3 Počítání v $\mathbb{Z}$ a v $\mathbb{Z}_n$

1. Pomocí Eukleidova algoritmu najděte největší společný dělitel čísel 754 a 466.
2. V $\mathbb{Z}_{143}$ najděte všechna x, pro která platí $104x = 39$.
3. Spočtěte zbytek při dělení čísla $(49^{107} + 46 \cdot 6^{22})$ číslem 40.
4. V $\mathbb{Z}_{11}$ spočtěte 21754^{1213}.
5. Spočtěte dvěma různými způsoby 11^{-1} v $\mathbb{Z}_{216}$.

► Počítejte algoritmicky, výsledky nehádejte.

(3.1) GCD → použít Eukleidův algoritmus

např. GCD(150, 54)

$150 = 2 \cdot 54 + 42$

$54 = 1 \cdot 42 + 12$

$42 = 3 \cdot 12 + \boxed{6}$ → GCD

$12 = 2 \cdot 6 + 0$

nesoudělná čísla GCD = 1 (resp. prvočíslo

tzn. $p \geq 2$, kde $1 | p$ a $p | p$)

soudělná čísla GCD není prvočíslo

(3.2) jde o diofantickou rovnici

1) převést do $\mathbb{Z}$ (např. $10x = 39$ v $\mathbb{Z}_{143} \Rightarrow 104x + 143y = 39$ v $\mathbb{Z}$)

2) využít GCD(n, a) a rozšířený Eukleid. alg.

GCD(150, 54)
n a

$150 = 2 \cdot 54 + 42$ $\quad 42 = 150 - 2 \cdot 54 = n - 2a$

$54 = 1 \cdot 42 + 12$ $\quad 12 = 54 - 1 \cdot 42 = a - (n - 2a) = 3a - n$

$42 = 3 \cdot 12 + \boxed{6}$ $\quad 6 = 42 - 3 \cdot 12 = n - 2a - 3(3a - n) = 4n - 11a$

$12 = 2 \cdot 6 + 0$ → GCD

GCD by mělo být prvočíslo

3) partikulární řešení rovnice → pomocí GCD vyjádřit P stranu rovnice a upravit na tvar $xa + yb = k.GCD$

$(x_p, y_p) = x_p a + y_p b$

4) homogenní řešení rovnice → P strana = 0

rovnice v $\mathbb{Z}$ / : GCD např. $104x + 143y = 0$ / : GCD

$(x_0, y_0) = x_0 x + y_0 y$

5) všechna řešení v $\mathbb{Z}$

$(x, y) = (x_p, y_p) + (x_0, y_0).k \quad , k \in \mathbb{Z}$

6) všechna řešení v $\mathbb{Z}_n$ $x = x_p + x_0.k$

~~$x = (x_p + x_0) \quad y = (y_p, y_0)$~~

$x \in \{k_0, k_1 \dots k_{GCD-1}\}$

$x \in \{k_0$ dosadit a vypočítat, event. modulo $\mathbb{Z}_n\}$

$\vdots$

$x \in \{k_{GCD-1} \dots \}$

(3.3) 1) $\mathbb{Z}_n = 40$

2) rozklad čísel tak, aby šlo udělat mod $\mathbb{Z}_{40}$

3) GCD (40, a) a GCD (40, b)

4) GCD = 1 → nesoudělná čísla

≠ 1 → soudělná čísla

NESOUDĚLNÁ ČÍSLA (např. 40, a)

1) použít Euler-Fermatova věta

Efa pro 40 → $\varphi(40) = \varphi(2^3 . 5) = \varphi(2^3) . \varphi(5)$

2) aplikovat vzorce pro $\varphi(5)$ $\varphi(p) = p - 1$

$\varphi(2^3)$ $\varphi(p^k) = p^k - p^{k-1}$

$\varphi(40) = (5-1) . (2^3 - 2^2) = 4 . 4 = 16$

→ GCD (40, a) = 1 → $a^{16} = 1$ v $\mathbb{Z}_{40}$

3) upravit exponent a rozkladem
např. $q^{107} \rightarrow 107 = 6.16 + 11$
$\rightarrow (q^6)^{16} . q^{11}$ v Z_{40}

4) použít výsledek E-F.V a upravit,
tzn. $a^{16} = q^{16} \rightarrow 1^6 . q^{11} = q^{11}$ v Z_{40}

5) dosadit do původní rovnice (resp. do verze mod Z_{40})

6) použít metodu OPAKOVANÝCH ČTVERCŮ
- pro další ~~úpravu~~ redukci exponentu
- bude a je soudělné s n a nejde použít E-F.V

např. $q^{11} \rightarrow$ 11 binárně 1 0 1 1
X S SXSX a = q

1
$x = 1 . q = q$
$S = q^2 = 81 \bmod 40 = 1$ v Z_{40}
$S = 1^2 = 1$
$x = 1 . q = q$
$S = q^2 = 81 \bmod 40 = 1$
$x = 1 . q = q$ $\Rightarrow q^{11} = q$ v Z_{40}

7) ~~dosadit~~ mělo by se dosáhnout kompletního odebrání exponentu

8) dosadit do původní rovnice a vypočítat výsledek

(3.4) 1) upravit základ, tj. rozložit ~~na mod~~ a zkrátit mod n.

2) redukce exponentu
- GCD (n, a) a zjistit soudělnost/nesoudělnost.

NESOUDĚLNÁ' č. – použít malou F.V
~~$a^{p-1} = 1 \pmod p$~~ $(p = n)$

1) zjistím, jaké $a^p = 1$

2) provedu rozklad původního čísla ze zadání tak, abych mohla aplikovat $a^r = 1$

např. $3^6 = 1 \rightarrow 3^{21} = 3^{6 \cdot 3 + 3} = (3^6)^3 \cdot 3^3 = 1^3 \cdot 3^3$

3) zredukuji a vypočtu

(3.5) 1) platí $a \cdot a^{-1} = 1$

1. ZPŮSOB – Bezoutova věta

- GCD větou rozšířeného Eukleida

např. $GCD(216, 11)$ v $\mathbb{Z}_{216}$

$GCD = 1 \longrightarrow 1 = 59a - 3n$

lze vypustit protože je násobek n

$1 = 59a \rightarrow a^{-1} = 59$

2. ZPŮSOB – algoritmus opakovaných čtverců

- GCD – pokud GCD = 1, pak
- E-F.V platí $\rightarrow a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$,
- aplikovat E-F.V a upravit zadání
- výpočet E. fce – viz (3.3)
- dosadit zpět do zadání a upravit
- na exponent použít algoritmus opak. čtverců
- dopočítat