Projekt 0.5 Euklids algoritme, primtal og primiske tal

De gulede øvelser ligger der svar på bagest i projektet

Betegnelser.
Mængden af hele tal (positive, negative og nul) betegnes $\mathbb{Z}$. At et tal a er et helt tal angives med: $a \in \mathbb{Z}$, der læses *a tilhører* $\mathbb{Z}$.
Når vi har to vilkårlige hele tal, $a,b \in \mathbb{Z}$ kan vi dividere a op i b ved den metode, vi lærte i folkeskolen. Resultatet skrives således:

$b = q \cdot a + r$, hvor $q \in Z$, og $0 \le r < a$ (*)

Vi vil altid skrive resultatet således, at resten r ligger i dette interval. Denne rest kaldes *den principale rest.*
Opskrivningen af (*) kaldes *divisionsligningen*.
Hvis *a går op i b*, dvs hvis resten er 0, siger vi at *a er divisor i b*, og vi skriver: $a \mid b$.
Hvis *a ikke går op i b* skriver vi det af og til således: $a \nmid b$, men det er ikke en del af det fælles internationale matematiske sprog.

Eksempel 1
a = 5, b = 32: $32 = 6 \cdot 5 + 2$
a = 3, b = 16: $16 = 5 \cdot 3 + 1$
a = 3, b = -16: $-16 = -6 \cdot 3 + 2$
Bemærk at kravet om $0 \le r < a$ giver en lidt anden divisionsligning for negative tal.

Eksempel 2
$6 \mid 216$ $37 \mid 2.954.524$ $113 \nmid 965.356$

Sætning 1
For vilkårlige tal $a,b \in \mathbb{Z}$ er divisionsligningen éntydig.

Bevis.
Antag at vi har to opskrivninger af divisionsligningen:
$b = q_1 \cdot a + r_1$
$b = q_2 \cdot a + r_2$, og lad os sige $r_1 \le r_2$
Træk fra og få:
$(q_1 - q_2) \cdot a = r_2 - r_1$
Da $0 \le r_1 < a$ og $0 \le r_2 < a$ vil $0 \le r_2 - r_1 < a$
Derfor må der gælde: $q_1 - q_2 = 0$, dvs $q_1 = q_2$.
Indsæt nu dette i de to første ligninger:
$b = q_1 \cdot a + r_1$
$b = q_1 \cdot a + r_2$, hvoraf vi let ser at også $r_2 = r_1$.
Konklusion: De to opskrivninger af divisionsligningen var i virkeligheden ens.

Definition. Største fælles divisor
Givet to tal $a,b \in \mathbb{Z}$. Det største tal blandt alle de fælles divisorer i *a* og *b* kaldes *den største fælles divisor i a og b* og betegnes med (a,b).

Bemærkning 1. Man møder ofte betegnelsen SFD(a,b), men vi nøjes med (a,b).
Bemærkning 2. Undersøg hvilken notation dit værktøjsprogram anvender.

Eksempel 3
(10,25) = 5 (42,14) = 14 (56,15) = 1

Øvelse 1
a) Hvilken strategi vil du anvende til at bestemme følgende, uden brug af dit værktøjsprogram:
1) (1134,6615) 2) (3026,1489)
b) Løs som kontrol opgaverne med brug af dit værktøjsprogram

Når vi har to ikke alt for store tal, som i øvelsen ovenfor, er det en overkommelig opgave at finde den største fælles divisor uden brug af værktøjsprogrammer, selvom det godt kan tage lidt tid. Specielt hvis man usystematisk gætter løs.

Den hurtigste metode, når vi har med overskuelige tal at gøre, er at finde de to tals fælles primfaktorer. Og vi kan jo nøjes med at finde det ene tals primfaktorer, og se hvilke der går op i det andet. Største fælles divisor er så produktet af disse primfaktorer.

Men hvad gør vi, hvis opgaven er at finde største fælles divisor mellem tallene: 182.135.106 og 13.974.858?

Der findes en metode til at regne sig frem til (a,b) for vilkårlige tal a og b. En regnemetode kaldes også en *algoritme*. Vi kender en hel del algoritmer: I folkeskolen lærte vi fx multiplikations- og divisionsalgoritmer, så vi kan gange og dividere vilkårlige tal med hinanden. Måske har du i gymnasiet lært algoritmen til at udføre polynomiers division, eller en algoritme til bestemmelse af nulpunkter, i tilfælde, hvor vi ikke har en formel.

Euklids algoritme

Metoden til at finde største fælles divisor har været kendt siden oldtiden og kaldes *Euklids algoritme*. Den virker på følgende måde overfor tallene *a* og *b*, hvor vi antager at *a* er større end *b* :
Først opskrives divisionsligningen for *a* divideret med *b*:

$$a = q_0 \cdot b + r_0$$

Dernæst divideres resten r_0 op i *b*:

$$b = q_1 \cdot r_0 + r_1$$

Således fortsættes. Næste trin er at dividere r_1 op i r_0 :

$$r_0 = q_2 \cdot r_1 + r_2$$

osv så vi får følgende system af ligninger:

$$\begin{aligned} a &= q_0 \cdot b + r_0 \\ b &= q_1 \cdot r_0 + r_1 \\ r_0 &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \qquad (**) \\ &\ldots \\ r_{n-1} &= q_{n+1} \cdot r_n + r_{n+1} \\ r_n &= q_{n+2} \cdot r_{n+1} \end{aligned}$$

På et tidspunkt vil divisionen gå op og resten blive 0, fordi alle rester er ≥ 0 og: $r_0 > r_1 > r_2 > \ldots > r_{n+1}$ (Overvej selv hvorfor dette er tilfældet).

Sætning 2
Det tal vi finder ved Euklids algoritme er den største fælles divisor: $(a,b)=r_{n+1}$

Før vi argumenterer for denne påstand ser vi på hvordan Euklids algoritme virker i praksis.

Eksempel 4
Vi ønsker at finde den største fælles divisor af to store tal, som fx 182.135.106 og 13.974.858.
Vi opskriver trin for trin divisionsligningerne efter systemet i (**):

$$182.135.106 = 13 \cdot 13.974.858 + 461.952$$
$$13.974.858 = 30 \cdot 461.952 + 116.298$$
$$461.952 = 3 \cdot 116.298 + 113.058$$
$$116.298 = 1 \cdot 113.058 + 3.240$$
$$113.058 = 34 \cdot 3.240 + 2.898$$
$$3.240 = 1 \cdot 2.898 + 342$$
$$2.898 = 8 \cdot 342 + 162$$
$$342 = 2 \cdot 162 + 18$$
$$162 = 9 \cdot 18$$

Altså er de to store tals største fælles divisor ifølge Euklids algoritme lug med 18.

Et lille teknisk råd: Ved de enkelte divisioner fås decimaltal fx:
13.974.858 : 461.952 = 30,25175343
De fleste værktøjsprogrammer kan udføre heltals division med rest – undersøg om dit kan. Hvis ikke, så kan heltalsdelen 30 let aflæses kvotienten. Resten findes lettest ved at gange decimalresten 0,25175343 med 461.952. Det giver den søgte rest: 116.298.

Bevis for sætning 2, dvs for at Euklids algoritme virker
Først vises, at r_{n+1} er en divisor i a og b.
Se igen på ligningssystemet (**) (og sammenlign evt med taleksemplet).
Gennemgå det nedefra og op:

Sidste ligning fortæller, at r_{n+1} går op i r_n.
Næstsidste ligning giver derfor, at r_{n+1} går op i begge led på højre side, derfor også op i venstre side, dvs r_{n+1} går op i r_{n-1}.
Tredjesidste ligning giver derfor ...
Og næstøverste ligning giver derfor at r_{n+1} går op i begge led på højre side, derfor også op i venstre side, dvs r_{n+1} går op i *b*.
Øverste ligning giver derfor at r_{n+1} går op i begge led på højre side, derfor også op i venstre side, dvs r_{n+1} går op i *a*.
Konklusion: r_{n+1} er en divisor i *a* og *b*.

Dernæst vises, at r_{n+1} er den største divisor i a og b. Dette gør vi ved at vise, at såfremt et tral *t* går op i både *a* og *b*, så går tallet *t* også op i r_{n+1}. Men så vil *t* specielt være mindre end r_{n+1}.
Dertil laver vi følgende lille ændring i ligningssystemet (**):

$$\begin{aligned} a - q_0 \cdot b &= r_0 \\ b - q_1 \cdot r_0 &= r_1 \\ r_0 - q_2 \cdot r_1 &= r_2 \\ r_1 - q_3 \cdot r_2 &= r_3 \qquad (***) \\ &\ldots \\ r_{n-1} - q_{n+1} \cdot r_n &= r_{n+1} \\ r_n - q_{n+2} \cdot r_{n+1} &= 0 \end{aligned}$$

Læs disse ligninger oppe fra og ned igennem:
Første ligning fortæller, at hvis et tal *t* er divisor i *a* og *b*, går det op i begge led på venstre side, derfor også op i højre side, dvs *t* er divisor i r_0.
Anden ligning fortæller, at hvis *t* er divisor i *b* og i r_0, så går det op i begge led på venstre side, derfor også op i højre side, dvs *t* er divisor i r_1.
Tredje ligning fortæller ...
Og næstsidste ligning giver endelig, at *t* går op i r_{n+1}.
Konklusion: Hvis et tal *t* er en divisor i *a* og *b* er det også en divisor i r_{n+1}. Denne må derfor være den største fælles divisor: $(a,b) = r_{n+1}$. (Slut på beviset!)

Euklids algoritme er et vigtigt værktøj i moderne kryptografiske systemer som RSA. Den anvendes bl.a. til at konstruere nøglen, der kan låse en smæklås op.
Følgende sætning, der er en af hovedsætningerne i talteorien, og som vi får ud fra Euklids algoritme, er et af de centrale værktøjer her:

Sætning 3
Den største fælles divisor *d* af to tal *a* og *b* ($(a,b) = d$)) kan skrives på formen:
$d = s \cdot a + t \cdot b$, hvor $s,t \in \mathbb{Z}$
Vi siger også, at *d* er skrevet som en linearkombination af *a* og *b*.

(*Bemærk, at et af tallene s og t naturligvis vil være negativt*)

Bevis.
Se på ovenstående udgave (***) af ligningssystemet, hvor alle r'erne er isoleret til højre. r_{n+1} er den største fælles divisor, som vi nu kalder d. Start med den næstnederste:

$$d = r_{n-1} - q_{n+1} \cdot r_n,$$

og indsæt heri r_n fra den tredjenederste, (der hedder $r_{n-2} - q_n \cdot r_{n-1} = r_n$)

$$\begin{aligned} d &= r_{n-1} - q_{n+1} \cdot r_n \\ &= r_{n-1} - q_{n+1} \cdot (r_{n-2} - q_n \cdot r_{n-1}) \\ &= (1 + q_{n+1} \cdot q_n) \cdot r_{n-1} - q_{n+1} \cdot r_{n-2} \end{aligned}$$

Nu er *d* skrevet som en kombination af r_{n-1} og r_{n-2}.
Indsæt heri r_{n-1} fra den fjerdenederste, (opskriv selv hvad denne hedder: $\ldots = r_{n-1}$), reducer og få *d* skrevet som en kombination af r_{n-2} og r_{n-3}.
…

Vi fortsætter nu med at indsætte ligning efter ligning op gennem rækken. For hvert trin skrives d som en kombination af *r*'erne, indtil vi til sidst indsætter r_1 og r_0. Tilbage på højre side er så 'et eller andet tal' gange a + 'et eller andet tal' gange b:

$$d = s \cdot a + t \cdot b, \text{ hvor } s,t \in \mathbb{Z}$$

Øvelse 2
18 kan altså skrives som en sådan kombination af de to store tal fra eksemplet ovenfor. Det kræver lidt regnearbejde. Men uden Euklids algoritme ville opgaven nok have virket uoverkommelig.
a) Undersøg om dit værktøjsprogram kan løse opgaven.
b) De 4 nederste divisionsligninger var:

$$3.240 = 1 \cdot 2.898 + 342$$
$$2.898 = 8 \cdot 342 + 162$$
$$342 = 2 \cdot 162 + 18$$
$$162 = 9 \cdot 18$$

og her står jo, at de4 også gælder at $(3240, 2898) = 18$.
Bestem ved håndkraft *s* og *t* så

$$18 = s \cdot 3240 + t \cdot 2898$$

Øvelse 3
a) Bestem største fælles divisor af tallene 53751 og 10465, og skriv den største fælles divisor som en *linearkombination* af de to tal, som angivet i sætning 3.
b) Vis, at største fælles divisor af tallene 1309 og 1235 er tallet 1, og bestem *s* og *t* så

$$1 = s \cdot 1309 + t \cdot 1235$$

Primiske tal og primtal

Øvelse 4.
For ethvert par af tal *s* og *t* vil $s \cdot a + t \cdot b$ være et helt tal. $d = (a, b)$ er et af disse tal ifølge sætning 3. Der gælder yderligere, at det er lige præcis *det mindste positive tal, der kan skrives således.* Vis dette.
(Hint: Der må findes et *mindste* positivt tal *e*, på formen: $s \cdot a + t \cdot b$. Vis at *e* = *d*)

Definition. Indbyrdes primisk
Hvis den største fælles divisor for *a* og *b* er 1, kaldes *a* og *b* for *indbyrdes primiske*.

Når $(a, b) = 1$ findes ifølge sætning 3 tal *s* og *t*, så

$$s \cdot a + t \cdot b = 1$$

Dette kan vi nu udnytte til at vise en vigtige sætning i talteorien:

Sætning 4
Hvis $p \mid (a \cdot b)$ og *p* er primisk med *a* (dvs $(a, p) = 1$), så gælder: $p \mid b$

Bevis
Når *p* er primisk med *a*, findes hele tal *s* og *t*, så:

$$s \cdot a + t \cdot p = 1$$

Gange ligningen igennem med *b*:

$$s \cdot a \cdot b + t \cdot p \cdot b = 1 \cdot b$$

p går op i tallene på venstre side af lighedstegnet.
Derfor går *p* også op i højre side: $p \mid b$.

To forskellige primtal er altid primiske. Og hvis et primtal går op i et andet primtal, må der være tale om det samme primtal. Sætning 4 giver derfor umiddelbart også:

Sætning 5
Antal tallet *N* er skrevet som et produkt af primtal: $N = p_1 \cdot p_2 \cdot p_3 \cdot ... p_n$.
Hvis *p* er et primtal, og $p|N$, så gælder, at : $p = p_i$ for et af primtallene i faktoriseringen af N.

Øvelse 5
Anvend sætning 5 til at bevise *aritmetikkens fundamentalsætning*:

Sætning 6 (Aritmetikkens fundamentalsætning)
Ethvert helt tal kan skrives på en og kun en måde som et produkt af primtal, dvs *primtalsfaktoriseringen af et helt tal er entydig*.

(Hint: Første del, nemlig at der findes en primtalsfaktorisering af ethvert helt tal, er simpelt: Enten er det selv et primtal, eller det er et sammensat tal, dvs det kan skrives som et produkt. Hver af disse tal er enten primtal eller sammensatte tal osv, indtil vi når frem til, at alle faktorer er primtal.
Anden del, entydigheden: Antag, at der to primtalsfaktoriseringer af et tal:

$$p_1 \cdot p_2 \cdot p_3 \cdot ... p_n = q_1 \cdot q_2 \cdot q_3 \cdot ... q_m \ ,$$

hvor alle faktorer er primtal. Anvend nu sætning 5 til at vise, at p_1 må være lig med et af *q'*erne. Forkort væk og tag fat på det næste *p* osv.)

Vi kalder denne opskrivning for *primfaktoropløsningen af N*. Sætningen siger altså at primfaktoropløsningen er éntydig.

Eksempel 4. Primfaktoropløsninger
a) $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ b) $574821 = 3^2 \cdot 13 \cdot 17^3$

Øvelse 6
Opskriv uden brug af værktøj en primfaktoropløsning af :

a) 42	b) 81	c) 225	d) 117
e) 1368	f) 2093	g) 1024	h)1025

Øvelse 7
Anvend dit værktøj til at opskrive en primfaktoropløsning af:

a) 3397	b) 1991009	c) 560560	d) $2^{32}+1$

Sætning 7
Den største fælles divisor for to hele tal a og b er produktet af deres fælles primfaktorer.

Bevis:
Vi opskriver en primfaktoropløsning af de to tal således:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot ... p_k \cdot q_1 \cdot q_2 \cdot q_3 \cdot ... q_s$$

$$b = p_1 \cdot p_2 \cdot p_3 \cdot ... p_k \cdot r_1 \cdot r_2 \cdot r_3 \cdot ... r_t$$

hvor *q*'erne og *r*'erne alle er forskellige.
Overvej selv hvorfor vi kan gøre det!
Sætningen siger: $d = (a,b) = p_1 \cdot p_2 \cdot p_3 \cdot .... \cdot p_k$

Det er klart at *d* er en divisor i a og b.
Lad os nu sige vi har et tal *e*, der er divisor i a og b. Opskriv så for *e*:

$$e = e_1 \cdot e_2 \cdot e_3 \cdot \ldots \cdot e_n$$

Alle e_i'erne er divisor i a og b.
Hvis e_1 går op i *a*, må det gå op i en af primfaktorerne; men e_1 er selv et primtal, så e_1 må være *lig med* en af *a*'s primfaktorer. Det samme må gælde for *b*. Så e_1 må være lig en af de *fælles* primfaktorer, altså netop lig en af *d*'s primfaktorer.
Således ser vi, at e_1 går op i *d*. Dette kan vi fortsætte, og får derfor, at *e* går op i *d*, så d er den *største fælles divisor*.

Øvelse 8
Når vi bevæger os op gennem talrækken til stadigt større tal, og på vores vej leder efter primtal, så smider vi undervejs alle sammensatte tal væk, dvs alle tal i 2-tabellen, alle tal i 3-tabellen, alle tal i 5-tabellen osv. Man kunne få den tanke, at vi på et tidspunkt får smidt alle tale væk, dvs at der ikke findes flere primtal. Men det gør der. Allerede hos Euklid finder vi den næste sætning, der i vores formulering lyder:

Sætning 7
Der findes uendeligt mange primtal.

Bevis:
Vi viser det indirekte.
Antag der kun var endeligt mange primtal: $p_1, p_2, p_3, \ldots, p_k$. Vi vil bevise, at dette fører til en modstrid. Dermed må vi så få, at antagelsen er forkert.
Betragt tallet: $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$
N er større end alle *p*'erne. Hvis *N* er et primtal har vi allerede en modstrid, for så har vi fundet endnu et primtal.
Hvis *N* er sammensat har det en primfaktor *q*. Hvis *q* er et af tallene $p_1, p_2, p_3, \ldots, p_k$ vil *q* gå op i tallet $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$. Men så kan *q* jo ikke også gå op i $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$. (q er større end 1, så "q-tabellens" skridt fremad på talaksen er større end 1). Derfor kan *q* ikke være et af tallene $p_1, p_2, p_3, \ldots, p_k$.
Altså har vi fundet et nyt primtal *q*. Men det var i modstrid med antagelsen.

Der findes således uendeligt mange primtal. Man har gennem tiderne været fascineret af disse mærkelige tal, og søgt at finde et system i dem. Men man regner i dag med, at der ikke kan findes en formel eller en algoritme, der giver os primtallene. Hvert nyt primtal må vi lede efter.

Men nøjes vi med at se statistisk på sagerne findes der et mærkeligt system i primtallene.
Man har i matematikhistorien indført en funktion, der betegnes $\pi(n)$, og som angiver *antallet af primtal der er mindre end n*.
Det viser sig nu, at der gælder følgende mærkelige formel (hvor tegnet $\approx$ betyder, det er en tilnærmelse:

$$\frac{\pi(n)}{n} \approx \frac{1}{\ln(n)}$$

Det var Gauss (1777-1855), en af de største matematikere, der har levet, der har æren af formlen. En dag, han som 14 årig sad og kiggede i en logaritme-tabel fik han ideen, og kradsede den ned i margenen. Et egentlig bevis blev først givet sidst i 1800-tallet, og beviset er meget vanskeligt. Men faktisk kan vi allerede hos Euler finde noget, der minder om denne formel. Leonard Euler (1707 - 1783) er den mest produktive matematiker, der har levet - han skrev 8-900 artikler og bøger, og en stor del af dem i de sidste 20 år af sit liv, hvor han var blind.

Øvelse 8

a) Giv en fortolkning af tallet $\frac{\pi(n)}{n}$

(Hint: Husk formlen fra sandsynlighedsregningen: Antal gunstige divideret med Antal mulige).
b) Vi trækker et tilfældigt tal mindre end 1 million. Vis, at sandsynligheden for, at det er et primtal er ca 7,2%.
c) Vis, at sandsynligheden for, at et tilfældigt valgt tal under 1 mia er et primtal, er ca 4,8% .

Øvelse 9
Kryptosystemet RSA, som vi undersøger i projekt 0.6, bygger netop på det manglende system i primtallene. For at undgå at koden kan knækkes ved at starte forfra med primtallene 2,3,5,... skal vi have nogle gigantiske primtal til rådighed. I RSA drejer det sig om primtal med et antal cifre på flere hundrede. Er det nu muligt overhovedet at finde primtal med feks 100 cifre? Kan du afgøre, hvad sandsynligheden er for, at et tilfældigt tal mellem 10^{99} og 10^{100} er primtal?

Øvelse 1 1) (1134,6615): 7 x 3 x 3 x 3 = 189
Øvelse 1 2) (3026,1489) =1
Øvelse 6 e) 1368 = 2^3 * 3^2 * 19
Øvelse 6 f) 2093 = 3^2 * 13 * 17^3