Matematiska Institutionen
KTH

Tentamensskrivning (rättad version) i Diskret Matematik för CINTE, CL och CMETE, SF1610 och 5B1118, måndagen den 17 oktober 2011, kl 08.00-13.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

13	poäng totalt eller mer ger minst omdömet	Fx
15	poäng totalt eller mer ger minst betyget	E
18	poäng totalt eller mer ger minst betyget	D
22	poäng totalt eller mer ger minst betyget	C
28	poäng totalt eller mer ger minst betyget	B
32	poäng totalt eller mer ger minst betyget	A

För ett godkänt resultat krävs också minst 12 poäng på del I.

Generellt gäller att för full poäng krävs korrekta och väl presenterade resonemang.

DEL I

Var och en av nedanstående uppgifter svarar mot en kontrollskrivning. Godkänt resultat på en kontrollskrivning ger automatiskt full poäng på motsvarande uppgift. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm
$$17^{2011} \pmod{10} .$$

2. (3p) En klass med de 10 flickorna F_1, F_2, ..., F_{10} och de 10 pojkarna P_1, P_2, ..., P_{10} skall utse en grupp om sex klassrepresentanter med lika många pojkar som flickor. På hur många olika sätt kan man sätta samman en sådan grupp om pojken P_3 deltar endast på villkor att minst en av flickorna F_4 och F_8 blir med i gruppen. För full poäng krävs att svaret ges i formen av ett heltal.

3. (3p) Bestäm fyra cykliska delgrupper till gruppen $G = (Z_{30}, +)$.

4. (a) (2p) Ett RSA-krypto har parametrarna $n = 95$, $e = 29$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.
   (b) (1p) Vilka värden på parametern n kan ett RSA-kryto ha om $45 \leq n \leq 55$.

5. (3p) Rita en komplett bipartit graf $K_{n,m}$ med totalt 8 noder, dvs $n+m = 8$, som har en Eulerkrets men inte har någon Hamiltoncykel.

DEL II

6. (3p) Förklara varför en graf, som har 30 noder med valens 1, 15 noder med valens 2 och minst 30 noder med valens minst 3, måste ha minst en cykel.

7. (3p) Bestäm antalet positiva hela tal som delar både talet 2156 och talet 2548.

8. (a) (2p) Bestäm antalet sätt som elementen i mängden $\{1, 2, 3, 4, 5, 6\}$ kan delas in i fyra icketomma delmängder så att elementen 1 och 2 hamnar i olika delmängder. Svaret skall ges i formen av ett heltal.

   (b) (3p) Bestäm antalet sätt som de 10 elementen i mängden $\{1, 2, 3, \ldots, 10\}$ kan delas in i fem icketomma delmängder så att elementen 1, 2 och 3 hamnar i olika delmängder. Svaret får innehålla beteckningar och symboler som presenterats i kursen.

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i lösningen.

9. Mängden av alla permutationer av elementen i mängden $\{1, 2, 3, 4\}$ bildar på sedvanligt sätt, dvs under operationen sammansättning av permutationer, en grupp som vi betecknar med $\mathcal{S}_4$.

   (a) (1p) Bestäm en ickecyklisk delgrupp till $\mathcal{S}_4$ med fyra element.

   (b) (2p) Visa att mängden av alla jämna permutationer i $\mathcal{S}_4$ bildar en delgrupp till $\mathcal{S}_4$ och att denna delgrupp har 12 element.

   (c) (2p) Bestäm den minsta delgrupp till $\mathcal{S}_4$ som innehåller permutationerna $(1\ 2\ 3)$ och $(3\ 4)$.

10. Under kursen fick ni se hur en 1-felsrättande kod C kan konstrueras med hjälp av en så kallad kontrollmatris (parity check-matris) $\mathbf{H}$, och där C ges av $\mathbf{H}$ enligt nedan:

$$c = (c_1, c_2, \ldots, c_n) \in C \qquad \Longleftrightarrow \qquad \mathbf{H}c^T = 0^T \ .$$

   (a) (2p) Vilka egenskaper måste $\mathbf{H}$ ha för att en kod C, konstruerad enligt ovanstående recept, skall vara 2-felsrättande?

   (b) (1p) Vilka egenskaper måste $\mathbf{H}$ ha för att en kod C, konstruerad enligt ovanstående recept, skall vara e-felsrättande?

   (c) (2p) Konstruera en 2-felsrättande kod med åtta ord. (Antalet poäng du får beror bland annat på ordlängden n. T ex kan du få 1p för en 2-felsrättande kod med 8 ord och med ordlängden $n = 15$.)