UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2019:19

Vilka tal kan skrivas som en summa av två kvadrater?

Sofie Eiderfors

Examensarbete i matematik, 15 hp
Handledare: Gunnar Berg
Examinator: Veronica Crispin Quinonez
Juni 2019

Department of Mathematics
Uppsala University

Innehåll

1 Inledning

1.1 Introduktion

Denna uppsats har för avsikt att skapa en överblick av de klassiska teorem som behandlar summor av kvadrater och att empiriskt undersöka och resonera kring vilka tal som kan skrivas som en summa av två kvadrater. Fokus för uppsatsen kommer att ligga på att analysera Don Zagiers version av Fermats bevis för vilka tal som kan skrivas som en summa av två kvadrater. Detta kommer att kompletteras med några översiktliga genomgångar av relaterade bevis. Slutligen kommer bevisen att diskuteras och sättas in i ett aktuellt vetenskapligt sammanhang.[1]

1.2 Historisk bakgrund

Kvadrattal har länge varit föremål för intresse hos många matematiker. Studier om summor och kvadrattal inom talteorin dateras tillbaka till antiken. Bland Pythagoréerna fanns exempelvis ett intresse för figurativa tal såsom kvadrattal, triangeltal och pentagonala tal. I Euklides Elementa byggde Euklides upp talteorin från grunden genom att systematiskt införa begrepp som exempelvis primtal och delbarhet. Ett av Euklides viktigaste bidrag till framtida framsteg inom talteorin var utvecklandet av matematiska redskap såsom divisionsalgoritmen, vilken ligger till grund för exempelvis kongruensräknandet och Euklides algoritm.

En annan tidigt verksam matematiker som var aktiv inom talteorin var Diophantus. Från sitt säte i Alexandria utvecklade han metoder för att lösa olika talteoretiska problem. Inom detta intresserade han sig särskilt för så kallade diofantiska ekvationer. Han arbetade även med representation av tal som potenser. Diofantos visste till exempel att tal på formen $8n + 7$ inte kan skrivas som en summa av tre kvadrater.[2] När Diophantos texter översattes till latin och trycktes kom även dessa att inspirera och bidra till framtida framsteg av summor av kvadrater inom talteorin.[3]

En matematiker som lät sig inspireras av Diophantos verk var Pierre de Fermat. Fermat var verksam under 1600–talet och blev den som först myntade påståendet att samtliga tal kan skrivas som en summa av fyra kvadrater. Det

[1] Zagier (1990), s. 144.
[2] van der Waerden (1963), s. 279.
[3] Weil (2006), ss. 11–12.

kom dock att dröja innan ett bevis för detta fördes fram. Euler spenderade 40 år med att försöka bevisa Fermats teorem, utan att lyckas helt. Det var Lagrange som med hjälp av Eulers arbete slutligen lyckades ta fram ett fullständigt bevis för att alla tal kan skrivas som en summa av fyra kvadrater.[4]

Men något Fermat kanske är mer känd för är hans teorem att alla primtal som kan skrivas på formen $4n + 1$ är en summa av två kvadrater. Med hjälp av metoden "infinite descent"kunde Fermat producera ett bevis för teoremet. Sedan dess har flera alternativa bevis för teoremet tagits fram av olika matematiker. Euler publicerade ett bevis för teoremet år 1754/5 av sådan karaktär att det inte följde de riktlinjer Fermat hade tänkt sig. Ett mer modernt bevis publicerades år 1990 av Don Zagier, i ett försök att sammanfatta detta omfattande bevis i endast en mening.[5]

1.3 De första 30 positiva heltalen som en summa av två kvadrater

Vilka tal kan skrivas som summan av två kvadrater? Låt oss undersöka Fermat theorem lite närmare och se om vi kan besvara frågan. Vi börjar med att undersöka de första 30 positiva heltalen. Vi ser då att talen 1 och 2 kan skrivas som summan av två kvadrater eftersom $1 = 1^2 + 0^2$ och $2 = 1^2 + 1^2$. Talet 3 däremot saknar möjlighet att skrivas som summan av två kvadrater. Vi sammanställer en tabell över de 30 första positiva heltalen för att se om det är möjligt att finna ett mönster som beskriver vilka tal som kan skrivas som summan av två kvadrater, se tabell 1.

För att göra processen mer överskådlig delar vi in alla heltal n i fyra grupper. Dessa är heltal som kan skrivas på formen $4n, 4n+1, 4n+2$ eller $4n+3$. Det vill säga när ett heltal n delas med 4 får vi resten 0, 1, 2 eller 3. Samtliga primtal ligger i grupperna $4n + 1$ och $4n + 3$, med undantag för primtalet 2 som skrivs på formen $4n + 2$. Denna indelning av n kommer vi att arbeta med i senare kapitel, då kvadrattal och deras summor behandlas. I tabellen nedan kan vi se vilken form de 30 första positiva heltalen skrivs på.

[4]Kline (1990), s. 609.
[5]Zagier (1990), s. 144; Kline (1990), s. 609.

Tabell 1: *Detta är en tabell över de första 30 positiva heltalen n med angiven form och skrivna som en summa av två kvadrater, om möjligt.*

De första 30 positiva heltalen					
n	Kvadrater	Form	n	Kvadrater	Form
1	$1^2 + 0^2$	$4n + 1$	16	$4^2 + 0^2$	$4n$
2	$1^2 + 1^2$	$4n + 2$	17	$4^2 + 1^2$	$4n + 1$
3	-	$4n + 3$	18	$3^2 + 3^2$	$4n + 2$
4	$2^2 + 0^2$	$4n$	19	-	$4n + 3$
5	$2^2 + 1^2$	$4n + 1$	20	$4^2 + 2^2$	$4n$
6	-	$4n + 2$	21	-	$4n + 1$
7	-	$4n + 3$	22	-	$4n + 2$
8	$2^2 + 2^2$	$4n$	23	-	$4n + 3$
9	$3^2 + 0^2$	$4n + 1$	24	-	$4n$
10	$3^2 + 1^2$	$4n + 2$	25	$4^2 + 3^2$	$4n + 1$
11	-	$4n + 3$	26	$5^2 + 1^2$	$4n + 2$
12	-	$4n$	27	-	$4n + 3$
13	$3^2 + 2^2$	$4n + 1$	28	-	$4n$
14	-	$4n + 2$	29	$5^2 + 2^2$	$4n + 1$
15	-	$4n + 3$	30	-	$4n + 2$

I tabell 1 ser vi att ett samband verkar existera mellan heltalets form och dess benägenhet att kunna skrivas som en summa av två kvadrater. Exempelvis ser vi att heltal på formen $4n+3$ i samtliga fall inte kan skrivas som en summa av två kvadrater. Vi skapar en hypotes: *Inga heltal på formen* $4n + 3$ *kan skrivas som en summa av två kvadrater.*

Vi ser även att de heltal i tabellen som skrivs på formen $4n + 1$ ofta verkar kunna skrivas som summan av två kvadrater. Av de 30 första positiva heltalen som vi har med i tabell 1 ser vi att 1, 5, 9 ,13, 17, 25 och 29 kan skrivas som summan av två kvadrater. Däremot kan talet 21 inte det. Vi frågar oss vad det kan bero på. I tabellen ser vi att många av talen på formen $4n+1$ är primtal. Talet 21 som inte kan skrivas som summan av två kvadrater är dock inte det.

Baserat på detta formulerar vi en andra hypotes: *Alla primtal på formen* $4n + 1$ *kan skrivas som en summa av två kvadrater.* Dessa två hypoteser kommer vi att testa i nästa kapitel. Vi kommer dessutom att undersöka huruvida ett samband existerar mellan övriga naturliga tal och tal som skrivs som summan av två kvadrater.

2 Primtal som summan av två kvadrater

Följande kapitel kommer att behandla de bevis som redogör för primtalens benägenhet att kunna skrivas som en summa av två kvadrater. Därmed kommer vi att söka svar på våra två hypoteser från föregående kapitel, vilka behandlas i respektive delkapitel.

2.1 Primtal på formen 4n+1

Vi börjar med att undersöka primtalen på formen $4n + 1$. Låt p vara ett primtal på formen $4n + 1$ och bilda mängden S av taltrippler (x, y, z) i N^3 sådana att $x^2 + 4yz = p$. Då kan vi först konstatera att vår mängd S inte är tom eftersom taltripplerna $(1, n, 1)$ och $(1, 1, n)$ ger $p = 4n + 1$ och därmed ingår i S. Vi kan även undersöka några exempel på fler taltrippler som ligger i mängden S.

$p = 5$	$x^2 + 4yz = 5$
$(4 \cdot 1 + 1)$	$S = \{(1, 1, 1)\}$
$p = 13$	$x^2 + 4yz = 13$
$(4 \cdot 3 + 1)$	$S = \{(1, 1, 3), (1, 3, 1), (3, 1, 1)\}$
$p = 17$	$x^2 + 4yz = 17$
$(4 \cdot 4 + 1)$	$S = \{(1, 1, 4), (1, 4, 1), (3, 1, 2), (3, 2, 1), (1, 2, 2)\}$
$p = 29$	$x^2 + 4yz = 29$
$(4 \cdot 7 + 1)$	$S = \{(1, 1, 7), (1, 7, 1), (3, 5, 1), (3, 1, 5), (5, 1, 1)\}$

Uträkningarna ovan visar en intressant faktor. Vi ser nämligen att mängderna i S alltid består av ett udda antar taltrippler. Primtalet 5 kan bara skrivas på

ett sätt och har alltså endast taltripplen $(1,1,1)$. Primtalet 13 kan skrivas på tre olika sätt med taltripplerna $(1,1,3)$, $(1,3,1)$ och $(3,1,1)$. Om så är fallet att S alltid består av udda taltrippler, är detta en faktor av stor relevans för vårt bevis. Låt oss därför gå vidare med våra beräkningar för att se om vi kan visa att S innehåller ett udda antal taltrippler.

Nästa steg är att dela in N i tre klasser I, II och III, där x avgränsas av $y-z$ och $2y$. Vi ser då att $x \neq y-z$, eftersom $x = y-z$ ger $x^2+4yz = (y-z)^2+4yz = y^2+z^2-2yz+4yz = y^2+z^2+2yz = (y+z)^2 \neq p$, eftersom ett primtal aldrig kan skrivas som ett kvadrattal. Vi ser även att $x \neq 2y$ eftersom $x = 2y$ ger $x^2+4yz = 4y^2+4yz = 4y(y+4z) \neq p$, eftersom ett primtal inte kan vara en multipel av fyra. Vi har därmed utnyttjat egenskaper hos ett primtal för att dra slutsatser om mängden S.

Vi kan även se att inget av talen x, y, z kan vara lika med noll. Att $x = 0$ ger $x^2+4yz = 0+4yz = 4yz \neq p$, eftersom ett primtal inte kan vara en multipel av fyra. Likaså ger $(y,z) = (0,0)$ istället att $x^2+4yz = x^2+0 \neq p$, eftersom ett primtal aldrig inte kan skrivas som ett kvadrattal. Återigen har vi använt oss av primtalens egenskaper för att dra slutsatser om mängden S.

Nu återvänder vi till vår mängd $S = \{(x,y,z) \in N^3 : x^2+4yz = p\}$. Eftersom alla tal i S är $\leq p$ kan vi även konstatera att mängden S är ändlig.

Låt sedan (x,y,z) avbildas enligt:

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{om } x < y-z \\ (2y-x, y, x-y+z) & \text{om } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{om } x > 2y \end{cases}$$

där villkoren representerar klasserna I, II och III. Då är $Im(S) \subset S$, det vill säga bilden av S är då en delmängd av S. Nedanstående beräkningar visar detta.

Klass I : $(x+2z)^2+4z(y-x-z) = x^2+\cancel{4xz}+\cancel{4z^2}+4zy-\cancel{4zx}-\cancel{4z^2} = x^2+4yz = p$

Klass II : $(2y-x)^2+4y(x-y+z) = \cancel{4y^2}-\cancel{4xy}+x^2+\cancel{4yx}-\cancel{4y^2}+4yz = x^2+4yz = p$

Klass III : $(x-2y^2)+4y(x-y+z) = x^2-\cancel{4yx}+\cancel{4y^2}+\cancel{4yx}-\cancel{4y^2}+4yz = x^2+4yz = p$

Nästa steg är att undersöka vad som händer med våra klasser då funktionen appliceras. Låt exempelvis (x, y, z) representera en uppsättning taltrippler som uppfyller villkoret $x < y - z$. Taltripplen befinner sig därmed per definition i klass I. Appliceras funktionen får vi $(x + 2z, z, y - x - z)$ vilket ligger i klass III, det vill säga där alla $x > 2y$. Vi ser nämligen att $x = x + 2z$ är större än $2y = 2z$. På samma sätt då vi låter (x, y, z) representera en uppsättning taltrippler som uppfyller villkoret $x > 2y$ för alla tal i klass III kan vi se att dessa avbildas på klass I. Appliceras funktionen får vi nämligen $x - 2y, x - y + z, y$, vilket ligger i klass I, där alla $x < y - z$. Detta eftersom vi ser att $x = x - 2y$ vilket är mindre än $y - z$ som i detta fall är $(x - y + z) - y = x - 2y + z$. Alltså ser vi att klass I avbildas på klass III och klass III avbildas på klass I av funktionen.

Undersöks klass II på samma sätt stöter vi på en intressant variation. Låt (x, y, z) representera en uppsättning taltrippler som uppfyller vilkoret $y - z < x < 2y$. Taltripplen befinner sig därmed per definition i klass II. Appliceras funktionen ger detta $(2y - x, y, x - y + z)$, vilket även det ligger i klass II. Vi ser nämligen att $y - z = y - (x - y + z) = 2y - x - z$ är mindre än $x = 2y - x$. Dessutom ser vi att x är mindre än $2y$. Alla tal i klass II avbildas därmed på sig själv efter att funktionen appliceras. Figuren nedan visar slutsatserna vi hittills har dragit.

$$\begin{cases} I \to III \\ II \to II \\ III \to I \end{cases}$$

Nu ställer vi oss frågan; vad händer då funktionen appliceras ytterligare en gång? Återupprepas processen på avbildningen av klass I $(x+2z, z, y-x-z)$, som vi tidigare konstaterat ligger i klass III, får vi återigen (x, y, z), vilka vi vet uppfyller villkoret $x < y-z$. Vi är alltså tillbaka i klass I efter att funktionen appliceras två gånger på taltripplerna (x, y, z) placerade i klass I. Motsvarande sker då funktionen appliceras ytterligare en gång på avbildningen av klass III $(x-2y, x-y+z, y)$, vilken ligger i klass I. Dess avbildning bildar (x, y, z), och vi är tillbaka i klass III. Klass II vet vi avbildas på sig själv redan efter ett steg. Appliceras funktionen igen på avbildningen $(2y-x, y, x-y+z)$ får vi även här (x, y, z), vilken ligger i klass II. Beräkningarna nedan visar samtliga steg för klassernas avbildningar.

$$\text{I} : (x, y, z) \to (x+2z, z, y-x-z) \to (x+\cancel{2z}-\cancel{2z}, \cancel{x}+\cancel{2z}-\cancel{z}+y-\cancel{x}-\cancel{z}, z) = (x, y, z)$$

$$\text{II} : (x, y, z) \to (2y-x, y, x-y+z) \to (\cancel{2y}-\cancel{2y}+x, y, \cancel{2y}-\cancel{x}-\cancel{y}+\cancel{x}-\cancel{y}+z) = (x, y, z)$$

$$\text{III} : (x, y, z) \to (x-2y, x-y+z, y) \to (x-\cancel{2y}+\cancel{2y}, y, \cancel{x}-\cancel{y}+z-\cancel{x}+\cancel{2y}-\cancel{y}) = (x, y, z)$$

Vi har nu visat att varje element i S avbildas på sig själv då funktionen appliceras två gånger. Figuren nedan visar avbildningarna av funktionen.

$$\begin{cases} I \to III \to I \\ II \to II \to II \\ III \to I \to III \end{cases}$$

Det har blivit dags att införa en definition. En funktion som *avbildar varje element på sig själv efter att funktionen upprepas två gånger* kallas för en *involution*. Klasserna för vår ekvation avbildas på sig själva efter två steg. Klass I avbildas på klass III och klass III avbildas på klass I. Klass II stannar alltid i samma mängd då den avbildas på sig själv redan efter ett steg. Våra tidigare beräkningar visar att villkoren för en involution gäller. Detta kan även uttryckas som $f(a) = b$ och $f(f(a)) = a$ av vilket följer att $f(b) = a$. Vår funktion kan vi därmed konstatera är en involution.

Antag också att vår funktion har en *fixpunkt*. En fixpunkt är en punkt som *alltid avbildas på sig själv av en funktion, sådan att* $f(a) = a$. En fixpunkt i vår ekvation måste därmed finnas i mängd II, eftersom detta är det enda stället där $f(a) = a$ kan vara möjligt. Vi undersöker om det stämmer att $(x, y, z) \to (2y - x, y, x - y + z) = (x, y, z)$ genom att ställa upp ekvationen elementvis.

$$\begin{cases} x = 2y - x \Rightarrow 2x = 2y \Rightarrow x = y \\ y = y \\ z = x - y + z \Rightarrow z = y - y + z \Rightarrow z = z \end{cases}$$

Vi ser direkt att $y = y$. Det framgår även att $x = y$, av vilket följer at $z = z$. Alltså vet vi att alla punkter av typen (x, x, z) är fix.

Villkoret $x^2 + 4yz = p$ kan som en följd av ovanstående slutsats skrivas som $x^2 + 4xz = p \Rightarrow x(1 + 4z) = p$. Från detta kan vi lösa ut endast ett möjligt

värde på x. Vi vet nämligen att p är nollskild, alltså kan x inte vara 0. Dessutom vet vi att p är ett primtal, vilket betyder att p endast är delbart med sig själv och med talet 1. Eftersom alla tal i S är $\leq p$ får vi att $x = 1$.

Av $x = 1$ följer att $y = 1$ eftersom $y = x$. Kvar av vårt villkor har vi dessutom $1 \cdot (1+4z) = p \Rightarrow (4z+1) = p$. Detta är då skrivet på samma form som primtal av formen $4n + 1$. Alltså är $z = n$. Av detta ser vi att vår funktion har exakt en fixpunkt i $(1, 1, n)$.

Eftersom funktionen är en involution kommer samtliga element, som tidigare nämnts, att avbildas på sig själv efter två steg. Detta skrivs $f(f(a)) = a$. Då $f(a) = b$ och $f(b) = f(f(a)) = a$ kan varje element i S sägas byta plats med ett annat element i S, för att sedan byta tillbaka till sin ursprungsplats. En involution som inte innehåller någon fixpunkt skulle därmed nödvändigtvis vara definierad på en mängd med ett jämnt antal element. Eftersom vi precis har visat att S innehåller exakt en fixpunkt medför detta att S har ett udda antal element, eftersom 1 är ett udda tal. Därmed vet vi att S innehåller ett udda antal taltrippler. Vi har därmed visat det våra inledande exempel antydde i början av detta kapitel. Kan vi nu använda denna information att S innehåller ett udda antal element till något mer konkret?

Vi vet nu att S är en involution med exakt en fixpunkt och att S därmed är udda eftersom en fixpunkt medför ett udda antal taltrippler i mängden. Låt oss nu bilda en ny funktion F på $S : (x, y, z) \mapsto (x, z, y)$. Detta ser vi är en involution eftersom $(x, y, z) \mapsto (x, z, y) \mapsto (x, y, z)$. Eftersom vi vet att S dessutom innehåller ett udda antal element måste F i enlighet med resonemanget ovan innehålla minst en fixpunkt. Vi kallar den för (a, b, c). För denna gäller att $(a, b, c) \mapsto (a, c, b) = (a, b, c)$. Alltså är $b = c$. Villkoret $x^2 + 4yz = p$ kan i detta särskilda fall då skrivas $a^2 + 4b^2 = p$ eller som summan av två kvadrater $a^2 + (2b)^2 = p$. Eftersom ekvationen är udda gäller detta för samtliga p. Vi har nu visat att p, och därmed alla tal på formen $4n+1$, kan skrivas som en summa av två kvadrater. □

2.2 Primtal på formen 4n+3

Vi har nu visat att alla primtal på formen $4n + 1$ kan skrivas som en summa av två kvadrater. Men hur är det med primtalen på formen $4n + 3$? I tabell 1 såg vi att heltal på formen $4n + 3$ tenderade att inte kunna skrivas som summan av två kvadrater. Låt oss undersöka om detta stämmer.

Det första vi behöver göra är att undersöka resterna då ett kvadrattal divideras med fyra. Vi utgår med andra ord från fyra grupper av heltal på formerna $4n$, $4n+1$, $4n+2$ och $4n+3$.

$4n$	$(4n)^2 + 0 = 4[\,] + \underline{0}$
$4n+1$	$(4n+1)^2 = 16n^2 + 8n + 1 = 4[\,] + \underline{1}$
$4n+2$	$(4n+2)^2 = 16n^2 + 16n + 4 = 4[\,] + \underline{0}$
$4n+3$	$(4n+3)^2 = 16n^2 + 24n + 9 = 16n^2 + 24n + 8 + 1 = 4[\,] + \underline{1}$

Uträkningarna visar att de enda möjliga resterna av kvadrattal vid division med fyra är 0 eller 1. Summan av två av dessa rester, exempelvis $0 + 1$ kan bilda talen 0, 1 eller 2. De kan dock aldrig bli 3, eftersom $1 + 1 = 2$ är det högsta möjliga talet. Detta stämmer överens med vår inledande hypotes och vi har därmed visat att primtal på formen $4n + 3$ aldrig kan skrivas som summan av två kvadrater.[6] □

En viktig anmärkning är att detta bevis till skillnad från beviset om primtal på formen $4n + 1$ aldrig krävde användning av primtals egenskaper för att bevisas. Alltså gäller detta bevis inte bara för primtalen, utan för samtliga tal som kan skrivas på formen $4n + 3$. Vi har därmed visat att vår hypotes från inledningen, att alla heltal på formen $4n + 3$ kan skrivas som en summa av två kvadrater är sann.

3 Sammansatta tal som summan av två kvadrater

Vi har nu tittat närmare på vilka primtal som kan skrivas som summan av två kvadrater. För att få en bild av samtliga godtyckliga naturliga heltal som kvadrattal behöver vi även inkludera de sammansatta talen. Vi tar hjälp av några satser för att få klarhet i saken.

3.1 Tillräckliga villkor

I tabell 1 i uppsatsens inledning kan vi se att talet 1 kan skrivas som en summa av $1^2 + 0^2$. Talet 2 är på samma sätt summan av $1^2 + 1^2$. Talet 3 har vi precis visat är ett tal på formen $4n + 3$ och kan därmed aldrig skrivas som

[6] Lindahl (2002), s. 52.

en summa av två kvadrater. Men hur är det med produkten av talet 1 och 2, vilka vi vet kan skrivas som summan av två kvadrater? Låt oss räkna på saken. Vi testar även att multiplicera två andra kända kvadrattal, nämligen talet 4 med talet 5.

$$1 \cdot 2 = (1^2 + 1^2) \cdot (0^2 + 1^2) = (0 + 1) + (1 + 0) = 2$$
$$4 \cdot 5 = (2^2 + 0^2) \cdot (2^2 + 1^2) = (16 + 0) + (4 + 0) = 20$$

Produkten av våra kända kvadrattal bildar talen 2 och 20, vilka vi från tabell 1 känner igen som tal som kan skriva som summan av två kvadrater. Vi drar slutsatsen att om två tal skrivas som summan av två kvadrater, verkar även deras produkt kunna det. Låt oss betrakta det generella fallet. Låt $m = a^2+b^2$ och $n = c^2 + d^2$. Då är $m \cdot n = (a^2 + b^2) \cdot (c^2 + b^2) = (ac + bd)^2 + (ad - cb)^2$ vilket är en summa av två kvadrater. Alltså har vi nu visat att produkten av två tal som kan skrivas som en summa av två kvadrater även den alltid kan skrivas som en summa av två kvadrater. Låt oss demonstrera detta med ett räkneexempel. Talet 234 kan exempelvis skrivas som produkten av $2 \cdot 3^2 \cdot 13$. Vi får då att:

$$2 \cdot 3^2 \cdot 13 = (1^2 + 1^2) \cdot (3^2 + 0^2) \cdot (2^2 + 3^2) = 3^2((1^2 + 1^2) \cdot (3^2 + 0^2) =$$
$$3^2((1 \cdot 2 + 1 \cdot 3)^2 + (1 \cdot 3 - 1 \cdot 2)^2) = 3^2(5^2 + 1^2) = (3 \cdot 5)^2 + (3 \cdot 1)^2 = 15^2 + 3^2$$

Nästa sats vi behöver visa är att om n är en summa av två kvadrater så är nx^2 också en summa av två kvadrater. Vi ser nämligen att $n = a^2 + b^2$ ger $nx^2 = (xa)^2 + (xb)^2$. Detsamma gäller för alla x med en jämn exponent, eftersom jämna exponenter är kvadrater av en kvadrat. Detta gäller samtliga tal x, även tal på formen $4n + 3$, som vi tidigare visat aldrig kan skrivas som en summa av två kvadrater.

En första slutsats vi kan dra av ovanstående satser är att ett naturligt tal N är en summa av två kvadrater om eventuella primfaktorer av formen $4n + 3$ förekommer med jämn exponent i primtalsframställningen av N.[7]

3.2 Nödvändiga villkor

Det som återstår att visa är att det endast är dessa tal som kan skrivas som en summa av två kvadrater. Detta bygger på hjälpsatsen att om $p = 4n+3$ är ett primtal som delar $n = a^2+b^2$ så kommer även p^2 att dela n. Vi vill nu visa

[7]Martin Aigner (2010), s. 23.

att p delar a och att p delar b, nämligen $p \mid a$ och $p \mid b$ vilket medför resultatet.

Antag att $p \nmid a$, vilket innebär att största gemensamma delaren $SGD(a, p) = 1$. Då finns heltal m_0 och n_0 sådana att $m_0 p + n_0 a = 1$. Detta är nämligen en konsekvens av Euklides algoritm. Om $p \mid a^2 + b^2$ så följer att $a^2 + b^2 \equiv 0$ (mod p) och multiplikation med n_0 ger $(n_0 a)^2 + (n_0 b)^2 \equiv 0$ (mod p). Men $m_0 p + n_0 a = 1$ ger att $n_0 a \equiv 1$ (mod p). Alltså har vi $1 + (n_0 b)^2 \equiv 0$ (mod p), vilket innebär att det finns ett heltal $(n_0 b)^2$, låt oss kalla det för c, sådant att $c^2 + 1 \equiv 0$ (mod p). Detta är dock omöjligt om p är ett primtal på formen $4n + 3$.[8]

Vår andra slutsats blir därmed att $p \mid a$. På samma sätt kan vi även visa att $p \mid b$. Alltså har vi visat att precis de sammansatta tal som antingen inte innehåller något primtal på formen $4n+3$, eller de tal som innehåller primfaktorer med jämn potens på formen $4n+3$, som kan skrivas som en summa av två kvadrater. Vi har därmed bestämt samtliga tal som kan skrivas som summan av två kvadrater. □

4 Vidareutvecklingar

4.1 Summan av tre kvadrater

Liksom Pythagoréerna intresserade sig för kvadrattal och triangeltal på fler former än två kvadrater, kan det även för denna uppsats vara intressant att gå in på summor av fler än två kvadrater. Som nämnts i inledningen kan vi med Lagranges teorem visa att samtliga naturliga tal kan skrivas som en summa av fyra kvadrater. Men hur är det med summan av tre kvadrater? Vi kommer kort att gå in på delar av beviset för tal som kan skrivas som en summa av tre kvadrater för att demonstrera likheten mellan detta och bevisen vi vi avhandlat ovan som berör summan av två kvadrater.

För att utreda vilka heltal som kan skrivas som en summa av tre kvadrater börjar vi med att undersöka resterna då ett kvadrattal divideras med åtta.

[8] Lindahl (2002), s. 38.

$8n$	$(8n)^2 = 8[\,] + 0$
$8n+1$	$(8n+1)^2 = 84n^2 + 16n + 1 = 8[\,] + 1$
$8n+2$	$(8n+2)^2 = 84n^2 + 32n + 4 = 8[\,] + 4$
$8n+3$	$(8n+3)^2 = 84n^2 + 48n + 9 = 8[\,] + 1$
$8n+4$	$(8n+4)^2 = 84n^2 + 64n + 16 = 8[\,] + 0$
$8n+5$	$(8n+5)^2 = 84n^2 + 80n + 25 = 8[\,] + 1$
$8n+6$	$(8n+6)^2 = 84n^2 + 96n + 36 = 8[\,] + 4$
$8n+7$	$(8n+7)^2 = 84n^2 + 112n + 49 = 8[\,] + 1$

Studeras dessa uträkningar ser vi att resterna 0, 1 och 4 är de enda möjliga utfallen. Vi undersöker vilka tal vi har möjlighet att bilda av dessa rester genom att addera tre av dem. Vi ser att vi kan bilda talen 1, 2, 3, 4, 5 och 6 genom addition av tre av resterna från kvadrattalen. Talet 7 är inte möjligt att bilda med hjälp av dessa rester. Se uträkningarna nedan.

$$0 = 0 + 0 + 0$$

$$1 = 1 + 0 + 0$$

$$2 = 1 + 1 + 0$$

$$3 = 1 + 1 + 1$$

$$4 = 4 + 0 + 0$$

$$5 = 4 + 1 + 0$$

$$6 = 4 + 1 + 1$$

$$7 = \text{ej möjlig}$$

Vi har därmed visat att inga tal på formen $8n+7$ kan skrivas som en summa av tre kvadrater. Vi kan vidare konstatera att om ett tal n som är delbart med 4 är en summa av tre kvadrater, gäller detta även för talet $n/4$. Vi visar detta genom att låta $n = x^2 + y^2 + z^2$ och antagandet att 4 delar n. Då är n jämnt och vi får två möjliga fall.

Fall 1: Talen x, y och z är jämna. Sätt $x = 2a$, $y = 2b$ och $z = 2c$. Vi får då att $n = (2x)^2 + (2y)^2 + (2z)^2 = 4x^2 + 4y^2 + 4z^2$. Av detta följer att $n/4 = x^2 + y^2 + z^2$.

Fall 2: Två av talen x, y och z är udda. Antag att $x = 2n + 1, y = 2p + 1$ och $z = 2q$. Vi får då att $n = x^2 + y^2 + z^2 = (2m + 1)^2 + (2p + 1)^2 + (2q)^2 = 4m^2 + 4m + 1 + 4p^2 + 4p + 1 + 4q^2 = 4(m^2 + m + p^2 + p + q^2) + 2$. Detta tal kan inte vara delbart med 4, alltså måste x,y och z vara jämna. Av detta följer att inget tal på formen $4^n(8n+7)$ är en summa av tre kvadrater. □

Vi ser att metoden för att bevisa att talen på formen $8n + 7$ inte kan skrivas som en summa av tre kvadrater nästan är densamma som den vi använde i föregående kapitel för att bevisa att inga heltal på formen $4n + 3$ kan skrivas som en summa av två kvadrater. Resterande tal kan, det vill säga alla tal utom de tal som skrivs på formen $8n + 7$ kan skrivas som summan av tre kvadrater. Beviset för detta kommer vi dock inte att gå in närmare på i denna uppsats. Liksom teoremen som rör summan av två eller fyra kvadrater myntades även teoremet om tre kvadrater ursprungligen av Fermat. Densamme producerade även ett ofullständigt bevis av teoremet, vilket år 1801 kom att kompletteras av Legendre.[9]

4.2 Vidare forskning och slutsats

I denna uppsats har vi djupdykt i ett par bevis som rör kvadrater och deras summor. Vi har därmed fått en viss inblick i representation av tal som summor av kvadrater som ett matematiskt fält och inte minst dess plats i ett historiskt perspektiv. Det är dock än idag ett område som fångar många moderna matematikers intresse.

Ett aktuellt område inom talteorin är Warings problem som behandlar framställning av naturliga tal som en summa av kvadrater, tredjepotenser och fjärdepotenser med flera. Waring påstod utan bevis att varje heltal är en summa av som mest 19 fjärdepotenser. Han framlade också den mer generella hypotesen att det till varje heltal k finns ett heltal $s(k)$ sådant att varje heltal är en summa av $s(k)$ stycken k-potenser. Exempelvis är $s(2) = 4$, $s(3) = 9$ och $s(4) = 19$. David Hilbert visade 1909 existensen av talen $s(k)$ men det har bara hittats exakta värden på talen $s(k)$ för ett fåtal värden på k. Exempelvis vet vi att $s(5) = 37$. Detta är som resultat fortfarande ett aktivt forskningsområde än idag.[10]

Vi kan därmed se att trots att kvadrattal och summor må ha varit en gren inom talteorin som blomstrade som mest under antiken och 1600-1700-talen,

[9] Legendre (1797)

[10] Kline (1990), s. 609; Lindahl (2002), s. 55.

så finns det än idag outforskade områden som i framtiden kan förväntas producera spännande nya resultat.

Referenser

Kline, M. (1990), *Mathematical Thought from Ancient to Modern Times*, Vol. 2, Oxford University Press.

Legendre, A.-M. (1797), *Essai sur la théorie des nombres*, Paris.

Lindahl, L.-A. (2002), *Lectures on Number Theory*, Uppsala Universitet Matematiska Institutionen.

Martin Aigner, G. M. (2010), *Proofs from THE BOOK*, Freie Universitat Berlin.

van der Waerden, B. L. (1963), *Science awakening*, New York.

Weil, A. (2006), *Number Theory: An approach through history from Hammurapi to Legendre*, Springer Science and Business Media.

Zagier, D. (1990), 'A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares', *The American Mathematical Monthly* **97**, 144.