MODELLTENTA DISKRET MATEMATIK moment B FÖR D2 och F, SF1631 resp SF1630.

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

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.

DEL I

1. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 33$ och $e = 7$. Dekryptera meddelandet 5.
2. (3p) Fyll i nedanstående tabell så att det blir multiplikationstabellen till en grupp:

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

3. (3p) Låt $G = (Z_{40}, +)$. Undersök om mängden

$$\{2, 7, 11, 18, 25, 32\},$$

kan vara sidoklass till någon delgrupp till G.

4. (3p) De inverterbara elementen i ringen Z_{15} bildar en grupp. (Detta behöver du ej visa.) Undersök om denna grupp är cyklisk.
5. (3p) Undersök om polynomet $x^3 + x + 1$ är irreducibelt i polynomringen $Z_7[x]$.

DEL II

6. (3p) Hur många olika pärlhalsband med sex pärlor i färgerna svart, vitt och grönt kan man tillverka.
7. (4p) Undersök om nedanstående mängd matriser med sedvanliga matrisoperationer bildar en ring utan etta:

$$\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a + b + c + d = 0, \quad a, b, c, d \in R. \}$$

8. (4p) Kroppen F med 25 element består av polynom av grad högst 1, med koefficienter i Z_5, och man räknar i F som om $x^2 + 2 = 0$. Dvs

$$F = \{ax + b \mid a, b \in Z_5\} \quad \text{och} \quad x^2 = 3.$$

Bestäm ett element z i denna kropp sådant att $(2x + 1)z = x$.

DEL III

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

9. (5p) Tyvärr råkade någon välja en oäkta kontrollmatris (paritycheck-matrix) för att skapa en 1-felsrättande kod, enligt nedan:

$$C = \{\bar{c} = (c_1, c_2, \ldots, c_7) \mid H\bar{c}^T = (0\ 0\ 0)^T\} \quad \text{där} \quad H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Det är för sent att ändra så vissa ord i koden går inte att använda. Man måste därför utesluta ord ur C och skapa en ny 1-felsrättande kod C', dvs

$$C' \subseteq C, \quad \text{och} \quad C' \quad \text{är 1-felsrättande.}$$

Hur många ord kan C' ha maximalt, givet kontrollmatrisen H ovan. (Denna kontrollmatris skall vid felrättning användas på sedvanligt sätt och mottagaren känner inte till att kontrollmatrisen är felaktig utan hanterar den på det sätt han blivit lärd.)

10. Låt F_4 beteckna nedanstående kropp med fyra element

$$F_4 = \{a + \iota b \mid a, b \in Z_2\} \quad \text{med } \iota \text{ uppfyllande ekvationen} \quad \iota^2 = \iota + 1.$$

(a) (1p) Gör en, ur matematisk synvinkel vettig, definition av vad som menas med att en kropp F är en delkropp till en kropp K.

(b) (2p) Visa att det inte går att konstruera en kropp med åtta element som innehåller F_4 som delkropp.

(c) (2p) Konstruera en kropp med 16 element som innehåller F_4 som delkropp.