Криптографија (Б и Ц)

Први колоквијум, 8.4.2014.

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

Задатак 1. (15 поена)

Највећи заједнички дјелилац бројева a и b је минимални елемент скупа

$$\{ax + by \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Доказати.

Задатак 2. (15 поена)

Доказати да за сваки природан број n постоји природан број a тако да су

$$a, a+1, a+2, \ldots, a+(n-1),$$

сложени бројеви.

Задатак 3. (15 поена)

Доказати да не постоје цијели бројеви x и y тако да је

$$x^2 - 5y^2 = 2.$$

Задатак 4. (15 поена)

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

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

Задатак 5. (20 поена)

Доказати да за сваки прост број p вриједи

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

Да ли вриједи обрнуто тврђење, ако за неки природан број n вриједи

$$(n-1)! \equiv -1 \pmod{n},$$

онда је n прост?

Питања (20 поена)

- Шта представља $\phi(n)$ ако је ϕ Ојлерова функција?
- Шта значи тврђење да је Ојлерова функција мултипликативна? Формулисати Ојлерову теорему.
- Како функционише Виженерова енкрипција? У чему је предност овог система у односу на сусптитуциони алгоритам?
- Које су методе напада (криптоанализе) на Виженеров крипто-систем?
- Описати DES криптосистем, енкрипцију и декрипцију. Каква је сигурност DES-а? Објаснити.