Lösningar till tentamensskrivning i Diskret matematik, SF1630 och SF1631, moment B, för F och D, den 18 augusti 2010

1. Observerar först att primtalsfaktoriseringen av 143 är $143 = 11 \cdot 13$. Söker då d sådant att
$$e \cdot d \equiv 1 \pmod{(11-1)(13-1)} .$$
Euklides algoritm ger
$$\begin{aligned} 120 &= 1 \cdot 103 + 17 \\ 103 &= 6 \cdot 17 + 1 \end{aligned}$$
så
$$1 = 103 - 6 \cdot 17 = 103 - 6(120 - 103) = 7 \cdot 103 - 6 \cdot 120,$$
varur vi sluter att
$$103 \cdot 7 \equiv 1 \pmod{120} ,$$
och alltså att $d = 7$. Svaret ges nu av $D(3) = 3^7 \pmod{143}$. Vi får
$$3^7 \equiv_{143} 3^5 \cdot 3^2 \equiv_{143} 100 \cdot 9 \equiv_{143} 6 \cdot 143 + 42 ,$$
så
SVAR: 42.

2. En sidoklass till en delgrupp innehåller lika många element som delgruppen den är sidoklass till. Enligt Lagranges sats saknar en grupp med 15 element delgrupper med fyra element så L_2 är inte sidoklass till någon delgrupp.
Det är lätt att kontrollera att L_3 är en cyklisk delgrupp till G:
$$L_3 =< 3 >= \{3, 3+3=6, 3+3+3=9, 3+3+3+3=12, 5 \cdot 3 = 0\} .$$
Så L_3 är sidoklassen
$$L_3 = 0 + < 3 > \ .$$
Om det funnes en delgrupp H till G sådan att $L_1 = a + H$ funnes h_1 och h_2 i H med
$$a + h_1 = 2 , \qquad a + h_2 = 6 .$$
Då skulle
$$4 = 6 - 2 = a + h_2 - (a + h_1) = h_2 - h_1 ,$$
tillhöra H, men då skulle även elementet
$$a + (h_2 + 4) = (a + h_2) + 4 = 10$$
tillhöra L_1 vilket det inte gör, så L_1 är inte en sidoklass till någon delgrupp.

3. (a) F:s multiplikativa grupp består av sju element. Ordningen av ett element delar antalet element i denna grupp, så alla element utom identiteten har ordning sju och genererar gruppen.

(b) Multiplicerar ekvationens bägge led med inversen till x och får då likheten

$$w = 1 + x^{-1} \ .$$

Eftersom $x(x^2 + x) = 1$ så är $x^{-1} = x^2 + x$ och vi får omedelbart
SVAR: $1 + x + x^2$.

4. (a) Vi tar den delgrupp som generas av elementet a^{12}, dvs

$$< a^{12} >= \{a^{12}, (a^{12})^2 = a^{24} = e\} \ .$$

(b) Enligt känd sats från läroboken har varje cyklisk grupp med n stycken element precis en delgrupp med d element för varje delare d till n. Antalet delgrupper till den givna gruppen är alltså lika med antalet delare till 24. Dessa delare är

$$1, 2, 3, 4, 6, 8, 12, 24 \ ,$$

så
SVAR: Totalt finns det 8 delgrupper till en cyklisk grupp med 24 element

5. Tetraedern har fyra hörn som vi betecknar med bokstäverna a, b, c och d. Tetraedern kan vridas, och dessa vridningar används i Burnsides lemma för att bestämma antalet färgläggningar. För hörnet a finns fyra möjliga mål, och när a blivit placerat finns tre möjligheter för hörnet b, so totalt 12 olika vridningar är möjliga. Vi gör nu en tabell över dessa vridningar och noterar också antalet F_φ av färgläggningar som lämnas oberörda av respektive vridning φ:

$\varphi \in G$	F_φ
id.	7^4
$(a)(b\ c\ d)$	7^2
$(a)(b\ d\ c)$	7^2
$(a\ b)(c\ d)$	7^2
$(a\ b\ c)(d)$	7^2
$(a\ b\ d)(c)$	7^2
$(a\ c)(b\ d)$	7^2
$(a\ c\ b)(d)$	7^2
$(a\ c\ d)(b)$	7^2
$(a\ d)(b\ c)$	7^2
$(a\ d\ c)(b)$	7^2
$(a\ d\ b)(c)$	7^2

Formeln i Burnsides lemma ger nu

SVAR:

$$\frac{1}{12}(7^4 + 11 \cdot 7^2)$$

6. (a) När ett ord rättas till ett ord i en 1-felsrättande kod, ändras värdet i en position i ordet, så om två olika ord c och c' rättas till samma ord d kan det ena erhållas ur det andra genom att c ändras i en position till ordet d varefter ytterligare en position ändras för att få c'. Totalt kan alltså c' fås från c genom att två (eller noll) positioner ändras, dvs avståndet mellan c och c' är 2 (eller noll). De två givna orden har dock det innbördes avståndet 3.

(b) Det finns bara en möjlighet för ett ord som ligger på avståndet 1 från alla tre ord, nämligen ordet 110001010.

Så vi skall bestämma en linjär 1-felsrättande kod med så många ord som möjligt och som innehåller detta ord, alternativt, en kotrollmatris av formatet $k \times 9$ med så få rader som möjligt, nio olika kolonner skilda från nollkolonnen, och med ordet 110001010 i matrisens nollrum.

Eftersom de nio kolonnerna skall vara olika måste antalet rader vara minst fyra. Vi tar nu fram en sådan matris, med lite trial and error:

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

(Det finns fler möjligheter) Antalet ord i koden blir $2^{9-4} = 32$, förutom det "givna" ordet och nollordet innehåller koden ordet 110100000.

7. Vi letar primitiva polynom bland de irreducibla 3-gradspolynomen (kroppen skall ju ha 3^3 element), har vi tur blir det första polynom vi hittar primitivt, dvs elementet x genererar kroppens multiplikativa grupp.

Testar polynomet $p(x) = x^3 + 2x + 1$ som ju är irreducibelt eftersom varken 0, 1 eller 2 är nollställen och polynomets grad är högst tre.

Eftersom multiplikativa gruppen har ordning 26 så har elementen ordning 1, 2, 13 eller 26, vilket är delarna till 26. Uppenbarligen har elementet x inte ordning 2 ty kroppen som konstrueras med hjälp av vårt polynom består av elementen

$$F_{27} = \{\ a_0 + a_1 x + a_2 x^2 \ \mid \ a_i \in Z_3\ \}\ ,$$

så x^2 och 1 är olika element i denna kropp.

Vi beräknar nu x^{13} och finner att

$$\begin{aligned} x^3 &= x + 2 \\ x^6 &= (x+2)^2 = x^2 + x + 1 \\ x^7 &= x(x^2 + x + 1) = x^3 + x^2 + x = x^2 + 2x + 2 \\ x^{13} &= (x^2 + x + 1)(x^2 + 2x + 2) = x^4 + 2x^2 + x + 2 = x(x+2) + 2x^2 + x + 2 = 2 \end{aligned}$$

Så vi hade tur vid vårt första försök ;-), och elementet x har varken ordning 1, 2, eller 13 utan enda möjligheten är att dess ordning är 26. Det polynom vi angav är då primitivt.

SVAR: T ex $p(x) = x^3 + 2x + 1$ är primitivt.

8. (a) Vi låter

$$G = (Z_2, +) \times (Z_2, +) \times (Z_2, +)\ ,$$

som ju har åtta element. Låt nu

$$H = \{(0,0,0),(1,0,0)\}\ , \quad K = \{(0,0,0),(0,1,0)\}\ , \quad L = \{(0,0,0)(1,1,0)\}\ .$$

Alla förutsättningar är uppfyllda och

$$H \cup K \cup L = \{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}\ ,$$

vilket ju är en grupp.

(b) Icketriviala delgrupper till en grupp men nio elemement innehåller precis tre element, antingen är två sådana grupper identiska eller innehåler de identiteten som det enda gemensamma elementet (enligt Langrages sats eftersom snittet av två grupper alltid är en grupp). Känt från tidigare tenta är att två delgruppers union aldrig är en delgrupp. Om i detta fall tre vore det skulle unionen innehålla identiteten och dessutom, för var och en av det tre delgrupperna, ytterligare två unika element. Totalt skulle unionen innehålla sju element, men ingen grupp med nio element har en delgrupp med sju element, enligt Lagranges sats.

9. (a) Med avseende på addition bildar elementen i en ring en abelsk grupp. Vi betecknar denna grupp $G = (\{0, a, b\}, +)$. Eftersom 3 är ett primtal är denna grupp cyklisk, och alltså, om a är gruppens generator, så är $b = a + a$.

Nu till ringens multiplikationstabell, i vilken vi kan utesluta elementet 0, eftersom $0 \cdot r = 0$ alltid skall gälla i en ring. Eftersom distributiva lagen alltid är giltig i en ring får vi nu multilikationstabellen

$\cdot$	a	$a+a$
a	$a \cdot a$	$a \cdot a + a \cdot a$
$a+a$	$a \cdot a + a \cdot a$	$a \cdot a + a \cdot a + a \cdot a + a \cdot a$

För varje element x i ringen gäller, eftersom additiva gruppen har tre element, att $x + x + x = 0$, och således att tabellen ovan kan skrivas

$\cdot$	a	$a+a$
a	$a \cdot a$	$a \cdot a + a \cdot a$
$a+a$	$a \cdot a + a \cdot a$	$a \cdot a$

Det finns nu tre fall att beakta, $a \cdot a = a$, $a \cdot a = a + a$ resp $a \cdot a = 0$. I det sista fallet får vi en ring där alla multiplikationer av element blir lika med 0. I de två första fallen ser vi i tabellan att a, resp $a + a$, då verkar som en multiplikativ "etta"$= 1$ och vi får en tabell, med $1 + 1 = 2$, som nedan

$\cdot$	1	2
1	1	2
2	2	1

dvs en ring som kan identifieras med ringen Z_3.

(b) Direkta produkter av ringar är ringar, så om vi bildar ringen

$$R = Z_3 \times Z_4 \times GF(4) \ ,$$

där $GF(4)$ är en ändlig kropp med fyra element, så har vi en ring med 48 element med delringarna

$$S = \{0\} \times Z_4 \times \{0\} \ , \qquad S' = \{0\} \times \{0\} \times GF(4) \ .$$

Låter vi nu $R' = R$ får vi ett positivt svar på frågan i denna uppgift.

10. (a) Eftersom en kropp med fyra element är en delkropp så är kroppens karakteristik lika med 2. En kropp med karakteristiken 2 och i vilken $z^7 - 1$ kan faktoriseras i förstagradsfaktorer är F_{64} eftersom dess multiplikativa grupp består av de 63 elementen

$$(F_{64} \setminus 0, \cdot) = \{\alpha, \alpha^2, \alpha^3, \ldots \alpha^{63} = 1\} \ ,$$

och det gäller att

$$(\alpha^{9k})^7 = 1 \ , \qquad k = 1, 2, \ldots, 7 \ ,$$

så ovanstående sju olika element är nollställen till polynomet $z^7 - 1$ och vi har då, enligt faktorsatsen, att

$$z^7 - 1 = \Pi_{i=1}^{7}(z - \alpha^{9i}) \ .$$

Vi letar nu rötter till ekvationen $z^7 = 1$ i mindre kroppar med karakteristiken 2, dvs element vars sjundepotenser blir lika med 1. Dessa mindre kroppar har multiplikativa grupper med 31, 15, 7 resp 3 element, och då skulle den enda möjliga kropp med element skilda från 1 som rötter till $z^7 = 1$ vara kroppen med 8 element, men den har ingen delkropp med fyra element. Skulle vi ha en faktorisering i förstagradsfaktorer, skulle, eftersom 1 är den enda roten till $z^7 = 1$ i dessa kroppar med färre än 64 element, vi ha att $z^7 - 1$ skulle ha faktoriseringen

$$(z - 1)^7 \ ,$$

som ju inte alls är lika med $z^7 - 1$.

SVAR: Kroppen med 64 element.

(b) Vi observerar först, enligt binomialsatsen, eller med direkta räkningar modulo 2, att

$$(z - 1)^{16} = z^{16} - 1 \ ,$$

och alltså kan $z^{16} - 1$ faktoriseras i förstagradsfaktorer i varje kropp med karakteristiken 2. Likaledes

$$z^{14} - 1 = (z^7 - 1)(z^7 - 1) \ ,$$

så om $z^7 - 1$ kan faktoriseras i förstagradsfaktorer så kan även $z^{14} - 1$ det. Om w satisfierar ekvationen $z^{14} = 1$ så kommer w^2 att satisfiera ekvationen $z^7 = 1$. Resonerar vi nu analogt med hur vi resonerade i uppgift (a) finner vi att i ingen mindre kropp än den med 64 element, innehålande en delkropp med fyra element, kan $z^{14} - 1$ faktoriseras i förstagradsfaktorer. Så även i detta fall har vi

SVAR: Den minsta kroppen med de givna egenskaperna är kroppen med 64 element.