Talteori og matematikhistorie - matematiske ideer

Matematik og tal

Matematik adskiller sig fra andre videnskaber idet man i stedet for at ekstrahere viden fra fænomener oplevet igennem ens sanser, i stedet forsøger at arbejde udelukkende indenfor en 'konsistent' og menneskeligt konstrueret verden. I fysik opstiller man love der stemmer overens med verden vi oplever, og forbedre eller finder flere love, når vi mener vi har opnået en dybere eller ny forståelse for hvordan verden omkring os kan beskrives. I matematik er dette ikke tilfældet. I stedet opstiller vi nogle grundregler som vi mener skal være gyldige indenfor vores system, kaldet aksiomer, og ud fra disse og grundlæggende 'logik', kommer matematik som vi kender det til livs.

Disse aksiomer eller grundregler har dog igennem tiden ændret sig, idet de enten ikke har givet mulighed for at vise nok sætninger, eller fordi matematik som helhed har skulle kunne forskellige ting i forskellige tidsaldre. I dette forløb skal vi ikke som udgangspunkt kigge på aksiomer, men i stedet på matematisk heuristik som helhed og prøve at se på hvordan matematik har ændret sig fra græske traditioner, til matematik i dag.

Fokus her er på to forskellige typer af tal: **primtal** og **perfekte tal**. Matematikhistorisk betragtet er begge taltyper interessante. Primtallene og de perfekte tal beskrives begge første gang i et matematisk værk skrevet 300 år f.Kr. nemlig i Euklids Elementer, som omtales flere gange i denne note. Der er matematikhistoriske indikationer af, at pythagoræerne også kendte til ideen om primtal, men der mangler tekstmateriale der direkte bekræfter det. Matematikere der arbejder med talteori søger stadig efter nye primtal og perfekte tal. Primtal har en central rolle i krypteringsteknologi, hvilket vi vender tilbage til senere. For at finde primtal benyttes i dag moderne computerteknologi, så her er der også en markant matematikhistorisk udvikling, i den måde man arbejder med matematik på. Perfekte tal har i dag en mere teoretisk betydning i matematik.

Vi følger udviklingen i matematik ved at betragte talteori. For at følge en matematikhistorisk udvikling, ser vi på hvordan både Euklid i hans store værk Elementer arbejdede med tallene på hvordan vi arbejder med tallene i dag. Vi kan også inddrage hvordan Euler, en af matematikkens største skikkelser, i 1700 tallet, beviste en sætning, der havde været et åbent problem i næsten 1000 år. Igennem disse eksempler får vi et indblik i den skiftende heuristik i matematik. Vi vil se hvordan både måden man definerer matematiske objekter på ændrer sig, og vi ser hvordan bevisførelsen bliver anderledes. På den måde blive vi klogere på, hvorfor vi i dag udfører matematik på den måde, vi gør det.

I gymnasiet arbejder vi stort set altid over den helt særlige struktur $\mathbb{R}$, eller de såkaldte reelle tal. Noget mange af jer nok vil tænke på som tallinjen. Dette er en naturlig struktur at arbejde over, da den har en masse prisværdige egenskaber. Vi kigger også på nogle særlige objekter nemlig funktioner, der fører elementer fra en mængde over i en anden og opfylder en særlig regel. Her giver det ofte mening at lade vores funktion f fører elementer fra $\mathbb{R}$ over i $\mathbb{R}$, da vi ønsker at f skal beskrive en handling over tid.

I dette forløb vil vi dog bevæge os væk fra $\mathbb{R}$ og i stedet betragte nogle mængder vi måske i større grad er bekendte med fra folkeskolen end gymnasiet, nemlig de naturlige tal, vi undervejs vil skrive som $\mathbb{N}$, og blot er, som skrevet før, $1, 2, 3, \ldots$. Udover det vil vi kigge på de hele tal, vi vil skrive som $\mathbb{Z}$ og som er mængden af $\ldots, -2, -1, 0, 1, 2, \ldots$, altså de naturlige tal, sammen med 0 og de negative naturlige tal. Der vil stadigvæk optræde funktioner, men disse vil tage input i $\mathbb{N}$, og også give et output i $\mathbb{N}$, så derfor måske være noget anderledes end hvad I er vant til. Alt dette for at sige at vi er på vej ind i en helt anden verden, talteorien.

Opgaver

Hvordan adskiller $\mathbb{R}$ sig fra $\mathbb{N}$ og $\mathbb{Z}$? (Er der ting vi kan gøre i de reelle tal vi ikke på samme måde er i stand til i nogle af de andre mængder?)

Primtal

a) Hvordan definerer man et primtal?
b) Bestem alle primtal fra 2 til 50.

Sammensatte tal

Et tal der er større end 1 og som ikke er et primtal betegnes et sammensat tal. Giv eksempler på sammensatte tal.

Sammensatte tal og primtal

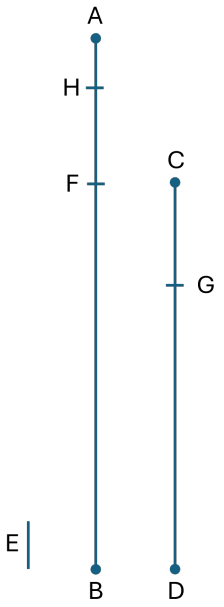
Betragt de primtal der blev bestemt tidligere, og betragt nogle af de sammensatte tal. Undersøg hvordan man kan bruge primtal til at "sammensætte"et sammensat tal.

Beviser i Euklids Elementer

Vi skal senere se nærmere på en sætning og et bevis, muligvis ser vi på flere, som er skrevet af Euklid. Læs nedenstående sætning og bevis, som er det, vi vil se nærmere på. Hvad genkender du? Hvad forekommer besynderligt? Hvad drejer beviset sig om? Dette er et modstridsbevis. Kan du gennemskue, hvorfor man kalder det et modstridsbevis? Et bestemt ord afslører det, hvis man ser godt efter.

Sætning (Elementer, Bog VII, Proposition 1 I)**. Når der foreligger to ulige store tal, og det mindre til stadighed trækkes fra det større, og hvis det resterende på intet tidspunkt måler det umiddelbart foregående tal, indtil resten er en ener, så vil de oprindelige tal være indbyrdes primiske.**
Hvis der fra de to tal AB og CD til stadighed trækkes det mindre fra det større, så lad det resterende tal på intet tidspunkt måle det umiddelbart foregående, indtil resten er en ener. Jeg påstår, at AB og CD er indbyrdes primiske, dvs. at kun en ener måler AB og CD.

Bevis. For hvis tallene AB og CD ikke er indbyrdes primiske, vil et tal måle dem. Lad dette måle dem og lad det det være E; lad CD ved at måle BF give resten FA mindre end det selv, lad AF ved at måde DG give resten GC mindre end det selv, og lad GC ved at måle FH give eneren HA som rest.
Da nu E måler CD, og CD måler BF, måler E altså også BF; men det måler også hele BA, og altså vil det også måle resten, AF. Men AF måler DG; og E måler altså DG, men det måler også hele DC; og derfor vil det måle resten, CG. Men CG måler FH; og E måler altså FH; men det måler også hele FA. Og da det er et tal, vil det derfor måle resten, eneren AH; hvilket er umuligt.
Altså vil et eller andet tal ikke måle tallene AB og CD. AB og CD er altså indbyrdes primiske. Hvilket skulle bevises. □



Figur 1: Figur til beviset

1 Det nødvendige fundament

Før vi kan arbejde med de historiske kilder er vi nødsaget til at udvikle et vist talteoretisk fundament der gør os i stand til at forstå de nødvendige grundlæggende begreber. Først betragter vi en defintion, som I godt kender til, men måske ikke har set på denne form tidligere. Definitionen er nyttig at holde sig for øje, når man skal læse Euklids definitioner.

Divisibilitet

Definition 1.1. Lad a, b være hele positive tal, da siger vi at $a \mid b$ udtalt a deler b hvis der findes heltal k så

$$a \cdot k = b.$$

Vi siger, at a er *divisor* i b. Tallet k kaldes for kvotienten ved division af b med a.
Hvis der ikke findes et sådant k skriver vi $a \nmid b$ udtalt a deler ikke b.
Mængden af divisorer for b betegner vi med $D(b)$.

Vi starter med at se flere af Euklids definitioner fra bog VII.
Man skal besvare spørgsmål, der knytter sig til definitionerne. Det er vigtigt, at man forsøger at tænke geometrisk, fx i form af linjestykker, og samtidig kobler dette til vores moderne forståelse af tal. Derfor kan det være en god ide at tegne fx. linjestykker, når man læser teksten.

Gennemlæs de udvalgte definitioner fra bog VII skrevet nedenfor. Forsøg at oversætte definitionerne til matematik du kender til, i det du besvarer spørgsmålene. Inddrag tegninger i dine overvejelser.

- Hvordan skal VII.D1 og VII.D2 forstås?
  - Er en ener et tal?
- Hvad mener Euklid med "måle"i VII.D3?
- Hvad mener Euklid med "måles"i VII.D5? Skriv VII.D5 som en ligning med a, b og k, man må gerne indføre tal. Relater ligningen til VII.D3.
- Giver VII.D6 mening for dig?
- Kan du skrive VII.D7 med moderne matematik, og hvad tænker du om at Euklid skriver to udsagn?
- Skriv et taleksempel for VII.D8.
- Man skal forstå VII.D9 således, hvor a, b og c er tal: a måles af b med c. Skriv det som en ligning.
  - Forsøg evt. at erstatte bogstaverne med tal, da det kan være en hjælp.
- Skriv et taleksempel for VII.D10.
- Beskriv, hvordan du forstår VII.D11.
- Kan du fra VII.D12 forstå, hvad der menes med indbyrdes primiske tal?
- Vi ser senere nærmere på, hvad der menes med et sammensat tal. Så skal vi se på VII.D13 igen!
- Husker du, hvad der menes med proportional? Forklarer det sætningen i VII.D20?
- Har du nogen som helst ide om, hvordan man skal forstå VII.D22?

Euclid Elementer bog VII. Definitionerne.

VII.D1 En ener er det, ifølge enhver af de eksisterende ting kaldes en,

VII.D2 og et tal er den sammenlagte mængde af enere.

VII.D3 Et mindre tal er del af et større tal, når det måler det større,

VII.D5 Et større tal er et multiplum af et mindre, når det måles af det mindre.

VII.D6 Et lige tal er et, som kan halveres,

VII.D7 og et ulige tal er et, som ikke kan halveres, eller som adskiller sig fra et lige tal med en ener.

VII.D8 Et lige-gange-lige tal er et, som kan måles af et lige tal med et lige tal.

VII.D9 Et lige-gange-ulige tal er et, som måles af et lige tal med et ulige tal.

VII.D10 Et ulige-gange-ulige tal er er, som måles af et ulige tal med et ulige tal.

VII.D11 Et primtal er et, som kun måles af en ener.

VII.D12 Indbyrdes primiske tal er de, som kun måles af en ener som fælles mål.

VII.D13 Et sammensat tal er et som måles af et andet tal,

VII.D20 Tal er proportionale, når det første er samme multiplum - eller samme del eller samme dele - af det andet, som det tredje er af det fjerde.

VII.D22 Et fuldkomment tal er det, som er lig med sine dele.

1.1 Divisorer og største fælles divisor

Lad os prøve at forstå Definition 1.1 bedre vha. eksempler. Lad for eksempel $a = 2$ og $b = 36$, da ser vi, at $2|36$, fordi der findes et helt tal $k = 18$, så $2 \cdot 18 = 36$. Altså er $D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

Opgaver

a) Bekræft ved egne overvejelser at $D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ og bestem $D(12)$ og $D(42)$.
b) Undersøg hvorvidt $15|225$, $22|356$, $17|357$.

Talteori og Nspire. Brug de nedenstående kommandoer i Nspire, og afgør, hvad kommandoerne giver som output.

- intDiv(8,2)
- mod(8,2)
- intDiv(45,5)
- mod(45,5)
- `delVoid(seq(when(mod(12,i)=0,i,_), i, 1, 12))`
- `delVoid(seq(when(mod(48,i)=0,i,_), i, 1, 48))`

Fra en af de tidligere opgaver, kan man se, at to hele tal kan have fælles divisorer. Dette betegnes også med en mængde, og det betegnes for tallene a og b som $D(a,b)$. Det gælder at $D(8,4) = D(4,8) = \{1,2,4\}$.

Opgaver

a) Bestem uden brug af Nspire $D(6,21)$.
b) Bestem uden brug af Nspire $D(12,36)$

Operatoren $|$ giver anledning til et meget vigtigt begreb indenfor talteori, nemlig den såkaldte største fælles divisor. Den gør det senere også muligt at for os, at definere de perfekte tal. Først ser vi nærmere på den største fælles divisor, og senere vender vi tilbage til de perfekte tal.

Største fælles divisor

Definition 1.2. Hvis a, b er naturlige tal, kaldes det største tal d der deler dem begge for den største fælles divisor, vi skriver dette som $\text{sfd}(a,b) = d$

Udfordring - største fælles divisor

Brug uden brug af Nspire din viden om divisorer til at afgøre, om alle nedenstående udsagn er korrekte.

- $\text{sfd}(10,35) = 5$
- $\text{sfd}(57,34) = 17$
- $\text{sfd}(8,18) = 3$
- $\text{sfd}(8,12) = 4$
- $\text{sfd}(10,85) = 10$
- $\text{sfd}(15,56) = 1$
- $\text{sfd}(18,117) = 9$

1.1.1 Sætninger om divisibilitet

Først ser vi på denne sætning, som vi ikke beviser. Forsøg med taleksempler at sandsynliggøre, at sætningen er korrekt. Det er naturligvis *ikke* en stringent måde at arbejde på i matematik.

Sætning 1.3.

a) Hvis $a \mid b$ og $b \mid c$ da vil $a \mid c$
b) Hvis $a \mid b$ og $c \mid d$ da vil $ac \mid bd$
c) Hvis $m \neq 0$ da vil $a \mid b$ hvis og kun hvis $ma \mid mb$
d) Hvis $d \mid a$ og $a \neq 0$ da vil $|d| \leq |a|$

Opgave

Undersøg ved at bruge konkrete taleksempler de to første udsagn i Sætning 1.3.

Vi viser tre sætninger, som vi får brug for senere. Først skal du tænke intuitive på følgende:
Du har to forskellige tal, som vi lige nu kalder for a og b. Begge tal har en divisor d. Kan du tegne dig frem til, at d også er divisor til $a+b$? Kan du gøre det samme for $a-b$?

Regneregler for divisibilitet

Sætning 1.4. Lad $d \mid a$ og lad $d \mid b$. Da gælder det at $d \mid (a+b)$.

Bevis. Da $d \mid a$ og $d \mid b$ eksisterer der hele tal k og l så $a = kd$ og $b = ld$.
Da gælder det at

$$a + b = kd + ld = d(k + l)$$

og da $k + l$ er et helt tal følger det heraf, at $d \mid (a+b)$. □

Sætning 1.5. Lad $d \mid a$ og lad $d \mid b$. Da gælder det at $d \mid (a-b)$.

Bevis. Da $d \mid a$ og $d \mid b$ eksisterer der hele tal k og l så $a = kd$ og $b = ld$.
Da gælder det at

$$a - b = kd - ld = d(k - l)$$

og da $k - l$ er et helt tal følger det heraf, at $d \mid (a-b)$. □

Sætning 1.6. Lad $d \mid a$ da gælder for at helt tal b at $d \mid (ab)$.

Bevis. Da $d \mid a$ eksisterer der et helt tal k så $a = kd$.
Da gælder det at

$$ab = (dk)b = d(kb)$$

og da kb er et helt tal følger det heraf, at $d \mid (ab)$. □

Euklids algoritme

I dag har vi computere, der nemt kan bestemme den største fælles divisor sfd(a, b). Bag skærmen og tastaturet bruger computere algoritmer. En algoritme er en trinvis metode til at løse et bestemt problem. Når man for eksempel lægger store tal sammen eller ganger med opstilling, følger man en fast række trin. Det er et eksempel på en algoritme. Euklids algoritme bygger netop på en sådan fremgangsmåde og bruges til at bestemme den største fælles divisor for to tal. I *Elementer* er Sætning 1 i Bog VII, som vi læste tidligere, et eksempel på en algoritmisk fremgangsmåde, og den er tæt knyttet til den metode, der i dag kaldes Euklids algoritme. Vi skal se nærmere på denne algoritme, og vi skal prøve at bruge den, så vi kan bestemme største fælles divisor.

Division med rest

Hvad menes der med division med rest?

Talteori og Nspire. Brug de nedenstående kommandoer i Nspire, og afgør, hvad kommandoerne giver som output.

- intDiv(9,2)
- mod(9,2)
- intDiv(49,5)
- mod(49,5)

Brug dit output fra Nspire til at forklare nedenstående, hvor det skal forklares, hvad der menes med en rest.

- $\frac{9}{2}$ og $9 = 4 \cdot 2 + 1$
- $\frac{49}{5}$ og $49 = 7 \cdot 5 + 4$
- $\frac{b}{a}$ og $b = k \cdot a + r$

Division med rest

Lad a, b være positive hele tal. Da findes der entydigt bestemte heltal k og r, så

$$b = k \cdot a + r, \qquad 0 \leq r < a.$$

Hvis $a \nmid b$, er $r > 0$, og hvis $a \mid b$, er $r = 0$.

Nu kan vi forstå den notation, der benyttes ved Euklids algoritme til at bestemmes største fælles divisor sfd(a, b) for de to naturlige tal $a \geq b$.

Euclids algoritme

For at bestemme sfd(a, b), hvor det her antages at $a \geq b$, benyttes nedenstående algoritme. Først bruges division med rest på parret a, b.

$$a = k_0 \cdot b + r_0, \quad \text{hvor} \quad 0 \leq r_0 < b$$

Hvis $r_0 = 0$ stopper vi. Ellers bruges division med rest på parret b, r_0:

$$b = k_1 \cdot r_0 + r_1, \quad \text{hvor} \quad 0 \leq r_1 < r_0$$

Sådan fortsættes indtil resten bliver 0:

$$\begin{aligned} r_0 &= k_2 \cdot r_1 + r_2, \quad \text{hvor} \quad 0 \leq r_2 < r_1 \\ r_1 &= k_3 \cdot r_2 + r_3, \quad \text{hvor} \quad 0 \leq r_3 < r_2 \\ r_2 &= k_4 \cdot r_3 + r_4, \quad \text{hvor} \quad 0 \leq r_4 < r_3 \\ &\vdots \\ r_n &= k_{n+2} \cdot r_{n+1} + 0 \end{aligned}$$

Her skal man lægge mærke til, hvornår algoritmen *afsluttes*, nemlig når der er en rest på 0. Det sker efter et endeligt antal trin, da der kun kan være endeligt mange tal i rækken af rester.
Det tal vi bestemmer ved Euklids algoritme er den største fælles divisor sfd$(a, b) = r_{n+1}$.

Eksempel på Euklids algoritme

Bestem sfd$(252, 198)$ ved brug af Euklids algoritme.
$252 = 1 \cdot 198 + 54$
$198 = 3 \cdot 54 + 36$
$36 = 2 \cdot 18 + 0$
Dermed er det bestemt at sfd$(252, 198) = 18$

Sætning 1.7. Den sidste positive rest r_{n+1} i Euklids algoritme for to naturlige tal $a \geq b$ er deres største fælles divisor. Altså sfd$(a, b) = r_{n+1}$

Euklids algoritme - opgaver

Bestem ved at bruge Euklids algoritme sfd$(124, 28)$, sfd$(1001, 715)$ og sfd$(544, 119)$.

Metoden er effektiv til at bestemme største fælles divisor for meget større tal, hvor det er meget vanskeligt at undersøge svaret ved at prøve sig frem. Det kan eksempelvis være sfd$(105063, 67578)$. Ved brug af algoritmen kan man med syv trin bestemme sfd$(105063, 67578) = 21$.

1.1.2 Ræsonnement for Euklids algoritme - taleksempel

Med et taleksempel og Sætning 1.4, Sætning 1.5 og Sætning 1.6 kan vi ræsonnere os frem til algoritmen. Lad os bestemme sfd$(84, 30)$. Vi starter med division med rest af 84 med 30, hvilket giver os:

$$84 = 2 \cdot 30 + 24$$

Nu kommer et centralt argument.
Fra Sætning 1.6 ved vi, at hvis d deler 30 så deler d også $2 \cdot 30$.
Fra Sætning 1.5 følger derfor, at hvis d deler både 84 og 30, så deler d også $84 - 2 \cdot 30 = 24$.
Så hvis et tal deler 84 og 30, så deler det også 24.
Derfor er enhver fælles divisor for 84 og 30 også en fælles divisor for 30 og 24.
Algoritmen fortsætter. Vi bruger igen division med rest. Denne gang på parret 30,24:

$$30 = 1 \cdot 24 + 6$$

Da $30 - 24 = 6$, vil enhver fælles divisor for 30 og 24 også dele 6 (Sætning 1.5).

Algoritmen fortsætter. Vi bruger igen division med rest. Denne gang på parret 24,6:

$$24 = 4 \cdot 6 + 0$$

Resten er 0, og vi stopper, og derfor er sfd$(24, 6) = 6$.

Betragt nu algoritmen bagfra.
Omvendt gælder det også, at 6 deler 6 og 24, da vi har

$$24 = 4 \cdot 6$$

Ved brug af Sætning 1.4 gælder derfor, at 6 også deler 30 da

$$6 + 24 = 30$$

Da 6 deler 24, følger det igen ved Sætning 1.4 og Sætning 1.6, at 6 deler

$$24 + 2 \cdot 30 = 84$$

Altså deler 6 både 84 og 30.

Vi har altså vist, at hvis et tal deler både 84 og 30, så deler det også 6. Derfor kan ingen fælles divisor for 84 og 30 være større end 6.
Omvendt har vi set, at 6 selv deler både 84 og 30. Altså er sfd$(84, 30) = 6$.

Taleksemplet illustrerer det ræsonnement, som i almindelighed ligger bag Euklids algoritme, og som formuleres i Sætning 1.7.