Övningssamling i Diskret Matematik

av Johan Karlander, överfört till LaTeX av Max Zomborszki
Med reservation för felaktigheter.
Eventuella fel och korrigeringar rapporteras till Max Zomborszki <max@e.kth.se>.

Innehåll

1 Uppgifter

1.1 Grundläggande talteori

1. Om p, q är primtal ≥ 3, kan då $pq + 3$ vara ett primtal?

2. Bestäm största gemensamma delare till

   (a) 54 och 40

   (b) 245 och 70

   (c) 1197 och 783

   (d) 865 och 161

   (e) 10879 och 3179

3. Bestäm minsta gemensamma multipel till

   (a) 27 och 21

   (b) 11 och 7

   (c) 36 och 4

   (d) 180 och 48

   (e) 48 och 30

4. Bestäm villkor på a och b så att

   (a) $\text{SGD}(a, b) = \text{MGM}(a, b)$

   (b) $\text{MGM}(a, b) = 2 \cdot \text{SGD}(a, b)$

   (c) $\text{MGM}(a, b)$ är ett primtal

5. Bestäm $\text{SGD}(389, 167)$ och skriv den på formen $389m + 167n$.

6. Antag att vi vill föra över vatten från en tank A till en tank B. Antag att vi har två spannar S_1 och S_2. S_1 rymmer 10 liter och S_2 rymmer 6 liter. Vilken är den minsta exakta mängd vatten större än noll som du med hjälp av S_1 och S_2 kan hälla upp i B?

7. Hitta tal p, q och r så att $12p + 9q + 14r = 1$. Går det att hitta p, q och r så att $12p + 9q + 15r = 1$?

8. Visa att

   (a) $n^2 + 3n$ är delbart med 2 för alla $n \geq 0$

   (b) $n^3 + 3n^2 - 4n$ är delbart med 6 för alla $n \geq 0$

   (c) $n^4 + 2n^3 + 11n^2 + 2n$ är delbart med 4 för alla $n \geq 0$

   (d) $4^{2n} - 1$ är delbart med 15 för alla $n \geq 1$

9. Antag att M är en mängd heltal sådan att om $a \in M$ och $b \in M$ så gäller $a + b \in M$. Antag vidare att för varje $a \in M$ gäller att $5|a$ eller $7|b$ eller båda. Visa att då måste det gälla att 5 delar alla tal i M eller 7 delar alla tal i M eller båda.

10. (a) Vad är det minsta värde > 0 som $\frac{a}{47} + \frac{b}{53}$ kan få om a och b är heltal?

    (b) Mer generellt: Om m och n är positiva heltal, vad är då det minsta värde som $\frac{a}{m} + \frac{b}{n}$ kan få om a och b är heltal?

11. Vi betraktar mängden av tal som kan skrivas som $5a + 4b$ där a och b är heltal ≥ 0. Alla tal går inte att skriva på den formen. Men det finns ett största tal k_0 som inte kan skrivas på den formen (ochalla större tal ka skrivas på formen). Vad är k_0? Förklara varför k_0 är det största talet.

12. Antag att m och n är positiva tal med $\text{SGD}(m, n) = 1$. Visa då att det bara finns ändligt många positiva heltal som inte går att skriva som $ma + nb$ med a, b positiva heltal.

13. Låt p_1, p_2, p_3, p_4 och p_5 vara 5 primtal. Antag att $m = {p_1}^3{p_2}^1{p_3}^0{p_4}^5{p_5}^6$ och $n = {p_1}^1{p_2}^1{p_3}^2{p_4}^0{p_5}^4$. Vad är $\text{SGD}(m, n)$ och $\text{MGM}(m, n)$?
Mer generellt: Om $m = {p_1}^{e_1}{p_2}^{e_2} \dots {p_k}^{e_k}$ och $n = {p_1}^{f_1}{p_2}^{f_2} \dots {p_k}^{f_k}$ vad är då $\text{SGD}(m, n)$ och $\text{MGM}(m, n)$?

14. Visa att om m, n och k är positiva heltal sådana att $m^2 = kn^2$ så är $k = a^2$ där a är ett positivt heltal. Använd resultatet för att visa att $\sqrt{K}$ måste vara irrationellt eller ett heltal för alla heltal K.

15. Måste de reella lösningarna till ekvationen $x^7 - 14x^6 + 4x^5 - 2x^4 + 3x^3 + 8x^2 + 7x + 5 = 0$ vara heltal eller irrationella eller kan det finnas rationella lösningar som inte är heltal?

16. Är $\log_{10} 2$ ett rationellt tal?

17. Et tal kallas för kvadratfritt om varje primtal i dess primtalsfaktorisering förekommer med grad högst 1. T ex är 14 och 15 kvadratfria medan 9 och 12 inte är det. Vilka av följande påståenden är sanna och varför?

    (a) a, b är kvadratfria $\implies \text{MGM}(a, b)$ är kvadratfri

    (b) $\text{MGM}(a, b)$ är kvadratfri $\implies a$, b är kvadratfria

    (c) a, b är kvadratfria $\implies \text{SGD}(a, b)$ är kvadratfri

    (d) $\text{SGD}(a, b)$ är kvadratfri $\implies a$, b är kvadratfria

1.2 Funktioner och kardinalitet

1. Låt funktionerna $f : \mathbb{Z} \to \mathbb{Z}$ och $g : \mathbb{Z} \to \mathbb{Z}$ vara definierade av $f(n) = n - 1$ och $g(n) = 3n$. Visa att $fg \neq gf$.

2. Är $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^3$ surjektiv, injektiv, bijektiv?

3. (a) För vilka värden på a och b är $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = ax + b$ en bijektion?

   (b) Samma fråga för $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = ax + b$.

4. Visa att om man har $n + 1$ stycken olika heltal x_1, x_2, …, x_{n+1} så finns det två av dem, kalla dem x_i och x_j sådana att $n | x_i - x_j$.

5. Låt X vara en delmängd av $\{1, 2, \dots, 2n\}$ och låt $Y = \{1, 3, 5, 7, \dots, 2n - 1\}$. Visa att om $|X| \geq n + 1$ så finns det två olika tal x_1 och x_2 så i X så att $x_1 | x_2$.

6. (a) Ange en delmängd X av $\{1, 2, \dots, 2n\}$ med $|X| = n$ som är sådan att inga tal i X delar varandra.

   (b) Använd resultatet från uppgift 5 och 6a för att visa att om $A = \{101, 102, 103, \dots, 200\}$ så finns det för varje val av två tal $a, b \in A$ ett udda tal m som bara delar ett av talen a och b.

7. Visa att funktionen $f : \mathbb{N} \to \mathbb{Z}$ definierad av.

$$f(n) = \begin{cases} \frac{n}{2} & \text{om } n \text{ är jämnt} \\ -\frac{n-2}{2} & \text{om } n \text{ är udda} \end{cases}$$

är en bijektion.

8. Visa att det finns oändligt många primtal.

9. (a) Visa att det finns oändligt många primtal på formen $4n + 3$. (Studera produkter av typen $4 \cdot p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m - 1$ och jämför med uppgift 8.

   (b) Förklara varför samma metod som i uppgift a med produkter av typen $4 \cdot p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m + 1$ *inte* duger för att visa att det finns oändligt många primtal på formen $4n + 1$.

10. Om tio punkter väljs i en kvadrat med sidan 1 så måste minst två ha ett avstånd mindre än eller lika med $\frac{\sqrt{2}}{3}$. Förklara varför.

11. Om M är en mängd så betecknar $P(M)$ mängden av alla delmängder till M. (Så om $M = \{1, 2\}$ så är $P(M) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$)
Visa att det inte kan finnas någon bijektion $f : M \to P(M)$. (Om M är ändlig är det ganska lätt att visa. Om M är oändlig är det mycket knepigt utan ledning.)

12. $\mathbb{N}^2$ består av alla talpar (0,0), (0,1), (0, 2), ..., (1, 0), (1, 1), (1, 2), ... Avgör om $f : \mathbb{N}^2 \to \mathbb{N}$ definierad av $f(a, b) = \frac{1}{2}(a+b)(a+b+1)+b$ är en bijektion mellan $\mathbb{N}^2$ och $\mathbb{N}$ eller inte.

1.3 Partitioner, multinomialkoefficienter och Sterlingtal

1. $P_k(n)$ betyder antalet sätt att dela upp n i en summa av exakt k termer. Beräkna $P_1(7), P_2(7), \ldots, P_7(7)$.

2. Vad finns det för samband mellan $P(n)$ och talen $P_1(n), P_2(7), \ldots$?

3. Visa att $P_k(n) = P_1(n-k) + P_2(n-k) + \ldots + P_k(n-k)$

4. Visa att $\binom{n}{a,b,c} = \binom{n-1}{a-1,b,c} + \binom{n-1}{a,b-1,c} + \binom{n-1}{a,b,c-1}$

5. Uttrycket $\frac{1}{k!}\Sigma\binom{n}{n_1,n_2,\ldots,n_k}$ där summationen görs över alla val av tal $n_1, n_2, \ldots, n_k$, alla större än 0, så att $n_1 + n_2 + \ldots + n_k = n$, kan skrivas på en enklare form. Vilken?

6. Vi har 10 kulor som är numrerade 1, 2, ..., 10. Vi har också 5 lådor. Kulorna ska fördelas i lådorna.

   (a) På hur många sätt kan kulorna fördelas om lådorna är särskiljbara?

   (b) Samma fråga som i a fast lådorna är inte särskiljbara.

   (c) Samma fråga som i a fast kulorna är inte särskiljbara.

   (d) Samma fråga som i a fast varken kulor eller lådor är särskiljbara.

   I samtliga fall förutsätts att lådor kan vara tomma.

1.4 Modulär aritmetik

1. Visa att om a är ett udda heltal så gäller $a^2 \equiv 1(mod\ 8)$. Visa också att om a är jämnt men $a/2$ är udda så gäller $a^2 \equiv 4(mod\ 8)$.

2. Beräkna inversen till alla tal $x : 1 \leq x \leq 16$ modulo 17.

3. Låt oss anta att vi vill beräkna resten vid division av x och n . Antag att x i decimalform ser ut som $x_k x_{k-1} \ldots x_1 x_0$ där $0 \geq x_i \geq 9$. Det betyder att $x = x_k \cdot 10^k + x_{k-1} \cdot 10^{k-1} \cdot \ldots \cdot x_1 \cdot 10 + x_0$.

   (a) Om $n = 3$ så gäller $x \equiv x_k + x_{k-1} + \ldots + x_1 + x_0(mod\ 3)$. Visa detta.

   (b) Om $n = 11$ så gäller $x \equiv (-1)^k x_k + (-1)^{k-1} x_{k-1} + \ldots + (-1)x_1 + x_0(mod\ 11)$

   (c) För varje n går det att ställa upp en regel på formen $x \equiv a_k x_k + a_{k-1} x_{k-1} + \ldots + a_1 x_1 + a_0 x_0(mod\ n)$. Kan du ange hur a_i-talen skall se ut?

4. Med hjälp av metoden i uppgift 3 ser vi att x är delbart med 3 omm $x_k + x_{k-1} + \ldots + x_1 + x_0$ är delbart med 3. Konstruera liknande delbarhetsregler för $n = 2$, 4, 5, 6, 7, 8, 9. Går regeln för $n = 6$ att uttrycka på ett annat sätt?

5. För vanliga bråk gäller $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ och $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
   Avgör om detta också är sant om vi räknar i $\mathbb{Z}_m$. ($\frac{1}{k}$ betyder k^{-1} i de fall då k^{-1} existerar).

6. Hur många lösningar till ekvationen $x^{-1} = x$ finns det i $\mathbb{Z}_p$ om p är ett primtal $\geq$ 3?

7. Beräkna produkten av alla nollskilda element i $\mathbb{Z}_p$ och visa med hjälp av den att $(p-1)! \equiv -1(mod\ p)$.

8. Visa "omvändningen" till uppgift 7: Om $(n-1)! \equiv -1(mod\ n)$ så är n ett primtal.

9. Lös följande ekvationer:

   (a) $x^2 + x + 1 = 0$ i $\mathbb{Z}_7$

   (b) $x^2 + 9x + 9 = 0$ i $\mathbb{Z}_{11}$

   (c) $x^2 + 7x + 2 = 0$ i $\mathbb{Z}_{13}$

10. För vilka tal k i $\mathbb{Z}_{17}$ existerar $\sqrt{k}$?

11. Försök generalisera resultatet i uppgift 10 och tag reda på för hur många tal k i $\mathbb{Z}_p$ som $\sqrt{k}$ existerar.

1.5 Gruppteori

1. Låt $\mathcal{M}$ vara mängden av 2×2-matriser $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ med $a, b, c, d \in \mathbb{Z}$ och $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. Är $\mathcal{M}$ en grupp under multiplikation?

2. $\mathbb{Z}_n$ är en grupp under addition. Låt A vara en delmängd av $\mathbb{Z}_n$.

   (a) Förklara varför det är så att om A är en delgrupp och $a \in A$ och $b \in B$ så måste $\mathrm{SGD}(a, b) \in A$.

(b) Förklara sedan varför det är så att om A är en delgrupp och d är det minsta talet i A förutom 0 så måste $d|a$ för alla $a \in A$.

(c) Om A är en delgrupp och d är det minsta talet i A förutom 0 så måste $d|n$. Visa detta.

(d) Visa omvändningen till a, b och c: att om A består av alla multiplar av d och $d|n$ så är A en delgrupp.

3. Bestäm samtliga delgrupper till $\mathbb{Z}_{20}$. (Använd uppgift 2)

4. Givet 2 reella tal x, y definierar vi operationen $\circ$ genom att sätta $x \circ y = \max(x, y)$ dvs det största talet av x och y. Är $\circ$ associativ?

5. Antag att G är en grupp med 300 element. Det finns ett tal n förutom 0 så att $a^n = 1$ för alla $a \in G$ (oberoende av filken grupp G är). Vad är n?

6. Antag att $a, b \in G$ och att G är en grupp.

   (a) Visa att inversen till ab är $b^{-1}a^{-1}$.

   (b) Visa att $ab = 1 \Rightarrow ba = 1$

   (c) Vosa att $(ab)^2 = a^2b^2 \Rightarrow ab = ba$

7. Antag att G är en grupp med egenskapen att $g^2 = 1$ för alla element g i G. Då måste G vara kommutativ. Förklara varför.

8. Antag att H och K är delgrupper till en grupp G. Är $H \cap K$ nödvändigtvis också en delgrupp? Är $H \cup K$ det?

9. Antag att g är ett element med ordningen m i G. Då är $A = \{g^0, g^1, \ldots, g^{m-1}\}$ en delgrupp av G. Verifiera att det är så.

1.6 Ringar

1. Låt $A = \{(a, b, c, d) : a, b, c, d \in \mathbb{R}\}$. Vi definierar två operationer $\oplus$ och $\odot$ genom:
   $(a, b, c, d) \oplus (e, f, g, h) = (a + e, b + fmc + g, d + h)$
   $(a, b, c, d) \odot (e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$
   Avgör om A med operationerna $\oplus$ och $\odot$ bildar en ring. Är ringen i så fall kommutativ? Finns multiplikativ enhet? Vilka element i A är inverterbara?

2. Låt A vara en ring sådan att $a^2 = a$ för alla $a \in A$ (En sådan ring kallas för en Boolesk ring).

   (a) Visa att i en sådan ring gäller $a + a = 0$ för alla a.

   (b) Visa också att en sådan ring är kommutativ.

   (c) Förenkling av algebraiska uttryck är enkelt i en Boolesk ring. Vad kan tex $a^7b^5 + c^{-5}(a^7b^{18} + b2a^6) + c^2a^{13}b^{17}c^{-3}$ förenklas till?

   (d) Vilka, om någon, av ringarna $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \ldots$ är Boolesk?

3. Om R är en ring och $x \in R$ så säger man att x är *nilpotent* om $x^n = 0$ för något n. Nilpotenta element har vissa speciella egenskaper:

   (a) Visa att x inte är inverterbart.

(b) $1+x$ går däremot att invertera. Inversen är $1-x+x^2-x^3+\ldots+(-1)^{n-1}x^{n-1}$. Verifiera det.

(c) Vilka är det nilpotenta elementen, om det finns några, i $\mathbb{Z}_{20}$?

(d) Det finns en regel som lyder: $\mathbb{Z}_k$ har nilpotenta element (förutom 0) om och endast om .... Vad ska det stå på ... ?

4. Visa att matrisen $\mathcal{M} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$ är nilpotent. Använd sedan formeln i 3b för att beräkna inversen till $\mathcal{M}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}$.

5. Antalet inverterbara element i olika ringar kan variera. Men 0 kan aldrig vara inverterbart. Antag att vi skulle ha ett element α så att $0 \cdot \alpha = \alpha \cdot 0 = 1$. Varför är det omöjligt?

6. Ge ett noggrant bevis för att $(-x)y = (-xy)$ och för att $(-x)(-y) = xy$. Ange exakt vilka gruppaxiom som används.

7. Beskriv strukturen av $\mathcal{U}(\mathbb{Z}_{10})$, $\mathcal{U}(\mathbb{Z}_{11})$ och $\mathcal{U}(\mathbb{Z}_{12})$.

8. Γ är mängden av komplexa tal $m+ni$ där m, n är heltal. Visa att Γ är en ring. Vad är $\mathcal{U}(\Gamma)$ (dvs beskriv strukturen).

9. En ring R är kommutativ om och endast om $(a+b)(a-b) = a^2 - b^2$ för alla $a, b \in R$. Visa att det är så.

1.7 Polynom

1. Vad är nollställena till följande ekvationer i $\mathbb{Z}_8$?

   (a) $(x+6)^3$

   (b) $(x+1)(x+5)$

2. Antag att F är en kropp och att $p(x)$ är ett n-tegradspolynom i $F(x)$. Antag också att $p(x)$ har n olika nollställen $\alpha_1, \alpha_2, \ldots, \alpha_n$ i F. Visa att då måste konstanta termen i $p(x)$ vara $(-1)^n \alpha_1 \alpha_2 \cdot \ldots \cdot \alpha_n$.

3. Derivatan Df av ett polynom beräknas på vanligt sätt även om man inte räknar med reella tal. Det betyder att $D(x^3+7x^2+2x+3) = 3x^2+14x+2$. Men om man räknar i tex $\mathbb{Z}_p[x]$ kan vissa nya fenomen uppträda:

   (a) Ge exempel på polynom $p(x)$ i $\mathbb{Z}_{11}[x]$ sådana att $Dp(x) = 0$ fast $p(x)$ inte är en konstant.

   (b) Givet ett primtal p och $\mathbb{Z}_p[x]$, kan du beskriva exakt hur $f(x)$ skall vara för att $Df(x) = 0$?

4. Antag att $p_1(x)$ och $p_2(x)$ är polynom i $\mathbb{R}[x]$ med grad $m \geq 2$ och grad $n \geq 2$.

   (a) Antag att $\mathrm{SGD}(p_1(x), p_2(x))$ är ett polynom av grad ≥ 1. Då går det att hitta polynom $q_1(x), q_2(x)$ av grad högst $n-1$ respektive $m-1$ så att $(p_1(x)q_1(x) = p_2(x)q_2(x)$. Förklara varför genom att tala om hur q_1 och q_2 kan väljas.

(b) Antag sedan att $\text{SGD}(p_1(x), p_2(x)) = 1$. Visa att då går det inte att hitta polynom $q_1(x)$ och $q_2(x)$ som uppfyller villkoren i a.

5. Vad är resten då $a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$ delas med $x - b$?

6. Beräkna kvot och rest vid division av

   (a) $x^3 + x^2 + 1$ med $x^2 + x + 1$ i $\mathbb{Z}_2[x]$

   (b) $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ med $x^2 + 2x + 3$ i $\mathbb{Z}_5[x]$

7. Bestäm en monisk SGD till $a(x)$ och $b(x)$ och skriv den på formen $f(x)a(x) + g(x)b(x)$ för:

   (a) $x^5 + x^3 + x^2 + 1$ och $x^4 + x^3 + x + 1$ i $\mathbb{Z}_2[x]$

   (b) $x^4 + 2x^2 + 2x + 2$ och $2x^4 + 2x^3 + 2x^2 + x + 2$ i $\mathbb{Z}_3[x]$

   (c) $x^4 + 2x^3 + 3x^2 + 3$ och $x^4 + 4x + 2$ i $\mathbb{Z}_5[x]$

8. Bestäm alla irreducibla faktorer till

   (a) $x^2 + 1$ i $\mathbb{Z}_5[x]$

   (b) $x^3 + 5x^2 + 5$ i $\mathbb{Z}_{11}[x]$

   (c) $x^4 + 3x^3 + x + 1$ i $\mathbb{Z}_5[x]$

9. Bestäm alla moniska irreducibla 2-gradspolynom i $\mathbb{Z}_3[x]$.

1.8 Felrättande koder

1. Låt C vara en binär kod av längd n (inte nödvändigtvis linjär) som rättar max e fel. Visa att C upptäcker åtminstone $2e$ fel. Det går att utvidga C till en kod C' med längd $n + 1$ som upptäcker $2e + 1$ fel. Utvidgningen fås genom att man lägger till en extra binär siffra till varje ord. Kan du föreslå hur den sista siffran skall väljas?

2. Bestäm parametrarna (n, k, δ) för den linjära koden med kontrollmatris

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

3. Tag samma kod som i uppgift 2. Avgör vilka av följande ord som är kodord och om de inte är kodord, rätta dem under antagandet att endast ett fel har uppstått.

   (a) 11111

   (b) 01101

   (c) 01100

4. Skriv upp en kontrollmatris för den linjära kod som består av alla ord av längd 7 med jämn vikt.

5. Visa att det inte finns någon kod C av längd 5 med $\delta = 3$ och $|C| = 6$.

6. Bevisa "triangelolikheten" $\delta(x, y) \leq \delta(x, z) \leq \delta(z, y)$ för Hammingmetriken.

7. Vad är den maximala dimensionen för en linjär kod av längd 8 som rättar 2 fel? Konstruera en sådan kod.

8. Låt C vara en linjär kod. Låt C_0 vara mängden av kodord i C med jämn vikt. Visa att C_0 är en kod. Antag sedan att C_0 är en äkta delmängd av C. Om C innehåller n ord, hur många ord innehåller då C_0?

9. Ange alla kodord i koden med kontrollmatrisen

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

   Vad är parametrarna n, k och δ?

10. Konstruera en kod som kan sända 256 olika meddelanden och rätta 1 fel. Välj koden så att längden blir så liten som möjligt. (Det räcker att ange kontrollmatrisen för koden).

2 Svar

2.1 Grundläggande talteori

1. Nej
2. (a) 2
   (b) 35
   (c) 9
   (d) 1
   (e) 11
3. (a) 189
   (b) 77
   (c) 4
   (d) 720
   (e) 720
4. (a) $a = b$
   (b) $a = 2b$ eller $b = 2a$
   (c) ($a = p$ och $b = 1$) eller ($a = 1$ och $b = p$) eller ($a = b = p$) där p är ett primtal
5. $\text{SGD}(389, 167) = 1 = 389 \cdot\ 82 - 167 \cdot\ 191$
6. 2 liter
7. Tex $1 = 12 \cdot\ 5 + 9 \cdot\ (-5) + 14 \cdot\ (-1)$. Nej
8.
9.
10. (a) $\frac{1}{2491}$
    (b) $\frac{1}{\text{MGM}_{(a,b)}}$
11. $k_0 = 11$
12.
13. $\text{SGD} = {p_1}{p_2}{p_5}^4$, $\text{MGM} = {p_1}^3{p_2}{p_3}^2{p_4}^5{p_5}^6$
14.
15. Lösningarna måste vara heltal eller irrationella
16. Nej
17. 1, 2 och 3 är sanna

2.2 Funktioner och kardinalitet

1.
2. Injektiv, men inte surjektiv eller bijektiv.
3. (a) $a = \pm 1$, b godtyckligt
   (b) $a \neq 0$, b godtyckligt
4.
5.
6. (a) $X = \{n+1, n+2, n+3, \ldots, 2n\}$
7.
8.
9.
10.
11.
12. Det är en bijektion.

2.3 Partitioner, multinomialkoefficienter och Sterlingtal

1. $P_1(7) = 1$, $P_2(7) = 3$, $P_3(7) = 4$, $P_4(7) = 3$, $P_5(7) = 2$, $P_6(7) = 1$ och $P_7(7) = 1$.
2. $P_n = P_1(n) + P_2(n) + \ldots + P_n(n)$
3.
4.
5. $S(n, k)$
6. (a) 5^{10}
   (b) $S(10,5) + S(10,4) + S(10,3) + S(10,2) + S(10,1)$
   (c) $\binom{14}{10}$ eller $\binom{14}{4}$
   (d) $P(10)$

2.4 Modulär aritmetik

1.
2. Inverserna är i turo och ordning 1, 9, 6, 13, 7, 3, 5, 15, 2, 12, 14, 10, 4, 11, 8 och 16.
3. (a)
   (b)
   (c) $a_i \equiv 10^i (mod\ n)$
4.

5. Det är sant i $\mathbb{Z}_m$.
6. 2 st.
7.
8.
9. (a) $x_1 = 4, x_2 = 2$
   (b) $x_1 = 6, x_2 = 7$
   (c) Lösning saknas
10. 0, 1, 2, 4, 8, 9, 13, 15, 16.
11. $\frac{p+1}{2}$ st.

2.5 Gruppteori

1. $\mathcal{M}$ är en grupp.
2.
3. Delgrupperna har formen $\{n : d|n\}$ där $d = 1, 2, 4, 5, 10$.
4. $\circ$ är associativ.
5. Det finns det $n = 300$.
6.
7.
8. $H \cap K$ är alltid en delgrupp. $H \cup K$ är inte det (utom i specialfall).
9.

2.6 Ringar

1. A är en icke-kommutativ ring. $(1, 0, 0, 1)$ är multiplikativ enhet. (a, b, c, d) är inverterbar omm $ad - bc = 1$.
2. (a)
   (b)
   (c) 0
   (d) $\mathbb{Z}_2$ är Boolesk. Ingen annan $\mathbb{Z}_n$-ring är det.
3. (a)
   (b)
   (c) 10 är nilpotent
   (d) "k innehåller en faktor p^m där $m > 1$"
4. Inversen är $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ -2 & 0 & 1 \end{pmatrix}$.

5.

6.

7. $\mathcal{U}(\mathbb{Z}_{10})$ består av $\{1,3,7,9\}$, $\mathcal{U}(\mathbb{Z}_{11})$ består av $\{1,2,3,4,5,6,7,8,9,10\}$ och $\mathcal{U}(\mathbb{Z}_{12})$ består av $\{1,5,7,11\}$.

8. $\mathcal{U}(\Gamma)$ består av $\{1,-1,i,-i\}$

9.

2.7 Polynom

1. (a) 0,2,4,6
   (b) 1,3,5,7

2.

3. (a) tex $p(x) = x^{11}$
   (b) $f(x)$ skall ha formen $f(x) = g(x^p)$

4. (a)
   (b)

5. $r = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$

6. (a) Kvot $= x$ Rest $= x + 1$
   (b) Kvot $= x^3 + 4x^2$ Rest $= 2x + 1$

7. (a) $x^4 + x^3 + x + 1$ (Som helt enkelt är det ena polynomet)
   (b) $x^3 + 2x^2 + 2 = 1 \cdot (x^4 + 2x^2 + 2x + 2) + 2 \cdot (2x^4 + 2x^3 + 2x^2 + x + 2)$
   (c) $x + 2 = (3x^2 + 2x + 3)(x^4 + 2x^3 + 3x^2 + 3) + (2x^2 + 2x + 4)(x^4 + 4x + 2)$

8. (a) $(x + 2)$ och $(x + 3)$
   (b) $(x + 8), (x + 9)$ och $(x + 10)$
   (c) $(x^2 + 2)$ och $(x^2 + 3x + 3)$

9. $x^2 + 1, x^2 + x + 2$ och $x^2 + 2x + 2$

2.8 Felrättande koder

1.

2. $n = 5, k = 2\delta = 3$

3. (a) Inte kodord. Rätt ord är 11110.
   (b) Kodord.
   (c) Inte kodord. Rätt ord är 01101.

4. $H = (1111111)$

5.

6.

7. Största dimension är 2. $\{(00000000), (11111000), (00011111), (11100111)\}$

8. $|C_0| = \frac{1}{2} \cdot |C|$

9. $\{(0000000), (1111001), (1110010), (0001011), (1010100), (0101101), (0100110), (1011111)\}$
   $n = 7, k = 3, \delta = 3$

10. $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$

    Fler lösningar finns.

3 Ledningar

3.1 Grundläggande talteori

1. Det finns ett tal som delar $pq + 3$
2. Använd Euklides algoritm
3. Beräkna först SGD
4. Använd beteckningarna $\text{SGD}(a, b) = d$, $a = a'd$, $b = b'd$. Då gäller $\text{MGM}(a, b) = a'b'd$
5. Euklides algoritm
6. Euklides algoritm
7. Bestäm SGD till 12, 9, 14
8. (a) $n^2 + 3n = n(n + 3)$
   (b) $n^3 + 3n^2 - 4n = n((n^2 + 3n) - 4)$. Använd deluppgift a för att visa att detta är delbart med 2. Visa sedan att $n^3 + 3n^2 - 4n$ är delbart med 3.
   (c) $2n^3 + 2n = 2n(n^2 + 1)$. Visa att detta är delbart med 4.
   $n^4 + 11n^2 = n^2(n^2 + 11)$. Visa att detta är delbart med 4.
   (d) $4^{2n} - 1 = 16^n - 1 = (15 + 1)^n - 1$. Visa att detta är delbart med 15
9. Kan det finnas $n_1, n_2 \in M$ så att $n_1|5$, $n_1 \not| 7$, $n_2|7$ och $n_2 \not| 7$?
10. (a) $\frac{a}{47} + \frac{b}{53} = \frac{53a+47b}{47 \cdot 53}$. Vad är det minsta värdet på täljaren?
    (b) Samma metod som i a.
11. $5 - 4 = 1$
12. Samma metod som i 11.
13. Vad är villkoret uttryckt i p_1, p_2, p_3, p_4, p_5 för att ett tal skall dela m och n?
14. Antag att p_1, p_2, ..., p_s är de primtal som förekommer i m, n och k. Antag att $m = {p_1}^{e_1}{p_2}^{e_2} \dots {p_s}^{e_s}$, $n = {p_1}^{f_1}{p_2}^{f_2} \dots {p_s}^{f_s}$ och $k = {p_1}^{g_1}{p_2}^{g_2} \dots {p_s}^{g_s}$. Använd aritmetikens fundamentalsats.
15. Gör ansatsen $x = \frac{m}{n}$. Sätt in i ekvationen och se vad som händer.
16. Gör ansatsen $x = \frac{m}{n}$. Tag båda led exponentierade.
17. Antag att $a = {p_1}^{e_1}{p_2}^{e_2} \dots {p_k}^{e_k}$ och $b = {p_1}^{f_1}{p_2}^{f_2} \dots {p_k}^{f_k}$.

3.2 Funktioner och kardinalitet

1.
2.
3.
4. Låt $f(x)$ vara resten vid division av x med n. Visa att det finns x_i, x_j så att $f(x_i) = f(x_j)$.

5. Låt $f(x)$ vara det största udda heltal som delar x. $f : \{1, 2, \ldots, 2n\} \to Y$. Visa med hjälp av lådprincipen att det finns x_1, x_2 så att $f(x_1) = f(x_2)$. Visa sedan att $x_1 | x_2$ eller $x_2 | x_1$.

6. (a)

   (b) Använd funktionen f från lösningen till uppgift 5.

7. Konstruera en invers $g(x) = n$ genom att lösa ut n ur $x = f(n)$.

8. Antag att $p_1, p_2, \ldots, p_m$ är alla primtal. Sätt $N = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$. Är N primtal? Är N sammansatt?

9. (a)

   (b) Om $n \equiv 1 \ (mod\ 4)$ och $p|n$, måste då $p \equiv 1 \ (mod\ 4)$?

10. Dela upp kvadraten i 9 delkvadrater.

11. Antag att det finns en bijektion $f : M \to P(M)$. Låt $A = \{a \in M : a \notin f(a)\}$. Om f är en bijektion så finns ett x så att $f(x) = A$. Gäller $x \in f(x)$ eller $x \notin f(x)$? Försök hitta en motsägelse.

12. Ordna upp paren i $\mathbb{N}^2$ i ordningen (0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (3,1), (2,2), (1,3), (0,3), osv. Kalla det första paret för par nummer 0. På vilken plats kommer (a, b)?

3.3 Partitioner, multinomialkoefficienter och Sterlingtal

1. Pröva alla möjliga partitioner.

2. En partition består av en term, två termer eller ...

3. Givet en partition av n i k termer så kan man minska varje term med 1. Vad får man då?

4. $\binom{n}{a,b,c}$ kan tolkas som antalet sätt att placera talen 1, 2, ..., n i olika lådor. Det finns 3 olika lådor att placera talet 1 i. Vad händer sedan?

5. Tänk först efter vad $\binom{n}{n_1, n_2, \ldots, n_n}$ räknar för något. Vad händer när man dividerar med $k!$?

6. Ett av svaren innehåller en potens, ett sterlingtal, ett $p(n)$-tal och en binomialkoefficient.

3.4 Modulär aritmetik

1. Testa de möjliga värdena för $a^2 (mod\ 8)$.

2. Prövning

3. $10^k \equiv 1 (mod\ 3), 10^k \equiv (-1)^{-k} (mod\ 11)$, osv.

4. Visa att $bd \cdot (\frac{a}{b} + \frac{c}{d}) = ad + bc$, osv.

5. $x^{-1} = x \iff x^2 - 1 = 0 \iff (x - 1)(x + 1) = 0$

6. Använd resultatet från uppgift 6.

7. Antag att $n = ab$ där $1 < a < n$. Visa att a inte kan dela $(n-1)! + 1$.
8. Använd formeln $x^2 + px + q = 0 \Longrightarrow x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$
9. Beräkna x^2 för $x = 0, 1, \ldots, 16$ i $\mathbb{Z}_{17}$.
10. Om $x^2 = y^2$, vad är då sambandet mellan x och y?

3.5 Gruppteori

1. Pröva att beräkna produkter av sådana matriser. Pröva att beräkna inverser. Har inverserna heltalskoefficienter?
2. (a) $ma + nb$ måste tillhöra A
   (b) Antag att d är det minsta talet i A. Antag att $a \in A$. $a = kd + r$. Vad är r?
   (c) Samma metod som i b.
   (d) Testa slutenhet, osv.
3. Leta efter delare till 20 och använd uppgift 2.
4. Vad blir $(x \circ y) \circ z$ för något egentligen?
5. Varje element a har en ordning k. Det går att visa att $k|300$.
6. (a) Visa att $(ab)(b^{-1}a^{-1}) = 1$.
   (b) Om $ab = 1$ så måste $b = a^{-1}$.
   (c) $(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2$. "Dividera" med lämpliga element.
7. $g^2 = 1 \Rightarrow g = g^{-1}$ och detta gäller för alla element, tex $g = ab$.
8. Antag att $a, b \in H \cap K$. Då gäller att $a, b \in H$ och $a, b \in K$. Använd detta för att visa att $a, b \in H \cap K$. Gör på liknande sätt för att visa att $a^{-1} \in H \cap K$. $H \cup K$ behöver inte vara en delgrupp. Konstruera ett exempel som visar detta genom att sätta $G = \mathbb{Z}_n$ och H, K till några lämpliga delgrupper (för något val av n).
9. $x^i \cdot x^j = x^k$. Vad är k? Inte nödvändigtvis $i + j$.

3.6 Ringar

1. Översätt elementen i A till matriser enligt mönstret $(a, b, c, d) \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
2. (a) Räkna på vad $(a + a)^2$ är.
   (b) Räkna på vad $(a + b)^2$ är.
   (c) Reducera uttrycket med hjälp av reglerna $a^k = a$ och $a^{-k} = a^{-1}$ samt utnyttja att vi har kommutativitet.
   (d) Kan $1 + 1 = 0$ i $\mathbb{Z}_n$?
3. (a) Antag att $xy = 1$ och att $x^n = 0$. Multiplicera första uttrycket med x^{n-1}.
   (b) Multiplicera uttrycken och se vad som händer.
   (c) $x^n = 0$ i $\mathbb{Z}_{20}$ betyder att $20|x^n$.

(d) $x^n = 0$ i $\mathbb{Z}_k$ betyder att $k|x^n$.

4. Beräkna $\mathcal{M}^k$ för olika k. Skriv $\mathcal{M}_1$ på formen $\mathcal{M}_1 = I + \mathcal{M}$.
5. Utgå ifrån $0 + 0 = 0$ och multiplicera med α
6. Visa först att $a \cdot 0 = 0$ och $0 \cdot a = 0$ för alla a.
7. $a \in \mathcal{U}(\mathbb{Z}_n)$ om och endast om $0 \leq a \leq n-1$ och $\text{SGD}(a, n) = 1$.
8. "Vanlig" räkning ger $(m + ni)^{-1} = \frac{m-ni}{m^2+n^2}$. När består detta uttryck av heltal?
9. Utveckla $(a + b)(a - b)$.

3.7 Polynom

1.
2. Tag $(x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$
3. När är $nx^{n-1} = 0$ för alla x?
4. Tänk så här: Om a, b är heltal och $\text{SGD}(a, b) = d$, hur skall a_1 och b_1 väljas för att $aa_1 = bb_1$? Använd samma resonemang på polynomen.
5. $f(x) = (x - b)g(x) + r(x)$
6.
7. Använd Euklides algoritm.
8. Leta först efter nollställen.
9. Gör upp en lista på de reducibla polynomen. De har formen $(x + a)(x + b)$

3.8 Felrättande koder

1. Lägg till siffran 1 om ordet har udda vikt och lägg till 0 om ordet har jämn vikt.
2.
3. Beräkna $H\bar{C}$ och se vad som händer.
4. Vad för ekvation gäller för ett ord med jämn vikt?
5. Varje ord har 5 grannar på avstånd 1. Använd "sfärpackningsolikheten".
6.
7. Det finns $1 + \binom{8}{1} + \binom{8}{2}$ ord som ligger på avstånd ≤ 2 från ett givet ord. Använd "sfärpackningsolikheten".
8. Visa först att $w(x + y) = w(x) + w(y) - 2 \cdot \#(i \text{ där } x_i = y_i = 1)$. ($w$ står för vikten).
9. Lös ut x_2, x_3, x_5, x_6 som funktioner av x_1, x_4, x_7.
10. Välj en matris med alla kolumner olika. Se till att $n - r = 8$ där n är antalet kolumner och r är rangen.

4 Lösningar

4.1 Grundläggande talteori

1. p och q måste vara udda. $pq+3$ är därför jämnt. Eftersom $2|pq+3$ och $pq+3 \neq 2$ så är det inte ett primtal.

2. Använd Euklides algoritm. Vi visar endast deluppgift a.

$$\begin{aligned} 54 &= 40+14 \\ 40 &= 2\cdot 14+12 \\ 14 &= 12+2 \\ 12 &= 2\cdot 6 \end{aligned}$$

   SGD $= 2$

3. Använd Euklides algoritm för att beräkna SGD(a,b). MGM$(a,b) = \frac{ab}{\text{SGD}(a,b)}$. Vi visar deluppgift a:

$$\begin{aligned} 27 &= 21+6 \\ 21 &= 3\cdot 6+3 \\ 6 &= 2\cdot 3 \end{aligned}$$

   SGD $= 3$. MGM $= \frac{27\cdot 21}{3} = 189$.

   (a) Följande gäller: SGD$(a,b) \leq a \leq$ MGM(a,b) och SGD$(a,b) \leq b \leq$ MGM(a,b). Därför gäller:
   SGD$(a,b) =$ MGM$(a,b) \iff$ SGD$(a,b) = a = b =$ MGM$(a,b) \iff a = b$. Villkoret är alltså $a = b$.

   (b) Sätt SGD$(a,b) = d$, $a = a'd$, $b = b'd$. Då är MGM$(a,b) = a'b'd$. MGM$(a,b) = 2\cdot$ SGD$(a,b) \iff a'b'd = 2d \iff a'b' = 2 \iff$($a' = 2$ och $b' = 1$) eller ($a' = 1$ och $b' = 2$). Villkoret är att $a = 2b$ eller $b = 2a$.

   (c) Samma beteckningar som i b. MGM(a,b) är ett primtal $\iff a'b'd$ är ett primtal $\iff$ exakt ett av a', b', d är ett primtal och de övriga är 1. Villkoret är att (a är ett primtal och $b = 1$) eller ($a = 1$ och b är ett primtal) eller (både a och b är lika med ett primtal p).

4.

$$\begin{aligned} 389 &= 2\cdot 167+55 \\ 167 &= 3\cdot 55+2 \\ 55 &= 27\cdot 2+1 \end{aligned}$$

   SGD$(389,167) = 1$.
   $1 = 55-27\cdot 2 = 55-(167-3\cdot 55)\cdot 27 = 55\cdot 82-167\cdot 27 = (389-2\cdot 167)\cdot 82-27\cdot 167 = 389\cdot 82-167\cdot 191$
   SGD$(389,167) = 1 = 389\cdot 82-167\cdot 191$

5. Varje vattenmängd $10m+6n$ där $m,n \in \mathbb{Z}$ går att hälla upp (om denna mängd har positivt värde förstås). Det minsta värde på detta uttryck är SGD$(10,6) = 2$. Den minsta mängden är 2 liter. $(2 = 2\cdot 6-10)$

6. Vi observerar först att $\text{SGD}(12,9) = 3$ och sedan att $\text{SGD}(3,14) = 1$. $14 = 3 \cdot 4 + 2$, $3 = 2 + 1$. Baklänges fås $1 = 3 - 2 = 4 - (14 - 3 \cdot 4) = 3 \cdot 5 - 14$. Sedan ser vi att $12 = 9 + 3$, $3 = 12 - 9$. Detta ger $1 = (12 - 9) \cdot 5 - 14 = 12 \cdot 5 - 9 \cdot 5 - 14$. Så $p = 5$, $q = -5$, $r = -1$. Eftersom 3 delar 12, 9 och 15 kan inte $12p + 9q + 15r$ vara likamed 1.

7. (a) $n^2 + 3n = n(n+3)$. Om n är udda så är $n+3$ jämnt och om n är jämnt är $n+3$ udda. I båda fall blir produkten jämn.

   (b) $n^3+3n^2-4n = n((n^2+3n)-4)$. Från deluppgift a vet vi att sista faktorn är jämn. n^3+3n^2-4n är därför jämn. $3n^2$ är delbar 3. $n^3-4n = n(n^2-4) = n(n-2)(n+2)$. En av n, $n-2$, $n+2$ måste vara delbar med 3. Så $n^3 + 3n^2 - 4n$ är delbart med 3 och därför även med 6.

   (c) $2n^3 + 2n = 2n(n^2+1)$. Om n är udda så är n^2+1 jämn. Därför är $2n^3 + 2n$ alltid delbart med 4. $n^4 + 11n^2 = n^2(n^2+11)$. Om n är jämnt är n^2 delbart med 4. Om $n = 2k+1$ så är $n^2 + 11 = 4k^2 + 4k + 1 + 11 = 4(k^2 + k + 3)$ som är delbart med 4. $n^4 + 11n^2$ är alltid delbart med 4. Därför är också $n^4 + 2n^3 + 11n^2 + 2n$ alltid delbart med 4.

   (d) $4^{2n} - 1 = 16^n - 1 = (15+1)^n - 1$. $(15+1)^n$ kommer att kunna skrivas på formen $1 + p$ där p är en produkt som innehåller 15 (binomialutveckling). Så $4^{2n} - 1 = p$ som är delbart med 15.

8. Antag att påståendet inte är sant. Då finns det ett $n_1 \in M$ så att $5|n_1$ och $7 \not| n_1$ samt ett $n_2 \in M$ så att $5 \not| n_2$ och $7|n_2$. Då gäller $n_1 + n_2 \in M$. Men vi ser ju att $5 \not| n_1 + n_2$ och $7 \not| n_1 + n_2$. Enligt antagandet är det omöjligt. 5 eller 7 delar alla tal i M.

9. (a) $\frac{a}{47} + \frac{b}{53} = \frac{53a+47b}{47 \cdot 53}$. $\text{SGD}(47,53) = 1$ så det minsta värde som $53a + 47b$ kan få är 1. Svaret är $\frac{1}{47 \cdot 53} = \frac{1}{2491}$.

   (b) $\frac{a}{m} + \frac{b}{n} = \frac{am+bn}{m \cdot n}$. Detta är minst då $am+bn = \text{SGD}(m,n)$. Detta ger det minimala värdet $\frac{\text{SGD}(m,n)}{m \cdot n} = \frac{1}{\text{MGM}(m,n)}$.

   Eftersom a och b skall vara positiva är det lätt att kontrollera om ett vissta tal k går att skriva som $5a + 4b$. Man kan se att de första talen som går att skriva på formen är 0, 4, 5, 8, 9, 10, 12, 13, 14, 15, ... Det verkar som alla tal > 11 går att skriva på formen. Det går att bevisa så här: Antag att $k \geq 12$. Då gäller $k = s \cdot 4 + r$ där $s \geq 3$ och $0 \leq r \leq 3$, $5 - 4 = 1$ och $5r - 4r = r$. Vi får att $k = 5r + 4(s - r)$. Eftersom $s - r \geq 0$ så kan k skrivas på den givna formen. $k_0 = 11$.

10. Eftersom $\text{SGD}(m,n) = 1$ så finns det tal p, q så att $mp + nq = 1$. Vi kan anta att $p > 0$ och $q > 0$. Låt nu $k \geq n(n-1)(-q)$ (positivt). $k = ns + r$ där $s \geq (n-1)(-q)$, $0 \leq r \leq n-1$ samt $mpr + nqr = r$. Vi får $k = mpr + n(s + qr)$. Eftersom $s + qr \geq (n-1)(-q) + (n-1)q = 0$ så kan k skrivas på den angivna formen.

11. $\text{SGD}(m,n) = {p_1}^1 {p_2}^1 {p_3}^0 {p_4}^0 {p_5}^4 = p_1 p_2 {p_5}^4$. Detta gäller eftersom ett tal d delar m och n om och endast om $d = {p_1}^{k_1} {p_2}^{k_2} {p_3}^{k_3} {p_4}^{k_4} {p_5}^{k_5}$ och $k_1 \leq 1$, $k_2 \leq 1$, $k_3 = 0$, $k_4 = 0$ och $k_5 \leq 4$. Den största delaren d fås då likhet råder i alla olikheterna.
   $\text{MGM}(m,n) = \frac{mn}{\text{SGD}(m,n)} = {p_1}^3 {p_2}^1 {p_3}^2 {p_4}^5 {p_5}^6$. I det generella fallet fås på samma sätt $\text{SGD}(m,n) = {p_1}^{l_1} {p_2}^{l_2} \ldots {p_k}^{l_k}$, $\text{MGM}(m,n) = {p_1}^{s_1} {p_2}^{s_2} \ldots {p_k}^{s_k}$ där $l_i = \min(e_i, f_i)$ och $s_i = \max(e_i, f_i)$.

12. Låt p_1, p_2, ..., p_s vara alla primtal som förekommer i något av m, n och k. Antag att $m = {p_1}^{e_1} {p_2}^{e_2} \ldots {p_s}^{e_s}$, $n = {p_1}^{f_1} {p_2}^{f_2} \ldots {p_s}^{f_s}$ och $k = {p_1}^{g_1} {p_2}^{g_2} \ldots {p_s}^{g_s}$

(några av e_i, f_i eller g_i kan vara 0). $m^2 = kn^2$ betyder att ${p_1}^{2e_1}{p_2}^{2e_2}\ldots{p_s}^{2e_s} = {p_1}^{g_1}{p_2}^{g_2}\ldots{p_s}^{g_s}{p_1}^{2f_1}{p_2}^{2f_2}\ldots{p_s}^{2f_s}$. Detta är endast möjligt om $2e_1 = g_1 + 2f_1$, $2e_2 = g_2 + 2f_2$, ..., $2e_s = g_s + 2f_s$ dvs $g_1 = 2(f_1 - e_1) \geq 0$, $g_2 = 2(f_2 - e_2) \geq 0$, ..., $g_s = 2(f_s - e_s) \geq 0$. Sätt nu $a = {p_1}^{f_1-e_1}{p_2}^{f_2-e_2}\ldots{p_s}^{f_s-e_s}$. Eftersom $f_i - e_i \geq 0$ måste gälla att detta är ett heltal och $a^2 = k$. Antag nu att $\sqrt{K}$ är rationellt, dvs $\sqrt{K} = \frac{m}{n}$. Då gäller att $m^2 = Kn^2$ och $K = a^2$ så $\sqrt{K} = a$ (dvs $a = \frac{m}{n}$, divisionen måste gå jämnt upp). Alltså är $\sqrt{K}$ antingen ett heltal eller irrationellt.

13. Lösningarna måste vara heltal eller irrationella. Antag nämnligen att $x = \frac{m}{n}$ med $\text{SGD}(m, n) = 1$ och $n > 1$. Då gäller $m^7 - 14m^6n + 4m^5n^2 - 2m^4n^3 + 3m^3n^4 + 8m^2n^5 + 7mn^6 + 5n^7 = 0$. Låt nu p vara ett primtal sådant att $p|n$ och $p \not| m$. p kan inte dela vänsterledet men delar högreledet. Detta ger motsägelse.

14. Nej. $x = \log_{10}2$ betyder att $2^x = 10$. x kan förstås inte vara ett heltal. Antag att $x = \frac{m}{n}$. $2^{\frac{m}{n}} = 10$ ger $2^m = 10^n$. Men högerledet är delbart med 5 medan vänsterledet inte är det. Det ger motsägelse vilket visar att $\log_{10}2$ inte kan ha formen $\frac{m}{n}$.

15. 1, 2 och 3 är sanna. Antag att $a = {p_1}^{e_1} \cdot \ldots \cdot {p_k}^{e_k}$ och $b = {p_1}^{f_1} \cdot \ldots \cdot {p_k}^{f_k}$. Då är $\text{MGM}(a, b) = {p_1}^{\max(e_1,f_1)} \cdot \ldots \cdot {p_k}^{\max(e_1,f_k)}$. Om $\text{MGM}(a, b)$ är kvadratfri är $\max(e_i, f_i) \leq 1$ så att $e_i \leq 1$, $f_i \leq 1$ dvs a och b är kvadratfria. Omvänt gäller att om a och b är kvadratfria så är $\max(e_i, f_i) \leq 1$ så att $\text{MGM}(a, b)$ är kvadratfri. Alltså är 1 och 2 sanna. Om a och b är kvadratfria så är $\min(e_i, f_i) \leq 1$ så $\text{SGD}(a, b) = {p_1}^{\min(e_1,f_1)} \cdot \ldots \cdot {p_k}^{\min(e_1,f_k)}$ är kvadratfri. Så 3 är sann. 4 däremot är falsk. Tag tex $a = 9$ och $b = 12$. a och b är inte kvadratfria men $\text{SGD}(9, 12) = 3$ är kvadratfri.

4.2 Funktioner och kardinalitet

1. $fg(n) = f(3n) = 3n - 1.gf(n) = g(n - 1) = 3n - 3$. Så $fg(n) \neq gf(n)$. (Inte ens för något värde på n, men det räcker att visa att det finns ett tal n så att $fg(n) \neq gf(n)$ för att visa $fg \neq gf$.)

2. f är inte surjektiv. Tex finns det inget heltal x så att $x^3 = 2$. f är injektiv. Antag nämligen att $x^3 = y^3$. Eftersom $3x^3 \geq 0$ så är x^3 hela tiden växande. Så $x = y$. Eftersom x^3 inte är surjektiv är inte heller x^3 bijektiv.

3. (a) $a = 0$ ger $f(x) = b$ som inte är en bijektion. Antag att $a \neq 0$ och $a \neq \pm 1$. Då gäller $ax + b \equiv b(mod\ a)$ oberoende av vad x är. f är då inte en bijektion. Antag att $a = \pm 1$. Då kan vi sätta $g(x) = \frac{x-b}{a}$. Eftersom $a = \pm 1$ är $g(x)$ ett heltal. $f(g(x)) = g(f(x)) = x$ så $g = f^{-1}$. f är bijektiv om och endast om $a = \pm 1$ oberoende av vad b är.

   (b) $a = 0$ ger inte en bijektion. Så antag att $a = 0$. Sätt $g(x) = \frac{x-b}{a}$. $g : \mathbb{Q} \longrightarrow \mathbb{Q}$. $f(g(x)) = g(f(x)) = x$ så $g = f^{-1}$. f är bijektiv om och endast om $a \neq 0$.

4. Sätt $f(x)$ = resten då x divideras med n. Då gäller $f : \mathbb{Z} \longleftarrow \{0, 1, \ldots, \text{n-1}\}$. Enligt lådprincipen måste då två av talen tex x_i, x_j ha samma funktionsvärde dvs $f(x_i) = f(x_j) = k$. $x_i = a_in + k, x_j = a_jn + k, x_i - x_j = (a_i - a_j)n, n|x_i - x_j$.

5. Låt $f(x)$ = det största udda tal som delar x. Då gäller $f : \{1, 2, \ldots, 2n\} \longrightarrow Y$. Y innehåller n tal. Om $|X| \geq n + 1$ måste $f(x_1) = f(x_2)$ för två tal x_1, x_2 i X. Antag att $f(x_1) = f(x_2) = k$. Då gäller att $x_1 = 2^{a_1}k, x_2 = 2^{a_2}k$. Antag att $x_1 < x_2$. Då gäller $a_1 < a_2$. $\frac{x_2}{x_1} = 2^{a_2-a_1}$. Eftersom detta är ett heltal gäller

6. (a) En möjlighet är $X = \{n+1, n+2, \ldots, 2n\}$. Om $a = n + k_1$ och $b = n + k_2$ med $k_1 < k_2$ så gäller $\frac{b}{a} = \frac{n+k_2}{n+k_1}$. Denna kvot måste vara mindre än $\frac{n+n}{n} = 2$ så $\frac{b}{a} < 2$ och kan därför inte vara heltal. Så inga av talen i X delar varandra.

   (b) Inga av talen i A delar varandra. Låt f vara definierad som i lösningen till uppgift 5. Då måste $f(a) \neq f(b)$ för alla $a, b \in A$. (Annars skulle $a|b$ eller $b|a$) Låt m vara det största av talen $f(a), f(b)$. m uppfyller då villkoret.

7. Vi kan konstruera en invers f^{-1}. Sätt

$$f^{-1}(x) = \begin{cases} 2x & \text{om } x \geq 0 \\ 1 - 2x & \text{om } x < 0 \end{cases}$$

   Det går då lätt att se att $f^{-1}(f(n)) = n$ och $f(f^{-1}(x)) = x$ för alla n och x. Så f är inverterbar och därför en bijektion.

8. Antag att $p_1, p_2, \ldots, p_m$ vore en lista över alla primtal. Låt $N = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$. Då gäller $N > p_i$ för $i = 1, \ldots, m$ och att $p_i \not| N$ $i = 1, \ldots, m$, N kan då inte vara primtal eftersom $p_m < N$, Men om N vore sammansatt måste det finnas ett primtal $p > p_m$ så att $p|N$. Båda fallen visar att p_m inte kan vara det största primtalet. Alltså finns det oändligt många primtal.

9. (a) Antag att p_m är det största primtalet på formen $4n+3$. Sätt $N = 4 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m - 1$ ($p_2 = 3, p_3 = 5$, osv.) Vi ser att $N \equiv 3(mod\ 4)$. Så N kan inte vara primtal. Vi ser också $p_i \not| N$ $i = 2, \ldots, m$. Så N är en produkt av primtal p större än p_m. Om alla dessa hade $p \equiv 1(mod\ 4)$ skulle $N \equiv 1(mod\ 4)$. Så minst ett p måste ha $p \equiv 3(mod\ 4)$. Det finns oändligt många primtal på formen $4n + 3$.

   (b) Gör som i a och antag att p_m är det största primtalet på formen $4n + 1$ och sätt $N = 4 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m + 1$. Då gäller $N \equiv 1(mod\ 4)$. Det måste finnas primtal $p > p_m$ som delar N. Men dessa primtal måste ha formen $4n + 3$ eftersom $p \equiv 3(mod\ 4), q \equiv 3(mod\ 4) \longrightarrow pq \equiv 1(mod\ 4)$. Denna metod duger alltså inte för satt visa att det finns oändligt många tal på formen $4n + 1$ (Men det går faktiskt att visa med krångligare bevismetoder).

10. Dela in kvadraten i delkvadrater med sidan $\frac{1}{3}$. 2 punkter måste ligga i samma delkvadrat. I en sådan kvadrat är diagonalen $\frac{\sqrt{2}}{3}$, alltså är det maximala avståndet $\frac{\sqrt{2}}{3}$.

11. Om M är ändlig och $|M| = n$ så är $|P(M)| = 2^n$. Eftersom $n \neq 2^n$ så finns ingen bijektion. Följande metod fungerar dock för både ändliga och oändliga mängder:
    Antag att $f : M \longleftarrow P(M)$ är en bijektion. Om $a \in M$ så gäller antingen $a \in f(a)$ eller $a \notin f(a)$ ($f(a)$ är en mängd). Låt nu $A = \{a \in M : a \notin f(a)\}$. Om f är en bijektion måste det då finnas ett x så att $f(x) = A$. Om $x \in A$ så gäller $x \in f(x)$. Det betyder $x \notin A$ enligt definitionen på A. Å andra sidan medför $x \notin A$ att $x \notin f(x)$ vilket ger $x \in A$. Motsägelsen visar att det inte kan finnas en bijektion f.

12. Det är en bijektion. Vi kan ordna upp paren i $\mathbb{N}^2$ i ordningen (0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (3,1), ... Kalla den första positionen för position 0. På vilken plats kommer paret (a, b)? Om $a + b = k$ så finns det $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$ stycken par med lägre komponentsumma som kommer före (a, b). Dessutom kommer $(a + b, 0)$, $(a + b - 1, 1)$,... , $(a + 1, b - 1)$ före. Det är b stycken par. Så (a, b) kommer på position $\frac{k}{2}(k + 1) + b = \frac{1}{2}(a + b)(a + b + 1) + b = f(a, b)$ (Kom ihåg att fösta position är 0). $f(a, b)$ är alltså paret (a, b):s position. Det visar att f är en bijektion.

4.3 Partitioner, multinomialkoefficienter och Sterlingtal

1. $7 = 7 \qquad P_1(7) = 1$
   $7 = 6 + 1 = 5 + 2 = 4 + 3 \qquad P_2(7) = 3$
   $7 = 5 + 1 + 1 = 4 + 2 + 1 = 3 + 3 + 1 = 3 + 2 + 2 \qquad P_3(7) = 4$
   $7 = 4 + 1 + 1 + 1 = 3 + 2 + 1 + 1 = 2 + 2 + 2 + 1 \qquad P_4(7) = 3$
   $7 = 3 + 1 + 1 + 1 + 1 = 2 + 2 + 1 + 1 + 1 \qquad P_5(7) = 2$
   $7 = 2 + 1 + 1 + 1 + 1 + 1 \qquad P_6(7) = 1$
   $7 = 1 + 1 + 1 + 1 + 1 + 1 + 1 \qquad P_7(7) = 1$

2. En partition av n består av 1, 2, 3, ... eller n termer.

   Alltså $P(n) = P_1(n) + P_2(n) + \ldots + P_k(n) + \ldots + P_n(n)$.

3. Antag att vi har en partition av n med k termer. Minska varje term med 1. Det ger en partition av $n - k$,med högst k termer. Tex $n = 8, k = 4$ och partitioner $3 + 2 + 2 + 1$ ger $2 + 1 + 1$, en partition av 4. Omvänt: Givet en partition av $n - k$ med högst k termer kan vi öka varje term med 1 och lägga till +1-termer så vi får en partition av n med k termer. Tex $2 + 2$ ger $3 + 3 + 1 + 1$, $(n = 8, k = 4)$. Detta visar att antalet partitioner av n i k termer = antalet partitioner av $n - k$ i högst k termer. Så $P_k(n) = P_1(n - k) + P_2(n - k) + \ldots + P_k(n - k)$.

4. $\binom{n}{a,b,c}$ är antalet sätt att dela in talen 1, 2, ..., n i tre särskiljbara mängder med a tal i den första, b i den andra och c i tredje mängden. Talet 1 kan placeras i den första mängden på $\binom{n-1}{a-1,b,c}$ sätt (eller rättare sagt kan de övriga talen placeras på så många sätt), i andra mängden på $\binom{n-1}{a,b-1,c}$ sätt och i trejde mängden på $\binom{n-1}{a,b,c-1}$ sätt.

   Så $\binom{n}{a,b,c} = \binom{n-1}{a-1,b,c} + \binom{n-1}{a,b-1,c} + \binom{n-1}{a,b,c-1}$.

5. $\binom{n}{n_1,n_2,\ldots,n_k}$ är lika med antalet sätt att dela in talen 1, 2, ..., n i k särskiljbara mängder med storlek $n_1, n_2, \ldots, n_k$. Om vi delar med $k!$ får vi antalet sätt att dela in 1, 2, ..., n i k icke-särskiljbara mängder av storlek $n_1, n_2, \ldots, n_k$. Om vi sedan summerar över alla val av $n_1, n_2, \ldots, n_k$ fås antalet sätt att dela in 1, 2, ..., n i k icke-särskiljbara delmängder. $\frac{1}{k!} \sum \binom{n}{n_1,n_2,\ldots,n_k} = S(n, k)$

6. (a) Välj först var kula 1 placeras, sedan var kula 2 placeras osv. Det finns totalt 5^{10} möjligheter

   (b) Om ingen låda skall vara tom finns det $S(10, 5)$ möjligheter. Om en låda skall vara tom finns det $S(10, 4)$ möjligheter osv. Det totala antalet är $S(10, 5) + S(10, 4) + S(10, 3) + S(10, 2) + S(10, 1)$.

   (c) En placering kan representeras med en sekvens enligt följande metod: Om tex 3 kulor placeras i låda 2, 1 kula i låda 3, 4 kulor i låda 4 och 2 kulor i låda 5 så representeras placeringen av (2, 2, 2, 3, 4, 4, 4, 4, 5, 5). Antalet sätt att välja sådana sekvenser är lika med antalet sätt att välja 10 element ur en mängd med 5 element och med återläggning. Så antalet är $\binom{5+10-1}{10} = \binom{14}{10}$

   (d) En sådan placering motsvarar ett sätt att skriva 10 som en summa. (Termerna motsvarar antalet kulor i de olika lådorna) Så antalet är $P(10)$.

4.4 Modulär aritmetik

1. Om a är udda så gäller något av följande: $a \equiv 1, a \equiv 3, a \equiv 5, a \equiv 7 (mod\ 8)$. Då vi kvadrerar får vi de olika fallen: $a^2 \equiv 1, a^2 \equiv 3 \equiv 9, a^2 \equiv 25 \equiv 1, a^2 \equiv 49 \equiv 1 (mod\ 8)$.

Om a är jämnt men $\frac{a}{2}$ är udda gäller något av följande: $a \equiv 2 \cdot 1 \equiv 2, a \equiv 2 \cdot 3 \equiv 6, a \equiv 2 \cdot 5 \equiv 2, a \equiv 2 \cdot 7 \equiv 6 (mod\ 8)$, dvs $a \equiv 2$ eller $a \equiv 6 (mod\ 8)$. Vi får då $a^2 \equiv 4$ eller $a^2 \equiv 36 \equiv 4 (mod\ 8)$. I alla fall gäller $a^2 \equiv 4 (mod\ 8)$.

2. Prövning ger $1^{-1} = 1, 2^{-1} = 9, 3^{-1} = 6, 4^{-1} = 13, 5^{-1} = 7, 6^{-1} = 3, 7^{-1} = 5, 8^{-1} = 15, 9^{-1} = 2, 10^{-1} = 12, 11^{-1} = 14, 12^{-1} = 10, 13^{-1} = 4, 14^{-1} = 11, 15^{-1} = 8$ och $16^{-1} = 16$. Prövningen kan underlättas av vissa enkla iakttagelser: Om $a^{-1} = b$ så är $b^{-1} = a$. Om vi dessutom använder oss av $9 = -8, 10 = -7, \ldots, 16 = -1$ så fås att om $a^{-1} = b$ så är $-a^{-1} = -b$.

3. (a) Vi ser att $10^i \equiv 1 (mod\ 3)$ för alla i. $x \equiv x_k \cdot 10^k + x_{k-1} \cdot 10^{k-1} + \ldots + x_1 \cdot 10 + x_0 \equiv x_k \cdot 1 + x_{k-1} \cdot 1 + \ldots + x_1 \cdot 1 + x_0 \equiv x_k + x_{k-1} + \ldots + x_1 + x_0 (mod\ 3)$

   (b) På samma sätt ses att $10^1 \equiv (-1)^1 (mod\ 11)$
   $x \equiv x_k \cdot (-1)^k + x_{k-1} \cdot (-1)^{k-1} + \ldots + x_1 \cdot (-1) + x_0 (mod\ 11)$

   (c) Med ledning av a och b sätter vi till resten av division av 10^i med n. Då fås $10^i \equiv a_i (mod\ n)$ och $x \equiv a_k x_k + a_{k-1} x_{k-1} + \ldots + a_1 x_1 + x_0 (mod\ n)$.

4. $n = 2$ ger $a_0 = 1, a_1 = 0, a_2 = 0, \ldots$
   x är delbart med 2 $\iff$ x_0 är delbart med 2.

   $n = 4$ ger $a_0 = 1, a_1 = 2, a_2 = 0, a_3 = 0, \ldots$
   x är delbart med 4 $\iff$ $2x_1 + x_0$ är delbart med 4.

   $n = 5$ ger $a_0 = 1, a_1 = 0, a_2 = 0, \ldots$
   x är delbart med 5 $\iff$ x_0 är delbart med 5.

   $n = 6$ ger $a_0 = 1, a_1 = 4, a_2 = 4, a_3 = 4, \ldots$
   x är delbart med 6 $\iff$ $\ldots + 4x_3 + 4x_2 + 4x_1 + x_0$ är delbart med 6.

   $n = 7$ ger $a_0 = 1, a_1 = 3, a_2 = 2, a_3 = 6, a_4 = 4, a_5 = 5$, sedan upprepar sig mönstret cykliskt
   x är delbart med 7 $\iff$ $\ldots + 5x_5 + 4x_4 + 6x_3 + 2x_2 + 3x_1 + x_0$ är delbart med 7.

   $n = 8$ ger $a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 0, \ldots$
   x är delbart med 8 $\iff$ $4x_2 + 2x_1 + x_0$ är delbart med 8.

   $n = 9$ ger $a_0 = 1, a_1 = 1, a_2 = 1, \ldots$
   x är delbart med 9 $\iff$ $\ldots + x_3 + x_2 + x_1 + x_0$ är delbart med 9.

   Fallet $n = 6$ kan enklare beskrivas:
   x är delbart med 6 $\iff$ x är delbart med 2 och 3 $\iff$ x_0 är delbarmed 2 och $\ldots + x_3 + x_2 + x_1 + x_0$ är delbart med 3.

5. Om b och d är inverterbara så är även bd inverterbart. $\frac{ad+bc}{bd}$ och $\frac{ac}{bd}$ existerar alltså som element i $\mathbb{Z}_m$. För att visa likheterna räcker det att kontrollera att $bd(\frac{a}{b} + \frac{c}{d}) = ad + bc$ och att $bd(\frac{a}{b} \cdot \frac{c}{d}) = ac$ i $\mathbb{Z}_m$
   $bd(\frac{a}{b} + \frac{c}{d}) = bd \cdot \frac{a}{b} + bd \cdot \frac{c}{d} = \frac{1}{b} \cdot bad + \frac{1}{d} \cdot dbc = ad + bc$
   $bd(\frac{a}{b} \cdot \frac{c}{d}) = \frac{1}{b} \cdot b \cdot a \cdot \frac{1}{d} \cdot d \cdot c = ac$

6. Ekvationen kan skrivas $x^2 - 1 = 0$, $(x + 1)(x - 1) = 0$. I $\mathbb{Z}_p$ finns inga nolldivisioner och därför gäller $x - 1 = 0$ eller $x + 1 = 0$ dvs $x = \pm 1$ och det är de enda lösningarna. Det finns alltså 2 lösningar. (Eftersom $p \geq 3$ så är $1 \neq -1$ i $\mathbb{Z}_p$)

7. Vi räknar ut produkten i $\mathbb{Z}_p$. Produkten kan å ena sidan skrivas som $(p-1)!$. Från uppgift 6 vet vi att om $a \neq 1, -1, 0$ så är $a^{-1} \neq a$. Produkten har därför å andra sidan 1 och -1 som faktorer ($-1 = p-1$) och består i övrigt av $\frac{p-3}{2}$ produkter på formen $a^{-1} \cdot a$. Dessa delprodukter är 1 och totala produkten är $1 \cdot (-1) \cdot 1 = -1$ så $(p-1)! = -1$ i $\mathbb{Z}_p$. Detta betyder att $(p-1)! \equiv -1 (mod\ p)$. (Fallet $p = 2$ är trivialt ty $(p-1)! = 1 = -1$ i $\mathbb{Z}_2$)

8. Antag att $(n-1)! \equiv -1 (mod\ n)$. Det betyder att $(n-1)! + 1$ är delbart med n. Antag nu att n inte är primtal och att $a|n$, $1 < a < n$. Då måste $a|(n-1)! + 1$. Men detta är omöjligt eftersom $a|(n-1)!$ men $a \not| 1$. n måste därför vara primtal.

9. (a) Använd formeln $x^2 + px + q = 0 \Rightarrow x = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}$ där $\sqrt{a}$ tolkas som de tal y som uppfyller $y^2 = a$. $x^2 + x + 1 = 0$ ger $x = \frac{1}{2} + \sqrt{\frac{1}{4} - 1}$.
I $\mathbb{Z}_7$ gäller $\frac{1}{2} = 4$, $-\frac{1}{2} = -4 = 3$, $\frac{1}{4} = 2$.
$x = 3 + \sqrt{1}$. $\sqrt{1} = 1, -1$. $x = 3 \pm 1$. $x_1 = 4$, $x_2 = 2$.

   (b) På samma sätt som i a fås $x^2 + 9x + 9 = 0 \Rightarrow x = -\frac{9}{2} + \sqrt{(\frac{9}{2})^2 - 9}$.
$\frac{1}{2} = 6$, $-\frac{1}{2} = -5$, $-\frac{9}{2} = 9 \cdot 5 = 1$, $(\frac{9}{2})^2 = 1^2 = 1$.
$x = 1 + \sqrt{-8} = 1 + \sqrt{3}$, $\sqrt{3} = \pm 5 = 5, 6$. $x_1 = 6$, $x_2 = 7$.

   (c) $x^2 + 7x + 2 = 0 \Rightarrow x = -\frac{7}{2} + \sqrt{(\frac{7}{2})^2 - 2}$.
$\frac{1}{2} = 7$, $-\frac{1}{2} = 6$, $-\frac{7}{2} = 7 \cdot 6 = 3$, $(\frac{7}{2})^2 = 3^2 = 9$.
$x = 3 + \sqrt{7}$. Men det finns inga kvadratrötter till 7 i $\mathbb{Z}_{13}$, vilket lätt kan kontrolleras. Ekvationen saknar lösning.

10. Vi ställer upp en tabell.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^2	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

    Vi ser att för $k = 0, 1, 2, 4, 8, 9, 13, 15, 16$ finns $\sqrt{k}$.

11. Låt $x \in \mathbb{Z}_p, y \in \mathbb{Z}_p$. Då gäller $x^2 = y^2 \iff x^2 - y^2 = 0 \iff (x+y)(x-y) = 0 \iff y = x$ eller $y = -x$. Om man beräknar x^2 för $x = 1, 2, \ldots, p-1$ så kommer varje värde på x^2 att dyka upp exakt två gånger. Det betyder att det finns $\frac{p-1}{2}$ stycken möjliga värden på x^2 då $x = 1, 2, \ldots, p-1$. För alla dessa $k = x^2$ existerar $\sqrt{k}$. Dessutom gäller $\sqrt{0} = 0$. Det finns totalt $\frac{p+1}{2}$ olika tal k så att $\sqrt{k}$ existerar.

4.5 Gruppteori

1. Produkten av två matriser med heltalskoefficienter blir en matris med heltalskoefficienter. Om det($\mathcal{M}_1$)=± 1 och det($\mathcal{M}_2$)=± 1 gäller det($\mathcal{M}_1 \cdot \mathcal{M}_2$)=$\pm 1$. $\mathcal{M}$ är sluten . Multiplikationen är associativ. Enhetsmatrisen I ligger i $\mathcal{M}$.
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Denna matris har heltalskoefficienter och tillhör därför $\mathcal{M}$. $\mathcal{M}$ uppfyller alla kraven på en grupp.

2. (a) Om SGD$(a, b) = d$ så dinn tal m, n så att $ma + nb = d$ (ma kan tolkas som $a + a + \ldots + a$ (m termer) osv). Om A är en delgrupp så gäller $ma \in A, nb \in A, ma + nb \in A$, dvs $d \in A$.

(b) Antag att A är en delgrupp och att d är det minsta talet i A. Antag sedan att $a \in A$. $a = kd + r$ där $0 \geq r < d$. $a - kd \in A$, alltså måste $r \in A$. Men eftersom d är det minsta talet i A förutom 0 måste $r = 0$, dvs $d|a$.

(c) Antag samma sak som i b. $n = kd + r$. I $\mathbb{Z}_n$ kan detta skrivas $r = -kd$. Då måste $r \in A$ och därför är $r = 0$, så $d|n$.

(d) Låt $A = \{kd.k \in \mathbb{Z}\}$. $k_1 d \in A, k_2 d \in A \Rightarrow (k_1 + k_2)d \in A$. $0d = 0 \in A$ så enhet finns. Om $k_1 d \in A$ så gäller $-k_1 d \in A$. A är alltså en grupp.

3. Enligt uppgift 2 skall vi leta efter d så att $d|20$. $d = 1, 2, 4, 5, 10$. Dessa d ger följande delgrupper:

$d = 0 : \{0\}$
$d = 1 : \mathbb{Z}$
$d = 2 : \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$
$d = 4 : \{0, 4, 8, 12, 16\}$
$d = 5 : \{0, 5, 10, 15\}$
$d = 10 : \{0, 10\}$

4. Låt $x \circ y = m = \max(x, y)$. Då är $(x \circ y) \circ z = m \circ z = \max(m, z) =$ det största talet av m och z. Men det är då klart att $(x \circ y) \circ z = \max(x, y, z)$, dvs det största talet av x, y och z. På samma sätt visas att $x \circ (y \circ z) = \max(x, y, z)$. Så $(x \circ y) \circ z = x \circ (y \circ z)$ och $\circ$ är alltså associativ.

5. Potenserna a^k kan inte alla vara olika eftersom det bara finns 300 element i G. Därför gäller $a^{k_1} = a^{k_2}$ för några k_1, k_2 båda mindre än 300. Sätt $k = |k_1 \cdot k_2|$. Då gäller $a_k = 1$. Så det finns minst ett sådant k. Antag att k är så litet som möjligt (fast > 0). Men vi vet inte vad k är. $\{a^0, a^1, a^2, \ldots, a^{k-1}\}$ är en delgrupp med k element. Enligt Lagranges sats måste $k|300$. Då gäller $a^{300} = (a^k)^{\frac{300}{k}} = 1^{\frac{300}{k}} = 1$. Så vi kan sätta $n = 300$.

6. (a) Det räcker att visa att $(ab) \cdot (b^{-1}a^{-1}) = 1$. $(ab) \cdot (b^{-1}a^{-1}) = a(b \cdot b^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1$.

(b) Om $ab = 1$ så måste $b = a^{-1}$. Då gäller $ba = a^{-1}a = 1$.

(c) $(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2 \Rightarrow aba = a^2b \Rightarrow ba = ab$

7. Om $g^2 = 1$ så gäller också $g^{-1} = g$ dvs alla element är sin egen invers. Låt nu a, b vara två element i G. $a, b = a^{-1}b^{-1} = (ba)^{-1} = ba$. Så $ab = ba$ gäller för alla element.

8. $H \cap K$ är en delgrupp. Antag nämnligen att $a, b \in H \cap K$. $a, b \in H \cap K \Rightarrow a, b \in H$ och $a, b \in K$. Eftersom H och K är delgrupper gäller då att $ab \in H$ och $ab \in K$ dvs $ab \in H \cap K$. $a \in H \cap K \Rightarrow a \in H$ och $a \in K \Rightarrow a^{-1} \in H$ och $a^{-1} \in K \Rightarrow a^{-1} \in H \cap K$. $H \cap K$ upppfyller alltså kraven på en delgrupp.

$H \cup K$ är inte nödvändigtvis en delgrupp. Tag tex $G = \mathbb{Z}_6$ med $+$ som gruppoperation. Sätt $H = \{0, 2, 4\}$ och $K = \{0, 3\}$. H och K är delgrupper. $H \cup K = \{0, 2, 3, 4\}$ och detta är inte en delgrupp eftersom tex $2 + 3 = 5$ och $5 \notin H \cup K$.

9. $g^0, g^1, \ldots, g^{m-1}$ är alla olika. (Lägg märke till att $g^0 = 1$). Antag att i, j är heltal och att $i, j \equiv k(mod\ m)$ och att $0 \leq k \leq m-1$. Då gäller $x^i \cdot x^j = x^{i+j} = x^{a \cdot m + k} = 1^a \cdot x^k = x^k$ dvs $x^i \cdot x^j = x^k$. Det betyder att produkten av två element i A ligger kvar i A. A är alltså sluten. Om $x^i \in A$ så gäller $x^i \cdot x^{m-i} = x^m = 1$. Inversen till x^i ligger alltså i A. A är en delgrupp till G.

4.6 Ringar

1. A utgör en ring som inte är kommutativ. $(1,0,0,1)$ är multiplikativ enhet. (a,b,c,d) är inverterbar omm $ad-bc \neq 0$. Detta visas lättast genom att översätta elementen i A till matriser:

   $(a,b,c,d) \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

   $\oplus$ och $\odot$ tolkas sedan som matrisaddition respektive matrismultiplikation.

2. (a) I alla ringar gäller $(a+a)^2 = a^2+aa+aa+a^2 = a^2+a^2+a^2+a^2$. I Booleska ringar blir detta $a+a+a+a$. Å andra sidan gäller i Booleska ringar att $(a+a)^2 = a+a$. Vi får $a+a+a+a = a+a$ vilket ger att $a+a = 0$ eller, om man vill, $a = -a$.

   (b) $(a+b)^2 = a^2+ab+ba+b^2$ gäller i alla ringar. I Booleska ringar ger detta $a+b = a+ab+ba+b$, dvs $ab+ba = 0$ och $ab = -ba$. Men från uppgift a vet vi att $-ba = ba$ så vi får $ab = ba$

   (c) Om tex a är inverterbar gäller $a^k \cdot a^{-k} = 1$. Men $a^k = a$ så $a \cdot a^{-k} = 1$ dvs $a^{-k} = a^{-1}$. Detta ger förenklingen $a^7b^5 + c^{-5}(a^7b^{18} + b2a^6) + c^2a^{13}b^{17}c^{-3} = ab + c^{-1}(ab+ba) + cbac^{-1} = ab + c^{-1} \cdot 0 + abcc^{-1} = ab + ab = 0$.

   (d) $\mathbb{Z}_2$ är uppenbarligen Boolesk. Ingen annan $\mathbb{Z}_n$-ring är Boolesk. Detta kan inses genom att $1+1 \neq 0$ utom i $\mathbb{Z}_2$.

3. (a) Antag att n är det minsta n så att $x^n = 0$. Antag sedan att $xy = 1$. Då är $x^n y = x^{n-1}$ och därför gäller $x^{n-1} = 0$. Men detta strider mot antagandet. Så x kan inte vara inverterbar.

   (b) $(1+x)(1-x+x^2+\ldots+(-1)^{n-1}x^{n-1} = 1-x+x^2+\ldots+(-1)^{n-1}x^{n-1}+x-x^2+\ldots+(-1)^{n-2}x^{n-1}+(-1)^{n-1}x^n = 1+(-1+1)x+(1-1)x^2+\ldots+((-1)^{n-1}+(-1)^{n-2})x^{n-1}+(-1)^{n-1}x^n = 1+(-1)^{n-1}x^n = 1$

   (c) $x^n = 0$ i $\mathbb{Z}_{20}$ betyder att $20|x^n$. Eftersom $20 = 2^2 \cdot 5$ så måste antingen $x = 0$ eller x innehålla faktorerna 2 och 5, dvs $x = 10$.

   (d) Om $x^n = 0$ i $\mathbb{Z}_k$ måste x innehålla alla primtalsfaktorer som finns i k. Samtidigt skall $x < k$. Det måste då stå följande: "k innehåller en faktor p^m där $m > 1$"

4. $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
   Så $\mathcal{M}^3 = 0$. $\mathcal{M}_1 = I + \mathcal{M}$. Detta ger $\mathcal{M}_1^{-1} = I - \mathcal{M} + \mathcal{M}^2 =$
   $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ -2 & 0 & 1 \end{pmatrix}$

5. $0+0 = 0$ måste gälla. Då gäller även $(0+0) \cdot \alpha = 0 \cdot \alpha = 1$. Men enligt distributiva lagen gäller $(0+0) \cdot \alpha = 0 \cdot \alpha + 0 \cdot \alpha = 1+1$. Så $1+1 = 1$, dvs $1 = 0$. Men det är omöjligt. α kan inte existera.

6. Det är bra att kunna använda påståendena $a \cdot 0 = 0$ och $0 \cdot a = 0$ för alla a. Men detta måste bevisas:

   $0+0 = 0$ (Detta är ett axiom), $a \cdot (0+0) = a \cdot 0$, $a \cdot 0 + a \cdot 0 = a \cdot 0$ (Axiomet om distributivitet), $(a \cdot 0 + a \cdot 0) + (-a \cdot 0) = (a \cdot 0) + (-a \cdot 0)$ (Enligt axiom så har $a \cdot 0$

additiv invers), $a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) = a \cdot 0 + (-a \cdot 0)$ (Enligt axiomet om att $+$ är associativ), $a \cdot 0 + 0 = 0$, $a \cdot 0 = 0$ (Enligt axiomet om att $x + 0 = 0$).

På samma sätt visas att $0 \cdot a = 0$. Vi visar nu att $(-x)y = -(xy)$:

$(-x)y + xy = (-x + x)y =$ (Enligt distributiva lagen) $= 0 \cdot y = 0$
Eftersom $(-x)y + xy = 0$ så måste $(-x)y$ vara inversen till xy, dvs $(-x)y = -xy$.

Vi visar sedan att $(-x)(-y) = xy$:

$(-x)(-y) + (-x)y = (-x)(-y + y) =$ (Enligt distributiva lagen) $= (-x) \cdot 0 = 0$.
$(-x)(-y) + (-x)y = 0$ medför att $(-x)(-y)$ är invers till $(-x)y$, dvs till $-(xy)$. Detta betyder att $(-x)(-y) = xy$.

7. Generellt gäller att $\mathcal{U}(\mathbb{Z}_n)$ består av tal k med $\text{SGD}(k, n) = 1$. $\mathcal{U}(\mathbb{Z}_{10})$ består av $\{1, 3, 7, 9\}$. Multiplikationstabell är:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	1	9
9	9	7	9	1

$\mathcal{U}(\mathbb{Z}_{11})$ består av $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Räkning visar att $\{2^0, 2^1, 2^2, \ldots, 2^9\} = \{1, 2, 3, \ldots, 10\}$. Det betyder att $\mathcal{U}(\mathbb{Z}_{11})$ är isomorf med C_{10}.

$\mathcal{U}(\mathbb{Z}_{12})$ består av $\{1, 5, 7, 11\}$. Multiplikationstabell är:

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

8. $a + bi, c + di \in \Gamma \Rightarrow (a + c) + (b + d)i \in \Gamma$ eftersom $a + c$ och $b + d$ är heltal om a, b, c, d är heltal.
$(a + bi)(c + di) = ac - bd + (ad + bc)i \in \Gamma$ på samma sätt.
Γ är sluten under addition och multiplikation. $0 = 0 + 0i$ och $1 = 1 + 0i$ tillhör båda Γ. Vi vet att $+$ och $\cdot$ är associativa, kommutativa och distributiva för räkning med "vanliga" komplexa tal. Γ är därför en ring.

Vilka $m + ni$ är inverterbara i Γ?
$(m + ni)^{-1} = \frac{m - ni}{m^2 + n^2}$. Observera att $|m| \leq m^2 + n^2$ och $|n| \leq m^2 + n^2$
$\frac{m}{m^2+n^2}$ är heltal $\iff$ $m = 0$ eller $|m| = m^2 + n^2$ $\iff$ $m = 0$ eller ($m = \pm 1$ och $n = 0$)
$\frac{-n}{m^2+n^2}$ är heltal $\iff$ $n = 0$ eller $|n| = m^2 + n^2$ $\iff$ $n = 0$ eller ($n = \pm 1$ och $m = 0$)
De inverterbara elementen är då $1, -1, i, -i$.

$\mathcal{U}(\Gamma)$ har multiplikationstabellen:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	1	-1
$-i$	$-i$	i	-1	1

9. R är kommutativ $\iff$ $ab = ba$ för alla a, b $\iff$ $ba - ab = 0$ för alla a, b $\iff$ $a^2 + ba - ab - b^2 = a^2 - b^2$ för alla a, b $\iff$ $(a + b)(a - b) = a^2 - b^2$ för alla a, b.

4.7 Polynom

1. (a) Vi kan först lösa ekvationen $y^2 = 0$ i $\mathbb{Z}_8$. Lösningarna är $y = 0, 2, 4, 6$. Detta ger $x = 0, 2, 4, 6$.

   (b) $x = -1 = 7$ och $x = -5 = 3$ är uppenbart lösningar. Men $x = 1$ (med $x + 1 = 2$ och $x + 5 = 6$) och $x = 5$ (med $x + 1 = 6$ och $x + 5 = 2$) är också lösningar. Så $x = 1, 3, 5, 7$

2. Eftersin F är en kropp kan $p(x)$ faktoriseras i irreducibla faktorer på ett unikt sätt. $p(x) = (x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$. Då kan vi skriva $p(x) =$ (*polynom utan konstant term*) $+ (-1)^n \alpha_1 \alpha 2 \cdot \ldots \cdot \alpha_n$

3. (a) Tag tex $p(x) = x^{11}$. Då gäller $Dp(x) = 11 \cdot x^{10} = 0$ eftersom $11 = 0$ i $\mathbb{Z}_{11}[x]$.

   (b) Antag att $f(x)$ är ett polynom sådant att $Df(x) = 0$. Om $f(x)$ har en term ax^{kp} så är $D(ax^{kp}) = kpax^{kp-1} = 0$ i $\mathbb{Z}_p[x]$. Men om $f(x)$ har en term bx^m där $p \not| m$ så är $D(bx^m) = mbx^{m-1}$) som inte är likamed 0. En sådan term kan inte försvinna. Därför måste $f(x)$ ha formen $f(x) = a_m x^{mp} + a_{m-1} x^{(m-1)p} 0 \ldots + a_1 x^p + a_0$. Om vi sätter $g(y) = a_m y^m + a_{m-1} y^{(m-1)} 0 \ldots + a_1 y + a_0$ gäller då $f(x) = g(x^p)$. Omvänt så har alla polynom på formen $g(x^p)$ där g är ett godtyckligt polynom derivata 0.

4. (a) Antag att $\text{SGD}(p_1, p_2) = d(x)$ och grad $d(x) = k$. Då gäller $p_1(x) = s_1(x)d(x)$ och $p_2 = s_2(x)d(x)$ där $\text{SGD}(s_1, s_2) = 1$. Sätt nu $q_1(x) = s_2(x)$ och $q_2(x) = s_1(x)$. Då gäller $p_1(x)q_1(x) = s_1(x)d(x)s_2(x) = p_2(x)q_1(x)$. Dessutom gäller $textupgradq_1(x) = n - l \leq n - 1$ och $textupgradq_2(x) = m - k \leq m - 1$.

   (b) Om $\text{SGD}(p_1(x), p_2(x)) = 1$ så finns polynom $a_1(x), a_2(x)$ så att $a_1(x)p_1(x) + a_2(x)p_2(x) = 1$. Om $p_1(x)q_1(x) = p_2(x)q_2(x)$ gäller då $q_1(x)a_1(x)p_1(x) + q_1(x)a_2(x)p_2(x) = q_1(x)$. Detta ger $q_1(x) = p_2(x)q_2(x)a_1(x) + q_1(x)p_1(x)a_2(x)$. Då måste $p_2(x) | q_1(x)$. Det betyder att grad $p_2 \leq$ grad q_1. Det gör att grad $p_2 = n$ så kan inte grad $q_1 \leq n - 1$.

5. Sätt $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Divisionsalgoritmen visar att $f(x) = g(x)(x - b) + r$ där r (resten) är ett tal. $f(b) = g(b)(b - b) + r = r$. Alltså gäller $r = f(b) = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b^1 + a_0$.

6. (a)

$$\begin{array}{r|l} & x \\ \hline x^2 + x + 1 & x^3 + x^2 + 1 \\ & \underline{-(x^3 + x2 + 1)} \\ & x + 1 \end{array}$$

   $x^3 + x^2 + 1 = (x^2 + x + 1)x + x + 1$
   Kvot $= x$ Rest $= x + 1$

(b)

$$\begin{array}{r|l}
 & x^3 - x^2 \\
\hline
x^2 + 2x + 3 & x^5 + x^4 + 2x^3 + x^2 + 4x + 2 \\
 & \underline{-(x^5 + 2x^4 + 3x^3)} \\
 & \quad - x^4 - x^3 + 4x + 2 \\
 & \quad \underline{-(-x^4 - 2x^4 - 3x^2)} \\
 & \quad\quad x^3 + 4x^2 + 4x + 2 \\
 & \quad\quad \underline{-(x^3 + 2x^2 + 3x)} \\
 & \quad\quad\quad 2x^2 + x + 2 \\
 & \quad\quad\quad \underline{-(2x^2 + 4x + 6)} \\
 & \quad\quad\quad\quad - 3x - 4
\end{array}$$

$x^5 + x^4 + 2x^3 + x^2 + 4x + 2 = (x^2 + 2x + 3)(x^3 - x^2) - 3x - 4 = (x^2 + 2x + 3)(x^3 - x^2) + 2x + 1$
Kvot $= x^3 + 4x^2$ Rest $= 2x + 1$

7. Använd Euklides algoritm.

(a)

$$\begin{array}{r|l}
 & x + 1 \\
\hline
x^4 + x^3 + x + 1 & x^5 + x^3 + x^2 + 1 \\
 & \underline{-(x^5 + x^4 + x^2 + x)} \\
 & \quad x^4 + x^3 + x + 1 \\
 & \quad \underline{-(x^4 + x^3 + x + 1)} \\
 & \quad\quad 0
\end{array}$$

Divisionen går jämnt upp. Det betyder att SGD $= x^4 + x^3 + x + 1 = b(x)$. (Vi kan sätta $f(x) = 0$ och $g(x) = 1$)

(b)

$$\begin{array}{r|l}
 & 2 \\
\hline
x^4 + 2x^2 + 2x + 2 & 2x^4 + 2x^3 + 2x^2 + x + 2 \\
 & \underline{-(2x^4 + x^2 + x + 1)} \\
 & \quad 2x^3 + x^2 + 1
\end{array}$$

$$\begin{array}{r|l}
 & 2x + 2 \\
\hline
2x^3 + x^2 + 1 & x^4 + 2x^2 + 2x + 2 \\
 & \underline{-(x^4 + 2x^3 + 2x)} \\
 & \quad x^3 + 2x^2 + 2 \\
 & \quad \underline{-(x^3 + 2x^2 + 2)} \\
 & \quad\quad 0
\end{array}$$

Divisionen går jämnt upp. En monisk SGD är $2(2x^3 + x^2 + 1) = x^3 + 2x^2 + 2$.
$2x^3 + x^2 + 1 = 2x^4 + 2x^3 + 2x^2 + x + 2 + 2 \cdot (x^4 + 2x^2 + 2x + 2)$
$x^3 + 2x^2 + 2 = 2 \cdot (2x^4 + 2x^3 + 2x^2 + x + 2) + (x^4 + 2x^2 + 2x + 2)$
$f(x) = 1$ och $g(x) = 2$

(c)

$$
\begin{array}{r|l}
\multicolumn{2}{r}{1} \\
\cline{2-2}
x^4+4x+2 & x^4+2x^3+3x^2+3 \\
 & \underline{-(x^4+4x+2)} \\
 & 2x^3+3x^2+x+1
\end{array}
$$

$$
\begin{array}{r|l}
\multicolumn{2}{r}{3x+3} \\
\cline{2-2}
2x^3+3x^2+x+1 & x^4+4x+2 \\
 & \underline{-(x^4+4x^3+3x^2+3x)} \\
 & x^3+2x^2+x+2 \\
 & \underline{-(x^3+4x^2+3x+3)} \\
 & 3x^2+3x+4
\end{array}
$$

$$
\begin{array}{r|l}
\multicolumn{2}{r}{4x+2} \\
\cline{2-2}
3x^2+3x+4 & 2x^3+3x^2+x+1 \\
 & \underline{-(2x^3+2x^2+x)} \\
 & x^2+x \\
 & \underline{-(x^2+x+3)} \\
 & 4x+3
\end{array}
$$

$$
\begin{array}{r|l}
\multicolumn{2}{r}{2x+3} \\
\cline{2-2}
4x+3 & 3x^2+3x+4 \\
 & \underline{-(3x^2+x)} \\
 & 2x+4 \\
 & \underline{-(2x+4)} \\
 & 0
\end{array}
$$

En monisk SGD är $4(4x+3) = x+2$.
$4x+3 = (2x^3+3x^2+x+1)-(4x+2)(3x^2+3x+4) = (2x^3+3x^2+x+1)-(4x+2)((x^4+4x+2)-(3x+3)(2x^3+3x^2+x+1)) = (2x^2+3x+2)(2x^3+3x^2+x+1)-(4x+2)(x^4+4x+2) = (2x^2+3x+2)((x^4+2x^3+3x^2+3)-(x^4+4x+2))-(4x+2)(x^4+4x+2) = (2x^2+3x+2)(x^4+2x^3+3x^2+3)-(2x^2+2x+4)(x^4+4x+2)$
$x+2 = (3x^2+2x+3)(x^4 2x^3+3x^2+3)+(2x^2+2x+4)(x^4+4x+2)$
$f(x) = 3x^2+2x+3 \qquad g(x) = 2x^2+2x+4$

8. (a) 2 och 3 är nollställen. $x^2+1 = (x-2)(x-3) = (x+3)(x+2)$. $(x+2)$ och $(x+3)$ är irreducibla faktorer.

   (b) 1, 2 och 3 är nollställen. $x^3+5x^2+5 = (x-1)(x-2)(x-3) = (x+10)(x+9)(x+8)$. $(x+10)$, $(x+9)$ och $(x+8)$ är irreducibla faktorer.

   (c) Polynomet saknar nollställe. Vi avgör om det kan skrivas som en produkt av andragradspolynom. Vi gör ansatsen $(x^2+ax+b)(x^2+cx+d) = x^3+3x^3+x+1$. $a+c = 3$, $b+d+ac = 0$, $ad+bc = 1$, $bd = 1$. Sätt först $c = 3-a$ och $d = \frac{1}{b}$. Sedan fås $b+\frac{1}{b}+(3-a)a = 0$ och $\frac{a}{b}+b(3-a) = 1$.
   Testa systematiskt: $b = 0$ är omöjligt.
   $b = 1 \Rightarrow 2+(3-a)a = 0$ och $a+(3-a) = 1$. Omöjligt.
   $b = 2 \Rightarrow (3-1)1 = 0$ och $3a+2(3-1) = 1$. $a = 0$ ger en lösning.
   $a = 0, b = 2 \Rightarrow c = 3, d = 3$
   $(x^2+2)(x^2+3x+3) = x^4+3x^2+x+1$
   (x^2+2) och x^2+3x+3 är irreducibla polynom.

9. De irreducibla andragradspolynomen kan skrivas på formen $(x+a)(x+b)$ där $a, b \in \mathbb{Z}_3$. De 6 olika möligheterna är: $x \cdot x = x^2$, $x \cdot (x+1) = x^2 + x$, $x \cdot (x+2) = x^2 + 2x$, $(x+1)(x+1) = x^2 + 2x + 1$, $(x+1)(x+2) = x^2 + 2$, $(x+2)^2 = x^2 + x + 1$.
De övriga moniska andragradspolynomen är irreducibla: x^2+1, x^2+x+2, x^2+2x+2.

4.8 Felrättande koder

1. En kod med minavstånd d rättar exakt e fel om $\left\lfloor \frac{d-1}{2} \right\rfloor = e$ och upptäcker k fel om $d - 1 = k$. Om d är minavståndet för C gäller då $d = 2e + 1$ eller $d = 2e + 2$. Fallen utreds var för sig.

   $d = 2e + 1$: Eftersom $d - 1 = 2e$ upptäcker C $2e$ fel. Till varje ord $x = x_1 x_2 \dots x_n$ lägger vi till siffran 1 om x har udda vikt och 0 om x har jämn vikt. Den nya koden får då minavståndet $2e + 2$ och upptäcker alltså $2e + 1$ fel.

   $d = 2e + 2 : d - 1 = 2e + 1$ visar att C upptäcker $2e + 1$ fel (och därmed även $2e$ fel). Koden C' kan fås genom att lägga till en godtycklig siffra till varje ord.

2. $n = antalet\ kolumner = 5$
   $k = n - rangen\ av\ matrisen.$
   Det går lätt att se att matrisen har rang 3. Så $k = 5 - 3 = 2$. Alla kolumner är olika och ingen består av nollor. Detta visar att koden rättar åtminstone ett fel och att $\delta \geq 3$. Men tex 10011 är ett kodord i koden. Så det finns ett kodord med vikt 3. Alltså är $\delta = 3$. Svaret är $(5, 2, 3)$.

3. (a) $H = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Det är fel i position 3. Rätt ord är 11110.

   (b) $H = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Det är ett kodord.

   (c) $H = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Det är fel i position 3. Rätt ord är 01101.

4. Ett ord $x_1x_2x_3x_4x_5x_6x_7$ har jämn vikt om och endast om $x_1+x_2+x_3+x_4+x_5+x_6+x_7 = 0$ i $\mathbb{Z}_2$. Detta ger att vi kan ta $H = (1111111)$ som kontrollmatris.

5. Varje ord x har 5 grannar med avstånd 1. Eftersom inget ord får vara granne till 2 kodord måste $|C| \cdot 6 \leq 2^5$ (2^5 är totala antalet ord). $|C| \leq \frac{32}{6} < 6$, så $|C|$ måste vara mindre än 6.

6. Antag att $x_i \neq y_i$. Då måste $x_i \neq z_i$ och/eller $y_i \neq z_i$ eftersom $x_i = z_i$ och $y_i = zi$ skulle leda till $x_i = y_i$.

   $\delta(x, y) =$ Antalet index i med $x_i \neq y_i$.

Varje index som ger bidrag till $\delta(x,y)$ ger också bidrag till $\delta(x,z)+\delta(z,y)$. Det visar att $\delta(x,y) \leq \delta(x,z)+\delta(z,y)$.

7. Låt $S(x)$ vara den mängd av kodord y som uppfyller $\delta(x,y) \leq 2$. Sådana ord kan fås genom att ta x och ändra i högst 2 positioner. Därför gäller $|S(x)| = 1+\binom{8}{1}+\binom{8}{2} = 37$. Om koden kan rätta 2 fel och har dimension k så måste $2^k \cdot 37 \leq 2^8$ dvs $k \leq 8-\log_2 37$. Detta leder till att $k \leq 2$. Största dimension är 2 (som ger $2^2 = 4$ kodord).

   Ett exempel på en sådan kod är $\{(00000000),(11111000),(00011111),(11100111)\}$. Det går lätt att se att mängden är sluten under addition och avståndet mellan 2 ord $\geq 2e+1 = 5$.

8. Låt $w(x) = \#(i \text{ där } x_i = 1)$. Om vi har två ord x, y gäller då $w(x) = \#(i \text{ dä r} x_i = 1 \text{ och } y_i = 0) + \#(i \text{ där } x_i = 1 \text{ och } y_i = 1)$ samt $w(y) = \#(i \text{ där } x_i = 0 \text{ och } y_i = 1) + \#(i \text{ där} x_i = 1 \text{ och } y_i = 1)$. $w(x+y) = \#(i \text{ där } x_i = 1 \text{ och } y_i = 0) + \#(i \text{ där } x_i = 0 \text{ och } y_i = 1)$. Alltså gäller $w(x+y) = w(x)+w(y)-2\cdot\#(i \text{ där } x_i = 1 \text{ och } y_i = 1)$.

   Om både $w(x)$ och $w(y)$ är jämna så måste $w(x+y)$ också vara jämnt. Det visar att $x, y \in C_0 \Rightarrow x+y \in C_0$. Så C_0 är en linjär kod. Vi ser också att om $w(x)$ är jämn och $w(y)$ är udda är $w(x+y)$ udda. Antag nu att C_0 är en äkta delmängd till C. Då finns det ett ord $y \in C$ med udda vikt. Om x är ett ord med jämn vikt så är $x+y$ ett ord i C med udda vikt. Funktionen $f(x) = x+y$ ger en funktion från C_0 till mängden av ord med udda vikt. Den är injektiv eftersom $f(x_1) = f(x_2) \Rightarrow x_1+y = x_2+y \Rightarrow x_1 = x_2$. Den är surjektiv eftersom vi till varje ord z med udda vikt kan välja $x = z+y$ (x har då jämn vikt). Då gäller $f(x) = z+y+y = z$. Det finns alltså en bijektion mellan orden med jämn vikt och de med udda vikt i C. Därför gäller $|C_0| = \frac{n}{2}$.

9. H ger följande ekvationer:

$$\begin{cases} x_1+x_2+x_4+x_7=0 \\ x_4+x_5+x_7=0 \\ x_1+x_3+x_4+x_7=0 \\ x_6+x_7=0 \end{cases} \qquad \begin{cases} x_2=x_1+x_4+x_7 \\ x_5=x_4+x_7 \\ x_3=x_1+x_4+x_7 \\ x_6=x_7 \end{cases}$$

   x_1, x_4, x_7 kan väljas godtyckliga. Sedan är x_2, x_3, x_5, x_6 entydigt bestämda. De 8 valen av x_1, x_4, x_7 ger orden $\{(0000000),(1111001),(1110010),(0001011),(1010100),$ $(0101101),(0100110),(1011111)\}$.
   $n = 7$ och $k = 3$. $\delta = 3$.

10. Vi vill ha en matris med n kolumner och rang r. Vi vill att $n-r = 8$ så att koden har $2^8 = 256$ ord. Vi vill dessutom att alla kolumner skall vara olika och att ingen kolumn har enbart nollor som element. Om m är antalet rader i H måste då $2^m > n$ och $m > r$. Vi sätter $m = r$ vilket ger $2^r > n = r+8$. Det minsta r och n som gör det möjligt är $r = 4$ och $n = 12$. Vi kan tex sätta

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