

Sprawdzian 2

1. Wyznaczyć element odwrotny do elementu $x = 3$ w $\mathbb{Z}_{65537}$.
2. W $\mathbb{Z}_{13}$ rozwiązać równanie $2x^2 + 2x + 2 = 0$.

Rozwiązania

1. Szukamy elementu $y \in \mathbb{Z}_{65537}$ takiego, aby $3 \odot_{65537} y = 1$, czyli - zgodnie z definicją działania $\odot_{65537}$ - $3 \cdot y$ przy dzieleniu przez 65537 dawało resztę 1. Wobec twierdzenia o dzieleniu z resztą szukamy y, z takich, aby:

$$3 \cdot y = 65537 \cdot z + 1.$$

Rozwiązujemy równanie diofantyczne $3 \cdot y - 65537 \cdot z = 1$; ma ono rozwiązanie, gdyż $NWD(3, -65537) = 1$ (bo 3 jest liczbą pierwszą). Zgodnie z algorytmem Euklidesa:

$$-65537 = 3 \cdot (-21846) + 1,$$

skąd:

$$3 \cdot 21846 - 65537 \cdot 1 = 1.$$

Tak więc elementem odwrotnym do 3 w ciele $\mathbb{Z}_{65537}$ jest 21846.

2. Znajdujemy wyróżnik:

$$\begin{aligned} \Delta &= 2^2 - 4 \cdot 2 \cdot 2 = 4 - 3 = 1, \\ \sqrt{\Delta} &= 1, \end{aligned}$$

i zgodnie ze znanymi wzorami:

$$\begin{aligned} x_1 &= \frac{-2-1}{4} = \frac{-3}{4} = \frac{10}{4} = 9 \quad (\text{bo } 4 \cdot 9 = 10), \\ x_2 &= \frac{-2+1}{4} = \frac{-1}{4} = \frac{12}{4} = 3 \quad (\text{bo } 4 \cdot 3 = 12). \end{aligned}$$