

Matematik, KTH

B.Ek

**Tentamen i kursen
SF1662, DISKRET MATEMATIK för CL1
måndagen den 28 maj 2012, klockan 8.00–13.00**

Examinator: Bengt Ek, tel 7906951.

Tillåtna hjälpmedel: Inga, inte ens räknedosa.

För **godkänt betyg**, dvs minst E, krävs **dels** minst 12p på del I, **dels** totalpoäng enligt följande.

För betyg	A	B	C	D	E	
krävs	32	27	22	18	15	poäng (inklusive bonus)

Den som inte blivit godkänd, men fått **minst 12p** totalt, får FX och därmed rätt att delta i en kompletteringsskrivning för betyg E. Se kurssidan.

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 Var och en av uppgifterna i denna del svarar mot kontrollskrivningen med samma nummer.

Godkänd kontrollskrivning ger automatiskt full poäng på uppgiften och det ger då ingen ytterligare poäng att lösa den uppgiften på skrivningen.

Ange på skrivningsomslaget vilka kontrollskrivningar du har klarat.

OBS! Utan minst 12p på denna del blir tentamen inte godkänd.

1a) (1p) Avgör för vart och ett av 153, 209 och 216 om det är inverterbart i $\mathbb{Z}_{323}$. ($323 = 17 \cdot 19$)

b) (2p) Bestäm inversen för ett av elementen i a).

2) (3p) Talföljden $\{a_n\}_{n=0}^\infty$ definieras av

$$\begin{cases} a_{n+2} = 5a_{n+1} + 14a_n, & \text{för } n \in \mathbb{N} \\ a_0 = 8, \ a_1 = 2. \end{cases}$$

Visa att $a_n = 2 \cdot 7^n + 6 \cdot (-2)^n$ för $n \in \mathbb{N}$.

3) Låt X vara mängden av funktioner $f : \{1, 2, \dots, 11\} \rightarrow \{1, 2, \dots, 15\}$.

a) (1p) Hur många $f \in X$ är injektioner?

b) (1p) För hur många $f \in X$ är $f(x)$ udda för udda x , jämn för jämna x ?

c) (1p) Hur många $f \in X$ är av precis endera av typerna i a) och b)?

(Svaret får innehålla heltal, potenser, faktorer och de fyra enkla räknesätten.)

4) Låt $(G, \cdot)$ vara en grupp. Vi söker $x, y, z \in G$ så att $x = y^2$, $y = z^2$, $z = x^2$.

a) (1p) Finn alla sådana $x, y, z \in G$, så att minst två av dem är lika.

b) (2p) Visa att om $|G| = 1000$ finns inga sådana $x, y, z \in G$ som alla är olika.

5) (3p) En plan, sammanhängande graf delar in planet i områden (ytor, fasetter). Av dem begränsas 1 av 10 kanter, 3 st av 5 kanter, 4 st av 4 kanter och 7 st begränsas av 3 kanter (och det finns inga fler områden).

Finn (med motivering förstås) antalet hörn (noder) i grafen.

Vänd!

DEL II

6) Man vill skapa ett RSA-system för kryptering med de ”stora” primtalen $p = 67$ och $q = 71$, dvs parametern $n = 67 \cdot 71 = 4757$.

a) (2p) Ange villkoren på talen e, d för att de skall kunna användas som krypterings- resp. avkrypteringsexponent med detta n .

b) (2p) Man vill ha ett d som inte är primtal och inte är för litet. Vilket är det minsta möjliga icke-prima d med $d \geq 25$?

7) Permutationerna $\pi_1, \pi_2, \pi_3 \in S_9$ (gruppen av permutationer av $\{1, 2, \dots, 9\}$) ges på tvåradarsform av

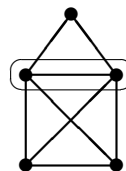
$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 4 & 8 & 6 & 3 & 5 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 6 & 2 & 9 & 8 & 4 & 3 & 1 \end{pmatrix},$$
$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 1 & 8 & 7 & 3 & 2 & 4 & 6 \end{pmatrix}.$$

a) (1p) Skriv π_1, π_2 och π_3 på cykelform och ange deras ordningar.

b) (3p) Finns det $\tau_i \in S_9$ så att $\pi_i = \tau_i^2$, dvs $\tau_i \tau_i$?

För $i = 1, 2, 3$, förklara varför inget sådant τ_i existerar, eller ge ett exempel på ett.

8) Grafen G bildas genom att två fullständiga grafer, K_m och K_n , med $m, n \geq 3$ ”sätts ihop” längs en kant (figuren visar fallet $m = 3, n = 4$, den gemensamma kanten inringad).



a) (1p) För vilka värden på m, n har G en eulerkrets?

b) (3p) För vilka värden på m, n har G en eulerväg (inte eulerkrets)?

DEL III

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

9) Låt $m, n \in \mathbb{N}$ ($1 \leq m < n$), H vara en delgrupp till S_m och

$$E_H = \{\pi \in A_n \mid \text{för något } \tau \in H : \pi(x) = \tau(x), \text{ alla } x = 1, 2, \dots, m\}.$$

(S_m är gruppen av permutationer av $\{1, 2, \dots, m\}$, A_n gruppen av jämna permutationer i S_n).

a) (2p) Visa att E_H är en delgrupp till A_n .

b) (3p) Bestäm för de tre fallen $n - m = 1, 2, 3$ alla möjliga värden för $\frac{|E_H|}{|H|}$.

10) (5p) Låt A vara en mängd av 681 st heltal mellan 1 och 1000, dvs

$$A \subset \{1, 2, \dots, 1000\}, \quad |A| = 681.$$

Visa att det finns $a_1, a_2, a_3 \in A$ med $a_3 = a_2 + 10 = a_1 + 20$.

(Ledning: Låt $B = \{a + 10 \mid a \in A\}$ och $C = \{a + 20 \mid a \in A\}$.

Förklara varför det räcker att visa $|A \cap B \cap C| > 0$ och gör det.)

**Lösningar kommer att läggas ut på kurssidan.
Där kommer så småningom också en kursenkät, fyll i den!**