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.