Problemløsing

Treningshefte foran
Niels Henrik Abels matematikk-konkurranse

Einar Andreas Rødland

199X

Innhold

Versjon: 18. mars 2006

1 Innledning

Løsing av problemer er en kunst som ikke i særlig grad blir trenet gjennom den vanlige undervisningen i skolen. De som deltar i Abel-konkurransen er derfor ofte ikke vant med typen problemstilling som oppstår: både i uttagningsrundene og i finalen. Målet med dette heftet er å gi et bedre grunnlag for å kunne angripe matematiske problemer, og det er spesielt rettet mot den type matematiske problemstillinger som man støter på i matematikk-konkurranser.

I motsetning til i de to uttagningsrundene, er finalen i Abel-konkurransen bevisorientert: problemet er ikke bare å finne riktig løsning, men å bevise det. Mange oppgaver vil faktisk være slik at svaret er oppgitt i oppgaven, og at problemet er å finne et bevis for at svaret er riktig. I tillegg til at elever sjelden har særlig erfaring med problemløsing, lærer man svært lite om beviser og bevisførsel i matematikk-undervisningen i skolen. Dette er forståelig, da bevisførsel setter store krav til teoretiske evner og matematikkundervisningen i skolen er rettet mot et bredere publikum. Det er dog en svært alvorlig mangel: matematikken er, som den eneste videnskap, bygget opp av logiske beviser og logiske deduksjoner, og kriteriet for at noe er sant er at det lar seg bevise. Uten bevis vil således matematikken stoppe opp.

Den beste måte å lære bevisførsel på er ved å lese beviser samt selv å jobbe med oppgaver. Av den grunn er dette hefter i stor grad viet til oppgaver.

Man må regne med å støte på vanskeligheter i løpet av heftet. Det er dog mulig å hoppe videre til neste kapittel selv om man ikke har forstått alt i de foregående; i mange tilfeller vil dette faktiske kunne være en stor fordel. Mitt råd er derfor at du ikke bør bli stående altfor lenge dersom det er noe som er vanskelig. Mye av poenget med heftet er oppgavene. Mange av oppgavene er resultater som er presentert i oppgaves form og der komplett løsning står i fasiten; andre oppgaver er oppgaver fra Abel-konkurransen eller på det nivået og for dem vil det ikke alltid være oppgitt fullstendig løsning i fasiten. Fasiten til oppgavene står bakerst i heftet, men jeg har også lagt med et kapittel med hint som du kan slå opp i dersom du skulle stå fast på en oppgave; hintene har som mål å kunne hjelpe litt på vei uten å røpe hele svaret slik at man fremdeles skal ha noe igjen å gjøre.

2 Logikk og beviser

Jeg vil her gi en kort innføring i et par logiske begreper. Dette er neppe riktig sted til å komme med en lengre innføring i formell logikk og hvordan beviser skal føres. Det læres lettest ved å studere notasjonen og bevisførselen i dette heftet. Jeg vil dog definere et par begreper som dere trolig har sett en del ganger før, men som det allikevel ikke skader å si noen ord om.

$\Rightarrow$: Implikasjon. Dette vil si at hvis uttrykket til venstre for pilen er riktig, så vil også uttrykket til høyre for pilen være riktig.

$\Longleftrightarrow$: Ekvivalens. Dette er det samme som implikasjon begge veier: uttrykket til venstre

er riktig hvis og bare hvis uttrykket til høyre er riktig.

Av disse to begrepene er det vanligste kun å benytte implikasjon; man starter gjerne med en antagelse og skal vise at da er ett eller annet riktig. I noen tilfeller benyttes ekvivalens, men det er heller sjelden. Ofte når man skal bevise en ekvivalens gjøres det ved først å vise implikasjonen den ene veien, og derefter den andre veien.

Eksempel 1. For å løse ligningen $\sin x = \cos x$ er det mulig å gå frem som følger:

$$\begin{aligned}
\sin x &= \cos x \\
\sin^2 x &= \cos^2 x \\
2\sin^2 x &= \cos^2 x + \sin^2 x = 1 \\
\sin^2 x &= \frac{1}{2} \\
\sin x &= \pm\frac{1}{\sqrt{2}} \\
x &= 45^\circ + k \cdot 360^\circ \text{ eller } 135^\circ + k \cdot 360^\circ \text{ der } k \in \mathbf{Z}
\end{aligned}$$

Vi har dog ikke vist at alle x som er som på nederste linje tilfredsstiller $\sin x = \cos x$. Faktisk vil vi få at $x = 45^\circ + k \cdot 360^\circ$ er alle mulige løsninger, mens $x = 135^\circ + k \cdot 360^\circ$ ikke gir noen løsning.

Oppgave 1. Hvilke av implikasjonene i eksempelet over er også ekvivalenser?

Heng deg ikke for mye opp i notasjonen. Matematisk notasjon er et sprog hvis mål er å formidle formelle definisjoner og logiske resonementer; det er således mere enn bare et sett med regneregler. Å forstå et bevis er langt mere enn å forstå hvert enkelt ledd og hver enkelt implikasjon: det er oversikt og intuisjon som ligger bak forståelse!

Ofte når noe skal bevises gjør man enkelte antagelser som ikke står i oppgaven. I utgangspunktet har man da kun bevist oppgaven for de tilfeller der disse antagelsene holder. Det er dog en del tilfeller der slike antagelser kan gjøres *uten tap av generalitet.* Dette forklares best med et eksempel.

Eksempel 2. Finn alle løsninger av $1/x + 1/y = 1/3$ der x og y er naturlige tall.

Siden vi kan bytte om x og y og fremdeles ha en løsning kan vi utan tap av generalitet anta at $x \leq y$; dersom omvendt skulle være tilfelle kunne vi selvsagt formulert beviset nedenfor, men byttet om x og y.

Siden $1/x \geq 1/y$ og $1/x + 1/y = 1/3$, må $1/x \geq 1/6 \geq 1/y$. Dette gir at $x \leq 6$. Ved å forsøke $x =$1, 2, 3, 4, 5 og 6 finner vi at kun $x = 4$ og $x = 6$ gir løsninger. Dette gir at (x, y) kan være $(4, 12)$, $(12, 4)$ eller $(6, 6)$.

Vanligvis er antagelser uten tap av generalitet utnyttelse av en symmetri der et bestemt valg foretrekkes. Symmetrien ovenfor er ombyttingen av x og y og valget at $x \leq y$. Eksempler på valg som kan gjøres uten tap av generalitet er:

- Dersom verdier $x_1, x_2, \ldots, x_n$ inngår i en oppgave og rekkefølgen av dem ikke har noe å si, kan man spesifisere at man krever en bestemt ordning: f.eks. at $x_1 \leq x_2 \leq \cdots \leq x_n$.
- Dersom man har en konstruksjon der absolutte lengder ikke er angitt, dvs. at hele konstruksjonen kan skaleres (forstørres/forminskes) uten å ha noen innvirkning, kan en bestemt størrelse spesifiseres, f.eks. ved å sette en bestemt lengde til 1.
- En geometrisk konstruksjon kan legges inn i et koordinatsystem og plasseres fritt med hensyn på origo og orientering, f.eks. ved å spesifisere at trekanten ABC har A i origo og B på x-aksen.

3 Geometri

Geometriske oppgaver er svært vanlige. Dessverre ser vi ofte at det er de geometriske oppgavene som volder de norske elever mest hodebry. Dette er kanskje en av de ting som det er lettest å trene på: det finnes en rekke resultater som kan være nyttige og som man kan lære seg. Her kommer jeg kun til å gjennomgå et par resulater og metoder.

Det er to vesentlig forskjellige angrepsmetoder på geometriske oppgaver. Den klassiske angrepsvinkelen omtales gjerne som den geometriske; her er likeformethet, parallellitet, like vinkler og lignende begreper sentrale. Alternativet er den algebraiske/aritmetriske angrepsvinkelen der man gir punktene koordinater eller beregner sidelengder, vinklers størrelse, etc. En klassisk geometrisk løsning skal ikke inneholde utregninger (ihvertfall ikke mere avanserte utregninger enn sum av vinkler eller sidelengder); dette er gjerne ansett som den 'reneste' løsning fra en rent estetisk synsvinkel. I mange tilfeller vil de to metodene kombineres.

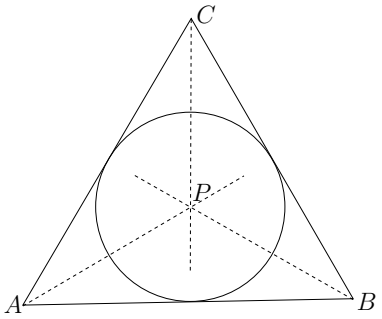
Jeg vil her konsentrere meg om de klassiske geometriske metoder; i det ligger dog ikke at de er de viktigste, kun at det i første omgang er de som er lettest å tilegne seg.

I geometriske konstruksjoner er det enkelte trekk som man bør lete efter:

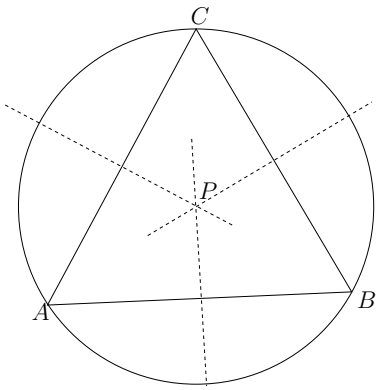
- Rette vinkler, normaler.
- Parallelle linjer.
- Linjestykker som har samme lengde eller vinkler som er like store.
- Likeformethet: deler av figuren er like, men i forskjellig målestokk.
- Punkter der flere linjer eller sirkler skjærer.

Noen resultater er verd å presentere. En trekant (i planet) har en *innskreven sirkel* og en *omskreven sirkel*. Den omskrevne sirkelen er sirkelen som går igjennom de tre hjørnene; den innskrevne sirkelen er sirkelen inni trekanten som tangerer trekantens tre kanter. Sentrum til hver av disse sirklene er knyttet opp imot to geometriske konstruksjoner.

Teorem 3. *La ABC være en trekant. Trekk linjen gjennom A som deler vinkelen $\angle CAB$ i to like vinkler og gjør tilsvarende for de andre to hjørnene. De tre linjene vil da skjære hverandre i ett punkt P som også er sentrum i den innskrevne sirkelen.*



Bevis. Linjen l som halverer $\angle CAB$ består av de punkter som ligger like langt fra linjen AB som fra linjen AC. Linjen m som halverer $\angle ABC$ består av punkter som ligger like langt fra AB som BC. For skjæringspunktet P mellom l og m vil vi da ha at avstanden fra P til AC er lik avstanden fra P til AB som igjen er lik avstanden fra P til BC. Dette gir at avstanden fra P til AC er lik avstanden fra P til BC, og følgelig ligger P på linjen som halverer $\angle BCA$. Dersom r er avstanden fra P til hver av sidekantene og vi trekker en sirkel om P med radius r, så vil den sirkelen tangere de tre kantene. □

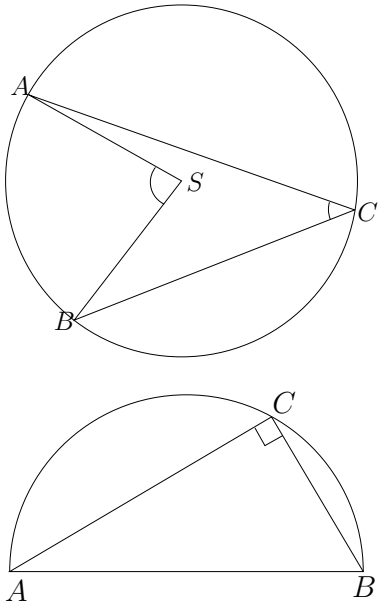


Oppgave 2. La ABC være en trekant. Midtnormalene til kantene BC, AC og AB skjærer hverandre da i ett punkt P som samtidig er sentrum i den omskrevne sirkelen.

Det er en rekke resultater som kan være nyttige; jeg har plukket ut ett som er mye brukt og som er langt fra trivielt.

Teorem 4 ((Sirkelens periferivinkel))**.** *Anta at vi har en sirkel med sentrum S. La A, B og C være punkter på sirkelen. Da er $\angle BSA = 2\angle BCA$. Spesielt ser vi at dersom A og B er gitt er $\angle ACB$ uavhengig av hvor på sirkelen C plasseres. (Dersom C ligger mellom A og B må den ytre vinkelen brukes.)*

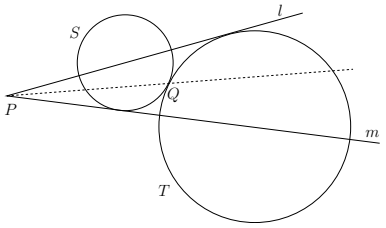
Bevis. Siden SCA og SBC er likebenede er $\angle SBC = \angle BCS$ og $\angle CAS = \angle SAC$. Vi har at $\angle BCA = \angle BCS + \angle SCA$. Vi har også at $\angle ASC = 180° - 2\angle SCA$ og $\angle CSB = 180° - 2\angle BCS$. Dette gir at $\angle BSA = 360° - \angle CSB - \angle ASC = 2\angle BCS + 2\angle CAS = 2\angle BCA$. □



Et spesialtilfelle av dette får vi dersom AB er diameter i en sirkel S og et C et punkt på sirkelen. Da er ABC en rettvinklet trekant. Dette kan forøvrig vises ganske lett uten å bruke setningen om periferivinkler.

Oppgave 3. La $ABCD$ være en firkant som er innskrevet i en sirkel S: dvs. at hjørnene A, B, C og D ligger på S. Vis at da er $\angle A + \angle C = \angle B + \angle D = 180°$.

Vis at også det motsatte gjelder: dersom $\angle A + \angle C = \angle B + \angle D = 180°$ kan firkanten innskrives i en sirkel.



Oppgave 4. La to linjer l og m skjære i et punkt P. To sirkler S og T har sentrum på hhv. l og m, tangerer den andre linjen og tangerer hverandre i et punkt Q. Vis at linjen PQ halverer vinkelen mellom l og m.

4 Reductio ad absurdum

Reductio ad absurdum er en svært vanlig bevisteknikk. Ideen er som følger. Du skal bevise en påstand. Anta i stedet at denne påstanden er gal; dersom du da kan utlede en selvmotsigelse eller noe annet som må være galt må påstanden være riktig.

Eksempel 5. Euklid beviste at det fantes uendelig mange primtall (naturlige tall som bare er delelige med 1 og seg selv).

Anta at det kun finnes et endelig antall: $p_1, p_2, \ldots, p_n$. La så $x = p_1 p_2 \cdots p_n + 1$; da er ingen av p'ene faktor i x og x må dermed ha andre primfaktorer enn de n som man hadde ifra før. Dette strider imot antagelsen om at $p_1, \ldots, p_n$ er alle primtall. Følgelig kan det ikke være endelig mange primtall.

(Det er et lite steg som er utelatt her, og det er beviset for at ethvert tall kan primtallsfaktoriseres, eller spesielt at x nødvendigvis må ha primfaktorer. Dette vil jeg komme tilbake til i seksjonen om tallteori.)

Eksempel 6. (Kan være vanskelig.) La M være en mengde (ikke nødevendigvis endelig) og la $\mathcal{P}(M)$ være potensmengden til M: mengden av alle delmengde av M. Vis at det ikke finnes noen funksjon $f\colon M \to \mathcal{P}(M)$ som er surjektiv (=på, dvs. at for enhver $a \in \mathcal{P}(M)$ finnes en $x \in M$ slik at $f(x) = a$). Dersom en slik funksjon skulle finnes ville det si at M inneholder minst like mange elementer som $\mathcal{P}(M)$ (hva nå enn det skulle bety for uendelige mengder som mengden av naturlige, rasjonale eller reelle tall).

For å bevise dette antar vi først at det finnes en slik funksjon. Ifra denne f kan vi da konstruere mengden A av elementer $x \in M$ slik at $x \notin f(x)$:

$$A = \Big\{ x \in M \mid x \notin f(x) \Big\}.$$

Dette kan forøvrig også uttrykkes

$$x \in A \iff x \notin f(x).$$

Siden A er en delmengde av M og f er surjektiv (på), finnes en $a \in M$ slik at $f(a) = A$. Er da $a \in A$? Ifølge definisjonen av A skal $a \in A$ hvis og bare hvis $a \notin f(a) = A$, altså

$$a \in A \iff a \notin f(a) \iff a \notin A.$$

Dette er en opplagt selvmotsigelse, og følgelig kan ikke en slik funksjon f eksistere.

5 Induksjonsbevis

En annen vanlig bevisteknikk er induksjon. Ideen er at hvis man har en rekke med påstander — la oss kalle dem $P_0, P_1, P_2, \ldots$ — og kan vise først at P_0 er riktig og dernest at $P_n \Rightarrow P_{n+1}$, så har man bevist at de alle er riktige: man har jo at $P_0 \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \cdots$. Ofte kalles P_0 for *null-hypotesen* og $P_n \Rightarrow P_{n+1}$ for *induksjonshypotesen*. I neste kapittel om kombinatorikk kommer du til å møte denne bevisteknikken en rekke ganger, jeg nøyer meg derfor med et kort eksempel.

Eksempel 7. Vis at $\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = n(n+1)/2$.

Det er flere måter å vise dette på, men jeg har tenkt å gjøre det ved hjelp av induksjon for å demonstrere metoden. La da P_n være påstanden $1 + 2 + \cdots + n = n(n+1)/2$. La $a_n = 1 + 2 + \cdots + n$ og $b_n = n(n+1)/2$. Nullhypotesen, at $a_1 = b_1$, er lett å se. For å

vise induksjonshypotesen kan vi først vise at $a_{n+1} = a_n + n + 1$ og $b_{n+1} = b_n + n + 1$. Siden vi antar at $a_n = b_n$ får vi at $a_{n+1} = a_n + n + 1 = b_n + n + 1 = b_{n+1}$. Dette beviser (ved induksjon) at $1 + 2 + \cdots + n = n(n+1)/2$ for alle n.

Det vil dukke opp rikelig av eksempler på induksjon; disse bør studeres inntil du føler deg helt trygg på metoden.

Oppgave 5. Vis at $\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = (\sum_{i=1}^{n} i)^2 = (1 + 2 + \cdots + n)^2$.

Oppgave 6. Hvor mange delmengder $A \subset \{1, 2, 3, \ldots, 11\}$ finnes slik at dersom $2m \in A$ er også $2m - 1$ og $2m + 1 \in A$?

6 Kombinatorikk

I navnet 'kombinatorikk' ligger at man skal gjøre kombinasjoner. Vanligvis går dette ut på å telle opp antall kombinasjoner av noe som tilfredsstiller bestemte regler.

Eksempel 8. Dersom man har n kuler som er nummerert ifra 1 til n, i hvor mange forskjellige rekkefølger er det da mulig å legge kulene?

Svaret er $n! = 1 \cdot 2 \cdot 3 \cdots n$; $n!$ uttales n *fakultet* og en slik omskyfling av rekkefølgen kalles en *permutasjon*. Dette kan bevises ved hjelp av induksjon.

Dersom $n = 1$ er det opplagt bare en mulighet. Vi antar som induksjonshypotese, at n kuler kan legges i $n!$ forskjellige rekkefølger. For $n + 1$ kuler kan man først legge kule nummer $n + 1$ i en av $n + 1$ forskjellige posisjoner, mens de resterende posisjonene fylles av de andre n kulene der de n gjenværende kulene har $n!$ forskjellige rekkefølger. Dette gir at antall rekkefølger for $n + 1$ kuler er $(n + 1) \cdot n! = (n + 1)!$.

Eksempel 9. Dersom man har n røde kuler og m blå kuler, hvor mange forskjellige rekkefølger kan man da legge dem i. (De røde kulene er like og de blå kulene er like.)

Dersom man nummererer alle kulene, kan de legges i $(n + m)!$ forskjellige rekkefølger. De røde kulene kan innbyrdes ordnes i $n!$ forskjellige rekkefølger og de blå i $m!$ forskjellige rekkefølger. For hver måte å ordne kulene på efter farve (altså uten at kulene er nummerert) finnes det derfor $n! \cdot m!$ forskjellige måter å nummerere dem på. Det vil si at blant de $(n + m)!$ forskjellige nummererte ordningene ligger hver farvekombinasjon på $n! \cdot m!$ forskjellige måter. Da må antall mulige farvekombinasjoner være

$$\binom{n+m}{n} = \binom{n+m}{m} = \frac{(n+m)!}{n! \cdot m!}$$

der $\binom{N}{n}$ er *binomialen* N over n.

Oppgave 7. Dersom det finnes n_1 kuler av en farve, n_2 kuler av en annen farve, osv. opp til n_m kuler av en m'te farve, hvor mange forskjellige ordninger av kulene finnes (dersom kuler av samme farve er identiske)?

7 Primtall og tallteori

Ett av de virkelig gamle feltene i matematikk er tallteorien: studien av de hele tallene. Sentralt i tallteorien er *primtall*. Primtallene er de naturlige tall større enn en som ikke har andre faktorer enn en og seg selv. De første primtallene er 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

For de hele tall er addisjon en enkel og godt forstått operasjon. Mulitiplikasjon er tilsynelatende også en relativt enkel operasjon; likevel ligger det et hav av uavklarte problemer knyttet til multiplikative egenskaper og delelighetsegenskaper ved de hele tall. Et så tilsynelatende enkelt problem som faktorisering av store tall er regnet som så vanskelig at anerkjente kryptosystemer (systemer for å lage hemmelige koder) baseres på at det er praktisk umulig for tilstrekkelig store tall.

Hvis x og y er hele tall vil vi si at x deler y — skrives $x \mid y$ — dersom det finnes et heltall n slik at $y = n \cdot x$.

Oppgave 8. Vis at følgende holder for alle heltall x, y og z:

1. $1 \mid x$.
2. $x \mid y$ og $y \mid x \Rightarrow x = \pm y$.
3. $x \mid y$ og $y \mid z \Rightarrow x \mid z$.
4. $xy \mid z \Rightarrow x \mid z$ og $y \mid z$.

Vanligvis når man snakker om delelighet begrenser man seg til å jobbe med de naturlige tall: 1, 2, 3, 4, ... På de naturlige tall er det for to tall, x og y, definert en *største felles divisor* — $\gcd(x, y)$ (Greatest Common Divisor); dette er definert som den største n slik at $n \mid x$ og $n \mid y$. En svært vanlig betingelse er at to heltall skal være *uten felles faktor* eller *relativt primiske:* det er det samme som at $\gcd(x, y) = 1$.

Oppgave 9. La x, y og z være naturlige tall. Vis at da holder følgende:

1. $\gcd(1, x) = 1$ og $\gcd(x, 0) = x$.
2. $x \mid y \Rightarrow \gcd(x, z) \mid \gcd(y, z)$.
3. $\gcd(x, y) = \gcd(x, y + mx)$ for alle $m \in \mathbf{Z}$.

Selv for store tall kan største felles divisor regnes ut ganske raskt. Algoritmen som brukes kalles *Euklids algoritme* og bygger på at $\gcd(x, y) = \gcd(x, y - mx)$.

Teorem 10 ((Euklids algoritme))**.** *Vi ønsker å regne ut* $\gcd(x, y)$ *der* $x, y \in \mathbf{N}$. *Anta at* $x > y$*; ellers kan man bare bytte dem om. Siden* $x > y$ *er* $x = ay + z$ *der* $a \in \mathbf{N}$ *og* z *er et heltall mellom null og* $y - 1$*; dersom man deler* x *på* y *får man* a *med* z *som rest. Da er* $\gcd(x, y) = \gcd(y, ay + z) = \gcd(y, z)$*. Denne prosessen gjentar man inntil den stopper opp: man får* $z = 0$.

Mere formelt kan man sette det opp som følger. La $x_0 = x$ *og* $x_1 = y$*. Vi kan la* $x_n = a_n x_{n+1} + x_{n+2}$ *for en* $a_n \in \mathbf{N}$ *ved å la* x_{n+2} *være resten man får når man deler* x_n

på n_{n+1}. Denne vil da tilfredsstille $\gcd(x_n, x_{n+1}) = \gcd(x_{n+1}, x_{n+2})$. *Vi fortsetter med dette helt inntil vi får* $x_{n+2} = 0$ *(altså at* $x_{n+1} \mid x_n$*); da er* $\gcd(x_0, x_1) = \gcd(x_1, x_2) = \cdots = \gcd(x_n, x_{n+1}) = \gcd(x_{n+1}, x_{n+2}) = \gcd(x_{n+1}, 0) = x_{n+1}$. *(Denne bevismetoden der man går nedover til man stopper kalles uendelig descent.)*

Algoritmen har et viktig biresultat; det finnes heltall r *og* s *slik at* $\gcd(x, y) = rx + sy$. *For å se dette kan vi bare se på hvordan følgen* x_i *er definert:* $x_{i+2} = x_i - a_i x_{i+1}$. *Dersom* $x_i = r_i x + s_i y$ *og* $x_{i+1} = r_{i+1} x + s_{i+1} y$ *blir* $x_{i+2} = r_{i+2} x + s_{i+2} y$ *der* $r_{i+2} = r_i - a_i r_{i+1}$ *og* $s_{i+2} = s_i - a_i s_{i+1}$. *Dersom* $x_{n+2} = 0$ *som over, vil da* $\gcd(x, y) = x_{n+1} = r_{n+1} x + s_{n+1} y$.

Eksempel 11. La oss ta to store tall: 779 og 1729. Vi har da at

$$\begin{aligned}\gcd(779, 1729) &= \gcd(779, 171 + 2 \cdot 779) = \gcd(779, 171) \\ &= \gcd(171, 95 + 4 \cdot 171) = \gcd(171, 95) \\ &= \gcd(95, 76 + 1 \cdot 95) = \gcd(95, 76) \\ &= \gcd(76, 19 + 1 \cdot 76) = \gcd(76, 19) \\ &= \gcd(19, 4 \cdot 19) = 19\end{aligned}$$

For primtall finnes en rekke sterkere resultater. De viktigste følger i oppgaven nedenfor.

Oppgave 10. La x, y og z være naturlige tall og la p og q være primtall. Vis at:

1. $p \mid q \Rightarrow p = q$.
2. $\gcd(p, x)$ er enten lik 1 eller lik p.
3. $p \mid xy \Rightarrow p \mid x$ eller $p \mid y$.

Det at $p \mid xy \Rightarrow p \mid x$ eller $p \mid y$ for p primtall gir opphav til noe av det viktigste ved primtall: entydig primfaktorisering. Det vil si at ethvert naturlig tall kan skrives som prudukt av primtall på en og bare en måte (opptil faktorenes orden). Altså, dersom vi ramser opp primtallene — $p_1, p_2, \ldots$ — kan ethvert naturlig tall x skrives $x = p_1^{n_1} p_2^{n_2} \cdots$ der $n_i \in \mathbf{N}_0$ (naturlige tall og null) på en eneste måte.

Oppgave 11. Vis at dersom $x^2 + y^2 = z^2$ der $x, y, z \in \mathbf{N}$, så finnes $u, v \in \mathbf{N}$ slik at $z = (u^2 + v^2)/2$ og x og y har verdiene $(u^2 - v^2)/2$ og uv.

8 Modulo-regning

Ved regning med hele tall er det fremdeles en ting som til tider skaper problemer: det er uendelig mange av dem. En metode for å bøte på det problemet er bruk av residual-regning eller *modulo-regning.* Ideen er at når man regner modulo n der n er et heltall, sier man at to tall er like (eller kongurente) dersom differansen er et heltallig multiplum av n. Dette er det samme som at man ser på resten når man deler tallet på n. La meg ta dette litt mere formelt.

Definisjon 12. La $n \in \mathbf{Z}$. Dersom $x, y \in \mathbf{Z}$ sier vi at x og y er *kongurente modulo* n dersom $n \mid x - y$; vi skriver da at $x \equiv y \bmod n$.

I stedet for å betrakte $\equiv \bmod n$ som en relasjon på de hele tall er det naturlig å samle kongurente tall til det vi kaller kongurensklasser. Dersom vi da ser på de hele tall modulo n (anta at n er et naturlig tall) kan vi da kalle kongurensklassene for $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{n-1}$; vi lar da $\mathbf{Z}_n$ betegne mengden av kongurensklasser modulo n. Vi har da at $\overline{x}$ svarer til tallene x, $x+n$, $x-n$, $x+2n$, $\ldots$.

Eksempel 13. Anta at vi har en mengde A som inneholder n forskjellige heltall. Hvis $m < n$ er et naturlig tall, så finnes det alltid to forskjellige elementer $x, y \in A$ slik at $x \equiv y \bmod m$: altså slik at $x - y$ er delelig med m.

Hvis vi lar elementene i A være $a_1, a_2, \ldots, a_n$ kan vi skrive disse modulo m: $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n} \in \mathbf{Z}_m$. Siden det kun finnes m elementer i $\mathbf{Z}_m$, så kan ikke alle n elementer i følgen $\overline{a_i}$ være forskjellige: altså må $\overline{a_j} = \overline{a_k}$ der $j \neq k$. Dette vil si at $a_j \equiv a_k \bmod m$.

Problemet med at $\mathbf{Z}$ har uendelig mange elementer finnes således ikke for $\mathbf{Z}_n$: $\mathbf{Z}_n$ har kun n elementer. Dette gjør at enkelte operasjoner blir langt mere oversiktlige i $\mathbf{Z}_n$ enn i $\mathbf{Z}$.

Oppgave 12. Det er en del viktige egenskaper med modulo-begrepet som gjør at det er interessant. For alle $x, y, z, u, n \in \mathbf{Z}$ holder:

1. $x \equiv y \bmod n$ og $y \equiv z \bmod n \Rightarrow x \equiv z \bmod n$.

2. $x \equiv y \bmod n$ og $z \equiv u \bmod n \Rightarrow x + z \equiv y + u \bmod n$ og $xz \equiv yu \bmod n$; kort sagt, kongurens modulo n bevares under addisjon og multiplikasjon.

Vi ser at vi fremdeles kan bruke addisjon og multiplikasjon nøyaktig som vi pleier. Tilsvarende kan vi bruke subtraksjon: $x - y = x + (-1) \cdot y$.

Eksempel 14. La oss gjøre noen utregninger modulo 13 og se hvordan det ser ut. Vi har at $2 \equiv 15 \bmod 13$, eller $\overline{2} = \overline{15}$ i $\mathbf{Z}_{13}$. Vi har også at $7 \equiv 20 \bmod 13$. Regnereglene sier da at $2 \cdot 7 = 14 \equiv 15 \cdot 20 = 300 \bmod 13$. Dersom vi tar differansen, får vi at $15 \cdot 20 - 2 \cdot 7 = 300 - 14 = 286 = 13 \cdot 22$.

Eksempel 15. Hvis vi ønsker å finne ut hva siste siffer i 97^{187} er så kan vi se på tallet modulo 10. Da har vi at $97^{187} \equiv 7^{187} \bmod 10$. Hvis vi ser på potenser av 7 modulo 10, så får vi at $7^2 = 49 \equiv 9 \equiv -1 \bmod 10$, og dermed at $7^4 = 49^2 \equiv (-1)^2 = 1 \bmod 10$. Vi kan så bruke at $7^4 \equiv 1 \bmod 10$ til å forenkle utregningen betraktelig. Vi har at $187 = 46 \cdot 4 + 3$ og dermed at $97^{187} \equiv 7^{187} = 7^{46 \cdot 4 + 3} = (7^4)^{46} \cdot 7^3 \equiv 1^{46} \cdot 7^3 = 7^3 = 7^2 \cdot 7 \equiv (-1) \cdot 7 = -7 \equiv 3 \bmod 10$. Altså er siste siffer 3.

Eksempel 16. Det er en kjent regneregel at dersom et tall er delelig med 9, så er også tverrsummen delelig med 9. Faktisk er x kongurent med tverrsummen av x modulo 9.

Hvis $x = x_0 + 10x_1 + 100x_2 + \cdots$, så følger jo at tverrsummen $x_0 + x_1 + \cdots \equiv x_0 + 10x_1 + \cdots = x \bmod 9$ fordi $1 \equiv 10 \equiv 100 \equiv \ldots \bmod 9$.

Eksempel 17. Dersom vi ser på x^2 mod 3 finner vi at det er begrenset hvilke verdier denne kan ta: i $\mathbf{Z}_3$ er $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$ og $\overline{2}^2 = \overline{1}$. Vi ser altså at x^2 aldri kan bli -1 mod 3.

Oppgave 13. Vis at det finnes uendelig mange tall som ikke kan skrives som sum av to kvadrattall.

Oppgave 14. Finn alle $n, m \in \mathbf{N}_0$ slik at $2^n + 1 = 5^m$.

Oppgave 15. Gitt fem forskjellige punkter i planet med heltallige koordinater. Vis at linjestykket mellom to av dem går gjennom et punkt i planet med heltallige koordinater.

Divisjon går dog ikke som før. Dersom for eksempel $n = 6$ vil vi ha at $2 \not\equiv 0 \bmod 6$ og $3 \not\equiv 0 \bmod 6$, men produktet av dem $2 \cdot 3 = 6 \equiv 0 \bmod 6$. Vi kan altså gange sammen tall forskjellige fra null og få null; her skiller modulo-regningen seg klart fra det vi er vant til fra de hele tallene. Dette problemet oppstår dog ikke dersom vi regner modulo et primtall.

Oppgave 16. Vis at dersom p er et primtall og $x, y \in \mathbf{Z}$ slik at $x \not\equiv 0 \bmod p$ og $y \not\equiv 0 \bmod p$, så er $xy \not\equiv 0 \bmod 0$. Altså, i $\mathbf{Z}_p$ er det slik at dersom produktet er null må en av faktorene være null.

9 Algebra og polynomer

Det er ganske vanlig at oppgaver inneholder polynomer. Det er et par ting som da kan være godt å huske på.

Dersom $p(x) = x^n + a_{n-1}x^n + \cdots + a_1x + a_0$ er slik at $p(b) = 0$, så kan vi skrive $p(x) = q(x) \cdot (x - b)$. En svært vanlig situasjon er kravet om at polynomet kan ha grad n og n røtter (dvs. nullpunkter); det vil si at $p(x) = (x - b_1)(x - b_2) \cdots (x - b_n)$. Videre kan man kreve at røtten skal være forskjellige (eller distinkte), dvs. at $b_i \neq b_j$ for $i \neq j$; det motsatte er at $p(x)$ har multiple røtter, f.eks. $x^2 + 2x + 1 = (x + 1)^2$.

Dersom $p(x) = x^n + a_{n-1}x^n + \cdots + a_1x + a_0 = (x - b_1)(x - b_2) \cdots (x - b_n)$, er $a_0 = (-1)^n b_1 b_2 \cdots b_n$ og $a_{n-1} = -(b_1 + b_2 + \cdots + b_n)$. (Merk at $(-1)^n$ er lik 1 dersom n er like og -1 dersom n er odde.)

Eksempel 18. Dersom du kan finne nullpuntktene til et polynom har du bestemt polynomet og vil i mange tilfeller være kommet langt på vei mot en løsning. Et eksempel på dette er polynomet $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ der vi får vite at $p(x) = x$ for $x = 1, 2, \ldots n$ og spørsmålet f.eks. er å finne $p(0)$. Da kan du benytte at $p(x) - x = 0$ for $x = 1, 2, \ldots, n$. Da vet vi at siden p er av grad n og har de n nullpunktene $1, 2, \ldots, n$ at $p(x) = a \cdot (x - 1) \cdot (x - 2) \cdots (x - n)$ der a må være lik 1. Ved å sette inn $x = 0$ får vi da at $p(0) = (-1) \cdot (-2) \cdots (-n) = (-1)^n \cdot n!$.

Oppgave 17. La $p(x)$ være et polynom av grad n slik at $p(k) = k/(k + 1)$ for $k = 0, 1, 2, \ldots, n$. Hva er da $p(n + 1)$?

Oppgave 18. Vis at dersom $x_i \geq 0$ så er

$$(1 + x_1) \cdot (1 + x_2) \cdots (1 + x_n) \geq 1 + x_1 + x_2 + \cdots + x_n.$$

Oppgave 19. Vis at dersom $a_1, \ldots, a_n \geq 1$, så er

$$(1 + a_1) \cdots (1 + a_n) \geq \frac{2^n}{n+1}(1 + a_1 + \cdots + a_n).$$

10 Ulikheter

Det finnes en rekke ulikheter som kan brukes. Den mest kjente er nok at $x^2 \geq 0$ for alle x. Fra denne er det mulig å utlede ulikheter som ikke er like opplagte.

Eksempel 19. Siden $(x - y)^2 \geq 0$ kan vi også gange ut og få $x^2 - 2xy + y^2 \geq 0$. Ved å flytte over gir dette den mere kjente ulikheten $x^2 + y^2 \geq 2xy$.

Eksempel 20. La $x, y \geq 0$. Da har vi at det geometriske gjennomsnittet $\sqrt{xy}$ er mindre enn eller lik det aritmetiske gjennomsnittet $\frac{x+y}{2}$. For å vise dette kan vi bruke at $(x+y)^2 = (x - y)^2 + 4xy \geq 4xy$. Ved å dele med 4 og ta kvadratroten får vi da $\frac{x+y}{2} \geq \sqrt{xy}$.

Oppgave 20. Vis at for $x > 0$ er $x + \frac{1}{x} \geq 2$. Når er det likhet?

Oppgave 21. Vis at $x^2 + y^2 + z^2 \geq xy + xz + yz$.

11 Hint

Denne seksjonen kunne selvsagt gitt fullstendige løsninger på alle oppgavene. Jeg tror dog at dere vil ha større utbytte av ikke å få hele svaret, men bare noen hint på veien når dere står fast. Disse hintene inneholder ofte bare henvisning til hvaslags resulater dere kan bruke for å løse oppgaven. Det er selvsagt også mulig at det finnes andre løsninger enn de jeg har funnet.

1. Husk at $x^2 = y^2$ $x = \pm y$.

2. Vis at $AP = BP = CP$.

3. La S være sentrum i sirkelen og bruk setningen om periferivinkler på $SABC$ og $SCDA$.

4. Vis at avstanden fra Q til l er lik avstanden fra Q til m.

5. La a_n og b_n være summen av hhv. venstre og høyre side. Vis at $a_1 = b_1$ og at $a_{n+1} - a_n = b_{n+1} - b_n$.

6. La antallet tillatte $A \subset \{1, 2, \ldots, n\}$ være a_n. Anta at a_{n-1} og a_{n-2} er kjent, og uttrykk a_n ved hjelp av dem. Det er ikke sikkert at tilfellene n odde og n like kan behandles helt likt.

7. Slå først sammen de $m - 1$ første farvene, og bruk resultatet fra eksempelet over.

8. Bruk definisjonen og finn hva n (fra definisjonen) må være.

9. Bruk definisjonen og resultatene om delelighet.

10. Definisjonen av primtall. På det siste punktet kan du bruke at $ap+bx = cp+dy = 1$ for passende heltall a, b, c, d.

11. Anta at x, y og z ikke har noen felles faktor og at x er odde. Bruk at $x^2 = (z-y)(z+y)$ og at $\gcd(z-y, z+y) = 1$.

12. Kun å sette inn for definisjonen.

13. Se på problemet modulo 4.

14. Vis først at m er et partall; se på ligningen modulo 8.

15. Se på punktene modulo 2; hvor mange 'forskjellige' punkter finnes det da.

16. Husk at $x \equiv 0 \bmod p \iff p \mid x$.

17. La $q(x) = (x+1) \cdot p(x) - x$.

18. La $p(x) = (x+x_1)\ldots(x+x_n)$ der du kan sette inn $x = 1$.

19. Sett inn $a_i = 1 + 2x_i$ der $x_i \geq 0$.

20. Bruk ulikheten $u^2 + v^2 \geq 2uv$ med passende verdier for u og v. Likhet når $x = 1$.

21. Bruk $x^2 + y^2 \geq 2xy$.

12 Fasit

Her kommer en mere utførlig fasit.

1. Den første implikasjonen gir ingen ekvivalens; f.eks. $x = 135°$ som i stedet gir $\sin x = -\cos x$. De andre fire implikasjonene er også ekvivalenser.

2. La først P være skjæringspunktet mellom midtnormalen på AB og BC. Siden P ligger på midtnormalen til AB må $AP = BP$; siden den ligger på midtnormalen til BC må $BP = CP$. Dette gir $AP = BP = CP$. En sirkel med sentrum i P og radius lik AP vil da gå igjennom samtlige tre hjørner.

3. La S være sentrum i sirkelen. Vi har da at $\angle CSA = 2\angle ABC$ og $\angle ASC = 2\angle CDA$. Siden $\angle CSA + \angle ASC = 360°$, må $\angle ABC + \angle CDA = 180°$. .. For å vise det motsatte kan vi trekke en sirkel gjennom A, B og C. Linjen CD skjærer da sirkelen i ett punkt i tillegg til C; kall dette punktet X. Da må $\angle CXA = 180° - \angle ABC = \angle CDA$. Denne vinkelen bestemmer posisjonen på linjen CD entydig, og derfor må $D = X$.

4. La S ha sentrum A og T ha sentrum B; disse punktene ligger hhv. på l og m. La S tangere m i M og T tangere l i L. La $a = AM$ være radien til S og $b = BL$ være radien til T. Normalene fra Q på l og m treffer l og m i punktene U og V. Der er AMB og QVB likeformede der størrelsene har forholdet $a + b : b$; følgelig er $QV = AM \cdot b/(a+b) = ab/(a+b)$. Tilsvarende er $QU = ab/(a+b) = QV$. Siden avstandene fra Q til l og m er like, må PQ dele vinkelen mellom l og m i to like deler.

5. La a_n og b_n være summen av hhv. venstre og høyre side. Da er $b_n = n^2(n+1)^2/4$. Vi har at $a_1 = b_1 = 1$; dette beviser nullhypotesen. .. Anta så at $a_n = b_n$. Vi har da at

$a_{n+1} = a_n + (n+1)^3$. Vi har at $b_{n+1} - b_n = (n+1)^2(n+2)^2/4 - n^2(n+1)^2/4 = (n+1)^3$. Da må også $a_{n+1} = b_{n+1}$.

6. Anta først at n er et partall. Dersom $n \in A$, må da også $n-1 \in A$; de resterende $n-2$ kan da velges på a_{n-2} tillatte måter. Dersom $n \notin A$ kan de resterende $n-1$ velges på a_{n-1} forskjellige måter. Altså er da $a_n = a_{n-1} + a_{n-2}$. .. Anta så at n er odde. Dersom $n \in A$ kan de resterende $n-1$ velges på a_{n-1} tillatte måter. Dersom $n \notin A$ må også $n-1 \notin A$; de resterende $n-2$ kan da velges på a_{n-2} tillatte måter. Igjen blir $a_n = a_{n-1} + a_{n-2}$. .. Vi har at $a_0 = 1$ og $a_1 = 2$. Videre får vi da at $a_2 = a_1 + a_0 = 3$, $a_3 = 5, \ldots, a_{11} = 233$.

7. Svaret er $\binom{N}{n_1, n_2, \ldots, n_m} = N!/(n_1! \cdot n_2! \cdots n_m!)$ der $N = n_1 + n_2 + \cdots + n_m$.

8. Vi har at $1 \mid x$ fordi $x = x \cdot 1$ (tilsvarer $n = x$ i definisjonen). Vi har at $y = ax$ og $x = by$ og følgelig at $ab = 1$; siden a og b er heltall, må $a = b = \pm 1$ hvilkget gir $x = \pm y$. Dersom $y = nx$ og $z = my$ er $z = nmx$. Dersom $z = nxy$ kan vi skrive det om til $z = ny \cdot x$ og $z = nx \cdot y$.

9. Det eneste tall som deler 1 er 1, derfor må $\gcd(1, x) = 1$ for alle x; $x \mid 0$, derfor må $\gcd(x, 0) = x$. Dersom $x \mid y$ og $n = \gcd(x, z)$ har vi pr. definisjon at $y = mx$, $x = na$ og $z = nc$; dette gir at $y = n \cdot ma$, og følgelig at $n \mid y$. Dersom $a \mid x$ og $a \mid y$, så vil $a \mid nx + my$ for alle heltall n og m, og følgelig må $\gcd(x, y) \mid \gcd(x, y + mx)$; siden $y = (y + mx) - mx$ kan vi bruke dette den andre veien og få $\gcd(x, y + mx) \mid \gcd(x, y)$; tilsammen gir dette at $\gcd(x, y) = \gcd(x, y + mx)$.

10. Et primtall p har ingen andre faktorer enn 1 og p, så hvis $p \mid q$ så må p, pr. definisjon av q som primtall, være enten 1 eller q; siden $p \neq 1$ må altså $p = q$. Av samme grunn kan ikke $\gcd(p, x)$ ta andre verdier enn 1 eller p. Dersom vi antar at $p \not| x$ og $p \not| y$ får vi at $\gcd(p, x) = \gcd(p, y) = 1$; dette gir at $1 = ap + bx = cp + dy$ for passende heltall a, b, c, d, og videre at $bdxy = (1 - ap)(1 - cp) = 1 + (ac - a - c)p$; herav følger at $\gcd(bdxy, p) = 1$ og følgelig er ikke p en faktor i xy.

11. Vi kan uten tap av generalitet, anta at x, y og z r uten felles faktor og at x er odde. Dersom de har felles faktor kan man dele hele ligningen med denne. Da må enten x eller y være odde og kan anta at det er x. Siden y og z da ikke begge kan være oddetall og de er uten felles faktor vil $\gcd(z - y, z + y) = \gcd(z - y, 2y)$ som siden $z - y$ er odde er lik $\gcd(z - y, y) = \gcd(z, y) = 1$. .. Vi har $x^2 = (z - y)(z + y)$. Dersom p er et primtall slik at $p|x$, så vil p dele enten $z - y$ eller $z + y$ men ikke den andre. La $x = uv$ der u inneholder alle primfaktorer som deler $z + y$ og v alle primfaktorer som deler $z - y$. Da er $z - y = v^2$ og $z + y = u^2$. Herav følger at $y = (u^2 - v^2)/2$ og $z = (u^2 + v^2)/2$.

12. Dersom $x - y = an$ og $y - z = bn$ er $x - z = (a + b)n$. Dersom $x - y = an$ og $z - u = bn$ er $(x + z) - (y + u) = (a + b)n$ og $xz - yu = (by + au + abn)n$.

13. Dersom vi jobber modulo 4 blir $0^2 \equiv 2^2 \equiv 0$ og $1^2 \equiv 3^2 \equiv 1$. Et tall som er ekvivalent med 3 modulo 4 kan derfor ikke skrives som sum av to kvadrattall.

14. Ved å betrakte ligningen modulo 8 ser vi at for $n \geq 3$ må $5^m \equiv 1 \bmod 8$. Eftersom $5^2 = 25 \equiv 1 \bmod 8$ mens $5 \not\equiv 1 \bmod 8$, ser vi at dersom $n \geq 3$ er $m = 2k$. Da har vi at $2^n = 5^{2k} - 1 = (5^k + 1)(5^k - 1)$; da må vi ha at $5^k - 1 = 2^p$ og $5^k + 1 = 2^q$ der $n = p + q$.

Siden dette gir at $2^p(2^{q-p}-1) = 2^q - 2^p = 2$ må $p = 1$ og $q = 2$. Dette gir $n = p+q = 3$, men $2^n + 1 = 9$ er ingen potens av 5, så det gir ingen løsning. .. De tre tilfellene $n = 0, 1$ og 2 må testes for seg, da de ikke er dekket av utledningene ovenfor. Ved å sette inn de tre verdiene finner vi at eneste løsning er $2^2 + 1 = 5$.

15. Hvis vi ser på punktene modulo to, finnes fire punkter: svarende til om x og y er odde eller like. Altså finnes det to punkter blandt de fem slik at differansen av koordinatene (avstandsvektoren) består av partall; derfor må midtpunktet mellom de to punktene være heltallig.

16. Dette er det samme som å si at dersom $p \nmid x$ og $p \nmid y$ så må $p \nmid xy$.

17. For $q(x) = (x+1)p(x) - x$ har vi at $q(k) = 0$ for $k = 0, 1, \ldots, n$. Siden $q(x)$ er av grad $n+1$ og vi har $n+1$ kjente nullpunkter, må $q(x) = ax(x-1)(x-2)\cdots(x-n)$. For å bestemme a kan vi bruke at $q(-1) = 1$, og dermed at $a = (-1)^{n+1}/(n+1)!$. Dette gir at $q(n+1) = (-1)^{n+1}$. Ved å sette inn dette og løse for $p(n+1)$ i definisjonen av $q(n+1)$ får vi at $p(n+1) = (n+1-(-1)^n)/(n+2)$ hvilket er lik $n/(n+2)$ for n like og 1 for n odde.

18. La $p(x) = (x+x_1)\cdots(x+x_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Da er $a_{n-1} = x_1 + \cdots + x_n$ og $a_i \geq 0$ for alle i. Dette gir at $p(x) \geq x^n + a_{n-1}x^{n-1}$. Sett inn $x = 1$ og dette gir ulikheten som skulle vises.

19. Dersom $a_i = 1 + 2x_i$, $x_i \geq 0$, får vi at $(1+a_1)\cdots(1+a_n) = 2^n(1+x_i)\cdots(1+x_n)$. Vi har at $(1+x_1)\cdots(1+x_n) \geq 1 + x_1 + \cdots + x_n$ når $x_i \geq 0$. Vi har også at $1 + a_1 + \cdots + a_n = n + 1 + x_1 + \cdots + x_n$; høyresiden er da lik $2^n(1 + (x_1 + \cdots + x_n)/(n+1))$. Siden $x_i \geq 0$ er dermed ulikheten opplagt.

20. Vi kan bruke ulikheten $u^2 + v^2 \geq 2uv$ der $u = \sqrt{x}$ og $v = 1/\sqrt{x}$. Det er også mulig å sette $u = x$ og $v = 1$, få $u^2 + 1 \geq 2u$ og så dele med u på begge sider.

21. Vi har $x^2 + y^2 \geq 2xy$, $x^2 + z^2 \geq 2xz$ og $y^2 + z^2 \geq 2yz$. Summerer vi de tre ulikhetene og deler på 2 på begge sider har vi løsningen.