

Noen tallteoretiske resultater av Fermat

Arne B. Sletsjøe

Universitetet i Oslo



Pierre de Fermat
(1601/1607 - 1665)

Fermats lille teorem

Fermats rettvinklede teorem

Fermats siste teorem



Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Det er umulig å dele en tredjepotens i to tredjepotenser, eller en fjerdepotens i to fjerdepotenser, eller helt generelt, en høyere potens enn to i to ledd av samme type. Jeg har funnet et praktfullt bevis for dette, men margen er for liten til å romme det.

Fermats lille teorem

Pierre de Fermat i brev datert 18. oktober 1640 til Frénicle de Bessy:

Tout nombre premier mesure infailliblement une des puissances 1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné 1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.

Et hvert primtall deler nødvendigvis en av potensene, minus 1, in en vilkårlig progresjon $[a, a^2, a^3, \dots]$ og eksponenten i denne potensen deler det gitte primtallet -1, og, når man har funnet den første eksponenten det her er snakk om, så vil alle de andre eksponentene være multipler av den første.

Teorem (de Fermat, 1640)

Dersom p er et primtall og a et heltall, så vil $a^p - a$ være delelig med p .

Eksempler:

$$5^7 - 5 = 78\,120 = 7 \cdot 11\,160 \quad (a = 5, p = 7)$$

$$8^{11} - 8 = 8\,589\,934\,584 = 11 \cdot 780\,903\,144 \quad (a = 8, p = 11)$$

Første publiserte bevis: Euler i "Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio" fra 1736

Upublisert bevis av Leibniz (før 1683)

Betegnelsen "Fermats lille teorem" stammer fra "Zahlentheorie" av Kurt Hensel (1913).

Anvendes innen kryptering, f.eks. for sikker kommunikasjon med nettbanken.

Halskjede-beviset: Vi har perler i a forskjellige farger og lager alle mulige lenker av lengde p . Til sammen gir dette a^p lenker. Ta bort de ensfargede, i alt a , vi har igjen $a^p - a$. Vi knytter sammen hver enkelt lenke til et kjede, og samler de som er like. Siden p er et primtall vil det være p kjeder i hver bunke. Mao, $a^p - a$ er delelig med p .

Teorem (Lehmer, 1927)

Gitt et heltall p . Anta at det finnes et helt tall a slik at $a^{p-1} - 1$ er delelig med p og slik at for alle primtall q som deler $p - 1$, så er $a^{\frac{p-1}{q}} - 1$ ikke delelig med p . Da er p et primtall.

**Et nødvendig mellomspill:
PPT-teoremet (Primitive Pythagoreiske Tripler)**

Teorem (Euklid)

Et hvert primitivt Pythagoreisk trippel $x^2 + y^2 = z^2$ kan skrives på formen

$$x = p^2 - q^2 \quad y = 2pq \quad z = p^2 + q^2$$

der p og q er innbyrdes primiske positive heltall.

Eksempler:

$$3^2 + 4^2 = 5^2, \quad p = 2, \quad q = 1$$

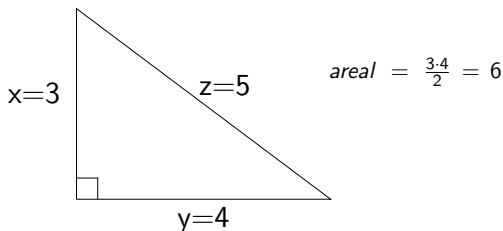
$$5^2 + 12^2 = 13^2. \quad p = 3, \quad q = 2$$

Fermats rettvinklede teorem

Teorem (de Fermat, ca. 1640)

Det finnes ingen rasjonale rettvinklede trekanter med areal lik et kvadrattall.

En **rasjonal** rettvinklet trekant er en rettvinklet trekant der alle sidelengdene er rasjonale tall. Ved å multiplisere med fellesnevneren kan vi anta at alle sidekantene er heltallige.



Arealet av en heltallig rettvinklet trekant kalles et **kongruens-tall**.

Bevis-ide: Anta at det finnes heltallige rettvinklede trekanter med kvadratisk areal. Velg trekanten med minst areal. Fermat viser at ved å bruke PPT-teoremet, så kan vi finne en heltallig rettvinklet trekant med ekte mindre (kvadratisk) areal. Dette gir oss en motsigelse. Bevis-metoden kalles **uendelig nedstiging** og baserer seg på at det finnes et minste positivt heltall (nemlig 1).

Ekvivalente påstander til Fermats rettvinklede trekant-formulering (FRT):

Fibonaccis Kongruum-påstand (FK): Dersom tre kvadrater danner en aritmetisk progresjon, så kan ikke avstanden mellom tallene selv være et kvadrat.

Dette ble formulert av Fibonacci i 1225, uten bevis. Fibonacci kaller denne avstanden for et **kongruum**.

De første kongruane er 24, 96, 120, 216, 240, 336, 384, 480, 600, 720.

2PT: Det finnes ikke to Pythagoreiske tripler slik at de to katetene i det ene tilsvarer kateten og hypotenusen i det andre.

(*): Likningen $x^4 - y^4 = z^2$ har ingen heltallige løsninger.

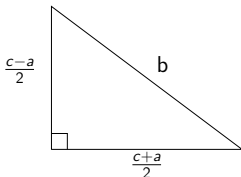
En umiddelbar konsekvens av den siste påstanden er at Fermats siste teorem er sant for eksponenten $n = 4$.

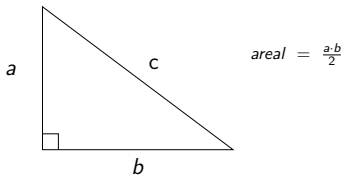
FRT $\Rightarrow$ FK: La a^2 , b^2 , c^2 være en aritmetisk progresjon med kongruum $K = b^2 - a^2 = c^2 - b^2 = \frac{c^2 - a^2}{2}$. Det gir oss et Pythagoreisk trippel:

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

hvor arealet av den tilhørende trekanten er

$$\frac{1}{2} \left(\frac{c+a}{2}\right) \cdot \left(\frac{c-a}{2}\right) = \frac{c^2 - a^2}{8} = \frac{1}{4} \cdot K$$





FK $\Rightarrow$ FRT: Anta $\frac{ab}{2} = d^2$. Det gir

$$(2d)^2 = 4d^2 = 2ab = \frac{(a+b)^2 - (a-b)^2}{2}$$

Det gir oss en aritmetisk progresjon

$$(a-b)^2, \quad (a-b)^2 + (2d)^2 = a^2 - 2ab + b^2 + 2ab = c^2, \quad (a+b)^2$$

FK $\Leftrightarrow$ 2PT: Vi har at

$$a^2 + d^2 = b^2 \quad \text{og} \quad b^2 + d^2 = c^2$$

danner en aritmetisk progresjon a^2, b^2, c^2 med kongruum $K = d^2$.

(*) $\Rightarrow$ FK: Dersom det finnes a, b, c, d slik at

$$a^2 + d^2 = b^2 \quad \text{og} \quad b^2 + d^2 = c^2$$

så vil

$$b^4 - d^4 = (b^2 - d^2)(b^2 + d^2) = a^2 c^2 = (ac)^2$$

FK $\Rightarrow$ (*): Dersom x, y, z uten felles faktor er en løsning av $x^4 - y^4 = z^2$, så vil heller ikke $x^2 + y^2$ og $x^2 - y^2$ ha noen felles faktor, annet enn muligens 2 (i dette tilfelle må argumentet modifiseres noe). Vi har

$$x^4 - y^4 = (x^2 - y^2)(x^2 + y^2) = z^2$$

Hvis $x^2 - y^2$ og $x^2 + y^2$ ikke har felles faktorer (og produktet er et kvadrat) må begge være kvadrater, som motsier FK.

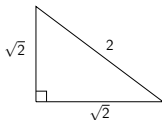
Kongruens-tall-problemet: Finn en generell måte for å avgjøre om et tall er et kongruens-tall.

Kongruens-tall: 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, ...

Teorem

$\sqrt{2}$ er et irrasjonalt tall.

Bevis. Anta $\sqrt{2}$ er et rasjonalt tall. Da er trekanten



en rasjonal rettvinklet trekant med areal $\frac{1}{2}\sqrt{2}\sqrt{2} = 1$ som er et kvadrattall. Umulig.

Fermats siste teorem



Sir Andrew Wiles
(1954-)

Teorem (Wiles, 1993-95)

Likningen

$$x^n + y^n = z^n$$

*har ingen ikke-trivielle
heltalls-løsninger for $n > 2$.*

Teorem (de Fermat, ca. 1640)

FLT er sann for $n = 4$.

Bevis-ide: Anta at det finnes Fermat-tripler for $n = 4$. Velg triplet med minst z -verdi. Fermat viser at ved å bruke PPT-teoremet, så kan vi finne et nytt Fermat-trippel med ekte mindre z -verdi. Dette gir oss en motsigelse. (Uendelig nedstiging)

Teorem (Euler, 1772)

Dersom $a^2 + 3b^2 = z^3$, hvor a og b er innbyrdes primiske, så er a , b og z på formen

$$a = p^3 - 9pq^2 \quad b = 3p^2q - 3q^3 \quad z = p^2 + 3q^2$$

der p og q er innbyrdes primiske positive heltall.

Nødvendig betingelse:

$$\begin{aligned}(p^3 - 9pq^2)^2 + 3(3p^2q - 3q^3)^2 \\&= p^6 - 18p^4q^2 + 81p^2q^4 + 27p^4q^2 - 54p^2q^4 + 27q^6 \\&= p^6 + 9p^4q^2 + 27p^2q^4 + 27q^6 = (p^2 + 3q^2)^3\end{aligned}$$

Teorem (Euler, 1772)

FLT er sann for $n = 3$.

Bevis-ide: Anta at det finnes Fermat-trippel $x^3 + y^3 = z^3$, hvor x og y er oddetall. Vi kan da skrive $x + y = 2p$ og $x - y = 2q$, som gir $x = p + q$ og $y = p - q$, hvor p og q ikke har noen felles faktor. Anta at dette er triplet med minst z -verdi. Vi har

$$z^3 = x^3 + y^3 = (p + q)^3 + (p - q)^3 = 2p(p^2 + 3q^2)$$

Ved å bruke forrige resultat viser Euler at vi kan finne et nytt Fermat-trippel med ekte mindre z -verdi. Dette gir oss en motsigelse. (Uendelig nedstiging)



Niels Henrik Abel
(1802 - 1827)

Foruden at jeg læser arbeider jeg ogsaa selv. Saaledes har jeg søgt at bevise Umuligheden af Ligningen $a^n = b^n + c^n$ i hele Tal naar n er større end 2; men jeg har jeg været hældet. Jeg har ikke kommet videre end til indlagte Theoremer, som ere snorrige nok.

Teorem (Abel, 1823)

Ligningen

$$a^n = b^n + c^n$$

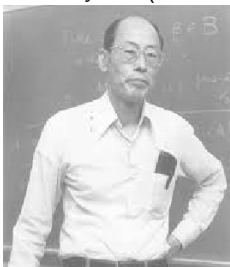
hvor n er et Primtal er umuelig naar een eller flere af Størrelserne:

$$a, b, c, a + b, a + c, b - c, \sqrt[n]{a}, \sqrt[n]{b}, \sqrt[n]{c}$$

ere Primtal.



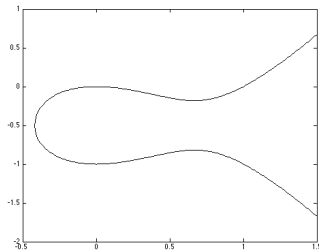
Yutaka Taniyama (1927-1958)



Goro Shimura (1928-)

Formodning (Taniyama-Shimura, 1955-57)

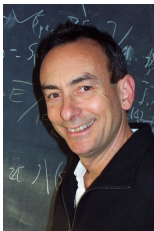
Elliptiske kurver er modulære.



$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 + y = x^3 - x^2\}$$



Gerhard Frey (1944-)



Ken Ribet (1948-)

En løsning

$$a^n + b^n = c^n$$

av Fermats likning gir opphav til
en elliptisk kurve

$$y^2 = x(x - a^n)(x + b^n)$$

(Frey-kurven)

Teorem (Ribet, 1986)

Frey-kurven er ikke modulær.

- En tenkt løsning av Fermats likning gir opphav til en elliptisk kurve, Frey-kurven
- Frey-kurven er ikke modulær
- Alle elliptiske kurver er modulære

Formodning (de Fermat, 1637)

Likningen

$$x^n + y^n = z^n$$

har ingen ikke-trivielle heltalls-løsninger for $n > 2$.

- En tenkt løsning av Fermats likning gir opphav til en elliptisk kurve, Frey-kurven
- Frey-kurven er ikke modulær
- Alle elliptiske kurver er modulære

Teorem (Frey, Ribet, Taylor, Wiles, 1993-95)

Likningen

$$x^n + y^n = z^n$$

har ingen ikke-trivielle heltalls-løsninger for $n > 2$.