Кільця лишків

1. Доведіть, що якщо n – непарне число, яке не ділиться на 3, то $n^2 \equiv 1 \pmod{24}$.

2. Для яких натуральних n відображення $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$, визначене за правилом $\varphi(x) = 6x+7$ є бієкцією?

3. Доведіть, що конгруенція $ax \equiv b \pmod{n}$ має розв'язок тоді і лише тоді, коли $(a,n)|b$.

4. Розв'яжіть конгруенції

   $a)\quad 2x \equiv 2 \pmod{5}$ $\qquad b)\ 4x+3 \equiv 4 \pmod{5}$ $\qquad c)\ 7x \equiv 4 \pmod{10}$

   $d)\quad 6x+3 \equiv 4 \pmod{10}$ $\qquad e)\ 6x+3 \equiv 1 \pmod{10}$

5. Розв'яжіть систему конгруенцій

$$a)\ \begin{cases} x \equiv 2 \pmod{5} \\ 3x \equiv 1 \pmod{8} \end{cases} \qquad b)\ \begin{cases} 3x \equiv 2 \pmod{5} \\ 2x \equiv 1 \pmod{3} \end{cases}$$

6. Розв'яжіть систему конгруенцій

$$a)\ \begin{cases} 3x+2y+4z \equiv 0 \pmod{5} \\ x+y+z \equiv 0 \pmod{5} \end{cases} \qquad b)\ \begin{cases} 3x+3y+3z \equiv 4 \pmod{5} \\ x+y+z \equiv 1 \pmod{5} \end{cases}$$

$$c)\ \begin{cases} 2x+7y \equiv 3 \pmod{11} \\ 3x+4z \equiv 6 \pmod{11} \\ 4x+7y+z \equiv 0 \pmod{11} \end{cases} \qquad d)\ \begin{cases} x-2y+z \equiv 5 \pmod{13} \\ 2x+2y \equiv 7 \pmod{13} \\ 5x-3y+4z \equiv 1 \pmod{13} \end{cases}$$

7. Доведіть, що за модулем майже кожного простого числа, тобто є лише скінченна кількість винятків, система

$$\begin{cases} x+2y+2z=2 \\ 2x+y-2z=1 \\ 2x-2y+z=1 \end{cases}$$

   має єдиний розв'язок. Знайдіть ті прості числа, які є винятками, і розв'яжіть систему за модулем кожного з них.

8. Доведіть, що для кожного натурального числа n виконується точно одна з конгруенцій $n^2 \equiv 0 \pmod{8}$, $n^2 \equiv 1 \pmod{8}$, $n^2 \equiv 4 \pmod{8}$.

9. Для яких натуральних n із конгруенції $x^2 \equiv 0 \pmod{n}$ випливає конгруенція $x \equiv 0 \pmod{n}$?

10. Доведіть, що якщо конгруекція $x^2 \equiv a \pmod{65}$ має розв'язок, то конгруекція $x^2 \equiv -a \pmod{65}$ теж має розв'язок.

11. Обчисліть $3^{1000} \pmod{13}$, $7^n + 11^n \pmod{19}$.

12. Розв'яжіть конгруенцію $2^n \equiv n \pmod{7}$.

13. Скільки розв'язків за модулем n може мати конгруенція $ax \equiv b \pmod{n}$.