Варіант 1

1. Знайти порядок елемента групи $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$ де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to Z, f(x) = [x]$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 2

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 200, k = 8$
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, c = 2, x_0 = -1$.
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 3

1. Знайти порядок групи поворотів правильного тетраедра
2. Розв'язати систему рівнянь $\begin{cases} 9x + 2y = 8 \\ 2x + 3y = 11 \end{cases}$ в полі Z_{13}
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{2x^3 - x^2 - 5x + 4}{(x+1)^5}$
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 4

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число a – фіксоване, відносно множення.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^+ \to R, f(x) = \log_2 x$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 2 у полі Z_7 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 5

1. Скласти таблицю Келі групи D_3, де D_n – група симетрій правильного n-кутника
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 140, k = 35$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 6

1. Знайти порядок елемента групи $g = \cos\frac{\pi}{5} + i\sin\frac{\pi}{5} \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$ в полі Z_5
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{x^3-10x+4}{(x-2)^5}$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 7

1. З'ясувати, чи буде групою множина всіх відображень множини $M = \{1, 2, \ldots, n\}$ у себе відносно суперпозиції відображень.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to R^+$, $f(x) = 2^x$
3. Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 8

1. Довести, що у групі $(ab)^{-1} = b^{-1}a^{-1}$.
2. Визначити кількість генераторів мультиплікативної групи поля $Z_3 7$. Знайти хоча б один.
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_3 за допомогою незвідного многочлена $F[x] = x^4 + x^3 + x^2 + x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 9

1. Довести, що в будь–якій групі парного ступеня є елемент порядку 2.
2. Знайти символ Лежандра/Якобі $\left(\frac{39}{209}\right)$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 10

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$
2. Розв'язати рівняння $x^2 - (3 + 3\sqrt{2})x + 4 + 6\sqrt{2}$ у полі $Q(\sqrt{2})$.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 3 у полі Z_5 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 11

1. Нехай порядок елемента x у групі дорівнює N. Довести, що порядок елемента x^{-1} також дорівнює N.
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{143}, a = 97$.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 12

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.
2. Розв'язати систему рівнянь $\begin{cases} 2x - y = 5 \\ x - 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_7 за допомогою незвідного многочлена $F[x] = x^3 + x^2 + x + 2$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 13

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого натурального числа n.
2. Знайти всі генератори мультиплікативної групи поля Z_19
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24, c = -2, x_0 = -1$.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 14

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина комплексних матриць вигляду $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to R^*, f(z) = \frac{1}{|z|}$
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 15

1. Знайти порядок елемента групи $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \in GL_3(Z)$, де $GL_n(Z)$ – група за множенням усіх невироджених цілочисельних матриць порядку n , обернені до яких також є цілочисельними
2. Обчислити всі квадратині корені з 2 у скінченному полі Z_17 за алгоритмом Чіпполи
3. Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 16

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3} + z\sqrt[3]{9}$, де $x, y, z \in \mathbb{Q}$
2. Визначити кількість генераторів мультиплікативної групи поля Z_31. Знайти хоча б один.
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 17

1. Довести, що в групі елементи x і yxy^{-1} мають однаковий порядок.
2. Розв'язати рівняння $x^2 - 2\sqrt{3}x - 1 = 0$ у полі $Q(\sqrt{3})$.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x, c = 1, x_0 = -2$.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 18

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3}$, де $x, y \in \mathbb{Q}$
2. Обчислити всі квадратині корені з 5 у скінченному полі $Z_1 1$ за алгоритмом Чіпполи
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - x^3 + 11x^2 - 2x - 2$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 19

1. Скласти таблицю Келі групи $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 105, k = 15$
3. Знайти порядок многочлена $x^3 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 20

1. Знайти порядок елемента групи $g = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^* \to R^*, f(x) = \frac{1}{x}$
3. Знайти порядок многочлена $x^3 + x^2 + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 21

1. Знайти порядок елемента групи $g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(C)$, де $GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{150}, a = 101$.
3. Знайти елемент обернений до $G[x] = x^4 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $F[x] = x^5 + x^2 + 1$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 22

1. З'ясувати, чи буде групою множина підстановок $\{(1)(2)(3)(4); (12)(34); (13)(24); (14)(23)\}$ відносно операції суперпозиції.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to C^*, f(z) = \frac{z}{|z|}$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 23

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt{3}$, де $x, y \in \mathbb{Q}$
2. Розв'язати рівняння $x^2 + x\sqrt{3} - 7 + 3\sqrt{3} = 0$ у полі $Q(\sqrt{3})$.
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_7 за допомогою незвідного многочлена $F[x] = x^3 + x^2 + x + 2$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 24

1. Скласти таблицю Келі групи Z_9^*, де Z_n^* – мультиплікативна група оборотних класів лишків за модулем числа n
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 10 & 11 \\ 5 & 8 \end{pmatrix}$ в полі Z_{13}
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 25

1. Довести, що група, в якій всі елементи мають порядок 2, комутативна.
2. Знайти всі генератори мультиплікативної групи поля Z_17
3. Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 26

1. Нехай порядок елемента xy дорівнює N. Довести, що порядок елемента yx також дорівнює N.
2. Розв'язати систему рівнянь $\begin{cases} 7x + 5y = 4 \\ 3x + 10y = 7 \end{cases}$ в полі Z_{13}
3. Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 27

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. Обчислити всі квадратині корені з 3 у скінченному полі Z_13 за алгоритмом Чіпполи
3. Знайти порядок многочлена $x^3 + x^2 + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 28

1. Знайти порядок групи поворотів куба
2. Розв'язати систему рівнянь $\begin{cases} 2x + y = 5 \\ x + 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 29

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 4 & 6 & 2 & 5 & 3 & 1 \end{pmatrix} \in S_8$
2. З'ясувати, чи буде множина М відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента а. $M = Z_{179}, a = 96$.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 30

1. З'ясувати, чи буде групою множина всіх комплексних коренів усіх степенів з одиниці відносно операції множення.
2. Знайти символ Лежандра/Якобі $\left(\frac{37}{151}\right)$
3. Знайти елемент обернений до $G[x] = x^4 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $F[x] = x^5 + x^2 + 1$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 31

1. Скласти таблицю Келі групи D_3, де D_n – група симетрій правильного n-кутника
2. З'ясувати, чи буде множина М відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента а. $M = Z_{150}, a = 101$.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 3 у полі Z_5 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 32

1. Нехай порядок елемента xy дорівнює N. Довести, що порядок елемента yx також дорівнює N.
2. Розв'язати систему рівнянь $\begin{cases} 7x + 5y = 4 \\ 3x + 10y = 7 \end{cases}$ в полі Z_{13}
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24, c = -2, x_0 = -1$.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 33

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to C^*, f(z) = \frac{z}{|z|}$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 2 у полі Z_7 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 34

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число a – фіксоване, відносно множення.
2. Визначити кількість генераторів мультиплікативної групи поля $Z_3 7$. Знайти хоча б один.
3. Знайти порядок многочлена $x^3 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 35

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. Розв'язати рівняння $x^2 - (3 + 3\sqrt{2})x + 4 + 6\sqrt{2}$ у полі $Q(\sqrt{2})$.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x, c = 1, x_0 = -2$.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 36

1. Скласти таблицю Келі групи Z_9^*, де Z_n^* – мультиплікативна група оборотних класів лишків за модулем числа n
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 105, k = 15$
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 37

1. Скласти таблицю Келі групи $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$
2. Обчислити всі квадратині корені з 2 у скінченному полі Z_17 за алгоритмом Чіпполи
3. Відокремити дійсні корені многочлена $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 38

1. З'ясувати, чи буде групою множина всіх відображень множини $M = \{1, 2, \ldots, n\}$ у себе відносно суперпозиції відображень.
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{179}, a = 96$.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, c = 2, x_0 = -1$.
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 39

1. Знайти порядок групи поворотів куба
2. Знайти всі генератори мультиплікативної групи поля Z_17
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{x^3-10x+4}{(x-2)^5}$
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 40

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 4 & 6 & 2 & 5 & 3 & 1 \end{pmatrix} \in S_8$
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 200, k = 8$
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{2x^3-x^2-5x+4}{(x+1)^5}$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 41

1. Знайти порядок елемента групи $g = \cos\frac{\pi}{5} + i\sin\frac{\pi}{5} \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^+ \to R, f(x) = \log_2 x$
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_3 за допомогою незвідного многочлена $F[x] = x^4 + x^3 + x^2 + x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 42

1. Знайти порядок елемента групи $g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(C)$, де $GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to Z, f(x) = [x]$
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - x^3 + 11x^2 - 2x - 2$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 43

1. Знайти порядок елемента групи $g = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. Розв'язати систему рівнянь $\begin{cases} 9x + 2y = 8 \\ 2x + 3y = 11 \end{cases}$ в полі Z_{13}
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 44

1. Знайти порядок елемента групи $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \in GL_3(Z)$, де $GL_n(Z)$ – група за множенням усіх невироджених цілочисельних матриць порядку n , обернені до яких також є цілочисельними
2. Обчислити всі квадратині корені з 5 у скінченному полі Z_11 за алгоритмом Чіпполи
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - x^3 + 11x^2 - 2x - 2$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 45

1. Довести, що у групі $(ab)^{-1} = b^{-1}a^{-1}$.
2. Знайти всі генератори мультиплікативної групи поля Z_19
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x, c = 1, x_0 = -2$.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 46

1. Довести, що в групі елементи x і yxy^{-1} мають однаковий порядок.
2. Знайти символ Лежандра/Якобі $\left(\frac{39}{209}\right)$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 3 у полі Z_5 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 47

1. З'ясувати, чи буде групою множина всіх комплексних коренів усіх степенів з одиниці відносно операції множення.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$ в полі Z_5
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 2 у полі Z_7 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 48

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3}$, де $x, y \in \mathbb{Q}$
2. Визначити кількість генераторів мультиплікативної групи поля $Z_3 1$. Знайти хоча б один.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 49

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого натурального числа n.
2. Розв'язати систему рівнянь $\begin{cases} 2x - y = 5 \\ x - 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_3 за допомогою незвідного многочлена $F[x] = x^4 + x^3 + x^2 + x + 1$
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 50

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина комплексних матриць вигляду $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$
2. Розв'язати систему рівнянь $\begin{cases} 2x + y = 5 \\ x + 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти елемент обернений до $G[x] = x^4 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $F[x] = x^5 + x^2 + 1$
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 51

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 10 & 11 \\ 5 & 8 \end{pmatrix}$ в полі Z_{13}
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24, c = -2, x_0 = -1$.
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 52

1. Знайти порядок групи поворотів правильного тетраедра
2. Обчислити всі квадратині корені з 3 у скінченному полі Z_13 за алгоритмом Чіпполи
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 53

1. Довести, що в будь–якій групі парного ступеня є елемент порядку 2.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to R^*, f(z) = \frac{1}{|z|}$
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_7 за допомогою незвідного многочлена $F[x] = x^3 + x^2 + x + 2$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 54

1. З'ясувати, чи буде групою множина підстановок $\{(1)(2)(3)(4); (12)(34); (13)(24); (14)(23)\}$ відносно операції суперпозиції.
2. Розв'язати рівняння $x^2 + x\sqrt{3} - 7 + 3\sqrt{3} = 0$ у полі $Q(\sqrt{3})$.
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 55

1. Знайти порядок елемента групи $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$ де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^* \to R^*, f(x) = \frac{1}{x}$
3. Знайти порядок многочлена $x^3 + x^2 + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 56

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt{3}$, де $x, y \in \mathbb{Q}$
2. Розв'язати рівняння $x^2 - 2\sqrt{3}x - 1 = 0$ у полі $Q(\sqrt{3})$.
3. Знайти порядок многочлена $x^3 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 57

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3} + z\sqrt[3]{9}$, де $x, y, z \in \mathbb{Q}$
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 140, k = 35$
3. Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 58

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$
2. Знайти символ Лежандра/Якобі $\left(\frac{37}{151}\right)$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 59

1. Довести, що група, в якій всі елементи мають порядок 2, комутативна.
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{143}, a = 97$.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, c = 2, x_0 = -1$.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 60

1. Нехай порядок елемента x у групі дорівнює N. Довести, що порядок елемента x^{-1} також дорівнює N.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to R^+, f(x) = 2^x$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 61

1. Знайти порядок елемента групи $g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(C)$, де $GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{150}, a = 101$.
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{2x^3 - x^2 - 5x + 4}{(x+1)^5}$
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 62

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3}$, де $x, y \in \mathbb{Q}$
2. Знайти символ Лежандра/Якобі $\left(\frac{37}{151}\right)$
3. Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 63

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt{3}$, де $x, y \in \mathbb{Q}$
2. Обчислити всі квадратині корені з 3 у скінченному полі Z_13 за алгоритмом Чіпполи
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{x^3 - 10x + 4}{(x-2)^5}$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 64

1. Знайти порядок елемента групи $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$ де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5
2. Розв'язати систему рівнянь $\begin{cases} 2x + y = 5 \\ x + 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 3 у полі Z_5 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 65

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. Обчислити всі квадратині корені з 2 у скінченному полі Z_17 за алгоритмом Чіпполи
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 66

1. Нехай порядок елемента x у групі дорівнює N. Довести, що порядок елемента x^{-1} також дорівнює N.
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{179}, a = 96$.
3. Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 67

1. Скласти таблицю Келі групи $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$
2. Знайти всі генератори мультиплікативної групи поля Z_19
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x, c = 1, x_0 = -2$.
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 68

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
2. Обчислити всі квадратині корені з 5 у скінченному полі Z_11 за алгоритмом Чіпполи
3. Відокремити дійсні корені многочлена $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 69

1. Довести, що група, в якій всі елементи мають порядок 2, комутативна.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to R^+, f(x) = 2^x$
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{2x^3 - x^2 - 5x + 4}{(x+1)^5}$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 70

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого натурального числа n.
2. Розв'язати систему рівнянь $\begin{cases} 7x + 5y = 4 \\ 3x + 10y = 7 \end{cases}$ в полі Z_{13}
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 71

1. Знайти порядок групи поворотів куба
2. Розв'язати систему рівнянь $\begin{cases} 2x - y = 5 \\ x - 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_7 за допомогою незвідного многочлена $F[x] = x^3 + x^2 + x + 2$
4. Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 72

1. Знайти порядок елемента групи $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \in GL_3(Z)$, де $GL_n(Z)$ – група за множенням усіх невироджених цілочисельних матриць порядку n , обернені до яких також є цілочисельними
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 140, k = 35$
3. Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Варіант 73

1. Довести, що в групі елементи x і yxy^{-1} мають однаковий порядок.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to Z, f(x) = [x]$
3. Знайти порядок многочлена $x^3 + x^2 + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 74

1. З'ясувати, чи буде групою множина всіх відображень множини $M = \{1, 2, \ldots, n\}$ у себе відносно суперпозиції відображень.
2. Знайти всі генератори мультиплікативної групи поля Z_17
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 75

1. З'ясувати, чи буде групою множина підстановок $\{(1)(2)(3)(4); (12)(34); (13)(24); (14)(23)\}$ відносно операції суперпозиції.
2. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a. $M = Z_{143}, a = 97$.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24, c = -2, x_0 = -1$.
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 76

1. З'ясувати, чи буде групою множина всіх комплексних коренів усіх степенів з одиниці відносно операції множення.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$ в полі Z_5
3. Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_3 за допомогою незвідного многочлена $F[x] = x^4 + x^3 + x^2 + x + 1$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 77

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$
2. Розв'язати рівняння $x^2 - (3 + 3\sqrt{2})x + 4 + 6\sqrt{2}$ у полі $Q(\sqrt{2})$.
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 2 у полі Z_7 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 78

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.
2. Визначити кількість генераторів мультиплікативної групи поля $Z_3 7$. Знайти хоча б один.
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, c = 2, x_0 = -1$.
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 79

1. Довести, що в будь–якій групі парного ступеня є елемент порядку 2.
2. Знайти символ Лежандра/Якобі $\left(\frac{39}{209}\right)$
3. Знайти порядок многочлена $x^3 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 80

1. Довести, що у групі $(ab)^{-1} = b^{-1}a^{-1}$.
2. Розв'язати систему рівнянь $\begin{cases} 9x + 2y = 8 \\ 2x + 3y = 11 \end{cases}$ в полі Z_{13}
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 81

1. Скласти таблицю Келі групи D_3, де D_n – група симетрій правильного n-кутника
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to R^*, f(z) = \frac{1}{|z|}$
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - x^3 + 11x^2 - 2x - 2$
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 82

1. Нехай порядок елемента xy дорівнює N. Довести, що порядок елемента yx також дорівнює N.
2. Розв'язати рівняння $x^2 + x\sqrt{3} - 7 + 3\sqrt{3} = 0$ у полі $Q(\sqrt{3})$.
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{x^3-10x+4}{(x-2)^5}$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 83

1. Скласти таблицю Келі групи Z_9^*, де Z_n^* – мультиплікативна група оборотних класів лишків за модулем числа n
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 10 & 11 \\ 5 & 8 \end{pmatrix}$ в полі Z_{13}
3. Знайти елемент обернений до $G[x] = x^4 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $F[x] = x^5 + x^2 + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.

Варіант 84

1. Знайти порядок елемента групи $g = \cos\frac{\pi}{5} + i\sin\frac{\pi}{5} \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 105, k = 15$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 85

1. З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число a – фіксоване, відносно множення.
2. Розв'язати рівняння $x^2 - 2\sqrt{3}x - 1 = 0$ у полі $Q(\sqrt{3})$.
3. Знайти порядок многочлена $x^3 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $x^4 + x + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 5$, число, що передається $u = 4$.

Варіант 86

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина комплексних матриць вигляду $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to C^*, f(z) = \frac{z}{|z|}$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
4. Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17}. Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Варіант 87

1. Знайти порядок елемента групи $g = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^+ \to R, f(x) = \log_2 x$
3. Знайти елемент обернений до $G[x] = x^4 + x + 1$ у розширенні поля Z_2 за допомогою незвідного многочлена $F[x] = x^5 + x^2 + 1$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сеансовий код Аліси $k = 3$, число, що передається $u = 2$.

Варіант 88

1. Знайти порядок групи поворотів правильного тетраедра
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^* \to R^*, f(x) = \frac{1}{x}$
3. Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Варіант 89

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина дійсних чисел вигляду $x + y\sqrt[3]{3} + z\sqrt[3]{9}$, де $x, y, z \in \mathbb{Q}$
2. Визначити кількість генераторів мультиплікативної групи поля $Z_3 1$. Знайти хоча б один.
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - x^3 + 11x^2 - 2x - 2$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Варіант 90

1. Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 4 & 6 & 2 & 5 & 3 & 1 \end{pmatrix} \in S_8$
2. У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 200, k = 8$
3. Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
4. Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Варіант 91

1. Знайти порядок елемента групи $g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(C)$, де $GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P
2. Розв'язати систему рівнянь $\begin{cases} 2x - y = 5 \\ x - 2y = 10 \end{cases}$ в кільці Z_{18}
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Варіант 92

1. Нехай порядок елемента xy дорівнює N. Довести, що порядок елемента yx також дорівнює N.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$ в полі Z_5
3. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{2x^3 - x^2 - 5x + 4}{(x+1)^5}$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сеансовий код Аліси $k = 2$, число, що передається $u = 5$.

Варіант 93

1. Знайти порядок групи поворотів куба
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \to R^+, f(x) = 2^x$
3. Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многчлени які можна з них одержати.
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$. Обчислити їх суму

Варіант 94

1. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.
2. Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \to C^*, f(z) = \frac{z}{|z|}$
3. Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
4. Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Варіант 95

1. Довести, що група, в якій всі елементи мають порядок 2, комутативна.
2. Знайти обернену матрицю до матриці $g = \begin{pmatrix} 10 & 11 \\ 5 & 8 \end{pmatrix}$ в полі Z_{13}
3. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x, c = 1, x_0 = -2$.
4. Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11}. Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Варіант 96

1. Знайти порядок елемента групи $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$ де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5
2. Обчислити всі квадратині корені з 5 у скінченному полі $Z_1 1$ за алгоритмом Чіпполи
3. Відокремити дійсні корені многочлена $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$
4. Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^2+x+2 за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сеансовий код Аліси $k = 5$, число, що передається $u = 3$.