Kamil Zarebný

(3.1) Pomocí Euklidova algoritmu najděte největší společný dělitel čísel 754 a 466.

$754 = 1 \cdot 466 + 288$

$466 = 1 \cdot 288 + 178$

$288 = 1 \cdot 178 + 110$

$178 = 1 \cdot 110 + 68$

$110 = 1 \cdot 68 + 42$

$68 = 1 \cdot 42 + 26$

$42 = 1 \cdot 26 + 16$

$26 = 1 \cdot 16 + 10$

$16 = 1 \cdot 10 + 6$

$10 = 1 \cdot 6 + 4$

$6 = 1 \cdot 4 + 2$

$4 = 2 \cdot 2 + 0$

Odtud, $\gcd(754, 466) = 2$

Kamil Dvořák

(3.2) V $\mathbb{Z}_{143}$ najděte všechna x, pro která platí $104x = 39$.

Problém převedeme na řešení rovnice v $\mathbb{Z}$. Budeme řešit rovnici

$$104x + 143y = 39 \quad \text{v } \mathbb{Z}$$

a) nalezneme partikulární řešení pomocí rozšířeného Eukleidova algoritmu.

$\gcd(143, 104)$

$143 = a \quad 104 = b$

$143 = 1 \cdot 104 + 39 \qquad 39 = 143 - 1 \cdot 104 = a - b$

$104 = 2 \cdot 39 + 26 \qquad 26 = 104 - 2 \cdot 39 = b - 2(a-b) = -2a + 3b$

$39 = 1 \cdot 26 + 13 \qquad 13 = 39 - 26 = a - b + 2a - 3b = 3a - 4b$

$26 = 2 \cdot 13 + 0$

$$39 = 3 \cdot 13 = 3 \cdot (3a - 4b) = 9a - 12b = 9 \cdot (143) - 12(104)$$

Partikulární řešení jsme vypočítali ve tvaru $(-12, 9)$

b) nalezneme nesoudělné řešení homogenní rovnice

$$104x + 143y = 0 \quad / : GCD = 13$$

$$8x + 11y = 0$$

$$(x_0, y_0) = (-11, 8)$$

c)

Všechna řešení v $\mathbb{Z}$

$(x, y) = (-12, 9) + k \cdot (-11, 8)$, kde $k \in \mathbb{Z}$

(3.2) pokračování

d) Všechna řešení v $\mathbb{Z}_{143}$

- zajímají nás pouze kladný x

$x = -12 - 11k \quad k \in \mathbb{Z}$

stačí nám spočítat pouze pro $k = 0, 1 \dots, 12$, potom se kladný začnou opakovat (viz $\gcd(143, 104) = 13$)

$x \in \{131, 120, 109, 98, 87, 76, 65, 54, 43, 32, 21, 10, 143\}$

Kamil Zavřel

(3.3) Spočítejte zbytek při dělení čísla $(49^{107} + 46 \cdot 6^{22})$ číslem 40.

Budeme počítat v $\mathbb{Z}_{40}$.

$$(49^{107} + 46 \cdot 6^{22}) = ((40+9)^{107} + (40+6) \cdot 6^{22}) = (9^{107} + 6^{23})$$

$\gcd(40, 9)$

$40 = 3 \cdot 9 + 4$

$9 = 2 \cdot 4 + 1$

$4 = 4 \cdot 1 + 0$

$\gcd(40, 6)$

$40 = 6 \cdot 6 + 4$

$6 = 1 \cdot 4 + 2$

$4 = 2 \cdot 2 + 0$

9^{107} musíme upravit podle Euler-Fermatovy věty.

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

platí tedy $9^{16} \equiv 1 \pmod{40}$

$$(9^{107} + 6^{23}) = ((9^{16})^6 \cdot 9^{11} + 6^{22}) = (9^{11} + 6^{23})$$

Zbytek dopočítáme pomocí algoritmu opakovaných čtverců.

a) 9^{11} v $\mathbb{Z}_{40}$

$(11)_2 = 1011$ $\quad \times \; S \; S \times S \times$

$\times \; 1 \cdot 9 = 9$

$S \; 9^2 = 81 = 1$

$S \; 1^2 = 1$

$\times \; 1 \cdot 9 = 9$

$S \; 9^2 = 81 = 1$

$\times \; 1 \cdot 9 = 9$

$9^{11} = 9$ v $\mathbb{Z}_{40}$

(3.3) mocnování

b) 6^{23} v $\mathbb{Z}_{40}$

23 : 2 = 11 1

11 : 2 = 5 1

5 : 2 = 2 1

2 : 2 = 1 0

1 : 2 = 0 1

$(23)_2 = 10111$

1

$\times$ 1.6 = 6

$\downarrow$ $6^2 = 36$

$\downarrow$ $36^2 = 16$

$\times$ 16.6 = 16

$\downarrow$ $16^2 = 16$

$\times$ 16.6 = 16

$\downarrow$ $16^2 = 16$

$\times$ 16.6 = 16

Výsledek:

$(9^{107} + 6^{23}) = 9 + 16 = 25$ v $\mathbb{Z}_{40}$

Kamil Šarelbr

(3.4) V $\mathbb{Z}_{11}$ spočtěte 21754^{1213}.

$21754^{1213} = (1977 \cdot 11 + 7)^{1213} = 7^{1213}$

Malá Fermatova věta nám dává návod, jak upravit exponent.

Ověříme podmínky věty:

- 11 je prvočíslo
- $\gcd(11, 7)$

$11 = 1 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

$\gcd(11, 7) = 1$

podmínky jsou ověřeny, platí tedy $7^{10} = 1$ v $\mathbb{Z}_{11}$

$7^{1213} = 7^{1210} \cdot 7^3 = (7^{10})^{121} \cdot 7^3 = 343 = (31 \cdot 11) + 2 = 2$

Spočítali jsme $21754^{1213} = 2$ v $\mathbb{Z}_{11}$.

Kamil Dvořák

(3.5) Spočtěte dvěma různými způsoby 11^{-1} v $\mathbb{Z}_{216}$

1) * $\gcd(216, 11)$

$216 = 19 \cdot 11 + 7$ $\quad n = 216 \quad 11 = a$

$11 = 1 \cdot 7 + 4$ $\quad 7 = 216 - 19 \cdot 11 = n - 19a$

$7 = 1 \cdot 4 + 3$ $\quad 4 = 11 - 1 \cdot 7 = a - n + 19a = -n + 20a$

$4 = 1 \cdot 3 + 1$ $\quad 3 = 7 - 1 \cdot 4 = n - 19a + n - 20a = 2n - 39a$

$3 = 3 \cdot 1 + 0$ $\quad 1 = 4 - 1 \cdot 3 = -n + 20a - 2n + 39a = -3n + 59a$

$\gcd(216, 11) = 1$

$59 \cdot 11 - 3 \cdot 216 = 1$

$11^{-1} = 59$

2) * Euler-Fermatova věta platí

$$11^{\varphi(216)} = 1 \text{ v } \mathbb{Z}_{216}$$

Můžeme tedy psát

$$11^{-1} = 1 \cdot 11^{-1} = 11^{\varphi(216)} \cdot 11^{-1} = 11^{\varphi(216)-1}$$

$$\varphi(216) = \varphi(3^3 \cdot 2^3) = \varphi(3^3) \cdot \varphi(2^3) = (3^3 - 3^2) \cdot (2^3 - 2^2) = 18 \cdot 4 = 72$$

$$11^{\varphi(216)-1} = 11^{72-1} = 11^{71}$$

Použijeme algoritmus opakovaných druhých

$71 : 2 = 35$ $\quad 1$

$35 : 2 = 17$ $\quad 1$

$17 : 2 = 8$ $\quad 1$

$8 : 2 = 4$ $\quad 0$

$4 : 2 = 2$ $\quad 0$

$2 : 2 = 1$ $\quad 0$

$1 : 2 = 0$ $\quad 1$

$(71)_2 = 1000111$

(3.5) pokračování

$\times\ 1 \cdot 11 = 11$

$\int 11^2 = 121$

$\int 121^2 = 14641 = 169$

$\int 169^2 = 28561 = 49$

$\int 49^2 = 2401 = 25$

$\times\ 25 \cdot 11 = 59$

$\int 59^2 = 3481 = 25$

$\times\ 25 \cdot 11 = 59$

$\int 59^2 = 25$

$\times\ 25 \cdot 11 = 59$

$11^{-1} = 59$