Lösningar till udda övningsuppgifter

Övning 0.1.

1. $B \cup C = A$.
2. $B \cap C = \emptyset$.
3. $D \cap C = \{4, 36\}$.
4. $\{x \in D : x \in B\} = D \cap B = \{1, 19, 101\}$.
5. $\{x \in A : x = y + 1 \text{ för något } y \in D\} = \{2, 5, 20, 37, 102\}$.
6. $\{x + 1 : x \in D\} = \{2, 5, 20, 37, 102\}$.

Övning 0.3. Tag $x \in ((A \cap C) \cup (B \cap C^c))^c$. Det betyder att $x \in \Omega$ och $x \notin (A \cap C) \cup (B \cap C^c)$. Alltså har vi att $x \notin A \cap C$ och $x \notin B \cap C^c$. Det finns nu två möjligheter: $x \in C$ och $x \notin C$.

I det första fallet, det vill säga $x \in C$, måste $x \notin A$ eftersom om $x \in A$ så skulle $x \in A \cap C$ vilket är falskt. Alltså gäller $x \in A^c$, vilket tillsammans med $x \in C$ ger att $x \in A^c \cap C$ i detta fall. I synnerhet har vi att $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I det andra fallet gäller $x \in C^c$ och då måste $x \in B^c$ eftersom om $x \in B$ så skulle $x \in B \cap C^c$ vilket är falskt. Alltså gäller $x \in B^c \cap C^c$, och i synnerhet $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I båda fallen gäller alltså $x \in (A^c \cap C) \cup (B^c \cap C^c)$, och eftersom x var godtycklig så visar detta att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$.

Omvänt, tag $x \in (A^c \cap C) \cup (B^c \cap C^c)$. Då gäller $x \in A^c \cap C$ eller $x \in B^c \cap C^c$ (eller båda). Vi har alltså dessa två fall.

I det första fallet, det vill säga $x \in A^c \cap C$, har vi att $x \notin A$ och $x \notin C^c$. I synnerhet har vi att $x \notin A \cap C$ (eftersom $x \notin A$) och att $x \notin B \cap C^c$ (eftersom $x \notin C^c$). Alltså tillhör x varken $A \cap C$ eller $B \cap C^c$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I det andra fallet, det vill säga $x \in B^c \cap C^c$ har vi att $x \notin B$ och att $x \notin C$. Det följer att $x \notin A \cap C$ och att $x \notin B \cap C^c$. Alltså gäller $x \notin (A \cap C) \cup (B \cap C^c)$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I båda fallen har det alltså visats att $x \in ((A \cap C) \cup (B \cap C^c))^c$, och eftersom x var godtycklig visar detta att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$.

Vi har alltså visat att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$ och att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$ och därmed att $((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c)$.

Övning 1.1.

1. $q = 2$, $r = 6$ eftersom $32 = 13 \cdot 2 + 6$.

2. $q = -4$, $r = 4$ eftersom $-24 = 7 \cdot (-4) + 4$.

3. $q = 176$, $r = 2$ eftersom $1762 = 10 \cdot 176 + 2$.

4. $q = 0$, $r = 10$ eftersom $10 = 1762 \cdot 0 + 10$.

5. $q = -2$, $r = 0$ eftersom $-70 = 35 \cdot (-2) + 0$.

Övning 1.3. Vi har att

$$0 = a - a = (b \cdot q + r) - (b \cdot q + \tilde{r}) = r - \tilde{r}.$$

Att $r - \tilde{r} = 0$ medför att $r = \tilde{r}$ (eftersom $r = r + (\tilde{r} - \tilde{r}) = (r - \tilde{r}) + \tilde{r} = 0 + \tilde{r} = \tilde{r}$).

Övning 1.5.

1. Låt a vara ett godtyckligt heltal. Vi har att $a = a \cdot 1$, vilket per definition betyder att $a \mid a$.

2. Antag att $a \mid b$ och $b \mid c$. Per definition finns då heltal q_1 och q_2 sådana att $b = a \cdot q_1$ och $c = b \cdot q_2$. Nu har vi att $c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot q_1 q_2$, vilket per definition betyder att $a \mid c$, eftersom $q_1 q_2$ är ett heltal.

3. Vi ska alltså visa att det finns heltal a och b sådana att $a \mid b$ men $b \nmid a$. Låt $a = 1$ och $b = 2$. Då gäller uppenbarligen detta.

Övning 2.1. Per definition gäller $d \in D(a)$ och $d \in D(b)$. Alltså har vi $d \in D(a) \cap D(b)$. Det återstår att visa att d är en övre begränsning för $D(a) \cap D(b)$. Tag $x \in D(a) \cap D(b)$. Enligt uppgiftslydelsen gäller $x \mid d$. Alltså finns ett heltal q sådant att $d = x \cdot q$. Eftersom både $d > 0$ och $x > 0$ så måste $q > 0$. I och med att q är ett heltal följer det att $q \geqslant 1$. Nu gäller

$$d = x \cdot q \geqslant x \cdot 1 = x.$$

Alltså har vi att $d \geqslant x$, för alla $x \in D(a) \cap D(b)$, vilket betyder att d är en övre begränsning för $D(a) \cap D(b)$. Saken är klar.

Övning 2.3. Vi har att

$$\begin{aligned} 139 &= 117 \cdot 1 + 22 \\ 117 &= 22 \cdot 5 + 7 \\ 22 &= 7 \cdot 3 + 1. \end{aligned}$$

Använd dessa uträkningar baklänges och få

$$\begin{aligned} 1 &= 22 - 7 \cdot 3 \\ &= 22 - (117 - 22 \cdot 5) \cdot 3 = -117 \cdot 3 + 22 \cdot 16 \\ &= -117 \cdot 3 + (139 - 117 \cdot 1) \cdot 16 = 139 \cdot 16 - 117 \cdot 19. \end{aligned}$$

Alltså är $x = 16$ och $y = -19$.

Övning 3.1. Vi har att

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3, \\ 26 &= 2 \cdot 13, \\ 55 &= 5 \cdot 11, \\ 98 &= 2 \cdot 7 \cdot 7, \\ 150 &= 2 \cdot 3 \cdot 5 \cdot 5, \\ 210 &= 2 \cdot 3 \cdot 5 \cdot 7, \\ 315 &= 3 \cdot 3 \cdot 5 \cdot 7, \\ 455 &= 5 \cdot 7 \cdot 13. \end{aligned}$$

Övning 3.3. Sätt $d = \text{sgd}\,(a, p)$. Då är d en delare till både a och p. Eftersom $d > 0$ är en delare till p och eftersom p är ett primtal så måste antingen $d = 1$ eller $d = p$. I det första fallet gäller $\text{sgd}\,(a, p) = d = 1$. I det andra fallet noterar vi att eftersom d är en delare till a och $d = p$ så gäller $p \mid a$.

Övning 4.1. Vi går igenom var och en av punkterna i tur och ordning. Vi sätter genomgående $z = a + b\text{i}$, $w = c + d\text{i}$ och $v = e + f\text{i}$.

1. Enligt definitionen får vi $z + w = a + c + (b + d)\text{i}$ och eftersom summan av två heltal är ett heltal följer att $a + c$ och $b + d$ är heltal. Därmed är $z + w$ ett nytt Gaussiskt heltal.

2. Produkten zw beräknas enligt definitionen av multiplikation som $zw = ac - bd + (ad + bc)\text{i}$. Produkten av två vanliga heltal är ett nytt heltal, och således är ac, bd, ad och bc heltal. Vi utnyttjar sedan att summor och differenser av heltal är heltal för att kunna dra slutsatsen att zw är ett Gaussiskt heltal.

3. Vi har $z + w = a + c + (b + d)\text{i}$, och eftersom ordningen inte spelar någon roll vid addition av heltal kan vi istället skriva $z + w = c + a + (d + b)\text{i}$. Detta är enligt definitionen lika med $w + z$, och därmed är likheten bevisad.

4. Vi har enligt definitionen av multiplikation att $zw = ac - bd + (ad + bc)\text{i}$ och $wz = ca - db + (da + cb)\text{i}$. Vi vet emellertid att $ac = ca$, $bd = db$, $ad = da$ och $bc = cb$ för heltal a, b, c och d. Genom att utnyttja detta finner vi att $zw = wz$.

5. Vi adderar först w och v och lägger därefter till z, och får

   $$z + (w + v) = a + b\text{i} + (c + e + (d + f)\text{i}) = a + (c + e) + (b + (d + f))\text{i}.$$

   Addition av vanliga heltal satisfierar associativa lagen, och detta betyder att högerledet ovan är lika med

   $$(a + c) + e + ((b + d) + f)\text{i},$$

   men detta är precis vad man får om man först beräknar $z + w$ och därefter adderar v. Likheten följer nu.

6. Vi beräknar först $wv = ce - df + (cf + de)\mathrm{i}$ och därefter

$$z \cdot (w \cdot v) = a(ce - df) - b(cf + de) + [a(cf + de) + b(ce - df)]\mathrm{i}.$$

Vi utvecklar sedan parenteserna och finner att

$$\begin{aligned} z \cdot (w \cdot v) = {} & ace - adf - bcf - bde \\ & + (acf + ade + bce - bdf)\mathrm{i}. \end{aligned}$$

Om vi istället först räknar ut $zw = ac - bd + (ad + bc)\mathrm{i}$ och därefter multiplicerar med v får vi

$$(z \cdot w) \cdot v = e(ac - bd) - f(ad + bc) + [e(ad + bc) + f(ae - bd)]\mathrm{i}.$$

Vi multiplicerar ut parenteserna och finner att

$$\begin{aligned} (z \cdot w) \cdot v = {} & ace - bde - adf - bcf \\ & + (ade + bce + acf - bdf)\mathrm{i}. \end{aligned}$$

Vi påminner oss om att ordningen inte spelar någon roll när vi adderar vanliga heltal och med detta i åtanke jämför vi nu uttrycken för $z \cdot (w \cdot v)$ och $(z \cdot w) \cdot v$ som vi har räknat ut. Vi finner att $z \cdot (w \cdot v) = (z \cdot w) \cdot v$, vilket skulle visas.

7. Vi räknar först ut högerledet i likheten vi ska visa. Vi har $zw = ac - bd + (ad + bc)\mathrm{i}$ och $zv = ae - bf + (af + be)\mathrm{i}$, vilket ger oss

$$zw + zv = ac + ae - bd - bf + (ad + bc + af + be)\mathrm{i}.$$

Därefter beräknar vi $w + v = c + e + (d + f)\mathrm{i}$ och får

$$z \cdot (w + v) = a(c + e) - b(d + f) + [a(d + f) + b(c + e)]\mathrm{i},$$

och efter att ha utvecklat parenteserna ser vi att $z \cdot (w + v)) = zw + zv$.

8. Denna punkt följer direkt från egenskapen $0 + a = a$ för varje heltal a: vi får $z + 0 = a + b\mathrm{i} + 0 + 0\mathrm{i} = a + 0 + (b + 0)\mathrm{i} = a + b\mathrm{i}$.

9. Vi vet att $a \cdot 1 = a$ för varje heltal a, och detta ger oss att $z \cdot 1 = (a + b\mathrm{i})(1 + 0\mathrm{i}) = a - 0 + (b + 0)\mathrm{i} = a + b\mathrm{i} = z$.

10. Om $z = a + b\mathrm{i}$ är $-z = -a - b\mathrm{i}$ ett Gaussiskt heltal eftersom $-a$ och $-b$ är heltal. Vidare gäller ju $a - a = 0$ för heltalet a, och motsvarande är ju även samt för b. Definitionen av addition medför nu att $z + (-z) = a - a + (b - b)\mathrm{i} = 0 + 0\mathrm{i} = 0$, vilket var precis vad vi skulle visa.

Övning 4.3. Vi börjar med det första påståendet. Vi beräknar

$$(a + b\mathrm{i})(a - b\mathrm{i}) = a^2 - ab\mathrm{i} + ab\mathrm{i} + b^2 = a^2 + b^2,$$

och enligt definitionen är det sista uttrycket till höger lika med $N(a + b\mathrm{i})$.

Vi sätter $z = a + b\mathrm{i}$ och $w = c + d\mathrm{i}$, tillämpar identiteten ovan på $N(z + w) = N(a + c + (b + d)\mathrm{i})$ och får

$$N(a + c + (b + d)\mathrm{i}) = (a + c + (b + d)\mathrm{i})(a + c - (b + d)\mathrm{i}).$$

Nu utvecklar vi produkten i högerledet och får

$$\begin{aligned}
&(a + c + (b + d)\mathrm{i})(a + c - (b + d)\mathrm{i}) \\
&= a^2 - iab + ac - iad + iab + b^2 + ibc + bd \\
&+ac - ibc + c^2 - icd + iad + bd + icd + d^2 \\
&= a^2 + b^2 + c^2 + d^2 + 2ac + 2bd \\
&= N(z) + N(w) + 2(ac + bd).
\end{aligned}$$

Detta visar likheten i uppgiften.

Övning 5.1.

1. Eftersom $4 + 3 = 7 = 5 \cdot 1 + 2 \equiv 2 \pmod 5$ så har vi att $4 + 3 = 2$ i ringen $\mathbb{Z}_5$.

2. Notera att $8 \cdot 7 = 56 = 9 \cdot 6 + 2 \equiv 2 \pmod 9$. Detta betyder att $8 \cdot 7 = 2$ i ringen $\mathbb{Z}_9$.

3. Till sist har vi att $3^3 = 9 \equiv -1 \pmod{10}$. Nu följer

   $$3^{100} = 3 \cdot 3^{99} = 3 \cdot (3^3)^{33} \equiv 3 \cdot (-1)^{33} = 3 \cdot (-1) = -3 \equiv 7 \pmod{10}.$$

   Alltså har vi att $3^{100} = 7$ i ringen $\mathbb{Z}_{10}$.

Övning 5.3. Per definition gäller $n \mid (a - b)$, det vill säga det finns ett heltal q sådant att $a - b = n \cdot q$. Nu följer

$$(-a) - (-b) = -(a - b) = -(n \cdot q) = n \cdot (-q),$$

vilket betyder att $n \mid ((-a) - (-b))$, och därmed $-a \equiv -b \pmod n$.

Övning 6.1. $D_t(y) = \mathrm{R}_{28}(y - t)$ är den sökta dekrypteringsfunktionen. För att visa att detta är fallet noterar vi först att

$$\begin{aligned}
D_t(\mathrm{R}_{28}(x + t)) &= \mathrm{R}_{28}(\mathrm{R}_{28}(x + t) - t) \\
&= \mathrm{R}_{28}(\mathrm{R}_{28}(x + t)) + \mathrm{R}_{28}(-t).
\end{aligned}$$

Därefter utnyttjar vi att $\mathrm{R}_n(\mathrm{R}_n(a)) = \mathrm{R}_n(a)$ och får

$$\begin{aligned}
&\mathrm{R}_{28}(\mathrm{R}_{28}(x + t)) + \mathrm{R}_{28}(-t) \\
&= \mathrm{R}_{28}(x + t) + \mathrm{R}_{28}(-t) \\
&= \mathrm{R}_{28}(x + t - t) = x,
\end{aligned}$$

vilket visar att $D(E(x)) = x$.