- $a, b \in \mathbb{Z}$: $a \equiv b \mod n$, $n \in \mathbb{N}$
  ↳ kongruentní
  jestliže $n \mid a-b$
- vlastnosti kongruence
  – relace ekvivalence

Nechť: $a \equiv b \mod n$.
$c \equiv d \pmod n$. Pak

- $a \pm c = b \pm d \mod n$
- $a^k \equiv b^k \mod n$
- $ac \equiv bd \mod n$
- $\frac{a}{q} \equiv \frac{b}{q} \mod n$, $q \mid a$, $q \mid b$
- $a \equiv b \mod n'$, $n' \mid n$ $(q, n) = 1$

Je-li $\left.\begin{array}{l} a \equiv b \ n_1 \\ a \equiv b \ n_2 \end{array}\right\} a \equiv b \mod NSN(n_1, n_2)$

Př. 1 (i) Zbytek podělení 7^{30} číslem 50

$-1 \equiv 49 \mod 50$

$7^2 \equiv -1 \mod 50$

$(7^2)^{15} \equiv (-1)^{15} \mod 50$

7^{30} ... -1 ... hledaný zbytek

(ii) Poslední dvě cifry 7^{30}

$\rightsquigarrow$ zbytek mod 100

$\rightsquigarrow$ možnosti 49 a 99

$49 = 48+1$ $\quad 99 = 96+3$

Zbytek podělení 4

$7 \equiv -1 \mod 4$

$7^{30} \equiv (-1)^{30} = 1 \mod 4$

Zbytek 1 $\quad$ 49

Pr 2.2:

(i) $a \equiv b \bmod m^n$

Pak $a^m \equiv b^m \bmod m^{n+1}$

$$a^m - b^m = (a-b)\left(a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}\right)$$

$m^n \mid$; $a \equiv b \bmod m$

$a^{m-1} \equiv a^{m-2}b \bmod m \;/\; a^{m-2}$

$a^2 \equiv b^2 \bmod m \;/\; a^{m-3}$

$a^{m-1} \equiv a^{m-3}b^2 \bmod m$

$$\Rightarrow a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}$$

$$\equiv m \cdot a^{m-1} \bmod m$$

$$\equiv 0 \bmod m$$

$$\Rightarrow m \mid a^{m-1} + \dots + b^{m-1}$$

(ii) a lichá $\Rightarrow a^4 \equiv 1 \bmod 16$

$\rightsquigarrow$ viz 1.1 (i)

$a \equiv 1 \mod 2 = 2^1$

$a^2 \equiv 1 \mod 2^2$

$a^4 \equiv 1 \mod 2^3 = 8 \rightsquigarrow$ falso

$a^2 \equiv 1 \mod 8 = 2^3$ ↓

$a^4 \equiv 1 \mod 2^4$

$a = 4k+1$ } ...
$a = 4k+3$ }

(iii) $a \equiv \pm 1 \mod 3 = 3^1$

$a^3 \equiv (\pm 1)^3 = \pm 1 \mod 9$

2.3 (ii) $n = \overline{a_k a_{k-1} \ldots a_1 a_0}$

$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$

$10 \equiv 1 \mod 9$

$10^k \equiv 1 \mod$

$\Rightarrow n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \mod 9$

(iii) $10 \equiv -1 \mod 11$

$10^k = (-1)^k \mod 11$

$N \equiv (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots) \mod 11$

(iv) $N = 1000a + b$

$1001 = 7 \cdot 11 \cdot 13$ $\quad 7, 11, 13$

$1000 \equiv -1 \mod m$

$N \equiv -a + b \mod m$

Eulerova funkce

$\varphi(m) = |\{a \in \mathbb{N} \mid 1 \le a \le m \text{ t.z. } (a, m) = 1\}|$

$m \in \mathbb{N}$ Zejm. $\varphi(p) = p - 1$

$\hookrightarrow$ prvočíslo

Obecněji $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$

$p_1, 2p_1, 3p_1, \dots, p^{\alpha-1} \cdot p$

$p^{\alpha-1}$ čísel

Jestě obecněj:

$\varphi(m_1 \cdot m_2) = \varphi(m_1)\,\varphi(m_2)$

$(m_1, m_2) = 1$

$\varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) =$

$= (p_1 - 1) p_1^{\alpha_1 - 1} \dots (p_k - 1) p_k^{\alpha_k - 1}$

Př. 2.4

(i) $\varphi(72) = \varphi(8 \cdot 9) = \varphi(2^3)\,\varphi(3^2)$

$= (1 \cdot 2^2) \cdot (2 \cdot 3^1) = 8 \cdot 6 = \underline{\underline{24}}$

(ii) $\varphi(4n+2) = \varphi(2)\,\varphi(2n+1)$

$2(2n+1)$ $\quad = 1$

(iii) $\varphi(n)$ licht

$n = \cdots p_i^{\alpha_i} \cdots$

p_i licht $\Big\} \varphi(p_i^{\alpha_i})$ sudé

$\alpha_i \geq 1$

$\Rightarrow n = 2^{\alpha} \Rightarrow \varphi(n) = 2^{\alpha-1}$

$\Rightarrow \alpha = 1$

Zonèn : $n = 2$ nebo $n = 1$

(iv) $\varphi(n) = 30$ má dělitele

$1, 2, 3, 5, 6, 10, 15, 30$

$n = \cdots p_i^{\alpha_i} \cdots$

$\alpha_i \geq 1 \Rightarrow p_i \in \{2, 3, 7, 11, 31\}$

$\alpha_i \in \{0,1,2\}$ $\quad \alpha_1 \in \{0,1\}$

$\varphi(p_i^{\alpha_i}) = (p_i - 1) p_i^{\alpha_i - 1}$

$n = 2^{\alpha_1} 3^{\alpha_2} 7^{\alpha_3} 11^{\alpha_4} 31^{\alpha_5}$

$\alpha_1, \alpha_2 \in \{0,1,2\}$ $\quad \alpha_3, \alpha_4, \alpha_5 \in \{0,1\}$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(2^2) = 2$ → ↙

$\varphi(3^2) = 6$ ↓

$\varphi(7) = 6$

$30 = 2 \cdot \underbrace{15}_{\varphi(m')}$ → $30 = 6 \cdot 5$

$\varphi(11) = 10 \longrightarrow 30 = 10 \cdot 3$

Zbyna: $n = 2^{\alpha_1} \cdot 3^1 \cdot 5^{\alpha_5}$

$\alpha_1, \alpha_2 \in \{0, 1\}$

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3 \cdot 1) = 30$

$\varphi(2 \cdot 3 \cdot 1) = 30$

} $n \in \{31, 62\}$

(v) $\varphi(n) = \frac{n}{3} \Rightarrow 3 \mid \varphi(n) = n$

$\alpha \geq 1$ $\quad n = 3^\alpha \cdot m' \quad , \overline{3 \nmid m'}$

$$\varphi(n) = \varphi(3^\alpha \cdot n') = \varphi(3^\alpha)\cdot\varphi(n')$$

$$= 2\cdot 3^{\alpha-1}\,\varphi(n')$$

$$\overset{n}{=} 3^{\alpha-1}\cdot n' \quad // \quad \rightsquigarrow \varphi(n') = \frac{n'}{2}$$

- $2 \mid \varphi(n') - n' = 2^\beta n''$

  $\forall\alpha \quad 2 \nmid n'' \wedge 3 \nmid n''$

$$\varphi(n') = \varphi(2^\beta n'') =$$

$$= \varphi(2^\beta)\,\varphi(n'')$$

$$= 2^{\beta-1}\,\varphi(n'')$$

$$\overset{n'}{=} 2^{\beta-1} n'' \quad // \quad \rightsquigarrow \varphi(n'') = n''$$

$$\Rightarrow n'' = 1$$

Tedy: $n = 3^\alpha \cdot 2^\beta$, $\alpha, \beta \geq 1$

$$\varphi(n) = (2 \cdot 3^{\alpha-1}) \cdot 2^{\beta-1}$$

$$= 3^{\alpha-1} \cdot 2^{\beta} = \frac{n}{3}$$

Trocha teorie:

- malá Fermatova věta
  p prvočíslo, pak
  $p \nmid a$, $a \in \mathbb{Z}$ $\quad a^p \equiv a \mod p$
- obecněji máme Eulerovu větu
  $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a,n) = 1$
  pak $\boxed{a^{\varphi(n)} \equiv 1 \mod n}$

$$a^{\varphi(n)+1} \equiv a \mod n$$

Př. 2.5

(i) Poslední dvojčíslí 7^{2013}

chtěli bychom $7^{(\dots)} \equiv 1 \mod 100$

$\varphi(100) = \varphi(2^2)\varphi(5^2) = 40$

$2 \qquad 4 \cdot 5$

$7^{40} \equiv 1 \mod 100 \quad / \,(\,)^{50}$

$(7^{40})^{50} \equiv 1 \mod 100$

$7^{2000} \equiv 1 \mod 100$

$7^{2013} \equiv 7^{13} \mod 100$

Platí: $7^2 \equiv -1 \mod 50$

$7^4 \equiv 1 \mod 50$

$7^4 \equiv 1$ nebo $51 \mod 100$

$7 \equiv -1 \mod 4$

$7^4 \equiv 1 \mod 4$

4 je řád 7 mod 100

$7^4 \equiv 1 \mod 100$

$7^{4^3} = 7^{12} \equiv 1 \mod 10$

$7^{13} \equiv 7 \mod 10$

Poszukiwana cyfra to 07.