Міністерство освіти і науки України
ДВНЗ "Ужгородський національний університет"
Фізичний факультет
Кафедра твердотільної електроніки та інформаційної безпеки

Юлія Мисло, Михайло Пагіря, Василь Різак

Елементи математичних методів у криптології

Навчальний посібник для студентів спеціальності "Кібербезпека та захист інформації"

Ужгород
Видавництво УжНУ "Говерла"
2023

УДК 003.26:51
Рецензенти:

Рубіш Василь Михайлович — доктор фізико–математичних наук, професор, академік Академії технологічних наук України, завідувач Ужгородської лабораторії матеріалів оптоелектроніки та фотоніки Інституту проблем реєстрації інформації НАН України;

Мич Ігор Андрійович — кандидат фізико–математичних наук, доцент, доцент кафедри кібернетики і прикладної математики Ужгородського національного університету.

М 65 **Мисло Ю.М., Пагіря М.М., Різак В.М.**
Елементи математичних методів у криптології
Навчальний посібник для студентів спеціальності "Кібербезпека та захист інформації". Ужгород, ДВНЗ "УжНУ", 2023. 136 с.
ISBN 978–617–7825–93–6

В навчальному посібнику вміщено вибрані розділи вищої математики на яких ґрунтується сучасні методи криптографії. Основна увага в посібнику зосереджена на розв'язанні типових задач з теорії множин, комбінаторики, вищої алгебри, теорії чисел та многочленів з однією змінною, теорії лишків.

Навчальний посібник розрахований на студентів фізичного факультету Ужгородського національного університету, які навчаються за спеціальністю "Кібербезпека та захист інформації", а також буде корисним для студентів інших факультетів.

Рекомендовано до друку:
Вченою радою УжНУ
(протокол № 5 від 04 травня 2023 року)
Редакційно–видавничою радою УжНУ
(протокол № 3 від 02 травня 2023 року).

ISBN 978–617–7825–93–6

Зміст

Перелік умовних позначень

$\triangle$	— позначка завершення розв'язання
$\circ$	— бінарна операція
$\sim$	— еквівалентність
$\emptyset$	— порожня множина
$[x]$	— ціла частина числа x
$\{x\}$	— ціла частина числа x
2^A	— булеан множини A
$[a_0; a_1, \ldots, a_n, \ldots]$	— правильний ланцюговий дріб
$[a_0; a_1, \ldots, a_n]$	— n–й підхідний дріб
a^{-1}	— обернений елемент до елемента a
$a \equiv b \pmod{m}$	— порівняння за модулем m
A_n^m	— кількість розміщень без повторення
$\overline{A_n^m}$	— кількість розміщень з повтореннями
$a \in A$	— належність елемента a множині A
$a \notin A$	— неналежність елемента a множині A
$\lvert A\rvert$	— потужність множини A
$\bar{A}$	— доповнення множини до універсальної
$A \subset B, B \supset A$	— множина A — підмножина множини B
$A \sim B$	— еквівалентність двох множин
$A \cup B$	— сума (об'єднання) множин
$A \cap B$	— добуток (переріз) множин
$A \Delta B$	— симетрична різниця множин
$A \backslash B$	— різниця множин
$\bigcup\limits_{i=1}^{n} A_i$	— об'єднання n множин
$\bigcap\limits_{i=1}^{n} A_i$	— переріз n множин
$b_0 + \mathop{\mathbf{K}}\limits_{i=1}^{\infty} \left(a_i/b_i\right)$	— ланцюговий дріб
$b_0 + \mathop{\mathbf{K}}\limits_{i=1}^{n} \left(a_i/b_i\right)$	— n–й підхідний дріб ланцюгового дробу
C_n^m	— кількість сполучень без повторення,
$\overline{C_n^m}$	— кількість сполучень з повтореннями
$C_n(n_1, \ldots, n_k)$	— кількість перестановок з повтореннями

$f_n(x)$	— многочлен степеня n
$f_n(c)$	— значення многочлена степеня n
$\ker f$	— ядро гомоморфізму
$K[x]$	— кільце многочленів
$\bar{k}$	— клас лишків за модулем
$m = \prod_{i=1}^{n} p_i^{k_1}$	— канонічне розвинення числа
$\mathbb{N}$	— множина натуральних чисел
$n!$	— $\boldsymbol{n}$–факторіал
P_n	— кількість перестановок (без повторення)
$p^{\#}$	— прайморіал числа p
$\mathbb{Q}$	— множина раціональних чисел
$\mathbb{R}$	— множина дійсних чисел
$\mathbb{R}^+$	— множина додатних дійсних чисел
$(x_1, x_2, \ldots, x_n)$	— перестановка
$(x; y)$	— впорядкована пара
$(x_1; x_2; \ldots; x_n)$	— кортеж
$X \times Y$	— декартів добуток множин X та Y
$X_1 \times X_2 \times \cdots \times X_n$	— декартів добуток n множин
X^n	— n–а декартова степінь множин X
$\mathbb{Z}$	— множина цілих чисел
$\mathbb{Z}_0$	— множина невід'ємних цілих чисел
$\mathbb{Z}_m^*$	— множина класів лишків за модулем m
$\varphi(n)$	— функція Ойлера
НСД	— найбільший спільний дільник
НСК	— найменше спільне кратне

Вступ

З давніх часів людство мало потребу оберігати свої знання, технології, дані особистого характеру від сторонніх очей. В наш час інформація перетворилася у високоцінний товар, стратегічний ресурс. З іншого боку, перехоплення повідомлень і подальше їх спотворення чи викривлення може призвести до серйозних наслідків — безпекових, військових, економічних, технологічних, моральних тощо.

Сучасні способи захисту особливо цінної інформації ґрунтуються як на технічних засобах, так і на програмних. Програмні методи є реалізацією того чи іншого алгоритмів криптології, однієї із частин прикладної математики. Термін криптологія походить від двох давньогрецьких слів $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$ — прихований, скритний і $\lambda\acute{o}\gamma o\varsigma$ — слово. Наука криптологія, яка традиційно ділиться на криптографію та криптоаналіз, бере свої початки в багатьох фундаментальних математичних теоріях і ввібрала в себе велику кількість термінів, теорем, тверджень, алгоритмічних підходів на яких будуються криптографічні схеми чи алгоритми шифрування, дешифрування, аналізу криптографічних перетворень. Методи криптографії розвиваються і удосконалюються разом із досягненнями в сучасних математичних теоріях і часто виступають рушієм розвитку самих теорій, а особливо їх практичних застосувань.

На шляху удосконалення та розвитку методів шифрування, дешифрування та криптоаналізу великі сподівання покладаються на розширенням можливостей сучасних комп'ютерів — збільшення оперативної пам'яті та швидкодії процесорів, розпаралелювання тощо. З'являються нові напрямки криптографії, такі як квантова і пост–квантова криптографія та біомолекулярна криптографія.

Даний навчальний посібник присвячений тим розділам сучасної математики, на яких ґрунтуються класичні криптографічні методи. Ці криптографічні методи пройшли перевірку часом і активно використовуються сьогодні в різних областях діяльності людини для захисту та збереження

цілісності важливої інформації.

В рамках підготовки фахівців із спеціальності "Кібербезпека та захист інформації" на фізичному факультеті Ужгородського національного університету читається ряд курсів з криптології.

Методи, алгоритми та підходи, що використовуються в задачах шифрування та дешифрування повідомлень викладаються в таких навчальних курсах як "Прикладна криптографія" та "Криптографічні перетворення". З теоретичними основами алгоритмів шифрування та дешифрування інформації можна ознайомитися з україномовних джерел, до прикладу [2, 13, 19], або з книг закордонних авторів [22, 23, 24]. Навчальний посібник має на меті не стільки виокремити із джерел необхідні теоретичні відомості про математичні методи криптології, як більш детально зосередитися на методах розв'язання задач по кожному розділу, щоб допомогти студентам, зокрема вказаних напрямків підготовки, засвоїти способи та підходами до розв'язання задач із розглянутих тем. Це особливо важливо, оскільки в теорії криптографічних перетворень вміння розв'язувати вказані типові задачі та здатність програмної реалізації їх розв'язання може забезпечити успіх. Навчальний посібник доповнює та розширює методичний посібник авторів [16].

Посібник містить наступні розділи вищої математики: **Теорія множин**, **Елементи комбінаторики**, **Окремі розділи алгебри**, **Елементи теорії чисел**, **Основи модульної арифметики**, **Многочлени**.

Перед **Вступом** наведено **Перелік умовних позначень**, які використовуються в навчальному посібнику. Першому розділі розглянуто основні поняття, операції над множинами, відображення множин, впорядковані пари. Другий розділ містить відомості про найважливіші комбінації, їх кількості та взаємозв'язки. Елементи вищої алгебри викладено в третьому розділі. Тут зокрема розглянуто перестановки, підстановки, бінарні алгебричні операції, групи, кільця, поля, гомоморфізм та ізоморфізм груп. Деяким елементам теорії чисел присвячений четвертий розділ. Тут зокрема розглянуто подільність цілих чисел, алгоритм Евкліда, елементи правильних ланцюгових дробів, прості числа, основна теорема арифметики та її наслідки. Наступний, п'ятий розділ, відведено під одну із найважливіших з точки зору теорій — теорію лишків за модулем. Відомості про многочлени однієї змінної над деяким полем наведено в п'ятому розділі. Розглянуто арифметичні дії над многочленами та деякі методи відшукання найбільшого спільного дільника двох многочленів. В кінці посібника вміщено

предметний покажчик основних термінів, які зустрічаються у тексті та список джерел. Всі розділи мають схожу структуру. На початку кожного параграфу наводяться без обґрунтування необхідні теоретичні відомості, які ілюструються прикладами. Далі розглянуто розв'язки типових задач із розглядуваної теми. Закінчення розв'язків завдань позначено значком "△".

В кінці розділу вміщено питання з теоретичного матеріалу, тести, на кожен з яких запропоновано три альтернативні відповіді, а також набір вправ для самостійного розв'язання. Завдання та вправи адаптовані до задач, які розглядаються при вивчені методів шифрування та дешифрування інформації.

Автори сподіваються, що запропонований навчальний посібник буде корисним при вивченні розглянутих тут розділів вищої математики.

Автори

Розділ 1

Елементи теорії множин

Теорія множин — фундамент низки нових розділів математики і присвячена вивченню загальних властивостей скінчених чи нескінчених множин ([3, 4, 7, 14, 15, 17]).

1.1 Поняття множини

Поняття **множини** належить до первинних понять сучасної математики, тобто тих найпростіших понять, які не можна означити через поняття ще більш прості. Поряд із такими первинними поняттями, як **точка, пряма, площина, поверхня, тіло тощо**, які добре відомі із курсу шкільної геометрії, поняття **множини** не означають, а сприймають інтуїтивно.

Засновник теорії множин німецький математик Георг Кантор стверджував, що **множина — це багато дечого, мислимого нами як єдине**. Можна уявляти собі множину як сукупність (сім'ю, набір, зібрання) деяких об'єктів, що мають спільну властивість.

Приклад 1.1.
Множина студентів 3–го курсу фізичного факультету УжНУ спеціальності "Кібербезпека та захист інформації".

Ця множина складається не із усіх студентів УжНУ, а лише з тих, які навчаються на 3–му курсі вказаної спеціальності фізичного факультету.

Приклад 1.2.
Множина літер української абетки, що використовуються при записі речення — ***Криптографія древня наука***.

Приклад 1.3.
Множина коренів квадратного рівняння

$$ax^2 + bx + c = 0.$$

Числа, які складають дану множину, мають бути коренями квадратного рівняння.

Множини складаються із окремих об'єктів, які називаються **елементами множини**. Множини, як правило, позначають великими латинськими літерами A, B, C, а елементи множин — малими латинськими літерами a, b, c, або малими літерами із індексами $a_1, a_2, \ldots$

Щоб вказати належність елемента a множині A, будемо писати $a \in A$ і казати "a **належить** A". А щоб підкреслити, що елемент b не належить множині **A** будемо записувати $b \notin A$ і говорити "b **не належить** A".

Означення 1.1.
Множина, елементи якої є множини, називається ***класом (сімейством).***

Означення 1.2.
Якщо елементи всіх множин вибирають з якоїсь однієї, досить широкої множини U, то таку множину називається ***універсальною.***

Вкажемо три найпоширеніші способи задання множини:

1. **Переліченням елементів**, які входять до множини. Так можна задавати ті множини, які містять скінчену кількість елементів.

   Приклад 1.4.
   $A = \{a_1; a_2; a_3; \ldots; a_n\}$ — *скінчена множина, яка нараховує n елементів.*

2. **Характеристичним предикатом**, тобто за допомогою деякого логічного твердження.

   Приклад 1.5.
   $B = \{b \mid 2 < b < 5\}$ — *множина всіх дійсних чисел, що знаходять між числами* 2 *і* 5.

3. **Рекурсивною процедурою**, тобто формулою, за допомогою якої послідовно отримують даний елемент множини через попередні елементи.

Приклад 1.6.
Послідовність чисел Фібоначчі:

$$N_F = \{F_k \mid F_1 = 1, F_2 = 1, F_k = F_{k-1} + F_{k-2}, k = 3, 4, 5, \dots\} =$$
$$= \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots\}.$$

Означення 1.3.
Множина, яка не містить жодного елемента, називається ***порожньою*** *і позначається символом* $\varnothing$.

Приклад 1.7.
Множина дійсних коренів наступного квадратного рівняння $x^2 + 1 = 0$ *буде порожньою множиною* $A = \{x \mid x^2 + 1 = 0\} = \varnothing$.

Наведемо приклади деяких числових множин, які будуть використовуватися далі.

Приклад 1.8.
Множина натуральних чисел

$$\mathbb{N} = \{1, 2, 3, \dots, n, \dots\}.$$

Приклад 1.9.
Множина невід'ємних цілих чисел

$$\mathbb{Z}_0 = \{0, 1, 2, 3, \dots, n, \dots\}.$$

Приклад 1.10.
Множина цілих чисел

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots, \pm n, \dots\}.$$

Приклад 1.11.
Множина невід'ємних цілих чисел менших за p

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p - 1\}.$$

Приклад 1.12.
Множина раціональних чисел

$$\mathbb{Q} = \left\{m/n \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N}\right\}.$$

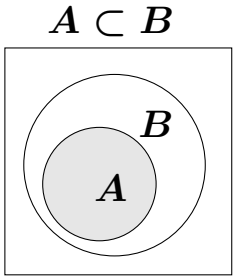
Приклад 1.13.
Множина дійсних чисел $\mathbb{R}$.

Приклад 1.14.
Множина літер української абетки
{а,б,в,г,ґ,д,е,є,ж,з,и,і,ї,й,к,л,м,н,о,п,р,с,т,у,ф,х,ц,ч,ш,щ,ь,ю,я}.

Приклад 1.15.
Множина літер латинської абетки
{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}.

Означення 1.4.
Множина $\boldsymbol{A}$ *називається* ***підмножиною*** *множини* $\boldsymbol{B}$, *що записується так* $\boldsymbol{A \subset B}$ *або так* $\boldsymbol{B \supset A}$, *якщо кожний елемент множини* $\boldsymbol{A}$ *також є елементом множини* $\boldsymbol{B}$.

Можна проілюструвати поняття підмножини за допомогою діаграми Венна.



Числові множини, які розглянуті вище, задовольняють наступну послідовність включень $\mathbb{N} \subset \mathbb{Z}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Означення 1.5.
Множини $\boldsymbol{A}$ *і* $\boldsymbol{B}$ *називаються* ***рівними***, *якщо* $\boldsymbol{A \subset B}$ *і* $\boldsymbol{B \subset A}$, *що записують так* $\boldsymbol{A = B}$.

Означення 1.6.
Кажуть, що між множинами $\boldsymbol{A}$ *і* $\boldsymbol{B}$ *встановлено взаємно–однозначна відповідність, якщо*

1. *кожному елементу* $\boldsymbol{a \in A}$ *поставлено у відповідність* ***один і тільки один*** *елемент* $\boldsymbol{b \in B}$, *тобто* $\boldsymbol{a \in A \to b \in B}$;
2. *різним елементам* $\boldsymbol{a \in A}$ *відповідають різні елементи* $\boldsymbol{b \in B}$;
3. *кожен елемент* $\boldsymbol{b \in B}$ *відповідає одному елементу* $\boldsymbol{a \in A}$.

Означення 1.7.
Множини A *і* B *між якими встановлена взаємно-однозначна відповідність називаються* ***еквівалентними****. Еквівалентність множин позначають наступним чином:* $A \sim B$.

Якщо множина $A \sim \{1, 2, \ldots, n\}$, то кажуть, що множина **A** має **потужність** n і записують $|A| = n$. Потужність $|\varnothing| = 0$. Якщо |**A**|=|**B**|, то множини **рівнопотужні**.

Потужність множини — це її **кардинальне (головне)** число. Потужність — це така властивість множини, яка притаманна всім еквівалентним, а отже рівнопотужним множинам.

Означення 1.8.
Множина всіх підмножин множини A *називається* ***булеаном*** *і позначається* 2^A*. Для скінчених множин потужність булеана рівна* $|2^A| = 2^{|A|}$.

Задача 1.1.
З'ясувати, чи належить літера ***"ю"*** *до множини літер повідомлення* ***"гарний текст"****.*

Розв'язання. Множина **A={а,г,е,и,й,к,н,р,с,т}** є множиною літер повідомлення **"гарний текст"**. Множина не містить літери **"ю"**. Отже, **"ю"** $\notin A$.

△

Задача 1.2.
Чи буде множина літер повідомлення ***"секрет"*** *підмножиною множини літер шифровки* ***"еаиаокгрестші"****.*

Розв'язання. Повідомлення **секрет** записано за допомогою множини літер **A={е,к,р,с,т}**. Шифровка **еаиаокгрестші** записана за допомогою літер **B={а,г,е,и,і,к,о,р,с,т,ш}**. Легко бачити, що літери множини **A** також належать до множини **B**. Тоді $A \subset B$. Отже, множина літер повідомлення є підмножиною літер шифровки.

△

Задача 1.3.
Записати булеан множини літер шифровки ***уосоус****.*

Розв'язання. Множина літер шифровки **A={о,с,у}**. Потужність множини $|A| = 3$. Тоді булеан 2^A буде мати потужність $2^{|A|} = 8$ і складається: 2^A**={{∅}, {о}, {с}, {у}, {о,с}, {о,у}, {с,у}, {о,с,у}}**.

△

1.2 Операції над множинами

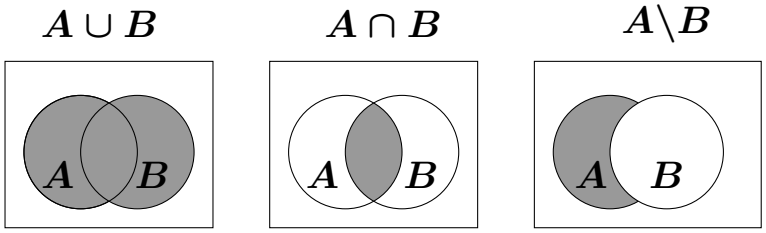
Над множинами можна виконувати операції.

Означення 1.9.
Будемо називати ***сумою (об'єднанням)*** *множин* A *та* B *множину* D *і записувати* $D = A \cup B$*, якщо вона містить всі елементи обох множин.*

Означення 1.10.
Будемо називати ***добутком (перерізом)*** *множин* A *та* B *множину* C *і записувати* $C = A \cap B$*, елементами якої є ті елементи множин, що одночасно належать і множині* A *і множині* B*.*

Означення 1.11.
Будемо називати ***різницею*** *множин* A *та* B *множину* E *і записувати* $E = A \backslash B$*, що містить лише ті елементи множини* A*, які не належать множині* B*.*

Операції суми, добутку та різниці множин ілюструються діаграмами Венна.

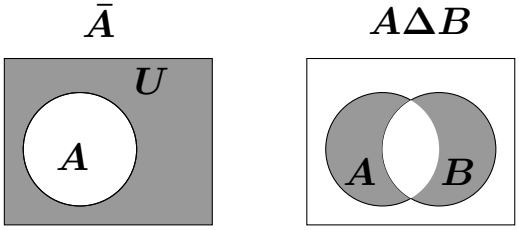


Означення 1.12.
Будемо називати ***доповненням*** *множини* A *до універсальної множини* U *множину, яку будемо записувати* $\bar{A}$*, що містить лише ті елементи множини* U*, які не належать множині* A*.*

Означення 1.13.
Симетрична різницю *множин* A *та* B*, яку записують* $A \Delta B$*, визначається співвідношенням*

$$A \Delta B = \Big(A \backslash B\Big) \cup \Big(B \backslash A\Big).$$

Маємо такі діаграми Венна операцій доповнення множини до універсальної та операції симетричної різниці множин.



Задача 1.4.
Нехай множини A, B *та універсальна множина* U *визначені наступним чином*

$$A = \{-2, -1, 0, 1, 2, 3, 4\}, \quad B = \{-3, -1, 1, 3, 5\},$$
$$U = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

Знайти множини
$C = A \cup B, D = A \cap B, E = A \backslash B, F = B \backslash A, \bar{A}, \bar{B}, H = A \Delta B.$

Розв'язання. Скориставшись означенням вказаних операцій над множинами, маємо:

$$C = A \cup B = \{-3, -2, -1, 0, 1, 2, 3, 4, 5\},$$
$$D = A \cap B = \{-1, 1, 3\},$$
$$E = A \backslash B = \{-2, 0, 2, 4\},$$
$$F = B \backslash A = \{-3, 5\}.$$
$$\bar{A} = \{-5, -4, -3, 5\},$$
$$\bar{B} = \{-5, -4, -2, 0, 2, 4\},$$
$$H = A \Delta B = \{-5, -4, -3, -2, 0, 2, 4, 5\}.$$

$\triangle$

Зауваження 1.1.
Операції перетину і об'єднання множин узагальнюють на більшу кількість множин, тобто

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

— об'єднання n *множин,*

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

— переріз n *множин.*

Задача 1.5.
Для множин

$$A = \{1, 2, 30, 31\}, \qquad B = \{1, 4, 23, 31\}, \qquad C = \{1, 2, 31\}$$

знайти множини

$$E = A \cup B \cup C, \qquad D = A \cap B \cap C.$$

Розв'язання. Згідно з означенням маємо

$$E = \{1, 2, 4, 23, 30, 31\}, \qquad D = \{1, 31\}.$$

$\triangle$

1.3 Впорядковані пари

Означення 1.14.
Нехай $x \in X$ і $y \in Y$. Пару елементів x та y, яка записана у вигляді $(x; y)$ називають ***упорядкованої парою*** *(елемент x — перша компонента пари, y — друга компонента пари).*

Означення 1.15.
Впорядковані пари $(x_1; y_1)$ і $(x_2; y_2)$ рівні тоді і тільки тоді, коли $x_1 = x_2$ і $y_1 = y_2$.

Із означення випливає, що, взагалі кажучи, $(x; y) \neq (y; x)$.

Означення 1.16.
Множина, усі елементи якої є впорядковані пари, називається ***прямим (декартовим) добутком множин****:*

$$X \times Y = \{(x; y) \mid x \in X, y \in Y\}.$$

Потужність прямого добутку $|X \times Y| = |X| \cdot |Y|$.

Зауваження 1.2.
Очевидно, що $X \times Y = Y \times X$ тоді, коли $X = Y$.

Зауваження 1.3.
Аналогічно, набір із n елементів $(x_1; x_2; \ldots; x_n)$ називаються ***кортежем****. Кортеж є елемент прямого (декартового) добутку n множин*

$X_1 \times X_2 \times \cdots \times X_n$.

Означення 1.17.
Прямий (декартів) добуток *множини X саму на себе n разів називається n–м декартовим степенем множини X:*

$$X^n = \underbrace{X \times X \times \cdots \times X}_{n \text{ разів}}.$$

Означення 1.18.
Відображенням *множини X у множину Y називається правило, за яким кожному елементу $x \in X$ ставиться у відповідність один елемент $y \in Y$ та позначають $f : X \to Y$.*

Відображення можна тлумачити, як дію, що переводить елемент $x \in X$ в деякий елемент $y \in Y$, який називають **образом елемента** x при відображені та позначають $f(x)$, X **— область визначення відображення**.

Означення 1.19.
Образом підмножини $X_1 \subset X$ *при відображенні f називається об'єднання образів всіх елементів $x \in X_1$. Образ підмножини позначаємо $f(X_1)$.*

Якщо $y \in Y$ фіксоване, то його **повним прообразом** при відображенні f називається множина всіх елементів із X, для яких y є образом при цьому відображенні. Повний прообраз позначають $f^{-1}(y)$. Довільний елемент із $f^{-1}(y)$ називають **прообразом елемента** y.

Нехай $X = \{x_1, x_2, \ldots, x_n\}$ — деяка скінчена множина, тоді відображення $f : X \to Y$ можна записати у вигляді дворяду

$$f = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ f(x_1) & f(x_2) & f(x_3) & \cdots & f(x_n) \end{pmatrix}.$$

Означення 1.20.
Якщо $f : X \to Y$ — однозначне відображення з X в Y, то відображення вигляду $f^{-1} : Y \to X$, яке ставить у відповідність кожному елементу $y \in Y$ його прообраз $f^{-1}(y) \in X$, називається ***оберненим*** *для відображення f.*

Нехай визначені два відображення $f : X \to Y$ і $g : Y \to Z$. Якщо поставити у відповідність кожному елементу $x \in X$ елемент $g(f(x)) \in Z$, то відображення множини X у множину Z називається **добутком (композицією)** відображень f і g та позначається gf.

Задача 1.6.
Задані множини $X = \{a, b\}, Y = \{e, h, g\}$. Знайти декартові добутки

множин $X \times Y, Y \times X$ *та степені множин* X^3, Y^2.

Розв'язання. Згідно із означенням

$$X \times Y = \{(a,e),(a,h),(a,g),(b,e),(b,h),(b,g)\},$$

$$Y \times X = \{(e,a),(e,b),(h,a),(h,b),(g,a),(g,b)\},$$

$$\begin{aligned} X^3 = X \times X \times X = \{&(a,a,a),(a,a,b),(a,b,a),(a,b,b),\\ &(b,a,a),(b,a,b),(b,b,a),(b,b,b)\}, \end{aligned}$$

$$\begin{aligned} Y^2 = Y \times Y = \{&(e,e),(e,h),(e,g),(h,e),(h,h),\\ &(h,g),(g,e),(g,h),(g,g)\}. \end{aligned}$$

$\triangle$

Задача 1.7.
Нехай відображення $f : X \to Y$ *елементу множини* $X = \{2,3,5,6\}$ *ставить у відповідність найменше спільне кратне цього числа і числа* 4. *Записати вказане відображення у вигляді дворяду.*

Розв'язання. Оскільки $f(2) = 4,\ f(3) = 12,\ f(5) = 20,\ f(6) = 12$, то отримаємо

$$f = \begin{pmatrix} 2 & 3 & 5 & 6 \\ 4 & 12 & 20 & 12 \end{pmatrix}.$$

$\triangle$

Задача 1.8.
Нехай відображення f, g, *які діють із* $\mathbb{R}$ *в* $\mathbb{R}$, *визначенні співвідношеннями* $f(x) = x^3,\ g(x) = \ln(x^2+1)$. *Знайти наступні композиції відображень* $fg, gf, f^3, g^2, f^{-1}, g^{-1}$.

Розв'язання. Знаходимо

$$fg = f(g(x)) = (\ln(x^2+1))^3 = \ln^3(x^2+1),$$

$$gf = g(f(x)) = \ln((x^3)^2+1) = \ln(x^6+1),$$

$$f^3 = f(f(f(x))) = ((x^3)^3)^3 = x^{27},$$

$$g^2 = g(g(x)) = \ln((\ln(x^2+1))^2+1) = \ln(\ln^2(x^2+1)+1).$$

$$f^{-1} = \sqrt[3]{x}, \quad g^{-1} = \sqrt{e^x - 1}.$$

$\triangle$

1.4 Питання, тести та вправи до розділу 1

1.4.1 Питання до розділу 1

1. Як позначається належність елемента a множині B?
2. Яка множина називається порожньою?
3. Дати означення класу.
4. Які є способи задання множини?
5. Коли множина A є підмножиною множини B?
6. Вказати приклади множин.
7. Дайте означення підмножини.
8. Коли множина A рівна множині B?
9. Дайте означення взаємно–однозначної відповідності двох множин.
10. Коли множина A еквівалентна множині B?
11. Що таке потужність скінченної множини?
12. Дайте означення булеана множини.
13. Як визначається сума двох множин?
14. Дайте означення добутку двох множин.
15. Що розуміють під різницею двох множин?
16. Як визначається сума та добуток n множин?
17. Дати означення впорядкованої пари.
18. Що таке декартів добуток множин?
19. Як розуміти n–а степінь множини X?
20. Дати означення відображення множини X у множину Y.
21. Що таке образ підмножини $X_1 \subset X$ при відображенні f?
22. Дати означення повного прообразу $y \in Y$ при відображенні f.

23. Яке відображення називається оберненим?

24. Дати означення композиції відображень.

1.4.2 Тести до розділу 1

Вказати правильну відповідь на кожен тест.

1. Задані множина B і елемент a. Елемент a належить B:

   (A) Ніколи; **(B)** Деколи; **(C)** Завжди.

2. Порожня множина $\emptyset$ містить:

   (A) Один елемент; **(B)** Безліч елементів; **(C)** Жодного елемента.

3. Задана множина $G = \{a, b, c, d, e\}$. Потужність булеана 2^G рівна:

   (A) 5; **(B)** 20; **(C)** 32.

4. Нехай $A \subset B$. Яке твердження вірне:

   (A) Кілька елементів з A належать B;

   (B) Всі елементи з A належать B;

   (C) Множини не мають спільних елементів.

5. Нехай $C = A \cup B$. Яке твердження вірне:

   (A) Множина C містить лише елементи множини A;

   (B) Множина C містить лише елементи множини B;

   (C) Множина C містить елементи обох множин.

6. Нехай $D = A \cap B$. Яке твердження вірне:

   (A) Множина D містить елементи множини A, що не належать множині B;

   (B) Множина D містить елементи множини B, що не належать множині A;

   (C) Множина D містить спільні елементи обох множин.

7. Нехай $E = A \backslash B$. Яке твердження вірне:

   (A) Множина E містить лише елементи множини A, які не належать множині B;

   (B) Множина E містить спільні елементи множин;

(C) Множина E містить елементи, які одночасно не належать A і B.

8. Нехай $C = A_1 \cup A_2 \cup A_3$. Яке твердження вірне:

   (A) Множина C містить елементи, які належать хоча б одній множині;

   (B) Множина C містить елементи, що належать або A_2, або A_3;

   (C) Множина C містить елементи, які не належать A_1.

9. Нехай $D = A_1 \cap A_2 \cap A_3$. Яке твердження вірне:

   (A) Множина D спільні елементи трьох множин;

   (B) Множина D містить елементи, що належать або A_1, або A_2;

   (C) Множина C містить елементи, які не належать A_3.

10. Нехай $x \in X, y \in Y$, де множини X, Y — різні. Для впорядкованих пар $(x; y)$ та $(y; x)$, яке твердження вірне:

    (A) Пари однакові; **(B)** Пари подібні; **(C)** Пари різні.

11. Нехай $X = \{a, b\}$. Множина $Y = \{(a; a), (a, b), (b, b)\}$ буде:

    (A) Декартовим квадратом множини X;

    (B) Підмножиною множини X^2;

    (C) Добутком X на X.

12. Задані множини $X = \{-2, -1, 0, 1, 2\}$ та $Y = \{1, 2, 5\}$. Вказати відображення $f : X \to Y$:

    (A) $y = x + 2$; **(B)** $y = x^2$; **(C)** $y = x^2 + 2$.

13. Задані два відображення $f(n) = n^2 + 2,\ g(n) = 2n + 1$ множини $\mathbb{N}$ в $\mathbb{N}$. Вказати композицію відображень $f(g(n))$:

    (A) $f(g(n)) = 4(n^2 + n + 1) - 1$;

    (B) $f(g(n)) = 4(n + 1)^2 + 1$;

    (C) $f(g(n)) = 4n^2 + 3$.

1.4.3 Вправи до розділу 1

Вправа 1.1.

З'ясувати, чи належить літери ***"ь", "є", "ґ"*** *множині літер виразу* ***"знову снігова заметіль вкрила дорогу"***.

Вправа 1.2.
Маємо шифрограму ***"сіцноправувашлоерта"****. З'ясувати, чи множина літер слова* ***"орел"*** *буде підмножиною літер шифрограми.*

Вправа 1.3.
Отримали шифровку ***"павуувапу"****. Записати булеан множини літер шифровки.*

Вправа 1.4.
Нехай $\boldsymbol{A}$ *— множина літер повідомлення* ***"дрібна дислокація"****, а* $\boldsymbol{B}$ *— множина літер повідомлення* ***"велика частина"****. Знайти суму, різниці та добуток, симетричну різницю цих множин та доповнення множин* $\boldsymbol{A}$ *і* $\boldsymbol{B}$ *до універсальної множини* $\boldsymbol{U}$ *— літер української абетки.*

Вправа 1.5.
Отримали три радіограми: ***"ґрунтову дорогу заміновано"****,* ***"річка броду не має"****,* ***"болотом проходить стежка"****. Утворити множини літер кожного повідомлення. Знайти суму та добуток трьох знайдених множин.*

Вправа 1.6.
Множини $\boldsymbol{A_1},\ \boldsymbol{A_2},\ \boldsymbol{A_3},\ \boldsymbol{A_4}$ *складаються, відповідно, із літер повідомлень*
$\boldsymbol{C_1}$ = ***"можливі зміни"****;*
$\boldsymbol{C_2}$ = ***"очікувати завтра"****;*
$\boldsymbol{C_3}$ = ***"зелена троянда"****;*
$\boldsymbol{C_4}$ = ***"зліва від зупинки"****.*
Знайти множини $\boldsymbol{B_1} = \bigcup\limits_{i=1}^{4} \boldsymbol{A_i},\ \boldsymbol{B_2} = \bigcap\limits_{i=1}^{4} \boldsymbol{A_i},\ \boldsymbol{B_1 \backslash \{A_2 \cup A_3\}}$.

Вправа 1.7.
Для множин $\boldsymbol{X = \{S, T\}, Y = \{b, c, d\}, Z = \{1, 2, 3, 4\}}$*, знайти декартові добутки множин* $\boldsymbol{X \times Y},\ \boldsymbol{X \times Z}, \boldsymbol{Z \times Y}$ *та декартові степені множин* $\boldsymbol{X^4},\ \boldsymbol{Y^3},\ \boldsymbol{Z^2}$.

Вправа 1.8.
Відображення $\boldsymbol{f : X \to Y}$ *ставить у відповідність кожному елементу множини* ***X={а,в,г,і,к}*** *порядковий номер літери в українській абетці. Записати вказане відображення у вигляді дворяду.*

Вправа 1.9.
Знайти відображення $\boldsymbol{fg, gf, f^2, g^3, g^{-1}}$*, якщо* $\boldsymbol{f = \sin x^2, g = e^x}$.

Розділ 2

Елементи комбінаторики

Комбінаторика або **комбінаторний аналіз** — розділ математики, що присвячений розв'язанню задач вибору та розміщення елементів деякої скінченної множини згідно із заданими правилами ([6, 9, 21]).

2.1 Комбінаторні схеми

Означення 2.1 (Правило суми).
Якщо A і B — скінчені множини, які не перетинаються, тобто $A \cap B = \emptyset$ і крім того $|A| = n, |B| = m$, тоді $|A \cup B| = n + m$.

Означення 2.2 (Правило прямого добутку).
Нехай A і B — скінчені множини, $|A| = n, |B| = m$. Тоді $|A \times B| = n \cdot m$.

Зауваження 2.1.
Нехай задані множини $X_1, X_2, \ldots, X_k$, що мають потужності $|X_i| = n_i$, $i = 1, 2, \ldots, k$, тоді виконуються рівності

$$\Big|X_1 \times X_2 \times \cdots \times X_k\Big| = n_1 \cdot n_2 \cdot \ldots \cdot n_k = \prod_{i=1}^{k} n_i,$$

$$\Big|\bigcup_{i=1}^{k} X_i\Big| = n_1 + n_2 + \cdots + n_k = \sum_{i=1}^{k} n_i, \quad X_i \cap X_j = \varnothing.$$

Задача 2.1.
Скільки тризначних парних чисел можна утворити із наступних цифр $\{0; 1; 2; 3; 4; 5; 6\}$, якщо цифри повторюються?

Розв'язання. Утворенні числа мають містити три цифри

$$A_1A_2A_3.$$

У першому, найстаршому розряді A_1 можуть бути всі цифри крім 0. Отже, потужність $|A_1| = 6$.

В якості другої цифри можна взяти довільну цифру, $|A_2| = 7$.

Оскільки число має бути парним, то в молодшому розряді має бути одна із цифр $A_3 = \{0; 2; 4; 6\}$, $|A_3| = 4$.

Згідно із **правилом прямого добутку, основного правила комбінаторики**, кількість тризначних непарних чисел N рівна

$$N = |A_1 \times A_2 \times A_3| = |A_1| \cdot |A_2| \cdot |A_3| = 6 \cdot 7 \cdot 4 = 168.$$

$\triangle$

Нехай X – скінчена, $|X| = n$. Вибираємо m елементів. Утворюються деякі підмножини із X, які називають **комбінаціями із n по m**.

Залежно від того, чи враховується **черговість** елементів, чи **входять всі елементи** чи тільки **частина**, розрізняють:

- розміщення із n елементів по m без повторення;
- перестановки із n елементів;
- сполучення із n елементів по m без повторення;
- розміщення із n по m з повторенням;
- перестановки із n елементів з повторенням;
- сполучення із n елементів по m з повторенням.

2.2 Розміщення із n елементів по m без повторення

Означення 2.3.
*Комбінації, кожна з яких містить m елементів, які вибрані із n різних елементів, $m \leqslant n$, і які відрізняються одна від одної або складом елементів або їх порядком, називаються **розміщення із n елементів по m (без повторення)**.*

Кількість розміщень без повторень обчислюється за формулою

$$A_n^m = n(n-1)\cdot(n-2)\cdots(n-m+1) = \frac{n!}{(n-m)!}, \qquad (2.1)$$

де $n! = 1\cdot 2\cdots n$ — факторіал натурального числа n. Домовимося надалі вважати, що $0! = 1$.

Задача 2.2.
Задана множина цифр $\{1; 2; 3; 4; 5; 6; 7; 8; 9\}$. *Знайти кільки семизначних чисел, які можна утворити із цифр множини, щоб жодна із цифр не повторювалася?*

Розв'язання. Цифри не мають повторюватися. Водночас, порядок входження цифр в число важливе. Маємо задачу на розміщення із 9 елементів (цифр) по 7. Скористаємося формулою (2.1). Тоді, кількість семизначних чисел N буде рівна

$$N = A_9^7 = 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3 = 181440.$$

$\triangle$

2.3 Перестановки із n елементів

Означення 2.4.
Комбінації, кожна з яких містить усі n *елементів із* n *можливих елементів, які взяті у певному порядку, називаються* ***перестановкою із*** n ***елементів****.*

Так як перестановка є розміщенням без повторення із n елементів по n, то кількість перестановок

$$P_n = A_n^n = n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1 = n! \qquad (2.2)$$

Задача 2.3.
Нехай задані цифри $\{1; 2; 3; 5; 7; 9\}$. *Скільки шестизначних парних чисел можна утворити із вказаних цифр, якщо цифри в числі не повторюються?*

Розв'язання. Утворені числа мають бути парними. Отже, всі вони в молодшому розряді мусять містити цифру 2. Решта 5 цифр можуть в

довільній послідовності без повторень займати $\mathbf{5}$ старших розрядів числа. Тоді згідно із формулою (2.2) маємо

$$\boldsymbol{N = A_5^5 = 5! = 120}.$$

$\triangle$

Задача 2.4.
У підгрупі $\mathbf{7}$ студентів. Староста складає графік чергування по одному студенту на день. Скільки існує різних варіантів графіку чергування?

Розв'язання. Кожен студент потрапляє у графік чергування один раз. Порядок чергування суттєвий. Маємо розміщення із $\mathbf{7}$ елементів по $\mathbf{7}$, тобто кількість перестановок із $\mathbf{7}$ елементів. За формулою (2.2) знаходимо

$$\boldsymbol{N = A_7^7 = 7! = 5040}.$$

$\triangle$

2.4 Сполучення із n елементів по m без повторення

Означення 2.5.
*Комбінації, кожна з яких містить $\boldsymbol{m}$ елементів із можливих $\boldsymbol{n}$ різних елементів, $\boldsymbol{m \leqslant n}$, які відрізняються одна від одної принаймні одним елементом називаються **сполученнями із $\boldsymbol{n}$ елементів по $\boldsymbol{m}$ без повторення**.*

Зауваження 2.2.
На відміну від розміщень, елементи у сполученнях не впорядковані.

Кількість сполучень визначається формулою

$$\boldsymbol{C_n^m = \frac{n \cdot (n-1) \cdot \dots \cdot (n-m+1)}{m!} = \frac{n!}{(n-m)!\, m!}}. \qquad (2.3)$$

.

Взаємозв'язок між розміщеннями та сполученнями без повторення задається співвідношенням

$$\boldsymbol{A_n^m = m! \cdot C_n^m}.$$

Числа $\boldsymbol{C_n^m}$ також називають **біноміальними коефіцієнтами**, оскільки для довільного $\boldsymbol{n}$ має місце формула бінома Ньютона

$$\boldsymbol{(a+b)^n = C_n^0 a^n b^0 + C_n^1 a^{n-1} b^1 + \dots + C_n^n a^0 b^n}.$$

Комбінації або біноміальні коефіцієнти володіють наступними властивостями:

1. $C_n^m = C_n^{n-m}$;
2. $C_n^0 = C_n^n = 1; \quad C_n^1 = n$;
3. $C_n^0 + C_n^1 + \cdots + C_n^{n-1} + C_n^n = 2^n$;
4. $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}, \qquad n > 1,\ 0 < m < n.$

Часто біноміальні коефіцієнти записують у **трикутник Паскаля**

$n=0$								1									
$n=1$							1		1								
$n=2$						1		2		1							
$n=3$					1		3		3		1						
$n=4$				1		4		6		4		1					
$n=5$			1		5		10		10		5		1				
$n=6$		1		6		15		20		15		6		1			
$n=7$	1		7		21		35		35		21		7		1		
$n=8$	1		8		28		56		70		56		28		8		1
	⋮		⋮		⋮		⋮		⋮		⋮		⋮		⋮		

Задача 2.5.
Скільки різних добутків можна утворити із дійсних чисел $a, b, c, d, e \in \mathbb{R}$, якщо кожний добуток містить три різні множники?

Розв'язання. Із середньої школи відомо, що у множині дійсних чисел $\mathbb{R}$ операція множення комутативна, тобто $ab = ba$. Тоді, порядок входження чисел у добуток не є важливим. Маємо сполуки із 5 елементів по 3. Згідно із формулою (2.3) маємо

$$K = C_5^3 = \frac{5 \cdot 4 \cdot 3}{6} = 10.$$

$\triangle$

Задача 2.6.
Скільки існує дільників числа 210?

Розв'язання.

Розкладемо число **210** на прості множники: $\mathbf{210 = 2 \cdot 3 \cdot 5 \cdot 7}$. Дільниками будуть числа **1,2,3,5,7,210**, тобто **6** чисел. Дільниками будуть добутки двох довільних простих дільників — **2,3,5,7**

$$C_4^2 = 6, \qquad \text{числа} \qquad 6, 10, 14, 15, 21, 35.$$

Дільниками також будуть добутки трьох простих дільників

$$C_4^3 = 4, \qquad \text{числа} \qquad 30, 42, 70, 105.$$

Число **210** має $6 + 6 + 4 = 16$ дільників.

$\triangle$

2.5 Розміщення з повтореннями

Означення 2.6.

Розміщенням *із* n *елементів по* m ***з повтореннями*** *називається комбінація* m *елементів із* n*, у кожне з яких може повторюватися.*

Число таких розміщень

$$\overline{A_n^m} = n^m. \tag{2.4}$$

Задача 2.7.

Визначити кількість семизначних чисел, які утворені із чисел $\{3, 4, 5, 6\}$*, якщо цифри можуть повторюватися.*

Розв'язання. Маємо розміщення з повтореннями. Скористаємося формулою (2.4), коли $n = 4, m = 7$.

$$\overline{A_4^7} = 4^7 = 16384.$$

$\triangle$

Задача 2.8.

Сейф замикається на замок, що має 5 *дисків, на кожному з яких зображені цифри* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$*. Замок відімкнуто, коли на дисках набрана певна комбінація цифр. Чи можна* ***"зламати"*** *сейф за* 10 *днів, якщо працювати щодня по* 13 *годин, а набір однієї комбінації цифр потребує* 5 *секунд.*

1	2	3	4	5	1
5	**6**	7	8	**6**	2
4	8	9	9	7	3
3	7	9	9	8	4
2	**6**	8	7	**6**	5
1	5	4	3	2	1

Рис. 2.1: Ґратка Кардано 6×6

Розв'язання. Всіх можливих комбінацій, які можна набрати на $\mathbf{5}$ дисках буде $\overline{A^5_{10}} = \mathbf{100000}$. Щоб набрати всі можливі комбінацій потрібно затратити $\mathbf{500000}$ секунд, або $\mathbf{500000/3600 = 138,888888889}$ годин, або $\mathbf{138,888888889/13 = 10,6838}$ "робочих днів". Отже, за $\mathbf{10}$ днів всі можливі комбінації не набрати.

△

Задача 2.9.

Для шифрування тексту виготовлено трафарет, ***ґратка Кардано****, з квадратного паперового аркушу у клітинку розміром $\ell \times \ell$, де ℓ—парне число. Одну із сторін трафарету помічено. Деякі із клітинок вирізано так, щоб при накладанні чистий квадрат такого ж розміру чотирма способами (помічена сторона* ***угорі, праворуч, унизу, ліворуч****) вирізані клітинки покрили всю площу квадрата, причому кожна клітинка мала опинитися під вирізом тільки один раз. Скільки різних трафаретів можна виготовити?*

Розв'язання. Усі клітинки квадрата розіб'ємо на групи, які не перетинаються, по чотири клітинки у кожній групі. Віднесемо клітинки до однієї групи, якщо при кожному повороті квадрата до його суміщення вони пересуваються на місця кліток із цієї групи. На рисунку 2.1 показано розбиття на групи кліток квадрата при $\mathbf{6 \times 6}$, де клітинки однієї групи помічено однаковою цифрою. Усього таких груп $m = \ell^2/4$ (m–ціле, бо ℓ–парне число.) При накладанні трафарету на квадрат рівно одна клітинка із заданою групи опиниться під вирізом. Кожному трафарету поставимо у відповідність упорядкований набір усіх кліток з таких груп, що будуть під вирізами при накладанні трафарету на квадрат поміченим боком угору. Усього таких трафаретів буде стільки, скільки існує відображень із m елементів у множину із чотирьох елементів ($n = 4$). Тобто маємо задачу про розміщення із повтореннями і за формулою $n^m = 4^{\ell^2/4}$ — кількість різних трафаретів.

△

2.6 Перестановки з повтореннями

Означення 2.7.
Перестановками *із n елементів з* ***повтореннями*** *називаються перестановки з n елементів, в кожну з яких входить n_1 однакових елемент першого типу, n_2 однакових елементів другого типу і т.д. до n_k однакових елементів k–го типу, де $n_1 + n_2 + \cdots + n_k = n$.*

Загальну кількість таких перестановок позначають

$$C_n(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \cdots n_k!}. \tag{2.5}$$

Задача 2.10.
Скільки існує семизначних чисел, у яких цифра 6 зустрічається 3 рази, а цифра 5 трапляється 4 рази?

Розв'язання. Маємо перестановки з повтореннями. Згідно із (2.5)

$$C_7(3, 4) = \frac{7!}{3! \cdot 4!} = 35.$$

△

Задача 2.11.
Скільки різних слів (не обов'язково зі змістом) можна утворити, якщо переставляти літери у словах:
a) ***абракадабра****; b)* ***баран****; c)* ***зебра****?*

Розв'язання. a) Слово **абракадабра** містить 5 літер **а**, по 2 літери **б** та **р** і по 1 літері **д** і **к**. Загалом у слові 11 літер. Тоді загальна кількість слів

$$N_a = C_{11}(5, 2, 2, 1, 1) = \frac{11!}{5! \cdot 2! \cdot 2! \cdot 1! \cdot 1!} = 83160.$$

b) У слові **баран** дві літери **а** і по одній літері **б, р, н**. Слово має 5 літер. Загальна кількість слів

$$N_b = C_5(2, 1, 1, 1) = \frac{5!}{2! \cdot 1! \cdot 1! \cdot 1!} = 60.$$

c) Слово **зебра** містить по одній літері **а, б, з, е, р**. Тоді

$$N_c = C_5(1, 1, 1, 1, 1) = \frac{5!}{1! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = 120.$$

△

2.7 Сполучення з повтореннями

Означення 2.8.
Сполученнями *із* n *елементів по* m *з* ***повтореннями*** *називаються комбінації, що містять* m *елементів без врахування порядку, при цьому кожен елемент може входити у комбінацію декілька разів, але не більше* m *раз.*

Зауваження 2.3.
При утворенні сполучень для 4 *комбінації* ***{a,a,b,a}***, ***{b,a,a,a}*** *не розрізняються, а* ***{a,c,a,a}*** *відрізняється від попередніх.*

Кількість сполучень із n елементів по m з повтореннями рівна

$$\overline{C_n^m} = C_{n+m-1}^m = C_{n+m-1}^{n-1}. \tag{2.6}$$

Задача 2.12.
В кондитерському магазині продавали тістечка 4 *видів: еклер, наполеон, пісочне та струдель. Скільки існує способів вибрати* 7 *тістечок?*

Розв'язання. Кожен спосіб вибору 7 тістечок — це комбінація з повторенням елементів вибору, у якій порядок входження не відіграє ролі. Отже, маємо сполучення із 4 елементів по 7. За формулою (2.6) знаходимо

$$\overline{C_4^7} = C_{10}^7 = \frac{10!}{7! \cdot 3!} = 120.$$

$\triangle$

Задача 2.13.
В ящику знаходяться по 20 *екземплярів кожної із літер* ***{a,b,c,d,e}***. *Скільки існує способів вибрати* ***11*** *літер із ящика, щоб далі утворити з них шифр?*

Розв'язання. Коли вибирають 11 літер з ящика, в якому є літери 5 видів, то деякі з них, якщо не всі, мусять повторюватися. Маємо сполуки із 5 елементів по 11. За (2.6) маємо

$$\overline{C_5^{11}} = C_{15}^{11} = \frac{15!}{11! \cdot 4!} = 1365.$$

$\triangle$

2.8 Питання, тести та вправи до розділу 2

2.8.1 Питання до розділу 2

1. Сформулювати правило суми.
2. Дайте означення правила прямого добутку.
3. Сформулювати правила суми та добутку для k множин.
4. Що таке комбінація із n елементів по m?
5. Дайте означення розміщення із n елементів по m без повторення.
6. Вкажіть формулу обчислення кількості розміщень із n елементів по m без повторення.
7. Що таке перестановки із n елементів без повторення?
8. Як записується формула підрахунку кількості перестановок із n елементів без повторення?
9. Дайте означення сполучення із n елементів по m без повторення.
10. За допомогою якої формули обчислюється кількість сполучень із n елементів по m без повторення?
11. Записати взаємозв'язок між розміщеннями та сполученнями без повторення.
12. Вказати основні властивості комбінацій без повторення (біноміальних коефіцієнтів).
13. Проілюструвати властивості біноміальних коефіцієнтів за допомогою трикутника Паскаля.
14. Дайте означення розміщення із n елементів по m з повтореннями.
15. Записати формулу обчислення розміщень із n елементів по m з повтореннями.
16. Як визначаються перестановки із n елементів з повтореннями.
17. За допомогою якої формули обчислюються кількості перестановок із n елементів з повтореннями?

18. Дати означення сполучення із n елементів по m з повтореннями.

19. Записати формулу обчислення кількості сполучень із n елементів по m з повтореннями.

2.8.2 Тести до розділу 2

Вказати правильну відповідь на кожен тест.

1. Нехай A, B, C – скінчені множини, які не перетинаються і мають потужності $|A| = n$, $|B| = m$, $|C| = k$. Яке твердження вірне:

   (A) $|A \cup B \cup C| = n + m - k$;

   (B) $|A \cup B \cup C| = n \cdot m + k$;

   (C) $|A \cup B \cup C| = n + m + k$.

2. Нехай A – скінченна множина, які має потужність $|A| = n$. Комбінації із n елементів по m можна утворити коли:

   (A) $m < 0$; **(B)** $0 \leqslant m \leqslant n$; **(C)** $m > n$.

3. Нехай A, B, C – скінченні множини, які мають потужності $|A| = n$, $|B| = m$, $|C| = k$. Яке твердження вірне:

   (A) $|A \cap B \cap C| = n + m \cdot k$;

   (B) $|A \cap B \cap C| = n \cdot m \cdot k$;

   (C) $|A \cap B \cap C| = n \cdot m^k$.

4. Нехай A – скінченна множина, які має потужність $|A| = n$. Два розміщення із n елементів по m без повторення будуть різні коли мають:

   (A) лише різні складові;

   (B) або різні складові, або різний порядок входження;

   (C) різну кількість елементів.

5. Нехай A – скінченна множина, які має потужність $|A| = n$. Дві перестановки із n елементів без повторення відрізняються, коли мають:

   (A) різні складові;

   (B) різний порядок входження;

   (C) ніколи.

6. Нехай A — скінченна множина, які має потужність $|A| = n$. Два сполучення із n елементів по m без повторення відрізняються, коли:

   (A) відрізняється порядок входження елементів;

   (B) містять різні елементи;

   (C) завжди.

7. Сума елементів п'ятого рядка трикутника Паскаля рівна

   (A) $\mathbf{17}$; **(B)** $\mathbf{24}$; **(C)** $\mathbf{32}$.

8. Нехай A — скінченна множина, які має потужність $|A| = n$. Кількість розміщень із n елементів по m з повтореннями рівна:

   (A) $\overline{A_n^m} = n^m$;

   (B) $\overline{A_n^m} = n \cdot (n-1) \cdot (n-2) \cdots (n+1-m)$;

   (C) $\overline{A_n^m} = n \cdot (n-m) \cdot (n+1) \cdot (n+2-m)$.

9. Нехай A — скінченна множина, які має потужність $|A| = n$. Кількість перестановок із n елементів з повтореннями, в які елементи групи k, де $k = 1, 2, \cdots, m$, входять n_k разів, $n_1 + n_2 + \cdots + n_m = n$ дорівнює:

   (A) $C_n(n_1, n_2, \ldots, n_m) = \dfrac{n!}{n_1! n_2! \ldots n_m!}$;

   (B) $C_n(n_1, n_2, \ldots, n_m) = n_1^n \cdot n_2^n \cdots n_m^n$;

   (C) $C_n(n_1, n_2, \ldots, n_m) = n^{n_1} \cdot n^{n_2} \cdots n^{n_m}$.

10. Нехай A — скінченна множина, які має потужність $|A| = n$. Кількість сполучень із n елементів по m з повтореннями дорівнює:

    (A) $\overline{C_n^m} = C_{n+m-1}^m$; **(B)** $\overline{C_n^m} = C_{n+m-1}^{m-1}$; **(C)** $\overline{C_n^m} = C_{n+m+1}^{m+1}$.

2.8.3 Вправи до розділу 2

Вправа 2.1.
Шифр сейфу містить $\mathbf{4}$ *значки і складається із малих літер* ***{a;b;c;d;e;f;h}*** *та цифр* ***{2;3;4;5;6}****, що повторюються. Перший значок не може бути цифра, а останній — літера. Скільки різних шифрів можна утворити?*

Вправа 2.2.
Задано множину літер ***{б,в,г,ґ,к,л,м,н,с,т,х,ц}****. Шифр сховища містить різних* $\mathbf{6}$ *літер із вказаної множини. Скільки існує різних шифрів?*

Вправа 2.3.
Диск сейфу містить цифри $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. *Скільки існує* 10*–ти значних шифрів, якщо кожна цифра набирається лише один раз?*

Вправа 2.4.
У підгрупі 7 *студентів. Староста складає графік чергування по два студенти. Скільки різних варіантів графіку чергування можна сформувати?*

Вправа 2.5.
У волейбольній команді ***"Буревісник–УжНУ"*** *нараховується* 18 *спортсменів. Скільки існує можливостей сформувати стартову шістку?*

Вправа 2.6.
Паролем доступу до комп'ютера є 10*–літерне слово у складі якого лише: а) дві літери —* ***{a,b}****; б) лише три літери —* ***{K,L,M}****. Скільки паролів доступу існує?*

Вправа 2.7.
Задана множина літер ***{а, в, д, і, к, л, о }****. Скільки слів, не обов'язково змістовних, що складаються із* ***4*** *літер можна утворити із літер множини, якщо літери можуть повторюватися?*

Вправа 2.8.
Ключ до шифру утворюється в результаті перестановки літер в слові ***диверсифікація****. Скільки існує різних шифрів?*

Вправа 2.9.
Скільки різних слів, не обов'язково змістовних, можна утворити, якщо переставляючи літери у слові ***кардинально****?*

Вправа 2.10.
В пакетику знаходяться по ***20*** *карамельки зі смаком вишні, черешні, яблука, абрикоса та полуниці. Скільки є варіантів взяти із пакетика* ***10*** *карамельок?*

Вправа 2.11.
Розсипані на підлозі лото з літерами ***{а, б, в, г}****. Кожної літери по* ***15*** *штук. Скільки маємо варіантів підняти з підлоги* ***9*** *лото з літерами?*

Розділ 3

Окремі розділи алгебри

Загальна алгебра знайшла своє достойне місце в багатьох областях природознавства. Алгебрична термінологія проникла не тільки у всі розділи математики, а також широко використовується в багатьох областях її застосування ([11, 20]).

3.1 Перестановки. Підстановки

Означення 3.1.
Довільне впорядковане розміщення елементів множини

$$X = \{x_1, x_2, x_3, \ldots, x_n\},$$

тобто розміщення, в якому вказано, який елемент перший, який другий і т.д. називається ***перестановкою*** *множини* X.

Перестановки будемо позначати $(x_1, x_2, \ldots, x_n)$.

Означення 3.2.
Дві перестановки ***однакові****, якщо порядок елементів в них однаковий.*

Приклад 3.1.
Перестановки (a, b, c, d, e), (a, c, d, e, b), (d, e, a, b, c), (a, b, c, e, d) — *різні перестановки множини* $\{a, b, c, d, e\}$.

Візьмемо одну перестановку і перенумеруємо її елементи від 1 до n. Нас цікавить тільки порядок елементів у перестановці.

Теорема 1 (Кількість перестановок).
Різних перестановок, які можна утворити із n *елементів множини* X *дорівнює* $n!$.

Означення 3.3.
Якщо в перестановці $(x_1, x_2, \ldots, x_n)$ *для елементів* x_i *і* x_j *має місце нерівність* $x_i > x_j$ *при* $i < j$, *то пара* (x_i, x_j) *називається* ***інверсією***.

Кількість інверсій у перестановці позначимо $J(x_1, x_2, \ldots, x_n)$.

Означення 3.4.
Перестановка множини X *називається* ***парною***, *якщо кількість інверсій* J *число парне і* ***непарною*** *у протилежному випадку.*

Задача 3.1.
Визначити парність перестановки $Y = (5, 2, 1, 6, 4, 3)$.

Розв'язання. В перестановці Y:

- перед елементом 1 містяться 2 два елементи $5, 2$;
- перед елементом 2 міститься 1 елемент 5;
- перед елементом 3 містяться 3 елементи $5, 6, 4$;
- перед елементом 4 містяться 2 елементи $5, 6$;
- перед елементом 5 містяться 0 елементів;
- перед елементом 6 містяться 0 елементів.

Тоді, $J(5, 2, 1, 6, 4, 3) = 2 + 1 + 3 + 2 + 0 + 0 = 8$. Отже, перестановка парна.

$\triangle$

Означення 3.5.
Будь–яке взаємно–однозначне відображення множини X *в саму себе називається* ***підстановкою*** *цієї множини.*

Зауваження 3.1.
Довільна підстановка може бути подана у вигляді двох перестановок, які записані одна під одною.

Якщо множина скінчена, тобто складається із n елементів $(1, 2, \ldots, n)$, то відображення $\pi : X \to X$ буде **підстановкою n –го степеня** і запишеться

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_n \end{pmatrix}, \quad \text{де } \pi_i = \pi(x_i) \text{ образ } x_i, i = 1, \ldots, n.$$

Означення 3.6.
Тотожною (одиничною) підстановкою e *називається підстановка, яка всі елементи множини переводить самі в себе, тобто*

$$e(x_i) = x_i, \qquad i = 1, 2, \ldots, n,$$

або

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Добуток підстановок $\pi : X \to X$ та $\sigma : X \to X$ визначається як послідовне виконання підстановок π та σ і задається формулою
$\pi\sigma(x) = \pi(\sigma(x)),$ для довільного $x \in X$.

Означення 3.7.
Підстановка π^{-1} *називається* ***оберненою*** *для підстановки* π*, якщо*

$$\pi^{-1}\,\pi = \pi\,\pi^{-1} = e.$$

Означення 3.8.
Добуток $\pi^k = \underbrace{\pi \cdot \ldots \cdot \pi}_{k \text{ разів}}$ *називається* k*–м степенем підстановки* π.

Означення 3.9.
Найменше натуральне число m*, для якого* $\pi^m = e$*, називається* ***порядком підстановки*** π.

Задача 3.2.
Знайти добутки підстановок $\pi\sigma$ *і* $\sigma\pi$ *та обернену підстановку* π^{-1}*, якщо*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

Розв'язання.

$$\pi\sigma = \pi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

$$\sigma\pi = \sigma(\pi) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

$$\pi^{-1} = \begin{pmatrix} 4 & 3 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}.$$

$\triangle$

Задача 3.3.
Знайти підстановку ξ *з рівності* $\pi\xi\sigma = \varphi$, *якщо*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 7 & 4 & 5 & 6 \end{pmatrix},$$

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 6 & 4 & 7 & 2 \end{pmatrix}.$$

Розв'язання. Підстановку

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 & \xi_6 & \xi_7 \end{pmatrix}$$

знайдемо із співвідношення $\xi = \pi^{-1}\varphi\sigma^{-1}$. Знаходимо

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 6 & 5 & 1 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}.$$

Тоді

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 6 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 6 & 4 & 7 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 6 & 7 & 1 & 3 & 5 \end{pmatrix}.$$

Отже, шукана підстановка

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 6 & 7 & 1 & 3 & 5 \end{pmatrix}.$$

$\triangle$

Означення 3.10.
Підстановка π, *яка діє таким чином, що в результаті елементи підстановки* $i_1, i_2, \ldots, i_k$ *переходять за правилом*

$$\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1,$$

а решта елементів підстановки залишаються на своїх місцях, називається ***циклом довжини*** k *і позначається* $(i_1, i_2, \ldots, i_k)$.

Кожна нетотожна підстановка π єдиним способом розкладається на добуток незалежних циклів $\sigma_1, \sigma_2, \ldots, \sigma_r$ (з точністю до перестановки множників).

Порядок m підстановки π дорівнює найменшому спільному кратному довжин циклів в добуток яких вона розкладається.

Задача 3.4.
Знайти π^{100}*, якщо*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}.$$

Розв'язання. Розкладемо підстановку π в добуток циклів

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix} = (1,3,4)(2,5,7)(8,6,10)(9).$$

Довжини незалежних циклів — $3, 3, 3, 1$. Найменше спільне кратне циклів рівне 3. Тоді $\pi^3 = e, \pi^{100} = \pi^{99}\pi = (\pi^3)^{33}\pi = \pi$.

$\triangle$

3.2 Бінарна операція

Означення 3.11.
Нехай $X \neq \varnothing$ *— деяка множина. Кажуть, що* ***бінарна алгебрична операція*** $\circ$ *визначена на множині* X*, якщо кожній упорядкованій парі* (x, y) *елементів множини* X *поставлено у відповідність однозначно визначений елемент* $z \in X$*. Цей елемент* $z = x \circ y$ *називають* ***композицією*** *елементів* x, y *відносно даної алгебричної операції.*

Якщо $X = \{x_1, x_2, \ldots, x_n\}$ — скінчена множина, то алгебричну операцію можна записати за допомогою таблиці Кейлі .

Таблиця Кейлі

$\circ$	x_1	x_2	x_3	x_4	$\ldots$	x_n
x_1	z_{11}	z_{12}	z_{13}	z_{14}	$\cdots$	z_{1n}
x_2	z_{21}	z_{22}	z_{23}	z_{24}	$\cdots$	z_{2n}
x_3	z_{31}	z_{32}	z_{33}	z_{34}	$\cdots$	z_{3n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	z_{n1}	z_{n2}	z_{n3}	z_{n4}	$\cdots$	z_{nn}

Означення 3.12.
Нейтральним елементом *відносно визначеної алгебричної операції* $\circ$ *називається елемент* $\boldsymbol{n \in X}$*, що для будь–якого елемента* $\boldsymbol{x \in X}$ *виконується рівність* $\boldsymbol{n \circ x = x \circ n = x}$*.*

Означення 3.13.
Алгебрична операція називається:

- ***комутативною****, якщо* $\boldsymbol{x \circ y = y \circ x}$*,*
- ***асоціативною****, якщо* $\boldsymbol{(x \circ y) \circ z = x \circ (y \circ z)}$*, де* $\boldsymbol{x, y, z}$ *— довільні елементи множини* $\boldsymbol{X}$*.*

Означення 3.14.
Елемент $\boldsymbol{x \in X}$ *називається* ***симетричним*** *до елемента* $\boldsymbol{y \in X}$ *відносно алгебричної операції* $\circ$*, якщо* $\boldsymbol{x \circ y = y \circ x = n}$*, де* $\boldsymbol{n}$ *— нейтральний елемент.*

Часто зручно і природно називати алгебричну операцію **додаванням** або **множенням** і позначати $\oplus$ та $\otimes$.

Операція	**Композиція**	**Нейтральний елемент**	**Симетричний елемент**
Множення $\otimes$	**добуток елементів** xy	**одиниця** **1 або** e	**обернений** x^{-1}
Додавання $\oplus$	**сума елементів** $x + y$	**нуль** 0	**протилежним** $-x$

Задача 3.5.
На множині натуральних чисел $\mathbb{N}$ *задана алгебрична операція наступним чином* $\boldsymbol{a \circ b = \max\{a, b\}}$*. З'ясувати, чи ця операція: комутативна, асоціативна, чи існує нейтральний елемент?*

Розв'язання. 1) Оскільки для довільних натуральних чисел $\boldsymbol{a, b \in \mathbb{N}}$ максимальний елемент також буде натуральним числом, то визначена бінарна операція на $\mathbb{N}$.

2) Виконується співвідношення $\boldsymbol{\max\{a, b\} = \max\{b, a\}}$. Отже, операція комутативна.

3) Вірною є рівність $\boldsymbol{\max\{\max\{a, b\}, c\} = \max\{a, \max\{b, c\}\}}$. Звідси робимо висновок, що операція асоціативна.

4) Для довільного $\boldsymbol{a \in \mathbb{N}}$ вірним є $\boldsymbol{\max\{1, a\} = \max\{a, 1\} = a}$. Отже, існує нейтральний елемент відносно введеної операції.

△

Задача 3.6.
Множина $A = \{2, 3, 5, 7, 11, 13, 17\}$ *містить перші 7–м простих чисел. Скласти таблицю Кейлі операції* $\odot$*, яка визначена на множині* A *наступним чином* $x \odot y = \min\{x, y\}$*. За допомогою побудованої таблиці з'ясувати: чи операція бінарна, чи операція комутативна, чи операція асоціативна, чи існує відносно операції нейтральний елемент?*

Розв'язання.
Утворимо табличку Кейлі вказаної операції.

$\odot$	2	3	5	7	11	13	17
2	2	2	2	2	2	2	2
3	2	3	3	3	3	3	3
5	2	3	5	5	5	5	5
7	2	3	5	7	7	7	7
11	2	3	5	7	11	11	11
13	2	3	5	7	11	13	13
17	2	3	5	7	11	13	17

Із побудованої таблиці безпосередньо випливає:

1) Що задана операція є бінарною операцією на множині A. Результат операції, композиція двох довільних елементів із множини є елемент, який належить множині.

2) Розглянута операція комутативна та асоціативна.

3) Нейтрального елемента не існує.

△

3.3 Група

Означення 3.15.
Групою *називається непорожня множина* G*, на якій визначена бінарна алгебрична операція* $\circ$*, що називається* ***груповою****, і задовольняє умови (аксіоми групи):*

1. *кожній упорядкованій парі* $(a; b)$ *елементів множини* G *однозначно поставлено у відповідність за допомогою введеної алгебричної операції визначений елемент* $c \in G$*, що записується як* $a \circ b = c$ *(****аксіома замкненості****);*

2. *операція $\circ$ асоціативна, тобто для будь–яких елементів a, b, c виконується $(a \circ b) \circ c = a \circ (b \circ c)$ (**аксіома асоціативності**);*

3. *у множині G існує нейтральний елемент e відносно введеної операції, тобто $a \circ e = e \circ a = a$, де $a \in G$ (**аксіома існування нейтрального елемента**);*

4. *для кожного елемента a множини G у цій множині існує симетричний елемент (**аксіома існування симетричного елемента**).*

Якщо в додаток до умов (аксіом групи) групова операція буде ще і комутативної, тобто $a \circ b = b \circ a$, то група називається **комутативною** або **абелевою**.

Групу називають **мультиплікативною**, якщо в ній групова операція є множення і **адитивною**, якщо групова операція є додавання.

Означення 3.16.
*Якщо у групі скінчена кількість елементів, то її називають **скінченною**, а кількість елементів — порядком і позначають $|G|$. В протилежному випадку, коли група має нескінчену кількість елементів її називають **нескінченною***
.

Приклад 3.2.
Маємо множини:

- *Множина цілих чисел $\mathbb{Z}$ буде адитивна група.*
- *Множина $\mathbb{Z}$ не є мультиплікативна група, бо для цілих чисел відмінних від ± 1 не існує обернених елементів, що належать $\mathbb{Z}$.*
- *Множина раціональних чисел $\mathbb{Q}$ буде адитивна група.*
- *Множина $\mathbb{Q}$ не буде мультиплікативна група, бо ділення на нуль неможливе.*
- *Якщо вилучити нуль з $\mathbb{Q}$, то множина всіх раціональних чисел відмінних від нуля, тобто $\mathbb{Q}\backslash\{0\}$, стане і мультиплікативною групою.*
- *Множини $\mathbb{R}$ та $\mathbb{C}$ — нескінчені адитивні абелеві групи дійсних та комплексних чисел відповідно.*
- *Множини всіх відмінних від нуля дійсних та комплексних чисел — мультиплікативні абелеві групи дійсних та комплексних чисел — $\mathbb{R}\backslash\{0\}$, $\mathbb{C}\backslash\{0\}$.*

- *Множина всіх невироджених квадратних матриць порядку n — нескінчена не комутативна мультиплікативна група.*

- *Множина всіх підстановок множини $\boldsymbol{X = \{1; 2; 3; \ldots; n\}}$ — скінченна мультиплікативна група, яку називають **симетричною групою** степеня $\boldsymbol{n}$ і позначають $\boldsymbol{S_n}$. Роль одиничного елемента в цій групі відіграє тотожна підстановка. Підстановка $\boldsymbol{\pi^{-1}}$ буде оберненим елементом до підстановки $\boldsymbol{\pi \in S_n}$. Симетрична група $\boldsymbol{S_2}$ степеня 2 — абелева, а при $\boldsymbol{n \geqslant 3}$, група $\boldsymbol{S_n}$ не буде абелева. Порядок симетричної групи — $\boldsymbol{|S_n| = n!}$.*

Задача 3.7.
На множині парних цілих чисел визначена операція додавання. З'ясувати, чи буде множина: а) групою? б) абелевою групою?

Розв'язання. Маємо множину $\boldsymbol{A = \{a : a = 2k, k \in \mathbb{Z}\}}$. Виберемо довільні три елемента $\boldsymbol{a = 2k, b = 2m, c = 2n}$, що належать $\boldsymbol{A}$. Групова операція — додавання чисел $+$. Перевіримо виконання всіх аксіом групи.

1) При довільних значеннях $\boldsymbol{k, m \in \mathbb{Z}}$ як результат суми двох парних чисел $\boldsymbol{a + b = 2k + 2m = 2(k + m)}$ отримуємо парне ціле число. Аксіома замкненості виконується.

2) Оскільки $\boldsymbol{(a + b) + c = 2(k + m) + 2n = 2(k + m + n)}$, а також $\boldsymbol{a + (b + c) = 2k + 2(m + n) = 2(k + m + n)}$, то виконується аксіома асоціативності.

3) Якщо $\boldsymbol{k = 0}$, то $\boldsymbol{a = 0 \in A}$. Число $\boldsymbol{0}$ буде виконувати роль *нейтрального елемента*, оскільки $\boldsymbol{0 + a = a + 0 = a}$ для довільного $\boldsymbol{a \in A}$. Аксіома існування нейтрального елемента справедлива.

4) Враховуючи, що якщо $\boldsymbol{a \in A}$, то $\boldsymbol{-a = 2(-k) \in A}$ і має місце співвідношення $\boldsymbol{a + (-a) = 0}$, приходимо до висновку, що аксіома існування симетричного елемента також вірна.

Отже, множина $\boldsymbol{A}$ є групою.

Крім того $\boldsymbol{a + b = 2(k + m) = b + a}$, тобто групова операція комутативна. Тоді $\boldsymbol{A}$ — **адитивна абелева група**.

$\triangle$

Означення 3.17.
*Якщо деяка підмножина $\boldsymbol{H}$ групи $\boldsymbol{G}$ відносно введеної групової операції сама утворює групу, то $\boldsymbol{H}$ називається **підгрупою** групи $\boldsymbol{G}$.*

Підгрупи групи G, які відмінні від її тривіальних підгруп $\{e\}$ та G називаються **власними підгрупами групи G**.

Теорема 2 (Перетин підгруп).
Якщо група G має підгрупи H_1 та H_2, то перетин підгруп $H_1 \cap H_2$ також буде підгрупою групи G.

Приклад 3.3.
Наведемо приклади.

- *Адитивна група всіх парних чисел буде власною підгрупою групи всіх цілих чисел.*
- *Адитивна група всіх цілих чисел буде власною підгрупою в адитивній групі всіх дійсних чисел.*
- *Множина всіх парних підстановок з n чисел утворює власну підгрупу симетричної групи підстановок S_n.*

Задача 3.8.
Задана множина $A = \{a : a = 3n, n \in \mathbb{Z}\}$. Показати, що A власна підгрупа адитивної групи цілих чисел.

Розв'язання. Очевидно, що $A \subset \mathbb{Z}$. Перевіримо, що множина A є адитивна група.

1) Аксіома замкненості виконується, оскільки, якщо $a = 3n, b = 3m$, де $n, m \in \mathbb{Z}$, то $a + b = 3(n + m) \in A$.

2) Якщо $c = 3k$, то $(a + b) + c = a + (b + c) = 3(n + m + k)$. Отже, аксіома асоціативності також має місце.

3) Нейтральним елементом буде $e = 0 = 3 \cdot 0$.

4) Аксіома існування симетричного елемента виконується. Симетричним для довільного елемента $a = 3n$ буде елемент $(-a) = 3(-n)$.

Аксіоми групи для множини A вірні, отже A власна підгрупа адитивної групи цілих чисел.

$\triangle$

3.4 Гомоморфізм та ізоморфізм груп

Означення 3.18.
Нехай G_1 та G_2 — дві групи із груповими операціями $\circ$ та $\bullet$ відповідно.

Кажуть, що відображення $f : G_1 \to G_2$ зберігає групову операцію, якщо для всіх елементів $a, b \in G_1$ виконується рівність $f(a \circ b) = f(a) \bullet f(b)$, а саме відображення при цьому називається ***гомоморфізмом*** *з групи G_1 у групу G_2.*

Означення 3.19.
Множина елементів $a \in G_1$, для яких $f(a) = e'$, де e' — нейтральний елемент групи G_2, називається ***ядром*** $\ker f$ ***гомоморфізму*** $f : G_1 \to G_2$.

Основні властивості гомоморфізму

- Нейтральному елементу групи G_1 ставиться у відповідність нейтральний елемент групи G_2.
- Якщо елементу $a \in G_1$ відповідає елемент $a_1 = f(a) \in G_2$, то елементу $a^{-1} \in G_1$ буде відповідати $a_1^{-1} \in G_2$.

Теорема 3 (Ядро гомоморфізму).
Нехай f — гомоморфізм з групи G_1 у групу G_2 і $H = \ker f$ — ядро гомоморфізму. Тоді H — підгрупа групи G_1.

Означення 3.20.
Якщо гомоморфізм є ще і взаємно однозначне відображення, то він називається ***ізоморфізмом*** *.*

Означення 3.21.
Якщо існує ізоморфізм групи G_1 на групу G_2, то кажуть, що група G_1 ізоморфна групі G_2 та записують $G_1 \cong G_2$.

Приклад 3.4.
Вкажемо ізоморфізми груп.

- *Ізоморфні між собою* ***адитивна група цілих чисел*** *та* ***адитивна група парних чисел****, хоча друга є підгрупою першої. Відображення, яке ставить довільному цілому числу n парне число $2n$ є взаємно однозначне.*
- *Мультиплікативна група всіх додатних дійсних чисел*

$$\mathbb{R}^+ = \{x : x \in \mathbb{R}, x > 0\}$$

ізоморфна адитивній групі всіх дійсних чисел $\mathbb{R}$, бо кожному додатному числу a можна поставити у відповідність число $\ln a \in \mathbb{R}$. Таке відображення зберігає групову операцію $\ln(ab) = \ln a + \ln b$.

З погляду алгебри ізоморфні групи не відрізняються, бо відображення, яке породжує ізоморфізм, як дзеркало, переводить елементи і групову операцію однієї групи в елементи і групову операцію іншої групи.

3.5 Кільця і поля

Означення 3.22.
Кільце *— це множина K, на якій визначені дві бінарні алгебричні операції* ***додавання*** *та* ***множення****, при цьому:*

- *для будь-яких елементів $a, b, c \in K$ виконується*
  $(a + b) + c = a + (b + c)$ *— додавання асоціативне;*
- *існує елемент $0 \in K$, що для будь–якого елемента $a \in K$ виконується рівність $a + 0 = 0 + a = a$ — існування нуля;*
- *для будь–якого елемента $a \in K$ існує обернений елемент $(-a)$, такий, що*
  $a + (-a) = 0$ *— існування оберненого елемента відносно додавання;*
- $a + b = b + a$ *— додавання комутативне;*
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *— множення асоціативне;*
- $a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c$ *— множення дистрибутивне ліворуч та праворуч.*

Означення 3.23.
Кільце називається ***комутативним****, якщо виконується властивість комутативності множення. Тобто $a \cdot b = b \cdot a$.*

Означення 3.24.
Комутативне кільце, на якому виконується властивість існування одиниці, тобто існує $e \in K$, що $e \cdot a = a \cdot e = a$, називається ***кільцем з одиницею****.*

Приклад 3.5.
Розглянемо множини:

1. *Множина цілих чисел $\mathbb{Z}$, множина раціональних чисел $\mathbb{Q}$, множина дійсних чисел $\mathbb{R}$, множина комплексних чисел $\mathbb{C}$ є прикладами кілець із звичайними **додаванням** та **множенням** чисел.*

2. *Множина цілих чисел $n\mathbb{Z}$, які кратні натуральному числу n.*

3. *Комутативне кільце з одиницею утворює арифметика цілих чисел на комп'ютері.*

4. *Множина додатних чисел не буде кільцем, бо для $a > 0, b > 0$ або $a - b < 0$, або $b - a < 0$, а отже не належить множині додатних дійсних чисел.*

5. *Не буде кільцем множина від'ємних дійсних чисел, бо їх добуток буде число додатне.*

6. *Некомутативним кільцем буде множина квадратних матриць із дійсними елементами фіксованого порядку n із звичайними операціями додавання та множення матриць. Кільце позначають $M_n(\mathbb{R})$. Роль одиниці в ньому відіграє одинична матриця.*

Означення 3.25.
*Два елементи кільця, добуток яких рівний нулю, хоча кожен із них відмінний від нуля, називаються **дільниками нуля**.*

Якщо кільце не містить дільників нуля, то його називають **кільцем без дільників нуля**, а інакше — **кільцем з дільниками нуля**.

Так кільце квадратних матриць $M_n(\mathbb{R})$ буде кільцем із дільниками нуля. Наприклад, якщо $n = 2$, то

$$\begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & -9 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Жодна із матриць не є нульовою матрицею, а результат добутку цих матриць є нульова матриця.

У кільці виконуються співвідношення:

- $0 \cdot a = a \cdot 0 = 0$;
- $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;
- $(-a) \cdot (-b) = a \cdot b$.

Означення 3.26.
Елемент a^{-1} кільця K з одиницею називається ***оберненим*** *до елемента $a \in K$, якщо $a \cdot a^{-1} = a^{-1} \cdot a = e$. Сам елемент a в такому разі називається* ***оборотним****.*

Означення 3.27.
Поле *— це множина F, на якій визначені дві бінарні алгебричні операції додавання та множення, при цьому:*

- *для будь-яких елементів $a, b, c \in F$ виконується $(a + b) + c = a + (b + c)$ — додавання асоціативне;*
- *існує елемент $0 \in F$, що для будь–якого елемента $a \in F$ виконується рівність $a + 0 = 0 + a = a$ — існування нуля;*
- *для будь–якого елемента $a \in F$ існує обернений елемент $(-a)$, такий, що $a + (-a) = 0$ — існування оберненого елемента відносно додавання;*
- *$a + b = b + a$ — додавання комутативне;*
- *$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ — множення асоціативне;*
- *існує такий елемент $1 \in F$, що $1 \cdot a = a \cdot 1 = a$ — існування одиниці;*
- *для кожного $a \in F$ існує обернений елемент a^{-1}, що $a^{-1} \cdot a = a \cdot a^{-1} = 1$ — існування оберненого елемента відносно множення;*
- *$a \cdot b = b \cdot a$ — множення комутативне;*
- *$a \cdot (b + c) = a \cdot b + a \cdot c$ — множення дистрибутивне відносно додавання.*

Із означення випливає:

- поле F — комутативна група за додаванням, нейтральним елементом якої є нуль;
- множина ненульових елементів не порожня та утворює комутативну мультиплікативну групу, одиничний елемент якої — 1.

Комутативну мультиплікативну групу поля F прийнято позначати як F^* (тобто $F^* = F \backslash \{0\}$).

Приклад 3.6.
Наведемо приклади полів.

1. *Поле дійсних чисел* $\mathbb{R}$*;*
2. *Поле раціональних чисел* $\mathbb{Q}$*;*
3. *Поле комплексних чисел* $\mathbb{C}$*.*

Співвідношення в полі

- $(-a) = a \cdot (-1)$;
- $-(a + b) = (-a) + (-b)$;
- якщо $a \neq 0$, то $(a^{-1})^{-1} = a$;
- якщо $a \cdot b = 0$, то $a = 0$ або $b = 0$ — властивість відсутності дільників нуля;
- якщо $a \neq 0$, то у полі єдиним способом розв'язується рівняння $a \cdot x + b = 0$ і його розв'язок $x = -(a^{-1}) \cdot b$.

3.6 Питання, тести та вправи до розділу 3

3.6.1 Питання до розділу 3

1. Дайте означення перестановки множини $X, |X| = n$.
2. Які дві перестановки однакові?
3. Нехай $X, |X| = n$. Скільки існує різних перестановок?
4. Що таке інверсія елементів перестановка? Як підраховується кількість інверсій в перестановці?
5. Дайте означення парної та непарної перестановки.
6. Що називається підстановкою множини $X, |X| = n$?
7. Яка підстановка буде тотожною (одиничної)?
8. Що розуміється під добутком підстановок?
9. Дайте означення оберненої підстановки.

10. Як визначається степінь підстановки? Що таке порядок підстановки?
11. Що розуміти під циклом підстановки?
12. Сформулюйте означення бінарної операції на множині.
13. Яка бінарна операція буде комутативна? Яка буде асоціативна?
14. Дайте означення нейтрального та симетричного елемента відносно бінарної операції.
15. Який вигляд має таблиця Кейлі для бінарної операції?
16. Дайте означення групи.
17. Яка група називається абелевою, мультиплікативною, адитивною?
18. Що таке порядок групи?
19. Дайте означення підгрупи.
20. Яке відображення називається гомоморфізмом?
21. Вкажіть властивості гомоморфізму.
22. Дайте означення ізоморфізму.
23. Яка множина називається кільцем?
24. Вказати, коли кільце називається комутативним.
25. Дайте означення кільця з одиницею.
26. Які елементи кільця називають дільниками нуля?
27. В якому випадку говорять про кільце без дільників нуля?
28. Який елемент кільця називається оборотним елементом?
29. Які співвідношення виконуються в кільці?
30. Дайте означення поля.
31. Вкажіть співвідношення в полі.

3.6.2 Тести до розділу 3

Вказати правильну відповідь на кожен тест.

1. Нехай $\boldsymbol{X}$ — перестановка. Яке твердження вірне:

   (A) Порядок елементів в $\boldsymbol{X}$ вказаний;

   (B) Порядок елементів в $\boldsymbol{X}$ довільний;

   (C) Порядок елементів в $\boldsymbol{X}$ не важливий.

2. Задано дві перестановки $\boldsymbol{X_1 = (a, b, c, d)}$ та $\boldsymbol{X_2 = (d, c, b, a)}$. Вказані перестановки:

   (A) однакові; **(B)** різні; **(C)** подібні.

3. Нехай задана множина $\boldsymbol{A = (1, 3, 5, 7, 9)}$. Кількість різних перестановок множини рівна:

   (A) $\mathbf{90}$; **(B)** $\mathbf{96}$; **(C)** $\mathbf{120}$.

4. Задана перестановка $\boldsymbol{X_1 = (4, 2, 8, 10, 6)}$. Кількість інверсій в перестановці дорівнює:

   (A) $\mathbf{2}$; **(B)** $\mathbf{3}$; **(C)** 4.

5. Задана перестановка $\boldsymbol{(x_1, x_2, x_3, \ldots, x_n)}$. Яке твердження вірне:

   (A) Перестановка парна, якщо $\boldsymbol{n}$ парне число;

   (B) Перестановка непарна, якщо $\boldsymbol{n}$ непарне число;

   (C) Перестановка парна, якщо число інверсій $\boldsymbol{J(x_1, x_2, x_3, \ldots, x_n)}$ парне число.

6. Яке твердження вірне:

   (A) Підстановка — це довільне відображення множини $\boldsymbol{X}$ в $\boldsymbol{X}$;

   (B) Підстановка — це взаємно–однозначне відображення множини $\boldsymbol{X}$ саму у себе;

   (C) Підстановка — це довільне перетворення множини $\boldsymbol{X}$.

7. Нехай $\boldsymbol{\pi}$ — підстановка. Підстановка $\boldsymbol{\pi^{-1}}$ буде обернена для $\boldsymbol{\pi}$, якщо

   (A) $\boldsymbol{\pi + \pi^{-1} = e}$; **(B)** $\boldsymbol{\pi\pi^{-1} = \pi^{-1}\pi = e}$; **(C)** $\boldsymbol{\pi\pi^{-1} = 0}$.

8. Запис π^k означає:

   (A) $\pi^k = \underbrace{\pi\pi\ldots\pi}_{k \text{ раз}}$; **(B)** $\pi^k = \underbrace{\pi+\pi+\cdots+\pi}_{k \text{ раз}}$; **(C)** $\pi^k = k \cdot \pi$.

9. Порядком підстановки π називається :

   (A) Найменше натуральне число m, для якого $\pi^m = e$;

   (B) Найбільше натуральне число m, для якого $\pi^m = e$;

   (C) Деяке натуральне число m, для якого $\pi^m = e$.

10. Нехай підстановка π є циклом $(i_1, i_2, \ldots, i_k)$. Яке твердження вірне:

    (A) Елементи циклу можна перемішувати довільним чином;

    (B) Елементи циклу не можна перемішувати;

    (C) Елементи циклу можна перемішувати лише по циклу.

11. Нехай на X визначено бінарну операцію $\circ$, так що $z = x \circ y$, коли $x, y \in X$. Тоді:

    (A) $z \in X$; **(B)** $z \notin X$; **(C)** $z \in Y$.

12. Нехай на X визначено бінарну операцію $\circ$. Тоді елемент $n \in X$, такий що $n \circ x = x \circ n = x, x \in X$ називається:

    (A) симетричним; **(B)** нейтральним; **(C)** нульовим.

13. Нехай на X визначено бінарну операцію $\circ$. Тоді елемент $y \in X$, такий що $y \circ x = x \circ y = n, x, n \in X$, де n — нейтральний елемент, називається:

    (A) симетричним; **(B)** нейтральним; **(C)** нульовим.

14. Нехай G — група з груповою операцією $\circ$. Тоді G буде абелева група, якщо:

    (A) $a \circ b = 0$; **(B)** $a \circ b = n$; **(C)** $a \circ b = b \circ a$.

15. Нехай G — група з груповою операцією $\circ$. Множина H буде підгрупа, якщо:

    (A) $H \subset G$;

    (B) $H \subset G$ і відносно групової операції утворює групу;

    (C) на множині визначена групова операція.

16. Якщо $f : G_1 \to G_2$ — гомоморфізм, то:
    (A) зберігається групова операція;
    (B) групи однакові;
    (C) не відбувається збереження групової операції.

17. Якщо $f : G_1 \to G_2$ — ізоморфізм, то це гомоморфізм, який є:
    (A) взаємно–однозначне відображення;
    (B) еквівалентне відображення;
    (C) обернено–зворотнє відображення.

18. Нехай K — кільце. В кільці визначено:
    (A) $\mathbf{1}$ операція; **(B)** $\mathbf{2}$ операції; **(C)** $\mathbf{3}$ операції.

19. Нехай K — кільце. Кільце буде комутативне, якщо:
    (A) $a + b = b + a$; **(B)** $a \cdot b = b \cdot a$; **(C)** $a \cdot b = e$.

20. Нехай K — кільце. Кільце буде кільцем з одиницею, якщо:
    (A) воно комутативне і знайдеться $e \in K$, що $e \cdot a = a \cdot e = a$;
    (B) знайдеться $e \in K$, що $e + a = a + e = a$;
    (C) знайдуться $a, b \in K$, що $a \cdot b = e$.

21. Нехай K — кільце з одиницею. Елемент a^{-1} кільця обернений до елемента $a \in K$, якщо:
    (A) $a + a^{-1} = 0$; **(B)** $a \cdot a^{-1} = 0$; **(C)** $a \cdot a^{-1} = e$.

22. Нехай F — поле. В полі визначено бінарних операцій:
    (A) 0; **(B)** 1; **(C)** 2.

23. Нехай F — поле. В полі дільників нуля:
    (A) немає; **(B)** лише два; **(C)** довільна кількість.

3.6.3 Вправи до розділу 3

Вправа 3.1.
Визначити парності перестановок:

$$a)\ X_1 = (3, 5, 7, 1, 4, 8, 2, 6); \quad b)\ X_2 = (6, 8, 1, 5, 2, 9, 3, 10, 7, 4).$$

Вправа 3.2.
Знайти добутки підстановок $\pi\sigma$ і $\sigma\pi$ та обернені підстановки π^{-1} та σ^{-1}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 6 & 3 & 1 & 5 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

Вправа 3.3.
Знайти добутки підстановок $\pi\sigma$ і $\sigma\pi$ та обернені підстановки π^{-1} та σ^{-1}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 5 & 3 & 1 & 2 & 4 & 7 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 2 & 5 & 4 & 6 \end{pmatrix}.$$

Вправа 3.4.
Знайти підстановку ξ з рівності $\pi\xi\sigma = \varphi$, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 9 & 1 & 4 & 7 & 5 & 6 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 5 & 9 & 3 & 8 & 7 & 1 & 2 \end{pmatrix},$$

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 1 & 4 & 8 & 9 & 2 & 5 & 6 \end{pmatrix}.$$

Вправа 3.5.
Знайти підстановку ξ з рівності $\pi\xi\sigma = \varphi$, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 10 & 6 & 9 & 4 & 3 & 1 & 2 & 7 & 5 \end{pmatrix},$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 4 & 7 & 2 & 9 & 8 & 10 & 3 & 1 \end{pmatrix},$$

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 6 & 7 & 9 & 8 & 3 & 5 & 10 & 1 \end{pmatrix}.$$

Вправа 3.6.
Знайти π^{182}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 4 & 7 & 11 & 8 & 9 & 10 & 3 & 12 & 1 & 2 \end{pmatrix}.$$

Вправа 3.7.
Обчислити π^{241}, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 9 & 12 & 14 & 15 & 1 & 2 & 3 & 6 & 11 & 8 & 5 & 10 & 4 & 7 & 13 \end{pmatrix}.$$

Вправа 3.8.
На множині цілих чисел $\mathbb{Z}$ визначена алгебрична операція наступним чином $a \circ b = a - b$. З'ясувати, чи ця операція: комутативна, асоціативна, чи існує нейтральний елемент?

Вправа 3.9.
На множині цілих чисел $\mathbb{Z}$ визначена алгебрична операція наступним чином $a \circ b = a \times b$. З'ясувати, чи ця операція: комутативна, асоціативна, чи існує нейтральний елемент?

Вправа 3.10.
Множина $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Алгебрична операція визначена наступним чином $a \circ b = 7 - \max\{a, b\}$. Скласти для операції таблицю Кейлі і за допомогою побудованої таблиці з'ясувати: чи операція бінарна, чи операція комутативна, чи операція асоціативна, чи існує відносно операції нейтральний елемент?

Вправа 3.11.
Множина $A = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$. На множині визначена алгебрична операція наступним чином $a \circ b = |a - b|$. Сформувати відносно операції таблицю Кейлі і за допомогою побудованої таблиці з'ясувати: чи операція бінарна, чи операція комутативна, чи операція асоціативна, чи існує відносно операції нейтральний елемент?

Вправа 3.12.
З'ясувати чи множина додатних дійсних чисел $\mathbb{R}^+$ утворює групу відносно операції множення. Визначити чи буде група абелева.

Вправа 3.13.
Дослідити чи множина раціональних чисел, знаменниками яких є степені числа 2 з цілими невід'ємними показниками, відносно операції множення утворює групи. У випадку позитивної відповіді з'ясувати, чи буде група абелева.

Вправа 3.14.
Показати, що множина

$$nZ = \{a : a = n \cdot k, n, k \in \mathbb{Z}, n - \text{фіксоване}\}$$

буде власною підгрупою адитивної групи цілих чисел.

Розділ 4

Елементи теорії чисел

Теорію чисел часом ще називають вищою арифметикою. Теорія чисел бере свої початки з вивчення властивостей натуральних чисел та питань подільності і розв'язання алгебричних рівнянь у натуральних числах. В теорії чисел також розглядаються функції різноманітного походження, які пов'язані з арифметикою цілих чисел та їх узагальнень ([1, 5, 8, 18, 22, 25]).

4.1 Подільність чисел

Розділ математики **теорія чисел** вивчає цілі числа. До цілих чисел відносять $0, -1, +1, -2, +2, -3, +3, \dots$. Множину цілих чисел, як відомо, традиційно позначають через

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}.$$

У множині цілих чисел $\mathbb{Z}$ сума $a + b$, різниця $a - b$ та добуток $a \cdot b$ чисел також будуть цілими числами, проте частка a/b від ділення a на $b, b \neq 0$, може і не бути цілим числом.

Те, що частка a/b – ціле число, позначають як $a = qb$, де $q \in \mathbb{Z}$ – ціле число. Число b називають **дільником** числа a, число a – **кратним** числа b, що стисло записують: або $b|a$ або $a \vdots b$.

В теорії подільності цілих чисел важливе місце займає наступне твердження.

Теорема 4 (Подільність з остачею).
Довільне число $a \in \mathbb{Z}$ єдиним чином можна подати у вигляді

$$a = bq + r, \qquad 0 \leqslant r < b, \qquad \text{де} \quad b, q, r \in \mathbb{Z}.$$

Число r називається **остачею від ділення**, а q — **неповною часткою**. Далі будемо розглядати лише **додатні дільники**.

Означення 4.1.
*Будь–яке ціле число d, на яке діляться одночасно цілі числа $a_1, a_2, \ldots, a_k$, називається їх **спільним дільником**.*

Числа можуть мати декілька спільних дільників.

Означення 4.2.
*Ціле число $d \neq 0$ називається **найбільшим спільним дільником (НСД)** чисел $a_1, a_2, \ldots, a_k$, якщо виконуються умови:*

1. *кожне із чисел $a_1, a_2, \ldots, a_k$ ділиться на d;*
2. *якщо $d_1 \neq 0$ — інший спільний дільник чисел $a_1, a_2, \ldots, a_k$, то d ділиться на d_1.*

***НСД** чисел $a_1, a_2, \ldots, a_k$ позначають **НСД**$(a_1, a_2, \ldots, a_k)$,*

Означення 4.3.
*Якщо **НСД**$(a_1, a_2, \ldots, a_k) = 1$, то числа називаються **взаємно простими**.*

Приклад 4.1.
*Так як **НСД**$(30, 20) = 10$, то числа 20 та 30 не є взаємно–простими, а оскільки **НСД**$(16, 27) = 1$, то числа 16 і 27 взаємно прості числа.*

Означення 4.4.
*Числа $a_1, a_2, \ldots, a_k$ називаються **попарно простими**, якщо при довільних $i \neq j, i, j = 1, 2, \ldots, k$, числа a_i та a_j взаємно прості.*

Із означення випливає, що попарно прості числа водночас будуть взаємно простими числами, але обернене твердження, взагалі кажучи, невірне.

Приклад 4.2.
*Числа $10, 14, 35$ — взаємно прості, позаяк **НСД**$(10, 14, 35) = 1$. Але числа не є попарно простими, оскільки **НСД**$(10, 14) = 2$, **НСД**$(10, 35) = 5$, **НСД**$(14, 35) = 7$.*

Приклад 4.3.
*Числа $(13, 14, 27)$ — попарно прості, бо **НСД**$(13, 14) = 1$, **НСД**$(13, 27) = 1$, **НСД**$(14, 27) = 1$. Звідки випливає, що дані три числа — взаємно прості.*

Властивості найбільшого спільного дільника чисел.

1. Якщо $a = bq$, то $\mathbf{НСД}(a, b) = b$.
2. Якщо $a = bq + r$, то спільні дільники чисел a і b збігаються із спільними дільниками чисел b і r. Зокрема $\mathbf{НСД}(a, b) = \mathbf{НСД}(b, r)$.
3. Для будь–якого додатного цілого числа m справджується рівність $\mathbf{НСД}(am, bm) = m \cdot \mathbf{НСД}(a, b)$.
4. Якщо $\mathbf{НСД}(a, b) = 1$, то $\mathbf{НСД}(ac, b) = \mathbf{НСД}(c, b)$.
5. Якщо $\mathbf{НСД}(a, b) = 1$ і $ac \vdots b$, то $c \vdots b$.

4.2 Алгоритм Евкліда знаходження найбільшого спільного дільника двох цілих чисел

Найбільший спільний дільник двох цілих чисел можна визначити за **евклідовим алгоритмом**.

Нехай a і b — цілі додатні числа і для визначеності $a > b$. Складемо низку рівностей:

$$\begin{array}{cc}
a = bq_1 + r_1, & 0 < r_1 < b; \\
b = r_1 q_2 + r_2, & 0 < r_2 < r_1; \\
r_1 = r_2 q_3 + r_3, & 0 < r_3 < r_2; \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}; \\
r_{n-2} = r_{n-1} q_n & r_n = 0.
\end{array}$$

Остання рівність, $r_n = 0$, обов'язково виконується, бо

$$b > r_1 > r_2 > \cdots > r_{n-1} > r_n = 0$$

послідовність спадних цілих чисел і не може містити більше, ніж b додатних чисел.

Із вказаних формул та властивостей **НСД** випливає, що

$$\mathbf{НСД}(a, b) = \mathbf{НСД}(b, r_1) = \mathbf{НСД}(r_1, r_2) = \cdots$$

$$\cdots = \mathbf{НСД}(r_{n-2}, r_{n-1}) = \mathbf{НСД}(r_{n-1}, 0) = r_{n-1}. \qquad (4.1)$$

Теорема 5 (НСД чисел).
Найбільший спільний дільник чисел a *та* b *рівний останній, відмінній від нуля, остачі* r_{n-1} *в ряді рівностей* (4.1) *вказаного алгоритму. Тобто*

$$НСД(a,b) = r_{n-1}.$$

Задача 4.1.
Знайти найбільший спільний дільник чисел ***4171*** *і* ***18527****.*

Розв'язання. Скористаємося евклідовим алгоритмом:

$$\begin{aligned} 18527 &= 4171\cdot 4 + 1843,\\ 4171 &= 1843\cdot 2 + 485,\\ 1843 &= 485\cdot 3 + 388,\\ 485 &= 388\cdot 1 + 97,\\ 388 &= 97\cdot 4 + 0. \end{aligned}$$

Отже, $\mathbf{НСД}(18527, 4171) = 97$.

$\triangle$

Задача 4.2.
Перевірити чи числа ***16675*** *та* ***6496*** *будуть взаємно простими.*

Розв'язання. Знайдемо $\mathbf{НСД}(16675, 6496)$. Для цього скористаємося евклідовим алгоритмом:

$$\begin{aligned} 16675 &= 6496\cdot 2 + 3683,\\ 6496 &= 3683\cdot 1 + 2813,\\ 3683 &= 2813\cdot 1 + 870,\\ 2813 &= 870\cdot 3 + 203,\\ 870 &= 203\cdot 4 + 58,\\ 203 &= 58\cdot 3 + 29,\\ 58 &= 29\cdot 2 + 0. \end{aligned}$$

Оскільки $\mathbf{НСД}(16675, 6496) = 29$, то числа не є взаємно простими.

$\triangle$

Задача 4.3.
Перевірити чи числа ***22275*** *та* ***5681*** *будуть взаємно простими.*

Розв'язання. Знайдемо $\mathbf{НСД}(22275, 5681)$ за допомогою евклідового

алгоритму.

$$\begin{aligned}
\mathbf{22275} &= \mathbf{5681}\cdot\mathbf{3} &&+\mathbf{5232},\\
\mathbf{5681} &= \mathbf{5232}\cdot\mathbf{1} &&+\mathbf{449},\\
\mathbf{5232} &= \mathbf{449}\cdot\mathbf{11} &&+\mathbf{293},\\
\mathbf{449} &= \mathbf{293}\cdot\mathbf{1} &&+\mathbf{156},\\
\mathbf{293} &= \mathbf{156}\cdot\mathbf{1} &&+\mathbf{137},\\
\mathbf{156} &= \mathbf{137}\cdot\mathbf{1} &&+\mathbf{19},\\
\mathbf{137} &= \mathbf{19}\cdot\mathbf{7} &&+\mathbf{4},\\
\mathbf{19} &= \mathbf{4}\cdot\mathbf{4} &&+\mathbf{3},\\
\mathbf{4} &= \mathbf{3}\cdot\mathbf{1} &&+\mathbf{1},\\
\mathbf{3} &= \mathbf{1}\cdot\mathbf{3} &&+\mathbf{0}.
\end{aligned}$$

Отримали, що $\mathbf{НСД}(\mathbf{22275}, \mathbf{5681}) = \mathbf{1}$. Числа є взаємно простими.

$\triangle$

Будь–яке ціле, яке ділиться без остачі на всі числа $a_1, a_2, \ldots, a_k$ називається їх **спільним кратним**. Найменше серед спільних кратних чисел називається **найменшим спільним кратним** (**НСК**). Для чисел a і b найменше спільне кратне позначають $\mathbf{НСК}(a, b)$. Має місце співвідношення:

$$\mathbf{НСК}(a, b) = \frac{a \cdot b}{\mathbf{НСД}(a, b)}. \tag{4.2}$$

Так для чисел **4171** та **18527**

$$\mathbf{НСК}(4171, 18527) = \frac{4171 \cdot 18527}{\mathbf{97}} = \mathbf{796661}$$

.

Задача 4.4.
*Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел **16303** та **34661**.*

Розв'язання. За допомогою евклідового алгоритму знайдемо $\mathbf{НСД}(\mathbf{34661}, \mathbf{16303})$.

$$\begin{aligned}
\mathbf{34661} &= \mathbf{16303}\cdot\mathbf{2} &&+\mathbf{2055},\\
\mathbf{16303} &= \mathbf{2055}\cdot\mathbf{7} &&+\mathbf{1918},\\
\mathbf{2055} &= \mathbf{1918}\cdot\mathbf{1} &&+\mathbf{137},\\
\mathbf{1918} &= \mathbf{137}\cdot\mathbf{14} &&+\mathbf{0}.
\end{aligned}$$

Отже, $\mathbf{НСД}(\mathbf{34661}, \mathbf{16303}) = \mathbf{137}$. Згідно із формулою (4.2) отримуємо

$$\mathbf{НСК}(\mathbf{34661}, \mathbf{16303}) = \frac{\mathbf{34661} \cdot \mathbf{116303}}{\mathbf{137}} = \mathbf{4124659}.$$

△

4.3 Правильні ланцюгові дроби

Означення 4.5.
Ланцюговим (неперервним) дробом *називають вираз вигляду*

$$f = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \ddots + \cfrac{a_n}{b_n + \ddots}}}.$$

Для короткого позначення ланцюгового дробу використовують:

$$f = b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} + \cdots = b_0 + \operatorname*{\mathbb{K}}_{i=1}^{\infty} \frac{a_i}{b_i}.$$

Скінчений ланцюговий дріб f_n, n–й підхідний дріб, що є n–м наближення ланцюгового дробу f, аналогом скінченної суми для ряду, коротко записують

$$f_n = b_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} = b_0 + \operatorname*{\mathbb{K}}_{i=1}^{n} \frac{a_i}{b_i}.$$

Елементи ланцюгового дробу $a_i, b_i, i = 1, 2, \ldots,$ називаються **частинними чисельниками та знаменниками**, відповідно, а b_0 — **вільним членом**. Елементи ланцюгового дробу належать деякому полю або кільцю.

В теорії чисел широко використовуються ланцюгові дроби, в яких вільний член є деяке ціле число, частинні чисельники всі рівні 1, частинні знаменники деякі натуральні числа. Такі ланцюгові дроби називаються **правильними ланцюговими дробами** і записуються коротко наступним чином

$$f = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots = [a_0; a_1, a_2, \ldots, a_n, \ldots],$$

де $a_i \in \mathbb{N}, a_0 \in \mathbb{Z}$.

Ланцюговому дробу f ставиться у відповідність послідовність підхідних дробів $\{p_i/q_i, i = 0, 1, \dots\}$, де

$$\frac{p_0}{q_0} = a_0,\ \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = [a_0; a_1],\ \frac{p_2}{q_2} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} = [a_0; a_1, a_2],$$

$$\dots,\ \frac{p_k}{q_k} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ \dots\ + \frac{1}{a_k} = [a_0; a_1, a_2, \dots, a_k],\ k \in \mathbb{N}.$$

Числа p_k та q_k називаються k–м **канонічним чисельником** та **знаменником** підхідного дробу.

Значення підхідних дробів p_k/q_k можна обчислювати за допомогою рекурентних співвідношень (формул Волліса)

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}, \qquad k \in \mathbb{N}, \tag{4.3}$$

$$p_{-1} = 1, \quad q_{-1} = 0, \quad p_0 = a_0, \quad q_0 = 1.$$

Властивості підхідних дробів правильного ланцюгового дробу

1. Має місце **детермінантна формула**

$$p_k \cdot q_{k-1} - p_{k-1} \cdot q_k = (-1)^{k-1}. \tag{4.4}$$

2. Підхідні дроби правильного ланцюгового дробу нескоротні.

3. Підхідні дроби парного порядку утворюють монотонно зростаючу послідовність, а підхідні дроби непарного порядку — монотонно спадну послідовність і при цьому

$$\frac{p_{2k}}{q_{2k}} < \frac{p_{2i-1}}{q_{2i-1}}, \qquad \text{при довільних значеннях } i, k.$$

4. Підхідні дроби правильного ланцюгового дробу задовольняють так званий "**принцип вилки**"

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_{2k}}{q_{2k}} < \dots < f < \dots < \frac{p_{2k-1}}{q_{2k-1}} < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1},$$

де

$$f = [a_0; a_1, a_2, \dots].$$

Зауваження 4.1.
Із останньої властивості, "принципу вилки", випливає, що послідовність підхідних дробів парних порядків p_{2k}/q_{2k}, яка монотонно зростає, буде давати наближене значення f з недостачею, а послідовність підхідних дробів непарного порядку p_{2k-1}/q_{2k-1}, яка монотонно спадає, буде давати наближене значення f з надлишком.

Задача 4.5.
Знайти розвинення числа $\sqrt{2}$ в правильний ланцюговий дріб і обчислити наближене значення з недостачею та надлишком з точністю $\varepsilon = 0{,}00001$.

Розв'язання. За умовою задачі потрібно знайти такі a_-, a_+, щоб

$$a_- < \sqrt{2} < a_+, \qquad \text{та} \quad |a - a_-| < \varepsilon,\ |a - a_+| < \varepsilon.$$

Виконаємо еквівалентні перетворення

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{(\sqrt{2}-1)(\sqrt{2}+1)}{\sqrt{2}+1} = 1 + \frac{1}{1+\sqrt{2}}.$$

Послідовно вкладаючи отримане співвідношення само в себе, отримаємо

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2} + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{1+\sqrt{2}} =$$
$$= \cdots = 1 + \frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2} + \frac{1}{1+\sqrt{2}} = \cdots =$$
$$= 1 + \frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2} + \cdots = [1; 2, 2, \ldots, 2, \ldots].$$

Використовуючи формули (4.3) обчислимо послідовність канонічних чисельників p_i та знаменників q_i, $i = 0, 1, 2, \ldots$. підхідних дробів

$$\begin{aligned}
&p_0 = 1, && q_0 = 1,\\
&p_1 = 2\cdot 1 + 1 = 3, && q_1 = 2\cdot 1 + 0 = 2,\\
&p_2 = 2\cdot 3 + 1 = 7, && q_2 = 2\cdot 2 + 1 = 5,\\
&p_3 = 2\cdot 7 + 3 = 17, && q_3 = 2\cdot 5 + 2 = 12,\\
&p_4 = 2\cdot 17 + 7 = 41, && q_4 = 2\cdot 12 + 5 = 29,\\
&p_5 = 2\cdot 41 + 17 = 99, && q_5 = 2\cdot 29 + 12 = 70,\\
&p_6 = 2\cdot 99 + 41 = 239, && q_6 = 2\cdot 70 + 29 = 169,\\
&p_7 = 2\cdot 239 + 99 = 577, && q_7 = 2\cdot 169 + 70 = 408,\\
&p_8 = 2\cdot 577 + 239 = 1393, && q_8 = 2\cdot 408 + 169 = 985.
\end{aligned}$$

Підхідні дроби $p_i/q_i, i = 0, 1, 2, \dots$ будуть рівні

$$\frac{p_0}{q_0} = \frac{1}{1} = 1, \quad \frac{p_1}{q_1} = \frac{3}{2} = 1{,}5, \quad \frac{p_2}{q_3} = \frac{7}{5} = 1{,}4, \quad \frac{p_3}{q_3} = \frac{17}{12} \approx 1{,}41667,$$

$$\frac{p_4}{q_4} = \frac{41}{29} \approx 1{,}41379, \quad \frac{p_5}{q_5} = \frac{99}{70} \approx 1{,}41429, \quad \frac{p_6}{q_6} = \frac{239}{169} \approx 1{,}41420,$$

$$\frac{p_7}{q_7} = \frac{577}{408} \approx 1{,}414215686, \quad \frac{p_8}{q_8} = \frac{1393}{985} \approx 1{,}414213197$$

Згідно із "принципом вилки" маємо, що

$$1 < \frac{7}{5} < \frac{41}{29} < \frac{239}{169} < \frac{1393}{985} < \sqrt{2} < \frac{577}{408} < \frac{99}{70} < \frac{17}{12} < \frac{3}{2}.$$

Крім того,

$$\frac{p_7}{q_7} - \frac{p_8}{q_8} < 0{,}000002.$$

Отже,

$$a_- = \frac{1393}{985}, \quad a_+ = \frac{577}{408}.$$

Або виконавши заокруглення до 6 знаку після десяткової коми, маємо

$$1,414215 < \sqrt{2} < 1,414216.$$

$\triangle$

4.4 Розв'язання невизначених рівнянь першого степеня з двома невідомими у цілих числах за допомогою ланцюгових дробів

Нехай a, b, c – цілі числа, x, y – цілі змінні. Розглядаються рівняння вигляду

$$ax + by = c, \tag{4.5}$$

де коефіцієнти a, b взаємно прості числа, тобто $\text{НСД}(a, b) = 1$.

При великих коефіцієнтах такі рівняння зручно розв'язувати за допомогою ланцюгових дробів. Припустимо, що $a/b = p_k/q_k$ – k-й підхідний дріб розвинення відношення чисел a/b в ланцюговий дріб. Знайдемо попередній p_{k-1}/q_{k-1} підхідний дріб. Згідно із детермінантною формулою (4.4) матимемо

$$aq_{k-1} - bp_{k-1} = (-1)^{k-1}.$$

Після множення лівої та правої частин рівності на $(-1)^{k-1}c$ отримуємо:

$$(-1)^{k-1}caq_{k-1} - (-1)^{k-1}cbp_{k-1} = c.$$

Нехай

$$x_0 = (-1)^{k-1}cq_{k-1}, \qquad y_0 = (-1)^{k-1}cp_{k-1}. \tag{4.6}$$

Тоді

$$ax_0 + by_0 = c,$$

або

$$a(x_0 + bt) + b(y_0 - at) = c.$$

Маємо загальний розв'язок рівняння (4.5)

$$x = x_0 + bt, \qquad y = y_0 - at, \qquad \text{де} \quad t = 0, \pm 1, \pm 2, \dots.$$

Задача 4.6.
Знайти цілочислові розв'язки рівняння

$$29x + 19y = 5.$$

Розв'язання. Відмітимо, що $\text{НСД}(29, 19) = 1$. Коефіцієнти рівняння взаємно прості числа. Розвинемо відношення $\dfrac{a}{b} = \dfrac{29}{19}$ в правильний ланцюговий дріб:

$$\frac{29}{19} = 1 + \frac{1}{\frac{19}{10}} = 1 + \frac{1}{1} + \frac{1}{\frac{10}{9}} = 1 + \frac{1}{1} + \frac{1}{1} + \frac{1}{9} = [1; 1, 1, 9].$$

Обчислимо підхідний дріб:

$$\frac{p_{k-1}}{q_{k-1}} = \frac{p_2}{q_2}, \quad p_2 = 3, \quad q_2 = 2.$$

Згідно із формулою (4.6) маємо

$$x_0 = (-1)^2 \cdot 5 \cdot 2 = 10, \qquad y_0 = (-1)^3 \cdot 5 \cdot 3 = -15,$$

$$x = 10 + 19t, \quad y = -15 - 29t, \qquad \text{де} \quad t = 0, \pm 1, \pm 2, \dots.$$

$\triangle$

Задача 4.7.
Знайти розв'язок рівняння першого степеня з двома невідомими

$$37x + 64y = 10.$$

Розв'язання. Розвинемо відношення коефіцієнтів в правильний ланцюговий дріб

$$\frac{37}{64} = \frac{1}{\frac{64}{37}} = \frac{1}{1} + \frac{1}{\frac{37}{27}} = \frac{1}{1} + \frac{1}{1} + \frac{1}{\frac{27}{10}} = \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{\frac{10}{7}} =$$

$$= \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{\frac{7}{3}} = \frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{3} =$$

$$= [0; 1, 1, 2, 1, 2, 1, 3].$$

Визначаємо значення підхідного дробу

$$\frac{p_{k-1}}{q_{k-1}} = \frac{p_5}{q_5}, \quad p_5 = 11, \quad q_5 = 19.$$

За формулою (4.6) обчислюємо

$$x_0 = (-1)^5 \cdot 10 \cdot 19 = -190, \qquad y_0 = (-1)^6 \cdot 10 \cdot 11 = 110.$$

$$x = -190 + 64t, \qquad y = 110 - 37t, \qquad \text{де} \quad t = 0, \pm 1, \pm 2, \ldots.$$

$\triangle$

4.5 Алгоритм Евкліда та розвинення раціонального дробу у правильний ланцюговий дріб

Нехай $p, q \in \mathbb{N}$ і дріб p/q — нескоротний. Операцію ділення з остачею в алгоритмі Евкліда перепишемо у вигляді

$$\begin{aligned}
\frac{p}{q} &= a_0 + \frac{r_1}{q}, && 0 < r_1 < q;\\
\frac{q}{r_1} &= a_1 + \frac{r_2}{r_1}, && 0 < r_2 < r_1;\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2}, && 0 < r_3 < r_2;\\
&\vdots && \vdots\\
\frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}}, && 0 < r_n < r_{n-1};\\
\frac{r_{n-1}}{r_n} &= a_n, && a_n > 1.
\end{aligned}$$

Запишемо дріб $\boldsymbol{p/q}$ наступним чином

$$\frac{\boldsymbol{p}}{\boldsymbol{q}} = \boldsymbol{a_0} + \frac{\boldsymbol{r_1}}{\boldsymbol{q}} = \boldsymbol{a_0} + \frac{\boldsymbol{1}}{\dfrac{\boldsymbol{q}}{\boldsymbol{r_1}}} = \boldsymbol{a_0} + \frac{\boldsymbol{1}}{\boldsymbol{a_1} + \dfrac{\boldsymbol{r_2}}{\boldsymbol{r_1}}} = \boldsymbol{a_0} + \frac{\boldsymbol{1}}{\boldsymbol{a_1} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{r_1}}{\boldsymbol{r_2}}}} =$$

$$= \boldsymbol{a_0} + \frac{\boldsymbol{1}}{\boldsymbol{a_1} + \dfrac{\boldsymbol{1}}{\boldsymbol{a_2} + \dfrac{\boldsymbol{r_3}}{\boldsymbol{r_2}}}} = \cdots = \boldsymbol{a_0} + \frac{\boldsymbol{1}}{\boldsymbol{a_1} + \dfrac{\boldsymbol{1}}{\boldsymbol{a_2} + \dfrac{\boldsymbol{1}}{\boldsymbol{a_3} + \ \cdots \ + \dfrac{\boldsymbol{1}}{\boldsymbol{a_n}}}}} =$$

$$= [\boldsymbol{a_0}; \boldsymbol{a_1}, \boldsymbol{a_2}, \boldsymbol{a_3}, \ldots, \boldsymbol{a_n}],$$

де $\boldsymbol{a_0} \in \mathbb{Z}, \boldsymbol{a_i} \in \mathbb{N}$.

Задача 4.8.

Розвинути раціональний дріб $\frac{\boldsymbol{1638}}{\boldsymbol{1495}}$ *у правильний ланцюговий дріб.*

Розв'язання. Послідовно виконуємо дії

$$\frac{\boldsymbol{1639}}{\boldsymbol{1495}} = \boldsymbol{1} + \frac{\boldsymbol{144}}{\boldsymbol{1495}} = \boldsymbol{1} + \frac{\boldsymbol{1}}{\dfrac{\boldsymbol{1495}}{\boldsymbol{144}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{55}}{\boldsymbol{144}}} = \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{144}}{\boldsymbol{55}}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{34}}{\boldsymbol{55}}}} = \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{55}}{\boldsymbol{34}}}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{21}}{\boldsymbol{34}}}}} == \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{34}}{\boldsymbol{21}}}}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{13}}{\boldsymbol{21}}}}}} = \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{21}}{\boldsymbol{13}}}}}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{8}}{\boldsymbol{13}}}}}}} =$$

$$= \boldsymbol{1} + \frac{\boldsymbol{1}}{\boldsymbol{10} + \dfrac{\boldsymbol{1}}{\boldsymbol{2} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\boldsymbol{1} + \dfrac{\boldsymbol{1}}{\dfrac{\boldsymbol{13}}{\boldsymbol{8}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{5}{8}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{8}{5}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{3}{5}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{5}{3}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{3}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{3}{2}}}}}}}} =$$

$$= 1 + \cfrac{1}{10 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}}}}}.$$

△

4.6 Прості числа

Означення 4.6.
*Натуральне число $p \in \mathbb{N}$ називається **простим**, якщо $p > 1$ і p ділиться тільки само на себе і на **1**. В протилежному випадку натуральне число називається **складеним**.*

Складене число ділиться не лише на один, само на себе, а ще хоча б одне натуральне число.

Першими простими натуральними числами є:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \ldots$$

Якщо n — число складене, то знайдеться таке ціле $a \in \mathbb{N}$, що

$$n = a \cdot b, \quad 1 < b < n, \quad b = n/a.$$

Очевидно, що всі парні числа, крім **2**, є складені.

Множина натуральних чисел $\mathbb{N}$ може бути розбита на три підмножини:

- множину простих чисел;
- множину складених чисел;
- число 1, яке не відноситься ні до складених ні до простих.

Властивості простих чисел

1. Для будь–якого цілого числа $n > 1$ найменший відмінний від одиниці додатний дільник — це завжди просте число.
2. Найбільший простий дільник, який відмінний від **1**, будь–якого складеного числа n не перевищує $\sqrt{n}$.
3. Простих чисел безліч.
4. Якщо добуток натуральних чисел $a \cdot b$ ділиться на просте число p, то хоча б одне з них ділиться на p.

4.7 Решето Ератосфена

Найпростішою процедурою отримання послідовності простих чисел є **решето Ератосфена**. Завдання методу — визначити (просіяти) всі додатні прості числа, які менші за деяке ціле значення $n > 0$. Згідно із методом відбувається поступове викреслювання, просіювання, в ряді чисел, які кратні простим числам, що менші за $\sqrt{n}$. Всі числа, які залишаться, будуть простими.

Проілюструємо метод решета Ератосфена для випадку, коли $n = 100$. Випишемо всі натуральні числа від **2** до **100**. Перше просте число у цьому ряді — **2**. Викреслимо, візьмемо в рамочку, всі числа ряду, які кратні **2** крім нього самого.

2, 3, 4, **5,** 6, **7,** 8, **9,** 10, **11,** 12, **13,** 14, **15,** 16, **17,** 18, **19,** 20, **21,**

22, **23,** 24, **25,** 26, **27,** 28, **29,** 30, **31,** 32, **33,** 34, **35,** 36, **37,** 38,

39, 40, **41,** 42, **43,** 44, **45,** 46, **47,** 48, **49,** 50, **51,** 52, **53,** 54, **55,**

56, **57,** 58, **59,** 60, **61,** 62, **63,** 64, **65,** 66, **67,** 68, **69,** 70, **71,** 72,

73, 74, **75,** 76, **77,** 78, **79,** 80, **81,** 82, **83,** 84, **85,** 86, **87,** 88, **89,**

90, **91,** 92, **93,** 94, **95,** 96, **97,** 98, **99,** 100.

Перше не викреслене, не взяте в рамочку, число після **2** буде число **3** і воно просте. Викреслимо в ряді всі числа, що не були викресленні на попередньому кроці, які кратні **3**. Починаємо викреслювати з $\mathbf{3^2 = 9}$.

2, 3, 4, **5,** 6, **7,** 8, 9, 10, **11,** 12, **13,** 14, 15, 16, **17,** 18, **19,** 20, 21, 22, **23,** 24, **25,** 26, 27, 28, **29,** 30, **31,** 32, 33, 34, **35,** 36, **37,** 38, 39, 40, **41,** 42, **43,** 44, 45, 46, **47,** 48, **49,** 50, 51, 52, **53,** 54, **55,** 56, 57, 58, **59,** 60, **61,** 62, 63, 64, **65,** 66, **67,** 68, 69, 70, **71,** 72, **73,** 74, 75, 76, **77,** 78, **79,** 80, 81, 82, **83,** 84, **85,** 86, 87, 88, **89,** 90, **91,** 92, 93, 94, **95,** 96, **97,** 98, 99, 100.

Наступним після **3** буде число **5**. Викреслимо в ряді чисел, що залишилися, усі числа, які кратні **5** починаючи з $\mathbf{5^2 = 25}$:

2, 3, 4, **5,** 6, **7,** 8, 9, 10, **11,** 12, **13,** 14, 15, 16, **17,** 18, **19,** 20, 21, 22, **23,** 24, 25, 26, 27, 28, **29,** 30, **31,** 32, 33, 34, 35, 36, **37,** 38, 39, 40, **41,** 42, **43,** 44, 45, 46, **47,** 48, **49,** 50, 51, 52, **53,** 54, 55, 56, 57, 58, **59,** 60, **61,** 62, 63, 64, 65, 66, **67,** 68, 69, 70, **71,** 72, **73,** 74, 75, 76, **77,** 78, **79,** 80, 81, 82, **83,** 84, 85, 86, 87, 88, **89,** 90, **91,** 92, 93, 94, 95, 96, **97,** 98, 99, 100.

Після **5** йде число **7**. Викреслимо всі числа, що кратні **7**. Розпочинаємо з $\mathbf{7^2 = 49}$.

2, 3, 4, **5,** 6, **7,** 8, 9, 10, **11,** 12, **13,** 14, 15, 16, **17,** 18, **19,** 20, 21, 22, **23,** 24, 25, 26, 27, 28, **29,** 30, **31,** 32, 33, 34, 35, 36, **37,** 38, 39, 40, **41,** 42, **43,** 44, 45, 46, **47,** 48, 49, 50, 51, 52, **53,** 54, 55, 56, 57, 58, **59,** 60, **61,** 62, 63, 64, 65, 66, **67,** 68, 69, 70, **71,** 72, **73,** 74, 75, 76, 77, 78, **79,** 80, 81, 82, **83,** 84, 85, 86, 87, 88, **89,** 90, 91, 92, 93, 94, 95, 96, **97,** 98, 99, 100.

Наступним після **7** числом, яке ще не викреслено, є число **11**. Але наступний крок просіювання чисел в алгоритмі решета Ератосфена виконувати не потрібно, оскільки $\mathbf{11 > \sqrt{100} = 10}$. Випишемо всі числа, які залишилися. Маємо всі прості числа, від **2** до **100**.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

4.8 Прайморіал простого числа

У 1987 році американський математик Гарві Дабнер ввів поняття прайморіала простого числа за аналогією до факторіалу натурального.

Означення 4.7.
Прайморіалом $p^{\#}$ простого числа $p > 0$ *називається добуток всіх простих чисел менших або рівних p.*

Приклад 4.4.
За означенням $2^{\#} = 2, \quad 5^{\#} = 2 \cdot 3 \cdot 5 = 30.$

Варто зауважити, що якщо q — наступне після p просте число, то має місце співвідношення $q^{\#} = p^{\#} \cdot q$.

Якщо розглядати числа вигляду $p^{\#} + 1$, то виявляється, що

$$2^{\#} + 1 = 3, \quad 3^{\#} + 1 = 6 + 1 = 7, \quad 5^{\#} + 1 = 30 + 1 = 31,$$

$$7^{\#} + 1 = 210 + 1 = 211, \quad 11^{\#} + 1 = 2310 + 1 = 2311$$

прості числа, але

$$13^{\#} + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

буде число складене. Хоча числа вигляду $p^{\#} + 1$ не завжди прості числа, але не мають дільників менших або рівних числу p.

Проблема також полягає в тому, що навіть при невеликих значеннях p прайморіал $p^{\#}$ — велике число.

Задача 4.9.
Обчислити прайморіал числа числа 19 *та з'ясувати, чи число* $19^{\#} + 1$ *буде простим числом.*

Розв'язання. Згідно із означенням

$$19^{\#} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690.$$

Але число

$$19^{\#} + 1 = 9699691 = 347 \cdot 27953$$

не є простим числом.

$\triangle$

4.9 Основна теорема арифметики

Теорема 6 (Основна арифметики).
Для довільного цілого числа $m \neq 1$ існує єдине ***канонічне розвинення на прості множники*** *(з точністю до їх перестановок), тобто*

$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n} = \prod_{i=1}^{n} p_i^{k_i},$$

де $p_1, p_2, \ldots, p_n$ — різні прості числа, а $k_1, k_2, \ldots, k_n$ — натуральні числа, що називаються ***кратності простих чисел*** *.*

Наслідки з основної теореми арифметики

1. Число
$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$
ділиться на число b тоді і тільки тоді, коли
$$b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_n^{t_n},$$
де $0 \leqslant t_1 \leqslant k_1, 0 \leqslant t_2 \leqslant k_2, \ldots, 0 \leqslant t_n \leqslant k_n$.

2. Число
$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$
тоді і тільки тоді буде точним ℓ–им степенем деякого цілого числа, коли всі показники $k_1, k_2, \ldots, k_n$ будуть ділитися на число ℓ.

3. Кількість усіх дільників числа
$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$
можна обчислити за формулою
$$\tau(m) = (k_1 + 1)(k_2 + 1) \cdots (k_n + 1). \tag{4.7}$$

4. Сума всіх дільників числа дорівнює
$$S(m) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_n^{k_n+1} - 1}{p_n - 1}. \tag{4.8}$$

Задача 4.10.
Знайти канонічне розвинення числа 16200 на прості множники.

Розв'язання. Послідовно виконуємо ділення на прості числа

16200	**2**		**225**	**3**
8100	**2**		**75**	**3**
4050	**2**		**25**	**5**
2025	**3**		**5**	**5**
675	**3**		**1**	

Отримуємо розвинення $\mathbf{16200 = 2^3 \cdot 3^4 \cdot 5^2}$.

△

Задача 4.11.
Показати, що число $\mathbf{14553}$ *ділиться на число* $\mathbf{2079}$.

Розв'язання. Знайдемо канонічні розвинення чисел $\mathbf{14553}$ та $\mathbf{2079}$ на прості множники. Послідовно ділимо на прості числа.

14553	**3**		**2079**	**3**
4851	**3**		**693**	**3**
1617	**3**		**231**	**3**
539	**7**		**77**	**7**
77	**7**		**11**	**11**
11	**11**		**1**	
1				

Отримали розвинення

$$\mathbf{14553 = 3^3 \cdot 7^2 \cdot 11}, \qquad \mathbf{2079 = 3^3 \cdot 7 \cdot 11}.$$

Числа розвинуті за одними і тими ж простими числами $\mathbf{3, 7, 11}$. Згідно із першим наслідком з основної теореми арифметики число $\mathbf{14553}$ ділиться на $\mathbf{2079}$.

△

Задача 4.12.
Знайти кількість дільників та їх суму числа $\mathbf{79625}$.

Розв'язання. Число має канонічне розвинення на прості множники

$$\mathbf{79625 = 5^3 \cdot 7^2 \cdot 13.}$$

Згідно із формулою (4.7) маємо

$$\boldsymbol{\tau(79625) = (3+1)(2+1)(1+1) = 24.}$$

За допомогою формули (4.8) знаходимо

$$S(79625) = \frac{5^4-1}{5-1} \cdot \frac{7^3-1}{7-1} \cdot \frac{13^2-1}{13-1} = 156 \cdot 57 \cdot 14 = 124488.$$

$\triangle$

Як наслідок із основної теореми алгебри випливає твердження.

Теорема 7 (Про канонічне розвинення).
Нехай маємо канонічні розвинення на множники двох чисел a та b

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, \quad b = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_n^{m_n},$$

причому деякі показники k_i і m_i можуть дорівнювати нулю. Тоді найбільший спільний дільник чисел a і b визначається за формулою

$$НСД(a,b) = p_1^{t_1} \cdot p_2^{t_2} \cdots p_n^{t_n}, \tag{4.9}$$

де $t_i = \min\{k_i; m_i\},\ i = 1, 2, \cdots, n$, а найменше спільне кратне цих чисел за формулою

$$НСК(a,b) = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}, \tag{4.10}$$

де $s_i = \max\{k_i; m_i\},\ i = 1, 2, \cdots, n$.

Задача 4.13.
*Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел $a = 7800$ та $b = 14586$.*

Розв'язання. Запишемо канонічне розвинення чисел на прості множники

$$a = 7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13, \qquad b = 14586 = 2 \cdot 3 \cdot 11 \cdot 13 \cdot 17.$$

Перепишемо розвинення у вигляді

$$a = 2^3 \cdot 3 \cdot 5^2 \cdot 11^0 \cdot 13 \cdot 17^0, \qquad b = 2 \cdot 3 \cdot 5^0 \cdot 11 \cdot 13 \cdot 17.$$

За допомогою формули (4.9) знаходимо

$$\text{НСД}(7800, 14586) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 11^0 \cdot 13^1 \cdot 17^0 = 78.$$

Аналогічно, згідно із формулою (4.10) маємо

$$\text{НСК}(7800, 14586) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 11^1 \cdot 13^1 \cdot 17^1 = 1458600.$$

$\triangle$

4.10 Важливі функції теорії чисел

Означення 4.8.
Функція $[x]$, яка визначена для довільного дійсного числа x і приймає найбільше ціле значення, що не перевищує x, називається його ***цілою частиною****.*

Означення 4.9.
Функція $\{x\}$, яка задається для довільного дійсного значення x, приймає значення з півінтервалу $[0;1)$ і визначена наступним чином

$$\{x\} \stackrel{def}{=} x - [x],$$

називається ***дробовою частиною*** *x.*

Задача 4.14.
Визначити цілу та дробову частини числа $5{,}26$ та числа $-3{,}75$.

Розв'язання. Маємо:

$$[5{,}26] = 5, \quad \{5,26\} = 5{,}26 - [5{,}26] = 5{,}26 - 5 = 0,26.$$

$$[-3{,}75] = -4, \quad \{-3{,}75\} = -3{,}75 - [-3{,}75] = -3{,}75 + 4 = 0{,}25.$$

$\triangle$

Означення 4.10.
Функція Ойлера $\varphi(n)$ визначена для всіх натуральних значень n і рівна кількості натуральних чисел, які взаємно прості з n і не перевищують його.

Задача 4.15.

$$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4,\ \varphi(6) = 2.$$

Властивості функції Ойлера

1. Нехай p — просте число, тоді

$$\varphi(p) = p - 1.$$

2. Нехай p — просте число, $k > 1$ — деяке натуральне, тоді

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

3. Якщо $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$ — канонічне розвинення числа на прості множники. Значення функції Ойлера $\varphi(a)$ обчислюють за допомогою однієї із формул

$$\varphi(a) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right),$$

$$\varphi(a) = \left(p^{k_1} - p^{k_1 - 1}\right)\left(p^{k_2} - p^{k_2 - 1}\right) \cdots \left(p^{k_n} - p^{k_n - 1}\right).$$

Приклад 4.5.
Оскільки 17 *— просте число, то* $\varphi(17) = 16$.

Задача 4.16.
Обчислити значення функції Ойлера чисел $64, 81$.

Розв'язання. Згідно із другою властивістю функції Ойлера маємо

$$\varphi(64) = \varphi(2^6) = 2^6 - 2^5 = 64 - 32 = 32.$$

Аналогічно

$$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 81 - 27 = 54.$$

$\triangle$

Задача 4.17.
Обчислити значення функції Ойлера числа 16200.

Розв'язання. Згідно із третьою властивістю функції Ойлера маємо

$$\varphi(16200) = \varphi(2^3 \cdot 3^4 \cdot 5^2) = (2^3 - 2^2)(3^4 - 3^3)(5^2 - 5) =$$

$$= (8 - 4)(81 - 27)(25 - 5) = 4 \cdot 54 \cdot 20 = 4320.$$

$\triangle$

4.11 Питання, тести та вправи до розділу 4

4.11.1 Питання до розділу 4

1. Що розуміють під множиною цілих чисел?
2. Які операції над елементами множини цілих чисел $\mathbb{Z}$ не виводять за межі цієї множини?

3. Дайте означення дільника на множині $\mathbb{Z}$.
4. Сформулюйте теорему про подільність з остачею цілих чисел.
5. Дайте означення найбільшого спільного дільника цілих чисел.
6. Які цілі числа називаються взаємно простими?
7. Коли цілі числа називаються попарно простими?
8. Сформулюйте алгоритм Евкліда відшукання найбільшого спільного дільника двох цілих чисел.
9. Дайте означення найменшого спільного кратного цілих чисел.
10. Який вираз називається ланцюговим дробом?
11. Вкажіть скорочені позначення для ланцюгового дробу.
12. Що розуміють під підхідним дробом ланцюгового дробу.
13. Дайте означення частинних чисельників та знаменників, а також вільного члена ланцюгового дробу.
14. Який ланцюговий дріб називають правильним ланцюговим дробом? Який короткий запис використовується?
15. Що розуміють під канонічним чисельником та канонічним знаменником ланцюгового дробу?
16. Запишіть формули Волліса.
17. Сформулюйте "детермінантну формулу" для правильного ланцюгового дробу.
18. Вкажіть властивості для послідовностей підхідних дробів парного і непарного порядків правильного ланцюгового дробу.
19. Сформулюйте "принцип вилки"для правильного ланцюгового дробу.
20. Який взаємозв'язок між евклідовим алгоритмом знаходження найбільшого спільного дільника двох чисел та розвиненням раціонального дробу у правильний ланцюговий дріб?
21. Які числа називають простими, а які складеними?

22. Якими властивостями володіють прості числа.
23. В чому полягає "решето Ератосфена"?
24. Дайте означення прайморіала простого числа.
25. Сформулюйте основну теорему арифметики.
26. Які наслідки випливають з основної теореми арифметики.
27. Вкажіть формулу для підрахунку кількості дільників числа.
28. За допомогою якої формули можна підрахувати суму всіх дільників числа?
29. Сформулюйте теорему про канонічне розвинення чисел.
30. Дайте означення функції цілої частини числа.
31. Як визначається функція дробової частини числа.
32. Сформулюйте означення функції Ойлера.
33. Які властивості має функція Ойлера у випадку простого числа.

4.11.2 Тести до розділу 4

Вказати правильну відповідь на кожен тест.

1. Сума, різниця та добуток двох цілих чисел буде цілим числом:
   (A) завжди; **(B)** ніколи; **(C)** деколи.
2. Результатом ділення цілого числа на ціле число буде ціле число:
   (A) завжди; **(B)** ніколи; **(C)** деколи.
3. Три цілі числа мають спільний дільник:
   (A) завжди; **(B)** ніколи; **(C)** деколи.
4. Якщо d_1 — найбільший спільний дільник чисел a_1 та a_2 і d_2 інший їх спільний дільник, то
   (A) d_2 ділиться на d_1; **(B)** d_1 ділиться на d_2; **(C)** d_2=d_1.

5. Нехай $a = bq + r$. Тоді

   (A) $\text{НСД}(a, b) = \text{НСД}(a, r)$;

   (B) $\text{НСД}(a, b) = \text{НСД}(b, r)$;

   (C) $\text{НСД}(a, b) = \text{НСД}(q, r)$.

6. Нехай m — додатне ціле число. Тоді

   (A) $\text{НСД}(ma, mb) = m \cdot \text{НСД}(a, mb)$;

   (B) $\text{НСД}(ma, mb) = m \cdot \text{НСД}(ma, b)$;

   (C) $\text{НСД}(ma, mb) = m \cdot \text{НСД}(a, rb$.

7. Найбільший спільний дільник чисел a та b згідно із евклідовим алгоритмом:

   (A) остання остача r_n;

   (B) передостання відмінна від нуля остача r_{n-1};

   (C) довільна, відмінна від нуля остача.

8. Якщо c_1 — найменше спільне кратне чисел a та b, а c_2 — інше спільне кратне цих чисел. Тоді:

   (A) $c_1 \leqslant c_2$; **(B)** $c_2 > c_2$; **(C)** $c_1 = c_2$.

9. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб. Тоді

   (A) $a_0 \in \mathbb{Z}$; **(B)** $a_0 \in \mathbb{R}$; **(C)** $a_0 \in \mathbb{C}$.

10. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб. Тоді:

    (A) $a_2 \in \mathbb{Z}$; **(B)** $a_2 \in \mathbb{N}$; **(C)** $a_2 \in \mathbb{R}$.

11. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Тоді

    (A) $p_1 = a_0 \cdot a_1 + 1$; **(B)** $p_1 = a_0 + 1$; **(C)** $p_1 = a_0$.

12. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Тоді

    (A) $q_2 = a_1 \cdot a_2 + 1$; **(B)** $q_2 = a_2 + 1$; **(C)** $q_2 = a_1$.

13. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Тоді має місце формула:

    (A) $q_5 = a_5 \cdot q_4 + q_3$; **(B)** $p_5 = a_5 \cdot q_4 + p_3$; **(C)** $q_5 = a_5 \cdot p_4$.

14. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Детермінантна формула має вигляд:

    (A) $p_k p_{k-1} - q_k q_{k-1} = (-1)^{k-1}$;

    (B) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$;

    (C) $p_k q_k - p_{k-1} q_{k-1} = (-1)^{k-1}$.

15. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Підхідні дроби:

    (A) мають спільні дільники; **(B)** нескоротні; **(C)** скоротні завжди.

16. Нехай $[a_0; a_1, a_2, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Вірним буде співвідношення:

    (A) $\frac{p_{2k}}{q_2 k} = \frac{p_{2k-1}}{q_{2k-1}}$; **(B)** $\frac{p_{2k}}{q_2 k} \geqslant \frac{p_{2k-1}}{q_{2k-1}}$; **(C)** $\frac{p_{2k}}{q_2 k} < \frac{p_{2k-1}}{q_{2k-1}}$.

17. Нехай $f = [a_0; a_1, \cdots]$ — правильний ланцюговий дріб, $\{p_i/q_i\}$ — послідовність підхідних дробів. Вірним буде співвідношення:

    (A) $\frac{p_{2k}}{q_2 k} < f < \frac{p_{2k-1}}{q_{2k-1}}$; **(B)** $\frac{p_{2k}}{q_2 k} > f > \frac{p_{2k-1}}{q_{2k-1}}$; **(C)** $\frac{p_{2k}}{q_2 k} = f = \frac{p_{2k-1}}{q_{2k-1}}$.

18. Просте число має:

    (A) два дільника; **(B)** жодного дільника; **(C)** лише один дільник.

19. Найбільший простий дільник дільник m, який відмінний від 1, довільного складеного числа n задовольняє нерівність:

    (A) $m = \sqrt{n}$; **(B)** $m > \sqrt{n}$; **(C)** $1 < m \leqslant \sqrt{n}$.

20. Простих чисел:

    (A) безліч; **(B)** скінчене велике число; **(C)** всі числа складені.

21. Метод відшукання простих чисел, які не перевищують n, називається:

    (A) Ситом Евкліда; **(B)** Решетом Ератосфена; **(C)** Сіткою Піфагора.

22. Нехай $p^{\#}$ — прайморіал простого числа p. Вірним буде твердження:

    (A) $p^{\#} < p$; **(B)** $p^{\#} = p$; **(C)** $p^{\#} > p$.

23. Якщо $p^{\#}$ — прайморіал простого числа p, тоді $p^{\#} + 1$ буде число

    (A) завжди просте;

    (B) завжди складене;

    (C) або просте, або складене.

24. Нехай $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, m > 1$ — канонічне розвинення числа на прості множники. Числа $k_1, k_2, \ldots, k_n$ можуть бути:

    (A) натуральні; **(B)** цілі; **(C)** дійсні.

25. Нехай $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, m > 1,$ — канонічне розвинення числа на прості множники. Числа $p_1, p_2, \ldots, p_n$ можуть бути:

    (A) однакові; **(B)** різні; **(C)** довільні.

26. Нехай $m_1 = 2^4 \cdot 3^5 \cdot 5^6$ і $m_2 = 2^5 \cdot 3^4 \cdot 5^3$. Тоді:

    (A) m_1 ділиться на m_2;

    (B) m_1 не ділиться на m_2;

    (C) $m_1 = m_2$;

27. Нехай $m = 3^6 \cdot 5^2 \cdot 7^4$. Число m:

    (A) куб деякого числа;

    (B) квадрат деякого числа;

    (C) деяке число у 5 степені.

28. Нехай $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, m > 1$ — канонічне розвинення числа на прості множники. Кількість дільників числа m рівна:

    (A) $\tau(m) = k_1 \cdot k_2 \cdot \ldots \cdot k_n$;

    (B) $\tau(m) = k_1 + k_2 + \cdots + k_n$;

    (C) $\tau(m) = (k_1 + 1) \cdot (k_2 + 1) \cdot \ldots \cdot (k_n + 1)$.

29. Функція $[x]$ визначає:

    (A) цілу частину числа; **(B)** дробову частину числа; **(C)** знак числа.

30. Функція $\{x\}$ задає:

    (A) цілу частину числа; **(B)** дробову частину числа; **(C)** знак числа.

31. Значення функції Ойлера $\varphi(11)$ рівне:

    (A) 9; **(B)** 10; **(C)** 11.

4.11.3 Вправи до розділу 4

Вправа 4.1.
*Знайти найбільший спільний дільник таких двох чисел **1989792** і **608580**.*

Вправа 4.2.
*Знайти найбільший спільний дільник таких чисел **2465680** і **623672**.*

Вправа 4.3.
*Перевірити чи числа **45747** та **20387** будуть взаємно простими.*

Вправа 4.4.
*Перевірити чи числа **71148** та **8325** будуть взаємно простими.*

Вправа 4.5.
*Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) таких двох чисел **701688** та **1117758**.*

Вправа 4.6.
*Знати найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел **456987** та **96877719**.*

Вправа 4.7.
Число

$$\varphi = \frac{\sqrt{5}-1}{2}$$

*називається **золотим перерізом**. Отримати розвинення (зображення) числа φ у правильний ланцюговий дріб та знайти наближене значення з точністю до шостого знаку після десяткової коми.*

Вказівка до розв'язання. Скористатися тотожністю

$$\frac{\sqrt{5}-1}{2} = 1 + \frac{1}{1 + \dfrac{\sqrt{5}-1}{2}}.$$

Вправа 4.8.
Отримати розвинення (зображення) числа $\sqrt{3}$ у правильний ланцюговий дріб та обчислити наближене значення числа з точністю до шостого знака після десяткової коми.

Вказівка до розв'язання. Обґрунтувати та скористатися тотожністю

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \sqrt{3}}}.$$

Вправа 4.9.
Розвинути раціональний дріб $\frac{8220}{2533}$ *у правильний ланцюговий дріб.*

Вправа 4.10.
Розвинути раціональний дріб $\frac{3632}{3033}$ *у правильний ланцюговий дріб.*

Вправа 4.11.
Знайти розв'язок рівняння першого степеня з двома невідомими

$$38x + 117y = 209.$$

Вправа 4.12.
Знайти розв'язок рівняння першого степеня з двома невідомими

$$122x + 129y = 2.$$

Вправа 4.13.
Використовуючи алгоритм решета Ератосфена, знайти прості числа від 2 *до* 300.

Вправа 4.14.
Обчислити прайморіал чисел $31, 37, 47$.

Вправа 4.15.
З'ясувати чи число $17^{\#} + 1$ *буде простим числом.*

Вправа 4.16.
Обчислити прайморіал числа числа 23 *та з'ясувати, чи число* $23^{\#} + 1$ *буде простим числом.*

Вправа 4.17.
Знайти канонічне розвинення числа 379456 *на прості множники.*

Вправа 4.18.
Знайти канонічне розвинення числа 29712375 *на прості множники.*

Вправа 4.19.
Показати, що число 83006 *ділиться на число* 539.

Вправа 4.20.
Показати, що число ***343343*** *ділиться на число* ***637****.*

Вправа 4.21.
Знайти кількість дільників та їх суму числа ***705551****.*

Вправа 4.22.
Знайти кількість дільників та їх суму числа ***7626125****.*

Вправа 4.23.
*Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел* $a = 429975$ *та* $b = 647360$.

Вправа 4.24.
*Обчислити найбільший спільний дільник (**НСД**) та найменше спільне кратне (**НСК**) чисел* $a = 714420$ *та* $b = 1028160$.

Вправа 4.25.
Визначити цілу та дробову частину числа $3{,}82$ *та числа* $-4{,}23$.

Вправа 4.26.
Обчислити значення функції Ойлера чисел $24, 29, 30, 31$.

Вправа 4.27.
Обчислити значення функції Ойлера чисел $125, 128, 243$.

Вправа 4.28.
Обчислити значення функції Ойлера чисел $21168, 496125$.

Розділ 5

Основи модульної арифметики

Модульна арифметика — це система арифметики цілих чисел, в якій числа "обертаються навколо" деякого значення, що називається **модулем**.

Ще один підхід до модульної арифметики пов'язаний з остачами від ділення цілих чисел на певне задане натуральне число і розглядаються класи еквівалентності ([1, 5, 10, 25, 18]).

5.1 Відношення порівняння

Нехай $m > 1$ — ціле додатне число, яке назвемо **модулем**.

Означення 5.1.
*Два числа a та b називаються **порівнянними за модулем m**, якщо їх різниця $a - b$ ділиться без остачі на число m.*

Таке співвідношення між числами a та b називається **порівнянням** чисел та записують

$$a \equiv b \mod m.$$

В такому записі про число a кажуть, що це — **лишок числа b за модулем m**. Запис $a \mod m$ означає лишок числа a, який рівний деякому цілому числу від 0 до $m - 1$. Операція $a \mod m$ називається **зведенням числа a за модулем m**.

Властивості відношення порівняння

- рефлексивність: $a \equiv a \mod m$ для будь–якого числа m;
- симетричність: якщо $a \equiv b \mod m$, то $b \equiv a \mod m$;

- транзитивність: якщо $a \equiv b \mod m$ та $c \equiv b \mod m$, то $a \equiv c \mod m$;
- якщо $a \equiv b \mod m$ і k — довільне ціле число, то $ka \equiv kb \mod m$;
- якщо $ka \equiv kb \mod m$, а k і m взаємно прості числа, то $a \equiv b \mod m$;
- якщо $a \equiv b \mod m$ і k — довільне натуральне число, то $ka \equiv kb \mod km$;
- Якщо $a \equiv b \mod m$ та $c \equiv d \mod m$, тоді $a \pm c \equiv b \pm d \mod m$;
- Будь–який доданок лівої та правої частин порівняння можна переносити з протилежним знаком в іншу частину, тобто:

  1) якщо $a \equiv b + c \mod m$, то $a - b \equiv c \mod m$, $a - c \equiv b \mod m$;

  2) якщо $a + b \equiv c \mod m$, то $a \equiv c - b \mod m$;
- Якщо $a \equiv b \mod m$, то $a^n \equiv b^n \mod m$ для будь–якого цілого $n \geqslant 0$;
- Якщо $a \equiv b \mod m$ і

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

  довільний багаточлен із цілими коефіцієнтами, то

$$f(a) \equiv f(b) \mod m.$$

Задача 5.1.
Чи будуть порівнянними за модулем 29 *такі числа* $-56, -43, -27, -14, 2, 60, 89, 102, 160$.

Розв'язання. Перевіряємо, чи ділиться без остачі різниця двох чисел $a - b$ на число 29. Візьмемо число -56. Тоді

$$(-43 + 56)/29 = 13/29; \qquad (-27 + 56)/29 = 1;$$

$$(-14 + 56)/29 = 42/29; \qquad (2 + 56)/29 = 2;$$

$$(60 + 56)/29 = 4; \qquad (89 + 56)/29 = 5;$$

$$(102+56)/29 = 158/29; \qquad (160+56)/29 = 216/29.$$

Отже, число -56 порівнянне за модулем 29 з числами $-27, 2, 60, 89$. В силу транзитивності відношення порівняння маємо, що всі числа із множини $A = \{-56, -27, 2, 60, 89\}$ попарно порівнянні за модулем 29.

Беремо число -43 і порівняємо його із числами, що не належать множині A .

$$(-14+43)/29 = 1; \quad (102+43)/29 = 5; \quad (160+43)/29 = 7.$$

Маємо, що число -43 порівнянне з числами $-14, 102, 160$ по модулю 29. Знову, в силу властивості транзитивності відношення порівняння, числа із множини $B = \{-43, -14, 102, 160\}$ попарно порівнянні по модулю 29.

$\triangle$

Задача 5.2.

Звести числа за модулем:

a) $123 \mod 47$*;* *b)* $-23 \mod 17$*;*

Розв'язання. a) Оскільки $123 = 2 \cdot 47 + 29$, то $123 \equiv 29 \mod 47$.

b) Аналогічно $-23 \equiv 34 - 23 \equiv 11 \mod 17$.

$\triangle$

Задача 5.3.

Довести, що для довільного натурального n число

$$a = 37^{n+2} + 16^{n+1} + 23^n$$

ділиться на 7.

Розв'язання. Нам потрібно показати, що остача від ділення числа a на 7 рівна 0. Виконаємо зведення по модулю 7. Маємо:

$$37 \equiv 2 \mod 7, \quad 16 \equiv 2 \mod 7, \quad 23 \equiv 2 \mod 7.$$

Тоді

$$37^{n+2} \equiv 2^{n+2} \mod 7,$$
$$16^{n+1} \equiv 2^{n+1} \mod 7,$$
$$23^n \equiv 2^2 \mod 7.$$

Використаємо властивість відношення порівняння. Маємо

$$37^{n+2} + 16^{n+1} + 23^n \equiv 2^{n+2} + 2^{n+1} + 2^n \mod 7,$$

$$37^{n+2} + 16^{n+1} + 23^n \equiv 2^n(4+2+1) \mod 7,$$

$$37^{n+2} + 16^{n+1} + 23^n \equiv 2^n \cdot 7 \mod 7 \equiv 0 \mod 7,$$

Отже,

$$37^{n+2} + 16^{n+1} + 23^n$$

ділиться на 7 для довільного натурального n.

$\triangle$

5.2 Адитивний ланцюг

Обчислення за модулем досить часто використовується в криптографії, оскільки його зручно реалізовувати на комп'ютері і скорочується діапазон проміжних значень і результатів. У процесі обчислень відбувається заміна будь–яких проміжних результатів на інші числа, які порівняльні з ним за модулем. Проілюструємо це на прикладах.

Приклад 5.1.
Потрібно обчислити $a^{16} \mod m$. *Але ми не будемо виконувати* 15 *множень та одне зведення великого числа за модулем*

$$a^{16} \mod m = \underbrace{a \cdot a \cdots a}_{15 \text{ раз}} \mod m,$$

а використаємо так званий ***адитивний ланцюг****. При використанні адитивного ланцюга потрібно буде виконати* 4 *множення і стільки ж зведень за модулем. При цьому, проміжні результати не будуть такими об'ємними:*

$$a^{16} \mod m = (((a^2 \mod m)^2 \mod m)^2 \mod m)^2 \mod m.$$

Задача 5.4.
Довести, що

$$3^{105} + 4^{105}$$

ділиться на 181.

Розв'язання. Для обчислення значення кожного із доданків утворимо адитивний ланцюг по модулую 181.

$$3^{105} = 3^{3 \cdot 5 \cdot 7} \equiv ((3^7 \mod 181)^5 \mod 181)^3 \mod 181 \equiv$$

$$\equiv ((2187 \mod 181)^5 \mod 181)^3 \mod 181 \equiv$$
$$\equiv ((15)^5 \mod 181)^3 \mod 181 \equiv$$
$$\equiv (759375 \mod 181)^3 \mod 181 \equiv$$
$$\equiv (80)^3 \mod 181 = 512000 \mod 181 \equiv 132 \mod 181 .$$
$$4^{105} = (4)^{3\cdot 5\cdot 7} \equiv ((4^7 \mod 181)^5 \mod 181)^3 \mod 181 \equiv$$
$$\equiv ((16384 \mod 181)^5 \mod 181)^3 \mod 181 \equiv$$
$$\equiv (94^5 \mod 181)^3 \mod 181 \equiv$$
$$\equiv (7339040224 \mod 181)^3 \mod 181 \equiv$$
$$\equiv 101^3 \mod 181 \equiv 1030301 \mod 181 \equiv 49 \mod 181 .$$

Таким чином

$$(3^{105} + 4^{105}) \mod 181 \equiv 132 \mod 181 + 49 \mod 181 =$$
$$= 181 \mod 181 \equiv 0 \mod 181 .$$

Отже довели, що $3^{105} + 4^{105}$ ділиться на 105.

$\triangle$

5.3 Клас лишків Z_m за модулем m

Відношення еквівалентності розбиває числову множину, на якій воно визначено, на **класи еквівалентності**. Всі числа, що належать одному класу, мають однакову, спільну остачу r при діленні на m. Довільне число із цього класу називається **лишком за модулем** m. Класи еквівалентності (класи лишків) позначають

$$\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{m-1}.$$

Клас лишків за модулем m, що містить число a позначається $\bar{a}$. Він є множиною чисел вигляду

$$a + km, \quad k \in \mathbb{Z},$$

число a називають **представником** цього класу:

$$\begin{aligned}
\bar{0} &= \{\ldots, -2m, -m, 0, m, 2m, \ldots\},\\
\bar{1} &= \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\},\\
&\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots\\
\overline{m-1} &= \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots\},
\end{aligned}$$

Із означення класу лишків випливає, що всім числам класу відповідає одна і та ж остача a.

Властивості класів лишків за даним модулем

1. Усі лишки одного і того ж класу порівнянні одним з одним за модулем m, а лишки різних класів — ні.

2. Кожен клас лишків містить нескінченну множину чисел.

   Кожне ціле число можна порівняти за модулем m тільки з одним із чисел $0, 1, 2, \ldots, m-1$.

   Приклад 5.2.
   За модулем 5 *можна назвати* 5 *наступних класів:*

$$\begin{aligned}
\bar{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\},\\
\bar{1} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\},\\
\bar{2} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\},\\
\bar{3} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\},\\
\bar{4} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

3. Якщо два класи мають принаймні одне спільне число, то вони збігаються.

4. Усі лишки одного класу $\bar{a}$ за модулем m мають із числом m однаковий найбільший спільний дільник.

Задача 5.5.
Визначити до якого класу лишків за модулем 17 *належать числа*

$$\{23, 38, 49, -3, -10, -24\}.$$

Розв'язання. Оскільки

$$23 = 17 + 6 \equiv 6 \mod 17,$$

то число 23 належить класу $\bar{6}$. Далі маємо, що

$$38 = 2 \cdot 17 + 4 \equiv 4 \mod 17.$$

Тоді число 38 належить класу $\bar{4}$. Аналогічно

$$49 = 2 \cdot 17 + 15 \equiv 15 \mod 17.$$

Число 49 належить класу $\overline{15}$. Так як

$$-3 = -17 + 14 \equiv 14 \mod 17,$$

то число (-3) належить класу $\overline{14}$. Із порівняння

$$-10 = -17 + 7 \equiv 7 \mod 17,$$

то число (-10) належить класу $\bar{7}$. Насамкінець

$$-24 = -2 \cdot 17 + 10 \equiv 10 \mod 17,$$

то число (-24) належить класу $\overline{10}$.

$\triangle$

Нехай $m \in \mathbb{N}$ — деяке натуральне число. Через Z_m позначимо множину чисел

$$Z_m = \{0, 1, 2, \ldots, m-1\},$$

яка є повною системою найменших невід'ємних лишків за модулем m і утворює множину класів лишків за модулем $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$.

На множині Z_m вводять дві операції, які називають **додаванням** та **множенням** класів лишків за модулем і позначають „$+$" та „$\cdot$". Для вказаних операцій покладемо

$$\begin{aligned} \bar{a} + \bar{b} &= \overline{a+b}, && \text{якщо } a + b < m; \\ \bar{a} + \bar{b} &= \overline{a+b-m}, && \text{якщо } a + b \geqslant m; \\ \bar{a} \cdot \bar{b} &= \bar{r}, && \text{де } a \cdot b = mq + r,\ 0 \leqslant r < m. \end{aligned}$$

За означенням, сумою і добутком класів $\bar{a}$ та $\bar{b}$ будуть класи чисел, які містять числа $a + b$ та $a \cdot b$.

Клас лишків $\overline{-a}$ називається **протилежним класу** $\bar{a}$. На множині Z_m маємо: $\overline{-a} = \overline{m-a}$.

Додавання та множення класів лишків зручно задавати за допомогою таблиць Кейлі.

Приклад 5.3.
Визначимо таблиці Кейлі операцій додавання та множення класів лишків $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ *за модулем* 5 *(таблиці на стор. 95).*

Приклад 5.4.
Визначимо таблиці Кейлі операцій додавання та множення класів лишків $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ *за модулем* 6.

На відміну від попереднього випадку число 6 *є складеним, а тому таблиці Кейлі мають вигляд (див. стор. 95). В середині таблиці Кейлі множення класів лишків з'явилися нулі.*

Таблиці Келі задачі 5.3

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

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Таблиці Келі задачі 5.4

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

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Множина класів лишків $\boldsymbol{Z_m}$ за модулем $\boldsymbol{m}$, що складається рівно із $\boldsymbol{m}$ елементів, відносно операцій додавання та множення є скінчене комутативне **кільцем класів лишків** за модулем $\boldsymbol{m}$ з одиницею.

Означення 5.2.
*Елемент кільця $\boldsymbol{Z_m}$, який позначається $\boldsymbol{a^{-1}}$ називається **оберненим** до елемента $\boldsymbol{a}$ у кільці $\boldsymbol{Z_m}$, а саме число $\boldsymbol{a}$ називається **оборотним**, якщо виконується рівність*

$$\boldsymbol{a \cdot a^{-1} \equiv 1 \mod m}, \quad \textit{або} \quad \boldsymbol{1 \equiv a \cdot a^{-1} \mod m}.$$

У кільці лишків за модулем $\boldsymbol{m}$ можуть бути дільники нуля тоді і тільки тоді, коли $\boldsymbol{m}$ — складене число. Кільце лишків за простим модулем не містить дільників нуля. В цьому можна пересвідчитися, якщо звернутися до наведених вище прикладів.

Означення 5.3.
Множина елементів в Z_m, для яких у цьому кільці існують обернені елементи відносно множення, утворюють мультиплікативну групу Z_m^*.

Теорема 8 (Про будову групи Z_m^*).
Елементами групи Z_m^* будуть тільки взаємно прості за модулем m елементи a кільця Z_m.

Теорема 9 (Ойлера).
Для будь–якого модуля m і будь–якого $a \geqslant 1$, яке взаємно просте з числом m, вірним є порівняння

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

Теорема 10 (Ферма).
Для будь–якого простого p і будь–якого $a \geqslant 1$, яке не ділиться на p, вірним є порівняння

$$a^{p-1} \equiv 1 \mod m.$$

Теорема Ферма є частинним випадком теореми Ойлера, бо якщо $p-$ просте число, то $\varphi(p) = p - 1$.

5.4 Відшукання оберненого елемента за модулем

Ідея розширеного евклідового алгоритму, який запропонований відомим американським вченим Дональдом Кнутом, полягає в тому, щоб на кожному кроці алгоритму відшукання **НСД**(a, b) подати залишок r_j у вигляді комбінації діленого a і дільника b, тобто

$$\begin{array}{ll}
a = bq_1 + r_1, & r_1 = ax_1 + by_1, \\
b = r_1q_2 + r_2, & r_2 = ax_2 + by_2, \\
r_1 = r_2q_3 + r_3, & r_3 = ax_3 + by_3, \\
\vdots & \vdots \\
r_{j-1} = r_jq_{j+1} + r_{j+1}, & r_{j+1} = ax_{j+1} + by_{j+1}, \\
\vdots & \vdots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, & r_{n-1} = ax_{n-1} + by_{n-1}, \\
r_{n-2} = r_{n-1}q_n, & r_n = 0.
\end{array}$$

Числа x_j та y_j визначаються за рекурентними формулами

$$x_j = x_{j-2} - q_jx_{j-1}, \quad y_j = y_{j-2} - q_jy_{j-1}, \quad j = 1, 2, \ldots, n, \qquad (5.1)$$

при початкових значеннях $x_{-1}=1, y_{-1}=0, x_0=0, y_0=1$.

Задача 5.6.
За допомогою розширеного евклідового алгоритму, знайти d=**НСД**(a,b) *та числа* α *і* β *у співвідношенні* $\alpha a+\beta b=d$, *якщо* $a=168156, b=38925$.

Розв'язання. Скористаємося формулами (5.1).

$$\begin{aligned}
&168156=4\cdot 38925+12456, && x_1=1-4\cdot 0=1, && y_1=0-4\cdot 1=-4,\\
&38925=3\cdot 12456+1557, && x_2=0-3\cdot 1=-3, && y_2=1+3\cdot 4=13,\\
&12456=8\cdot 1557+0. &&&&
\end{aligned}$$

Отримали

$$\alpha=-3,\quad \beta=13,\qquad -3\cdot 168156+13\cdot 38925=1557,$$

d=**НСД**$(168156, 38925)$=1557.

△

Коли числа m та a взаємно прості, то **НСД**$(m,a)=1$. Згідно із розширеним евклідовим алгоритмом для a та m знайдуться такі числа α, β, що $\alpha\cdot m+\beta\cdot a=1$, а це в Z_m^* еквівалентно тотожності

$$\beta\cdot a\equiv 1 \mod m,\qquad \text{тобто}\quad \beta=a^{-1}.$$

Задача 5.7.
За розширеним евклідовим алгоритмом, знайти елемент, який обернений до елемента 173 *у кільці лишків* Z_{659}^*.

Розв'язання. За допомогою розширеного евклідового алгоритму знайдемо **НСД**$(659, 173)$ та числа α, β:

$$\begin{aligned}
&659=173\cdot 3+140, && x_1=1-0=1, && y_1=0-3=-3;\\
&173=140\cdot 1+33, && x_2=0-1=-1, && y_2=1+3=4;\\
&140=33\cdot 4+8, && x_3=1+4=5, && y_3=-3-16=-19;\\
&33=8\cdot 4+1, && x_4=-1-20=-21, && y_4=4+76=80;\\
&8=8\cdot 1+0. &&&&
\end{aligned}$$

Отже, $\text{НСД}(659, 173)=1,\ (-21)\cdot 659+80\cdot 173=1,\ \beta=80$

$$80\cdot 173\equiv 1 \mod 659 \Rightarrow 173^{-1} \mod 659=80 \mod 659.$$

△

Згідно із теоремою Ойлера для будь–якого модуля m і будь–якого числа $a \geqslant 1$, яке взаємно просте з числом m, справедливе порівняння

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

а звідки

$$a^{-1} \equiv a^{\varphi(m)-1} \mod m.$$

Задача 5.8.
За допомогою теореми Ойлера знайти обернений елемент до елемента 7 *у кільці лишків* Z_{13}^*.

Розв'язання. Оскільки модуль 13 — просте число, то

$$\varphi(13) = 13 - 1 = 12, \quad \text{звідки} \quad 7^{-1} \mod 13 \equiv 7^{11} \mod 13 =$$

$$\equiv 7^{11} \mod 13 = 1977326743 \mod 13 =$$

$$= 152102057 \cdot 13 + 2 \mod 13 = 2 \mod 13.$$

Отже,

$$7^{-1} \mod 13 \equiv 2 \mod 13.$$

$\triangle$

5.5 Питання, тести та вправи до розділу 5

5.5.1 Питання до розділу 5

1. Коли два числа a та b порівнянні за модулем m?
2. Дайте означення операції зведення числа за модулем.
3. Сформулюйте властивості рефлексивності, симетричності та транзитивності відношення порівняння.
4. Коли можна скорочувати на спільний множник у порівняннях за модулем?
5. Сформулюйте умови, при виконанні яких можна домножувати всі частини відношення порівняння.
6. Як здійснюється додавання чи віднімання відношення порівняння?
7. Вкажіть правила перенесення доданків з різних частин порівняння.

8. Сформулюйте метод піднесення до цілого степеня частин порівняння.
9. Дайте означення класів лишків.
10. Як визначаються операції додавання та множення класів лишків за модулем?
11. Який клас лишків називається протилежним і як він визначається?
12. Дайте означення оберненого елемента в кільці $\boldsymbol{Z_m}$.
13. Коли кільце лишків за модулем не містить дільників нуля?
14. З чого складається мультиплікативна група $\boldsymbol{Z_m^*}$?
15. Сформулюйте теорему Ойлера для модуля $\boldsymbol{m}$.
16. Сформулюйте теорему Ферма для простого числа $\boldsymbol{p}$.

5.5.2 Тести до розділу 5

Вказати правильну відповідь на кожен тест.

1. Чи буде число $\mathbf{10}$ порівняним із числом $\mathbf{7}$ за модулем $\mathbf{3}$

   (A) так; **(B)** ні; **(C)** не завжди.

2. Якщо $\boldsymbol{a \equiv b \mod m}$, то $\boldsymbol{b \equiv a \mod m}$ виконується:

   (A) завжди; **(B)** ніколи; **(C)** якщо $\boldsymbol{m}$ просте.

3. Якщо $\boldsymbol{a \equiv b \mod m}$ і $\boldsymbol{a \equiv c \mod m}$. Тоді порівняння $\boldsymbol{c \equiv b \mod m}$ має місце коли $\boldsymbol{m}$:

   (A) парне; **(B)** просте; **(C)** довільне.

4. Якщо $\boldsymbol{ka \equiv kb \mod m}$. Порівняння $\boldsymbol{a \equiv b \mod m}$ вірне, якщо:

   (A) $\boldsymbol{m}$ — просте число;

   (B) $\boldsymbol{k}$ — довільне число;

   (C) $\boldsymbol{k}$ та $\boldsymbol{m}$ — взаємно прості числа.

5. Якщо $\boldsymbol{a \equiv b \mod m}$ і $\boldsymbol{k}$ деяке натуральне число. Яке порівняння вірне:

   (A) $\boldsymbol{ka \equiv kb \mod m}$;

(B) $ka \equiv b \mod km$;

(C) $ka \equiv kb \mod km$.

6. Нехай $a \equiv b \mod m$ і $c \equiv d \mod m$. Буде виконуватися порівняння $a \pm c \equiv b \pm d \mod m$, якщо

   (A) m — просте число;

   (B) a та c і b та d — взаємно прості;

   (C) для довільних a, b, c, d.

7. Якщо $a \equiv b \mod m$. Порівняння $a^n \equiv b^n \mod m$ виконується, коли n:

   (A) $n \geqslant 0$; **(B)** $n \in \mathbb{Z}$; **(C)** n — просте.

8. Два числа a та b належать одному класу еквівалентності за модулем m. Тоді остача від ділення цих чисел на m буде:

   (A) кратна m; **(B)** різна; **(C)** однакова.

9. Клас лишків $\bar{a}$ за модулем m містить:

   (A) m елементів; **(B)** $2m$ елементів; **(C)** нескінчену кількість.

10. Число c належить двом класам лишків $\bar{a}$ та $\bar{b}$. Яке твердження вірне:

    (A) класи лишків перетинаються;

    (B) класи лишків збігаються;

    (C) класи лишків не мають інших спільних елементів.

11. Множина класів лишків Z_m відносно операцій додавання та множення буде:

    (A) комутативне кільце без одиниці; **(B)** не комутативне кільце;

    (C) комутативне кільце з одиницею.

12. Елемент a^{-1} кільця Z_m називається оберненим, якщо

    (A) $a \cdot a^{-1} = 1$; **(B)** $a + a^{-1} = 0$; **(C)** $a \cdot a^{-1} \equiv 1 \mod m$.

13. Серед елементів групи Z_m^* будуть лише:

    (A) не нульові елементи кільця Z_m;

    (B) взаємно прості елементи кільця Z_m;

    (C) не нульові елементи кільця Z_m.

5.5.3 Вправи до розділу 5

Вправа 5.1.
Які числа множини

$$A = \{-68, -34, -31, -29, 8, 40, 43, 45, 80, 82, 114, 119, 154\}$$

будуть порівнянними за модулем 37.

Вправа 5.2.
Звести числа за модулем.
1) $23 \mod 17$; *2)* $64 \mod 31$; *3)* $-23 \mod 13$; *4)* $-3 \mod 7$; *5)* $-67 \mod 19$.

Вправа 5.3.
Знайти остачу від ділення числа $9^{75} - 95$ *на* 7.

Вправа 5.4.
Переконатися, що вірним є порівняння

$$8^{30} \equiv 34 \mod 55.$$

Вправа 5.5.
Знайти залишок від ділення

$$(9674^6 + 28)^{15}$$

на число 39.

Вправа 5.6.
Визначити до якого класу лишків за модулем 19 *належать числа*

$$\{21, 38, 44, -2, -8, -14\}.$$

Вправа 5.7.
Перевірити чи належать числа

$$\{25, -2, 48, -21, 33, -13\}$$

до одного класу лишків за модулем 23.

Вправа 5.8.
Побудувати таблиці Кейлі додавання та множення класів лишків

$$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$$

за модулем 7.

Вправа 5.9.
Побудувати таблиці Кейлі додавання та множення класів лишків

$$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$$

за модулем 8.

Вправа 5.10.
За допомогою розширеного евклідова алгоритму знайти d=$НСД(a, b)$ *та числа* α, β *у рівності* $\alpha \cdot a + \beta \cdot b = d$, *коли*

$$a = 116675,\ b = 90468.$$

Вправа 5.11.
Використовуючи розширений евклідів алгоритм знайти d=$НСД(a, b)$ *та числа* α, β *у рівності* $\alpha \cdot a + \beta \cdot b = d$, *коли*

$$a = 827793,\ b = 275094.$$

Вправа 5.12.
За розширеним евклідовим алгоритмом знайти елемент, що обернений до елемента 233 *у кільці лишків* Z^*_{719}.

Вправа 5.13.
Використовуючи розширений евклідів алгоритм знайти у кільці лишків Z^*_{761} *обернений елемент до* 443.

Вправа 5.14.
За допомогою теореми Ойлера знайти обернений елемент до елемента 9 *у кільці лишків* Z^*_{11}.

Вправа 5.15.
За допомогою теореми Ойлера знайти до елемента 12 *у кільці лишків* Z^*_{17} *обернений елемент.*

Розділ 6

Многочлени

У математиці **многочлен** від однієї чи багатьох змінних — це вираз, що складається з невідомих змінних і коефіцієнтів, який включає лише операції додавання, віднімання, множення та цілі додатні степені змінних.

Множина многочленів, коефіцієнти яких належать кільцю цілих, раціональних або дійсних чисел, відносно операції додавання та множення володіють тими ж властивостями, що і множина цілих чисел $\mathbb{Z}$ відносно операцій додавання та множення цілих чисел ([12, 11]).

6.1 Операції над многочленами

Означення 6.1.
Многочленом (багаточленом, поліномом) *степеня* n *відносно змінної* x *називається вираз*

$$f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = \sum_{i=0}^{n} a_i x^{n-i}, \qquad (6.1)$$

де $a_i (0 \leqslant i \leqslant n)$ *— коефіцієнти многочлена,* $a_0 \neq 0$ *— старший коефіцієнт,* a_n *— вільний член.*

Відносно коефіцієнтів многочлена припускають, що вони належать деякому кільцю $\mathbf{K}$ або полю $\mathbf{F}$. Наприклад полю дійсних $\mathbb{R}$, раціональних $\mathbb{Q}$ або комплексних $\mathbb{C}$ чисел. Тоді кажуть, що многочлен заданий над полем або над кільцем.

Деколи многочлен записують не тільки за спадними степенями x, а також степенями зростання:

$$f_n(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n = \sum_{i=0}^{n} b_i x^i. \qquad (6.2)$$

Зауваження 6.1.
Многочлен (6.1) *(або* (6.2)*) називається* ***нормованим (зведеним)****, якщо коефіцієнт при старшому степені рівний* ***1****, тобто коли* $a_0 = 1$ *(або* $b_n = 1$*).*

Задача 6.1.
Знайти нормований (зведений) многочлен для многочлена

$$f_5(x) = 3x^5 + 6x^4 - 9x^3 + 7x^2 - 2x - 1.$$

Розв'язання. Розділивши всі коефіцієнти многочлена $f_5(x)$ на старший коефіцієнт, будемо мати

$$p_5(x) = x^5 + 2x^4 - 3x^3 + \frac{7}{3}x^2 - \frac{2}{3}x - \frac{1}{3}.$$

Многочлен $p_5(x)$ буде нормованим (зведеним) многочленом, який відповідний многочлену $f_5(x)$.

△

Всяке число, яке відмінне від нуля буде **многочленом нульової степені** $f_0(x) = a_0, a_0 \neq 0$. Число 0 також належить до многочленів, але оскільки степінь його не визначена, то його називають **нульовим многочленом**.

Многочлен першого степеня $f_1(x) = a_0x + a_1$ називається **лінійним**, другого степеня $f_2(x) = a_0x^2 + a_1x + a_2$ – **квадратним**, третього степеня $f_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3$ – **кубічним**.

Зауваження 6.2.
Вигляд многочлена (6.2) *називають* ***канонічним****. Якщо многочлен не містить якогось степеня* x*, то у канонічному записі коефіцієнт при такому степені* x *ставлять рівним* ***0****.*

Приклад 6.1.
Многочлен

$$f_6(x) = x^6 - 3x^3 + 5x^2 + 1$$

записують у канонічному вигляді як

$$f_6(x) = x^6 + 0x^5 + 0x^4 - 3x^3 + 5x^2 + 0x + 1.$$

Коефіцієнти многочлена, який записаний в канонічному вигляді, рівні

$$a_0 = 1, a_1 = 0, a_2 = 0, a_3 = -3, a_4 = 5, a_5 = 0, a_6 = 1.$$

Задача 6.2.
Записати канонічний вигляд многочлена

$$f_7(x) = 2x^7 + 6x^4 + x.$$

Розв'язання. В записі многочлена $f_7(x)$ відсутні коефіцієнти при степенях x^6, x^5, x^3, x^2, x^0. Вважаючи, що коефіцієнти при цих степенях рівні 0, тоді многочлен може бути записаний в наступному канонічному вигляді

$$f_7(x) = 2x^7 + 0x^6 + 0x^5 + 6x^4 + 0x^3 + 0x^2 + 1x^1 + 0x^0.$$

$\triangle$

Означення 6.2.
Два многочлени

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

та

$$\varphi_m(x) = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m$$

називаються ***рівними****, якщо* $n = m$ *та* $a_i = b_i, i = 0, 1, \ldots, n$. *Рівність многочленів записують так* $f_n(x) = \varphi_n(x)$.

Протилежним *для многочлена*

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

буде многочлен

$$-f_n(x) = -a_0x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_{n-1}x - a_n.$$

Нехай маємо многочлени

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n,$$

$$\varphi_m(x) = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m,$$

$$g_k(x) = c_0x^k + c_1x^{k-1} + c_2x^{k-2} + \cdots + c_{k-1}x + c_k.$$

Означення 6.3.
Сумою *многочленів* $f_n(x)$ *та* $\varphi_m(x)$ *називається многочлен*

$$g_k(x) = f_n(x) + \varphi_m(x) = c_0x^k + c_1x^{k-1} + \cdots + c_{k-1}x + c_k,$$

де $k = \max(n, m)$,

$$c_i = \begin{cases} a_i + b_i, & \text{для} \quad i \leqslant \min(n, m); \\ a_i, & \text{для} \quad \min(n, m) < i \leqslant n, \quad \text{якщо} \quad n > m; \\ b_i, & \text{для} \quad \min(n, m) < i \leqslant m, \quad \text{якщо} \quad n < m. \end{cases}$$

Означення 6.4.
Різницею *двох многочленів* $f_n(x) - \varphi_m(x)$ *називається такий многочлен* $g_k(x)$, *що* $f_n(x) = \varphi_m(x) + g_k(x)$.

Означення 6.5.
Добутком *многочленів* $f_n(x)$ *та* $\varphi_m(x)$ *називається многочлен*

$$g_{m+n}(x) = (a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n)\times$$
$$\times(b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \cdots + b_{m-1}x + b_m)$$

степеня $n + m$ *вигляду*

$$g_{m+n}(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} +$$
$$+(a_0b_2 + a_1b_1 + a_2b_0)x^{n+m-2} + \cdots + (a_0b_k + a_1b_{k-1} +$$
$$+ \cdots + a_kb_0)x^{n+m-k} + \cdots + (a_nb_{m-1} + a_{n-1}b_m)x + a_nb_m.$$

Зауваження 6.3.
Множина многочленів над кільцем K *з введеними вище операціями додавання та множення утворює кільце, яке називається* ***кільцем многочленів над*** K *і позначається* $K[x]$. *Роль нульового елемента цього кільця відіграє нульовий многочлен. Деякі властивості кільця* K *переймає кільце* $K[x]$. *Наприклад,* $K[x]$ *— комутативне кільце з одиницею лише при умові, що кільце* K, *над яким визначений многочлен, саме комутативне з одиницею, або ж кільце многочленів* $K[x]$ *не має дільників нуля, коли їх не містить кільце* K.

Задача 6.3.
Знайти суму, різницю та добуток многочленів

$$f_3(x) = 3x^3 - 4x^2 + 6x, \quad g_4(x) = -2x^4 + 5x^3 + 2x^2 - 8.$$

Розв'язання. Знаходимо суму

$$f_3(x) + g_4(x) = (3x^3 - 4x^2 + 6x) + (-2x^4 + 5x^3 + 2x^2 - 8) =$$
$$= (0 - 2)x^4 + (3 + 5)x^3 + (-4 + 2)x^2 + (6 + 0)x + (0 - 8) =$$

$$= -2x^4 + 8x^3 - 2x^2 + 6x - 8.$$

Різницею многочленів буде многочлен

$$f_3(x) - g_4(x) = (3x^3 - 4x^2 + 6x) - (-2x^4 + 5x^3 + 2x^2 - 8) =$$
$$= (0+2)x^4 + (3-5)x^3 + (-4-2)x^2 + (6-0)x + (0+8) =$$
$$= 2x^4 - 2x^3 - 6x^2 + 6x + 8.$$

Підрахуємо добуток

$$f_3(x) \times g_4(x) = (3x^3 - 4x^2 + 6x) \times (-2x^4 + 5x^3 + 2x^2 - 8) =$$
$$= (-6)x^7 + (15+8)x^6 + (6-20-12)x^5 + (-8+30)x^4 +$$
$$+(-24+12)x^3 + (32)x^2 + (-48)x + (0) =$$
$$= -6x^7 + 23x^6 - 26x^5 + 22x^4 - 12x^3 + 32x^2 - 48x.$$

$\triangle$

6.2 Ділення многочленів

Означення 6.6.
Часткою від ділення *многочлена $f_n(x)$ на многочлен $\varphi_m(x)$ називається многочлен $g_{n-m}(x)$ (при умові, що він існує), який при його множені на многочлен $\varphi_m(x)$ дає многочлен $f_n(x)$, тобто*

$$g_{n-m}(x) = \frac{f_n(x)}{\varphi_m(x)}, \qquad \text{якщо} \quad g_{n-m}(x)\varphi_m(x) = f_n(x).$$

У цьому випадку говорять, що ***многочлен $f_n(x)$ ділиться на многочлен $\varphi_m(x)$ без остачі,*** *а множники $\varphi_m(x)$ та $g_{n-m}(x)$ називаються* ***дільниками многочлена $f_n(x)$.***

Якщо многочлен $f_n(x)$ не ділиться націло на многочлен $\varphi_m(x)$, то вводять операцію **ділення многочленів з остачею**.

Для будь–яких многочленів $f_n(x)$ та $\varphi_m(x)$ існують і визначаються єдиним способом многочлени $q_{n-m}(x)$ та $r_k(x)$, для яких

$$f_n(x) = q_{n-m}(x)\varphi_m(x) + r_k(x), \qquad \text{де} \quad k < m. \tag{6.3}$$

Многочлен $q_{n-m}(x)$ називається **часткою**, а многочлен $r_k(x)$ — **остачею від ділення** многочлена $f_n(x)$ на $\varphi_m(x)$.

Властивості ділення многочленів

1. Якщо многочлен $f_n(x)$ ділиться націло на многочлен $\varphi_m(x)$, а многочлен $\varphi_m(x)$ ділиться націло на многочлен $g_k(x)$, то многочлен $f_n(x)$ ділиться націло на многочлен $g_k(x)$.

2. Якщо многочлени $f_n(x)$ і $\varphi_m(x)$ діляться націло на многочлен $g_k(x)$, то $f_n(x) \pm \varphi_m(x)$ буде ділитися націло на $g_k(x)$, а добуток многочленів $f_n(x)\varphi_m(x)$ – на многочлен $g_k^2(x)$.

3. Якщо многочлен $f_n(x)$ ділиться націло на многочлен $\varphi_m(x)$, то добуток многочлена $f_n(x)$ на будь–який многочлен $g_k(x)$ також буде ділитися націло на многочлен $\varphi_m(x)$.

4. Якщо добуток $\varphi_m(x)g_k(x)$ ділиться націло на двочлен $x - \alpha$, то принаймні один із многочленів $\varphi_m(x)$ чи $g_k(x)$ ділиться націло на $x - \alpha \neq 0$.

На практиці многочлен ділять на многочлен або методом **"ділення кутом"**, або метод **невизначених коефіцієнтів**. Проілюструємо кожен із них на прикладах.

Задача 6.4.
Розділити $f_5(x) = 2x^5 - 3x^4 + 5x^3 + x^2 + 3x + 28$ *на многочлен* $\varphi_3(x) = 2x^3 + 3x^2 + 6x + 7$.

Розв'язання.

$$
\begin{array}{rl|l}
2x^5-3x^4+5x^3+\ \ x^2+\ 3x+28 & & 2x^3+3x^2+6x+7 \\
\cline{3-3}
-\ \underline{2x^5+3x^4+6x^3+\ 7x^2} & & x^2-3x+4 \\
\cline{1-1}
\quad -6x^4-\ \ x^3-\ 6x^2+\ 3x & & \\
-\ \underline{-6x^4-9x^3-18x^2-21x} & & \\
\quad\ \ 8x^3+12x^2+24x+28 & & \\
-\ \underline{8x^3+12x^2+24x+28} & & \\
\quad\ \ 0 & &
\end{array}
$$

$\triangle$

Задача 6.5.
За допомогою методу ***"ділення кутом"*** *розділити з остачею многочлен*

$$f_6(x) = x^6 - x^5 + x^4 + 3x^3 + x - 8$$

на многочлен

$$g_3(x) = x^3 + 2x^2 + 3x + 4.$$

Розв'язання. Аналогічно виконуємо дії.

$$\begin{array}{r} x^6 - x^5 + x^4 + 3x^3 + 0x^2 + x - 8 \\ \underline{-x^6 + 2x^5 + 3x^4 + 4x^3} \\ -3x^5 - 2x^4 - x^3 + 0x^2 \\ \underline{-3x^5 - 6x^4 - 9x^3 - 12x^2} \\ 4x^4 + 8x^3 + 12x^2 + x \\ \underline{4x^4 + 8x^3 + 12x^2 + 16x} \\ -15x - 8 \end{array} \left| \begin{array}{l} x^3 + 2x^2 + 3x + 4 \\ \hline x^3 - 3x^2 + 4x \end{array} \right.$$

Отримали частку

$$q_3(x) = x^3 - 3x^2 + 4x$$

і остачу

$$r_1(x) = -15x - 8.$$

Має місце рівність

$$x^6 - x^5 + x^4 + 3x^2 + x - 8 =$$

$$= (x^3 + 2x^2 + 3x + 4)(x^3 - 3x^2 + 4x) - 15x - 8.$$

$\triangle$

Задача 6.6.

За допомогою методу ***"невизначених коефіцієнтів"*** *розділити з остачею многочлен*

$$f_5(x) = x^5 + 4x^3 - 5x^2 + x - 7$$

на многочлен

$$g_3(x) = x^3 - 6x^2 + 8x - 4.$$

Розв'язання. Згідно із (6.3) маємо, що

$$f_5(x) = q_2(x)g_3(x) + r_2(x),$$

де коефіцієнти многочленів $q_2(x), r_2(x)$ потрібно знайти. Маємо

$$x^5 + 4x^3 - 5x^2 + x - 7 = (Ax^2 + Bx + C)(x^3 - 6x^2 + 8x - 4) +$$

$$+ Dx^2 + Ex + F.$$

У правій частині зведемо коефіцієнти при однакових степенях x. Отримуємо

$$x^5 + 0x^4 + 4x^3 - 5x^2 + x - 7 = Ax^5 + (-6A + B)x^4 + \\ +(8A - 6B + C)x^3 + (-4A + 8B - 6C + D)x^2 + \\ +(-4B + 8C + E)x + (-4C + F).$$

Прирівнюємо коефіцієнти при однакових степенях x в лівій та правій частинах рівності.

x^5	$1 = A$	$A = 1$
x^4	$0 = -6A + B$	$B = 6$
x^3	$4 = 8A - 6B + C$	$C = 32$
x^2	$-5 = -4A + 8B - 6C + D$	$D = 143$
x	$1 = -4B + 8C + E$	$E = -231$
x^0	$-7 = -4C + F$	$F = 121$

Отримали, що частка від ділення $q_2(x) = x^2 + 6x + 32$ і остача від ділення $r_2(x) = 143x^2 - 231x + 121$.

△

Схема Горнера є наслідком методу невизначених коефіцієнтів і використовується при діленні многочлена $f_n(x)$ на двочлен $x - c$, де c — стала. Згідно із формулою (6.3), якщо

$$f_n(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x^1 + a_n,$$

то

$$f_n(x) = q_{n-1}(x)(x - c) + r,$$

де

$$q_{n-1}(x) = b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-2}x + b_{n-1}, \quad r = \text{const}.$$

Коефіцієнти $b_0, b_1, \ldots, b_{n-1}$ та стала r визначаються за формулами:

$$b_0 = a_0; \quad b_k = a_k + cb_{k-1}; \quad k = 1, 2, \ldots, n-1; \quad r = a_n + cb_{n-1}.$$

Процес ділення за схемою Горнера записують у вигляді таблиці.

	a_0	a_1	$\ldots$	a_{n-1}	a_n
c	$b_0 = a_0$	$b_1 = a_1 + cb_0$	$\ldots$	$b_{n-1} = a_{n-1} + cb_{n-2}$	$r = a_n + cb_{n-1}$

У верхньому рядку таблиці містяться коефіцієнти многочлена $f_n(x)$, який записаний у канонічному вигляді за степенями x, а у нижньому — коефіцієнти многочлена частки $q_{n-1}(x)$ та остача r.

Задача 6.7.
За допомогою схеми Горнера знайти частку та остачу від ділення многочлена

$$f_5(x) = 2x^5 + 3x^3 - 2x + 6$$

на двочлен $x + 3$.

Розв'язання. Запишемо многочлен $f_5(x)$ у канонічному вигляді

$$f_5(x) = 2x^5 + 0x^4 + 3x^3 + 0x^2 - 2x + 6,$$

і застосуємо схему Горнера при $c = -3$

$c = -3$						
a_i	2	0	3	0	-2	6
b_i, r	2	-6	21	-63	187	-555

Отримали частку $q_4(x) = 2x^4 - 6x^3 + 21x^2 - 63x + 187$ і остачу від ділення $r = -555$.

$\triangle$

6.3 Евклідів алгоритм знаходження найбільшого спільного дільника двох многочленів

Означення 6.7.
Многочлен $g_k(x)$ *називається* ***спільним дільником*** *двох многочленів* $f_n(x)$, $\varphi_m(x)$, *якщо він є дільником кожного із них.*

Усі многочлени нульового степеня будуть спільними дільниками будь–яких двох многочленів $f_n(x)$ і $\varphi_m(x)$. Якщо ці два многочлени не мають інших спільних дільників, то вони називаються **взаємно простими**.

Означення 6.8.
Спільний дільник двох многочленів називається ***найбільшим спільним дільником (НСД)****, якщо він ділиться на будь–який інший спільний дільник цих многочленів.*

НСД многочленів $f_n(x)$ та $\varphi_m(x)$ визначається з точністю до сталого множника, який відмінний від нуля, і позначається $d(f_n(x); \varphi_m(x))$ або **НСД**$(f_n(x); \varphi_m(x))$.

Властивості найбільшого спільного дільника многочленів

1. Множина всіх дільників **НСД** многочленів $f_n(x)$ та $\varphi_m(x)$ збігається із множиною всіх спільних дільників цих многочленів.
2. Якщо $d(x) = \text{НСД}(f_n(x); \varphi_m(x))$, то найбільшими спільними дільниками многочленів також будуть усі многочлени виду $Cd(x)$, де $C = const$.
3. Якщо многочлени $f_n(x)$ та $\varphi_m(x)$ мають раціональні або дійсні коефіцієнти, то їх **НСД** буде многочленом із раціональними або дійсними коефіцієнтами.
4. $\text{НСД}(f_n(x); \varphi_m(x); \psi_k(x)) = \text{НСД}(\text{НСД}(f_n(x); \varphi_m(x)); \psi_k(x))$.
5. Якщо $d(x) = \text{НСД}(f_n(x); \varphi_m(x))$, то знайдуться такі єдині многочлени $u_p(x)$ та $v_q(x)$, що

$$f_n(x)u_p(x) + \varphi_m(x)v_q(x) = d(x),$$

де $p < m, q < n$.

НСД двох многочленів можна знайти за **евклідовим алгоритмом**, який базується лише на операції ділення многочленів з остачею.

Задача 6.8.
*За евклідовим алгоритмом знайти **НСД** многочленів*

$$f_4(x) = x^4 - 2x^3 - 4x^2 + 4x - 3, \quad \varphi_3(x) = 2x^3 - 5x^2 - 4x + 3.$$

Зауваження 6.4.
***НСД** визначається із точністю до сталого множника, відмінного від нуля. Тому в процесі застосування евклідового алгоритму, щоб спростити обчислення, многочлени та проміжні результати при діленні будемо домножати на "зручні" коефіцієнти. Такі випадки будемо помічати подвійною рискою.*

Розв'язання. Поділимо многочлен $2 \cdot f_4(x)$ на $\varphi_3(x)$:

$$\begin{array}{r|l}
2x^4 - 4x^3 - 8x^2 + 8x - 6 & 2x^3 - 5x^2 - 4x + 3 \\
\cline{2-2}
2x^4 - 5x^3 - 4x^2 + 3x & x \| + 1 \\
\cline{1-1}
x^3 - 4x^2 + 5x - 6 & \\
\cline{1-1}
2x^3 - 8x^2 + 10x - 12 & \\
2x^3 - 5x^2 - 4x + 3 & \\
\cline{1-1}
-3x^2 + 14x - 15 &
\end{array}$$

Поділимо многочлен $\varphi_3(x)$ на остачу $-3x^2+14x-15$:

$$\begin{array}{r|l}
2x^3-\ 5x^2-\ \ 4x+\ \ 3 & -3x^2+14x-15 \\
\cline{2-2}
6x^3-15x^2-\ 12x+\ \ 9 & -2\,x\| -13 \\
6x^3-28x^2+\ 30x & \\
\cline{1-1}
\ \ 13x^2-\ 42x+\ \ 9 & \\
\cline{1-1}
\ 39x^2-126x+\ 27 & \\
39x^2-182x+195 & \\
\cline{1-1}
\ \ 56x-168 & \\
\cline{1-1}
\ \ x-\ \ 3 &
\end{array}$$

Тепер поділимо многочлен $3x^2-14x+15$ на $x-3$:

$$\begin{array}{r|l}
3x^2-\ 14x+15 & x-3 \\
\cline{2-2}
3x^2-\ \ 9x & 3x-5 \\
\cline{1-1}
\ \ -5x+15 & \\
-5x+15 & \\
\cline{1-1}
\ \ 0 &
\end{array}$$

Отже, найбільший спільний дільник многочленів

$$f_4(x)=x^4-2x^3-4x^2+4x-3 \quad \text{та} \quad \varphi_3(x)=2x^3-5x^2-4x+3$$

буде $x-3$, тобто $\text{НСД}(f_4(x);\varphi_3(x))=x-3$.

$\triangle$

Задача 6.9.

*За евклідовим алгоритмом знайти **НСД** наступних многочленів*

$$f_5(x)=x^5-5x^2+x-3, \quad \varphi_3(x)=x^3-x-6.$$

Розв'язання. Знайдемо неповну частку $q_2^{(1)}(x)$ та остачу $r_2^{(1)}(x)$ при діленні $f_5(x)$ на $\varphi_3(x)$ за допомогою методу невизначених коефіцієнтів.

Нехай

$$q_2^{(1)}(x)=Ax^2+Bx+C \quad \text{і} \quad r_2^{(1)}(x)=Dx^2+Ex+F.$$

Тоді

$$x^5-5x^2+x-3=(Ax^2+Bx+C)(x^3-x-6)+Dx^2+Ex+F.$$

$$x^5-5x^2+x-3=Ax^5+Bx^4+(-A+C)x^3+$$

$$+(-6A - B + D)x^2 + (-6B - C + E)x + (-6C + F).$$

Прирівняємо коефіцієнти при однакових степенях

$$\begin{array}{c|l|l} x^5 & 1 = A & A = 1 \\ x^4 & 0 = B & B = 0 \\ x^3 & 0 = -A + C & C = 1 \\ x^2 & -5 = -6A - B + D & D = 1 \\ x^1 & 1 = -6B - C + E & E = 2 \\ x^0 & -3 = -6C + F & F = 3 \end{array}$$

Отримали:

$$q_2^{(1)}(x) = x^2 + 1, \quad r_2^{(1)}(x) = x^2 + 2x + 3. \quad r_2^{(1)}(x) \not\equiv 0.$$

Розділимо $\varphi_3(x)$ на $r_2^{(1)}(x)$. Маємо:

$$x^3 - x - 6 = (Ax + B)(x^2 + 2x + 3) + Cx + D.$$

Або

$$x^3 - x - 6 = Ax^3 + (2A + B)x^2 + (3A + 2B + C)x + 3B + D.$$

Тоді

$$\begin{array}{c|l|l} x^3 & 1 = A & A = 1 \\ x^2 & 0 = 2A + B & B = -2 \\ x^1 & -1 = 3A + 2B + C & C = 0 \\ x^0 & -6 = 3B + D & D = 0 \end{array}$$

Отже, $r_1^{(2)}(x) \equiv 0$. Тоді отримуємо $\mathbf{НСД}(f_5(x); \varphi_3(x))$=$x^2 + 2x + 3$.

$\triangle$

6.4 Корені многочленів. Звідність многочленів над полем

Означення 6.9.
Значенням многочлена

$$f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

при $x = c$ називається число, яке дорівнює

$$f_n(c) = a_0c^n + a_1c^{n-1} + \cdots + a_{n-1}c + a_n.$$

Задача 6.10.
Знайти значення многочлена

$$f_5(x) = x^5 + 4x^4 + 3x^3 + 2x^2 + x + 5$$

для $x = -2, x = -1, x = 0, x = 1, x = 2$.

Розв'язання. Коли підставити замість x значення -2, то отримаємо

$$f_5(-2) = -32 + 64 - 24 + 8 - 2 + 5 = 19.$$

Аналогічним чином

$$f_5(-1) = -1 + 4 - 3 + 2 - 1 + 5 = 6, \quad f_5(0) = 5,$$

$$f(1) = 1 + 4 + 3 + 2 + 1 + 5 = 16,$$

$$f(2) = 32 + 64 + 24 + 8 + 2 + 5 = 135.$$

△

Означення 6.10.
Коренем (нулем) многочлена $f_n(x)$ *називається число* c*, при якому числове значення многочлена рівне нулю,* $f_n(c) = 0$.

Задача 6.11.
Перевірити, чи будуть коренями многочлена

$$f_4(x) = x^4 - 4x^3 - x^2 + 16x - 12$$

числа $x_1 = 0, x_2 = -2, x_3 = 1$.

Розв'язання. Підставимо замість x значення $0, -2, 1$ і знаходимо значення.

$$f_4(0) = -12, \quad f_4(-2) = 16 + 32 - 4 - 32 - 12 = 0,$$

$$f_4(1) = 1 - 4 - 1 + 16 - 12 = 0.$$

Отримали, що числа -2 та -1 є коренями (нулями) многочлена $f_4(x)$, а число 0 — не є коренем (нулем).

△

Теорема 11 (Безу).
Остача від ділення многочлена $f_n(x)$ *на лінійний многочлен* $x - c$ *дорівнює значенню* $f_n(c)$.

Наслідок 6.1.
Число c тоді і тільки тоді корінь многочлена $f_n(x)$, якщо многочлен ділиться націло на лінійний двочлен $x - c$.

Задача 6.12.
Обчислити остачу від ділення многочлена

$$f_6(x) = 2x^6 + 7x^4 + 5x^3 - 4x + 10$$

на двочлен $x + 2$.

Розв'язання. Згідно із теоремою Безу остача від ділення буде рівна значенню $f_6(-2)$. Маємо

$$f_6(-2) = 2(-2)^6 + 7(-2)^4 + 5(-2)^3 - 4(-2) + 10 = 218.$$

$\triangle$

Означення 6.11.
*Якщо многочлен $f_n(x)$ ділиться на $(x - c)^k$, де $k \in \mathbb{N}$ і не ділиться на $(x - c)^{k+1}$, то число k називається **кратністю кореня** c. Однократний корінь многочлена ($k = 1$) називається **простим коренем**.*

Приклад 6.2.
Нехай задано многочлен

$$f_8(x) = (x - 2)^2(x + 1)^3(x - 3)(x^2 + 1).$$

Число 2 буде коренем кратності 2, число (-1) буде коренем кратності 3 і число 1 буде простим коренем многочлена.

Задача 6.13.
Довести, що многочлен

$$f_5(x) = x^5 - 7x^4 + 12x^3 + 27x - 81$$

має корінь $x = 3$ та визначити його кратність.

Розв'язання. Використаємо схему Горнера ділення многочлена на двочлен. Ділення будемо проводити до того часу, поки остача від ділення не стане відмінною від нуля.

$c = 3$						
a_i	1	-7	12	0	27	-81
b_i, r	1	-4	0	0	27	0

Остача від ділення рівна 0. Отже, $x = 3$ — корінь многочлена і має місце рівність

$$f_5(x) = (x-3)(x^4 - 4x^3 + 27).$$

Ділимо $x^4 - 4x^3 + 27$ на $x - 3$ за схемою Горнера.

$c = 3$					
a_i	1	-4	0	0	27
b_i, r	1	-1	-3	9	0

Остача від ділення рівна 0, а тоді

$$f_5(x) = (x-3)^2(x^3 - x^2 - 3x + 9).$$

Повторно розділимо $x^3 - x^2 - 3x + 9$ на $x - 3$.

$c = 3$				
a_i	1	-1	-3	-9
b_i, r	1	2	3	0

Оскільки остача знову рівна 0, то

$$f_5(x) = (x-3)^3(x^2 + 2x + 3).$$

В результаті ділення $x^2 + 2x + 3$ на $x - 3$ за схемою Горнера, отримуємо

$c = 3$			
a_i	1	2	3
b_i, r	1	5	18

Маємо остачу відмінну від нуля. Таким чином доведено, що $x = 3$ — корінь кратності 3 многочлена $f_5(x) = x^5 - 7x^4 + 12x^3 + 27x - 81$.

$\triangle$

Теорема 12 (основна теорема алгебри).
Будь–який многочлен

$$f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

степеня $n \geqslant 1$ має у полі $\mathbb{C}$ принаймні один корінь.

Наслідок 6.2.
Будь–який многочлен $f_n(x)$ степеня n з дійсними чи комплексними коефіцієнтами має у полі комплексних чисел $\mathbb{C}$ рівно n коренів, якщо кожен корінь рахувати стільки разів яка його кратність.

Із основної теореми алгебри та теореми Безу випливає, що для многочлена $f_n(x)$ має місце **розвинення на множники**:

$$f_n(x) = a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m},$$

$$k_1 + k_2 + \cdots + k_m = n.$$

Відомо, що будь–яке натуральне число можна розвинути у добуток простих чисел. При розвиненні многочлена на множники роль простих чисел відіграють так звані незвідні многочлени.

Означення 6.12.
*Кажуть, що многочлен степеня n є **незвідним многочленом над деяким полем F**, якщо він не ділиться на жоден многочлен степеня $k, 0 < k < n$, коефіцієнти належать цьому полю.*

Незвідний многочлен неможливо подати як добуток інших многочленів над цим полем, степені яких менші за n. У протилежному випадку многочлен буде **звідним**.

Зауваження 6.5.
Багаточлени нульового степеня і сам нульовий многочлен не належать ні до незвідних, ні до звідних многочленів.

Зауваження 6.6.
Властивість звідності чи незвідності многочлена над деяким полем F залежить від властивості самого поля.

Приклад 6.3.
Наведемо приклади:

1. *Над **полем комплексних чисел** $\mathbb{C}$ незвідними є тільки многочлени першого степеня $x - c$, де $x, c \in \mathbb{C}$.*
2. *Над **полем дійсних чисел** $\mathbb{R}$ незвідними будуть многочлени першого степеня виду $x - c$ та многочлени 2–го степеня $x^2 + px + q$, де $p^2 - 4q < 0, x, p, q, c \in \mathbb{R}$.*

З урахуванням кратності дійсних та комплексних коренів, для многочлена $f_n(x)$ з дійсними коефіцієнтами має місце розвинення на лінійні та квадратні множники:

$$f_n(x) = a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m}\times$$

$$\times(x^2+p_1x+q_1)^{l_1}(x^2+p_2x+q_2)^{l_2}\cdots(x^2+p_sx+q_s)^{l_s},$$

де $k_1+k_2+\cdots+k_m+2l_1+2l_2+\cdots+2l_s=n$, $k_i,l_j\in\mathbb{N}$.

6.5 Питання, тести, вправи до розділу 6

6.5.1 Питання до розділу 6

1. Дайте означення многочлена n–го степеня змінної x.
2. Який коефіцієнт многочлена n–го степеня називається старшим, а який вільним членом?
3. Коли многочлен називається нормованим?
4. Що таке многочлен нульового степеня?
5. Що розуміють під нульовим многочленом?
6. Який вигляд многочлена називають канонічним?
7. Коли два многочлени називають рівними?
8. Дайте означення протилежного многочлена.
9. Сформулюйте правило додавання двох многочленів.
10. Як отримується добуток многочленів?
11. Які властивості успадковує кільце многочленів $K[x]$ від кільця коефіцієнтів K?
12. Що таке частка від ділення двох многочленів та остача?
13. Сформулюйте основні властивості операції ділення многочленів.
14. Які два многочлени називаються взаємно простими?
15. Дайте означення найбільшого спільного дільника двох многочленів.
16. Перерахуйте властивості найбільшого спільного дільника многочленів.
17. Вкажіть основні елементи алгоритму Евкліда відшукання найбільшого спільного дільника двох многочленів.

18. Що потрібно розуміти під значенням многочлена в точці?
19. Дайте означення кореня (нуля) многочлена.
20. Сформулюйте теорему Безу.
21. Яке число називається кратністю кореня?
22. У якому випадку корінь буде простим коренем?
23. Сформулюйте основну теорему алгебри та наслідок із теореми.
24. Що означає розвинути многочлен на множники?

6.5.2 Тести до розділу 6

Вкажіть правильну відповідь на кожний тест.

1. Вираз $2x + 3x^3 - 4$ є многочлен степеня:
   (A) 2; **(B)** 3; **(C)** 4.
2. Старший коефіцієнт многочлена $4x^2 + 7x^3 - x^4 + 6x - 5$ рівний:
   (A) 4; **(B)** 7; **(C)** -1.
3. Задано многочлен $f_4(x) = 3x^4 + 9x^2 + 12$. Многочлен запишеться в канонічному вигляді:
   (A) $f_4(x) = x^4 + 3x^2 + 4$;
   (B) $f_4(x) = 12 + 9x^2 + 3x^4$;
   (C) $f_4(x) = 3x^4 + 0x^3 + 9x^2 + 0x + 12$.
4. Задано многочлен $f_3(x) = 2x^3 + 8x^2 + 16$. Відповідний нормований многочлен запишеться у вигляді:
   (A) $f_3(x) = x^3 + 2x^2 + 4$;
   (B) $f_3(x) = 16 + 8x^2 + 2x^3$;
   (C) $f_3(x) = 2x^3 + 8x^2 + 0x + 16$.
5. Сумою многочленів $f_3(x) = x^3 + 3x - 4$ та $g_2(x) = -3x^2 + 5$ буде многочлен:
   (A) $h_3(x) = -2x^3 + 8x - 4$;
   (B) $h_2(x) = -2x^2 + 1$;
   (C) $h_3(x) = x^3 - 3x^2 + 3x + 1$.

6. Задані многочлени $f_4(x) = x^4 + 2x^2 + 1$ та $g_3(x) = x^3 + 2x^2 + 2$. Різниця $f_4(x) - g_3(x)$ рівна:

   (A) $h_4(x) = x^4 + x^3 + 4x^2 + 3$;

   (B) $h_4(x) = x^4 - x^3 - 1$;

   (C) $h_4(x) = x^4 + x^3$.

7. Добуток многочлена $f_3(x) = x^3 + x^2 + x + 1$ на $g_2(x) = x^2 - 1$ рівний:

   (A) $h_5(x) = x^5 + x^4 - x - 1$;

   (B) $h_4(x) = x^4 + x^3 + x - 1$;

   (C) $h_5(x) = x^5 - x^2 - 1$.

8. Нехай многочлен $f_n(x)$ ділиться націло на многочлен $\varphi_m(x)$, а многочлен $\varphi_m(x)$ ділиться націло на многочлен $g_k(x)$. Тоді многочлен $f_n(x)$ ділиться на многочлен $g_k(x)$:

   (A) з остачею; **(B)** з надлишком; **(C)** націло.

9. Нехай многочлени $f_n(x)$ і $\varphi_m(x)$ діляться націло на многочлен $g_k(x)$. Тоді на многочлен $g_n^2(x)$ ділиться націло многочлен:

   (A) $f_n(x) + g_k(x)$; **(B)** $f_n(x) \times g_k(x)$; **(C)** $f_n(x)/g_k(x)$.

10. Нехай многочлен $f_n(x)$ ділиться націло на многочлен $\varphi_m(x)$. Тоді многочлен $f_n(x) \cdot g_k(x)$, де $g_k(x)$ – довільний многочлен, ділиться на многочлен $\varphi_m(x)$:

    (A) націло; **(B)** з остачею; **(C)** з надлишком.

11. Нехай $d(x) = \text{НСД}(f_n(x); \varphi_m(x))$ і $h(x)$ деякий спільний дільник многочленів $f_n(x)$ та $\varphi_m(x))$. Тоді

    (A) Многочлен $h(x)$ ділить $d(x)$;

    (B) Многочлен $h(x)$ не належить множині дільників $d(x)$;

    (C) Многочлен $h(x)$ може належати множині дільників $d(x)$, а може і не належати.

12. Нехай $d(x) = \text{НСД}(f_n(x); \varphi_m(x))$. Тоді

    (A) $Cd(x)$ спільний дільник;

    (B) $Cd(x)$, спільний дільник, якщо $C > 0$;

    (C) $Cd(x)$, спільний дільник, якщо $C < 0$.

13. Нехай $d(x) = \text{НСД}(f_n(x); \varphi_m(x); \psi_k(x))$. Крім того маємо, що $d_1(x) = \text{НСД}(f_n(x); \varphi_m(x))$. Тоді
(A) $d(x) = \text{НСД}(d_1(x); \psi_k(x))$;
(B) $d(x) = \text{НСД}(d_1(x)) \times \psi_k(x)$;
(C) $d(x) = \text{НСД}(d_1(x) + \psi_k(x))$.

14. Результат при діленні многочлена $f_6(x) = x^6 - 8$ на $x^4 + 2x^2 + 4$ рівний:
(A) $x - 2$; **(B)** $x^2 + 2$; **(C)** $x^2 - 2$.

15. Многочлени $x^4 - 81$ та $x^2 + 9$ будуть:
(A) взаємно простими;
(B) мають спільні дільники;
(C) мають спільні значення.

16. Нехай $d_k(x) = \text{НСД}(f_n(x); g_m(m))$ двох многочленів. Про многочлен $d_k(x)$ можна сказати:
(A) визначається однозначно;
(B) визначається із точністю до сталого множника;
(C) не завжди визначається.

17. Нехай $f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ – многочлен. Під значенням многочлена $f_n(c)$ розуміють:
(A) Довільне число із області значень;
(B) Довільне число із області визначення;
(C) Число, яке отримується, коли у многочлен підставили $x = c$.

18. Нехай $f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ – многочлен, а c – нуль (корінь) многочлена. Тоді
(A) $c = a_n = 0$; **(B)** $c = 0$; **(C)** $f_n(c) = 0$.

19. Нехай $f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ – многочлен. Згідно із теоремою Безу:
(A) $f_n(x) = (x - c)g_{n-1}(x)$;
(B) $f_n(x) = Ag_{n-1}(x) + (x - c)$;
(C) $f_n(x) = g_{n-1}(x)(x - c) + f_n(c)$.

20. Нехай $f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ — многочлен.
    Число c корінь многочлена $f_n(x)$. Тоді:
    (A) $f_n(x) = (x - c)g_{n-1}(x)$;
    (B) $f_n(x) = Ag_{n-1}(x) + (x - c)$;
    (C) $f_n(x) = g_{n-1}(x)(x - c) + f_n(c)$.

21. Нехай $f_n(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ — многочлен.
    Число c буде простим коренем многочлена $f_n(x)$, якщо:
    (A) Число c — просте число;
    (B) c корінь кратності 1;
    (C) $f_n(x) = g_{n-1}(x)(x - c) + f_n(c)$.

22. Нехай $f_n(x) = (x - c)^{k+1}(x^2 + x + 2)$. Число c буде коренем кратності:
    (A) k; **(B)** $k + 1$; **(C)** $k - 1$.

23. Нехай многочлен задано у вигляді:
$$f_n(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_m)^{k_m}.$$
    Яке співвідношення буде вірним:
    (A) $k_1 + k_2 + \cdots + k_m > n$;
    (B) $k_1 + k_2 + \cdots + k_m < n$;
    (C) $k_1 + k_2 + \cdots + k_m = n$.

6.5.3 Вправи до розділу 6

Вправа 6.1.
Знайти нормований (зведений) многочлен для многочлена
$$f_6(x) = 2x^6 + x^5 - 4x^4 - 6x^3 + 3x^2 + 4x - 5.$$

Вправа 6.2.
Знайти нормований (зведений) многочлен для многочлена
$$f_7(x) = -4x^7 + 2x^6 - x^5 + 3x^4 - 5x^3 - 8x^2 + 12x - 8.$$

Вправа 6.3.
Записати канонічний вигляд многочлена

$$f_8(x) = -3x^8 + 4x^5 - 3x^2 + 5.$$

Вправа 6.4.
Записати канонічний вигляд многочлена

$$f_9(x) = x^9 - 7x^6 + 5x^3 - 2x.$$

Вправа 6.5.
Знайти суму, різницю та добуток многочленів

$$f_5(x) = -2x^5 - 3x^3 + 4x^2 - 8,$$
$$g_4(x) = 3x^4 + 4x^3 - 5x^2 + 6x - 7.$$

Вправа 6.6.
Знайти суму, різницю та добуток многочленів

$$f_6(x) = 3x^6 - 4x^5 + 5x^4 - 4x^3 + 3x^2 - 2x + 1,$$
$$g_5(x) = -3x^5 + 2x^4 + 6x^3 - 7x^2 + 8x - 9.$$

Вправа 6.7.
Розділити без остачі многочлен

$$f_6(x) = 3x^6 + 5x^5 - 16x^4 + 2x^3 + 27x^2 - 28x + 10$$

на многочлен

$$\varphi_2(x) = 3x^2 - 4x + 2.$$

Вправа 6.8.
Розділити без остачі многочлен

$$f_7(x) = -5x^7 + 7x^6 - 5x^5 - 13x^4 - 33x^3 - 37x^2 + 41x - 10$$

на многочлен

$$\varphi_3(x) = 5x^3 + 3x^2 - 4x + 1.$$

Вправа 6.9.
За допомогою методу "ділення кутом" розділити многочлен

$$f_7(x) = x^7 + 6x^5 - 3x^3 + 4x^2 + 9$$

на многочлен

$$g_4(x) = x^4 - 5x^3 - 4x^2 + 7x + 3.$$

Вправа 6.10.
За допомогою методу "ділення кутом" розділити многочлен

$$f_8(x) = -5x^8 + 4x^7 - 3x^5 + 2x^3 - 3x^2 + 5x + 9$$

на многочлен

$$g_3(x) = 2x^3 + 3x^2 - 6x + 5.$$

Вправа 6.11.
За допомогою методу "невизначених коефіцієнтів" розділити многочлен

$$f_6(x) = x^6 + 5x^5 + 2x^4 - 3x^3 + 6x^2 - 4x + 9$$

на многочлен

$$g_4(x) = x^4 - 7x^3 + 5x^2 + 3x - 8.$$

Вправа 6.12.
За допомогою методу "невизначених коефіцієнтів" розділити многочлен

$$f_7(x) = 2x^7 - 5x^6 + 4x^5 - 3x^4 + 7x^3 - 2x^2 + 5x + 3$$

на многочлен

$$g_4(x) = x^4 + 3x^3 - 4x^2 + 6x + 9.$$

Вправа 6.13.
За допомогою схеми Горнера знайти частку та остачу від ділення многочлена $f_6(x) = -3x^6 + 2x^5 - x^4 + x^2 - 7$ *на двочлен* $x - 2$.

Вправа 6.14.
За допомогою схеми Горнера знайти частку та остачу від ділення многочлена $f_7(x) = 3x^7 - 4x^6 + 4x^4 - 5x^3 + 3x + 8$ *на двочлен* $x - 2$.

Вправа 6.15.
За допомогою евклідового алгоритму знайти найбільший спільний дільник многочленів

$$f_6(x) = x^6 + 3x^5 + 3x^4 + 8x^3 - 4x^2 + 3x - 14$$

та

$$\varphi_4(x) = x^4 + 3x^3 + x^2 + x - 6.$$

Вправа 6.16.
За евклідовим алгоритмом знайти ***НСД*** *многочленів*

$$f_7(x) = x^7 - 2x^6 + 4x^5 - 2x^4 + 6x^3 - 5x^2 + 4x - 10$$

та

$$\varphi_4(x) = 5x^4 - 2x^3 + 4x^2 + 3x - 7.$$

Вправа 6.17.
Знайти значення многочлена

$$f_6(x) = x^6 - 4x^3 + 5x - 6$$

для $x = -3, x = -2, x = 2, x = 3$.

Вправа 6.18.
Знайти значення многочлена

$$f_4(x) = x^4 - 2x^3 + 3x^2 + 6x - 7$$

для $x = -2\sqrt{3}, x = -1, x = 4, x = 5\sqrt{2}$.

Вправа 6.19.
Перевірити, чи будуть коренями (нулями) многочлена

$$f_5(x) = x^5 - x^4 - 12x^3 - x^2 + x + 12$$

числа $x_1 = -2, x_2 = 1, x_3 = 3$.

Вправа 6.20.
Знайти остачу від ділення многочлена

$$f_7(x) = 3x^7 - 4x^5 + 2x^3 - 6x - 12$$

на двочлен $x - 3$.

Вправа 6.21.
Знайти остачу від ділення многочлена

$$f_8(x) = 3x^8 - 5x^7 + x^6 - 3x^5 + 2x^4 - 4x^3 + 7x^2 - 6x - 10$$

на двочлен $x + 2$.

Вправа 6.22.
Вкажіть кратності коренів многочлена

$$f_{10}(x) = (x + a)^5(x + b)^3(x - c)^2.$$

Вправа 6.23.
Довести, що многочлен

$$f_6(x) = x^6 + 9x^5 + 33x^4 + 64x^3 + 72x^2 + 48x + 16$$

має корінь $x = -2$ *та визначити його кратність.*

Вправа 6.24.
Довести, що многочлен

$$f_7(x) = x^7 - 5x^6 + 11x^5 - 15x^4 + 15x^3 - 11x^2 + 5x - 1$$

має корінь $x = 1$ *та визначити його кратність.*

Післямова

Основу навчального посібника склали типові задачі з тих розділів сучасної математики, які утворюють підґрунтя для різноманітних криптографічних алгоритмів як зі секретним (симетричним) ключем, так зі відкритим (асиметричним) ключем. Подібні задачі пропонуються студентам для розв'язання на практичних (лабораторних) заняттях. Підбір типів задач визначався теоретичним матеріалом, що вдається розглянути в наявній кількості годин. Значна кількість типів задач залишилася за межами посібника. В той же час, мета розглянути всі типи задач і не ставилася.

Бібліографія

[1] *Андрійчук В.І.,Забавський Б.В.* Алгебра і теорія чисел. Львів. Видавничий центр ЛНУ ім. Івана Франка 2005. 238 с.

[2] *Бабенко Т.В.,Гулак Г.М.,Сушко С.О.,Фомичова Л.Я.* Криптологія у прикладах, тестах і задачах: навч. посібник. Дніпропетровськ. Нац. гірн. ун–т, 2013. 318 с.

[3] *Балога С.І.* Дискретна математика. Навчальний посібник. Ужгород. ПП "АУТДОР–ШАРК", 2021. 124 с.

[4] *Бардачов Ю.М., Соколова Н.А., Ходаков В.Є.* Дискретна математика. Підручник. Київ. Вища школа, 2002. 287 с.

[5] *Богуш В.М.,Мухачов В.А.* Криптографічні застосування елементарної теорії чисел. Навч. посібник. Київ. ДУІКТ, 2006. 126 с.

[6] *Бушмакін В.М., Ганулiч В.К, Мохонько А.З., Томецька С.І., Тимошенко Н.М.* Комбінаторика. Львів. Нац. ун-т «Львів. політехніка», 2002. 195 с.

[7] *Бондаренко М.Ф., Білоус Н.В., Руткас А.Г.* Комп'ютерна дискретна математика. Підручник. Харків. Компанія СМІТ, 2004. 480 с.

[8] *Вербицький О.В.* Вступ до криптології. Львів. ВНТЛ, 1998. 248 с.

[9] *Вишенський В.А.,Перестюк М.О.* Комбінаторика: перші кроки. Кам'янець–Подільський. Аксіома, 2010. 324 с.

[10] *Гудивок П.М., Кирилюк О.А., Погоріляк Є.Я., Тилищак О.А., Юрченко Н.В.* Практикум з алгебри і теорії чисел. Ужгород. Видавництво УжНУ "Говерла", 2008. 64 с.

[11] *Завало С.Т.* Курс алгебри. Київ. Вища школа, 1985. 503 с.

[12] *Кожухівський А.Д., Горбенко Т.Д., Гайдур Г.І., Кожухівська О.А, Марченко В.В.* Математичні методи криптології: Навчальний посібник. Київ. Державний університет телекомунікацій, 2021. 244 с.

[13] *Кузнецов Г.В.,Фомичов В.В.,Сушко С.О.,Фомичова Л.Я.* Математичні основи криптографії: Навч. посібник, Ч. 1. Дніпропетровськ. Нац. гірн. ун–т, 2004. 391 с.

[14] *Клесов О.І.* Елементарна теорія чисел та елементи криптографії. Підручник. Київ. ТВіМС, 2016. 412 с.

[15] *Коцовський В.М.* Основи дискретної математики: навчальний посібник. Ужгород. ПП "АУТДОР–ШАРК", 2020. 128 с.

[16] *Мисло Ю.М., Пагіря М.М., Різак В.М.* Математичні основи криптографії: Методичний посібник до практичних занять.Ужгород:УжНУ, 2022. 77 с.

[17] *Оглобліна О.І., Сушко Т.С., Шрамко Ю.В.* Елементи теорії чисел : навч. посіб. Суми. Сумський держ. ун–т, 2015. 186 с.

[18] *Стасюк, Марта* Елементи математичних основ криптографії. Львів, ЛДУ БЖД, 2021. 216 с.

[19] *Фільштінський В.А., Бережний А.В.* Математичні основи криптографії: конспект лекцій. Суми. Сумський держ. ун–т, 2011. 138 с

[20] *Шапочка І.В.* Курс лекцій з алгебри. Навчальний посібник. Ужгород. Видавництво УжНУ "Говерла", 2013. 221 с.

[21] *Швай О.Л.* Комбінаторні задачі. Навчальний посібник. Луцьк. СНУ імені Лесі Українки, 2018. 142 с.

[22] *Cozzens M.,Miller S.J.* The Mathematics of Encryption. An Elementary Introduction. AMS, 2013. 332 p.

[23] *Menezes A.J.,Van Oorschot P.C.,Vanstone S.A.* Handbook of applied cryptography. CRC press, 2018. 780 p.

[24] *Hoffstein H., Pipher J., Silverman J.H.* An Introduction to Mathematical Cryptography. Springer Science & Business Media, 2014. 538 p.

[25] *Koblitz, N.* A course in number theory and cryptography. Springer Science & Business Media, 1994. 235 p.

Предметний покажчик

МИСЛО Юлія Михайлівна
ПАГІРЯ Михайло Михайлович
РІЗАК Василь Михайлович

ЕЛЕМЕНТИ МАТЕМАТИЧНИХ МЕТОДІВ У КРИПТОЛОГІЇ

Навчальний посібник для студентів спеціальності "Кібербезпека та захист інформації "

Гарнітура Times New Roman
Формат 60x84/16. Зам. № 44.
Ум.друк.арк.7.56. Наклад 100 прим.

Редакційно–видавничий відділ ДВНЗ «УжНУ».
88015, м. Ужгород, вул. Заньковецької, 89.
E–maill: dep-editors@uzhnu.ed.ua

Видавництво УжНУ "Говерла"
8800, м. Ужгород, вул. Капітульна, 18
Свідоцтво про внесення до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції Серія Зт № 32 від 31 травня 2006 року