МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

МЕТОДИЧНІ ВКАЗІВКИ
до виконання розрахунково-графічної роботи
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Математичні основи криптографії. Методичні вказівки до виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с.

Укладачі: СИНЕНКО МАРИНА АНАТОЛІЇВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат фізико-математичних наук, доцент;
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор
МЕХЕД ДМИТРО БОРИСОВИЧ, доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент
ГОЛОВАТЕНКО ІННА МИКОЛАЇВНА, викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – КОРНІЄНКО СВІТЛАНА ПЕТРІВНА,
доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук, доцент

ЗМІСТ

ВСТУП

Метою викладання навчальної дисципліни *“Математичні основи криптографії*” є формування у майбутніх фахівців базових математичних знань для розв’язування задач у професійній діяльності, вмінь аналітичного мислення та математичного формулювання задач кіберзахисту, зокрема криптографії та криптоаналізу.

Основними завданнями вивчення дисципліни “*Математичні основи криптографії*” є:

- надання студентам знань зі спеціальних розділів математики, а саме: з теорії чисел, теорії множин та комбінаторики, абстрактної алгебри та логіки, теорії графів ;

- підготовка студентів до вивчення спеціальних дисциплін в галузі інформаційних технологій, а саме теорії інформації, криптографічних основ захисту інформації;

- розвиток у студентів навичок використання математичних методів дослідженнях під час підготовки курсових та дипломних робіт;

- підготовка студентів до науково-дослідної роботи, розробка та аналіз математичних моделей у кіберзахисті, застосування математичних методів під час розв’язання конкретних завдань галузі.

Запропоновані завдання для розрахунково-графічної роботи студентів включають методичні вказівки до виконання, завдання та критерії оцінювання. За допомогою розрахунково-графічної роботи та запропонованого завдання досягається більш глибоке опанування теорії та дає змогу студентам закріпити на практиці нові для них поняття.

Завдання для розрахунково-графічної роботи студентів може використовуватися як для аудиторної, так і домашньої роботи. Вони спрямовані на розвиток у студентів організаційних та аналітичних здібностей, а також уміння користуватися теоретичними посиланнями у вирішенні практичних ситуацій та вміння користуватися спеціальною літературою. Завдання для

розрахунково-графічної роботи студентів можуть значною мірою полегшити вивчення дисципліни студентами очної форми навчання.

Під час виконання розрахунково-графічної роботи студенти повинні ознайомитися та вивчити лекційний матеріал, запропонований викладачем. Основою для вивчення є літературні джерела, наведені в даній методичній розробці. За наявності незрозумілих питань студентам рекомендується звернутись за консультаціями до викладача з метою отримання всіх необхідних пояснень щодо організації розрахунково-графічної роботи, виконання завдання та пошуку додаткових літературних джерел. Викладачем надаються додаткові роз'яснення та індивідуальні консультації для підвищення компетентності студентів та розширення спектру їх знань з даної дисципліни.

Метою розрахунково-графічної роботи є перевірка рівня засвоєння студентами знань з дисципліни «Математичні основи криптографії» та вміння самостійно вирішувати поставлені перед ними практичні задачі. Розрахунково-графічна робота виконуються в п'ятому семестрі навчання, після вивчення студентами найважливіших тем з дисципліни.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					Усього	у тому числі				
		Л	П	Лаб	інд	с.р.		л	П	Лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. ЕЛЕМЕНТИ ТЕОРІЇ ГРАФІВ.												
Тема 1. Графи. Основні означення та властивості.		2	2			6						
Тема 2. Шляхи та цикли. Зв'язність.		2	2			6						
Тема 3. Дерева		1	1			6						
Тема 4 . Зважені графи та алгортми пошуку найкоротших шляхів.		1	1			6						
Разом за змістовим модулем 1	**36**	**6**	**6**			**24**						
Змістовний модуль 2. КОНГРУЕНЦІЇ ЗА МОДУЛЕМ ***m***												
Тема 5. Основні положення теорії подільності цілих чисел		2	2			6						
Тема 6. Конгруенції за модулем. Властивості конгруенцій		1	2			6						
Тема 7. Класи еквівалентності за модулем m. Арифметика на класах еквівалентності.		1	1			6						
Тема 8. Китайська теорема про остачі. Квадратичні конгуенції		2	1			6						
Разом за змістовим модулем 2	**36**	**6**	**6**			**24**						
Змістовий модуль 3.												
Тема 9. Булеві функції		2	1			6						
Тема 10. Спеціальні форми подання булевих функцій		2	1			6						

Разом за змістовим модулем 3	**18**	**4**	**2**			**12**						
Разом за семестр	**90**	**16**	**14**			**60**						

КРИТЕРІЇ ОЦІНЮВАННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Шкала оцінювання знань студентів при виконанні
розрахунково-графічної роботи

Рівень виконання розрахункової роботи	**Кількість балів**	
- завдання виконано повністю і правильно, містять відповідні пояснення; - показано вміння самостійно формулювати висновки за результатами виконаного завдання;	9…	10
- завдання виконані повністю, але при розв'язуванні допущені незначні помилки; - не аргументовано викладено матеріал; - у висновках містяться помилки та недоречності	6…	8
- завдання виконано не у повному обсязі та містить грубі помилки; - не сформульовані висновки за результатами розрахунків	3…	5
- завдання виконані частково і неякісно	0…	2

ВИМОГИ ДО ОФОРМЛЕННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Робота оформляється на листах А4 з однієї сторони, поля: з лівого боку – 20 мм, з правого боку – 10 мм, зверху – 20 мм, знизу – 20 мм. Завдання повинні бути виконані акуратно, розбірливим почерком (або надруковані), з детальними поясненнями та всіма проміжними розрахунками. В кінці розрахункового завдання пишеться висновок (відповідь).

Вимоги до комп'ютерного набору розрахункової роботи:

– текстовий редактор – WORD;

– гарнітура шрифту – Times New Roman;

– кегль шрифту (розмір) – 14;

– міжрядковий інтервал – полуторний;

– абзац – 1,25 см;

– розташування тексту роботи – вирівнювання по ширині;

– міжрядковий інтервал між заголовком (назвою розділу чи підрозділу) і текстом повинна дорівнювати 1 інтервалу.

Приклад оформлення титульної сторінки розрахунково-графічної роботи наведено у Додатку А.

Повністю оформлена і виконана розрахункова робота подається на кафедру в термін, що визначений у плані-графіку виконання розрахункової роботи для перевірки її викладачем. Якщо робота виконана не вчасно без поважних причин, то студенту ставиться 0 балів («незадовільно») і він повинен виконати додатково один з варіантів, який вказує викладач. Розрахункова робота оцінюється після особистої співбесіди з викладачем. В разі зауважень з боку викладача, робота повинна бути доопрацьована в зазначений термін і подана на перевірку. До підсумкового контролю допускаються лише студенти, що вчасно здали і захистили свою роботу.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Графи. Основні поняття та властивості.

Означення 1.1. ***Простий граф G*** *(graph) складається із скінченної непорожньої множини елементів* ***V****, які називають вершинами графа (vertices) та скінченої множини* ***E*** *невпорядкованих пар елементів із* ***V****, які називають ребрами графа (edges).*

Таким чином, V – множина вершин, а E – множина ребер простого графа G. У простому графі будь-які дві вершини можуть бути з'єднані не більше ніж одним ребром.

Нехай $G = (V, E)$ – деякий граф. Вершини u, v графа G називаються ***суміжними***, якщо ці вершини з'єднані ребром графа, тобто пара $\{u, v\} \in E$. Ребра e_1, e_2 називаються ***суміжними,*** якщо вони мають спільну вершину. Вершина u та ребро e називаються ***інцидентними***, якщо u є кінцем ребра e.

Степенем вершини v графа G називають кількість *інцидентних* їй ребер. Для позначення вершини використовують символ $\deg(v)$. Так, на рис.1.2

Означення 1.2. ***Орієнтований граф G (орграф)*** *складається із скінченної непорожньої множини елементів* ***V****, які називають вершинами графа та скінченої множини* ***E впорядкованих*** *пар елементів із* ***V****, які називають орієнтованими ребрами або* ***дугами*** *графа.*

Якщо (u, v) – дуга оргафа G, то вершина u називається початковою, а вершина v – кінцевою.

Для орграфа замість поняття степеня вершини розглядають поняття ***напівстепеня входу*** $(deg^-(v))$ та ***напівстепеня виходу*** $(deg^+(v))$**.**

Напівстепенем входу вершини v орграфа G називають кількість дуг цього графа, для яких вершина v є кінцевою.

Напівстепенем виходу вершини v орграфа G називають кількість дуг цього графа, для яких вершина v є початковою.

Лема про рукопотискання. *Для будь-якого (неорієнтованого) графа сума степенів його вершин дорівнює подвоєному числу його ребер, тобто, якщо* ***G=(V,E)*** *– неорієнтований граф, і* $|\boldsymbol{V}| = \boldsymbol{n}; |\boldsymbol{E}| = \boldsymbol{m}$*, то має місце рівність:*

$$\sum_{i=1}^{n} \boldsymbol{v_i} = \boldsymbol{2m}$$

Наслідок. *У будь-якому графі кількість вершин непарного степеня парна.*

Аналог леми про рукопотискання для орграфів формулюється таким чином:

Сума напівстепенів входу вершин довільного орграфа дорівнює сумі напістепенів виходу і дорівнює числу його дуг.

Приклад 1.1 *Чи існує простий граф, для якого степені його вершин задаються наступними послідовностями:*
а) {1,1,2,2,3}; б) {1,2,3,4,4,}; b) {0,1,2,2,3}.

Розв'язання. Очевидно, графа, який би визначався послідовністю степенів вершин (а) не існує, оскільки така послідовність протирічить лемі про рукопотискання.

Припустимо, що граф, який визначається послідовністю (б) існує, тоді такий граф має 5 вершин. Степені вешин v_4 і v_5 дорівнюють чотирьом ($\boldsymbol{\deg(v_4) = \deg(v_5) = 4}$**),** отже, ці вершини з'єднані ребрами з кожною з решти чотирьох вершин, але тоді не може існувати вершини, степінь якої дорівнює 1. Отримане протиріччя доводить, що такого графа не існує.

Граф, який визначаєть посідовністю степенів вершин (*в*), існує. Для доведення достатньо його побудувати, що ми пропонуємо зробити читачам самостійно.

Способи аналітичного задання графів

Для того, щоб алгоритми на графах можна було реалізовувати з використанням комп'ютера, необхідно уміти задавати графи аналітично. Ми розглянемо три способи аналітичного задання графів, а саме, за допомогою матриць суміжності та інцидентності, а також списками суміжності.

Матриця суміжності. Нехай $G = (V, E) -$ простий граф, який містить $\boldsymbol{n}$ вершин, $|V| = n$. Занумеруємо вершини графа $v_1, v_2, \dots, v_n$.

Матрицею суміжності $\boldsymbol{A}$ *графа* $\boldsymbol{G}$ *, яка відповідає заданій нумерації вершин, називають матрицю, елементи* $\boldsymbol{a_{ij}}$ *якої визначаються рівностями:*

$$\boldsymbol{a_{ij}} = \begin{cases} \mathbf{1}, & \text{якщо } \{\boldsymbol{v_i}, \boldsymbol{v_j}\} \in \boldsymbol{E} \\ \mathbf{0}, & \text{у протилежному випадку} \end{cases}$$

Нехай $G = (V, E)$ −орграф, який містить $\boldsymbol{n}$ вершин, $|V| = n$. Тоді його *матриця суміжності* $\boldsymbol{A}$ *з елементами* $\boldsymbol{a_{ij}}$ *визначається рівностями:*

$$\boldsymbol{a_{ij}} = \begin{cases} \mathbf{1}, & \text{якщо } (\boldsymbol{v_i}, \boldsymbol{v_j}) \in \boldsymbol{E}; \\ \mathbf{0}, & \text{у протилежному випадку} \end{cases}$$

Матриця інцидентності. Нехай $G = (V, E)$ − простий граф, який містить $\boldsymbol{n}$ вершин, $|V| = n$, та m ребер, $|E| = m$. $V = \{v_1, v_2, \dots, v_n\}$;

$E = \{e_1, e_2, \dots, e_m\}$.

Матрицею інцидентності $\boldsymbol{A}$ *графа* $\boldsymbol{G}$ *, яка відповідає заданій нумерації вершин та ребер, називають матрицю, елементи* $\boldsymbol{a_{ij}}$ *якої визначаються рівностями:*

$$\boldsymbol{a_{ij}} = \begin{cases} \mathbf{1}, & \text{якщо вершина } \boldsymbol{v_i} \text{ та ребро } \boldsymbol{e_j} \text{ інцидентні}; \\ \mathbf{0}, & \text{у протилежному випадку} \end{cases}$$

Матрицею інцидентності $\boldsymbol{A}$ *орграфа* $\boldsymbol{G}$ *, яка відповідає заданій нумерації вершин та дуг, називають матрицю, елементи* $\boldsymbol{a_{ij}}$ *якої визначаються рівностями:*

$$\boldsymbol{a_{ij}} = \begin{cases} \mathbf{1}, & \text{якщо дуга } \boldsymbol{e_j} \text{ виходить з вершини } \boldsymbol{v_i}; \\ \mathbf{-1}, & \text{якщо дуга } \boldsymbol{e_j} \text{ входить у вершину } \boldsymbol{v_i}; \\ \mathbf{2}, & \text{якщо дуга } \boldsymbol{e_j} \text{ петля у вершині } \boldsymbol{v_i}; \\ \mathbf{0}, & \text{в інших випадках.} \end{cases}$$

Подання графа списком пар. Графи також зручно подавати як списки пар, які відповідають ребрам неорієнтованих та дугам орієнтованих графів. Часто це є більш економним щодо пам’яті комп’ютера.

Означення булевої функції. Способи задання булевих функцій.

Означення. Булевою функцією f *змінних* $x_1, x_2, \dots x_n$ *називають функцію, яка може набувати лише двох значень 0 або 1, причому будь-яка змінна* x_i*, від якої залежить функція, також набуває лише цих двох значень.*

Булеву функцію, яка залежить від $\boldsymbol{n}$ змінних, називають ***n-місною.*** Множину усіх n-місних булевих функцій позначають $P_2(n)$. Згідно з означенням область визначення n-місної булевої функції – сукупність усіх можливих упорядкованих наборів довжини $\boldsymbol{n}$ виду:

$$D_f = \{(x_1, x_2, \dots x_n) | x_i \in \{0,1\}\};$$

Таким чином, щоб задати довільну n-місну булеву функцію у вигляді таблиці, запишемо усі можливі набори аргументів (інтерпретації) функції в порядку зростання їх номерів та співставимо кожному набору число з множини $\{0,1\}$ – значення функції на даному наборі. У результаті маємо таблицю, яку будемо називати таблицею булевої функції:

Номер набору	$(x_1, x_2, \dots x_n)$	$f(x_1, x_2, \dots x_n)$
0	000…0	$f(00 \dots 0)$
1	000…1	$f(00 \dots 1)$
2	00…10	$f(0 \dots 10)$
⋮	⋮	⋮
2^{n-1}	11…11	$f(11 \dots 1)$

множина значень - $E_f = \{0,1\}$.

Легко бачити, що область визначення n-місної булевої функції – скінченна множина, яка містить 2^n елементів, $|D_f| = 2^n$, що дозволяє задавати булеві функції у вигляді таблиці. Відмітимо, що будь-якому набору нулів та одиниць з області визначення n-місної булевої функції можна співставити цілком певне ціле число, записане у двійковій системі числення. Так, упорядкованому набору $(a_1, a_2, \dots, a_n), a_i \in \{0,1\}$ відповідає число

$$\overline{a_1 a_2 \dots a_{n_2}} = a_1 \cdot 2^{n-1} + a_2 \cdot 2^{n-2} + \dots + a_{n-1} \cdot 2 + a_n.$$

Це число прийнято називати номером набору. Наприклад, номером набору 1011 з області визначення чотирьохмісної булевої функції є число

$\overline{1011}_2 = 1 \cdot 2^3 + 0 + 1 \cdot 2 + 1 = 11$. Номери наборів значень n-місної булевої функції змінюються від 0 до 2^{n-1}.

Спочатку означимо елементарні булеві функції.

Одномісні булеві функції:

x	$f_1(x) = 0$ (константа нуль)	$f_2(x) = 1$ (константа один)	$f_3(x) = x$ (тотожна функція)	$f_4(x) = \bar{x}$ (заперечення *x*)

0	0	1	0	1
1	0	1	1	0

Двомісні булеві функції:

x	y	$f_5(x,y)=xy$ (кон'юнкція)	$f_6(x,y)=x\vee y$ (диз'юнкція)	$f_7(x,y)=x\to y$ (імплікація)	$f_8(x,y)=x\sim y$ (еквівалентність)
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

x	y	$f_9(x,y)=x\oplus y$ (додавання за mod 2)	$f_{10}(x,y)=x\|y$ (штрих Шеффера)	$f_{11}(x,y)=x\downarrow y$ (стрілка Пірса)
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

За допомогою елементарних функцій будь-яку булеву функцію можна задати аналітично. Для цього використовують суперпозиції елементарних функцій, перейменування змінних та їх ототожнення.

Приклад 4.1. *Булеву функцію реалізовано формулою* $\boldsymbol{\bar{x}\sim(z\to(y\oplus x\bar{z}))}$. *Подати її за допомогою таблиці*. *Знайти номер даної функції.*

Щоб задати булеву функцію за допомогою таблиці, спочатку визначаємося з пріоритетом операцій – згідно з установленими правилами спочатку виконуємо заперечення, а далі операції в дужках, починаючи з внутрішніх. Отже, маємо наступний порядок: $\bar{x};\ \bar{z};\ x\bar{z};\ y\oplus x\bar{z};\ z\to y\oplus x\bar{z};\ \bar{x}\sim(z\to(y\oplus x\bar{z}))$. Далі, користуючись таблицею елементарних булевих функцій, знаходимо значення кожної операції. У результаті маємо таблицю.

x	y	z	$\bar{x}$	$\bar{z}$	$x\bar{z}$	$y\oplus x\bar{z}$	$z\to y\oplus x\bar{z}$	$\bar{x}\sim(z\to(y\oplus x\bar{z}))$.
0	0	0	1	1	0	0	1	1
0	0	1	1	0	0	0	0	0
0	1	0	1	1	0	1	1	1
0	1	1	1	0	0	1	1	1
1	0	0	0	1	1	1	1	0
1	0	1	0	0	0	0	0	1
1	1	0	0	1	1	0	1	0
1	1	1	0	0	0	1	1	0

Щоб визначити номер даної булевої функції, скористаємося знайденим вектором значень $(1,0,1,1,0,1,0,0)$ та запишемо відповідне йому число у двійковій системі числення.

$$\overline{10110100}_2 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0 = 180$$

Отже, номер функції 180.

ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ

Означення Цілі числа $\boldsymbol{a}$ та $\boldsymbol{b}$ $(\boldsymbol{a},\ \boldsymbol{b}\ \in \boldsymbol{Z})$називають рівними (конгруентними) за модулем $\boldsymbol{m}$, $(\boldsymbol{m} \in \boldsymbol{N})$, якщо при діленні на $\boldsymbol{m}$ вони дають однакову остачу.

$$\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m});\quad \boldsymbol{a} \overset{m}{=} \boldsymbol{b}$$

Цілі числа $\boldsymbol{a}$ та $\boldsymbol{b}$ $(\boldsymbol{a},\ \boldsymbol{b}\ \in \boldsymbol{Z})$називають рівними (конгруентними) за модулем $\boldsymbol{m}$, $(\boldsymbol{m} \in \boldsymbol{N})$, якщо їх різниця націло ділиться на $\boldsymbol{m}$.

$$\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m}) \Leftrightarrow (\boldsymbol{a} - \boldsymbol{b}) \vdots \boldsymbol{m}$$

- Якщо $\boldsymbol{a, b, c, d}$ – довільні цілі числа, такі що $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$ **і** $\boldsymbol{c} \equiv \boldsymbol{d}(\boldsymbol{mod}\ \boldsymbol{m})$**,** то спрведливі наступні конгуренції:
  $\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d}(\boldsymbol{mod}\ \boldsymbol{m});\ \boldsymbol{a} - \boldsymbol{c} \equiv \boldsymbol{b} - \boldsymbol{d}\ (\boldsymbol{mod}\ \boldsymbol{m});\quad \boldsymbol{ac} \equiv \boldsymbol{bd}(\boldsymbol{mod}\ \boldsymbol{m})$**;**
- Якщо $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$**,** то $\boldsymbol{ka} \equiv \boldsymbol{kb}(\boldsymbol{mod}\ \boldsymbol{m})$,
- Якщо $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$, то $\boldsymbol{a^n} \equiv \boldsymbol{b^n}(\boldsymbol{mod}\ \boldsymbol{m})$**;**
- Якщо числа $\boldsymbol{c}$ і $\boldsymbol{m}$ взаємно прості, і $\boldsymbol{ac} \equiv \boldsymbol{bc}(\boldsymbol{mod}\ \boldsymbol{m})$, то $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$**;**
- Якщо $\boldsymbol{ac} \equiv \boldsymbol{bc}\ (\boldsymbol{mod}\ \boldsymbol{mc})$, то $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$;
- Якщо $\boldsymbol{a} \equiv \boldsymbol{b}(\boldsymbol{mod}\ \boldsymbol{m})$ і $\boldsymbol{b} \equiv \boldsymbol{c}(\boldsymbol{mod}\ \boldsymbol{m})$, то $\boldsymbol{a} \equiv \boldsymbol{c}(\boldsymbol{mod}\ \boldsymbol{m})$.

Означення Функцією Ейлера називають функцію, яка кожному натуральному $\boldsymbol{n}$ ставить у відповідність ***кількість*** натуральних чисел, які взаємо прості з $\boldsymbol{n}$ і не перевищують ***n-1.***

Функцію Ейлера будемо позначати $\boldsymbol{\varphi(n)}$

За означенням $\varphi(1) = 1$.

$$\varphi(6) = 2;\ \varphi(7) = 6;\ \varphi(9) = 6;$$

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

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k};$$

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

Теорема Ейлера Для будь-якого n, $n \in \boldsymbol{N}$ і для будь-якого ***a*** взаємо простого з ***n*** справедливе твердження:

$$\boldsymbol{a^{\varphi(n)} \equiv 1 (mod\ n)}.$$

Приклад.

У кільці лишків Z_{37} обчислити 19^{721}.

Помічаємо, що $\varphi(37) = 36$, $721 = 36 \cdot 20 + 1$.

Тоді

$$19^{721} = 19^{36 \cdot 20 + 1} = (19^{36})^{20} \cdot 19$$

Але за теоремою Ейлера $19^{36} \equiv 1 (\text{mod } 37)$, тому

$$19^{721} = 19^{36 \cdot 20 + 1} = (19^{36})^{20} \cdot 19 \equiv 1^{20} \cdot 19 (\text{mod } 37) = 19 (\text{mod } 37).$$

Лінійні конгруенції.

Лінійною конгруенцією по модулю *m* називають конгруенцію виду:

$$\boldsymbol{ax \equiv b (mod\ m)}$$

Розв'язати конгруенцію означає знайти у кільці лишків Z_m значення *x*, при якому вона є істинною.

Оскільки кільце Z_m містить скінченну кількість елементів, то теоретично це можна зробити методом перебору. Для невеликих значень *m* метод перебору реально працює. Для прикладу розглянемо конгруенцію:

$$2x \equiv 3 (mod\ 7)$$

$$Z_7 = \{0,1,2,3,4,5,6\}$$

Перевіряючи по черзі усі елементи $\boldsymbol{Z_7}$, приходимо до висновку, що у кільці $\boldsymbol{Z_7}$ існує єдине значення, яке задовольняє дану конгруенцію – ***x=5.***

Можливі наступні випадки.

- $(a, m) = 1$, ***(числа a, m взаємо прості).*** *У* цьому випадку у кільці Z_m конгруенція має єдиний розв'язок, знайти який можна за допомогою теореми Ейлера:

$$ax \equiv b(mod\ m) \Leftrightarrow a^{\varphi(m)}x \equiv a^{\varphi(m)-1}b(mod\ m) \Leftrightarrow x \equiv a^{\varphi(m)-1}b(mod\ m)$$

- ***Числа a, m мають спільний дільник d, але b не ділиться на d.***

У цьому випадку конгруенція не має розв'язків. (Це можна довести від супротивного)

- ***Числа a, b, m мають спільний дільник d.***

Тоді конгруенцію можна скоротити на ***d:***

$$ax \equiv b(mod\ m) \Rightarrow a_1x \equiv b_1(mod\ m_1)$$

Якщо отримана конгруенція має розв'язок, то початкова має d розв'язків

$$x \equiv x^* + m_1k, \quad k = 0, 1, 2, \dots d-1.$$

Для розв'язування лінійних конгруенцій використовують наступні методи:

- Метод перебору;
- Метод, що базується на теоремі Ейлера;

Означення. *Елементи a, b кільця* Z_m *називаються* ***мультиплікативно оберненими,*** *якщо* $ab \equiv 1(mod\ m)$**.**

Наприклад, елементи 3, 4 з кільця лишків Z_{11} є мультиплікативно оберненими, оскільки $3 \cdot 4 \equiv 1(mod\ 11)$.

Елемент, мультиплікативно обернений до a будемо позначати $a^{-1}; a, a^{-1} \in Z_m$. Щоб знайти елемент мультиплікативно обернений до a у кільці лишків Z_m достатньо розв'язати конгруенцію

$$ay \equiv 1\ (mod\ m).$$

Однак, як випливає з вище сказаного, така конгрунція має у кільці лишків Z_m єдиний розв'язок тоді і тільки тоді, коли $(a, m) = 1$, тобто мультиплікативно обернений елемент у кільці лишків Z_m існує лише для тих a, які взаємо прості з m.

$$y = a^{-1} = a^{\varphi(m)-1}.$$

Для великих значень $\boldsymbol{m}$ мультиплікативно обернені елементи зручніше знаходити за допомогою теореми Безу.

Дійсно, згідно з теоремою Безу $\boldsymbol{mx + ay = 1}$; ($x,\ y -$ множники Безу).

Але $\boldsymbol{mx \equiv 0(mod\ m) \Rightarrow ay \equiv 1(mod\ m)}$

(Елемент, мультиплікативно обернений до *a*, конгруентний по модулю *m* *другому множнику Безу, який знаходимо за допомогою розширеного алгоритму Евкліда.)*

Зауважимо, що якщо $\boldsymbol{p}$ - просте число, то для кожного елемента $\boldsymbol{Z_p}$ існує мультиплікативно обернений елемент.

Квадратичні конгруенції.

Означення. Число $\boldsymbol{a}$ називається квадратичним лишком по модулю $\boldsymbol{p}$, $\boldsymbol{a} \in \boldsymbol{Z_p}$, якщо існує таке $\boldsymbol{x} \in \boldsymbol{Z_p}$, квадрат якого конгруентний $\boldsymbol{a}$ по модулю $\boldsymbol{p}$, тобто коруенція

$$\boldsymbol{x^2 \equiv a(mod\ p)}$$

має розв'язки в $\boldsymbol{Z_p}$. У іншому випадку $\boldsymbol{a}$ називається квадратичним нелишком по модулю $\boldsymbol{p}$.

Приклад.

$$\boldsymbol{Z_7 = \{0; 1; 2; 3; 4; 5; 6\}}$$

$$\boldsymbol{1^2 \equiv 1(mod\ 7); 2^2 \equiv 4(mod\ 7); 3^2 \equiv 2(mod\ 7);}$$

$$\boldsymbol{4^2 \equiv 2(mod\ 7); 5^2 \equiv 4(mod\ 7); 6^2 \equiv 1(mod\ 7).}$$

Отже, квадратичні лишки (QR): {1; 2; 4}

Критерій Ейлера

Нехай $\boldsymbol{p}$ *–* ***просте число*** $\boldsymbol{(p \geq 3)}$.

Теорема. *Число a є квадратичним лишком по модулю p тоді і тільки тоді, коли*

$$\boldsymbol{a^{\frac{p-1}{2}} \equiv 1(mod\ p)};$$

і, відповідно, є квадратичним нелишком, якщо

$$\boldsymbol{a^{\frac{p-1}{2}} \equiv -1(mod\ p)}.$$

Якщо $\boldsymbol{a}$ *є квадратичним лишком по модулю* $\boldsymbol{p}$ *і* $\boldsymbol{p = 4k + 3}$, то

$$\boldsymbol{x^2 \equiv a(mod\ p) \Leftrightarrow x \equiv \pm a^{\frac{p+1}{4}}(mod\ p)}.$$

Розглянемо приклад розв'язання квадратичної конгруенції.

$$\boldsymbol{x^2 \equiv 7(mod\ 11)}$$

$$\boldsymbol{7^5 = 7 \cdot (7^2)^2 = 7 \cdot 49^2 \equiv 7 \cdot 5^2 \equiv 7 \cdot 3 \equiv 10 \equiv -1(mod\ 11)}.$$

Отже, число 7 є квадратичним нелишком в $\boldsymbol{Z_{11}}$, і конгруенція не має розв'язків.

$$\boldsymbol{x^2 \equiv 5(mod\ 11)}$$

$$\boldsymbol{x \equiv \pm 5^{\frac{11+1}{4}}(mod\ 11) \equiv \pm 4(mod\ 11)}$$

Розглянемо квадратичні конгруенції по складеному модулю $\boldsymbol{m = p_1 p_2 \dots p_k}$;.

$$\boldsymbol{x^2 \equiv a(mod\ p) \Leftrightarrow \begin{cases} x^2 \equiv a(mod\ p_1) \\ x^2 \equiv a(mod\ p_2) \\ \vdots \\ x^2 \equiv a(mod\ p_k) \end{cases} \Leftrightarrow \begin{cases} x \equiv \pm b_1 \\ x \equiv \pm b_2 \\ \vdots \\ x \equiv \pm b_k \end{cases}}$$

Далі для побудови розв'язку квадратичної конгруенції використовуємо ***китайську теорему про остачі.***

Китайська теорема про остачі.

Нехай $\boldsymbol{b_1, b_2, \dots b_k}$ – довільні цілі числа, $\boldsymbol{m_1, m_2, \dots, m_k}$ – натуральні та попарно взаємо прості, тобто $\boldsymbol{(m_i, m_j) = 1,\ i \neq j}$. Тоді система конгруенцій

$$\boldsymbol{\begin{cases} x \equiv b_1(mod\ m_1) \\ x \equiv b_2(mod\ m_2) \\ \vdots \\ x \equiv b_k(mod\ m_k) \end{cases}}$$

має єдиний розв'язок у кільці лишків $\boldsymbol{Z_M}$, $\boldsymbol{M = m_1 m_2 \dots m_k}$, **причому**

$$\boldsymbol{x \equiv \sum_{i=1}^{k} M_i y_i b_i\ (mod\ M)},$$

де $\boldsymbol{M_i = \frac{M}{m_i};\ y_i M_i \equiv 1(mod\ m_i)}$.

Приклад.

Розв'язати систему конгрунцій***:***

$$\begin{cases} \boldsymbol{x \equiv 3(mod\ 7)} \\ \boldsymbol{x \equiv 1(mod\ 4)} \\ \boldsymbol{x \equiv 2(mod\ 11)} \end{cases}$$

Скористаємося китайською теоремою про остачі:

$$\boldsymbol{m_1 = 7; m_2 = 4; m_3 = 11; M = 7 \cdot 4 \cdot 11 = 308;}$$

$$\boldsymbol{M_1 = \frac{M}{m_1} = 4 \cdot 11 = 44; M_2 = \frac{M}{m_2} = 7 \cdot 11 = 77; M_3 = \frac{M}{m_3} = 4 \cdot 7 = 28.}$$

Для кожного елемента $\boldsymbol{M_i}$ обчислимо мультиплікативно обернений елемент $\boldsymbol{y_i}$. ***Для цього розв'яжемо*** конгруенції

$$\boldsymbol{M_i y_i \equiv 1(mod\ m_i)}$$

$$\boldsymbol{44y_1 \equiv 1(mod\ 7) \Leftrightarrow 2y_1 \equiv 1(mod\ 7) \Leftrightarrow y_1 = 4;}$$

$$\boldsymbol{77y_2 \equiv 1(mod\ 4) \Leftrightarrow y_2 \equiv 1(mod\ 4);}$$

$$\boldsymbol{28y_3 \equiv 1(mod\ 11) \Leftrightarrow 6y_3 \equiv 1(mod\ 11) \Leftrightarrow y_3 = 2.}$$

Отже,

$$\boldsymbol{x \equiv \sum_{i=1}^{3} M_i y_i b_i\ (mod\ M) = 3 \cdot 44 \cdot 4 + 1 \cdot 77 \cdot 1 + 2 \cdot 2 \cdot 28 = 717 \equiv}$$

$$\boldsymbol{\equiv 101(mod\ 308)}$$

Безпосередньою підставкою переконуємось у правильності отриманого розв'язку.

Приклад. Розв'язати квадратичну конгруенцію

$$\boldsymbol{x^2 \equiv 16(mod\ 161)}.$$

Помічаємо, що $161 = 7 \cdot 23$. Тоді

$$\boldsymbol{x^2 \equiv 16(mod\ 161) \Leftrightarrow \begin{cases} x^2 \equiv 16(mod\ 7) \\ x^2 \equiv 16(mod\ 23) \end{cases}}$$

Спочатку переконаємось, що число 16 є квадратичним лишком по модулю 7 і 23. Скористаємось критерієм Ейлера.

$$16^3 \equiv 2^3 \equiv 8 \equiv 1(mod\ 7);$$

$$16^{11} \equiv 16 \cdot 16^{10} \equiv 16 \cdot (-7)^{10} \equiv 16 \cdot 49^5 \equiv 16 \cdot 3^5 \equiv 16 \cdot 13 \equiv 1(mod\ 23);$$

Розв’яжемо кожну конгруенцію системи.

$$\boldsymbol{x^2 \equiv 16(mod\ 7) \Leftrightarrow x^2 \equiv 2(mod\ 7) \Leftrightarrow x \equiv \pm 2^{\frac{7+1}{4}}(mod\ 7)}$$

$$\boldsymbol{x \equiv \pm 4(mod\ 7)}$$

$$\boldsymbol{x^2 \equiv 16(mod\ 23) \Leftrightarrow x \equiv \pm 16^{\frac{23+1}{4}}(mod\ 7) \Leftrightarrow \pm 16^6(mod\ 23)}$$

$$\boldsymbol{x \equiv \pm 4(mod\ 23)}.$$

Таким чином, для обчислення $\boldsymbol{x}$ маємо сукупність чотирьох систем.

$$\begin{cases} \begin{cases} \boldsymbol{x \equiv 4(mod\ 7)} \\ \boldsymbol{x \equiv 4(mod\ 23)} \end{cases} \\ \begin{cases} \boldsymbol{x \equiv 4(mod\ 7)} \\ \boldsymbol{x \equiv 19(mod\ 23)} \end{cases} \\ \begin{cases} \boldsymbol{x \equiv 3(mod\ 7)} \\ \boldsymbol{x \equiv 4(mod\ 23)} \end{cases} \\ \begin{cases} \boldsymbol{x \equiv 3(mod\ 7)} \\ \boldsymbol{x \equiv 19(mod\ 23)} \end{cases} \end{cases}$$

Розв’яжемо кожну систему, скориставшись китайською теоремою про остачі.

$$\begin{cases} x \equiv 4 \cdot 23 \cdot 4 + 4 \cdot 7 \cdot 10 = 648 \equiv 4(mod 161) \\ x \equiv 4 \cdot 23 \cdot 4 + 19 \cdot 7 \cdot 10 = 1698 \equiv 88(mod 161) \\ x \equiv 3 \cdot 23 \cdot 4 + 4 \cdot 7 \cdot 10 = 556 \equiv 73(mod 161) \\ x \equiv 3 \cdot 23 \cdot 4 + 19 \cdot 7 \cdot 10 = 1606 \equiv 157(mod 161) \end{cases}$$

Таким чином, квадратична конгруенція має чотири розв’язки: $\boldsymbol{x \equiv 4(mod 161)}$;

$$\boldsymbol{x \equiv 88(mod 161);\ \ x \equiv 73(mod 161);\ \ x \equiv 157(mod 161)}$$

Розглянемо конгруенцію

$$\boldsymbol{x^2 \equiv 10(mod\ 253)}.$$

Помічаємо, що $253 = 11 \cdot 23$. Тоді

$$\boldsymbol{x^2 \equiv 10(mod\ 253) \Leftrightarrow \begin{cases} x^2 \equiv 10(mod\ 11) \\ x^2 \equiv 10(mod\ 23) \end{cases}}$$

Але, згідно критерію Ейлера,

$$10^5 \equiv (-1)^5 \equiv -1(mod\ 11),$$

Тобто 10 – квадратичний нелишок по модулю 11. Конгруенція не має розв’язків.

ЗАВДАННЯ ДО РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

ЕЛЕМЕНТИ ТЕОРІЇ ГРАФІВ

1. Для заданих множин $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{U}$ знайдіть $\boldsymbol{A} \cap \boldsymbol{B}$; $\boldsymbol{A} \cup \boldsymbol{B}$; $\overline{\boldsymbol{A}}$; $\boldsymbol{B} \backslash \boldsymbol{A}$; $\boldsymbol{A} \Delta \boldsymbol{B}$.

1.1 $A = \{x|\ x^2 - |x| - 12 \leq 0\};\ B = \{-5; -4; -2; 0; 12\};\ U = R.$
1.2 $A = \{x|\ x^2 + |x| - 12 \geq 0\};\ B = \{-5; -4; -2; 0; 12\};\ U = R.$
1.3 $A = \{x|\ x^2 - 5x - 15 \leq 0\};\ B = \{-5; -4; -2; 0; 6; 8; 15\};\ U = R.$
1.4 $A = \{x|\ 2|x| - 12 \geq 0\};\ B = \{-7; -4; -2; 0; 11; 12\};\ U = R.$
1.5 $A = \{x|\ x^2 - 3|x| - 10 \leq 0\};\ B = \{-6; -4; -2; 0; 3; 12\}; U = R.$
1.6 $A = \{x|\ x^2 + 3|x| - 10 \leq 0\};\ B = \{-5; -4; -2; 3; 12\};\ U = R.$
1.7 $A = \{x|\ x^2 - |x| - 20 \leq 0\};\ B = \{-5; -4; -2; 0; 1; 2\};\ U = R.$
1.8 $A = \{x|\ x^2 + |x| - 20 \geq 0\};\ B = \{-5; -4; -2; 0; 12\};\ U = R.$
1.9 $A = \{x|\ x^2 - 5|x| - 14 \leq 0\};\ B = \{-5; -4; -2; 1; 12\};\ U = R.$
1.10 $A = \{x|\ x^2 + 5|x| - 14 \geq 0\};\ B = \{-5; -2; 0; 12; 14\};\ U = R.$
1.11 $A = \{x|\ x^2 - 8|x| + 18 \leq 0\};\ B = \{-5; -4; -2; 0; 6\};\ U = R.$
1.12 $A = \{x|\ x^2 - 8|x| + 12 \geq 0\};\ B = \{-5; -4; -2; 0; 8; 12\};\ U = R.$
1.13 $A = \{x|\ x^2 + 3|x| - 10 \geq 0\};\ B = \{-7; -4; -2; 0; 11\};\ U = R.$
1.14 $A = \{x|\ x^2 + 4|x| - 21 \leq 0\};\ B = \{-5; -4; -2; 0; 10\};\ U = R.$
1.15 $A = \{x|\ x^2 - |x| - 12 \leq 0\};\ B = \{-5; -4; -2; 0; 12\};\ U = R.$
1.16 $A = \{(x; y)|\ x^2 + y^2 - 16 \leq 0\};\ B = \{(x; y)|x^2 + y^2 \leq 8y\}; U = R^2$
1.17 $A = \{(x; y)|\ x^2 + y^2 - 16 \leq 0\};\ B = \{(x; y)|x^2 + y^2 \geq -8x\};$
$U = R^2$

1.18 $A = \{(x; y)|\ x^2 + y^2 - 9 \leq 0\};\ B = \{(x; y)|y \geq |x|\}; U = R^2$
1.19 $A = \{(x; y)|\ x^2 + y^2 \geq 4y\};\ B = \{(x; y)|y \leq 4 - |x|\}; U = R^2$
1.20 $A = \{(x; y)|\ x^2 + y^2 \geq 2x\};\ B = \{(x; y)|y \leq |x - 1|\}; U = R^2$
1.21 $A = \{(x; y)|\ x^2 + y^2 \geq -6y\};\ B = \{(x; y)|y \leq x^2 - 3\}; U = R^2$
1.22 $A = \{(x; y)|\ x^2 + y^2 \leq 4x\};\ B = \{(x; y)|y \leq -|x - 2|\}; U = R^2$
1.23 $A = \{(x; y)|\ x^2 + y^2 \geq 8y\};\ B = \{(x; y)|x^2 + y^2 \leq 4\}; U = R^2$
1.24 $A = \{(x; y)|\ x^2 + y^2 \geq 2y\};\ B = \{(x; y)|x^2 + y^2 \leq 2x\}; U = R^2$
1.25 $A = \{(x; y)|\ x^2 + y^2 \leq 4y\};\ B = \{(x; y)|y \leq 2 + x^2\}; U = R^2$
1.26 $A = \{(x; y)|\ x^2 + y^2 \geq 4y\};\ B = \{(x; y)|y \geq 2 + |x|\}; U = R^2$
1.27 $= \{(x; y)|\ x^2 + y^2 < 4y\};\ B = \{(x; y)|y \geq 2 + |x|\}; U = R^2$
1.28 $= \{(x; y)|\ x^2 + y^2 \geq -2y\};\ B = \{(x; y)|y < 2 - |x|\}; U = R^2$
1.29 $= \{(x; y)|\ x^2 + y^2 < 4x\};\ B = \{(x; y)|y \geq |x - 2|\}; U = R^2$
1.30 $= \{(x; y)|\ x^2 + y^2 \geq -6x\};\ B = \{(x; y)|y \geq -|x + 3|\}; U = R^2$

2. Для заданої послідовності степенів вершин графа перевірити чи існує відповідний граф. Відповідь обгрунтувати, тобто якщо графа заданою послідовнітю степенів вершин не існує, пояснити чому. У випадку існування графа достатньо його побудувати.

Номер варіанта	Послідовність степенів вершин	Номер варіанта	Послідовність степенів вершин
1	{1,1,1,1,1}	16	{2,3,3,3,4,4}
2	{1,1,1,3,3}	17	{3,3,3,3,3,3}
3	{0,1,1,1,1}	18	{5,5,5,5,5,5}
4	{2,2,2,2,2}	19	{0,1,1,1,1,1}
5	{4,4,4,4,4}	20	{4,4,4,4,4,4}
6	{1,1,2,2,3}	21	{0,1,1,3,3,4}
7	{3,3,3,3,3}	22	{1,2,2,2,2,3}
8	{3,3,3,3,4}	23	{1,1,1,1,1,1,1}
9	{1,2,3,4,4}	24	{1,1,1,2,3,3,3}
10	{0,1,2,2,3}	25	{1,1,2,2,4,4,4}
11	{2,2,3,3,4}	26	{1,2,3,4,5,6,6}
12	{1,1,1,1,1,1}	27	{0,1,1,5,5,5,5}
13	{1,1,1,1,2,2}	28	{0,1,1,6,6,6,6}
14	{1,2,3,4,5,5}	29	{1,1,2,2,2,2,2}
15	{0,1,2,3,4,5}	30	{1,1,3,3,4,4,4}

3. Орграф ***G= (V,E)***, де ***V***- множина вершин, ***E*** –множина дуг, заданий аналітично. Задати його графічно та записати матрицю суміжності.

Нномер Варіанта	
1	V=$\{v_1, v_2, v_3, v_4, v_5, v_6\}$;

	$E = \{(v_1, v_2), (v_2, v_5), (v_3 v_4), (v_4, v_5), (v_4 v_6), (v_6 v_2), (v_6, v_3)\}$
2	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_2, v_4), (v_3 v_4), (v_4 v_6), (v_6 v_5), (v_6, v_6)\}$
3	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_1), (v_1, v_3)(v_2, v_5), (v_3 v_5), (v_4, v_5)(v_6 v_5)\}$
4	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_1, v_3), (v_3 v_4), (v_4 v_6), (v_5 v_2), (v_6, v_1)\}$
5	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_4), (v_2, v_1), (v_3 v_4), (v_4, v_1), (v_4 v_6), (v_6 v_2), (v_6, v_5)\}$
6	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_2, v_2), (v_3, v_2), (v_4, v_5), (v_4 v_1), (v_6 v_5)\}$
7	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_1, v_5), (v_3 v_4), (v_4, v_5), (v_4 v_6), (v_6 v_2)\}$
8	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_2, v_6), (v_3 v_4), (v_4, v_4), (v_4 v_6), (v_6 v_1), (v_6, v_5)\}$
9	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_5), (v_2, v_5), (v_3 v_4), (v_4, v_5), (v_4 v_6), (v_6 v_2), (v_6, v_6)\}$
10	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6\}$; $E = \{(v_1, v_2), (v_2, v_4), (v_3 v_4), (v_4, v_1), (v_4 v_6), (v_6 v_2)\}$
11	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_2), (v_1, v_6), (v_1 v_7), (v_2, v_3), (v_3, v_5), (v_6 v_2),\}$
12	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_2), (v_2, v_3), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_6 v_2), (v_6, v_7)\}$
13	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_2), (v_1 v_4)(v_2, v_3), (v_3 v_7), (v_4, v_5), (v_5 v_7), (v_6 v_2), (v_7, v_6)\}$
14	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_2), (v_2, v_7), (v_3 v_6), (v_4, v_3), (v_5 v_6), (v_6 v_1), (v_7, v_7)\}$
15	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_2), (v_2, v_3), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_7)\}$
16	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_7), (v_2, v_3), (v_3 v_1), (v_4, v_6), (v_5 v_6), (v_6 v_2)\}$
17	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_2), (v_2, v_3), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_6 v_2), (v_6, v_7)\}$
18	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_6), (v_2, v_5), (v_3 v_4), (v_3, v_1), (v_5 v_3), (v_6 v_2), (v_6, v_7)\}$
19	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_1), (v_2, v_1), (v_3 v_1), (v_3, v_5), (v_5 v_4), (v_4 v_7), (v_7, v_6)\}$
20	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7\}$; $E = \{(v_1, v_4), (v_2, v_3), (v_3 v_3), (v_4, v_3), (v_5 v_6), (v_6 v_1), (v_6, v_7)\}$
21	V=$\{v_{1,} v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$;

	E $= \{(v_1, v_2), (v_2, v_3), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_6, v_8)(v_7 v_1), (v_8, v_7)\}$
22	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_2), (v_1, v_8)(v_2, v_4), (v_3 v_4), (v_4, v_7), (v_5 v_6), (v_5, v_8)(v_8 v_1), (v_8, v_7)\}$
23	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_5), (v_2, v_5), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_2)$
24	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; E= $\{(v_1, v_4), (v_2, v_2), (v_3 v_7), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_3)\}$
25	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_2), (v_2, v_7), (v_3 v_8), (v_4, v_5), (v_4 v_2), (v_5, v_7)(v_6 v_1), (v_8, v_7)\}$
26	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\}$; $= \{(v_1, v_2), (v_2, v_3), (v_2 v_9)(v_3 v_4), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_7, v_9), (v_9, v_5)\}$
27	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_2), (v_2, v_8), (v_3 v_3), (v_4, v_3), (v_5 v_6), (v_5, v_8)(v_6 v_2), (v_8, v_5)\}$
28	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $= \{(v_1, v_2), (v_2, v_3), (v_3 v_4), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_7)$
29	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$; $E = \{(v_1, v_2), (v_2, v_7), (v_3 v_4), (v_4, v_1), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_4)\}$
30	V=$\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\}$; $E = \{(v_1, v_2), (v_2, v_3), (v_2 v_9)(v_3 v_4), (v_4, v_5), (v_5 v_6), (v_5, v_8)(v_6 v_1), (v_8, v_9)\}$

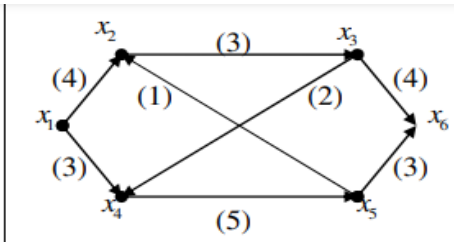
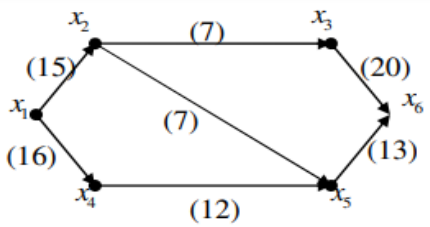
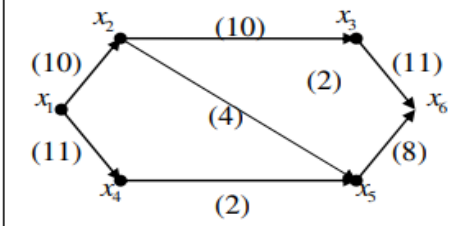
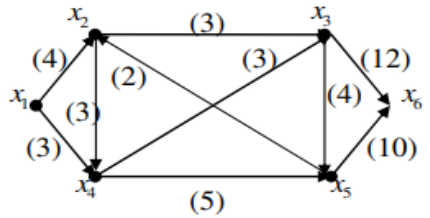
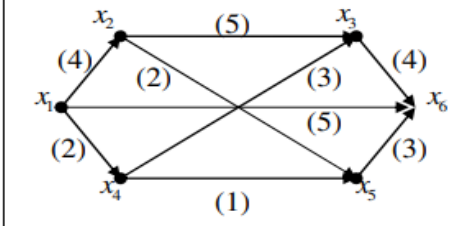
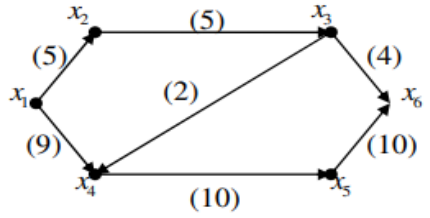
4. Знайдіть число вершин простого графа, якщо відомо:

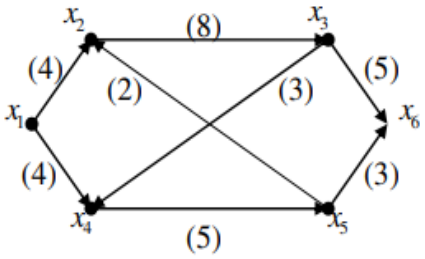
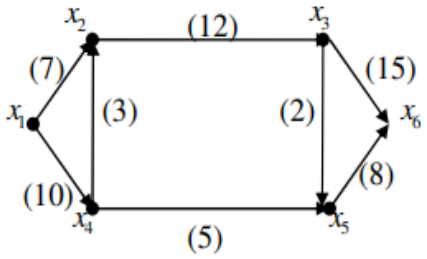
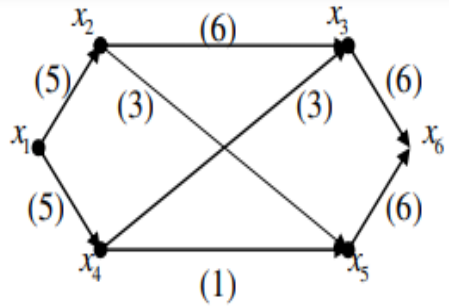
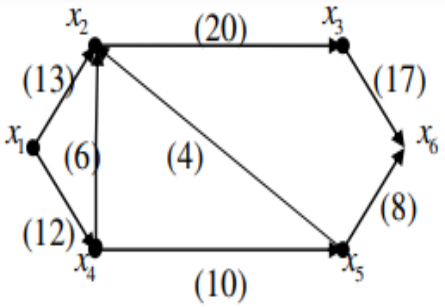
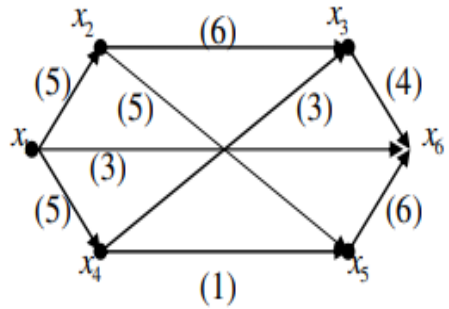
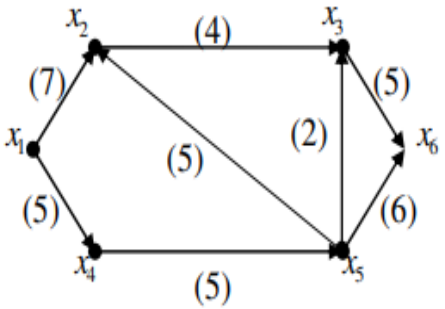
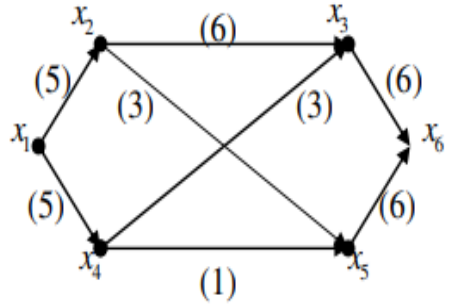
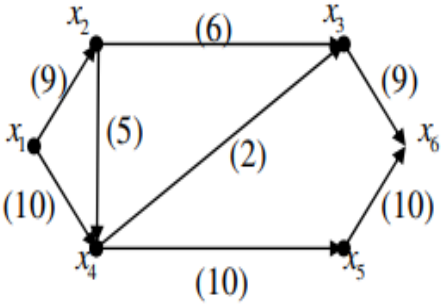
Номер варіанта	**Властивість**
1	Граф є повним та має ***m*** ребер; ***m*= 45**
2	Граф є повним та має ***m*** ребер; ***m*= 66**
3	Граф є повним та має ***m*** ребер; ***m*= 36**
4	Граф є повним та має ***m*** ребер; ***m*= 55**
5	Граф є повним та має ***m*** ребер; ***m*= 28**
6	Граф є повним та має ***m*** ребер; ***m*= 78**

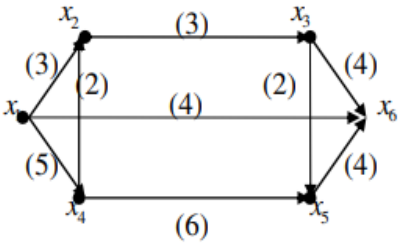
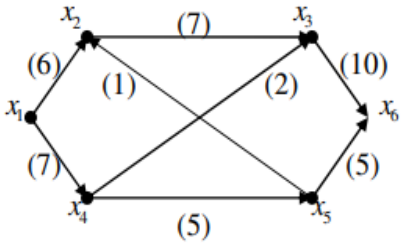
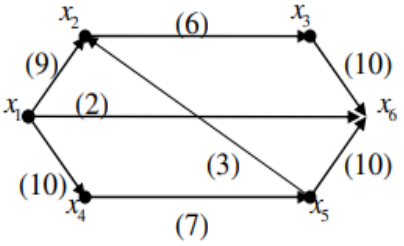
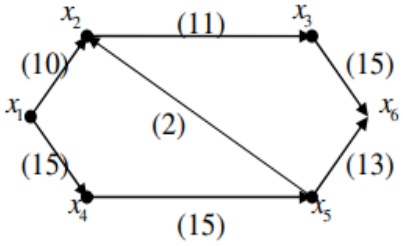
7	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 105**
8	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 91**
9	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 136**
10	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 120**
11	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 171**
12	Граф є повним та має $\boldsymbol{m}$ ребер; $\boldsymbol{m}$**= 21**
13	Граф має дві компоненти зв'язності $\boldsymbol{K_3, K_p}$. Число ребер графа $\boldsymbol{m=31}$
14	Граф має дві компоненти зв'язності $\boldsymbol{K_4, K_p}$. Число ребер графа $\boldsymbol{m=51}$
15	Граф має дві компоненти зв'язності $\boldsymbol{K_2, K_p}$. Число ребер графа $\boldsymbol{m=37}$
16	Граф має дві компоненти зв'язності $\boldsymbol{O_1, K_p}$. Число ребер графа $\boldsymbol{m=55}$
17	Граф має дві компоненти зв'язності $\boldsymbol{O_1, K_p}$. Число ребер графа $\boldsymbol{m=78}$
18	Граф має дві компоненти зв'язності $\boldsymbol{K_5, K_p}$. Число ребер графа $\boldsymbol{m=28}$
19	Граф має дві компоненти зв'язності $\boldsymbol{K_4, K_p}$. Число ребер графа $\boldsymbol{m=61}$
20	Граф має дві компоненти зв'язності $\boldsymbol{K_4, K_p}$. Число ребер графа $\boldsymbol{m=72}$
21	Граф має дві компоненти зв'язності $\boldsymbol{K_3, K_p}$. Число ребер графа $\boldsymbol{m=58}$
22	Граф має дві компоненти зв'язності $\boldsymbol{K_3, K_p}$. Число ребер графа $\boldsymbol{m=39}$
23	Граф має дві компоненти зв'язності $\boldsymbol{K_4, K_p}$. Число ребер графа $\boldsymbol{m=27}$

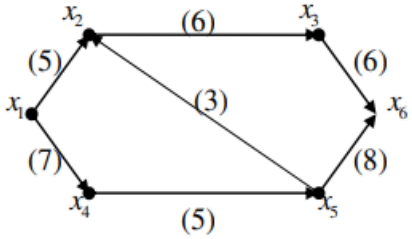
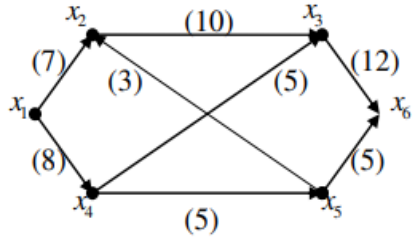
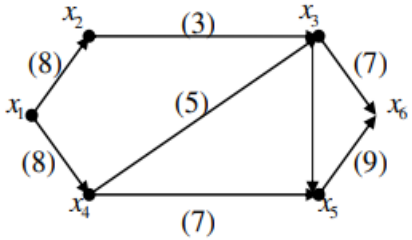
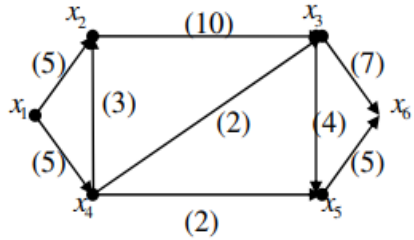
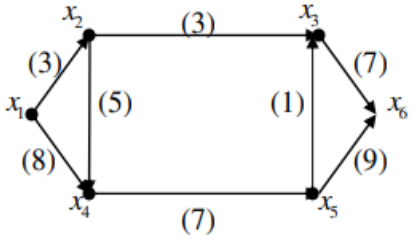
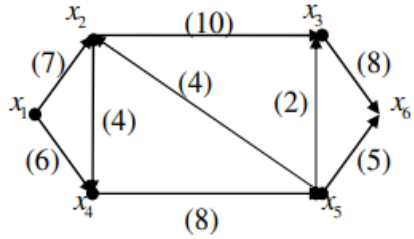
24	Граф має дві компоненти зв'язності $\boldsymbol{K_3}, \boldsymbol{K_p}$. Число ребер графа ***m=49***
25	Граф є ***r***- регулярним***, r =6;*** число ребер ***m=24***
26	Граф є ***r***- регулярним***, r =3;*** число ребер ***m=15***
27	Граф є ***r***- регулярним***, r =5;*** число ребер ***m=30***
28	Граф є ***r***- регулярним***, r =7;*** число ребер ***m=35***
29	Граф є ***r***- регулярним***, r =12;*** число ребер ***m=120***
30	Граф є ***r***- регулярним***, r =4;*** число ребер ***m=18***

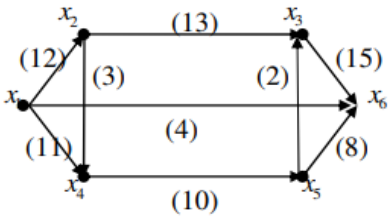
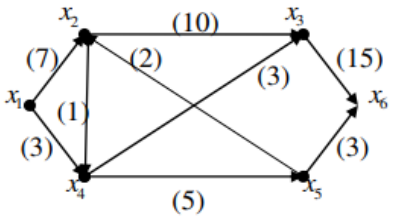
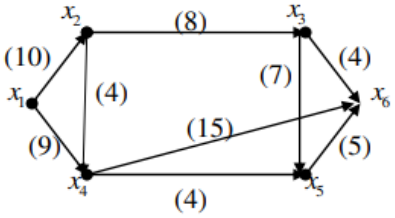
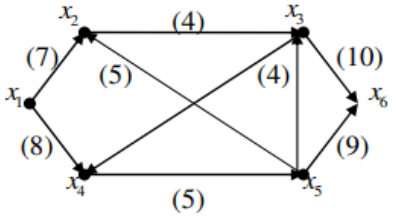
5. Користуючись алгоритмом Дейкстри знайти найкоротший шлях від вершини x_1 до вершини x_6.

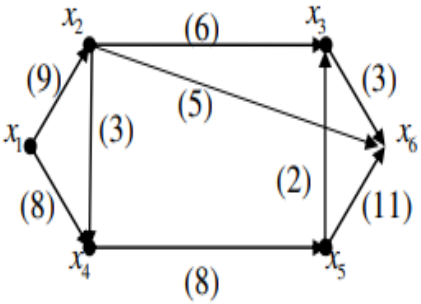
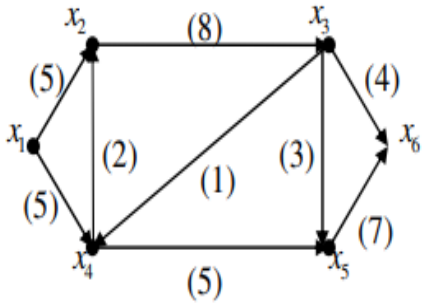
01		16	
02		17	
03		18	

04		19	
05		20	
06		21	
07		22	

08		23	
09		24	

10		25	
11		26	
12		27	

13		28	
14		29	

15		30	

БУЛЕВІ ФУНКЦІЇ

1. Булеву функцію задано формулою. Задайте цю функцію у вигляді таблиці. На основі отриманої таблиці для даної функції побудуйте її ДДНФ. Знайдіть номер функції.

Варіант	$\boldsymbol{f(x,y,z)}$	**Варіант**	$\boldsymbol{f(x,y,z)}$
1	$((x\|y)\downarrow \bar{z})\sim(\bar{x}\vee z)$	16	$\overline{\boldsymbol{x}\to\bar{\boldsymbol{z}}}\oplus(\boldsymbol{y}\sim\bar{\boldsymbol{x}}\boldsymbol{z})$
2	$(\bar{x}\ \oplus yz)\to(y\sim\bar{z})$	17	$((x\downarrow y)\downarrow \overline{xz})\sim(y\to z)$
3	$\overline{(x\bar{y}\sim zx)}\downarrow y$	18	$\overline{(x\bar{y}\sim zx)}\|(y\sim\bar{x}z)$
4	$x\oplus(x\vee\bar{y})\to(x\to\bar{z})$	19	$x\sim(x\vee\bar{y})\to(x\oplus y\bar{z})$
5	$x(y\vee\bar{z})\sim(\bar{y}\oplus z)$	20	$x\oplus(y\bar{z})\sim(\bar{y}\oplus z)$

6	$\overline{xz \to \bar{y}} \vee (xy \sim \bar{z})$	21	$\overline{xz \to \bar{y}} \mid (xy \sim \bar{z})$
7	$(x \oplus y\bar{z}) \mid (xz \to \bar{y})$	22	$(x \vee y\bar{z}) \downarrow (xz \to \bar{y})$
8	$((x \oplus \bar{y}) \downarrow \overline{yz}) \sim \bar{x}$	23	$((x \to \bar{y}) \downarrow \overline{yz}) \sim x\bar{y}$
9	$(xy \to \bar{z}) \mid (\bar{x} \to yz)$	24	$(xy \to \bar{z}) \oplus (\bar{x} \to yz)$
10	$(x \downarrow \bar{y}) \mid \overline{x \vee \bar{z}}$	25	$(x \mid \bar{y}) \sim \overline{x \vee \bar{z}\bar{y}}$
11	$(\bar{x} \mid (x \to \overline{y \sim z})) \sim y\bar{z}$	26	$(\bar{x} \downarrow (x \sim \overline{y \sim z})) \to y\bar{z}$
12	$x \oplus (y \downarrow (\bar{x} \vee z))$	27	$xz \oplus (y \mid (\bar{x} \vee z))$
13	$(x \sim y\bar{z}) \mid (\bar{x} \vee \bar{z})$	28	$(\bar{x} \to y\bar{z}) \downarrow (\bar{x} \vee \bar{z})$
14	$\overline{x \to (\bar{y} \vee z)} \downarrow (\bar{x} \vee \bar{y})$	29	$\overline{x \oplus (\bar{y} \vee z)} \mid (\bar{x} \oplus \bar{y})$
15	$\big(x \downarrow (y\bar{z})\big) \mid (x \oplus \bar{y})$	30	$\big(x \mid (y \oplus \bar{z})\big) \to (x \mid \bar{y})$

2. Булева функція задана вектором значень. Користуючись методом невизначених коефіцієнтів, запишіть її у вигляді многочлена Жегалкіна.

Варіант	$\boldsymbol{f(x, y, z)}$	Варіант	$\boldsymbol{f(x, y, z)}$
1	(1; 1; 0; 0; 0; 1; 0; 1)	16	(0; 1; 0; 1; 1; 1; 0; 1)
2	(1; 1; 1; 0; 1; 0; 0; 1)	17	(1; 0; 0; 0; 1; 1; 0; 0)
3	(1; 1; 0; 1; 0; 1; 1; 1)	18	(0; 0; 0; 0; 0; 1; 0; 1)
4	(0; 1; 1; 0; 0; 1; 0; 1)	19	(1; 1; 0; 1; 0; 0; 0; 0)
5	(1; 1; 1; 0; 0; 0; 0; 1)	20	(1; 0; 0; 1; 0; 0; 0; 0)
6	(1; 0; 1; 0; 1; 1; 0; 1)	21	(0; 0; 1; 0; 0; 1; 0; 1)
7	(1; 0; 0; 1; 0; 1; 0; 1)	22	(0; 1; 0; 0; 0; 1; 1; 1)
8	(1; 1; 0; 0; 0; 1; 0; 1)	23	(1; 1; 0; 0; 0; 1; 0; 1)
9	(1; 0; 0; 0; 0; 1; 1; 1)	24	(0; 1; 1; 0; 1; 1; 0; 0)
10	(0; 1; 1; 0; 0; 1; 0; 0)	25	(1; 1; 0; 0; 0; 0; 0; 1)
11	(1; 1; 1; 0; 0; 1; 1; 1)	26	(0; 1; 0; 0; 1; 1; 0; 1)
12	(1; 0; 0; 0; 1; 1; 0; 1)	27	(0; 1; 0; 0; 1; 1; 1; 1)
13	(0; 1; 1; 0; 1; 1; 0; 1)	28	(1; 1; 0; 0; 0; 1; 0; 1)
14	(1; 0; 0; 0; 0; 1; 1; 0)	29	(1; 1; 1; 0; 0; 1; 0; 0)

15	(1; 0; 0; 1; 1; 1; 0; 1)	30	(0; 1; 0; 0; 0; 1; 1; 1)

ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ. КОНГРУННЦІЇ

1. Користуючись розширеним алгоритмом Евкліда для даних чисел ***a; b*** знайти найбільший спільний дільник, множники Безу та записати НСД у вигляді лінійної комбінації чисел ***a; b.***

Варіант	***A***	***B***	Варіант	***A***	***B***
1	336	468	16	1053	286
2	595	918	17	336	588
3	2548	620	18	918	306
4	984	756	19	342	261
5	760	342	20	845	585
6	816	936	21	348	609
7	560	1134	22	496	837
8	594	847	23	312	234
9	435	406	24	231	847
10	248	372	25	705	564
11	592	208	26	638	232
12	575	285	27	875	650
13	196	273	28	444	592
14	369	656	29	306	425
15	516	602	30	209	187

2. Для даних чисел $n_1; n_2$ обчисліть функцію Ейлера.

Варіант	n_1	n_2	Варіант	n_1	n_2
1	23	1440	16	51	912
2	31	336	17	79	1104

3	101	1080	18	51	1488
4	103	448	19	84	1968
5	19	1664	20	62	837
6	29	544	21	41	1161
7	43	864	22	107	1107
8	53	832	23	95	2160
9	59	960	24	74	1125
10	17	1216	25	37	1375
11	73	1053	26	67	1625
12	61	1863	27	83	800
13	97	1377	28	85	400
14	46	325	29	87	1701
15	34	775	30	111	1215

3. Користуючись властивостями конгруенцій на множині класів еквівалентності Z_m обчисліть значення виразу.

Варіант	Z_m	
1	Z_{17}	$19^{17} + 37^{23} + 53$
2	Z_{23}	$47^{91} + 26^{13} + 65$
3	Z_{32}	$63^{37} + 34^{11} - 45$
4	Z_{18}	$37^{97} + 34^{15} + 44$
5	Z_{23}	$71^{19} + 22^{57} - 43$
6	Z_{37}	$73^{56} + 39^{11} + 67$
7	Z_{11}	$13^{15} + 21^{19} - 19$
8	Z_{35}	$106^{93} + 30^{11} + 85$
9	Z_{33}	$37^{17} + 65^{81} - 97$
10	Z_{13}	$40^{75} + 12^{83} - 76$
11	Z_{28}	$55^{43} + 86^{13} + 49$

12	Z_{23}	$72^{33} + 68^{43} - 98$
13	Z_{17}	$35^{22} + 20^{11} + 32$
14	Z_{13}	$41^{15} + 38^{23} - 143$
15	Z_{25}	$53^{14} + 49^{37} + 154$
16	Z_{20}	$65^{9} + 19^{22} + 197$
17	Z_{19}	$39^{64} + 18^{12} - 43$
18	Z_{36}	$39^{23} + 71^{45} + 101$
19	Z_{31}	$63^{82} + 65^{9} - 93$
20	Z_{28}	$27^{53} + 59^{11} + 95$
21	Z_{22}	$43^{17} + 82^{7} - 87$
22	Z_{41}	$43^{7} + 81^{31} + 93$
23	Z_{19}	$58^{97} + 17^{13} - 112$
24	Z_{32}	$95^{51} + 34^{15} + 103$
25	Z_{27}	$80^{43} + 29^{10} - 101$
26	Z_{16}	$33^{67} + 50^{13} + 109$
27	Z_{26}	$25^{37} + 54^{9} - 96$
28	Z_{14}	$44^{17} + 55^{23} + 90$
29	Z_{21}	$68^{9} + 43^{77} + 105$
30	Z_{15}	$33^{7} + 44^{18} - 113$

4. У кільці Z_m методом множників Безу для елемента ***a*** обчисліть мультиплікативно обернений. Зробіть перевірку.

Варіант	Z_m	$\boldsymbol{A}$	Варіант	Z_m	$\boldsymbol{A}$
1	Z_{29}	17	16	Z_{43}	28
2	Z_{43}	20	17	Z_{29}	14

3	Z_{23}	18	18	Z_{19}	12
4	Z_{19}	7	19	Z_{31}	25
5	Z_{31}	23	20	Z_{53}	28
6	Z_{17}	9	21	Z_{71}	34
7	Z_{53}	26	22	Z_{97}	50
8	Z_{71}	30	23	Z_{61}	45
9	Z_{61}	33	24	Z_{101}	42
10	Z_{97}	40	25	Z_{59}	27
11	Z_{101}	51	26	Z_{83}	44
12	Z_{59}	12	27	Z_{47}	21
13	Z_{83}	45	28	Z_{107}	63
14	Z_{107}	48	29	Z_{17}	10
15	Z_{47}	10	30	Z_{13}	8

5. Користуючись китайською теоремою про остачі, розв’яжіть систему конруенцій. Зробіть перевірку.

Варіант		**Варіант**	
1	$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}$	16	$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 5 \pmod{7} \\ x \equiv 6 \pmod{11} \end{cases}$
2	$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 8 \pmod{13} \\ x \equiv 4 \pmod{7} \end{cases}$	17	$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 9 \pmod{23} \\ x \equiv 7 \pmod{12} \end{cases}$
3	$\begin{cases} x \equiv 10 \pmod{17} \\ x \equiv 3 \pmod{7} \\ x \equiv 9 \pmod{1} \end{cases}$	18	$\begin{cases} x \equiv 10 \pmod{11} \\ x \equiv 9 \pmod{17} \\ x \equiv 3 \pmod{21} \end{cases}$

4 $\begin{cases} x \equiv 2 \pmod{19} \\ x \equiv 5 \pmod{7} \\ x \equiv 13 \pmod{15} \end{cases}$

5 $\begin{cases} x \equiv 7 \pmod{17} \\ x \equiv 6 \pmod{9} \\ x \equiv 8 \pmod{13} \end{cases}$

6 $\begin{cases} x \equiv 8 \pmod{10} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$

7 $\begin{cases} x \equiv 12 \pmod{31} \\ x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{8} \end{cases}$

8 $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}$

9 $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{8} \end{cases}$

10 $\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{4} \end{cases}$

11 $\begin{cases} x \equiv 5 \pmod{19} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{10} \end{cases}$

19 $\begin{cases} x \equiv 8 \pmod{9} \\ x \equiv 6 \pmod{7} \\ x \equiv 13 \pmod{17} \end{cases}$

20 $\begin{cases} x \equiv 11 \pmod{13} \\ x \equiv 6 \pmod{20} \\ x \equiv 12 \pmod{19} \end{cases}$

21 $\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{15} \end{cases}$

22 $\begin{cases} x \equiv 18 \pmod{43} \\ x \equiv 9 \pmod{11} \\ x \equiv 2 \pmod{5} \end{cases}$

23 $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}$

24 $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 4 \pmod{7} \\ x \equiv 8 \pmod{13} \end{cases}$

25 $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{5} \end{cases}$

26 $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{23} \end{cases}$

12 $\begin{cases} x \equiv 9 \pmod{11} \\ x \equiv 6 \pmod{29} \\ x \equiv 2 \pmod{5} \end{cases}$

27 $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 5 \pmod{17} \\ x \equiv 3 \pmod{12} \end{cases}$

13 $\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 11 \pmod{15} \end{cases}$

28 $\begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 1 \pmod{5} \\ x \equiv 11 \pmod{21} \end{cases}$

14 $\begin{cases} x \equiv 22 \pmod{41} \\ x \equiv 6 \pmod{7} \\ x \equiv 1 \pmod{5} \end{cases}$

29 $\begin{cases} x \equiv 12 \pmod{29} \\ x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$

15 $\begin{cases} x \equiv 7 \pmod{31} \\ x \equiv 6 \pmod{10} \\ x \equiv 3 \pmod{7} \end{cases}$

30 $\begin{cases} x \equiv 8 \pmod{19} \\ x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{20} \end{cases}$

6. Користуючись критерієм Ейлера, визначити чи є елемент ***a*** кваратичним лишком на множині Z_m.

Варіант	Z_m	***A***	Варіант	Z_m	***A***
1	Z_{13}	7	16	Z_{17}	9
2	Z_{23}	12	17	Z_{19}	10
3	Z_{11}	9	18	Z_{43}	19
4	Z_{19}	11	19	Z_{31}	17
5	Z_{17}	5	20	Z_{11}	8
6	Z_{19}	8	21	Z_{29}	12
7	Z_{31}	20	22	Z_{53}	11
8	Z_{11}	9	23	Z_{37}	24
9	Z_{13}	10	24	Z_{13}	9
10	Z_{17}	7	25	Z_{53}	28
11	Z_{23}	6	26	Z_{29}	21

12	Z_{19}	15	27	Z_{29}	14
13	Z_{11}	7	28	Z_{37}	35
14	Z_{31}	10	29	Z_{17}	12
15	Z_{13}	5	30	Z_{41}	25

7. Розв’яжіть конгруенцію, або покажіть, що вона не має розв’язків.

1	$x^2 \equiv 9(mod\ 77)$	16	$x^2 \equiv 16(mod\ 161)$
2	$x^2 \equiv 16(mod\ 209)$	17	$x^2 \equiv 6(mod\ 217)$
3	$x^2 \equiv 12(mod\ 217)$	18	$x^2 \equiv 8(mod\ 517)$
4	$x^2 \equiv 10(mod\ 341)$	19	$x^2 \equiv 12(mod\ 77)$
5	$x^2 \equiv 9(mod\ 133)$	20	$x^2 \equiv 6(mod\ 517)$
6	$x^2 \equiv 16(mod\ 161)$	21	$x^2 \equiv 20(mod\ 301)$
7	$x^2 \equiv 9(mod\ 301)$	22	$x^2 \equiv 21(mod\ 341)$
8	$x^2 \equiv 18(mod\ 209)$	23	$x^2 \equiv 6(mod\ 77)$
9	$x^2 \equiv 7(mod\ 341)$	24	$x^2 \equiv 24(mod\ 517)$
10	$x^2 \equiv 8(mod\ 161)$	25	$x^2 \equiv 5(mod\ 217)$

11	$x^2 \equiv 20(mod\ 517)$	26	$x^2 \equiv 4(mod\ 301)$
12	$x^2 \equiv 8(mod\ 301)$	27	$x^2 \equiv 3(mod\ 217)$
13	$x^2 \equiv 10(mod\ 133)$	28	$x^2 \equiv 10(mod\ 301)$
14	$x^2 \equiv 5(mod\ 209)$	29	$x^2 \equiv 15(mod\ 161)$
15	$x^2 \equiv 16(mod\ 341)$	30	$x^2 \equiv 10(mod\ 253)$

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Мехед Д.М., Ткач Ю.М. Базелевич В.М. Спеціальні глави математики. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 124с.
2. Нікольський Ю.В., Пасічник В.В., Щербина Ю.М. Дискретна математика. – Львів: «Магнолія -2006», 2019. – 432 с.
3. Higher mathematics. Part 1: Manual : навч. посібник / V.P. Denisiuk, L.I. Grishina, O.V. Karupu, T.A. Oleshko, V.V. Pakhnenko, V.K. Repeta.; NAU.- Kyiv: NAU, 2006.-268 p.
4. Ганюшкін О.Г., Безущак О.О. Теорія груп.- Київ: Видавничо-поліграфічний центр «Київський університет», 2005. 126 с.
5. Гасяк О.С. Формальна логіка. Розв'язкові процедури, алгоритми, словник базових термінів і понять: навч.посібник. – Чернівці: Чернівецький нац. ун-т, 2014. – 544 с.