Криптографија (Б и Ц)

Први колоквијум, 6.4.2015.

Укупно вријеме рада је **90** минута. **Нечитко исписани одговори и некомплетна рјешења се неће бодовати**. Срећно!

Задатак 1. (20 поена)

Нека је $d = \textbf{нзд}(a_1, a_2, \ldots, a_n)$. Тада је d најмањи позитивни елемент скупа

$$S = \{a_1t_1 + a_2t_2 + \cdots + a_nt_n \mid t_1, t_2, \ldots, t_n \in \mathbb{Z}\}.$$

Доказати.

Задатак 2. (20 поена)

Нека су a и b узастопни цијели бројеви и n природан број. Доказати да је $\textbf{нзд}(an + b, bn + a)$ непаран број.

Задатак 3. (15 поена)

Одредити све природне бројеве $n > 1$ за које је број $\dfrac{n(n+1)}{2} - 1$ прост.

Упуство: Трансформисати дати израз.

Задатак 4. (20 поена)

Доказати да за сваки прости број p и природан број k такав да $0 < k < p$, вриједи

$$p \mid \binom{p}{k}.$$

Упуство: Искористити чињеницу да је $\binom{p}{k} = s$, гдје је s природан број.

Задатак 5. (25 поена)

а. Користећи кинеску теорему о остацима, ријешити систем конгруенција

$$\begin{aligned} \mathrm{x} &\equiv 2^{91889} \pmod{119} \\ \mathrm{x} &\equiv 2^{2119} \pmod{19} \end{aligned}$$

б. Доказати да је m прост број ако и само ако је $\phi(m) = m - 1$, гдје је ϕ Ојлерова функција.