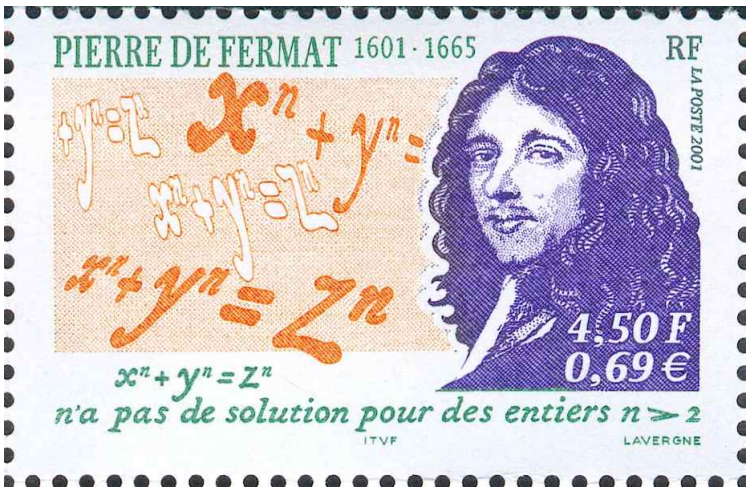
PIERRE DE FERMAT - amatör och innovatör

Anders Tengstrand



Här kommer en ny text om matematik som ger min gammelmanstillvaro ökat innehåll. De två tidigare *Fyra fundamentala teorem* och *Några prydnadsstenar i klassisk geometri* får sällskap med en tredje, *Pierre de Fermat, amatör och innovatör*. De flesta som känner till Fermat gör det nog för det som kallas Fermats gåta eller Fermats förmodan eller Fermats stora sats. Kärt barn har många namn. Hans påstående att ekvationen $x^n + y^n = z^n$ saknar positiva heltalslösningar om heltalet $n \geq 3$ formulerades på 1630-talet och han trodde själv att han hade bevisat det. Men något bevis har man inte hittat bland hans efterlämnade papper. Många av de främsta matematikerna har under sekler försökt visa förmodan men bara klarat av det för vissa heltal n t.ex. $n = 3$. Problemet har också lockat många matematiskt intresserade amatörer att pröva sina krafter. Det kan ju förstås utan en avancerad matematisk terminologi. Det blev till slut en engelsk matematiker Andrew Wiles som år 1995 med avancerade algebraiska metoder visade påståendet. Han blev fascinerad av problemet redan som barn och lyckades alltså till slut lösa det.

Pierre de Fermat var själv en amatör som matematiker. Han var till yrket jurist och domare och ägnade sig åt matematiken på sin fritid. Han levde, som det verkar, ett stilla liv i Toulouse som med den tidens samfärdsmedel var långt från Paris - ett centrum för den tidens matematiker. Hans publikationer är mycket få och han meddelade sina resultat genom brev till kollegor. Trots det var han den tidens största talteoretiker och han bidrog med banbrytande arbeten som förebådade differential- och integralkalkylen. Hans brevväxling med den tjugo år yngre Blaise Pascal betraktas som sannolikhetslärans födelse. En av prydnadsstenarna i den andra av mina texter kallas Fermats punkt. Kanske ett mindre bidrag i jämförelse med de övriga jag nämnt men det visar på hans allsidighet och hans förmåga att se och formulera matematiska samband.

Den här texten har jag precis som de två föregående skrivit för min egen skull. Men målsättningen har varit att lägga ut den på nätet så att andra ska kunna ta del av den. Det skärper sinnet och det kan vara viktigt i min ålder. Men till en eventuell läsare skickar jag med samma råd som förut. Läs så mycket ni har lust och ork och hoppa över om det blir för tekniskt. Det är inte frågan om någon kurslitteratur och kommer inte upp på någon tenta.

Växjö 23 april 2026
Anders Tengstrand

Pierre de Fermat - juristen som skapade banbrytande matematik på sin fritid

Vad stort sker det sker tyst
Ur Odalbonden av Erik Gustav Geijer (1783-1847)

Pierrre Fermat föddes kanske 1601 och dog med säkerhet 1665. Det finns tveksamhet om hans födelseår. Hans ett år äldre bror dog vid späd ålder och fick också namnet Pierre och man är inte säker på vems fördelseår det egentligen gäller. Att han dog 1665 är däremot säkert men han dödförklarades redan 1653 under den pest som drabbade regionen. Fermat fick själv tillkännage att ”ryktet om hans död var överdrivet”.

Figur 1: Pierre de Fermat på äldre dar

Fermats födelseort är Beaumont-de-Lomagne i södra Frankrike drygt sex mil nordväst om Toulouse. Hans far var en välbärgad köpman och han fick sin grundläggande utbildning vid en klosterskola. Därefter läste han något år vid universitetet i Touluse innan han nitton år gammal flyttade till Bordeaux. Där

studerade han matematik och intresserade sig för Apollonius verk om kägelsnitt. Han kom i kontakt med andra matematikintresserade och hans arbete genererade viktiga resultat om maxima och minima. Från Bordeaux flyttade Fermat så småningom till Orleans där han avlade examen i juridik. År 1631 anställdes han som jurist i Toulouse och där blev han kvar livet ut. Fermat var alltså jurist till yrket och matematik blev en fritidssysselsättning. Man brukar kalla honom för världens främste amatörmatematiker. Som domare kunde han nu ändra sitt namn till Pierre de Fermat.

Under första halvan av 1600-talet var den franske munken Marin Mersenne (1588-1648) en ledande gestalt inom matematik och fysik. Förutom att han bidrog med viktiga resultat inom området hade han en omfattande kontaktnät med den tidens forskare. I det ingick bl.a. Etienne Pascal (1588-1651) och han son Blaise (1623-62), René Descartes (1596-1650), Giles de Roberval (1602-75), Evangelista Torricelli (1608-47) och Christian Huygens (1629-95). Han kommunicerade med brev och ordnade konferenser och blev ett nav i diskussioner kring vetenskapliga problem. Verksamheten kom att kallas Académie Parisienne eller Académie Mersenne. När ryktet om Fermats matematiska upptäckter nådde honom bad han Fermat att delta i verksamheten. Fermat skickade 1638 in tre arbeten som Mersenne sedan vidarebefordrade till medlemmarna i kontaktnätet. Ett av bidragen hade titeln *Metod för att bestämma maxima och minima och tangenter till kurvor*. Det bidraget kritiserades hårt av Descartes som såg en konkurrent inom ett område där han ansåg sig vara den självklara mästaren nämligen analytiskt geometri. Descartes var som person självmedveten, högdragen och arrogant och Fermat var hans motsats. Fermat svarade emellertid med att ge kritiska synpunkter på delar av Descartes arbete inom optik, *La Dioptrique*.

Under perioden 1643-54 hade inte Fermat kontakt med Académie Mersenne. Det kan ha flera orsaker. Arbetet som domare krävde mycket av hans tid och det inkräktade på hans matematiska verksamhet. Under perioden drabbades regionen av en svår pest och Fermat blev felaktigt dödförklarad. Dessutom skakades regionen av ett inbördeskrig.

Det var under denna period som Fermat började intressera sig för talteori. Senare försökte han få de andra matematikerna i Mersennes kontaktnät att engagera sig i talteoretiska problemställningar. Bortsett från Mersenne själv, som bidragit med resultat om primtal, var intresset lågt och ämnesområdet var för de flesta matematiker inte prioriterat.

År 1654 tog Blaise Pascal kontakt med Fermat för att diskutera ett problem inom hasardspel. Det var början till en brevväxling som brukar betraktas som sannolikhetslärans födelse. Korrespondensen är bevarad och finns på nätet. Man slås av skillnaden mellan Pascals fantasifulla

och ibland snåriga resonemang och Fermats distinkta och klara framställning. Trots olikheterna i temperament är de noga med att betyga den respekt de har för varandra. Till slut kunde de enas om ett rimligt sätt att bestämma vad vi idag kallar sannolikheter. Fermat fortsatte att diskutera sannolikhetsbegreppet med Huygens som 1657 publicerade en grundläggande skrift inom sannolikhetsläran.

Fermat intresserade sig också för frågeställningar inom optik där han härledde ljusets brytning vid övergången mellan olika media om man utgår från att ljuset tar den snabbaste vägen. Han intresserade sig även för klassisk geometri. I en tidigare text i denna serie har jag behandlat upptäckten av vad som kallas Fermatpunkten.

Det finns inte så många tryckta verk av Fermat. De flesta av hans resultat är bevarade genom brev till kollegor. Många gånger saknades bevis och om de fanns var de ofta ofullständiga. Det var kanske hans arbete som hög tjänsteman som gjorde att han inte fick tid att utarbeta manuskript som skulle publiceras. Kanske låg det också i hans natur. I en biografi om honom av M.S. Mahoney karakteriseras han på följande sätt: ”Hemlighetsfull och tystlåten tyckte han inte om att tala om sig själv och var ovillig att avslöja alltför mycket om hur han tänkte.”[1]Det ska tilläggas att han sällan råkade i konflikt med sina kollegor även om de hade olika åsikter. Han var alltid respektfull i de diskussioner han förde med olika matematiker med undantag av den dispyt han hade med Descartes om hans verk om maxima och minima.

Fermat dog 1665 i Castre, en liten by sju mil öster om Toulouse. Hans samlade verk gavs ut 1678. Han har fått en månkrater uppkallad efter sig.

Vi ska i det följande ta upp några av Fermats arbeten om talteori, hans banbrytande verk om maxima och minima samt hans brevväxling med Pascal om problem inom hasardspel.

[1] M S Mahoney, *The mathematical career of Pierre de Fermat,* Princeton University Press, 1994.

Fermats stora sats

Det viktiga med ett problem är inte dess lösning
utan den styrka vi får genom att hitta lösningen.
Virginia Satir (1916-88)

> Att dela upp en kub i två andra kuber, en fjärdepotens eller allmänt varje potens större än två i två potenser av samma ordning är omöjligt och jag ha hittat ett underbart bevis av det, men marginalen är för liten för att rymma det,

De orden skrev Fermat ner när han studerade en av Diofantos skrifter och med det formulerade han den hypotes som skulle bli känd som Fermats stora sats eller Fermats förmodan. Ingen kan i Fermats efterlämnade skrifter kunnat hitta det ”underbara bevis” som han skriver om och med största säkerhet var det antingen felaktigt eller ofullständigt. Vi skriver om satsen med moderna beräkningar.

> Det finns inga naturliga tal x, y och z sådana att
>
> $$x^n + y^n = z^n$$
>
> om $n \geq 3$.

Många av de främsta matematikerna har arbetat med problemet men misslyckats. Leonard Euler (1707-83) lyckades visa påståendet för $n = 3$ men det dröjde ända till 1995 då den engelske matematikern Andrew Wiles (1953–) kunde konstruera ett bevis och det publicerades i tidskriften *Annals of Mathematics*. Artikeln har titeln *Modular elliptic curves*

and Fermat's Last Teorem och är på åtta sidor. Beviset är komplicerat och använder sig av djupa resultat inom abstrakt algebra. Det är inte orimligt att tänka sig att några av de abstrakta begrepp och de teorier som Wiles stöder sig på har utvecklats under försöken att bevisa Fermats stora sats för att sedan bli effektiva verktyg för specialister inom modern algebra i andra sammanhang. Ett slumpvis valt citat ur artikeln visar på djupet av de algebraiska kunskaper som krävs för att förstå Wiles bevis.

> ... Whith these hypothesis there are unique local $R_D \rightarrow O$ homeomorphisms of O-algebras which takes the universal deformation to (there class of) $\rho_{t.\lambda}$ ...

Själv är jag inte tillräckligt förtrogen med abstrakt algebra för att förstå artikeln. Långt ifrån. Men jag är inte ensam. En tid efter det att beviset hade publicerats besökte jag biblioteket på Matematiska institutionen i Lund och råkade stöta på Lars Hörmander - en av världens främsta experterna inom teorin för diffentialekvationer. [2] Han visade mig en bunt papper och sade: "Jag har skrivit ut Wiles bevis men jag har inga förhoppningar om att förstå det." Matematiken har alltså blivit så specialiserad att det finns mycket få i världen som har kunnat läsa igenom Wiles bevis och intygat att det är korrekt. Wiles hade faktiskt en tidigare version där man hittade stora luckor i bevisföringen. Han lyckades till slut täppa till dem men var ett tag nära att ge upp. För sin prestation belönades Andrew Wiles med en summa pengar som långt tidigare avsatts till den som löste problemet. Han blev också adlad och kan nu kalla sig sir Andrew Wiles.[3]

Det problem som Fermat ställde fick alltså sin lösning men först efter 350 år. De metoder och begrepp som krävdes låg på en mycket hög abstraktionsnivå och var naturligtvis helt främmande för den tiden. Fermat själv var föregångare i många avseenden och han var en av de första som använde den då nya algebran som innebar att man kunde räkna med obekanta storheter. Det är den algebra vi idag lär ut i grundskolan. Det finns naturligtvis inga möjligheter att det bevis Fermat syftar på i sin marginalanteckning skulle ha klarat de krav som ställs på ett matematiskt bevis.

Fermat hade alltså med intill visshet gränsande sannolikhet inte bevisat den hypotes som han ställt. Men han hade formulerat den och det har utmanat matematiker av alla kategorier att försöka hitta en lösning. Det har bidragit till att många människor har fördjupat sitt intresse för

[2] Lars Hörmander (1931-1012) var då professor vid Lunds universitet. Han är den ende svensk som tilldelats den prestigefyllda Fieldsmedaljen som delas ut vart fjärde år av International Mathematical Union.

[3] En ingående beskrivning av Wiles arbete med problemet finns i Simon Singhs bok *Fermats gåta*, Norstedts förlag. 1998.

matematik. Då också flera av de stora matematikerna antog utmaningen kom också matematiken som ämne att utvecklas.

Vad kan det då ha varit som kom Fermat att formulera sin stora sats? Det var ju i Diofantos arbeten från ungefär 250 e.Kr. som han skrev ner den i marginalen. Diofantos studerade pythagoreiska tal d.v.s. naturliga tal x, y och z som uppfyller $x^2 + y^2 = z^2$. Låt oss därför studera dem litet närmare.

Pythagoreiska tal

Diofantos var verksam i Alexandria omkring 250 e.Kr. Han stora verk är *Arithmetica* som omfattade tretton böcker varav sex är bevarade. Det är en samling av lösta problem som ofta leder fram till ekvationer. Diofantos bröt mot den tradition i antiken där matematiken kläddes i en geometrisk språkdräkt. Han arbetade med tal och området var aritmetik. De flesta problemen leder fram till ekvationer som oftast har många lösningar. Den typen av ekvationer kallas därför idag för diofantiska. De bevarade böckerna har översatts av den brittiske matematikhistorikern T.L.Heath (1861-1940) som också gett problemen och lösningarna en modern form som gör att de lättare kan förstås av dagens läsare.

Speciellt berömt är problem nr 8 i den andra boken som lyder på följande sätt

Att skriva ett kvadrattal som summan av två kvadrattal.

Det måste ha varit här som Fermat gjorde sin berömda marginalanteckning. Vi ska inte gå in på Diofantos sätt att lösa problemet. Han arbetar med konkreta tal och hans metoder kan verka egendomliga för dagens matematikintresserade. Vi ska med hjälp av den algebra, som vi har lärt oss i skolan och som Diofantos inte kände till, ge en lösning till problemet.

Problemet är att beskriva alla pythagoreiska tal d.v.s. alla positiva heltalslösningar till ekvationen

$$x^2 + y^2 = z^2.$$

Vi bekantar oss först med problemet genom ett antal exempel. De flesta av oss är känner till att $x = 3, y = 4$ och $z = 5$ är en lösning till ekvationen. Andra lösningar är $x = 5, y = 12$ och $z = 13$ samt $x = 15, y = 8$ och $z = 17$. Vi kommer i fortsättningen ofta kalla lösningarna för pythagoreiska tripplar. Det verkar finnas många men det är inte lätt att hitta dem. Vi ska nu härleda ett sätt att beskriva tripplarna som gör detta enkelt. Härledningen görs i ett antal steg där algebraiska räkningar blandas med resonemang om delbarhet.

1. Vi observerar först att om x, y och z löser problemet så gör också kx, ky och kz där k är ett positivt heltal . Vi söker därför i första hand de lösningar där x, y och z saknar gemensamma delare som är större än 1 d.v.s. $\gcd(x, y, z) = 1$.[4] Eftersom $z^2 = x^2 + y^2$ så är en gemensam delare till två av talen x, y och z också delare till det tredje och vi kan utgå från att

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1.$$

2. De tre talen x, y och z kan inte alla vara jämna då $gcd(x, y, z) = 1$. Om två tal är jämna så är det tredje också jämnt. Alltså måste två av talen vara udda och då är det tredje jämnt.
   Vi skriver $x = 2s + 1, y = 2t + 1$ och $z = 2u$ där s, t och u är positiva heltal och får att

   $$x^2 + y^2 = 4s^2 + 4s + 1 + 4t^2 + 4t + 1 = 2(2s^2 + 2s + 2t^2 + 2t + 1)$$

   som är ett jämnt tal men det är inte delbart med 4 (talet i den sista parentesen är ju udda) vilket däremot $z^2 = 4u^2$ är. Alltså kan inte både x och y vara udda.
   Den enda möjligheten är då att det ena av talen x och y är udda och det andra jämnt medan z är udda. Vi antar i fortsättningen att x är udda, y är jämnt och z är udda.

3. Vi använder konjugatregeln och får

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

   som medför att

   $$\frac{y}{z + x} = \frac{z - x}{y}.$$

   Vi sätter

   $$\frac{z - x}{y} = \frac{z}{y} - \frac{x}{y} = \frac{m}{n}$$

   där m och n är naturliga tal och vi antar att vi förkortat bråket m/n så mycket som möjligt d.v.s. att $gcd(m, n) = 1$. Då är

   $$\frac{z + x}{y} = \frac{z}{y} + \frac{x}{y} = \frac{n}{m}.$$

   Kombinerar vi nu de båda likheterna får vi att

   $$\frac{z}{y} = \frac{1}{2}(\frac{m}{n} + \frac{n}{m}) \text{ och } \frac{x}{y} = \frac{1}{2}(\frac{m}{n} - \frac{n}{m})$$

[4] gcd står för greatest common divisor

eller

$$\frac{z}{y} = \frac{m^2+n^2}{2mn} \text{ och } \frac{x}{y} = \frac{m^2-n^2}{2mn}.$$

Vi observerar att $m > n$ och vill nu kunna sluta oss till att

$$x = m^2 - n^2, y = 2mn \text{ och } z = m^2 + n^2$$

men för att kunna göra det måste vi visa att

$$\gcd(m^2 - n^2, 2mn) = \gcd(m^2 + n^2, 2mn) = 1.$$

4. Vi visar först att av talen m och n är det ena jämnt och det andra udda.
   Båda kan uppenbarligen inte vara jämna eftersom $\gcd(m, n) = 1$.
   Båda kan inte vara udda ty i så fall vore $z = m^2 + n^2$ jämnt.
   Den enda återstående möjligheten är att ett av talen m och n är jämnt och det andra är udda.

5. Vi visar nu att

   $$\gcd(m^2 - n^2, 2mn) = \gcd(m^2 + n^2, 2mn) = 1$$

   Antag att $d > 1$ är en delare till mn. Eftersom $\gcd(m, n) = 1$ så är d delare till endera m eller n t.ex. m. Då delar d talet m^2 men inte n^2 och därför inte heller $m^2 + n^2$. Alltså är $\gcd(m^2 + n^2, mn) = 1$. Vidare är 2 inte en delare till $m^2 + n^2$. Alltså har vi att visat att $gcd(m^2+n^2, 2mn) = 1$. På samma sätt visas att $\gcd(m^2-n^2, 2mn)$ $=1$.

6. Vi kan nu dra slutsatsen att pythagoreiska triplar (x, y, z) där $\gcd(x, y, z) = 1$ kan skrivas

   $$x = m^2 - n^2, y = 2mn \text{ och } z = m^2 + n^2.$$

   Om x, y och z är pythagoreiska tal kan de alltså skrivas

   $$x = k(m^2 - n^2), y = 2kmn \text{ och } z = k(m^2 + n^2)$$

   där k, m och n är naturliga tal och $m > n$.

7. Vi har visat att pythagoreiska tal x, y och z kan skrivas på ovanstående form. Att varje taltrippel som är av den formen verkligen är pythagoreisk följer av identiteten

   $$k^2(m^2 - n^2)^2 + 4k^2m^2n^2 = k^2(m^2 + n^2)^2.$$

De positiva heltalslösningarna till den diofatiska ekvationen

$$x^2 + y^2 = z^2$$

kan alltså skrivas

$$x = k(m^2 - n^2), y = 2kmn \text{ och } z = k(m^2 + n^2)$$

där k, m och n är godtycklig heltal med $m > n$.

Om vi sätter $k = 1, m = 2$ och $n = 1$ får vi $(x, y, z) = (3, 4, 5)$ och $k = 1, m = 3$ och $n = 2$ ger $(x, y, z) = (5, 12, 13)$. Dessa pythagoreiska trippler har nog de flesta stött på. För $k = 1, m = 8$ och $n = 5$ får vi $(x, y, z) = (39, 80, 89)$ och alltså är

$$39^2 + 80^2 = 89^2$$

för att ta ett exempel som de flesta nog inte känner till.

Diofantos, som formulerade problemet, kände inte till den allmänna lösning och det gjorde förmodligen inte heller Fermat som studerade det 1 400 år senare. Fermat generaliserade det till ett annat mycket svårare problem, som löstes först efter 350 år av Andrew Wiles.

Fermats lilla sats

Man vet aldrig när ett snöre kan komma till användning.
Medan man tänker på det kan man sätta sig ner och vila lite.
Ur Nalle Puh av A.A.Milne

Talteorin var ett av Fermats stora intressen. Hans entusiasm delades emellertid inte av den tidens matematiker. De prioriterade andra områden. Många intresserade sig för problem och metoder som senare skulle leda till differential- och integralkalkylen eller kalkylen som området kom att kallas. Den nya algebran som utvecklats av Francias Viète (1540-63) och Descartes öppnade nya möjligheter. Men för talteori var intresset lågt utom för Fermat. Han studerade primtal ur olika synvinklar. Talen i serien

$$2^{2^n}+1$$

där $n = 1, 2, 3, \ldots$ kallas nu fermatska. De fyra första talen är 5, 17, 257 och 65 5337 och de är alla primtal och Fermat antog att alla talen i följden var det. Hans hypotes var emellertid felaktig. Euler visade 1732 att

$$2^{2^5}+1 = \ 4\ 294\ 967\ 297 = 641 \cdot \ 6\ 700\ 417$$

- en imponerande prestation i en tid utan mekaniska eller digitala hjälpmedel för att utföra de vanliga räkneoperationerna. Man har faktiskt inte hittat några fler fermatska primtal än de fyra första.

Fermat frågade sig också vilka primtal som kunde skrivas som en summa av två kvadrater. Han kom fram till att om $p > 2$ så är

$$p = x^2 + y^2,$$

där x och y är naturliga tal, ett primtal då och endast då $p = 4k + 1$ där k är ett naturligt tal. Fermat gav ett bevis för det men i beviset fanns oklarheter och det fyllde knappast de krav man ställer på ett matematiskt bevis. Euler kunde senare råda bot på det.

Talteorin var alltså ett stort intresse hos Fermat. Han undersökte de naturliga talen som kanske är de viktigaste grundstenarna i matematiken. Han hittade mönster och ställde frågor och i en del fall bevisade han sina påståenden, men bevisen var ofta ofullständiga. Matematiker i senare generationer som Euler och Carl Friedrich Gauss (1777-1855) såg storheten i hans arbete, kunde konstruera hållbara bevis och ibland göra generaliseringar. Man kan fråga sig vad man hade för nytta av resultaten. Utanför matematiken var det svårt att hitta exempel. Talteorin var en konstart för sig och Gauss kallade den för matematikens drottning. En av Fermats upptäckter skulle emellertid långt senare - mot slutet av 1900-talet - vara ett viktigt verktyg inom informationsteknologin. Det är den som kallas Fermats lilla sats och den säger följande:

> Om p är ett primtal så är $a^p - a$ delbart med p för varje heltal a.

Vi ger några exempel. Om $p = 3$ så är

$$2^3 - 2 = 3 \cdot 2, 3^3 - 3 = 3 \cdot 8, 4^3 - 4 = 3 \cdot 20, 5^3 - 5 = 3 \cdot 40 \ldots$$

och om $p = 5$ så har vi

$$2^5 - 2 = 5 \cdot 6, 3^5 - 3 = 5 \cdot 48, 4^5 - 4 = 5 \cdot 204, 5^5 - 5 = 5 \cdot 624 \ldots$$

Talen blir större och större och det blir allt svårare att utföra beräkningarna åtminstone om man måste räkna för hand. Fermat såg mönstret men formulerade inte något bevis. Det blev Gottfried Wilhelm von Leibniz (1646-1716) som bevisade Fermats lillas sats ett halvsekel senare och efter ytterligare några decennier skulle Euler göra en generalisering. Vi ska ge två bevis, ett induktionsbevis och ett bevis som utgår från det bevis som Gauss ger i sitt stora verk *Disquisitionis Aritmeticae* eller på svenska *Aritmetiska undersökningar* från 1801.

Ett induktionsbevis

Fermats lilla sats säger att om p är ett primtal så är $a^p - a$ delbart p för alla heltal a.
Vi konstaterar först att om $p = 2$ så är $a^2 - a = a(a - 1)$ delbart med 2 eftersom ett av talen a och $a - 1$ är jämnt. Vi förutsätter därför i

fortsättningen att primtalet $p \geq 3$.
Vidare räcker det att visa påståendet för $a \geq 0$. Om $b = -a$ där $a > 0$ så är $b^p - b = -(a^p - a)$ eftersom p är udda och om p är en delare till $a^p - a$ så är p också en delare till $b^p - b$.

Uppenbarligen gäller påståendet för $a = 0$ och $a = 1$ eftersom då är $a^p - a = 0$.
Antag nu att påståendet är sant för $a \geq 1$ d.v.s. att $a^p - a$ är delbart med p och visa att då måste också $(a+1)^p - (a+1)$ vara delbart med p. Binomialteoremet ger

$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \cdots + \binom{p}{k}a^k + \ldots + \binom{p}{1}a + 1.$$

Binomialkoefficienterna

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

där $1 \leq k \leq p-1$ naturliga tal. De är också delbara med p ty

$$p! = k!(p-k)!\binom{p}{k}$$

och p delar uppenbarligen vänsterledet och därmed också högerledet. Men primtalet p är inte delare till någon av faktorerna i $k!$ och $(p-k)!$ eftersom de alla är mindre än p. Alltså måste p vara en delare till $\binom{p}{k}$. Alla termer i binomialutvecklingen utom den första och den sista är alltså delbara med p och vi har att

$$(a+1)^p = a^p + n \cdot p + 1$$

för något heltal n. Då är

$$(a+1)^p - (a+1) = a^p + np + 1 - (a+1) = (a^p - a) + np$$

som är delbart med p eftersom $a^p - a$ är det enligt induktionsantagandet. Fermats lilla sats är härmed bevisad.

Bevis i Gauss anda

I sitt stora verk *Aritmetiska undersökningar* från 1801 ger Gauss talteorin en logisk struktur. Många kända resultat från antiken och framåt fogade han in i ett system som påminner om Euklides *Elementa*. Här

finns resultat från antiken och från Fermat, Leibniz, Euler, Joseph-Louis Lagrange (1736-1813) m.fl. Gauss bidrog också med nytt material. Alla satser är bevisade och stilen är klar och enkel. De grundläggande delarna är en förebild för dagens läroböcker i talteori. En av mina elever hade fått i uppgift att gå igenom delar av *Aritmetiska undersökningar* och sade vid redovisningen· ”Varför skriver man egentligen nya böcker i grundläggande talteori. Gauss framställning är ju oöverträffad.”

Moduloräkning

Gauss inför modulobegreppet och det innebär att framställningen kan kortas ner och därmed blir mer överskådlig. Han gör följande definition:

> Låt n vara ett naturligt tal. Om a och b är heltal så säger vi att a är kongruent med b modulo n om $a - b$ är delbart med n. Vi skriver då
>
> $$a \equiv b \mod n.$$

Vi kan också säga att $a \equiv b \mod n$ precis då heltalen a och b ger samma rest vid division med n.

Gauss visade följande två grundläggande men enkla samband som innebär att man på ett enkelt sätt kan räkna med modulobegreppet:

> Om n är ett naturligt tal och a, b, c och d är hela tal sådana att
>
> $$a \equiv b \mod n \text{ och } c \equiv d \mod n$$
>
> så gäller att
>
> $$(a \pm c) \equiv (b \pm d) \mod n \text{ och } a \cdot c \equiv b \cdot d \mod n.$$

Vi visar den del som avser multiplikation och lämnar addition och subtraktion till den eventuelle läsaren.

> Anta att $a \equiv b \mod n$ och $c \equiv d \mod n$. Det innebär att $a - b = sn$ respektive $c - d = tn$ där s och t är heltal. Då är
>
> $$a \cdot c = (b + sn) \cdot (d + tn) = b \cdot d + n(s + t + st)$$
>
> och eftersom $s + t + st$ är ett heltal betyder det att $a \cdot c \equiv b \cdot d \mod n$.

Vi använder många gånger modulo-begreppet i vardagen om än omedvetet. Idag är det torsdag. Vilken veckodag är det om 100 dagar? Vi

sätter ett nummer på varje veckodag och ger söndag nummer 0, måndag nummer 1 o.s.v. Torsdag har alltså nummer 4. Vi konstaterar att

$$4 + 100 = 104 \equiv 6 \mod 7.$$

Dagen vi söker alltså en lördag.

En mer teoretisk frågeställning är följande: Bestäm entalssiffran i talet $37^5 \cdot 54^3$. I detta fallet räknar vi modulo 10. Eftersom $37 \equiv 7 \mod 10$ har vi att

$$37^5 \equiv 7^5 \equiv 49 \cdot 49 \cdot 7 \equiv 9 \cdot 9 \cdot 7 \equiv 81 \cdot 7 \equiv 1 \cdot 7 \equiv 7 \mod 10$$

och då $54 \equiv 4 \mod 10$ har vi att

$$54^3 \equiv 4^3 \equiv 64 \equiv 4 \mod 10$$

Vi har sammanfattningsvis

$$37^5 \cdot 54^3 \equiv 7 \cdot 4 \equiv 28 \equiv 8 \mod 10$$

och den efterfrågade entalssiffran är alltså 8.

Vid räkning modulo n så gäller att varje heltal a är kongruent med precis ett av talen 0, 1, 2, ... $n-1$ d.v.s de rester man får om man dividerar a med n.

Vi har sett att vi på vanligt sätt addera, subtrahera och multiplicera. Kan man dividera? Knappas troligt eftersom kvoten av två vanliga heltal i regel inte är ett heltal. Men det visar sig att det finns en slags motsvarighet till division om vi räknar modulo p där p är ett primtal. Det finns en sats som säger att om p är ett primtal och p inte är en delare till a så har den diofantiska ekvationen

$$ax + py = 1$$

alltid lösningar x och y som är heltal. Beviset grundar sig på Euklides algoritm och finns i den första texten i denna serie, *Fyra fundamentala teorem*, och det skulle gå alltför långt att gå igenom det här. Det kan nämnas att Euklides algoritm finns i *Elementa* men då i geometrisk form.

Antag nu att p är ett primtal och att a är ett heltal sådant att p inte är en delare till a d.v.s. att *inte* $a \equiv 0 \mod p$. Då finns alltså heltal x och y sådana att $ax + py = 1$ d.v.s. $ax = 1 - py$ vilket medför att $ax \equiv 1 \mod p$. Vi betecknar i fortsättningen ett sådant x med a'. Vi har visat att

> Om p är ett primtal och om a är ett heltal som inte är delbart med p så finns ett heltal a' sådan att $a \cdot a' \equiv 1 \mod p$.

Vi ger några exempel: $5 \cdot 3 \equiv 1 \mod 7$ och $3 \cdot 3 \equiv 1 \mod 7$.

Beviset

Fermats lilla sats kan formuleras på följande sätt:

> Om p är ett ett primtal så gäller att
>
> $$a^p \equiv a \mod p$$
>
> för alla heltal a.

Antag att a är ett heltal som inte är delbart med p. Varje tal i följden

$$1, a, a^2, a^3, a^4, \ldots, a^n, \ldots$$

har en rest som är något av talen 1, 2, ..., $p-1$. Resten kan inte vara 0 för det skulle innebära att p är en delare till a^j för något $j > 0$ vilket i sin tur skulle innebära att p delar a och det strider mot förutsättningarna. Antalet möjliga olika rester i följden är alltså $p-1$ och det betyder att alla talen i den oändliga följden inte kan var olika.

För att förenkla framställningen inför vi beteckningss $\bar{a}$ för den rest man får om heltalet a divideras med p. Alltså är $\bar{a}$ ett av talen $0, 1, \ldots, p-1$.

Det finns alltså j och k där $j < k$ sådana att $\bar{a^j} = \bar{a^k}$ Anta att k är det minsta talet sådant att a^k ger samma rest som ett av de föregående talen.
Det betyder att $1, \bar{a}, \ldots, \overline{a^{k-1}}$ alla är olika och att $\bar{a^j} \equiv \bar{a^k}$ för något heltal j sådant att $j < k$.
Eftersom p är ett primtal och p inte delar a så finns ett tal a' sådant att $a \cdot a' \equiv 1 \mod p$. Vi multiplicerar båda sidor i ekvivalensen

$$a^k \equiv a^j \mod p$$

med $(a')^j$ vilket ger

$$a^{k-j} \equiv 1 \mod p.$$

Vi sätter $k - j = s$ och konstaterar att talen $1, \bar{a}, \bar{a^2}, \ldots \bar{a^{s-1}}$ alla är olika eftersom $s < k$. Dessutom gäller

$$a^s \equiv 1 \mod p.$$

Vi noterar att om t är ett godtyckligt naturligt tal så är a^t kongruent med något av talen $1, a, a^2, \ldots, a^{s-1}$ Med hjälp av divisionsalgoritmen kan vi ju skriva $t = s \cdot q + r$ där $0 \leq r < s$ och

$$a^t \equiv a^{sq+r} \equiv a^{sq} \cdot a^r \equiv a^r \mod p \text{ där } 0 \leq r < s.$$

Vi betraktar nu mängden

$$H = \{1, \bar{a}, \bar{a^2}, \ldots, \overline{a^{s-1}}\}$$

som har s tal som alla är olika.

Om H innehåller alla rester modulo p så är $s = p$ och då är $a^{p-1} = a^{s-1} \equiv 1 \mod p$ då a inte har resten 0 modulo p. Om vi multiplicerar båda leden med a får vi att $a^p \equiv a \mod p$ som gäller också då $a \equiv 0 \mod p$.

Anta nu att det finns ett tal b som inte är delbart med a och att $\bar{b}$ inte tillhör H. Då sätter vi

$$\bar{b}H = \{\overline{ba}, \overline{ba^2}, \ldots, \overline{ba^{s-1}}\}.$$

Alla talen i $\bar{b}H$ är olika. Om $b\bar{a^u} = b\bar{a^v}$ där $0 \leq u < v < s$ d.v.s. om

$$ba^u \equiv ba^v \mod p$$

så multiplicerar vi båda sidor i ekvivalensen med b' där b' är ett heltal sådant att $b \cdot b' \equiv 1 \mod p$ och får att

$$a^u \equiv a^v \mod p \text{ där } 0 \leq u < v < s$$

vilket innebär en motsägelse.

Vi visar nu att ingen av resterna i $\bar{b}H$ kan tillhöra H.
Antag motsatsen. Det skulle innebära att $ba^u \equiv a^v \mod p$ för några heltal u och v där $0 \leq u \leq s-1, 0 \leq v \leq s-1$.
Om $v \geq u$ så multiplicerar vi båda sidor i ekvivalensen med $(a')^u$ och får $b \equiv a^v(a')^u \equiv a^{v-u} \mod p$ vilket innebär att $\bar{b}$ tillhör H och det innebär en motsägelse.
Om $v < u \leq s-1$ så multiplicerar vi ekvivalensen med $(a')^{s-1-u}$ och får $ba^{s-1} \equiv a^{v+s-1-u} \mod p$ d.v.s. $b \equiv a^t$ där t är ett positivt heltal och det medför också att $\bar{b}$ ligger i H vilket också innebär en motsägelse.

Mängderna H och $\bar{b}H$ innehåller alltså s rester vardera och de har ingen gemensam rest. Om de tillsammans utgör alla $p-1$ rester som inte är 0 så är totala antalet sådana rester lika med $2s$ och alltså är $2s = p-1$ och vi har att

$$a^{p-1} \equiv a^{2s} \equiv (a^s)^2 \equiv 1^2 \equiv 1 \mod p$$

för alla heltal a som inte är delbara med p. Om vi multiplicerar båda sidor med a får vi att $a^p \equiv a \mod p$ för alla heltal a.

Om det finns en rest $\bar{c}$ som varken ligger i H eller $\bar{b}H$ så bildar vi $\bar{c}H$ och visar på analogt sätt att var och en av $H, \bar{b}H$ och $\bar{c}H$ innehåller s olika rester och att ingen rest samtidigt ligger i två av mängderna. Om det inte finns rester som inte ligger i någon av mängderna $H, \bar{b}H$ eller $\bar{c}H$ så är totala antalet rester skilda från 0 lika med $3s$ och vi har $p - 1 = 3s$. och kan på samma sätt som i förra fallet visa att $a^p \equiv a \mod p$.

Om det finns en rest $\bar{d}$ som inte ligger i någon av $H, \bar{b}H$ eller $\bar{c}H$ så bildar vi $\bar{d}H$ och så vidare. Eftersom antalet rester som är skilda från 0 är ändligt kommer vi till slut att få n mängder med $s - 1$ rester vardera där ingen rest samtidigt ligger i två av mängderna. Alltså är $p - 1 = ns$ och vi kan som förut visa att $a^p \equiv a \mod p$.

Fermats lilla sats är därmed bevisad.

För många känns kanske det första beviset enklare. Det andra innehåller mängder av små korta resonemang som kanske döljer den bärande idén: Att det går att dela upp de $p - 1$ resterna i ett antal delar där de olika delarna innehåller lika många rester och att ingen rest samtidigt finns med i två delar. Induktionsbeviset visar att det mönster Fermat sett stämmer. Det gör givetvis det andra också men det leder samtidigt till ett sätt att resonera som man kan finna i teorin för ändliga grupper. I Gauss bevis känner man igen det som kallas Lagranges sats och som säger att om G är en ändlig grupp och om H är en undergrupp till G så är antalet element i H en delare till antalet element i G. Lagrange sats är grundläggande i gruppteorin. För den som vill bekanta sig med gruppteori och Lagranges sats hänvisas till elementära läroböcker i modern algebra t.ex. Per-Anders Svenssons *Abstrakt algebra*, Studentlitteratur. 2001.

Fermat bestämmer maxima och minima

Ju mer originell en upptäckt är desto mer uppenbar är den efteråt.
Arthur Koestler (1908-83)

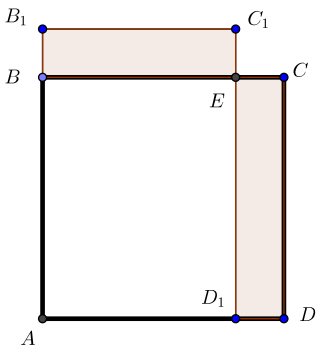
Många problem i verkligheten handlar om optimering. ”Hur kan jag maximera vinsten av en verksamhet under givna villkor?” Eller lite mer pessimistiskt: ”Hur kan jag minimera förlusten?” I matematiken finns det en särskild gren som kallas Optimeringslära och enklare typer av optimeringsproblem ingår i de vanliga matematikkurserna på gymnasiet. De verktyg man använder hämtas från differentialkalkylen. ”För att bestämma maxima och minima sätter vi derivatan lika med 0.” Det är ofta den första tanke man får när man ska bestämma maximum och minimum till ett givet uttryck.

Utan tillgång till symbolisk algebra och utan derivator löste man redan under antiken optimeringsproblem. Problemen var oftast geometriska. Ibland kunde man göra kvalificerade gissningar genom att förmoda att den optimala lösningen borde ha vissa symmetriegenskaper. Därefter ger man ett stringent bevis för att förmodan är korrekt. Vi ger ett exempel som är hämtat från Euklides *Elementa*.

> Bestäm den rektangel med en given omkrets som har störst area.

En rektangel med mycket liten höjd bör ha en area som är nära noll och desamma gäller om basen är mycket liten. Rektanglarna blir

då smala remsor. En rimlig gissning är att den största rektangeln är en kvadrat och för att visa det hänvisar vi till figur 1.



Figur 2:

Rektangeln $ABCD$ är en kvadrat med den föreskrivna omkretsen och $AB_1C_1D_1$ är en rektangel med samma omkrets.
Arean av rektangeln $AB_1C_1D_1$ får vi genom att från kvadraten $ABCD$ subtrahera arean av rektangeln D_1ECD och addera arean av rektangeln BB_1C_1E.
Eftersom $ABCD$ och $AB_1C_1D_1$ har samma omkrets så måste $EC = EC_1$.
Eftersom $B_1C_1 < BC$ så är arean av BB_1C_1D mindre än arean av D_1ECD .
Då, vi från kvadraten $ABCD$ subtraherar mer än det vi adderar till den, måste arean av rektangeln $AB_1C_1D_1$ vara mindre än arean av kvadraten $ABCD$
Alltså är kvadraten större än eller lika med varje rektangel med samma omkrets

Visserligen är resonemanget i detta fallet enkelt och lösningen är elegant, men den ger knappast någon ledning till hur man ska lösa andra liknande optimeringsproblem. Fermat kände naturligtvis till det klassiska problemet från *Elementa*. Han hade också blivit bekant med den nya symboliska algebran i den form den introducerades av Francois Viète

där man kunde räkna med obekanta storheter som symboliserades med bokstäver. Fermat såg hur man kunde utnyttja det för att lösa problemet med en metod som borde kunna användas för att lösa andra problem av liknande natur. Hans lösning är som följer.

> *Att dela en given sträcka AC i en punkt E så att $AE \cdot EC$ är maximal.*

Figur 3:

> Vi sätter $AC = b$; låt a vara den ena av de båda delarna. Då är den andra $b-a$ och produkten vars maximum ska beräknas är $ba - a^2$. Låt nu den första delen vara $a + e$ och den andra $b - a - e$ och produkten $ba - a^2 + be - 2ae - e^2$. Detta måste var ungefär lika med $ba - a^2$. Om vi avlägsnar gemensamma termer betyder det att $be \sim 2ae + e^2$. Dividera med e och sätt $e = 0$; $b = 2a$. Lösningen till problemet är alltså att vi ska välja a lika med halva b.
>
> Vi kan knappast tänka oss en mer allmän metod.

Lösningen är hämtad från D.J.Struik, *A Source Book in Mathematics, 1200-1800*[5] där man också kan se hur Fermat använde samma teknik för att bestämma tangenter till kurvor. Texten måste vara tillrättalagd så att den ska vara lätt att förstå utan att huvudidén går förlorad. Fermats ursprungliga text är från ett brev till Mersenne 1638 och har titeln *En metod att bestämma maximum och minimum samt tangenter till kurvor*. Det publicerades först 1678 i samband med utgivningen av Fermats samlade verk. Förmodligen var Fermats algebraiska räkningar svårare att följa än vad den är i ovanstående text. Han använde sig av Viètes notationssystem som var klumpigare än det vi använder idag, som har sitt ursprung i Descartes *La Géometrie*. Descartes var mycket kritisk till Fermats metoder. Fermat tog för ovanlighetens skull illa vid sig och svarade med en kritik av Descartes verk.

[5] D.J.Struik, *A Source Bokk in Maathematics, 1200-1800*, Harvard University Press/Oxford University Press. London. 1969.

Naturligtvis finns det en del att invända mot Fermats resonemang. Han förutsätter att $e \neq 0$ och sätter sedan $e = 0$. Han påstår också att i närheten av ett maximum så är variationen nästan lika med 0. Det var något som Johan Kepler (1571-1630) hade hävdat några decennier tidigare.

Fermats metod att lösa optimeringsproblem är ett av de arbeten som banade väg för en ny gren av matematiken, differential- och integralkalkylen. Kalkylen, som den också kom att kallas, var revolutionerande inte bara för matematiken utan också för fysiken. De grundläggande verken av Newton och Leibniz publicerades på 1680-talet. Det var inte bara Fermats arbeten som banade väg för kalkylen. Matematiker som Bonaventura Cavalieri (1598-1647), Gil de Roberval (1602-75) och Blaise Pascal beräknade areor av områden som begränsades av krökta kurvor som $y = x^n$ där $n = 3, 4$, cykloiden och $y = \sin x$. Den metod de använde handlade om att dela in ett område i oändligt många oändligt små delar och den förebådade integralkalkylen. Samma typ av resonemang finns hos några av antikens stora matematiker som t.ex. Arkimedes (287-212 f.Kr.). Fermats arbete är mig veterligen ett av de få som förebådar differentialkalkylen.

Fermat och Pascal diskuterar hasardspel - sannolikhetsläran föds

Kunskapens början är upptäckten av något som vi inte förstår.
Blaise Pascal (1623-62)

År 1654 ställde den franske adelsmannen Chevalier de Méré, som var en passionerad spelare och dessutom intresserad av matematik, en fråga till den då trettioettårige matematikern Blaise Pascal: ”Hur ska insatsen i ett spel fördelas om det avbryts i förtid?”. Ett exempel får belysa frågeställningen: Anta att man spelar krona och klave till dess antingen krona eller klave kommer upp fyra gånger. Spelare A vinner om krona kommer upp fyra gånger och B vinner om klave kommer upp fyra gånger. Efter högst sju kast har antingen A eller B vunnit. Båda spelarna har satsat lika mycket och den som vinner får hela potten. Anta att spelet av olika skäl måste avbrytas efter fem kast. Då har krona kommit upp tre gånger och klave två. Hur ska insatsen fördelas?

Pascal var trots sin ungdom välkänd i matematiska kretsar och hade bidragit med viktiga resultat inom både matematik och fysik. Han var en del av Mersennes nätverk där också Fermat ingick. Pascal tog kontakt med den 22 år äldre Fermat för att diskutera de Mérés problem. Det var upprinnelsen till en korrespondens som väsentligen ägde rum under sommaren 1654 och den brukar betcknas som sannolikhetslärans födelse.

En engelsk översättning av brevväxlingen finns tillgänglig på nätet.[6] Tyvärr saknas det första brevet från Pascal till Fermat som satte igång diskussionen. Man slås av tonen i breven. Båda är angelägna om att betona den andres storhet trots att de påpekar bristerna i motpartens resonemang. Förmodligen var det sättet man vanligen kommunicerade på men känslan verkar ändå uppriktig. Den unge geniförklarade Pascal tar kontakt med den äldre Fermat som han tydligen respekterar och Fermat behandlar den tjugo år yngre Pascal som en jämlike. Det är en akademisk diskussion när den är som bäst. Man vänder ut och in på frågeställningarna och landar till slut i en samsyn.

I det första brevet, som vi inte har tillgång till, behandlar Pascal ett problem liknande det vi tidigare beskrivit. Av svaret från Fermat framgår att han inte kan accepetera Pascals resonemang och han anger en egen lösning av problemet. Det problem Pascal studerar är som följer.

> Två spelare A och B spelar krona och klave. Varje gång myntet visar krona får A en poäng och om det visar klave får B en poäng. Den som först kommer till tio har vunnit. Båda satsar lika mycket och segraren får hela potten. Antag att spelet bryts då A saknar två poäng och B tre. Hur ska då de satsade medlen fördelas mellan dem?

För att lösa problemet studerar Fermat vad som skulle ske om inte spelet avbrutits. Efter ytterligare fyra spel måste spelet var avgjort. Då måste A ha fått minst ytterligare två poäng eller B tre. Fermat bestämmer vad som kan hända under de fyra kommande spelen och får följande möjligheter

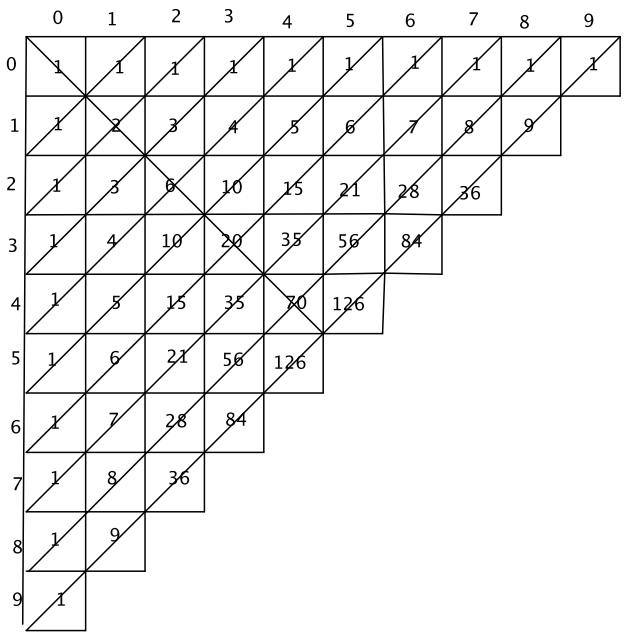
$$\begin{array}{cccc} AAAA & AAAB & AABA & AABB \\ ABAA & ABAB & ABBA & ABBB \\ BAAA & BAAB & BABA & BABB \\ BBAA & BBAB & BBBA & BBBB \end{array}.$$

Av dessa vinner A alla utom $ABBB, BABB, BBAB, BBBA$ och $BBBB$. Alltså vinner A 11 och B 5 gånger. Om de båda spelarna satsat 8 pistoler var så ska A ha 11 och B 5 pistoler.

Pascal förstår resonemanget men har svårt att acceptera att Fermat räknar med händelser som aldrig kommer att äga rum som t.ex. $AAAA$ och $BBBA$. I det första exemplet avbryts spelet efter två kast eftersom A redan då har vunnit och de tredje och fjärde kasten behöver inte göras. I det andra exemplet har B vunnit efter tre kast och något fjärde kast görs inte. I Fermats lista finns många exempel på sådana händelser. Pascal vill i sina beräkningar bara utgå från de händelser som verkligen kan

[6] Se york.ac.uk

inträffa. Hans resonemang blir då betydligt mer omständligt än Fermats och han får inte samma resultat. Fermat går igenom Pascals räkningar och hittar ett fel. Pascal inser felet, rättar det och kommer då till samma resultat som Fermat. Han gör en generalisering där man har tre spelare istället för två. Det resultat han kommer fram till med den metod han tillämpat i fallet med två spelare stämmer inte med det som han anser att Fermats metod ger. Fermat svarar att Pascal missuppfattat hans metod och i själva verket ger de båda metoderna samma resultat. De avslutar diskussionen i enighet.



Figur 4: Pascal kommer i brevväxlingen in på kombinatoriska problem som senare skulle resultera i en artikel om vad vi vi idag kallar Pascals triangel. Hans aritmetiska triangel är rätvinklig och likbent med kateten 10. Den innehåller likformiga trianglar med kateterna 1, 2, ..., 9. De olika kolonnerna numreras från 0 till 9. För att bestämma antalet kombinationer av 2 element valda bland 4 följer man hypotenusan i triangel nummer 4 och väljer det tal som som står i kolonn 2. Resultatet är 6. Triangeln är konstruerad så att 6 är summan av talen närmast över och närmast till vänster d.v.s. $6 = 3 + 3$.

I brevväxlingen tar de båda matematikerna upp en rad andra frågeställningar. Fermat försöker intressera Pascal för talteoretiska problem men Pascal är kallsinnig. Pascal kommer i sina resonemang in på kombinatoriska problem som leder fram till det vi idag kallar Pascals triangel och som han tio år senare publicerar i artikeln *Traité de triangle arithmétique*. Hur Pascas triangel såg ut i sin ursprungliga form finns figur 3.

De två parterna skiljs i enighet och betygar varandra sin vördnad. Fermat vill gärna att de träffas men har varken tid eller ork att åka hela vägen från Toulouse till Paris. Han föreslår att de möts på halva vägen, men Pascal tycker inte han har tid med det. Han tycker inte längre matematiken är så viktig och har börjat ägna sig åt religiösa frågor och välgörenhetsarbete. Han skriver

> För att tala uppriktigt till er om matematik, så är den för mig den allra bästa intellektuella träning, men på samma gång anser jag den så oanvändbar att jag inte kan skilja mellan en matematiker och en duktig hantverkare. Även om jag anser den vara det bästa hantverket i världen så är den bara ett hantverk och jag har ofta sagt att den är bra att träna sig på men inte att att ägna hela sin kraft åt.

Pascals religiösa tankar finns i hans mest berömda verk från 1669 och som översatts till svenska och heter *Tankar*. Han återkommer emellertid till matematiken men även i *Tankar* finns det en mening som man kan associera till vadhållning och spel: ”Jag skulle hellre leva mitt liv som om det finns en Gud och dö för att upptäcka att det inte gör det, än att leva som det inte finns någon och dö för att upptäcka det gör det.”

Fermat lämnade inte helt problematiken kring hasardspel. Han förmedlade sin korrespondens med Pascal till Christian Huygens (1629-95) som 1657 publicerade det första sammanhängande verket om sannolikheter *De ratiociniisin ludo aleae* som översatt till svenska blir ”Att resonera om chanser vid spel”. Arbetet är kort och koncist. Det omfattar bara fjorton sidor och Huygens använder sig av den nya symboliska algebran. I sin brevväxling använder sig varken Fermat eller Pascal av begreppet ”sannolikhet”. Det finns implicit i resonemangen om hur potten ska fördelas. Huygens använder sig inte heller av ordet men han är mycket nära i en av de grundläggande propositionerna som lyder

> Antag att jag har p möjligheter att tjäna a och q möjligheter tjäna b. Om varje möjlighet förutsätts ha samma chans så kommer min förväntade förtjänst att vara $(ap + bq)/(p + q)$.

Sannolikhetsläran är nu en oundgänglig del av matematiken och den har uppstått kring frågeställningarna kring hasardspel. Redan Girolamo

Cardano (1501-76) diskuterade hasardspel i sitt verk *Liber de ludo alea* där en stor del ägnas åt glädjen och faran med spelandet, men han gör också försök att mäta chanser. Han lät aldrig trycka sitt verk så det kom inte att ha någon större betydelse för utvecklingen.[7] Det var alltså Fermats och Pascals brevväxling som blev början till sannolikhetsläran som sedan fortsatte med Huygens arbete och senare med viktiga verk som t.ex. Jacob Bernoullis (1654-1705) arbete *Ars conjectandi*, "Konsten att gissa", från 1713 och Pierre Simon Laplaces (1749-1827) *Théorie anlytique de probabilités* från 1812. Sannolikhetsläran skulle under första hälften av 1900-talet kopplas samman med ämnet statistik och är nu ett effektivt hjälpmedel för att beskriva olika delar av verkligheten och för att utforma underlag för beslutsprocesser på olika nivåer. Den utvecklingen startades av Pascal och Fermat.

[7] *Liber de ludo aleae* publicerade först 1663 nästan hundra år efter Cardanos död.