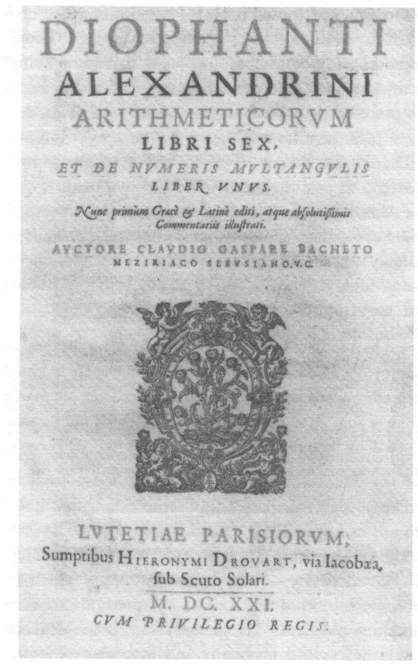
Kapittel 35

# Et løst og et par uløste matematiske problem

I dette kapitlet skal vi fortelle deg om et berømt matematisk problem som nylig ble løst etter 325 år, og om et par som fortsatt er uløste.

## Et løst problem
## Fermats siste teorem

Den berømte franske matematikeren Pierre de Fermat døde i 1665, sekstifire år gammel. Da sønnen ryddet papirene etter faren, fant han en fransk utgave fra 1621 (MDCXXI) av boka Aritmetica, som ble forfattet av grekeren Diofantos. Diofantos (ca. 250 e.Kr.) fortalte vi om i kapitlet om ligninger av første grad med én ukjent.


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 HIERONYMI DROVART, via Iacobæa, sub Scuto Solari.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

I margene i boka hadde Fermat skrevet matematiske påstander. Bevis for påstandene manglet enten helt eller var bare antydet.

I 1670 ble en ny utgave av boka til Diofantos der Fermats margnotater var tatt inn, utgitt.

Nå ble matematikere interesserte i påstandene til Fermat, og det gikk sport i å bevise eller motbevise dem. En etter en ble de bevist å være sanne. Men én påstand lot seg verken bevise eller motbevise. Det var følgende:

òCubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere.ò

som er latin og betyr:

Det er umulig å skrive en tredjepotens som summen av to tredjepotenser eller en fjerdepotens som en sum av to fjerdepotenser eller generelt, en potens av grad større enn 2 som en sum av to potenser av samme grad.

Når en matematisk påstand er bevist, kaller vi den en setning eller et teorem. Teorem kan brukes til å bevise nye påstander. Når vi utvider matematikken på denne måten, sier vi (som du fikk vite i kapitlet òInnledning til geometriò) at vi bruker den deduktive metoden.

Den ene påstanden i Fermats margnotater som en ikke klarte å bevise, og som følgelig ennå ikke var et teorem, ble likevel populært kalt òFermats siste teoremò.

Fermat hadde begynt på et bevis, men plassen i margen ble for liten, og han avsluttet med setningen:

òCuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.ò

som betyr (litt fritt oversatt):

Jeg har et i sannhet vidunderlig bevis på denne påstanden, men margen er for liten til å skrive det ut.

Vi tar med den franske versjonen av påstanden og kommentaren til beviset:

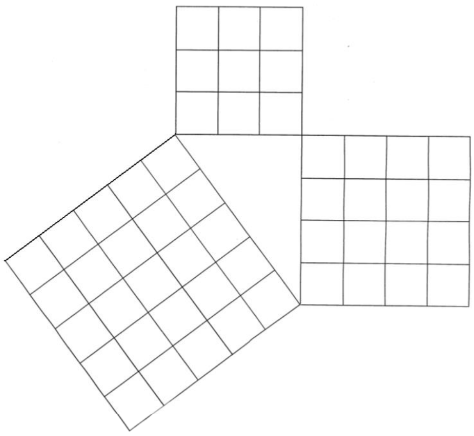
| | | |
|---|---|---|
| $x^n + y^n = z^n$ ? |  | Grand théorème *ou* Dernier théorème de Fermat<br>- *D'autre part, un cube n'est jamais somme de deux cubes, une puissance quatrième n'est jamais somme de deux puissances quatrièmes, et plus généralement aucune puissance supérieure stricte à 2 n'est somme de deux puissances analogues.*<br>- *J'ai trouvé une merveilleuse démonstration de cette proposition, mais je ne peux l'écrire dans cette marge car elle est trop longue* |

Vi skal se litt nærmere på hva Fermat har påstått, og tar utgangspunkt i Pytagorasô setning (teorem) som gjelder for en rettvinklet trekant med kateter a og b og hypotenus c:

$$\boxed{c^2 = a^2 + b^2}$$

Vi kan kalle setningen en ligning fordi den består av en venstre side, et likhetstegn og en høyre side. I denne ligningen er det mange heltallskombinasjoner som passer, for eksempel a = 3, b = 4 og c = 5. En slik heltallskombinasjon kaller vi en heltallsløsning av ligningen.

Under presenterer vi grafisk 3-4-5-løsningen og et utvalg av andre heltallsløsninger:



$$5^2 + 12^2 = 13^2$$
$$8^2 + 15^2 = 17^2$$
$$7^2 + 24^2 = 26^2$$
$$9^2 + 40^2 = 41^2$$
$$11^2 + 60^2 = 61^2$$
$$12^2 + 35^2 = 37^2$$
$$13^2 + 84^2 = 85^2$$
$$20^2 + 21^2 = 29^2$$

Fermats påstand kan vi formulere slik:

Hvis n er større enn 2, så finnes det ingen heltallsløsninger på ligningen: $\boxed{c^n = a^n + b^n}$

Fermats ry som matematiker gjorde at en trodde han når han påsto at han hadde et bevis. Dermed ble det å bevise påstanden en styrkeprøve som mange betydelige matematikere prøvde seg på. Men alle måtte gi seg, påstanden lot seg ikke bevise. Noen gav seg tidlig, mens andre brukte store deler av sitt liv på oppgaven.

En som tilhører den siste gruppen, engelskmannen Andrew Wiles som emigrerte til USA og ble professor ved Princeton University, holdt 23. juni 1993 en dramatisk forelesning som, uten at han hadde kunngjort det på forhånd, konkluderte med at Fermats påstand var bevist. 323 år etter utgivelsen av Aritmetica med Fermats margnotater var òFermats siste teoremò endelig blitt et teorem, trodde en.


Wilesô bevis, som var langt, ble nå undersøkt meget kritisk. Og en fant en overgang som ikke holdt mål. Dermed måtte beviset forkastes.

For å understreke viktigheten av å være kritisk (spesielt i matematikken, men også ellers), skal vi gi deg et eksempel på et bevis som ikke holder. Vi skal òbeviseò at 7 = 5. Dersom du ikke finner feil i beviset, er det ikke så farlig i dette tilfellet. Du godtar likevel ikke at 7 = 5. Men i andre tilfeller kan det være katastrofalt å overse en feil i et bevis. Med den deduktive metoden vil vi da bygge videre på noe vi tror er rett, men som kanskje er feil.

Vi begynner med den enkle førstegradsligningen

$$\boxed{2x = 2}$$

Vi skal ikke løse ligningen, men tøyse litt med den slik:

$$2x = 2$$

2x kan omskrives til 7x ï 5x, og 2 kan omskrives til 7 ï 5.

$$7x - 5x = 7 - 5$$

Et ledd i en ligning kan flyttes til den andre siden og skrives der med motsatt fortegn. Vi ommøblerer litt på leddene:

$$7x - 7 = 5x - 5$$

7x ï 7 kan faktoriseres til 7(x ï 1).
5x ï 5 kan faktoriseres til 5(x ï 1).

$$7(x - 1) = 5(x - 1)$$

Vi dividerer begge sidene på (x ï 1).

$$\frac{7(x-1)}{(x-1)} = \frac{5(x-1)}{(x-1)}$$

Dersom vi avslutter med å forkorte brøkene i ligningen, har vi, hvis du ikke finner den overgangen som ikke holder mål, tilsynelatende bevist at 7 = 5. For sikkerhets skyld avsanner vi det vi har òbevistò, med teksten til høyre for konklusjonen.

$7 = 5$ $\Leftarrow$ Dette er ikke korrekt

Tilbake til Andrew Wiles og hans forsøk på å bevise òFermats siste teoremò. I 1995 klarte Wiles, med hjelp fra en av hans studenter, å forbedre den overgangen som ikke holdt mål, slik at den kunne godtas. Dermed fikk han æren for å være den første som klarte å bevise òFermats siste teoremò, dvs. for å være den første som klarte å få påstanden til å bli et ekte teorem.

Og hva så? Hvilken nytteverdi har det at en eller annen bruker store deler av sitt liv til å bevise at ligningen $c^n = a^n + b^n$ ikke har heltallsløsninger når n er større enn 2?

Når noen driver grunnforskning, er det vanlig å holde spørsmålet om nytteverdi i bakgrunnen.

Resultatet av Andrew Wilesô arbeid er litt ny matematikk som han utviklet mens han arbeidet med å bevise påstanden til Fermat og den beviste påstanden.

Den beviste påstanden, dvs. teoremet, har gitt oss mer kunnskap om tallene og kan kanskje med tiden, sammen med andre teorem og den deduktive metoden, gi oss enda mer kunnskap. Det kan kanskje også den nye matematikken som Wiles utviklet. Og når teoretikerne har forsket fram ny kunnskap, bruker praktikerne å være flinke til å finne måter å bruke den nye kunnskapen på.

Et eksempel på at praktikere har funnet bruksområder for matematikk som en i utgangspunktet kanskje skulle tro bare var interessant for teoretikere, har med primtall å gjøre. Et primtall er som nevnt, blant annet i kapitlet om brøk, et tall som bare er delelig med seg selv og 1, dvs. tallene 1, 2, 3, 5, 7, 11, 13, 17, 19, 23 osv. Alle andre tall kan faktoriseres i primtallsfaktorer. For eksempel kan tallet 75 600 faktoriseres slik:

$$75\,600 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7$$

En måte å finne primtallsfaktorene på ble gjennomgått i kapitlet om brøk.

Godt kjennskap til primtallene og egenskapene til dem har gjort det mulig å kryptere data effektivt. Å kryptere data vil si å omskrive (kode) dem slik at det blir vanskelig for uvedkommende å få informasjon fra dem, samtidig som rette vedkommende lett kan omforme dem tilbake til sin opprinnelige form.

Et av de mest berømte bevisene i matematikkens historie har med primtall å gjøre. Euklid, som vi også omtaler i kapitlene òInnledning til geometriò, òGeometriò og òGlimt fra matematikkens historieò, beviste at det finnes uendelig mange primtall. Beviset til Euklid er samtidig et eksempel på en måte å bevise på som vi kaller òbevis ved selvmotsigelseò eller på latin: òreductio ad absurdumò. Denne typen bevis kalles også òindirekte bevisò.

Beviset til Euklid går slik (vi har redigert det litt):

Vi begynner med å forutsette at det bare finnes et endelig antall primtall og kaller antallet n. De n primtallene kan vi kalle $p_1$, $p_2$, $p_3$, é , $p_n$.

Vi ser på tallet q = ($p_1 \cdot p_2 \cdot p_3 \cdot$ é $\cdot p_n$) + 1

Nå skal vi vurdere to muligheter:

I q er et primtall.
II q er ikke et primtall.

I Hvis q er et primtall, så er vår forutsetning om at det bare finnes et endelig antall primtall, dvs. primtallene $p_1$, $p_2$, $p_3$, é , $p_n$, feil. Hvis den er feil, så finnes det uendelig mange primtall.

II Hvis tallet q ikke er et primtall, så må det kunne faktoriseres i primtallsfaktorer. Det er da delelig på hver av sine primtallsfaktorer. Men her passer ingen av primtallene $p_1$, $p_2$, $p_3$, é , $p_n$. Dersom vi dividerer q = ($p_1 \cdot p_2 \cdot p_3 \cdot$ é $\cdot p_n$) + 1 på ett av dem, vil vi få 1 til rest. Det må derfor finnes andre primtall enn primtallene $p_1$, $p_2$, $p_3$, é , $p_n$. Også i dette tilfellet er vår forutsetning om at det bare finnes et endelig antall primtall, dvs. primtallene $p_1$, $p_2$, $p_3$, é , $p_n$, feil. Hvis den er feil, så finnes det uendelig mange primtall.

Enten er tallet q et primtall, eller så er det ikke et primtall. Uansett om det ene eller det andre er tilfellet, har vi funnet at det må eksistere flere primtall enn de n stk. som vi forutsatte var alle. Det betyr at vår forutsetning, at det bare finnes et endelig antall primtall, er feil. Da må det finnes uendelig mange primtall.

Her slutter Euklids bevis. Matematikere bruker gjerne adjektivene elegant og vakkert om dette og lignende bevis. Kanskje var Fermats eget bevis på òFermats siste teoremò tilsvarende vakkert og elegant.

Ny matematikk i framtiden vil sikkert komme fra nye aksiom og det en kan utlede fra dem, men kanskje også fra eksisterende teorem og nye som med den deduktive metoden etableres ut fra de aksiomene og de teoremene vi allerede har. Vi avslutter med et par påstander som kanskje blir teorem en gang:

I Det finnes uendelig mange tvillingprimtall.
II Det finnes uendelig mange perfekte tall.

I Et primtall er alltid et oddetall. Ingen partall er primtall fordi alle partall er delelig på 2. Den minst mulige avstanden mellom to primtall er derfor 2. Primtall som har denne avstanden, kalles tvillingprimtall. 5 og 7 er et eksempel på tvillingprimtall. 17 og 19 er et annet. 1 000 000 000 061 og 1 000 000 000 063 er enda et. En tror at det også finnes uendelig mange tvillingprimtall, men til nå har ingen klart å bevise eller motbevise det.

II Et perfekt tall er et tall som er lik summen av sine divisorer, dvs. de tallene (inklusive tallet 1) som tallet er delelig på.

6 og 28 er perfekte tall fordi

| | | | |
|---|---|---|---|
| 1, 2 og 3 | går opp i 6 | og | 1 + 2 + 3 = 6 |
| 1, 2, 4, 7 og 14 | går opp i 28 | og | 1 + 2 + 4 + 7 + 14 = 28 |

Matematikere har gjennom tidene lett etter nye perfekte tall, men funnet få og bare partall. Fram til 1997 hadde en bare funnet tretti perfekte tall. Det største har 130 000 siffer, men kan kort skrives slik:

$2^{216\,090} \cdot (2^{216\,091}$ ï 1)

Hvorvidt det bare finnes et endelig antall perfekte tall og i tilfellet hvilke eller om det finnes uendelig mange, venter fortsatt på en avklaring. Fordi en til nå bare har funnet perfekte partall, og fordi ingen har bevist at et oddetall ikke kan være et perfekt tall, er det også uavklart om det finnes perfekte tall som er oddetall.