

Matematiska Institutionen  
KTH

**Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631(5B1204) och SF1630(5B1203), den 20 augusti 2008 kl 14.00-19.00.**

**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 vt08 adderas till skrivningspoängen. Maximalt har man kunnat få 6 bonuspoäng.

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

## DEL I

- (3p) Du skall konstruera ett RSA-krypto som har parametern  $n = 51$  och ett värde på parametern  $e$  som du väljer själv. Välj en parameter  $e$  och dekryptera meddelandet 2, dvs bestäm  $D(2)$  i det krypto du konstruerat.
- (3p) Avgör om polynomet  $x^2 + x + 1$  är irreducibelt i polynomringen  $Z_7[x]$ .
- Mängden  $\{1, 2, 3, 4, \dots, 12\}$  bildar under operationen multiplikation modulo 13 en cyklisk grupp  $G$  med 12 element.
  - (2p) Bestäm en generator för denna cykliska grupp  $G$ .
  - (1p) Bestäm en delgrupp till  $G$  med sex element.
- (3p) Betrakta mängden  $G = \{e, a, b, c, d\}$  med multiplikationstabellen

$\circ$	$e$	$a$	$b$	$c$	$d$
$e$	$e$	$a$	$b$	$c$	$d$
$a$	$a$	$c$	$d$	$e$	$b$
$b$	$b$	$d$	$e$	$a$	$c$
$c$	$c$	$b$	$a$	$d$	$e$
$d$	$d$	$e$	$c$	$b$	$a$

Utgör mängden  $G$  med denna multiplikationstabell en grupp?

- (3p) Gruppen  $(Z_{20}, +)$  har ett antal delgrupper och en samling av olika sidoklasser till dessa delgrupper. En av dessa sidoklasser innehåller precis fem element varav elementet 3 är ett av dessa fem element. Ange samtliga element i denna sidoklass.

## DEL II

6. (3p) Låt  $F_9$  beteckna den kropp med nio element som på sedvanligt sätt konstrueras med hjälp av det irreducibla polynomet  $p(x) = x^2 + 1$  i ringen  $Z_3[x]$ . Lös den binomiska ekvationen  $z^6 = 1$  i denna kropp, dvs bestäm samtliga element  $z \in F_9$  sådana att  $z^6 = 1$ .
7. (a) (2p) Visa att det inte finns någon 1-felsrättande linjär kod  $C$  med 32 ord och som innehåller de tre orden
- $$c_1 = 111100000, \quad c_2 = 011001100, \quad c_3 = 100101010.$$
- (b) (2p) Undersök om en sådan kod  $C$  kan finnas om bara två av de tre givna orden ovan skall finnas med bland de 32 orden i  $C$ .
8. (4p) Låt  $S_4$  beteckna mängden av alla permutationer av elementen i en mängd med fyra element.  $S_4$  är en grupp med 24 element. Bestäm minst en delgrupp till  $S_4$  med åtta element.

## DEL III

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

9. För grupper  $G_1$  och  $G_2$  med gruppoperationerna  $\circ_1$  respektive  $\circ_2$  så definieras den direkta produkten av dessa grupper som mängden

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, \quad g_2 \in G_2\}$$

med gruppoperationen  $\circ$  definierad av

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2).$$

- (a) (2p) Under vilka förutsättningar gäller att om  $G_1 \times G_2$  är en ändlig cyklisk grupp så är både  $G_1$  och  $G_2$  cykliska grupper.
- (b) (3p) Under vilka förutsättningar gäller att om  $G_1$  och  $G_2$  är ändliga cykliska grupper så är  $G_1 \times G_2$  en cyklisk grupp.

**OBS:** För full poäng krävs givetvis korrekta bevis och motiveringar.

10. Betrakta polynomen  $p_1(x) = x^3 + x + 1$  och  $p_2(x) = x^3 + x^2 + 1$  i polynomringen  $Z_2[x]$ . Dessa polynom är irreducibla och kan därför användas till att konstruera kroppar  $K_1$  respektive  $K_2$  bägge med åtta element. Enligt den allmänna teorin för kroppar är  $K_1$  och  $K_2$  isomorfa som kroppar.
- (a) (3p) Bestäm en isomorfi  $\varphi$  mellan dessa kroppar.
- (b) (2p) Finns det mer än en sådan isomorfi. (Kvaliten på ditt svar avgör antalet poäng som du får på denna deluppgift.)