Getallen als de som van twee kwadraten

C.M.Madlener

1 april 2021

Wiskunde B
Hoofddorp

Inhoudsopgave

1 Samenvatting

Dit profielwerkstuk gaat over de getallen die te schrijven zijn als de som van twee kwadraten. Deze noem ik blije getallen. Het blijkt dat er een simpel trucje bestaat om direct aan een priemgetal te zien of het wel of niet schrijven is als de som van twee kwadraten. Zo ja, dan kan dit op exact één manier, dus die representatie is uniek voor het priemgetal. Hoewel wiskundige G.H.Hardy beweerde dat er geen eenvoudig bewijs bestaat hiervan, bleek het tegendeel waar te zijn.

De hoofdvraag van dit profielwerkstuk is: Welke natuurlijke getallen kunnen worden geschreven als de som van twee kwadraten en op hoeveel manieren kan dit?

Elk natuurlijk getal is op een unieke manier te schrijven als het product van priemgetallen, de priemontbinding. Deze kan gebruikt worden om het eerste deel van de hoofdvraag te beantwoorden. Het gaat daarbij om de priemfactoren die drie meer zijn dan een viervoud. Wanneer die priemfactoren allemaal een even aantal keer voorkomen in de priemontbinding van het getal, dan is het getal te schrijven als de som van twee kwadraten. Het blijkt ook dat dit een vereiste is voor een blij getal. Het is andersom dus ook waar.

Het aantal manieren om een natuurlijk getal te schrijven als de som van twee kwadraten, noem ik de kwadraticiteit. Deze kan worden bepaald aan de hand van de oneven delers van dat getal. Daarvoor wordt de helft van het verschil berekend tussen het aantal delers dat één meer is dan een viervoud en het aantal delers dat drie meer is dan een viervoud. Wanneer de uitkomst naar boven wordt afgerond, komt hieruit het aantal manieren om een natuurlijk getal te schrijven als de som van twee kwadraten.

2 Inleiding

In dit profielwerkstuk onderzoek ik de natuurlijke getallen die te schrijven zijn als de som van twee kwadraten.

Al een paar jaar geleden wist ik dat ik mijn profielwerkstuk zou gaan houden over een wiskundig onderwerp. Eind 2019 had ik gehoord dat alle priemgetallen in de vorm $4k+1$ te schrijven zijn als de som van twee kwadraten. Dit vond ik klinken als een mooie stelling, dus ik ging op internet zoeken naar de bewijzen daarvan. Die waren erg moeilijk en gebruikten veel technieken die ik niet kende. Een maand later kwam er een video online, waarin een relatief nieuw bewijs werd gepresenteerd. Dit bewijs was zo elegant, dat ik zelf ook onderzoek ging doen naar getallen die te schrijven zijn als de som van twee kwadraten. Uiteindelijk slaagde ik erin om op een begrijpelijke manier te bewijzen welke getallen wel of niet te schrijven waren als de som van twee kwadraten. Op dat moment wist ik waar mijn profielwerkstuk over zou gaan.

Mijn hoofdvraag is:
Welke natuurlijke getallen kunnen worden geschreven als de som van twee kwadraten en op hoeveel manieren kan dit?

Dit ga ik beantwoorden met behulp van drie vragen:
1. Welke priemgetallen kunnen worden geschreven als de som van twee kwadraten?
2. Welke natuurlijke getallen kunnen worden geschreven als de som van twee kwadraten?
3. Op hoeveel manieren kunnen natuurlijke getallen worden geschreven als de som van twee kwadraten?

Om dit profielwerkstuk zo toegankelijk mogelijk te maken, gebruik ik alleen technieken die weinig voorkennis vereisen en zal ik voor bijna al mijn gebruikte stellingen een bewijs leveren. Daarnaast zal ik veel stellingen voorzien van een voorbeeld en licht ik termen toe waarvan ik denk dat veel mensen niet weten wat ze betekenen. Ook ga ik alleen gebruik maken van gehele getallen. Verder heb ik besloten om sommige concepten die veel in de tekst voorkomen een korte naam te geven.

3 Priemgetallen als de som van twee kwadraten

In dit hoofdstuk ga ik me richten op priemgetallen. Priemgetallen zijn alle positieve gehele getallen, die alleen deelbaar zijn door 1 en zichzelf. Voorbeelden van priemgetallen zijn 2, 3 en 5. Andere getallen, zoals 1, 4 en 6, zijn geen priemgetal, want ze hebben minder of meer dan 2 delers.

In dit hoofdstuk laat ik zien welke priemgetallen te schrijven zijn als de som van twee kwadraten. Op het eerste gezicht hebben priemgetallen en kwadraten niet zo veel met elkaar te maken. Toch blijkt dat het eenvoudig is om aan een priemgetal te zien of het te schrijven is als de som van twee kwadraten. Er geldt namelijk dat alle priemgetallen op te schrijven zijn als de som van twee kwadraten, behalve de priemgetallen die een rest 3 hebben bij deling door 4.

Wanneer een priemgetal te schrijven is als de som van twee kwadraten, dan kan dat zelfs op een unieke manier. Dat bewijs zal ik hieronder toelichten. [Mat20]

3.1 De verschillende soorten priemgetallen

Om erachter te komen welke priemgetallen te schrijven zijn als de som van twee kwadraten, moeten we eerst kijken naar de kleine gevallen. We starten daarom met het onderzoeken van de priemgetallen kleiner dan 40.

We vinden:

$$2 = 1^2 + 1^2$$
$$3 \neq \square + \square$$
$$5 = 1^2 + 2^2$$
$$7 \neq \square + \square$$
$$11 \neq \square + \square$$
$$13 = 2^2 + 3^2$$
$$17 = 1^2 + 4^2$$
$$19 \neq \square + \square$$
$$23 \neq \square + \square$$
$$29 = 2^2 + 5^2$$
$$31 \neq \square + \square$$
$$37 = 1^2 + 6^2$$

De rode priemgetallen zijn niet te schrijven als de som van twee kwadraten en de priemgetallen in het groen zijn dat wel. Er valt op dat de priemgetallen die een rest hebben van 3 bij deling door 4 altijd rood zijn, terwijl de priemgetallen die een rest geven van 1 bij deling door 4 altijd groen zijn. Wanneer we een geheel getal delen door 4, dan krijgen we een rest van 0, 1, 2 of 3. Gehele getallen zijn dus te schrijven als $4k$, $4k+1$, $4k+2$ of $4k+3$.

De getallen die te schrijven zijn als $4k$ of $4k+2$ zijn even en getallen die te schrijven zijn als $4k+1$ of $4k+3$ zijn oneven. We kijken eerst naar de even priemgetallen. Het enige even priemgetal is 2. Dit is te schrijven als de som van twee kwadraten: $2 = 1^2 + 1^2$.

Het blijkt dat priemgetallen in de vorm $4k+3$ nooit te schrijven zijn als de som van twee kwadraten. Sterker nog, geen enkel getal in de vorm $4k+3$ is te schrijven als de som van twee kwadraten!

Stel dat er een getal in de vorm $4k+3$ zou bestaan, dat te schrijven is als de som van twee kwadraten. Dan zou $4k+3 = a^2 + b^2$. De kwadraten a^2 en b^2 zijn even en oneven, want hun som is oneven. Laat a^2 het even kwadraat zijn en b^2 het oneven kwadraat. We schrijven $a = 2c$ en $b = 2d+1$.

Invullen geeft echter:

$$4k+3 = a^2+b^2 = (2c)^2+(2d+1)^2 = 4c^2+4d^2+4d+1 = 4(c^2+d^2+d)+1.$$

Dat kan niet, want er staat dat $4k+3 = 4(c^2+d^2+d)+1$, terwijl een getal in de vorm $4k+3$ nooit een getal is in de vorm $4k+1$.

We concluderen dat priemgetallen in de vorm $4k+3$ nooit te schrijven zijn als de som van twee kwadraten. [Mat20]

3.2 Priemgetallen in de vorm 4k+1

Nu kijken we naar de priemgetallen in de vorm $4k+1$. De twee kwadraten stelling van Fermat zegt dat elk priemgetal in de vorm $4k+1$ te schrijven is als de som van twee kwadraten. De wiskundige G.H.Hardy beweerde zelfs dat er geen enkel eenvoudig van deze stelling bestaat! [Lev15]

Dat bleek later niet waar te zijn. In de jaren 90 werd er een bewijs gepubliceerd, bestaande uit niet meer dan één zin! Hoewel het bewijs best wel ingewikkeld is, bleek later dat het deels kon worden gevisualiseerd. Dit bewijs is heel erg elegant. Ik heb dit bewijs daarom verwerkt in een lemma (een hulpstelling), zodat ik het later kon gebruiken voor sterkere resultaten. In het bewijs maak ik veel gebruik van het begrip pariteit. Pariteit betekent of een getal even of oneven is. Een oneven getal krijgt pariteit 1 en een even getal krijgt pariteit 0. De pariteit van 2021 is bijvoorbeeld 1, want 2021 is oneven. Een natuurlijk getal is een positief geheel getal.

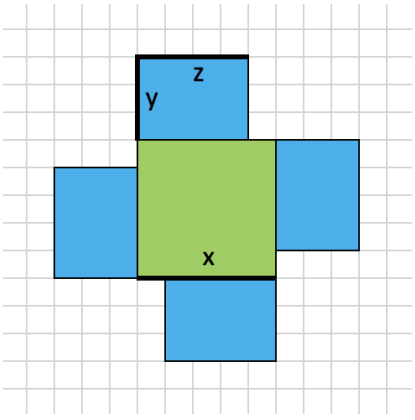
Lemma 1 *Gegeven een natuurlijk getal n in de vorm $4k+1$, geen kwadraat. Het aantal manieren waarop n te schrijven is als de som van twee kwadraten heeft dezelfde pariteit als het aantal manieren waarop n te schrijven is als het product van twee natuurlijke getallen.*

Als n te schrijven is als de som van twee kwadraten, dan is $n = a^2 + b^2$. Omdat n oneven is, hebben a^2 en b^2 verschillende pariteiten. Laat a oneven zijn en b even. Dit kunnen we schrijven als $a = x$ en $b = 2y$, waarbij x oneven is. Invullen geeft: $n = x^2 + (2y)^2 = x^2 + 4y^2$.

We zoeken nu dus de oplossingen van deze vergelijking. Daarvoor bekijken we de oplossingen met $y = z$ van een algemenere vergelijking: $n = x^2 + 4yz$. Kijk bijvoorbeeld naar $n = 29$. De oplossingen (x, y, z) van de vergelijking $29 = x^2 + 4yz$ zijn hierbij: $(1, 1, 7)$, $(1, 7, 1)$, $(3, 1, 5)$, $(3, 5, 1)$ en $(5, 1, 1)$. Hierbij is duidelijk te zien dat er veel dubbele oplossingen zijn, namelijk de oplossingen in de vorm (x, y, z) en (x, z, y). De enige oplossingen die niet in tweetallen voorkomen ontstaan als (x, y, z) en (x, z, y) hetzelfde zijn, dus $y = z$.

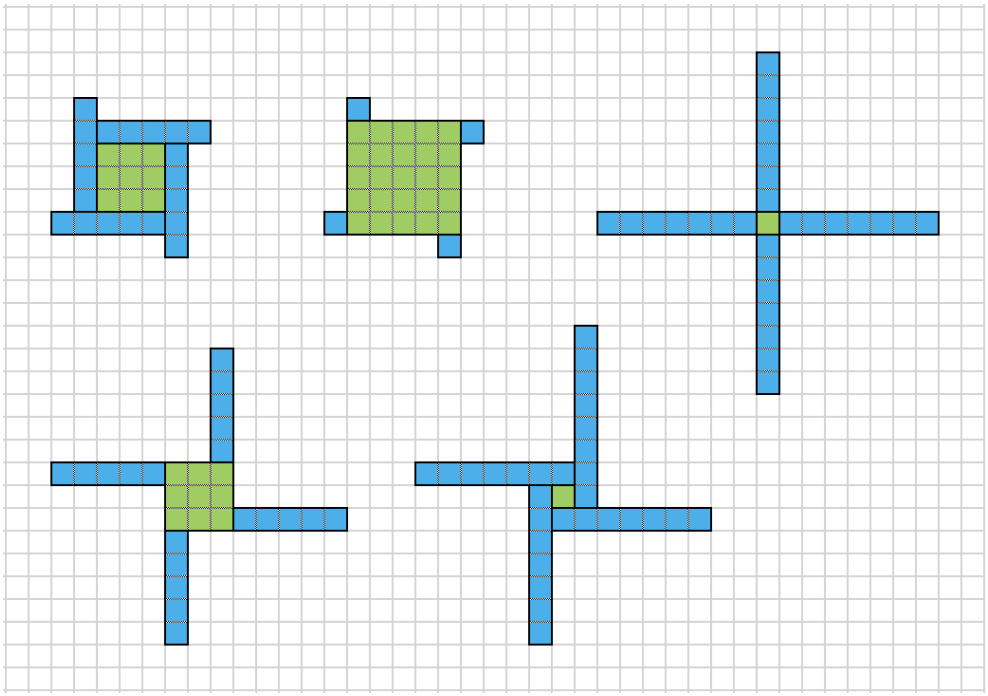
Als we nu kijken naar de pariteit van het totaal aantal oplossingen (x, y, z), dan zien we dat de tweetallen niet uitmaken voor de pariteit. De pariteit van het aantal oplossingen waarin $y = z$ is dus gelijk aan de pariteit van het totaal aantal oplossingen. Daaruit volgt dat het aantal manieren om n te schrijven als de som van twee kwadraten dezelfde pariteit heeft als het aantal oplossingen (x, y, z).

Om te zien dat het aantal oplossingen (x, y, z) samenhangt met het aantal manieren om n te schrijven als het product van twee getallen, zullen de oplossingen (x, y, z) worden gevisualiseerd. Merk op dat $x^2 + 4yz$ te tekenen is als een vierkant met zijde x en vier rechthoeken met zijdes y en z. De oplossingen zijn dus alle manieren om n te schrijven als een vierkant en vier rechthoeken. Wanneer deze op een bepaalde manier worden gestructureerd, komt dit er als volgt uit te zien:



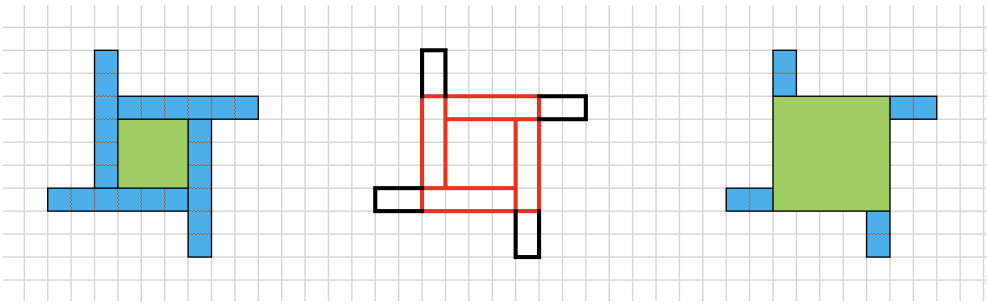
De algemene vorm om een getal te schrijven als $x^2 + 4yz$.

De oplossingen voor 29 zien er dan zo uit:



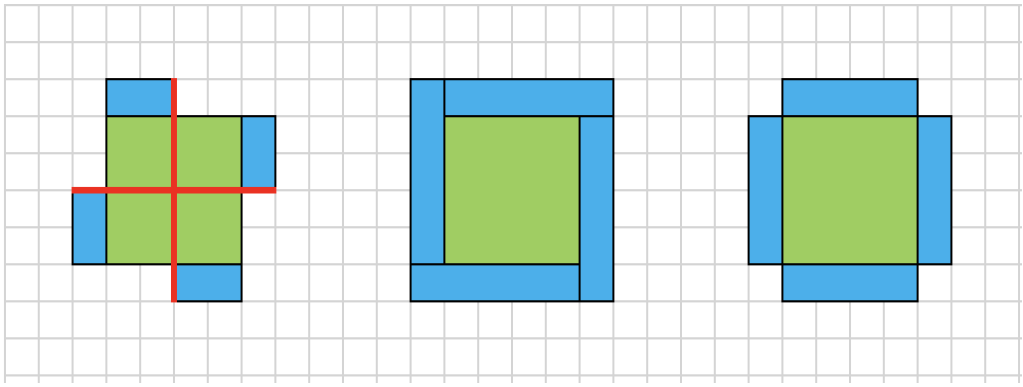
Alle mogelijkheden om 29 te schrijven als $x^2 + 4yz$.

Merk op dat de oplossingen op een andere manier tweetallen vormen, op basis van overeenkomstige buitenlijnen. Hoewel veel oplossingen op deze manier tweetallen vormen, zijn er oplossingen mogelijk die zich niet op deze mooie manier laten categoriseren. De tweetallen zijn oplossingen van categorie 1. Ze hebben de overeenkomstige buitenlijnen:



De oplossingen die tweetallen vormen zijn op de volgende methode te construeren.

Er zijn drie andere categorieën van oplossingen (x,y,z):



Categorie 2 *Categorie 3* *Categorie 4*

Categorie 2 kan niet, want de lijnen snijden in het midden van x, terwijl x oneven is. Categorie 3 kan ook niet. Als het wel zou kunnen, zou n een kwadraat zijn.

Oplossingen van categorie 4 hebben de vorm van een kruis. Dit zijn de oplossingen met $x = z$, dus $n = x^2 + 4yx = x(x + 4y)$. Het blijkt dat de oplossing van $n = x(x + 4y)$ correspondeert met een oplossing van $n = uv$.

Dit blijken alle manieren te zijn om n te schrijven als het product van twee delers. Stel dat $n = uv$. We willen dat u en v te schrijven zijn als x en $x+4y$. Het kan niet dat $u = v$, want dat zou $n = uv = u^2$, terwijl n geen kwadraat mag zijn. Merk op dat u en v kunnen worden geschreven als x en $x + 4y$ als het tussen u en v deelbaar is door 4.

We weten dat n te schrijven is als $4k + 1$, dus u en v zijn in ieder geval oneven. Ze zijn dus te schrijven als $4k + 1$ of als $4k + 3$. Stel dat de één in de vorm $4k + 1$ is en de ander in de vorm $4k + 3$. Dat kan niet, want het product van een getal in de vorm $4k + 1$ en een getal in de vorm $4k + 3$ is altijd te schrijven als $4k + 3$. Dat willen we niet, want hun product moet te schrijven zijn als $4k + 1$.

Wanneer u en v beiden te schrijven zijn als $4k + 1$, of juist allebei als $4k + 3$, dan is het verschil tussen u en v deelbaar door 4. Als we nu kijken naar de pariteit van het aantal oplossingen (x, y, z), dan zien we dat de tweetal-

oplossingen niet uitmaken. De enige oplossingen die wel invloed hebben op de pariteit zijn dan de oplossingen die niet in tweetallen zitten. Dat kunnen alleen de oplossingen zijn die een kruis vormen, waarbij we weten dat aantal oplossingen in de vorm van een kruis gelijk is aan het aantal manieren om te schrijven $n = uv$.

De pariteit van het aantal oplossingen $n = uv$ is dus gelijk aan de pariteit van het aantal oplossingen $n = x^2 + 4y$. Omdat er al eerder was bewezen dat de pariteit van het aantal oplossingen van $n = x^2 + 4yz$ gelijk is aan de pariteit van het aantal oplossingen $n = x^2 + 4y^2$, kunnen we concluderen dat het aantal oplossingen van $n = a^2 + b^2$ en het aantal oplossingen van $n = uv$ dezelfde pariteit hebben. Het lemma is dus bewezen. □

Merk op dat priemgetallen in de vorm $4k+1$ aan de voorwaarden van lemma 1 voldoen. Ze zijn natuurlijke getallen, te schrijven als $4k + 1$ en nooit een kwadraat. Stel dat er wel een priemgetal is dat een kwadraat is. Noem dat priemgetal p. Dan is $p = t^2$. Merk op dat t deelbaar is door 1, t en t^2. Als $t > 1$, dan zijn dat verschillende delers. Als $t = 1$, dan zou $p = 1$, wat geen priemgetal is.

Een leuke eigenschap van een priemgetal p is dat p op exact één manier te schrijven is als het product van natuurlijke getallen, namelijk $p = 1 \cdot p$. Omdat priemgetallen in de vorm $4k + 1$ op een oneven aantal manieren te schrijven zijn als het product van twee getallen, moeten ze ook op een oneven aantal manieren te schrijven zijn als de som van twee kwadraten. Nul is even, dus priemgetallen in de vorm $4k + 1$ zijn altijd te schrijven als de som van twee kwadraten.

Hieruit kunnen we concluderen dat alle priemgetallen in de vorm $4k + 1$ te schrijven zijn als de som van twee kwadraten. [Mat20]

3.3 Uniciteit

Het blijkt dat priemgetallen nooit op meerdere manieren te schrijven zijn als de som van twee kwadraten. Hiervoor bewijs ik weer een lemma. Het lemma

is een vorm van de stelling van Brahmagupta-Fibonacci.

Hoewel het al bekend was, bewees ik het lemma zelf. [Lev15; Mat20]

Lemma 2 *De algemene oplossing om een natuurlijk getal n dat op twee manieren te schrijven is als de som van twee kwadraten, is*

$$n = (rt + qs)^2 + (qt - rs)^2 = (rt - qs)^2 + (qt + rs)^2 = (q^2 + r^2)(s^2 + t^2).$$

Hierin zijn q, r s en t gehele getallen.

Stel dat $n = a^2 + b^2 = c^2 + d^2$. Het kan niet dat $n = 4k + 3$, want getallen die te schrijven zijn als $4k + 3$ zijn nooit te schrijven als de som van twee kwadraten.
Als $n = 4k$, dan moeten a, b, c en d even zijn.
Als $n = 4k + 2$, dan zijn a, b, c en d allemaal oneven.
Als $n = 4k + 1$, dan zijn a en b van verschillende pariteit, net als c en d. Laat a en c de oneven getallen zijn en b en d de even getallen. Door deze eisen weten we dat $a+c$, $a-c$, $d+b$ en $d-b$ allemaal even getallen moeten zijn.

Stel dat $a^2 = c^2$. Omdat $a^2 + b^2 = c^2 + d^2$, betekent dit dat $b^2 = d^2$.
We kunnen nu inderdaad schrijven dat $n = (rt + qs)^2 + (qt - rs)^2 = (rt - qs)^2 + (qt + rs)^2 = (q^2 + r^2)(s^2 + t^2)$.
Als $s = 0$ en $t = 1$, dan wordt de vergelijking $n = r^2 + q^2 = r^2 + q^2 = (q^2 + r^2)(1^2 + 0^2)$. Als we vervolgens invullen dat $r = a$ en $q = b$, dan krijgen we $n = a^2 + b^2 = a^2 + b^2 = (b^2 + a^2) \cdot 1$. De vergelijking klopt. Het is in de vorm die we willen hebben, want $c^2 = a^2$ en $d^2 = b^2$.

In het andere geval is $a^2 \neq c^2$. Wanneer we de vergelijking $a^2 + b^2 = c^2 + d^2$ omschrijven, krijgen we $a^2 - c^2 = d^2 - b^2$. Hierin zien we aan beide kanten een merkwaardig product. Wanneer we dat product ontbinden, krijgen we $(a - c)(a + c) = (b - d)(b + d)$. De uitkomst hiervan is niet 0, want dat zou betekenen dat $a^2 = c^2$ en $b^2 = d^2$.

We weten dat $a + c$, $a - c$, $d + b$ en $d - b$ even zijn, dus we maken van het merkwaardig product $\frac{a+c}{2}\frac{a-c}{2} = \frac{d+b}{2}\frac{d-b}{2}$.

Dit kunnen we omschrijven naar een vergelijking met breuken, want het is niet 0. Laat $\frac{s}{t}$ een volledig vereenvoudigde versie van de volgende breuk zijn:

$$\frac{(\frac{a-c}{2})}{(\frac{d+b}{2})} = \frac{(\frac{d-b}{2})}{(\frac{a+c}{2})} = \frac{s}{t}.$$

Dit betekent dat we kunnen schrijven $\frac{a-c}{2} = qs$ en $\frac{d+b}{2} = qt$. We kunnen ook zeggen dat $\frac{d-b}{2} = rs$ en $\frac{a+c}{2} = rt$. Nu kunnen we a, b, c en d uitrekenen:

$$a = \frac{a+c}{2} + \frac{a-c}{2} = rt + qs, \qquad b = \frac{d+b}{2} - \frac{d-b}{2} = qt - rs,$$
$$c = \frac{a+c}{2} - \frac{a-c}{2} = rt - qs, \qquad d = \frac{d+b}{2} + \frac{d-b}{2} = qt + rs$$

Invullen geeft:

$$\begin{aligned} a^2 + b^2 = (rt + qs)^2 + (qt - rs)^2 &= (rt)^2 + (qs)^2 + (qt)^2 + (rs)^2 \\ c^2 + d^2 = (rt - qs)^2 + (qt + rs)^2 &= (rt)^2 + (qs)^2 + (qt)^2 + (rs)^2 \\ (q^2 + r^2)(s^2 + t^2) &= (rt)^2 + (qs)^2 + (qt)^2 + (rs)^2 \end{aligned}$$

Dit betekent dat de vergelijking klopt. Het is dus inderdaad de algemene vorm. □

Hiermee kunnen we bewijzen dat priemgetallen die te schrijven zijn als de som van twee kwadraten dat maar op één manier doen. Stel dat er een priemgetal p bestaat, zodat $p = a^2 + b^2 = c^2 + d^2$. Vanwege de algemene oplossing betekent dit dat $p = (q^2 + r^2)(s^2 + t^2)$. De enige manier op p te schrijven als het product van twee getallen is $1 \cdot p$. Dat zou betekenen dat $q^2 + r^2 = 1$ of $s^2 + t^2 = 1$.

Als $q^2, r^2, s^2, t^2 \geq 1$, dan zou $q^2 + r^2 \geq 2$ en $s^2 + t^2 \geq 2$. Hieruit volgt dat $q^2 = 0$, $r^2 = 0$, $s^2 = 0$ of $t^2 = 0$, dus $4qrst = 0$. Merk op dat $a^2 - c^2 = (rt + qs)^2 - (rt - qs)^2 = 4qrst$, dus het zou betekenen dat $a^2 = c^2$, waardoor ook $b^2 = d^2$. Dit betekent dat $p = a^2 + b^2$ dezelfde manier is om p te schrijven als de som van twee kwadraten als $p = c^2 + d^2$.

We concluderen dat een priemgetal op één manier te schrijven is als de som van twee kwadraten.

4 Natuurlijke getallen als de som van twee kwadraten

In dit hoofdstuk ga ik de algemene twee-kwadraten-stelling bewijzen: Een positief geheel getal is te schrijven als de som van twee kwadraten dan en slechts dan als alle priemgetallen in de vorm $4k + 3$ van dat getal een even aantal keer voorkomen in de priemontbinding. De term 'dan en slechts dan als' betekent dat de stelling twee kanten op werkt.

In dit hoofdstuk ga ik een nieuw begrip gebruiken: "blij". Een positief geheel getal is blij, wanneer het te schrijven is als de som van twee kwadraten. Getallen die niet te schrijven zijn als de som van twee kwadraten zijn niet blij.

4.1 Getallen als het product van priemgetallen

Het eerste deel van het hoofdstuk gaat over het schrijven van een willekeurig positief getal als het product van priemgetallen. De getallen 1 tot en met 10 zijn ook allemaal te schrijven als het product van priemgetallen:

$$
\begin{aligned}
1 &= \bullet \\
2 &= 2 \\
3 &= 3 \\
4 &= 2 \cdot 2 \\
5 &= 5 \\
6 &= 2 \cdot 3 \\
7 &= 7 \\
8 &= 2 \cdot 2 \cdot 2 \\
9 &= 3 \cdot 3 \\
10 &= 2 \cdot 5
\end{aligned}
$$

Bij 1 is er iets raars aan de hand. Het is namelijk het zogenoemde "lege product": datgene wat je krijgt wanneer je niks met elkaar vermenigvuldigt. Dit wordt vaak toch gezien als een geldige manier om 1 te schrijven als het product van priemgetallen.

De hoofdstelling van de rekenkunde stelt dat elk positief geheel getal op een unieke manier wordt geschreven als het product van priemgetallen. De manier om een getal te schrijven als het product van priemgetallen wordt ook wel de priemontbinding of priemfactorisatie genoemd.

Het bewijs van de hoofdstelling van de rekenkunde bestaat uit twee delen: In het eerste deel wordt de existentie bewezen van een priemfactorisatie. Het tweede deel bewijst de uniciteit.

Stelling 1 *Elk natuurlijke getal is te schrijven als het product van priemgetallen.*

Stel dat er natuurlijke getallen zouden bestaan zonder een priemfactoratie. Dan bestaat er een kleinste getal dat niet te schrijven is als het product van priemgetallen. Noem dat getal k. Het enige getal met exact één deler is 1. Dit is echter te schrijven als het lege product, dus k heeft meerdere delers. Als k exact twee positieve delers zou hebben, dan is k een priemgetal, dus $k = k$ is een geldige priemfactorisatie.

We weten dus dat k ten minstens drie verschillende positieve delers heeft. Hieruit volgt dat k een positieve deler d heeft, zodat $d > 1$ en $d \neq k$. Het feit dat d een deler is van k betekent dat een een natuurlijk getal m bestaat, zodat $k = dm$. Omdat de grootste deler van een getal zichzelf is, betekent $d \neq k$ dat $d < k$. Verder is $m < k$, want $d > 1$ betekent dat $k = dm > m$.

We hebben aangenomen dat k het kleinste positieve gehele getal is zonder priemfactorisatie, dus d en m zijn allebei te schrijven als het product van priemgetallen. Omdat d en m te schrijven zijn als het product van priemgetallen en k het product is van d en m, is k zelf ook te schrijven als het product van priemgetallen.

De aanname dat er getallen bestaan zonder priemfactorisatie is onjuist, dus elk natuurlijk getal is te schrijven als het product van priemgetallen. □

[Hof21]

Stelling 2 *De priemfactoristie van een natuurlijk getal is uniek.*

Stel dat er positieve getallen bestaan die op meerdere manieren te schrijven zijn als het product van priemgetallen. Noem het kleinste positieve getal met meerdere priemfactorisaties k. Merk op dat $k > 1$. De enige manier om 1 te krijgen als het product van priemgetallen is het lege product. Wanneer 1 het product is van priemgetallen, dan is het deelbaar door die priemgetallen. De enige deler van 1 is echter 1, wat geen priemgetal is.

Als k meerdere priemfactorisaties zou hebben, geen van beide het lege product, dan kunnen we k op meerdere manieren schrijven als het product van priemgetallen: $k = p \cdot a = q \cdot b$, waarbij p en q priemgetallen zijn. Hierin stellen $p \cdot a$ en $q \cdot b$ de twee verschillende priemfactoristaties voor van k.

Als $p = q$, dan zou $ap = bp = k$, dus $a = b < k$. Omdat $a < k$, moet a een unieke priemontbinding hebben, dus b heeft dezelfde priemfactorisatie als a. Daaruit volgt dat $a \cdot p$ dezelfde priemontbinding is als $b \cdot q$. We hadden aangenomen dat dit twee verschillende priemontbindingen zijn, dus het kan niet dat $p = q$.

Omdat $p \leq q$ en $p \neq q$, moet $p < q$. Laat $t = q - p$. Dan is $q > t > 0$. Laat verder $m = b \cdot t$, waardoor $k = bq > bt = m > 0$. Omdat $k > m > 0$, heeft m een unieke priemfactoristie. Merk op dat $k - m = bq - bt = b(q - t) = bp$, dus $m = k - bp = ap - bp = (a - b)p$. Omdat $m = (a - b) \cdot p$, is de unieke priemontbinding van m is te schrijven als het product van p en de priemontbinding van $a - b$.

We weten nu dat p in de priemfactorisatie zit van m. Omdat $m = b \cdot t$ is de priemfactoristatie van m ook te schrijven als het product van de priemfactorisatie van b en de priemfactorisatie van t. Dat betekent dat p in de priemontbinding van t zit of dat p in de priemontbinding zit van b.

Als p in de priemfactorisatie van t zit, dan is p een deler van t, dus p is een deler van $q - p$. Dat zou betekenen dat p een deler is van q. We weten echter dat q een priemgetal is, dus de enige delers van q zijn 1 en zichzelf. We weten dat $p \neq 1$, want 1 is geen priemgetal. Ook weten we dat $p \neq q$.

Het kan dus niet dat p in de priemfactorisatie zit van t. Hieruit volgt dat p in de priemfactoristatie zit van b, dus p is een deler van b. Schrijf $b = p \cdot c$. Dan zien we dat $k = a \cdot p = b \cdot q = c \cdot pq$, dus $a = c \cdot q < k$.

Omdat $a < k$, is de priemfactoristatie van a uniek, dus de priemfactorisatie van a is hetzelfde als de priemfactorisatie van $c \cdot q$.

Dit betekent echter dat de priemfactorisaties van ap en $cpq = bq$ hetzelfde zijn, terwijl we hadden aangenomen dat dit verschillende priemontbindingen zijn. We hebben dus een tegenspraak. De aanname dat er een getal bestaat met meerdere priemfactorisaties is onjuist, dus de priemfactorisatie van een getal is uniek. □

We hebben nu bewezen dat elk positief getal op een unieke manier te schrijven is als het product van priemgetallen. Het blijkt dat de priemontbinding van een getal veel zegt over haar eigenschappen. De priemfactorisatie wordt meestal geschreven in de vorm van machten, omdat het dan veel makkelijker te lezen is. Een voorbeeld hiervan is $2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 3^4 \cdot 5^2$. [Hof21]

4.2 Getallen die te schrijven zijn als de som van twee kwadraten

Het blijkt dat de priemfactorisatie van een getal kan worden gebruikt om te controleren of het te schrijven is als de som van twee kwadraten. In de volgende twee paragrafen zullen we de "som van twee kwadratenstelling"bewijzen. Een natuurlijk getal is te schrijven als de som van twee kwadraten dan en slechts dan als dat getal een even aantal priemfactoren heeft van elk priemgetal in de vorm $4k + 3$. [Bri21]

Neem bijvoorbeeld het getal 2025. De priemfactorisatie van 2025 is $3^4 \cdot 5^2$. De enige priemfactor in de vorm $4k + 3$ van 2025 is 3. Omdat 2025 vier priemfactoren 3 heeft, zou het te schrijven moeten zijn als de som van twee kwadraten. Dat klopt: $2025 = 27^2 + 36^2$.

Hier zal ik bewijzen dat een getal daadwerkelijk te schrijven is als de som van twee kwadraten, wanneer de priemontbinding van het getal een even aantal priemfactoren bevat van elk priemgetal in de vorm $4k + 3$. Daarvoor bewijs ik eerst het volgende lemma:

Lemma 3 *Het product van n blije getallen is zelf ook te schrijven als de som van twee kwadraten, voor gehele getallen* $n \geq 0$.

Om dit te bewijzen gaan we het principe van inductie toepassen. Wanneer een stelling klopt in het geval van $n = 0$ en het kloppend zijn van de stelling voor $n = k$ impliceert dat de stelling ook klopt voor $n = k + 1$, dan klopt de stelling voor elk geheel getal $n \geq 0$.

Het kloppen voor $n = 0$ heet de inductiebasis. Het deel waarin bewezen wordt dat het kloppen voor $n = k$ impliceert dat het ook klopt voor $n = k+1$, wordt de inductiestap genoemd.

Inductiebasis: Het product van 0 blije getallen is het lege product 1. Dat is te schrijven als $1 = 0^2 + 1^2$.

Inductiestap: Als het product van k blije getallen te schrijven is als de som van twee kwadraten, dan is het product van $k + 1$ blije getallen ook te schrijven als de som van twee kwadraten.

Wanneer x_1 tot en met x_{k+1} allemaal blij zijn, dan is

$$x_1 \cdot x_2 \cdot \ldots \cdot x_k \cdot x_{k+1} = (x_1 \cdot x_2 \cdot \ldots \cdot x_k) \cdot x_{k+1} = (a^2+b^2) \cdot (c^2+d^2) = (ac+bd)^2+(ad-bc)^2$$

We wisten immers dat het product van x_1 tot en met x_k te schrijven moest zijn als de som van twee kwadraten. Dat werd $a^2 + b^2$. Ook was x_{k+1} te schrijven als de som van twee kwadraten, namelijk $x_{k+1} = c^2 + d^2$.

We hebben nu met inductie bewezen dat product van n blije getallen zelf ook een blij getal is, voor alle gehele getallen $n \geq 0$. □

Dit kunnen we gebruiken in het volgende bewijs:

Stelling 3 *Een natuurlijk n, waarvan alle priemfactoren in de vorm $4k+3$ een even exponent hebben in de priemfactorisatie, is te schrijven als de som van twee kwadraten.*

Vanwege de hoofdstelling van de rekenkunde is n op een unieke manier te ontbinden als het product van priemgetallen. We verdelen de priemfactoren in twee groepen: De priemgetallen in de vorm $4k+3$ en de andere priemgetallen.

De priemgetallen in de vorm $4k+3$ noemen we q. Omdat de exponenten allemaal even zijn, kunnen we deze schrijven als $2e$. Dat betekent dat $q_1^{2e_1} \cdot q_2^{2e_2} \cdot q_3^{2e_3} \cdot \ldots$ het product van de priemgetallen in de vorm $4k+3$. Omdat alle exponenten even zijn, is

$$q_1^{2e_1} \cdot q_2^{2e_2} \cdot q_3^{2e_3} \cdot \ldots = (q_1^{e_1} \cdot q_2^{e_2} \cdot q_3^{e_3} \cdot \ldots)^2 = m^2.$$

We weten dat n het product is van priemgetallen in de vorm $4k+3$ en andere priemgetallen. Het product van de priemgetallen in de vorm $4k+3$ is gelijk aan m^2, wat te schrijven is als de som van twee kwadraten: $m^2 = 0^2 + m^2$.

De priemgetallen niet in de vorm $4k+3$ zijn ook te schrijven als de som van twee kwadraten. Dat betekent dat n het product is van getallen die te schrijven zijn als de som van twee kwadraten. Vanwege lemma 3 moet n zelf ook te schrijven zijn als de som van twee kwadraten. □

4.3 Getallen die niet te schrijven zijn als de som van twee kwadraten

In deze paragraaf zullen we de andere kant van de stelling bewijzen: een getal is niet te schrijven als de som van twee kwadraten, wanneer niet alle priemgetallen in de vorm $4k+3$ een even aantal keer in de priemontbinding voorkomen.

Stelling 4 *Een natuurlijk getal is niet te schrijven als de som van twee kwadraten wanneer het een priemfactor in de vorm $4k+3$ bevat met een oneven exponent.*

Stel dat er wel blije getallen bestaan met een priemgetal in de vorm $4k+3$ met een oneven exponent. Noem het kleinste blije getal met die eigenschappen n. Dan is $n = a^2 + b^2$, zodat $a \geq b$.

Als n even is, dan zouden a^2 en b^2 van dezelfde pariteit moeten zijn, net als a en b. Dat zou betekenen dat $a - b$ en $a + b$ even zijn. Laat $2r = a - b \geq 0$ en $2s = a + b$. Dat zou echter betekenen dat

$$2n = 2a^2 + 2b^2 = (a-b)^2 + (a+b)^2 = (2q)^2 + (2r)^2 = 4(q^2 + r^2),$$

dus $q^2 + r^2 = \frac{n}{2}$.

Merk op dat de priemontbinding van $\frac{n}{2}$ hetzelfde is als die van n, wanneer we alleen kijken naar de oneven priemgetallen. Dat kan niet, want we namen aan dat n het kleinste blije getal is met een priemfactor in de vorm $4k+3$ met een oneven exponent. Er is dus tegenspraak. De aanname dat n even kan zijn is dus onjuist. Hieruit volgt dat n oneven is.

Stel dat n op meerdere manieren te schrijven is als de som van twee kwadraten. We weten dat een getal dat op meerdere manieren te schrijven is als de som van kwadraten, het product is van twee kleinere blije getallen. Dat zou betekenen dat n het product is van twee kleinere blije getallen u en v.

We hadden aangenomen dat n het kleinste blije getal is, deelbaar door een priemgetal in de vorm $4k+3$ dat een oneven aantal keer voorkomt in de priemfactorisatie van n. Daar volgt uit dat de priemontbindingen van u en v geen priemgetallen in de vorm $4k+3$ een oneven aantal keer mogen bevatten. Omdat $n = uv$ wordt het priemgetal dat een oneven aantal keer voorkomt in de priemontbinding van n verdeeld over de priemontbindingen van u en v. Het kan niet dat de priemontbindingen van u en v allebei een even aantal krijgen van dat priemgetal, want dan zou de priemfactoristie van n de priemgetal een even aantal keer moeten bevatten. De aanname dat n op meerdere manieren te schrijven is als de som van twee kwadraten is onjuist.

We weten dat getallen in de vorm $4k+3$ niet te schrijven zijn als de som van twee kwadraten, dus n is in de vorm $4k+1$. Schrijf $n = q^{2c+1} \cdot m$, waarin q een priemgetal is in de vorm $4k+3$ en q geen deler is van m. We kunnen lemma 1 toepassen op n, want n is in de vorm $4k+1$ en n is geen kwadraat, omdat n een priemgetal bevat dat een oneven aantal keer voorkomt in haar priemontbinding.

Vanwege lemma 1 heeft het aantal manieren om n te schrijven als de som van twee kwadraten dezelfde pariteit als het aantal oplossingen van $n = uv$. Omdat n op één manier te schrijven is als de som van twee kwadraten, moet er een oneven aantal oplossingen zijn van de vergelijking $n = uv$.

Het blijkt dat het aantal oplossingen $n = uv$ voor een niet-kwadraat n gelijk is aan de helft van het aantal delers van n. Elke oplossing van $n = uv$ geeft namelijk 2 verschillende delers van n, namelijk u en v. Ze zijn verschillend, want $u = v$ zou betekenen dat $n = u^2$. Omdat we een oneven getal krijgen wanneer we de helft nemen van het aantal delers van n, mag het aantal delers van n niet deelbaar zijn door 4.

Het blijkt echter dat het aantal delers van $n = q^{2c+1} \cdot m$ deelbaar moet zijn door 4, wanneer p een priemgetal is in de vorm $4k+3$. Merk op dat alle delers van n op een unieke manier kunnen worden geschreven als $q^d \cdot t$, waarin q geen deler is van t. We kunnen t namelijk schrijven als het product van alle priemgetallen die niet q zijn.

Als $q^d \cdot t$ een deler is van n, dan is t een deler van n en is q^d een deler van n. We weten dat $n = q^{2c+1} \cdot m$. Hierin is q^{2c+1} het deel in de priemontbinding met priemgetallen q en m is de rest van de priemontbinding. Hetzelfde geldt voor t en q^d. Hieruit volgt dat t een deler moet zijn van m en q^d een deler moet zijn van q^{2c+1}. We kunnen voor t elke mogelijke deler nemen van m en voor q^d elke mogelijke deler van q^{2c+1}. Deze twee zijn onafhankelijk van elkaar, dus het totaal aantal delers van n is gelijk aan het product van het aantal delers van m en het aantal delers van q^{2c+1}.

Het aantal delers van q^{2c+1} is even, want het is geen kwadraat. Als het aantal delers van m een even getal is, dan zou het aantal delers van n deelbaar zijn door 4, wat niet mag. Omdat het aantal delers van m oneven is, moet het een kwadraat zijn. Als $m = w^2$, dan is

$$n = q^{2c+1} \cdot m = q \cdot q^{2c} \cdot w^2 = q \cdot (q^c \cdot w)^2 = q \cdot s^2$$

We weten dat n oneven is, dus s is ook oneven. Een oneven kwadraat is altijd in de vorm $4k + 1$, terwijl q in de vorm $4k + 3$ is.

Het product van een getal in de vorm $4k + 3$ en een getal in de vorm $4k + 1$ is altijd in de vorm $4k + 3$, terwijl we eerder zagen dat n in de vorm $4k + 1$ is. Er is dus tegenspraak.

We concluderen dat er geen blije getallen bestaan, die deelbaar zijn door een priemgetal in de vorm $4k + 3$ dat een oneven aantal keer voorkomt in hun priemontbinding.

5 Aantal representaties van getallen als de som van twee kwadraten

Definieer de kwadraticiteit van een getal n als volgt:
De kwadraticiteit van een natuurlijk getal n is gelijk aan het aantal oplossingen (x, y), zodat $n = x^2 + y^2$, waarin x en y gehele getallen zijn en $x \geq y \geq 0$. De kwadraticiteit van 5 is 1, want $5 = 1^2 + 2^2$ is de enige manier om 5 te schrijven als de som van twee kwadraten.

In dit hoofdstuk zal ik de kerststelling van Fermat bewijzen:
Gegeven een positief geheel getal met a delers in de vorm $4k+1$ en b delers in de vorm $4k+3$. De kwadraticiteit van dat getal is dan gelijk aan $\lceil \frac{1}{2} \cdot (a-b) \rceil$. De vierkante haakjes betekenen dat de uitkomst naar boven wordt afgerond, op gehelen.

Neem bijvoorbeeld 2025. De 15 delers van 2025 zijn 1, 3, 5, 9, 15, 25, 27, 45, 75, 81, 135, 225, 405, 675 en 2025. Daarvan zijn er 9 delers in de vorm $4k+1$ en 6 delers in de vorm $4k+3$. De kwadraticiteit van 2025 is dan $\lceil \frac{1}{2} \cdot (9-6) \rceil = \lceil \frac{3}{2} \rceil = 2$.

Er zijn inderdaad exact twee manieren om 2025 te schrijven als de som van twee kwadraten, namelijk $2025 = 27^2 + 36^2$ en $2025 = 0^2 + 45^2$. [Mat19]

5.1 Even getallen

Lemma 4 *De kwadraticiteit van n en $2n$ is hetzelfde.*

Er kunnen tweetallen worden gemaakt van oplossingen (a, b) en (c, d) van $n = a^2 + b^2, a \geq b \geq 0$ en $2n = c^2 + d^2, c \geq d \geq 0$, met $(c, d) = (a + b, a - b)$, want:

$$n = a^2 + b^2 \Rightarrow 2n = 2a^2 + 2b^2 = (a+b)^2 + (a-b)^2 = c^2 + d^2$$

Deze oplossingen voldoen aan de vereisten, want $a + b \geq a - b \geq 0$ als $a \geq b \geq 0$. Op die manier vormt elke (a, b) een tweetal met een (c, d).

Andersom is dit ook waar. Stel dat $2n = c^2 + d^2$, waarbij $c \geq d \geq 0$. Omdat $c^2 + d^2$ even is, hebben c en d dezelfde pariteit. Dit betekent dat $c+d$ en $c-d$ even zijn. Laat $a = \frac{c+d}{2}$ en $b = \frac{c-d}{2}$. Dan zijn $a+b = c$ en $a-b = d$. Invullen in $2n = c^2 + d^2$ geeft:

$$2n = c^2 + d^2 = (a+b)^2 + (a-b)^2 = 2a^2 + 2b^2 \Rightarrow n = a^2 + b^2$$

Dit is duidelijk een voorbeeld van de gezochte tweetallen, want $\frac{c+d}{2} \geq \frac{c-d}{2} \geq 0$, als $c \geq d \geq 0$. Hier volgt uit dat elke (c, d) in een tweetal zit met een (a, b). Omdat de vergelijking twee kanten op werkt is er voor elke (a, b) maar één (c, d) en andersom. Kortom, er zijn net zo veel (a, b) als (c, d). □

Het lemma is consistent met de kerststelling van Fermat, want n en $2n$ hebben dezelfde oneven delers. Merk op dat het lemma tot gevolg heeft dat $n = 2^l m$ dezelfde kwadraticiteit heeft als m, waarin m oneven is. De kerststelling van Fermat hoeft dus alleen nog maar bewezen te worden voor de oneven getallen.

5.2 Getallen deelbaar door een priemgetal in de vorm $4k + 3$

Stel dat een natuurlijk getal deelbaar is door een priemgetal q. Dan is het deelbaar door q^2, of het aantal factoren q in de priemontbinding is oneven. Het blijkt dat n en $q^2 n$ op evenveel manieren te schrijven zijn als de som van twee kwadraten.

Lemma 5 *Laat q een priemgetal zijn in de vorm $4k + 3$. Dan hebben n en $q^2 n$ dezelfde kwadraticiteit.*

Stel dat q een deler is van $c^2 + d^2$. Laat qx en qy de veelvouden zijn van q die het dichtst bij c en d zitten. Omdat het verschil tussen twee opeenvolgende veelvouden van q gelijk is aan q, is het verschil tussen c en qx en het verschil tussen d en qy, hooguit $\frac{1}{2} \cdot q$. Schrijf $c = qx + u$ en $d = qy + v$, waarin u en v ook negatief mogen zijn. Wanneer we dit invullen voor c en d, dan zien we dat q een deler moet zijn van

$$(qx + u)^2 + (qy + v)^2 = q(qx^2 + 2ux + qy^2 + 2vy) + u^2 + v^2,$$

dus q is een deler van $u^2 + v^2$. Omdat $|u| \leq \frac{1}{2} \cdot q$ en $|v| \leq \frac{1}{2} \cdot q$, moet $u^2 \leq (\frac{1}{2} \cdot q)^2 = \frac{1}{4} \cdot q^2$ en $v^2 \leq (\frac{1}{2} \cdot q)^2 = \frac{1}{4} \cdot q^2$, dus $u^2 + v^2 \leq 2 \cdot \frac{1}{4} \cdot q^2 = \frac{1}{2} \cdot q^2$.

Vanwege stelling 4 hebben alle blije getallen een even aantal priemfactoren van priemgetallen in de vorm $4k + 3$.
We weten dat q een deler is van $u^2 + v^2$. Omdat het een even aantal factoren q heeft, moet q^2 ook een deler zijn van $u^2 + v^2$. Schrijf $u^2 + v^2 = q^2 m$.

Hiervoor zagen we al dat $u^2 + v^2 \leq \frac{1}{2} \cdot q^2$. Invullen van $u^2 + v^2 = q^2 m$ geeft dat $q^2 m \leq \frac{1}{2} \cdot q^2$, dus $m \leq \frac{1}{2}$. Dat betekent dat $m \leq 0$. Omdat kwadraten nooit negatief kunnen zijn, moet $0 \leq u^2 + v^2 = q^2 m$, dus $m \geq 0$. Dat betekent dat $m = 0$, dus $u^2 + v^2 = 0$. Dit kan alleen als $u = v = 0$. Hieruit volgt dat $c = qx$ en $d = qy$.

We weten nu dat $q^2 n = c^2 + d^2$ impliceert dat q een deler is van c en d. Alle oplossingen van $q^2 n = c^2 + d^2$ zijn dus oplossingen in de vorm $q^2 n = (aq)^2 + (bq)^2$. Alle oplossingen in de vorm $q^2 n = (aq)^2 + (bq)^2$ geven oplossingen van $n = a^2 + b^2$ en andersom. Dit bewijst dat de kwadraticiteit van $q^2 n$ gelijk is aan de kwadraticiteit van n. □

We moeten nu bewijzen dat dit inderdaad consistent is met de kerststelling van Fermat. Dit doen we door te laten zien dat het verschil tussen het aantal delers in de vorm $4k + 1$ en $4k + 3$ hetzelfde is bij n en nq^2, wanneer q een priemgetal is in de vorm $4k + 3$.

Lemma 6 *Het verschil tussen het aantal delers in de vorm $4k + 1$ en $4k + 3$ is hetzelfde bij n en nq^2, wanneer n een natuurlijk getal is en q een priemgetal in de vorm $4k + 3$.*

We verdelen de delers van nq^2 in drie groepen. De eerste groep bestaat uit alle delers van n. Wanneer een getal een deler is van n, dan is het ook een deler van nq^2. De tweede groep bestaat uit de delers van nq, die geen deler zijn van n. De derde groep bestaat uit de delers van nq^2, die geen deler zijn van nq.

Wanneer groepen 2 en 3 samen net zo veel delers in de vorm $4k+1$ hebben als in de vorm $4k+3$, dan wordt het verschil tussen het aantal delers in de vorm $4k+1$ en $4k+3$ van nq^2 volledig bepaald door het verschil tussen de delers in de vorm $4k+1$ en $4k+3$ van groep 1, de delers van n.

We willen bewijzen dat groep 2 en 3 samen net zo veel delers in de vorm $4k+1$ bevatten als delers in de vorm $4k+3$. Stel dat een getal d in groep 2 zit. Dan is $\frac{nq}{d}$ een geheel getal, maar $\frac{n}{q}$ is geen geheel getal. Dit is hetzelfde als zeggen dat $\frac{nq^2}{dq}$ een geheel getal is, terwijl $\frac{nq}{dq}$ geen geheel getal is. Hieruit volgt dus dat dq in groep 3 zit.

Stel dat een getal c in groep 3 zit. Dan is c geen deler van nq, maar wel van nq^2. Laat m het getal zijn, zodat $cm = nq^2$. We weten nu dat q een deler is van cm. Omdat q een priemgetal is, betekent dit dat q een deler zijn van m of c. De vergelijking $cm = nq^2$ schrijven we om naar $\frac{nq}{c} = \frac{m}{q}$.

We weten dat c geen deler is van nq, dus $\frac{nq}{c}$ is geen geheel getal. Hieruit volgt dat $\frac{m}{q}$ ook geen geheel getal kan zijn, dus q is geen deler van m. Daar volgt uit dat q een deler moet zijn van c. Omdat q een deler is van c, is $\frac{c}{q}$ een geheel getal. Omdat c in groep 3 zit, is $\frac{nq^2}{c} = \frac{nq}{(\frac{c}{q})}$ een geheel getal, maar $\frac{nq}{c} = \frac{n}{(\frac{c}{q})}$ is geen geheel getal, dus $\frac{c}{q}$ zit per definitie in groep 2.

Voor elke d in groep 2, zit dq in groep 3 en voor elke c in groep 3, zit $\frac{c}{q}$ in groep 2. Als we $\frac{c}{q}$ schrijven als d, dan is er voor elke d in groep 2 een dq in groep 3, en andersom.

We kunnen groep 2 en groep 3 verdelen in tweetallen van d en dq, zodat d de algemene vorm is een getal in groep 2 en dq de algemene vorm is van een element van groep 3. Elk tweetal bevat net zo veel delers in de vorm $4k+1$ als het delers bevat in de vorm $4k+3$. Als d even is, dan is dq ook even, dus tellen ze niet mee.

Als d en dq allebei in de vorm $4k+1$ zijn of allebei in de vorm $4k+3$, dan is $d+dq$ in de vorm $4k+2$, wat zou betekenen dat het niet deelbaar is door 4. We weten echter dat q in de vorm $4k+3$ is, dus $q+1$ is deelbaar

door 4. Hieruit volgt dat $d(q+1) = d + dq$ ook deelbaar is door 4. Omdat elk tweetal evenveel getallen bevat in de vorm $4k+1$ als het getallen bevat in de vorm $4k+3$, bevatten groep 2 en groep 3 samen net zo veel getallen in de vorm $4k+1$ als getallen in de vorm $4k+3$.

We concluderen dat n en nq^2 hetzelfde verschil hebben tussen het aantal delers in de vorm $4k+1$ en het aantal delers in de vorm $4k+3$, als q een priemgetal in de vorm $4k+3$ is. □

Nu we dit hebben bewezen, weten we dat de kerststelling van Fermat consistent is met het feit dat n en nq^2 dezelfde kwadraticiteit hebben, wanneer q een priemgetal is in de vorm $4k+3$.

Stel dat de kerststelling van Fermat klopt bij alle natuurlijke getallen kleiner dan n. Wanneer n deelbaar is door een kwadraat van een priemgetal q in de vorm $4k+3$, dan weten we dat het kleinere getal $\frac{n}{q^2}$ hetzelfde verschil heeft tussen het aantal delers in de vorm $4k+1$ en $4k+3$ als n.

Volgens de kerststelling van Fermat betekent dit dat n en $\frac{n}{q^2}$ dezelfde kwadraticiteit hebben, wat inderdaad ook zo is. Om deze reden hoeven we de kerststelling van Fermat alleen nog te bewijzen voor de natuurlijke getallen die niet deelbaar zijn door het kwadraat van een priemgetal in de vorm $4k+3$. We willen ten slotte laten zien dat de kerststelling van Fermat consistent is met stelling 4.

Lemma 7 *Een natuurlijk getal n met een oneven aantal priemfactoren q, heeft net zo veel delers in de vorm $4k+1$ als dat het delers heeft in de vorm $4k+3$.*

Schrijf $n = q^{2e+1}m$, waarin q geen deler is van m. Het verschil tussen het aantal delers in de vorm $4k+1$ en $4k+3$ is vanwege lemma 6 hetzelfde bij $q^{2e+1}m = (q^2)^e \cdot qm$ als bij qm.

We willen nu laten zien dat qm net zo veel delers heeft in de vorm $4k+1$ als in de vorm $4k+3$. De delers van qm splitsen we op in de delers van m en

de delers van qm die geen deler zijn van m. Als d een deler is van qm, maar geen deler is van m, dan $\frac{m}{d}$ geen geheel getal, maar $q \cdot \frac{m}{d}$ is wel een geheel getal.

Hieruit volgt dat de noemer van de vereenvoudigde breuk van $\frac{m}{d}$ een noemer heeft gelijk aan q, dus q is een deler van d. Stel dat qc een deler is van qm. Omdat q geen deler is van m, valt qc onder de delers van qm die geen deler zijn van m. Dit is hetzelfde als zeggen dat $\frac{qm}{qc}$ een geheel getal is, terwijl $\frac{m}{qc}$ geen geheel getal is. Omdat $\frac{qm}{qc} = \frac{m}{c}$, is c een deler van m.

Voor elke deler qc van qm die geen deler is van m, is c een deler van m. Dit geldt ook andersom: als c een deler is van m, dan is qc een deler van qm, maar niet van m.
We kunnen dus tweetallen c en qc maken van de delers van qm. Als c even is, dan is qc oneven, als c in de vorm $4k+1$ is, dan is qc in de vorm $4k+3$, en qc is in de vorm $4k+1$ als c in de vorm $4k+3$ is. Omdat elk tweetal net zo veel getallen bevat in de vorm $4k+1$ als in de vorm $4k+3$, heeft qm net zo veel delers in de vorm $4k+1$ als in de vorm $4k+3$.

Dat betekent dat n net zo veel delers heeft in de vorm $4k+3$ als dat n delers heeft in de vorm $4k+1$. □

We zien dat een getal n dat deelbaar is door een priemgetal q, maar niet door het kwadraat van q een kwadraticiteit heeft van 0, wanneer q een priemgetal is in de vorm $4k+3$. We hoeven dus niet meer te kijken naar de kwadraticiteit van getallen die deelbaar zijn door een priemgetal in de vorm $4k+3$. Ook zagen we dat we niet meer hoefden te kijken naar even getallen, want die volgen uit de oneven getallen.

5.3 Getallen met elke priemfactor in de vorm $4k+1$

De enige getallen waarvoor we nog niet hebben aangetoond dat de kerststelling van Fermat klopt, zijn de getallen met alle priemfactoren in de vorm $4k+1$. Omdat delers van zulke getallen ook allemaal het product zijn van priemgetallen in de vorm $4k+1$, zijn die in de vorm $4k+1$. De kerststelling van Fermat zegt dus in dit geval dat de kwadraticiteit van een getal n met

alle priemfactoren in de vorm $4k+1$ gelijk is aan $\lceil \frac{1}{2} \cdot m \rceil$, waarin m het aantal delers is van n.

Merk op dat dit gelijk is aan het aantal oplossingen van $n = uv$. Als n geen kwadraat is, dan is het aantal oplossingen van $n = uv$ gelijk aan de helft van het aantal verschillende delers van n, dus het aantal oplossingen is gelijk aan $\frac{1}{2} \cdot m = \lceil \frac{1}{2} \cdot m \rceil$. Wanneer n wel een kwadraat is, dan is er één oplossing van $n = uv$, zodat $u = v$. De andere oplossingen komen wel voor in tweetallen. Hieruit volgt dat de andere het aantal oplossingen $n = uv$ gelijk is aan $\frac{1}{2} \cdot (m-1) + 1 = \lceil \frac{1}{2} \cdot m \rceil$.

We willen bewijzen dat het aantal oplossingen van $n = a^2 + b^2$ gelijk is aan het aantal oplossingen van $n = uv$, wanneer elke priemfactor van n in de vorm $4k+1$ is. Dit doen we door te laten zien dat het aantal oplossingen van $n = a^2 + b^2$, met $\gcd(a, b) = d$, gelijk is aan het aantal oplossingen van $n = uv$, met $\gcd(u, v) = d$, voor elk natuurlijk getal d.
Dit is hetzelfde als het bewijzen dat het aantal oplossingen van $n = (ad)^2 + (bd)^2$, met $\gcd(a, b) = 1$, gelijk is aan het aantal oplossingen van $n = (ud) \cdot (vd)$, met $\gcd(u, v) = 1$.

In andere woorden: Het aantal oplossingen van $\frac{n}{d^2} = a^2 + b^2$, met $\gcd(a, b) = 1$ is gelijk aan het aantal oplossingen van $\frac{n}{d^2} = uv$, met $\gcd(u, v) = 1$.

Omdat $\frac{n}{d^2}$ een deler is van n, is $\frac{n}{d^2}$ het product van priemgetallen in de vorm $4k+1$. Als we aannemen dat n het kleinste getal met alle priemfactoren in de vorm $4k+1$ is, waarvoor de kerststelling van Fermat niet waar is, dan moet het fout gaan bij $d = 1$. Dit is dus de enige d waarvoor we het aan hoeven tonen, want we mogen aannamen dat het klopt bij alle $d > 1$.
Het betekent dus hetzelfde om te bewijzen dat het aantal oplossingen $n = a^2 + b^2$, met $\gcd(a, b) = 1$ gelijk is aan het aantal oplossingen van $n = uv$, met $\gcd(u, v) = 1$, voor n met elke priemfactor in de vorm $4k+1$.

Het bewijs hiervan gaat iets te ver voor dit profielwerkstuk, dus ik zal het hier niet in verwerken.

6 Conclusie

Om te bepalen of een priemgetal te schrijven is als de som van twee kwadraten, hoeft er alleen gekeken te worden naar de rest na deling door 4. De enige mogelijkheid waarin deze rest even is, is bij het priemgetal 2, wat te schrijven is als de som van twee kwadraten: $1^2 + 1^2 = 2$.

Wanneer deze rest gelijk is aan 3, dan is het priemgetal te schrijven als $4k+3$. Zulke priemgetallen zijn nooit te schrijven als de som van twee kwadraten. Geen enkel getal in de vorm $4k + 3$ is te schrijven als de som van twee kwadraten.

De stelling van Fermat over de som van twee kwadraten stelt dat priemgetallen in de vorm $4k + 1$ altijd te schrijven zijn als de som van twee kwadraten. Wanneer een priemgetal te schrijven is als de som van twee kwadraten, dan volgt uit een vorm van de stelling van Brahmagupta-Fibunacci, dat dit op exact één manier kan.

Getallen die te schrijven zijn als de som van twee kwadraten, noem ik blije getallen. De hoofdstelling van de rekenkunde stelt dat elk natuurlijke getal op een unieke manier te schrijven is als het product van priemgetallen. Deze priemfactorisatie kan worden gebruikt om van een natuurlijk getal te bepalen of het wel of niet blij is. De algemene twee-kwadraten-stelling stelt namelijk dat een natuurlijk getal is te schrijven als de som van twee kwadraten dan en slechts dan als alle priemfactoren in de vorm $4k + 3$ van het getal een even exponent hebben.

Het aantal manieren om een geheel getal te schrijven als de som van twee kwadraten noem ik de kwadraticiteit. De kerststelling van Fermat geeft een formule voor de kwadraticiteit van natuurlijke getallen, op basis van de oneven delers van een getal.

De kwadraticiteit van een natuurlijk getal n is gelijk aan de helft van het verschil tussen het aantal delers in de vorm $4k + 1$ en het aantal delers in de vorm $4k + 3$. Wanneer hier geen geheel getal uitkomt, moet de uitkomst naar boven worden afgerond (op gehelen).

Met deze handige methode is het alleen nodig om het aantal delers in de vorm $4k+1$ en in de vorm $4k+3$ te tellen, om erachter te komen op hoeveel manieren een natuurlijk getal te schrijven is als de som van twee kwadraten.

Door het schrijven van dit profielwerkstuk ben ik beter geworden in het gebruiken van LaTeXvoor grote teksten. Ook ben ik beter geworden in het bedenken en vereenvoudigen van ingewikkelde bewijzen. Het vlak waarop ik het meest ben gegroeid is getaltheorie. Vooral bewijzen met priemgetallen en kwadratische residuen. Ik heb geleerd om kwadratische reciprociteit toe te passen en ik kan nu omgaan met kwadratische vormen.

Eigenlijk had ik in mijn profielwerkstuk ook willen laten zien welke getallen te schrijven zijn als de som van drie kwadraten. Het bewijs hiervoor was echter te ingewikkeld. Ik wilde hiervoor Legendre's bewijs gebruiken. Voor twee van de drie belangrijkste lemma's heb ik een redelijk elegant bewijs gevonden. Voor het laatste lemma wilde ik een zwakke versie van Dirichlet's stelling over priemgetallen in rekenkundige rijen bewijzen, maar dat heb ik naar mijn eigen mening onvoldoende kunnen vereenvoudigen. Ik zal me blijven verdiepen in het bewijs, in de hoop dat ik op een eleganter bewijs stuit.

Referenties

[Bri21] Brilliant. *Sum of squares theorems*. Mrt 2021. URL: brilliant.org/wiki/fermats-sum-of-two-squares-theorem/.

[Hof21] Henk Hofstede. *Priemfactoren*. Feb 2021. URL: h.hofstede.nl/modulus/priemfactoren.htm.

[Lev15] Paul Levrie. „Som van twee kwadraten". In: *Pythagoras* september (2015), p. 22–26.

[Mat19] Mathologer. *Fermat's Christmas theorem: Visualising the hidden circle in pi/4 = 1–1/3+1/5-1/7+...* Dec 2019. URL: youtube.com/watch?v=00w8gu2aL-w&t=980s.

[Mat20] Mathologer. *Why was this visual proof missed for 400 years? (Fermat's two square theorem)*. Jan 2020. URL: youtube.com/watch?v=DjI1NICfjOk.