Zjistila jsem chybu, znovu předávám opravené.

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)

(4.2.) Spočtěte reziduálně AB a A^B v $\mathbb{Z}_{440}$
pro $A = 21754$
$B = 1213$

Pro výpočet použijí výpočty z příkladu 4.1.
Tím: $440 = 8.5.11 = 2^3.5.11$

$q_5 = \cancel{88}\ 176$
$q_8 = \cancel{330}\ 385$
$q_{11} = \cancel{280}\ 320$

AB a A^B budu počítat v $\mathbb{Z}_5$, $\mathbb{Z}_8$ a $\mathbb{Z}_{11}$.

(A.B)

v $\mathbb{Z}_5$ $A.B = 21754.1213 = 4.3 = 12 \mod 5 = \underline{2}$
v $\mathbb{Z}_8$ $A.B =$ —"— $= 2.5 = 10 \mod 8 = \underline{2}$
v $\mathbb{Z}_{11}$ $A.B =$ —"— $= 4.\pm 3 = \pm 21 \mod 11 = \cancel{1}\ \underline{10}$

v $\mathbb{Z}_{440}$ $A.B = 2.q_5 + 2.q_8 + 10.q_{11} =$
$= \cancel{288 + 2330 + 280} = 2.176 + 2.385 + 10.320$
$= \cancel{4166} \mod 440 = \cancel{336}\ 362$
4.322

(A^B)

v $\mathbb{Z}_5$ $A^B = 4^B = 4^{1213} \overset{E.F.V.}{=} 4^{4.303+1} = (4^4)^{303}.4^1 =$
$= 1^{303}.4 = \underline{4}$

$GCD(5,4)$ $5 = 4.1 + \boxed{1} \rightarrow GCD = 1$
$4 = 1.4 + 0$

$\Rightarrow$ lze použít E.F.V $\rightarrow 4^4 \equiv 1$ v $\mathbb{Z}_5$

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)

v $\mathbb{Z}_8$ $A^3 = 2^3 = 2^{1213}$
$= 0$ v $\mathbb{Z}_8$

GCD (8, 2) → čísla jsou soudělná, použij binární rozklad

1213 binárně = 1 0 0 1 0 1 1 1 1 0 1
X S S S X S S X S X S X S X S S X

$a = 2$

1

$x = 1 . 2 = 2$
$S = 2^2 = 4$
$S = 4^2 = 16 \mod 8 = 0$
$S = 0^2 = 0$
⋮ ⋮ ⋮ další výpočty nejsou nutné
$x = 0$

⟶ $2^{1213} = 0$ v $\mathbb{Z}_8$

v $\mathbb{Z}_{11}$ $A^3 = 4^3 = 4^{1213} \overset{\text{E.F.V}}{=} 4^{10 \cdot 121 + 3} = (4^{10})^{121} \cdot 4^3$
$= 1^{211} \cdot 343 = 343 \mod 11 = 2$

GCD (11, 7) $11 = 4 . 1 + 4$
$4 = 4 . 1 + 3$
$4 = 3 . 1 + 1$
$3 = 1 . 2 + 1$ → GCD = 1
$1 = 1 . 1 + 0$

→ $4^{10} \equiv 1$ v $\mathbb{Z}_{11}$

v $\mathbb{Z}_{440}$ $A^3 = 4q_5 + 0q_8 + 2q_{11} = 4 . 88 + 0 + 2 . 280$
$= 912 \mod 440 = 32$ 24
1.344