Lemma: $\forall a,b \in \mathbb{Z} \quad NSD(a,b) = NSD(b, a \bmod b)$

$\downarrow$

Eukleidův algoritmus: VSTUP: $a,b \in \mathbb{N}$, $a \geq b$
VÝSTUP: $NSD(a,b)$

$a_0 := a, \quad a_1 := b$

$a_{i+1} := a_{i-1} \bmod a_i$

if $a_{i+1} = 0$ then return a_i

$\downarrow$

Bézoutovy koeficienty

Rozšířený Eukleidův algoritmus: VSTUP: $a,b \in \mathbb{N}$, $a \geq b$
VÝSTUP: $NSD(a,b)$, u,v t.ž. $NSD(a,b) = ua + vb$

$a_0 := a, \; a_1 := b, \quad (u_0,v_0) := (1,0), \; (u_1,v_1) := (0,1)$

$a_{i+1} := a_{i-1} \bmod a_i, \quad (u_{i+1},v_{i+1}) := (u_{i-1},v_{i-1}) - (a_{i-1} \operatorname{div} a_i) \cdot (u_i,v_i)$

if $a_{i+1} = 0$ then return a_i, u_i, v_i

Základní věta aritmetiky: Buď $a \in \mathbb{N}$, $a > 1$.

Pak existují po dvou různá prvočísla $p_1, \dots, p_n$ a exponenty $k_1, \dots, k \in \mathbb{N}$ takové, že

$$a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$$

Navíc, tento zápis je jednoznačný až na pořadí činitelů.

$\boxed{\underline{\text{def}}: \quad a \equiv b \pmod{m} \iff m \mid a-b \qquad \text{"a je } \underline{\text{kongruentní}} \text{ b modulo m"}}$ $\quad (a, b \in \mathbb{Z},\ m \in \mathbb{N})$

$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$

$\equiv \pmod{m}$ je ekvivalence na $\mathbb{Z}$, tj. $\forall a, b, c$

$a \equiv a \pmod{m}$

$a \equiv b \Rightarrow b \equiv a$

$a \equiv b,\ b \equiv c \Rightarrow a \equiv c$

<u>Tvrzení</u> (invariance vůči $+, \cdot$):

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Longrightarrow \begin{array}{ll} (1) & a + c \equiv b + d \pmod{m} \\ (2) & a \cdot c \equiv b \cdot d \pmod{m} \\ (3) & \forall k \quad a^k \equiv b^k \pmod{m} \end{array}$$

<u>Tvrzení</u> (krácení): Buď $a, b, c \in \mathbb{Z}$, $c \neq 0$, $m \in \mathbb{N}$.

(1) $a \equiv b \pmod{m} \iff a \cdot c \equiv b \cdot c \pmod{m \cdot c}$

(2) $NSD(c, m) = 1 \Rightarrow \left[\, a \equiv b \pmod{m} \iff a \cdot c \equiv b \cdot c \pmod{m} \,\right]$

__def__: $\varphi(n) := \#$ čísel $k \in \{1, \dots, n\}$ nesoudělných s n

__Tvrzení__: $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ prvočíselný rozklad

$$\Rightarrow \varphi(n) = p_1^{k_1-1}(p_1-1) \cdot \ldots \cdot p_m^{k_m-1}(p_m-1)$$

__malá Fermatova věta__: (1640, 1736)

p prvočíslo, $p \nmid a \Rightarrow \boxed{a^{p-1} \equiv 1 \pmod{p}}$

__Eulerova věta__: (1763)

$\mathrm{NSD}(a,m) = 1 \Rightarrow \boxed{a^{\varphi(m)} \equiv 1 \pmod{m}}$

__Lemma__:

$$\left.\begin{array}{l} \mathrm{NSD}(a,m) = 1 \\ \Phi_m := \{k \in \{1, \dots, n\} : \mathrm{NSD}(k,n) = 1\} \\ f_a : \Phi_m \to \Phi_m \\ \quad x \mapsto ax \bmod m \end{array}\right\} \Rightarrow f_a \text{ je dobře definovaná } \underline{\text{bijekce}}$$

$\boxed{\text{RSA}}$ (Rivest, Shamir, Adleman 1977)

Inicializace: zvol prvočísla p, q

$N := p \cdot q$, $\varphi(N) = (p-1)\cdot(q-1)$

zvol e nesoudělné s N

spočti d t.ž. $d \cdot e \equiv 1 \pmod{\varphi(N)}$

VEŘEJNÝ KLÍČ: N, e (pro zašifrování)

TAJNÝ KLÍČ: d (pro dešifrování)

ZPRÁVA: $x \in \{1, \dots, N\}$ nesoudělné s N

Zašifrování: $x \mapsto x^e \pmod{N}$

Dešifrování: $y \mapsto y^d \bmod N$

Čínská věta o zbytcích (Sun-c', 3. století):

Buď $m_1, \dots, m_n \in \mathbb{N}$ po dvou nesoudělná.

Buď $u_1, \dots, u_n \in \mathbb{Z}$ libovolná.

Označ $M := m_1 \cdot \ldots \cdot m_n$.

Pak $\exists!\, x \in \{0, \dots, M-1\}$ splňující

$$x \equiv u_1 \pmod{m_1}$$
$$\vdots$$
$$x \equiv u_n \pmod{m_n}$$