Matematiska Institutionen
KTH

Tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610 och 5B1118, fredagen den 25 oktober 2013, kl 14.00-19.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (**OBS:** Totalsumma poäng vid denna tentamensskrivning är **38p**.)

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 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 498 och 713.
2. (3p) Tio identiska bollar fördelas bland fyra barn. På hur många olika sätt kan detta ske. Svaret skall ges som ett heltal, dvs som något av talen 1, 2, 3, ...
3. Betrakta gruppen $G = (Z_{21}, +)$.
   (a) (1p) Bestäm en icke-trivial delgrupp H till G.
   (b) (1p) Vilka möjligheter finns det för ordningen av element i G.
   (c) (1p) Bestäm ordningen av elementet 2 i G.
4. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 85$ och $e = 13$. Kryptera medelandet 2, dvs bestäm E(2), och dekryptera meddelandet 3, dvs bestäm D(3).
5. (3p) För vilka hela tal n och m har den kompletta bipartita grafen $K_{n,m}$ en Eulerkrets (sluten Eulerväg, alt. sluten Eulerpromenad), och för vilka hela tal n och m har den kompletta bipartita grafen $K_{n,m}$ en Hamiltoncykel.

VGV

DEL II

6. (a) (1p) Skriv den Booleska funktionen $f(x,y,z,w) = (x\bar{y} + \bar{x})\bar{z}\bar{w} + \bar{y}(\bar{x} + z)$ på en disjunktiv normalform, dvs på d.n.f. .

   (b) (2p) Låt $f(x,y,z,w)$ vara som ovan och och låt $g(x,y,z,w) = \bar{y}(\bar{w} + z) + \bar{x}\bar{z}(\bar{y} + y\bar{w})$. Är $f(x,y,z,w)$ och $g(x,y,z,w)$ samma Booleska funktion.

   (c) (2p) Bestäm antalet Booleska funktioner $h(x,y,z,w)$ som är sådana att

   $$|\{(x,y,z,w) \mid f(x,y,z,w) = 1\} \cap \{(x,y,z,w) \mid h(x,y,z,w) = 1\}| = 3.$$

   Svaret får innehålla summor och produkter av tal.

7. Låt $\mathcal{S}_7$ beteckna mängden av alla permutationer av mängden $\{1, 2, \ldots, 7\}$, och låt ψ beteckna permutationen $\psi = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6)(7)$ i $\mathcal{S}_7$.

   (a) (2p) Bestäm en permutation φ i $\mathcal{S}_7$ sådan att permutationen $\psi\varphi$ har ordning 12.

   (b) (2p) Bestäm antalet permutationer $\varphi \in \mathcal{S}_7$ sådana att permutationen $\psi\varphi$ har ordning 12. Lösningen skall motiveras och svaret ges i formen av ett heltal, dvs som något av talen 1, 2, 3, ...

8. (4p) Bestäm samtliga samanhängande grafer sådana att antalet noder av valens (grad) 2 är dubbelt så stort som antalet noder av valens (grad) 3, och antalet noder av valens (grad) 1 är tre gånger så så stort som antalet noder av valens (grad) 3. Grafen har inga noder av valens (grad) större än 3. Möjligheten att grafen skulle kunna ha multipla (parallella) kanter och loopar (öglor) är inte utesluten. (Vid poängsättningen av din lösning till denna uppgift kommer särskild vikt också att läggas vid att lösningen är så komplett och fullständig som möjligt.)

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. *Vikten* av ett binärt ord definieras som antalet ettor i ordet. Vikten av ett ord $\bar{c}$ betecknas $\mathrm{w}(\bar{c})$. Ett binärt ord $\bar{c}$ har *jämn vikt* om $\mathrm{w}(\bar{c})$ är ett jämnt tal.

   (a) (1p) Den 1-felsrättande koden C har kontrollmatrisen (parity-check matrisen)

   $$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

   Bestäm två ord $\bar{c}_1$ och $\bar{c}_2$, båda skilda från nollordet, sådana att $\bar{c}_1$ har jämn vikt och $\bar{c}_2$ inte har jämn vikt.

   (b) (2p) Bestäm kontrollmatrisen till en 1-felsrättande kod C av längd 11 med 64 stycken ord, och sådan att samtliga ord i C har jämn vikt.

   (c) (2p) Undersök om det finns någon 1-felsrättande kod av längd 15 med 2048 stycken ord, och sådan att samtliga ord i C har jämn vikt.

10. Låt p och q vara två olika primtal och låt $n = p^2q^4$.

    (a) (3p) Visa att antalet tal a i intervallet $1 \leq a \leq n$ som är relativt prima till n är lika med $p(p-1)q^3(q-1)$.

    (b) (2p) Visa att för varje inverterbart element a i ringen Z_n så gäller att

    $$a^{p(p-1)q^3(q-1)} = 1.$$