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

Vrsta: _____ Stolpec: _____

ALGEBRA IN DISKRETNA MATEMATIKA

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

18. januar 2011

1. **[25]** Alice si izbere praštevili $p = 7$ in $q = 23$ ter izračuna $n = pq$. Nato si izbere še $e = 5$. Par (n, e) predstavlja njen javni ključ. *Vse odgovorore dobro utemelji.*

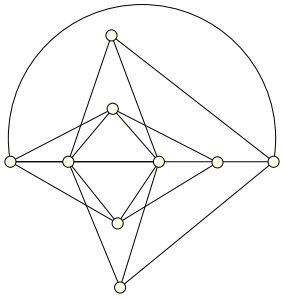
   (a) **[5]** Izračunaj $\varphi(n)$ in pokaži, da je Alicin javni ključ dober.

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

   (c) **[5]** Bob želi Alice poslati sporocilo 42. 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. Za graf na spodnji sliki ugotovi:



(a) **[5]** ali ima eulerjev sprehod oziroma obhod;

(b) **[5]** ali ima hamiltonovo pot oziroma cikel;

(c) **[10]** ali je ravninski;

(d) **[5]** kakšno je njegovo kromatično število.

3. Dani sta števili $\alpha = 2057$ in $\beta = 1445$.

   (a) **[5]** Števili α in β razstavi na produkt praštevil.

   (b) **[10]** Izračunaj $\gcd(\alpha, \beta)$ in $\operatorname{lcm}(\alpha, \beta)$.

   (c) **[5]** Naj bo $m = \alpha\beta$. Izračunaj $\varphi(m)$.

   (d) **[5]** Izračunaj $63^{2034561} \mod m$. (*Nasvet:* Uporabi Eulerjev izrek.)

4. **[25]** V neki anketi so n ljudi vprašali, kateri okus žvečilnih gumijev jim je všeč. Ugotovili so, da je dvaindvajsetim všeč okus po sadju, petindvajsetim okus po mentolu, devetintridesetim pa okus po grozdju. Nadalje, devetim sta všeč tako okus po mentolu kot okus po sadju, sedemnajstim sta všeč okus po sadju in okus po grozdju, dvajsetim pa sta všeč okus po mentolu in okus po grozdju. Šest oseb je odgovorilo, da so jim všeč vsi trije okusi, štiri osebe pa, da ne marajo nobenega od navedenih okusov. Koliko oseb so anketirali?

5. **[25]** Dokaži ali ovrži naslednji sklep:

$$p \Leftrightarrow q, \neg p, \neg(q \Rightarrow r) \vee t, s \vee t \Rightarrow r \models r \wedge \neg q.$$

TEORETIČNI IZPIT

1. Naj bodo $A_1, \ldots, A_k$ in B izjave, sestavljene iz atomarnih izjav $p_1, \ldots, p_m$. Kdaj pravimo, da je sklep

$$A_1, \ldots, A_k \vDash B$$

veljaven? Navedi zgled veljavnega sklepa in zgled neveljavnega sklepa.

2. Pojasni, zakaj je element $a \in \mathbb{Z}_n$ obrnljiv, če in samo če je tuj proti številu n.