Institutionen för matematik
KTH

Tentamensskrivning, 2002–12–16, kl. 14^{00}–19^{00}.

5B1118 Diskret matematik, för IT.

Inga hjälpmedel tillåtna!

För godkänt=betyg 3 krävs minst 15 poäng, för betyg 4 minst 22 poäng och för betyg 5, minst 30 poäng. De som har blivit godkända på både inlämningsuppgiften och kontrollskrivningen någon av veckorna får tillgodoräkna sig motsvarande uppgift på tentan, dvs vecka 1 svarar mot uppgift 1 osv.

Redovisa lösningarna så att beräkningar och resonemang är lätta att följa. Motivera väl!

1. Ge en explicit bijektion från de naturliga talen till mängden av alla udda heltal, $M = \{\ldots, -3, -1, 1, 3, \ldots\}$. (3p)

2. Finn ett alternativt uttryck för den booleska funktionen

   $$f(x,y,z,w) = \bar{x}\bar{y}\bar{z}w + \bar{x}\bar{y}zw + \bar{x}y\bar{z}\bar{w} + \bar{x}y\bar{z}w + \bar{x}yzw + \bar{x}yz\bar{w} + xy\bar{z}w + x\bar{y}\bar{z}w + x\bar{y}zw$$

   med så få termer som möjligt. (3p)

3. Ett 9-spel består av en platta med 8 bitar och en tom plats och det är tillåtet att skjuta biten närmast till höger om, vänster om, ovanför eller nedanför tomrummet till den tomma platsen. T ex kan vi som första steg, i den vänstra figuren nedan, flytta Y eller T till den tomma platsen. Visa att det inte går, med tillåtna drag, att ändra uppställningen till vänster så att den blir den till höger.

A	E	I	A	Y	I
O	U	Y	R	O	T.
R	T		E	U	

   (3p)

4. Finn polynom $\mu(x)$ och $\lambda(x)$ i $\mathbf{Z}_5[x]$ sådana att

   $$\mu(x)(x^2 + 3x + 2) + \lambda(x)(x^3 + 2x^2 + 3x) = 1.$$

   (3p)

5. Förklara hur man med hjälp av kantfärgning kan utvidga nedanstående latinska rektangel till en latinsk kvadrat.

A	D	E	B	C
C	B	A	D	E
E	C	B	A	D

   (3p)

V.g. vänd!

6. Visa att det inte kan finnas någon perfekt binär kod med längd 6 som rättar ett fel. Ge exempel på en linjär kod med längd 6, som rättar ett fel och som är maximal med avseende på antalet kodord. (4p)

7. Finn samtliga delgrupper till $U(\mathbf{Z}_{24})$, dvs den multiplikativa gruppen av inverterbara element i $\mathbf{Z}_{24}$. (4p)

8. Bevisa med ett kombinatoriskt argument identiteten

$$\binom{n}{4} = \sum_{k=0}^{n-4} \binom{n-1-k}{3},$$

för alla $n \geq 4$. (4p)

9. Den underliggande mängden i den booleska algebran $\mathcal{B}_n$ är mängden av alla binära ord med längd n, V^n. I $\mathcal{B}_n$ har vi de tre operationerna $+, \cdot$ och $^-$. Vi har också, i samband med felrättande koder, definierat en annan addition på V^n, som vi kan beteckna $\oplus$, genom att addera komponentvis modulo 2. Uttryck operationen $\oplus$ med $+, \cdot$ och $^-$. Visa också att $(V^n, \oplus, \cdot)$ är en ring. (4p)

10. RSA-kryptering fungerar tack vare identiteten

$$x^{k(p-1)(q-1)+1} \equiv x \pmod{pq},$$

som gäller då p, q är två olika primtal och k, x är två heltal. Bevisa identiteten. (4p)