Talteori og Euklid

Talteori er grundlæggende studiet af de naturlige tal:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ...

I denne note vil vi i afsnit 1 beskæftige os med begrebet divisor, herunder begrebet største fælles divisor. I afsnit 2 vil vi beskæftige os med primtallene, som er en særlig gruppe af naturlige tal.

1. Største fælles divisor og Euklids algoritme

Går 6 op i 12? Du vil formentlig svare ja på dette spørgsmål og begrunde dit svar med, at 6 går 2 gange op i 12. Vi vil nu se en formel definition af, hvad det betyder, at et tal går op i et andet tal.

Definition 1
Vi siger, at et helt tal a går op i eller er en divisor i et andet helt tal b, hvis der findes et helt tal q, så

$$b = q \cdot a.$$

For eksempel går 6 op i 12, fordi vi kan vælge $q = 2$ og så er

$$12 = q \cdot 6.$$

Vi vil nu se nærmere på begrebet største fælles divisor.

Definition 2
Lad a og b være hele tal, som ikke begge er lig 0. Det største naturlige tal, der er en divisor i både a og b, kaldes deres *største fælles divisor* og betegnes sfd(a,b).
Tallene a og b kaldes *indbyrdes primiske*, hvis sfd(a,b)=1.

For eksempel er sfd(30,21)=3, fordi 3 er det største tal, som går op i både 30 og 21.
Derimod er sfd(8, 21)=1, fordi 1 er det største tal, som går op i både 8 og 21. Vi siger derfor, at 8 og 21 er indbyrdes primiske.

For store tal er det svært umiddelbart at bestemme deres største fælles divisor, men Euklid præsenterer i bog VII af *Elementerne* en metode til effektivt til at bestemme den største fælles divisor for to tal. Metoden gennemgås nedenfor ved hjælp af et eksempel.

Eksempel (Euklids algoritme)
I dette eksempel anvendes Euklids algoritme til at bestemme den største fælles divisor for tallene 30 og 21. I metoden laves gentagne divisioner med rest. Vi deler metoden op i en række trin:

1. Start med at dividere det største tal med det mindste tal. I dette tilfælde skal vi dividere 30 med 21. Tallet 21 kan gå 1 gang op i 30, og så er der en rest på 9 tilbage. Dette kan vi skrive på nedenstående måde:

$$30 = 21 \cdot 1 + 9$$

2. Vi skal nu dividere 21 med resten 9 fra før. Tallet 9 kan gå 2 gange op i 21, og så er der en rest på 3 tilbage. Dette kan vi skrive på nedenstående måde:

$$21 = 9 \cdot 2 + 3$$

3. Vi skal nu dividere 9 med resten 3 fra før. Tallet 3 går 3 gange op i 9, og der er ingen rest. Dette kan vi skrive på nedenstående måde:

$$9 = 3 \cdot 3 + 0$$

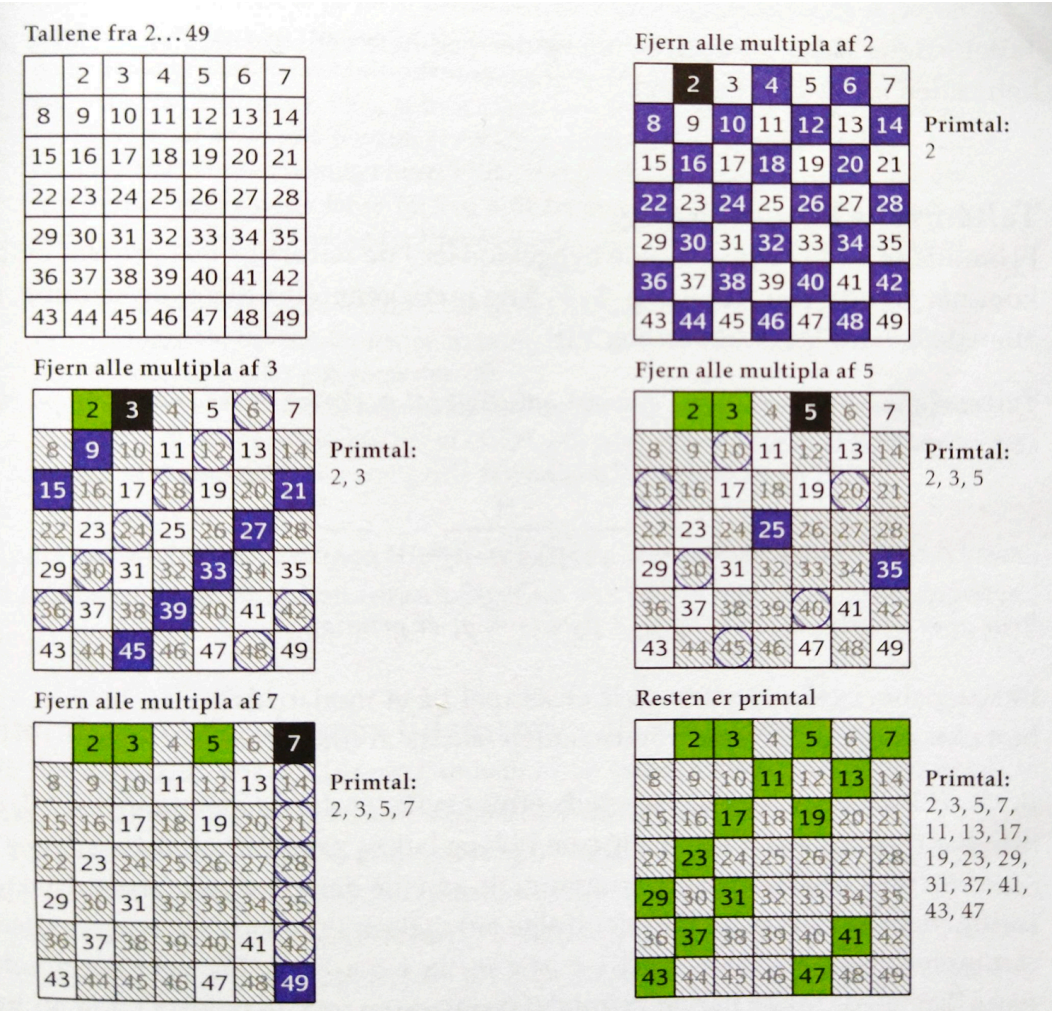
4. Vi forsætter på denne måde, indtil der ikke længere er en rest. I dette tilfælde stopper vi derfor ved trin 3. Den største fælles divisor er den sidste rest, vi har fået. I dette tilfælde er dette 3. Vi kan altså konkludere, at sfd(30,21)=3.

2. Primtal

Vi starter med en definition af, hvad et primtal er.

Definition (primtal):
Et naturligt tal større end 1 kaldes et primtal, hvis det ikke kan deles af andre tal end 1 og tallet selv.

Eksempler på primtal er 2, 3, 5 og 7. Matematikeren Eratosthenes[1] har udviklet en metode kaldet 'Eratosthenes si' til at finde primtal. I metoden sier man alle andre tal end primtallene bort. Man starter således med at skrive alle tal op, som er større end eller lig 2. Dernæst markerer man det mindste tal 2 og sier alle andre tal bort, som 2 går op. Dernæst markerer man det mindste tilbageværende tal 3 og sier alle andre tal bort, som 3 går op i. Sådan fortsættes indtil man kun har primtallene tilbage.



Figur 1. Trinene i Erathostenes' si anvendt på tallene 2-49.
Kilde: Figur 4 (s. 59) fra bogen Matematiske mysterier.

[1] Matematikeren Eratosthenes (født omkring 280 f.v.t) er uddannet ved museet i Alexandria og har muligvis haft Euklid som lærer.

Primtallene er de fundamentale byggeklodser i de naturlige tals verden, idet ethvert naturligt tal større end 1 kan skrives som et produkt af primtal. F.eks. er $18 = 2 \cdot 3 \cdot 3$ og $15 = 3 \cdot 5$. Når vi har opskrevet et naturligt tal, som et produkt af primtal, siger vi, at vi har *primtalsfaktoriseret* tallet. Når vi har primtalsfaktoriseret et tal, er det ikke muligt at finde andre primtalsfaktoriseringer. F.eks. er det ikke muligt at opskrive 18 som et produkt af primtal på andre måder, end vi allerede har gjort ($18 = 2 \cdot 3 \cdot 3$). Opsummerende kan vi altså sige, at ethvert naturligt tal større end 1kan primtalsfaktoriseres på en entydig måde. Dette er netop, hvad nedenstående sætning fra Euklids bog VII udtrykker på en generel måde.

Talteoriens hovedsætning
Ethvert naturligt tal n større end 1 kan på én og kun én måde faktoriseres i et produkt af primtal:

$$n = \underbrace{p_1 \cdot \ldots \cdot p_1}_{a_1} \cdot \underbrace{p_2 \cdot \ldots \cdot p_2}_{a_2} \cdot \ldots \cdot \underbrace{p_k \cdot \ldots \cdot p_k}_{a_k}$$

hvor a'erne er positive hele tal, og $p_1 < p_2 < \cdots < p_k$ er primtal.

I eksemplet med $18 = 2 \cdot 3 \cdot 3$ er $p_1 = 2$ og $p_2 = 3$. Da $p_1 = 2$ optræder 1 gang i faktoriseringen er $a_1 = 1$, og da $p_2 = 3$ optræder 2 gang i faktoriseringen er $a_2 = 2$.

Bemærk, at talteoriens hovedsætning både består af en eksistensdel og en entydighedsdel. Eksistensdelen siger, at der eksisterer en primtalsfaktorisering for ethvert naturligt tal større end 1, mens entydighedsdelen siger, at der kun findes én primtaltsfaktorisering for hvert naturligt tal større end 1.

Bevis for talteoriens hovedsætning:
Vi vil her kun bevise eksistensdelen. Et bevis for entydighedsdelen kan findes i bogen *Tal og Mængder* af Johan P. Hansen.

Eksistensdel:
Beviset for eksistensdelen er et såkaldt modstridsbevis. I et modstridsbevis antager man det modsatte af, hvad man vil vise, og målet er så at nå frem til en modstrid (noget vrøvl), fordi man så kan konkludere, at den oprindelige antagelse var forkert.

Vi antager således, at der findes naturlige tal større end 1, som ikke har en primtalsfaktorisering. Vi vælger det mindste af sådanne tal og kalder dette tal n.
Tallet n er ikke et primtal, fordi ellers havde n jo en primtalsfaktorisering med kun én faktor, $n = p$.
Da n ikke er et primtal, så findes der et naturligt tal d, som er forskelligt fra 1 og n, og som er en divisor i n. Da d er en divisor i n, findes jf. definition 1 et naturligt tal q, så

$$n = d \cdot q,$$

hvor $1 < q < n$.

Vi husker, at n er det mindste tal, som ikke har en primtalsfaktorisering, og da både $1 < d < n$ og $1 < q < n$, så må både d og q en primtalsfaktorisering. Samler vi nu primtalsfaktoriseringerne af d og q til et samlet produkt, så har vi en primtalsfaktorisering af n, hvilket er i modstrid med vores oprindelige antagelse. Derfor må vores antagelse være forkert, og vi kan konkludere, at der ikke findes naturlige tal større end 1 uden en primtalsfaktorisering, hvilket afslutter beviset.

Talteoriens hovedsætning kan anvendes til at bevise, at der findes uendeligt mange primtal, og dette gjorde Euklid i Bog IX af Elementerne. Nedenfor findes Euklids bevis (dog skrevet med en moderne notation).

Sætning
Der findes uendeligt mange primtal.

Uendelighedsbegrebet i sætningen skal forstås på den måde, at det altid er muligt at finde flere primtal end ethvert forelagt antal primtal.

Bevis:
Lad $p_1, p_2, \ldots, p_k$ være primtal. Betragt tallet

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1.$$

Hvis vi dividerer n med p_1, vil vi få en rest på 1. Vi kan dermed konkludere, at p_1 ikke går op i n. Med et helt tilsvarende argument kan vi konkludere, at $p_2, \ldots, p_k$ ikke går op i n.
Vi ved dog, at n har en primtalsfaktorisering jf. talteoriens hovedsætning, og alle primtallene i denne faktorisering vil gå op i n. Da $p_1, p_2, \ldots, p_k$ ikke går op i n, og primtallene i faktoriseringen går op i n, så må sidstenævnte primtal være andre primtal end $p_1, p_2, \ldots, p_k$. Heraf følger, at der må være uendeligt mange primtal.

Kilder

Denne note er en sammenskrivning af følgende to kilder:

Hansen, J. P. (2012). *Tal og Mængder: Begreber, metoder og resultater*. Aarhus Universitetsforlag.

Hansen, J. P. (2013). Primtalsmysterier. I: H. A. Salomonsen (Red.), *Matematiske mysterier: Historien, forklaringerne og løsningerne* (s. 55-75). Aarhus Universitetsforlag.