AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

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.

Počet stran: 1 + 8

Datum: 4. dubna 2011

Podpis: jandora

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(3) POČÍTÁNÍ V $\mathbb{Z}$ a v $\mathbb{Z}_n$

(3.1.) Pomocí Eukleidova algoritmu najděte největší společný dělitel čísel 454 a 466.

$a = 454$
$b = 466$
hledám $GCD(454, 466)$

$454 = 1 \cdot 466 + 288$

$466 = 1 \cdot 288 + 178$

$288 = 1 \cdot 178 + 110$

$178 = 1 \cdot 110 + 68$

$110 = 1 \cdot 68 + 42$

$68 = 1 \cdot 42 + 26$

$42 = 1 \cdot 26 + 16$

$26 = 1 \cdot 16 + 10$

$16 = 1 \cdot 10 + 6$

$10 = 1 \cdot 6 + 4$

$6 = 1 \cdot 4 + 2$

$4 = 2 \cdot 2 + 0$

$GCD(454, 466)$ je 2.

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(2)

(3.2) V $\mathbb{Z}_{143}$ najděte všechna x, pro která platí $10x = 39$.

Půjde o výpočet Diofantické rovnice.
Nejprve si rovnici převedu do $\mathbb{Z}$

$$10x = 39 \quad \text{v } \mathbb{Z}_{143}$$
$$\hookrightarrow 104x + 143y = 39 \quad \text{v } \mathbb{Z}$$

Dále kjsklím $GCD(143, 104)$ $\quad 143 = n,\ 104 = a$

$143 = 104 \cdot 1 + 39 \rightarrow 39 = 143 - 104 = n - a$

$104 = 39 \cdot 2 + 26 \rightarrow 26 = 104 - 2 \cdot 39 = a - 2(n - a)$
$26 = 3a - 2n$

$39 = 26 \cdot 1 + \boxed{13} \rightarrow 13 = 39 - 26 = 3n - 4a$

$26 = 13 \cdot 2 + 0$ $\quad GCD$, 13 = prvočíslo

Nyní vyjádřím <u>parkikulární řešení</u>:

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

$$39 = 9n - 12a \rightarrow (x_n, y_n) = (-12, 9)$$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(3)

Homogenní rovnice - řešení:

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

$$8x + 11y = 0 \rightarrow (x_0, y_0) = (-11, 8)$$

Všechna řešení rovnice v $\mathbb{Z}$ jsou:

$$(x, y) = (-12, 9) + k(-11, 8)$$

Všechna řešení rovnice v $\mathbb{Z}_{143}$ jsou:

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

$x \in \{k_0, k_1, k_2, \dots k_{12}\}$.

$x \in \{$

$k_0 = 131$ $\quad -12 - 11.0 = -12 + 143$

$k_1 = 120$ $\quad -12 - 11.1 = -23 + 143$

$k_2 = 109$ $\quad -12 - 11.2 = -34 + 143$

$k_3 = 98$

$k_4 = 87$

$k_5 = 76$

$k_6 = 65$

$k_7 = 54$

$k_8 = 43$

$k_9 = 32$

$k_{10} = 21$

$k_{11} = 10$

$k_{12} = 142\}$ $\quad -12 - 11.12 = -144 + 143 =$

$= -1 + 143 = 142$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(4)

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

$$(49^{107} + 46 \cdot 6^{22}) = 40 + 9^{107} + (40+6) \cdot 6^{22} \quad \curvearrowright \mathbb{Z}_{40}$$
$$= 9^{107} + 6 \cdot 6^{22} \quad \text{“}$$
$$= 9^{107} + 6^{23} \quad \text{“}$$

$GCD(40, 9) \rightarrow 40 = 9 \cdot 4 + 4$
$9 = 4 \cdot 2 + \boxed{1} \longrightarrow GCD = 1$
$4 = 1 \cdot 4 + 0$

40 a 9 jsou nesoudělná

$GCD(40, 6) \rightarrow 40 = 6 \cdot 6 + 4$
$6 = 4 \cdot 1 + \boxed{2} \longrightarrow GCD = 2$
$4 = 2 \cdot 2 + 0$

40 a 6 jsou soudělná

40 a 9 jsou nesoudělná → lze použít E.F.V
E. fce pro 40 → $\varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5)$
použiji vzorce $\varphi(p) = p - 1$ pro $\varphi(5)$
$\varphi(p^k) = p^k - p^{k-1}$ pro $\varphi(2^3)$

$\varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$
$\varphi(5) = 5 - 1 = 4$
$\varphi(40) = 4 \cdot 4 = \underline{16}$

~~dosadíme $9^{107} = 9^{16}$ $\curvearrowright \mathbb{Z}_{40}$~~

dle E.F.V.
$GCD(40, 9) = 1 \rightarrow 9^{16} = 1 \curvearrowright \mathbb{Z}_{40}$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(5)

$107 = 6 \cdot 16 + 11$

$q^{107} = (q^6)^{16} \cdot q^{11} \quad v\ Z_{40}$

$= (q^{16})^6 \cdot q^{11} = 1^6 \cdot q^{11} = \underline{q^{11} \quad v\ Z_{40}}$

dosadím zpět do příkladu

$q^{107} + 6^{23} = q^{11} + 6^{23} \quad v\ Z_{40}$

pro další výpočet použiji metodu opakovaných čtverců

$q^{11} \Rightarrow$ 11 binárně = 1 0 1 1

x s s x s x $\quad a = 9$

1

$x = 1 \cdot 9 = 9$

$s = 9^2 = 81 \mod 40 = 1$

$s = 1^2 = 1$

$x = 1 \cdot 9 = 9$

$s = 9^2 = 81 \mod 40 = 1$

$x = 1 \cdot 9 = 9$

$\underline{q^{11} = 9 \quad v\ Z_{40}}$

$6^{23} \rightarrow$ 23 binárně = 1 0 1 1 1

x s s x s x s x $\quad a = 6$

1

$x = 1 \cdot 6 = 6$

$s = 6^2 = 36$

$s = 36^2 = 1296 \mod 40 = 16$

$x = 16 \cdot 6 = 96 \mod 40 = 16$

$s = 16^2 = 256 \quad " \quad = 16$

$x = 16 \cdot 6 = 96 \quad " \quad = 16$

$s = 16^2 = 256 \mod 40 = 16$

$x = 16 \cdot 6 = 96 \quad " \quad = 16$

$\underline{6^{23} = 16 \quad v\ Z_{40}}$

$(49^{107} + 46 \cdot 6^{22}) = 9 + 16 =$

$= 25 \quad v\ Z_{40}$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011 (6)

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

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

$21754 = 1977 \cdot 11 + 7 \longrightarrow 21754^{1213} = 7^{1213}$ v $\mathbb{Z}_{11}$

Nyní se pokusím „snížit" exponent.
Nejprve zjistím, zda jsou čísla 7 a 11 soudělná nebo nesoudělná. Toto zjistím pomocí GCD.

$GCD(11, 7)$

$11 = 7 \cdot 1 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + \boxed{1} \longrightarrow GCD = 1 \rightarrow$ čísla 11 a 7 jsou nesoudělná

$3 = 1 \cdot 3 + 0.$

Vzhledem k tomu, že 11 je prvočíslo, použiji F. V. $a^{p-1} = 1 \pmod p$

$7^{11-1} = 1 \pmod{11} \rightarrow 7^{10} = 1 \pmod{11}$

$7^{1213} = 7^{1210} \cdot 7^3 = (7^{10})^{121} \cdot 7^3 = 1 \cdot 7^3 = 7^3 \pmod{11}$

$7^3 \pmod{11} = 343 \pmod{11} = 341 + 2 \pmod{11}$

$\rightarrow \underline{7^3 = 2 \pmod{11}}$

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(7)

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

1. způsob

platí $A \cdot A^{-1} = 1$

Použiju pro výpočet Bezoutovu větu, ~~resp.~~ ~~důkaz~~

$GCD(216, 11)$ $\qquad 216 = n, \quad 11 = a$

$216 = 11 \cdot 19 + 7 \quad \rightarrow \quad 7 = 216 - 19a$

$\qquad 7 = n - 19a$

$11 = 7 \cdot 1 + 4 \quad \rightarrow \quad 4 = 11 - 7$

$\qquad 4 = a - (n - 19a) = 20a - n$

$7 = 4 \cdot 1 + 3 \quad \rightarrow \quad 3 = 7 - 4$

$\qquad 3 = n - 19a - (20a - n)$

$\qquad 3 = 2n - 39a$

$4 = 3 \cdot 1 + 1 \quad \rightarrow \quad 1 = 4 - 3$

$\qquad 1 = 20a - n - (2n - 39a)$

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

$3 = 1 \cdot 3 + 0$

$A \cdot A^{-1} = 1 = 59a - 3n = 59 \cdot 11 \rightarrow \underline{A = 59}$

$3n = 3 \cdot 216$ lze v $\mathbb{Z}_{216}$ z dalších výpočtů vypustit

11^{-1} v $\mathbb{Z}_{216} = 59$

AD7B01MCS - Matematika pro informatiky
Domácí úlohy pro kombinované studium 2010/2011

Zpracovala: **Radoslava Jandová, jandora1**

Obor: **STM, softwarové inženýrství**
Semestr: **4. semestr, léto 2010/2011**

(8)

2. způsob

Pro výpočet použiji algoritmus opakovaných čtverců.

$11^{-1} \pmod{Z_{216}} = 1 . 11^{-1} \pmod{Z_{216}}$

$GCD(216, 11) = 1$ - viz výpočet v 1. metodě

↓

dle E.F.V. platí, že $11^{\varphi(216)} = 1 \pmod{Z_{216}}$
pokud se GCD = 1

$\rightarrow 1 . 11^{-1} = 11^{\varphi(216)} . 11^{-1} = 11^{\varphi(216)-1} \pmod{Z_{216}}$

Výpočet E. funkce $\varphi(216)$

$\varphi(216) = 2^2 . 54 = 2^2 . 2 . 3 . 3^2 = 2^3 . 3^3$

$\varphi(216) = \varphi(2^3) . \varphi(3^3)$

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

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

$\varphi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$

$\varphi(216) = 4 . 18 = \underline{72}$

dosadím zpět $11^{\varphi(216)-1} = 11^{72-1} = 11^{71} \pmod{Z_{216}}$

71 vyjádřím binárně = 1 0 0 0 1 1 1 1
X S S S S X S X S X

$a = 11$

1

$x = 1 . 11 = 11$

$S = 11^2 = 121$

$S = 121^2 = 14.641 = 169 \pmod{Z_{216}}$

$S = 169^2 = 28\,561 = 49$ "-

$S = 49^2 = 2\,401 = 25$ "-

$x = 11 . 25 = 275 = 59$ "-

$S = 59^2 = 3\,481 = 25$ "-

$x = 11 . 25 = 275 = 59 \pmod{Z_{216}}$

$S = 59^2 = 3\,481 = 25$ "-

$x = 11 . 25 = 275 = \underline{59}$ "-

$11^{-1} \pmod{Z_{216}} = 59$