

7. Решить систему уравнений $\begin{cases} x+2z=1 \\ y+2z=2 \\ 2x+z=1 \end{cases}$ а) в Z_3 ; б) в Z_5 .

а) Z_3

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array} \right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 \end{array} \right) - \text{система несовместна}$$

б) Z_5

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 2 & 0 & 1 & 1 \end{array} \right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 2 & 4 \end{array} \right) \begin{cases} z=2 \\ y=3 \\ x=2 \end{cases}$$

8. Решить уравнения в Z_{11} а) $x^2=5$; б) $x^7=7$.

Z_{11}

а) $x^2=5$

$$\begin{array}{ll} 1^2=1 & 6^2=3 \\ 2^2=4 & 7^2=5 \\ 3^2=9 & 8^2=9 \\ 4^2=5 & 9^2=4 \\ 5^2=3 & 10^2=1 \end{array} \quad \text{Ответ: } x_1=4, x_2=7$$

9. Доказать, что $(p-1)! \equiv -1 \pmod{p} \Leftrightarrow p$ — простое число.

$$(p-1)! \equiv -1 \pmod{p}$$

1) $\exists p$ — составное $\Rightarrow (p-1)! \equiv 0 \not\equiv -1 \pmod{p}$

2) $\exists p$ — простое

$$(p-1)! = (p-1)(p-2) \dots (2-1) = (p-1) \cdot 1 = -1 \pmod{p}$$

10. Найти все порождающие элементы в мультипликативных группах поля: а) Z_7 ; б) Z_{11} .

а) $Z_7^* = \{1, \dots, 6\}$

1 — X 4 — X

2 — X 5 — ✓

3 — ✓ 6 — X

б) $Z_{11}^* = \{1, 2, \dots, 10\}$

1 — X 4 — X 7 — ✓ 10 — X

2 — ✓ 5 — X 8 — ✓

3 — X 6 — ✓ 9 — X