Ime in priimek: _____ Vpisna št: | | | | | | | | |

# ALGEBRA IN DISKRETNA MATEMATIKA

## 2. KOLOKVIJ (naloge 1–4) / PRAKTIČNI IZPIT(naloge 2–5)

24. januar 2012

1. Alice si izbere praštevili $p = 11$ in $q = 13$ ter izračuna $n = pq$. Nato si izbere še $e = 7$. Par $(n, e)$ predstavlja njen javni ključ.

   (a) **[5]** Izračunaj $\varphi(n)$ in pokaži, da je Alicin javni ključ dober.

   (b) **[10]** Izračunaj Alicin zasebni ključ $d$.

   (c) **[5]** Bob želi Alice poslati sporočilo 71. Zakodiraj Bobovo sporočilo, tako da ga bo lahko prebrala samo Alice.

   (d) **[5]** Preveri, da Alice, ko odkodira Bobovo sporočilo, res prebere pravo sporočilo.

2. **[25]** Koliko permutacij besede SEMNAMORJU ne vsebuje *nobenega* od strnjenih podnizov SEM, NA, MORJU? (Nasvet: *Pomagaj si z načelom vključitev in izključitev. Bodi pozoren na podniz SEMORJU.*)

3. Na voljo imamo neomejeno število tlakovcev oblik I in L.


(a) **[15]** Naj $a_n$ označuje število možnih različnih tlakovanj pravokotnega hodnika velikosti $2 \times n$ s tlakovci oblik I in L. Izpelji rekurzivno enačbo za $a_n$.

(b) **[10]** Na koliko načinov lahko s tlakovci I in L tlakujemo hodnik velikosti $2 \times 10$?

4. Naj bo $G$ graf, ki ga dobimo iz Petersenovega grafa tako, da odstranimo eno vozlišče na zunanjem ciklu.

   (a) **[15]** Ali ima $G$ kakšno hamiltonovo pot? Kaj pa hamiltonov cikel?

   (b) **[10]** Določi kromatično število $\chi(G)$.

5. **[25]** Na množici $\mathbb{R} \times \mathbb{R}$ definiramo relacijo $\mathcal{R}$ s predpisom:

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow a^2 - d^2 = c^2 - b^2.$$

Pokaži, da je $\mathcal{R}$ ekvivalenčna relacija in določi ekvivalenčne razrede.

**Dodatni list.**

**TEORETIČNI IZPIT**

IME IN PRIIMEK: _____ VPISNA ŠT: | | | | | | | | |

1. Poišči dve interpretaciji spodnje izjavne formule; eno, pri kateri formula preide v pravilno izjavo in eno, pri kateri preide v nepravilno izjavo.

$$(\forall x)(\exists y)(P(y,x) \Rightarrow P(x,y))$$

2. Kako definiramo binomski koeficient

$$\binom{n}{k}?$$

Navedi rekurzivno zvezo, ki ji zadoščajo binomski koeficienti.

3. Kdaj pravimo, da je barvanje vozlišč grafa pravilno? Kaj je kromatično število grafa? Kaj pravi Brooksov izrek?