Kapittel 25

Elementær tallteori

Delbarhet

La $\mathbb{Z}$ være mengden av alle heltall. Divisjon av heltall går ikke alltid opp (eksempel: 12 kan deles på 4 siden $3 \cdot 4 = 12$, men 12 kan ikke deles på 5). Vi definerer begreper og notasjon som lar oss snakke om dette på en praktisk måte:

Definisjon 25.1 Delbarhet

La a og b være heltall med $b \neq 0$. Hvis det finnes et heltall q slik at $q \cdot b = a$, sier vi at b *deler* a, og skriver $b|a$. (Vi sier også at b er en *divisor* av a, eller at a er *delelig* på 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 Det følger at $7|21$ og $3|(-12)$ men $5 \nmid 18$. I tillegg: $1|c$, $c|c$ og $c|0$ for alle $c \in \mathbb{Z} \setminus \{0\}$. ♦

Eksempel Hvis et tall deler et annet, og det igjen deler et tredje, så må det første tallet også være en divisor av det tredje. Altså: Hvis $c|b$ og $b|a$, så følger det at $c|a$. Hvorfor er det slik? Jo, siden $c|b$, sier definisjonen at det finnes et heltall q_1 slik at $q_1 \cdot c = b$. Og siden $b|a$, sier definisjonen at det finnes et heltall q_2 slik at $q_2 \cdot b = a$. Men da har vi at

$$a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) = (q_2 q_1) \cdot c,$$

og det betyr (ved å bruke definisjonen igjen) at $c|a$. ♦

Eksempel Hvis $b|a$ og $d|c$, så følger det at $(b \cdot d)|(a \cdot c)$, fordi $q_1 \cdot b = a$ og $q_2 \cdot d = c$ gir at $(q_1 \cdot b) \cdot (q_2 \cdot d) = (q_1 \cdot q_2) \cdot (b \cdot d) = a \cdot c$. ♦

Videre skal vi se på hva som skjer når b ikke er delelig på a.

Heltallsdivisjon

Hvis b er en divisor av a, så kan vi finne et heltall q slik at $a = q \cdot b$. Dette handler jo egentlig om å dele a på b, for q blir kvotienten a/b.

Hva hvis b ikke er en divisor av a? Vi kan likevel prøve å dele a på b, men vi vil få en *rest*. Istedenfor $a = q \cdot b$, får vi $a = q \cdot b + r$, der r er resten.

Definisjon 25.2 Heltallsdivisjon
La a og b være heltall, med $b > 0$. Da finnes heltall q og r slik at

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

og disse er entydig bestemt av a og b. Vi kaller q for en *kvotient* og r for en *rest*.

Vi bryr oss ofte mer om resten r enn om kvotienten q. Resten kalles 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* 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*.

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. La $p_1, p_2, \ldots, p_n$ være primtall, og la

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

Da har vi, for hver i fra 1 til n, at $P \bmod p_i = 1$, så $p_i \nmid P$.

La q være den minste divisoren av P utenom 1. Da må q være et primtall. Men siden ingen av p_i-ene er divisorer av P, kan ikke q være lik noen av dem. Altså har vi funnet et primtall som ikke var med i listen $p_1, p_2, \ldots, p_n$.

Dette fungerer uansett hvilken endelig liste av primtall vi starter med. Altså finnes det ingen endelig liste som inneholder alle primtall, og da må det være uendelig mange. ♦

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 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, og anta at minst ett av dem ikke er 0. Den *største felles divisoren* til a og b er tallet d som oppfyller følgende krav:

(1) Vi har både at $d|a$ og at $d|b$.

(2) For alle tall c: hvis $c|a$ og $c|b$, så er $c \leqslant d$.

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 – altså største felles divisor til teller og nevner. ♦

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

Løsning Vi ser igjen at $\gcd(12, 20) = 4$ og den kan settes utenfor parentes på venstre side av likningen: $4(3x + 5y) = 14$.

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. Siden $4 \nmid 14$, har likningen ingen heltallsløsninger. ♦

Diofantiske likninger

En *lineær diofantisk likning* er en likning på formen

$$ax + by = c,$$

der a, b og c er heltall, og vi vil finne heltall x og y som får likningen til å gå opp. Hvordan kan vi se om en slik likning har løsninger eller ikke?

Vi så i eksempelet over at $12x+20y = 14$ ikke har noen løsninger fordi den største felles divisoren til 12 og 20, nemlig 4, ikke er en divisor av 14. Med tilsvarende argumentasjon ser vi at hvis $\gcd(a, b) \nmid c$, så har likningen $ax + by = c$ ingen løsning.

Men hva om $\gcd(a, b)$ *er* en divisor av c? Kan vi da være sikre på at likningen har en løsning? Og hvordan kan vi finne en løsning?

Den mest åpenbare måten å gå frem på er å prøve seg frem med mange forskjellige verdier av x og y, og se hvilke verdier $ax + by$ kan få. Et uttrykk på formen $ax + by$ kalles en *lineærkombinasjon* av a og b.

Definisjon 25.5

La a og b være heltall, ikke begge 0. Da finnes heltall x og y slik at en *diofantisk likning* $ax + by$ har følgende løsning:

$$\gcd(a, b) = ax + by.$$

Med andre ord: Den største felles divisoren til a og b kan skrives som en *lineærkombinasjon* av a og b.

Eksempel Se på disse likningene:

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

Har de heltallsløsninger? Vi får at $\gcd(7, 12) = 1$, $\gcd(15, 9) = 3$, $\gcd(16, 22) = 2$.

Vi får da at den første likningen har en løsning (siden $1|1$), den andre har ingen løsning (siden $3 \nmid 23$), og den tredje har en løsning (siden $2|358$).

Merk at vi i hvert tilfelle kan si helt sikkert om det eksisterer en løsning eller ikke, selv om vi ikke har funnet noen løsninger. ♦

Relativt primske 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 det 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, så de fortjener å ha et eget navn og en spesiell notasjon:

Definisjon 25.6

Hvis $\gcd(a, b) = 1$, sier vi at tallene a og b er *relativt primiske*, og skriver $a \perp b$.

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

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

$$ax + by = 1.$$

Dersom et tall n er en divisor av produktet ab av to andre tall, kan vi da konkludere med at det er en divisor av a eller av b? Nei, for eksempel er 9 en divisor av $12 \cdot 15 = 180$, men ikke av hverken 12 eller 15. Men hvis vi også antar at n er relativt primisk til a, da må n være en divisor av b.

Siden n og a er relativt primiske, får vi at det finnes x og y slik at $nx + ay = 1$. Vi multipliserer dette med b og får $bnx + aby = b$. Da ser vi at n deler venstre side av likheten (siden $n|ab$), og dermed har vi $n|b$.

Hvis to tall m og n begge deler det samme tallet a, får vi da at mn deler a? Igjen er dette noe som ikke stemmer for alle tall, men det stemmer hvis m og n er relativt primiske.

Dersom $mn|a$, så følger det at både m og n er divisorer av a, i og med at de begge er divisorer av mn (her trenger vi ikke antagelsen om at m og n er relativt primiske).

Anta nå at $m|a$ og $n|a$. Da finnes heltall s og t slik at $ms = a$ og $nt = a$. Siden $m \perp n$ får vi at det finnes heltall x og y slik at

$$mx + ny = 1.$$

Vi ganger med a på begge sider og får:

$$max + nay = a$$

Ved å sette inn $a = nt$ og $a = ms$, kan vi skrive dette slik:

$$m(nt)x + n(ms)y = a$$

Det vil si at $a = mn(tx + sy)$, så $mn|a$. Dette er viktig å ta med seg videre.

Euclids algoritme

Vi har sett at vi kan beregne $\gcd(a, b)$ ved å finne alle divisorene til a, finne alle divisorene til b, se hvilke divisorer som er felles, og plukke ut 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 ideen vi skal benytte oss av er at hvis vi skal regne ut $\gcd(a, b)$, så kan vi bytte ut et av tallene med et mindre tall. Istedenfor å regne ut største felles divisor av noen veldig store tall, kan vi regne ut største felles divisor av noen litt mindre tall.

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

Vi kan observere 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 det 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 $\gcd(a, b) = \gcd(a - b, b)$.

Om vi for eksempel vil bruke dette til å regne ut $\gcd(74, 22)$, så ser vi at vi kan erstatte 74 med $74 - 22$ og forenkle til $\gcd(52, 22)$. Så kan vi bruke resultatet igjen, og erstatte 52 med $52 - 22$. Vi får:

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

Til slutt kommer vi til at det første tallet er mindre enn det andre. Men hva er det vi har gjort nå? Vi har trukket 22 fra 74 gjentatte ganger til vi satt igjen med en rest som var 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 det 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 $b|a$, 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 teoremet gjentatte ganger, helt til vi kommer til en situasjon der vi kan bruke første del av teoremet.

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 teoremet 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 teoremet 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 teoremet og får $\gcd(9, 6) = \gcd(6, 3)$.

Så vi vil 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 teoremet! 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. ♦

Euclids utvidede algoritme

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

For å kunne bruke dette resultatet, må vi klare å regne ut $\gcd(a, b)$, og der er Euklids algoritme til hjelp. 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 det – 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 av det forrige eksempelet, 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:

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

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 $d \nmid c$: Da har likningen ingen løsninger.
(3) Hvis $d|c$: Benytt Euklids utvidede algoritme til å gå baklengs gjennom utregningene for å finne u og v slik at $\gcd(a, b) = au + bv$. Finn x og y ved å gange opp u og v med tallet c/d.

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 multipler av dette tallet: 4, 6, 8, og så videre. Gjør deretter følgende:

(1) Finn minste tall 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 primfaktorer. Men hva om det bare 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 å skrive n som et produkt av to mindre tall:

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

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 $n = (a - b)(a + b)$.

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

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

Minste felles multiplum

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

Definisjon 25.7

La a og b være heltall. *Minste felles multiplum* av a og b er det minste tallet m som er et multiplum av både a og b, altså som kan skrives som $m = ac = bd$ for heltall c og d. Vi skriver $\operatorname{lcm}(a, b) = m$.

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 $\operatorname{lcm}(6, 8) = 24$. $\blacklozenge$

La oss definere dette litt mer formelt:

Definisjon 25.8

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 er

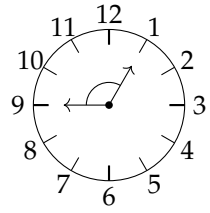
$$\operatorname{lcm}(a, b) = p_1^{s_1} \cdot p_2^{s_2} \cdots p_r^{s_r},$$

der s_i er den største av k_i og l_i.

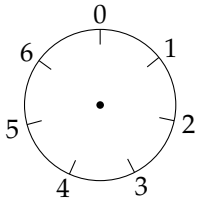
Eksempel Vi har at $6 = 2^1 \cdot 3^1$ og $8 = 2^3 \cdot 3^0$, så da er $\gcd(6, 8) = 2^3 \cdot 3^1 = 24$. ♦

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

Kongruensregning



$9 + 4 \equiv 1 \pmod{12}$



$3 \cdot 4 = 12 \equiv 5 \pmod{7}$

Kongruensregning kan også kalles *klokkearitmetikk*, fordi det minner om måten tallene er ordnet på en klokke. Hvis klokken er ni nå, så er den ett om fire timer. Med andre ord har vi $9 + 4 = 1$ på klokken. Tilsvarende har vi for eksempel at $3 = 15 = 27$, og $12 = 0$.

Vi kan også lage oss en teoretisk klokke som har for eksempel 7 forskjellige tall istedenfor 12. På den klokken har vi at $7 = 0$, og $3 \cdot 4 = 12 = 5$.

Hvis vi vil si at to tall er like i klokkesystemet med m forskjellige tall, så sier vi at de to tallene er *kongruente modulo* m. Vi har en egen notasjon for dette, slik at vi ser forskjell på om tallene faktisk er like, eller om de bare er like innenfor et bestemt klokkesystem.

Definisjon 25.9

La a, b og m være heltall, med $m > 0$. Hvis $m|(a - b)$, sier vi at a er *kongruent med* b *modulo* m, og skriver:

$$a \equiv b \pmod{m}$$

Tallet m i kongruensen kalles *modulus*. Hvis a ikke er kongruent med b modulo m, skriver vi:

$$a \not\equiv b \pmod{m}$$

Eksempel For eksempel er $50 \equiv 2 \pmod{12}$, siden vi har at $12|(50-2)$. Men $9 \not\equiv 23 \pmod{4}$, siden $4 \nmid (9-23)$. ♦

Oppgave Hva betyr det at to tall er kongruente modulo 10? Med andre ord: Hvis vi har $a \equiv b \pmod{10}$, hva kan vi da si om a og b? Tilsvarende: Hva betyr det at to tall er kongruente modulo 2? ♦

Løsning Dersom to tall er kongruente modulo 10 så betyr det at siste siffer av a og siste siffer av b er identiske, fordi vi fjerner alle multiplum av 10 i tallene. Dersom to tall er kongruente modulo 2 så betyr det at de har samme paritet, altså, at begge to er oddetall eller at begge to er partall. ♦

Ordet «mod» i kongruensnotasjonen ser kjent ut, for vi har tidligere definert en operator som heter det samme. Vi definerte $a \bmod b$ til å bety resten vi får når a deles på b. Det er viktig å ikke blande sammen de to betydningene – det er ikke samme «mod» i uttrykket $a \bmod b$ som i $a \equiv b \pmod{m}$!

Men er det noen sammenheng mellom de to ulike betydningene av «mod»? Ja, for det at to tall er kongruente modulo m betyr at de gir samme rest når de deles på m. Vi har altså følgende resultat:

Vi har $a \equiv b \pmod{m}$ hvis og bare hvis $a \bmod m = b \bmod m$.

Vi kan også merke oss at vi kan beskrive $a \bmod m$ på denne måten: $a \bmod m$ er det tallet r som oppfyller både $a \equiv r \pmod{m}$ og $0 \leqslant r < m$.

Det er ingen tilfeldighet at tegnet $\equiv$ for kongruens ligner på likhetstegnet. Vi tenker på kongruenser som en slags likheter, og mange av regnereglene som vi er vant til å bruke for likheter gjelder også for kongruenser.

Eksempel Vi vil løse likningen $x + 5 \equiv 1 \pmod{7}$. Ved å bruke regnereglene for kongruenser kan vi gå frem på samme måte som om vi skulle løse en vanlig likning. Vi får:

$$x \equiv 1 - 5 = -4 \equiv 3 \pmod{7}$$

Løsningen er altså $x \equiv 3 \pmod{7}$. ♦

Legg merke til hvordan vi setter flere kongruenser sammen på samme linje, og dessuten blander inn en likhet:

$$x \equiv 1 - 5 = -4 \equiv 3 \pmod{7}$$

Dette leses som «x er kongruent med $(1-5)$, som er lik -4, som er kongruent med 3, der kongruensene er modulo 7». Merk at $\pmod{7}$ her beskriver begge

de to kongruensene. Når vi setter flere kongruenser etter hverandre på denne måten, må de ha samme modulus, og den skriver vi bare én gang.

Selv om vi for det meste kan behandle kongruenser som likheter, er det ett viktig unntak: Vi kan ikke uten videre forkorte bort en felles faktor fra begge sider av en kongruens. Altså: Hvis vi har en kongruens $ca \equiv cb \pmod{m}$, der $c \not\equiv 0 \pmod{m}$, får vi ikke nødvendigvis at $a \equiv b \pmod{m}$. For eksempel er $2 \cdot 9 \equiv 2 \cdot 5 \pmod{8}$, men $9 \not\equiv 5 \pmod{8}$.

Vi skal imidelrtidig se at vi alltid kan gå fra $ca \equiv cb$ til $a \equiv b$, men de to kongruensene blir ikke nødvendigvis modulo samme tall.

Oppgave Vis at dersom $ca \equiv cb \pmod{m}$ og $d = \gcd(c, m)$, så er $a \equiv b \pmod{\frac{m}{d}}$. ♦

Løsning Kongruensen $ca \equiv cb \pmod{m}$ betyr, per definisjon, at $m|(ca - cb)$, og dermed finnes et heltall e slik at $em = ca - cb$. La $m' = m/d$ og $c' = c/d$. Da har vi:

$$em'd = em = ca - cb = c(a - b) = c'd(a - b)$$

Nå kan vi forkorte bort d og få:

$$em' = c'(a - b)$$

Det betyr at $m'|c'(a - b)$, og siden vi dessuten har $m' \perp c'$, git at $m'|(a - b)$. Dermed har vi vist at $a \equiv b \pmod{m'}$. ♦

Eksempel Fra teksten overnfor har vi $2 \cdot 9 \equiv 2 \cdot 5 \pmod{8}$, og da får vi at $9 \equiv 5 \pmod{4}$. ♦

Følgende to resultater, som følger lett fra oppgaven over, beskriver tilfeller der vi kan forkorte bort en felles faktor fra begge sider av en kongruens uten å skifte modulus.

Eksempel Hvis $ca \equiv cb \pmod{m}$ og $c \perp m$, så er $a \equiv b \pmod{m}$. Siden $c \perp m$ er $\gcd(c, m) = 1$, får vi at $a \equiv b \pmod{\frac{m}{1}}$. ♦

Eksempel Hvis $ca \equiv cb \pmod{p}$, der p er et primtall og $p \nmid c$, så er $a \equiv b \pmod{p}$. Siden p er et primtall og $p \nmid c$ får vi $p \perp c$, og resultatet følger. ♦

Modulære inverser

Hvis vi skal løse en lineær likning

$$ax = b$$

over de reelle tallene (eller de rasjonale tallene), så vil vi ganske enkelt dele på a på begge sider og få $x = b/a$. Dette kan vi også tenke på som at vi ganger med $1/a$:

$$\underbrace{\frac{1}{a} \cdot a}_{=1} \cdot x = \frac{1}{a} \cdot b$$

Når vi skal løse kongruenslikningen

$$ax \equiv b \pmod{m}$$

kan vi ikke dele på a eller gange med $1/a$. Men noen ganger kan vi gjøre noe veldig liknende. Dersom det finnes et tall c som er slik at

$$ac \equiv 1 \pmod{m},$$

så vil c spille en tilsvarende rolle som tallet $1/a$ gjør: Å gange med det opphever virkningen av å gange med a.

Hvis vi har funnet et slikt tall c, så kan vi gange med det på begge sider av likningen og få:

$$\underbrace{a \cdot c}_{\equiv 1} \cdot x \equiv bc \pmod{m}$$

Dermed har vi løsningen $x \equiv bc \pmod{m}$.

Når vi snakker om reelle eller rasjonale tall, sier vi at tallet $1/a$ er *inversen* til a. Tilsvarende snakker vi i kongruensregning om «invers modulo m».

Definisjon 25.10

La a, c og m være heltall, med $m > 0$. Hvis $ac \equiv 1 \pmod{m}$, sier vi at c er en *invers* til a *modulo* m.

Eksempel La oss løse kongruenslikningen

$$12x \equiv 4 \pmod{25}.$$

Det går selvfølgelig fint å løse den på vanlig måte med Euklids algoritme, men dersom vi prøver oss litt frem så ser vi at

$$12 \cdot 23 \equiv 1 \pmod{25}.$$

Vi ganger så med inversen på begge sider av likningen:

$$\underbrace{12 \cdot 23}_{\equiv 1} \cdot x \equiv 4 \cdot 23 \pmod{25}.$$

Dermed får vi $x \equiv 4 \cdot 23 = 92 \equiv 17 \pmod{25}$. ♦

Men er det alltid mulig å finne en invers? La oss se på et nytt eksempel.

Eksempel Finnes det noen invers til 4 modulo 6? Ethvert heltall er kongruent modulo 6 med enten 0, 1, 2, 3, 4 eller 5. La oss sjekke om noen av disse tallene oppfyller kriteriet for å være en invers til 4 (alle kongruensene er modulo 6):

$$4 \cdot 0 = 0 \not\equiv 1 \qquad 4 \cdot 3 = 12 \equiv 0 \not\equiv 1$$
$$4 \cdot 1 = 4 \not\equiv 1 \qquad 4 \cdot 4 = 16 \equiv 4 \not\equiv 1$$
$$4 \cdot 2 = 8 \equiv 2 \not\equiv 1 \qquad 4 \cdot 5 = 20 \equiv 2 \not\equiv 1$$

Vi har altså funnet ut at 4 ikke har noen invers modulo 6. ♦

Det at a har en invers modulo m er det samme som at likningen $ax \equiv 1 \pmod{m}$ er løsbar. Ved hjelp av det vi vet om slike likninger kan vi beskrive akkurat hvilke tall som har inverser:

Oppgave La a og m være heltall, med $m > 0$. Vis at a har invers modulo m hvis og bare hvis $a \perp m$. ♦

Løsning Tallene som er inverser til a er nøyaktig de som er løsninger av liknignen $ax \equiv 1 \pmod{m}$. Tidligere har vi sett at denne likningen har løsning hvis og bare hvis $\gcd(a, m) = 1$, altså hvis og bare hvis $a \perp m$. ♦

Det er lett å se at 0, og alle tall som er kongruente med 0, ikke kan ha noen invers. Men hvis modulusen er et primtall, har alle andre tall inverser. Dette skjer hvis og bare hvis modulusen er et primtall, som beskrevet i følgende oppgave.

Oppgave Vis at alle tall (unntatt de som er kongruente med 0) har invers modulo m hvis og bare hvis m er et primtall. ♦

Løsning Anta først at m er et primtall og a et tall slik at $a \not\equiv 0 \pmod{m}$. Da er $a \perp m$, og dermed vet vi at a har en invers modulo m.

Anta nå at m ikke er et primtall. Hvis $m = 1$, er alle tall kongruente med 0 modulo m, så det er ingenting å vise. Anta derfor at $m > 1$, så m er et sammensatt tall. Da finnes en divisor d av m slik at $1 < d < m$, og vi vet at at d ikke har invers modulo m. Altså finnes det minst ett tall som ikke er kongruent med 0 og som heller ikke har invers. ♦

Eksempel La oss finne alle inverser modulo 7. Vi vet fra tdligere at alle tall som ikke er kongruente med 0 har inverser. For å finne inversene kan vi prøve oss frem ved å gange sammen forskjellige tall, og observere at:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ 2 \cdot 4 &= 8 \equiv 1 \pmod{7} \\ 3 \cdot 5 &= 15 \equiv 1 \pmod{7} \\ 6 \cdot 6 &\equiv (-1) \cdot (-1) = 1 \pmod{7} \end{aligned}$$

Dermed kan vi lage følgende oversikt over inverser modulo 7:

a:	1	2	3	4	5	6
invers til a modulo 7:	1	4	5	2	3	6

♦

Modulær potensregning

Vi vil se på hvordan vi kan regne ut et uttrykk på formen

$$a^e \bmod m$$

når eksponenten e kan være veldig stor.

Eksempel Vi vil regne ut 3^{371} mod 5. Den åpenbare måten å gjøre det på er å først regne ut 3^{371}, og så dele på 5 og finne resten. Problemet er at 3^{371} er et veldig stort og uhåndterlig tall. Vi kan bruke kongruensregning til å gjøre utregningen på en smartere måte, der vi unngår å få store tall underveis.

Vi begynner med å se på noen lavere potenser av 3 redusert modulo 5:

$$\begin{aligned} 3^2 &= 9 \equiv 4 \pmod 5 \\ 3^3 &= 3^2 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod 5 \\ 3^4 &= 3^3 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 1 \pmod 5 \end{aligned}$$

Legg merke til at når vi først vet at 3^2 er kongruent med 4, så kan vi regne ut 3^3 som $4 \cdot 3$. Og når vi vet at 3^3 er kongruent med 2, så kan vi regne ut 3^4 som $2 \cdot 3$. Slik klarer vi å hele tiden holde oss til små tall.

Legg også merke til det vi fant på den siste linjen: $3^4 \equiv 1 \pmod 5$. Der hadde vi kjempeflaks, for nå kan vi enkelt regne ut så store potenser av 3 som vi vil modulo 5. Vi ville regne ut 3^{371} mod 5. Vi får:

$$3^{371} = 3^{92 \cdot 4 + 3} = (3^4)^{92} \cdot 3^3 \equiv 1^{92} \cdot 2 = 2 \pmod 5$$

Altså har vi 3^{371} mod $5 = 2$. ♦

I dette eksempelet hadde vi flaks og fikk at 3^4 var kongruent med 1, slik at vi umiddelbart kunne se bort fra alle potenser av 3^4, eller med andre ord alle multipler av 4 i eksponenten.

Vi kan imidlertid ikke regne med å ha like mye flaks alltid. Hvis vi ikke satser på et lykketreff, er det en bedre strategi å regne ut

$$a^2,\ a^4,\ a^8,\ a^{16},\ a^{32},\ \ldots$$

modulo m, og så finne a^e mod m ved å kombinere disse. Det neste eksempelet viser denne fremgangsmåten.

Eksempel Vi vil regne ut 5^{22} mod 77. Vi begynner med å regne ut 5 opphøyd i toerpotensene 2, 4, 8 og 16:

$$\begin{aligned} 5^2 &= 25 \\ 5^4 &= 5^2 \cdot 5^2 = 25 \cdot 25 \equiv 9 \pmod{77} \\ 5^8 &= 5^4 \cdot 5^4 \equiv 9 \cdot 9 \equiv 4 \pmod{77} \\ 5^{16} &= 5^8 \cdot 5^8 \equiv 4 \cdot 4 = 16 \pmod{77} \end{aligned}$$

Vi kan skrive eksponenten 22 som en sum av toerpotenser slik:

$$22 = 16 + 4 + 2$$

Dermed har vi:

$$5^{22} = 5^{16+4+2} = 5^{16} \cdot 5^4 \cdot 5^2 \equiv 16 \cdot 9 \cdot 25 \equiv 58 \pmod{77}$$

Dette vil si at 5^{22} mod $77 = 58$. ♦

Denne fremgangsmåten baserer seg på at vi alltid kan skrive et naturlig tall e som en sum av toerpotenser. Dette tilsvarer å skrive tallet e i *totallssystemet*, eller som *binærtall*.

I titallssystemet, som vi bruker til vanlig, står hvert siffer for en tierpotens:

$$1387_{10} = 1 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$$

I totallssystemet står hvert siffer for en toerpotens. Da trenger vi bare sifrene 0 og 1:

$$10110_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 22$$

Hvordan kan vi skrive et tall e i totallssystemet? Merk at siste siffer må være 0 hvis e er et partall, og 1 hvis det er et oddetall. Vi kan dele e på 2 med heltallsdivisjon og få:

$$e = q \cdot 2 + r \qquad 0 \leqslant r < 2$$

La $d_s, d_{s-1}, \ldots, d_2, d_1, d_0$ være sifrene til e i totallssystemet. Da har vi:

$$e = (\underbrace{d_s\ d_{s-1}\ \cdots\ d_2\ d_1}_{q}\ \underbrace{d_0}_{r})_2$$

Altså: Det siste sifferet er e mod 2. De øvrige sifrene er lik sifrene for tallet $q = \frac{e-(e \bmod 2)}{2}$.

Eksempel Vi vil skrive tallet 83 i totallssystemet. Vi har:

$$\begin{aligned} 83 &= 41 \cdot 2 + 1 & 5 &= 2 \cdot 2 + 1 \\ 41 &= 20 \cdot 2 + 1 & 2 &= 1 \cdot 2 + 0 \\ 20 &= 10 \cdot 2 + 0 & 1 &= 0 \cdot 2 + 1 \\ 10 &= 5 \cdot 2 + 0 \end{aligned}$$

Fra den første linjen ser vi at siste siffer i 83 er 1, og alle sifrene unntatt det siste er sifrene for 41. Neste linje gir oss at siste siffer i 41 skal være 1, og at alle unntatt det siste er sifrene for 20. Så får vi at siste siffer i 20 er 0, og så videre. Totalt får vi:

$$83_{10} = 1010011_2$$ ♦

Eksempel Vi regner ut 36^{83} mod 125. Vi begynner med å opphøye 36 i toerpotenser og redusere modulo 125 (alle kongruensene er modulo 125):

$$\begin{aligned} 36^1 &= 36 & 36^{16} &\equiv 81^2 = 6561 \equiv 61 \\ 36^2 &= 1296 \equiv 46 & 36^{32} &\equiv 61^2 = 3721 \equiv 96 \\ 36^4 &\equiv 46^2 = 2116 \equiv 116 & 36^{64} &\equiv 96^2 = 9216 \equiv 91 \\ 36^8 &\equiv 116^2 = 13456 \equiv 81 \end{aligned}$$

Vi vet fra forrige eksempel at

$$83_{10} = 1010011_2 = 64 + 16 + 2 + 1,$$

og dermed får vi:

$$\begin{aligned} 36^{83} &= 36^{64+16+2+1} = 36^{64} \cdot 36^{16} \cdot 36^2 \cdot 36^1 \\ &\equiv 91 \cdot 61 \cdot 46 \cdot 36 \equiv 81 \pmod{125} \end{aligned}$$

Dette betyr at $36^{83} \bmod 125 = 81$. ♦

Fermats lille teorem

I første eksempel over så vi at $3^4 \bmod 5 = 1$. Ved å regne litt, kan vi også se at vi for eksempel har $6^{16} \bmod 17 = 1$, og $4^{28} \bmod 29 = 1$. Faktisk er det slik at hvis vi tar et hvilket som helst tall a, og regner ut $a^{p-1} \bmod p$, der p er et primtall, så får vi 1 som svar. (Det eneste unntaket er hvis vi starter med et tall a som er kongruent med 0 modulo p, da får vi selvfølgelig 0.)

Dette resultatet ble oppdaget av Pierre de Fermat, og det er derfor oppkalt etter ham. For å skille det fra det kjente *Fermats siste teorem*, kalles dette teoremet vanligvis *Fermats lille teorem*:

La p være et primtall, og a et heltall slik at $p \nmid a$. Da er

$$a^{p-1} \equiv 1 \pmod{p}.$$

Hvorfor stemmer dette? Se på tallene

$$0 \cdot a, \quad 1 \cdot a, \quad 2 \cdot a, \quad \ldots, \quad (p-1) \cdot a.$$

Vi begynner med å observere at ingen av disse er kongruente med hverandre modulo p. For hvis vi har $i \cdot a \equiv j \cdot a \pmod{p}$, så får vi også $i \equiv j \pmod{p}$ fordi p er et primtall. Og når både i og j er hentet fra mengden $\{0, 1, \ldots, (p-1)\}$, betyr det at $i = j$.

Så vi har altså listen $0 \cdot a$, $1 \cdot a$, $\ldots$, $(p-1) \cdot a$ med p ulike tall, og vi vet at ingen av dem er kongruente med hverandre modulo p. Men hvert av dem må jo være kongruent modulo p med et av tallene

$$0, \quad 1, \quad 2, \quad \ldots, \quad (p-1).$$

Det at ingen av de p tallene våre er kongruente med hverandre, gjør at nøyaktig ett av dem må være kongruent med 0, ett med 1, ett med 2, og så videre. Når vi ser på alle tallene $0 \cdot a$, $1 \cdot a$, $\ldots$, $(p-1) \cdot a$, er de altså kongruente med tallene 0, 1, $\ldots$, $(p-1)$, i en eller annen rekkefølge.

Ved å ta produktet av alle tallene i hver av disse listene (unntatt 0), får vi dermed kongruensen

$$(1 \cdot a) \cdot (2 \cdot a) \cdots ((p-1) \cdot a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

Uttrykket på høyre side av kongruensen er lik $(p-1)!$, og det på venstre side er lik $(p-1)! \cdot a^{p-1}$, og vi har altså:

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Siden $p \nmid (p-1)!$ kan vi forkorte bort $(p-1)!$ fra begge sider av kongruensen. Da får vi

$$a^{p-1} \equiv 1 \pmod{p},$$

som var det vi ville vise.

Ved hjelp av Fermats lille teorem kan vi lett regne ut potenser modulo primtall.

Eksempel Vi regner ut 6^{195} mod 17. Fra Fermats lille teorem vet vi at $6^{16} \equiv 1 \pmod{17}$, siden 17 er et primtall. Da får vi:

$$\begin{aligned} 6^{195} &= 6^{12 \cdot 16 + 3} = (6^{16})^{12} \cdot 6^3 \\ &\equiv 1^{12} \cdot 6^3 = 216 \equiv 12 \pmod{17} \end{aligned}$$

Dermed har vi $6^{195} \bmod 17 = 12$. ♦