Algebra 2 26.5.2004

Jméno: .....

Na každý příklad získáte nezáporný počet bodů.
Na práci máte 90 minut.

Hodnocení						∑	

1. (10krát ±2 body — správně 2 body, chybně −2, bez odpovědi 0)
Odpovězte (škrtnutím nehodícího se **ano** nebo **ne** na patřičném řádku),
zda jsou pravdivá následující tvrzení (čtěte **velmi** pozorně!):

(a) **ano** — **ne** Kongruence $x^2 \equiv a \pmod{p}$, kde $a \in \mathbb{Z}$ a $p \in \mathbb{N}$ je prvočíslo, je řešitelná právě tehdy, když $\left(\frac{a}{p}\right) = 1$.

(b) **ano** — **ne** Je-li $f(x) \in \mathbb{Z}[x]$ polynom stupně n a $p \in \mathbb{N}$ je prvočíslo, pak má kongruence $f(x) \equiv 0 \pmod{p}$ nejvýše n řešení modulo p.

(c) **ano** — **ne** Pro každé reálné číslo x platí, že $[x]$ není větší než x.

(d) **ano** — **ne** Eulerova funkce φ je příkladem multiplikativní aritmetické funkce.

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

(f) **ano** — **ne** Libovolná binomická kongruence $x^n \equiv 1 \pmod{m}$ má řešení.

(g) **ano** — **ne** Primitivní kořeny neexistují modulo žádné složené číslo větší než 4.

(h) **ano** — **ne** Je-li m liché složené číslo, $a \in \mathbb{Z}$ takové, že $\left(\frac{a}{m}\right) = -1$, pak kongruence $x^2 \equiv a \pmod{m}$ nemá řešení.

(i) **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 $(m_1, m_2) \mid (b_1 - b_2)$.

(j) **ano** — **ne** Pro každé prvočíslo p a přirozené číslo α platí $\varphi(p^\alpha) = \varphi(2p^\alpha)$.

2. (10 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).

3. (15 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.

4. (10 bodů) Řešte rovnici $\varphi(pm) = \varphi(qm)$ (pro neznámé $m \in \mathbb{N}$ a prvočísla p, q)

5. (10 bodů) Nechť $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$ a $a \equiv b \pmod{m^n}$. Pak $a^m \equiv b^m \pmod{m^{n+1}}$. Dokažte.

6. (10 bodů) Řešte kongruenci $x^2 + x - 2 \equiv 0 \pmod{49}$.

7. (5 bodů) Zformulujte Bezoutovu větu a aplikujte ji na čísla 2003 a 572.