Institutionen för matematik
KTH
B.Ek

Tentamen i 5B1204, DISKRET MATEMATIK för D
Fredagen den 7 mars 2003

Skrivtid: 14.00 – 19.00
Examinator: Bengt Ek, tel 7906951.
Inga hjälpmedel tillåtna, inte ens räknedosa.

Betygsgränser (preliminära): 25 poäng ger betyg 3, 33 poäng ger betyg 4 och 42 poäng ger betyg 5.
Slutbetyget på kursen bestäms av betyget på skrivningen och betyget på uppsatsen.

Teoridel

Den som vt 2003 blivit godkänd på lappskrivning nr i får automatiskt 4 poäng på uppgift nr i (i=1,2,3,4,5), och skall inte göra denna uppgift.
Ange på skrivningsomslaget vilka lappskrivningar du klarat.

1a) (1p) Ekvationen $a_{n+1} = 2a_n + 2n,\ n = 0, 1, \ldots$ har $a_n = -2n - 2$ som lösning (behöver inte visas). Bestäm den allmänna lösningen till ekvationen.
b) (1p) Vad menas med en **eulerväg** (eng. Eulerian walk) i grafen $G = (V, E)$?
c) (2p) Formulera **välordningsaxiomet** (eng. well-ordering axiom) för heltalen $\mathbb{Z}$ och förklara hur **induktionsprincipen** följer ur det.

2a) (1p) Vad menas med att funktionen $f : X \to Y$ är en **surjektion**?
b) (2p) Vad menas med att en permutation $\pi \in S_n$ är **jämn** eller **udda**? Är $\pi \in S_7$ som ges av att $\pi(1) = 6$, $\pi(2) = 3$, $\pi(3) = 7$, $\pi(4) = 5$, $\pi(5) = 4$, $\pi(6) = 1$, $\pi(7) = 2$ jämn eller udda?
c) (1p) Formulera **binomialsatsen** (eng. the binomial theorem) i fallet att exponenten är ett positivt heltal (dvs det fall som behandlats i kursen).

3a) (1p) På hur många sätt kan r st identiska kulor fördelas i n st olika lådor?
b) (2p) Vad menas med en **partition** av en mängd? Det finns ett nära samband mellan partitioner och **ekvivalensrelationer**. Vilket?
c) (1p) Hur definieras Eulers ϕ-funktion?

4a) (2p) Finns det något x så att $x \equiv_{18} 7$, $x \equiv_{49} 23$, $x \equiv_{55} 11$? Om det finns ett sådant x, hur fås **alla** sådana x med hjälp av det? (Även om ett sådant x skulle finnas, behöver du inte bestämma det.)
b) (1p) Formulera **Eulers sats** om vissa potenser av heltal $\pmod n$.
c) (1p) Vad menas med att en grupp är **cyklisk**?

5a) (1p) Formulera **Lagranges sats** om delgrupper till ändliga grupper.
b) (2p) Om en grupp G verkar på en mängd X, vad menas med **stabilisatorn** (eng. stabilizer) G_x och **banan** (eng. orbit) Gx för $x \in X$? Vad kan sägas om antalet element i G_x och Gx?
c) (1p) Vad säger satsen om **entydig faktorisering** av polynom?

Vänd!

Problemdel

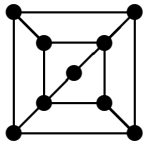
För att ge full poäng måste lösningarna vara ordentligt motiverade.

6a) (2p) En linjär, binär kod ges av kontrollmatrisen (eng. check matrix) $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. Orden $(011110), (110110), (110011)$ har mottagits. Vilka kodord har sänts, om högst ett fel har uppstått i varje ord?
b) (2p) Ett system för RSA-kryptering har den offentliga nyckeln $n = 299$, $e = 53$. Avkryptera meddelandet 55. $[299 = 13 \cdot 23]$.
c) (2p) Finn ett element av ordning 33 i U_{299}, de inverterbara elementen i $\mathbb{Z}_{299}$.

7a) (2p) Hur många olika ord kan man bilda genom att kasta om bokstäverna i ordet 'IRREDUCIBILITET'?
b) (2p) Hur många blir det om varken alla 'I' eller alla 'E' får stå tillsammans? [Svaren till a) och b) får innehålla fakulteter och de fyra räknesätten.]
c) (2p) Varje kant i grafen K_{17}, den fullständiga grafen (eng. complete graph) med 17 hörn, ges en av tre färger. Visa att det finns minst en enfärgad triangel.

8a) (2p) Låt p vara ett primtal och $n > 3$. Bestäm det största heltalet r så att $p^r \mid \binom{2n}{n}$ i de två fallen i) $\frac{2}{3}n \leq p \leq n$, ii) $n < p < 2n$.
b) (2p) Låt m, n vara naturliga tal med $d = \text{sgd}(m, n)$ (eng. $\gcd(m, n)$). Visa att $\phi(mn)\phi(d) = d\phi(m)\phi(n)$, där ϕ är Eulers ϕ-funktion.
c) (2p) Visa att om $5 \mid n$ finns inget x som uppfyller $x^6 + 3 \equiv 0 \pmod{n}$.

9a) (2p) Avgör (med motivering) i vart och ett av fallen i), ii) och iii) om det finns någon graf med åtta hörn med valenser:
i) $2, 3, 3, 3, 3, 3, 4, 5$, ii) $0, 1, 2, 3, 3, 5, 5, 6$, iii) $1, 1, 3, 3, 5, 5, 5, 7$.
(Liksom i kursboken betraktar vi bara grafer utan loopar och multipla kanter.)
b) (2p) Avgör om vidstående graf har någon Hamiltoncykel (ge exempel eller motivera varför ingen finns).
c) (2p) Hur många färger behövs för att kantfärga samma graf?



10a) (2p) Finn den största gemensamma delaren till polynomen $x^5 + 3x^3 + 3x^2 + 4$ och $x^4 + x^3 + 2x^2 + 4x + 1$ i $\mathbb{Z}_5[x]$.
b) (2p) Vilken är den största ordningen (som gruppelement) någon permutation i S_{13} har?
c) (2p) På en kvadratisk bricka med identisk över- och undersida färgas var och en av de fyra kanterna vit eller svart och vart och ett av de fyra hörnen grönt eller rött. Hur många verkligt olika brickor (dvs brickor som inte blir lika hur man än vrider dem i rummet) kan man få?

Lycka till!

Lösningar läggs ut på kurssidan efter skrivningens slut.
Där meddelas också när tentan och uppsatsen är rättade.