

Hodnocení							$\Sigma$	

Jméno: .....

Na každý příklad získáte nezáporný počet bodů.

Minimum je 25 bodů.

Na práci máte 90 minut.

1. (10krát  $\pm 1$  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** Lineární diofantická rovnice  $ax = b$  má pro libovolná  $a, b \in \mathbb{Z}$  splňující  $a \mid b$  nekonečně mnoho řešení.
- (b) **ano** — **ne** Kongruence  $ax^2 \equiv b \pmod{m}$ , kde  $a, b, m \in \mathbb{N}$ , nemá řešení, pokud  $(a, m) \nmid b$ .
- (c) **ano** — **ne** Jsou-li  $p, q$  lichá prvočísla taková, že platí  $p \equiv 1 \pmod{4}$ , pak  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ .
- (d) **ano** — **ne** Primitivní kořeny neexistují modulo žádné složené číslo větší než 4.
- (e) **ano** — **ne** Číslo 5 je jediným řešením rovnice  $\varphi(m) = 4$ .
- (f) **ano** — **ne** Pro každé  $x \in \mathbb{R}$ ,  $n \in \mathbb{N}$  platí:  $[x + n] = [x] + n$ .
- (g) **ano** — **ne** Soustava kongruencí

$$a_1x \equiv b_1 \pmod{m_1}$$

$$a_2x \equiv b_2 \pmod{m_2}$$

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

- (h) **ano** — **ne** Pro Jacobiho symbol  $\left(\frac{a}{b}\right)$ , kde  $2 \nmid b$ , platí: je-li  $\left(\frac{a}{b}\right) = -1$ , pak kongruence  $x^2 \equiv a \pmod{b}$  není řešitelná.
- (i) **ano** — **ne** Polynomiální kongruence  $f(x) \equiv 0 \pmod{p}$ , kde  $p$  je prvočíslo, má nejvýše  $\text{st}(f)$  kořenů.
- (j) **ano** — **ne** Pro každé  $a, m \in \mathbb{N}$ ,  $(a, m) = 1$  je řád čísla  $a$  modulo  $m$  násobkem  $\varphi(m)$ .
2. (8 bodů) Rozhodněte, které z následujících kongruencí (resp. soustav kongruencí) jsou řešitelné.

(a)  $x \equiv 1 \pmod{3}$   
 $x \equiv -1 \pmod{9}$

(d)  $x^2 \equiv 3 \pmod{29}$   
 $x^2 \equiv 5 \pmod{47}$

(b)  $4x \equiv 1 \pmod{1234567891011}$

(e)  $x^2 \equiv 5 \pmod{29}$

(c)  $x \equiv 3 \pmod{29}$

$x^2 \equiv 3 \pmod{47}$

$x \equiv 5 \pmod{47}$

(f)  $x^{10} \equiv 7 \pmod{3^{10}}$

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 sedminásobku součinu věků obou dětí je o 16 větší než šestinásobek druhé mocniny synova věku.“ Určete věk obou dětí (všechny možnosti).
4. (8 bodů) Řešte rovnici  $\varphi(pm) = \varphi(qm)$  (pro neznámé  $m \in \mathbb{N}$  a prvočísla  $p, q$ )
5. (8 bodů) Určete, pro která prvočísla  $p$  je řešitelná kongruence

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

Je těch prvočísel, pro která je kongruence řešitelná, konečně nebo nekonečně mnoho? Zdůvodněte.

6. (8 bodů) Určete, pro která  $n \in \mathbb{N}$  platí  $6^n - 1 \mid 7^n - 1$ .