Tal- og gruppeteori

Jesper M. Møller

Author address:

Matematisk Institut, Universitetsparken 5, 2100 København Ø
E-mail address: moller@math.ku.dk

RESUME. Noter til brug ved undervisningen i Mat 1 (algebra). I stikordsform er indholdet: Induktionsaksiomet, Divisionsalgoritmen, største fælles divisor og mindste fælles multiplum, Euklids Algoritme, primtal, entydighed af primtalsfaktorisering, grupper, Cayley tabel, undergrupper, gruppehomomorfier, kernen for en gruppehomomorfi, Lagranges Sætning, aritmetik modulo n, Eulers Sætning, Fermats lille sætning, Den kinesiske Restklassesætning.

Disse noter ligger på kursets hjemmeside.

Indhold

KAPITEL 1

Talteori

1. Induktion

Alle kender de naturlige tal

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

og de hele tal

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

så de behøver ingen yderligere introduktion.

De naturlige tal opfylder

INDUKTIONSAKSIOMET 1.1. *Lad $S \subseteq \mathbb{N}$ være en delmængde af de naturlige tal som opfylder følgende to egenskaber:*

1. $1 \in S$.
2. *For alle $n \in \mathbb{N}$ gælder at hvis $n \in S$, så er $n + 1 \in S$.*

Da er $S = \mathbb{N}$.

Induktionaksiomet optræder i mange forskellige varianter og forklædninger. Her er en af dem:

INDUKTIONSAKSIOMET 1.2. *Lad, for hvert naturligt tal n, $P(n)$ være en påstand, som afhænger af n. Antag, at*

1. *$P(1)$ er sand, og*
2. *$P(n)$ medfører $P(n+1)$ for ethvert naturligt tal n,*

da er $P(n)$ sand for alle naturlige tal n.

De to versioner af induktionsaksiomet er ækvivalente. Forbindelsen mellem dem ses ved at sætte $S = \{n \in \mathbb{N} \mid P(n) \text{ er sand}\}$ til at være mængden af de natrurlige tal for hvilke $P(n)$ er sand.

Her kommer et eksempel på en typisk anvendelse af Induktionsaksiomet.

EKSEMPEL 1.3. Vi ønsker at vise, at

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \tag{1.4}$$

for alle naturlige tal $n \geq 1$.

Lad $P(n)$ betegne den påstand at formlen (1.4) holder for det naturlige tal n. Læg mærke til:

(I1): $P(1)$ er sand fordi $1 = \frac{1\cdot 2}{2}$.
(I2): Antag at $P(n)$ er sand. Vi har da

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)(\frac{n}{2}+1) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

hvilket viser at $P(n+1)$ er sand.

Ifølge Induktionsaksiomet (1.2) kan vi nu slutte at $P(n)$ er sand for alle $n \geq 1$.

Du kan selv øve dig ved at tænke over:

ØVELSE 1.5. Vis, at

$$1+3+\cdots+(2n-1) = n^2$$

for alle naturlige tal $n \in \mathbb{N}$.

Nu, hvor jeg er kommet op i fart, snupper vi lige endnu en variant:

INDUKTIONSAKSIOMET 1.6. *Lad, for hvert naturligt tal n, $P(n)$ være en påstand, som afhænger af n. Antag, at*

1. *$P(1)$ er sand, og*
2. *sandheden af $P(i)$ for alle $i \leq k$ medfører sandheden af $P(k+1)$ for ethvert naturligt tal k,*

da er $P(n)$ sand for alle naturlige tal n.

Overvej selv, hvorfor denne tilsyneladende stærkere antagelse alligevel ikke får den store indflydelse. (Hvis nu $P(n)$ er som ovenfor, indfør en ny påstand $Q(n)$ som siger, at $P(i)$ er sand for alle $i \leq n$. Brug nu den første variant.)

Til slut skal vi se på endnu en variant, som er lidt mindre gennemskuelig. Vi indfører først det meget naturlige begreb *et mindste element*.

DEFINITION 1.7. *Lad $S \subseteq \mathbb{N}$ være en delmængde af de naturlige tal. Vi siger, at det naturlige tal m er det mindste element i S, hvis*

1. *m ligger i S, og*
2. *$m \leq s$ for ethvert $s \in S$.*

Det vil sige, at s er det mindste element i S, hvis s er i S og s er mindre end eller lig med alle elementer i S.

Vi skriver $\min S$ for det mindste element i S; f.eks. er

$$\min\{n \in \mathbb{N} \mid n^2 \geq 4\} = 2$$

(Faktisk har jeg snydt en lille smule ved allerede at tale om *det* mindste element; kunne der ikke tænkes at findes en delmængde af de naturlige tal med to mindste elementer?)

Kan du komme i tanke om en eneste delmængde, bortset fra den tomme mængde, af de naturlige tal som *ikke* har et mindste element? Er det sådan, at alle delmængder af $\mathbb{N}$ har et mindste element? Kan du bevise det? (Vendingen "Så må der da for F..... være" er blasfemisk og derfor ikke tilladt.)

SÆTNING 1.8. *(Princippet om det mindste element) Enhver delmængde $S \subseteq \mathbb{N}$ af de naturlige tal, som ikke er tom, har netop et mindste element.*

BEVIS. For ethvert naturligt tal n, lad $P(n)$ være påstanden

$P(n)$: Alle delmængder $S \subseteq \mathbb{N}$, som indeholder mindst et af tallene $1, \dots, n$, har et mindste element.

Vi bruger Induktionsaksiomet til at vise, at $P(n)$ er sand for alle n. Påstanden $P(1)$ er sand, for hvis $1 \in S$, da er 1 det mindste element for S. Lad os nu antage, at $P(n)$ er sand for et $n \in \mathbb{N}$. Vi vil vise, at så er også $P(n+1)$ sand. Lad derfor S være en mængde af naturlige tal, så $S \cap \{1, 2, \dots, n+1\} \neq \emptyset$. Hvis så også, $S \cap \{1, 2, \dots, n\} \neq \emptyset$, da har S et mindste element ifølge induktionsantagelsen $P(n)$; men hvis $S \cap \{1, 2, \dots, n\} = \emptyset$, da er $n+1$ et mindste element for S.

Til sidst, lad S være en vilkårlig, ikke-tom mængde af naturlige tal. Da S ikke er tom, indeholder den et element, s. Så er $S \cap \{1, 2, \dots, s\} \neq \emptyset$, og alle delmængder med denne egenskab har et mindste element, da $P(s)$ er sand. □

Vi har altså set, at

$$\text{Induktionsaksiomet} \Rightarrow \text{Princippet om det mindste element.}$$

Den modsatte implikation gælder også; de to er ækvivalente.

ØVELSE 1.9. Vis den modsatte implikation. (Vink: Antag Princippet om det mindste element. Lad $P(n)$ være en påstand, der afhænger af det naturlige tal n og opfylder de to krav i Induktionsaksiomet. Sæt S til at være $\{n \in \mathbb{N} \mid P(n) \text{ er falsk}\}$. Har S et mindste element?)

Garvede matematikere vil sige at Princippet om det mindste element siger, at $\mathbb{N}$ er velordnet. Læg mærke til, at Princippet om det mindste element *ikke* gælder for de reelle tal $\mathbb{R}$.

ØVELSE 1.10. Hvis $\emptyset \neq A \subseteq B \subseteq \mathbb{N}$, så er $\min A \geq \min B$.

2. Divisionsalgoritmen

I dette afsnit udnytter vi Princippet om det mindste element til at bevise Divisionsalgoritmen.

Først vil det være bekvemt at indføre betegnelsen

$$\mathbb{N}_0 = \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, \dots\}$$

for mængden af de naturlige tal og 0.

Dividerer vi 11 med 4, så vil vi se, at 4 går op 2 gange i 11 og resten er 3. Eller, som de udtrykker det i tredje klasse:

$$11 = 4 \cdot 2 + 3$$

Dette illustrerer det næste resultat:

SÆTNING 2.1. *(Divisionsalgoritmen.) Lad $a \in \mathbb{Z}$ være et helt tal og $b \in \mathbb{N}$ et naturligt tal (så $b \neq 0$). Der findes da entydigt bestemte hele tal q og r så*

$$a = bq + r$$

hvor $0 \leq r < b$. (q kaldes kvotienten, r resten.)

Hvis $a = 11$ og $b = 4$, da er kvotienten $q = 2$ og resten er $r = 3$. Sætningen tillader også division op i negative tal; dividerer vi $a = -11$ med $b = 4$ får vi kvotienten $q = -3$ og resten $r = 1$ fordi $-11 = 4 \cdot (-3) + 1$ hvor jo $0 \leq 1 < 4$. Sætningen siger derimod ikke noget om division med negative tal, tallet b, det vi dividerer med, er altid positivt; resten r er også altid positiv eller 0.

ØVELSE 2.2. Lad a og b være positive, hele tal. Antag, at $a = bq + r$ med $0 \leq r < b$. Hvad giver Divisionsalgoritmen, når vi dividerer a med $-b$?

Din erfaring (empirien) siger dig, at man med et givent input, a og b, altid kan finde q og r som påstået i Divisionsalgoritmen. Men er din empiriske erfaring dermed en universel sandhed? NIX! Vi er nødt til at give et

BEVIS. Denne sætning er et eksempel på en eksistens- og entydighedssætning. Beviset falder derfor i to dele. Den ene del argumenterer for eksistensen, den anden for entydigheden.

Eksistens: Lad S være mængden af alle hele tal som

- er ≥ 0
- kan skrives på formen $a - bq$ for et $q \in \mathbb{Z}$.

Dvs, at

$$S = \{a - bq \mid q \in \mathbb{N}\} \cap \mathbb{N}_0$$

Efter et øjebliks overvejelse indser du, at denne mængde af hele tal ikke er tom. Ifølge Princippet om det mindste element findes der derfor et mindste element i S. (Snydes der her?) Lad os kalde det mindste element for r:

$$r = \min S$$

Så er $r \geq 0$. Påstanden i sætningen er, at også $r < b$. Lad os prøve at antage, at $r \geq b$. Da er $r - b \geq 0$ og

$$r - b = (a - bq) - b = a - b(q + 1)$$

så $r - b$ er et tal i S, som er mindre end r. Det strider mod, at r er det mindste element i S. Da antagelsen fører os lige lukt i en modstrid, kan den ikke opretholdes. Vi må altså have $r < b$.

Entydighed: Lad

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b,$$
$$a = bq_2 + r_2, \quad 0 \leq r_2 < b,$$

være to fremstillinger af a. Vi skal vise, at $q_1 = q_2$ og $r_1 = r_2$.

$$r_1 - r_2 = -b(q_1 - q_2)$$

ligger i b-tabellen og opfylder

$$-b < r_1 - r_2 < b$$

fordi begge tal ligger mellem 0 og b. Hvor mange tal fra b-tabellen ligger der mellem $-b$ og b (endepunkterne fraregnet)? □

Hvis resten r er 0 siger vi at b går op i a. Vi kan definere dette begreb for vilkårlige to hele tal.

DEFINITION 2.3. *Lad $a \in \mathbb{Z}$ og $b \in \mathbb{Z}$ være to hele tal. Vi siger, at b går op i a, at b er en divisor i a, at a er et multiplum af b, eller at a er delelig med b, og vi skriver $b|a$, hvis der findes et helt tal $q \in \mathbb{Z}$ så $a = bq$.*

Alle hele tal er divisorer i 0, går op i 0. Alle andre hele tal har kun endelig mange divisorer.

BEMÆRKNING 2.4. Tallet b går op i tallet a, netop når a ligger i b-tabellen, eller netop når b-tabellen indeholder i a-tabellen. Da b-tabellen er mængden $b\mathbb{Z} = \{aq \mid q \in \mathbb{Z}\}$, og a-tabellen er $a\mathbb{Z}$, kan vi skrive:

$$b|a \Leftrightarrow b\mathbb{Z} \supseteq a\mathbb{Z}.$$

Der gælder følgende regneregler, hvis verifikation jeg overlader til dig.

SÆTNING 2.5. *Lad a og b være to hele tal.*

1. *$a|b \Rightarrow a|bc$ for ethvert helt tal c.*
2. *$ac|bc \Leftrightarrow a|b$ for ethvert helt tal $c \neq 0$. (Forkortningsreglen.)*
3. *Hvis $a|b$ og $b|c$, så vil $a|c$.*
4. *Hvis $a|b$ og $a|c$, så vil $a|(xb + yc)$ for alle $x, y \in \mathbb{Z}$.*
5. *Hvis $a|b$ og $b|a$, så er $a = \pm b$.*
6. *$a|0$.*
7. *$\pm 1|a$.*
8. *Hvis $a|b$ og $b \neq 0$, så er $|a| \leq |b|$.*

ØVELSE 2.6. Vi betragter her kun naturlige tal. Lad os skrive $a \leq b$ når vi mener $a|b$. (Det bringer forvirringen op på et højere niveau.) Omskriv (de relevante dele af) Sætning (2.5) med dette symbol. Find det "største" tal, som er "$\leq$" både 12 og 18. Find det "mindste" tal, som er "$\geq$" både 12 og 18. Kender du et andet navn for disse tal? (Eleverne i folkeskolen gør!)

2.7. Mindste fælles multiplum. Lad $a \in \mathbb{Z}$ og $b \in \mathbb{Z}$ være hele tal. I dette delafsnit vil vi antage, at hverken a eller b er 0. (Det er ikke en strengt nødvendig antagelse. Overvej, hvad der sker hvis enten a eller b er 0.)

DEFINITION 2.8. *Et fælles multiplum af a og b er et helt tal m, som er både a-tabellen og i b-tabellen.*

Da a-tabellen netop er $a\mathbb{Z}$, og b-tabellen $b\mathbb{Z}$ er fællesmængden

$$a\mathbb{Z} \cap b\mathbb{Z}$$

netop mængden af fælles multipla. Produktet ab er et fælles multiplum. Der er undeligt mange fælles multipla, f.eks. alle tal i ab-tabellen $\mathbb{Z}ab$.

EKSEMPEL 2.9. Et fælles multiplum af $a = 63$ og $b = 105$ er $ab = 6615$, men også $5 \cdot 63 = 315 = 3 \cdot 105$ er et fælles multiplum.

Et særligt interessant fælles multiplum, 315 i eksemplet, er det mindste fælles multiplum, der defineres sådan her:

DEFINITION 2.10. *Det hele tal m er et* mindste fælles multiplum *af a og b, hvis*

- *m er positiv*
- *m er et fælles multiplum af a og b*
- *m går op i ethvert fælles multiplum*

Vi konfronterer nu eksistens- og entydighedsproblemet for mindste fælles multiplum.

LEMMA 2.11 (Entydighed). *Der findes* højst *et mindste fælles multiplum af a og b.*

BEVIS. Antag, at både m_1 og m_2 er fælles multipla. Da m_2 er et fælles multiplum og m_1 et mindste fælles multiplum, vil m_1 gå op i m_2. Da m_1 er et fælles multiplum og m_2 et mindste fælles multiplum, vil m_2 gå op i m_1. Derfor er $m_1 = m_2$. □

LEMMA 2.12 (Eksistens). *Lad m være det mindste positive tal, som står både i a-tabellen og i b-tabellen. Da er m et mindste fælles multiplum af a og b.*

BEVIS. Påstanden er, at

$$m = \min((a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N})$$

er et mindste fælles multiplum af a og b – altså at m opfylder de tre krav fra Definition 2.10. (Naturligvis har du allerede lynhurtigt overvejet, at mængden $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}$ af positive tal, der står i både a-tabellen og i b-tabellen, ikke er tom.)

Det er klart, at $m > 0$ (for $m \in \mathbb{N}$), og at m er et fælles multiplum, for $a\mathbb{Z} \cap b\mathbb{Z}$ er jo simpelthen mængde af fælles multipla. Lad M være et (andet) fælles multiplum. Jeg påstår, at m går op i M. Ifølge Divisionsalgoritmen (2.1)

kan M skrives på formen $M = qm + r$, hvor $q \in \mathbb{Z}$ og $0 \leq r < m$. Vi kan ikke have $0 < r < m$, for da ville $r = M - qm$ være et positivt fælles multiplum, som var mindre end det mindste, m. Altså er $r = 0$, og $m \mid M$. Dette viser, at m er et mindste fælles multiplum. □

Vi ved nu, at der altid findes netop et mindste fælles multiplum af a og b. Vi betegner det med $\mathrm{mfm}(a, b)$.

Vi samler nu vores erfaring, og lidt til, i en sætningen om eksistens- og entydighed af mindste fælles multiplum.

SÆTNING 2.13 (Eksistens og entydighed af mindste fælles multiplum). *Lad $a \neq 0$ og $b \neq 0$ være to hele tal. Så gælder:*

1. *Der findes netop et mindste fælles multiplum,* $\mathrm{mfm}(a, b)$*, af a og b.*
2. $\mathrm{mfm}(a, b) = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N})$.
3. $\mathrm{mfm}(a, b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

BEVIS. Kun punkt (3) kræver en bemærkning: Da $\mathrm{mfm}(a, b)$ er et fælles multiplum, er $\mathrm{mfm}(a, b)\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$. Da ethvert fælles multiplum er et multiplum af $\mathrm{mfm}(a, b)$ er $a\mathbb{Z} \cap b\mathbb{Z} \subseteq \mathrm{mfm}(a, b)\mathbb{Z}$. □

EKSEMPEL 2.14. $\mathrm{mfm}(12, 18) = \min(12\mathbb{Z} \cap 18\mathbb{Z} \cap \mathbb{N}) = \min\{36, 72, \dots\} = 36$.

ØVELSE 2.15. Lad m være et naturligt tal, sådan et $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Vis, at $m = \mathrm{mfm}(a, b)$.

ØVELSE 2.16. Vis, at m er det mindste fælles multiplum af a og b hvis og kun hvis

- m er positiv
- m er et fælles multiplum af a og b
- m er mindre end eller lig med ethvert positivt fælles multiplum af a og b

Du skal altså vise, at den mindste af de positive fælles divisor er den mindste fælles divisor!

I næste afsnit kan du finde en algoritme til beregning af $\mathrm{mfm}(a, b)$.

2.17. Største fælles divisor. Lad $a \in \mathbb{Z}$ og $b \in \mathbb{Z}$ være to hele tal. I dette delafsnit vil vi antage, at ikke både a og b er 0. (Det er ikke en strengt nødvendig antagelse. Overvej, hvad der sker hvis både a og b er 0.)

DEFINITION 2.18. *En fælles divisor for a og b er et helt tal, m, som går op i både a og b (både a og b er i m-tabellen).*

Ethvert helt tal forskellig fra 0 har kun endeligt mange divisorer. (For hvis $m|a$, hvor $a \neq 0$, så er $|m| \leq |a|$.) Der findes derfor kun endeligt mange fælles divisorer for a og b.

EKSEMPEL 2.19. De fælles positive divisorer for $a = 12$ og $b = 18$ er $1, 2, 3, 6$. De fælles positive divisorer for $a = 30$ og $b = 42$ er også $1, 2, 3, 6$.

Vi kan også karakterisere de fælles divisorer på denne (mere gennemskuelige?) måde:

$$\begin{aligned} & m \text{ er en fælles divisor for } a \text{ og } b \\ \Leftrightarrow & \mathbb{Z}m \supseteq \mathbb{Z}a \text{ og } \mathbb{Z}m \supseteq \mathbb{Z}b \\ \Leftrightarrow & \mathbb{Z}m \supseteq \mathbb{Z}a \cup \mathbb{Z}b \\ \Leftrightarrow & \mathbb{Z}m \supseteq \mathbb{Z}a + \mathbb{Z}b \end{aligned}$$

Her benytter jeg benytter skrivemåden

$$\mathbb{Z}a + \mathbb{Z}b = \{sa + tb \mid s \in \mathbb{Z}, t \in \mathbb{Z}\}$$

for mængde af alle hele tal, der kan skrives som en sum af et tal fra a-tabellen og et tal fra b-tabellen. Vi har

$$\mathbb{Z}a + \mathbb{Z}b \supseteq \mathbb{Z}a \cup \mathbb{Z}b$$

så den sidste biimplikationspil er OK i den ene retning. Den anden retning kræver en lille overvejelse.

Hvis $D(a)$ står for mængden af divisorer i a, så er fællesmængden $D(a) \cap D(b)$ netop mængden af fælles divisorer for a og b.

Vi skal nu se på en algoritme, *Euklids algoritme*, til bestemmelse af de fælles divisorer.

Lad os sige, vi ønsker at bestemmme de fælles divisorer for a_0 of a_1. Vi antager, at $a_0 \geq a_1 > 0$. Divider nu a_0 med a_1 og kald resten a_2:

$$a_0 = q_1 a_1 + a_2, \quad a_1 > a_2 \geq 0.$$

Hvis $a_2 = 0$ stopper algoritmen her. Men hvis $a_2 > 0$, dividerer vi a_1 med a_2, og kalder resten a_3. Hvis $a_3 = 0$ stopper algoritmen her. Men hvis $a_3 > 0 \ldots$

Generelt, kan vi sige at output fra Euklids algoritme er en dalende følge af hele tal

$$a_0 > a_1 > \cdots > a_{i-1} > a_i > a_{i+1} > \cdots \geq 0$$

hvor a_{i+1} er den rest der opstår når vi dividerer a_{i-1} med a_i,

$$a_{i-1} = q_i a_i + a_{i+1}, \quad a_i > a_{i+1} \geq 0, \tag{2.1}$$

hvis ellers $a_i > 0$. Algoritmen stopper, hvis $a_i = 0$. Læg mærke til, at algortimen *må* stoppe efter endelig mange skridt, da der kun findes endeligt mange tal mellem a_0 og 0. Lad os sige, at $a_n > 0$, men at $a_{n+1} = 0$. Overvej nøje, at ligningen (2.1), som definerer Euklids algoritme, viser (og det fortjener et lille argument!), at

$$D(a_{i-1}) \cap D(a_i) = D(a_i) \cap D(a_{i+1}), \quad 1 \leq i \leq n,$$

dvs. at a_{i-1} og a_i har de samme fælles divisorer som a_i og a_{i+1}. Da $a_{n+1} = 0$ får vi

$$D(a_0) \cap D(a_1) = D(a_n) \cap D(0) = D(a_n) \cap \mathbb{Z} = D(a_n),$$

som siger, at mængde af fælles divisorer for a_0 og a_1 er mængden af divisorer i det sidste positive tal, a_n i Euklids algoritme.

EKSEMPEL 2.20. Med input $a_0 = 712$ og $a_1 = 123$ producerer Euklids algoritme den endelige følge

$$712, 123, 97, 26, 19, 7, 5, 2, 1, 0$$

som output. De fælles divsorer for 712 og 123 er derfor $D(712) \cap D(123) = D(1) = \{-1, 1\}$.

Det er ganske enkelt at implementere Euklids algoritme på en computer, f.eks. i et regneark eller i Turbo Pascal.

Lad os vende tilbage til ligningen (2.1) endnu en gang. En anden konsekvens (og det fortjener igen et argument!) er identiteterne

$$a_{i-1}\mathbb{Z} + a_i\mathbb{Z} = a_i\mathbb{Z} + a_{i+1}\mathbb{Z}, \quad 1 \leq i \leq n,$$

som viser, at

$$a_0\mathbb{Z} + a_1\mathbb{Z} = a_n\mathbb{Z} + 0\mathbb{Z} = a_n\mathbb{Z},$$

dvs. at tallene fra a_n-tabellen præcis er de tal, der kan skrives som en sum af et tal fra a_0-tabellen og et tal fra a_1-tabellen. Det følger, at

$$a_n = \min((a_0\mathbb{Z} + a_1\mathbb{Z}) \cap \mathbb{N})$$

dvs. at a_n er det mindste positive tal, der kan fås som sum af et tal fra a_0-tabellen med ét fra a_1-tabellen. (F.eks. siger Euklids algoritme, at 1 kan fås som en sum af et tal fra 712-tabellen med et tal fra 123-tabellen.)

Det er klart, at tallet a_n selv er den mest interessante fælles divisor, for alle fælles divisorer er også divisorer i a_n. Hvordan kan vi karakterisere dette tal?

DEFINITION 2.21. *Det hele tal D er en* største fælles divisor *for a og b, hvis*

- $D > 0$
- *D er en fælles divior for a og b*
- *Enhver fælles divisor går op i D*

Tallet a_n fra Euklids algoritme med input $a_0 = a$ og $a_1 = b$ (hvis ellers $a \geq b > 0$) er en største fælles divisor for a og b. Kunne der være andre og er vi sikre på at der altid findes én?

LEMMA 2.22 (Entydighed). *Der findes* højst *en største fælles divisor for a og b.*

BEVIS. Prøv selv! □

LEMMA 2.23 (Eksistens). *Det mindste naturlige tal, der kan skrives som en sum af et tal fra a-tabellen og et tal fra b-tabellen, dvs. det mindste positive tal som kan skrives på formen $sa + bt$ for $s, t \in \mathbb{Z}$, er en største fælles divisor.*

BEVIS. Påstanden er at

$$D = \min((a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N})$$

er en største fælles divisor – altså at D opfylder de tre krav fra Definition 2.21. (Overvej, at mængden $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}$ ikke er tom.)

Det er klart, at $D>0$. D går også op i a. For at se det, skriv (2.1) a på formen $a=Dq+r$ hvor $q\in\mathbb{Z}$ og $0\leq r<D$. Husk på, at der findes hele tal, s og t, så $D=as+bt$. Altså kan resten

$$r=a-Dq=a-(as+bt)q=(1-qs)a+(-tq)b$$

skrives som en sum af et tal fra a-tabellen og et tal fra b-tabellen. Vi kan ikke have $0<r<D$, for da ville r være mindre end det mindste naturlige tal, D, med denne egenskab. Altså er $r=0$, så D går op i a. På akkurat tilsvarende måde kan man vise, at D går op i b. D er altså en fælles divisor. Lad d være en (anden) fælles divisor. Da D har formen $D=as+bt$, $s\in\mathbb{Z}$, $t\in\mathbb{Z}$, vil d gå op i D. Dette viser, at D er en største fælles divisor. □

Vi ved nu, at der altid findes netop en største fælles divisor for a og b. Vi betegner den med $\mathrm{sfd}(a,b)$.

Vi samler vores erfaring, og lidt til, i sætningen om eksistens- og entydighed af største fælles divisor.

SÆTNING 2.24 (Eksistens og entydighed af største fælles divisor). *Lad a og b være hele tal, ikke begge 0. Da gælder:*

1. *Der findes netop en største fælles divisor,* $\mathrm{sfd}(a,b)$ *for a og b.*
2. $\mathrm{sfd}(a,b)=\min((a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N})$.
3. $\mathrm{sfd}(a,b)\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$.

BEVIS. Kun punkt (3) kræver en bemærkning: Da $\mathrm{sfd}(a,b)$ er en sum af et tal fra a-tabellen og et tal tal fra b-tabellen, er $\mathrm{sfd}(a,b)\mathbb{Z}\subseteq a\mathbb{Z}+b\mathbb{Z}$. Vi har også $a\mathbb{Z}+b\mathbb{Z}\subseteq\mathrm{sfd}(a,b)\mathbb{Z}$, fordi en sum af et tal fra a-tabellen og et tal fra b-tabellen er deleligt med $\mathrm{sfd}(a,b)$. □

Læg mærke til at punkt (3) siger, at den største fælles divisor er en sum af et tal fra a-tabellen og et tal fra b-tabellen. Det er så nyttigt, at jeg får lyst til at fremhæve det i et

KOROLLAR 2.25. *Lad a og b være hele tal, ikke begge 0. Sæt $D=\mathrm{sfd}(a,b)$. Da findes hele tal s og t så*

$$D=sa+tb$$

ØVELSE 2.26. Find s og t, så $1=712s+123t$.

ØVELSE 2.27. Lad D være et naturligt tal sådan at $D\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$. Vis, at $D=\mathrm{sfd}(a,b)$.

ØVELSE 2.28. Vis, at $\max(D(a)\cap D(b))=\mathrm{sfd}(a,b)$; altså, at den største fælles divisor er den største fælles divisor!

Vi ved allerede fra Euklids algoritme, hvordan den største fælles divisor beregnes.

SÆTNING 2.29. *Antag at* $a_n > 0$ *og at* $a_{n+1} = 0$ *i Euklids algoritme med input* $a_0 > a_1 \geq 0$. *Da er* $\mathrm{sfd}(a_0, a_1) = a_n$ *og* $\mathrm{mfm}(a_0, a_1) = \frac{a_0 a_1}{a_n}$.

Den sidste påstand følger af Opgave 17, som siger at $\mathrm{sfd}(a,b)\cdot\mathrm{mfm}(a,b) = |ab|$.

Euklids algoritme fortæller også, hvordan vi finder s og t, så $D = as + bt$. Beregningen af s og t kan godt formuleres algoritmisk, men vi skal her nøjes med et eksempel.

EKSEMPEL 2.30. Med $a_0 = 2415$ og $a_1 = 945$ som input genererer Euklids algoritme tallene

$$2415, 945, 525, 420, 105, 0$$

som output og altså er $\mathrm{sfd}(2415, 945) = 105$ og $\mathrm{mfm}(2415, 945) = 21735$. Dette output er et resulat af divisionerne

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0. \end{aligned}$$

Ligningerne ovenfor kan også skrives

$$\begin{aligned} 525 &= 2415 - 945 \cdot 2 \\ 420 &= 945 - 525 \cdot 1 \\ 105 &= 525 - 420 \cdot 1 \end{aligned}$$

og idet vi starter forneden og arbejder os opad, får vi heraf

$$\begin{aligned} 105 &= 525 - 420 = 525 - (945 - 525) = 525 \cdot 2 - 945 \\ &= (2415 - 945 \cdot 2) \cdot 2 - 945 = 2415 \cdot 2 + 945 \cdot (-5). \end{aligned}$$

Vi kan altså bruge $s_0 = 2$ og $s_1 = -5$. Der er også andre muligheder, for da $2415 = 105 \cdot 23$ og $945 = 105 \cdot 9$ er $0 = 2415 \cdot 9 - 945 \cdot 23$ og $105 = 105 + 0 = (2415 \cdot 2 + 945 \cdot (-5)) + (2415 \cdot 9 - 945 \cdot 23) = 2415 \cdot 11 + 945 \cdot (-28)$.

ØVELSE 2.31. Find s og t så $712s + 123t = 1$.

ØVELSE 2.32. Skriv et computerprogram der med input (a_0, a_1) giver output $\mathrm{sfd}(a_0, a_1)$ samt hele tal (s_0, s_1) så $a_0 s_0 + a_1 s_1 = \mathrm{sfd}(a_0, a_1)$.

2.33. Indbyrdes primiske tal. Tallene 123 og 712 er et eksempel på to indbyrdes primiske hele tal, da 1 er det eneste positive tal, som går op i både 123 og 712. Den generelle definition lyder sådan her:

DEFINITION 2.34. *De to hele tal* a *og* b *er* indbyrdes primiske *hvis* $\mathrm{sfd}(a, b) = 1$.

Vi vil i det følgende antage at både a og b er forskellige fra 0.

LEMMA 2.35. *Hvis a og b er indbyrdes primiske, og a går op i bc, da vil a gå op i c.*

BEVIS. Da $a \mid bc$ og $\mathrm{sfd}(a,b) = 1$, er (2.4, 2.24) $bc\mathbb{Z} \subseteq a\mathbb{Z}$ og $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Altså er

$$c\mathbb{Z} = c(a\mathbb{Z} + b\mathbb{Z}) = ca\mathbb{Z} + cb\mathbb{Z} \subseteq a\mathbb{Z} + a\mathbb{Z} = a\mathbb{Z}$$

så $a \mid c$. □

LEMMA 2.36. $\mathrm{sfd}(a,b) = 1 \Leftrightarrow \mathrm{mfm}(a,b) = |ab|$.

BEVIS. Antag, at $\mathrm{sfd}(a,b) = 1$. Vi skal vise, at ab går op i ethvert fælles multiplum. Lad $M = sa = tb$ være et fælles multiplum. Da $a \mid tb$ og $\mathrm{sfd}(a,b) = 1$ vil (2.35) a gå op i t og ab vil gå op i $tb = M$.

Antag, at $\mathrm{mfm}(a,b) = |ab|$. Vi skal vise, at de eneste fælles divisorer er ± 1. Lad d være en fælles divisor, $a = da'$ og $b = db'$. Da $da'b'$ er et fælles multiplum, vil $ab = d^2a'b'$ gå op i $da'b'$, og derfor vil d gå op i 1. □

Vi samler til sidst resultaterne fra Sætning 2.13, Sætning 2.24 og Lemma 2.36 i en sætning.

SÆTNING 2.37. *Lad a og b være to hele tal. Da er følgende betingelser ækvivalente:*

1. $\mathrm{sfd}(a,b) = 1$
2. $\mathrm{mfm}(a,b) = |ab|$
3. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$
4. $a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$
5. *Der findes hele tal s og t så $as + bt = 1$.*

Vi vil i en senere anvendelse (II.7.1) af Sætning 2.37 erstatte 2.37.(4) med det tilsyneladende svagere $a\mathbb{Z} \cap b\mathbb{Z} \subseteq ab\mathbb{Z}$. Det kan vi tillade os fordi fordi inklusionen $ab\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$ altid gælder.

KOROLLAR 2.38. *Hvis a og b er indbyrdes primiske, og a og b går op i c, da vil ab gå op i c.*

BEVIS. Tallet c er et fælles multiplum af a og b, så det mindste fælles multiplum, $\mathrm{mfm}(a,b) = ab$, går op i c. □

.

3. Primtal

Primtallene har fascineret mennesket gennem i hvert fald de seneste par tusind år, og det vil de nok fortsætte med vores tid ud.

DEFINITION 3.1. *Det naturlige tal n kaldes et* sammensat tal*, hvis der findes hele tal, n_0 og n_1, så $n = n_0n_1$, hvor $1 < n_0 < n$ og $1 < n_1 < n$. Et* primtal *er et naturligt tal $p > 1$ som ikke er sammensat.*

Et primtal er altså et naturligt tal, som er større end 1, og som ikke har andre positive divisorer end 1 og sig selv. De første primtal er

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$$

og det er faktisk ret let at finde alle primtal under 100 – f.eks. ved at bruge:

BEMÆRKNING 3.2. (Eratostenes' si.) Gem tallet 2. Fjern dernæst alle multipla af 2 fra mængden af naturlige tal $n > 1$. Det mindste tilbageblivende tal er 3. Gem det, for det er et primtal. Fjern derefter alle multipla af 3. Gem det mindste af de tilbageblivende tal, 5. Fjern alle multipla af 5 – osv. Det der bliver tilbage er primtallene. Hvis vi er interesseret i at finde alle primtal $\leq N$ kan vi nøjes med at fjerne alle multipla af n for $2 \leq n \leq \sqrt{N}$. Skriv et computerprogram der beregner alle primtal $\leq N$. Find alle primtal < 10000. (Vel, har du ikke adgang til en computer, kan du nøjes med at finde alle primtal < 100.)

Hvis p er et primtal, og a et naturligt tal, så er $\mathrm{sfd}(p, a) = 1$, hvis og kun hvis p ikke er en divisor i a. Derfor er følgende to observationer faktisk specialtilfælde af (2.35) og (2.38).

LEMMA 3.3 (Primtalsdivisionssætningen, Euklid). *Lad p være et primtal og a og b to hele tal. Hvis $p \mid ab$, da vil $p \mid a$, eller $p \mid b$.*

BEVIS. Hvis $p \mid a$ er der intet at vise. Hvis p ikke er en divisor i a, da er a og p indbyrdes primiske og så vil $p \mid b$ ifølge (2.35). □

LEMMA 3.4 (Coprimtalsdivisionssætningen). *Lad p og q være to forskellige primtal. Hvis $p \mid a$ og $q \mid a$, da vil $pq \mid a$.*

BEVIS. Da $p \neq q$, er p og q indbyrdes primiske, $\mathrm{sfd}(p, q) = 1$, og resultatet følger direkte af Korollar 2.38. □

SÆTNING 3.5. *Ethvert naturligt tal $n > 1$ er et produkt af primtal.*

BEVIS. Lad $P(n)$, $n \geq 2$, være påstanden, at n er et produkt af primtal. $P(2)$ er sand, for 2 er et primtal. Antag at $P(k)$ er sand for $1 < k < n$. Hvis n er et primtal, er $P(n)$ oplagt sand. Hvis ikke, er $n = n_0 n_1$, hvor $1 < n_0 < n$ og $1 < n_1 < n$, og begge faktorer er ifølge induktionsantagelsen produkter af primtal. Derfor er også n et produkt af primtal. Dette viser at $P(n)$ er sand.

Ifølge Induktionsaksiomet (1.6) følger det nu, at alle naturlige tal kan skrives som produkter af primtal. □

KOROLLAR 3.6. *Ethvert naturligt tal $n > 1$ har en primtalsdivisor.*

I fremstillingen af n som et produkt af primtal kan det samme primtal godt forekomme flere gange som i eksemplet

$$12 = 2 \cdot 2 \cdot 3. \tag{3.7}$$

Samler vi alle faktorer af samme primtal p og udtrykker produktet som en potens af p, kan enhver primfaktoropløsning af $n > 1$ skrives på formen

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \tag{3.8}$$

hvor $1 < p_1 < p_2 < \cdots < p_r$ er forskellige primtal og $\alpha_i$erne er naturlige tal. På den måde kan (3.7) omskrives til

$$12 = 2^2 \cdot 3.$$

Sætning 3.5 siger, at ethvert naturligt tal $n > 1$ har mindst en fremstilling af formen (3.8). Kan n have mere end en fremstilling? Svaret er, ifølge den følgende sætning om entydig faktorisering, nej.

SÆTNING 3.9 (Aritmetikkens Hovedsætning). *Antag at*

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

hvor $1 < p_1 < p_2 < \dots p_r$, $1 < q_1 < q_2 < \dots q_s$, *alle* p_i *og alle* q_j *er primtal, og alle* α_i *og* β_j *er naturlige tal. Da er* $r = s$, *og* $p_i = q_i$ *og* $\alpha_i = \beta_i$ *for alle* $i = 1, 2, \dots, r$.

BEVIS. Lad $P(n)$, $n > 1$, stå for den påstand, at n kun har én primfaktoropløsning (3.8). $P(2)$ er klart sand, da 2 er et primtal.

Antag at $P(k)$ er sand for $1 < k < n$. Hvis n er et primtal, findes kun en faktorisering af formen (3.8), så $P(n)$ er sand i dette tilfælde. Hvis n er et sammensat tal, lad

$$p_1 p_2 \dots p_u = n = q_1 q_2 \dots q_v \tag{3.10}$$

være to fremstillinger af n. (Her er antallene af faktorer $u \geq 2$ og $v \geq 2$, da n ikke er et primtal.) Vi kan ordne faktorerne i voksende orden så vi opnår at

$$p_1 \leq p_2 \leq \cdots \leq p_u, \quad q_1 \leq q_2 \leq \cdots \leq q_v.$$

Vi stiler mod at vise, at $u = v$, og $p_i = q_i$ for alle $i = 1, 2, \dots, u$.

Antag nu at $p_1 \neq q_1$. Da p_1 og q_1 går op i n, og p_1 og q_1 er indbyrdes primiske, vil (3.4) produktet $p_1 q_1$ gå op i n. Skriv n på formen $n = p_1 q_1 r$ og lad $r = r_1 \dots r_l$ være en fremstilling af r som et produkt (3.5) af primtal. Da er

$$n = p_1 q_1 r_1 \dots r_l$$

en fremstiling af n som et produkt af primtal. Nu ved vi, at

$$p_1 p_2 \dots p_u = n = p_1 q_1 r_1 \dots r_l$$

eller (ved division med p_1) at

$$p_2 \dots p_u = \frac{n}{p_1} = q_1 r_1 \dots r_l.$$

Fra induktionsantagelsen slutter vi, at disse to fremstillinger af $\frac{n}{p_1} < n$ har de samme faktorer. Specielt må q_1 på højresiden være lig med et af tallene $p_2, \ldots, p_u$ på venstresiden. Altså er $q_1 \geq p_1$, da $p_2 \geq p_1, \ldots, p_u \geq p_1$. Tilsvarende er

$$q_1 q_2 \ldots q_v = n = p_1 q_1 r_1 \ldots r_l$$

eller

$$q_2 \ldots q_v = \frac{n}{q_1} = p_1 r_1 \ldots r_l$$

og induktionsantagelsen giver, at faktoren p_1 fra højresiden er lig med en af faktorerne $q_2, \ldots, q_v$ fra venstresiden, og det følger, at $p_1 \geq q_1$, da $q_2 \geq q_1, \ldots, q_v \geq q_1$. Vi kan nu konkludere, at $p_1 = q_1$. Det er i åbenlys modstrid med antagelsen $p_1 \neq q_1$.

Vi ser heraf, at $p_1 \neq q_1$ ikke kan gælde. Altså må vi have $p_1 = q_1$, og vi kan nu dividere begge sider af fremstillingen (3.10) med $p_1 = q_1$. Det giver:

$$p_2 \ldots p_u = \frac{n}{p_1} = \frac{n}{q_1} = q_2 \ldots q_v$$

og da $\frac{n}{p_1} = \frac{n}{q_1}$ er mindre end n, giver induktionsantagelsen, at $u = v$ (eller rettere at $u - 1 = v - 1$) og at $p_i = q_i$ for alle $i = 2, \ldots, u$. Dette viser, at $P(n)$ er sand, også hvis n er sammensat.

Induktionsaksiomet tillader os nu at konkludere, at alle hele tal $n > 1$ har en entydig primtalsfaktorisering. □

ØVELSE 3.11. Skriv et computerprogram, der beregner primtalsfaktoriseringer.

Sætningen om Entydig Faktorisering har sandsynligvis været kendt i en eller anden form siden Euklid, men den første eksplicitte formulering skyldes Gauss i 1801. Den næste sætning skyldes faktisk Euklid, så den dateres til ca. -400, hvor Euklid viste, at "der er flere primtal end ethvert forelagt antal af primtal".

SÆTNING 3.12 (Euklid). *Der findes uendeligt mange primtal.*

BEVIS. Antag, at der kun findes endelig mange primtal. Lad $p_1, \ldots, p_k$ være listen over alle primtal. Sæt

$$n = 1 + p_1 \ldots p_k.$$

Ifølge (3.6) har n en primtalsdivisor, p. Men dette primtal p er forskelligt fra $p_1, \ldots, p_k$, for ingen af disse primtal går op i n (resten ved division af n med p_i er 1). Det er i modstrid med antagelsen, at vores liste bestod af *alle* primtal. □

Selv om der altså findes uendeligt mange pritmal, så findes der på den anden side vilkårligt lange primtalsfri zoner.

BEMÆRKNING 3.13. Lad n være et helt tal. De $n - 1$ tal

$$n! + 2, n! + 3, \ldots, n! + n$$

er alle sammensatte, for $2|n!+2, 3|n!+3, \ldots, n|n!+n$. Vi kan altså finde vilkårligt lange strækninger af primtalsfrie naturlige tal.

Her er nogle af eksempler på uløste problemer om primtal:

- Goldbachs formodning fra 1742: Ethvert lige tal > 2 er en sum af to primtal. F.eks. er $4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, \ldots, 36 = 13 + 23$.
- Hvis både p og $p + 2$ er primtal, siges de at være primtalstvillinger. Det formodes, men vides ikke, at der findes uendeligt mange primtalstvillinger. I begyndelsen af talrækken er primtalstvillinger ret hyppige, 2 og 3, 3 og 5, 5 og 7. Også 250049 og 2500051 er (lidt større) tvillinger. Det siges, at $242206083 \cdot 2^{38880} \pm 1$ er primtalstvillinger.
- En sætning af Gauss, som han beviste, da han var 19, siger, at den regulære p-kant, hvor p er et ulige primtal, er konstruerbar hvis og kun hvis p er et Fermat tal. Et Fermat tal er et tal af formen $F_t = 2^{2^t} + 1$ for et $t \geq 0$. Fermat påstod, at alle tal af denne form, var primtal, og godt nok er $3, 5, 17, 257, 65537$ svarende til $t = 0, 1, 2, 3, 4$ alle primtal. (Den regulære 257-kant kan altså konstrueres med passer og lineal.) L. Euler (1707–1783) viste imidlertid, at

  $$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417,$$

  er sammensat. F_6 er produktet af primtallet 274177 og et andet primtal med 14 cifre. Faktisk ved man i dag, at $F_5, \ldots, F_{20}$ alle er sammnensatte tal. Mange talteoretikere tror nu, at alle Fermat tal efter F_4 er sammensatte [**3**].

Læs mere om primtal på
http://www.utm.edu/research/primes/index.html

Opgaver

OPGAVE 1. Vis, at $2^n > n^2 + 1$ for alle naturlige tal $n \geq 5$.

OPGAVE 2. Vis, at

$$\sum_{k=1}^{n} 2^{k-1} = 2^n - 1$$

for alle naturlige tal $n \in \mathbb{N}$.

OPGAVE 3. Vis, at

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

for all naturlige tal $n \in \mathbb{N}$.

OPGAVE 4. Vis, at

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

for alle naturlige tal $n \in \mathbb{N}$.

OPGAVE 5. Vis, at $n! > 2^n$ for alle naturlige tal $n \geq 4$.

OPGAVE 6. Vis, at 9 går op i $10^{n+1} + 3 \cdot 10^n + 5$ for alle naturlige tal $n \in \mathbb{N}$.

OPGAVE 7. Vis, at enhver *opad* begrænset mængde $S \subseteq \mathbb{Z}$ har et største element, $\max S$. Vink: $\max S = -\min(-S)$.

OPGAVE 8. Lad $S \subseteq \mathbb{Z}$ være nedad begrænset. Vis, at $\min(aS) = a\min(S)$ når $a > 0$. Hvad kan du sige når $a < 0$?

OPGAVE 9. Vis, at $\min(S_1) \geq \min(S_2)$ når $S_1 \subseteq S_2 \subseteq \mathbb{Z}$ er nedad begrænsede mængder af hele tal.

OPGAVE 10. Brug Euklids algoritme til at beregne $\text{sfd}(a, b)$ og finde hele tal s og t så $as + bt = \text{sfd}(a, b)$ for $a = 1091, b = 165$ og $a = 1324, b = 56$.

OPGAVE 11. Vis, at $\text{sfd}(a, b) = \text{sfd}(-a, b) = \text{sfd}(-a, -b) = \text{sfd}(b, a) = \text{sfd}(|a|, |b|)$. Gælder noget tilsvarende for $\text{mfm}(a, b)$?

OPGAVE 12. Antag, at $a > 0$ og $b > 0$ og vis: $\text{sfd}(a, b) = a \Leftrightarrow a \mid b \Leftrightarrow \text{mfm}(a, b) = b$.

OPGAVE 13. Vis, at $\text{sfd}(a, b + sa) = \text{sfd}(a, b)$. Brug dette til at beregne $\text{sfd}(572, 112)$.

OPGAVE 14. Antag (for nemheds skyld) at $a > 0, b > 0, c > 0$. Vis, at

$$\text{sfd}(ca, cb) = c\,\text{sfd}(a, b)$$
$$\text{mfm}(ca, cb) = c\,\text{mfm}(a, b)$$

OPGAVE 15. Vis, at $\text{sfd}(a, bc) = \text{sfd}(a, \text{sfd}(a, b)c)$. Vink: $a\mathbb{Z} + bc\mathbb{Z} = a\mathbb{Z} + (a\mathbb{Z} + b\mathbb{Z})c$.

OPGAVE 16. Kik på denne tabel:

a	b	ab	$\text{mfm}(a, b)$	$\text{sfd}(a, d)$
2	6	12	6	2
-4	6	-24	12	2
6	8	48	24	2
6	-9	-54	18	3
24	36	864	72	12

Formuler en formodning om sammmenhængen mellem tallen i de tre sidste søjler. Regn den næste opgave.

OPGAVE 17. Vis, at $\text{mfm}(a, b) \cdot \text{sfd}(a, b) = |ab|$ (når $a \neq 0$ og $b \neq 0$).

OPGAVE 18. Vis, at $\text{sfd}(a^2, b^2) = \text{sfd}(a^2, \text{sfd}(\text{sfd}(a, b)^2, b)b)$. Slut heraf at hvis $\text{sfd}(a, b) = 1$, da er også $\text{sfd}(a^2, b^2) = 1$.

OPGAVE 19. Hvad siger Opgave 18 om $\text{sfd}(\frac{a^2}{\text{sfd}(a,b)^2}, \frac{b^2}{\text{sfd}(a,b)^2})$? Konkludér, at $\text{sfd}(a^2, b^2) = \text{sfd}(a, b)^2$.

OPGAVE 20. Antag, at a er indbyrdes primisk med $a_1, \ldots, a_r$. Vis, at a er indbyrdes primisk med produktet $a_1 \ldots a_r$. (Vink: Induktion.)

OPGAVE 21. Lad p være et primtal og $a_1, \ldots, a_r$ hele tal. Vis, at hvis p går op i produktet $a_1 \ldots a_r$, da vil $p \mid a_i$ for (mindst) et i, $1 \leq i \leq r$. (Vink: Se (3.3) og brug induktion.)

OPGAVE 22. Antag, at tallene $a_1, \ldots, a_r$ er parvis indbyrdes primiske, dvs. at $\text{sfd}(a_i, a_j) = 1$ for $i \neq j$, og at de alle går op i b. Vis, at produktet $a_1 \ldots a_r$ går op i b. (Vink: Se (2.38) og brug induktion.)

OPGAVE 23. Lad a_1, a_2, a_3 være hele tal. Vis at a_1, a_2, a_3 er parvis indbyrdes primiske, dvs $\text{sfd}(a_2, a_3) = \text{sfd}(a_1, a_3) = \text{sfd}(a_1, a_2) = 1$, hvis og kun hvis der findes hele tal s_1, s_2, s_2 så $s_1 a_2 a_3 + s_2 a_1 a_3 + s_3 a_1 a_2 = 1$. Kan du generalisere dette resulat?

OPGAVE 24. Antag at $p \mid a^2$ hvor p er et primtal og a et helt tal. Vis, at $p \mid a$.

OPGAVE 25. Er 499 et primtal? Er 501? (Se (3.2.))

OPGAVE 26. Skriv 9464 som et produkt af primtal.

OPGAVE 27. Vis, at der ikke findes hele tal m og n så $m^2 = 2n^2$. Slut at $\sqrt{2}$ ikke er rational (dvs. ikke kan skrives på formen $\frac{m}{n}$). (Se Messer p. 121.)

OPGAVE 28. Skriv $a > 0$ og $b > 0$ på formen

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}.$$

Hvis vi tillader at $\alpha_i$erne og $\beta_i$erne kan antage værdien 0, kan vi godt antage at det er de samme primtal der forekommer i begge faktoriseringer hvor $p_1 < p_2 < \ldots p_r$. Vis, at

1. $a|b \Leftrightarrow \alpha_i \leq \beta_i$ for alle $i = 1, \ldots, r$.
2. $\text{sfd}(a, b) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}}$
3. $\text{mfm}(a, b) = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}}$

KAPITEL 2

Gruppeteori

En gruppe er en algebraisk struktur som optræder meget hyppigt i matematik. Faktisk drejede hele første kapitel sig om den abelske gruppe af hele tal. Andre eksempler på grupper er symmetrigrupper, f.eks. symmetrigruppen af et molekyle.

1. Funktioner

Formålet med dette afsnit er at indføre nogle begreber. Det indeholder sikkert ikke noget der er nyt for dig, så jeg udelader beviserne. (Se også Messer p. 219–221.)

Lad A og B være mængder. En funktion $f\colon A \to B$ med *domæne* $\mathrm{dom}(f) = A$ og *codomæne* $\mathrm{codom}(f) = B$ er en forskrift der til ethvert element a i A knytter netop et element $f(a)$ i B. Elementet $f(a) \in B$ er *billedet* af $a \in A$.

For delmængder $A_1 \subseteq A$ og $B_1 \subseteq B$ kaldes

$$f(A_1) = \{f(a_1) \mid a_1 \in A_1\}$$

for *billedet* af A_1 og

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}$$

for *originalmængden* af B_1. Specielt, for et element $b \in B$, betegner

$$f^{-1}(b) = f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$$

af alle elementer i A som afbildes i $b \in B$, originalmængden til b.

DEFINITION 1.1. *Funktionen $f\colon A \to B$ er*

1. surjektiv *hvis ethvert element i B er billede af mindst et element i A*
2. injektiv *hvis ethvert element i B er billede af højst et element i A*
3. bijektiv *hvis ethvert element i B er billede af netop et element i A.*

Funktionen f er surjektiv, hvis $f^{-1}(b) \neq \emptyset$ for alle $b \in B$, injektiv hvis $f^{-1}(b)$ indeholder højst et element for alle $b \in B$, bijektiv hvis $f^{-1}(b)$ indeholder netop et element for alle $b \in B$. En funktion er bijektiv hvis og kun hvis den er surjektiv og injektiv.

Hvis $f\colon A \to B$ og $g\colon B \to C$ er to funktioner med $\mathrm{codom}(f) = \mathrm{dom}(g)$, da er sammensætningen $g \circ f\colon A \to C$ funktionen defineret ved $g \circ f(a) = g(f(a))$ for all $a \in A$.

SÆTNING 1.2. *(Sammensætning af funktioner er associativ). Lad* $f\colon A \to B$, $g\colon B \to C$ *og* $h\colon C \to D$ *være funktioner. Da er*

$$h \circ (g \circ f) = (h \circ g) \circ f\colon A \to D.$$

Da det alligevel ikke spiller nogen rolle hvor parenteserne placeres, skriver vi $h \circ g \circ f$ for en af de to sammensatte funktioner i Sætning 1.2.

ØVELSE 1.3. Enhver funktion kan skrives som sammensætningen af en surjektion efterfulgt af en injektion.

Identitetsfunktionen $\mathrm{id}_A\colon A \to A$ eller $1_A\colon A \to A$ er den funktion der til ethvert element $a \in A$ knytter a.

Vi siger, at $g\colon B \to A$ er en *invers* til $f\colon A \to B$ hvis $g \circ f = 1_A$ og $f \circ g = 1_B$. Hvis f har en invers, da er den entydigt bestemt og vi betegner den med f^{-1}. Men ikke alle funktioner har en invers.

SÆTNING 1.4. *En funktion har en invers hvis og kun hvis den er bijektiv.*

ØVELSE 1.5. Hvis både f og g er bijektive og $\mathrm{codom}(f) = \mathrm{dom}(g)$, da er $g \circ f$ bijektiv med invers $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Den inverse funktion f^{-1} er bijektiv og dens inverse er $(f^{-1})^{-1} = f$.

Jeg slutter med en meget simpel, men overraskende nyttig observation.

SÆTNING 1.6. *(Skuffeprincippet.) Antag at* A *og* B *er to endelige mængder og at antallet af elementer i* A *er lig med antallet af elementer i* B. *Lad* $f\colon A \to B$ *være en afbildning fra* A *til* B. *Da er følgende betingelser ækvivalente:*

1. f *er injektiv.*
2. f *er surjektiv.*
3. f *er bijektiv.*

Som ethvert postbud ved, hvis 100 breve fordeles i 100 postkasser så der højst ligger et brev i hver postkasse, da vil der faktisk ligge netop et brev i hver postkasse.

2. Transformationer af planen

Den geometriske plan kan identificeres med mængden $\mathbb{R}^2$ af alle reelle talpar ved valg af et koordinatsystem. Ved en (ortogonal) transformation af planen forstår vi en afbildning af planen ind i sig selv givet ved en drejning om $(0,0)$ eller en spejling i en ret linje gennem $(0,0)$.

Vi vil bruge betegnelsen $D(\alpha)\colon \mathbb{R}^2 \to \mathbb{R}^2$ for drejningen mod uret med vinkel α omkring $(0,0)$. Vi vil bruge betegnelsen $S(\beta)\colon \mathbb{R}^2 \to \mathbb{R}^2$ for spejlingen i den rette linje gennem $(0,0)$ der danner vinklen (!) $\frac{\beta}{2}$ med x-aksen.

I polære koordinater er funktionerne $D(\alpha)$ og $S(\beta)$ givet ved

$$D(\alpha)(r\cos\phi, r\sin\phi) = (r\cos(\phi+\alpha), r\sin(\phi+\alpha))$$
$$S(\beta)(r\cos\phi, r\sin\phi) = (r\cos(\beta-\phi), r\sin(\beta-\phi)).$$

For alle $\alpha \in \mathbb{R}$ og $\beta \in \mathbb{R}$, er

$$D(\alpha + 2\pi) = D(\alpha), \quad S(\beta + 2\pi) = S(\beta).$$

$D(0)$ er identiteten, ofte betegnet med E, af $\mathbb{R}^2$.

Ud fra disse to eksplicitte udtryk for drejningen $D(\alpha)$ og spejlingen $S(\beta)$ er det meget nemt at finde ud af deres opførsel under sammensætning.

SÆTNING 2.1. *Der gælder*

$$\begin{aligned} D(\alpha) \circ D(\beta) &= D(\alpha + \beta) \\ S(\alpha) \circ S(\beta) &= D(\alpha - \beta) \\ D(\alpha) \circ S(\beta) &= S(\alpha + \beta) \\ S(\alpha) \circ D(\beta) &= S(\alpha - \beta) \end{aligned}$$

Heraf følger at både $D(\alpha)$ og $S(\beta)$ er bijektioner med inverse

$$D(\alpha)^{-1} = D(-\alpha), \quad S(\beta)^{-1} = S(\beta).$$

Bemærk specielt at en spejling er sin egen inverse, $S(\beta) \circ S(\beta) = E$.

3. Kvadratets symmetrigruppe

Lad K være kvadratet i planen med hjørner $(\pm 1, \pm 1)$. Vi skal undersøge mængden D_4 af symmetrier af K, dvs. mængden af de transformationer $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ som opfylder $f(K) = K$. (D_4 er mængden af symmetrier af en 4-kant.)

Symmetrierne af K er identitetsafbildningen, drejninger med vinkel $\frac{\pi}{2}$, π og $\frac{3\pi}{2}$ samt spejlingerne i koordinatakserne og de to diagonaler. Dvs.

$$D_4 = \{e, d_1, d_2, d_3, s_1, s_2, s_3, s_4\}$$

hvor

$$\begin{aligned} &e = E, \\ &d_1 = D(\frac{\pi}{2}), d_2 = D(\pi), d_3 = D(\frac{3\pi}{2}), \\ &s_1 = S(0), s_2 = S(\frac{\pi}{2}), s_3 = S(\pi), s_4 = S(\frac{3\pi}{2}). \end{aligned}$$

Dette er imidlertid ikke hele historien. For sammensætningen af to symmetrier er igen en symmetri. Vi siger, at mængden D_4 er *lukket* under sammensætning. F.eks. er

$$\begin{aligned} d_1 \circ d_1 &= d_2 \\ d_1 \circ s_1 &= D(\frac{\pi}{2}) \circ S(0) = S(\frac{\pi}{2}) = s_2 \end{aligned}$$

ifølge Sætning 2.1.

Vi kan sætte beregningen af alle sammensætninger af to symmetrier op i en tabel, en såkaldt Cayley tabel:

D_4	e	d_1	d_2	d_3	s_1	s_2	s_3	s_4
e	e	d_1	d_2	d_3	s_1	s_2	s_3	s_4
d_1	d_1	d_2	d_3	e	s_2	s_3	s_4	s_1
d_2	d_2	d_3	e	d_1	s_3	s_4	s_1	s_2
d_3	d_3	e	d_1	d_2	s_4	s_1	s_2	s_3
s_1	s_1	s_4	s_3	s_2	e	d_3	d_2	d_1
s_2	s_2	s_1	s_4	s_3	d_1	e	d_3	d_2
s_3	s_3	s_2	s_1	s_4	d_2	d_1	e	d_3
s_4	s_4	s_3	s_2	s_1	d_3	d_2	d_1	e

hvor sammensætningen $f \circ g$ er skrevet ind i krydset mellem f-rækken og g-søjlen.

Ved hjælp af Cayley tabellen er det let at beregne sammensætninger af kvadratets symmetrier. Bemærk specielt, at $d_1^2 = d_2$, $d_1^3 = d_1 d_1^2 = d_1 d_2 = d_3$, og

$$s_1^2 = s_1 \circ s_1 = e$$
$$d_1^4 = d_1 \circ d_1^3 = d_1 \circ d_3 = e$$
$$s_1 \circ d_1 \circ s_1 = s_4 \circ s_1 = d_3 = d_1^3.$$

Mere generelt bemærker vi

1. For alle $f, g, h \in D_4$ gælder $f \circ (g \circ h) = (f \circ g) \circ h$.
2. For alle $f \in D_4$ gælder $f \circ e = f = e \circ f$.
3. For ethvert $f \in D_4$ findes et $g \in D_4$ så $f \circ g = e = g \circ f$.

Den første påstand, som involverer 8^3 tilfælde, er måske lidt omstændelig at verificere ud fra Cayley tabellen; det er nemmere at benytte Sætning 1.2. De to andre egenskaber ved D_4 ses umiddelbart ud fra Cayley tabellen.

Det er disse egenskaber der gør D_4 til en *gruppe*.

4. Grupper

Gruppebegrebet er en formalisering af de egenskaber ved D_4 som vi observerede i forrige afsnit.

DEFINITION 4.1. *En* gruppe *er en mængde sammen med en afbildning*

$$G \times G \to G$$
$$(f, g) \to f \bullet g$$

som opfylder de tre betingelser:

1. *(Associativitet) For alle $f, g, h \in G$ gælder $f \bullet (g \bullet h) = (f \bullet g) \bullet h$.*
2. *(Neutralt Element) Der findes et element $e \in G$, så $f \bullet e = f = e \bullet f$ for alle $f \in G$.*
3. *(Inverst element) For ethvert element $f \in G$ findes et element $g \in G$, så $f \bullet g = e = g \bullet f$.*

Et element e der opfylder (2) kaldes et *neutralelement*; et element g der opfylder (3) siges at være et *inverst element* til f. (Lige om lidt viser vi, at der kun findes et neutralelement og kun et inverst element.)

Gruppen $(G, \bullet)$ består således af både mængde G og af *kompositionsreglen* eller *gruppemultiplikation* $\bullet\colon G \times G \to G$ som er en forskrift der fortæller hvordan elementet $f \bullet g$ dannes ud fra f og g. For øvrigt udelades symbolet for kompositionsreglen ofte, og man skriver bare fg for $f \bullet g$.

EKSEMPEL 4.2. $(D_4, \circ)$ er en gruppe, kompositionsreglen er sammensætning. Mængden af alle transformationer af planen er en gruppe, $\mathrm{O}(2)$, med sammensætning som gruppemultiplikation. $(\mathbb{Z}, +)$ er en gruppe, kompositionsreglen er addition. $(\mathbb{N}, +)$ er *ikke* en gruppe, der mangler et neutralt element. $(\mathbb{N}_0, +)$ er heller ikke en gruppe, der mangler inverse elementer. Den *trivielle gruppe* $\{e\}$ indeholder et enkelt (neutral)element.

Her er nogle umiddelbare konsekvenser af definitionen (4.1) af en gruppe.

PROPOSITION 4.3. *Neutralelementet er entydigt bestemt.*

BEVIS. Lad e_1 og e_2 være neutralelementer. Da er

$$e_1 = e_1 \bullet e_2 = e_2$$

hvor det venstre lighedstegn skyldes at e_2 er et neutralelement, og det højre at e_1 er et neutralelement. □

PROPOSITION 4.4. *Inverse elementer er entydige.*

BEVIS. Lad g_1 og g_2 være inverse til f. Da er

$$g_1 = g_1 \bullet e = g_1 \bullet (f \bullet g_2) = (g_1 \bullet f) \bullet g_2 = e \bullet g_2 = g_2$$

hvor vi benytter alle tre egenskaber fra Definition 4.1. □

Det inverse element til f, som altså er entydigt bestemt af f, betegnes f^{-1}.

EKSEMPEL 4.5. Mængden af alle bijektioner $f\colon A \to A$ med sammensætning som komposition er en gruppe. Kompositionsreglen er associativ fordi (1.2) sammensætning af funktioner er associativ. Neutralelementet er identitetsafbildningen 1_A og den inverse til gruppeelementet f er den inverse funktion f^{-1}.

PROPOSITION 4.6. *(Forkortning) Hvis $g \bullet x = g \bullet y$ eller $x \bullet g = y \bullet g$, da er $x = y$.*

BEVIS. Multiplicer fra venstre eller højre med g^{-1}. □

For $n \in \mathbb{N}$ sætter vi

$$f^n = \underbrace{f \bullet f \cdots \bullet f}_{n \text{ faktorer}}, \quad f^{-n} = (f^{-1})^n = \underbrace{f^{-1} \bullet f^{-1} \cdots \bullet f^{-1}}_{n \text{ faktorer}}$$

og vi sætter $f^0 = e$ til at være neutralelementet. Så gælder de sædvanlige regler for potensregning.

PROPOSITION 4.7. *Lad f og g være elementer i gruppen $(G, \bullet)$. Så gælder:*

1. $(fg)^{-1} = g^{-1}f^{-1}$
2. $(f^{-1})^{-1} = f$
3. $f^m f^n = f^{m+n}$ *for alle hele tal* $m, n \in \mathbb{Z}$
4. $(f^m)^n = f^{mn}$ *for alle hele tal* $m, n \in \mathbb{Z}$
5. $(f^n)^{-1} = f^{-n}$ *for alle hele tal* $n \in \mathbb{Z}$

EKSEMPEL 4.8. I symmetrigruppen D_4 er $d_1^{-1} = d_1^{-1}e = d_1^{-1}d_1^4 = d_1^3 = d_3$ og $(d_1s_2)^{-2} = ((d_1s_2)^{-1})^2 = (s_2^{-1}d_1^{-1})^2 = (s_2d_3)^2 = s_3^2 = e$.

Gruppens *orden*, $|G|$, er antallet af elementer i G. En *endelig gruppe* er en gruppe med en endelig orden. D_4 er en endelig gruppe af orden $|D_4| = 8$. De hele tals gruppe er uendelig.

I almindelighed er $f \bullet g \neq g \bullet f$. I D_4 f.eks. er $d_1 \circ s_1 = s_2$ mens $s_1 \circ d_1 = s_4$. I gruppen $(\mathbb{Z}, +)$ derimod gælder at $m + n = n + m$ for alle $m, n \in \mathbb{Z}$. De hele tal er et eksempel på en *kommutativ* eller *abelsk* gruppe.

DEFINITION 4.9. *En* abelsk *gruppe er en gruppe $(G, \bullet)$ som opfylder at*

$$f \bullet g = g \bullet f$$

for alle elementer $f \in G$ og $g \in G$.

I den abelske gruppe $(\mathbb{Z}, +)$ er $2^{-1} = -2$. Det ser jo lidt mærkværdigt ud. Det er da også sædvane at betegne kompositionsreglen i en abelsk gruppe med $+$, neutralelementet med 0 og det inverse, eller *modsatte*, element til f med $-f$. Potensen f^n defineret ved $f^n = f + \cdots + f$ betegnes nf og $f^{-n} = (-f) + \cdots + (-f)$ betegnes $(-n)f$ for $n \in \mathbb{N}$. Med disse notationskonventioner får regnereglerne fra Proposition 4.7 udseendet:

1. $-(f + g) = (-f) + (-g)$
2. $-(-f) = f$
3. $mf + nf = (m + n)f$
4. $n(mf) = (nm)f$
5. $-(nf) = (-n)f$

for alle gruppeelementer $f, g \in G$ og for alle hele tal $m, n \in \mathbb{Z}$.

ØVELSE 4.10. (=Opgave 41) Lad $(G, \bullet)$ og $(H, *)$ være grupper. Vis, at produktet $G \times H$ på naturlig måde er en gruppe. (Husk at verificere betingelserne fra Definition 4.1!) Hvad er ordenen af produktgruppen hvis begge grupper er endelige? Vis, at produktgruppen er abelsk hvis (og kun hvis?) G og H er abelske.

5. Undergrupper og gruppehomomorfier

Hvis du kigger på det øverste venstre hjørne af Cayley tabellen for symmetrigruppen D_4 vil du lægge mærke til at delmængden bestående af de 4 elementer

$\{e, d_1, d_2, d_3\}$ danner en mindre gruppe inden i D_4. Dette er et eksempel på en undergruppe.

DEFINITION 5.1. *Lad $(G, \bullet)$ være en gruppe. En* undergruppe *af G er en delmængde $H \subseteq G$ så*

1. $e \in H$
2. $f \bullet g \in H$ *for alle* $f \in H$ *og* $g \in H$
3. $f^{-1} \in H$ *for alle* $f \in H$.

Betingelse (2) udtrykker at H er lukket under gruppemultiplikationen, og betingelse (3) at H er lukket under dannelse af inverse elementer.

Bemærk, at hvis H er en undergruppe af G, da er H med den arvede gruppemultiplikation igen en gruppe:

PROPOSITION 5.2. *Enhver undergruppe $H \subseteq G$ er en gruppe.*

EKSEMPEL 5.3. G har altid de to undergrupper G og $\{e\}$. $3\mathbb{Z}$, og mere generelt $n\mathbb{Z}$, er en undergruppe i $\mathbb{Z}$. Symmetrigruppen D_4 indeholder en undergruppe $\{e, d_1, d_2, d_3\}$ af orden 4, som igen indeholder undergruppen $\{e, d_2\}$ af orden 2. D_4 er selv en undergruppe af gruppen $\mathrm{O}(2)$ af alle transformationer af planen. Og $\mathrm{O}(2)$ er en undergruppe af alle bijektioner $\mathbb{R}^2 \to \mathbb{R}^2$.

ØVELSE 5.4. Det er klart, at a-tabellen $a\mathbb{Z}$, for ethvert helt tal $a \in \mathbb{Z}$, er en undergruppe af $\mathbb{Z}$. Vi vil vise, at der ikke er andre.

Lad H være en undergruppe af $\mathbb{Z}$. Hvis $H = \{0\}$ er triviel, er vi hjemme, da $\{0\} = 0\mathbb{Z}$. Antag derfor, at H ikke er triviel. Vis, at da er $H \cap \mathbb{N} \neq \emptyset$ og at tallet $a = \min(H \cap \mathbb{N})$ derfor er defineret. Overbevis nu dig selv, og hvem der ellers befinder sig indenfor hørevidde, om at $a > 0$, $a \in H$ og $a\mathbb{Z} \subseteq H$. For at vise den anden inklusion, $H \subseteq a\mathbb{Z}$, vælg et vilkårligt element $n \in H$ og skriv n på formen $n = aq + r$ hvor $0 \leq r < a$ (Divisionsalgoritmen!). Argumenter for, at $r = 0$ er den eneste mulighed, og slut at $n \in a\mathbb{Z}$.

Undergrupper kan f.eks. opstå som billeder af såkaldte gruppehomomorfier.

DEFINITION 5.5. *Lad $(G, \bullet)$ og $(H, *)$ være grupper. En (gruppe)homomorfi er en afbildning $\phi\colon G \to H$ som opfylder*

$$\phi(g_1 \bullet g_2) = \phi(g_1) * \phi(g_2)$$

for alle $g_1 \in G$ og $g_2 \in G$.

En *epimorfi* er en surjektiv homomorfi, en *monomorfi* er en injektiv homomorfi, en *isomorfi* er en bijektiv homomorfi. En *endomorfi* er en homomorfi af en gruppe ind i sig selv, en *automorfi* er en bijektiv endomorfi.

EKSEMPEL 5.6. Lad g være et element i en gruppe G og lad $\phi_g\colon \mathbb{Z} \to G$ være afbildningen givet ved $\phi_g(n) = g^n$, $n \in \mathbb{Z}$. Da (se (4.7))

$$\phi_g(n + m) = g^{n+m} = g^n g^m = \phi_g(n)\phi_g(m)$$

er $\phi_g\colon \mathbb{Z} \to G$ en homomorfi.

ØVELSE 5.7. Find to forskellige gruppehomomorfier $\phi\colon \mathbb{Z} \to \mathbb{Z}$, med billede $\phi(\mathbb{Z}) = n\mathbb{Z}$ lig med n-tabellen. Find en automorfi af $\mathbb{Z}$ som sender den ene homomorfi over i den anden. Hvor mange automorfier af $\mathbb{Z}$ findes der?

PROPOSITION 5.8. *Identitetsafbildningen er en homomorfi. Sammensætningen af to homomorfier er en homomorfi. Den inverse afbildning til en isomorfi er en isomorfi.*

BEVIS. Prøv selv!. □

Vi siger, at grupperne G og H er isomorfe, $G \cong H$, hvis der findes en gruppeisomorfi mellem dem. Isomorfe (endelige) grupper har samme orden. (Men er to grupper af samme orden isomorfe?)

ØVELSE 5.9. Find isomorfier mellem gruppen $(\mathbb{R}_+, \cdot)$ af positive, reelle tal med multiplikation og gruppen $(\mathbb{R}, +)$ af reelle tal med addition.

PROPOSITION 5.10. *Enhver gruppehomomorfi afbilder neutralelement i neutralelement og inverst element i inverst element.*

BEVIS. Vi har

$$\phi(e) = \phi(ee) = \phi(e)\phi(e)$$

og multiplicerer vi denne ligning på begge sider med $\phi(e)^{-1}$, får vi, at $\phi(e)$ er neutralelementet i H. Multiplicerer vi nu begge sider af ligningen

$$\phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

med $\phi(g)^{-1}$ fra venstre følger det, da jo $\phi(e)$ er neutralelement i H, at $\phi(g)^{-1} = \phi(g^{-1})$. □

EKSEMPEL 5.11. Lad S_4 være gruppen af alle bijektive afbildninger af $\{1, 2, 3, 4\}$ ind i sig selv. S_4 er med andre ord gruppen af alle permutationer af tallene 1,2,3,4. Ordenen er $|S_4| = 4! = 24$.

Nummerer hjørnerne i kvadratet med tallene 1,2,3 og 4. Da enhver af kvadratets symmetrier permuterer hjørnerne, vil enhver symmetri bestemme en permutation af $\{1, 2, 3, 4\}$. Til enhver symmetri har vi altså knyttet en permutation, dvs. vi har en afbildning af D_4 ind i S_4. Denne afbildning $\phi\colon D_4 \to S_4$ er en gruppehomomorfi. F.eks. er (hvis du ellers har nummereret kvadratets hjørner som jeg har)

$$\phi(d_1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\phi(s_1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

og

$$\phi(d_1 s_1) = \phi(s_2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \phi(d_1)\phi(s_1)$$

hvilket viser, at ϕ opfylder kravet til en homomorfi i hvert fald for produktet $d_1 s_1$.

DEFINITION 5.12. *Kernen for homomorfien $\phi\colon G \to H$ er originalmængden til neutralelementet, dvs.*

$$\ker \phi = \phi^{-1}(e) = \{g \in G \mid \phi(g) = e\}$$

Vi viser nu, at både kernen og billedet, $\operatorname{im} \phi = \phi(G)$, for en homomorfi er undergrupper.

PROPOSITION 5.13. *Kernen for homomorfien $\phi\colon G \to H$ er en undergruppe i G og billedet er en undergruppe i H.*

BEVIS. Lad $\phi\colon G \to H$ være en homomorfi. Vi skal nøjes med at vise, at kernen $\ker \phi$ er en undergruppe i G. Da ϕ sender neutralelement i neutralelement, er $e \in K$. Hvis g_1 og g_2 ligger i kernen, vil også produktet $g_1 g_2$ ligge i kernen, for $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = ee = e$. Hvis g ligger i kernen, vil også dets inverse ligge i kernen for $\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e$. □

Faktisk er billedet af enhver undergruppe af G og originalmængden af enhver undergruppe af H igen en gruppe.

BEMÆRKNING 5.14. Der gælder

$$\phi(K) = \{e\} \Leftrightarrow K \subseteq \ker \phi$$

for enhver delmængde (specielt undergruppe) $K \subseteq G$.

Kernen afgør om en homomorfi er injektiv.

SÆTNING 5.15. *Lad $\phi\colon G \to H$ være en homomorfi. Da gælder:*

$$\ker \phi = \{e\} \Leftrightarrow \phi \text{ er en monomorfi.}$$

BEVIS. Det er klart, at hvis ϕ er injektiv, så er kernen triviel. Antag omvendt at kernen er triviel. Lad g_1 og g_2 være to elementer af G med samme billede, $\phi(g_1) = \phi(g_2)$. Da $\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = e$, ligger $g_1 g_2^{-1}$ i kernen og er derfor lig med neutalelementet, dvs. $g_1 = g_2$. □

EKSEMPEL 5.16. Kernen for homomorfien $\phi\colon D_4 \to S_4$ fra Eksempel 5.11 består af de symmetrier der fixer alle kvadratets hjørner. Men det gør kun identiteten og derfor er $\ker \phi = \{e\}$ den trivielle gruppe og ϕ er en monomorfi. Dette viser (Opgave 34), at permutationsgruppen S_4 indeholder en undergruppe isomorf med kvadratets symmetrigruppe D_4.

BEMÆRKNING 5.17. Lad G og H være endelige grupper af *samme orden* (f.eks. $G = H$) og $\phi\colon G \to H$ en homomorfi mellem dem. Da gælder:

$$\begin{aligned} &\phi \text{ er en isomorfi} \\ \Leftrightarrow &\phi \text{ er en epimorfi} \\ \Leftrightarrow &\phi \text{ er en monomorfi} \\ \Leftrightarrow &\ker \phi = \{e\}. \end{aligned}$$

Dette følger ved at kombinere Sætning 5.15 med Skuffeprincippet 1.6.

Vi viser nu, at ordenen af en undergruppe (og ordenen af et element) i en endelig gruppe er divisor i hele gruppens orden.

SÆTNING 5.18 (Lagranges Sætning). *Ordenen af en undergruppe af en endelig gruppe går op i gruppens orden.*

BEVIS. Lad G være en endelig gruppe og H en undergruppe af G. Vi ønsker at vise at $|H|$ går op i $|G|$.

For $g \in G$, lad $gH = \{gh \mid h \in H\}$ være mængden af alle produkter af g med et element fra undergruppen H. Læg mærke til, at hvis to af disse mængder skærer hinanden, da er de identiske:

$$g_1H \cap g_2H \neq \emptyset \Leftrightarrow g_1H = g_2H, \quad g_1, g_2 \in G.$$

Denne egenskab medfører, at der findes $g_1, \ldots, g_r \in G$ så

$$G = g_1H \cup \cdots \cup g_rH \tag{5.19}$$

er en opsplitning af G i disjunkte delmængder.

Vælg nemlig først et element $g_1 \in G$. Hvis $g_1H = G$, er vi færdige. Hvis ikke, vælg $g_2 \in G \setminus g_1H$. Da er $g_1H \cup g_2H$ en disjunkt foreningsmængde. Hvis $g_1H \cup g_2H = G$, er vi færdige. Hvis ikke, vælg $g_3 \in G \setminus (g_1H \cup g_2H)$. Denne proces må stoppe efter et endeligt antal skridt, da G er endelig.

Bemærk nu at mængden g_iH indeholder præcis lige så mange elementer som H. For der findes nemlig en bijektion $H \to g_iH$ givet ved $h \to g_ih$ (hvad er den inverse?). Den disjunkte opsplitning (5.19) viser derfor, at $|G| = r|H|$. □

Vi skal til sidst se en anvendelse af Lagranges sætning på elementorden.

DEFINITION 5.20. *Lad $g \in G$ være et element i gruppen G. Vi siger, at g har endelig orden, hvis der findes et naturligt tal n, så $g^n = e$. Det mindste naturlige tal med denne egenskab kaldes for ordenen af g, og det betegnes med* $\operatorname{ord}_G g$. *Hvis g ikke har endelig orden, siges g at have uendelig orden.*

Det eneste element med orden 1 er neutralelementet. I symmetrigruppen D_4 er $\operatorname{ord}_{D_4} s_1 = 2$ og $\operatorname{ord}_{D_4} d_1 = 4$.

ØVELSE 5.21. For ethvert element g af endelig orden gælder

- $g^{\operatorname{ord}_G g} = e$.

- For ethvert helt tal m er $g^m = g^r$, hvor r er resten ved division af m med $\operatorname{ord}_G g$.

EKSEMPEL 5.22. Kernen for homomorfien $\phi_g \colon \mathbb{Z} \to G$ fra Eksempel 5.6 er undergruppen

$$\ker \phi_g = \{n \in \mathbb{Z} \mid g^n = e\}$$

af $\mathbb{Z}$ og billedet er undergruppen

$$\operatorname{im} \phi_g = \{g^n \mid n \in \mathbb{Z}\}$$

frembragt af g (som ofte betegnes med $\langle g \rangle$). Bemærk, at

$$\phi_g \text{ er ikke-injektiv} \Leftrightarrow g \text{ har endelig orden}$$

og at hvis g har endelig orden n, da frembringer g en undergruppe

$$\operatorname{im} \phi_g = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

af orden n. Vi kan altså sige, at

$$\operatorname{ord}_G g = \min\{n \in \mathbb{N} \mid g^n = e\} = |\langle g \rangle| \quad \text{og} \quad \ker \phi_g = (\operatorname{ord}_G g)\mathbb{Z}$$

når g har endelig orden.

SÆTNING 5.23. *Lad G være en endelig gruppe og g et element i G. Da gælder*

1. *g har endelig orden.*
2. *$\operatorname{ord}_G g$ går op i $|G|$.*
3. *$g^{|G|} = e$.*

BEVIS. Dette følger umiddelbart af det foregående fordi

1. Homomorfien $\phi_g \colon \mathbb{Z} \to G$ kan ikke være injektiv, da G er en endelig gruppe.
2. $\operatorname{ord}_G g$, som er lig med ordenen af undergruppen $\langle g \rangle$ frembragt af g, går op i gruppens orden ifølge Lagranges Sætning.
3. $g^{|G|} = g^0 = e$, da resten ved division af $|G|$ med $\operatorname{ord}_G g$ er 0.

□

ØVELSE 5.24. Vis, at $\operatorname{ord}_{G \times H}(g, h) = \operatorname{mfm}(\operatorname{ord}_G g, \operatorname{ord}_H h)$, hvis gruppeelementerne $g \in G$ og $h \in H$ begge har endelig orden. Find f.eks. $\ker \phi_{(g,h)}$ og benyt Eksempel 5.22

6. Modulær aritmetik

Lad $n \geq 1$ være et naturligt tal. Vi siger, at de to hele tal x og y er *kongruente modulo n*, $x \equiv y \bmod n$, hvis n går op i differensen $x - y$. Det kan udtrykkes på flere ækvivalente måder: De syv påstande

- $x \equiv y \bmod n$
- $n | x - y$
- $n | y - x$
- der findes et helt tal $s \in \mathbb{Z}$ så $y = x + ns$
- der findes et helt tal $t \in \mathbb{Z}$ så $x = y + nt$

- x og y har samme rest ved division med n
- $x + n\mathbb{Z} = y + n\mathbb{Z}$

er alle ensbetydende.

Mængden $x + n\mathbb{Z}$, n-tabellen afsat ud fra x, består af alle hele tal, der har samme rest ved division med n som x har. Den kaldes for *restklassen af x modulo n* og betegnes også med $\underline{x}_n$ eller blot $\underline{x}$; dvs.

$$\begin{aligned}\underline{x}_n &= x + n\mathbb{Z} \\ &= \{y \mid \text{der findes et } s \in \mathbb{Z} \text{ så } y = x + ns\} \\ &= \{\ldots, x - 2n, x - n, x, x + n, x + 2n, \ldots\}\end{aligned}$$

Relationen $x \equiv y \bmod n$ har en hel del til fælles med lighedstegnet:

PROPOSITION 6.1. *Lad x, y og z være hele tal. Da gælder:*

1. $x \equiv x \bmod n$
2. $x \equiv y \bmod n \Rightarrow y \equiv x \bmod n$
3. *Hvis* $x \equiv y \bmod n$ *og* $y \equiv z \bmod n$, *da er* $x \equiv z \bmod n$

Vi udtrykker indholdet af Proposition 6.1 ved at sige, at $x \equiv y \bmod n$ er en *ækvivalensrelation*.

ØVELSE 6.2. Vis, at

$$x \equiv y \bmod n \Leftrightarrow \frac{x}{d} \equiv \frac{y}{d} \bmod \frac{n}{d}$$

hvis d går op i alle de tre tal x, y og n. (Eller regn den mere generelle Opgave 61.)

Da restklassen $\underline{0}_n$ består af alle tal, der får resten 0 ved division med n, restklassen $\underline{1}_n$ består af alle tal, der får resten 1 ved division med n, osv., indtil restklassen $\underline{n-1}_n$, som består af alle tal, der får resten $n - 1$ ved division med n, ser vi, at de hele tal

$$\mathbb{Z} = \underline{0} \cup \underline{1} \cup \cdots \cup \underline{n-1} = (0 + n\mathbb{Z}) \cup (1 + n\mathbb{Z}) \cup \cdots \cup ((n-1) + n\mathbb{Z})$$

kan skrives som den disjunkte foreningsmængde af de n restklasser modulo n. Vi har altså n restklasser modulo n, og vi skriver,

$$\mathbb{Z}/n = \{\underline{0}, \underline{1}, \ldots, \underline{n-1}\}$$

for mængden af de n restklasser. (Ja, du så rigtigt: $\mathbb{Z}/n$ er en mængde af mængder.) Bemærk, at $\underline{n} = \underline{0}$, $\underline{n+1} = \underline{1}$, ja, at

$$\underline{x} = \underline{y} \Leftrightarrow x \equiv y \bmod n$$

for alle hele tal $x, y \in \mathbb{Z}$.

EKSEMPEL 6.3. Der er 12 restklasser modulo 12. Vi har $\underline{13} = \underline{1}$, $\underline{14} = \underline{2}, \ldots, \underline{23} = \underline{11}, \underline{24} = \underline{0}$.

Vi ønsker at definere addition og multiplikation af restklasser modulo n. Det er fristende at sætte

$$\underline{x} + \underline{y} = \underline{x + y}$$

og

$$\underline{x} \cdot \underline{y} = \underline{xy}$$

men der er et problem her fordi restklasserne har mange forskellige repræsentanter. (Tænk lige over det!) Problemet forsvinder imidlertid, så snart vi har vist:

LEMMA 6.4. *Antag at* $x_1 \equiv x_2 \bmod n$ *og* $y_1 \equiv y_2 \bmod n$. *Da er*

1. $x_1 + y_1 \equiv x_2 + y_2 \bmod n$
2. $x_1 y_1 \equiv x_2 y_2 \bmod n$

BEVIS. Da n går op i $x_2 - x_1$ og i $y_2 - y_1$ vil n også gå op i

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2)$$

og i

$$x_1 y_1 - x_2 y_2 = x_1 y_1 - x_1 y_2 + x_1 y_2 - x_2 y_2 = x_1(y_1 - y_2) + (x_1 - x_2) y_2.$$

Dette viser de to påstande. □

Det er nu ganske let at verificere de sædvanlige regneregler

$$\begin{aligned}
&\underline{x} + \underline{y} = \underline{y} + \underline{x} \\
&(\underline{x} + \underline{y}) + \underline{z} = \underline{x} + (\underline{y} + \underline{z}) \\
&\underline{0} + \underline{x} = \underline{x} \\
&\underline{x} + \underline{-x} = \underline{0} \\
&\underline{x} \cdot \underline{y} = \underline{y} \cdot \underline{x} \\
&(\underline{x} \cdot \underline{y}) \cdot \underline{z} = \underline{x} \cdot (\underline{y} \cdot \underline{z}) \\
&\underline{1} \cdot \underline{x} = \underline{x} \\
&\underline{x} \cdot (\underline{y} + \underline{z}) = \underline{x} \cdot \underline{y} + \underline{x} \cdot \underline{z}
\end{aligned}$$

(Disse regneregler gør mængden af restklasser mod$n$ til en *ring*.) Idet vi nu bare fokuserer på additionen og ignorerer multiplikationen, får vi umiddelbart:

SÆTNING 6.5. $(\mathbb{Z}/n, +)$ *er en abelsk gruppe,* den abelske gruppe af restklasser modulo n, *af orden* n *med neutralelement* $\underline{0}$ *og invers* $-\underline{x} = \underline{-x}$.

Vi kan nu tillade os at bruge de regneregler vi fandt i forrige afsnit (4.6, 4.7) i gruppen $(\mathbb{Z}/n, +)$.

EKSEMPEL 6.6. Cayley tabellen for den abelske gruppe $(\mathbb{Z}/6, +)$ af retsklasser modulo 6

$(\mathbb{Z}/6,+)$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

viser, at $\mathbb{Z}/6$ indeholder undergrupperne $\{0, 3\} \cong \mathbb{Z}/2$ og $\{0, 2, 4\} \cong \mathbb{Z}/3$.

BEMÆRKNING 6.7. Her er nogle småbemærkninger:

- Afbildningen $R_n \colon \mathbb{Z} \to \mathbb{Z}/n$, som sender $x \in \mathbb{Z}$ i $R_n(x) = \underline{x} \in \mathbb{Z}/n$, er en epimorfi med kerne $n\mathbb{Z}$.
- Faktisk er R_n blot et nyt navn for $\phi_{\underline{1}}$, så det følger, at $\operatorname{ord}_{\mathbb{Z}/n}\underline{1} = n$, dvs. at $\mathbb{Z}/n = \langle \underline{1} \rangle$ er frembragt af elementet $\underline{1} \in \mathbb{Z}/n$.
- Lad $g \in G$ være et gruppeelement af endelig orden. Afbildningen $\mathbb{Z}/(\operatorname{ord}_G g) \to \langle g \rangle$ som sender $\underline{x}$ i g^x er en (veldefineret!) isomorfi.

Vi betragter nu den multiplikative struktur på $\mathbb{Z}/n$.

ØVELSE 6.8. Betragt ligningen $\underline{4} \cdot \underline{x} = \underline{6}$ i mængden af restklasser modulo n. Vis, at

1. Hvis $n = 8$, er der ingen løsninger.
2. Hvis $n = 10$, er der netop to løsninger.
3. Hvis $n = 15$, er der netop en løsning.

Mutliplikationen i $\mathbb{Z}/n$ er godt nok associativ, og $\underline{1}$ er et neutralelement, men ikke alle elementer har inverse. F.eks. har $\underline{0}$ aldrig nogen invers, og $\underline{2}$ har ikke noget inverst element i $\mathbb{Z}/6$. Så $(\mathbb{Z}/n, \cdot)$ er *ikke* en gruppe. Men indskrænker vi til mængden $(\mathbb{Z}/n)^*$ af multiplikativt invertible elementer (idet vi bemærker, at produktet af to invertible elementer er invertibelt) ja, da får vi faktisk en gruppe. Gruppen af multiplikativt invertible restklasser modulo n betegnes $((\mathbb{Z}/n)^*, \cdot)$.

EKSEMPEL 6.9. Cayley tabellen for $((\mathbb{Z}/4), \cdot)$

$(\mathbb{Z}/4,\cdot)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

viser, at $(\mathbb{Z}/4)^* = \{\underline{1}, \underline{3}\} \cong \mathbb{Z}/2$.

Vi bestemmer nu elementerne i gruppen $(\mathbb{Z}/n)^*$. Bemærk først, at multiplikation med $m \in \mathbb{Z}$ er en endomorfi af (en vilkårlig abelsk gruppe og specielt af) $\mathbb{Z}/n$: Multiplikation med m sender $\underline{x} \in \mathbb{Z}/n$ i $m\underline{x} = \underline{m} \cdot \underline{x} = \underline{mx}$.

LEMMA 6.10. *Lad m og n være hele tal. Da er følgende betingelser ækvivalente:*

1. *$\underline{m}$ har en multiplikativ invers i $\mathbb{Z}/n$.*
2. *Multiplikation med m, $m\colon \mathbb{Z}/n \to \mathbb{Z}/n$, er en automorfi.*
3. $\mathrm{sfd}(m,n) = 1$.

Hvis en af disse betingelser er opfyldt, og $sm + tn = 1$, så er $\underline{m}^{-1} = \underline{s}$.

BEVIS. Vi viser (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

Antag (1). Vælg $\underline{s}$ så $\underline{m} \cdot \underline{s} = \underline{1}$. Da viser

$$\underline{y} = \underline{1} \cdot \underline{y} = \underline{m} \cdot \underline{s} \cdot \underline{y} = \underline{m} \cdot (\underline{s} \cdot \underline{y}) = \underline{m} \cdot \underline{sy} = m(\underline{sy})$$

at multiplikation med m er en epimorfi, og derfor (5.17) en automorfi.

Antag (2). Da multiplikation med m er en automorfi, findes $s \in \mathbb{Z}$ så $\underline{m} \cdot \underline{s} = \underline{1}$ eller $\underline{1 - ms} = \underline{0}$, dvs, at $1 - ms$ er et multiplum af n, og (I.2.37) at m og n er indbyrdes primiske.

Antag (3). Da $\mathrm{sfd}(m,n) = 1$ findes (I.2.37) hele tal $s, t \in \mathbb{Z}$ med $ms + nt = 1$. Så er $\underline{1} = \underline{ms + nt} = \underline{ms} + \underline{ns} = \underline{ms} = \underline{m} \cdot \underline{s}$, så $\underline{s}$ er en multiplikativ invers til $\underline{m}$. □

EKSEMPEL 6.11. $(\mathbb{Z}/6)^* = \{\underline{1}, \underline{5}\}$ er isomorf med $\mathbb{Z}/2$. $(\mathbb{Z}/5)^* = \{\underline{1}, \underline{2}, \underline{3}, \underline{4}\}$ er isomorf med $\mathbb{Z}/4$: Overvej, at $\phi\colon \mathbb{Z}/4 \to (\mathbb{Z}/5)^*$ givet ved $\phi(\underline{x}) = \underline{2}^x$ er en (veldefineret!) isomorfi. $(\mathbb{Z}/9)^* = \{\underline{1}, \underline{2}, \underline{4}, \underline{5}, \underline{7}, \underline{8}\}$ er en gruppe af orden 6.

DEFINITION 6.12. *Funktionen ϕ givet ved*

$$\phi(n) = |(\mathbb{Z}/n)^*|$$

kaldes for Eulers ϕ-funktion.

Eulers ϕ-funktion er altså givet ved at $\phi(n)$ er antallet af naturlige tal m med $0 < m < n$ som er indbyrdes primiske med n. F. eks. er $\phi(4) = 2\phi(6)$. Specielt er $\phi(p) = p - 1$ for ethvert primtal p. Du kan finde mere om beregningen af Eulers ϕ-funktion i opgaverne.

SÆTNING 6.13 (Eulers Sætning). *Lad n være et naturligt tal og m et helt tal, som er indbyrdes primisk med n. Så er*

$$m^{\phi(n)} \equiv 1 \bmod n$$

BEVIS. Anvend Sætning 5.23 på $\underline{m} \in (\mathbb{Z}/n)^*$. □

KOROLLAR 6.14 (Fermats lille sætning). *Lad p være et primtal og x et helt tal som ikke er divisibelt med p. Da er*

$$x^{p-1} \equiv 1 \bmod p$$

BEVIS. $\phi(p) = p - 1$. □

EKSEMPEL 6.15. $2^{10} \equiv 1 \bmod 11$, $31 \mid 20^{30} - 1$, $378^{1060} - 1$ er deleligt med 1061.

Det næste eksempel handler om løsning af (lineære) ligninger i gruppen $\mathbb{Z}/n$.

EKSEMPEL 6.16. Lad m og n være naturlige tal med største fælles divisor $d = \text{sfd}(m,n)$. Vælg hele tal s og t, så $ms + nt = d$.

Ligningen $mx \equiv a \bmod n$ har en løsning, hvis og kun hvis $a \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, dvs. hvis og kun hvis d går op i a.

Antag derfor, at d går op i a. Så gælder

$$\begin{aligned} mx \equiv a \bmod n &\Leftrightarrow \frac{m}{d}x \equiv \frac{a}{d} \bmod \frac{n}{d} \\ &\Leftrightarrow \frac{sm}{d}x \equiv \frac{sa}{d} \bmod \frac{n}{d} \\ &\Leftrightarrow x \equiv \frac{sa}{d} \bmod \frac{n}{d} \end{aligned}$$

hvor den første biimplikation er Øvelse 6.2, den anden skyldes Lemma 6.10, og den tredje kommer af at $s\frac{m}{d} \equiv 1 \bmod \frac{n}{d}$ (se Lemma 6.10).

ØVELSE 6.17. Brug Eksempel 6.16 og Eksempel 2.30 til at vise at

$$945x \equiv 525 \bmod 2415 \Leftrightarrow x \equiv 21 \bmod 23.$$

ØVELSE 6.18. Lad $m\colon \mathbb{Z}/n \to \mathbb{Z}/n$ være endomorfien af $\mathbb{Z}/n$ givet ved multiplikation med m. Da er

$$\begin{aligned} \text{im}(m) &= \langle \underline{m} \rangle = \{\underline{0}, \underline{d}, 2\underline{d}, \ldots, (\frac{n}{d} - 1)\underline{d}\} \cong \mathbb{Z}/(\frac{n}{d}) \\ \ker(m) &= \{\underline{0}, \underline{\frac{n}{d}}, 2\underline{\frac{n}{d}}, \ldots, (d-1)\underline{\frac{n}{d}}\} = \langle \underline{\frac{n}{d}} \rangle \cong \mathbb{Z}/d \end{aligned}$$

hvor $d = \text{sfd}(m,n)$ er den største fælles divisor af m og n. (Er det et tilfælde at produktet af kernens og billedets orden er lig med domænets orden?) Med andre ord, er $\text{ord}_{\mathbb{Z}/n}\,\underline{m} = |\langle \underline{m} | \rangle = \frac{n}{\text{sfd}(m,n)}$.

7. Den kinesiske restklassesætning

Lad a og b være to naturlige tal. Betragt afbildningen

$$\begin{aligned} f\colon \mathbb{Z}/(ab) &\to \mathbb{Z}/a \times \mathbb{Z}/b \\ \underline{x} &\to (\underline{x}, \underline{x}) \end{aligned}$$

fra $\mathbb{Z}/(ab)$ ind i produktet af $\mathbb{Z}/a$ og $\mathbb{Z}/b$. (Det fremgår ikke eksplicit af notationen, at det første $\underline{x}$ er element i gruppen $\mathbb{Z}/(ab)$, det andet i $\mathbb{Z}/a$ og det tredje i $\mathbb{Z}/b$.) Det fortjener lige en overvejelse at denne afbildning i det hele taget er veldefineret! (Hvad er problemet?) Selvom du selvfølgelig husker det, vil jeg lige minde dig om (Opgave 41), at codomænet er en abelsk gruppe med

$$(\underline{x_1}, \underline{y_1}) + (\underline{x_2}, \underline{y_2}) = (\underline{x_1} + \underline{y_1}, \underline{x_2} + \underline{y_2})$$

som gruppestruktur. Det er nu klart, at f er en homomorfi for

$$\begin{aligned} f(\underline{x}+\underline{y}) &= f(\underline{x+y}) = (\underline{x+y},\underline{x+y}) = (\underline{x}+\underline{y},\underline{x}+\underline{y}) = (\underline{x},\underline{x})+(\underline{y},\underline{y}) \\ &= f(\underline{x})+f(\underline{y}) \end{aligned}$$

for alle $\underline{x},\underline{y} \in \mathbb{Z}/(ab)$.

LEMMA 7.1. *Homomorfien $f\colon \mathbb{Z}/(ab) \to \mathbb{Z}/a \times \mathbb{Z}/b$ er en isomorfi, hvis og kun hvis a og b er indbyrdes primiske. I så fald er den inverse $f^{-1}\colon \mathbb{Z}/a \times \mathbb{Z}/b \to \mathbb{Z}/(ab)$ givet ved*

$$f^{-1}(\underline{x},\underline{y}) = bt\underline{x}+as\underline{y}, \quad (\underline{x},\underline{y}) \in \mathbb{Z}/a \times \mathbb{Z}/b,$$

hvor de hele tal s og t er valgt (I.2.37), så $as+bt=1$.

BEVIS. Kernen for homomorfien f er billedet $R_{ab}(a\mathbb{Z} \cap b\mathbb{Z})$ af undergruppen $a\mathbb{Z} \cap b\mathbb{Z} \subseteq \mathbb{Z}$ ved afbildningen $R_{ab}\colon \mathbb{Z} \to \mathbb{Z}/(ab)\colon x \to \underline{x}$ fra Bemærkning 6.7. Altså gælder:

$$\begin{aligned} f \text{ er en isomorfi} &\Leftrightarrow \ker f = \{\underline{0}\} \\ &\Leftrightarrow R_{ab}(a\mathbb{Z} \cap b\mathbb{Z}) = \{\underline{0}\} \\ &\Leftrightarrow a\mathbb{Z} \cap b\mathbb{Z} \subseteq \ker R_{ab} \\ &\Leftrightarrow a\mathbb{Z} \cap b\mathbb{Z} \subseteq ab\mathbb{Z} \\ &\Leftrightarrow \mathrm{sfd}(a,b) = 1 \end{aligned}$$

hvor vi har benyttet (5.17), (5.14), (6.7) og (I.2.37) (og i øvrigt holdt hovedet koldt).

Vi antager nu, at a og b er indbyrdes primiske hele tal og forsøger at finde den inverse til isomorfien f. Lad $g\colon \mathbb{Z}/a \times \mathbb{Z}/b \to \mathbb{Z}/(ab)$ være funktionen givet ved

$$g(\underline{x},\underline{y}) = bt\underline{x}+as\underline{y}, \quad (\underline{x},\underline{y}) \in \mathbb{Z}/a \times \mathbb{Z}/b,$$

hvor de hele tal s og t er valgt (I.2.37) så $as+bt=1$. Det kræver en lille overvejelse, som jeg trygt overlader til dig, at vise, at g er veldefineret, og at g er en homomorfi. Idet vi benytter bl.a. regel (3) fra Proposition 4.7, får vi for alle $\underline{x} \in \mathbb{Z}/(ab)$,

$$(g \circ f)(\underline{x}) = g(\underline{x},\underline{x}) = bt\underline{x}+as\underline{x} = (bt+as)\underline{x} = \underline{x} \tag{7.2}$$

og for alle $(\underline{x},\underline{y}) \in \mathbb{Z}/a \times \mathbb{Z}/b$,

$$(f \circ g)(\underline{x},\underline{y}) = f(bt\underline{x}+as\underline{y}) = (bt\underline{x},as\underline{y}) = ((1-as)\underline{x},(1-bt)\underline{y}) = (\underline{x},\underline{y}) \tag{7.3}$$

og derfor er f og g hinandens inverse. □

ØVELSE 7.4. Hvorfor kan den ene af udregningerne (7.2) og (7.3) udelades?

ALTERNATIVT BEVIS FOR 7.1. Antag, at a og b er indbyrdes primiske hele tal. Læg mærke til, at billedet $\operatorname{im} f = \operatorname{im} \phi_{(\underline{1},\underline{1})} = \langle(\underline{1},\underline{1})\rangle$ er undergruppen frembragt af $(\underline{1},\underline{1}) \in \mathbb{Z}/a \times \mathbb{Z}/b$, som har orden

$$|\langle(\underline{1},\underline{1})\rangle| = \operatorname{ord}_{\mathbb{Z}/a\times\mathbb{Z}/b}(\underline{1},\underline{1}) = \operatorname{mfm}(\operatorname{ord}_{\mathbb{Z}/a}\underline{1}, \operatorname{ord}_{\mathbb{Z}/b}\underline{1}) = \operatorname{mfm}(a,b) = ab$$

ifølge Øvelse 5.24. Dette viser, at f er en epimorfi og derfor en isomorfi ifølge Skuffeprincippet 1.6. Den inverse f^{-1} findes som i det første bevis.

Antag dernæst, at a og b ikke er indbyrdes primiske. Så er $\underline{\operatorname{mfm}(a,b)}$ et element i $\ker f$ som ikke er lig med neutralelementet $\underline{0}$. Derfor (5.15) er f ikke injektiv, specielt ikke en isomorfi. □

SÆTNING 7.5. *Lad $m_1, m_2, \ldots, m_r$ være parvis indbyrdes primiske naturlige tal. Da er den naturlige homomorfi*

$$f : \mathbb{Z}/(m_1 m_2 \ldots m_r) \to \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \ldots \mathbb{Z}/m_r$$
$$\underline{x} \to (\underline{x}, \ldots, \underline{x})$$

en isomorfi.

BEVIS. Vi benytter induktion efter antallet r af faktorer. Hvis $r = 2$ er vi tilbage i Lemma 7.1. Antag, at sætningen er sand for produkter med $< r$ faktorer. Lad $m = m_1 m_2 \ldots m_r$ være et produkt af r parvis indbyrdes primiske faktorer. Bemærk først, at m_1 og $m_2 \ldots m_r$ er indbyrdes primiske. (Se Opgave 20.) Lemma 7.1 giver nu, at

$$\mathbb{Z}/m \cong \mathbb{Z}/m_1 \times \mathbb{Z}/(m_2 \ldots m_r)$$

hvor

$$\mathbb{Z}/(m_2 \ldots m_r) \cong \mathbb{Z}/m_2 \times \cdots \times \mathbb{Z}/m_r$$

ifølge induktionsantagelsen. □

KOROLLAR 7.6. *(Den Kinesiske Restklassesætning) Lad $m_1, m_2, \ldots, m_r$ være parvis indbyrdes primiske naturlige tal og lad $a_1, a_2, \ldots a_r$ være hele tal. Der findes et helt tal $a \in \mathbb{Z}$ så*

$$a \equiv a_i \mod m_i$$

for alle $i = 1, \ldots, r$.

BEVIS. Vælg a så $\underline{a} \in \mathbb{Z}/(m_1 \ldots m_r)$ afbildes i $(\underline{a_1}, \ldots, \underline{a_r}) \in \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$ ved isomorfien f fra Sætning 7.5. □

BEMÆRKNING 7.7. Den Kinesiske Restklassesætning, eller rettere Sætning 7.5, siger, at løsningen til ligningssystemet (bestående af r ligninger)

$$x \equiv a_i \mod m_i, \quad 1 \leq i \leq r,$$

er

$$x \equiv a \mod m_1 \ldots m_r$$

hvor $f(\underline{a}) = (\underline{a_1}, \ldots, \underline{a_r})$. Der siges intet eksplicit om, hvordan a findes, for f^{-1} er ikke eksplicit angivet. Dog ved vi fra Lemma 7.1 at i tilfældet $r = 2$ er

$$a = m_2 s_2 a_1 + m_1 s_1 a_2$$

hvor s_1 og s_2 er valgt så $m_1 s_1 + m_2 s_2 = 1$. Ved en trinvis procedure kan man derfor faktisk finde a; se Eksempel 7.8.

EKSEMPEL 7.8. Ligningssystemet

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 4 \mod 7 \\ x &\equiv 3 \mod 6 \end{aligned}$$

er, da $1 = (-4)\cdot 5 + 3\cdot 7$ ifølge Euklids algoritme, ækvivalent med ligningssystemet

$$\begin{aligned} x &\equiv 32 \mod 35 \\ x &\equiv 3 \mod 6 \end{aligned}$$

som, da $1 = (-1)\cdot 35 + 6\cdot 6$, er ækvivalent med ligningen

$$x \equiv 207 \mod 210.$$

BEMÆRKNING 7.9. Programmeringssproget PASCAL kan kun behandle latterligt små hele tal. Den Kinesiske Restklassesætning kan anvendes til at udvide det tilladte område, idet man udnytter, at hvis man kan regne modulo $p_1, \ldots, p_r$, da kan man også regne modulo $p_1 \ldots p_r$.

Vi kunne specielt anvende Sætning 7.5 på primfaktoropløsningen (I.3.8) af n og opnå en faktorisering af $\mathbb{Z}/n$.

KOROLLAR 7.10. *Hvis n har primtalsfaktoriseringen*

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

da er homomorfien

$$\begin{aligned} f\colon \mathbb{Z}/n &\to \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r} \\ \underline{x} &\to (\underline{x}, \ldots, \underline{x}) \end{aligned}$$

en isomorfi.

Opgaver

OPGAVE 29. Lad $g \circ f\colon A \to C$ være den sammensatte funktion af $f\colon A \to B$ og $g\colon B \to C$. Vis, at

$$(g \circ f)^{-1}(c) = f^{-1}(g^{-1}(c))$$

for alle $c \in C$. Vis også, at

$$\begin{aligned} g \circ f \text{ er injektiv} &\Rightarrow f \text{ er injektiv} \\ g \circ f \text{ er surjektiv} &\Rightarrow g \text{ er surjektiv} \end{aligned}$$

OPGAVE 30. Vis, at sammensætningen af to surjektive (injektive) afbildninger er surjektiv (injektiv).

OPGAVE 31. Vis, at alle elementer i symmetrigruppen D_4 er frembragt af d_1 og s_1, dvs. at elle elementer kan skrives som produkter af de to elementer d_1 og s_1.

OPGAVE 32. Lad $f\colon D_4 \to D_4$ være afblildningen givet ved $f(x) = x^3$. Vis, at f er bijektiv. Er f en homomorfi?

OPGAVE 33. Definer $c_g\colon G \to G$ ved $c_g(h) = ghg^{-1}$. Er c_g en homomorfi? Er c_g en automorfi? Find $c_g \circ c_h$ og $(c_g)^{-1}$.

OPGAVE 34. Vis, at enhver monomorfi $\phi\colon G \to H$ bestemmer en isomorfi $G \cong \phi(G)$ mellem domænet og billedet.

OPGAVE 35. Lad D_3 betegne symmetrigruppen for en ligesidet trekant centreret i $(0,0)$. Hvad er ordenen af D_3? Opstil Cayley tabellen. Er D_3 abelsk?

OPGAVE 36. Lad D_n betegne symmetrigruppen for en ligesidet n-kant centreret i $(0,0)$. Hvad er ordenen af D_n? Er D_n abelsk?

OPGAVE 37. Lad S_n betegne mængden af alle bijektive afbildninger af $\{1, 2, \ldots, n\}$ ind i sig selv. Vis, at S_n er en gruppe. Find $|S_n|$.

OPGAVE 38. Find Cayley tabellen for symmetrigruppen af et rektangel som ikke er et kvadrat. Hvad er gruppens orden? Er gruppen abelsk? Vis, at denne gruppe er isomorf med et produkt af to af sine undergrupper. (Har vi et generelt fænomen her?)

OPGAVE 39. Hvad er cirklens symmetrigruppe?

OPGAVE 40. Vis, at ligningerne $xg = h$ og $gx = h$ begge har netop en løsning i enhver gruppe.

OPGAVE 41. Lad $(G, \cdot)$ og $(H, *)$ være grupper. Vis, at produktet $G \times H$ på naturlig måde er en gruppe. (Husk at verificere betingelserne fra Definition 4.1!) Hvad er ordenen af produktgruppen hvis begge grupper er endelige? Vis, at produktgruppen er abelsk hvis (og kun hvis?) G og H er abelske.

OPGAVE 42. Vis, at $G_1 \times H_1$ er en undergruppe i $G \times H$ hvis G_1 er en undergruppe i G og H_1 en undergruppe i H. Er alle produktgruppens undergrupper af denne form?

OPGAVE 43. Opstil Cayley tabellen for $\mathbb{Z}/2 \times \mathbb{Z}/2$ og for $\mathbb{Z}/2 \times \mathbb{Z}/3$. Er $\mathbb{Z}/4$ og $\mathbb{Z}/2 \times \mathbb{Z}/2$ isomorfe? Er $\mathbb{Z}/6$ og $\mathbb{Z}/2 \times \mathbb{Z}/3$ isomorfe?

OPGAVE 44. Er $\mathbb{Z}/n^2$ og $\mathbb{Z}/n \times \mathbb{Z}/n$ isomorfe for noget $n > 1$? (Øvelse 6.18 kan måske være til nytte.)

OPGAVE 45. Find en undergruppe isomorf med $\mathbb{Z}/n$ i D_n.

OPGAVE 46. Konstruer en (interessant) gruppehomomorfi $D_n \to S_n$. Er din homomorfi en monomorfi?

OPGAVE 47. Vis at symmetrigruppen D_3 fra Opgave 35 er isomorf med permutationsgruppen S_3.

OPGAVE 48. Vis, at enhver undergruppe af de hele tal $\mathbb{Z}$ har formen $a\mathbb{Z}$ for et $a \in \mathbb{Z}$. (Vink: (I.1.8), (I.2.1))

OPGAVE 49. Vis, at $H \subseteq G$ er en undergruppe af G hvis og kun hvis

1. $H \neq \emptyset$.
2. $fg^{-1} \in H$ for alle $f \in H$ og $g \in H$

OPGAVE 50. Bevis Proposition II.5.8.

OPGAVE 51. Lad $\phi\colon G \to H$ være en homomorfi mellem to endelige grupper. Find en bijektion mellem $\ker \phi = \phi^{-1}(e)$ og originalmængden $\phi^{-1}(\phi(g))$ for $g \in G$, f.eks. ved at vise $\phi^{-1}(\phi(g)) = g \ker \phi$. Konkluder, at $|G| = |\ker \phi||\operatorname{im} \phi|$.

OPGAVE 52. Hvor mange homomorfier $\mathbb{Z}/5 \to \mathbb{Z}/7$ findes der?

OPGAVE 53. Vis, at $\mathbb{Z}/n$ indeholder en undergruppe isomorf med $\mathbb{Z}/m$ hvis og kun hvis m går op i n. Hvis $m \mid n$, hvor mange undergrupper isomorfe med $\mathbb{Z}/m$ har $\mathbb{Z}/n$? (Vink: (5.23), (6.18).)

OPGAVE 54. Vis, at $(\mathbb{Z}/5)^* \cong \mathbb{Z}/4$ og at $(\mathbb{Z}/7)^* \cong \mathbb{Z}/6$. Kan du ane et muligt generelt fænomen her?

OPGAVE 55. Find $\phi(n)$ for for $2 \leq n \leq 20$.

OPGAVE 56. Vis, at $\phi(p^r) = |(\mathbb{Z}/p^r)^*| = p^r - p^{r-1} = p^{r-1}(p-1)$ for ethvert primtal p.

OPGAVE 57. Vis, at $(\mathbb{Z}/8)^*$ er isomorf med $\mathbb{Z}/2 \times \mathbb{Z}/2$.

OPGAVE 58. Find $\sqrt{\underline{2}} \subseteq (\mathbb{Z}/7)^*$, dvs find alle $x \in (\mathbb{Z}/7)^*$ som opfylder ligningen $x^2 = \underline{2}$.

OPGAVE 59. Vis, at isomorfien fra Sætning 7.5 bestemmer en isomorfi

$$(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{\alpha_1})^* \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r})^*$$

og konkluder heraf at

$$\phi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$$

OPGAVE 60. (Uløst problem) Vis, at der for ethvert $n \geq 2$ findes et $m \neq n$ så $\phi(m) = \phi(n)$.

OPGAVE 61. Antag, at det hele tal c går op i a og b. Vis, at

$$a \equiv b \mod n \Leftrightarrow \frac{a}{c} \equiv \frac{b}{c} \mod \frac{n}{d}$$

hvor $d = \text{sfd}(c, n)$ er den største fælles divisor af c og n. (Øvelse 6.2 indeholder et specialtilfælde.)

OPGAVE 62. Vis, at grupperne $\mathbb{Z}/9 \times \mathbb{Z}/15$ og $\mathbb{Z}/45 \times \mathbb{Z}/3$ er isomorfe.

OPGAVE 63. (Midtvej 95/96)

1. Find mængden af løsninger $x \in \mathbb{Z}$ til ligningen $3072x \equiv 3 \mod 51$.
2. Vis, at ligningen $3072x \equiv 4 \mod 51$ ikke har nogen løsninger $x \in \mathbb{Z}$.

OPGAVE 64. Løs ligningerne

$$(a) \quad 2x \equiv 4 \mod 6 \qquad (c) \quad 3x \equiv 4 \mod 10$$
$$(b) \quad 4x \equiv 6 \mod 10 \qquad (d) \quad 2x \equiv 3 \mod 30$$

f.eks. ved at hente inspiration i Eksempel 6.16.

OPGAVE 65. Løs ligningerne

$$(a) \quad 56x - 3 \equiv 133 \mod 1324$$
$$(b) \quad 200x - 12 \equiv 35x + 4 \mod 1091$$

f.eks. ved at se tilbage på Opgave 10 og Eksempel 6.16.

OPGAVE 66. Find alle hele tal x så

$$(a) \quad x \equiv 2 \mod 5 \text{ og } x \equiv 8 \mod 14$$
$$(b) \quad x \equiv 56 \mod 123 \text{ og } x \equiv 212 \mod 712$$

f.eks. ved at benytte Bemærkning 7.7 og (for (b)) Øvelse 2.31.

OPGAVE 67. Find den inverse til isomorfien f fra Sætning 7.5 for $r = 3$. (Vink: Se Opgave 23.)

OPGAVE 68. Betragt homomorfien $f\colon \mathbb{Z}/(ab) \to \mathbb{Z}/a \times \mathbb{Z}/b$ givet ved $f(\underline{x}) = (\underline{x}, \underline{x})$ (som i Lemma 7.1) hvor $(a, b) = (2, 5)$ eller $(a, b) = (2, 6)$.

1. Find $f(\underline{x})$ for alle $\underline{x}$ i de to tilfælde.
2. Vis, at billedet $f(\mathbb{Z}/(ab))$ er isomorft med $\mathbb{Z}/\,\text{mfm}(a, b)$ og at kernen $\ker f$ er isomorf med $\mathbb{Z}/\,\text{sfd}(a, b)$ i de to tilfælde.

OPGAVE 69. Vis, at produktgruppen $\mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ indeholder en undergruppe isomorf med $\mathbb{Z}/\,\text{mfm}(m_1, m_2)$.

OPGAVE 70. Lad $m_1 > 0$ og $m_2 > 0$ være naturlige tal med største fælles divisor $d = \text{sfd}(m_1, m_2)$ og mindste fælles multiplum $m = \text{mfm}(m_1, m_2)$. Betragt afbildningen $f\colon \mathbb{Z} \to \mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ givet ved $f(x) = (\underline{x}, \underline{x})$, dvs. $f = \phi_{(\underline{1},\underline{1})}$.

1. Vis, at f er en homomorfi.

2. Vis, at kernen for f er $\ker f = m\mathbb{Z}$ og at billedet er
$$\operatorname{im} f = \{(\underline{0},\underline{0}), (\underline{1},\underline{1}), 2(\underline{1},\underline{1}), \ldots, (m-1)(\underline{1},\underline{1})\} \cong \mathbb{Z}/m.$$
3. Vis, at $\operatorname{im} f$ også kan beskrives som undergruppen
$$\operatorname{im} f = \{(\underline{a_1},\underline{a_2}) \mid a_1 \equiv a_2 \mod d\}.$$
4. Konkluder, at der findes et $x \in \mathbb{Z}$ så
$$x \equiv a_1 \mod m_1 \quad \text{og} \quad x \equiv a_2 \mod m_2$$
hvis og kun hvis $a_1 \equiv a_2 \mod d$.
5. Find løsningsmængden til ligningssystemet i punkt (4).

Litteratur

[1] Ireland and Rosen, *A classical introduction to modern number theory. Graduate Texts in Mathematics 84*, Springer-Verlag, Berlin-Heidelberg-New York, 1990.

[2] C.R. Jordan and D.A. Jordan, *Groups*, Edward Arnold, London, 1994.

[3] C. Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1484.

[4] Joseph J. Rotmann, *The theory of groups. An introduction*, Allyn and Bacon, Boston, 1976.

[5] Harold N. Shapiro, *Introduction to the theory of numbers*, John Wiley and Sons, New York, 1983.