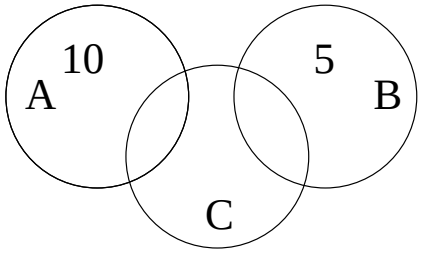
Lösningar till utvalda uppgifter i kapitel 2

2.15 Ett Venn-diagram över situationen ser ut så här:



För att få ihop 30 element totalt så måste de tre okända fälten innehålla exakt 15 element och alla dessa ligger i C som därför måste innehålla exakt 15 element.

2.16 (a) Sant, ty $A \Delta A^c = (A \setminus A^c) \cup (A^c \setminus A) = A \cup A^c = U$.

(b) Falsk, ty om vi t.ex. tar $B = C = \emptyset$ så blir likheten $\emptyset = A$ vilket inte stämmer för alla A.

(c) Falsk, ty om vi t.ex. tar $A = B = \{1, 2\}$ och $C = \{1\}$ så blir $(A \setminus B) \setminus C = \emptyset$ medan $A \setminus (B \setminus C) = \{1\}$.

(d) Falsk alltid då $A \neq B$.

(e) Falsk, ty om vi t.ex. tar $A = \{2\}$, $B = \{1\}$ och $U = \{1, 2\}$ så blir $(A \cup B)^c = \emptyset$ medan $A^c \cup B^c = U$.

Lösningar till utvalda uppgifter i kapitel 3

3.37 (a) Att '$\leq$' är reflexiv, antisymmetrisk och transitiv följer direkt av att 'den vanliga' $\leq$ är det på $\mathbb{N}$ och $\mathbb{Z}$.

(b) Följden $m_n = (-n, -n)$ där $n = 0, 1, 2, \ldots$ är ett exempel på en strängt avtagande följd i $\mathbb{Z} \times \mathbb{Z}$ som är oändlig och därmed är '$\leq$' inte välgrundad på $\mathbb{Z} \times \mathbb{Z}$.

(c) Antag att vi har en strängt avtagande följd i $\mathbb{N} \times \mathbb{N}$ med första element (a, b). Då kan denna innehålla högst $a + b + 1$ par, ty någon av de båda koordinaterna måste minska i varje steg i följden per definition av '$\leq$' och den första kan minska högst a gånger och den andra högst b gånger. Alltså är varje strängt avtagande följd ändlig och därmed är '$\leq$' välgrundad på $\mathbb{N}$.

3.29 (a) Relationen $\mathcal{R}_1$ är reflexiv, ty $f(x) \leq f(x)$ för alla naturliga tal x och alla $f \in M$.

Relationen $\mathcal{R}_1$ är antisymmetrisk, ty om $f(x) \leq g(x)$ och $g(x) \leq f(x)$ för alla naturliga tal x så är $f = g$.

Relationen $\mathcal{R}_1$ är transitiv, ty om $f(x) \leq g(x)$ och $g(x) \leq h(x)$ för alla naturliga tal så är uppenbarligen $f(x) \leq h(x)$ för alla naturliga tal x.

Därmed har vi visat att $\mathcal{R}_1$ är en partiell ordning.

Ingen av de två andra relationerna är antisymmetriska (och inte heller transitiva) och därmed inga partiella ordningar. Om vi t.ex. väljer $f(x) = 0$ och $g(x) = x$ så gäller det att $f\mathcal{R}_2 g$, $g\mathcal{R}_2 f$ och $f\mathcal{R}_3 g$, $g\mathcal{R}_3 f$ eftersom $f(0) = g(0)$ och $\sum_{i=0}^{0} f(i) = \sum_{i=0}^{0} g(i)$.

(b) Minimalt och minsta element är $f(x) = 0$. Största och maximala element saknas eftersom $\mathbb{N}$ saknar sådana element.

3.32 (a) Tag $(a, b) \in \mathcal{R} \circ \mathcal{R}^{-1}$. Per definition är detta ekvivalent med att det finns $c \in M$ sådant att $a\mathcal{R}c$ och $c\mathcal{R}^{-1}b$. Det ger per definition av $\mathcal{R}^{-1}$ att $c\mathcal{R}^{-1}a$ och $b\mathcal{R}c$ och alltså $(b, a) \in \mathcal{R} \circ \mathcal{R}^{-1}$ vilket visar att $\mathcal{R} \circ \mathcal{R}^{-1}$ är symmetrisk.

(b) Vi har

$$\begin{aligned}\mathcal{R}\circ\mathcal{R}^{-1} \text{ reflexiv} &\iff \forall a\in M\ a(\mathcal{R}\circ\mathcal{R}^{-1})a\\ &\iff \forall a\in M\ \exists c\in M\ (a\mathcal{R}c\wedge c\mathcal{R}^{-1}a)\\ &\iff \forall a\in M\ \exists c\in M\ a\mathcal{R}c.\end{aligned}$$

Alltså uttryckt i ord så måste alla element i M vara relaterat till åtminstone ett element.

3.37 (a) Tag t.ex. $A = C = \{0\}$ och $B = \{0, 1\}$ och $f(x) = g(x) = 0$ för alla x i respektive definitionsmängd.

(b) Antag att $g \circ f$ är bijektiv. Tag $x, y \in A$ med $f(x) = f(y)$. För att visa att f är injektiv så ska vi visa att i så fall är $x = y$. Men $g \circ f(x) = g \circ f(y)$ och eftersom $g \circ f$ är bijektiv och speciellt injektiv så följer det att $x = y$ och alltså är f injektiv.

Antag återigen att $g \circ f$ är bijektiv. För att visa att g är surjektiv så ska vi visa att $g(B) = C$. Men $g \circ f$ är bijektiv och speciellt surjektiv så $g \circ f(A) = C$. Men $f(A) \subseteq B$ så vi får $C = g(f(A)) \subseteq g(B)$ och alltså är $g(B) = C$ och därmed är g surjektiv.

3.37 (a) För negativa x avtar funtionen ifrån oändligheten mot 2 eftersom $-3x$ är strängt avtagande. Funktionen fortsätter avta för positiva x med start vid 2 eftersom $-x^2$ är strängt avtagande för positiva x och går mot minus oändligheten då x går mot oändligheten. Alltså antar funktionen alla reella tal precis en gång.

(b) Sätt $y = g(x)$. Då är $x = g^{-1}(y)$. För $x < 0$ är $y > 2$ och då har vi $y = 2 - 3x$ så $x = (2 - y)/3$. Alltså är

$$g^{-1}(y) = \frac{2-y}{3}, \text{ för } y > 2.$$

För $x \geq 0$ är $y \leq 2$ och då har vi $y = 2 - x^2$ så $x = \sqrt{2-y}$. Alltså är

$$g^{-1}(y) = \sqrt{2-y}, \text{ för } y \leq 2.$$

Sammantaget får vi alltså

$$g^{-1}(y) = \begin{cases} \frac{2-y}{3} & \text{för } y > 2, \\ \sqrt{2-y} & \text{för } y \leq 2. \end{cases}$$

3.38 (a) En av grundtankarna med personnumret är ju att varje person ska få ett unikt nummer, med andra ord att denna funktion är injektiv. Den är inte surjektiv eftersom det finns många fler 12-siffriga tal än det finns människor på jorden och speciellt börjar alla personnummmer med en etta eller tvåa.

(b) Inte heller denna är surjektiv eftersom första siffran i $g(x)$ kommer alltid att vara en etta eller tvåa. Det största möjliga tal man kan få från funktionen idag är garanterat mindre än 20100828 och det minsta är garanterat större än $18950000 - 9999 = 18940001$. Alltså är antalet möjliga värden högst $20100828 - 18940000 = 1160828$ vilket är mindre än antalet personer med svenskt personnummer. Alltså är funktionen inte injektiv.

3.39 (a) Funktionen är inte injektiv eftersom $\varphi(p, q) = \varphi(q, p)$ per definition.

(b) Funktionen är inte surjektiv eftersom vi bara får polynom med reella nollställen så att t.ex. $(0, 1)$ som svarar mot $x^2 + 1$ träffas inte av φ.

(c) Polynomet som har p och q som nollställen är

$$(x - p)(x - q) = x^2 - (p + q)x + pq$$

så $\varphi(p, q) = (-(p + q), pq)$. Vi får alltså ekvationssystemet

$$\begin{aligned} p &= -p - q \\ q &= pq. \end{aligned}$$

Om $q \neq 0$ så ger den andra ekvationen $p = 1$ vilket ger $q = -2p = -2$ enligt den första. Andra möjligheten är $q = 0$ vilket ger $p = 0$. Vi har alltså två lösningspar: $(0, 0)$ och $(1, -2)$

3.12 (a) Den är injektiv, ty de tre elementen i definitionsmängden avbildas på tre olika element. Den är inte surjektiv, ty inget element avbildas på 4 som finns i målmängden.

(b) Den är inte injektiv, ty $g(3) = g(4)$. Den är surjektiv, ty alla de tre elementen i målmängden finns i värdemängden.

(c) Vi har att

$$f \circ g : B \longrightarrow B,\ f \circ g(1) = 1,\ f \circ g(2) = 2,\ f \circ g(3) = f \circ g(4) = 3,$$

samt

$$g \circ f : A \longrightarrow A,\ g \circ f(x) = x \text{ för alla } x.$$

(d) Vi ser ifrån svaret på förra deluppgiften att $g \circ f$ är identitetsfunktionen på A och därmed är den både injektiv och surjektiv. För $f \circ g$ får vi att den inte är surjektiv (ty 4 finns i målmängden men inte i värdemämgden) och inte heller injektiv (ty $f \circ g(3) = f \circ g(4)$).

3.42 Vi definierar $f, g \in M$ genom

$$\begin{cases} f(0) &= 1, \\ f(1) &= 0, \\ f(x) &= x, \text{ då } x > 1, \end{cases} \quad \text{och} \quad \begin{cases} g(0) &= 2, \\ g(1) &= 0, \\ g(2) &= 1, \\ g(x) &= x, \text{ då } x > 2. \end{cases}$$

Vi får då att

$$\begin{aligned} f \star g(0) &= f(g(f^{-1}(g^{-1}(0)))) \\ &= f(g(f^{-1}(1))) = f(g(0)) = f(2) = 2 \end{aligned}$$

och att

$$\begin{aligned} g \star f(0) &= g(f(g^{-1}(f^{-1}(0)))) \\ &= g(f(g^{-1}(1))) = g(f(2)) = g(2) = 1. \end{aligned}$$

Alltså är $f \star g \neq g \star f$ och därmed är $\star$ inte kommutativ.

3.43 (a) Ja, den är kommutativ ty

$$\begin{aligned}(c+dx)\star(a+bx) &= (ca-db)+(da+cb)x \\ &= (ac-bd)+(ad+bc)x = (a+bx)\star(c+dx)\end{aligned}$$

eftersom multiplikation av tal är kommutativ.

(b) Ja, den är associativ ty

$$\begin{aligned}((a+bx)\star(c+dx)) \quad \star \quad (e+fx) &= ((ac-bd)+(ad+bc)x)\star(e+fx) \\ &= (ac-bd)e-(ad+bc)f+((ac-bd)f+(ad+bc)e)x \\ &= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)x\end{aligned}$$

och

$$\begin{aligned}(a+bx)\star((c+dx) \quad \star \quad (e+fx)) &= (a+bx)\star((ce-df)+(cf+de)x) \\ &= a(ce-df)-b(cf+de)+(a(cf+de)+b(ce-df))x \\ &= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)x\end{aligned}$$

där vi utnyttjar att multiplikation av tal är associativ och kommutativ.

(c) Ja, konstanta poynomet $1 = 1+0x$ är en identitet, ty

$$(1+0x)\star(a+bx) = 1\cdot a-0\cdot b+(1\cdot b+0\cdot x)x = a+bx$$

och vice versa eftersom den är kommutativ.

(d) Om man sätter $x^2 = -1$ så är operatorn helt enkelt multiplikation av poynom med denna extra regel, så i själva verket är det multiplikation av komplexa tal om man tänker sig att $a+bx$ betyder $a+bi$.

3.45 (a) Alla element i $[(1,0)] = \{(x,0) : x \neq 0\}$ och i $[(0,0)] = \{(0,0)\}$ ger värdet 0. Alla andra ekvivalensklasser innehåller bara element (x,y) med $y \neq 0$. Tag två godtyckliga element (x,y) och (cx,cy) ur samma ekvivalensklass $(c, y \neq 0)$. Eftersom $\frac{x}{y} = \frac{cx}{cy}$ så ger f samma värde för de båda elementen i $[(x,y)]$ och alltså beror inte värdet av f på vilken representant man väljer.

(b) T.ex. är $(1,1)$ och $(2,2)$ i samma ekvivalensklass, men g ger värdena 1 respektive 4.

(c) Den är inte injektiv, ty $[(0,0)] \neq [(1,0)]$ men $f([(0,0)]) = f([(1,0)])$.

(d) Den är surjektiv, ty givet $r \in \mathbb{R}$ så är $f([(r,1)]) = r$.

3.47 Vi ska visa att $\mathcal{R}$ är reflexiv, antisymmetrisk och transitiv.

Reflexiv: Låt a vara ett godtyckligt element i M. Vi har $0 \in P$ enligt första villkoret och $a = a \star 0$ så $(a,a) \in \mathcal{R}$. Alltså är $\mathcal{R}$ reflexiv.

Antisymmetrisk: Låt a och b vara godtyckliga element i M. Antag att $(a,b),(b,a) \in \mathcal{R}$. Vi ska visa att i så fall är $a = b$. Från antagandet följer det att det finns $p_1, p_2 \in P$ sådana att

$$a = b \star p_1 \text{ och } b = a \star p_2.$$

Vi får då (genom att utnyttja associativiteten)

$$b = a \star p_2 = (b \star p_1) \star p_2 = b \star (p_1 \star p_2).$$

Genom att "addera" $-b$ från vänster på båda sidor och utnyttja $0 \star x = x$ så får vi $0 = p_1 \star p_2$ och därmed att $p_1 = -p_2$. Vi har alltså att $p_2 \in P$ och $-p_2 = p_1 \in P$ och enligt tredje villkoret är därmed $p_2 = 0$. Alltså är

$$b = a \star p_2 = a \star 0 = a$$

och vi har därmed visat att $\mathcal{R}$ är antisymmetrisk.

Transitiv: Låt a, b och c vara godtyckliga element i M. Antag att $(a,b),(b,c) \in \mathcal{R}$ och visa att i så fall $(a,c) \in \mathcal{R}$. Från vårt antagande följer det att det finns $p_1, p_2 \in P$ sådana att

$$a = b \star p_1 \text{ och } b = c \star p_2.$$

Vi får (genom att återigen utnyttja associativiteten)

$$a = b \star p_1 = (c \star p_2) \star p_1 = c \star (p_2 \star p_1).$$

Men $p_2 \star p_1 \in \mathcal{R}$ enligt det andra villkoret och därmed har vi att $(a, c) \in \mathcal{R}$. Alltså är $\mathcal{R}$ transitiv och därmed en partiell ordning.

3.48 (a) Tag t.ex. $\mathcal{R} = \{(1,2),(1,3),(2,3)\}$. Då gäller att $\mathcal{R}^2 = \{(1,3)\}$ och $\mathcal{R}^3 = \emptyset$

(b) Relationen $\mathcal{R}$ kan inte innehålla något element av typen (a, a), ty i så fall kommer detta att ingå i varje potens. (Man kan köra hur många varv som helst i en loop.)

Om den innehåller ett par av par av typen (a, b) och (b, a) så kommer $\mathcal{R}^2$ att innehålla (a, a) och (b, b). Därmed kommer sedan $\mathcal{R}^3$ återigen att innehålla (a, b) och (b, a). Induktivt får vi att $\mathcal{R}^{2n+1}$ innehåller (a, b) och (b, a) och $\mathcal{R}^{2n}$ innehåller (a, a) och (b, b) för alla naturliga tal n. Därmed kan $\mathcal{R}$ inte innehålla något sådant par av par.

Därmed kan den högst innehålla ett av varje möjligt par av olika element, dvs. högst 3 stycken. Men i förra uppgiften såg vi att det gick att hitta 3 stycken par så att det gäller så svaret är: 3.

Lösningar till utvalda uppgifter i kapitel 4

4.7 Vi visar först att $A_{2n} = 3 \cdot 2^n - 2$ med ett induktionsbevis.

Basfall: $n = 0$

Vi har att

$$3 \cdot 2^0 - 2 = 1 = A_0,$$

och alltså gäller likheten för $n = 0$.

Induktionssteget: Antag nu att det gäller för ett fixt jämnt naturligt tal $2n$. Visa att då gäller det också för $2(n+1)$. Vi får

$$A_{2n+2} = 2A_{2n+1} = 2(A_{2n} + 1) = 2(3 \cdot 2^n - 2 + 1) = 3 \cdot 2^{n+1} - 2,$$

och alltså gäller likheten också för $2(n+1)$.

Enligt induktionsprincipen gäller därmed likheten för alla jämna naturliga tal.

För de udda talen observerar vi bara att $A_{2n+1} = A_{2n} + 1 = 3 \cdot 2^{n+1} - 1$ enligt ovan.

4.8 Vi gör ett induktionsbevis.

Basfall: $n = 0$

Då gäller att

$$\sum_{i=1}^{0} F(2i-1) = 0 = F(2 \cdot 0),$$

och alltså gäller likheten för $n = 0$.

Induktionssteget: Antag nu att det gäller för ett fixt naturligt tal n. Visa att då gäller det också för $n+1$. Vi får

$$\begin{aligned}\sum_{i=1}^{n+1} F(2i-1) &= \sum_{i=1}^{n} F(2i-1) + F(2(n+1)-1) \\ &= F(2n) + F(2n+1) = F(2n+2) = F(2(n+1))\end{aligned}$$

och alltså gäller likheten också för $n+1$.

Enligt induktionsprincipen gäller därmed likheten för alla naturliga tal.

4.9 Vi gör ett induktionsbevis.

Basfall: Vi får i fallet $n = 4$ att $2^4 = 16 < 24 = 4!$ så påståendet är sant för $n = 4$.

Induktionssteg: Antag att påståendet är sant för något n med $n \geq 4$. Vi ska visa att då är det också sant för $n+1$. Genom att utnyttja induktionsantagandet och att $(n+1) > 4 > 2$ så får vi

$$(n+1)! = (n+1)n! > (n+1)2^n > 2 \cdot 2^n = 2^{n+1},$$

vilket är precis påståendet för $n+1$. Därmed följer det av induktionsprincipen att påståendet är sant för alla naturliga tal $n > 3$.

4.10 Sätt $f(n) = \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right)$ och $g(n) = \frac{n+1}{2n}$. Då ska vi bevisa att $f(n) = g(n)$ för alla naturliga tal $n > 1$. Vi gör ett induktionsbevis.

Basfall: $n = 2$. Då har vi

$$f(2) = \prod_{i=2}^{2} \left(1 - \frac{1}{i^2}\right) = 1 - \frac{1}{2^2} = \frac{3}{4} = \frac{2+1}{2 \cdot 2} = g(2),$$

så påståendet är sant för $n = 2$.

Induktionssteg: Antag att det är sant för n och visa att då är det också sant för $n+1$. Genom att utnyttja induktionsantagandet så får vi

$$\begin{aligned} f(n+1) &= \prod_{i=2}^{n+1} \left(1 - \frac{1}{i^2}\right) = \prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right) \\ &= f(n) \cdot \frac{(n+1)^2 - 1}{(n+1)^2} = g(n) \cdot \frac{n^2 + 2n}{(n+1)^2} = \frac{n+1}{2n} \cdot \frac{n^2 + 2n}{(n+1)^2} \\ &= \frac{n(n+2)}{2n(n+1)} = \frac{n+2}{2(n+1)} = g(n+1). \end{aligned}$$

Enligt induktionsprincipen är påståendet därmed sant för alla heltal $n > 1$.

4.11 (a) Genom att utnyttja rekursionen så får vi

$$\begin{aligned} F_1(x) &= (x-1)+x^2 \\ F_2(x) &= (x^2+x-1)(x-1)+x^2 = x^3+x^2-2x+1 \\ F_3(x) &= (x^3+x^2-2x+1)(x-1)+x^2 = x^4-2x^2+3x-1 \end{aligned}$$

(b) Vi sätter $f(n) = F_n(0)$ och $g(n) = (-1)^n$ och ska alltså visa att $f(n) = g(n)$ för alla $n \in \mathbb{N}$. Vi gör ett induktionsbevis:
Basfall: $n = 0$. Vi har $f(0) = 1$ per definition och $g(0) = (-1)^0 = 1$ så det stämmer för $n = 0$.
Induktionssteg: Antag att $f(n) = g(n)$ för något fixt tal $n \geq 0$. Vi ska visa att i så fall är $f(n+1) = g(n+1)$. Om vi utnyttjar rekursionen

$$f(n+1) = f(n)(0-1)+0 = -f(n)$$

och induktionsantagandet så får vi

$$f(n+1) = -f(n) = -g(n) = -(-1)^n = (-1)^{n+1} = g(n+1).$$

Nu följer det av induktionsaxiomet att $f(n) = g(n)$ för alla naturliga tal n.

4.13 Basfall: $n = 0$. Vi har att båda leden är lika med 1. Alltså stämmer det för $n = 0$.

Induktionssteg: Antag att påståendet är sant för n. Vi ska visa att då är det också sant för $n+1$. Genom att använda induktionsantagandet så får vi

$$\begin{aligned} \sum_{i=1}^{n+1} a^i &= \sum_{i=1}^{n} a^i + a^{n+1} = \frac{a^{n+1}-1}{a-1} + a^{n+1} \\ &= \frac{a^{n+1}-1}{a-1} + \frac{a^{n+1}(a-1)}{a-1} = \frac{a^{n+2}-1}{a-1}, \end{aligned}$$

vilket är lika med högerledet för $n+1$.

Alltså är påståendet sant för $n+1$ om man antar att det är sant för n och därmed följer det av induktionsaxiomet att det är sant för alla naturliga tal n.

4.16 Vi gör ett induktionsbevis.

Basfall: $n = 1$

Då gäller att

$$VL = \sum_{k=1}^{1} k \cdot 2^{k-1} = 1 \cdot 2^0 = 1 \text{ och } HL = (1-1) \cdot 2^1 + 1 = 1,$$

och alltså gäller likheten för $n = 1$.

Induktionssteget: Antag nu att det gäller för ett fixt positivt heltal n. Visa att då gäller det också för $n+1$. Vi får

$$\begin{aligned} \sum_{k=1}^{n+1} k \cdot 2^{k-1} &= \sum_{k=1}^{n} k \cdot 2^{k-1} + (n+1) \cdot 2^n = \\ &= (n-1) \cdot 2^n + 1 + (n+1) \cdot 2^n = 2n \cdot 2^n + 1 = \\ &= ((n+1)-1) \cdot 2^{n+1} + 1, \end{aligned}$$

och alltså gäller likheten också för $n+1$.

Enligt induktionsprincipen gäller därmed likheten för alla positiva heltal.

4.17 Vi gör ett induktionsbevis.

Basfall: Vi behöver två fall $n = 3$ och $n = 4$. Vi har

$$\begin{aligned} L(3) &= L(2) + L(1) = b + a \\ bF(3-1) + aF(3-2) &= b + a \end{aligned}$$

och

$$\begin{aligned} L(4) &= L(3) + L(2) = (b+a) + b = 2b + a \\ bF(4-1) + aF(4-2) &= b \cdot 2 + a \cdot 1 = 2b + a \end{aligned}$$

så båda basfallen stämmer.

Induktionssteg: Antag att det är sant för alla k sådana att $k \leq n$ där $n \geq 4$ och visa att då är det också sant för $n+1$. Genom att utnyttja induktionsantagandet och rekursionen för Fibonacci-talen så får vi

$$\begin{aligned} L(n+1) &= L(n) + L(n-1) \\ &= bF(n-1) + aF(n-2) + bF(n-1-1) + aF(n-1-2) \\ &= b(F(n-1) + F(n-2)) + a(F(n-2) + F(n-3)) \\ &= bF(n) + aF(n-1) \end{aligned}$$

vilket var precis vad vi skulle visa.

Enligt induktionsprincipen är påståendet därmed sant för alla positiva heltal $n > 2$.

4.18 Vi gör ett induktionsbevis.

Basfall: $n = 0$. Vi har att båda leden är lika med 0. Alltså stämmer det för $n = 0$.

Induktionssteg: Antag att påståendet är sant för n. Vi ska visa att då är det också sant för $n+1$. Genom att använda induktionsantagandet så får vi

$$\begin{aligned} \sum_{i=1}^{n+1} i \cdot i! &= \sum_{i=1}^{n} i \cdot i! + (n+1)(n+1)! \\ &= ((n+1)! - 1) + (n+1)(n+1)! \\ &= (1 + n + 1)(n+1)! - 1 \\ &= (n+2)(n+1)! - 1 = (n+2)! - 1, \end{aligned}$$

vilket är lika med högerledet för $n+1$.

Alltså är påståendet sant för $n+1$ om man antar att det är sant för n och därmed följer det av induktionsaxiomet att det är sant för alla naturliga tal n.

4.19 Definiera först

$$f(n) = \sum_{k=1}^{n} \frac{1}{k^2} \text{ och } g(n) = 2 - \frac{1}{n}.$$

Vi ska då visa att $f(n) < g(n)$, eller ekvivalent att $f(n) - g(n) < 0$, för alla heltal $n > 1$. Vi gör ett induktionsbevis.

Basfall: Om $n = 2$ så får vi

$$f(2) - g(2) = \sum_{k=1}^{2} \frac{1}{k^2} - \left(2 - \frac{1}{2}\right) = 1 + \frac{1}{4} - \frac{3}{2} = -\frac{1}{4} < 0.$$

Alltså stämmer det för $n = 2$.

Induktionssteg: Antag att $f(p) < g(p)$ för något $p > 1$. Visa att i så fall är $f(p+1) < g(p+1)$. Vi tittar på differensen och får om vi i andra steget utnyttjar induktionsantagandet att

$$\begin{aligned}
f(p+1) - g(p+1) &= \left(f(p) + \frac{1}{(p+1)^2}\right) - g(p+1) \\
&< g(p) + \frac{1}{(p+1)^2} - g(p+1) \\
&= \left(2 - \frac{1}{p}\right) + \frac{1}{(p+1)^2} - \left(2 - \frac{1}{p+1}\right) \\
&= -\frac{1}{p} + \frac{1}{(p+1)^2} + \frac{1}{p+1} \\
&= \frac{-(p+1)^2 + p + p(p+1)}{p(p+1)^2} \\
&= \frac{-p^2 - 2p - 1 + p + p^2 + p}{p(p+1)^2} \\
&= \frac{-1}{p(p+1)^2} < 0.
\end{aligned}$$

Enligt indukionsprinipen gäller därmed, med stöd av basfall och induktionssteg, att $f(n) < g(n)$ för alla heltal $n > 1$.

4.20 Definiera först

$$f(n) = \sum_{k=1}^{2n} (-1)^{k+1} \frac{1}{k} \text{ och } g(n) = \sum_{k=n+1}^{2n} \frac{1}{k}.$$

Vi ska då visa att $f(n) = g(n)$ för alla heltal $n \geq 1$. Vi gör ett induktionsbevis.

Basfall: Om $n = 1$ så får vi

$$f(1) = \sum_{k=1}^{2} (-1)^{k+1} \frac{1}{k} = 1 - \frac{1}{2} = \frac{1}{2},$$
$$g(1) = \sum_{k=2}^{2} \frac{1}{k} = \frac{1}{2}.$$

Alltså stämmer det för $n = 1$.

Induktionssteg: Antag att $f(p) = g(p)$ för något $p \geq 1$. Visa att i så fall är $f(p+1) = g(p+1)$. Vi startar med $f(p+1)$ och får om vi i fjärde steget utnyttjar induktionsantagandet att

$$\begin{aligned}
f(p+1) = \sum_{k=1}^{2(p+1)} (-1)^{k+1} \frac{1}{k} &= \sum_{k=1}^{2p} (-1)^{k+1} \frac{1}{k} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= f(p) + \frac{1}{2p+1} - \frac{1}{2p+2} = g(p) + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= \sum_{k=p+1}^{2p} \frac{1}{k} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= \sum_{k=(p+1)+1}^{2(p+1)} \frac{1}{k} + \frac{1}{p+1} - \frac{1}{2p+1} - \frac{1}{2p+2} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= g(p+1) + \frac{1}{p+1} - 2\frac{1}{2p+2} = g(p+1).
\end{aligned}$$

Enligt indukionsprinipen gäller därmed, med stöd av basfall och induktionssteg, att $f(n) = g(n)$ för alla heltal $n \geq 1$.

Lösningar till utvalda uppgifter i kapitel 5

5.3. Vi använder Euklides algoritm och får

$$\begin{aligned} 4485 &= 1 \cdot 3042 + 1443 \\ 3042 &= 2 \cdot 1443 + 156 \\ 1443 &= 9 \cdot 156 + 39 \\ 156 &= 4 \cdot 39. \end{aligned}$$

Alltså är $\text{sgd}(3042, 4485) = 39$. Om vi startar från näst sista likheten och successivt ersätter med ekvationen ovanför så får vi

$$\begin{aligned} 39 &= 1443 - 9 \cdot 156 = 1443 - 9(3042 - 2 \cdot 1443) \\ &= -9 \cdot 3042 + 19 \cdot 1443 \\ &= -9 \cdot 3042 + 19(4485 - 3042) = 19 \cdot 4485 - 28 \cdot 3042. \end{aligned}$$

Alltså är $19 \cdot 4485 - 28 \cdot 3042 = \text{sgd}(3042, 4485)$.

5.12. Vi ser direkt att 5 delar 1615 och vi har $1615 = 5 \cdot 323$. Testa successivt om primtalen 3, 5, 7, 11, 13 och 17 delar 323. (Vi behöver inte kolla längre eftersom $19^2 = 361 > 323$.). För 17 finner vi att divisionen går jämnt ut och vi får $323 = 17 \cdot 19$. Svaret är alltså $1615 = 5 \cdot 17 \cdot 19$.

Första kandidaten 1617 kan vi utesluta eftersom siffersumman är 15 och alltså delbar med 3 och därmed är 1617 delbart med 3.

Nästa kandidat är 1619. Vi behöver testa alla primtal p som uppfyller $p \leq \sqrt{1619} < 41$. Dessa är 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 och 37. De tre första utesluter vi omedelbart och

sedan får vi successivt

$$\begin{aligned}
1619 &= 7 \cdot 231 + 2 \\
1619 &= 11 \cdot 147 + 2 \\
1619 &= 13 \cdot 124 + 7 \\
1619 &= 17 \cdot 95 + 4 \\
1619 &= 19 \cdot 85 + 4 \\
1619 &= 23 \cdot 70 + 9 \\
1619 &= 29 \cdot 55 + 24 \\
1619 &= 31 \cdot 52 + 7 \\
1619 &= 37 \cdot 43 + 28.
\end{aligned}$$

Inget av de möjliga primtalen delar 1619 och alltså är detta det efterfrågade primtalet.

5.7. Euklides algoritm ger:

$$\begin{aligned}
504 &= 1 \cdot 301 + 203 \\
301 &= 1 \cdot 203 + 98 \\
203 &= 2 \cdot 98 + 7 \\
98 &= 14 \cdot 7
\end{aligned}$$

Alltså är $\text{sgd}(504, 301) = 7$. Vi ersätter successivt de erhållna resterna och får:

$$\begin{aligned}
7 &= 203 - 2 \cdot 98 = 203 - 2 \cdot (301 - 1 \cdot 203) = 3 \cdot 203 - 2 \cdot 301 \\
&= 3 \cdot (504 - 1 \cdot 301) - 2 \cdot 301 = 3 \cdot 504 - 5 \cdot 301.
\end{aligned}$$

En lösning är alltså $x = 3$ och $y = -5$. Om vi förkortar med 7 så får vi ekvationen $72x + 43y = 1$ och alla lösningar ges därmed av $x = 3 + 43n$ och $y = -5 - 72n$ med $n \in \mathbb{Z}$.

5.8. Euklides algoritm ger:

$$\begin{aligned}
336 &= 2 \cdot 147 + 42 \\
147 &= 3 \cdot 42 + 21 \\
42 &= 2 \cdot 21.
\end{aligned}$$

Vi observerar att $2121 = 101 \cdot 21$ och alltså finns det heltalslösningar till ekvationen. För att förenkla räkningarna något förkortar vi ekvationen med den största gemensamma delaren 21 och får

$$7x + 16y = 101.$$

Om vi dividerar alla talen i vår kalkyl med Euklides algoritm ovan så får vi

$$\begin{aligned} 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1. \end{aligned}$$

Vi ersätter successivt de erhållna resterna och får:

$$1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (16 - 2 \cdot 7) = 7 \cdot 7 - 3 \cdot 16.$$

En lösning till $7x + 16y = 1$ är alltså $x = 7$ och $y = -3$. Därmed får vi en lösning $x = 7 \cdot 101 = 707$ och $y = -3 \cdot 101 = -303$ till vår ekvation. Den allmänna lösningen är då

$$\begin{cases} x = 707 - 16k \\ y = -303 + 7k \end{cases}$$

med $k \in \mathbb{Z}$. Det minsta tal k sådant att $y = -303 + 7k > 0$ är $k = 44$ som ger $y = 5$ och $x = 3$. Om $k > 44$ så är

$$x = 707 - 16k < 707 - 16 \cdot 45 = -13 < 0,$$

så $y = 5$ och $x = 3$ är enda positiva heltalslösningen.

5.19. Man kan antingen prova alla klasser modulo 11 eller t.ex. kvadratkomplettera

$$x^2 + x + 1 \equiv (x + 6)^2 - 36 + 1 \equiv (x + 6)^2 - 2.$$

Detta ger

$$x^2 + x + 1 \equiv 2 \iff (x + 6)^2 \equiv 4 \iff x + 6 \equiv \pm 2 \iff x \equiv 5 \pm 2.$$

De x som uppfyller ekvationen är alltså alla som är kongruenta med 3 eller 7 modulo 11.

5.19. Välj $a = 3$. Då är $a^0 \equiv 1$, $a^1 \equiv 3$, $a^2 \equiv 2$, $a^3 \equiv 6$, $a^4 \equiv 4$, $a^5 \equiv 5$ så $a = 3$ uppfyller kravet. Även $a = 5$ duger.

5.27 Primtalsfaktoriseringen blir $5418 = 2 \cdot 3^2 \cdot 7 \cdot 43$. Från multiplikativiteten hos Eulers Φ-funktion och att

$$\Phi(p^k) = p^{k-1}(p-1)$$

om p är ett primtal samt primatalsfaktoriseringen från första deluppgiften får vi att

$$\Phi(5418) = \Phi(2) \cdot \Phi(3^2) \cdot \Phi(7) \cdot \Phi(43) = 1 \cdot (3 \cdot 2) \cdot 6 \cdot 42 = 1512.$$

Enligt Eulers sats vet vi att

$$5^{\Phi(5418)} = 5^{1512} \equiv 1 \pmod{5418},$$

ty $\text{sgd}(5, 5418) = 1$. Det ger att

$$5^{1513} \equiv 5 \pmod{5418}$$

så svaret är 5.

5.28 Vi primtalsfaktoriserar $132 = 2^2 \cdot 3 \cdot 11$ och multiplikativiteten för Φ och formeln för dess värde på primtalspotenser ger att

$$\Phi(132) = \Phi(2^2)\Phi(3)\Phi(11) = 2 \cdot (2-1) \cdot (3-1) \cdot (11-1) = 40.$$

Vi ser direkt att varken 2 eller 3 delar 1121 och eftersom $1122 = 11 \cdot 102$ så gäller också $11 \nmid 1121$. Alltså är $\text{sgd}(1121, 132) = 1$. (Man kunde förstås också visat detta med Euklides algoritm.) Vi får också (första steget i Euklides algoritm, så där hade man lite nytta av om man gjort detta redan) att

$$1121 = 8 \cdot 132 + 65 \text{ så } 1121 \equiv 65 \pmod{132}.$$

Vi utnyttjar Eulers sats, $a^{\Phi(n)} \equiv 1 \pmod{n}$ om $\text{sgd}(a, n) = 1$, med $a = 1121$ och $n = 132$ och får

$$1121^{1121} = 1121^{28 \cdot 40 + 1} = \left(1121^{40}\right)^{28} \cdot 1121^1 \equiv 1^{28} \cdot 65 \equiv 65 \pmod{132}.$$

Svaret är alltså $m = 65$.

5.30 Vi gör ett induktionsbevis.

Basfall: $n = 0$

Vi har att $F(0) = 0$ och $F(1) = 1$ och eftersom $\text{sgd}(0, 1) = 1$ så gäller påståendet för $n = 0$.

Induktionssteget: Antag nu att det gäller för ett fixt naturligt tal n, dvs. $\text{sgd}(F(n), F(n+1)) = 1$. Vi ska visa att då gäller det också att $\text{sgd}(F(n+1), F(n+2)) = 1$.

Ett positivt heltal k som delar både $F(n+1)$ och $F(n+2)$ delar också $F(n) = F(n+2) - F(n+1)$. Eftersom $\text{sgd}(F(n), F(n+1)) = 1$ så följer det att $k = 1$ och därmed att $\text{sgd}(F(n+1), F(n+2)) = 1$.

Enligt induktionsaxiomet gäller därmed påståendet för alla naturliga tal.

5.31 Påståendet kan formuleras som så att om $n = 5k$, $k \in \mathbb{N}$, så gäller att $5 \mid F(n)$. (Vi behöver inte oroa oss för de n som inte är delbara med 5 för då är implikationen automatiskt uppfylld eftersom premissen är falsk.) Vi gör ett induktionsbevis över k.

Basfall: Vi testar för $k = 0$ och finner att det stämmer eftersom $F(0) = 0$ och $5 \mid 0$.

Induktionssteg: Antag att det är sant för något k, d. v. s. $5 \mid F(5k)$, där $k \geq 0$ och visa att då är det också sant för $k+1$. Genom att utnyttja induktionsantagandet och defintionen av Fibonacci-talen i flera steg så får vi

$$\begin{aligned} F(5(k+1)) &= F(5k+5) = F(5k+4) + F(5k+3) \\ &= F(5k+3) + 2F(5k+2) + F(5k+1) \\ &= F(5k+2) + 4F(5k+1) + 2F(5k) \\ &= 5F(5k+1) + 3F(5k). \end{aligned}$$

Eftersom $5 \mid F(5k)$ enligt antagandet och $F(5k+1) \in \mathbb{N}$ så gäller att

$$5 \mid 5F(5k+1) + 3F(5k)$$

och därmed är saken klar.

5.32 Enligt induktionsaxiomet är påståendet därmed sant för alla naturliga tal n.

Euklides algoritm ger:

$$\begin{aligned} 97 &= 1 \cdot 54 + 43 \\ 54 &= 1 \cdot 43 + 11 \\ 43 &= 3 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + 1 \end{aligned}$$

Alltså är $\text{sgd}(97, 54) = 1$. Vi ersätter successivt de erhållna resterna och får:

$$\begin{aligned} 1 &= 11 - 1 \cdot 10 = 11 - (43 - 3 \cdot 11) = 4 \cdot 11 - 1 \cdot 43 \\ &= 4(54 - 1 \cdot 43) - 1 \cdot 43 = 4 \cdot 54 - 5 \cdot 43 \\ &= 4 \cdot 54 - 5(97 - 54) = 9 \cdot 54 - 5 \cdot 97. \end{aligned}$$

En lösning är alltså $x = -5 \cdot 6 = -30$ och $y = 9 \cdot 6 = 54$. Alla lösningar ges därmed av $x = -30 + 54n$ och $y = 54 - 97n$ med $n \in \mathbb{Z}$.

5.33 (a) Villkoret för att vara reflexiv är att $a\mathcal{R}_n a$ för alla $a \in \mathbb{Z}$. Men

$$a\mathcal{R}_n a \Leftrightarrow n \mid a + a \Leftrightarrow n \mid 2a$$

och detta gäller för alla a om och endast om $n \mid 2$, d. v. s. $n \in \{1, 2\}$.

(b) Den är alltid symmetrisk ty addition är kommutativ så

$$a\mathcal{R}_n b \Leftrightarrow n \mid a + b \Leftrightarrow n \mid b + a \Leftrightarrow b\mathcal{R}_n a.$$

(c) Den är aldrig antisymmetrisk, ty t. ex. har vi att $n\mathcal{R}_n 2n$ och $2n\mathcal{R}_n n$ och $n \neq 2n$ för alla n.

(d) Antag att $a\mathcal{R}_n b$ och $b\mathcal{R}_n c$. Då finns $k, l \in \mathbb{Z}$ sådana att $a + b = nk$ och $b + c = nl$. Vi får då att

$$a + c = (a + b) + (b + c) - 2b = n(k + l) - 2b.$$

Villkoret att $a\mathcal{R}_n c$ är alltså ekvivalent med att $n \mid 2b$. Men detta ska gälla för alla b, så enda möjligheterna är $n \in \{1, 2\}$ för vilka $\mathcal{R}_n$ är transitiv.

5.34 (a) **Reflexiv:** Vi har att $a \cdot a = a^2$ så $a\mathcal{R}a$.
Symmetrisk: Vi har att $ab = ba$ så $a\mathcal{R}b \Longrightarrow b\mathcal{R}a$.
Transitiv: Antag att $a\mathcal{R}b$ och $b\mathcal{R}c$ så $ab = n^2$ och $bc = m^2$ med $m, n \in \mathbb{Z}$. Då gäller att

$$ac = \frac{(ab)(bc)}{b^2} = \frac{n^2m^2}{b^2} = \left(\frac{nm}{b}\right)^2.$$

Alltså är ac ett rationellt tal i kvadrat, men eftersom det uppenbarligen är ett heltal så är $\frac{nm}{b}$ ett heltal och $a\mathcal{R}c$.

Alltså är $\mathcal{R}$ en ekvivalensrelation.

(b) Vi har per definition att

$$[p] = \{a \in \mathbb{Z}_+ : \exists n \in \mathbb{Z}_+ \; pa = n^2\}.$$

Villkoret ger att $p \mid n^2$ och därmed att $p \mid n$ eftersom p är ett primtal. Det betyder att $n^2 = p^2n_1^2$ för något $n_1 \in \mathbb{Z}$ och alltså att $a = pn_1^2$. Här kan n_1 nu vara vilket positivt heltal som helst och vi får att

$$[p] = \{pn^2 : n \in \mathbb{Z}_+\}.$$

(c) Betrakta primtalsfaktoriseringen av ett positivt heltal n. Plocka ut de primtal $p_1, \ldots, p_r$ som ingår med udda potens. Då kan man skriva faktoriseringen som

$$n = p_1 \cdots p_r q_1^{2k_1} \cdots q_s^{2k_s} = p_1 \cdots p_r n_1^2$$

där $q_1, \ldots, q_s$ är övriga primtalsfaktorer som alla kommer att ha jämn potens (dessa kan innehålla primtalen $p_1, \ldots p_r$ om dessa ingår med potensen $3, 5, 7, \ldots$). Om man multiplicerar två tal som har samma mängd av primtal med udda potens så kommer man att få en kvadrat (och alltså är de relaterade) och om mängderna skiljer sig åt så kommer det inte att bli en kvadrat. Speciellt gäller att

$$(p_1 \cdots p_r)\, \mathcal{R}\, \left(p_1 \cdots p_r \cdot n^2\right), \; n \in \mathbb{Z}_+$$

och därmed kommer alla tal att vara relaterade till exakt en sådan produkt av olika primtal med $r \geq 0$. Specialfallet $r = 0$ betyder att man har representanten 1

vars klass innehåller alla kvadrater. En möjlig mängd som uppfyller kraven är alltså

$$\{p_1 \cdots p_r : p_i \text{ olika primtal}, r \geq 0\}.$$

5.40 (a) Vi har t. ex. att $4 \mid 2^2$ men $4 \nmid 2$.

(b) Låt $a = p^2 b$. Då gäller att $b \in \mathbb{N}$ eftersom $p^2 \mid a$. Sätt nu $n = pb$. Då gäller att $n^2 = p^2 b^2 = ab$ så $a \mid n^2$, men $a > n$ så $a \nmid n$.

(c) Antag att $a \mid n^2$ och visa att då gäller att $a \mid n$. Låt $a = \prod_{i=1}^{r} p_i$ där p_i är olika primtal. Vi får att $p_i \mid n^2$ för alla p_i. Men för primtal p gäller att om $p \mid ab$ så har vi att $p \mid a$ eller $p \mid b$, så vi kan dra slutsatsen att $p_i \mid n$. Därmed ingår alla p_i i primtalsfaktoriseringen av n, så $n = m \prod_{i=1}^{r} p_i = ma$ där m är ett naturligt tal. Alltså har vi att $a \mid n$ vilket var precis vad vi skulle visa.

5.41 Antag först att det finns $p, q \in \mathbb{N}$ sådana att $n = p^2 - q^2$ och $p - q > 1$. Vi ska visa att i så fall är n inte ett primtal. Vi får

$$n = p^2 - q^2 = (p - q)(p + q)$$

och dessutom är $p + q \geq p - q > 1$ så vi har en icketrivial faktorisering av n som således ej är primtal.

Omvänt så antag att n inte är ett primtal. Vi ska då visa att det finns $p, q \in \mathbb{N}$ som uppfyller de föreskrivna kraven. Eftersom n ej är primtal så finns det en icketrivial faktorisering $n = rs$ med $r \geq s > 1$ och r och s udda (kom ihåg att vi antog n udda från början). Vi får då

$$n = rs = ((r + s)/2)^2 - ((r - s)/2)^2.$$

Sätt $p = (r + s)/2$ och $q = (r - s)/2$. Då gäller att $p, q \in \mathbb{N}$ ty $r \pm s \geq 0$ och jämna. Dessutom gäller att $p - q = s > 1$ och saken är klar.

5.42 Antag att $m = 2n$ är ett jämnt tal (så $n \in \mathbb{N}$). Vi har då att

$$2^m - 1 = 2^{2n} - 1 = (2^n)^2 - 1 = (2^n - 1)(2^n + 1)$$

enligt konjugatregeln. Om $2^n - 1 > 1$ så har vi alltså en icke-trivial faktorisering av $2^m - 1$ så då kan det inte vara ett primtal. Enda möjliga fallen för att få primtal är alltså $2^n - 1 \leq 1$ vilket ger $n \in \{0, 1\}$. Fallet $n = 0$ ger $2^m - 1 = 0$ och fallet $n = 1$ ger $2^m - 1 = 3$. Enda fallet med primtal är alltså då $m = 2 \cdot 1 = 2$.

5.43 (a) Vi beräknar $s(n)$ för alla $1 \leq n \leq 10$:

$$\begin{aligned} s(1) &= 0 \\ s(2) &= 1 \\ s(3) &= 1 \\ s(4) &= 1 + 2 = 3 \\ s(5) &= 1 \\ s(6) &= 1 + 2 + 3 = 6 \text{ Perfekt!} \\ s(7) &= 1 \\ s(8) &= 1 + 2 + 4 = 7 \\ s(9) &= 1 + 3 = 4 \\ s(10) &= 1 + 2 + 5 = 8. \end{aligned}$$

Vi ser att bara 6 är perfekt.

(b) Eftersom $q = 2^p - 1$ är ett primtal så har n bara två primtalsdelare: 2 och q. Det betyder att alla positiva delare till n som är mindre än n ges av

$$\{1, 2, 2^2 \ldots 2^{p-1}, q, 2q \ldots 2^{p-2}q\}.$$

Vi får att

$$\begin{aligned} s(n) &= \sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-2} 2^k q = \frac{2^p - 1}{2 - 1} + q\frac{2^{p-1} - 1}{2 - 1} \\ &= 2^{p-1}(2 + q) - (1 + q) = 2^{p-1}(2^p + 1) - 2^p \\ &= 2^{p-1}(2^p + 1 - 2) = 2^{p-1}(2^p - 1) = n, \end{aligned}$$

och alltså är n perfekt.

5.44 **Sats:** Ett positivt heltal n kan skrivas som differensen mellan kvadraterna av två heltal om och endast om n är udda eller $4 \mid n$

Bevis: Låt n vara ett positivt heltal. Om n är differensen mellan kvadraten av två heltal så är

$$n = x^2 - y^2 = (x - y)(x + y)$$

för $x, y \in \mathbb{Z}$. Om x och y båda är udda eller båda är jämna, så är både $x + y$ och $x - y$ jämna. Då kommer $4 \mid n$. Om x och y inte är kongruenta modulo 2 så kommer $x+y$ och $x-y$ båda att vara udda så då kommer också n att vara udda. Vi har nu visat att villkoren i satsen är nödvändiga.

Vi ska visa att de också är tillräckliga genom att ge konkreta exempel på x och y. Antag först att n är udda. Om vi väljer $x = y + 1$ så får vi

$$x^2 - y^2 = (x - y)(x + y) = 1 \cdot (2y + 1) = 2y + 1,$$

så vi kan få *alla* udda tal genom att ta $y = 0, 1, 2, \ldots$ och $x = y + 1$.

Antag nu att $4 \mid n$. Om vi väljer $x = y + 2$ så får vi

$$x^2 - y^2 = (x - y)(x + y) = 2 \cdot (2y + 2) = 4(y + 1),$$

så vi kan få *alla* multipler av 4 genom att ta $y = 0, 1, 2, \ldots$ och $x = y + 2$. Alltså är villkoren i satsen också tillräckliga.

5.45 Vi tittar på ekvationen modulo 4. Vi har att $s_n + 1$ uppenbarligen är delbart med 4, eftersom $(s_n+1)/4$ är heltalet som består av $n+1$ ettor. Alltså är $s_n \equiv 3 \pmod 4$. Å andra sidan så är $x^2 \equiv 0 \pmod 4$ eller $x^2 \equiv 1 \pmod 4$ (och samma för y^2 förstås), eftersom om man kvadrerar $0, 1, 2, 3$ så får man $0, 1, 0, 1$ modulo 4. Det betyder att x^2+y^2 är kongruent med $0, 1$ eller 2 modulo 4. Alltså saknar ekvationen $x^2 + y^2 = s_n$ lösning för alla $n \geq 0$.

5.46 (a) Enligt Eulers sats är $k^{p-1} \equiv 1 \pmod{p}$. Det ger att

$$1 + \sum_{k=1}^{p-1} k^{p-1} \equiv 1 + \sum_{k=1}^{p-1} 1 = p \equiv 0 \pmod{p},$$

d. v. s. p delar uttrycket.

(b) Ta t. ex. $p = 4$. Då är

$$1 + \sum_{k=1}^{p-1} k^{p-1} = 1 + 1^3 + 2^3 + 3^3 = 37 \equiv 1 \pmod{4},$$

så det gäller inte att 4 delar uttrycket. Alltså gäller det inte alltid då p inte är ett primtal.

5.47 (a) Formeln för en geometrisk summa ger

$$\sum_{r=0}^{2m} (-x)^r = \frac{1 - (-x)^{2m+1}}{1 - (-x)} = \frac{1 - (-x^{2m+1})}{1 + x} = \frac{1 + x^{2m+1}}{1 + x}$$

så $x^{2m+1} + 1 = (x + 1) \sum_{r=0}^{2m} (-x)^r$ vilket ger att $x + 1$ delar $x^{2m+1} + 1$ eftersom summan uppenbarligen är ett heltal.

(b) Vi visar det kontrapositiva påståendet att om k inte är en tvåpotens så är det inte ett primtal. Om k inte är en tvåpotens så har k en udda faktor så $k = s(2m + 1)$ för några positiva heltal s och m. Om vi sätter $x = 2^s$ i första deluppgiften så får vi att $2^s + 1$ delar

$$(2^s)^{2m+1} + 1 = 2^{s(2m+1)} + 1 = 2^k + 1.$$

Eftersom $s > 0$ så är $2^s + 1 \geq 3$ och eftersom $m > 0$ så är $2^k > 2^s$ så $2^s + 1$ är en äkta delare till $2^k + 1$. Alltså är $2^k + 1$ inget primtal.

Lösningar till utvalda uppgifter i kapitel 6

6.10. (a) Om vi bortser från villkoret så finns det $\binom{14}{5}$ olika arbetsgrupper. Ifrån detta tal får vi sedan subtrahera det antal grupper som innehåller både Herr V och Fru M. En sådan grupp väljs ut genom att de övriga 3 medlemmarna väljs bland de återstående 12. Det finns alltså $\binom{12}{3}$ sådana grupper. Svaret är alltså

$$\binom{14}{5} - \binom{12}{3} = 1782.$$

(b) Samma resonemang som ovan ger

$$\binom{n}{k} - \binom{n-2}{k-2}.$$

6.11. Det finns 1 rad med 13 rätt. För 12 rätt finns det $\binom{13}{1} = 13$ olika matcher som kan missas och för var och en av dessa finns det 2 möjligheter. Det blir totalt $13 \cdot 2 = 26$ rader med 12 rätt. För 11 rätt finns det $\binom{13}{2} = 78$ olika par av matcher som kan missas och för var och en av dessa par finns det 4 möjligheter. Det blir totalt $78 \cdot 4 = 312$ rader med 11 rätt. För 10 rätt finns det $\binom{13}{3} = 286$ olika tripplar av matcher som kan missas och för var och en av dessa tripplar finns det 8 möjligheter. Det blir totalt $286 \cdot 8 = 2288$ rader med 10 rätt. Sammantaget får vi följande svar:

$$1 + 26 + 312 + 2288 = 2627.$$

(Chansen att få 9 rätt är alltså mer än 4 gånger så stor som att få in en vinst. Något man bör ha i åtanke när man förbannar sin otur efter ännu en vecka med retfulla 9 rätt.)

6.12. Vi har sex siffror givna så vi ska välja en siffra bland de återstående 7 så vi har 7 olika möjliga val av siffror. (Fallet där 0 är med är speciellt, men vi bortser först från det och återkommer till det i slutet.)

Antalet permutationer av 7 element med en dubblett och en triplett är $7!/2!3!$ så totala antalet blir $7 \cdot 7!/2!3!$. Men nu har

vi också (felaktigt) räknat de som inleds med en nolla. Vi får dra bort dessa. Det handlar här om en permutation av 6 stycken med en dubblett och en triplett och alltså $6!/2!3!$ stycken. Sammantaget så får vi:

$$7\frac{7!}{2!3!} - \frac{6!}{2!3!} = 7^2 \cdot 5 \cdot 4 \cdot 3 - 5 \cdot 4 \cdot 3 = 48 \cdot 5 \cdot 4 \cdot 3 = 2880.$$

Nu till frågan hur många av dessa som är udda. Vi börjar med att räkna de som slutar på en etta. Vi bortser återigen först ifrån att första siffran inte får vara en nolla. Det finns $\binom{7}{2} = 21$ olika sätt att placera ut de två ettorna och 6 av dessa kommer att ha en etta sist. Alltså kommer $\frac{6}{21} = \frac{2}{7}$ av alla talen att sluta på en etta. Detta blir totalt $\frac{2}{7} \cdot 7 \cdot 7!/2!3! = 840$ stycken. Men nu måste vi subtrahera de med en nolla först (och en etta sist). Detta svarar mot en permutation av 5 siffror med en triplett, d. v. s. $5!/3! = 20$ stycken och vi får alltså 820 stycken som slutar med en etta.

Vi måste också göra en separat analys på de som slutar med en trea. Då har vi 7 alternativ för den icke specificerade siffran och sedan en permutation av 6 siffror med en dubblett och en triplett. Totalt blir det $7 \cdot 6!/3!2 = 420$ stycken. Men vi måste subtrahera de som börjar med en nolla vilket svarar mot en permutation av 5 siffror med en dubblett och en triplett, d. v. s. $5!/3!2 = 10$ stycken. Kvar är alltså 410 stycken.

För de övriga tre möjliga udda slutsiffrorna blir det samma antal och detta svarar mot en permutation av 6 siffror med en dubblett och en triplett, d. v. s. $6!/3!2! = 60$ stycken.

Totalt får vi alltså $820 + 410 + 3 \cdot 60 = 1410$ stycken udda tal.

6.13. (a) Man kan välja 11 bland 22 på $\binom{22}{11}$ sätt och 5 bland de återstående på $\binom{11}{5}$ sätt. Totalt får vi

$$\binom{22}{11} \cdot \binom{11}{5} = \frac{22!}{11!11!}\frac{11!}{6!5!} = \frac{22!}{11!5!6!}$$

(b) Vi räknar först ut på hur många sätt hon kan välja de som inte är målvakt. Det handlar om att först välja 10

bland 19 och sedan 4 bland de återstående 9. Hon kan sedan fördela de 3 målvakterna på $3! = 6$ sätt. Totalt blir det alltså

$$6 \cdot \binom{19}{10} \cdot \binom{9}{4}$$

olika lag. (Om man räknar ut det så blir det 69837768. Tufft att vara förbundskapten om man har ambitionen att fundera över alla möjligheter.)

6.14. Det kommer antingen att vara två pojkar och tre flickor eller tvärtom och dessa två möjligheter har förstås inga gemensamma utfall. Tre pojkar och två flickor kan väljas på

$$\binom{10}{2}\binom{8}{3} = 45 \cdot 56 = 2520$$

sätt och två pojkar och tre flickor kan väljas på

$$\binom{10}{3}\binom{8}{2} = 120 \cdot 28 = 3360$$

sätt så totalt blir det $2520 + 3360 = 5880$ olika möjligheter.

6.15. Vi startar med LEMURELL. Det finns 8 bokstäver och av dessa finns det en dubbel (E) och en trippel (L). Det betyder att det totala antalet möjliga ord är

$$\frac{8!}{2!3!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{2 \cdot 6} = 8 \cdot 7 \cdot 5 \cdot 4 \cdot 3 = 56 \cdot 60 = 3360.$$

För JONASSON blir det istället tre dubbla (O, N, S) så

$$\frac{8!}{2!2!2!} = 7! = 5040.$$

Det är enklare att räkna ut antalet som innehåller två E i rad (för LEMURELL, för JONASSON är det lika enkelt oavsett) och subtrahera detta från det totala antalet. Antalet möjliga ord med de övriga sex bokstäverna är $6!/3!$. Man kan sedan

placera in E-paret på sju olika ställen. Det ger att antalet utan två E i rad för LEMURELL är

$$3360 - 7 \cdot \frac{6!}{3!} = 3360 - \frac{7!}{3!} = 3360 - 840 = 2520.$$

Totalt blir det alltså $2520 + 5040 = 7560$.

6.16. Vi har möjligheterna att antalet svarta bollar är 0, 2 eller 4. Man kan välja k svarta bollar på $\binom{11}{k}$ sätt och $5-k$ vita bollar på $\binom{7}{5-k}$ sätt. Totalt blir det alltså

$$\binom{11}{0}\binom{7}{5} + \binom{11}{2}\binom{7}{3} + \binom{11}{4}\binom{7}{1} = 1 \cdot 21 + 55 \cdot 35 + 330 \cdot 7 = 4256.$$

6.17. (a) Välja sex bland tolv kan göras på

$$\binom{12}{6} = 924$$

olika sätt.

(b) Välja tre pojkar bland sju kan göras på

$$\binom{7}{3} = 35$$

olika sätt och välja tre flickor bland fem kan göras på

$$\binom{5}{3} = 10$$

olika sätt. Totalt blir det $35 \cdot 10 = 350$ olika sätt.

(c) Antalet sätt att välja både Pelle och Anna är samma som antalet sätt att välja fyra bland övriga tio personer. Detta kan göras på

$$\binom{10}{4} = 210$$

olika sätt. Dessa ska subtraheras ifrån det totala antalet som är 924 enligt första deluppgiften. Antalet olika sätt är alltså $924 - 210 = 714$.

6.18. Om vi börjar med lucian så kan den väljas på 10 olika sätt. Därefter finns det 9 flickor kvar att välja bland så de 4 tärnorna kan väljas på

$$\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 126$$

sätt. Till slut finns det 13 pojkar att välja stjärngossar bland vilket går på

$$\binom{13}{2} = \frac{13 \cdot 12}{2 \cdot 1} = 78$$

sätt. Enligt multiplikationsprincipen blir det totalt

$$10 \cdot 126 \cdot 78 = 98280.$$

6.19. Först väljer vi 4 personer till ett lag. Det går på

$$\binom{12}{4} = \frac{12 \cdot 11 \cdot 10 \cdot 9}{4 \cdot 3 \cdot 2} = 55 \cdot 9 = 495$$

sätt. Därefter är det 8 personer att välja på till det andra laget som då kan väljas på

$$\binom{8}{4} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2} = 14 \cdot 5 = 70$$

sätt. Nu gäller det att inte missa att vi kan permutera de tre lagen och få samma uppdelning av personer på $3! = 6$ olika sätt. Det totala antalet olika uppdelningar blir därför

$$\binom{12}{4}\binom{8}{4} \cdot \frac{1}{6} = 165 \cdot 35 = 5775.$$

6.20. Vi tar ut de två lagen som ska spela basket först. Då ska vi först välja 4 personer till ett av lagen bland 16 personer och

sedan 4 personer till andra laget bland de 12 som är kvar. Detta kan göras på

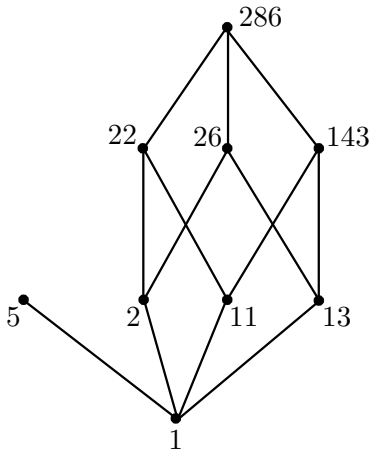
$$n_1 = \binom{16}{4}\binom{12}{4}$$

sätt. Fast då räknar vi dubbelt för man kan permutera de två lagen utan att ändra valet så det blir $n_1/2$ möjliga val för basketlagen. Därefter är det dags att ta ut de två innebandylagen. Man kan välja ut ett lag på $\binom{8}{4}$ olika sätt och sedan är det andra laget bestämt. Men nu räknar vi återigen dubbelt för att välja 4 personer blir samma som att välja de andra 4 personerna. Totalt får vi alltså

$$\frac{\binom{16}{4}\binom{12}{4}\binom{8}{4}}{4} (= 15'765'750).$$

Lösningar till utvalda uppgifter i kapitel 7

7.7. Minimalt och minsta element: 1
Maximala element: 5 och 286
Största element saknas.



Figur F.2: Hasse-diagrammet till mängden M.

7.17. (a) $S_n = \{1, p, q, r, p^2, pq, pr, qr, p^2q, p^2r, pqr, n\}$

(b)