Matematik, KTH
B.Ek

Tentamen i kursen
(SF1630,) SF1631, DISKRET MATEMATIK för (F,) D
lördagen den 28 januari 2012, klockan 9.00–14.00

OBS! Detta är tentamen TEN1, för hela kursen.
Äldre som bara vill tentera första delen av kursen skall ha TENA.

Examinator: Bengt Ek, tel 7906951.
Tillåtna hjälpmedel: Inga, inte ens räknedosa.

Högsta möjliga poäng på skrivningen är 47p. Till den läggs bonus från lapp-skrivningar ht 2011, högst 10p.

Betygsgränser:

För betyg	A	B	C	D	E	
krävs	42	35	29	24	20	poäng (inklusive bonus)

16–19 poäng ger omdömet Fx, dvs rätt att delta i en komplettering för betyg E.

För att ge full poäng måste lösningarna vara ordentligt motiverade. Satser från kursen får (utom då annat sägs) användas utan bevis, om det klart anges vad de säger.

DEL I

1) (4p) Låt G vara en hamiltonsk graf, dvs en graf som har en hamiltoncykel. Visa att om man tar bort $k(= 1, 2, \dots)$ hörn (och alla vidhängande kanter) från G, får man en graf med högst k komponenter.

2) (4p) Finn alla x i $\mathbb{Z}_{246}$ som uppfyller

$$117x = 36 \quad (\text{i } \mathbb{Z}_{246}, \text{ förstås}).$$

3) (4p) 30 (identiska) bullar och 15 (identiska, men skilda från bullarna) tårtbitar skall fördelas bland 20 (särskiljbara) barn. På hur många sätt kan det ske om varje barn skall få minst en bulle och högst en tårtbit?
Svaret får innehålla heltal, fakulteter, potenser och de fyra vanliga räknesätten.

4) (4p) Låt $f_{a,b} : \mathbb{Z}_3 \to \mathbb{Z}_3$ vara definierad av $f_{a,b}(x) = ax + b$. Visa att $\{f_{a,b} \ ; \ a, b \in \mathbb{Z}_3,\ a \neq 0\}$, med operationen sammansättning av funktioner, är en grupp. Visa också att denna grupp är isomorf med S_3, gruppen av permutationer av tre element.

5) (4p) Visa att om p är ett primtal är $x^{p-1} - 1$ i $\mathbb{Z}_p[x]$ delbart med $x - a$ för alla $a \in \mathbb{Z}_p$, $a \neq 0$.

Vänd!

DEL II

6) (5p) Finn det minsta talet $e \geq 100$ sådant att $(1189, e)$ kan användas som krypteringsnyckel i ett RSA-system. Finn också ett tal d, så att $(1189, d)$ är en motsvarande dekrypteringsnyckel. $[1189 = 29 \cdot 41]$

7) Permutationen $\alpha \in S_9$ ges av

$$\alpha(1) = 3,\ \alpha(2) = 7,\ \alpha(3) = 1,\ \alpha(4) = 9,$$
$$\alpha(5) = 8,\ \alpha(6) = 5,\ \alpha(7) = 4,\ \alpha(8) = 6,\ \alpha(9) = 2.$$

a) (2p) Skriv α och α^{-1} på cykelform.
b) (3p) Finn ett $\sigma \in S_9$ så att $\sigma\alpha = \alpha^{-1}\sigma$.

8) (5p) Finn alla monadiska (dvs högstagradskoefficienten = 1) irreducibla polynom i $\mathbb{Z}_5[x]$ som är delare till både $p(x) = x^6 + 4x^5 + x^4 + x^3 + x^2 + 2x + 1$ och $q(x) = x^5 + 2x^4 + 3x^3 + x^2 + 4x + 3$.

DEL III

För full poäng på dessa uppgifter krävs särskilt väl strukturerade och presenterade lösningar.

9) (6p) Varje kant i K_{17}, den fullständiga (eng. complete) grafen med 17 hörn, ges en av tre färger. Visa att det finns en enfärgad triangel, dvs tre hörn vars tre inbördes kanter alla har samma färg.

10a) (3p) Låt p vara ett primtal, $p \equiv 3 \pmod 4$. Visa att det för alla heltal m gäller $p \nmid m^2 + 1$, dvs att $m^2 + 1$ inte är delbart med p.
b) (3p) Låt p vara ett primtal, $p \equiv 1 \pmod 4$. Visa att det finns ett heltal n, sådant att $p \mid n^2 + 1$.
[Ledning för a) och b): Betrakta sambanden som ekvationer för m, n i kroppen $\mathbb{Z}_p$.]

Lösningar kommer att läggas ut på kurssidan.