M6520 20. 12. 2017

Jméno: . . . .

Hodnocení						Sem.	$\sum$

Na každý příklad získáte nezáporný počet bodů.
Minimum (včetně semestrální písemky) je 30 bodů.
Na práci máte 90 minut.

1. (6krát ± 1 bod — správně 1 bod, chybně -1, bez odpovědi 0)
Odpovězte (škrtnutím nehodícího se **ano** nebo **ne** na patřičném řádku), zda jsou pravdivá následující tvrzení (čtěte **velmi** pozorně!):

(a) **ano — ne** Zobrazení $f : x \to x^3$ je bijekcí na libovolné redukované soustavě zbytků mod 28.

(b) **ano — ne** Pro každé přirozené číslo m je $(\varphi(m), m) = 1$.

(c) **ano — ne** Existuje nekonečně mnoho prvočísel tvaru $5k + 9$.

(d) **ano — ne** Existuje 2^7 primitivních kořenů modulo prvočíslo $p = 2^8 + 1$.

(e) **ano — ne** Pro důkaz řešitelnosti diofantické rovnice $f(x, y) = 0$, kde $f(x, y) \in \mathbb{Z}[x, y]$, stačí dokázat řešitelnost kongruencí $f(x, y) \equiv 0 \pmod m$ pro každé $m \in N$.

(f) **ano — ne** Libovolná polynomiální kongruence $f(x) \equiv 0 \pmod m$, kde $m \in \mathbb{N}$ a ne všechny koeficienty polynomu f jsou násobky m, má nejvýše $\mathrm{st}(f)$ řešení modulo m.

2. (6 bodů) Definujte pojmy *pseudoprvočíslo o základu a*, *Carmichaelovo číslo* a dokažte (bez použití Korseltova kritéria), že číslo 1105 je Carmichaelovo.

3. (6 bodů) Řešte rovnici $x^2 - y^2 = 12z - 2$ v oboru celých čísel.

4. (6 bodů) Určete nějaké řešení kongruence $x^5 + 10 \equiv 0 \pmod{121}$ a rozhodněte, kolik řešení má tato kongruence modulo 1331.

5. (10 bodů) Řešte kongruenci $7x^2 + 112x + 42 \equiv 0 \pmod{473}$.
(Nápověda: Modul není prvočíslo.)

6. (6 bodů) Buď p prvočíslo a g primitivní kořen modulo p. Dokažte, že řád čísla $g + p$ modulo p^2 je buď $p - 1$ nebo $p(p - 1)$.