Matematiska Institutionen
KTH

**Tentamensskrivning i Diskret Matematik för CINTE och CMETE, m fl, SF1610, tisdagen den 2 juni 2015, kl 14.00-19.00.**

**Examinator:** Olof Heden

**Hjälpmedel:** Inga hjälpmedel är tillåtna på tentamensskrivningen.

**Betygsgränser:** (**OBS:** Totalsumma poäng vid denna tentamensskrivning 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 |

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

**DEL I**

Var och en av nedanstående fem uppgifter svarar mot en kontrollskrivning. Godkänt resultat på kontrollskrivning nr. $i$ under vårterminen 2015 ger automatiskt full poäng på uppgift nr. $i$. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (a) (1p) Bestäm $53^{100} (\text{mod } 101)$.
   (b) (2p) Lös ekvationen $43x + 12 = 53$ i ringen $Z_{97}$.

2. (3p) Ange nedanstående binomialkoefficient, multinomialkoefficient respektive Stirlingtal som hela tal:
$$\binom{45}{42}, \qquad \binom{20}{14, 2, 2, 2}, \qquad \mathrm{S}(8, 7).$$

3. Betrakta gruppen $G = (Z_{21}, +)$
   (a) (1p) Bestäm ett element av ordning 7 i $G$.
   (b) (1p) Bestäm en cykliska delgrupp till $G$ med sju element.
   (c) (1p) Finns det någon sidoklass $S$ till en delgrupp till $G$ sådan att $S$ har fem element?

4. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 187$ och $e = 89$. Dekryptera meddelandet 2, dvs bestäm D(2).

5. Den planära och sammanhängande grafen $G$ har noder med valenserna (graderna)
$$1,\ 2,\ 2,\ 2,\ 3,\ 3,\ 3,\ 3,\ 4,\ 4,\ 5,\ 5,\ 7.$$
   (a) (2p) Bestäm antalet områden (regioner) som uppstår när grafen $G$ ritas plant.
   (b) (1p) Vilket är det minsta antal kanter som behöver läggas till för att grafen $G$ skall få en Eulerkrets.

## DEL II

6. (3p) Bestäm antalet ord av längd 7 som man kan bilda med hjälp de sju bokstäverna A, B, C, D, E, F och G (varje bokstav skall förekomma precis en gångi ordet) och som är sådana att inget av orden EFGA, ABC och BEF får finnas med som delord i ordet. (T ex så är ordet ABCEDFG ett förbjudet ord, eftersom ABC är ett delord, DFAE är för kort och ordet AAABBBB innehåller inte samtiga sju bokstäver.)

7. (4p) Bestäm en 1-felsrättande kod $C$ av längd 12 sådan att $C$ innehåller 128 ord varav ordet 111111111111 är ett av kodens ord samt sådan att ordet 111000000000 rättas till ordet 111100000000.

8. (4p) Betrakta gruppen $\mathcal{S}_8$ som består av alla permutationer av elementen i mängden $\{1, 2, \ldots, 8\}$. Bestäm antalet permutationer i $\mathcal{S}_8$ som har ordning 4.

## 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. Låt $\operatorname{sgd}(a, b)$ och $\operatorname{mgm}(a, b)$ beteckna den största gemensamma delaren respektive den minsta gemensamma multipeln till heltalen $a$ och $b$.

   (a) (1p) Förklara varför det inte finns några hela tal $a$ och $b$ som uppfyller
   $$\operatorname{sgd}(a, b) = 96, \qquad \operatorname{mgm}(a, b) = 492.$$

   (b) (1p) Låt $p$ vara ett primtal och $n$ ett positivt heltal. Bestäm samtliga positiva heltal $a$ och $b$ sådana att
   $$\operatorname{sgd}(a, b) \cdot \operatorname{mgm}(a, b) = p^n.$$

   (c) (3p) Låt $n$ och $m$ vara två positiva hela tal. Ge en formel för antalet oordnade par av positiva hela tal $\{a, b\}$ sådana att
   $$\operatorname{sgd}(a, b) = n, \qquad \operatorname{mgm}(a, b) = m.$$

10. Låt $\mathcal{F}$ beteckna mängden av alla booleska funktioner i de oändligt många booleska variablerna $x_1, x_2, \ldots$. Låt N beteckna de naturliga talen, dvs 0,1,2, ... och låt $2^{\mathrm{N}}$ beteckna mängden av alla delmängder till N. Låt $\mathcal{B}$ beteckna mängden av bijektioner från N till N.

    (a) (2p) Har $\mathcal{F}$ samma kardinalitet som mängden av alla delmängder till $2^{\mathrm{N}}$?

    (b) (3p) Utgick pga felformulering.