UMOCŇOVÁNÍ V $\mathbb{Z}_n$

(PŘ) zbytek po dělení 7 v $X = 352 \cdot 71 + 37^{123}$

ve + a, nahradím ~~as~~ zbytky mod 7

$X = 2 \cdot 1 + 2^{123}$

$37^{123} = 37 \cdot 37 \cdot 37 \ldots \cdot 37$

$\Rightarrow$ i v základu mocniny lze dát zbytek

?: - lze nějak snížit také exponent?

Malá Fermatova věta

Nechť p je prvočíslo.

Pro každé $a \neq kp$ je $a^{p-1} \equiv 1 \pmod p$

a není dělitelné p

ANEB: po p krocích se výsledky mocnin zacyklí

$a, a^2, a^3 \ldots, a^{p-1} = 1$

$a^p = a^{p-1} \cdot a = 1 \cdot a = a$

Dějme pro $a = k \cdot p$ je $a^t \equiv 0 \pmod p$

Zpět k (PŘ) v $\mathbb{Z}_7$ $2^{7-1} = 2^6 = 1$ (dle M.F.V) ~~(dle F.m.F.v.)~~

$2^{123} = \underbrace{2^6 \cdot 2^6 \cdot 2^6 \ldots 2^6}_{(2^6)^{20}} \cdot 2^3 = 1 \cdot 1 \cdot \ldots \cdot 2^3 = 8$

$\Rightarrow X = 2 \cdot 1 + 8 = 10 = 3$ v $\mathbb{Z}_7$

Lze M.F.V. kobercit pro $n \neq p^z$?
prvočíslo

potřebujeme Eulerova fci $\varphi : \mathbb{N} \to \mathbb{N}$:

$\varphi(n)$ = počet přirozených čísel $< n$ nesoudělných s n
(od 0 do $n-1$)

např.: $\varphi(6)$ $0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5} \to \varphi(6) = 2$

vzorce: $\varphi(p)$ $0, 1, \dots (p-1) \to \varphi(p) = p-1$

$\varphi(p^k)$ $0, 1, \dots \frac{1}{p} \dots \frac{2}{p} \dots p^{k-1} \cdot \frac{1}{p} \to p^k$

E. fce pro prvočíslo

E. fce pro prvočíslo na „k"

vyškrtám všechny násobky p těch je p^{k-1}

$\to \varphi(p^k) = p^k - p^{k-1}$

Když je n, m nesoudělná, pak
$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$
(z čínské věty o zbytcích)

Důsledek: Znám-li prvočíselný rozklad pro n

$n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$

mocniny různých prvočísel jsou nesoudělné

lak umím spočítat $\varphi(n) = \prod \varphi(p_i^{k_i})$

PŘ $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (4-2)(25-5) = \underline{40}$

Pozn.: $\varphi(n)$ = počet invertibilních prvků v $\mathbb{Z}_n$

v $\mathbb{Z}_{100}$ má 40 prvků inverzi

$(a \neq 2.k \quad \underset{\text{ani}}{\wedge} \quad a \neq 5.k)$

Euler - Fermatova věta

Pro každé a nesoudělné s n je $a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$

M. F. V - pro $n = p$ $a^{\varphi(n)} = a^{p-1} \equiv 1$ v $\mathbb{Z}_p$

ANEB:

při umocňování v $\mathbb{Z}_n$ nebo v exponentu počítat mod $\varphi(n)$, ALE jen pro základ nesoudělný s n!

(PŘ) Kolik vyjde 41^{64} v $\mathbb{Z}_{18}$

$41^{64} = (41 - 2.18)^{64} = 5^{64}$ v $\mathbb{Z}_{18}$

Ověřím $GCD(5, 18) = 1 \longrightarrow$ 5 a 18 jsou nesoudělné

$\longrightarrow$ lze použít E.-F. V

$\varphi(n) = \varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot (9-3) = 6$

$\xrightarrow{\text{E.-F. V}} \quad 5^6 = 1$ v $\mathbb{Z}_{18}$

$5^{64} = (5^6)^{10} \cdot 5^4 = 1 \cdot 5^4 = 1 \cdot 25^2 = 7^2 = 49 = 13$ v $\mathbb{Z}_{18}$

PŘ v $\mathbb{Z}_{14}$ spočtěte $x = 5 \cdot 3^{21} + 4^{21}$

$GCD(3,14) = 1 \rightarrow$ lze použít E.-F.V.

~~$3^{\varphi(14)} = \varphi(2 \cdot 7$~~

$3^{\varphi(14)} = 1$ v $\mathbb{Z}_{14}$

~~$\varphi(14) = \varphi(2 \cdot 14$~~

$\varphi(14) = \varphi(2 \cdot 7) = 1 \cdot 6 = 6$

$3^6 = 1$

tedy $3^{21} = 3^{6 \cdot 3 + 3} = 3^3 = 27 = (-1)$

$GCD(4,14) = 2 \rightarrow$ nesoudělné $\rightarrow$ nelze E.-F.V.

? $\rightarrow$ použije se

ALGORITMUS OPAKOVANÝCH ČTVERCŮ

v $\mathbb{Z}_{14}$ $= 4^{21} = (4^{10})^2 \cdot 4 = ((4^5)^2)^2 \cdot 4 = (((((4^2)^2) \cdot 4)^2)^2) \cdot 4$

a^b v $\mathbb{Z}_n$ $\Rightarrow$ umocňuje na druhou, resp. násobím základem v $\mathbb{Z}_{14}$ - pořadí určuje binární rozvoj exponentu

- do mezer S (= square)
- kde je 1, tam X (= times a)

časová náročnost je dána - $\log_2 b$

prostorová - " - - n^2

$\rightarrow$ lze použít vždy, když nelze E.-F.V

- a soudělné s n
- $b < \varphi(n)$

PŘ - pokrač.

$b = 21 = 16 + 4 + 1$

binárně $(21)_2 = 1\ 0\ 1\ 0\ 1$

↑ ↑ ↑ ↑ ↑

S x S S x S S x

1

v $\mathbb{Z}_{14}$ x 4

S $4^2 = 16 = 2$

S $2^2 = 4$

x $4 \cdot 4 = 16 = 2$

S $2^2 = 4^2$

S $4^2 = 16 = 2$

x $2 \cdot 4 = 8 = 4^{21}$

$x = 5 \cdot 3^{21} + 4^{21} = 5 \cdot (-1) + 8 = \underline{3}$ v $\mathbb{Z}_{14}$

Pozn: 2. metoda pro hledání A^{-1} v $\mathbb{Z}_n$

1. metoda = je-li a nesoudělné s n (tehdy existuje A^{-1} v $\mathbb{Z}_n$)

tak $a^{\varphi(n)-1}$ v $\mathbb{Z}_n$ (opakují se čtverce)

DK E.-F. $GCD(a, n) = 1 \rightarrow a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$

$a \cdot \underbrace{a^{\varphi(n)-1}}_{A^{-1}} = 1$

PŘ k minulé hodině 19^{-1} v $\mathbb{Z}_{26}$

$[19^{-1} = 19^{\varphi(26)-1} = 19^{11} = \ldots\ldots 11]$

Zde potřebuji znát prvočíselný rozklad n pro výp. $\varphi(n)$.