M6520 22. 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** Pro všechna přirozená čísla n platí $\varphi(2n) = \varphi(n)$.

(b) **ano** — **ne** Diofantická rovnice $x^n + y^n = z^n$ s neznámými $x, y, z \in \mathbb{N}$ nemá pro parametr $n \in \mathbb{N} \setminus \{1\}$ žádné řešení.

(c) **ano** — **ne** Relace dělitelnosti na množině celých čísel je antisymetrická.

(d) **ano** — **ne** Binomická kongruence $x^n \equiv a \pmod{p}$, kde $a, n \in \mathbb{N}$ a p je prvočíslo splňující $(n, p-1) = 1$, má jediné řešení modulo p.

(e) **ano** — **ne** Je-li celé číslo g primitivním kořenem modulo $m \in \mathbb{N}$, pak je primitivním kořenem také g^d pro libovolné $d \in \mathbb{N}$, pro které $(d, \phi(m)) = 1$.

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

2. (6 bodů) Určete, pro které hodnoty prvočíselného parametru p má rovnice

$$2x^2 - x - 36 = p^2$$

celočíselné řešení. Zdůvodněte a rovnici vyřešte.

3. (6 bodů) Rozhodněte, pro která přirozená čísla n platí $3^n \equiv n \pmod{13}$. Je čísel vyhovujících této kongruenci nekonečně mnoho?

4. (8 bodů) Určete počet řešení kongruence $3x^2 + 6x + 1 \equiv 0 \pmod{4673}$, víte-li, že 4673 je prvočíslo.

5. (8 bodů) Uvažte *speciální* prvočíslo $m = 2017$ a určete:

(a) inverzi c *kolumbovského* čísla 1492 modulo m, pro níž navíc $1 \le c \le m$,

(b) počet a součet dělitelů čísla c,

(c) všechna $n \in \mathbb{N}$ taková, že $\varphi(n) = m$,

(d) počet přirozených čísel menších než m, nesoudělných s 25.

6. (6 bodů)

(a) Dokažte, že má-li a řád r modulo m, má a^k modulo m řád $\frac{r}{(r,k)}$.

(b) S využitím předchozí části dokažte, že číslo a, které je kvadratickým zbytkem modulo prvočíslo p, nemůže být primitivním kořenem modulo p.

(c) S využitím předchozích částí dokažte, že je-li $a \in \mathbb{N}$ primitivní kořen modulo prvočíslo $p = 719$, pak musí být větší než 10.

Pozn: Využít výsledek předchozí části můžete i v případě, že jste ji nevyřešili.