Kryptografia
Ćwiczenia 1
Wykład przypominający

2025-10-03

Adrian Herda
Politechnika Wrocławska

Niech $a, b \in \mathbb{Z}$ a $m \in \mathbb{Z}^+$

$$a \equiv b \bmod m \Leftrightarrow m|(b-a) \tag{1}$$

$$\exists_{k \in \mathbb{Z}} a = k * m + b \tag{2}$$

$$b = (a \bmod m) \text{ - b to reszta z dzielenia } \frac{a}{m} \tag{3}$$

$$\{0, 1, ..., m-1\} = \mathbb{Z}_M \tag{4}$$

- $+$ - jak w $\mathbb{Z}$, ale wynik $\bmod m$
- $\cdot$ - jak w $\mathbb{Z}$, ale wynik $\bmod m$

$$-x = (0 - x) = \begin{cases} m - x \text{ ,jeśli } x > 0 \\ 0 \text{ , jeśli } x = 0 \end{cases} \tag{5}$$

$$\gcd(a, m) = 1 \Leftrightarrow \exists_{k \in \mathbb{Z}_m} a * k = 1 \tag{6}$$

Zbiór liczb calkowitych dodatnich $< m$, które są względnie pierwsze z m oznaczamy $\mathbb{Z}_m^*$, $*_{\bmod m}$

0.1. Algorytm Euklidesa

$$\begin{aligned} a = r_0 &= q_1 \cdot r_1 + r_2 \\ b = r_1 &= q_2 \cdot r_2 + r_3 \\ &\vdots \end{aligned} \tag{7}$$

dajsda

0.2. Równanie diofantyczne

$$ax + by = \gcd(a, b) \tag{8}$$

0.3. Chińskie tweirdzenie o resztach (ang. CRP)

Mamy układ kongruencji

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned} \tag{9}$$

$$M = \prod_{i=1}^{r} m_i \tag{10}$$

$$\forall_{i,j,i \neq j} \gcd\big(m_i, m_j\big) = 1 \tag{11}$$

Weźmy funkcję $X(x) = (x \bmod m_1, x \bmod m_2, \cdots, x \bmod m_r)$
Szukamy funkcji X^{-1}

Theorem 0.1. Dla $1 \leq i \leq r$,

$$\begin{gathered} x \equiv a_r \bmod m_r \\ M_i = \frac{M}{m_i} \\ \gcd(M_i, m_i) = 1 \\ y_i = M_i^{-1} \bmod m_i \end{gathered} \tag{12}$$

$$\begin{aligned} \varphi(a_1, \cdots, a_r) &= \sum_{i=1}^{r} a_i M_i y_i \bmod M \\ &= X^{-1} \end{aligned} \tag{13}$$

1. Grupy, ciała i ideały