M6520 6. 1. 2017

Jméno: ....

Hodnocení						Sem.	$\sum$

Na každý příklad získáte nezáporný počet bodů.

Minimum (včetně semestrální písemky a DÚ) 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** 5 je primitivní kořen modulo 31.

(b) **ano — ne** Libovolná redukovaná soustava zbytků modulo prvočíslo $p > 2$ obsahuje stejný počet kvadratických zbytků a nezbytků.

(c) **ano — ne** Zobrazení $f : x \to x^3$ je bijekcí na libovolné redukované soustavě zbytků modulo 31.

(d) **ano — ne** Číslo $(1111111111)_7$, zapsané v soustavě o základu 7, je dělitelné osmi.

(e) **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.

(f) **ano — ne** Platí-li $a \mid b$, $a \mid c$, pak $a^2 \mid bc$.

2. (6 bodů) Nechť p je prvočíslo. Dokažte (aniž byste se pouze odkázali na příslušnou větu) :

i) $(p-1)! \equiv -1 \pmod{p}$.

ii) Pro celé číslo $0 \le a \le p-1$ platí

$$\binom{p-1}{a} \equiv (-1)^a \pmod{p}.$$

3. (8 bodů) Řešte kongruenci $x^3 - x + 4 \equiv 0 \pmod{125}$.

4. (6 bodů) Alice chce zašifrovat zprávu pomocí RSA, vybere si $n = 17 \cdot 19 = 323$ a $e = 65$ jako svůj veřejný klíč. Proveďte výpočet Alicina soukromého klíče. Dále s využitím algoritmu modulárního umocňování vypočtěte, jak Bob zašifruje pro Alici zprávu "B" (zakódovanou do čísla 2). Uveďte též (již bez výpočtu), jak Alice tuto zprávu dešifruje.

5. (8 bodů)

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

(b) S využitím tvrzení předchozí části dokažte, že číslo a, které je kvadratickým zbytkem modulo prvočíslo $p \neq 2$, nemůže být primitivním kořenem modulo p.

(c) S využitím tvrzení předchozích částí dokažte, že je-li $a \in \mathbb{N}$ primitivní kořen modulo prvočíslo $p = 311$, pak musí být větší než 16.

Části b) i c) můžete řešit i bez vyřešených předchozích částí!

6. (6 bodů) Řešte diofantickou rovnici: $72x + 63y + 56z = 3$.