Matematiska Institutionen
KTH

Tentamensskrivning i Diskret Matematik för IT2, CL2 och Media 1, SF1610 och 5B1118, torsdagen den 20 december 2007, kl 08.00-13.00.

Examinator: Olof Heden.

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

12	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

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 den största gemensamma delaren till talen 573 och 654.
2. (3p) Fem pojkar och fyra flickor skola ställa sig på ett led. På hur många olika sätt kan detta ske om varje flicka skall stå mellan två pojkar. Svaret får innehålla de fyra räknesätten addition, subtraktion, multiplikation och division.
3. (3p) Gruppen $G = (Z_{11} \setminus \{0\}, \cdot)$ är cyklisk. Bestäm en generator till G.
4. (3p) Ett RSA-krypto har $n = 39$ och $e = 7$.
   (a) (1p) Kryptera meddelandet 2.
   (b) (1p) Bestäm d.
   (c) (1p) Dekryptera meddelandet 3.
5. (3p) Den bipartita grafen med nodmängderna $X = \{a, b, c, d\}$ och $Y = \{1, 2, 3, 4, 5\}$ har kanterna $\{a1, a3, b3, c2, d2, d4, d5\}$. Bestäm en alternerande stig till matchningen $M = \{a3, d2\}$.

DEL II

6. Låt som vanligt S_5 beteckna mängden av alla permutationer på mängden $\{1, 2, 3, 4, 5\}$.

   (a) (1p) Visa att permutation $(1\ 3)(1\ 2)(1\ 3)$ är en transposition (dvs 2-cykel) och bestäm vilken.

   (b) (1p) Skriv permutationen
   $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$
   som en produkt av transpositioner av typen $(1\ x)$ där $x \in \{2, 3, 4, 5\}$. (Du får använda samma transposition mer än en gång.)

   (c) (1p) Kan alla permutationer i S_5 skrivas som en produkt av transpositioner av typen $(1\ x)$ där $x \in \{2, 3, 4, 5\}$. Motivera ditt svar.

7. (4p) Beskriv, på ett lämpligt sätt, en 1-felsrättande kod C av längd 9 som

   (a) (1p) innehåller 16 ord.

   (b) (1p) innehåller ordet 111111111.

   (c) (1p) är sådan att ordet 111100000 ligger på avstånd ett från precis ett kodord.

   (d) (1p) är sådan att ordet 000011110 ligger på avstånd två från minst ett ord i C.

   Anm. Antalet poäng på uppgiften blir lika med antalet av krav ovan som är uppfyllda.

8. (4p) Låt M betckna mängden av surjektioner f från mängden $\{A, B, C, D, E, F\}$ på mängden $\{1, 2, 3\}$ som uppfyller följande två villkor

   (a) M innehåller ingen surjektion f sådan att $f(A) = f(B) = f(C)$.

   (b) M innehåller ingen surjektion f sådan att $f(A) \neq f(B)$, $f(A) \neq f(C)$ och $f(C) \neq f(B)$.

   Bestäm antalet surjektioner som finns i mängden M. Svaret skall ges i formen av ett heltal.

DEL III

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

9. (a) (2p) Visa, t ex med hjälp av principen om inklusion exklusion, att om n är en produkt av två olika primtal p och q, dvs $n = p \cdot q$ så gäller att antalet tal d, sådana att $1 \leq d \leq n$ och d relativt primt till n, är lika med $(p-1)(q-1)$, dvs lika med talet
   $$n(1 - \frac{1}{p})(1 - \frac{1}{q}).$$

   (b) (3p) Generalisera denna formel till ett godtyckligt heltal n.
   (**Anm.** Delpoäng erhålles för välmotiverade gissningar, halvfärdiga lösningar m.m.)

10. (5p) Låt $\sigma(a)$ och $\sigma(b)$ beteckna ordningarna av elemeneten a och b i en grupp G, med gruppoperationen $\circ$. Visa att påståendet

    $\sigma(a \circ b)$ delar $mgm(\sigma(a), \sigma(b))$ för alla $a, b \in G$

    är giltigt för alla abelska (kommutativa grupper) G samt visa, t ex genom ett exempel, att påståendet inte går att visa generellt för alla icke abelska grupper. ($mgm(n, d)$ betecknar den minsta gemensamma multiplen av talen n och d.)