Diszkrét matematika II. vizsga

minta feladatsor

Név:
Neptun kód:

	pontszám
Beugró	/15
Fogalmak	/27
Kvíz	/36
Bizonyítások	/22
Összesen	/100

A vizsga két részből, írásbeli és szóbeli, áll. A szóbeli részen való részvétel feltétele, hogy az 1. részből (Beugró) legalább 12 pontot **és** *összesen 40 pontot szerezzen. Az írásbeli részre 90 perc áll rendelkezésére.*

1. Beugró (5 × 3 pont, kérdéseken belül részpont nincs)

1. Definiálja a legnagyobb közös osztót! Mi lesz $(12, 18)$?
2. Definiálja a kongruencia relációt! Mondjon példát két különböző x egészre, mely teljesíti az $x \equiv 3 \mod 4$ relációt!
3. Mondja ki a Kinai maradéktételt! Megoldható-e az

$$\left.\begin{array}{ll} x \equiv 1 & \mod 2 \\ x \equiv 2 & \mod 3 \end{array}\right\}$$

   Ha igen, adja meg az összes megoldást, ha nem, indokoljon!
4. Definiálja az Euler-féle φ függvényt! Mi lesz $\varphi(6)$?
5. Mondja ki a polinom foka és gyökeinek száma közötti összefüggést! Hány gyöke lehet az $f = x^5 + x + 1 \in \mathbb{Q}[x]$ polinomnak?

2. Fogalmak (9 × 3 pont)

1. Definiálja a legnagyobb közös osztót egész számok körében!
2. Definiálja a lineáris diofanktikus egyenlet fogalmát egész számok körében!
3. Definiálja a kongruencia fogalmát egész számok körében!
4. Írja le a bővített eukildeszi algoritmust polinomok körében!
5. Mondja ki a kongruencia és az alapműveletek közötti összefüggésre vonatkozó tételt!
6. Mondja ki a Lagrange interpolációra vonatkozó tételt és írja le az interpolációt!
7. Definiálja a prefix kód fogalmát!
8. Mondja ki a Singleton-korlátot tetszőleges (nem feltétlen lináris) kódokra!
9. Definiálja a szisztematikus kódolás fogalmát!

3. Kvíz (9 kérdés, jó válasz 4 pont, rossz válasz -1 pont)

1. Legyenek p, q különböző prímszámok. Ekkor az Euler-féle φ függvény a következő tulajdonságot teljesíti

   a) $\varphi(p) + \varphi(q) = \varphi(p + q)$
   b) $\varphi(p) + \varphi(q) = \varphi(p \cdot q)$
   c) $\varphi(p) \cdot \varphi(q) = \varphi(p + q)$
   d) $\varphi(p) \cdot \varphi(q) = \varphi(p \cdot q)$

2. A $g = 3$ generátor modulo 17, és $\log_3 2 = 14$. Mennyi lesz $\log_3 12$

   a) 4
   b) 5
   c) 13
   d) 28

3. A Diffie-Hellman kulcscsere protokoll során az egyik részvevő (Alice) a következő adatokat küldi el publikus csatornán

   a) p prímszámot, g generátort modulo p és $g^a \bmod p$-t valamely a számra;
   b) egy k hosszú véletlen $0 - 1$ sorozatot;
   c) p és q prímek esetén a $p \cdot q$ szorzatot és az e titkosító exponenst, melyre $(a, \varphi(pq)) = 1$;
   d) a protokoll során Alice nem küld el publikus csatornán adatokat.

4. Legyen $f, g \in \mathbb{R}[x]$ két polinom. Ekkor

   a) $\deg f + \deg g = \deg(f + g)$
   b) $\deg f + \deg g = \deg(f \cdot g)$
   c) $\deg f \cdot \deg g = \deg(f + g)$
   d) $\deg f \cdot \deg g = \deg(f \cdot g)$

5. Legyen f és g két 100-ad fokú polinom. Nagyságrendileg hány maradékos osztással lehet f és g legnagyobb közös osztóját kiszámolni?

   a) 10
   b) 100
   c) 1 000
   d) 10 000

6. Hány olyan $f \in \mathbb{Z}_5[x]$ *4-ed fokú* polinom van, melyre $f(0) = 1$, $f(1) = 2$, $f(2) = 3$, $f(3) = 4$,

   a) 1
   b) 4
   c) 16
   d) 64.

7. Egy φ függvény kódolás, ha

   a) injektív
   b) ha a betűnkénti kódolás egyértelműen dekodólható
   c) ha a φ által indukált kódszavak prefixmentesek
   d) ha a φ által indukált kódszavak lineáris alteret alkotnak

8. Melyik állítás *nem* igaz

   a) minden vesszős kód felbontható
   b) minden egyenletes kód prefix kód
   c) minden vesszős kód egyenletes
   d) minden prefix kód felbontható.

9. Legyen $d(\mathbf{u}, \mathbf{v})$ a Hamming távolság. Melyik állítás igaz

   a) minden minden $\mathbf{u}$-hoz és $\varepsilon > 0$ értékhez létezik $\mathbf{v}$, hogy $d(\mathbf{u}, \mathbf{v}) < \varepsilon$;
   b) ha $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{u}, \mathbf{c}) + d(\mathbf{c}, \mathbf{v})$, akkor $\mathbf{u}, \mathbf{c}, \mathbf{v}$ egy egyenesen vannak;
   c) $d(\mathbf{u}, \mathbf{v}) = \sqrt{(u_1 - v_1)^2 + \cdots + (u_n - v_n)^2}$
   d) egyik sem a fentiek közül.

4. Tételek bizonyítása (22 pont)

(A tétel kimondásáért nem jár pont.)

1. Bizonyítsa be az Euler-Fermat tételt! (12 pont)

2. Bizonyítsa be, hogy a prefix kódok felbonthatóak! (10 pont)