Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 25 maj 2010 kl 08.00-13.00.

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

Bonuspoäng: Bonuspoäng erhållna från lappskrivningar till kursen under vt09 adderas till skrivningspoängen.

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

DEL I

1. (3p) Till ett RSA-krypto väljer man primtalen $p = 3$ och $q = 23$, vilka skall användas i denna uppgift.

   (a) (1p) Vilket, eller vilka, av följande värden på parametern e kan man använda: $e = 9$, $e = 10$ och/eller $e = 11$.

   (b) (2p) Välj ett tillåtet värde på parametern e och dekryptera meddelandet 2, dvs bestäm $D(2)$.

2. Nedanstående matris är en parity-check (kontroll-) matris till en 1-felsrättande kod C

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

   (a) (1p) Undersök om koden C kan rätta ordet 01110111, och rätta ordet i så fall.

   (b) (1p) Ange antalet ord i C.

   (c) (1p) Bestäm antalet ord som ”kan rättas” av C.

3. (3p) Betrakta gruppen $G = (Z_{20}, +)$ som innehåller elementen $\{0, 1, 2, \ldots, 19\}$ och där man räknar modulo 20. En av sidoklasserna (”coset”) till en av gruppens delgrupper innehåller elementet 2 och tre element till. Bestäm dessa tre element.

4. Låt F vara kroppen med de 16 elementen

$$F = \{\ a_0 + a_1 x + a_2 x^2 + a_3 x^3 \ \mid \ a_0, a_1, a_2, a_3 \in Z_2\ \} \qquad ;,$$

   och där man räknar som om $x^4 + x + 1 = 0$.

   (a) (2p) Bestäm det element z i F som är invers till x, dvs sådant att $x \cdot z = 1$.

   (b) (1p) Bestäm ett element w i F sådant att $x \cdot w = x^2 + x + 1$.

5. (4p) Betrakta gruppen $G = (Z_{24}, +)$ som innehåller elementen $\{0, 1, 2, \ldots, 23\}$ och där man räknar modulo 24.

   (a) (2p) Bestäm en delgrupp till G som innehåller elementet 16, men inte innehåller elementet 3.

   (b) (2p) Visa att om en delgrupp H till G innehåller både elementet 3 och elementet 16 så måste $H = G$.

DEL II

6. (3p) Mängden av element i ringen Z_{24} som är inverterbara med avseende på multiplikation bildar en grupp. Undersök om denna grupp är cyklisk.

7. (3p) Är polynomet $x^4 + x - 1$ irreducibelt i polynomringen $Z_5[x]$?

8. (4p) Undersök om det finns någon grupp G med delgrupper H och K sådana att $H \not\subseteq K$, $K \not\subseteq H$ men $H \cup K$ är en delgrupp till G.

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. Det sägs ju att alla lika stora ändliga kroppar är isomorfa, och det handlar det om nu.

   (a) (1p) Ge en lämplig definition av vad som menas med att två kroppar K och F är isomorfa.

   (b) (2p) Låt K vara den kropp med åtta element som definieras med hjälp av polynomet $p(x) = x^3 + x^2 + 1$, som ju är irreducibelt i $Z_2[x]$ och F den kropp med åtta element som definieras med hjälp av polynomet $q(x) = x^3 + x + 1$ som är irreducibelt i $Z_2[x]$. Beskriv en isomorfi mellan K och F.

   Ett svar som saknar motivering ger noll poäng.

   (c) (2p) Bestäm antalet olika isomorfier mellan K och F.

10. (5p) Låt $\varphi(n)$ beteckna antalet tal m, med $1 \leq m \leq n$, som är relativt prima med n. Visa att för alla positiva hela tal n, och alla primtal p, gäller att n är en delare till $\varphi(p^n - 1)$.