M6520 5. 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 libovolná $x, y \in \mathbb{N}$ existují $k, l \in \mathbb{N}$ tak, že $k \cdot x + l \cdot y = (x, y)$.

(b) **ano** — **ne** Je-li $m \in \mathbb{N}$, pak pro každé přirozené číslo d takové, že $d \mid \varphi(m)$ existuje $x \in \mathbb{Z}$ řádu d modulo m.

(c) **ano** — **ne** Pro všechna přirozená čísla $n > 1$ platí $\sum_{d|n} \mu(d) = 0$ (μ zde označuje Möbiovu funkci).

(d) **ano** — **ne** Je-li $2^n - 1$ prvočíslo, pak je i n prvočíslo.

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

(f) **ano** — **ne** Rovnost v Cauchyově nerovnosti $(x_1^2+x_2^2+x_3^2)(y_1^2+y_2^2+y_3^2) \geq (x_1y_1+x_2y_2+x_3y_3)^2$ nastává právě když $x_1 = y_1, x_2 = y_2, x_3 = y_3$.

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 $0 \leq a \leq p-1$ platí

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

(Poznámka: Obě části lze řešit nezávisle na sobě.)

3. (6 bodů) Jedenáct děvčat a n chlapců se vydalo na houby. Celkem nasbírali n^2+9n-2 hub, přitom každý z houbařů (i houbařek) našel stejný počet hub. Určete počet hub, který každý nasbíral.

4. (8 bodů) Určete nějaký primitivní kořen modulo 113. Dále určete všechna celá čísla $0 \leq a < 113$, pro něž platí

$$70^{92} + 1 \equiv a^{26} \pmod{113}.$$

5. (6 bodů) Řešte v oboru celých čísel rovnici

$$2x^2 + xy = y^2 + 63.$$

6. (4 body) 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.