Vnitrosemestrální práce MB204 1.4.2014 A

1 (2,5b). Dokažte, že pro libovolné $n \in \mathbb{N}$ je číslo $2^{3^{4n+1}} + 3$ složené.

Řešení. Dokážeme $11 | 2^{3^{4n+1}} + 3$. Z Eulerovy (Fermatovy) věty je $2^{10} \equiv 1 \pmod{11}$ a protože $\varphi(10) = 4$ a $(3, 10) = 1$, platí také $3^4 \equiv 1 \pmod{10}$. Odtud $3^{4n+1} \equiv 3 \pmod{10}$ a $2^{3^{4n+1}} \equiv 2^3 = 8 \pmod{11}$. Celkem $2^{3^{4n+1}} + 3 \equiv 0 \pmod{11}$.

2 (2,5b). Mějme kongruenci $1480x \equiv 9135 \pmod{455}$. Pomocí kritéria udávajícího řešitelnost (a počet řešení) lineární kongruence určete počet řešení této kongruence a pak kongruenci vyřešte.

Řešení. Zjistíme $(1480, 455) = 5 | 9135$, a proto má kongruence pět řešení modulo 455. Ty jsou dané podmínkou $296x \equiv 1827 \pmod{91}$. Protože $91 = 7 \cdot 13$, dostáváme ekvivalentní soustavu $8x \equiv 0 \pmod{7}$, $10x \equiv 7 \pmod{13}$. Odtud $x = 7t$ a $t \equiv 4 \pmod{13}$, tj. $x \equiv 7 \cdot 4 = 28 \pmod{91}$. Pět řešení modulo 455 pak má tvar $x \equiv 28, 119, 210, 301, 392$.

3 (2,5b). Dokažte neexistenci primitivních kořenů modulo 28.

Řešení. Protože $\varphi(28) = \varphi(4)\varphi(7) = 12$, stačí testovat g^4 a g^6. Primitivní kořen musí být zejména nesoudělný s modulem. Také nemusíme testovat mocniny menších čísel (jejich řád dělí řád základu). A protože $15 \equiv -14, \cdots, 25 \equiv -3$ a počítáme jen sudé mocniny, stačí otestovat následující

g	3	5	11	13
g^2	9	-3	9	1
g^4	-3	9	-3	1
g^6	1	1	1	1

Řád všech nesoudělných čísel s 28 je tedy maximáklně 6, nikoli 12.

4 (2,5b). Mějme kongruenci $5x^{31} \equiv 9 \pmod{26}$. Pomocí kritéria udávajícího řešitelnost (a počet řešení) binomické kongruence určete počet řešení této kongruence a pak kongruenci vyřešte. Kolik existuje primitivních kořenů modulo 26?

Řešení. Je výhodné si kongruenci hned na začátku rozdělit na soustavu $x^{31} \equiv 1 \pmod{2}$, $5x^{31} \equiv 9 \pmod{13}$. První kongruence nám říká, že x je liché, zatímco druhá je ekvivalentní $x^{31} \equiv 7 \pmod{13}$. Protože $\varphi(13) = 12$, $(12, 31) = 1$ a $7^{12} \equiv (-3)^6 \equiv (-4)^3 \equiv 1 \pmod{13}$, má daná kongruence právě jedno řešení modulo 26. Primitivní kořen pro 13 je $g = 2$ a $7 \equiv 2^{11}$, a proto dostáváme $31x_a \equiv 11 \pmod{12}$. Této kongruenci vyhovuje právě $x_a \equiv 5 \pmod{12}$. Odtud $x \equiv 2^5 \equiv 6 \pmod{13}$. Navíc musí být liché, tj. $x \equiv 19 \pmod{26}$. Libovolný primitivní kořen g generuje celou redukovanou zbytkovou třídu. Proto každý jiný primitivní kořen můžeme napsat jako g^k pro vhodné k. Řád g je $\varphi(26) = 12$, a proto je řád g^k roven 12 (maximální) právě tehdy, když $(k, \varphi(26)) = 1$. Takových $k < 12$ je tedy právě $\varphi(\varphi(26)) = \varphi(12) = 4$ a stejný počet je primitivních kořenů.