



Ansats till att bevisa Fermats stora sats, $x^n + y^n = z^n$

Sina Mozayyan Esfahani N3D, Kungsholmens Gymnasium

Gymnasiearbete 100 poäng

Naturvetenskapligt program

Läsåret: 2013-2014

Handledare: Helena Danielsson Thorell

Handledare från KTH: Thomas Ohlson Timoudas

Abstract

Fermats lilla sats, $a^p \equiv a \pmod{p}$, avslöjar nya användningsområden för primtal. Satsen har en fundamental betydelse i modulära uträkningar samtidigt som den höjer säkerheten i krypterade meddelanden. Fermats satser har varit en av matematikens stötestenar. Dels att bevisa dem och dels att utforska nya användningsområden. Hans satser väcker oftast ett brinnande intresse hos läsaren att själv försöka hitta nya bevis och nya användningsområden. Ännu en gång görs ett försök att bevisa Fermats stora sats som inte fick bevis förrän flera hundra år efter. Den här gången genom Fermats lilla sats.

Nyckelord: Fermats lilla sats, Fermats stora sats.

Fermat's little theorem, $a^p \equiv a \pmod{p}$, reveals new sides of primes. The theorem has a fundamental importance in modular calculation while it raises the security of encrypted messages. Fermat's theorems have been one of the stumbling-blocks for mathematicians; partly to prove them and partly to explore new uses. His theorems often awaken a passion in the reader to try to find new proof and new applications. Once again, an attempt to prove Fermat's last theorem that did not get proven until several hundred years later was made. This time by using Fermat's little theorem.

Keywords: Fermat's little theorem, Fermat's last theorem.

Innehållsförteckning

Lista över symboler	4
1. Inledning.....	5
2. Bakgrundshistoria om Pierre de Fermat	5
3. Fermats lilla sats.....	5
4. Ansats till att bevisa Fermats stora sats.....	6
Tillkännagivande.....	14
Litteraturförteckning	15

Lista över symboler

Symbol	Förklaring och exemplifiering
\mathbb{Z}	Alla heltal $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
\mathbb{Q}	Rationella tal som kan skrivas i form av $\frac{p}{q}$ där båda är heltal och $q \neq 0$
$a \in b$	a är element i mängden B , t.ex. $-3 \in \mathbb{Z}$
$a \rightarrow b$	a medför till b med t.ex. om $x > 2 \rightarrow x^2 > 4$. Observera att motsatsen inte gäller.
$a \leftrightarrow b$	a är ekvilans med b . T.ex. om $x - a = 0 \rightarrow x = a$ och $x = a \leftrightarrow x - a = 0$
$a \leq b$	a är mindre eller lika med b .
$a b$	a delar b . $a = bc$ där a, b, c är heltal.
$a \nmid b$	a delar inte b , d.v.s. deras minsta gemensamma nämnare är 1.
$a \equiv b \pmod{c}$	$a = cd + b$ för heltal a, b, c . $d, b < c$. T.ex. $3 \equiv 1 \pmod{2}$
$\{a\}$	$a \pmod{1}$, d.v.s. decimaldelen av a . T.ex. $a = 1,5 \rightarrow \{a\} = 0,5$
$a!$	$a(a-1)(a-2) \cdot \dots \cdot 2 \cdot 1$ för $a \geq 1$. För fullständighetens skull definieras $0! = 1$
$C(a, b) = \binom{a}{b}$	Antal möjligheter att välja a element utan hänsyn till innebörders ordning ur mängden b . Betecknas som $\binom{a}{b} = \frac{a!}{b!(a-b)!}$ För $0 \leq b \leq a$
$(a+b)^p$	Binomialsatsen. $\sum_{i=0}^n \binom{n}{k} a^{n-k} \cdot b^k$
$\binom{n}{k}$	Binomialkoefficienterna. Samma koefficienter som finns i n : te leden i Pascals triangel
SGD	Största gemensamma delare. T.ex. $SGD(12, 3) = 3$
MGN	Minsta gemensamma delare. T.ex. $MGN(12, 3) = 12$
■	Avslutning av ett bevis. Något som skulle bevisas. VSB eller Q.E.D

1. Inledning

Pierre de Fermat presenterade för första gången sin lilla sats år 1640. Upptäckten visade att ett positivt tal a , multiplicerad med sig självt p -gånger (där p är ett udda primtal) minus a kommer alltid att vara delbart med p , med andra ord, $a^p \equiv a \pmod{p}$. Fermats stora sats förmedlar att den diofantiska ekvationen $x^n + y^n = z^n$ saknar positiva heltalslösningar då $n > 2$. I den här rapporten görs en ansats till att bevisa Fermats stora sats. Det befintliga beviset av Fermats stora sats är komplicerat. Den här gången görs ett försök att bevisa Fermats stora sats med jämförelsevis enklare matematik.

2. Bakgrundshistoria om Pierre de Fermat

Pierre de Fermat, född 1601, död 1665, var en fransk matematiker som till yrket arbetade som jurist. Fermat kan påstås vara grundaren av den moderna talteorin. Till skillnad från Diafantos fokuserade Fermat på heltalen, och hans arbete behandlar bl.a. problem rörande delbarhet, primtal och diofantiska ekvationer, ekvationer där man söker efter heltal- och rationella lösningar.

Matematiken tycks ha varit självlärd för honom och fungerade som en hobby. Arkimedes analytiska metoder och Diafantos talteori var något som väckte den unge Fermats intresse. Senare i livet utvecklade Fermats sina idéer gällande analytisk geometri, differentialkalkyl och talteori och lyckades upptäcka många fundamentala satser. (Nationalencyklopedin, 2013) Fermat brukade inte publicera sina upptäckter inom matematiken, då han inte var intresserad av andra vetenskapsmäns uppmärksamhet. Vid de få tillfällen som Fermat lämnade sina satser till andra matematiker, utmanade han dem att själva hitta beviset. Efter hans bortgång blev hans upptäckter mer kända, en del redovisar han i brev till sina vänner och en del i marginalen av Diafantos bok, "Arithmetika". Under flera århundraden försökte många matematiker hitta bevis för hans satser. Vilket senare gjorde honom till en av världens mest kända matematiker (Persson, NE diofantisk ekvation, 2013; Kullberg & Sandström, 2007).



Figur 1 Pierre de Fermat

Han upptäckte två grundläggande talteoretiska satser inom modern matematik, Fermats lilla sats: $a^p \equiv a \pmod{p}$ vilket rapporten kommer att handla om och själva satsen kommer att beskrivas mer ingående. Hans andra sats, Fermats stora sats, även känd som "Fermats förmodan" förmedlar att den diofantiska ekvationen $x^n + y^n = z^n$ saknar positiva heltalslösningar då $n > 2$. Satsen var länge ett av de mest kända, olösta matematiska problemen. Efter 350 års försök av forskare i hela världen lyckades slutligen Andrew Wiles presentera ett bevis 1995 (Persson, NE Fermats förmodan, 2013).

3. Fermats lilla sats

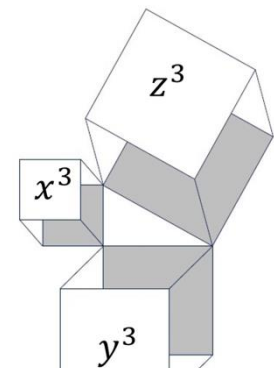
Pierre de Fermat redovisade först sin lilla sats i ett brev 18 oktober 1640 till sin vän Frénicle de Bessat (de Fermat, 1640). Fermats upptäckte följande samband: p delar $a^p - a$ då p är ett primtal större än 2 och a är ett positivt heltal som inte delar p , $a \nmid p$:

$$a^p \equiv a \pmod{p} \leftrightarrow a^{p-1} \equiv 1 \pmod{p}$$

Såsom tidigare lämnade Fermat inte några bevis. Det första publicerade beviset är från Euler 1736 som bevisade satsen med induktion. Satsen har bevisats på olika sätt under åren och ibland har matematiker lyckats utveckla och generalisera den. Bland de mest kända är Eulers sats $a^{\varphi(n)} \equiv 1 \pmod{n}$ och det i sin tur har generaliserats till Carmichaels sats. (Persson, NE Fermats förmodan, 2013)

4. Ansats till att bevisa Fermats stora sats

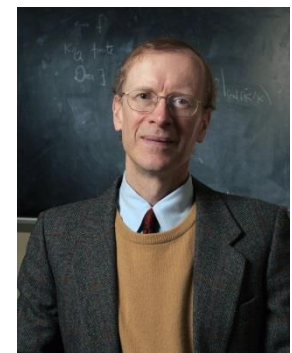
Fermat upptäckte 1637 följande olikhet, som senare blev kallad för Fermats stora sats, att $x^n + y^n \neq z^n$ för alla positiva heltal då $n > 2$. Satsen påminner om Pythagoras sats som gäller när $n = 2$ och som har oändligt med lösningar och tiotals bevis. Fermats generalisering är mycket svårare att bevisa men problemet i sig är enkelt att förstå, vilket har frustrerat matematikerna. Det kan ha varit orsaken till att det gjorts flest felaktiga bevis till Fermats stora sats än till någon annan matematisk sats i historia (Persson, NE Fermats förmodan, 2013).



Figur 2 Enligt Fermats stora sats saknar Pythagoras sats, heltalslösningar när kvadrater ersätts med kub, dvs. $n = 3$

Fermats stora sats var nedskriven i marginalen i Diafantos "Arithmetika", "Jag har ett i sanning underbart bevis för detta påstående, men marginalen är alltför trång för att rymma detsamma". (Kullberg & Sandström, 2007) Satsen var i flera hundra år bland världens svåraste och olösta matematiska problem. Målet för matematiker under tre hundra år var att hitta ett bevis till Fermats stora sats. Amatörer likväl professionella matematiker som Euler och Gauss misslyckades med att bevisa den. Men slutligen 1995 kunde, Andrew Wiles, den brittiske matematikern, bevisa den efter 8 års isolering.

Matematikerna som ville bevisa satsen började med att bevisa den med kunskaper som var aktuella under Fermats tid men förstod genast att man behövde upptäcka nya matematiska områden. En förutsättning för att lyckas var att man behövde ett samarbete med andra matematiker och bygga sitt bevis på andra matematikers upptäckter. Till slut, efter 350 år intensiv forskning, då man såg ett samband mellan Fermats stora sats och elliptiska ekvationer, kunde Wiles lägga ihop alla upptäckterna och kunde slutligen bevisa satsen med ett mycket omfattande och komplicerat bevis. Många anser att Fermats bevis skulle ha varit olikt Wiles bevis (Singh, 1997).



Figur 3 Andrew Wiles

Den här ansatsen är ett försök från min sida att bevisa en övervägande del av Fermats stora sats med hjälp av Fermats lilla sats. Mitt syfte är inte att hitta ett bevis som har tagit flera hundra år att hitta. Däremot vill jag påpeka att eftersom det inte finns ett bestämt bevis till Fermats satser kan man, oavsett sin matematiska kunskapsnivå, försöka att bevisa Fermats satser. Beviset är inte lika omfattande som Wiles men det har sin enkelhet.

Sats: (Fermat) Ekvationen nedan saknar heltalslösningar då $n > 2$.

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

Beviset kommer att bygga på motsägelsebevis. Att använda sig av motsägelsebevis är mycket passande i den här ansatsen, eftersom att beviset får en annan struktur. När ett matematiskt samband bevisas ska den vara generaliserad, i form av ett algebraiskt bevis och gälla alltid för de definierade villkoren. Men i vissa satser, som Fermats stora sats, är det fokus att något inte gäller, i dessa fall är motsägelsebevis en bra lösningsmetod. Eftersom det är tillräckligt att motbevisa med ett enda fall och då har man lyckats bevisa olikheten. Om någon påstår att alla rätvinkliga fyrhörningar är kvadrater, det räcker endast att motbevisa i ett fall, en rektangel, för att motbevisa påståendet. Motsägelsebevis fungerar utmärkt i följande ansats då alla antagande att z är ett heltal ofrånkomligt leder till en motsägelse, då är den jämförelsevis lätta svårigheten att hitta motsägelsen.

Eftersom att Fermats stora sats berör så omfattande delar av tal med olika egenskaper kan man inte bevisa det med ett enda bevis. Fermats stora sats har fyra kända variabler, x, y, z, n varav 3 av dessa är nödvändiga och leder till den fjärde variabeln. I beviset fokuseras det endast på x, y, n , och med hjälp av endast dessa variabler bevisas att z inte kan vara ett heltal. De tre variablerna i VL kan man välja utefter ungefär 9 bestämda scenarier. Efter definitionen av dessa scenarier exemplifieras hjälpsatsen med ett exempel. Alla de 8 första scenarierna kommer att bevisas, förutom den sista och därför är beviset inte komplett.

1. Hjälpsats 4.1: n är ett tal som kommer före ett udda primtal och att $x, y \nmid n$. Till exempel $3^{7-1} + 2^{7-1}$.
2. Hjälpsats 4.2: n är ett udda primtal med följande villkor: $x, y < n, x + y < n$ och att $x, y \nmid n$. Till exempel $3^7 + 2^7$
3. Hjälpsats 4.3: n är ett udda primtal med följande villkor: $x, y < n, x + y > n$ och att $x, y \nmid n$. Till exempel $3^7 + 5^7$
4. Hjälpsats 4.4: n är ett udda primtal med följande villkor: $x > n, y < n, x + y > n$ och att $x, y \nmid n$. Till exempel $9^7 + 3^7$ och $9^7 + 6^7$
5. Hjälpsats 4.5: n är ett udda primtal med följande villkor: $x, y > n, x + y > n$ och att $x, y \nmid n$. Till exempel $9^7 + 11^7$ och $9^7 + 13^7$.
6. Hjälpsats 4.6: En av x, y är delbart med n (vilket Fermats lilla sats inte är definierad för). Till exempel $7^7 + 9^7$
7. Hjälpsats 4.7: Både x och y är delbara med n . Till exempel $14^7 + 7^7$
8. Hjälpsats 4.8: n är en produkt av två eller flera primtal med villkoret att $x, y \nmid n$. Till exempel $(3^3)^7 + (11^3)^7$
9. n är ett udda primtal med följande villkor att $x + y = n$. Till exempel $3^7 + 4^7$

Hjälpsats 4.1: Fermats stora sats saknar heltalslösningar då $n = p - 1$ och p är ett udda primtal och att $x, y \nmid p$. Till exempel $3^{7-1} + 2^{7-1}$

Bevis 4.1: Man bestämmer två godtyckliga positiva heltal för x, y och antar att z är också ett heltal.

$n = p - 1$, p ett primtal större än 3. Annars skulle exponenten bli 2, då gäller inte Fermats stora sats.

$x^{p-1} + y^{p-1} = z^{p-1} \rightarrow \frac{x^{p-1}}{p} + \frac{y^{p-1}}{p} = \frac{z^{p-1}}{p}$, Första ledet är en omskrivning av Fermats stora sats och senare delas båda sidor med exponenten p . Vilket liknar Fermats lilla sats: $a^{p-1} \equiv 1 \pmod{p}$

$x^{p-1} + y^{p-1} \equiv 1 + 1 \pmod{p}$; $z^p \equiv 1 \pmod{p}$, genom Fermats lilla sats

$VL = 2$; $HL = 1$, $VL \neq HL$, en följd av kongruens då i Fermats stora sats är HL lika med VL .

Beviset leder till en motsägelse vilket endast beror det felaktiga antagandet att z är också ett heltal. Det medför att z kan inte vara ett heltal då x och y är positiva heltal som inte delar exponenten. Därmed bevisas hjälpsatsen att z inte kan vara heltal då exponenten är talet innan ett udda primtal.

■

Hjälpsats 4.2: Fermats stora sats saknar heltalslösningar då n är ett udda primtal med följande villkor: $x, y < n$, $x + y < n$ och att $x, y \nmid n$. Till exempel $3^7 + 2^7$

Bevis 4.2: Man bestämmer två godtyckliga positiva heltal för x och y som följer ovanstående villkor och antar att även z är ett heltal.

$n = p$ Ett udda primtal

$$x^p + y^p = z^p \rightarrow \frac{x^p}{p} + \frac{y^p}{p} = \frac{z^p}{p}$$

$$x^p + y^p \equiv x + y \pmod{p}; z^p \equiv z \pmod{p}$$

$x + y = z + kp$; $k = 0 \rightarrow x + y = z$. Anledningen till att k i det här fallet är lika med noll är p.g.a. villkoret att $x + y < n$. Fermats lilla sats beräknas alltid den minsta resten och enligt hjälpsatsen fick inte x och y vara större än n , och därför kommer inte $x + y$ att överstiga p .

$$\begin{cases} x + y = z \rightarrow (x + y)^p = z^p \\ x^p + y^p = z^p \end{cases}$$

$$x^p + y^p = z^p \rightarrow x^p + y^p = (x + y)^p$$

$$x^p + y^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} \cdot y^k + y^p$$

$$HL = 0; VL = \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} \cdot y^k$$

$$HL \neq VL$$

Det är en motsägelse då binomialkoefficienterna i HL är skilda från noll och enligt definitionen är x och y positiva heltal, å andra sidan är VL lika med noll. Likt beviset för hjälpsatsen 4.1 är den enda orsaken till motsägelsen, det är antagandet att z är ett heltal. Därför bevisas hjälpsatsen att z inte kommer att vara ett heltal när x och y är mindre än exponenten.

■

Hjälpsats 4.3: Fermats stora sats saknar heltalslösningar då n är ett udda primtal med följande villkor: $x, y < n$, $x + y > n$ och att $x, y \nmid n$. Till exempel $3^7 + 5^7$

Bevis 4.3: Man bestämmer två godtyckliga positiva heltal för x och y som uppfyller ovanstående villkor. Man antar att även z är ett heltal.

$n = p$ Ett udda primtal

$$x^p + y^p = z^p \rightarrow \frac{x^p}{p} + \frac{y^p}{p} = \frac{z^p}{p}$$

$$x^p + y^p \equiv x + y \pmod{p}; z^p \equiv z \pmod{p}$$

$x + y = z + k \cdot p$; $k = 1 \rightarrow x + y = z + p$, som resultat från kongruensuträkningen. Anledningen till att man adderar endast en period av p är att summan av två minimala rester inte kan överstiga själva perioden mer än en gång. Vilket medför följande gränsvärde $p < x + y < 2p$. Detta är viktigt att ta hänsyn till i fortsättningen av beviset.

$$\begin{cases} x + y - p = z \\ x^p + y^p = z^p \end{cases}$$

$$x^p + y^p = z^p \rightarrow x^p + y^p = (x + y - p)^p$$

Det är en motsägelse och det kommer visas först genom specifika exempel som följer hjälpsatsens villkor, att $x, y < p$; $p < x + y < 2p$; $x, y \in \mathbb{Z}^+$, men som leder till en motsägelse. Senare visas även en algebraiskt generaliserad modell.

Ex 1. $x = 3, y = 5, p = 7$ alltså $3^7 + 5^7 = z^7$

$$x^p + y^p = (x + y - z)^p \rightarrow 3^7 + 5^7 \neq (8 - 7)^7 \rightarrow 3^7 + 5^7 > (1)^7; VL \neq HL$$

Ex 2., $x = 6, y = 6, p = 7$ alltså $6^7 + 6^7 = z^7$

$$x^p + y^p = (x + y - z)^p \rightarrow 6^7 + 6^7 \neq (12 - 7)^7 \rightarrow 3^7 + 5^7 > (5)^7; VL \neq HL$$

Ex 3. $x = p - 1, y = p - 1, p = p$ alltså $(p - 1)^7 + (p - 1)^7 = z^7$

$$x^p + y^p = (x + y - z)^p \rightarrow (p - 1)^p + (p - 1)^p \neq (2(p - 1) - p) \rightarrow$$

$$2(p - 1)^p > (p - 2)^p; VL \neq HL$$

Generalisering: Enligt satsen gränsvärde kan man skriva om x och y på följande sätt:

$$x = p - a; y = p - b \text{ där } 2 \leq a + b < p \text{ eftersom att } a, b \geq 1$$

$$x^p + y^p = (x + y - p)^p$$

$$(p - a)^p + (p - b)^p = (p - a + p - b - p)^p$$

En omskrivning leder till en motsägelse då VL kommer alltid att vara större än HL. På grund av att $p - a - b$ är alltid positiv.

$$(p - a)^p + (p - b)^p > (p - a - b)^p; VL \neq HL$$

Med hjälp av de tre exempel och dessutom den generaliserade exemplen ser man likheten från ekvationssystemet som är till följd av villkoren att $x, y < n$ och $x + y > n$, leder till motsägelse att, $x^p + y^p \neq (x + y - z)^p$, och alltid kommer VL att minst vara dubbelt så stort som HL. Med motsägelsen kan man säga att antagandet att z är ett heltal, är felaktigt. Därför saknar Fermats stora sats heltalslösningar då $x + y < n$ och $x, y \nmid p$ där p är ett udda primtal.

■

Hjälpssats 4.4: Fermats stora sats saknar heltalslösningar då n är ett udda primtal med följande villkor: $x > n, y < n, x + y > n$ och att $x, y \nmid n$. Till exempel $9^7 + 3^7$ och $9^7 + 6^7$

Bevis 4.4: Man bestämmer två godtyckliga positiva heltal för x och y som uppfyller ovanstående villkor. Man antar att även z är ett heltal.

$n = p$ Ett udda primtal

$$x = k \cdot p + a; k, a \in \mathbb{Z}^+$$

$$x^p + y^p = z^p \rightarrow \frac{x^p}{p} + \frac{y^p}{p} = \frac{z^p}{p}$$

$$x^p + y^p \equiv a + y \pmod{p}; z^p \equiv z \pmod{p}$$

$a + y = z$ eller $a + y = z + p$. Anledningen till att det förekommer två alternativa lösningar är att om summan av a och y blir större än p eller inte. Om summan blev mindre då är ett exempel följande $9^7 + 3^7 \equiv 2 + 3 \pmod{7}$. Vilket liknar hjälpsatsen 4.2 och som kan bevisas på samma sätt. När det gäller det andra alternativet, t.ex. $9^7 + 6^7 \equiv 2 + 6 \pmod{7} \equiv 1 \pmod{7}$. Det likar den förra hjälpsatsen, 4.3 och kan bevisas på samma sätt. Med andra ord saknar Fermats stora sats heltalslösningar oavsett huruvida en av variablerna x eller y förhåller sig storleksmässigt med exponenten så länge de inte delar exponenten. Därmed bevisas hjälpsatsen.

■

Hjälpsats 4.5: Fermats stora sats saknar heltalslösningar då n är ett udda primtal med följande villkor: $x, y > n$, $x + y > n$ och att $x, y \nmid n$. Till exempel $9^7 + 11^7$ och $9^7 + 13^7$.

Bevis 4.5: Man bestämmer två godtyckliga positiva heltal för x och y som uppfyller ovanstående villkor. Man antar att även z är ett heltal.

$n = p$ Ett udda primtal

Eftersom båda x, y är större än n så är z också större än n . Därför kan x, y, z skrivas om som:

$$x = k \cdot p + a; \quad y = n \cdot p + b; \quad z = m \cdot p + c$$

$k, n, m \in \mathbb{Z}^+$ och att $1 < a, b, c < p$

$x^p + y^p = z^p \rightarrow (kp + a)^p + (np + b)^p = (mp + c)^p$, en omskrivning av Fermats stora sats p.g.a. villkoret att $x, y, z > n$.

$$x^p = (kp + a)^p = \sum_{i=0}^p \binom{p}{i} (kp)^{p-i} a^i \equiv a^p \pmod{p} \equiv a \pmod{p}.$$

$(kp)^{p-i}$ är alltid delbart med p när exponenten är skild från noll, därför kommer även produkten $(kp)^{p-i} a^i$ vara delbart med p under intervallet, $0 \leq i < p$. Följaktligen kommer uttrycket för x vara kongruens med a^p , vid modulo p . Det i sin tur liknar Fermats lilla sats och eftersom $a \nmid p$, gäller följande, $x^p \equiv a^p \pmod{p} \equiv a \pmod{p}$. Samma resonemang gäller även för y och z .

$$y^p = (np + b)^p = \sum_{i=0}^p \binom{p}{i} (np)^{p-i} b^i \equiv b^p \pmod{p} \equiv b \pmod{p}$$

$$z^p = (mp + c)^p = \sum_{i=0}^p \binom{p}{i} (mp)^{p-i} c^i \equiv c^p \pmod{p} \equiv c \pmod{p}$$

Alltså kan HL och VL i Fermats stora sats skrivas som:

$$HL = x^p + y^p = (kp + a)^p + (np + b)^p \equiv a^p + b^p \pmod{p} \equiv a + b \pmod{p}$$

$$VL = z^p \equiv (mp + c)^p \pmod{p} \equiv c^p \pmod{p}$$

Enligt Fermats stora sats är HL lika med VL, då skapas följande ekvationssystem, beroende på vilka egenskaper a, b har. Om $a + b < p$ då gäller fall-a, och om $a + b > p$ gäller fall-b.

$$\text{Fall } a = \begin{cases} a + b = c \\ a^p + b^p = c^p \end{cases} \quad \text{Fall } b = \begin{cases} a + b - p = c \\ a^p + b^p = (c + p)^p \end{cases}$$

Likt det förra beviset förekommer här två alternativ. Ett exempel för fall-a är

$$9^7 + 11^7 \equiv 2 + 4 \pmod{7} \text{ där summan av resterna är mindre än exponenten och för fall b}$$

$$9^7 + 13^7 \equiv 2 + 6 \pmod{7} \equiv 1 \pmod{7}, \text{ överstiger summan av resterna exponenten. Fall-a liknar}$$

hjälpssatsen 4.2, och kan bevisas på samma sätt. Slutligen kommer fram till att c inte kan vara heltal,

och om c är inte ett heltal kan inte z vara heltal för att $z = mp + c$ och produkten mp är alltid

heltal. Med samma resonemang som beviset för 4.3 kan man bevisa fall b och då kommer följaktligen

att z inte vara heltal. Därmed bevisas hjälpsatsen att oavsett huruvida variablerna x eller y förhåller sig storleksmässigt med exponenten och så länge att de inte delar exponenten; har inte Fermats stora sats

heltalslösningar. (Dock skiljer sig resonemanget när $x + y = n$ vilket lämnas obevisad.) ■

Hjälpsats 4.6: Fermats stora sats saknar heltalslöningar även om x eller y delar exponenten n (vilket Fermats lilla sats inte är definierad för). Till exempel $7^7 + 9^7$

Bevis 4.6: För att inte upprepa samma metod för alla de tidigare scenarierna bevisas hjälpsatsen endast för då n är ett udda primtal. Man bestämmer två godtyckliga positiva heltal x och y då exempelvis x delar n och antar återigen att z är ett heltal.

$n = p$ Ett udda primtal

$$x^p + y^p = z^p \rightarrow \frac{x^p}{p} + \frac{y^p}{p} = \frac{z^p}{p}$$

$$x^p + y^p \equiv 0 + y \pmod{p}; z^p \equiv z \pmod{p}$$

$y = z$, Resultat från kongruensuträkningen

$$\begin{cases} y = z \rightarrow y^p = z^p \\ x^p + y^p = z^p \end{cases}$$

$$x^p + y^p = z^p \rightarrow x^p + y^p = y^p \rightarrow VL = x^p; HL = 0; VL \neq HL$$

Enligt definitionerna om att x är positivt heltal och p ett udda primtal, kan inte HL vara lika med noll. Därför bevisar satsen att Fermats stora sats stämmer även då minst en av x och y är delbara med exponenten n .

■

Hjälpsats 4.7: Fermats stora sats saknar heltalslöningar när både x och y delar exponenten. Till exempel $14^7 + 7^7$

Bevis 4.7: Likt förgående bevisen kan man bevisa hjälpsatsen 4.7 på olika sätt beroende på olika scenarier. Man bestämmer två positiva heltal för x och y som delar exponenten och antar som tidigare att z är ett heltal.

$n = p$ Ett udda primtal

$$x = p \cdot a; \quad y = p \cdot b; \quad a, b \in \mathbb{Z}^+; \quad a, b \geq 1$$

Eftersom VL är delbart med p så innebär det att HL är också delbart med p . Det kan skrivas om:

$$z = p \cdot c; \quad c \in \mathbb{Z}^+; \quad c \geq 1$$

$$x^p + y^p = z^p \rightarrow (p \cdot a)^p + (p \cdot b)^p = (p \cdot c)^p$$

$$p^p(a^p + b^p) = p^p c^p \rightarrow a^p + b^p = c^p$$

Härmed kan man, likt bevisen för hjälpsatserna 4.2 till 4.6 kan man bevisa fortsättningen av beviset beroende på vilka egenskaper a och b har i jämförelse med exponenten p . Därmed bevisas hjälpsatsen att Fermats stora sats saknar heltalslöningar även om x , y och z är delbara med n .

■

Hjälpsats 4.8: Fermats stora sats saknar heltals lösningar då n är en produkt av två primtal när $x, y \nmid n$ och att $x + y \neq p$. Till exempel $(3^3)^7 + (11^3)^7$

Bevis 4.8: Man bestämmer två godtyckliga positiva heltal för x och y som följer ovanstående definitioner och antar att även z är ett heltal.

$n = p \cdot q$; både p och q är ett eller olika udda primtal

$$x^{pq} + y^{pq} = z^{pq} \rightarrow (x^p)^q + (y^p)^q = (z^p)^q$$

$$x^p = a; y^p = b; z^p = c$$

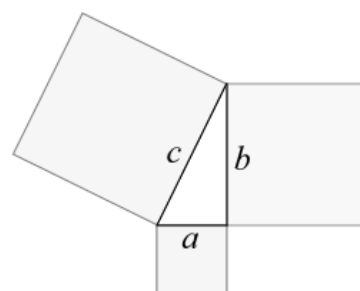
$$a^q + b^q = c^q \rightarrow \frac{a^q}{q} + \frac{b^q}{q} = \frac{c^q}{q}$$

Som det bevisades i de fyra första hjälpsatserna har det ingen betydelse hur variablerna x och y också a och b förhåller sig storleksmässigt till exponenten n . Man vet från tidigare att $c = z^p$ och om $c \notin \mathbb{Q}$ kan inte heller p -roten ur den bli ett heltal. Av samma resonemang kan man ytterligare generalisera hjälpsatsen och säga att Fermats stora sats saknar heltals lösningar även om n är en produkt av flera primtal.

■

Eftersom hittills i ansatsen har man fokuserat på de tillfällen där Fermats stora sats inte är definierad, kanske ifrågasätter man huruvida bevismetoden är rätt. Därför kan man prova Fermats stora sats då n är lika med två d.v.s. enligt Pytagoras sats, $a^2 + b^2 = c^2$, och rättare sagt en pythagoreisk trippel d.v.s. då alla sidorna är heltal.

Pythagoreisk trippel har många speciella egenskaper bl.a. att en av a eller b är udda och c är alltid ett udda tal. Ytterligare en egenskap för en pythagoreisk trippel är att antingen a eller b kommer att vara delbart med 3. Vilket i sin tur kan bevisas med det lämnas till intresserade läsare.



Figur 4 - Pythagoreisk trippel

Bevisa med hjälp av Fermats lilla sats att pythagoreiska tripplar finns och dessutom oändligt många.

$$n = p - 1 \text{ och } p = 3. n = 2$$

$x \nmid 3$; man kunde lika gärna påstå att y delar 3.

$$\frac{x^2}{3} + \frac{y^2}{3} = \frac{c^2}{3}$$

$$x^2 + y^2 \equiv 0 + 1 \pmod{3}; z^2 \equiv 1 \pmod{3}$$

$$VL = HL; 1 = 1, \text{ Resultat från kongruensuträkningen}$$

Att $VL = HL$ är en självklarhet och därför visas det att Fermats lilla sats fungerar när det inte skapar paradoxer i den matematiska världen. Med hjälp av hjälpsatserna 4.1 till 4.8 bevisas med motsägelsebevis att en övervägande del av Fermats stora sats stämmer.

Anledning till att beviset inte är komplett är p.g.a. två obevisade scenarier, ena är då när antingen när $x + y = p$ t.ex. $3^7 + 4^7$ eller när resterna från x och y kongruens med p är lika med exponenten som är ett primtal, t.ex. $10^7 + 11^7$. Därmed bevisas stora delar av Fermats lilla sats med hjälp av Fermats lilla sats.



Hittills har matematiker inte kunnat hitta andra sätt att förklara och därmed bevisa Fermats stora sats. Den här ansatsen visar att man hela tiden kan sträva efter att hitta nya vägar i matematiken och använda befintliga kunskaper för att applicera dem i ett nytt område som ingen tidigare har gjort.

Det presenterade beviset är inte komplett men med tanke på den stora satsens långa historia och alla misslyckade försök är ansatsen ett positivt försök. Om någon i framtiden, likt Andrew Wiles, lyckas knäcka den troligtvis sista scenarion har hon eller han bevisat Fermats stora sats i en mycket enklare form med kunskaper som var aktuella under Fermats tid.

Tillkännagivande

Det här arbetet hade inte varit möjligt utan flera personers hjälp och engagemang. Först och främst vill jag tacka mina matematiklärare på Kungsholmens gymnasium, Markus Karlsson och Lena Comstedt Ekelund, dels för den stabila grunden de har givit mig i matematik och dels för deras uppmuntran till att tänka själv och prova nya vägar i matematik. Jag vill rikta ett stort tack till doktoranden Thomas Ohlson Timoudas vid Matematiska institutionen på KTH för uppmuntran, värdefulla diskussioner och hans noggrannhet och ärlighet vid granskning av ansatsen till beviset för Fermats stora sats. Denna handledning skulle inte vara möjligt utan Roy M Skjelnes, (universitetslektor vid KTH) initiativ till stöd från KTH:s institution för Matematik. Jag vill även tacka min handledare Helena Danielsson Thorell, kemilektor och matematiklärare, på Kungsholmens gymnasium, som har lärt mig forskningens grundstenar. Tack slutligen till Maria Suchowiak för hennes hjälp i författandet av rapporten.

Litteraturförteckning

- de Fermat, P. (den 18 10 1640). *https://web.archive.org/*. Hämtat från <https://web.archive.org/web/20061222105104/http://www.cs.utexas.edu/users/wzhao/fermat2.pdf> den 10 12 2013
- Nationalencyklopedin. (2013). *NE Pierre de Fermat*. Hämtat från <http://www.ne.se/lang/pierre-de-fermat> den 06 11 2013
- Persson, U. (2013). *NE diofantisk ekvation*. Hämtat från <http://www.ne.se/diofantisk-ekvation> den 06 11 2013
- Persson, U. (2013). *NE Fermats förmodan*. Hämtat från <http://www.ne.se/lang/fermats-f%C3%B6rmodan> den 06 11 2013
- Singh, S. (1997). *Fermats Gåta, Historien om hur världens svåraste matematiska problem löstes*. Nordstedts Förlag.