1. Modulo

$$a \equiv b \mod m \Leftrightarrow m|a-b$$

2. Chińskie reszty

Niech $m_1, \ldots, m_n$ to liczby parami względnie pierwsze. $r_i \in Z$.

$$NWD\left(m_i, m_{i+1}\right) = 1$$

Wtedy równanie:

$$\begin{cases} x \equiv_{m_1} r_1 \\ x \equiv_{m_2} r_2 \\ x \equiv_{m_n} r_n \end{cases}$$

Ma jedno rozwiązanie $\mod M = \prod_{i=1}^{n} m_i$ postaci:

$$x = N_1 M_1 + \cdots + N_n M_n, \quad \text{gdzie:}$$
$$M_i = \frac{M}{m_i}$$
$$M_i N_i \equiv_{m_i} r_i$$

3. Algosy

3.1. Euklides NWD

$$a, b \in N, a > b$$

Dzielenie z resztą a/b, jeżeli reszta $r \neq 0$ to dzielimy z resztą b/r_1. Ostatnia nie zerowa reszta to wynik.

1. Równania liniowe

$$NWD\left(a, b, c\right) = NWD\left(NWD\left(a, b\right), c\right)$$

$$ax + by = c \Leftrightarrow NWD\left(a, b\right)|c$$

$$ax = b \text{ w } Z_m \Leftrightarrow NWD\left(a, m\right)|b$$

$$x_n = x_0 + \frac{bn}{NWD\left(a, b\right)} \quad y_n = y_0 - \frac{an}{NWD\left(a, b\right)}$$