TALTEORI

x-klasserne
Gammel Hellerup Gymnasium

November 2023 ; Michael Szymanski ; mz@ghg.dk

Indholdsfortegnelse

FORORD

Talteori er ofte meget abstrakt og træner hjernen til at tænke skarpt, og disse noter er ikke skrevet med henblik på anvendelser i den fysiske verden, men med underholdning for øje. Tallene undersøges for deres egen skyld.

Som filosoffen Immanuel Kant engang skrev, skal man handle, så mennesket aldrig opfattes som middel, men som mål i sig selv. Og denne tekst behandler altså i denne henseende tallene, som mennesker bør behandles.

Når du læser beviser for sætninger, er det vigtigt, at du IKKE ønsker at blive overbevist om en sætnings rigtighed. Overvej selv hvorfor!

INDLEDNING

En af verdenshistoriens helt store begavelser Carl Friedrich Gauss (1777-1855) skrev: *Matematik er dronningen af alle videnskaber, og talteori er matematikkens dronning*. Pythagoras (ca. 580 fvt. – ca. 500) og hans skole er kendt for sætningen: *Alt er tal*. Som ukritisk menneske må man naturligvis tage sådanne udtalelser fra så store autoriteter for gode varer.

Talteori handler grundlæggende om at forstå og finde nye egenskaber for tal. Da tal er en ikke uvæsentlig del af matematik, er det ikke overraskende, at talteori breder sig og indgår i andre områder af matematikken. Da tal desuden bruges i alle kulturer, kendes sætninger og opdagelser fra mange dele af verden

Endelig har tal været kendt i flere tusinde år, så det kan heller ikke være overraskende, at de første talteoretiske undersøgelser går langt tilbage i tiden.

Omvendt kan det måske virke overraskende, at talteori stadig er et stort forskningsområde inden for matematik, og at der er adskillige sætninger, der endnu ikke er bevist. Vores viden om tal er stor, og vi kender til mange ting, vi ikke ved. Men hvor meget, vi ikke ved, det ved vi ikke.

I talteori beskæftiger man sig ofte med de hele tal. Mange sætninger og egenskaber virker dog på samme måde inden for de naturlige tal, hvilket vi skal se senere.

Man kan også arbejde med større talmængder, men i overskriften til hvert kapitel står hvilken talmængde, der arbejdes med i det pågældende kapitel.

Når du skal arbejde med hele tal, er det vigtigt, at du er opmærksom på, at brøkstreger IKKE eksisterer! Det samme gælder decimaler i tal. Så kommaer eksisterer heller ikke.

Vi kommer ind på et tidspunkt, hvor addition, subtraktion og multiplikation er på plads, og vi skal nu lære om …

Kapitel 1: DIVISION (hele tal)

Definition 1.1: Et tal *n* siges at være divisibelt med tallet *d*, hvor $d \neq 0$, hvis der findes et tal *k*, så

$$n = k \cdot d$$

Tilføjelse 1.2: At *n* er divisibelt med *d* udtrykkes også ved "*d* går op i *n*", hvilket skrives $d \mid n$.

Betegnelser: *n* ~ dividend
d ~ divisor ('faktor' bruges også, men 'divisor' er specifikt knyttet til talteori)
k ~ kvotient

Eksempler:

a) Tallet 14 er divisibelt med tallet 7, fordi man kan finde tallet 2, hvor $14 = 2 \cdot 7$. Tallet 14 er dividend, tallet 7 er divisor og tallet 2 er kvotient.
b) 65 er divisibelt med -13, fordi $65 = (-5) \cdot (-13)$. Her er kvotienten altså negativ.
c) -27 er ikke divisibelt med 5, da man ikke kan finde et tal *k*, så $-27 = k \cdot 5$.

Bemærkning: Alle tal forskellige fra 0 er divisible med sig selv og 1 (begge tal $\pm$). Derfor kaldes 1 og tallet selv for *trivielle* divisorer.

Opgave 1.3: Bestem divisorerne til 42 og de mulige kvotienter.
Opgave 1.4: Bestem divisorerne til -12 og de mulige kvotienter.
Opgave 1.5: Bestem divisorerne til 13 og de mulige kvotienter.
Opgave 1.6: Bestem divisorerne til 1 og de mulige kvotienter.
Opgave 1.7: Efter ovenstående kunne det være fristende at drage konklusionen, at de mulige kvotienter også altid vil være divisorer i det pågældende tal. Men er det rigtigt?
Opgave 1.8: Alle tallene fra opgaverne 1.3-1.6 har et lige antal divisorer. Findes der et eller flere tal med et ulige antal divisorer?

Øvelse 1.9: Vis, at et tal er divisibelt med 3, netop hvis dets tværsum er divisibel med 3.
Øvelse 1.10: Vis, at det for alle tal *n* gælder, at $n^3 - n$ er divisibelt med 6.

Efter at have defineret det at være divisibelt med et tal skal vi nu se nogle sætninger, der behandler denne egenskab:

Sætning 1.11:

a) Hvis $a \mid b$, så gælder for alle tal *c*, at $a \mid (b \cdot c)$.

b) $a \mid b$, netop hvis $(a \cdot c) \mid (b \cdot c)$ for alle tal $c \neq 0$.

c) Hvis $a \mid b$ og $b \mid c$, så gælder $a \mid c$

d) Hvis $a \mid b$ og $a \mid c$, så gælder $a \mid (b \cdot x + c \cdot y)$ for alle *x* og *y*.

Bevis:

a) Dette er en "Hvis….., så….."-sætning. Der er flere måder at bevise sådan en sætning, men en direkte måde er at antage "hvis-delen" og ud fra denne antagelse vise "så-delen".
Så vi antager, at $a \mid b$.

Altså findes der et tal *k*, så $b = k \cdot a$. Dette udsagn er stadig sandt, hvis man ganger med *c* på begge sider (også selvom *c* er 0), dvs. $(c \cdot b) = (c \cdot k) \cdot a$. Men dette viser netop, at $a \mid (b \cdot c)$, hvor kvotienten så er $(c \cdot k)$. Det er undervejs benyttet, at faktorernes orden er ligegyldig.

b) Dette er en "….netop hvis…."-sætning. Det svarer til $a \mid b \Leftrightarrow (a \cdot c) \mid (b \cdot c)$. Man skal altså vise begge veje i biimplikationen.
Lad *c* være et tal forskelligt fra 0. Man har så:

$a \mid b \Leftrightarrow b = k \cdot a$ *for et tal* k $\quad$ (*definition* 1.1)

$\Leftrightarrow c \cdot b = c \cdot k \cdot a$ $\quad$ ($da\ c \neq 0$)

$\Leftrightarrow (b \cdot c) = k \cdot (a \cdot c)$ $\quad$ (*faktorernes orden er ligegyldig*)

$\Leftrightarrow (a \cdot c) \mid (b \cdot c)$ $\quad$ (*definition* 1.1)

Da der er benyttet biimplikationspile hele vejen, er sætningen altså bevist.

c) og d) udskydes til øvelser.

Opgave 1.12: Gælder sætning 1.11.a) også omvendt, hvis $c \neq 0$?
Dvs. gælder der, at $a \mid (b \cdot c) \Rightarrow a \mid b$?
Hvis du mener, at det gælder, skal du finde et bevis for det. Hvis du ikke mener, at det gælder, skal du finde et modeksempel.

Øvelse 1.13: Hvad skal der gælde om *a, b* og *c,* for at man skaber et modeksempel på sætningen fra opgave 1.12?

Øvelse 1.14: Find på beviser for sætningerne 1.11 c) og d).

Det er jo kun 0, der har uendelig mange divisorer, og man har også brug for at kunne arbejde med tal, der ikke nødvendigvis er divisorer. Så her følger en mere generel sætning om division:

Sætning 1.15: Lad *n* være et vilkårligt tal og *d* et positivt tal. Der findes så entydigt bestemte tal *k* og *r*, hvorom det gælder, at:

$$n = k \cdot d + r \quad ; \quad 0 \leq r < d$$

Eksempler: 1) Lad $n = 23$ og $d = 4$. Da $23 = 5 \cdot 4 + 3$, har man $k = 5$ og $r = 3$, hvor det skal bemærkes, at $0 \leq 3 < 4$ er et sandt udsagn.

2) Lad $n = -47$ og $d = 12$. Her er de entydigt bestemte tal $k = -4$ og $r = 1$, da man har $-47 = -4 \cdot 12 + 1$, hvor det igen bemærkes, at $0 \leq 1 < 12$ er et sandt udsagn.

3) Lad $n = -60$ og $d = 5$. Da $-60 = -12 \cdot 5$ er $k = -12$ og $r = 0$. Og atter bemærkes det, at $0 \leq 0 < 5$ er et sandt udsagn.

Tilføjelser og overvejelser 1.16:

1) Med definition 1.1 og sætning 1.15 er begrebet *division* kommet på plads. Tallet *k* i sætning 1.15 kaldes for kvotienten ligesom i definition 1.1.
2) Med *d* er det anderledes. Her gælder, at *d* fra sætning 1.15 kaldes divisor i *n*, netop hvis *r* = 0 (overvej selv dette).
3) Sætning 1.15 giver altså en måde at afgøre, om et tal er divisor i et andet tal (dvs. om det går op i tallet): Man ser, om resten er 0.
   Med eksemplerne ovenfor ses det altså, at:
   4 er ikke divisor i 23, da resten er 3.
   12 er ikke divisor i -47, da resten er 1.
   5 er divisor i -60, da resten er 0.

Inden sætning 1.15 bevises, kommer først nogle overvejelser:

Det er væsentligt at bemærke, at *k* og *r* skal være entydigt bestemte, og at *r* klemmes inde mellem 0 og *d*. For ellers ville sætningen ikke være så svær at bevise. F.eks. ville tallene *k* = 0 og *r* = *n* være løsninger til ligningen (overvej dette).

Og der ville være flere muligheder, som dette konkrete eksempel viser:

Lad *n* = 23 og *d* = 5. Så vil følgende talpar (*k*,*r*) være nogle blandt uendeligt mange, der er løsninger til ligningen: (0, 23), (1, 18), (3, 8), (4,3), (6,-7), (9, -22), (-1, 28) , (-3, 38). Kontrollér nogle af dem.

Øvelse 1.17: Find flere talpar, der er løsninger til ligningen.

Alle de tal *r*, der er en del af sådanne talpar, kaldes for *rester*. Mens det entydigt bestemte tal *r* fra sætning 1.15 kaldes for *den principale rest*.

Bevis for sætning 1.15: Lad *n* være et vilkårligt tal og *d* et positivt tal. Se så på den uendelige følge

…, -4d, -3d, -2d, -1d, 0d, 1d, 2d, 3d, …

Tallet *n* vil enten være lig med et af tallene i følgen eller være placeret mellem 2 konsekutive tal i følgen (nok ikke den skarpeste iagttagelse, men dog alligevel vigtig for det følgende).

Lad nu *k* være bestemt som det tal, hvorom det gælder, at:

$$k \cdot d \le n < (k+1) \cdot d \quad \Leftrightarrow \quad 0 \le n - k \cdot d < d$$

Bemærk, at denne er en veldefineret måde at bestemme tallet *k* på.

Med dette *k* kan man nu fastsætte *r* som:

$$r = n - k \cdot d$$

Hermed er:

$$0 \le r < d\,.$$

Og disse tal *k* og *r* opfylder udtrykket, da $k \cdot d + r = k \cdot d + (n - k \cdot d) = n$.

Det er altså nu vist, at den pågældende metode er en veldefineret måde at bestemme *k* og *r*. Men det viser jo ikke, at der ikke kunne være andre metoder, hvor man kunne bestemme andre talpar, der også opfylder sætningens betingelser.

Vi **antager** altså nu, at vi har fundet et passende talpar, og det skal så vises, at det må være det tidligere fundne:

Lad altså $n = k \cdot d + r \quad ; \quad 0 \le r < d$.

Så er $r = n - k \cdot d$, og dermed $0 \le n - kd < d \quad \Leftrightarrow \quad kd \le n < (k+1)d$,

og dette viser, at *(k,r)* er det talpar (*k*,*r*), der blev bestemt ved den pågældende metode.

Opgave 1.18: Find (evt. med brug af Maple) kvotienten og den principale rest i følgende tilfælde:

a) $n = 493$ og $d = 8$

b) $n = 28518$ og $d = 317$

c) $n = -17$ og $d = 5$

d) $n = -555$ og $d = 15$

Opgave 1.19: Kort formulering: Find mængden A bestående af alle de tal, der giver samme principale rest ved division med 7 som 43 gør.

Lang formulering: Når man dividerer 43 med 7, får man en rest r (der er et af tallene 0 – 6). Der er andre tal end 43, der divideret med 7 giver resten r. Find alle disse tal – opskrevet som en mængde.

Opgave 1.20: Find mængden B bestående af alle de tal, der giver samme principale rest ved division med 7 som 41 gør.

Opgave 1.21: Find mængden C bestående af alle de tal, der giver den principale rest 0 ved division med 7.

Opgave 1.22: Find 2 tal – ét i mængden A og ét i mængden B – hvis sum IKKE ligger i mængden C.

Opgave 1.23: Hvad er fælles for alle de tal, man får, hvis man subtraherer et element fra mængden B fra et element fra mængden A?

Kapitel 2: RESTKLASSER (hele tal)

De afsluttende opgaver i forrige kapitel skulle gerne have givet en fornemmelse for indholdet af den følgende definition, der bruges til at kæde tal med en bestemt egenskab sammen.

Definition 2.1: Lad d være et positivt tal. Så kaldes to tal a og b *kongruente modulo* d , hvis de giver samme principale rest ved division med d, og man skriver:

$$a \equiv b \pmod{d}.$$

Opgave 2.2: Bestem mængden D af tal, der er kongruente med 24 modulo 5.

Opgave 2.3: Bestem mængden E af tal, der er kongruente med -13 modulo 6.

Opgave 2.4: Bestem mængden F af tal, der er kongruente med 217 modulo 1.

Opgave 2.5: Hvad er fælles for alle de tal, man får, hvis 2 elementer fra D subtraheres?

Opgave 2.6: Hvad er fælles for alle de tal, man får, hvis 2 elementer fra E subtraheres?

Øvelse 2.7: Find et bevis for, at følgende 2 udsagn a) og b) er ensbetydende (bemærk altså, at dette er et "…netop hvis…"-udsagn):

a) a og b giver samme principale rest ved division med d.

b) $d \mid (a-b)$

Det var Gauss, der i 1801 i sit værk *Disquisitiones Arithmeticae* indførte betegnelserne fra definition 2.1 (blandt en masse andre ting). Man havde tidligere arbejdet med problemer af den slags, for de opstår helt naturligt, når vi opdeler dagene i uger og måneder (kongruens modulo 7 og kongruens modulo 12), men Gauss systematiserede det og brugte det til at udlede og bevise en hel del sætninger (heriblandt den *kinesiske restklassesætning* som du selv må finde, hvis du vil vide, hvad den går ud på).

Nu kan begrebet restklasser indføres:

Definition 2.8: Lad *d* være et givet positivt tal. Så er restklassen $[a]$:

$$[a] = \{b \mid b \equiv a \pmod{d}\}$$

Bemærk sammenhængen mellem denne definition og opgaverne 2.2-2.6.

Eksempel 2.9: For $d = 9$ er $[7] = \{\ldots,-11,-2,7,16,25,\ldots\}$ & $[5] = \{\ldots,-13,-4,5,14,23,\ldots\} = [-13] = [23]$

Bemærkning 2.10: Ligesom man indførte den principale rest blandt uendelig mange mulige rester, så begrænser man sig også til restklasserne $[0] - [d-1]$. Disse *d* restklasser kan man så regne med efter nogle bestemte regler.

Kapitel 3: FÆLLES DIVISORER (hele tal)

Definition 3.1: Tallet *d* kaldes en *fælles divisor* for *a* og *b*, hvis $d \mid a$ *og* $d \mid b$.

Eksempler:

1) Lad $a = 12$ og $b = 9$: Tallet 3 går op i både *a* og *b*, og derfor er 3 en fælles divisor for 12 og 9.
2) Lad $a = 12$ og $b = 9$: Tallet -4 går op i *a*, men det går ikke op i *b*. Dermed er -4 ikke en fælles divisor for *a* og *b*.
3) Lad $a = 37$ og $b = -7$. Tallet 3 går hverken op i *a* eller *b* og er derfor ikke en fælles divisor for *a* og *b*.

Bemærkning 3.2: Alle tal – bortset fra 0 – har et begrænset antal divisorer, og 1 er divisor i alle tal. Så hvis *a* og *b* ikke begge er 0, er mængden af fælles divisorer hverken tom eller indeholder uendeligt mange elementer. Dermed må der være et største tal blandt disse fælles divisorer, og det kaldes den *største fælles divisor* for *a* og *b*. Man skriver dette tal som **sfd(*a*,*b*)**, gcd(*a*,*b*) eller bare (*a*,*b*).

Eksempel: Lad $a = 15$ og $b = 12$.

Divisorerne til A er elementerne i mængden $A = \{-15,-5,-3,-1,1,3,5,15\}$.

Divisorerne til B er elementerne i mængden $B = \{-12,-6,-4,-3,-2,-1,1,2,3,4,6,12\}$.

De fælles divisorer er så elementerne i $C = \{-3,-1,1,3\}$.

Og af disse divisorer er 3 den største, og dermed er *sfd*(15,12) = 3

Følgende definition passer naturligt ind efter bemærkning 3.2, og derfor indføres den, selvom den først skal bruges senere.

Definition 3.3: To tal *a* og *b* kaldes (indbyrdes) primiske, hvis sfd(*a*,*b*) = 1

Eksempler:

1) Fra eksemplet ovenfor har man, at *sfd*(15,12) = 3, og 15 og 12 er dermed ikke indbyrdes primiske.
2) Se på $a = 21$ og $b = 10$.
   Divisorerne til A er elementerne i mængden $A = \{-21,-7,-3,-1,1,3,7,21\}$.
   Divisorerne til B er elementerne i mængden $B = \{-10,-5,,-2,-1,1,2,5,10\}$.
   De fælles divisorer er så elementerne i $C = \{-1,1\}$.
   Og af disse divisorer er 1 den største, og dermed er *sfd*(21,10) = 1.
   Altså er 21 og 10 indbyrdes primiske.
   Bemærk, at ingen af dem er primtal (se evt. definitionen i kapitel 6).

Opgave 3.4: Hvilke af nedenstående sætninger er IKKE rigtige for *a* og *b* forskellige fra 0:

a) sfd(a,b) ≥ 1
b) sfd(a,b) = sfd(b,a)
c) sfd(a,0) = a
d) sfd(a,b) = sfd(a,-b)
e) sfd(a,0) = sfd(b,0)
f) $sfd(a,b) \mid a$
g) $sfd(a,b) \mid (a \cdot b)$

Og så skal vi også lige have en definition, der ikke er specielt knyttet til talteori, men som oftest finder anvendelse i ligningssystemer, vektorregning og differentialligninger. Den skal benyttes i det efterfølgende, og vi har allerede stiftet bekendtskab med den i sætning 1.11 d).

Definition 3.5: Lad *a* og *b* være to givne tal. En *linearkombination* af disse tal er et udtryk af formen

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

hvor *x* og *y* er to tal, der kaldes linearkombinationens koefficienter.

Eksempel 3.6: En linearkombination af tallene -3 og 18 kunne være $4 \cdot (-3) + (-1) \cdot 18 = -30$.
Det kunne også være $0 \cdot (-3) + 2 \cdot 18 = 36$.

Bemærkning 3.7: Man kan lave linearkombinationer af flere end to tal, og man kan lave det af funktioner eller andre udtryk. Gæt selv hvordan.

Øvelse 3.8: Bestem sfd(6,4) ; sfd(11,2) ; sfd(17,45) ; sfd(70,21) ; sfd(-66,90) og sfd(317,0).
Øvelse 3.9: I Maple kan du skrive gcd(17,45) for at finde sfd(17,45). Kontrollér dine svar.

Eksempel: Man kan lave alle mulige linearkombinationer af to tal. Med udgangspunkt i tallene 6 og 4 fra øvelse 3.8 og den kommende øvelse 3.10 kan man bl.a. danne følgende linearkombinationer:

$$-1 \cdot 6 + 3 \cdot 4 = 6$$
$$7 \cdot 6 + 10 \cdot 4 = 82$$
$$0 \cdot 6 + 0 \cdot 4 = 0$$
$$-5 \cdot 6 - 2 \cdot 4 = -38$$

Der er ikke noget specielt ved disse linearkombinationer. Det er bare eksempler som indledning til følgende øvelse:

Øvelse 3.10: Du skal nu finde den linearkombination af følgende talpar, der giver det lavest mulige positive tal:

a) 6 og 4
b) 11 og 2
c) 17 og 45
d) 70 og 21
e) -66 og 90
f) 317 og 0

En matematikprofessor fra matematisk institut på KU har engang sagt: *Der findes to slags matematiske sætninger: De trivielle og de forkerte.*
Den følgende sætning er ikke forkert.

Sætning 3.11: Lad *a* og *b* være tal, der ikke begge er 0. Så findes der en linearkombination af *a* og *b*, så:

$$sfd(a,b) = a \cdot x + b \cdot y$$

Bevis: Lad *a* og *b* være tal, der ikke begge er 0, og lad L være mængden bestående af de linearkombinationer af *a* og *b*, der er positive. Det er vigtigt at bemærke, at mængden L ikke kan være tom, for man kan altid finde en positiv linearkombination (f.eks. vil $a \cdot a + 0 \cdot b > 0$, hvis *a* ikke er 0, og hvis *a* er 0, vælger man blot at multiplicere *b* med *b*).

L er ikke begrænset opad til, men den må indeholde et mindste element, da den er begrænset nedad til (Dette er en af de egenskaber, der gælder for naturlige tal, men ikke for reelle tal).

Lad *m* være dette mindste element. Dvs. man har:

$$m = x \cdot a + y \cdot b \quad og \quad m \geq 1 .$$

Vi sammenligner sfd(*a*,*b*) og *m*.

Da $sfd(a,b) \mid a$ og $sfd(a,b) \mid b$, følger det af sætning 1.11 d), at $sfd(a,b) \mid m$,

hvilket igen fører til, at $sfd(a,b) \leq m$.

Vi kan nu gennemføre beviset med et indirekte bevis (modstridsbevis):

Vi antager derfor, at m IKKE går op i *a*. Og lad os så se, hvad det fører til:

Ifølge sætning 1.15 findes så *k* og *r*, så $a = k \cdot m + r \quad ; \quad 0 < r < m$.

Bemærk altså, at antagelsen førte til, at *r* > 0. Man har så:

$$r = a - k \cdot m \quad \Leftrightarrow \quad r = a - k \cdot (x \cdot a + y \cdot b) \quad \Leftrightarrow \quad r = (1 - k \cdot x) \cdot a + (-k \cdot y) \cdot b .$$

Men hov! Her står jo en linearkombination af *a* og *b*, og da *r* > 0, så må *r* ligge i L. Men da vi også har, at $r < m$, kommer vi i modstrid med, at *m* er det mindste element i L. Vi kan altså se, at vores antagelse om, at *m* ikke går op i *a*, har ført til en modstrid. Dermed må denne antagelse være forkert, og altså må *m* gå op i *a*.

Præcis samme argumentation kan gennemføres med *b*, så man har altså, at $m \mid a \quad og \quad m \mid b$.

Dvs. at *m* er en fælles divisor i *a* og *b*. Men da *sfd*(*a*,*b*) er STØRSTE fælles divisor, så ved man, at $m \leq sfd(a,b)$. Da vi også ved, at $sfd(a,b) \leq m$, kan vi altså se, at $sfd(a,b) = m$, og hermed er sætningen vist.

Her følger så 2 korollarer. Et korollar er en sætning, der følger lige efter en anden sætning og kræver intet eller kun et lille bevis. Det kan følge direkte af den foregående sætnings ordlyd – evt. kombineret med en anden sætning eller en definition – eller af beviset for den foregående sætning.

Det første korollar følger af beviset for sætning 3.11:

Korollar 3.12: Det mindste, positive tal, der kan fremkomme ved en linearkombination af *a* og *b*, er sfd(*a*,*b*).

Dette korollar kan sætte en stopper for et evigt forsøg på at finde mindre positive tal i opgaver som øvelse 3.10.

Det andet korollar følger af definition 3.3 og korollar 3.12 (dvs. sætning 3.11 samt beviset for denne sætning):

Korollar 3.13: *a* og *b* er indbyrdes primiske, netop hvis der findes en linearkombination

$$1 = x \cdot a + y \cdot b$$

Eksempel: Man har, at $1 = 20 \cdot 5 + (-3) \cdot 33$.

Heraf kan man konkludere, at 5 og 33 er indbyrdes primiske. Men ikke blot det. Faktorernes orden er jo ligegyldig, så man har også, at:
20 og 33 er indbyrdes primiske og
20 og -3 er indbyrdes primiske og
5 og -3 er indbyrdes primiske.

Øvelse 3.14: Det kan være meget fint med en sætning som sætning 3.11. Men prøv engang at finde sfd(7176,11856) uden brug af Maple og bagefter at finde den linearkombination af tallene, der giver denne største fælles divisor.

Som det gerne skulle fremgå af ovenstående, fortæller sætning 3.11 kun noget om, at der eksisterer en linearkombination, der giver den største fælles divisor. Det er en såkaldt "Eksistens-sætning". Men den kan ikke bruges til at finde hverken største fælles divisor eller den søgte linearkombination.

Der findes imidlertid en sådan metode, der har været kendt i over 2000 år. Den står i kapitel 7 i sin oprindelige (oversatte) ordlyd. Men i første omgang gennemgås den i kapitel 5. Her kommer først nogle sætninger om største fælles divisorer:

Kapitel 4: SÆTNINGER OM STØRSTE FÆLLES DIVISORER (hele tal)

I matematik kan man sagtens formulere og bevise sætninger, fordi man har lyst. Der behøver ikke at være et formål med det. "Desværre" er det ikke tilfældet med de 4 sætninger i dette kapitel. De første bruges til at vise de sidste, og de sidste bruges……ikke til at vise de første, for den slags går kun inden for pseudovidenskaber, men til at vise sætninger i kapitlerne 5 og 6. Og hvem ved, måske skal de pludselig bruges i andre kapitler til at redde os ud af en håbløs situation? Det gør jeg, og det skal de ikke.

Sætning 4.1: Alle fælles divisorer for a og b går op i $sfd(a,b)$

Eksempler:

1) Lad $a = 30$ og $b = 42$.
   Divisorerne i a er elementerne i $A = \{-30,-15,-10,-6,-5,-3,-2,-1,1,2,3,5,6,10,15,30\}$.
   Divisorerne i b er elementerne i $B = \{-42,-21,-14,-7,-6,-3,-2,-1,1,2,3,6,7,14,21,42\}$.
   De fælles divisorer er så elementerne i $C = \{-6,-3,-2,-1,1,2,3,6\}$.
   Dermed er $sfd(30,42) = 6$.
   Og som det bemærkes, så er samtlige elementer i C divisorer i 6, hvilket er i overensstemmelse med sætning 4.1.

2) Lad $a = -13$ og $b = 27$.
   Divisorerne i a er elementerne i $A = \{-13,-1,1,13\}$.
   Divisorerne i b er elementerne i $B = \{-27,-9,-3,-1,1,3,9,27\}$.
   De fælles divisorer er så elementerne i $C = \{-1,1\}$.
   Dermed er $sfd(-13,27) = 1$.
   Og da -1 og 1 begge er divisorer i 1, så er der igen overensstemmelse med sætning 4.1.

Bevis: Sætning 3.11 siger, at der findes en linearkombination af a og b, så $sfd(a,b) = x \cdot a + y \cdot b$.
Hvis d_f er en fælles divisor for a og b (dvs. $d_f \mid a$ og $d_f \mid b$), så følger af sætning 1.11 d), at $d_f \mid sfd(a,b)$.

Hvis du mener, at beviset ikke er fyldestgørende eller indeholder fejl, så gå til øvelse 4.2.
Hvis du efter nøje overvejelse og med din kritiske sans fulde brug mener, at beviset – og dermed sætningen – er rigtigt, så gå til øvelse 4.3

Øvelse 4.2: Find to tal a og b og en fælles divisor for disse, der IKKE går op i $sfd(a,b)$.
Øvelse 4.3: Find samtlige fælles divisorer for 24 og 18 og se, at de går op i den største af dem.

Opgave 4.4: Find 2 tal, hvor samtlige fælles divisorer er følgende 14 tal $\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm9,\pm12\}$.

Opgave 4.5: Find de 2 mindste, forskellige, positive tal, hvor samtlige fælles divisorer er følgende 8 tal $\{\pm1,\pm2,\pm5,\pm10\}$

Sætning 4.6: For ethvert positivt tal c gælder $sfd(c \cdot a, c \cdot b) = c \cdot sfd(a,b)$

Eksempel:

Lad $a = -20, b = 110$ og $c = 7$.
Du kan evt. bruge Maple til at vise:
$c \cdot a = -140$
$c \cdot b = 770$
$sfd(a,b) = sfd(-20,110) = 10$
$sfd(c \cdot a, c \cdot b) = sfd(-140,770) = 70$
Og ved indsættelse ses dette at være i overensstemmelse med sætning 4.6, da man har det sande udsagn: $70 = 7 \cdot 10$.

Her følger to ret forskellige beviser for sætning 4.6.

Bevis 1: I dette bevis benyttes en fremgangsmåde, der delvist blev benyttet i sidste del af beviset for sætning 3.11. Sætningen vises nemlig ved, at der først gøres rede for, at højresiden er divisor i venstresiden, og derefter at venstresiden er divisor i højresiden:

Man har, at $sfd(a,b)\,|\,a$ og $sfd(a,b)\,|\,b$. Og da c er positivt, har man altså ifølge sætning 1.11 b), at $c\cdot sfd(a,b)\,|\,c\cdot a$ og $c\cdot sfd(a,b)\,|\,c\cdot b$. Dette viser, at $c\cdot sfd(a,b)$ er divisor i både $c\cdot a$ og $c\cdot b$, dvs. det er en fælles divisor for $c\cdot a$ og $c\cdot b$. Og ifølge sætning 4.1 gælder altså, at $\underline{c\cdot sfd(a,b)\,|\,sfd(c\cdot a,c\cdot b)}$.

Det er oplagt, at $c\,|\,c\cdot a$ og $c\,|\,c\cdot b$ (kvotienterne er henholdsvis a og b). Men hermed er c en fælles divisor for $c\cdot a$ og $c\cdot b$. Ifølge sætning 4.1 har man altså, at $c\,|\,sfd(c\cdot a,c\cdot b)$. Dermed gælder ifølge definition 1.1, at $sfd(c\cdot a,c\cdot b)=k\cdot c$.

Da $k\cdot c$ altså er den største fælles divisor for $c\cdot a$ og $c\cdot b$, så gælder specielt, at $k\cdot c\,|\,c\cdot a$ og $k\cdot c\,|\,c\cdot b$. Men så kan sætning 1.11 b) jo bruges igen! Da c ikke er nul, gælder altså:

$k\,|\,a$ og $k\,|\,b$. Dvs. k er fælles divisor for a og b, og dermed $k\,|\,sfd(a,b)$ (sætning 4.1).

Og her kommer sætning 1.11 b) ind igen. Den giver, at $c\cdot k\,|\,c\cdot sfd(a,b)$. Og nu kender vi jo allerede $k\cdot c$ fra tidligere, så vi har: $\underline{sfd(c\cdot a,c\cdot b)\,|\,c\cdot sfd(a,b)}$.

Og sammenholdes de 2 understregede konklusioner, er sætningen vist.

Bevis 2: Dette bevis er bygget op omkring korollar 3.12:

Ifølge sætning 3.11 findes der tal x og y, så $sfd(c\cdot a,c\cdot b)=c\cdot a\cdot x+c\cdot b\cdot y=c\cdot\left(a\cdot x+b\cdot y\right)$

Da $sfd(c\cdot a,c\cdot b)>0 \text{ og } c>0$, er også linearkombinationen $a\cdot x+b\cdot y>0$.

Men vi ved fra korollar 3.12, at $a\cdot x+b\cdot y\geq sfd(a,b)$, og dermed $\underline{sfd(c\cdot a,c\cdot b)\geq c\cdot sfd\left(a,b\right)}$

Hvis man i stedet tager udgangspunkt i $c\cdot sfd\left(a,b\right)$, siger sætning 3.11, at der findes tal x_1 og y_1 (faktisk er det de samme tal som x og y, men det kan man først vide, når beviset er gennemført), således at $c\cdot sfd\left(a,b\right)=c\cdot\left(a\cdot x_1+b\cdot y_1\right)=\left(c\cdot a\right)\cdot x_1+\left(c\cdot b\right)\cdot y_1$.

Da $sfd(a,b)>0 \text{ og } c>0$, er også linearkombinationen $\left(c\cdot a\right)\cdot x_1+\left(c\cdot b\right)\cdot y_1>0$.

Så ved vi fra korollar 3.12, at $\left(c\cdot a\right)\cdot x_1+\left(c\cdot b\right)\cdot y_1\geq sfd\left(c\cdot a,c\cdot b\right)$.

Dermed er $\underline{sfd(c\cdot a,c\cdot b)\leq c\cdot sfd\left(a,b\right)}$

Sammenlignes de to understregede udsagn, har man $sfd(c\cdot a,c\cdot b)=c\cdot sfd(a,b)$

Øvelse 4.7: Er det nødvendigt, at tallet c er positivt? Kan det ikke bare være forskelligt fra 0?
Øvelse 4.8: Hvor i bevis 1 benyttes implicit, at c er positivt?

Eksempel: Sætning 4.6 giver en metode til at finde største fælles divisorer (som nævnt følger endnu en i kapitel 5). Så lad os prøve at finde største fælles divisor for 660 og 780:

$$sfd(660,780) = 2 \cdot sfd(330,390) = 2 \cdot 2 \cdot sfd(165,195) = 2 \cdot 2 \cdot 3 \cdot sfd(55,65) =$$
$$2 \cdot 2 \cdot 3 \cdot 5 \cdot sfd(11,13) = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 1 = \underline{\underline{60}}$$

Denne metode kan selvfølgelig kun bruges, når det er nemt at finde tal, der går op i både *a* og *b*.

Øvelse 4.9: Find uden brug af Maple den største fælles divisor for følgende talpar og kontrollér derefter med Maples 'gcd':

a) 184 og 136
b) 408 og 600
c) 150 og 525
d) 756 og 972

Sætning 4.10: $c \mid a \cdot b \ \wedge \ sfd(c,b) = 1 \ \Rightarrow \ c \mid a$

I ord siger sætningen altså, at hvis *c* er divisor i et produkt af 2 faktorer og indbyrdes primisk med den ene faktor, så er den divisor i den anden faktor.

Eksempel:

Lad $a = 33$, $b = 5$ og $c = 11$.
Så har man $a \cdot b = 33 \cdot 5 = 165$
Og nu ser man så på ordlyden af sætning 4.10:
Man kan se, at $c \mid a \cdot b$, og desuden er *sfd(11,5) = 1*, så betingelserne er opfyldt.
Dermed skal der gælde, at $c \mid a$, og det passer.

Men nu viser et eksempel jo ikke, om en sætning er rigtig, så her kommer et par beviser:

Bevis 1: Lad $c \mid a \cdot b \ \wedge \ sfd(c,b) = 1$.

Sætning 4.6 giver $a \cdot sfd(c,b) = a \cdot 1 \ \Leftrightarrow \ sfd(a \cdot c, a \cdot b) = |a|$ (overvej numerisktegnet!).
Hermed er den ene forudsætning benyttet.
Man har, at $c \mid a \cdot c$, og ifølge forudsætningen gælder også $c \mid a \cdot b$. Dvs. at *c* er fælles divisor for $a \cdot c$ og $a \cdot b$, og dermed gælder altså ifølge sætning 4.1, at *c* er divisor i $sfd(a \cdot c, a \cdot b)$.
Men hermed må *c* altså også være divisor i *a*, da et evt. fortegn ikke ændrer ved divisorerne.

Bevis 2: Lad $c \mid a \cdot b \ \wedge \ sfd(c,b) = 1$.

Da *b* og *c* er indbyrdes primiske, følger af korollar 3.13, at der findes tal *x* og *y*, så:
$c \cdot x + b \cdot y = 1$ og dermed $a \cdot c \cdot x + a \cdot b \cdot y = a$
Da $a \cdot b$ er divisibelt med *c* (ifølge antagelsen), findes et tal *k*, således at $a \cdot b = k \cdot c$
Dermed har man: $a \cdot c \cdot x + k \cdot c \cdot y = c \cdot (a \cdot x + k \cdot y) = a$
Men størrelsen inde i parentesen er et tal, så ifølge definition 1.1 gælder altså $c \mid a$.

Øvelse 4.11: Du får oplyst, at 17 er divisor i 680782. Benyt sætning 4.10 til at vise, at 17 også er divisor i 340391.

Og her følger så til sidst en sætning, der skal bruges i næste kapitel.

Sætning 4.12: Lad r være den principale rest ved division af b med a. Så er $sfd(a,b) = sfd(a,r)$

Eksempel: Lad $a = 6435$ og $b = 57460$.
Da $57460 = 8 \cdot 6435 + 5980$, er den principale rest altså 5980.
Og man kan – evt. ved brug af Maple – vise, at der gælder:
Sfd(6435,57460) = 65 og *sfd(6435,5980) = 65*.

Eksempel: Lad a = 57460 og b = 6435.
Da $6435 = 0 \cdot 57460 + 6435$, er den principale rest altså 6435.
I dette tilfælde er $r = b$, og så er sætningens konklusion oplagt.

Øvelse 4.13: Afprøv, om sætning 4.12 holder i situationerne:

a) b = 72 og a = 30
b) b = 119 og a = 51
c) b = 18479 og a = 5723
d) b =18446 og a = 11822
e) b = 100 og a = 50

Bevis for sætning 4.12: Lad r og k være de entydigt bestemte tal ifølge sætning 1.15. Så er:

$$b = k \cdot a + r \quad ; \quad 0 \le r < a$$

Da sfd(a,r) er divisor i både a og r, følger af sætning 1.11.d), at sfd(a,r) er divisor i b.
Og da sfd(a,r) derfor er fælles divisor for a og b, så følger af sætning 4.1, at $sfd(a,r) \mid sfd(a,b)$.

Se nu på sfd(a,b):
Man kan omskrive udtrykket $b = k \cdot a + r$ til $r = b - k \cdot a$, og da sfd*(a,b)* er divisor i både a og b, følger af sætning 1.11.d), at sfd(a,b) er divisor i r. Og da sfd(a,b) derfor er fælles divisor for a og r, følger af sætning 4.1, at $sfd(a,b) \mid sfd(a,r)$.

Ved at betragte de 2 understregede udtryk ses det, at sætningen er vist.

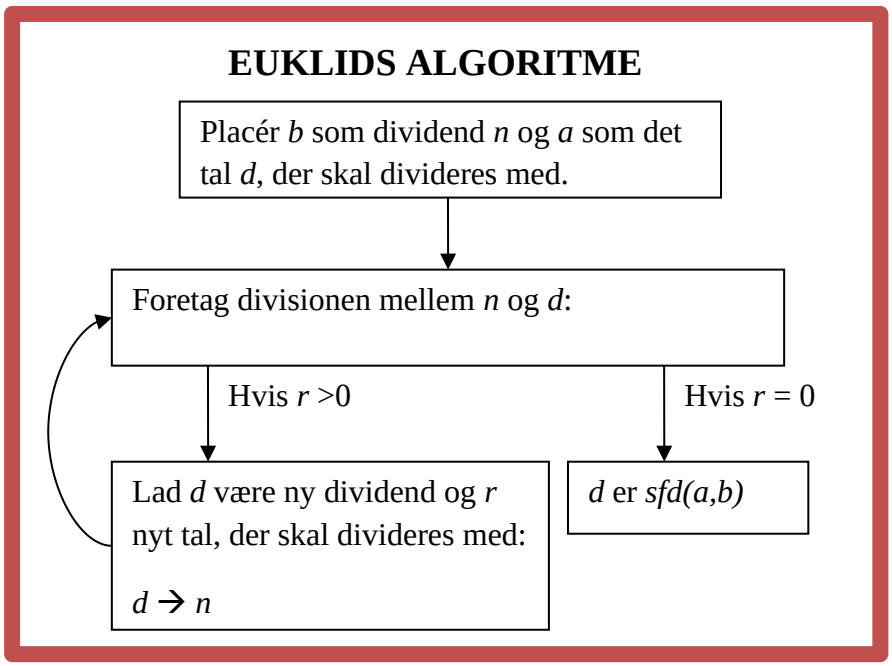
Opgave 4.14: Der er noget overflødigt i sætningens formulering, der også giver sig udtryk i, at der er en betingelse i beviset, der faktisk ikke bruges til noget. Hvad er det?

Kapitel 5: EUKLIDS ALGORITME

(naturlige tal) ← Bemærk!!!

Algoritme: En algoritme er en forskrift for en følge af beregningstrin, der kan bruges på nogle konkrete data til at komme frem til et ønsket resultat.
Dvs. man beskriver en række mekaniske trin, der skal foretages – ofte igen og igen indtil et bestemt resultat fremkommer. En computer er god til sådanne beregninger, der ikke kræver, at man skal tænke, og derfor benyttes algoritmer meget inden for datalogi.

Euklids algoritme kan benyttes til at finde den største fælles divisor for 2 tal (a og b), og den kan desuden konstruere den linearkombination, der er lig med den største fælles divisor.
Der ses i første omgang kun på den del af algoritmen, der giver den største fælles divisor. Hvordan man finder linearkombinationer, beskrives senere.



Bemærkning 5.1: At dette virkelig fører til den største fælles divisor for a og b ses på følgende måde. Når $r = 0$, har man, at $d \mid n$ og dermed $d = sfd(d,n)$. Hvis divisionen gik op i første skridt, er det a og b, der svarer til d og n. Men ellers er det r og d fra det tidligere skridt (husk, at $d \rightarrow n$ og $r \rightarrow d$). Men ifølge sætning 4.12 er $sfd(d,n) = sfd(d,r)$, dvs. man vil i alle skridt have, at den største fælles divisor for dividenden og tallet, der divideres med, er den samme som for tallet, der divideres med, og resten. Og i sidste ende er det altså største fælles divisor for a og b.

Eksempel 5.2: Man skal finde største fælles divisor for 2805 og 6188.

Først sættes 6188 som dividend og 2805 som tallet, der divideres med (da 6188 > 2805). Så foretages divisionen, der giver:

$$6188 = 2 \cdot 2805 + 578$$

Da 578 > 0 , sætter man nu 2805 som ny dividend og 578 som nyt tal, der skal divideres med, og en ny division udføres:

$$2805 = 4 \cdot 578 + 493$$

Da 493 > 0 , sættes 578 som ny dividend og 493 som nyt tal, der skal divideres med:

$$578 = 1 \cdot 493 + 85$$

Da 85 > 0 , skal man foretage samme skridt igen:

$$493 = 5 \cdot 85 + 68$$

Da 68 > 0, fortsættes:

$$85 = 1 \cdot 68 + 17$$

Da 17 > 0, fortsættes:

$$68 = 4 \cdot 17 + 0$$

Her er resten 0, og da 17 er den sidst anvendte divisor, har man $sfd(2805,6188) = 17$

Faktisk er det ikke vigtigt, om man placerer *a* eller *b* som dividend eller som tal, der skal divideres med. Hvis det største tal havner som tal, der skal divideres med, vil algoritmen blot skulle køre ét skridt mere som følgende eksempel viser:

Eksempel 5.3: Man skal finde største fælles divisor for 121030 og 75141.

$$75141 = 0 \cdot 121030 + 75141$$
$$121030 = 1 \cdot 75141 + 45889$$
$$75141 = 1 \cdot 45889 + 29252$$
$$45889 = 1 \cdot 29252 + 16637$$
$$29252 = 1 \cdot 16637 + 12615$$
$$16637 = 1 \cdot 12615 + 4022$$
$$12615 = 3 \cdot 4022 + 549$$
$$4022 = 7 \cdot 549 + 179$$
$$549 = 3 \cdot 179 + 12$$
$$179 = 14 \cdot 12 + 11$$
$$12 = 1 \cdot 11 + 1$$
$$11 = 11 \cdot 1$$

Dvs. at 1 er sfd(121030,75141).

Øvelse 5.4: Benyt Euklids algoritme til – uden Maples 'gcd' - at finde største fælles divisor for følgende talpar og kontrollér derefter resultater med Maple:

a) 42 og 30
b) 91 og 17
c) 18479 og 5723
d) 11822 og 18446
e) 193365 og 330869
f) 198782 og 298173
g) 101173 og 52153

Med bogstaver kommer opskrivningen til at se således ud:

$$\begin{aligned} b &= k_1 \cdot a + r_1 \\ a &= k_2 \cdot r_1 + r_2 \\ r_1 &= k_3 \cdot r_2 + r_3 \\ r_2 &= k_4 \cdot r_3 + r_4 \\ &\vdots \\ r_{m-2} &= k_m \cdot r_{m-1} + r_m \\ r_{m-1} &= k_{m+1} \cdot r_m \end{aligned}$$

Hvor altså $r_m = sfd(a,b)$.

Hvis bemærkning 5.1 var svær at overskue, bliver det måske nemmere ved at se på ovenstående følge. Igen skal der argumenteres for, at algoritmen fører frem til sfd(*a*,*b)*.

Ved gentagen brug af sætning 4.12 på ovenstående begyndende fra toppen får man:

$$sfd(a,b) = sfd(a,r_1) = sfd(r_1,r_2) = sfd(r_2,r_3) = sfd(r_3,r_4) = \ldots = sfd(r_{m-1},r_m) = sfd(r_m,0) = r_m$$

Nu skal vi så se på, hvordan man finder linearkombinationen, der giver sfd(*a*,*b*).
For overskuelighedens skyld ses på en mindre følge, hvor man desuden isolerer resterne:

$$\begin{aligned} b &= k_1 \cdot a + r_1 & \qquad r_1 &= b - k_1 \cdot a \\ a &= k_2 \cdot r_1 + r_2 & \qquad r_2 &= a - k_2 \cdot r_1 \\ r_1 &= k_3 \cdot r_2 + r_3 & \qquad r_3 &= r_1 - k_3 \cdot r_2 \\ r_2 &= k_4 \cdot r_3 + r_4 & \qquad r_4 &= r_2 - k_4 \cdot r_3 \\ r_3 &= k_5 \cdot r_4 \end{aligned}$$

Man begynder så nedefra i følgen til højre og får ved gentagne indsættelser af den ovenstående linjes højreside (undervejs indføres nogle nye konstanter q for at gøre opskrivningen simplere):

$$\begin{aligned} sfd(a,b) = r_4 &= r_2 - k_4 \cdot (r_1 - k_3 \cdot r_2) = (1 + k_3 \cdot k_4) \cdot r_2 - k_4 \cdot r_1 = q_1 \cdot r_2 - k_4 \cdot r_1 \\ &= q_1 \cdot (a - k_2 \cdot r_1) - k_4 \cdot r_1 = q_1 \cdot a + (-q_1 \cdot k_2 - k_4) \cdot r_1 = q_1 \cdot a + q_2 \cdot r_1 \\ &= q_1 \cdot a + q_2 \cdot (b - k_1 \cdot a) = (q_1 - q_2 \cdot k_1) \cdot a + q_2 \cdot b = \underline{q_3 \cdot a + q_2 \cdot b} \end{aligned}$$

Og vupti! Her er så den søgte linearkombination. Som det ses, kan man udvide metoden til rækker af vilkårlig længde.

Her kommer et konkret eksempel, hvor man benytter udregningen fra eksempel 5.2:

Eksempel 5.5: Først ses på rækken fra eksempel 5.2, hvor resterne er isoleret:

$$578 = 6188 - 2 \cdot 2805$$
$$493 = 2805 - 4 \cdot 578$$
$$85 = 578 - 1 \cdot 493$$
$$68 = 493 - 5 \cdot 85$$
$$17 = 85 - 1 \cdot 68$$

Og som du måske erindrer, er sfd(6188,2805) = 17.

Man får så følgende udregning, der følger ovennævnte metode:

$$\begin{aligned} 17 &= 85 - 1 \cdot (493 - 5 \cdot 85) = 6 \cdot 85 - 1 \cdot 493 \\ &= 6 \cdot (578 - 1 \cdot 493) - 1 \cdot 493 = -7 \cdot 493 + 6 \cdot 578 \\ &= -7 \cdot (2805 - 4 \cdot 578) + 6 \cdot 578 = 34 \cdot 578 - 7 \cdot 2805 \\ &= 34 \cdot (6188 - 2 \cdot 2805) - 7 \cdot 2805 = \underline{-75 \cdot 2805 + 34 \cdot 6188} \end{aligned}$$

Så her er den ønskede linearkombination. Kontrollér selv, at det passer.

Opgave 5.6: Benyt Euklids algoritme til at finde største fælles divisor og benyt derefter metoden fra Eksempel 5.5 til at finde linearkombinationen i følgende tilfælde:

a) 105 og 154
b) 31207 og 8511
c) Tallene fra Eksempel 5.3

Kapitel 6: PRIMTAL

(naturlige tal – bortset fra 6.28'erne)

Først skal det lige defineres, hvad et primtal er (husk, at vi nu arbejder med naturlige tal):

Definition 6.1: Et *primtal* er et tal $p > 1$, der kun har trivielle divisorer.

Opgave 6.2: Man kunne også finde andre formuleringer af definitionen. Hvilken eller hvilke af nedenstående er dog IKKE rigtige:

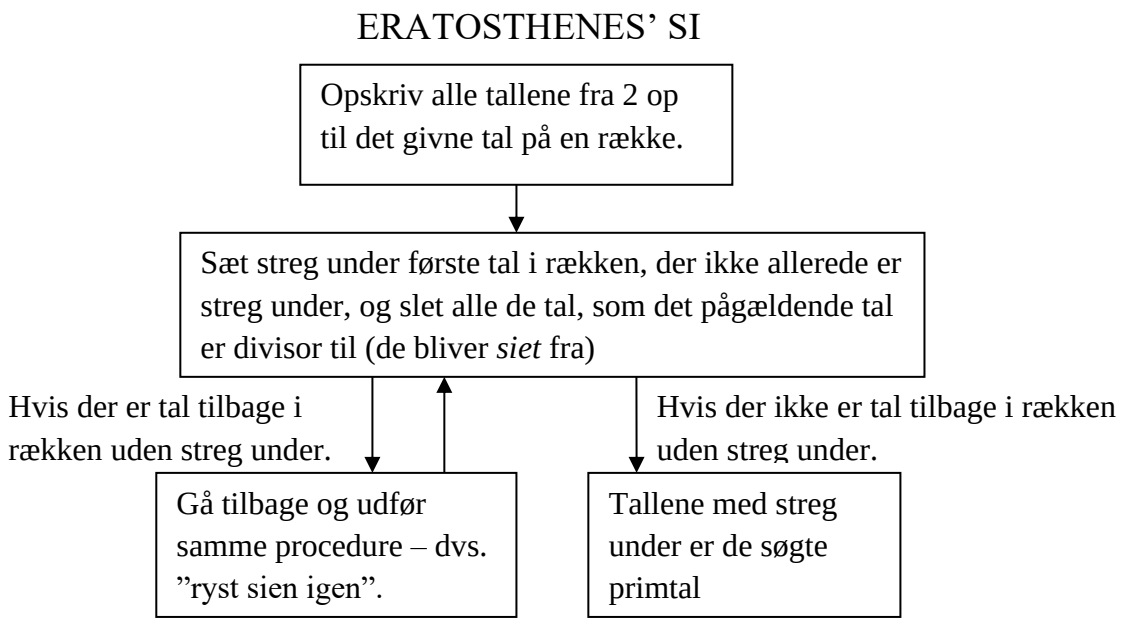
a) Et primtal er et tal med netop 2 divisorer.
b) Et primtal er et tal, der kun har trivielle divisorer.
c) Et primtal er et tal, hvor kun 1 og tallet selv er divisorer.
d) Et primtal er et tal større end 1, der ikke kan skrives som produkt af 2 tal uden at 1 er den ene faktor.

Opgave 6.2.a: Find det mindste primtal p, der har den egenskab, at $\sqrt{p}$ er et helt tal.

Definition 6.3: Et tal $s > 1$, der ikke er et primtal, kaldes et *sammensat tal*.

Vi skal nu se på en måde at finde primtallene op til et givet tal. Metoden kaldes *Eratosthenes' si*, og det er en algoritme. Den går ud på følgende:

Eratosthenes' si 6.4:



Eksempel: Primtallene under 30 skal findes:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	3		5		7		9		11		13		15		17		19		21		23		25		27		29	
2	3		5		7				11		13				17		19				23		25				29	
2	3		5		7				11		13				17		19				23						29	
2	3		5		7				11		13				17		19				23						29	

Dvs. at primtallene op til 30 er: 2, 3, 5, 7, 11, 13, 17, 19, 23 og 29

Øvelse 6.5: Bestem antallet af primtal under 51 og tjek, at der er 15.

Som du måske kunne få en fornemmelse af, så er dette oplagt et arbejde for en computer, eller en……

Weekendøvelse 6.5.a: Find alle primtallene op til 10000, og tjek, at der er 1229 – der selv er et primtal!

Vi er nu nået til en af de helt store sætninger inden for talteori: *Aritmetikkens Fundamentalsætning.* Aritmetik betyder på græsk 'regnekunst', så aritmetikken kan betragtes som en del af talteorien. En fundamentalsætning er en yderst vigtig sætning, der bruges meget inden for stort set hele det pågældende område (i dette tilfælde aritmetikken).

Men inden vi viser den, skal vi først vise et såkaldt *Lemma*, der er en hjælpesætning, der oftest indføres lige inden beviset for en større sætning (i dette tilfælde *Aritmetikkens Fundamentalsætning*), og som bruges i beviset for denne.

Det smarte ved lemmaer er, at de gør beviserne for de større sætninger mere overskuelige, og desuden fungerer et lemma som en almindelig sætning (da det bevises), så man kan henvise til det senere.

Lemma 6.6: For ethvert primtal p gælder: $p \mid a \cdot b \;\Rightarrow\; p \mid a \;\vee\; p \mid b$.

Eksempler:

1) Lad p være primtallet 17, og lad $a = 23$ og $b = 39$. Da 17 hverken er divisor i 23 eller 39, kan 17 heller ikke være divisor i $23 \cdot 39 = 897$, for HVIS 17 var divisor i 897, så ville den ifølge sætningen være divisor i 23 eller 39.

2) Ved en tilfældighed har man fundet ud af, at det om primtallet 293 gælder, at $293 \mid 326607979$, og man ved naturligvis, at $326607979 = 265751 \cdot 1229$. Fra sin weekendøvelse 6.5.a husker man, at 1229 er et primtal, så 293 kan ikke gå op i 1229. Man kan derfor ved hjælp af lemma 6.6 konkludere, at $293 \mid 265751$, hvilket altid er rart at vide.

Lemma 6.6 kan bevises ved at bruge korollar 3.13 og antage, at p ikke er divisor i enten a eller b (følger som en øvelse), men det kan gøres endnu nemmere ved at bruge sætning 4.10. Så inden du læser beviset nedenfor, så tag et kig tilbage og tænk over indholdet af denne sætning.

Bevis: Lad p være et primtal, og lad $p \mid a \cdot b$. Hvis $p \mid a$, passer sætningen. Så nu antager vi, at p IKKE er divisor i a. Da p er et primtal, har det kun divisorerne 1 og p, så man har *sfd(a,p)=1*, og så siger sætning 4.10, at $p \mid b$. Tænk lidt over det og opdag, at beviset er ført.

Øvelse 6.7: Overvej, om denne sætning kan udvides til at gælde for flere tal, dvs. $p \mid a \cdot b \cdot c$.

Øvelse 6.8: Formulér den pågældende sætning og find et bevis for den.

Spørgsmål 6.9: Kan du føre et bevis for, at sætningen også gælder for $p \mid a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$?

Hvis ja, så gå til øvelse 6.10. Hvis nej, så gå til øvelse 6.11.

Øvelse 6.10: Formulér sætningen og gennemfør beviset. Du vil nok – eksplicit eller implicit – komme til at bruge det såkaldte *induktionsaksiom.*

Øvelse 6.11: Find et bevis for lemma 6.6, hvor du bruger korollar 3.13

Aritmetikkens Fundamentalsætning 6.12: Ethvert tal $n > 1$ er enten et primtal eller kan skrives **entydigt** som et produkt af primtal $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_s^{\alpha_s}$, hvor det for alle $i, j \in \{1, 2, 3, ..., s\}$ gælder, at p_i er et primtal, og $i < j \Rightarrow p_i < p_j$.

Det er væsentligt at bemærke, at sætningen består af en *eksistens-del* (ordet "kan") og en *entydigheds-del*. Inden selve beviset skal vi se lidt på disse to dele i helt konkrete tilfælde. At finde en opskrivning $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_s^{\alpha_s}$ kaldes også at "opløse tallet i primfaktorer".

Øvelse 6.13: *Eksistens.* Opløs følgende tal i primfaktorer: 6, 65, 42, 220, 286440 og 485100.

Øvelse 6.14: *Entydighed.* Hvilke opløsninger kom klassens elever frem til?

Øvelse 6.15: Maple kan finde sådanne faktoriseringer. Det foregår ved at skrive "*ifactor(***)*". Prøv dette på tallene fra øvelse 6.13.

Ovenstående øvelser skulle gerne have givet dig en idé om indholdet af denne fundamentale sætning. Og nu kommer så beviset:

Bevis for 6.12: Først ses på eksistensen. Lad n være et tal større end 1. Hvis n er et primtal, er der ikke noget at vise, for så siger sætningen ikke noget. Så lad n være et sammensat tal. Det kan derfor skrives som et produkt $n = a_1 \cdot a_2$ af tal større end 1.

Tallene a_1 og a_2 kan nu hver især være et primtal eller et sammensat tal. Hvis det er et primtal, gør man ikke mere ved det, men hvis det er sammensat, skrives det som et produkt af to tal større end 1. Antag f.eks., at a_1 er et sammensat tal og a_2 et primtal. Så får man nu $n = a_{11} \cdot a_{12} \cdot a_2$.

Samme procedure anvendes nu på a_{11} og a_{12}. Hvis tallet er et primtal røres det ikke, men hvis det er sammensat skrives det som produkt af to tal større end 1. Hvis f.eks. både a_{11} og a_{12} er sammensatte tal, får man $n = a_{111} \cdot a_{112} \cdot a_{121} \cdot a_{122} \cdot a_2$.

Og sådan fortsættes, så længe der er mindst ét sammensat tal blandt faktorerne.

Og her kommer så pointen: Denne opløsning må nødvendigvis stoppe på et tidspunkt, da de sammensatte tals faktorer er mindre end tallet selv, så tallet n kan i hvert fald ikke opløses mere end n gange ved denne proces (faktisk langt mindre - antallet af faktoriseringer kan ikke overstige $\frac{\ln(n)}{\ln(2)}$ - men det væsentlige er at have en øvre grænse).

Til sidst har man altså fået opskrevet n som et produkt af primtal, f.eks.

$$n = a_{1111} \cdot a_{111211} \cdot a_{111212} \cdot a_{11122} \cdot a_{112} \cdot a_{1211} \cdot a_{12121} \cdot a_{12122} \cdot a_{122} \cdot a_2$$

Alle disse primtal omdøbes nu og ordnes (faktorernes orden er ligegyldig), så de mindste primtal står til venstre. Nogle af disse primtal kan godt være ens, f.eks. kunne $a_{122} = a_{111211}$, og i så fald skrives de som potenser. På den måde fremkommer $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_s^{\alpha_s}$

Nu gælder det så entydigheden af denne opløsning:

Lad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_s^{\alpha_s}$ være en fundet opløsning. Lad $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_t^{\beta_t}$ være en anden fundet opløsning. Det ønskes nu vist, at disse to opløsninger nødvendigvis må være ens.

Man har: $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_s^{\alpha_s} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_t^{\beta_t}$.

Vi ser nu på det mindste primtal, der optræder i denne ligning. Det er enten p_1 eller q_1 (vi viser lige om lidt, at $p_1 = q_1$, så faktisk er det "både-og", og man kan frit vælge et af dem). Antag, at det er p_1. Det er divisor i venstresiden, og det må derfor også være divisor i højresiden. Men så må p_1 ifølge Lemma 6.6 (på formen fra Spørgsmål 6.9) også være divisor i en af faktorerne q_i på højresiden. Men q_i er jo et primtal, så det har kun trivielle divisorer. Så dermed må $p_1 = q_i$, og altså $q_i = q_1$, da ingen af q'erne var mindre end p_1.

Hvis man havde taget udgangspunkt i q_1, var man også kommet frem til $p_1 = q_1$ med samme argumenter. Denne faktor kan altså forkortes væk fra begge sider, og man udfører samme procedure på den nye ligning. Hermed viser det sig, at $\alpha_1 = \beta_1$, for hvis et af primtallene p_1 og q_1 blev forkortet helt væk før det andet, ville man få en modstrid.

Sådan fortsættes, og man får efterhånden forkortet alle de faktorer, der fremkommer på begge sider, væk fra ligningen, således at der ikke er flere primtal tilbage på den ene side, dvs. kun tallet 1 står tilbage.

Men så må det samme gælde på den anden side af lighedstegnet, for ellers ville udsagnet ikke være sandt, og man har dermed vist, at de to opløsninger er identiske.

Eksempel 6.16: Sætning 6.12 kan bruges til at bestemme divisorerne, hvis man kan finde primfaktoropløsningen. Hvis man f.eks. kender primfaktoropløsningen $195 = 3 \cdot 5 \cdot 13$, kan man ved alle de mulige kombinationer af de 3 primfaktorer finde divisorerne, der altså er (husk, at vi nu har begrænset os til naturlige tal):

$$d_0 = 1$$
$$d_1 = 3$$
$$d_2 = 5$$
$$d_3 = 13$$
$$d_4 = 3 \cdot 5 = 15$$
$$d_5 = 3 \cdot 13 = 39$$
$$d_6 = 5 \cdot 13 = 65$$
$$d_7 = 3 \cdot 5 \cdot 13 = 195$$

Eksempel 6.17: Et andet eksempel er $145748 = 2^2 \cdot 83 \cdot 439$, der har divisorerne:

$$d_0 = 1$$
$$d_1 = 2$$
$$d_2 = 83$$
$$d_3 = 439$$
$$d_4 = 2 \cdot 2 = 4$$
$$d_5 = 2 \cdot 83 = 166$$
$$d_6 = 2 \cdot 439 = 878$$
$$d_7 = 83 \cdot 439 = 36437$$
$$d_8 = 2 \cdot 2 \cdot 83 = 332$$
$$d_9 = 2 \cdot 2 \cdot 439 = 1756$$
$$d_{10} = 2 \cdot 83 \cdot 439 = 72874$$
$$d_{11} = 2 \cdot 2 \cdot 83 \cdot 439 = 145748$$

Benyt i de følgende tre opgaver Maple til at opløse tallet i primfaktorer og bestem derefter…:

Opgave 6.18: divisorerne i 12192937.

Opgave 6.19: divisorerne i 417567.

Opgave 6.20: divisorerne i 124729.

Opgave 6.21: Et tal *n* kan opløses i primfaktorerne $n = p_1 \cdot p_2$, hvor primtallene er forskellige. Hvor mange divisorer har tallet?

Opgave 6.22: Et tal *n* kan opløses i primfaktorerne $n = p_1 \cdot p_2 \cdot p_3$, hvor primtallene er forskellige. Hvor mange divisorer har tallet?

Opgave 6.23: Et tal *n* kan opløses i primfaktorerne $n = p_1^2 \cdot p_2$, hvor primtallene er forskellige. Hvor mange divisorer har tallet?

Opgave 6.24: Et tal *n* kan opløses i primfaktorerne $n = p_1^2 \cdot p_2^2 \cdot p_3$, hvor primtallene er forskellige. Hvor mange divisorer har tallet?

Opgave 6.25: Et tal *n* kan opløses i primfaktorerne $n = p_1^4$. Hvor mange divisorer har tallet?

Opgave 6.26: Et tal *n* kan opløses i primfaktorerne $n = p_1^7$. Hvor mange divisorer har tallet?

Opgave 6.27 (fra Georg Mohr 2006): Et naturligt tal *n*, som højst er 500, har den egenskab, at når man vælger et tal *m* tilfældigt blandt tallene 1, 2, 3, …, 499, 500, så er sandsynligheden $\frac{1}{100}$ for at *m* går op i *n*. Bestem den størst mulige værdi af *n*.

Som du nok husker fra overskriften til kapitlet, går vi nu for en kort stund væk fra begrænsningen til naturlige tal og ser på nogle sætninger (i daglig tale omtalt som 6.28'erne), hvoraf den første egentligt i sin ordlyd er overflødig, da den - som du snart vil se - er et simpelt korollar til sætning 6.28.b. Men det er et herligt bevis, så alene af den grund kommer den her:

Sætning 6.28: $\sqrt{2}$ er et irrationalt tal.

Bevis: Sætningen bevises ved et indirekte bevis (modstridsbevis).

Antag, at $\sqrt{2}$ er rationalt, dvs. at det kan skrives som en uforkortelig brøk: $\sqrt{2} = \frac{n}{m}$.

m kan ikke være 1, da man så har $\sqrt{2} = n$, dvs. så skulle det være et naturligt tal, hvilket vi ved, at det ikke er. *n* kan heller ikke være 1, for så giver brøken et tal mindre end 1, og vi ved, at $\sqrt{2}$ er et tal større end 1. Dvs. at *n* og *m* begge er større end 1.

n og *m* kan ifølge *Aritmetikkens Fundamentalsætning* begge skrives som et produkt af primfaktorer, og da brøken er uforkortelig, har de ingen fælles faktorer. Dvs:

$$\sqrt{2} = \frac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}}{q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\beta_t}} \Leftrightarrow \sqrt{2} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\beta_t} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \Leftrightarrow 2 \cdot q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdot \ldots \cdot q_t^{2\beta_t} = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2} \cdot \ldots \cdot p_s^{2\alpha_s}$$

Men så må et af primtallene på højresiden – hvis de er ordnet, er det p_1 – være tallet 2, for det går jo op i venstresiden og må derfor også gå op i et af primtallene på højresiden (jævnfør beviset for *AF* eller lemma 6.6). Vi kan derfor forkorte med tallet 2 på begge sider, og da $p_1 = 2$, får man altså $q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdot \ldots \cdot q_t^{2\beta_t} = 2 \cdot p_1^{2\alpha_1 - 2} \cdot p_2^{2\alpha_2} \cdot \ldots \cdot p_s^{2\alpha_s}$.

Men nu kan vi altså se, at et af primtallene på venstresiden må være 2 (hvis de er ordnet, er det q_1), for 2 er jo divisor i højresiden. Dette er i modstrid med, at *n* og *m* ikke har fælles faktorer, for de har jo begge faktoren 2. Vores antagelse om at $\sqrt{2}$ er rationalt, må altså være forkert. Dermed kan det konkluderes, at $\sqrt{2}$ er et irrationalt tal.

Det gik jo meget nemt. Skal vi så ikke fortsætte med at bevise, at π også er et irrationalt tal?

Nej, det er langt fra så let. Det blev først vist i 1761 af Johann Heinreich Lambert, da han arbejdede med tangensfunktionen. Man havde regnet med, at π var irrationalt, men beviset havde ladet vente på sig. Samme år udgav Lambert desuden et værk om stjerner og galakser. Så han havde gang i lidt forskellige ting.

Men lad os vende tilbage til kvadratrødderne. Er der noget specielt i, at $\sqrt{2}$ er irrationalt, eller gælder det for andre kvadratrødder? Det er jo ikke svært at finde kvadratrødder, der er naturlige tal. Her tager man bare alle kvadrattallene som radikander. Men findes der naturlige tal, hvis kvadratrødder er rationale, men ikke naturlige, tal?

Øvelse 6.28.a: Prøv at finde et eller flere naturlige tal, hvis kvadratrødder er rationale – men ikke naturlige – tal, og når du er kommet frem til, at det ikke kan lade sig gøre, kan du gå videre til sætning 6.28.b. og blive bekræftet i din formodning.

Sætning 6.28.b: Hvis *n* er et naturligt tal, er $\sqrt{n}$ enten et naturligt tal eller et irrationalt tal.

Bevis: Sætningen bevises endnu en gang med et modstridsbevis, og det minder om beviset for 6.28.

Lad os antage, at *n* er et naturligt tal, og $\sqrt{n}$ er et rationalt – men ikke et naturligt – tal.

Der findes så indbyrdes primiske (hele) tal *a* og *b*, hvor $b>1$, og hvor $\sqrt{n}=\frac{a}{b}$.

Tæller og nævner kan opløses i primtal ifølge *Aritmetikkens Fundamentalsætning*, så man har:

$$\sqrt{n}=\frac{p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}}{q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_t^{\beta_t}} \Leftrightarrow n\cdot q_1^{2\beta_1}\cdot q_2^{2\beta_2}\cdot\ldots\cdot q_t^{2\beta_t}=p_1^{2\alpha_1}\cdot p_2^{2\alpha_2}\cdot\ldots\cdot p_s^{2\alpha_s},$$

hvor der er mindst ét q_1, men hvor man evt. har $a=1$, dvs. formelt *s = 0* i tælleren, da der så ikke er nogen primtal i tælleren. Og da *a* og *b* er indbyrdes primiske, er der ingen fælles primtal i tæller og nævner.

Men her er der så en modstrid, for de to sider i ligningen er jo samme tal, men venstresidens opløsning i primfaktorer indeholder mindst ét primtal q_1, og dette primtal indgår ifølge antagelsen om indbyrdes primiske tal IKKE på højresiden. Men da primfaktoropløsningen er entydig ifølge *Aritmetikkens Fundamentalsætning*, så kan højre- og venstresiden ikke være ens.

Vores antagelse om, at $\sqrt{n}$ er et rationalt tal, fører altså til en modstrid, så sætningen er bevist.

Og så tilbage til primtallene!

Du skal være opmærksom på, at Maple har en test af primtal "*isprime*", der fortæller, om et tal er et primtal. F.eks. vil "*isprime(7)*" give svaret "*true*".

Hvis man ser på primtallene ordnet efter størrelse og stillet op på en række, kan man snart opdage, at tætheden af dem som helhed hurtigt bliver mindre og mindre. Det virker nok ikke så mærkeligt, da et stort tal alt andet lige må have flere "muligheder" for at have ikke-trivielle divisorer.

Men prøver man at tælle videre, vil man opdage, at antallet af primtal inden for et vist interval afgjort ikke kan beskrives på en simpel måde. Se på nedenstående tabel, der angiver antallet af primtal i 10 intervaller på 1000 tal:

Tallene	1-1000	1001-2000	2001-3000	3001-4000	4001-5000	5001-6000	6001-7000	7001-8000	8001-9000	9001-10000
Antal primtal	168	135	127	120	119	114	117	107	110	112

Først ses et klart fald, men derefter bliver det mere kryptisk.

Så lad os i stedet se på noget, man har mere styr på:

Sætning 6.29: Der er uendelig mange primtal.

Det er vist mest almindeligt at bevise dette med et indirekte bevis – hvilket kan have historiske årsager, som vi skal se i næste kapitel - og det følger som 'Bevis A'. Der er dog en vigtig pointe i et andet – direkte – bevis, så det følger som 'Bevis B':

Bevis A for sætning 6.29: Det antages, at der IKKE er uendelig mange primtal. Samtlige primtal kan derfor skrives som en endelig følge $p_1, p_2, p_3,\ldots,p_n$. Se nu på tallet:

$P=p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_n+1$. Dette tal er enten et primtal eller kan opløses i primfaktorer ifølge *Aritmetikkens Fundamentalsætning*. Men det sidste kan ikke være muligt, for ingen af primtallene $p_1, p_2, p_3,\ldots,p_n$ kan være divisor i *P*, da de er divisorer i $p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_n$, men ikke i 1. Dermed må *P* være et primtal. Men det er i modstrid med, at $p_1, p_2, p_3,\ldots, p_n$ udgjorde samtlige primtal. Vores antagelse om endeligt mange primtal må derfor være forkert.

Øvelse 6.30: I beviset benyttes $P = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$ til at skabe et nyt primtal. Kan man altid skabe et nyt primtal på denne måde ud fra 2 eller flere primtal?
Hvis ja, gå til øvelse 6.31. Hvis nej, gå til Opgave 6.32.

Øvelse 6.31: Prøv at bruge metoden på de 6 laveste primtal. Gå derefter til Opgave 6.32.

Opgave 6.32: Hvordan kan det gå galt, når det gik godt i beviset? Er der noget, vi har overset i beviset, eller hvor er "fejlen"?

Opgave 6.33: Bestem det mindste "primtal" skabt på denne måde, der IKKE er et primtal.

Men vi skal nu se, hvordan man faktisk KAN skabe et nyt primtal.

Bevis B for sætning 6.29: Lad der være givet *n* forskellige primtal $p_1, p_2, p_3, ..., p_n$.

Nu konstrueres endnu et primtal på en snedig måde. Se som før på tallet $p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Lad nu *P* være den mindste primfaktor i dette tal. En sådan findes nødvendigvis, for enten er tallet et primtal og er derfor selv den mindste primfaktor, eller også kan tallet ifølge *Aritmetikkens Fundamentalsætning* opløses i primfaktorer, hvoraf én er den mindste. At denne primfaktor er forskellig fra alle primtallene $p_1, p_2, ..., p_n$ følger af, at de alle er divisorer i $p_1 \cdot p_2 \cdot ... \cdot p_n$, men ikke i 1. *P* er altså et nyt primtal, og med samme metode – hvor *P* inkluderes blandt primtallene – kan man altså blive ved med at konstruere nye primtal, dvs. der må være uendelig mange primtal.

Opgave 6.34: Er det nødvendigt, at man netop vælger den mindste primfaktor?

Eksempel 6.34.a: Efter i opgave 6.34 at have overbevist sig selv om, at man kunne vælge en hvilken som helst af primfaktorerne, kan man naturligvis lige så godt tage skridtet fuldt ud og sige, at man benytter samtlige forskellige primfaktorer som nye primtal. Så bliver "fremstillingen" af primtal jo mere effektiv. Så lad os se på, hvordan metoden fra bevis B fungerer i praksis.

Hertil har vi brug for et eller flere primtal som udgangspunkt. Lad os begynde helt fra bunden, så vi nøjes med ét.

Og nu har vi jo brug for et vilkårligt primtal, så jeg tager min tyvesidede terning og slår, indtil jeg får et primtal……..det blev 13. Så nu begynder fremstillingen:

Vi skal tage produktet af alle vores primtal (her blot 13) og lægge 1 til:

$13 + 1 = 14$

14 er et sammensat tal, der kan primfaktoropløses: $14 = 2 \cdot 7$

Dvs. 2 og 7 er de nye primtal, og hermed har man primtallene 13, 2 og 7.

Så tager vi igen produktet og lægger 1 til:

$2 \cdot 7 \cdot 13 + 1 = 183$

Dette er et sammensat tal med primfaktoropløsningen: $183 = 3 \cdot 61$

Dvs. at listen med primtal nu er 13, 2, 7, 3 og 61.

Processen kører igen:

$2 \cdot 3 \cdot 7 \cdot 13 \cdot 61 + 1 = 33307 = 19 \cdot 1753$

Ny primtalsliste: 2, 3, 7, 13, 19, 61 og 1753.

$2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 61 \cdot 1753 + 1 = 1109322943 = 97 \cdot 11436319$

Ny primtalsliste: 2, 3, 7, 13, 19, 61, 97, 1753 og 11436319.

$2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 61 \cdot 97 \cdot 1753 \cdot 11436319 + 1 = 1230597390756858307$

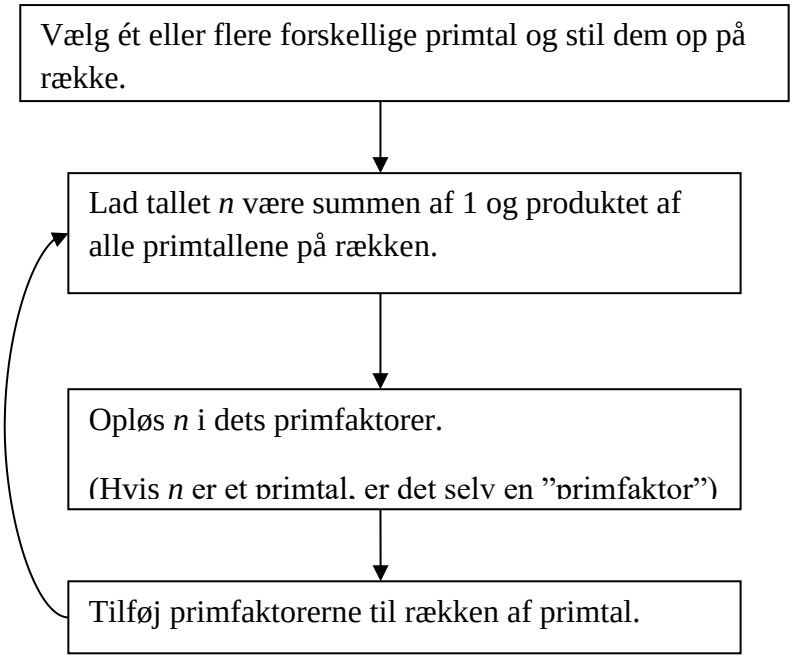
Og her er så et tilfælde, hvor det fremkomne tal faktisk ER et primtal, som i dette tilfælde udgør det ekstra primtal, så listen nu lyder:

2, 3, 7, 13, 19, 61, 97, 1753, 11436319 og 1230597390756858307

Og sådan fortsætter man. Bemærk at de fremkomne primfaktorer altid er **nye** primtal, hvilken jo også fremgik af beviset.

Du skulle gerne have bemærket, at eksempel 6.34.a angiver en algoritme til at fremstille flere og flere primtal. Den kunne lyde:

ALGORITME TIL FREMSTILLING AF PRIMTAL



Eksempel 6.34.b: Nu bruger jeg algoritmen med primtallet 2 som udgangspunkt. Jeg skriver kun de fremkomne lister op, så du kan selv prøve algoritmen, hvis du vil kontrollere det:

2
2, 3
2, 3, 7
2, 3, 7, 43
2, 3, 7, 13, 43, 139
2, 3, 7, 13, 43, 139, 3263443
2, 3, 7, 13, 43, 139, 547, 607, 1033, 31051, 3263443
2, 3, 7, 13, 43, 139, 547, 607, 1033, 29881, 31051, 67003, 3263443, 9119521, 6212157481

Eksempel 6.34.c: Med tallet 5 som udgangspunkt fås:

5
2, 3, 5
2, 3, 5, 31
2, 3, 5, 7, 19, 31
2, 3, 5, 7, 19, 31, 37, 3343
2, 3, 5, 7, 19, 31, 37, 79, 3343, 193662529
2, 3, 5, 7, 19, 31, 37, 79, 3343, 122449, 1650601, 193662529, 1158105259

Eksempel 6.34.d: Med primtallene 3, 7 og 11 som udgangspunkt fås:

3, 7, 11
2, 3, 7, 11, 29
2, 3, 7, 11, 29, 13399
2, 3, 7, 11, 29, 13399, 179519803
2, 3, 7, 11, 29, 307, 673,13399, 84913, 1836949, 179519803

Eksempel 6.34.e: Med primtallene 2, 3, 5, 7, 11, 13 og 17 som udgangspunkt fås:

2, 3, 5, 7, 11, 13, 17
2, 3, 5, 7, 11, 13, 17, 19, 97, 277
2, 3, 5, 7, 11, 13, 17, 19, 67, 97, 109, 277, 35686837
2, 3, 5, 7, 11, 13, 17, 19, 67, 97, 109, 151, 277, 35686837, 37475773, 12003037661557

Opgave 6.34.f: Benyt algoritmen med 3 som udgangspunkt.
Hvad er det største primtal, du har fået skabt, når du i alt har 15 primtal?

Opgave 6.34.g: Benyt algoritmen med 11 som udgangspunkt.
Hvad er det største primtal blandt de første 16 primtal, du har skabt?

Hvis du fik lavet opgave 6.34.g, har du fået forbedret dine forudsætninger for at kunne gennemføre øvelserne 6.35-6.41.

Bemærk manglen på system i ovenstående rækker af primtal. Eller måske kan du se et system i tallene? Hvis du kan, er der temmelig mange universiteter, der gerne vil høre fra dig.

Eksemplerne og opgaverne i 6.34-serien lægger op til en del spørgsmål:

Findes der et udgangspunkt af ét eller flere primtal, der fører til primtallet 9119521? Her kender vi dog svaret, da vi i eksempel 6.34.b så, at udgangspunktet 2 fører til dette tal.

Men hvad med primtallet 98143? Eller generelt: Vil alle primtal kunne fremstilles på denne måde?

Tallet 2 og tallet 3 som udgangspunkt for algoritmen fører til de samme primtal. Er der flere tal, der efter et vist antal skridt kommer ind på samme 'spor' og derefter fører til samme primtal? Og er der uendeligt mange? Nu er der ikke mere plads på siden, så find selv på flere spørgsmål.

Der foregår en løbende jagt på større og større primtal. Computeres regnekraft har gjort dette arbejde muligt.

Det størst kendte primtal var i 1999 tallet $2^{26972593} - 1$, der er et tal med 2.098.960 cifre.

I 2008 var man nået op på $2^{43112609} - 1$, der har 12.978.189 cifre.

Fem år senere blev det overgået med $2^{57885161} - 1$, der har 17.425.170 cifre.

I 2016 lykkedes det så at finde $2^{74207281} - 1$, der har 22.338.618 cifre.

I januar 2020 fandt man $2^{82589933} - 1$, der har 24.862.048 cifre.

I begyndelsen af 1990'erne var det $2^{216091} - 1$, et tal der ikke længere er blandt de 100 største, kendte primtal.

De 8 største, kendte primtal er alle såkaldte Mersenne-primtal (se kapitel 9). Men nu melder det vigtige spørgsmål sig så:

Øvelse 6.35: Når man kan snakke om det største, kendte primtal, kan der så findes en metode til at konstruere nye primtal? Hvis ja, så gå til øvelse 6.36. Hvis nej, gå til øvelse 6.37.

Øvelse 6.36: Men hvis der findes en sådan metode, hvorfor bruger man den så ikke til at konstruere et primtal, der er større end det størst kendte?
Hvis det skyldes, at metoden blot giver et nyt primtal, men ikke nødvendigvis et stort primtal, så gå til øvelse 6.38. Hvis du nu har ændret mening og kan se, at der ikke kan være en metode, så gå til øvelse 6.37. Hvis du mener, at du har en ikke omtalt forklaring, så gå til øvelse 6.39.

Øvelse 6.37: Men i bevis B for sætning 6.29 og i alle eksempler og opgaver i 6.34-serien viste vi jo netop en algoritme til at konstruere nye primtal. Hvis du mener, at der er noget i beviset eller algoritmen, der ikke holder, så gå til øvelse 6.40. Hvis du har ændret mening, så du nu mener, at der findes en sådan metode, så gå til øvelse 6.36.

Øvelse 6.38: Men er det ikke blot et spørgsmål om at bruge metoden igen og igen, indtil der ikke er flere forskellige primtal mindre end det største, kendte primtal, hvorefter det næste primtal nødvendigvis må være større? Hvis du mener, at det kræver for mange udregninger, så gå til øvelse 6.41. Hvis du har ændret din mening, så gå tilbage til øvelse 6.36.

Øvelse 6.39: Forklar din lærer, hvad du mener, der er galt. Hvis din forklaring er forkert, så gå tilbage til øvelse 6.36. Hvis din forklaring er god, har du vundet, og kan springe ned til efter øvelserne.

Øvelse 6.40: Forklar din lærer, hvad der er galt i beviset. Hvis det lykkes, så har du vundet. Hvis det ikke lykkes, så gå tilbage til øvelse 6.37.

Øvelse 6.41: Det er en god pointe, men det er ikke årsagen i dette tilfælde. Gå tilbage til øvelse 6.36.

Der er noget fascinerende ved metoden i ’Bevis B for sætning 6.29’. Den giver faktisk en metode til at bestemme nye primtal, men det er en metode, der KUN fungerer, HVIS man er i stand til at opløse det pågældende tal i primfaktorer. Man ved, at der findes sådan en primfaktoropløsning, for det siger *Aritmetikkens Fundamentalsætning*, men den siger ikke noget om, HVORDAN man finder en sådan opløsning. Og det viser sig faktisk at være temmelig svært, når tallene bliver store.

Hvis du ikke fik lavet opgave 6.34.g, har du indtil videre benyttet Maples ’ifactor’-funktion uden problemer, men prøv at benytte den på følgende tal (ét tal pr. linje), der alle består af 2 primfaktorer:

2942579833

690658583643821537280313356554382510858861825938017254 1

2626201490012248960996342309824296480856894874 19

4520190173752212659968884844160748157219904959320818381073694953884093914468773716038430990162872390489

4039730531721464800046401099250298709464840759958196296054782984234969952602118827814243651953454944253772354972041370 03

Tjek tiderne for Maples behandling. Det tredje tal tager lidt længere tid end det andet tal, selvom dette er længere. Det hænger sammen med, at det består af et relativt lille primtal ganget med et relativt stort primtal, mens de andre tal består af 2 primtal af nogenlunde samme størrelse.

Det næstsidste tal kunne en lommeregner ikke klare. En elev prøvede med helt nye batterier i en juleferie, og batterierne blev brugt op, uden at et resultat blev nået. Det består af 102 cifre.

Det sidste tal er ”fremstillet” af matematikeren Anders Thorup fra KU ud fra 2 primtal med 60 cifre. Han hævdede, at ingen læser nogensinde ville være i stand til at opløse dette tal med 120 cifre i sine 2 primfaktorer. At han kunne hævde dette så skråsikkert skyldes, at antallet af tests for primfaktorer, der skal gennemføres, vokser eksponentielt med tallets størrelse. Så det løber helt løbsk, og selvom computeres regnekraft også vokser voldsomt, så kunne han nok godt regne med, at regnekraften ikke ville blive stor nok.

Nu viste det sig imidlertid, at en gruppe matematikere i april 2003 alligevel fik faktoriseret dette tal ved at lade en meget kraftig computer regne uafbrudt i 10 dage.

Så i dette tilfælde var matematikeren lidt for kry. Men faktisk behøver han ikke at være så ked af det, for med den forbedrede regnekraft, vil han nemt kunne finde to nye primtal med f.eks. 70 cifre, og hvis han ganger dem sammen får han et nyt tal, som den pågældende computer aldrig kan klare.

Det væsentlige i alt dette er nemlig, at det er nemmere at konstruere et tal, der er et produkt af to primtal, end det er at faktorisere det pågældende tal.

Dette bruges inden for kryptering, og det er et af de områder, man mener et bevis for ét af de mest berømte uløste matematiske problemer – Riemann-hypotesen – vil kunne belyse. Men hvis du vil vide mere om dette, må du selv finde mere information.

Som afslutning på dette kapitel ses på endnu en anvendelse af primfaktoropløsninger, nemlig hvordan man nemt kan bestemme det mindste fælles multiplum. Metoden fungerer dog kun, HVIS man kan finde primfaktoropløsninger, så der er – som nævnt ovenfor – nogle begrænsninger.

Men først skal begrebet multiplum lige defineres:

Definition 6.42: Et *multiplum* af et tal a er et tal, der har a som divisor.

Bemærkning 6.43: Man kan også finde betegnelsen *mangefold* brugt i stedet for *multiplum*. Det er oplagt, at der er uendeligt mange multipla af et tal a, nemlig tallene:

$$1\cdot a,\ 2\cdot a,\ 3\cdot a,\ 4\cdot a,\ 5\cdot a,\ 6\cdot a,\ \ldots$$

Bemærkning 6.44: Betegnelsen multiplum kan også bruges om andet end tal, hvor 'divisor' så skal erstattes af 'faktor', men så er det jo ikke længere talteori…..

Som bekendt er det ikke svært at finde et fælles multiplum for 2 eller flere tal. Man multiplicerer bare de pågældende tal (en metode der kan bruges, når man skal finde fællesnævner for brøker). Men hvis man nu gerne vil finde det mindste fælles multiplum (og det kunne være rart, hvis brøkerne skal blive så overskuelige som muligt), så kan man se på tallenes primfaktoropløsninger.

Eksempel: Man vil finde det mindste fælles multiplum for tallene 62700, 101200 og 17480, der har primfaktoropløsningerne:

$$62700 = 2^2\cdot 3\cdot 5^2\cdot 11\cdot 19$$

$$101200 = 2^4\cdot 5^2\cdot 11\cdot 23$$

$$17480 = 2^3\cdot 5\cdot 19\cdot 23$$

Hvis man bare multiplicerer tallene, får man 110914795200000, der altså er et fælles multiplum. Men nu skal det mindste fælles multiplum findes:

Begynd med det første tals primfaktoropløsning:

$$2^2\cdot 3\cdot 5^2\cdot 11\cdot 19$$

Hvis det andet tal skal være divisor i det søgte tal, mangler der to 2-taller og tallet 23, der derfor tilføres:

$$2^2\cdot 3\cdot 5^2\cdot 11\cdot 19\cdot 2^2\cdot 23$$

Og som det ses indeholder ovenstående alle de primfaktorer (også regnet med multiplicitet – dvs. antallet af gange det pågældende primtal optræder), som det tredje tal består af, så det er divisor i ovenstående.

Dermed er $2^2\cdot 3\cdot 5^2\cdot 11\cdot 19\cdot 2^2\cdot 23 = 5768400$ mindste fælles multiplum.

Det er klart, at man egentlig skal bevise, at ovenstående fører til det mindste fælles multiplum, men det udsættes til øvelse 6.48.

Opgave 6.45: Bestem det mindste fælles multiplum for følgende talsæt (du må gerne bruge Maple til at finde primfaktoropløsninger):

a) 3732498, 896769 og 2157093
b) 375668979, 161000991 og 876560951
c) 562500 og 18000
d) 2490026 og 2980185

Opgave 6.46: Du skal nu tænke dig frem til hvilke af følgende sætninger, der er rigtige:

a) For alle talsæt bestående af n tal, hvor $n > 1$, findes et mindste fælles multiplum.
b) Det mindste fælles multiplum for et talsæt er divisor i alle fælles multipla for talsættet.
c) Hvis et talsæt består af tal, der alle er indbyrdes primiske, så er det mindste fælles multiplum produktet af alle tallene.
d) Hvis tallene a og b har det mindste fælles multiplum b, så er a divisor i b.

Øvelse 6.47: Prøv at finde beviser for nogle af ovenstående sætninger.
Øvelse 6.48: Vis, at den gennemgåede metode fører til det mindste fælles multiplum.

Kapitel 7: EUKLIDS VERSION

(naturlige tal – næsten)

Euklid var som bekendt en græsk matematiker, der samlede, videreudviklede og systematiserede en stor del af sin tids matematik i flere værker, hvoraf nogle er bevaret, og blandt disse er *Elementer* det mest kendte. Han levede omkring 300 fvt. Dette er fastsat ud fra, hvem han levede samtidigt med, for man kender hverken hans alder, fødsels- eller dødsår. Det fortælles, at han på kong Ptolemaios I's forespørgsel i forbindelse med læsningen af *Elementer*, om der ikke fandtes en lettere måde at lære matematikken på, skulle have svaret, at "der findes ingen kongevej til geometrien".

Kong Ptolemaios I regerede Ægypten fra 323 fvt. til 283 fvt., og Euklid levede i Alexandria, der på den tid var samlingssted for viden inden for mange områder.

Hvad en græker lavede i en by, der nu ligger i Ægypten, og om al denne viden befandt sig i hovederne på mennesker eller måske i et eller andet bibliotek eller evt. begge dele, ja, det er en længere historie, som du selv må grave i, hvis du vil vide mere.

Euklids kommentar til kong Ptolemaios er naturligvis guf for matematikere, men Ptolemaios havde nu fat i noget, for *Elementer* er virkelig ikke så let tilgængelig som moderne undervisningsbøger i matematik.

Den består af 13 bøger, der behandler forskellige emner.

Første bog indledes med 23 definitioner, der fastlægger begreber inden for geometri (bl.a. punkt, linje, cirkel og trekanter), 5 postulater og 5 aksiomer, der er påstande eller sætninger, der ikke kan bevises, men som regnes for at være så oplagte, at alle kan godtage dem.

Derefter kommer første sætning med efterfølgende bevis, så næste sætning med bevis, osv. Og første bog slutter med sætningerne 47 og 48 (der er Pythagoras' læresætning).

Anden bog begynder med 2 nye definitioner, hvorefter der følger flere sætninger.

Og sådan fortsættes. Nødvendige begreber defineres, og sætninger indføres og bevises. Aldrig kommentarer, eksempler, opgaver eller perspektivering. Alt er ren matematik.

Egentlig kan man ikke bare springe ind midt i *Elementer*, for sætningerne baseres hele tiden på det foregående. Men det gør vi nu alligevel…..

Vi skal se på, hvordan Euklid beskrev flere af de sætninger eller egenskaber, som vi allerede har været inde på.

I dette historiske tilbageblik kommer vi ind i begyndelsen af *Elementernes* bog 7. Euklid indfører ingen steder nye postulater eller aksiomer, dvs. han arbejder hele tiden med de 5 postulater og 5 aksiomer fra begyndelsen af første bog. Men han indfører som nævnt nye definitioner i begyndelsen af bøgerne, og da han efter at have arbejdet med geometriske figurer i de 6 foregående bøger nu er nået til tallene, har han brug for en række nye definitioner, der følger her – dog er 10 af dem udeladt:

Euklids definitioner i begyndelsen af bog VII:

1. Enheden er det, i kraft af hvilket enhver ting benævnes én.
2. Et tal er en af enheder sammensat mængde.
3. Et mindre tal er del af et større tal, når det måler det.
4. Og en samling dele, når det ikke måler det.
5. Og et større er mangefold af et mindre, når det måles af det mindre.
6. Et lige tal er et, som kan halveres.
7. Et ulige tal er et, som ikke kan halveres, eller hvis forskel fra et lige tal er enheden.
11. Et primtal er et tal, som kun måles af enheden.
12. Indbyrdes primiske tal er dem, der alene måles af enheden som fælles mål.
13. Et sammensat tal er et, som måles af et eller andet tal.
14. Indbyrdes sammensatte tal er dem, der måles af et tal som fælles mål.
22. Et perfekt tal er et, der er lige med dets dele.

Som det ses, indfører Euklid mange af de samme begreber, som vi allerede har gennemgået. Men der er nogle væsentlige forskelle, som de følgende opgaver omhandler.

Opgave 7.1: Hvilket eller hvilke tal, som vi arbejdede med i størstedelen af afsnit 6, betragter Euklid IKKE som et tal?

Opgave 7.2: I hvilke af definitionerne fremgår dette?

Euklid forklarer ikke, hvad der menes med, at et tal 'måles' af et andet tal. Måske er det et udtryk for en geometrisk tankegang, hvor et linjestykke fastsat som en enhed kan bruges til at udmåle, hvor mange enheder et givent linjestykke udgør. Det benyttes tydeligvis sammen med begrebet 'del' til at beskrive divisibilitet som i definition 1.1. Dog med én væsentlig forskel:

Euklid betragter ikke et tal som en del af sig selv, hvor vi betragter et tal som divisor i sig selv. Det fremgår implicit af definition 3, hvor han eksplicit lader de to tal være forskellige. På samme måde fremgår det af definition 5. Det bliver dog helt tydeligt i definition 11, hvor han definerer et primtal som et tal, der kun kan måles af enheden. Endelig fremgår det også af definition 22.

Ikke desto mindre skal du lægge mærke til, at han faktisk lader et tal måle sig selv i beviset for sætning 7.8 senere i dette kapitel.

Når man ikke arbejder med tal, bruger man stadig betegnelsen ”mål” i stedet for ”divisor”.

En lille pudsig detalje er definition 7, hvor Euklid giver to forskellige definitioner for det samme. Den sidste af dem er muligvis af ældre dato end den første. Aristoteles kritiserer denne definition (og Aristoteles levede før Euklid) for at være dårlig, da den definerer ulige ud fra lige.

Og så kan man jo også nyde definition 1. Det er ikke sort snak, men det er vist nærmere filosofi end matematik.

Opgave 7.3: Hvad menes i vores sprog med ’et perfekt tal’?
Opgave 7.4: Bestem de 2 laveste perfekte tal.

Og nu går det så løs med sætninger. Vi begynder med Euklids 1. sætning fra bog VII.

Euklids sætning 1 bog VII 7.5: Lad to ikke ens tal være givet, og lad det mindste vedvarende subtraheres fra det største. Hvis det tal, der bliver tilbage, ikke måler tallet før det indtil en enhed bliver tilbage, er de oprindelige tal indbyrdes primiske.

Det er nok ret svært at tolke, hvad Euklid egentlig mener. Men måske kunne du genkende Euklids algoritme i det særlige tilfælde, hvor de to tal er indbyrdes primiske? Hvis ikke, så gå tilbage og repetér denne algoritme og prøv at genkende den i sætningen.

Euklids bevis: Ved vedvarende subtraktion af det mindste af to ikke ens tal AB, CD fra det største, lad da det tal, der er tilbage, aldrig måle tallet før dette indtil en enhed bliver tilbage.

Jeg siger så, at AB, CD er indbyrdes primiske, dvs. at det kun er enheden, der måler AB, CD.

For hvis AB, CD ikke er indbyrdes primiske, så er der et tal, der måler dem.

Lad et tal måle dem, og lad det være E. Lad CD målende BF efterlade FA mindre end sig selv.

Lad AF målende DG efterlade GC mindre end sig selv og lad GC målende FH efterlade en enhed HA.

Eftersom E måler CD, og CD måler BF, måler E også BF.

Men det måler også hele BA. Derfor vil det også måle resten AF.

Men AF måler DG. Derfor måler E også DG.

Men det måler også hele DC. Derfor vil det også måle resten CG.

Men CG måler FH. Derfor måler E også FH.

Men det måler også hele FA. Derfor vil det også måle resten, enheden AH, selvom det er et tal, hvilket er umuligt.

Derfor vil intet tal måle tallene AB, CD. Derfor er AB, CD indbyrdes primiske.

Opgave 7.6: Vi har set denne type bevis før. Hvad er det for en slags?

Det er værd at bemærke, at Euklid ikke bruger kræfter på at forklare, at der ikke er noget specielt i, at det netop er AH, der er en enhed. Han lader det være op til læseren at se, at argumentationen kan føres på samme måde, uanset hvornår enheden optræder som resten ved en subtraktion.

Men det kan måske være svært at læse beviset, da notationen er anderledes end normalt. Så nu skal du prøve at gøre det lettere tilgængeligt:

Øvelse 7.7: Tegn tallene AB og CD som linjestykker og lav en skitse som illustration af beviset. Du skal kunne gennemføre beviset på tavlen ved hjælp af skitsen.

Ovenstående var som nævnt det, vi nu kalder 'Euklids algoritme' benyttet på indbyrdes primiske tal. I sætningen lige efter kommer så selve algoritmen:

Sætning 2 bog VII 7.8: Givet to ikke indbyrdes primiske tal, hvordan det største fælles mål findes.

Euklids bevis: Lad AB, CD være de to givne, ikke indbyrdes primiske tal.

Det kræves så at finde deres største fælles mål.

Hvis CD måler AB – og det måler også sig selv – er CD et fælles mål for CD, AB.

Og det er åbenbart, at det også er det største. For intet tal større end CD vil måle CD.

Men, hvis CD ikke måler AB, så vil det mindste af tallene AB, CD vedvarende subtraheret fra det største efterlade et tal, der vil måle tallet før dette.

For en enhed vil ikke blive efterladt. For så ville AB, CD være indbyrdes primiske, hvilket er i modstrid med antagelsen.

Derfor vil der efterlades et tal, der måler tallet før dette.

Lad nu CD målende BE efterlade EA mindre end sig selv, og lad EA målende DF efterlade FC mindre end sig selv. Og lad CF måle AE.

Eftersom CF måler AE, og AE måler DF, vil CF også måle DF.

Men det måler også sig selv. Derfor vil det også måle hele CD.

Men CD måler BE. Derfor måler CF også BE.

Men det måler også EA. Derfor vil det også måle hele BA.

Men det måler også CD. Derfor måler CF tallene AB, CD.

Derfor er CF et fælles mål for AB, CD.

Jeg siger dernæst, at det også er det største.

For hvis CF ikke er det største fælles mål for AB, CD, så vil et tal større end CF måle tallene AB, CD.

Lad sådan et tal måle dem, og lad det være G.

Eftersom G måler CD, mens CD måler BE, måler G også BE.

Men det måler også hele BA. Derfor vil det også måle resten AE.

Men AE måler DF. Derfor vil G også måle DF.

Men det måler også hele DC. Derfor vil det også måle resten CF, dvs. den større vil måle den mindste, hvilket er umuligt.

Derfor er der intet tal større end CF, der måler tallene AB, CD. Derfor er CF det største fælles mål for AB, CD.

Porisme: Ud fra dette er det åbenbart, at hvis et tal måler to tal, så vil det også måle deres største fælles mål.

Man kan sige, at der ikke var nogen grund til at se dette bevis, da vi allerede har bevist sætningen tidligere. Men nu fik du Euklids version og har måske fået en fornemmelse for hans måde at tænke på.

Opgave 7.9: Hvilket ord har vi tidligere brugt om det, Euklid kalder et 'porisme'.

Euklids næste sætning berører noget, vi ikke tidligere har været inde på:

Sætning 3 bog VII 7.10: Givet tre ikke parvis primiske tal, hvordan det største fælles mål findes.

Han gennemgår altså en metode til at finde den største fælles divisor for 3 tal, der ikke er parvis primiske, og han beviser – selvfølgelig – også, at den virker. Men først skal du prøve at finde en metode:

Øvelse 7.11: Kan du finde en metode til at bestemme sådan en største fælles divisor? Hvis ja, så gå til opgave 7.12. Hvis nej, så gå til forklaring 7.13.

Opgave 7.12: Bestem den største fælles divisor for følgende taltripler:

a) 924, 1380 og 38748
b) 331149, 624351 og 889707
c) 2050898, 20224493 og 8843835

Forklaring 7.13: Metoden går ud på, at man først bestemmer den største fælles divisor *d* for 2 af tallene, og derefter bestemmer man den største fælles divisor for *d* og det sidste tal. Brug metoden til at løse opgave 7.12.

Øvelse 7.14: Kan du argumentere for, at din – eller Euklids – metode rent faktisk giver den største fælles divisor? Hvis ja, så meld dig til at gå til tavle og give din forklaring.

Euklid arbejder så videre med en række sætninger og kommer lidt senere til følgende:

Sætning 16 bog VII 7.15: Hvis to tal ved multiplikationer med hinanden giver nogle bestemte tal, så vil disse af de første bestemte tal være lige store.

Opgave 7.16: Hvordan udtrykker vi normalt denne sætning?

At Euklid beviser sådan en sætning, viser noget om grækernes syn på matematik. De færreste mennesker ville nok have tænkt på, at man kunne – eller skulle – bevise denne sætning. Grækerne forsøgte at komme helt ned og få styr på matematikkens grundlag.

I beviset benytter Euklid tidligere sætningers resultater, så vi springer det over.

Lidt senere følger en række sætninger om primtal og primiske tal, men vi tager nu et spring to bøger frem til en velkendt sætning på en ikke velkendt form:

Sætning 20 bog IX 7.17: Der er flere primtal end et hvilket som helst fastsat antal primtal.

Opgave 7.18: Hvilken sætning fra kapitel 6 svarer denne sætning til?

Når Euklid ikke bruger betegnelsen 'uendelig', hænger det sammen med grækernes "modvilje" over for dette begreb. Bemærk forskellen mellem de 2 formuleringer.

Men beviser minder meget om bevis A for sætning 6.29, der – som du måske erindrer – var et indirekte bevis:

Euklids bevis: Lad A, B, C være det fastsatte antal primtal. Jeg siger så, at der er flere primtal end A, B, C.

For lad det mindste tal, der måles af A, B, C være fundet, og lad det være DE. Lad enheden DF blive lagt til DE.

Så er EF enten et primtal eller ikke et primtal.

Lad det først være et primtal. Så har man fundet tallene A, B, C, EF, hvilket er flere end A, B, C.

Lad derefter EF ikke være et primtal. Det måles så af et primtal [Dette er indholdet af Euklids sætning 31 i bog VII. Bemærk at sådan en sætning følger af aritmetikkens fundamentalsætning, men at det omvendte ikke gælder.].

Lad EF være målt af primtallet G.

Jeg siger så, at G ikke er det samme som et af tallene A, B, C.

For, hvis det var muligt, så lad det være sådan.

Nu gælder A, B, C måler DE. Derfor vil G også måle DE.

Men det måler også EF.

Derfor vil G, der er et tal, måle resten, der er enheden DF, og det er en modstrid.

Derfor er G ikke det samme som et af tallene A, B, C.

Og ud fra hypotesen er det altså et primtal.

Derfor har man fundet primtallene A, B, C, G, hvilket er flere end det fastsatte antal A, B, C.

Hvis man ser på dette bevis og beviset for sætning 7.5, bemærker man måske, at når Euklid skal vise, at noget gælder for et vilkårlig stort, fastsat antal tal eller skridt, så viser han det for 3 tal eller skridt. Det kunne minde lidt om talemåden ”En, to, mange”.

Matematikere er ikke længere tilfredse med den slags beviser. De vil normalt bruge et *induktionsbevis*, der som udgangspunkt anvendes, hvis man skal vise, at et udsagn er sandt for alle naturlige tal:

1) Man viser først, at sætningen gælder for tallet 1 (nogle sætninger gælder måske kun for $n > 2$, og så viser man i stedet, at det gælder for tallet 3).
2) Så viser man, at HVIS sætningen gælder for tallet n, SÅ gælder den også for tallet $n + 1$.

Prøv at overveje, hvordan dette kan bevise en sætning, der skal gælde for alle naturlige tal.

Øvelse 7.19: Hvordan kan man bruge metoden til at vise sætninger, der gælder for alle hele tal?

Men hvordan beviser man så, at et induktionsbevis rent faktisk er ”tilladt” som bevis?

Svaret er, at det gør man ikke – for det KAN man ikke. Man betragter det som en ubeviselig egenskab ved de naturlige tal, og man kalder det så for *induktionsaksiomet*.

Du får ingen induktionsbeviser at se her. Hvis du vil vide mere om dem, må du selv finde yderligere informationer eller prøve at konstruere dine egne induktionsbeviser.

Kapitel 8: DIOFANTISKE TREKANTER

(naturlige tal)

Diofant menes at være født mellem 200-214 evt., og han levede ligesom Euklid i Alexandria – der stadig var centrum for viden. Han skrev bl.a. værket *Arithmetika*, der bestod af 13 bøger, hvoraf 6 er bevaret. I dette værk arbejder han med ligninger, der har hele eller rationale tal som løsninger. Det var usædvanligt, da grækerne ikke tidligere havde anset brøker som rigtige tal. Diofant fik senere tilnavnet "Algebraens fader".

Som det ses ovenfor, ved man ikke, hvornår han blev født. Men man regner med at kende hans levealder, da han indgår i en samling af talgåder fra det 5. århundrede:

Opgave 8.1: Diofants ungdom varede en sjettedel af hans liv; efter en syvendedel mere blev han gift; han fik skæg efter endnu en tolvtedel. Fem år senere fik han en søn, som levede halvt så længe som faderen, og Diofant døde fire år efter sønnen.
Hvor gammel blev Diofant?

Man har så senere – med henvisning til *Arithmetika* – indført betegnelsen diofantiske ligninger om ligninger, hvor man kun søger heltalsløsninger. Man kan dog også opleve betegnelsen brugt om ligninger, hvor man søger rationale løsninger. Vi vil her bruge betegnelsen *diofantisk* i den heltallige version, og når vi ifølge overskriften skal undersøge nogle *diofantiske trekanter*, er det altså trekanter, hvor sidelængderne er hele tal. Et eksempel kunne være den velkendte retvinklede trekant med sidelængderne 3, 4 og 5.

Først ser vi lige på den Pythagoræiske Læresætning og den Omvendte Pythagoræiske Læresætning (som nævnt Euklids sætninger 47 og 48 fra første bog i *Elementer*). Den første siger som bekendt, at i en retvinklet trekant er kvadratet på hypotenusen lig med summen af kateternes kvadrater (oftest skrevet $a^2 + b^2 = c^2$), mens den anden siger, at hvis trekantens sidelængder *a, b* og c, hvor *c* er den største, tilfredsstiller ligningen $a^2 + b^2 = c^2$, så er den retvinklet med den rette vinkel *C*.

Men dette er jo geometriske sætninger, så hvor kommer talteori ind i billedet?

Det gør det, når vi tager ligningen $a^2 + b^2 = c^2$ ud af sammenhængen og betragter den som en diofantisk ligning, dvs. vi vil prøve at finde heltalsløsninger til ligningen. Det fører så bagefter til, at vi kan bestemme samtlige pythagoræiske talsæt dvs. samtlige diofantiske, retvinklede trekanter, men så er vi igen tilbage til geometrien, og igen har Euklid på sin hjemmebane givet et bevis for den sætning, vi nu skal bevise rent talteoretisk.

Egentlig ønsker vi kun at finde de løsninger til $a^2 + b^2 = c^2$, der er naturlige tal, men du kan selv tænke lidt over det og se, at det ikke spiller den store rolle.

Vi kunne sådan set gå direkte til sætningen, men for at gøre beviset mere overskueligt indføres først en række lemmaer. Og husk: Vi arbejder i dette kapitel med naturlige tal.

Lemma 8.2: For vilkårlige tal *p* og *q* gælder $\left(p^2 + q^2\right)^2 = \left(p^2 - q^2\right)^2 + \left(2 \cdot p \cdot q\right)^2$

Øvelse 8.3: Bevis lemma 8.2.

Øvelse 8.4: Lad *p* og *q* være to tal, hvor *p* > *q*. Findes der en fast rækkefølge i størrelsen af tallene $\left(p^2 - q^2\right); \left(p^2 + q^2\right) og \left(2 \cdot p \cdot q\right)$? Eller måske er der ét af tallene, der altid er mindst? Prøv evt. med forskellige tal og se, om du kan finde noget, der gælder generelt. Prøv evt. også, om du kan finde et bevis for din påstand.

Lemma 8.5: For alle tal p og q, hvor $p > q$, gælder $\left(p^2+q^2\right) > 2\cdot p\cdot q$ og $\left(p^2+q^2\right) > \left(p^2-q^2\right)$.

Bevis: Det er oplagt, at sidste del af lemmaet gælder. For q^2 er positiv, og når man lægger noget positivt til et tal, p^2, så bliver resultatet større, end hvis man trækker det fra.

Så lad os se på første del.

Og lad os endnu engang gribe til et indirekte bevis.

Så vi antager, at $\left(p^2+q^2\right) \le 2\cdot p\cdot q$, hvilket fører til:

$$p^2+q^2-2\cdot p\cdot q \le 0 \quad \Leftrightarrow (p-q)^2 \le 0$$

Men da $p > q$, er udtrykket i parentesen ikke 0, så venstresiden er positiv, hvorved vi har den søgte modstrid, og lemmaet er altså bevist.

Bemærk, at lemmaet ikke siger noget om en sammenligning af tallene $\left(p^2-q^2\right)$ og $(2\cdot p\cdot q)$. Det skyldes, at der ikke gælder en lignende velordning. Så man kan altså kun sige, hvad det største af de 3 nævnte tal er, og det er $\left(p^2+q^2\right)$.

Som du måske er ved at fornemme, vil den kommende sætning beskæftige sig med tallene

$$(2\cdot p\cdot q),\ \left(p^2+q^2\right) \text{og } \left(p^2-q^2\right).$$

Øvelse 8.6: Prøv nu at se på de 2 sidste af ovennævnte tal. Hvis du fik at vide, at de begge var ulige, ville du så kunne sige noget om p og q med hensyn til lige/ulige? Hvis ja, så prøv at bevise din påstand. Hvis nej, så prøv dig frem med forskellige tal og se, om du kan finde et system.

Lemma 8.7: Hvis tallene $\left(p^2+q^2\right)$ og $\left(p^2-q^2\right)$ er ulige, så er netop et af tallene p og q lige.

Bevis: Det kan diskuteres, hvor meget der skal gøres ud af følgende bevis, for egentlig kan det gøres meget kort:

En sum eller differens af 2 tal bliver ulige, netop når netop ét af tallene er lige, og et kvadrat p^2 er ulige, netop når p er ulige. Dermed er sætningen vist.

Men man kan også gå mere systematisk til værks. F.eks. beviser Euklid i bog XI af *Elementer* (sætningerne 24-27), hvad man får ved at trække lige/ulige fra lige/ulige.

Et bevis for påstanden om, at kvadratet på et lige tal, giver et lige tal, mens kvadratet på et ulige tal, giver er ulige tal, kunne være:

$$p \text{ er lige} \Leftrightarrow p = 2n \Leftrightarrow p^2 = 4\cdot n^2 = 2\cdot\left(2\cdot n^2\right) \Rightarrow p^2 \text{ er lige}$$

$$p \text{ er ulige} \Leftrightarrow p = 2n+1 \Leftrightarrow p^2 = 4\cdot n^2+4n+1 = 2\cdot\left(2\cdot n^2+2n\right)+1 \Rightarrow p^2 \text{ er ulige}$$

Opgave 8.8: I linjerne 3 og 4 i beviset indgår ordene lige/ulige 4 gange. Hvilken eller hvilke af de 4 gange kan man IKKE bruge det andet af ordene (dvs. udskifte "lige" med "ulige" eller omvendt)?

Det er nok ikke særlig nemt at se, hvor disse lemmaer fører hen, for hvorfor kan det være interessant, om tal er lige eller ulige? Svaret på det følger senere. Nu skal vi først for en stund vende tilbage til ligningen $a^2+b^2=c^2$, for det må ikke glemmes, at det er den, det hele drejer sig om.

Hvis man har det pythagoræiske talsæt $(a,b,c)=(3,4,5)$, er det klart, at også talsættene $(a,b,c)=(6,8,10)$, $(a,b,c)=(9,12,15)$ og $(a,b,c)=(300,400,500)$ er pythagoræiske, for man har jo:

$$a^2+b^2=c^2 \quad \Leftrightarrow$$
$$n^2\cdot a^2+n^2\cdot b^2=n^2\cdot c^2 \quad \Leftrightarrow$$
$$(n\cdot a)^2+(n\cdot b)^2=(n\cdot c)^2$$

Dvs. hvis man har fundet ét pythagoræisk talsæt, så kan man skabe vilkårligt mange sæt ved enten at forlænge sættet med et naturligt tal eller forkorte det med en evt. fælles divisor.

Øvelse 8.9: Tag udgangspunkt i det pythagoræiske talsæt (10, 24, 26). Prøv at se, hvor mange pythagoræiske talsæt, du kan skabe på ½ minut, og prøv derefter at slå din egen rekord.

Opgave 8.10: Hvad gælder om alle de retvinklede trekanter (med hensyn til vinkler), du er kommet frem til i øvelse 8.9?

Det er oftest ikke så interessant med alle de ekstra pythagoræiske talsæt, man kan skabe ved ovenstående metode. Så man indfører en betegnelse, der fremhæver "grundstammen" blandt alle sådanne talsæt (lidt ligesom man tidligere fremhævede den principale rest):

Definition 8.11: Et *primitivt* talsæt er et talsæt, der ikke har andre fælles faktorer end 1.

Eksempler: 1) Talsættet (3,6,7) er primitivt, for godt nok indeholder 3 og 6 begge faktoren 3, men den er ikke en faktor i 7. Så der er ikke andre fælles faktorer end 1.
2) Talsættet (4,10,12) er ikke primitivt, for alle tre tal indeholder faktoren 2.

Opgave 8.12: Hvilke af følgende talsæt er primitive?

a) (2,7,9)
b) (1,2,4)
c) (3,4,5)
d) (6,8,10)
e) (5,12,13)
f) (15,36,39)
g) (12,35,37)
h) (2,3,5,15)

Opgave 8.13: Hvilke af talsættene fra opgave 8.12 er pythagoræiske talsæt?

Opgave 8.14: Hvilke af talsættene fra opgave 8.12 er primitive pythagoræiske talsæt?

Øvelse 8.15: Prøv at finde et talsæt (a,b,c), der opfylder ligningen $a^2+b^2=c^2$, og hvor netop 2 af tallene har en fælles faktor. Prøv evt. også at finde et bevis for, hvor mange af den slags talsæt, der findes. Hvis du går død i denne øvelse, så spring hastigt videre til næste lemma, der behandler dette problem.

Lemma 8.16: Lad talsættet (a,b,c) opfylde ligningen $a^2+b^2=c^2$. Hvis 2 af tallene har en fælles faktor, så indeholder det tredje tal også denne faktor.

Bevis: De to tal *a* og *b* står på samme måde i ligningen, så man skal kun undersøge de 2 muligheder, at det er *a* og *b*, der har en fælles faktor, eller at det er *a* og *c*.

Antag, at *a* og *b* har en fælles faktor, og lad den være *d*. Så gælder $a = d \cdot k_a$ og $b = d \cdot k_b$.

Man har så:

$$a^2 + b^2 = c^2 \quad \Leftrightarrow \quad (d \cdot k_a)^2 + (d \cdot k_b)^2 = c^2 \quad \Leftrightarrow \quad d^2 \cdot (k_a^2 + k_b^2) = c^2 \quad \Leftrightarrow$$

$$d \cdot \sqrt{k_a^2 + k_b^2} = c \quad \Leftrightarrow \frac{c}{d} = \sqrt{k_a^2 + k_b^2}$$

Argumentet under kvadratroden er et naturligt tal, så vi ved ifølge sætning 6.28.b, at kvadratroden enten er et naturligt tal eller et irrationalt tal. Og som det ses af ovenstående, er det ikke irrationalt, da det kan skrives som en brøk med hele tal i tæller og nævner, så det må være et naturligt tal. Og det næstsidste udtryk af ovenstående viser så, at *d* også er divisor i *c*.

Herefter antages, at *a* og *c* har en fælles faktor, og man får på samme måde som ovenfor:

$$a^2 + b^2 = c^2 \quad \Leftrightarrow \quad (d \cdot k_a)^2 + b^2 = (d \cdot k_c)^2 \quad \Leftrightarrow \quad d^2 \cdot (k_c^2 - k_a^2) = b^2 \quad \Leftrightarrow$$

$$d \cdot \sqrt{k_c^2 - k_a^2} = b \quad \Leftrightarrow \frac{b}{d} = \sqrt{k_c^2 - k_a^2}$$

Og så kan man bruge samme argument som ovenfor, hvor man lige skal bemærke, at argumentet under kvadratroden er positivt.

Bemærk også, at det gennem hele beviset ikke er noget problem, hvis *d* = 1.

Øvelse 8.16.b: Gennemfør beviset for lemma 8.16 ved hjælp af Aritmetikkens Fundamentalsætning, så du undgår de "forbudte" kvadratrødder og brøker.

Øvelse 8.17: Prøv at se på et primitivt pythagoræisk talsæt (a,b,c). Kan man sige noget om, hvor mange af tallene, der er lige, og evt. hvilket eller hvilke, det må være? Prøv at bevise din påstand. Igen skal du gå videre til det følgende lemma, hvis du går død i øvelsen.

Lemma 8.18: Lad (a,b,c) være et primitivt pythagoræisk talsæt, hvor $a^2 + b^2 = c^2$. Så er netop ét af tallene lige, og det er *a* eller *b*.

Bevis: Lad (a,b,c) være et primitivt pythagoræisk talsæt, hvor $a^2 + b^2 = c^2$.

Hvis alle tre tal er lige, så indeholder de faktoren 2, dvs. det er ikke et primitivt talsæt.

Hvis to af tallene er lige, så indeholder de faktoren 2, og ifølge lemma 8.16 indeholder det tredje tal også faktoren 2, dvs. igen er talsættet ikke primitivt.

Alle tallene kan ikke være ulige, for hvis *a* og *b* er ulige, så er a^2 og b^2 også ulige, og dermed er deres sum c^2 lige, hvorfor *c* er lige.

Dermed må netop ét af tallene være lige.

Og så kommer den vanskeligste del af beviset. Vi skal nu se, at det ikke kan være *c*, der er lige. For hvis *c* er lige, har man: $c = 2 \cdot k \Leftrightarrow c^2 = 4 \cdot k^2$, dvs. at 4 er divisor i c^2.

Og hvis *c* er lige, så må *a* og *b* være ulige, og man har så:

$$a^2 + b^2 = (2n+1)^2 + (2m+1)^2 = 4n^2 + 4n + 1 + 4m^2 + 4m + 1 = 4 \cdot (n^2 + n + m^2 + m) + 2$$

Det ses hermed, at tallet 4 IKKE går op i $a^2 + b^2$, da divisionen giver resten 2.

Og da 4 som nævnt er divisor i c^2, har vi altså en modstrid.

Det må altså være ét af tallene *a* og *b*, der er lige.

Lemma 8.19: Hvis to tal x og y er indbyrdes primiske, og deres produkt er et kvadrattal, så er x og y selv kvadrattal (dvs. $sfd(x,y)=1 \wedge x\cdot y=z^2 \Rightarrow x=z_1^2 \wedge y=z_2^2$).

Øvelse 8.20: Prøv selv at bevise ovenstående lemma. Det kan ofte være en god idé at inddrage *Aritmetikkens Fundamentalsætning*. Hvis du går helt i stå, kan du få hjælp i beviset nedenfor.

Bevis: Vi antager altså, at $sfd(x,y)=1 \wedge x\cdot y=z^2$. Ifølge *Aritmetikkens Fundamentalsætning* kan z opløses i primfaktorer, og man får så:

$$x\cdot y=(p_1\cdot p_2\cdot\ldots\cdot p_s)^2 \quad\Leftrightarrow\quad x\cdot y=p_1^2\cdot p_2^2\cdot\ldots\cdot p_s^2.$$

Primtallene på højresiden er altså enten faktorer i x, y eller begge. Men da x og y er indbyrdes primiske, indeholder de ingen fælles primfaktorer, dvs. **hvis** p_i er divisor i x, så er den ikke divisor i y, og dermed må begge p_i være en del af primfaktoropløsningen af x. Samme sætning kan siges med ombytninger af x og y.

De enkelte primfaktorer kan altså knyttes til enten x eller y, hvilket formelt kan gøres på følgende måde.

Man kan bytte rundt på højresidens primfaktorer, som man vil, dvs. nummereringen af primtallene er vilkårlig. Man kan derfor skrive:

$$x=p_1^2\cdot p_2^2\cdot\ldots\cdot p_t^2 \Leftrightarrow x=(p_1\cdot p_2\cdot\ldots\cdot p_t)^2$$

$$y=p_{t+1}^2\cdot p_{t+2}^2\cdot\ldots\cdot p_s^2 \Leftrightarrow y=(p_{t+1}\cdot p_{t+2}\cdot\ldots\cdot p_s)^2 \quad , \quad hvor \;\; 0\le t\le s$$

(Hvis $t = 0$ er $x = 1$, og hvis $t = s$ er $y = 1$)

Hermed er det vist, at både x og y er kvadrattal.

Og så mangler vi lige sidste lemma inden sætningen. Først som øvelse:

Øvelse 8.21: Prøv at bevise følgende lemma.

Lemma 8.22: Hvis b og c er ulige, indbyrdes primiske tal, hvor c > b, så er tallene $\frac{c+b}{2}$ og $\frac{c-b}{2}$ også indbyrdes primiske.

Bevis: Bemærk først, at tællerne i de to brøker er lige tal, da b og c er ulige, så brøkerne er naturlige tal, og dermed er lemmaet ikke meningsløst.

Lad altså b og c være indbyrdes primiske. Endnu engang benyttes et indirekte bevis.

Antag at $\frac{c+b}{2}$ og $\frac{c-b}{2}$ ikke er indbyrdes primiske, dvs. de har en fælles divisor d > 1:

$$\frac{c+b}{2}=k_1\cdot d \quad og \quad \frac{c-b}{2}=k_2\cdot d$$

Men se så på følgende udregninger:

$$\frac{c+b}{2}+\frac{c-b}{2}=\frac{c+b+c-b}{2}=\frac{2c}{2}=c \qquad dvs. \quad k_1\cdot d+k_2\cdot d=c \quad\Leftrightarrow\quad (k_1+k_2)\cdot d=c$$

$$\frac{c+b}{2}-\frac{c-b}{2}=\frac{c+b-c+b}{2}=\frac{2b}{2}=b \qquad dvs. \quad k_1\cdot d-k_2\cdot d=b \quad\Leftrightarrow\quad (k_1-k_2)\cdot d=b$$

Dette viser, at d så også ville være divisor i b og c, men de er jo indbyrdes primiske, så her er den søgte modstrid.

Og nu er tiden så kommet for sætningen, som lemmaerne har ført hen mod. Den kaldes sommetider *Euklids sætning*, da den følger af Euklids sætning 8 i bog II af *Elementer* (der dog er en geometrisk og ikke en talteoretisk sætning).

Euklids sætning 8.23: De primitive pythagoræiske talsæt (a,b,c) er netop talsættene af formen $(2pq, p^2-q^2, p^2+q^2)$, hvor p og q er indbyrdes primiske tal, hvoraf netop det ene er lige, og $p > q$.

Opgave 8.24: Hvilken eller hvilke af nedenstående sætninger kunne erstatte "netop det ene er lige" i sætningen?

a) Netop det ene er ulige.
b) Ikke begge er lige.
c) Ikke begge er ulige.

Opgave 8.25: Hvilken eller hvilke af nedenstående former kunne også bruges som talsæt i sætningen?

a) $(2pq, p^2+q^2, p^2-q^2)$
b) $(p^2-q^2, 2pq, p^2+q^2)$
c) $(p^2+q^2, p^2-q^2, 2pq)$

Bevis: Bemærk, at sætningen siger to ting.

1) Hvis et talsæt skal opfylde $a^2+b^2=c^2$, skal det være af formen $(2pq, p^2-q^2, p^2+q^2)$
2) Hvis et talsæt er af formen $(2pq, p^2-q^2, p^2+q^2)$, så opfylder det $a^2+b^2=c^2$.

Del 2) følger direkte af lemma 8.2. Så vi mangler nu kun at vise del 1).

Vi antager altså, at vi har et primitivt pythagoræisk talsæt (a,b,c), og så ved vi ifølge lemma 8.18, at netop ét af tallene er lige, og at det er *a* eller *b*. Da man ikke kan skelne mellem *a* og *b* i Pythagoras' Læresætning, kan vi selv vælge, hvilket af tallene vi vil lade være lige. For at få det til at passe med ordlyden af sætningen, lader vi det være *a* (det er jo $2pq$, der er det lige tal i talsættet, så hvis vi lod *b* være det lige tal, ville det svare til formuleringen b) fra opgave 8.25).

Dermed kan følgende omskrivning foretages:

$$a^2+b^2=c^2 \quad \Leftrightarrow \quad a^2=c^2-b^2 \quad \Leftrightarrow \quad a^2=(c+b)\cdot(c-b) \quad \Leftrightarrow \quad \left(\frac{a}{2}\right)^2=\left(\frac{c+b}{2}\right)\cdot\left(\frac{c-b}{2}\right)$$

I sidste skridt er der divideret med 4 på begge sider af lighedstegnet.

Og her er det vigtigt at bemærke, at dette KUN kan lade sig gøre, fordi tallene *a*, *c*+*b* og *c*-*b* er lige. Ellers ville vi jo have fået ikke-naturlige tal ved divisionen med 2.

Ifølge lemma 8.16 er *b* og *c* indbyrdes primiske, for hvis de ikke var, ville de have en fælles divisor større end 1, der også ville være divisor i *a*, hvilket ville være i modstrid med, at talsættet er primitivt.

Men lemma 8.22 giver så, at $\frac{c+b}{2}$ og $\frac{c-b}{2}$ er indbyrdes primiske.

Og da deres produkt er et kvadrattal $\left(\frac{a}{2}\right)^2$, er de ifølge lemma 8.19 selv kvadrattal.

Dermed findes der altså hele tal p og q så: $\frac{c+b}{2}=p^2$ *og* $\frac{c-b}{2}=q^2$, *hvor* $p>q$.

Da $\frac{c+b}{2}$ og $\frac{c-b}{2}$ er indbyrdes primiske, er altså p^2 og q^2 indbyrdes primiske, og dermed er p og q indbyrdes primiske. For hvis p og q indeholdt en fælles faktor $d > 1$, så ville p^2 og q^2 indeholde den fælles faktor d^2.

Men ovenstående fastsættelser giver så:

$$\frac{c+b}{2}+\frac{c-b}{2}=p^2+q^2 \quad \Leftrightarrow \quad c=p^2+q^2$$

$$\frac{c+b}{2}-\frac{c-b}{2}=p^2-q^2 \quad \Leftrightarrow \quad b=p^2-q^2$$

Da b og c er ulige, er ifølge lemma 8.7 netop et af tallene p og q lige.

Nu mangler vi blot at vise, at $a = 2 \cdot p \cdot q$ følger af ovenstående:

$$\left(\frac{a}{2}\right)^2=\left(\frac{c+b}{2}\right)\cdot\left(\frac{c-b}{2}\right) \quad \Leftrightarrow \quad \left(\frac{a}{2}\right)^2=p^2\cdot q^2 \quad \Leftrightarrow \quad \frac{a}{2}=p\cdot q \quad \Leftrightarrow \quad a=2\cdot p\cdot q$$

Og hermed er sætningen bevist.

Vi er altså nu kommet frem til, hvordan man konstruerer primitive pythagoræiske talsæt.

Eksempel: 6 og 11 er indbyrdes primiske tal, 6 er lige og 11 ulige, og 11 > 6. Dermed sættes $p = 11$ og $q = 6$, og man har så:

$$a = 2 \cdot p \cdot q = 2 \cdot 11 \cdot 6 = 132$$

$$b = p^2 - q^2 = 11^2 - 6^2 = 85$$

$$c = p^2 + q^2 = 11^2 + 6^2 = 157$$

(132,85,157) er altså et primitivt pythagoræisk talsæt. Og (85,132,157) er det samme sæt.

Eksempel: 5682 og 4315 er indbyrdes primiske tal, 5682 er lige og 4315 ulige, og 5682 > 4315. Dermed sættes $p = 5682$ og $q = 4315$, og man har så:

$$a = 2 \cdot p \cdot q = 2 \cdot 5682 \cdot 4315 = 49035660$$

$$b = p^2 - q^2 = 5682^2 - 4315^2 = 13665899$$

$$c = p^2 + q^2 = 5682^2 + 4315^2 = 50904349$$

(49035660,13665899,50904349) er altså et primitivt pythagoræisk talsæt.

Du kan selv kontrollere, at talsættet er både primitivt og pythagoræisk.

Opgave 8.26: Hvilke af nedenstående talpar kan bruges til at konstruere primitive pythagoræiske talsæt?

a) 5 og 12
b) 8 og 1
c) 13 og 19
d) 15 og 6
e) 1 og 7
f) 14 og 71
g) 26 og 82
h) 7 og 3
i) 11 og 10
j) 100 og 1

Opgave 8.27: Benyt talparrene fra a) , b) , i) og j) i ovenstående til at konstruere det pågældende primitive pythagoræiske talsæt.

Opgave 8.28: Hvilke talpar (p,q) er brugt til at konstruere de primitive pythagoræiske talsæt:

a) (3,4,5)
b) (5,12,13)
c) (7,24,25)
d) (33,56,65)

Hvis man ønsker at skabe et overblik over de primitive pythagoræiske talsæt, må man gå systematisk til værks. Man kan begynde med at fastsætte p og derefter finde de q, der kan bruges. Det giver et skema, der kan fortsættes, indtil (regne-)kræfterne slipper op:

p	Mulige q-værdier					
2	1					
3	2					
4	1	3				
5	2	4				
6	1	5				
7	2	4	6			
8	1	3	5	7		
9	2	4	8			
10	1	3	7	9		
11	2	4	6	8	10	
12	1	5	7	11		
13	2	4	6	8	10	12
14	1	3	5	9	11	13
15	2	4	8	14		

Nu var der jo en masse lemmaer, der ledte frem til Euklids sætning 8.23. Så der er "heldigvis" også lidt ekstra information at hente fra sætningen:

Korollar 8.29: Pythagoræiske trekanter har altid et heltalligt areal.

Opgave 8.30: Hvordan følger dette af Euklids sætning 8.23?

Som afslutning på dette kapitel ser vi på nogle andre diofantiske trekanter, der – hvis du skulle have glemt det efter alle lemmaerne – er trekanter med heltallige sidelængder.

Først skal vi følge op på korollar 8.29 ved at indføre såkaldte *heroniske trekanter*. De er opkaldt efter Heron, der levede i det første århundrede evt., og som er mest kendt for sin sætning om at finde en trekants areal T ved:

$T = \sqrt{s \cdot (s-a) \cdot (s-b) \cdot (s-c)}$, hvor a, b og c er trekantens sidelængder og s den halve omkreds.

Da denne formel giver en måde at bestemme en trekants areal, forklarer den oprindelsen til følgende definition:

Definition 8.31: En diofantisk trekant med et heltalligt areal kaldes en *heronisk* trekant.

En anden slags diofantisk trekant indføres med følgende definition:

Definition 8.32: En diofantisk trekant, hvor areal og omkreds er lige store, kaldes en *perfekt* trekant.

Øvelse 8.33: Hvorfor giver definition 8.32 ikke mening som geometrisk definition eller hvis man arbejder med enheder på tal?

Eksempel: Trekanten med sidelængderne 13, 14 og 15 er diofantisk.

Da $13^2+14^2 \neq 15^2$ er den ikke retvinklet.

Men Herons arealformel giver:

$$s = \frac{13+14+15}{2} = 21$$

$$T = \sqrt{21\cdot(21-13)\cdot(21-14)\cdot(21-15)} = 84$$

Derfor er trekanten heronisk.

Da omkredsen er 42 og altså forskellig fra arealet, er trekanten ikke perfekt.

Eksempel: Trekanten med sidelængderne 5, 12 og 13 er diofantisk.

Da $5^2+12^2=13^2$, er den også retvinklet.

Herons arealformel giver:

$$s = \frac{5+12+13}{2} = 15$$

$$T = \sqrt{15\cdot(15-5)\cdot(15-12)\cdot(15-13)} = 30$$

Så den er også heronisk.

Da omkredsen er 30 ligesom arealet, er den også perfekt.

Konklusion: Det er en herlig trekant! ← Det er ikke en definition.

Opgave 8.34: Afgør om trekanterne med følgende sider er diofantiske, retvinklede, heroniske og/eller perfekte:

a) 6, 8 og 10
b) 12, 35 og 37
c) 5, 6 og 7
d) $\frac{3}{2}$, 5 og 6
e) 6, 25 og 29

Opgave 8.35: Hvilke af følgende udsagn er sande?

a) Hvis en trekant er diofantisk, er den også heronisk.
b) Hvis en trekant er heronisk, er den også diofantisk.
c) Hvis en trekant er pythagoræisk, er den også heronisk.
d) Hvis en trekant er heronisk, er den også pythagoræisk
e) Hvis en trekant er perfekt, er den også heronisk.
f) Hvis en trekant er heronisk, er den også perfekt.
g) Hvis en trekant er retvinklet og heronisk, er den også perfekt.
h) Hvis en trekant er perfekt, er den også pythagoræisk.
i) Hvis en trekant er pythagoræisk, er den også perfekt.

Der findes ikke mange perfekte trekanter. Faktisk findes der kun 5 – hvilket kan bevises. Ud over de 3, der er benyttet i det foregående, er det trekanterne givet ved talsættene (9,10,17) og (7,15,20).

Kapitel 9: SPECIELLE SÆTNINGER

(naturlige tal)

Dette kapitel er helliget en række forskellige kendte sætninger eller formodninger om tal. Det vil i modsætning til de foregående kapitler ikke indeholde beviser – hvilket hænger godt sammen med begrebet *formodning.*

Pierre de Fermat (1601-1665): Fermat var uddannet og ernærede sig som jurist, hvilket pr. definition giver ham betegnelsen "amatør", når man betragter ham som matematiker. Han udgav aldrig nogle af sine resultater, men han korresponderede med mange af datidens matematikere, hvor han fortalte om sine sætninger og sommetider skitserede idéer til beviser.

Han udviklede selv forskellige metoder. F.eks. udviklede han en metode til at finde maksimum for visse kurver, hvilket var en forløber for differentialregningen. Han bidrog også sammen med Blaise Pascal til sandsynlighedsregningens indtog. Men han er mest kendt for sine bidrag til talteorien, bl.a. fordi han fremsatte en masse sætninger, der først blev bevist eller modbevist (vi skal se et eksempel på hver slags) mange år efter hans død.

Her kommer første eksempel (bemærk, at Fermat kun arbejdede med naturlige tal – ligesom overskriften siger):

Sætning 9.1: Ligningen $a^n + b^n = c^n$ har ingen løsninger for $n > 2$.

Dette er et eksempel på en diofantisk ligning. Vi kender den allerede for $n = 2$, hvor vi i Euklids sætning 8.23 så, at der var uendelig mange løsninger, der ikke blot var forlængelser af hinanden.

Så at der ikke findes en eneste løsning, når $n > 2$, kan måske virke overraskende……eller kan det? Fermat kan jo ikke have ment, at det var så overraskende, for han fremsatte sætningen sandsynligvis uden at have et bevis for den. Eller måske troede han, at han havde et bevis?

Fermat udgav som nævnt aldrig sine resultater, og ofte skrev han blot i marginen på de værker, han sad og læste. Og om netop denne sætning skrev han følgende meget berømte kommentar i marginen på Diofants *Arithmetika* (se kapitel 8):

"Det er umuligt at dele en tredjepotens i to tredjepotenser, eller en fjerdepotens i to fjerdepotenser, eller generelt, en vilkårlig potens større end 2 i to af de samme potenser. Jeg har opdaget et ganske bemærkelsesværdigt bevis for dette, som marginen er for smal til at indeholde."

Dette "bemærkelsesværdige bevis" har man aldrig fundet. Fermat beviste selv sætningen i det særlige tilfælde $n = 4$, og efter hans død blev der gennemført beviser for $n = 3$ og en hel masse primtal (da det kan vises, at man kun behøver at vise sætningen for primtal og tallet 4). Men det afgørende bevis kom først i 1993, da det efter mange års ihærdigt arbejde, der byggede på en masse nye resultater inden for matematik, lykkedes for Andrew Wiles at bevise sætningen.

Troede han! For beviset viste sig at indeholde en fejl. Denne fejl lykkedes det dog for Wiles at rette, så han kunne levere et bevis for sætningen i 1994.

Der gik altså ca. 350 år fra sætningen blev fremført, til den blev bevist.

Øvelse 9.2: Undersøg, om ikke $1782^{12} + 1841^{12} = 1922^{12}$ skulle være en løsning til ligningen fra sætning 9.1.

Øvelse 9.3.a: Hvis det ikke lykkedes at modbevise sætning 9.1 med ovenstående, må hårdere midler tages i brug. Prøv med $3987^{12} + 4365^{12} = 4472^{12}$.

Øvelse 9.3.b: Find et dansk ordsprog, der beskriver øvelserne 9.2 og 9.3.a.

Øvelse 9.4: Fermat beviste sætningen i tilfælde $n = 4$ ved at vise, at HVIS der var en løsning, så kunne man altid finde en ny løsning med mindre tal end den oprindelige. Begrund, at dette beviser sætningen i tilfældet $n = 4$.

Sætning 9.1 kaldes *Fermats store sætning* eller *Fermats sidste sætning* (fordi det var den sidste af Fermats mange sætninger, der manglede at blive bevist eller modbevist).

Når der er en stor sætning, må der vel også være en lille sætning?

Ja, det er der, og det var også en sætning, som Fermat fremførte uden bevis. Den blev bevist af G.W. Leibniz (ikke offentliggjort) og senere – i 1736 - af Leonhard Euler (offentliggjort). Her er en version af sætningen, men du kan også finde den i andre versioner – bl.a. én med restklasser:

Sætning 9.5: Hvis p er et primtal og a et tal, der er primisk med p, så er p divisor i $a^{p-1}-1$.

Øvelse 9.5.a: Afprøv denne sætning med forskellige tal, der opfylder betingelserne – og du kan evt. også prøve med tal, der ikke opfylder dem.

Sætning 9.5 anvendes ofte som en – ikke ufejlbarlig – primtalstest kaldet *Fermats primtalstest*. Man undersøger, om p er divisor i $a^{p-1}-1$, og hvis det ikke er, så er p ikke et primtal. Men hvis det er, så KAN p være et primtal. Der er dog også sammensatte tal n, der opfylder ovenstående for alle tal a, som de er primiske med. Disse tal kaldes *Carmichael tal* (efter den amerikanske matematiker Robert Carmichael (1879-1967)), og er en speciel slags *pseudoprimtal*, der er sammensatte tal, der deler egenskaber med primtallene.

Der findes uendeligt mange af sådanne pseudoprimtal. Men du skal have været meget heldig, hvis du har fundet nogle, da du arbejdede med øvelse 9.5.a

Der findes også uendeligt mange Carmichael tal. Det blev bevist i 1992.

Følgende sætning kan bruges til at kontrollere, om et tal er et Carmichael tal……hvis man altså er i stand til at finde primfaktoropløsningen, hvilket som bekendt er et af de helt store problemer inden for talteorien, hvis tallene bliver meget store.

Sætning 9.6: Et sammensat tal n er et Carmichael tal, netop hvis det ikke indeholder kvadrater, og det for alle primfaktorerne p_i i tallet gælder, at $(p_i - 1) \mid (n-1)$.

At n ikke indeholder kvadrater, kan også udtrykkes ved, at alle primfaktorerne i primfaktor-opløsningen er forskellige.

Eksempel: Tallet 561 er det mindste Carmichael tal. Sætning 9.6 bruges til at kontrollere, at det faktisk er et Carmichael tal.

Først tjekkes det, at det faktisk er et sammensat tal, og primfaktoropløsningen bestemmes:

$$561 = 3 \cdot 11 \cdot 17$$

Det ses altså, at 561 er sammensat, og der er ingen primfaktorer, der optræder mere end én gang.

Så kontrolleres anden del af sætningen:

$$(3-1) \mid (561-1) \quad \Leftrightarrow \quad 2 \mid 560 \quad \textit{sandt}$$

$$(11-1) \mid (561-1) \quad \Leftrightarrow \quad 10 \mid 560 \quad \textit{sandt}$$

$$(17-1) \mid (561-1) \quad \Leftrightarrow \quad 16 \mid 560 \quad \textit{sandt}$$

Dermed er det vist, at tallet er et Carmichael tal.

Eksempel: Lad os prøve om 715 er et Carmichael tal.

Først tjekkes det, at det faktisk er et sammensat tal, og primfaktoropløsningen bestemmes:

$$715 = 5 \cdot 11 \cdot 13$$

Det ses altså, at 715 er sammensat, og der er ingen primfaktorer, der optræder mere end én gang.

Så kontrolleres anden del af sætningen:

$$(5-1) \mid (715-1) \quad \Leftrightarrow \quad 4 \mid 714 \quad \textit{falsk}$$

Da dette udsagn er falsk, behøver man ikke at undersøge mere, men kan sige, at tallet IKKE er et Carmichael tal.

Eksempel: Lad os nu prøve med 1229.

Det viser sig at være et primtal (hvilket du sikkert erindrer, hvis du har lavet weekendøvelse 6.5.a). Dermed er det ikke et Carmichael tal.

Eksempel: Nu skal 2793 tjekkes.

Det viser sig at være sammensat med primfaktoropløsningen $2793 = 3 \cdot 7 \cdot 7 \cdot 19$.

Som det ses, indeholder primfaktoropløsningen to 7-taller (hvilket i formuleringen af sætning 9.6 vil sige, at det indeholder kvadratet 7^2), og dermed er det IKKE et Carmichael tal.

Opgave 9.6.a: Afgør, hvilke af nedenstående tal, der er Carmichael tal:

a) 969
b) 1105
c) 1331
d) 1637
e) 1729
f) 2023
g) 41041

Den sidste af Fermats sætninger, som vi skal se på her, er:

Sætning 9.7: Alle tal på formen $F_n = 2^{2^n} + 1$, hvor *n* er et ikke-negativt heltal, er primtal.

Det kan lige bemærkes, at vi altså her bevæger os lige uden for de naturlige tal, da 0 inddrages.

Fermat beviste ikke denne sætning.

Opgave 9.8: Bestem de første 9 'Fermat-tal' (dvs. tal fundet på ovenstående måde).

Øvelse 9.9 *(*frivillig): Find den fejl, der er placeret i facit til ovenstående opgave.

Øvelse 9.10: Benyt Maples primtalstest (isprime) til at kontrollere sætningens rigtighed for så mange af Fermat-tallene, som Maple kan klare.

Øvelse 9.11: Prøv at primfaktoropløse så mange af Fermat-tallene, som Maple kan klare.

Som du nok opdagede, er det faktisk kun de første 5 Fermat-tal, der er primtal – i hvert fald af dem som Maple kunne teste.

Leonhard Euler (1707-1783) fandt i 1732 primfaktoropløsningen for F_5 (som du også fandt i øvelse 9.11). Euler fik regnet meget i sin levetid, men han arbejdede dog ikke helt på må og få. Han vidste nemlig, at de eneste mulige faktorer var af formen $a \cdot 64 + 1$, hvor *a* er et naturligt tal.

Så her var altså en sætning, der viste sig ikke at være rigtig.

Øvelse 9.12: Tjek, at de to tal i primfaktoropløsningen er af den pågældende form, som Euler arbejdede ud fra.

Man har prøvet at finde flere primtal end de 5 første blandt Fermat-tallene, men det er endnu ikke lykkedes.

Man har på nuværende tidspunkt (juli 2020) fået faktoriseret alle Fermat-tallene F_5-F_{11} fuldstændigt, mens man bl.a. har fundet faktorer i Fermat-tallene F_{12}-F_{19}. F_{33} er det mindste Fermat-tal større end F_4, der kan vise sig at være et primtal.

På følgende hjemmeside kan man følge med i udviklingen:
http://www.prothsearch.net/fermat.html

Så man kan sige, at denne sætning af Fermat har fået en noget anden ordlyd, men man ved ikke, hvilken eller hvilke af nedenstående sætninger, der er sande:

1) Der findes kun 5 primtal blandt Fermat-tallene.
2) Der findes uendelig mange primtal blandt Fermat-tallene.
3) Der findes uendelig mange sammensatte tal blandt Fermat-tallene.

Opgave 9.13: Er der nødvendigvis mindst én af ovenstående sætninger, der er sande?

Én af dem, som Fermat korresponderede med, var Marin Mersenne, der har lagt navn til:

Definition 9.14: Et tal på formen $M_n = 2^n - 1$ kaldes et *Mersenne-tal*.

Det kan vises, at hvis n ikke er et primtal, så er M_n det heller ikke.

Men der gælder ikke, at hvis n er et primtal, så er M_n også et primtal. I så fald ville man have en effektiv og ufejlbarlig måde at skabe vilkårligt store primtal.

Øvelse 9.14.a: Hvordan ville man kunne skabe vilkårligt store primtal, hvis det havde været sandt – men det er det ikke – at hvis n er et primtal, så er M_n også et primtal.

Man er ofte mest interesseret i primtallene blandt Mersenne-tallene, og derfor bruges betegnelsen "Mersenne-tal" sommetider om de af ovenstående tal, hvor n er et primtal.

Og man kalder et primtal på formen fra definition 9.14 for et *Mersenne-primtal*.

Det er oftest blandt Mersenne-tallene, at man søger efter primtal, når man prøver at finde større og større primtal. Det skyldes ikke, at denne forskrift er specielt god til at skabe primtal, men mere at man har gode metoder til at undersøge, om sådanne tal er primtal.

Vigtig bemærkning 9.15: Sætning 9.7 og definition 9.14 er begge metoder til at skabe vilkårligt store tal. Hvis sætning 9.7 havde været sand, havde man slet ikke kunnet snakke om et "største kendte primtal", for man kunne jo bare sætte større og større tal ind og konstruere vilkårligt store primtal.

Mersenne har lagt navn til disse tal, fordi han lavede en liste over primtallene blandt denne type tal op til og med M_{257}.

Det var imponerende, men han skulle nok være stoppet lidt før, for netop M_{257} regnede han fejlagtig som et primtal.

Det samme gjaldt for M_{67}, mens han havde overset M_{61}, M_{89} og M_{107}. Og det kan vi jo sagtens pege fingre af med hjælp fra vores lommeregnere og computere.

Opgave 9.16: Brug Maple til at finde de 4 mindste Mersenne-tal (forstået på formen, hvor *n* er et primtal), der IKKE er primtal.

Inden årtusindskiftet havde man fundet de første 38 primtal blandt Mersenne-tallene. Siden da er der ca. fundet ét nyt Mersenne-primtal om året, så man i 2007 var nået op på 44 kendte Mersenne-primtal. De første 39 ligger "tæt", dvs. man ved, at der ikke findes andre end de 38 kendte Mersenne-primtal mindre end det 39. i rækken.

Man ved ikke, om der er uendeligt mange primtal blandt Mersenne-tallene.

Goldbachs formodning Version I 9.17:
Ethvert tal større end 2 kan skrives som summen af 3 primtal.

Christian Goldbach (1690-1764) skrev i 1742 til Leonhard Euler om denne sætning.

Øvelse 9.18: Prøv at se, om du kan finde et eller flere modeksempler på ovenstående.

Øvelse 9.19: Kan du give en forklaring på, hvordan Goldbach kunne komme med sådan en formodning, når det så let kan vises, at den ikke er rigtig? Hvis ikke, så begynd at læse videre.

Goldbach regnede 1 som et primtal (det er jo et definitionsspørgsmål). Men sætningen kan sådan set stadig bruges. Den skal bare omformuleres til:

Goldbachs formodning Version II 9.20:
Ethvert tal større end 5 kan skrives som summen af 3 primtal.

Øvelse 9.21: Prøv at finde et eller flere modeksempler på denne sætning.

Det var faktisk Euler, der skrev tilbage og foreslog den skarpere version (da den oprindelige version I simpelt kunne udledes fra den skarpere), der nu er den version, vi kalder:

Goldbachs formodning (Endelig Version) 9.22:
Ethvert lige tal større end 2 kan skrives som summen af 2 primtal.

Øvelse 9.23: Afprøv sætningen for alle lige tal op til og med 30.
Er de pågældende primtal entydigt bestemt?

Goldbachs formodning regnes for at være sand, men den er aldrig bevist. Du kan evt. prøve at tænke over, hvorfor en så simpel sætning kan være så svær at bevise.

Den 13. maj 2013 publicerede Harald Helfgott et bevis for den svage udgave (9.20). Det ser ud til at være accepteret.

Definition 9.24: En *primtalstvilling* består af 2 primtal, hvis differens er 2.

Opgave 9.25: Bestem de 5 mindste primtalstvillinger.

Øvelse 9.26: Overvej, om der findes uendeligt mange primtalstvillinger.

Dette er endnu et uafklaret spørgsmål. Man ved ikke, om antallet af primtalstvillinger er uendeligt. Det mest nærliggende er at tro det, men der mangler et bevis.

Definition 9.27: En *primtalstrilling* består af 3 forskellige primtal, hvor differensen mellem det største og det mindste er 4.

Øvelse 9.28: Prøv at se, hvor mange primtalstrillinger, du kan finde.

Definitionerne 9.24 og 9.27 kunne sagtens være anderledes. Man kunne også i definition 9.24 sige, at det var to primtal, der netop havde ét andet tal imellem sig.

Øvelse 9.29: Bevis, at der findes netop én primtalstrilling.

Definition 9.30: Et *fuldkomment tal* er et tal, der er lig med summen af sine divisorer – sig selv ikke medregnet.

Man kalder sommetider også denne slags tal for *perfekte tal*. Det gjorde Euklid f.eks. i sin definition 22 i kapitel 7.

Definition 9.30 af fuldkomne tal kan desuden bruges til at opdele de naturlige tal ved at indføre betegnelsen *defektivt tal* om de tal, hvor den pågældende sum er mindre end tallet selv, og betegnelsen *excessivt tal* om de tal, hvor den pågældende sum er større end tallet selv.

Opgave 9.30.a: Kan man sige noget om, hvorvidt primtal altid vil være enten defektive, fuldkomne eller excessive? Og i bekræftende fald: Hvilken af disse slags tal hører alle primtal til?
Opgave 9.30.b: Opdel tallene under 21 i defektive, fuldkomne og excessive?

Det fremgår af opgave 9.30.b, at 80% af tallene op til og med 20 er defektive, 5% er fuldkomne og 15% er excessive.

Opgave 9.30.c: Overvej, om denne procentfordeling vil ændre sig markant, hvis man ser på alle naturlige tal. Og hvis du mener, at den vil ændre sig, hvilke procentdele vil så gå op, og hvilke vil gå ned?

Øvelse 9.30.d: Prøv at forklare, hvorfor svaret på opgave 9.30.c IKKE betyder, at der ikke er nogen fuldkomne tal over en vis størrelse.
Øvelse 9.30.e: Overvej, om der mon findes ulige, excessive tal? Svaret følger i bemærkning 9.35.a.

Platon arbejdede med de fuldkomne tal, men det er fra Euklid, at man kender følgende sætning:

Sætning 9.31: Tallene $\left(2^{n+1}-1\right)\cdot 2^n$ er fuldkomne, hvis $2^{n+1}-1$ er et primtal.

Opgave 9.32: Er tallet 1 fuldkomment?

Opgave 9.33: Find de 4 mindste fuldkomne tal, der kan findes med Euklids sætning.

Det lykkedes senere Leonhard Euler at vise, at de fuldkomne tal, der fremkommer ved sætning 9.31, også er de eneste, lige fuldkomne tal.

Opgave 9.34: Brug din viden om Mersenne-tallene til at svare på følgende:
Ved man, om der findes uendeligt mange lige, fuldkomne tal?

Bemærkning 9.34.a: Faktisk følger det af ovenstående, at der er en én-til-én relation mellem Mersenne-primtallene og de lige, fuldkomne tal. Man fandt derfor også nr. 44 i rækken af lige, fuldkomne tal i september 2006, da man fandt det 44. Mersenne-primtal.
Relationen begynder:

Mersenne – primtal		*Lige, fuldkomment tal*
3	←→	6
7	←→	28
31	←→	496
127	←→	8128
8191	←→	33550336
131071	←→	8589869056
524287	←→	137438691328
2147483647	←→	2305843008139952128

Og herfra kan du nok fornemme, at tallene vokser voldsomt.

De 4 første af ovenstående lige, fuldkomne tal har været kendt siden oldtiden. Det har ført til nogle antagelser, som, du ved at kigge på den opskrevne del af relationen kan se, er forkerte. F.eks. blev det foreslået, at det 5. fuldkomne tal ville have 5 cifre (overvej selv hvorfor), samt at det sidste ciffer i tallene skiftevis ville være 6-8-6-8-6-8-6….
Men mon de lige, fuldkomne tal altid slutter på enten 6 eller 8?

Bemærkning 9.35.: Man har aldrig fundet et ulige, fuldkomment tal, og man ved ikke, om et sådant findes.

Bemærkning 9.35.a: Det kunne måske være fristende at tro, at der så heller ikke er fundet ulige, excessive tal, men det er der faktisk. Prøv selv at tjekke 945. Her er summen af de egentlige divisorer (altså divisorerne fraregnet 945) 975. Det er det mindste, ulige, excessive tal.
Bemærk desuden primfaktoropløsningen af 945. Den skulle gerne give dig en idé om, hvad der "kræves" af primfaktoropløsninger, hvis et tal skal være excessivt.

Som afslutning på dette kapitel ser vi på en sætning, der blev postuleret i 1845:

Sætning 9.36: Bertrands postulat: Mellem n og $2n$ ligger altid et primtal for $n > 1$.

Bemærk, at der ikke står "netop ét", men bare "et" primtal.

Øvelse 9.37: Afprøv sætningen for de 5 mindste værdier af n.

Postulatet blev bevist – og dermed gjort til en sætning – i 1852 af den russiske matematiker Pafnuty Chebyshev. Så det er ikke alle postulater, der skal vente flere hundrede år på at blive bevist.

Kapitel 10: EULERS φ-FUNKTION

(naturlige tal og 0)

I dette sidste teoretiske og ret korte kapitel skal vi se på en speciel funktion:

Definition 10.1: *Eulers φ-funktion* $\varphi(n)$ angiver antallet af tal, der er indbyrdes primiske med og mindre end *n*, hvor *n* er et naturligt tal.

Bemærk, at 0 er blandt de tal, der arbejdes med, selvom det kun har betydning for $n = 1$.

Opgave 10.2: Bestem værdierne af Eulers φ-funktion for *n*-værdierne op til og med 20.

Opgave 10.3: Hvilke af nedenstående sætninger er rigtige:

a) Hvis *p* er et primtal, er $\varphi(p) = p - 1$

b) $\varphi(n)$ er lige for $n > 2$

c) Hvis *p* er et primtal, er $\varphi(p^2) = (p-1)^2$

d) Hvis *p* er et primtal, er $\varphi(p^2) = 2 \cdot p$

e) Hvis *p* er et primtal, er $\varphi(p^2) = p \cdot (p-1)$

f) Hvis *p* og *q* er forskellige primtal, er $\varphi(p \cdot q) = (p-1) \cdot (q-1)$

g) Hvis *p* og *q* er forskellige primtal, er $\varphi(p \cdot q) = p \cdot (q-1)$

h) For alle $n > 2$ gælder $\varphi(2 \cdot n) = 2 \cdot \varphi(n)$

i) For alle $n > 2$ gælder $\varphi(2 \cdot n) = \varphi(n)$

j) For alle ulige primtal *p* gælder $\varphi(2 \cdot p) = \varphi(p)$

k) For alle primtal *p* gælder $\varphi(2 \cdot p) = \varphi(p)$

Øvelse 10.4: Find beviser (eller forklaringer) på de rigtige sætninger.

En vigtig sætning, der kunne have været brugt til at bevise nogle af ovenstående sætninger, men som her fremføres uden bevis er:

Sætning 10.5: For tallet *n*, hvor $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_s^{a_s}$, hvor *p*'erne er forskellige primtal, er

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \left(1 - \frac{1}{p_3}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)$$

Egentlig kan denne sætning ikke opskrives på denne måde inden for de naturlige tal, da brøkerne ikke bliver naturlige tal. Ved at gange *n* (angivet ved sin primfaktoropløsning) ind i parenteserne kan man dog hurtigt indse, at man altid ender med et naturligt tal – hvilket man selvfølgelig også skal, hvis sætningen er sand.

Eksempel: Man har, at $754899946334724599048968749365 39 = 2381 \cdot 34729^2 \cdot 55103 \cdot 78137^3$

Dermed er:

$$\varphi(754899946334724599048968749365 39) =$$

$$754899946334724599048968749365 39 \cdot \left(1 - \frac{1}{2381}\right) \cdot \left(1 - \frac{1}{34729}\right) \cdot \left(1 - \frac{1}{55103}\right) \cdot \left(1 - \frac{1}{78137}\right) =$$

$$754537816578326311610400589900 80$$

Afsluttende bemærkning 10.6: Og her kunne man måske så forhaste sig til at tænke, at det er uhyre let at bestemme $\varphi(n)$ for alle *n*. Men ak! Igen stoppes man af manglen på en effektiv metode til at bestemme primtalsopløsninger for store tal.

Absolut afsluttende bemærkning 10.7: En af de i øjeblikket væsentligste anvendelse af talteori er kryptering. RSA-kryptering er en metode til at kryptere meddelelser, der blev opfundet i 1977, og som bruges i bl.a. dankort og sikring ved udveksling af informationer over internettet. Den er nøje hængt op på problemerne med at finde primfaktoropløsningen for meget store tal, men hvis du prøver at sætte dig mere ind i dette emne, skal du være forberedt på, at du har brug for mere viden om restklasser end gennemgået i kapitel 2.

Kapitel 11: GEORG MOHR-OPGAVER:

I dette kapitel får du lov at slippe kreativiteten løs. Det indeholder en række talopgaver, der har været stillet til Georg Mohr-konkurrencerne, dvs. du har kun papir og blyant til rådighed. Måske kan du bruge nogle af tankerne fra de 10 foregående kapitler, måske finder du selv på veje eller måske kan du finde hjælp i de hints, der angives under opgaverne. Men lad være med at give op for tidligt!

Opgave 11.1: Georg Mohr 2004

Vis, at hvis *a* og *b* er hele tal, og a^2+b^2+9ab er delelig med 11, så er a^2-b^2 delelig med 11.

Første hint: Prøv at få omskrevet udtrykket med de 3 led, så det kommer til at indeholde leddet 11ab, hvor 11 jo er divisor. Og vurdér så hvad du kan udlede ud fra det.

Andet hint: Hvis et primtal går op i et kvadrattal, hvad kan man så konkludere?

Løsning: Man har $a^2+b^2+9ab=(a-b)^2+11ab$, hvilket kan tjekkes ved udregning. Hvis venstresiden er delelig med 11, er højresiden også, og da det andet led her er deleligt med 11, så er det første også. Da 11 er divisor i kvadratet $(a-b)^2$ og samtidig et primtal, er 11 også divisor i $(a-b)$, og dermed i $a^2-b^2=(a+b)\cdot(a-b)$.

Opgave 11.2: Georg Mohr 2006

Af tallene 1, 2, 3, … , 2006 skal udtages 10 forskellige.

Vis, at man kan udtage 10 forskellige tal med sum større end 10039 på flere måder end man kan udtage 10 forskellige tal med sum mindre end 10030.

Første hint: Tænk på hvad tallene *n* og (2007 – *n*) har med hinanden at gøre.

Andet hint: Hvis du kan udtage n_1 til n_{10} på *m* måder. Hvor mange måder kan du så udtage (2007 – n_1) til (2007 – n_{10}) på?

Tredje hint: Hvis den første måde bliver et tal mindre end 10030, hvad bliver så den tilsvarende anden måde?

Fjerde hint: Findes der 10 tal blandt de 2006 mulige, hvis sum er 10040?

Løsning: De to måder nævnt i andet hint svarer til at begynde i hver sin ende af talrækken fra 1 til 2006. Så der er lige mange måder. Hvis den ene måde giver under 10030, kan man regne sig frem til, at den anden tilsvarende måde giver over 10040. Dvs. der er lige så mange måder, der giver under 10030, som der giver over 10040. Og da det ikke er synderlig svært at finde 10 tal (prøv selv), der giver 10040, så ved man altså, at der er flere, der giver over 10039 end mindre end 10030.

Opgave 11.3: Georg Mohr 2003

Bestem de hele tal *n*, hvor $\left|2n^2+9n+4\right|$ er et primtal.

Første hint: Find 2 faktorer at opskrive udtrykket i.

Andet hint: De to faktorer er en parentes med *n* plus fire, og den anden parentes er to gange *n* plus 1. Tænk så på hvad der kræves, før dette er et primtal.

Løsning: $\left|2n^2+9n+4\right| = \left|(n+4)\cdot(2n+1)\right|$. Hvis det skal være et primtal, så skal nødvendigvis én af faktorerne være 1 eller -1. Dette er dog ikke tilstrækkeligt, men det kan afprøves. De 4 *n*-værdier, der gør en af faktorerne til 1 eller -1, er: 0, -1, -3 og -5. Ved indsættelse ses, at det kun er -1 og -3, der gør tallet til et primtal, så det er de 2 eneste muligheder for *n*.

Kapitel 12: FACITLISTE

Opgave 1.3: Divisorer: -42, -21, -14, -7, -6, -3, -2, -1, 1, 2, 3, 6, 7, 14, 21, 42
Kvotienter: -42, -21, -14, -7, -6, -3, -2, -1, 1, 2, 3, 6, 7, 14, 21, 42

Opgave 1.4: Divisorer: -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12
Kvotienter: -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12

Opgave 1.5: Divisorer: -13, -1, 1, 13
Kvotienter: -13, -1, 1, 13

Opgave 1.6: Divisorer: -1 og 1
Kvotienter: -1 og 1

Opgave 1.7: Det er ikke rigtigt. F.eks. har tallet 0 divisoren 6, hvor kvotienten bliver 0, men 0 er ifølge definition 1.1 ikke en mulig divisor.

Opgave 1.8: Nej.

Opgave 1.12: Et modeksempel er a = 5, b = 7 og c = 10.

Opgave 1.18: a) $k = 61 \quad r = 5$ b) $k = 89 \quad r = 305$ c) $k = -4 \quad r = 3$ d) $k = -37 \quad r = 0$

Opgave 1.19: $A = \{..., -20, -13, -6, 1, 8, 15, 22, 29, 36, 43, 50, 57, ...\}$

Opgave 1.20: $B = \{..., -15, -8, -1, 6, 13, 20, 27, 34, 41, 48, 55, 62, ...\}$

Opgave 1.21: $C = \{..., -21, -14, -7, 0, 7, 14, 21, 28, 35, 42, 49, 56, ...\}$

Opgave 1.22: Det kan ikke lade sig gøre.

Opgave 1.23: Man får et tal, der giver resten 2 ved division med 7 (dvs. tallene $7 \cdot m + 2$)

Opgave 2.2: $D = \{..., -6, -1, 4, 9, 14, 19, 24, 29, ...\}$

Opgave 2.3: $E = \{..., -25, -19, -13, -7, -1, 5, 11, 17, ...\}$

Opgave 2.4: $F = \{..., -3, -2, -1, 0, 1, 2, 3, 4, ...\}$

Opgave 2.5: 5 går op i dem.

Opgave 2.6: 6 går op i dem.

Opgave 3.4: c og e

Opgave 4.4: Det kan man ikke, da 9 ikke går op i 12 (jf. sætning 4.1)

Opgave 4.5: 10 og 20

Opgave 4.14: Det behøver ikke at være den principale rest. Enhver rest kan bruges.

Opgave 5.5: a) $7 = 3 \cdot 105 - 2 \cdot 154$

b) $2837 = 4 \cdot 8511 - 1 \cdot 31207$

c) $1 = -6296 \cdot 121030 + 10141 \cdot 75141$

Opgave 6.2: b) og c)

Opgave 6.2.a: Sådan et primtal findes ikke, for hvis $\sqrt{p} = n$, hvor $n>1$, er $p = n \cdot n$ dvs. et sammensat tal.

Opgave 6.18: 1, 2953, 4129 og 12192937

Opgave 6.19: 1, 3, 181, 543, 769, 2307, 139189 og 417567

Opgave 6.20: 1, 11, 17, 23, 29, 187, 253, 319, 391, 493, 667, 4301, 5423, 7337, 11339, 124729

Opgave 6.21: 4

Opgave 6.22: 8

Opgave 6.23: 6

Opgave 6.24: 18

Opgave 6.25: 5

Opgave 6.26: 8

Opgave 6.27: 81

Opgave 6.32: Vores antagelse i beviset var forkert (hvilket var hele pointen), og dermed kan vi heller ikke bruge konklusionen.

Opgave 6.33: 15

Opgave 6.34: Nej.

Opgave 6.34.f: 6212157481

Opgave 6.34.g: 4560435889

Opgave 6.45: a) 12291115914 b) 7889048559 c) 2250000 d) 7420738134810

Opgave 6.46: a) Ja b) Ja c) Ja d) Ja

Opgave 7.1: 1

Opgave 7.2: 2, 13 og 14

Opgave 7.3: Det er et tal, hvor summen af alle dets positive divisorer bortset fra tallet selv er lig med tallet selv. Man bruger både betegnelserne ’perfekt’ og ’fuldkomment’.

Opgave 7.4: 6 og 28

Opgave 7.6: Indirekte bevis

Opgave 7.9: Korollar.

Opgave 7.12: a) 12 b) 273 c) 589

Opgave 7.16: Faktorernes orden er ligegyldig.

Opgave 7.18: Sætning 6.29

Opgave 8.1: 84 år
Opgave 8.8: 1. gang.
Opgave 8.10: De er ensvinklede
Opgave 8.12: a, b, c, e, g og h
Opgave 8.13: c, d, e, f og g
Opgave 8.14: c, e og g
Opgave 8.24: a og c
Opgave 8.25: b
Opgave 8.26: a, b, f, i og j
Opgave 8.27: a) (120,119,169) b) (16,63,65) i) (220,21,221) j) (200,9999,10001)
Opgave 8.28: a) (2,1) b) (3,2) c) (4,3) d) (7,4)
Opgave 8.30: En retvinklet trekants areal er $T = ½ \cdot a \cdot b$, og da a er lige, bliver ½a er helt tal.
Opgave 8.34: a) Diofantisk, retvinklet, heronisk og perfekt.
b) Diofantisk, retvinklet og heronisk. c) Diofantisk. d) –
e) Diofantisk, heronisk og perfekt.
Opgave 8.35: b, c og e
Opgave 9.6.a: b, e og g
Opgave 9.8: 3
5
17
257
65537
4294967297
18446744073709551617
340282366920938463463374607431768211457
115792089237316195423570985008687907853269984655640564039457584007913129639937
Opgave 9.13: Ja.
Opgave 9.16: M_{11}, M_{23}, M_{29} og M_{37}.
Opgave 9.25: 3 og 5
5 og 7
11 og 13
17 og 19
29 og 31
Opgave 9.30.a: Ja, alle primtal hører til de defektive tal.
Opgave 9.30.b: Defektive: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17 og 19
Fuldkomne: 6
Excessive: 12, 18 og 20
Opgave 9.30.c: Fordelingen er 75,2% defektive, 0% fuldkomne og 24,8% excessive.
Opgave 9.32: Nej.
Opgave 9.33: 6, 28, 496 og 8128
Opgave 9.34: Nej.
Opgave 10.2:
$\varphi(1)=1$; $\varphi(2)=1$; $\varphi(3)=2$; $\varphi(4)=2$; $\varphi(5)=4$; $\varphi(6)=2$; $\varphi(7)=6$; $\varphi(8)=4$;
$\varphi(9)=6$; $\varphi(10)=4$; $\varphi(11)=10$; $\varphi(12)=4$; $\varphi(13)=12$; $\varphi(14)=6$; $\varphi(15)=8$;
$\varphi(16)=8$; $\varphi(17)=16$; $\varphi(18)=6$; $\varphi(19)=18$; $\varphi(20)=8$
Opgave 10.3: a) , b) , e) , f) og j)

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.