M6520 12. 1. 2018

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** Mají-li celá čísla x, resp. y řád a, resp. b modulo $m \in \mathbb{N}$, pak má číslo $x \cdot y$ řád $a \cdot b$ modulo m.

(b) **ano** — **ne** Lineární kongruence $ax \equiv b \pmod{m}$, kde a, b, m jsou přirozená čísla, nemá více než a řešení modulo m.

(c) **ano** — **ne** Soustava kongruencí

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \end{aligned}$$

je řešitelná právě když $(m_1, m_2) \mid (b_1 - b_2)$.

(d) **ano** — **ne** Je-li číslo $n > 4$ složené, pak $n \mid (n-1)!$.

(e) **ano** — **ne** Jsou-li p, q lichá prvočísla taková, že platí $p \equiv 3 \pmod 4$ nebo $q \equiv 3 \pmod 4$, pak $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(f) **ano** — **ne** Při komunikaci prosřednictvím RSA si komunikující strany nejprve vymění dvojici velkých prvočísel.

2. (6 bodů) Určete, pro která prvočísla p je řešitelná kongruence

$$x^2 - 15 \equiv 0 \pmod{p}.$$

Vše řádně zdůvodněte.

3. (8 bodů) Učitel matematiky se zmínil, že dnes mají narozeniny obě jeho děti. Když se ho žáci zeptali na jejich věk, odpověděl hádankou: „Součet trojnásobku druhé mocniny dceřina věku a sedmináso bku součinu věků obou dětí je o 168 větší než šestinásobek druhé mocniny synova věku.“ Určete věk obou dětí (všechny možnosti).

4. (6 bodů) Řešte v $\mathbb{N}$ rovnici $\varphi(m) = \frac{m}{3}$.

5. (8 bodů) Řešte kongruenci $x^3 + 2x + 18 \equiv 0 \pmod{125}$.

6. (6 bodů) Řešte diofantickou rovnici: $286x + 104y + 39z = 26$.