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

DEL I

1. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 33$ och $e = 7$. Dekryptera meddelandet 5.

   Lösning: Vi behöver ta rätt på primtalen p och q sådana att $n = p \cdot q$, vilket är lätt då $33 = 3 \cdot 11$. Får att få dekrypteringsnyckeln d behöver vi endast beräkna inversen till e i ringen Z_m, där $m = (p-1)(q-1)$ eftersom $e \cdot d \equiv 1 \pmod{m}$.

   I detta fall är $m = 20$ och $e = 7$ och vi gissar lätt att $d = 3$ eftersom $7 \cdot 3 \equiv_{20} 1$.

   Vi kan nu dekryptera meddelandet 5:

   $$D(5) = 5^d \pmod{n} = 5^3 \pmod{33} = 125 \pmod{33} = 26.$$

   SVAR: 26.

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					

   Lösning: Eftersom $a \circ a = a$ så måste a vara identitetselementet. Eftersom 5 är ett primtal så har alla element i gruppen, utom identitetselementet, ordning 5 och gruppen är cyklisk och isomorf med t ex gruppen $(Z_5, +)$. Låter vi a svara mot 0 och b, c, d, e svara mot elementen 1, 2, 3 respektive 4 i $(Z_5, +)$ så får vi tabellen nedan:

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

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

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

   kan vara sidoklass till någon delgrupp till G.

   Lösning: Den angivna mängden innehåller sex stycken element. Antalet element i en sidoklass till en delgrupp H till en grupp G innehåller alltid samma antal element som delgruppen H. Enligt Lagranges sats delar antalet elment i H antalet element i G. Eftersom 6 inte delar 40 så finns ingen delgrupp till G med sex element och därmed inte heller någon sidoklass med sex element.

4. (3p) De inverterbara elementen i ringen Z_{15} bildar en grupp. (Detta behöver du ej visa.) Undersök om denna grupp är cyklisk.

   Lösning: Elementet a i ringen Z_n är inverterbart om och endast om $sgd(a, n) = 1$. De inverterbara elementen i ringen Z_{15} är alltså

   $$G = U(Z_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

   Antalet element i G är 8 och gruppen G är då cyklisk om och endast om G har ett elemenet av ordning 8. Vi vet också att ordningen av ett element alltid delar antalet element i gruppen i fråga. I detta fall gäller alltså att

   $$g \in G \quad \Rightarrow \quad \sigma(g) \in \{1, 2, 4, 8\}.$$

   Vi undersöker nu ordningen av elementen i G med hjälp av denna information.

   Då $(\pm 1)^2 \equiv 1 \pmod{15}$ och då

   $$(\pm 2)^4 \equiv 1 \pmod{15}, \quad (\pm 4)^2 \equiv 1 \pmod{15}, \quad (\pm 7)^4 \equiv 1 \pmod{15},$$

   så har inget element ordning 8 och gruppen kan inte vara cyklisk.

5. (3p) Undersök om polynomet $x^3 + x + 1$ är irreducibelt i polynomringen $Z_7[x]$.

   Lösning: Eftersom polynomet $p(x)$ har en grad av högst tre, i detta fall precis tre, så räcker det att undersöka om det har nollställen för att avgöra om det är irreducibelt. Vi undersöker nu detta:

   $$\begin{array}{rrcl} & p(0) & = & 0^3 + 0 + 1 = 1 \neq 0 \\ & p(1) & = & 1^3 + 1 + 1 = 3 \neq 0 \\ & p(2) & = & 2^3 + 2 + 1 = 4 \neq 0 \\ & p(3) & = & 3^3 + 3 + 1 = 3 \neq 0 \\ p(4) = & p(-3) & = & -3^3 - 3 + 1 = 6 \neq 0 \\ p(5) = & p(-2) & = & -2^3 - 2 + 1 = 5 \neq 0 \\ p(6) = & p(-1) & = & -1^3 - 1 + 1 = 6 \neq 0 \end{array}$$

   Polynomet saknar nollställen och är då irreducibelt (eftersom polynomets grad är högst tre).

DEL II

6. (3p) Hur många olika pärlhalsband med sex pärlor i färgerna svart, vitt och grönt kan man tillverka.

   Lösning: Vi använder oss av det så kallade Burnsides lemma som säger att antalet banor som uppstår när en grupp G verkar på en mängd S ges av formeln

   $$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |Fix_S(g)|,$$

   där $|\mathcal{O}|$ betecknar antalet banor, och $|Fix_S(g)|$ betecknar antalet element i S som fixeras vid verkan av gruppelemenetet g.

   I vårt fall är S mängden av alla möjliga färgläggningar av halsbandet och G gruppen av samtliga vridningar och vändningar av halsbandet. Vi numrerar pärlorna med numren 1, 2, 3, 4, 5 och 6. Vridning ett sjättedels varv ger då permutationen $\varphi = (1\ 2\ 3\ 4\ 5\ 6)$ och det finns bara tre färgläggningar som fixeras av denna vridning nämligen de färgläggningar där alla pärlor får samma färg, svart vitt eller grönt. Vridning två sjättedels varv ger permutationen $\varphi^2 = (1\ 3\ 5)(2\ 4\ 6)$ och pärlorna 1, 3 och 5 måste ha samma färg liksom pärlorna 2, 4 och 6.

Vi får följande tabell, där ψ_i är vändning av halsbandet runt axeln mellan pärla nummer i och $i+3$, för $i = 1, 2, 3$. Vidare har vi γ_i för vändning av halsbandet mellan pärlorna i och $i+1$.

$g \in G$	$\lvert Fix_S(g)\rvert$
$id.$	3^6
$\varphi = (1\ 2\ 3\ 4\ 5\ 6)$	3
$\varphi^2 = (1\ 3\ 5)(2\ 4\ 6)$	3^2
$\varphi^3 = (1\ 4)(2\ 5)(3\ 6)$	3^3
$\varphi^4 = (1\ 5\ 3)(2\ 6\ 4)$	3^2
$\varphi^5 = (1\ 6\ 5\ 4\ 3\ 2)$	3
$\psi_1 = (1)(4)(2\ 6)(3\ 5)$	3^4
$\psi_2 = (2)(5)(1\ 3)(4\ 6)$	3^4
$\psi_3 = (3)(6)(1\ 5)(2\ 4)$	3^4
$\gamma_1 = (1\ 2)(3\ 6)(4\ 5)$	3^3
$\gamma_2 = (1\ 4)(2\ 3)(5\ 6)$	3^3
$\gamma_3 = (1\ 6)(2\ 5)(3\ 4)$	3^3

Formeln i Burnsides lemma ger nu omdelbart vårt

SVAR:

$$\frac{1}{12}(3^6 + 3 \cdot 3^4 + 4 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3).$$

7. (4p) Undersök om nedanstående mängd matriser med sedvanliga matrisoperationer bildar en ring utan etta:

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

Lösning: Vi förutsätter att med R menas de reella talen. Mängden är inte sluten under operationen matrismultiplikation ty matrisen

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

tillhör den givna ringen men A multiplicerad med sig själv, dvs AA, gör det inte eftersom

$$AA = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

och $1 + 0 + 0 + 1 = 2 \neq 0$.

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 $(2x+1)z = x$.

Lösning: Det sökta elementet z ges av

$$z = (2x+1)^{-1}x.$$

Vi söker nu inversen till elementet $2x+1$ i kroppen F med hjälp av Euklides algoritm, där det visar sig att det räcker med precis ett steg för att hitta inversen:

$$x^2 + 2 = (3x+1)(2x+1) + 1 \qquad \text{som ger} \quad 1 = (x^2+2) - (3x+1)(2x+1).$$

Använder vi nu att $x^2 + 2 = 0$ får vi att

$$-(3x+1)(2x+1) = 1$$

och alltså

$$(2x+1)^{-1} = -(3x+1).$$

Därmed är

$$z = -(3x+1)x = -3x^2 - x = -3 \cdot 3 - x = 1 - x = 4x + 1.$$

SVAR: $z = 4x + 1$.

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.)

Lösning: Tyvärr inget ord alls. Antag att avsändaren bara använder ett ord, ordet $\bar{c}$. Om ett fel uppstår i position nummer 1 så kommer

$$H\bar{c}^T = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},$$

och mottagaren vet inte om felet uppstått i position nummer ett eller fyra.

10. (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.

Lösning: F är en delkropp till K om F med samma operationer som i K utgör en kropp och om varje element i F också är ett element i K.

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

Lösning: Multiplikativa gruppen till en kropp med åtta element består av sju element. Om F_4 skulle vara en delkropp till en kropp med åtta element skulle dess multiplikativa grupp vara en delgrupp till multiplikativa gruppen till kroppen med åtta element. Multiplikativa gruppen till en kropp med 8 element består av sju element och kroppen med fyra element har en multiplikativ grupp med tre element. Enligt Lagranges sats, skulle då antalet element i denna multiplikativa grupp, dvs talet 3, dela talet 7. Detta är ju omöjligt.

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

Lösning: Vi behöver ett irreducibelt polynom av grad två i polynomringen $F_4[x]$. För att underlätta sökandet skriver vi upp multiplikationstabellen för den multiplikativa gruppen i F_4:

$\cdot$	1	i	$i+1$
1	1	i	$i+1$
i	i	$i+1$	1
$i+1$	$i+1$	1	i

Vi finner att polynomet $p(z) = z(z+1)$ antar följande värden

$$p(0) = 0, \quad p(1) = 0, \quad p(i) = 1, \quad p(i+1) = 1.$$

Polynomet $q(z) = p(z) + i$ har då inget nollställe eftersom

$$q(0) = 0 + i, \quad q(1) = 0 + i, \quad q(i) = 1 + i, \quad q(i+1) = 1 + i.$$

Den sökta kroppen består alltså av elementen i mängden

$$F_{16} = \{\alpha_0 + \alpha_1\tau \mid \alpha_0, \alpha_1 \in F_4\},$$

och där man räknar som om $\tau(\tau+1) + i = 0$, dvs som om

$$\tau^2 = \tau + i,$$

eftersom vi använder oss av det irreducibla polynomet $q(z) = z^2 + z + i$ vid konstruktionen av kroppen F_{16}.