б) $1 + x + x^2 + x^3 + x^4 = y^2$.

12. Знайти найбільше k, при якому число:
    а) $\frac{3^{2^n}-1}{2^k}$ є цілим; б) $\frac{2^{3^n}+1}{3^k}$ є цілим.

Задачі видатних математиків

13. (Задача Остроградського) Довести, що довільне раціональне число з інтервалу $(0,1)$ можна однозначно подати у вигляді

$$\frac{1}{a_1}+\frac{1}{a_1a_2}+\cdots+\frac{1}{a_1a_2\cdots a_n},$$

де a_i – натуральні числа, $a_{i+1}\geqslant a_i, a_i\geqslant 2$, причому у такому вигляді подаються лише раціональні числа з цього інтервалу.

14. Довести, що має місце формула Ейлера: $1+\frac{1}{2^2}+\frac{1}{3^2}\cdots+\frac{1}{n^2}+\cdots=\frac{\pi^2}{6}$.

15. Довести, що будь-яке раціональне число, менше за $\frac{\pi^2}{6}-1$, можна подати у вигляді суми різних дробів, обернених квадратам натуральних чисел.

16. Довести, що кількість всіх правильних нескоротних дробів з знаменником a^n-1 ділиться на n, якщо $a,n\in\mathbb{N}$.

17. Довести, що для будь-яких натуральних m і $n, m>n$, число

$$\frac{1}{2n+1}+\frac{1}{2n+3}+\frac{1}{2n+5}+\cdots+\frac{1}{2m+1}$$

не є цілим.

18. Довести, що коли ціле число a ділиться на 2^n-1, то в двійковому записі числа a не менше n одиниць.

19. Довести, що для будь-якого натурального n і довільного натурального $m\geqslant 4n^2$ між числами m і $2m$ є не менше n простих чисел.

20. Довести, що всі непарні числа виду $4k+1$ з проміжку $[1,2^n-1]$, можна розставити по колу так, що для будь-яких трьох сусідніх чисел a,b,c різниця b^2-ac буде ділитися на 2^n. Довести, що це можна зробити і для всіх непарних чисел виду $4k+3$, однак цього не можна зробити для всіх непарних чисел.

21. Довести, що при простому p число:
    а) (Вільсон - Лейбніц) $(p-1)!$ ділиться на p;
    б) (Беббідж) $C^p_{2p-1}-1$ ділиться на p^3, якщо $p>2$.

Відповіді. Вказівки. Розв'язки

Розділ: Теорія подільності в кільці цілих чисел

§ 1.1. Відношення подільності. Ділення з остачею

1. а) $q=-2$; б) такого q не існує; в) $q=1$; г) такого q не існує.

2. а) $q=-8, r=5$; б) $a=-712+r, r\in\{0,1,2,3,4,5,6,7\}$; в) таких цілих b і r не існує, оскільки $0<-23-13b<|b|$; г) $a=9+36t, q=-t, t\in\mathbb{Z}$; д) $(b,q)\in\{(51,-5),(-51,5),(85,-3),(-85,3),(255,-1),(-255,1)\}$; е) $a=15t+11, b=t$, де $|t|>11$.

3. а) $3n$; б) $5n+2$; в) $n=(-7)q+r$, $r\in\{1,2,3,4,5,6,\}$; г) $n=6k\pm1$.

4. Ділиться. Застосуйте формулу бінома Ньютона так: $23^{23}=(20+3)^{23}=20^{23}+20^{22}\cdot3+\cdots+20\cdot3^{22}+3^{23}=10\cdot q+3^{23}$. Отже, дане число ділиться на 10 тоді і тільки тоді, коли на 10 ділиться $8\cdot3^{23}-2^{32}$. Далі, $3^{23}=3^3\cdot(3^4)^5=3^3\cdot81^5=(20+7)(80+1)^5=10q_2+7$ і $2^{32}=(2^5)^5\cdot2^5\cdot2^2=10q_1+6$. Тоді $8\cdot3^{23}-2^{32}=8\cdot(10q_2+7)-(10q_1+6)=10g$. **5.** а) 1; б) 2; ; в) 6; г) 1,2,4.

6. а) 121; б) розгляньте числа виду $6g+5$ і виберіть з них найменше, яке задовольняє умову задачі: 59. **7.** а) 0; б) 1; в) 1; г) 2. **8.** 1,8,0. **9.** а) 5; б) 7; в) 7; г) 6. **10.** а) Обчисліть суму членів геометричної прогресії та врахуйте, що різниця a^n-b^n ділиться на $a-b$; б) $11^{2n}+31^{2n}+38\cdot11^n\cdot31^n=(11^n-31^n)^2+40\cdot11^n\cdot31^n=(11^{n-1}+11^{n-2}31+\cdots+31^{n-1})^2\cdot400+40\cdot11^n\cdot31^n$; в) $(n+1)^{3n}-n^{2n}(n+3)^n=(n^3+3n^2+3n+1)^n-(n^3+3n^2)^n$; г) Покажіть, що $(n^4+6n^3+11n^2+6n)=n(n+1)(n+2)(n+3)$. **11.** а) 1,4,7,16; б) 1; в) 1,3,25; г) 3. **12.** Нехай $m=q_1n+r$, $m+n=q_2(m-n)+r$ і $r\neq0$. Припущення про те, що $q_1=1$ приводить до протиріччя. Тому $q_1>1$. Тоді маємо: $m>2n$, $n<\frac{m}{2}$, $m+n<\frac{3m}{2}$, $m-n>\frac{m}{2}$ і $1\leqslant q_2<3$. Перебором для q_2 встановлюємо, що $\frac{m}{n}=\frac{5}{2}$.

16. В задачах: а)–г) слід застосувати формулу $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$; д) записати $144^n=(133+11)^n$; е)–к) можна застосувати метод математичної індукції. **17.** Дивись розв'язок задачі 28.

18. а) Подайте числа m та n у виді $3q+r$ і розгляньте всі можливі варіанти. б) Застосуйте метод від супротивного. **19.** Площа ділиться на 2,3,4,6 і може ділитися на 5,7,8,9,10.

23. 1996. Дійсно, $(\frac{1}{1997}-\frac{1997}{m}>0,\ \frac{1}{1998}-\frac{1997}{m}<0)\leftrightarrow1997\cdot1997<m<1997\cdot1998$. Тому $m=1997\cdot1997+k$ для $k=1,\ldots,1996$. Для всіх цих m дріб $\frac{1997}{m}$ буде нескоротним, оскільки число 1997 просте. **24.** Так, буде. Це $\left(\frac{10^{1998}+2}{3}\right)^2$. **25.** Не може, оскільки число 2001 не можна подати у виді

$7k+4$. **26.** Розглянемо послідовність $\{b_i,\ i \geqslant 0\}$ таку, що

$$b_0 = b_1 = 1, \quad b_{i+1} = \frac{f(b_i)}{b_{i-1}} \text{ для } i \geqslant 1.$$

Методом математичної індукції доведемо, що всі $b_i \in \mathbb{N}$. Цей факт, очевидно, є вірним для $i \leqslant 3$. Припустимо, що це твердження виконується для всіх $i \leqslant k$ $(k \geqslant 3)$, і доведемо його для $i = k+1$. Маємо, що $b_{k+1} = \frac{f(b_k)}{b_{k-1}} = =$ $\frac{1}{b_{k-1}} f\left(\frac{f(b_{k-1})}{b_{k-2}}\right) = \frac{1}{b_{k-1}}\left(\frac{f^n(b_{k-1})}{b_{k-2}^n} + a_1\frac{f^{n-1}(b_{k-1})}{b_{k-2}^{n-1}} + \ldots + a_{n-1}\frac{f(b_{k-1})}{b_{k-2}} + 1\right) =$ $\frac{f^n(b_{k-1}) + a_1 f^{n-1}(b_{k-1}) b_{k-2} + \ldots + a_{n-1} f(b_{k-1}) b_{k-2}^{n-1} + b_{k-2}^n}{b_{k-1} b_{k-2}^n}$.

Оскільки, за означенням послідовності, $b_i b_{i+2} = f(b_{i+1})$ та вільний член многочлена дорівнює 1, b_i та b_{i+1} взаємно прості. З припущення індукції ми маємо, що чисельник останнього дробу в (1) ділиться на b_{k-2}^n, і тому нам досить довести, що він ділиться на b_{k-1}. Маємо, що при діленні на b_{k-1} $f(b_{k-1})$ дає остачу 1; тому весь чисельник дає таку ж остачу, як і

$$1 + a_1 b_{k-2} + \ldots + a_{n-1} b_{k-2}^{n-1} + b_{k-2}^n = f(b_{k-2})$$

(тут ми використали умову $a_i = a_{n-i}$). $f(b_{k-2}) = b_{k-1} b_{k-3}$, де, за припущенням індукції, всі b_i — натуральні числа. Тому наш чисельник ділиться на b_{k-1}.

Також, $b_2 > b_1$, і для всіх наступних i

$$b_{i+1} = \frac{f(b_i)}{b_{i-1}} > \frac{b_i^n}{b_{i-1}} > b_i^{n-1} \geqslant b_i.$$

Тепер легко бачити, що нескінченна послідовність різних пар чисел $(b_i,\ b_{i+1})$, $i \geqslant 0$, задовольняє умову задачі.

27. Якщо $a^2 b + a + b$ ділиться на $ab^2 + b + 7$, то таку подільність має і число $b(a^2 b + a + b) - a(ab^2 + b + 7) = b^2 - 7a$.

Оскільки $a \geqslant 1$, ми маємо $b^2 - 7a < ab^2 + b + 7$. Тому, якщо $b^2 - 7a \geqslant 0$, то $b^2 - 7a = 0$. Тоді b ділиться на 7, і $(a, b) = (7c^2, 7c)$ для деякого натурального числа c. Легко переконатись, що кожна така пара задовольняє умову.

Нехай $b^2 - 7a < 0$. Тоді $7a - b^2$ ділиться на $ab^2 + b + 7$, $0 < 7a - b^2 < 7a$. Це можливе лише тільки для $b = 1$ або $b = 2$, оскільки інакше $ab^2 + b + 7 > 9a$.

Для $b = 1$ ми отримуємо, що $7a - 1$ повинно ділитися на $a + 8$. Маємо $7a - 1 = 7(a+8) - 57$, $57 = 1 \cdot 57 = 3 \cdot 19$, звідки можливими є тільки $a = 11$ або $a = 49$. Перевірка показує, що (11, 1) та (49, 1) задовольняють умову.

Для $b = 2$ число $7a - 4$ повинно ділитися на $4a + 9$. Оскільки $4(7a - 4) = 7(4a + 9) - 79$, та 79 не має дільників вигляду $4a + 9$, то в цьому випадку немає розв'язків.

Відповідь: $(a,b)=(7c^2,7c)$, $c=1,2,\ldots$, та $(a,b)=(11,1)$, $(a,b)=(49,1)$.

28. Нехай $a_1,a_2,a_3,\cdots,a_{100}$ - дані числа. Розгляньте тепер числа $a_1,a_1+a_2,a_1+a_2+a_3,\cdots,a_1+a_2+a_3+\cdots+a_{100}$. Можливі два варіанти: одне з цих чисел ділиться на 100, або два з цих чисел при діленні на 100 дають однакові остачі. В другому випадку різниця таких чисел буде шуканою.

29. Для $n=2$ твердження є очевидним. Нехай $n>2$. Тоді $n^n-n^2+n-1=(n^{n-2}-1)n^2+(n-1)=(n-1)(n^{n-3}+\cdots+1)+(n-1)n^0=(n-1)(n^{n-1}+\cdots+n^2+n^0)$. Оскільки n^k-1 ділиться на $n-1$ для кожного $k=0,2,3,\cdots,n-1$, то $n^{n-1}+\cdots+n^2+n^0$ також ділиться на $n-1$. Тому число $(n-1)(n^{n-1}+\cdots+n^2+1)$ ділиться на $(n-1)^2$.

30. Перевірте, що для будь-яких цілих k і k' числа $(1+\frac{kn}{m})(1+\frac{k'n}{m})$ і $(1+\frac{(k+k')n}{m})$ дають однакову остачу при діленні на n. Тому, $(1+\frac{n}{m})^s-1$ кратне n тоді і тільки тоді, коли s кратне n.

31. а) Згрупуйте рівновіддалені від кінців доданки. б) Знайдеться така перестановка чисел $x_1,x_2,\cdots x_{p-1}$, що при всіх k число kx_k-1 ділиться на p. Тому, враховуючи, що

$$\frac{2}{p}(1+\frac{1}{2}+\cdots+\frac{1}{p-1})=\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\cdots\frac{1}{(p-1)1},$$

маємо, що чисельник цього дробу дає таку ж остачу, що і число

$$-((p-1)!)^2(x_1^2+\cdots+x_{p-1}^2)=-((p-1)!)^2(1^2+\cdots+(p-1)^2)=$$

$$=-((p-1)!)^2\cdot\frac{p(p-1)(2p-1)}{6}.$$

Останнє ж ділиться на p (оскільки $p\geqslant 5$). **32.** Оскільки при непарному $n=2m+1$ серед чисел $1,2,\ldots,n$ є лише m парних, то серед $m+1$ чисел $k_1,k_3,k_5,\ldots,k_n$ знайдеться хоча б одне непарне. Нехай це k_{2i+1}. Відповідний співмножник $k_{2i+1}-(2i+1)$ нашого добутку є тоді парним. Отже, парний і весь добуток. **33.** Нехай $k=10^{n+1}$. Тоді перше число в умові дорівнює k^3+2k^2-1, а друге – $k+1$. Отже, маємо $k^3+2k^2-1=(k+1)(k^2+k-1)$. **34.** Нехай $n^2+19n+99=m^2$. Тоді $4(n^2+19n+99)=4m^2$ і $4m^2-(2n+19)^2=35$ або $(2m-2n-19)(2m+2n+19)=35$. Розглядаючи тепер всі можливі розклади числа 35 на множники ми прийдемо до систем лінійних рівнянь, які дадуть шукані розв'язки: $n\in\{-18,-10,-9,-1\}$.

§ 1.2. Найбільший спільний дільник і найменше спільне кратне. Алгоритм Евкліда. Взаємно прості числа

2. $(n,n+1)=1,[n,n+1]=n\cdot(n+1)$; $(n,n+1,n+2)=1$; якщо n - непарне, то $[n,n+1,n+2]=n(n+1)(n+2)$; якщо n - парне, то

$[n, n+1, n+2] = \frac{1}{2}n(n+1)(n+2)$; **3.** Нехай $(m, n) = d, m = dm_1, n = dn_1$. Тоді $[m, n] = dm_1n_1$. **4.** а) Перша рівність виконується завжди, а друга – не завжди: $(7, 3) = 1$, а $(7+3, 7-3) = 2$; б),в), г) – виконуються завжди. **5.** а) Так; б) так ; в) ні, наприклад, при $n = 7$ маємо (6,15)= 3; г) так. **6.** Ні. **7.** Ні. Застосуйте метод від супротивного. **8.** а) 21; б) 105; в) 71; г) 33. **9.** а) 1,13; б) 1,3,7,21. **10.** 5.

11. а) $6 = -135 \cdot 822 + 64 \cdot 1734$; б) $1 = 17 \cdot 4373 + 90 \cdot (-826)$; в) $43 = 903 \cdot (-4) + (-731) \cdot (-5)$; г) $17 = -10 \cdot 1445 + 23 \cdot 629$. **12.** а) 3276; б) 67818; в) 12180; г) 2940. **13.** а) $a = 4, b = 180; a = 20, b = 36$ і навпаки; б) $a = 4, b = 24; a = 8, b = 12$ і навпаки; в) $a = 552, b = 115; a = 435, b = 232$ і навпаки; г)$a = 20, b = 120$ і навпаки; $a = 24, b = 60$ і навпаки; $a = 30, b = 40$ і навпаки.

14. а) Оскільки $\frac{8n+71}{5n+46} = 1+\frac{3n+25}{5n+46}$, то даний дріб є скоротним тоді і тільки тоді коли скоротним є дріб $\frac{3n+25}{5n+46}$. Останній дріб є скоротним тоді і тільки тоді коли скоротним є дріб $\frac{5n+46}{3n+25}$. Продовжуючи далі аналогічні міркування (тобто, застосовуючи фактично алгоритм Евкліда) ми отримаємо, що даний дріб є скоротним тоді і тільки тоді коли скоротним є дріб $\frac{13}{n+4}$. Останній дріб є скоротним, коли $n = 13k - 4$, де $k \in \mathbb{N}$. б) Застосувавши рівність з задачі 4, отримаємо: $(4n-5, 3n-31) = (3n-31, n+26) = (2n-57, n+26) = (n-83, n+26) = (-109, n+26)$. Це означає, що даний дріб можна скоротити на 109 при $n = -26 + 109k$, де $k \in \mathbb{N}$. в) Дріб можна скоротити на 5 при $n = 3 + 5k, k \in \mathbb{Z}$; при інших значеннях n він є нескоротним. г) Дріб скорочується: на 2 – при $n = 2k$; на 3 – при $n = 1+3k$; на 6 – при $n = 4+6k$; на 9 – при $n = 7 + 9k$; на 18 – при $n = 16 + 18k$; при інших значеннях n він є нескоротним. **15.** 57. **16.** Застосуйте метод від супротивного. **17.** а) Позначивши $d_1 = (m, n)$ та $d_2 = (7m + 5n, 4m + 3n)$, доведіть, що $d_1 \vdots d_2$ та $d_2 \vdots d_1$; б),в),г) - застосуйте формулу для обчислення НСК двох чисел.

18. а) - в) - застосуйте метод від супротивного; г) Нехай $(2^m-1, 2^n-1) = d$ і при діленні з остачею маємо $m = nq + r$. Тоді $2^m - 1 = 2^{nt+r} - 1 = 2^r \cdot 2^{nt} - 2^r + 2^r - 1 = 2^r \cdot (2^{nt} - 1) + (2^r - 1) = 2^r \cdot ((2^n)^t - 1) + (2^r - 1) = 2^r \cdot (2^n-1) \cdot (2^{n(t-1)} + \cdots + 1) + (2^r-1)$. Тому $(2^r-1) \vdots d$. Застосовуючи до m та n алгоритм Евкліда, ми прийдемо до $(2^1-1) \vdots d$, тобто $d = 1$. д) Нехай $m > n$. Тоді $2^{2^m} + 1 = (2^{2^m} - 1) + 2 = (2^{2 \cdot 2^{m-1}} - 1) + 2 = (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1) + 2 = (2^{2^{m-1}} + 1)(2^{2^{m-2}} + 1)(2^{2^{m-2}} - 1) + 2 = \cdots = (2^{2^{m-1}} + 1)(2^{2^{m-2}} + 1) \cdots (2^{2^n} + 1) \cdots (2^2 + 1)(2 + 1) + 2$. Якщо $(2^{2^n} + 1, 2^{2^m} + 1) = d$, то $2 \vdots d$ і $1 \vdots d$; тому $d = 1$. е) Доведіть, що $(2m + n, m) = 1$ та врахуйте 18 а). **19.** Нехай $(2^m-1, 2^n-1) = 1$ і $(m, n) = d$. Тоді $m = dg$ і $n = ds$. Але $2^m - 1 = 2^{dg} - 1 =$

$(2^d)^g - 1 = (2^d - 1)q_1$. Аналогічно $2^n - 1 = 2^{ds} - 1 = (2^d)^s - 1 = (2^d - 1)q_2$. Це означає, що $2^d - 1 = 1$ і $d = 1$.

20. Нехай $a = 2^{1986} - 1$ та $b = 2^{1983} - 1$. Тоді $a - b = 7 \cdot 2^{1983}$ і числа a та b є непарними. Тому $(a, b) = 7$ або $(a, b) = 1$. Але $a = 2^{1986} - 1 = (2^3 - 1)(2^{1983} + 2^{1980} + \cdots + 2 + 1)$ ділиться на 7. Тому $b = a - (a - b)$ також ділиться на 7. Отже, $(a, b) = 7$.

21. Задамо на множині M відношення: $s \sim t$ тоді і тільки тоді, коли s і t пофарбовано в один колір. Очевидно, що " $\sim$ " є відношенням еквівалентності. Нехай $n = kq + r$, де $0 < r < k$. Розглянемо число $n - k$ яке взаємно просте з n. За умовою а) $k \sim (n - k)$. Крім того, це число задовольняє умову б). Дійсно, візьмемо $s \in M \setminus \{n - k\}$. За а) маємо $s \sim (n - s)$, а за умовою б) для числа $k - (n - s) \sim |k - (n - s)| = |k - n + s| = |(n - k) - s|$. Отже, $s \sim |(n - k) - s|$. Застосовуючи аналогічні міркування покажемо послідовно, що числа $n - 2k, \cdots, n - qk = r$ задовольняють умову б) і взаємно прості з n та k. Оскільки $(n, k) = (k, r) = \cdots = 1$, то число 1 також задовольняє умову б). Тоді для кожного $i \in M \setminus \{1\}$ маємо $i \sim |1 - i|$. Звідки $2 \sim 1, 3 \sim 2, 4 \sim 3, \cdots, (n - 1) \sim (n - 2)$. Таким чином, всі числа множини M пофарбовано одним кольором.

26. Гіпотеза: твердження є істиним висловленням. **27.** Доведіть, що рівність $|kn - lm| = 1$ є достатньою умовою. Перевірте, чи є вона необхідною умовою. **30.** $-9, -3, -1, 7$. **31.** Нехай $(2^m - 1, 2^n + 1) = d$ і $2^m - 1 = ad$, $2^n + 1 = bd$. Тоді $2^{mn} = (ad + 1)^n = (bd - 1)^m$. Оскільки число m є непарним, то ми отримали при діленні числа 2^{mn} на d остачу 1 та -1. Отже, $d = 1$.

33. Нехай $m > n$. Оскільки 5 та 7 взаємно прості, маємо, що НСД$(5^m + 7^m, 5^n + 7^n)$ = НСД$(5^m + 7^m - 5^{m-n}(5^n + 7^n), 5^n + 7^n)$ = НСД$(7^n(7^{m-n} - 5^{m-n}), 5^n + 7^n)$ = НСД$(7^{m-n} - 5^{m-n}, 5^n + 7^n)$. Продовжуючи такі дії далі, з алгоритму Евкліда отримаємо, що шукане значення обов'язково є дільником одного з чисел

$$5^{\text{НСД}(m,n)} + 7^{\text{НСД}(m,n)}, \quad 7^{\text{НСД}(m,n)} - 5^{\text{НСД}(m,n)}.$$

Тому для взаємно простих $m,\ n$ це значення обов'язково є дільником 12.

З іншого боку, сума однакових непарних степенів ділиться на суму основ (це випливає з відомого розкладу такого двочлена на множники). Тому для непарних m та n числа $5^m + 7^m$ та $5^n + 7^n$ будуть ділитися на 12, і тому їх найбільший спільний дільник дорівнює 12.

Якщо, наприклад, число m парне, то розгляд значень остач при діленні $5^m + 7^m$ на 3 та 4 показує, що подільності на 3 та 4 немає. Тому шуканий НСД може дорівнювати тільки 1 або 2. Очевидно, що розглядувані значення парні, тому в цьому випадку НСД дорівнює 2.

Відповідь: 12 для обох непарних $m,\ n$; 2 в інших випадках.

34. Врахуйте, що кожний спільний дільник чисел $1979^2 + 2^{1979}$ та 1979 є дільником числа 2^{1979}. **36.** а) Так, наприклад, $m = n = 2000$. б) Ні. У всіх випадках (m і n — парні, m і n — непарні, m і n — різної парності) значення виразу є числом парним і не може дорівнювати 2001.

§ 1.3. Прості і складені числа. Канонічна форма натурального числа

1. Просте, складене, складене, просте, складене. **2.** а) 79,83,89, 97; б) 151,157,163,167,173; в) 2551,2557. **3.** Ні. **4.** 121. **5.** 1 або 5. **6.** а) $2^4 \cdot 31$; б) $3 \cdot 587$; в) $5^3 \cdot 17^2$; г)-к) Застосуйте формули розкладу на множники відповідних многочленів.г) $2^3 \cdot 3 \cdot 31$; д) $3 \cdot 5 \cdot 7 \cdot 37 \cdot 59$; е) $2 \cdot 11 \cdot 31 \cdot 173$; є) $2^2 \cdot 31 \cdot 127$; ж) $13 \cdot 37 \cdot 61 \cdot 73 \cdot 181$; з) $2^6 \cdot 3 \cdot 5^2 \cdot 1201$; к) $3 \cdot 7 \cdot 11 \cdot 19 \cdot 89$. **7.** 2^{k-1}. **8.** Ні. Застосуйте метод від супротивного. **9.** а) Ні; б) Ні; в) $p = 3$. Це єдина трійка чисел-близнят(трійнят); г) $p = 3$. **10.** а),б),в),г) - $p = 3$; д) $p = 2$; е) $p = 5$.

11. 3,4. Добуток $|n-2| \cdot |n-5|$ буде простим числом тоді і тільки тоді, коли один із співмножників дорівнює одиниці, а другий при цьому є простим числом.

12. $p = 13$. Розгляньте рівняння $2p + 1 = (2n + 1)^3$. **13.** Вказівка: для перевірки доведіть спочатку, що $x^2 - y^2$ ділиться на 3, а потім застосуйте рівності

$$\frac{x^2 + 2y^2}{3} = \left(\frac{x - 2y}{3}\right)^2 + 2\left(\frac{x + y}{3}\right)^2 = \left(\frac{x + 2y}{3}\right)^2 + 2\left(\frac{x - y}{3}\right)^2.$$

14. $2^{mk} - 1 = (2^m)^k - 1 = (2^m - 1)a, a \in \mathbb{N}$. **15.** Застосуйте формулу суми членів арифметичної прогресії. **16.** Застосуйте основну теорему арифметики. **17.** Виділіть повний квадрат.

18. б) Припустимо, що множина простих чисел виду $3k + 8 = 3(k + 1) + 2$ скінченна. Нехай це числа $p_1 < p_2 < \cdots < p_s$. Розглянемо число $t = 3p_1p_2 \cdots p_s + 2$. Зрозуміло, що це число виду $3n + 2$. Оскільки $t > p_s$ і $t > 1$, то t складене. Отже, воно ділиться хоча б на одне просте число. На 3 воно не ділиться. Зрозуміло також, що всі прості дільники числа t не мають виду $3n + 1$. Отже, число t ділиться хоча б на один простий дільник виду $3n + 2$. Оскільки всі такі прості числа знаходяться серед чисел $p_1p_2 \cdots p_s$, то t ділиться на одне з них. Тоді з рівності $t = 3p_1p_2 \cdots p_s + 2$ випливає, що на це число поділиться і число 2. Дістали суперечність.

19. а), б) Використайте метод математичної індукції; в) $p_1p_2 \cdots p_{k-1} = p_sq (s > k, q \geqslant 1)$, звідки $p_s \leqslant p_1p_2 \cdots p_{k-1}$ і $p_s < p_1p_2 \cdots p_k$. Тоді $p_{k+1} < p_1p_2 \cdots p_k$; г) Нехай p_k – найбільше просте число, що не перевищує $n > 2$. Канонічний розклад числа $t = p_1p_2 \cdots p_{k-1}$ містить тільки прості числа, більші за n. Отже, $t > n$, а тому $p_1p_2 \cdots p_k > n$.

20. Якщо n має хоча б один непарний дільник $d > 1$, то

$$2^n + 1 = (2^{\frac{n}{d}} + 1)(2^{\frac{n}{d}(d-1)} - 2^{\frac{n}{d}(d-2)} - \cdots - 2^{\frac{n}{d}} + 1),$$

де обидва множники більші від 1, оскільки $n \geqslant 3, d \geqslant 3$. Тоді число $2^n + 1$ було б складеним, що суперечить умові. Отже, $n = 2^k$.

21. Нехай $m = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_1^{\alpha_k}$ і $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $k = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$,де $\alpha_i, \beta_i, \gamma_i \geqslant 0$. Розглянемо просте число p_i, де $0 \leqslant i \leqslant k$. Для показників, з якими це число входить в узагальнені канонічні розклади m, n і k можливі 6 варіантів: $\alpha_i \leqslant \beta_i \leqslant \gamma_i$, $\alpha_i \leqslant \gamma_i \leqslant \beta_i$, $\beta_i \leqslant \alpha_i \leqslant \gamma_i$, $\beta_i \leqslant \gamma_i \leqslant \alpha_i$, $\gamma_i \leqslant \alpha_i \leqslant \beta_i$, $\gamma_i \leqslant \beta_i \leqslant \alpha_i$. Залишається перевірити з яким показником входить просте число p_i у ліву і праву частини рівності. Так, наприклад, у першому випадку у добуток $mnk(m,n,k)$ воно входить з показником $\alpha_i + \beta_i + \gamma_i + \alpha_i$, а в добуток $[m,n,k](m,n)(m,k)(n,k)$ – з показником $\gamma_i + \alpha_i + \beta_i + \alpha_i$, тобто показники однакові. Аналогічно перевіряться у всіх інших випадках. Це означає, що має місце рівність $mnk(m,n,k) = [m,n,k](m,n)(m,k)(n,k)$.

22. 1,4,9,19,25. **24.** До 39 - прості числа.

28. Розкладемо число 1998 на прості множники ($1998 = 2 \cdot 3^3 \cdot 37$) і скористаємось тим, що вік кожної особи сім'ї є дільником цього числа. Далі перебором встановлюємо, що татові 37 років, матері — 27, одній дитині 2 роки, а дві інші дитини мають по одному року.

30. За формулою бінома Ньютона маємо $(p-m)^p = p^p - C_p^1 p^{p-1} m + \cdots + C_p^{p-1} p(-m)^{p-1} + (-m)^p$. Тому при довільному m і простому p сума $m^p + (p-m)^p$ ділиться на p^2. Оскільки при $m = 1, 2, 3, \cdots, p-1$ самі числа m^p та $(p-m)^p$ на p^2 не діляться, то сума остач від ділення цих чисел на p^2 дорівнює p^2. Тоді сума остач від ділення на p^2 чисел $1^p, 2^p, \cdots, (p-1)^p$, тобто $1^p, (p-1)^p; 2^p, (p-2)^p; \cdots$ (всього $\frac{p-1}{2}$ пар) дорівнює $p^2 \cdot \frac{p-1}{2}$.

31. Покажіть, що хоча б одне з чисел a, b, c, d дорівнює 2 (інакше ліва частина рівняння ділиться на 4, а права – ні). Рівняння з трьома невідомими досліджується аналогічно. **32.** Вказівка: доведіть, що $a_n - 22$ ділиться на a_{n-6}. **33.** Вказівка: позначіть $x = 991$ і подайте отриманий многочлен у вигляді добутку. **34.** Для доведення застосуємо метод від супротивного. Припустимо, що якесь просте число p входить у канонічний розклад числа $a - b$ у непарному степені $2k+1$. Оскільки $ab \vdots (a-b)$, то одне з чисел a або b ділиться на p^k. Якщо $a \vdots p^k$, то $b = a - (a-b)$ також ділиться на p^k. Це означає, що число c ділиться на p і ми прийшли до висновку, що всі числа a, b, c мають спільний простий дільник p. Отримане протиріччя з умовою означає, що показник простого числа p може бути тільки парним числом. Таким чином, число c є квадратом деякого натурального числа.

35. Вказівка: зауваживши, що число k є парним покажіть, що можливі тільки варіанти, коли $l < n < m$ або $m < n < l$. При цьому отримаємо відповіді $k = 2, l = 4, m = 11, n = 6$ або $k = 2, l = 11, m = 4, n = 6$.

36. Подамо добуток довільної пари (a, b) чисел з даного набору у вигляді добутку квадрата натурального числа на добуток простих дільників у першому степенях. поставимо у відповідність парі (a, b) отриманий набір простих дільників. Всіх різних пар (a, b) з даного набору з 48 чисел можна скласти $C_{48}^2 = 48 \cdot \frac{47}{2}$, а число наборів з 10 простих дільників (по одному, по два і т. д. включаючи пустий набір) рівне 2^{10}. Оскільки $C_{48}^2 > 2^{10}$, то знайдуться дві різних пари (a, b) і (c, d) з набору, яким відповідає один і той же набір $(p_1, p_2, \ldots, p_k)$ простих дільників $0 \leqslant k \leqslant 10$. Тому $abcd$ – точний квадрат.

Якщо при цьому пари (a, b) і (c, d) не мають спільного елемента, то числа a, b, c, d шукані. Якщо ж спільний елемент є, наприклад $b = d$, то тоді ac є точним квадратом. Виключимо на деякий час пару (a, c) з розгляду. Тоді ми маємо набір з 46 чисел, добуток яких має не більше 10 простих дільників.

Оскільки $C_{46}^2 > 2^{10}$, то провівши аналогічні міркування, ми приходимо до висновку про існування двох різних пар чисел (x, y) (z, t) з набору, для яких $xyzt$ є точним квадратом. Якщо спільного елемента у цих пар немає, то x, y, z, t – шукані чотири числа; якщо ж спільний елемент є, наприклад $x = t$, то yz – точний квадрат. В цьому випадку шуканою четвіркою чисел є a, c, y, z.

§ 1.4. Системні числа

1. а) CCCXXVI; б) MMMMMMMLXM; в) MMDCLIV; г) MIIIC. **2.** а) 24; б) 157; в) 741; г) 1999; д) 2001; е) 1648. **3.** а) 6; б) 12; в) 4; г) 11. **4.** а) Так; б) ні; в) ні; г) так. **5.** а) 10^9; б) 8387; в) 25,9375; г) 287,408203125. **6.** Збільшиться в 6, 36, 216 раз. **7.** а) 23032_4; б) 14134_5; в) 503205_6; г) 40230101_{10}. **8.** $x = 100, y = 10, z = 1$. **9.** 29786 + 850 + 850 = 31486. Доведіть спочатку, що $n = 0$ і $e = 5$ та $o = 9$. **10.**

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	12	13	14	15

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	51

11. а) 410042_7; б) -10533_6; в) 3406555_7; г) 1035_6; д) $12,34244_6$; е) $3,71(25)_8$. **12** а) 1; б) 3; в) 1; г) 4_6. **13.** а) $4(10)2(11)_{12}$; б) 4126_8; в)

$5342_8; 101011100010_2$; г) 2184_9; д) 11202102120100_3; е) 2121311_5. **14.** а) $x = 6$; б) $x = 5$; в) $x = 201401_6$; г) $x = 8$; д) $x_1 = y_1 = 0, x_2 = 3, y_2 = 1$; е) $x = y = z = 0$. **15.** $10^{k-1}, k \in \mathbb{N}$. **16.** а) $25^2 = 625$ та $76^2 = 5776$; б) $625^2 = 390625$ та $376^2 = 141376$. **17.** Якщо в записі числа p^n є тільки по 2 однакових цифри, то їх сума дорівнює 90 і число p^n ділиться на 3.

20. а) $2(g-1) = \overline{1(g-2)}_g$; б) $(g-1)^2 = \overline{(g-2)1}_g$. **21.** 9376. **22.** Перейдіть до систематичного запису числа та застосуйте властивості подільності. **23.** Так, можна. Застосуйте трійкову систему числення в якій використовуються цифри 0,-1 та 1. **4.28.** 2100010006. **29.** Доведіть, що число $(n+9)(n+10)(n+11) - (n-1)n(n+1)$ ділиться на 10. **30.** $a = 33\cdots3$ (n цифр). **31.** Відповідь: (882,828,288), (774,747,477), (666,666,666), (558,585,855).

32. Неважко помітити, що останні чотири цифри чисел 5^n, починаючи з $n = 5$, періодично повторюються: 3125, 5625, 8125, 0625, 3125, 5625,.... Тому останніми чотирма цифрами числа 5^{1998} будуть 5625, а числа $1997 \cdot 5^{1998}$ — 3125. Цими ж цифрами закінчується друге число. **33.** Вказане число ділиться на число $111111 = 111 \cdot 1001 = 37 \cdot 3 \cdot 1001$.

34. Позначимо $b = \overline{a_2a_3a_4a_5a_6}$. Тоді $A = \overline{a_1a_2a_3a_4a_5a_6} = 10^5a_1 + b$ та $B = \overline{a_2a_3a_4a_5a_6a_1} = 10b + a_1$. З останніх рівностей маємо $10A - B = 10^6a_1 + 10b - 10b - a_1 = 99999a_1$. Оскільки 99999 ділиться на 37, то $10A - B$ ділиться на 37. Отже, $B = \overline{a_2a_3a_4a_5a_6a_1}$ ділиться на 37.

35. 8. Це: 123, 145, 167, 348, 268, 578, 356, 247. **36.** Врахуйте, що $\overline{abcdmn} = \overline{abc} \cdot 999 + \overline{abc} + \overline{dmn}$.

37. Доведіть,що коли число з k цифр ділиться на 2^k, то до нього зліва можна приписати цифру 1 або 2 так, що отримане число буде ділитися на 2^{k+1}. Тому існує число, яке ділиться на 2^n і записане тільки одиницями і двійками.

39. Потрібно спочатку довести, що коли сума двох цілих чисел дорівнює числу $999\ldots99$, то при їх додаванні ні в одному розряді не відбулося переносу у наступний розряд. **40.** Потрібно спочатку довести, що при додаванні ні в одному розряді не відбулося переносу одиниці у наступний розряд.

41. Зауважимо, що нулі в кінці числа n можна відкидати (дійсно, якщо $n = a \cdot 10^t$, то $\overleftarrow{n} = \overleftarrow{a}$ кратне до k, а тому і $a = \overleftarrow{(\overleftarrow{a})}$ кратне k). Нехай $n = \overline{a_1a_2\ldots a_{n-1}a_n}$ ділиться на k і $a_n \geqslant 1$. Віднімаючи від $n \cdot 10^{n+2}$ число $\overleftarrow{n}$ "в стовбчик", отримаємо різницю

$$m = \overline{a_1a_2\ldots a_{n-1}(a_n-1)99(9-a_n)(9-a_{n-1})\ldots(9-a_2)(9-a_1)}.$$

Додаючи тепер "в стовпчик"числа m і $\overleftarrow{m}$ отримаємо число

$$y = 10\overbrace{999\ldots99}^{n-1}98\overbrace{900\ldots000}^{n-1},$$

яке ділиться на k. Якщо виконати ті ж дії, починаючи з чисел $n \cdot 10^{n+3}$ і $\overleftarrow{n}$, то одержимо число

$$x = 10\overbrace{999\ldots99}^{n-1}998\overbrace{900\ldots000}^{n-1},$$

яке також ділиться на k. Але тоді $\overleftarrow{(x-y)} = 99$ ділиться на k.

§ 1.5. Числові функції.

1. а) 9;511; б) 2; 258; в) 4;1500; г) $9;553 \cdot 1893 = 1046829$. **2.** 54; 128; 1210; 1872. **3.** а) -1; б) 0; в) 0,7; г) $-0,25$. **4.** $\tau(p) = 2; \sigma(p) = p+1; \varphi(p) = p-1$. **5.** $p^3 - p^2$. **6.** 27. **7.** $n = 2 \cdot 3^6$. **8.** 499 нулів. Необхідно підрахувати скільки разів множник 5 входить в канонічний розклад добутку. **9.** а) 675; б) 180; в) $3^3 5^4$; г) 1400. **10.** а) 8; б) 66; в) 40; г) 12. **11.** а) 28; б) 280. **12.** а) $x \in \{36, 28, 13, 26, 21, 42\}$; б) $x = 2^k, k \in \mathbb{N}$; в) розв'язків немає; г) 3; д) $x \in [\frac{5}{16}; \frac{5}{8}[$; е) 0,1,3,4.

15. а) $2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$; б) $2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$; в) $2^{16} \cdot 3^8 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$; г) $2^2 \cdot 5^2 11 \cdot 13 \cdot 17 \cdot 19$.

16. а) $[\frac{10^7}{786}] - [\frac{10^6}{786}] = 11450$; б) $1000 - [\frac{1000}{5}] - [\frac{1000}{7}] + [\frac{1000}{35}] = 686$; в) 5634; г) 393. **23.** $n = 2$. **5.24.** 0 або 1. **25.** $S(n) = \frac{n\varphi(n)}{2}$.

28. Нехай $[x] = n, \{x\} = \alpha, n \in \mathbb{Z}, n \neq 0, 0 < \alpha < 1$. Тоді $n - \alpha = \frac{1}{\alpha} - \frac{1}{n} = \frac{n-\alpha}{\alpha n}$. Оскільки $n \neq \alpha$, то $\alpha n = 1$. Звідки $\alpha = \frac{1}{n}, n \geqslant 1$. Отже, $x = \frac{n^2+1}{n}$, де $n \in \mathbb{N}$.

29. а) Число 997920 ділиться на $11 \cdot 5$ та $12 \cdot 7$. Оскільки 11 і 5 взаємно прості, то таких, що задовольняють умові задачі є $\frac{n}{p} - \frac{n}{pq} = \frac{997920}{11} - \frac{997920}{55} = 72576$, тобто більше ніж 2080. Перших менше; б) перших більше.

30. Для взаємно простих натуральних чисел a та b буде $\tau(ab) = \tau(a)\tau(b)$. Нехай $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, де $p_1, p_2, \ldots, p_t$ — різні прості числа. Тоді $\tau(n) = (m_1+1)(m_2+1)\cdots(m_t+1)$, $\tau(n^2) = (2m_1+1)(2m_2+1)\cdots(2m_t+1)$. Звідси випливає, що $\tau(n^2)$ є обов'язково непарним, тому умову задачі можуть задовольняти лише непарні k. Тепер ми доведемо, що такими є всі непарні числа. Для цього досить показати, що

$$k = \frac{2m_1+1}{m_1+1} \cdot \frac{2m_2+1}{m_2+1} \cdots \frac{2m_t+1}{m_t+1}$$

для деяких натуральних чисел $m_1, m_2, \ldots, m_t$.

Ми використаємо індукцію по k. Доведемо твердження: якщо число x задовольняє умову, то таким буде і $2^m x - 1$ для всіх $m \geq 1$. Нехай ℓ є таким, що $\frac{\tau(\ell^2)}{\tau(\ell)} = x$. Для $m = 1$ візьмемо $n = p^{x-1}\ell$, де p — просте число, що не

є дільником ℓ. Тоді $\dfrac{\tau(n^2)}{\tau(n)} = \dfrac{2x-1}{x} \cdot x = 2x-1$. Для $m > 1$ візьмемо

$$n = p_1^{2^{m-1}3x-2} p_2^{2^{m-2}3^2x-2} \cdots p_{m-1}^{2\cdot 3^{m-1}x-2} p_m^{3^m x-1} \ell,$$

де $p_1, p_2, \ldots, p_m$ — довільні прості числа, на які не ділиться ℓ. В цьому випадку $\frac{\tau(n^2)}{\tau(n)} = \frac{2^m 3x-3}{2^{m-1}3x-1} \cdot \frac{2^{m-1}3^2x-3}{2^{m-2}3^2x-1} \cdots \frac{2^2 3^{m-1}x-3}{2\cdot 3^{m-1}x-1} \cdot \frac{2\cdot 3^{m-1}x-1}{3^{m-1}x} \cdot x = 2^m x - 1$. Наше твердження доведено.

Тепер покажемо, що кожне непарне число задовольняє умову задачі. Число 1 є таким, оскільки $\dfrac{\tau(1^2)}{\tau(1)} = 1$. Для довільного непарного числа $k > 1$ ми можемо записати $k+1 = 2^m x$, де $x < k$ — непарне. Оскільки число x задовольняє умову, таким буде і $k = 2^m x - 1$.

31. $n \in \{8p, 12p\}$. Нехай d є дільником n. Очевидно, що коли d не ділиться на p, то d також є дільником $\tau(n)$. В потилежному випадку $\frac{d}{p}$ є дільником $\tau(n)$. Тепер легко отримати, що $\tau(n) \leqslant 2\tau(\tau(n))$. Позначимо $\tau(n) = b$. Оскільки b не може ділитися на числа $c > \frac{b}{2}$, за єдиним випадком, коли $c = b$, то з нерівності $\tau(b) \geqslant \frac{b}{2}$ слідує, що b ділиться на всі числа, які менші $\frac{b}{2}$, крім, може бути, одного. Звідси отримуємо, що $b \in \{12, 8, 6, 4, 3, 2\}$ і $n = pb$. Залишається перебрати всі числа виду pb. **32.** Число n повинно бути квадратом натурального числа.

§ 1.6. Скінченні ланцюгові дроби.

1. а) Так; б) ні(остання цифра 1); в) ні(третя неповна частка не може бути від'ємною); г) так. **2.** [1;1,1,4,2]. Розкладіть дріб $\frac{14}{9}$ в ланцюговий. **3.** 1. **4.** а) Так, наприклад, для числа $\frac{105}{38}$; б) ні; в) ні; г) ні. **5.** а) Так, наприклад, для числа $\frac{105}{38}$; б) ні; в) ні; г) ні. **6.** $\frac{3}{11}$ з недостачею; $\frac{45}{44}$ з надвишком; $\frac{1}{44}$ з недостачею; 0. **7.** Якщо n парне, то $x < y$; якщо n непарне, то $x > y$.

8. а) $[0;1,1,1,1,1,1,2,6]$, $\frac{P_k}{Q_k}: 0, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \frac{8}{13}, \frac{21}{34}, \frac{134}{217}$;

б) $[1;2,2,2,2,5,3]$, $\frac{P_k}{Q_k}: 1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{222}{157}, \frac{707}{500}$;

в) $[-1;2,2,1,1,6,2]$, $\frac{P_k}{Q_k}: -1, -\frac{1}{2}, -\frac{3}{5}, -\frac{4}{7}, -\frac{7}{12}, -\frac{46}{79}, -\frac{99}{170}$;

г) $[-2;2,1,3,1,1,4,3]$, $\frac{P_k}{Q_k}: -2, -\frac{3}{2}, -\frac{5}{3}, -\frac{18}{11}, -\frac{23}{14}, -\frac{41}{25}, -\frac{187}{114}, -\frac{602}{367}$;

д) $[-7;1,1,28]$, $\frac{P_k}{Q_k}: -7, -\frac{6}{1}, -\frac{13}{2}, -\frac{370}{57}$;

е) $[0;1,2,3,4,5]$, $\frac{P_k}{Q_k}: 0, 1, \frac{2}{3}, \frac{7}{10}, \frac{30}{43}, \frac{157}{225}$;

є) $[0;2,1,1,1,1,2,6]$, $\frac{P_k}{Q_k}: 0, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{5}{13}, \frac{13}{34}, \frac{83}{217}$;

ж) $[1;1,1,2,1,1,6,2]$, $\frac{P_k}{Q_k}: 1, \frac{2}{1}, \frac{3}{2}, \frac{8}{5}, \frac{11}{7}, \frac{19}{12}, \frac{125}{79}, \frac{269}{170}$.

9. а) $\frac{43}{19}$; б) $\frac{99}{464}$; в) $-2\frac{11}{39}$; г) $-5\frac{159}{215}$; д) $\frac{47}{167}$; е) $\frac{120}{167}$.

10. а) $[1;1,1,13,1,1,1,2]$, $\frac{P_k}{Q_k}: 1, \frac{2}{1}, \frac{3}{2}, \frac{41}{27}, \frac{44}{29}, \frac{81}{56}, \frac{129}{85}, \frac{343}{226}$ та $[0;1,1,1,13,1,1,1,2]$, $\frac{P_k}{Q_k}: 0, 1, \frac{1}{2}, \frac{2}{3}, \frac{27}{41}, \frac{29}{44}, \frac{56}{85}, \frac{85}{129}, \frac{226}{343}$;

б) $[-1;1,1,1,1,1,1,2,6]$, $\frac{P_k}{Q_k}: -\frac{1}{1}, \frac{0}{1}, -\frac{1}{2}, -\frac{1}{3}, -\frac{2}{5}, -\frac{3}{8}, -\frac{5}{13}, -\frac{13}{34}, -\frac{83}{217}$ та $[-3;2,1,1,2,6]$, $\frac{P_k}{Q_k}: -3, -\frac{5}{2}, -\frac{8}{3}, -\frac{13}{5}, -\frac{34}{13}, -\frac{217}{83}$.

11. а) $[1;4,1,4]$; б) $[1,4,1,5]$; в) $[1;4,1,4,1,4]$; г) якщо довжина дробу є парною і рівна $2n$, то в результаті отримаємо ланцюговий дріб довжиною $2n-1$ – $[1;4,1,4,\cdots,1,4,1,5]$; якщо довжина дробу є непарною і рівна $2n+1$, то в результаті отримаємо ланцюговий дріб довжиною $2n+1$ – $[1;4,1,4,\cdots,1,4,1,4]$. **12.** а) $q_0=2$; б) $q_3=2$; в) $q_1=3$; г) $n=3, x_1=2, x_2=3, x_3=4$. **13.** а) $\frac{7}{23}$; б) $\frac{17}{13}$; в) $-\frac{234}{195}$; г) $-\frac{271}{100}$.

14. а) Розв'язків немає; б) $x=9+31t, y=2-12t, t\in\mathbb{Z}$; в) $x=-35+18t, y=45-23t, t\in\mathbb{Z}$; г) $x=75+23t, y=-120-37t, t\in\mathbb{Z}$.

15. а) Розв'язків немає; б) $x=4+42t, y=23t, t\in\mathbb{N}$; в) $x=3, y=5$; г) розв'язків немає. **16.** а) 4 точки - вершини та $X(0,2)$; б) Вершини B і C; в) 2 точки - вершина C і точка $X(6,7)$; г) Ні через жодну точку. **17.** а) $\frac{22}{7}$; б) $\frac{187}{36}$; в) ні; г) $\frac{170}{101}, \frac{69}{41}$. **18.** Можна: $\frac{100}{77}=\frac{8}{11}+\frac{4}{7}$. **19.** Треба взяти 19 дощок шириною 11 см та 7 дощок шириною 13 см. **20.** Перепелів — 9, голубів — 10, півнів — 11. **34.** $x_1=1, x_2=1, x_3=3, \cdots, x_{2001}=2001$. **35.** Оскільки $[0;2,3,\ldots,n]<\frac{1}{2}$, то $1-[0;2,3,\ldots,n]=[0;x_1,x_2,\ldots,x_n]>\frac{1}{2}$ і $x_1=1$. Далі, з рівності $1-\frac{1}{2+[0;3,4,\ldots,n]}=\frac{1}{1+[0;x_2,x_3,\ldots,x_n]}$ отримаємо $[0;x_2,x_3,\ldots,x_n]=\frac{1}{1+[0;3,4,\ldots,n]}=[0;1,3,4,\ldots,n]$. Отже, $x_1=1, x_2=1, x_3=3, \cdots, x_n=n$.

Розділ: Кільця

§ 2.1. Кільце та його найпростіші властивості. Підкільце

1. а) Так; так; б) так; так; в) так; так; г) не кільце; д) так; так; е) так; не містить одиниці; є) так; так. **2.** а) Ні; б) ні; в) так; г) ні. **3.** $\{a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}\}$. **4.** 2,4, 6. **5.** Множини остач від ділення на 3 та на 5. **6.** а) $\mathbb{C}, \mathbb{R}; \mathbb{Z}[x]; \mathbb{C}[x]$; б) $M_2(\mathbb{Z}), M_3(\mathbb{R})$; в) множини остач від ділення на 4 та 6; г) множини остач від ділення на 5 та 7; д) $M_2(\mathbb{Z}), M_3(\mathbb{R})$; е) $2\mathbb{Z}, 3\mathbb{R}$; є) $5M_2(\mathbb{Z}), 7M_3(\mathbb{Z})$; ж) $M_2(\mathbb{Z}_2), M_3(\mathbb{Z}_2)$. **7.** а) Це пари протилежних чисел; б) це числа виду $z, -z, iz, -iz$, де $z\in\mathbb{C}$.

8. в) 1, -1; д) кожний ненульовий елемент; е) $\pm(\frac{1+\sqrt{3}}{2})^n, n\in\{0,1,2\}$. **9.** Асоційованими є пари чисел $(a+bi,-b+ai), (a+bi,-a-bi), (a+bi,b-ai)$.

10. а) Ні; б) поле; в) некомутативне кільце без одиниці; г) поле; д) некомутативне кільце без одиниці; е) некомутативне кільце без одиниці; є) комутативне кільце з одиницею; дільниками одиниці є матриці $\begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}$;

дільниками нуля є матриці $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ і $\begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix}$, де $a, b \neq 0$; ж) комутативне кільце з одиницею; дільниками одиниці є матриці $\begin{pmatrix} \pm 1 & \pm b \\ 0 & \pm 1 \end{pmatrix}$; дільниками нуля є матриці $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, де $b \neq 0$.

11. а) Так; комутативне; одиницею є функція $f(x) = 1$; дільниками одиниці є всі функції, які на відрізку $[a, b]$ не приймають нульових значень; дільниками нуля є всі функції, які на відрізку $[a, b]$ приймають хоча б одне нульове значення; б) ні; в),г) – так; комутативне; одиницею є функція $f(x) = 1$; дільниками одиниці є всі функції, які на відрізку $[a, b]$ не приймають нульових значень; дільниками нуля є всі функції, які на відрізку $[a, b]$ приймають хоча б одне нульове значення; д),е) – так; комутативне; одиницею є функція $f(x) = 1$; дільниками одиниці є всі многочлени нульового степеня; дільників нуля немає.

12. а) Не кільце; б) комутативне кільце з одиницею $(1, 0)$; дільниками одиниці є $(1, 0), (-1, 0)$; дільниками нуля є пари виду $(a, a), (a, -a)$, де $a \neq 0$; в) комутативне кільце з одиницею $(1, 1)$; дільниками одиниці є $(\pm 1, \pm 1)$; дільниками нуля є пари виду $(a, 0), (, b)$, де $a, b \neq 0$; г) комутативне кільце з одиницею $(1, 0)$; дільниками одиниці є $(1, 0), (-1, 0)$; дільників нуля немає. **13.** а) Ні; б) ні; в) так; г) так.

14. а) Обидва рівняння не мають розв'язку; б) перше рівняння розв'язків не має, а друге - має безліч розв'язків, які задаються формулою $Y = \begin{pmatrix} 4 - 2a & a \\ 6 - 2b & b \end{pmatrix}$, де $a, b \in \mathbb{R}$; в) $X = \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, Y = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} \\ -1 & 1 \end{pmatrix}$; г) Обидва рівняння мають безліч розв'язків, які задаються формулами: $X = \begin{pmatrix} 4 - a & 4 - b \\ a & b \end{pmatrix}$, $Y = \begin{pmatrix} 4 - 2a & a \\ 8 - 2b & b \end{pmatrix}$, де $a, b \in \mathbb{R}$. **15.** Підкільця мають вид $m\mathbb{Z}$, де $m \in \mathbb{N}$.

§ 2.2. Область цілісності та поле часток. Подільність в області цілісності

1. а) 0; б) 0. **2.** 8. **3.** Такого числового кільця не існує. **4.** Ні. **5.** Ні, $\mathbb{Q}[i]$. **6.** В кільці $\mathbb{Z}[i\sqrt{2}]$ простими є числа $\pm i\sqrt{2}$, а $3 = (1 - i\sqrt{2})(1 + i\sqrt{2}), 2 = i\sqrt{2}(-i\sqrt{2})$ – складені; в кільцях $\mathbb{Q}$ і $\mathbb{C}$ простих елементів немає.

7. Не завжди; кожний простий елемент в L є простим в K. **8.** Так: $13 = (3 - 2i)(3 + 2i)$ і обидва числа не є дільниками одиниці. **9.** Просте.

10. а) Так; нулем є -1, а одиницею – 0; б) так; нулем є -5, а одиницею – -4. **11.** Обидва поля часток рівні $\mathbb{Q}[i\sqrt{3}]$. Покажіть спочатку, що

$\mathbb{Z}[-\frac{1}{2}+\frac{i\sqrt{3}}{2}]=\{\frac{a+bi\sqrt{3}}{2}|a,b\in\mathbb{Z},(a-b)\vdots 2\}$. **12.** $\{\pm 2,\pm 3,\pm(1\pm i\sqrt{5})\}$. **13.** Число 2 є простим в кільці $\mathbb{Z}[i\sqrt{3}]$ і складеним в $\mathbb{Z}[i]: 2=(1-i)(1+i)$.

14. а) $\{\pm 1,\pm 2,\pm 4,\pm(1\pm i\sqrt{3})\}$; б) $\{\pm 1,\pm 2,\pm(1\pm i\sqrt{3})\}$; в) не існує (серед всіх спільних дільників немає такого, який ділиться на всі інші); г) $4=2\cdot 2=(1-i\sqrt{3})(1+i\sqrt{3})$. **15.** а) $2=2^{\frac{1}{2}}2^{\frac{1}{2}}=2^{\frac{1}{4}}2^{\frac{1}{4}}2^{\frac{1}{4}}2^{\frac{1}{4}}=\ldots$; б) $5=5^{\frac{1}{2}}5^{\frac{1}{2}}=5^{\frac{1}{4}}5^{\frac{1}{4}}5^{\frac{1}{4}}5^{\frac{1}{4}}=\ldots$; в) $6=6^{\frac{1}{2}}6^{\frac{1}{2}}=6^{\frac{1}{4}}6^{\frac{1}{4}}6^{\frac{1}{4}}6^{\frac{1}{4}}=\ldots$; г) $m=m^{\frac{1}{2}}m^{\frac{1}{2}}=m^{\frac{1}{4}}m^{\frac{1}{4}}m^{\frac{1}{4}}m^{\frac{1}{4}}=\ldots$.
16. $6=2\cdot 3=(1-i\sqrt{5})(1+i\sqrt{5})$; $18=2\cdot 3^2=(1-i\sqrt{17})(1+i\sqrt{17})$.
17. $2,\frac{2}{3},\frac{2}{5}$.

§ 2.3. Ідеали кільця. Конгруенції за ідеалом та фактор-кільце

1. Тривіальні ідеали є ідеалами; $U_1=\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}|a,b\in\mathbb{R}\right\}$ – лівий ідеал та $U_2=\left\{\begin{pmatrix} a & 0\\ b & 0\end{pmatrix}|a,b\in\mathbb{R}\right\}$ – правий ідеал в кільці $M(2,\mathbb{R})$.

2. а) Так є лівим і правим ідеалом; б) не є ніяким ідеалом; в) не є ніяким ідеалом; г) лівий, але не правий ідеал; д) правий, але не лівий ідеал; е) не є ніяким ідеалом. **3.** $5-3i\in(3+5i),(5-3i)=(3+5i)$. **4.** Рівність виконується при умові, що число n при діленні на 6 дає остачу 5.

5. $-3+5i\equiv 25+3i\equiv 1+i\equiv 1-i\pmod{(2)}, 2+i\equiv -2+3i\pmod{(2)}$.
6. а) Нескінченну множину; б) 1; в) 4; г) 6.

8. а) $(3,7)=\mathbb{Z}$; б) $(4,6)=(2)$; в)$(6,10)=(2)$; г) $(2,4,6)=(2)$; д)$(3,5,7)=\mathbb{Z}$; е)$(3,-6,9)=(3)$.

9. а) (15); б) (15); в) $\mathbb{Z}$; г) (8); д) (32); е) (4); є) (24); ж) (48); з) (2).

10. Упорядковані множини $(A;\subseteq)$ і $(B;\vdots)$ є ізоморфними при відображенні $f: B\to A$ такому, що $f(n)=n\mathbb{Z}$. **11.** а) Ні; б) ні; в) ні; г) так; д) так; е) так. **12.** В кільці $\mathbb{Z}_4$ дільником нуля є клас $\bar{2}$; в кільці $\mathbb{Z}_7$ дільників нуля немає. Мультиплікативні групи такі: $\mathbb{Z}_4^*=\{\bar{1},\bar{3}\}$ і $\mathbb{Z}_7^*=\{\bar{1},\{\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$.
13. а) $x=\bar{4}$; б) $x=\bar{5}$; в) $x=\bar{4}$; г) $x_1=\bar{0}$, $x_2=\bar{3}$; д) $\varnothing$; е) $x=\bar{0}$; є) $\varnothing$; ж) $\varnothing$. **14.** $(\mathbb{Z}[i]/(3))^*=\{\overline{1},\overline{2},\overline{1+i},\overline{1+2i},\overline{2+2i},\overline{i},\overline{2i},\overline{2+i},\}$. **15.** 25; не поле, оскільки класи $1-2i+(5)$ і $1+2i+(5)$ є дільниками нуля.

16. а) Дільниками нуля є $\overline{2},\overline{2i},\overline{1+i},\overline{2+2i},\overline{3+i},\overline{3+3i}$; оберненим елементом до $\overline{i}$ є $\overline{3i}$, до $\overline{1-2i}$ є $\overline{3+2i}$, до $2i$ оберненого елемента немає; б) Дільниками нуля є $\overline{2},\overline{3},\overline{4},\overline{2i},\overline{3i},\overline{4i},\overline{1+i},\overline{1+3i},\overline{1+5i},\overline{2+2i},\overline{2+4i},\overline{3+i},\overline{3+3i},\overline{3+5i},\overline{4+2i},\overline{4+4i},\overline{5+i},\overline{5+3i},\overline{5+5i}$. оберненим елементом до $\overline{2+5i}$ є $\overline{2+3i}$, до $\overline{4+i}$ є $\overline{2+i}$.

17. а) тривіальні та $(\bar{2}),(\bar{3})$; б) тривіальні та $(\bar{2}),(\bar{4}),(\bar{8})$.

§ 2.4. Гомоморфізми та ізоморфізми кілець

1. Кожному цілому числу n слід поставити у відповідність його остачу від ділення на 3. **2.** Ні. **3.** Так. Якщо $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ і $\mathbb{Z}_2 = \{\breve{0}, \breve{1}\}$, то покладемо $f(\bar{0}) = f(\bar{2}) = \breve{0}, f(\bar{1}) = f(\bar{3}) = \breve{1}$. **5.** а) Ні; б) так; в) ні; г) ні.

6. $f(a+bi) = a+bi$ і $f(a+bi) = a-bi$. **7.** $f(a+b\sqrt{2}) = a-b\sqrt{2}$ і $f(a+b\sqrt{2}) = a+b\sqrt{2}$. **12.** Можна. Операції $\star$ та $\circ$ можна задати, наприклад, так:

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

$\circ$	1	2	3
1	1	1	1
2	1	2	3
3	1	3	2

15. а) $f(a+b\sqrt{2}) = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$;

б) $f(a+bi) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$;

в) $f(a+bi\sqrt{3}) = \left\{ \begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$;

г) $f(3a+3bi) = \left\{ \begin{pmatrix} 3a & -3b \\ 3b & 3a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$.

16. а) Врахуйте, що кільце $M(2, \mathbb{R})$ є некомутативним;

17. Задайте, для прикладу, гомоморфізм кільця $\mathbb{Z}$ на кільце $\mathbb{Z}_4$.

19. $\mathrm{Ker}\varphi = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in \mathbb{Z} \right\}$. **20.** $\mathrm{Ker}\varphi = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} \middle| b \in \mathbb{Q} \right\}$.

21. $\mathrm{Ker}\varphi$ є множина всіх функцій f з кільця $C_{[-1,2]}$ таких, що $f(1) = 0$.

§ 2.5. Факторіальні кільця. Кільця головних ідеалів та евклідові кільця

1. а) У всіх областях цілісності; наприклад, в $\mathbb{Z}[\sqrt{2}]$; б) в кільці чисел виду $\sum_{i=1}^{n} a_i 2_i^r$, де $a_i \in \mathbb{Z}, r_i \in \mathbb{Q}$ число 2 не можна розкласти у добуток простих елементів; в) г) в кільці $\mathbb{Z}$; д) е) в кільці $\mathbb{Z}$.

2. Є евклідовим кільцем. **3.** а) Ні; б) так; в) так; г) ні. **4.** $(3, 1+i\sqrt{5}) = 1, [3, 1+i\sqrt{5}] = 3+3i\sqrt{5}$. **6.** Так.

7. а) Так; б) так; в) Розглянемо відображення $f : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}$, задане формулою $\varphi_1(a+b\sqrt{3}) = |a^2-3b^2|$. Легко перевірити, що $\varphi_1((a+b\sqrt{3})(c+d\sqrt{3})) = |a^2-3b^2||c^2-3d^2| = \varphi_1(a+b\sqrt{3})\varphi_1(c+d\sqrt{3})$ та обмеження φ_1 на $\mathbb{Z}[\sqrt{3}]$ співпадає з φ. Візьмемо $a+b\sqrt{3}, c+d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ і $c+d\sqrt{3} \neq 0$. Очевидно, що $\frac{a+b\sqrt{3}}{c+d\sqrt{3}} = u+v\sqrt{3}$, де $u, v \in \mathbb{Q}$. Розглянемо числові відрізки $[u-\frac{1}{2}; u+\frac{1}{2}]$ та $[v-\frac{1}{2}; v+\frac{1}{2}]$. Кожному з них належить хоча б одне ціле число x_0 та y_0 відповідно. Позначимо $q = x_0 + y_0\sqrt{3}$ і $r = (a+b\sqrt{3}) - (c+d\sqrt{3})q$.

Тоді $a+b\sqrt{3}=(c+d\sqrt{3})q-r$, причому $q,r\in\mathbb{Z}[\sqrt{3}]$. Якщо $r\neq 0$, то $\varphi(r)=\varphi_1(r)=\varphi_1((a+b\sqrt{3})-(c+d\sqrt{3})q)=\varphi_1((\frac{a+b\sqrt{3}}{c+d\sqrt{3}}-q)(c+d\sqrt{3}))=\varphi_1((u+v\sqrt{3})-(x_0+y_0\sqrt{3})(c+d\sqrt{3}))=\varphi_1((u-x_0)+(v-y_0)\sqrt{3})\varphi_1(c+d\sqrt{3})=|(u-x_0)^2-3(v-y_0)^2|\varphi(c+d\sqrt{3})$. Оскільки $(x_0-u)^2\leqslant\frac{1}{4}$ і $(y_0-v)^2\leqslant\frac{1}{4}$ та модуль різниці двох різних чисел менший суми модулів зменшуваного і від'ємника, то $|(u-x_0)^2-3(v-y_0)^2|<|(u-x_0)^2|+|3(v-y_0)^2|\leqslant\frac{1}{4}+3\frac{1}{4}=1$. Отже, $\varphi(r)<\varphi(c+d\sqrt{3})$ і кільце $\mathbb{Z}[\sqrt{3}]$ є евклідовим. г) ні.

8. У всіх випадках є кільцем з дільниками нуля. **9.** а)1; б) 10; в) НСД(m,n,k,l,s,t); г) НСК((m,n,k),(l,s,t)). **10.** а) $3-2i$ та $75-50i$; б) $1+2i$ та $7-i$; в) $3+i$ та $-5+15i$; г) $1+i$ та $61+7i$. **11.** а) $(2+i)(2-i)$; б) $(1-i)(2+i)(2-i)$; в) $3^2(1+i)^2(2+i)^2(2-i)$; г) $(1+i)(2-i)$; д) $7+8i$; е) $(4+5i)(4-5i)$.

16. Прикладом такого ідеалу є множина всіх многочленів з парним вільним членом.

Розділ: Конгруенції

§ 3.1. Конгруенції в кільці цілих чисел та їх властивості

1. а) $81\equiv 3 \pmod{13}$; б) $n\equiv 1 \pmod 2$; в)$n\equiv 5 \pmod 7$; г) $(n^3-8)\equiv 0 \pmod 3$. **2.** а) Остача при діленні числа 137 на 11 дорівнює 5; б) Числа 256 і 6 є парними; в) Остачі при діленні чисел $\overline{a_2a_1a_0}_{10}$ та $a_2+a_1+a_0$ на 3 однакові; г) Число 7^{29} не можна подати у вигляді $2+5t$, де $t\in\mathbb{Z}$. **3.** а) $21\equiv 33 \pmod 4$; б) $220\equiv 283 \pmod 7, 231\equiv 119 \pmod 7, 231\equiv 301 \pmod 7, 119\equiv 301 \pmod 7$; в) таких пар немає; г) $725\equiv 190 \pmod{15}, 315\equiv 465 \pmod{15}$. **4.** Ні. **5.** а) $x+3\equiv 0 \pmod 5$; б) $2x+3\equiv 2 \pmod{11}$; в) $4x-1\equiv 3 \pmod{13}$;г) $2x-1\equiv 1 \pmod 2$. **6.** а) 1; б) 2; в) 3; г) 1; д) 12; е) 30. **7.** а) 7; б) 6; в) 5; г) 6; д) 3; е) 4. **8.** а) 88; б) 67; в) 09; г) 01; д) 99; е) 25. **9.** 6. **10.** $n=2k, k\in\mathbb{Z}$. **11.** 5.

12. Очевидно, що $x=y=1$ є розв'язком даного рівняння. Якщо $x<0, y>0$ є розв'язком даного рівняння, то повинна мати місце цілочислова рівність $1+2^{-x}=2^{-x}3^y$. Проте тут $2^{-x}3^y\equiv 0 \pmod 2$, $1+2^{-x}\equiv 1 \pmod 2$, що неможливо. Аналогічно не можуть бути розв'язками $x<0, y<0$ та $x>0, y<0$. Якщо $x>1$ є розв'язком даного рівняння, то $2^x\equiv 0 \pmod 4$ і $2^x+1\equiv 1 \pmod 4$. При цьому число y не може бути непарним. Дійсно, якби $y=2k+1$, то $3^y=3^{2k+1}=(3^2)^k\cdot 3\equiv 3 \pmod 4$, що протирічить попередньому. Нехай $y=2k$. Тоді $2^x=3^{2k}-1=(3^k-1)(3^k+1)$. Остання ж рівність виконується у єдиному випадку, коли $k=1, x=3$. Таким чином, дане рівняння має два розв'язки $x=y=1$ і $x=3, y=2$.

13. а) Використайте формулу бінома Ньютона. б) Врахуйте, що $p-k \equiv -k \pmod p$ для всіх $0<k<p$. г) д) Доведіть спочатку, що $p^{p+2}+(p+2)^p \equiv 0 \pmod 2$ і $p^{p+2}+(p+2)^p \equiv 0 \pmod{(p+1)}$. е) Застосуйте метод від супротивного.

14. У всіх задачах застосуйте властивості конгренцій. Наприклад, б): за умовою $a-5b \equiv 0 \pmod{17}$. Помноживши обидві частини цієї конгруенції на 2, одержимо $2a-10b \equiv 0 \pmod{17}$. Тепер додамо до лівої частини число $17b$. Отримуємо $2a+7b \equiv 0 \pmod{17}$, тобто шуканий висновок. Тут обернене твердження також істинне.

17. Обидві частини рівності $a=b+pt$ піднести до p-го степеня і застосувати формулу бінома Ньютона. **18.** З того, що $(3a-b) \vdots 11$ слідує $(36a-45b) \vdots 11$ і $(4a-5b) \vdots 11$. **19.** Застосуйте метод математичної індукції. **20.** а) $3^x \equiv (-1)^x \pmod 4$, $9^y \equiv 1^y \pmod 4$, тобто $3^x+9^y \equiv (-1)^x+1 \pmod 4$. В той же час $17^z \equiv 1 \pmod 4$. Оскільки $(-1)^x+1 \not\equiv 1 \pmod 4$, то дане рівняння не має розв'язків у натуральних числах. б) – г) доводяться аналогічно. **21.** Починаючи з $n=2$ числа закінчуються цифрою 7. **23.** Перших чисел більше. Врахуйте, що $10xy-x^2-y^2=2(x+y)^2-3(x-y)^2=2u^2-3v^2$ та покажіть, що рівняння $10xy-x^2-y^2=5$ не має цілих розв'язків.

§ 3.2. Класи лишків. Повна і зведена система лишків. Теореми Ейлера і Ферма

1. а) 3, -2; б) 7, -7; в) 5; г) 55, -1; д) 17; е) 59, -59. **2.** а) Ні; б) так; в) так; г) ні; д) так; е) ні. **3.** а) Ні; б) так; в) так; г) ні; д) так; е) так.

4. а) $K_0^{(2)}=K_0^{()6} \cup K_2^{(6)} \cup K_4^{(6)}$, $K_1^{(2)}=K_1^{(6)} \cup K_3^{(6)} \cup K_5^{(6)}$; б) $K_0^{(4)}=K_0^{(8)} \cup K_4^{(8)}$, $K_1^{(4)}=K_1^{(8)} \cup K_5^{(8)}$, $K_2^{(4)}=K_2^{(8)} \cup K_6^{(8)}$, $K_3^{(4)}=K_3^{(8)} \cup K_7^{(8)}$; в) $K_0^{(6)} \cup K_2^{(6)} \cup K_4^{(6)}=K_0^{(10)} \cup K_2^{(10)} \cup K_4^{(10)} \cup K_6^{(10)} \cup K_8^{(10)}$; г) $K_i^{(3)} \cap K_j^{(8)} \neq \varnothing$ для будь-яких $0 \leqslant i \leqslant 2, 0 \leqslant j \leqslant 7$ д) $K_i^{(5)} \cap K_j^{(9)} \neq \varnothing$ для будь-яких $0 \leqslant i \leqslant 4, 0 \leqslant j \leqslant 8$; е) кожний клас лишків за модулем 7 є об'єднанням двох класів за модулем 14.

5. а) Ні; б) так; в) ні; г) так; д) ні; е) так. **6.** а) Так; б) ні; в) ні; г) так; д) ні; е) так. **7.** а) Ні; б) так; в) ні; г) так. **8.** У всіх кільцях є дільники нуля. **16.** а) $\mathbb{Z}_6^*=\{\bar 1, \bar 5\}$; б) $\mathbb{Z}_{15}^*=\{\bar 1, \bar 2, \bar 4, \bar 7, \bar 8, \overline{11}, \overline{13}, \overline{14}\}$; в) $\mathbb{Z}_{20}^*=\{\bar 1, \bar 3, \bar 7, \bar 9, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$; г) $\mathbb{Z}_{23}^*=\{\bar 1, \bar 2, \cdots, \overline{22}\}$. **17.** а) Група не циклічна; б) група циклічна з твірними елементами $\overline 2, \overline 5$; в) група циклічна з твірними елементами $\overline 3, \overline 7$; г) група не циклічна; **18.** а) $\bar x=\bar 6$; б) розв'язку немає; в) $\bar x=\bar 8$; г) розв'язку немає. **19.** а) $\bar x=\bar 10$; б) $\bar x=\bar 18$; в) $\bar x=\bar 19$; г) $\bar x=\bar 13$. **20.** а) 1; б)

5; в) 1; г) 1. **21.** а) 13; б) 14; в) 65; г) 49. **22.** а) 2; б) 5; в) 2; г) 7. **23.** а) 67; б) 01; в) 61; г) 84. **24.** а) 0, якщо $a \vdots 5$ та 1, якщо $a \not\vdots 5$; б) $\frac{m+1}{2}$; в) $\frac{m+1}{2}$, якщо $m = 4k-1$; г) 1. **25.** а) 4; б) 6; в) 15; г) 20. **29.** Числа $m-a_1, m-a_2, \cdots, m-a_{\varphi(m)}$ також утворюють ту ж саму зведену систему лишків. Склавши числа з обох систем, отримаємо шукану формулу.

34. За теоремою Ферма, для кожного цілого a мають місце конгруенції: $a^2 \equiv 1 \pmod 3$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$. Тоді $a^{80} \equiv 1 \pmod 3$, $a^{80} \equiv 1 \pmod{11}$, $a^{80} \equiv 1 \pmod{17}$. Тому $a^{80} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$. Отже, $a^{560} \equiv 1 \pmod{561}$ і $a^{561} \equiv a \pmod{561}$.

38. За теоремою Ферма, $5^p \equiv 5 \pmod p$, $2^p \equiv 2 \pmod p$. Тому $5^p - 2^p \equiv 3 \pmod p$. Отже, з $5^p - 2^p \equiv 0 \pmod p$ слідує $p = 3$. Нехай прості числа p і q задовольняють умову задачі. Якщо $5^p - 2^p \equiv 0 \pmod{pq}$, то $p = 3$ і $q = 3$ або $p = 3$ і $q = 13$(зауважимо, що $5^3 - 2^3 = 3 \cdot 3 \cdot 13$); якщо $5^q - 2^q \equiv 0 \pmod{pq}$, то $q = 3$ і $p = 3$ або $q = 3$ і $p = 13$; якщо $5^p - 2^p \equiv 0 \pmod{pq}$ та $5^q - 2^q \equiv 0 \pmod q$, то $p = q = 3$. Нарешті, нехай $5^p - 2^p \equiv 0 \pmod q$ та $5^q - 2^q \equiv 0 \pmod p$. При $p = q$ отримуємо, що $p = q = 3$. Далі, очевидно, можна вважати, що $p > q > 3$. Оскільки числа p і q взаємно прості, то існують такі $a, b \in \mathbb{N}$, що $ap - b(q-1) = 1$. При умові $5^p - 2^p \equiv 0 \pmod q$ маємо: $q \neq 2$ і $q \neq 5$, а тому $5^{q-1} \equiv 1 \pmod q$ та $2^{q-1} \equiv 1 \pmod q$ і $5^{q-1} \equiv 2^{q-1} \pmod q$. Оскільки $5^p \equiv 2^p \pmod q$, то $5^{ap} \equiv 2^{ap} \pmod q$, тобто $5^{b(q-1)+1} \equiv 2^{b(q-1)+1} \pmod q$. Але $5^{b(q-1)+1} \equiv 5 \pmod q$ і $2^{b(q-1)+1} \equiv 2 \pmod q$. Звідки $5 \equiv 2 \pmod q$, що неможливо для $q > 3$. Таким чином, шуканими парами є: $p = q = 3; p = 3, q = 13; q = 3, p = 13$.

§ 3.3. Конгруенції першого степеня з одним невідомим

1. а) Ні; б) так; в) не завжди; г) так. **2.** а) Єдиний; б) ні одного; в) 3; г) 7. **5.** а) $x \equiv 2 \pmod 5$; б) $x \equiv 5 \pmod 7$; в) $x \equiv 4, 9 \pmod{10}$; г) $x \equiv 2, 5, 8, 11 \pmod{12}$. **6.** а) $x \equiv 3, 10 \pmod{14}$; б) $x \equiv 6 \pmod{23}$; в) $x \equiv 11 \pmod{41}$; г) $x \equiv 38 \pmod{51}$.

7. а) $x \equiv 3 \pmod{12}$; б) $x \equiv 13 \pmod{34}$; в) розв'язків немає; г) $x \equiv 3 \pmod{22}$.

8. а) $x \equiv 28 \pmod{119}$; б) розв'язків немає; в) $x \equiv 73 \pmod{177}$; г) $x \equiv 51, 130, 209, 288, 367 \pmod{395}$.

9. а) $x = K_5^{(26)}$; б) $x = K_{13}^{(17)}$; в) $x = K_{100}^{(107)}$; г) $x = K_{21}^{(30)}$.

10. а) $x = 2 + 3t, y = -2t, t \in \mathbb{Z}$; б) $x = 2 + 3t, y = 2 + 4t, t \in \mathbb{Z}$; в) $x = 3 + 4t, y = 1 - 3t, t \in \mathbb{Z}$; г) $x = 3 + 4t, y = -3 - 5t, t \in \mathbb{Z}$.

11. а) розв'язків немає; б) $x = -1 + 16t, y = -3 + 17t, t \in \mathbb{N}$; в) $x = 1 + 4t, y = 2 + 13t, t \in \mathbb{N} \cup \{0\}$; г) $x = 1 - 3t, y = 2 - 5t$, де t – недодатнє.

12. а) $x \equiv 12 \pmod{35}$; б) $x \equiv 170b_1 + 52b_2 \pmod{221}$; в) $x \equiv 1 \pmod{5}, y \equiv 2 \pmod{5}$; г) розв'язків немає.

13. а) $x \equiv 59 \pmod{60}$; б) розв'язків немає; в) $x \equiv 17 \pmod{90}$; г) $x \equiv 4 \pmod{105}$.

14. а) $a \equiv 5 \pmod{6}$; б) $a \equiv 0 \pmod{4}$; в) $a \equiv 1 \pmod{6}$; г) $a \equiv 1 \pmod{7}$. **15.** а) 2; б) 19; в) 7; г) 8. **16.** а), б) через 12 точок. **17.** 11 червня. **18.** 2 і 39. **19.** 301. **20.** $x \equiv 34 \pmod{35}$; приписати можна 34 або 69. **21.** Такого числа не існує. **22.** $x \equiv 200 \pmod{440}$; приписати можна 200 або 640. **23.** 188.

§ 3.4. Конгруенції вищих степенів з одним невідомим

4. а) Ні; б) так; в) так; г) так. **6.** а) 3; б) 4; в) 2; г) розв'язків немає. **7.** а) $x \equiv 1, 2, 3, 4, 5, 6 \pmod{7}$; б) $x \equiv 4 \pmod{11}$; в) $x \equiv 7, 9 \pmod{11}$; г) $x \equiv 7, 13 \pmod{23}$. **8.** а) $x \equiv 1, 2, 4, 5 \pmod{6}$; б) $x \equiv 2 \pmod{10}$; в) $x \equiv 2, 5, 11 \pmod{15}$; г) розв'язків немає; д) $x \equiv 0, 14, 20, 34 \pmod{35}$; е) $x \equiv 2, 7, 24, 29 \pmod{55}$. **9.** а) $x \equiv 2, 3 \pmod{25}$; б) $x \equiv 13 \pmod{25}$; в) $x \equiv 17 \pmod{49}$; г) розв'язків немає. **10.** а) $x \equiv 8 \pmod{27}$; б) $x \equiv 22 \pmod{27}$; в) $x \equiv 22, 53 \pmod{64}$; г) $x \equiv 113 \pmod{125}$. **11.** а) Розв'язків немає; б) $x \equiv 8, 44, 58 \pmod{63}$; в) $x \equiv 36, 136 \pmod{175}$; г) $x \equiv 42 \pmod{45}$. **12.** а) 6; б) 8; в) 9; г) 9. **13.** а) $f(x) = x^3 - 2x + 1 \equiv (x-1)(x-2)^2 \pmod{5}$; б) $f(x) = 3x^3 + 2x^2 - 2x - 3 \equiv 3(x-1)(x-2)(x-3) \pmod{5}$. **14.** а) $f(x) = 5x^3 + 4x^2 - 8x - 1 \equiv 5(x-1)(x-3)(x-5) \pmod{7}$; б) не розкладається. **15.** а) $f(x) = 6x^3 + 5x^2 - 2x - 9 \equiv 6(x-1)(x-2)(x-9) \pmod{11}$; б) $f(x) = x^4 + x + 4 \equiv (x-2)^2(x-3)(x-4) \pmod{11}$. **16.** $x \equiv 3, 13 \pmod{20}$.

25. $p \equiv 1 \pmod{n}$ і $a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$. **26.** $(a, 7) = (b, 7) = 1$.

§ 3.5. Квадратичні лишки. Символ Лежандра

2. Звести до системи конгруенцій за модулями 4, 5, 9. **3.** а) 9; б) 18. **4.** Для простого непарного p і цілого a такого, що $(a, p) = 1$. **5.** а) 1; б) -1; в) 1; г) -1.

6. а) $x \equiv 2, 3 \pmod{5}$; б) $x \equiv 1 \pmod{7}$; в) розв'язків немає; г) $x \equiv 4, 6 \pmod{11}$. **7.** а) $x \equiv 1, 7 \pmod{10}$; б) $x \equiv 6, 12 \pmod{15}$; в) $x \equiv 12, 13 \pmod{17}$; г) $x \equiv 4, 7 \pmod{23}$; д) $x \equiv 13, 16 \pmod{24}$; е) розв'язків немає. **8.** а) 1, 2, 4; б) 1, 3, 4, 5, 9; в) 1, 3, 4, 9, 10, 12; г) 1, 2, 4, 8, 9, 13, 15, 16; д) 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18; **9.** а) 2; б) 2, 6, 7, 8, 10; в) 2, 5, 6, 7, 8, 11; г) ; д) ; е) 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35. **10.** а) 1; б) 1; в) -1; г) -1; д) 1; е) -1. **11.** а) 2; б) 0; в) 0; г) 0. **12.** а) Так; б) ні; в) ні; г) так. **13.** а) $x = \pm 2 + 5t, y = 2 \pm 16t + 20t^2, t \in \mathbb{Z}$; б) розв'язків немає; в)

$x = 8+11t, y = -1+6t+11t^2, t \in \mathbb{Z}$ або $x = 2+11t, y = -1-6t+11t^2, t \in \mathbb{Z}$; г) $x = 10+13t, y = -1+13t^2, t \in \mathbb{Z}$ або $x = 11-13t, y = -1+13t^2, t \in \mathbb{Z}$.

26. Для $p = 2$ маємо $a_1 \vdots p$, а для $p = 3$ – $a_2 \vdots p$. Нехай $p > 3$. Оскільки $a_n = (n^2+2)(n^2+3)(n^2-6)$, то досить довести, що принаймні одна з конгруенцій $n^2 \equiv -2 \pmod p$, $n^2 \equiv -3 \pmod p$, $n^2 \equiv 6 \pmod p$ має розв'язки. Припускаючи, що $\left(\frac{-2}{p}\right) = -1$ та $\left(\frac{-3}{p}\right) = -1$ отримуємо: $\left(\frac{6}{p}\right) = \left(\frac{-2}{p}\right) \cdot \left(\frac{-3}{p}\right) = 1$.

§ 3.6. Показник числа і класу лишків за модулем. Первісні корені

1. Порядок кожного елемента групи є дільником порядку групи. **2.** Всі, крім 1, мають порядок 2. **3.** $\varepsilon_1, \varepsilon_5$. **4.** $(a, m) = 1$. **5.** а) $-5 \equiv 13 \equiv 1 \pmod 6, 5 \equiv 41 \equiv -1 \pmod 6, P_6(1) = 1, P_6(-1) = 2$; для чисел 2 і 33 показника не існує; б) до одного показника належать 13 та 50 і -4,10 та 45; для числа 119 показника не існує; в) всі числа належать до одного показника; г) всі. **6.** Ні. **7.** 12. **8.** а) 2; б) 8; в) 10; г) 18.

9. а) $P_{11}(1) = 1, P_{11}(10) = 2, P_{11}(3) = P_{11}(4) = P_{11}(5) = P_{11}(9) = 5, P_{11}(2) = P_{11}(6) = P_{11}(7) = P_{11}(8) = 10$;

б) $P_{15}(1) = 1, P_{15}(4) = P_{15}(11) = P_{15}(14) = 2, P_{15}(2) = P_{15}(7) = P_{15}(8) = P_{15}(13) = 4$; для решти класів показника не існує;

в) $P_{19}(1) = 1, P_{19}(18) = 2, P_{19}(7) = P_{19}(11) = 3, P_{19}(8) = P_{19}(12) = 6, P_{19}(4) = P_{19}(5) = P_{19}(6) = P_{19}(9) = P_{19}(16) = P_{19}(17) = 9; P_{19}(2) = P_{19}(3) = P_{19}(10) = P_{19}(13) = P_{19}(14) = P_{19}(15) = 18$;

г) $P_{21}(1) = 1, P_{21}(8) = P_{21}(13) = P_{21}(20) = 2, P_{21}(4) = P_{21}(16) = 3, P_{21}(2) = P_{21}(5) = P_{21}(10) = P_{21}(11) = P_{21}(13) = P_{21}(19) = 6$.

10. а) 12,3,2,1; б) 10,10,2,5; в) 6,2,12, не існує; г) 5,10,2,10.

11. а) 3; б) 6; в) 2; г) 1. **12.** а) не існує; б) 4 – 7, 13, 17, 19; в) 10; г) не існує. **13.** а) 3; б) 5; в) 6; г) 2. **14.** 6,7,11.

15. а) 2,6,7,8; б) 2,3,10,13,14,15; в) 2,3,8,10,11,14,15,18,19,21,26,27; г) не існує.

16. а) $x \in \mathbb{N}$; б) $x = 6n, n \in \mathbb{N}$; в) $x = 20n, n \in \mathbb{N}$; г) $x = 14n, n \in \mathbb{N}$.

17. $x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$. **18.** $x \equiv 108 \pmod{131}$. **19.** 5,6,9,13,22. **20.** а) $b \equiv 1, 4, 7 \pmod 9$; б) $(b, 9) = 1$.

30. Оскільки $2^n \equiv -1 \pmod{3^m}$, то $2^{2n} \equiv 1 \pmod{3^m}$. А тому $2n \vdots P_{3^m}(2)$. $P_{3^m}(2)$ – парне число та $\varphi(3^m) \vdots P_{3^m}(2)$. А тому $2n \vdots P_{3^m}(2)$. $P_{3^m}(2)$ – парне число та $\varphi(3^m) \vdots P_{3^m}(2)$. Але $\varphi(3^m) = 2 \cdot 3^{m-1}$. Звідки дістаємо, що число $P_{3^m}(2)$ має вигляд $2 \cdot 3^t$, де $0 \leqslant t < m$. За індукцією неважко довести (зробіть це!), що канонічний розклад числа $2^{3^t} + 1$ трійка входить з пока-

зником $m+1$. Далі $2^{P_{3^m}(2)} = 2^{2\cdot 3^t} - 1 = (2^{3^t}-1)(2^{3^t}+1) \vdots 3^m, 2^{3^t} - 1 \not\equiv 0 \pmod 3$, і ми бачимо, що $2^{3^t}+1) \vdots 3^m$. Але з цього випливає, що $m \leqslant t+1$. Таким чином, $m = t+1$ та $P_{3^m}(2) = 2\cdot 3^{m-1}$, Отже, $2n \vdots 2\cdot 3^{m-1}$ і $n \vdots 3^{m-1}$.

§ 3.7. Індекси за простим модулем та їх застосування

2. Можна, якщо за цим модулем існує первісний корінь. **3.** Пеший спосіб розв'язування зводиться до виконання дії добування кореня: $5x^{47} = 6$, $x^{47} = \frac{6}{5}$ і $x = \sqrt[47]{1,2}$. Другий спосіб полягає в застосуванні дії логарифмування: рівняння $x^{47} = \frac{6}{5}$ логарифмують при основі, наприклад, 10: $47 \lg x = \lg \frac{6}{5}$. Далі $\lg x = \frac{1}{47} \lg \frac{6}{5}$ і $x = 10^{\frac{1}{47} \lg \frac{6}{5}}$.

4. Дану конгруенцію можна розв'язати методом підстановки ПСЛ або застосуванням теорії індексів. При розв'язуванні другим способом потрібно конгруенцію $5x^{47} \equiv 6 \pmod{11}$ проіндексувати за модулем 11 при основі 2. Отримаємо конгруенцію першого степеня $47 \cdot \operatorname{ind}_2 x \equiv (\operatorname{ind}_2 6 - \operatorname{ind}_2 5) \pmod{10}$. За таблицями індексів маємо $47 \cdot \operatorname{ind}_2 x \equiv 5 \pmod{10}$. Оскільки $(47, 10)$=1, то ця конгруенція має єдиний розв'язок: $7 \cdot \operatorname{ind}_2 x \equiv 5 \pmod{10}$, $21 \cdot \operatorname{ind}_2 x \equiv 15 \pmod{10}$ і $\operatorname{ind}_2 x \equiv 5 \pmod{10}$. За таблицею антиіндексів знаходимо $x \equiv 9 \pmod{11}$. Зауважимо, що основу індексації можна в подальшому не писати, маючи на увазі, що для простоти індексують за найменшим первісним коренем.

5. Так, можна. Дана конгруенція рівносильна системі двох конгруенцій $\begin{cases} 5x^4 - 6 \equiv 0 \pmod 3, \\ 5x^4 - 6 \equiv 0 \pmod 7. \end{cases}$ Тепер кожну конгруенцію за простим модулем 3 і 7 можна розв'язати за допомогою індексів. **6.**

а)

N	0	1	2	3	4	5	6	7	8	9
0		0	3	1	2					

;

б)

N	0	1	2	3	4	5	6	7	8	9
0		0	7	2	8	6	1	3	9	4
1	5									

;

в)

N	0	1	2	3	4	5	6	7	8	9
0		0	5	8	10	9	1	7	3	4
1	2	11	6							

;

г)

N	0	1	2	3	4	5	6	7	8	9	10
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		

.

7. а) $x \equiv 31 \pmod{37}$; б) $x \equiv 30 \pmod{73}$; в) $x \equiv 74 \pmod{79}$; г) $x \equiv 51 \pmod{97}$.

8. а) $x \equiv 10, 43 \pmod{53}$; б) $x \equiv 27, 40 \pmod{67}$; в) $x \equiv 2, 7 \pmod{11}$; г) $x \equiv 3, 31 \pmod{47}$. **9.** а) 4; б) 1; в) 7; г) 0.

10. а) $x \equiv 4, 33 \pmod{37}$; б) розв'язків немає; в) $x \equiv 2, 18, 23, 39 \pmod{41}$; г) $x \equiv 17 \pmod{67}$; д) $x \equiv 10, 13 \pmod{23}$; е) $x \equiv 17 \pmod{73}$; є) розв'язків немає; ж) $x \equiv 3, 24, 46 \pmod{73}$.

11. а) $x \equiv 10 \pmod{29}$; б) $x \equiv 24 \pmod{37}$; в) $x \equiv 14 \pmod{41}$; г) $x \equiv 47 \pmod{71}$.

12. а) 16; б) 29; в) 17; г) не існує.

13. а) Розв'язків немає; б) $x \equiv 27 \pmod{30}$; в) $x \equiv 11 \pmod{28}$; г) $x \equiv 27 \pmod{30}$.

14. а) $x \equiv 38 \pmod{66}$; б) $x \equiv 3 \pmod{72}$; в) $x \equiv 3, 16, 29, 42, 55, 68 \pmod{78}$; г) $x \equiv 5, 46 \pmod{82}$.

15. а) 11; б) 7; в) 5; г) 13. **7.16.** а) Ні; б) так; в) ні; г) так.

17. а) 7;37; б) 3; 5; 12; 18; 19; 20; 26; 28; 29; 30; 33; 34; в) 3; 27; 41; г) 2; 6; 7; 10; 17; 18; 26; 30; 31; 35; 43; 44; 51; 54; 55; 59.

§ 3.8. Арифметичні застосування конгруенцій

3. а) $q \in \{11, 33, 99\}$; б) $q \in \{27, 37, 111, 333, 999\}$. **4.** а) $q \in \{22, 55, 66, 165, 198, 495\}$; б) $q \in \{12, 36, 60, 125, 150, 180, 225, 300, 450, 900\}$. **5.** а) Ні; б) так; в) так; г) так. **6.** а) $3^3 \cdot 5^2 \cdot 11^2 \cdot 2999$; б) $29 \cdot 31 \cdot 101$; в) $17^2 \cdot 19 \cdot 557$; г) $7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 101 \cdot 137 \cdot 257$. **7.** а) $x = 8, y = 0, z = 6$; б) $x = 1, y = 2$; в) $x = 1, y = 5$ або $x = 6, y = 0$; г) $x = 2, y = 8$. **8.** а) 3; б) 53; в) 19; г) 48. **11.** $g = 21$. **12.** а) 16; б) 18; в) 28; г) 3; д) 21; е) 58; є) 33; ж) 147; з) 6; к) 2; л) 42; м) 6; н) 6; о) 16; п) 48; р) 176. **13.** а) 2;6; б) 2;2; в) 2;1; г) 4;2; д) 2;1; е) 2;2; є) 1;18; ж) 4;16; з) 2;18; к) 2;22; л) 4;48; м) 3;13. **14.** а) $\frac{36}{11}$; б) $\frac{3527}{9900}$; в) $\frac{110119}{9999}$; г) $\frac{51487}{9900}$. **26.** а) $q \in \{220, 550, 660, 1100, 1650, 1980, 3300, 4950, 9900\}$; б) $q \in \{540, 740, 1350, 1850, 2220, 2700, 3700, 5550, 6660, 11100, 16650, 19980, 33300, 49950, 99900\}$

Таблиця простих чисел від 2 до 4057 та їх найменших первісних коренів

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277'	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	2	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Таблиця простих чисел від 2 до 4057 та їх найменших

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	1.3
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571.	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3259	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	6	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

Індекси

Просте число 3 Первісні корені: **2**

N	0	1	2	3	4	9	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							

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								

Просте число 17. Первісні корені: **3, 5, 6, 7, 10,11, 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, 13, 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
2	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		

---

* Скрізь за основу таблиці індексів береться найменший первісний корінь.

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	3	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, 33, 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	17	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, 80, 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	9	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	22	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	35
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	48	65	37
2	32	17	51	74	64	34	23	69	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, 60, 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
8	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	46	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	8	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	63	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	38
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				

Додаток 3. Таблиця квадратів

	0	1	2	3	4	5	6	7	8	9
0	0	1	4	9	16	25	36	49	64	81
1	100	121	144	169	196	225	256	289	324	361
2	400	441	484	529	576	625	676	729	784	841
3	900	961	1024	1089	1156	1225	1296	1369	1444	1521
4	1600	1681	1764	1849	1936	2025	2116	2209	2304	2401
5	2500	2601	2704	2809	2916	3025	3136	3249	3364	3481
6	3600	3721	3844	3969	4096	4225	4356	4489	4624	4761
7	4900	5041	5184	5329	5476	5625	5776	5929	6084	6241
8	6400	6561	6724	6889	7056	7225	7396	7569	7744	7921
9	8100	8281	8464	8649	8836	9025	9216	9409	9604	9801

Алфавіти

Латинський алфавіт

Букви	Назви букв	Букви	Назви букв
Aa	а	Nn	ен
Bb	бе	Oo	о
Cc	це	Pp	пе
Dd	де	Qq	ку
Ee	е	Rr	ер
Ff	еф	Ss	ес
Gg	ге	Tt	те
Hh	ха	Uu	у
Ii	і	Vv	ве(фау)
Jj	йот(а)	Ww	дубльве
Kk	ка	Xx	ікс
Ll	ель	Yy	іпсілон
Mm	ем	Zz	зета

Грецький алфавіт

Букви	Назви букв	Букви	Назви букв
$A\alpha$	альфа	$N\nu$	ню
$B\beta$	бета	$\Xi\xi$	ксі
$\Gamma\gamma$	гама	Oo	омікрон
$\Delta\delta$	дельта	$\Pi\pi$	пі
$E\varepsilon$	епсилон	$P\rho$	ро
$Z\zeta$	дзета	$\Sigma\sigma$	сигма
$H\eta$	ета	$T\tau$	тау
$\Theta\theta$	тета	$\Upsilon\upsilon$	іпсилон
$I\iota$	йота	$\Phi\varphi$	фі
$K\kappa$	капа	$X\chi$	хі
$\Lambda\lambda$	ламбда	$\Psi\psi$	псі
$M\mu$	мю	$\Omega\omega$	омега

Основні позначення.

$\mathbb{N} = \{1, 2, 3, \ldots\}$ — множина всіх натуральних чисел;
$\mathbb{Z}$ — множина всіх цілих чисел;
$\mathbb{Z}^+$ — множина всіх цілих додатних чисел;
$n\mathbb{Z}$ — множина всіх цілих чисел, які діляться на натуральне n;
$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ — множина всіх цілих гауссових чисел;
$\mathbb{Z}[\sqrt[m]{n}] = \{a + b\sqrt[m]{n} | a, b, n \in \mathbb{Z}, m \in \mathbb{N}\}$;
$\mathbb{Z}_n = \mathbb{Z}/(n) = \mathbb{Z}/n$ — кільце класів лишків за модулем n;
$\mathbb{Q}$ — множина всіх раціональних чисел;
$\mathbb{Q}^+$ — множина всіх додатних раціональних чисел;
$\mathbb{Q}_p = \{\frac{m}{n} | m, n \in \mathbb{Q}, p \in \mathbb{N}, (p, n) = 1\}$;
$\mathbb{Q}[\sqrt[m]{n}] = \{a + b\sqrt[m]{n} | a, b \in \mathbb{Q}, n \in \mathbb{Z}, m \in \mathbb{N}\}$;
$\mathbb{R}$ — множина всіх дійсних чисел;
$D_k = \{a_1 \cdot k^{r_1} + a_2 \cdot k^{r_2} + \cdots + a_n \cdot k^{r_n} | k, n \in \mathbb{N} \wedge a_i \in \mathbb{Z} \wedge r_i \in \mathbb{Q}^+ \cup \{0\}\}$;
$\mathbb{C}$ — множина всіх комплексних чисел;
K — кільце;
$K \times L$ — прямий добуток кілець K і L;
K^* — мультиплікативна група кільця K (множина всіх дільників одиниці кільця K);
$M(n, \mathbb{R})$ — множина всіх матриць n-го порядку над полем $\mathbb{R}$;
K/I — фактор-кільце кільця K за ідеалом I;
$\bar{a} = K_a^{(m)}$ — клас лишків з представником a за модулем m;
$C_{[a,b]}$ — множина всіх функцій від однієї змінної неперервних на відрізку $[a, b]$;
(a) — головний ідеал кільця K, породжений елементом $a \in K$;
$(\{a, b\}) = (a, b)$ — найменший ідеал кільця K, який містить елементи $a, b \in K$;
$a \equiv b \pmod{I}$ — елементи a і b кільця K конгруентні за ідеалом I;
$(a_1 a_2 \ldots a_n)_g = \overline{a_1 a_2 \ldots a_{n_g}}$ – систематичний запис числа за основою g;
I, V, X, L, C, D, M — цифри римської нумерації, якими позначають числа 1, 5, 10, 50, 100, 500, 1000, відповідно;
$a \equiv b \pmod{m}$ — цілі числа a і b конгруентні за модулем m;
$m \vdots n$ — число m ділиться на число n;
НСД$(a, b) = (a, b)$ — найбільший спільний дільник чисел a і b;
НСК$(a, b) = [a, b]$ — найменше спільне кратне чисел a і b;
$\left(\frac{m}{n}\right)$ — символ Лежандра;
$[q_0; q_1, \ldots, q_n]$ — скінченний ланцюговий дріб;
$\frac{P_k}{Q_k}$ — підхідні дроби даного ланцюгового дробу;

$\tau(n)$ — число натуральних дільників числа n;
$\sigma(n)$ — сума натуральних дільників числа n;
$\varphi(n)$ — число натуральних чисел менших n і взаємно простих з n;
$[x]$ — ціла частина дійсного числа x;
$\{x\}$ — дробова частина дійсного числа x;
$\mathrm{Ker} f$ — ядро гомоморфізму f;
C_m^n — число комбінацій m з елементів по n елементів;
$P_m(a)$ — показник числа за модулем m;
$\mathrm{ind}_g a \pmod m$ — індекс числа a за модулем m при основі g.

Предметний показчик.

Література

[1] Завало С.Т., Костарчук В.М., Хацет Б.І. Алгебра і теорія чисел. – К.: Вища школа, 1976.–Ч. 2.– 402 с.

[2] Завало С.Т., Костарчук В.М., Хацет Б.И. Алгебра и теория чисел.– К.: Вища школа, 1980.–Ч.2.– 384 с.

[3] Куликов Л.Я. Алгебра и теория чисел.– М.: Высшая школа, 1979. – 559 с.

[4] Бородін О.І. Теорія чисел.–К.: Вища школа, 1970.– 262 с.

[5] Кулик В.Т., Рокіцький І.О., Алгебра. Оглядові лекції до державних екзаменів.– Вінниця.: педуніверситет, 1999.– 249 с.

[6] Алгебра и теория чисел, ч. 3. Учебное пособие для студентов-заочников пединститутов (под редакцией Н.Я.Виленкина).– М.: Просвещение, 1974.– 200 с.

[7] Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокіцький І.О., Алгебра і теорія чисел. Практикум. – К.: Вища школа, 1986.– Ч. 2.– 264 с.

[8] Куликов Л.Я., Москаленко А.И., Фомин А.А., Сборник задач по алгебре.– М.: Просвещение, 1993.– 288 с.

[9] Шнеперман Л.Б., Сборник задач по алгебре и теории чисел.– Минск: Высшейшая школа, 1982.– 233 с.

[10] Кострикин А.И., Сборник задач по алгебре.– М.: Факториал, 1995. – 454 с.

[11] Фаддеев Д.К., Соминский И.С., Сборник задач по высшей алгебре. М.: Наука, 1977.– 288 с.

[12] Лейфура В.М., Мітельман І.М., Радченко В.М., Ясінський В.А., Задачі міжнародних математичних олімпіад.– Л.: Євросвіт, 1999.– 128 с.

[13] Гальперин Г.А., Толпыго А.К., Московские математические олимпиады.– М.: Просвещение, 1986.– 302 с.

Гарвацький Володимир Сергійович

Кулик Володимир Тихонович

Рокіцький Іван Олександрович

Рокіцький Ростислав Іванович

Ясінський В'ячеслав Андрійович

ЗБІРНИК
задач з теорії чисел

Виготовлено з оригінал-макету в Вінницькому державному педагогічному університеті імені Михайла Коцюбинського, 21100, м. Вінниця, вул. Острозького, 32.

Зам. № _____ Наклад_____ _____