2.5 (i) Poslední dvojčíslí čísla 7^{2013}

$7^{2013} \mod 100$

Chceme

$7^{\text{něco}} \equiv 1 \mod 100$ $\quad (7,100)=1$

↳ $7^{\varphi(m)} = \boxed{7^{40} \equiv 1} \mod 100$

$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2 \cdot 4 \cdot 5 = 40$

↳ $7^{2013} = 7^{13} \cdot (7^{40})^{50} \equiv 7^{13} \mod 100$

Poté: $7^4 = (-1)^2 \equiv 1 \mod 50$

$7^4 \equiv (1 \text{ nebo } 51) \mod 100$

$7^4 \equiv (-1)^4 \equiv 1 \mod 4$

$\Rightarrow \boxed{7^4 \equiv 1 \mod 100}$

$7^{2013} \equiv 7^{13} \equiv 7 \cdot (7^4)^3 \equiv 7 \mod 100$

Závěr: Poslední dvojčíslí je 07

(ii) $2^{50}+3^{50}+4^{50} \mod 17$

$\varphi(17) = 16$

$\Rightarrow 2^{16} \equiv 3^{16} \equiv 4^{16} \mod 17$

$50 = 3 \cdot 16 + 2$

$2^{50}+3^{50}+4^{50} \equiv 2^2+3^2+4^2 \equiv$

$\equiv 4+9+16 \equiv 29 \equiv 12 \mod 17$

(iii) Poslednji dvojčísli čísla $7^{9^{5^3}}$.

$7^4 \equiv 1 \mod 100$

$9^{5^3} \equiv 1 \mod 4$ $\Rightarrow$

$\Rightarrow 7^{9^{5^3}} \equiv 7^1 = 7 \mod 100$

$\Rightarrow$ poslednji dvojčísli - 07

(IV) Poslední dvojčíslí $14^{14^{14}}$

$\rightsquigarrow (14, 100) = 2$

$\rightsquigarrow 14^{něco} \equiv 1 \mod 100$

nejde

$100 = 4 \cdot 25 \rightsquigarrow$ zkusme

určit $14^{14^{14}} \mod 25$

$4 \mid 14^{14^{14}}$

$14^{14^{14}} \mod 100$ bude $a, 25+a, 50+a$

$\rightsquigarrow$ nebo $75+a$

jediné zlichá bude dělitelné čtyřmi

$\varphi(25) = \varphi(5^2) = 4 \cdot 5 = 20$

$14^{20} \equiv 1 \mod 25$

$\hookrightarrow$ určíme $1 \cdot 4^{14} \mod 20$

$20 = 5 \cdot 4$, $4 \mid 4^{14}$

$14 \equiv -1 \mod 5$

$14^{14} \equiv 1 \mod 5$

$14^{14} \equiv^{11} 1 \text{ nebo } 6 \text{ nebo } 11 \text{ nebo } 16 \mod 20$

$\Rightarrow \boxed{14^{14} \equiv 16 \mod 20}$

$14^{14^{14}} \equiv 14^{16} \mod 25$

$14^{16} = (-11)^8 = 121^8 \equiv 21^8$

$\equiv (-4)^8 = 16^4 \equiv (-9)^4 = 81^2 \equiv$

$\equiv 6^2 \equiv 36 \equiv 11 \mod 25$

$\Rightarrow 14^{14^{14}}$ dává zbytek 36 dělení 100

$11 \text{ nebo } \boxed{36} \text{ nebo } 61 \text{ nebo } 86$

nebot' $4 \mid 14^{44^{44}}$

Závěr: poslední dvojciferí je 36

RSA šifrování

Bob a Alice komunikují

- zvolí dvě prvočísla p, q

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

n → veřejný klíč

$\varphi(n)$ → těžko zjistitelné

Alice zvolí číslo e t.ž.

$(e, \varphi(n)) = 1$ → dopočítá

veřejné známé

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

(n, e) veřejný klíč

Bob pošle zprávu M jako M^e pošle Alici

Alice M^e dešifruje jako

$(M^e)^d = M^{ed} \equiv M^1 = M \mod n$

Př 31: RSA šifra

Honza má veřejný klíč $(n=91, e=23)$ a dostal zprávu 3. Dešifrujte ji.

- $n = 91 = 7 \cdot 13$
- $\varphi(n) = 6 \cdot 12 = 72$
- chceme d t.ž. $e \cdot d \equiv 1 \mod 72$

23 a 72 nesoudělná

$72 = 3 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2 = 3 - (23 - 7 \cdot 3) = 8 \cdot 3 - 23$

$= 8(72 - 5 \cdot 23) - 23 =$

$= 8 \cdot 72 - 25 \cdot 23 = 1$

$\hookrightarrow (-25) \cdot 23 \equiv \underbrace{47 \cdot 23}_{d} \pmod{72}$

Dokončení zpravy: mod 91

$5^{47} \equiv (5^4)^{10} \cdot 5 \equiv 81^{10} \cdot 5 \equiv$

$\equiv (-10)^{10} \cdot 5 = 100^5 \cdot 5 =$

$= (+9)^5 \cdot 5 = +9 \cdot (81)^2 \cdot 5 =$

$\equiv +9 \cdot (-10)^2 \cdot 5 \equiv +5 \cdot 9 \cdot 100 \equiv$

$\equiv +3 \cdot 9 \cdot (+9) \equiv 5 \cdot 81 \equiv 5 \cdot (-10)$

$\equiv -50 \equiv 61$

Počet: $\varphi(72) = \varphi(6 \cdot 12) = \varphi(2^3 \cdot 3^2)$

$= 2^2 \cdot 2 \cdot 3 = 24$

$\Rightarrow 23^{24} \equiv 1 \mod 72$

$23 \cdot 23^{23} \equiv 1 \mod 72$

$e \quad d$

Teorie: $a \in \mathbb{Z}_1$ $m \in \mathbb{N}$

- řád čísla a mod m

je číslo $m \in \mathbb{N}$ nejmenší takové, že $a^m \equiv 1 \mod m$

$\rightsquigarrow$ platí $a^{\varphi(m)} \equiv 1 \mod m$

takže řád $m \leq \varphi(m)$

$\rightsquigarrow$ zejména $m \mid \varphi(m)$

- a primitivní kořen mod m

je takové řád $= \varphi(m)$

- primitivní kořeny existují pro n prvočísla a mocniny

- test primitivnosti $(a,n)=1$ kořene a mod n:

$$\varphi(n) = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$$

a primitivní $\Leftrightarrow$

$\Leftrightarrow a^{\frac{\varphi(n)}{q_1}} \not\equiv 1 \mod n$

$\vdots$

$a^{\frac{\varphi(n)}{q_k}} \not\equiv 1 \mod n$

Příklad 3.2

$\varphi(8) = \varphi(2^3) = 4$

- primitivní kořeny mod 8

$\rightsquigarrow$ kandidáti jsou 3, 5, 7

$3^2 = 9 \equiv 1 \mod 8$

$5^2 = 25 \equiv 1 \mod 8$

$7^2 = 49 \equiv 1 \mod 8$

8 nemá primitivní kořeny

• primitivní kořeny 11:

$\varphi(11) = 10$

$\Rightarrow$ možné řády jsou $2, 5, 10$

$a = 2 \Rightarrow 2^2 \not\equiv 1 \mod 11$

je primitivní $2^5 = 32 \equiv -1 \not\equiv 1 \mod 11$

$a = 3 \Rightarrow 3^2 = -2 \not\equiv 1$

není primitivní $3^5 = 3 \cdot 81 \equiv 3 \cdot 4 \equiv 1 \mod 11$

Výsledek: $2, 6, 7, 8$

Obecně, máme-li primitivní kořen a, pak a^x je také kořen, když $(a^x)^y \equiv 1 \mod m$

$\Leftarrow \varphi(m) \mid x \cdot y$

a^x není primitivní, jestliže $d = (x, \varphi(m)) > 1$, $y = \frac{\varphi(m)}{d}$

a^x prim. jestliže $(x, \varphi(m)) = 1$

$\varphi(m) = 10 \Rightarrow x := 1, 3, 7, 9$

$\varphi(10) = 4$

$\Rightarrow$ primitivní kořeny

$2, 2^3, 2^7, 2^9$ mod 11

$\| \quad \| \quad \| \quad \|$

8 $\quad 2 \cdot 64 \quad 8 \cdot 64$

$\| \quad \| \quad \|$

$2 \cdot (-2) \quad 8 \cdot (-2)$

$\| \quad \| \quad \|$

$-4 \quad -16 \quad -5$

$\| \quad \| \quad \|$

7 $\quad$ 6

Prim. kořeny jsou 2, 6, 7, 8

- $n = 41$ $\rightsquigarrow$ primitivní kořen 6 a jeho libovolné mocniny (vůči příslušnému)
- $n = 41^2$, $\varphi(n) = 2 \cdot 40 = 80$
  $\Rightarrow$ mocniny budou $1, 2, 4, 5, 8, 10, 20$

Z kterého vyplývá $\underline{a = 6}$.

- buď $6^{40} \not\equiv 1 \mod 41^2$
  $\hookrightarrow$ pak je to primitivní kořen
- nebo $6^{40} \equiv 1 \mod 41^2$

pak $(41+6)$ bude primitivní

neboť $(41+6)^{40} =$

$$= 41^2(\ldots) + \underbrace{\binom{40}{1} \cdot 41 \cdot 6^{39}}_{\not\equiv 0} + \underbrace{6^{40}}_{\equiv 1} \mod 41^2$$

Pbt: $6^{40} \equiv 1 \bmod 41^2 \not\equiv 1 \bmod 41^2$

tj. 6 je primitivni