Криптографија (Ц)

Први колоквијум, 26.03.2013.

Максималан број бодова на испиту је 100. Укупно вријеме рада је **90** минута. **Нечитко исписани одговори и некомплетна рјешења се неће бодовати**. Срећно!

Задатак 1. (20 поена)

а. Ако је $\textbf{нзд}(a, b) = 1$ и ако $c \mid a + b$, доказати да је $\textbf{нзд}(a, c) = 1$ и $\textbf{нзд}(b, c) = 1$.

б. Наћи све просте бројеве p такве да је $17p + 1$ квадрат природног броја.

Задатак 2. (15 поена)

а. Ако је број 4 елемент групе $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$, подразумијевајући операцију множења по модулу 19, наћи $4^{-4} \pmod{19}$.

б. Наћи сва рјешења једначине $x^3 - x^2 + 2x - 2 \equiv 0 \pmod{11}$.

Задатак 3. (20 поена)

а. Доказати да сваки сложен број n има бар један прости дјелитељ мањи или једнак $\sqrt{n}$.

б. Ако је $\textbf{нзд}(a, b) = 1$ онда $\textbf{нзд}(2a + 3b, a + 2b) = 1$.

Задатак 4. (20 поена)

Нека су p, q различити прости бројеви такви да вриједи

$$2^p \equiv 2 \pmod{q} \text{ и } 2^q \equiv 2 \pmod{p}.$$

Доказати да је онда

$$2^{pq} \equiv 2 \pmod{pq}.$$

Напомена: Искористити дате чињенице у комбинацији са малом Фермаовом теоремом за бројеве 2 и p, односно за 2 и q.

Задатак 5. (25 поена)

Доказати да је Ојлерова ϕ функција мултипликативна, а потом да је и

$$g(n) = \sum_{d|n} \phi(d)$$

такође мултипликативна.

Име и презиме
