Vnitrosemestrální práce MB204 1.4.2014 B

1 (2,5b). Dokažte, že pro libovolné $n \in \mathbb{N}$ je číslo $2^{2^{2n}} - 2$ dělitelné sedmi.

Řešení. Z Eulerovy (Fermatovy) věty je $2^6 \equiv 1 \pmod 7$, a protože $2^2 \equiv 1 \pmod 3$, je $2^{2n} \equiv 4 \pmod 6$. Odtud $2^{2^{2n}} \equiv 2^4 \equiv 2 \pmod 7$.

2 (2,5b). Mějme kongruenci $861x \equiv 10416 \pmod{264}$. Pomocí kritéria udávajícího řešitelnost (a počet řešení) lineární kongruence určete počet řešení této kongruence a pak kongruenci vyřešte.

Řešení. Zjistíme $(861, 264) = 3|10416$, a proto má kongruence tři řešení modulo 264. Ty jsou dané podmínkou $287x \equiv 3472 \pmod{88}$. Protože $88 = 8 \cdot 11$, dostáváme ekvivalentní soustavu $7x \equiv 0 \pmod 8$, $x \equiv 7 \pmod{11}$. Odtud $x = 8t$ a $t \equiv 5 \pmod{11}$, tj. $x \equiv 8 \cdot 5 = 40 \pmod{88}$. Tři řešení modulo 264 pak mají tvar $x \equiv 40, 128, 216$.

3 (2,5b). Dokažte neexistenci primitivních kořenů modulo 21.

Řešení. Protože $\varphi(21) = \varphi(3)\varphi(7) = 12$, 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 $11 \equiv -10, 16 \equiv -5, 19 \equiv -2$ a počítáme jen sudé mocniny, stačí otestovat následující

g	2	5	10
g^2	4	4	16
g^4	16	16	4
g^6	1	1	1

Řád všech nesoudělných čísel s 21 je tedy maximáklně 6, nikoli 12.

4 (2,5b). Mějme kongruenci $24x^{34} \equiv 34 \pmod{41}$. Pomocí kritéria udávajícího řešitelnost (a počet řešení) binomické kongruence určete počet řešení této kongruence a pak kongruenci vyřešte.

Řešení. Kongruenci upravíme na $x^{34} \equiv -2 \pmod{41}$. Protože $\varphi(41) = 40$, $(40, 34) = 2$ a $(-2)^{20} \equiv (-9)^4 \equiv (-1)^2 \equiv 1 \pmod{41}$, má daná kongruence právě dvě řešení modulo 41. Primitivní kořen pro 41 je $g = 6$ a $-2 \equiv 6^6$, a proto dostáváme $34x_a \equiv 6 \pmod{40}$, tj. $17x_a \equiv 3 \pmod{20}$, tj. $x_a \equiv -1 \pmod{20}$. Zadané kongruenci vyhovuje tedy vyhovují právě $x \equiv 6^{19} \equiv 34 \pmod{41}$ a $x \equiv 6^{39} \equiv 7 \pmod{41}$.