KTH Matematik
B.Ek

Tentamen i 5B1204, DISKRET MATEMATIK för D
Onsdagen den 9 mars 2005

Skrivtid: 8.00 – 13.00
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 2005 blivit godkänd på lappskrivning nr i får automatiskt 4 poäng på uppgift nr i (i=1,2,3,4,5), och skall inte göra den uppgiften.
Ange på skrivningsomslaget vilka lappskrivningar du klarat.

1a) (1p) Ange en linjär rekursionsekvation som har den allmänna lösningen $a_n = A \cdot 7^n + B \cdot (-2)^n$, där A, B är godtyckliga konstanter.
b) (1p) Vad menas med **valensen** (eng. degree) $\delta(v)$ för ett hörn v i en graf $G = (V, E)$?
c) (2p) Definiera vad som (i grafteorin) menas med ett **träd** (eng. tree).

2a) (1p) Vad menas med en **latinsk kvadrat** (eng. latin square)?
b) (1p) En **plan graf** har v hörn, e kanter och c komponenter. Den delar in planet i r ytor (inklusive ytan "utanför" grafen). Vilket samband råder mellan v, e, c, r?
c) (2p) Ange **Halls villkor** (eng. Hall's condition) för existens av en fullständig matchning i en bipartit graf. Är villkoret nödvändigt? Är det tillräckligt?

3a) (1p) Vad menas med att funktionen $f : X \to Y$ är en **bijektion**?
b) (1p) På hur många sätt kan r st identiska kulor fördelas i n st olika lådor?
c) (2p) Vad menas med att permutationen $\pi \in S_n$ är **jämn** respektive **udda** (eng. even, odd)? Är $\pi \in S_7$, given av att $\pi(1) = 4, \pi(2) = 7, \pi(3) = 6, \pi(4) = 2, \pi(5) = 5, \pi(6) = 3, \pi(7) = 1$, jämn eller udda?

4a) (1p) Hur definieras Eulers ϕ-funktion?
b) (1p) Formulera **Fermats lilla sats** om vissa potenser $\pmod p$, p primtal.
c) (2p) Vad menas med att $r \in \mathbb{Z}_m$ är **inverterbart** (eng. invertible)? Ange ett nödvändigt och tillräckligt villkor för att r skall vara inverterbart.

5a) (1p) Gäller för alla m, n att $S_m \times S_n \approx S_{m+n}$? Motivera ditt svar! ($S_n$ är den symmetriska gruppen, '$\approx$' betecknar isomorfi.)
b) (1p) Gruppen G har ett element av ordning 15. Vilka av följande värden är möjliga för $|G|$, G:s ordning: 20, 27, 30, 35, 49, 105, 111?
c) (2p) Formulera och bevisa kortfattat **Lagranges sats** för ändliga grupper.

Vänd!

Problemdel

För att ge full poäng måste lösningarna vara ordentligt motiverade.

6a) (2p) Ett system för RSA-kryptering har den offentliga nyckeln $n = 703$, $e = 77$. Finn en motsvarande avkrypteringsnyckel $(703, d)$. $[703 = 19 \cdot 37]$.
b) (2p) En linjär, binär kod ges av kontrollmatrisen (eng. check matrix) $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$. Hur många ord finns det i koden? Vilket kodord har sänts, om (11010) mottagits och högst ett fel har uppstått?
c) (2p) Finn alla heltal x så att $x^2 \equiv x \pmod{703}$.

7a) (2p) Vid en tentamen med 10 uppgifter kan varje uppgift ge 0, 1 eller 2 poäng. Hur många olika poängfördelningar är möjliga?
b) (2p) Hur många av dessa har minst en uppgift vardera bedömd med 0, 1 och 2 poäng?
c) (2p) Hur många av dem har minst två uppgifter vardera bedömda med 0, 1, 2 poäng?
[Svaren får innehålla fakulteter, potenser och de fyra räknesätten.]

8a) (2p) Finn alla heltal x som uppfyller $x \equiv 1 \pmod{12}$, $x \equiv 6 \pmod{13}$.
b) (2p) Finn alla $n \in \mathbb{N}$ så att $\phi(n) = 10$. ϕ är här Eulers funktion.
c) (2p) Finn alla heltal $n > 0$ så att $1193^n \equiv 1 \pmod{861}$. $[861 = 3 \cdot 7 \cdot 41]$

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) $0, 1, 2, 3, 3, 4, 5, 6$, ii) $2, 3, 4, 4, 4, 5, 5, 6$, iii) $1, 1, 2, 3, 4, 5, 6, 6$.
b) (2p) Tio tentander har gjort en tentamen med tio uppgifter. Varje uppgift klarades av minst sex skrivande, Varje skrivande klarade minst fyra uppgifter. Visa att man kan fördela uppgifterna med en per tentand, så att var och en har klarat sin uppgift.
c) (2p) Låt $G = (V, E)$ vara en plan, sammanhängande, 3-reguljär graf med r_i st ytor med i kanter ($i = 3, 4, \dots$). Visa att

$$3r_3 + 2r_4 + r_5 - r_7 - 2r_8 - \cdots = \sum_{i=3}^{\infty} (6 - i) r_i = 12$$

(Liksom i kursboken betraktar vi bara grafer utan loopar och multipla kanter.)

10a) (2p) Bestäm kvot och rest (eng. quotient, remainder) vid division av $2x^5 + 2x^4 + x^2 + 2$ med $x^3 + 2x^2 + x + 2$ i $\mathbb{Z}_3[x]$.
b) (2p) Hur många $\pi \in S_8$ uppfyller $\pi^3 = id$, identitetspermutationen?
c) (2p) Av sex sugrör formas en käck prydnad i form av en tetraeder (med sugrören som kanter). På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider dem i rummet) kan det göras, om man har sugrör av k olika färger att tillgå?

Lycka till!

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