Kapittel 25

Tallteori

I dette kapitlet lærer du grunnleggende tallteori. Vi snakker om delbarhet for heltall, lærer å løse Diofantiske likninger, definerer største felles divisor og minste felles multiplum, og lærer å faktorisere tall.

Delbarhet

I de neste kapitlene skal vi se nærmere på $\mathbb{Z}$, mengden av **heltall** (*eng: integers*), $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ og på hva som skjer når vi forsøker å dele et heltall på et annet. For eksempel kan 12 deles på 4, fordi $3 \cdot 4 = 12$, men 12 kan ikke deles på 5, fordi vi får 2 i rest. Divisjon av heltall går ikke alltid opp. Vi begynner med å definere noen begreper og litt notasjon som lar oss snakke om dette på en presis måte.

Definisjon 25.1 Delbarhet

La a og b være heltall slik at $b \neq 0$. Hvis det finnes et heltall q slik at $a = q \cdot b$, sier vi at b **deler** (*eng: divides*) a, og skriver $b \mid a$. Vi sier også at b er en **divisor** (*eng: divisor*) av a og at a er **delelig** (*eng: divisible*) med b. Hvis b ikke deler a, skriver vi $b \nmid a$.

Dette vil vise seg å være veldig nyttig fremover. La oss se på noen eksempler.

Eksempel Vi har at $7 \mid 21$, fordi det finnes et heltall q, nemlig 3, slik at $21 = q \cdot 7$. Det er også slik at $3 \mid (-12)$, fordi $-12 = -4 \cdot 3$. Det er derimot *ikke* slik at $5 \mid 18$, og vi skriver $5 \nmid 18$, fordi det *ikke* finnes et heltall q slik at $18 = q \cdot 5$. ♦

Legg merke til at $1 \mid a$, $a \mid a$ og $a \mid 0$ for alle $a \in \mathbb{Z} \setminus \{0\}$.

Eksempel **Transitivitet av divisjon**. *Hvis ett heltall deler et annet heltall, og dette igjen deler et tredje heltall, så må det første heltallet også dele det tredje.* Vi kan skrive dette slik: Hvis $c \mid b$ og $b \mid a$, så følger det at $c \mid a$. Hvorfor er det slik? Definisjonen sier at

$c \mid b$ betyr at det finnes et heltall q slik at $b = q \cdot c$. Og $b \mid a$ betyr at det finnes et heltall r slik at $a = r \cdot b$. Ved å sette disse to sammen, får vi

$$a = r \cdot b = r \cdot (q \cdot c) = (r \cdot q) \cdot c,$$

og det betyr, ved definisjonen av delbarhet, at $c \mid a$. ♦

Eksempel Hvis $b \mid a$ og $d \mid c$, så følger det at $b \cdot d \mid a \cdot c$, fordi $a = q \cdot b$ og $c = r \cdot d$ gir at

$$a \cdot c = (q \cdot b) \cdot (r \cdot d) = (q \cdot r) \cdot (b \cdot d).$$ ♦

Nå skal vi se på hva som skjer når a *ikke* er delelig med b.

Heltallsdivisjon

Hvis b er en divisor av a, så kan vi finne et heltall q slik at $a = q \cdot b$. Hvis vi tenker nærmere over dette, ser vi at q blir lik *kvotienten* a/b, nemlig det vi får når vi deler a på b.

Men, hva hvis b *ikke* er en divisor av a? Vi kan allikevel forsøke å dele a på b, men vi vil få en *rest*. I stedet for $a = q \cdot b$, får vi $a = q \cdot b + r$, der r er *resten*.

Definisjon 25.2 Heltallsdivisjon

La a og b være heltall slik at $b > 0$. Dersom vi finner heltall q og r slik at

$$a = q \cdot b + r \qquad \text{og} \qquad 0 \leqslant r < b,$$

da kaller vi q for en **kvotient** (*eng: quotient*) og r for en **rest** (*eng: remainder*).

Man kan bevise at det alltid finnes en slik q og en slik r, og at disse er unike når a og b er gitt. Generelt bryr vi oss ofte mer om resten r enn om kvotienten q.

Resten kalles også for «a **modulo** b», og den har en egen notasjon: $r = a \bmod b$. For eksempel har vi at $27 \bmod 12 = 3$, og $15 \bmod 5 = 0$. Men noen heltall er mer spesielle enn andre:

Definisjon 25.3 Primtall

Et naturlig tall $p > 1$ er et **primtall** (*eng: prime number*) hvis det ikke har noen andre positive divisorer enn 1 og p. Et naturlig tall $n > 1$ som ikke er et primtall kalles et **sammensatt tall** (*eng: composite number*).

Tallet 1 holdes utenfor definisjonen; det er hverken et primtall eller et sammensatt tall. Primtall er viktige fordi de er de minste tallene vi kan redusere til dersom vi prøver å faktorisere et tall.

Oppgave Hvor mange primtall finnes det? ♦

Løsning Det finnes uendelig mange primtall. Anta at det finnes et endelig antall primtall, og la $p_1, p_2, \ldots, p_n$ være alle primtallene. Definer

$$P = p_1 \cdot p_2 \cdots p_n + 1.$$

Da har vi, for hvert tall i fra 1 til n, at $P \bmod p_i = 1$, så $p_i \nmid P$. Det betyr at ingen av p_i-ene er divisorer av P, så da må enten P være et primtall eller så vil P være delelig på et tall som er større enn p_n men mindre enn P, og som heller ikke er delelig på noen av primtallene p_1 til p_n. Da må dette tallet være et primtall. Vi har altså funnet et primtall som ikke var med i listen $p_1, p_2, \ldots, p_n$, og det gir en motsigelse. Det må derfor finnes uendelig mange primtall. ♦

Største felles divisor (gcd)

De positive divisorene til tallet 12 er 1, 2, 3, 4, 6 og 12. De positive divisorene til 20 er 1, 2, 4, 5, 10 og 20. Tallene 12 og 20 har divisorene 1, 2 og 4 til felles. Den største av disse, altså 4, kaller vi for den *største felles divisoren* til 12 og 20.

Definisjon 25.4 Største felles divisor

La a og b være heltall slik at ikke begge er 0. Den **største felles divisoren** (*eng: greatest common divisor*) til a og b er tallet d som oppfyller følgende krav:

(1) Tallet d deler både a og b.

(2) Ethvert tall som deler både a og b, er mindre enn, eller lik, d.

Da skriver vi $\gcd(a, b) = d$.

Vi vil se at å finne største felles divisor kan forenkle mange beregninger, samt at å beregne denne raskt har anvendeleser innen kryptografi, når vi skal jobbe med veldig store tall for å legge til rette for sikker kommunikasjon.

Eksempel Vi vil forkorte brøken 12/20 så mye som mulig:

$$\frac{12}{20} = \frac{4 \cdot 3}{4 \cdot 5} = \frac{3}{5}.$$

Det største tallet vi kan forkorte bort, er det største tallet som både er en faktor i telleren og en faktor i nevneren, det vil si største felles divisor til teller og nevner. ♦

Relativt primiske tall

Hvis vi ser på de positive divisorene til to tall, a og b, så må de alltid ha minst én divisor felles, nemlig 1. Hva om dette er den *eneste* felles divisoren? I så fall er $\gcd(a, b) = 1$. Denne situasjonen minner litt om definisjonen av primtall: Et primtall er et tall som har så få divisorer som mulig. Nå ser vi på *to tall* som har så få felles divisorer som mulig. Tallpar med denne egenskapen spiller en viktig rolle, og de fortjener å ha et eget navn og en spesiell notasjon:

Definisjon 25.5 Relativt primiske tall

Hvis $\gcd(a, b) = 1$, sier vi at tallene a og b er **relativt primiske** (*eng: relatively prime / coprime*) til hverandre, og skriver $a \perp b$.

Eksempel **Relativt primiske tall**. Vi ser at $9 \perp 14$, og $10 \perp 27$. Tallene 14 og 8, derimot, er ikke relativt primiske, fordi $\gcd(14, 8) = 2 \neq 1$. ♦

To heltall a og b er relativt primiske hvis og bare hvis det finnes heltall x og y slik at

$$ax + by = 1.$$

Dersom m deler produktet $a \cdot b$, følger det at m deler a eller b? **Nei**, for eksempel deler 9 produktet $12 \cdot 15 = 180$, men 9 deler hverken 12 eller 15.

Dersom m deler produktet $a \cdot b$, og m er relativt primisk til a, følger det da at m deler b? **Ja**, hvis m og a er relativt primiske, får vi at det finnes x og y slik at $mx + ay = 1$. Hvis vi multipliserer dette med b, får vi $b \cdot mx + b \cdot ay = b$. Vi ser at m deler både $b \cdot mx$ og $b \cdot ay$ (fordi m deler $a \cdot b$). Da må m dele b.

Dersom produktet $m \cdot n$ deler a, følger det at både m og n deler a? **Ja**, fordi både m og n deler $m \cdot n$, og $m \cdot n$ deler a, må både m og n også dele a. Her trenger vi *ikke* antagelsen om at m og n er relativt primiske.

Dersom både m og n begge deler det samme tallet a, må da produktet $m \cdot n$ også dele a? **Nei**, igjen er dette noe som ikke stemmer for alle tall, men det stemmer dersom m og n er relativt primiske.

Dersom både m og n begge deler det samme tallet a, og m og n er relativt primiske, følger det at produktet $m \cdot n$ deler a? **Ja**, og her er et bevis: Anta at m deler a og at n deler a. Da finnes det per definisjon heltall q og r slik at $a = q \cdot m$ og $a = r \cdot n$. Anta også at $m \perp n$. Da finnes det heltall x og y slik at $mx + ny = 1$. Ved å gange med a på begge sider, får vi $a \cdot mx + a \cdot ny = a$. Nå kan vi erstatte de to forekomstene av a på venstresiden med henholdsvis $r \cdot n$ og $q \cdot m$, og da får vi:

$$(r \cdot n) \cdot mx + (q \cdot m) \cdot ny = a.$$

Legge merke til at begge tallene som summeres på venstresiden inneholder *både* m og n. Vi kan skrive det om til:

$$(m \cdot n) \cdot r \cdot x + (m \cdot n) \cdot q \cdot y = a.$$

Det vil si at $a = (r \cdot x + q \cdot y) \cdot (m \cdot n)$, og det betyr at $m \cdot n$ deler a. Dette er et viktig resultat, som vi tar med oss videre.

Euklids algoritme

Vi har sett at vi kan beregne $\gcd(a, b)$ ved å finne alle divisorene til a og b, se på hvilke av disse divisorene som deler *både* a og b, og velge den største av disse. Men, hvis a og b er store tall, blir dette veldig mye jobb. Nå skal vi se at det finnes en enklere måte å regne ut $\gcd(a, b)$ på. Den kalles *Euklids algoritme*.

Den viktigste idéen vi skal benytte oss av, er at hvis vi skal regne ut $\gcd(a, b)$, så kan vi bytte ut ett av tallene med et mindre tall. I stedet for å regne ut den største felles divisoren for noen veldig store tall, kan vi regne ut den største felles divisoren for noen litt mindre tall.

For enkelhets skyld kan vi anta at vi kun jobber med positive tall, og vi kan anta at a er det største tallet av a og b. Fordi a er det største tallet, vil vi i første omgang prøve å bytte ut a med et mindre tall.

Vi observerer at enhver felles divisor av a og b også må være en divisor av $a - b$. Dessuten kan vi se at et tall som er en divisor av både $a - b$ og b også må være en divisor av a. Det betyr at den største felles divisoren til a og b er den samme som den største felles divisoren til $a - b$ og b. Vi har altså vist følgende resultat: La a og b være heltall slik at $a > b > 0$. Da er $\gcd(a, b) = \gcd(a - b, b)$.

Vi kan bruke dette resultatet til å regne ut, for eksempel, $\gcd(74, 22)$. Vi ser at vi kan erstatte 74 med $74 - 22$ og forenkle uttrykket til $\gcd(52, 22)$. Nå kan vi bruke resultatet på nytt og erstatte 52 med $52 - 22$. Ved å fortsette slik, får vi følgende:

$$\begin{aligned}\gcd(74, 22) &= \gcd(74 - 22, 22) = \gcd(52, 22) \\ &= \gcd(52 - 22, 22) = \gcd(30, 22) \\ &= \gcd(30 - 22, 22) = \gcd(8, 22).\end{aligned}$$

Til slutt kommer vi til at det første tallet er mindre enn det andre. Men, hva er det nå vi har gjort? Vi har trukket 22 fra 74 gjentatte ganger til vi sitter igjen med en rest som er mindre enn 22. Men, det er jo det samme som å dele 74 på 22 og finne resten!

Hvis vi generaliserer dette, ser vi at den største felles divisoren til a og b, er den samme som den største felles divisoren til b og $a \bmod b$:

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Nå kan vi bruke denne regelen gjentatte ganger til å forenkle uttrykket vårt. La oss se på $\gcd(74, 22)$ igjen. Vi får altså:

$$\begin{aligned}\gcd(74, 22) &= \gcd(22, 74 \bmod 22) = \gcd(22, 8) \\ &= \gcd(8, 22 \bmod 8) = \gcd(8, 6) \\ &= \gcd(6, 8 \bmod 6) = \gcd(6, 2).\end{aligned}$$

Nå har vi forenklet det opprinnelige problemet vårt, å regne ut $\gcd(74, 22)$, til et enklere problem: å regne ut $\gcd(6, 2)$. Siden 2 er en divisor av 6, er det klart at $\gcd(6, 2) = 2$. Dermed har vi funnet ut at $\gcd(74, 22) = 2$.

La oss oppsummere dette resultatet. La a og b være naturlige tall:

(1) Hvis b deler a, så er $\gcd(a, b) = b$.

(2) $\gcd(a, b) = \gcd(b, a \bmod b)$.

Euklids algoritme for beregning av største felles divisor går ut på å bruke den andre delen av dette resultatet gjentatte ganger, helt til vi kommer til en situasjon der vi kan bruke første del av resultatet.

Eksempel Vi regner ut $\gcd(321, 78)$. Vi begynner med å dele 321 på 78. Da får vi:

$$321 = 4 \cdot 78 + 9.$$

Siden 78 ikke er en divisor av 321 (vi fikk en rest som ikke er 0), kan vi ikke bruke første del av resultatet her. Derfor bruker vi andre del, som forteller oss at $\gcd(321, 78) = \gcd(78, 9)$.

Dermed kan vi regne ut $\gcd(78, 9)$ isteden. Vi deler 78 på 9 og får:

$$78 = 8 \cdot 9 + 6.$$

Igjen er resten ikke 0, så vi bruker andre del av resultatet og får $\gcd(78, 9) = \gcd(9, 6)$. Så vi vil regne ut $\gcd(9, 6)$. Vi deler 9 på 6 og får:

$$9 = 1 \cdot 6 + 3.$$

Resten er ikke 0, så vi bruker andre del av resultatet og får $\gcd(9, 6) = \gcd(6, 3)$.

Så vil vi regne ut $\gcd(6, 3)$. Vi deler 6 på 3 og får:

$$6 = 2 \cdot 3 + 0.$$

Resten er 0, altså er 3 en divisor av 6. Det betyr at denne gangen kan vi bruke første del av resultatet! Da får vi at $\gcd(6, 3) = 3$.

Totalt har vi altså:

$$\begin{aligned}\gcd(321, 78) &= \gcd(78, 9) = \gcd(9, 6) \\ &= \gcd(6, 3) = 3.\end{aligned}$$

Når vi bruker Euklids algoritme, skriver vi vanligvis bare ned likhetene vi får fra hver divisjon, og passer på å holde orden på hvilke tall vi skal ta med oss videre til neste steg. Utregningen over kunne vi altså skrevet slik (de understrekede tallene er de som blir med videre):

$$\begin{aligned} 321 &= 4 \cdot \underline{78} + \underline{9} \\ 78 &= 8 \cdot \underline{9} + \underline{6} \\ 9 &= 1 \cdot \underline{6} + \underline{3} \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Svaret finner vi da som den siste resten som ikke er 0. ♦

Diofantiske likninger

La oss se på følgende likning og finne ut om den kan løses.

Oppgave Har likningen $12 \cdot x + 20 \cdot y = 14$ noen heltallsløsninger? ♦

Løsning Nei. Vi ser igjen at $\gcd(12, 20) = 4$, og 4 kan derfor settes utenfor parentes på venstre side av likningen, slik: $4 \cdot (3 \cdot x + 5 \cdot y) = 14$. Men, det betyr at 4 er en divisor av uttrykket på venstre side. For at likningen skal gå opp, må 4 også være en divisor av det som står på høyre side. Fordi 4 ikke deler 14, vil likningen ikke ha noen heltallsløsninger. ♦

Likninger som i denne oppgaven er veldig spesielle, og de har fått et eget navn.

Definisjon 25.6 Lineær diofantiske likning

En **lineær diofantisk likning** (*eng: linear Diophantine equation*) er en likning på formen

$$a \cdot x + b \cdot y = c,$$

der a, b og c er heltall. Ofte skrives diofantiske likninger uten symbolet for multiplikasjon, slik: $ax + by = c$.

Når en lineær diofantisk likning er gitt, ønsker vi å finne ut om det finnes heltall x og y som får likningen til å gå opp.

Hvordan kan vi finne ut om en slik likning har løsninger eller ikke?

Vi så i oppgaven over at $12x + 20y = 14$ ikke har noen løsninger fordi den største felles divisoren til 12 og 20, nemlig 4, ikke deler 14. Vi kan generalisere dette argumentet og vise at hvis $\gcd(a, b)$ og c er relativt primiske, så vil ikke likningen $a \cdot x + b \cdot y = c$ ha noen løsninger.

Men, hva om $\gcd(a, b)$ og c *ikke* er relativt primiske og $\gcd(a, b)$ deler c? *Vil da likningen ha en løsning? Og hvordan kan vi i så fall finne en løsning?*

Den mest åpenbare måten å gå frem på er å ved å prøve seg frem med mange forskjellige verdier av x og y for å se hvilke verdier $ax + by$ kan få.

Definisjon 25.7 Lineærkombinasjon

Et uttrykk på formen $a \cdot x + b \cdot y$ kalles en **lineærkombinasjon** (*eng: linear combination*) av a og b.

Vi skal foreløpig ta det følgende resultatet for gitt. Resten av dette kapitlet handler om å bygge opp en forståelse for hvorfor dette er slik.

La a og b være heltall slik at ikke begge er 0. Da finnes det heltall x og y slik at den diofantiske likningen $ax + by = \gcd(a, b)$ er oppfyllbar. Det er med andre ord slik at den største felles divisoren til a og b alltid kan skrives som en *lineærkombinasjon* av a og b. Videre er det også slik at *alle* lineærkombinasjoner av a og b er multipler av $\gcd(a, b)$. Med andre ord vil en lineær diofantisk likning $ax + by = c$ være løsbar *hvis og bare hvis* $\gcd(a, b) \mid c$.

Oppgave Avgjør om følgende diofantiske likninger har heltallsløsninger.

$$7x + 12y = 1 \qquad 15x + 9y = 23 \qquad 16x + 22y = 358$$

♦

Løsning Vi får at $\gcd(7, 12) = 1$. Den første likningen vil dermed ha en løsning, fordi $1 \mid 1$. For den andre likningen, får vi at $\gcd(15, 9) = 3$. Fordi alle lineærkombinasjoner av 15 og 9 vil være multipler av 3, og 3 ikke deler 23, vil den andre likningen *ikke* ha en løsning. For den tredje likningen, får vi at $\gcd(16, 22) = 2$. Fordi 2 deler 358, må det finnes en løsning. ♦

Legg merke til at vi her sier helt sikkert *om* det eksisterer løsninger eller ikke, selv om vi finner noen konkrete løsninger.

Euklids utvidede algoritme

Tidligere så vi at en lineær diofantisk likning $ax + by = c$ er løsbar hvis og bare hvis $\gcd(a, b) \mid c$.

For å kunne bruke dette resultatet, må vi klare å regne ut $\gcd(a, b)$, og det kan vi bruke Euklids algoritme til. Dermed har vi nå en effektiv metode for å finne ut om en gitt likning har løsninger eller ikke.

Men, Euklids algoritme gjør mer enn dette; den kan faktisk også fortelle oss *hva* løsningene er! Hvis vi skriver opp alle divisjonene vi gjør i utføringen av

Euklids algoritme, på samme måte som på slutten i det forrige eksemplet, så står $\gcd(a, b)$ som den siste resten som ikke er 0. Vi kan da jobbe oss baklengs gjennom likhetene for å uttrykke $\gcd(a, b)$ som en lineærkombinasjon av a og b. Dette metoden kalles *Euklids utvidede algoritme*. La oss se på to eksempler.

Eksempel La oss løse likningen $321x + 78y = 3$.

Vi regnet ut at $\gcd(321, 78) = 3$, og dermed vet vi at likningen skal ha en løsning.

Fra nest siste linje i utregningen i forrige eksempel får vi at $3 = 9 - 1 \cdot 6$. Her har vi uttrykt 3 som en lineærkombinasjon av 9 og 6. Men, linjen over gir oss at $6 = 78 - 8 \cdot 9$, så vi kan sette inn dette og få:

$$3 = 9 - 1 \cdot 6 = 9 - 1 \cdot (78 - 8 \cdot 9) = (-1) \cdot 78 + 9 \cdot 9.$$

Nå har vi altså uttrykt 3 som en lineærkombinasjon av 78 og 9. Deretter kan vi erstatte 9 på samme måte ved å bruke den øverste linjen i utregningen, og da ender vi opp med en lineærkombinasjon av 321 og 78.

Til sammen gjør vi altså dette:

$$\begin{aligned} 3 &= \underline{9} - 1 \cdot \underline{6} \\ &= \underline{9} - 1 \cdot (\underline{78} - 8 \cdot \underline{9}) \\ &= (-1) \cdot \underline{78} + 9 \cdot \underline{9} \\ &= (-1) \cdot \underline{78} + 9 \cdot (\underline{321} - 4 \cdot \underline{78}) \\ &= 9 \cdot \underline{321} + (-37) \cdot \underline{78}. \end{aligned}$$

Dermed er $x = 9$ og $y = -37$ en løsning. ♦

Eksempel La oss løse likningen $321x + 78y = 15$.

I forrige eksempel fant vi ut at

$$321 \cdot 9 + 78 \cdot (-37) = 3.$$

Hvis vi ganger begge sider med 5, får vi

$$321 \cdot 45 + 78 \cdot (-185) = 15.$$

Altså er $x = 45$ og $y = -185$ en løsning. ♦

For å løse en lineær diofantisk likning $ax + by = c$, kan vi altså gjøre følgende:

(1) Beregn $d = \gcd(a, b)$ med Euklids algoritme.
(2) Hvis $d \nmid c$, så har likningen ingen løsninger.
(3) Hvis $d \mid c$, så benytter vi Euklids utvidede algoritme til å gå baklengs gjennom utregningene for å finne u og v slik at $\gcd(a, b) = au + bv$. Vi finner x og y ved å gange opp u og v med tallet c/d.

Minste felles multiplum

Det «omvendte» av største felles divisor er minste felles multiplum, som vi kan definere slik:

Definisjon 25.8 Minste felles multiplum I

La a og b være heltall. **Minste felles multiplum** (*eng: least common multiple*) av a og b er det minste tallet m som er et multiplum av både a og b, altså som kan skrives som $m = a \cdot c = b \cdot d$ for heltall c og d. Da skriver vi $\operatorname{lcm}(a, b) = m$.

Eksempel Hva er minste felles multiplum av 6 og 8? Multiplene av 6 er 6, 12, 18, 24, 30, 36, og så videre. Multiplene av 8 er 8, 16, 24, 32, 40, 48, og så videre. Det minste som er felles er $24 = 4 \cdot 6 = 3 \cdot 8$. Dermed er $\operatorname{lcm}(6, 8) = 24$. ♦

La oss definere dette litt mer formelt:

Definisjon 25.9 Minste felles multiplum II

La a og b være naturlige tall, og anta at

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r},$$
$$b = p_1^{l_1} \cdot p_2^{l_2} \cdots p_r^{l_r},$$

der vi for hver i har at p_i er et primtall, og $k_i \geqslant 0$ og $l_i \geqslant 0$. Da definerer vi

$$\operatorname{lcm}(a, b) = p_1^{s_1} \cdot p_2^{s_2} \cdots p_r^{s_r},$$

der s_i er den største av k_i og l_i.

Eksempel Vi har at $6 = 2^1 \cdot 3^1$ og $8 = 2^3 \cdot 3^0$, så da er $\operatorname{lcm}(6, 8) = 2^3 \cdot 3^1 = 24$. ♦

Eksempel La a og b være heltall, ikke begge 0. Da er $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$. ♦

Eratosthenes' sil

Vi har sett at for å faktorisere et tall, kan vi først dele på 2 så mange ganger som mulig, så dele på 3 så mange ganger som mulig, så på 5, på 7, og så videre. For å kunne gjøre dette er det nyttig å ha en ferdig liste med primtall, for eksempel alle primtallene som er mindre enn 100 eller alle som er mindre enn 1000.

Det finnes en smart metode for å finne alle primtallene som er mindre enn et gitt tall n. Den kalles *Eratosthenes' sil*, og fungerer slik:

Skriv opp alle tallene fra 2 til n. Sett ring rundt det minste tallet (altså 2). Kryss ut alle multipler av dette tallet: 4, 6, 8, og så videre. Gjør deretter følgende:

(1) Finn det minste tallet som ikke er ringet rundt eller krysset ut. Kall det p.
(2) Sett ring rundt p.
(3) Hvis $p^2 > n$, sett ring rundt alle tallene du ennå ikke har gjort noe med, og du er ferdig. Hvis $p^2 \leqslant n$, fortsett til neste steg.
(4) Kryss ut multipler av p, altså $2p$, $3p$, $4p$, og så videre, til slutten av listen.
(5) Gå tilbake til steg (1), og gjenta prosedyren.

Tallene som har fått ring rundt seg er primtall, og de som er krysset ut er sammensatte. *Klarer du se hvorfor det er nok å sjekke tallene* p *slik at* $p^2 \leqslant n$*?*

Fermats faktoriseringsmetode

Eratosthenes' sil – å prøve å dele på 2, 3, 5, 7, 11, 13, 17, og så videre – fungerer fint hvis tallet har ganske små primtallsfaktorer. Men, hva om det kun har store faktorer?

Sett at vi for eksempel vil faktorisere tallet 119113. Da må vi helt opp til 311 for å finne en faktor. Det viser seg nemlig at $119113 = 311 \cdot 383$.

Vi skal nå se på en annen faktoriseringsmetode, som er egnet for tall som er produktet av to omtrent like store primtall. Denne metoden kalles *Fermats faktoriseringsmetode*.

La n være tallet vi vil faktorisere. Vi leter etter to tall a og b som er slik at

$$a^2 - b^2 = n.$$

Hvis vi finner slike tall, kan vi skrive n som et produkt av to mindre tall:

$$n = a^2 - b^2 = (a - b) \cdot (a + b).$$

Metoden er spesialisert for tall med to nesten like store primtallsfaktorer, så vi gjetter at b skal være liten, og dermed at a er ganske nær kvadratroten av n. Likningen $a^2 - b^2 = n$ kan vi skrive om til $a^2 - n = b^2$.

Vi starter med å sette a_1 til å være $\sqrt{n}$ rundet opp til nærmeste heltall. Så undersøker vi om $a_1^2 - n$ er et kvadrattall. Hvis det ikke er det, forsøker vi å øke a-verdien med 1: Vi setter $a_2 = a_1 + 1$, og undersøker om $a_2^2 - n$ er et kvadrattall. Slik fortsetter vi, med

$$a_{i+1} = a_i + 1,$$

frem til vi kommer til en a_k slik at $a_k^2 - n$ er et kvadrattall. Da setter vi

$$a = a_k \qquad \text{og} \qquad b = \sqrt{a_k^2 - n},$$

og vi har en faktorisering $n = (a - b) \cdot (a + b)$.

Eksempel La oss faktorisere $n = 119113$ med Fermats metode. Vi har $\sqrt{119113} \approx 345.1$, så vi begynner med å sette $a_1 = 346$. Da er

$$a_1^2 - n = 346^2 - 119113 = 603,$$

og vi kan lett sjekke at 603 ikke er et kvadrattall ved å se at kvadratroten ikke er et heltall. Dermed går vi videre til $a_2 = a_1 + 1 = 347$. Da er

$$a_2^2 - n = 347^2 - 119113 = 1296,$$

som er et kvadrattall: $1296 = 36^2$. Vi setter derfor $a = a_2 = 347$ og $b = 36$, og vi har funnet faktorene

$$a - b = 347 - 36 = 311 \quad \text{og} \quad a + b = 347 + 36 = 383 \quad \text{av} \quad 119113. \qquad \blacklozenge$$