Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik för F3 och F1spec (5B1203) onsdag den 18 augusti 2004 kl. 14.00-19.00.

Examinator: Anders Björner.

Hjälpmedel: Inga hjälpmedel är tillåtna.

Betygsgränser: 10 poäng ger betyget 3, 14 poäng ger betyget 4, 18 poäng ger betyget 5.

Obs: Alla lösningar och svar skall utförligt motiveras.

1. Antag att du som deltagare i ett system för RSA-kryptografi har offentliga nummer $n = 91$ och $e = 5$.

(a) Kryptera meddelandena 3 och 6. **(1 p)**

(b) Dekryptera de chiffrerade meddelandena 3 och 41. **(1 p)**

2. Grafen G har 87 noder, 80 kanter och precis en cykel. Hur många sammanhängande komponenter består G av? **(2 p)**

3. (a) Hur många tal större än 3552412 kan bildas genom permutation av siffrorna $1, 2, 2, 3, 4, 5, 5$? **(1 p)**
(Exempel: 5232451 är ett sådant tal.)

(b) Hur många strängar av 5 nollor och 10 ettor finns där inga nollor står direkt bredvid varandra? **(1 p)**
(Exempel: 110101110110110 är en sådan sträng.)

4. (a) Visa att ett polynom $a_0 + a_1x + \cdots + a_nx^n$ i $\mathbb{Z}_3[x]$ av grad $n \geq 1$ saknar förstagradsfaktorer om och endast om **(1 p)**

$$a_0 \neq 0, \qquad \sum_{i=0}^{n} a_i \neq 0, \qquad \sum_{i=0}^{n} (-1)^i a_i \neq 0.$$

(b) Bestäm alla irreducibla polynom i $\mathbb{Z}_3[x]$ av grad 2. **(1 p)**

5. Varje publicerad bok har en s.k. ISBN-kod (ISBN betyder "international standard book number"). ISBN-koden är en sträng $c_1c_2\ldots c_{10}$ av heltal, där $0 \leq c_i \leq 9$ för $1 \leq i \leq 9$ och $0 \leq c_{10} \leq 10$. Det sista talet i koden, c_{10}, är en checksiffra som beräknas enligt formeln **(3 p)**

$$c_{10} = \sum_{i=1}^{9} ic_i \qquad (\text{mod } 11) \qquad (*)$$

Visa att om två olika tal c_j och c_k i en ISBN-kod byter plats ($1 \leq j < k \leq 10$ och $c_j \neq c_k$), eller om ett tal c_j ändras ($1 \leq j \leq 10$), så gäller inte längre relationen $(*)$.

6. En leksakspyramid har kvadratisk bas och fyra lika stora triangulära sidor (dvs. alla fyra kanter mellan pyramidens bas och dess spets är lika långa). Pyramiden kan röra sig fritt i rummet. Vi har m färger till förfogande och vill färglägga pyramidens fem sidor så att varje sida är helt enfärgad. **(3 p)**

(a) Hur många distinkta sådana färgläggningar finns det?

(b) Hur många distinkta sådana färgläggningar finns det i vilka basens färg inte förekommer på någon triangulär sida?

7. Låt $\mathbb{F}_q$ vara en ändlig kropp med q element, och låt G vara mängden av avbildningar $f_{a,b} : \mathbb{F}_q \to \mathbb{F}_q$ av typen **(6 p)**

$$f_{a,b}(x) = ax + b,$$

för $a, b \in \mathbb{F}_q, a \neq 0$.

(a) Visa att varje sådan avbildning $f_{a,b}$ är en permutation.

(b) Visa att G är en grupp under komposition.

(c) Bestäm $|G|$.

(d) Visa att stabilisatordelgruppen G_c har ordning $q-1$ för alla $c \in \mathbb{F}_q$.

(e) Visa att stabilisatordelgruppen G_0 är cyklisk.

(f) Antag att $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ och $x_1 \neq y_1, x_2 \neq y_2$. Visa att det finns en avbildning $f_{a,b} \in G$ så att

$$f_{a,b}(x_1) = x_2, \qquad f_{a,b}(y_1) = y_2.$$

8. Visa följande gränser för Eulers φ-funktion:

(a) $\varphi(n) \leq n - \sqrt{n}$, för alla sammansatta tal n, **(2 p)**

(b) $\varphi(n) \geq \sqrt{n}$, för alla udda tal $n > 1$. **(2 p)**