Universiteit Utrecht

DIOPHANTISCHE DRIETALLEN EN ELLIPTISCHE KROMMEN

DEPARTEMENT WISKUNDE

BACHELORSCRIPTIE

Luke van de Kraats

Begeleid door
Prof. dr. G.L.M. CORNELISSEN

Academiejaar 2021-2022

Inleiding

Een diophantisch $m-$tupel, of $m-$tal, is een verzameling $\{a_1, a_2, \ldots, a_m\}$ waarvoor geldt dat als $a_i \cdot a_j + 1$ een perfect kwadraat is voor alle $1 \leq i < j \leq m$ met $i \neq j$. Al in het oude Griekenland werd er over deze verzamelingen nagedacht. Ook werd er naar het algemene geval bekeken waarbij niet $a_i \cdot a_j + 1$ een perfect kwadraat moet zijn maar $a_i \cdot a_j + a$ voor een willekeurige a. Het was de wiskundige Diophantus van Alexandrië die het als eerste bestudeerde. Voor $a = 1$ vond hij de algemene oplossing $x, x+2$ en $4x+4$ met $x \in \mathbb{Q}$. Later in de zestiende eeuw kwam F.Viète met een oplossing voor een willekeurige a. In de zeventiende eeuw was het de wiskundige Sluse die een andere algemene oplossing vond. In de achttiende eeuw was het werd er nog een oplossing gevonden door N. Saunderson.

Verder in de scriptie focussen wij ons op het geval dat $a = 1$. Voor dit geval was het Diophantus die zich afvroeg of er een diophantisch viertal bestaat. Op dat hij al een drietal had gevonden ging hij opzoek naar een uitbreiding van dit drietal. Zo vond hij geen algemene oplossing maar wel een viertal breuken die aan de eigenschap voldoen. Fermat was de eerste die een oplossing vond met gehele getallen. Maar het was Euler die als eerste met een algemene oplossing kwam. De oplossing vinden wij in stelling 1.1. Daarna ging Euler opzoek naar een vijftal, hij vond echter alleen een rationale uitbreiding.

In het volgende hoofdstuk bekijken wij de eigenschappen van diophantische $m-tupels$. Met name de vraag hoe groot deze verzamelingen kunnen worden. Wanneer wij naar rationale getallen kijken weten we dat er in ieder geval een zestal bestaat. Als eerst zien we een resultaat dat een diophantisch drietal altijd uitgebreid kan worden tot een diophantisch viertal. Dit zien wij in stelling 2.5. Verder zien wij het begrip van reguliere diophantische $m-$tupels. En een vermoeden dat elk diophantisch viertal regulier is. Tot slot zien we in stelling 2.9 dat er geen diophantische vijftallen bestaan.

Het hoofdstuk hierna gaat over de theorie van de elliptische krommen, en met name over de groepsstructuur die bij deze krommen hoort. Voordat wij een elliptische krommen definiëren, moeten wij eerst kubische krommen definiëren. Daarna behandelen wij bepaalde eigenschappen die deze krommen kunnen hebben. Zo behandelen wij eerst niet singuliere krommen. Daarna kijken wij naar krommen in het projectieve vlak en hoe we kubische krommen in Weierstrass normaal vorm kunnen schrijven . Nu we deze begrippen kennen kunnen wij elliptische krommen gaan definiëren.

Vervolgens gaan we de groepsstructuur op elliptische krommen behandelen. Zo definiëren wij de optelling van twee punten op de kromme door een lijn door deze punten te nemen, dan het derde snijpunt te nemen op de kromme en dan het punt in de x-as te spiegelen. Verder zien we ook een voorbeeld hoe deze optelling te werk gaat op een kromme. Als laatste zien wij de stelling van Mordell over elliptische krommen.

In het laatste hoofdstuk van deze scriptie zien wij hoe we de theorie van de elliptische krommen kunnen toepassen op diophantische drietallen. Hierbij zien we dat we een elliptische kromme kunnen maken op basis van een diophantisch drietal. Zo nemen wij voor het drietal $\{a,b,c\}$ de geïnduceerde kromme $y^2 = (ax+1)(bx+1)(cx+1)$. Eerst zien wij een aantal standaard punten die op deze kromme liggen. Verder zien we dat een punt op de geïnduceerde kromme een uitbreiding is van ons drietal. In stelling 4.4 zien wij de voorwaarde voor een rationaal punt op de kromme. Hierdoor kunnen we nieuwe punten vinden op de kromme en daardoor mogelijke uitbreidingen van het diophantisch drietal. Daarna hebben wij een stelling die ons een vijfde punt geeft op de kromme. En als slot hebben wij een stelling die zegt dat elk diophantisch viertal uitgebreid kan worden tot een rationaal vijftal. Zo moet er zelfs gelden dat het vijfde punt strikt kleiner is dan één.

Bewijzen heb ik zelf uitgewerkt, i.h.b. 1.1, 2.5 , 4.2 en 4.3 t.e.m. 4.5 zonder referentie naar descent op elliptische krommen.

Inhoudsopgave

1 Historische achtergrond

1.1 Drietallen waarvoor het product van twee van hen, verhoogd met a, een kwadraat is

In [4, pp.513–520] zien we dat het volgende wordt beschreven. De Griekse wiskundige Diophantus van Alexandrië bestudeerde als eerste het probleem van het vinden van drie rationale getallen zodanig dat het product van iedere combinatie van twee van hen, vermeerderd met een getal a, een perfect kwadraat is. Voor $a = 12$ vond hij de getallen $2, 2$ en $\frac{1}{8}$. We zien namelijk dat $2 \cdot 2 + 12 = 4^2$ en $2 \cdot \frac{1}{8} + 12 = (\frac{7}{2})^2$. Voor $a = 1$ vond hij oneindig veel oplossingen, namelijk in de vorm $x, x+2$ en $4x+4$ met $x \in \mathbb{Q}$. We zien dan dat

$$(x+2)x+1 = (x+1)^2$$
$$(4x+4)x+1 = (2x+1)^2$$
$$(x+2)(4x+4)+1 = 4x^2+10x+9 = (2x+3)^2$$

En dus voldoen deze getallen aan onze gevraagde eigenschap.

F.Viète kwam in 1591 als eerste met een oplossing voor dit probleem voor een willekeurige a. Laat A het eerste getal zijn van onze drietal. Dan geldt dat $\frac{B^2-a}{A}$ en $\frac{D^2-a}{A}$ het tot een drietal maken wanneer $\frac{B^2-a}{A} \cdot \frac{D^2-a}{A} + a$ een perfect kwadraat is. We kunnen nu $F^2 = B^2 - a$ en $G^2 = D^2 - a$ op oneindig veel manieren maken. Omdat $\frac{B^2-a}{A} \cdot \frac{D^2-a}{A} + a$ een perfect kwadraat moet zijn zien we dat $F^2G^2 + aA^2$ een perfect kwadraat moet zijn. Stel dat dit gelijk is aan $(FG - HA)^2$ voor een bepaalde H, dan moeten we F en G zodanig kiezen dat $A = 2HFG/(H^2 - a)$. En dit kan op oneindig veel manieren.

De Sluse vond in 1668 een andere oplossing voor het probleem. Hij zocht drie getallen x, y en z zodanig dat de gewenste eisen golden. Hij stelde b^2 gelijk aan een willekeurig kwadraat. Daarna stelde hij $d = b^2 - a$ en $xy = x^2 + 2xb + d$. Hieruit volgt dat $xy + a = (x+b)^2$. Op een zelfde manier stelde hij $z = \frac{xc^2}{e^2} + \frac{2bc}{e} + \frac{d}{x}$. Hieruit volgde dat $xz + a = (\frac{x}{ce} + b)^2$. Nu moet alleen $yz + a$ nog een kwadraat zijn. Hij nam aan dat $yz + a$ het kwadraat was van $\frac{cx+cb}{e} + b + \frac{d}{x}$. Daaruit volgt dat

$$\frac{2b^2c}{e} + \frac{dc^2}{e^2} = \frac{b^2c^2}{e^2} + \frac{2dc}{e}.$$

Wanneer b^2 vervangen wordt door $d + a$ dan wordt dit vereenvoudigd tot $2 = \frac{c}{e}$. Hieruit volgt dan dat de oplossing gegeven wordt door $x, y = x + 2b + \frac{d}{x}$ en $z = 4x + 4b + \frac{d}{x}$. Wanneer $a < 0$ stel $a = -A$ dan krijgen we $x, y = x + \frac{A}{x}$ en $z = \frac{xb^2}{c^2} + \frac{A}{x}$. Hierdoor zien we dat $xy - A = x^2, xz - A = \frac{x^2b^2}{c^2}$ en $yz - A = (\frac{xb}{c} + \frac{A}{x})^2$ als $\frac{b}{c} = 2$.

De blinde wiskundige N. Saunderson gaf in 1740 de volgende oplossing

$$x = \frac{r^2 - a}{r - s}, \quad y = \frac{s^2 - a}{r - s}, \quad z = r - s \quad \text{of} \quad z = 2x + 2y - (r - s).$$

waarbij $r, s > \sqrt{a}$ en $r > s$. Voor $a = 1$ vond hij de oplossing

$$x, \quad y = \alpha x + 2\alpha \quad z = \beta^2 x + 2\beta, \quad \text{met } \alpha - \beta = \pm 1.$$

1.2 Viertallen met a gelijk aan één

Later vroeg Diophantus zich af of het ook mogelijk was om 4 rationale getallen te vinden zodat het product van iedere combinatie van twee van hen, vermeerderd met 1, een perfect kwadraat is. Omdat hij al een vorm had gevonden voor drie van deze getallen ging Diophantus op zoek naar een vierde getal. Voor de eerste drie getallen koos hij dus $x, x+2$ en $4x+4$. Echter vond hij nu geen algemene oplossing voor het probleem. Toen hij $9x + 6$ als vierde nam, zag hij dat $(9x + 6)x + 1 = (3x + 1)^2$.

Maar Diophantus zag nu dat $(x+2)(9x+6)+1 = 9x^2+24x+13$ in het algemeen geen perfect kwadraat was. Voor $x=1$ zien we bijvoorbeeld dat $9x^2+24x+13 = 46$ wat geen kwadraat is. Echter geldt dat $(4x+4)(9x+6)+1 = 36x^2+60x+25 = (6x+5)^2$ wel een perfect kwadraat is. Diophantus zag dus dat voor elke $x \in \mathbb{Q}$ we een viertal van getallen hebben gevonden als $9x^2+24x+13$ een perfect kwadraat is. Als oplossing vond Diophantus $x = \frac{1}{16}$. Hij vond dit door $9x^2+24x+13$ gelijk te stellen aan $(3x-4)^2$. Diophantus had dus een viertal gevonden die aan de eisen voldeed namelijk $\frac{1}{16}, \frac{33}{16}, \frac{17}{4}$ en $\frac{105}{16}$.

Het was de Franse wiskundige Pierre de Fermat die als eerste een viertal vond van gehele getallen. Hij nam $1, 3$ en 8 als eerste drie getallen. Deze kreeg hij door bij de algemene oplossing van Diophantus voor de drietallen $x = 1$ in te vullen. Nu vroeg Fermat zich af of dit kon worden uitgebreid naar een viertal dus moest Fermat een getal x vinden zodanig dat $x+1 = \square, 3x+1 = \square$ en $8x+1 = \square$ waarbij $\square$ staat voor en perfect kwadraat. Hij vond al snel een oplossing namelijk $x = 120$. We zien namelijk dat

$$\begin{aligned} 1\cdot 3+1 &= 2^2, \quad 1\cdot 120+1 = 11^2 \\ 1\cdot 8+1 &= 3^2, \quad 3\cdot 120+1 = 19^2 \\ 3\cdot 8+1 &= 5^2, \quad 8\cdot 120+1 = 31^2 \end{aligned}$$

Het was Euler die als eerste een algemene oplossing van een viertal vond. Zijn resultaat vinden we in de volgende stelling [9, pp.329–344].

Stelling 1.1. Euler (1783). *Zij $a,b \in \mathbb{Q}$ waarvoor geldt dat $ab+1 = l^2$ met $l \in \mathbb{Q}$. Definieer $c = a+b+2l$ en $d = 4l(l+a)(l+b)$. Dan geldt dat het product van iedere combinatie van twee uit $\{a,b,c,d\}$, plus één, een perfect kwadraat is.*

Bewijs. We zien dat $bc+1$ en $bd+1$ perfecte kwadraten zijn dan en slechts dan als $ac+1$ en $ad+1$ perfecte kwadraten zijn. Eerst zien we dat

$$ac+1 = a(a+b+2l)+1 = a^2+ab+2al+1 = a^2+2al+l^2 = (a+l)^2.$$

Verder zien we dat

$$\begin{aligned} ad+1 = 4al(l+a)(l+b)+1 &= 4al(l^2+al+bl+ab)+1 \\ &= 4al^3+4a^2l^2+4abl^2+4a^2bl+1 \\ &= 4al^3+4a^2l^2+4(l^2-1)l^2+4a(l^2-1)l+1 \\ &= 4al^3+4a^2l^2+4l^4-4l^2+4al^3-4al+1 \\ &= 4a^2l^2+(8l^3-4l)a+4l^4-4l^2+1 \\ &= (2al)^2+4al(2l^2-1)+(2l^2-1)^2 \\ &= (2al+2l^2-1)^2. \end{aligned}$$

Nu rest ons alleen nog om aan te tonen dat $cd+1$ een perfect kwadraat is. We zien dan dat

$$\begin{aligned} cd+1 &= 4l(a+b+2l)(l+a)(l+b)+1 \\ &= 4l(a+b+2l)(l^2+al+bl+ab)+1 \\ &= 4l(al^2+bl^2+2l^3+a^2l+abl+2al^2+abl+b^2l+a^2b+ab^2+2abl)+1 \\ &= 4al^3+4bl^3+8l^4+4a^2l^2+4abl^2+8al^3+4abl^2+4b^2l^2+4a^2bl+4ab^2l+8abl^2+1 \\ &= 12al^3+12bl^3+8l^4+4(a^2+2ab+b^2)l^2+4a^2bl+4ab^2l+8abl^2+1 \\ &= 12al^3+12bl^3+8l^4+4(a+b)^2l^2+4a(l^2-1)l+4b(l^2-1)l+8(l^2-1)l^2+1 \\ &= 12al^3+12bl^3+8l^4+4(a+b)^2l^2+4al^3-4al+4bl^3-4bl+8l^4-8l^2+1 \\ &= 16l^4+16(a+b)l^3-8l^2+4(a+b)^2l^2-4(a+b)l+1 \\ &= (4l^2+2(a+b)l-1)^2 \end{aligned}$$

□

Daardoor vond Euler het viertal $3, 8, 21$ en 2080. Ook het door Fermat gevonden viertal is van deze vorm.

1.3 Vijftallen en meer

Vervolgens vroeg Euler zich af of het mogelijk was om dit het door hem gevonden viertal uit te breiden tot een vijftal die aan deze voorwaarde voldeed. Met andere woorden Euler zocht een getal z zodat $az+1, bz+1, cz+1$ en $dz+1$ allemaal kwadraten waren. Hij deed dit door het product van deze termen te nemen die hij P noemde. Laat

$$P = 1 + pz + qz^2 + rz^3 + sz^4$$

waarbij $p = a+b+c+d$, $q = ab+ac+ad+bc+bd+cd$, $r = abc+abd+acd+bcd$ en $s = abcd$. Hieruit leidde Euler af als

$$z = \frac{4r+2p(1+s)}{(s-1)^2}$$

dat P een kwadraat is. Daarna verklaarde Euler dat elke term $az+1, bz+1, cz+1$ en $dz+1$ een kwadraat is. Voor het viertal $1, 3, 8$ en 120 vond Euler dat

$$z = \frac{777480}{8288641}$$

het viertal een vijftal maakte. Voor een vijftal met kleinere getallen vond hij ook

$$\frac{1}{2}, \frac{5}{2}, 6, 48, \frac{44880}{128881}.$$

Tot nu toe is er nog nooit een vijftal getallen gevonden waarbij alle getallen gehele getallen zijn. In 1999 werd de eerste zestal gevonden door Gibbs [10] bestaande uit

$$\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}.$$

2 Diophantische m-tupels

2.1 Inleiding

In de geschiedenis zijn er al veel verzamelingen gevonden met de eigenschap dat het product van twee van hen plus één een perfect kwadraat is. Hieronder geven we een formele definitie van verzameling met die eigenschap. Ook maken we onderscheid voor verzamelingen bestaande uit gehele en rationale getallen.

Definitie 2.1. *Een verzameling $\{a_1, a_2, \ldots, a_m\}$ van natuurlijke getallen heet een diophantische $m-$tupel als $a_i \cdot a_j + 1$ een perfect kwadraat is voor alle $1 \leq i < j \leq m$ met $i \neq j$.*

Definitie 2.2. *Een verzameling $\{a_1, a_2, \ldots, a_m\}$ van rationale getallen ongelijk aan nul heet een rationale diophanitsche $m-$tupel als $a_i \cdot a_j + 1$ een perfect kwadraat is voor alle $1 \leq i < j \leq m$ met $i \neq j$.*

Voorbeeld 2.3. Zo hebben we gezien dat $\{1, 3, 8, 120\}$ een diophantische $4-$tupel is. Dit wordt ook een diophantische viertal genoemd.

Ook zien we dat $\{a_1, \ldots a_{m-1}\}$ een (rationale) diophantische $(m-1)$-tupel is wanneer $\{a_1, \ldots a_m\}$ een (rationale) $m-$tupel is. Dus als we een element uit een diophantische $m-$tupel halen houden we een diophantische $(m-1)$-tupel over.

Een eerste vraag die we ons kunnen stellen is hoe groot deze diophantische m-tupels kunnen worden. Voor rationale gevallen hebben we al gezien dat er een rationale diophantische zestal bestaat. Het is onbekend of er een absolute bovengrens bestaat voor de grootte van rationale diophantische $m-$tupels. In het geval van gehele getallen hebben we al gezien dat er oneindig veel diophantische drietallen bestaan. Ook zijn er oneindig veel diophantische tweetallen. Als $k^2 \in \mathbb{Q}$ dan vormt de verzameling $\{1, k^2 - 1\}$ een diophantisch tweetal. Deze constructie werkt ook als $k^2 \in \mathbb{Z}_{\geq 0}$. Voor een willekeurige $x \in \mathbb{Q}$ bewees Diophantus zelf dat $\{x, x+2, 4x+4\}$ een diophantische drietal is. In stelling 1.1 zagen we dat we een diophantisch tweetal kunnen uitbreiden naar een diophantisch viertal. Omdat we oneindig veel tweetallen hebben zullen er ook oneindig veel viertallen bestaan. Voor diophantische vijftallen is er recentelijk pas antwoord gekomen of ze bestaan of niet. Lang was er het het volgende vermoeden.

Vermoeden 2.4. *Er bestaan geen diophantische vijftallen.*

Later, in 2019, is dit vermoeden bewezen.

2.2 Diophantische vijftallen

Voordat we gaan kijken naar diophantische vijftallen kijken we eerst naar diophantische viertallen. Om preciezer te zijn kijken we eerst naar diophantische drietallen. Nu kunnen we ons de vraag stellen of elke diophantische drietal uit te breiden is tot een viertal. In stelling 1.1 zagen we dat elke diophantisch tweetal uitgebreid kan worden tot diophantisch drietal en viertal. In [1] zien we het volgende resultaat.

Stelling 2.5. *Zij $\{a, b, c\}$ een diophantisch drietal waarbij er $r, s, t \in \mathbb{N}$ bestaan zodanig dat $ab + 1 = r^2$, $ac + 1 = s^2$ en $bc + 1 = t^2$. Definieer $d_+ = a + b + c + 2abc + 2rst$ dan vormt $\{a, b, c, d_+\}$ een diophantisch viertal.*

Bewijs. We zien dat

$$\begin{aligned} ad_+ + 1 &= a(a + b + c + 2abc + 2rst) + 1 \\ &= a^2 + ab + ac + 2a^2bc + 2arst + 1 \\ &= a^2 + a^2bc + ab + ac + a^2bc + 1 + 2arst \\ &= a^2(bc + 1) + (ab + 1)(ac + 1) + 2arst \\ &= a^2t^2 + r^2s^2 + 2arst \\ &= (at + rs)^2 \end{aligned}$$

We moeten nu nog aantonen dat $bd_+ + 1$ en $cd_+ + 1$ een perfecte kwadraten zijn. Omdat dit analoog is met het aantonen dat $ad_+ + 1$ een kwadraat is zien we dat $bd_+ + 1 = (bs + rt)^2$ en $cd_+ + 1 = (cr + st)^2$ en is ons bewijs voltooid. □

Voorbeeld 2.6. Voor het diophantisch drietal $\{1,3,8\}$ vond Fermat dat 120 het tot een viertal maakt. Wanneer we $a=1,b=3$ en $c=8$ dan zien we dat $r=2,s=3$ en $t=5$ invullen in stelling 2.5 dan vinden we dat $d_+ = 1+3+8+2\cdot1\cdot3\cdot8+2\cdot2\cdot3\cdot5 = 12+48+60 = 120$, wat het door Fermat gevonden viertal is. Wanneer we $a=1,b=3$ en $c=120$ invullen dan vinden we $d_+ = 1+3+120+2\cdot1\cdot3\cdot120+2\cdot2\cdot11\cdot19 = 1680$. Hierdoor hebben we een nieuw diophantisch viertal gevonden, namelijk $\{1,3,120,1680\}$.

Nu we d_+ hebben gedefinieerd voor een diophantisch drietal kunnen we naar het volgende vermoeden kijken.

Vermoeden 2.7. *Als $\{a,b,c,d\}$ een diophantisch viertal is met $d > \max\{a,b,c\}$ dan geldt dat $d = d_+$.*

We merken op dat dit vermoeden sterker is dan vermoeden 2.4. We zien namelijk dat dit vermoeden impliceert dat er geen diophantische vijftallen bestaan. Dit komt doordat de uitbreiding van een diophantische viertal uniek moet zijn volgens vermoeden 2.7. Nu is dit vermoeden wel bewezen voor een aantal diophantische drietallen. In [2] wordt aangetoond dat als $\{1,3,8,d\}$ een diophantische viertal is dan moet gelden dat $d = 120$, de uitbreiding is uniek.

Omdat diophantische viertallen in de vorm van stelling 2.5 veel voorkomen hebben ze een eigen naam gekregen.

Definitie 2.8. *Een diophantisch viertal $D = \{a,b,c,d\}$ met $a < b < c < d$ heet regulier als $d = d_+$.*

Nu blijkt dat alle diophantische viertallen $\{a,b,c,d\}$ waarvoor geldt dat $\max\{a,b,c,d\} < 10^6$ regulier zijn. In totaal zijn dat 207 viertallen. Uiteindelijk krijgen we de volgende stelling

Stelling 2.9. *Er bestaan geen diophantische vijftallen.*

Deze stelling is in 2019 bewezen, en het bewijs vinden we in [11].

3 Elliptische krommen

3.1 Inleiding

Voordat we verder gaan kijken naar diophantische $m-$tupels gaan we eerst kijken naar kubische krommen, en in het bijzonder de elliptische krommen. In [12, pp.8–27] zien we dat

$$ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j=0$$

waarbij de termen $a,\ldots,i$ constanten zijn, de vergelijking geeft voor een algemene kubische kromme. We kunnen ons afvragen voor welke waarden van x en y geldt dat $(x,y)\in\mathbb{Q}^2$, dus welke rationale punten liggen er op de krommen.

Voorbeeld 3.1. Als we kijken naar de kromme $x^3+y^3=1$, dan blijkt het dat er geen rationale punten op deze kromme liggen. Als $(x,y)\in\mathbb{Q}^2$ een oplossing is van deze vergelijking dan zien we wanneer

$$x=\frac{a}{b} \quad \text{en} \quad y=\frac{c}{d}$$

dat geldt dat

$$\frac{a^3}{b^3}+\frac{c^3}{d^3}=1.$$

Dit is equivalent met

$$(ad)^3+(cb)^3=(bd)^3.$$

Onze oorspronkelijke krommen is dus homogeen met $X^3+Y^3=Z^3$. Wanneer we de rationale punten op $x^3+y^3=1$ willen vinden, kunnen we dus op zoek naar drie gehele getallen X,Y en Z waarvoor geldt dat $X^3+Y^3=Z^3$. Maar dankzij de laatste stelling van Fermat weten wij dat dit geen oplossingen heeft met $XYZ\neq 0$. Dus er zijn geen rationale punten op de kromme $x^3+y^3=1$ naast de twee triviale rationale punten $(1,0)$ en $(0,1)$.

Nu willen we gaan kijken of we een groep kunnen definiëren op de rationale punten op deze krommen. Dit blijkt echter niet het geval voor alle kubische krommen. We hebben eerst een paar eisen nodig voor de krommen voordat we een groep kunnen definiëren. Voor de groepsoperatie die we later gaan definiëren hebben we de raaklijn in een punt op de kromme nodig. Hiervoor introduceren wij eerst het volgende begrip.

Definitie 3.2. *Zij K een kubische kromme gegeven door $f(x,y)=0$ en $P\in K$ een punt op deze kromme. We noemen P singulier punt op K als $\frac{\partial f}{\partial x}(P)=\frac{\partial f}{\partial y}(P)=0$.*

Wanneer een punt P op een kubische kromme een partiële afgeleide heeft ongelijk aan nul noemen we dit punt niet-singulier.

Definitie 3.3. *Zij K een kubische kromme. Als voor alle $P\in K$ geldt dat P niet-singulier is, noemen we de kromme K niet-singulier.*

Een niet singuliere kubische kromme wordt ook wel een gladde kubische kromme genoemd.

3.2 Weierstrass normaal vorm

We hebben nu alleen nog één probleem wanneer we een groep definiëren op een niet-singuliere kubische kromme. Wanneer een punt een verticale raaklijn heeft kan het voorkomen dat deze de kromme alleen maar raakt in dat punt, en dus de kromme niet snijdt in een ander punt. Om dit probleem tegen te gaan moeten we een punt in oneindig definiëren. Dit doen we door onze kromme uit te breiden naar het projectieve vlak. In [12, pp.267] wordt het projectieve vlak als volgt gedefinieerd met behulp van een equivalentie klasse.

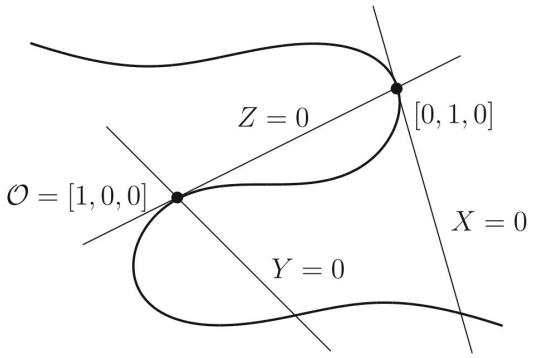
Definitie 3.4. *Zij $\sim$ een equivalentie klassen op $A=\{[a,b,c]\,|\,a,b,c\in\mathbb{R}\}\backslash[0,0,0]$ gegeven door $[a,b,c]\sim[a',b',c']$ als $a=ta',b=tb'$ en $c=tc'$ voor een $t\neq 0$. Dan noemen we de verzameling $\mathbb{P}^2=A/\sim$ het projectieve vlak.*

De getallen a,b,c noemen we de homogene coördinaten van het punt $[a,b,c]$ in $\mathbb{P}^2$. Nu kunnen we ook een lijn definiëren in $\mathbb{P}^2$ als de verzameling van punten $[a,b,c] \in \mathbb{P}^2$ van wie de coördinaten voldoen aan de vergelijking $\alpha X + \beta Y + \gamma Z = 0$ voor niet nul constanten α, β en γ.

We gaan nu kijken naar kubische krommen in de vorm

$$y^2 = x^3 + bx + c.$$

Deze vorm wordt ook wel de Weierstrass vorm genoemd. We gaan nu laten zien dat elke kubische kromme C met een rationaal punt $\mathscr{O}$ equivalent is met een kromme in Weierstrass vorm. We beschouwen de kromme C nu in het projectieve vlak. We gaan voor C de coördinaten van projectieve vlak bepalen zodanig dat C een makkelijkere vorm heeft. Als eerst kiezen we de lijn $Z = 0$ als de raaklijn in $\mathscr{O}$. Deze raaklijn snijdt de kromme in een ander punt. Nu kiezen we $X = 0$ als de raaklijn door dit nieuwe punt. Tot slot kiezen we $Y = 0$ als een andere lijn ongelijk aan $Z = 0$ die door $\mathscr{O}$ gaat. Zie figuur 1. Als we de assen bepaald hebben



Figuur 1: Bepalen van de assen[12, pp.17]

op deze manier laten we $x = X/Z$ en $y = Y/Z$, dit geeft een projectieve transformatie. Dan krijgen we C in de vorm

$$xy^2 + (ax+b)y = cx^2 + dx + e.$$

Als we vervolgens beide kanten met x vermenigvuldigen krijgen we

$$(xy)^2 + (ax+b)xy = cx^3 + dx^2 + ex.$$

Wanneer we xy opnieuw y noemen, dan krijgen we dat

$$y^2 + (ax+b)y = \text{derdegraads veelterm in } x.$$

Wanneer we opnieuw een lineaire transformatie uitvoeren waarbij y vervangen wordt door $y - \frac{1}{2}(ax+b)$ dan krijgen we

$$y^2 = \text{derdegraads veelterm in } x.$$

De derdegraads veelterm heeft misschien niet een kopcoëfficiënt van 1, maar dan kunnen we x en y vervangen door respectievelijk λx en $\lambda^2 y$ waarbij λ de kopcoëfficiënt is. Nu moeten we nog van de x^2 term af in de veelterm. Dit kunnen we doen als we x vervangen door $x - \alpha$ voor een goed gekozen α. Wat we nu overhouden is een kromme in Weierstrass normaal vorm die equivalent is met de kromme waarmee we begonnen zijn. In deze vorm zien we dat $\mathscr{O}$ naar het punt $Z = 0$ is gegaan. Nu kunnen we ook het begrip van elliptische krommen definiëren.

Definitie 3.5. *Een elliptische kromme is een niet-singuliere kubische kromme met een rationaal punt.*

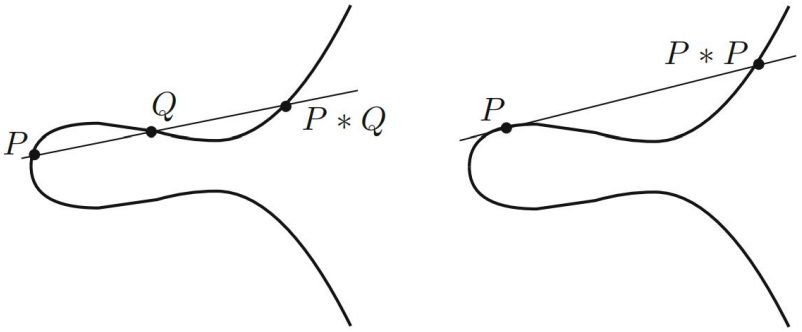
Als E een elliptische kromme is dan noteren we $E(\mathbb{Q})$ als de verzameling van rationale punten op de elliptische kromme. Vaak wordt een elliptische kromme gegeven door de vergelijking $y^2 = x^3 + ax + b$ waarbij $a,b \in \mathbb{R}$, dit is de vereenvoudigde vergelijking in Weierstrass normaal vorm. Verder moet hier gelden dat $\Delta = -16(4a^3 + 27b^2)$ niet nul mag zijn, Δ wordt de discriminant genoemd. Als de discriminant nul is dan heeft de kromme tenminste één singulier punt.

3.3 Groepsstructuur op kubische krommen

Het blijkt nu dat als we twee rationale punten hebben op een kubische krommen hebben, het mogelijk is om een derde rationaal punt te vinden. Wanneer we een lijn door de oorspronkelijke twee punten trekken dan heeft deze lijn rationale coëfficiënten. Deze lijn snijdt de kromme in een derde punt. Wanneer we de drie snijpunten van een rationale lijn, een lijn met rationale coëfficiënten, dan krijgen we een vergelijking met rationale coëfficiënten. Als twee nulpunten van deze vergelijking rationaal zijn dan moet de derde dat ook zijn. Nu kunnen we een compositie operatie definiëren op een kubische kromme.

Definitie 3.6. *Zij P en Q twee punten op een niet singuliere kubische kromme, dan noemen we $P*Q$ de compositie zoals hierboven gedefinieerd.*

Zelfs al we maar een rationaal punt op een kubische kromme hebben kunnen we een tweede rationale punt vinden. Stel dat P ons rationale punt is. Dan kunnen we de raaklijn in P tekenen. Wat we dan eigenlijk doen is de lijn door P en P tekenen. De raaklijn "raakt" het punt P dan eigenlijk twee keer. Nu is het andere snijpunt van de raaklijn weer een rationaal punt. Hierdoor kunnen we definitie 3.6 ook toepassen voor $P*P$. In figuur 2 zien we de compositie uitgebeeld. We zien dus wanneer we een rationaal punt hebben op een



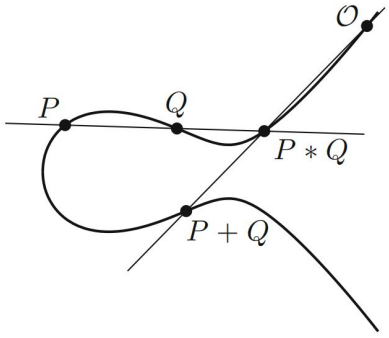
Figuur 2: Compositie tussen twee punten op een kubische kromme [12, pp.9]

kubische kromme, we meer rationale punten kunnen construeren. Het lijkt er nu op dat we de verzameling van rationale punten op een kubische kromme een groep is met betrekking tot de compositie. Maar echter is dit niet waar. Met onze definitie van de compositie zien we dat er geen identiteit bestaat. We kunnen geen punt $\mathcal{O}$ aanwijzen waarvoor geldt dat $P*\mathcal{O} = P$ voor alle rationale punten P.

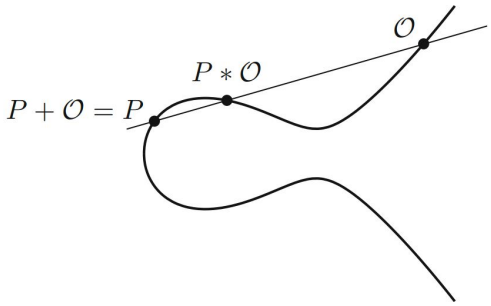
Stelling 3.7. *Zij P,Q en $\mathcal{O}$ rationale punten op een niet-singuliere kubische kromme in $\mathbb{P}^2$. Dan geeft $P+Q = \mathcal{O}*(P*Q)$ een optelling voor een groep met $\mathcal{O}$ als identiteit.*

Een exact bewijs van deze stelling vinden we in [12, pp.23–27]. Deze optelling trekt eerst een lijn door P en Q, en vinden hierdoor het punt $P*Q$. Daarna tekenen we de lijn door $P*Q$ en $\mathcal{O}$ om het punt $P+Q$ te vinden. In figuur 3 zien we dit uitgebeeld. We zien ook dat de kromme in het projectieve vlak gedefinieerd is. Dit komt wanneer we een punt hebben met een verticale raaklijn dan snijdt deze lijn de kromme niet in een ander punt. We moeten het punt $Z = 0$ meenemen in de groep. Wanneer we de compositie nemen van dit punt A, dan tekenen we een verticale lijn door P. Dan is het punt $P*A$ het nieuwe snijpunt van de kromme met de verticale lijn.

Het blijkt dat de optelling commutatief is. We zien namelijk dat $P+Q = Q+P$ voor alle rationale punten P en Q. Dit komt doordat de lijn door P en Q dezelfde lijn is als de lijn door Q en P. Dus $P*Q = Q*P$. We gaan nu een schets geven van het bewijs van stelling 3.7. Als eerst zien we dat $\mathcal{O}$ daadwerkelijk een identiteit definieert. We beweren dat $P+\mathcal{O} = P$ voor alle P op de kromme. Dit is equivalent met de bewering dat $\mathcal{O}*(P*\mathcal{O})$. Eerst we de lijn door P en $\mathcal{O}$ om $P*\mathcal{O}$ te bepalen. Wanneer we dan de lijn door $P*\mathcal{O}$ en $\mathcal{O}$ maken zien we dat dit weer dezelfde lijn is. Omdat P het derde punt op de lijn is geldt dat $P+\mathcal{O} = \mathcal{O}*(P*\mathcal{O}) = P$. Dit zien we in figuur 4. Nu moeten we een inverse element vinden voor elk punt Q op de kromme. Om de inverse te vinden zoeken we een punt $-Q$ zodat $Q+(-Q) = \mathcal{O}$. Dit doen we door eerst de raaklijn door $\mathcal{O}$ te tekenen. Het snijpunt van de kromme met de raaklijn noemen we S, dus



Figuur 3: Optelling van de groep op een kubische krommen[12, pp.12]



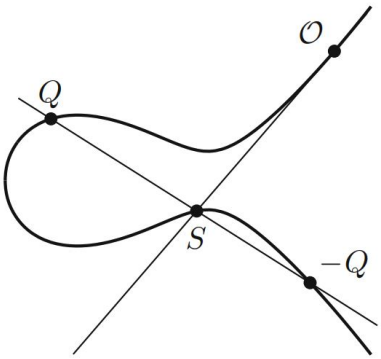
Figuur 4: Identiteit van de groep[12, pp.12]

$S = \mathscr{O} * \mathscr{O}$. Dan definiëren we $-Q = Q * S$. Wanneer we nu Q en $-Q$ bij elkaar optellen moeten we eerst de lijn door deze punten trekken. Dan is het derde punt op deze lijn S, dus $Q * -Q = S$. Om de optelling te voltooien moeten we nu de lijn door S en $\mathscr{O}$ tekenen. We zien dan dat deze lijn $\mathscr{O}$ raakt in plaats van snijd. De lijn raakt het punt $\mathscr{O}$ dus twee keer. We zien dan dat $\mathscr{O} * S = \mathscr{O}$. Nu volgt hieruit dat $Q + (-Q) = \mathscr{O}$. Dit wordt in figuur 5 weergeven.

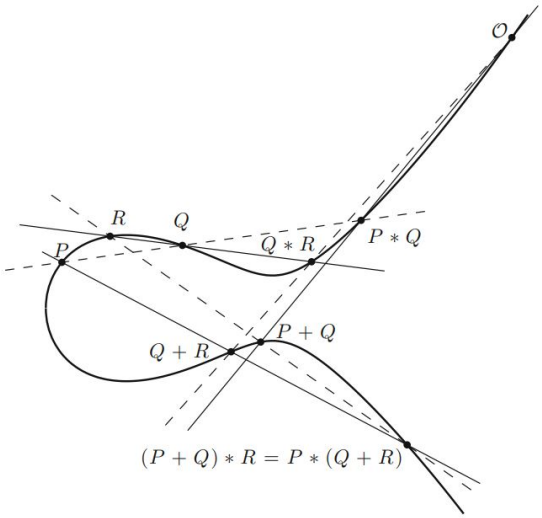
We moeten nu alleen nog laten zien dat de optelling associatief is. Laat P, Q en R drie punten op de kromme zijn. Dan gaan we laten zien dat $(P+Q)+R = P+(Q+R)$. Om $P+Q$ te krijgen moeten we eerst het punt $P*Q$ krijgen door een lijn door P en Q te trekken. Daarna moeten we de lijn door $\mathscr{O}$ en $P*Q$ maken. Om vervolgens $(P+Q)+R$ te vinden moeten we eerst het punt $(P+Q)*R$ maken. Daarna moeten we nog een lijn door $(P+Q)*R$ en $\mathscr{O}$. Om dit duidelijk in een figuur weer te kunnen geven gaan we laten zien dat $(P+Q)*R = P*(Q+R)$. Wanneer dat dezelfde punten zijn volgt direct dat $(P+Q)+R = P+(Q+R)$. Om $P*(Q+R)$ te maken moeten we eerst $Q*R$ maken, en dan een lijn te trekken door $Q*R$ en $\mathscr{O}$. Hierdoor vinden we $Q+R$. Dan moeten we $Q+R$ en P met een lijn verbinden. Waardoor wij het punt $P*(Q+R)$ kunnen vinden. Nu blijkt het dat dit hetzelfde punt is als $(P+Q)*R$. Zie figuur 6.Een exact bewijs van de associativiteit van de groep vinden we in [12, pp.23–27]. We hebben nu alle groepsaxioma's behandeld. Verder zien we dat we een groep hebben die afhankelijk is van onze keuze van $\mathscr{O}$. Wanneer we een andere identiteit $\mathscr{O}'$ kiezen blijkt het dat de groep zich hetzelfde blijft gedragen. De afbeelding $P \mapsto P + \mathscr{O}'$ is een isomorfisme van de groep $(C, \mathscr{O}, +)$ naar $(C, \mathscr{O}', +')$ voor een kubische kromme C, waarbij de nieuwe optelling is gedefinieerd als $P +' Q = P + Q - \mathscr{O}'$.

Voorbeeld 3.8. Zij $y^2 = x^3 + 17$ een kubische kromme. Dan zien we dat $P = (-1,4)$ en $Q = (2,5)$ twee rationale punten op deze kromme zijn. Om een derde rationale punt op deze kromme te vinden gaan we eerst $P*Q$ uitrekenen. De vergelijking van de lijn door P en Q wordt gegeven door

$$y = \frac{1}{3}x + \frac{13}{3}.$$



Figuur 5: Inverse element[12, pp.13]



Figuur 6: Inverse element[12, pp.14]

Wanneer we dit in de oorspronkelijke vergelijking invullen krijgen we

$$(\frac{1}{3}x+\frac{13}{3})^2 = x^3+17.$$

Wanneer we dit uitwerken krijgen we

$$0 = x^3 - \frac{1}{9}x^2 - \frac{26}{9}x - \frac{16}{9}.$$

Omdat we al twee oplossing weten van deze vergelijking kunnen we de vergelijking eenvoudig ontbinden. We zien dan dat

$$0 = (x+1)(x-2)(x+\frac{8}{9}).$$

Daaruit volgt dat $P * Q = (-\frac{8}{9}, \frac{109}{27})$. We hebben nu een derde rationale punt gevonden op de kromme. We merken op dat het punt $(-\frac{8}{9}, -\frac{109}{27})$ ook op onze kromme ligt, omdat de kromme symmetrisch is in de x-as. Om nog een punt te kunnen berekenen kunnen we ook eerst het punt $P * P$ bepalen. Hiervoor moeten we eerst de raaklijn in P bepalen. Omdat de y-coördinaat van P positief is kijken we naar de functie $f(x) = \sqrt{x^3+17}$. We zien dan dat

$$f'(x) = \frac{3x^2}{2\sqrt{x^3+17}}.$$

De richtingscoëfficiënt van de raaklijn in P wordt dan gegeven door $f'(-1) = \frac{3}{8}$. De vergelijking van de raaklijn wordt nu gegeven door $y = \frac{3}{8}x + \frac{35}{8}$. Om het snijpunt van de raaklijn met de kubische kromme te bepalen moeten we de volgende vergelijking oplossen

$$(\frac{3}{8}x + \frac{35}{8})^2 = x^3 + 17.$$

Dit is equivalent met

$$0 = x^3 - \frac{9}{64}x^2 - \frac{105}{32}x - \frac{137}{64}.$$

Omdat de raaklijn de kromme in P raakt weten we dat $x = -1$ een oplossing is met multipliciteit twee. Daaruit volgt dat

$$0 = x^3 - \frac{9}{64}x^2 - \frac{105}{32}x - \frac{137}{64} = (x+1)^2(x - \frac{137}{64}).$$

We zien nu dat $P * P = (\frac{137}{64}, \frac{2651}{512})$. We hebben nu drie nieuwe rationale punten gevonden op de kubische kromme.

In het bovenstaande voorbeeld hebben we gezien hoe we nieuwe rationale punten kunnen vinden op een kubische kromme. Nu is het de vraag of we met deze methode alle rationale punten kunnen vinden gegeven een aantal rationale punten. Het antwoord op deze vraag vinden we in de volgende stelling.

Stelling van Mordell 3.9. *Als een niet singuliere kubische kromme een rationaal punt bevat, dan is de groep van rationale punten eindig voortgebracht.*

Een bewijs van deze stelling vinden we in [12, pp.95]. Wat deze stelling ons verteld voor een kromme C, is dat er rationale punten $P_1, \ldots, P_t \in C(\mathbb{Q})$ bestaan zodat voor elk punt $p \in C(\mathbb{Q})$ in de vorm $\sum_{k=1}^{t} a_k P_k$ met $a_k \in \mathbb{Z}$ voor alle $1 \leq k \leq t$ geschreven kan worden. We zien nu dat voor ieder van de punten P_i twee dingen kan gelden, ze hebben een eindige orde of zijn van orde oneindig. Wanneer ze een eindige orde hebben bestaat er een n_i zodat $n_i P_i = \mathcal{O}$. Dit wordt ook wel een torsie punt genoemd. Voor de groep $E(\mathbb{Q})$ zien we nu dat

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus < T >,$$

Waarbij T een torsiegroep is, een groep waar elk element een eindige orde heeft.

4 Het verband tussen diophantische m-tupels en elliptische krommen

4.1 Diophantische drietallen en elliptische krommen

Zij $\{a,b,c\}$ een diophantisch drietal, dan bestaan er $r,s,t \in \mathbb{N}$ zodanig dat

$$ab+1=r^2, \quad ac+1=s^2, \quad bc+1=t^2.$$

Wanneer we dit willen uitbreiden naar een diophantisch viertal dan zoeken we een getal $x \in \mathbb{N}$ zodanig dat

$$ax+1=\square, \quad bx+1=\square, \quad cx+1=\square. \tag{*}$$

Hierbij staat de notatie $\square$ voor een perfect kwadraat. Nu kunnen we een elliptische kromme maken uit de waarde van het diophantisch drietal.

Definitie 4.1. *Zij $\{a,b,c\}$ een diophantisch drietal. We noemen $E: y^2=(ax+1)(bx+1)(cx+1)$ de door $\{a,b,c\}$ geïnduceerde elliptische kromme.*

Omdat a,b en c allemaal verschillend zijn is E niet singulier. Wanneer x een oplossing is van $(*)$ dan zien we dat het punt (x,y) een punt is op de elliptische kromme. Nu moeten we ons nog gaan afvragen welke rationale punten op de kromme een oplossing geven voor het stelsel $(*)$.

We vinden nu drie rationale punten op E, namelijk $A=(-\frac{1}{a},0), B=(-\frac{1}{b},0)$ en $C=(-\frac{1}{c},0)$. Wanneer we naar de groep van E kijken met het punt in oneindig als identiteit dan zien we dat A,B en C allemaal orde twee hebben. Dit komt doordat doordat de raaklijn in de punten A,B en C verticale lijnen zijn. Verder is $P=(0,1)$ ook een rationaal punt op E. In [6] zien het volgende. Ook hebben we nog een vijfde rationaal punt op de kromme E. Dit punt wordt gegeven door $S=(\frac{1}{abc},\frac{rst}{abc})$. Daarna vinden wij een punt R waarvoor geldt dat $S=2R$. Dit punt wordt gegeven door

$$R=(\frac{rs+rt+st+1}{abc},\frac{(r+s)(r+t)(s+t)}{abc}).$$

We gaan nu eerst een tweetal lemma's definiëren en bewijzen. Deze lemma's gaan we nodig hebben voor een stelling die later volgt.

Lemma 4.2. *Zij $(G,+)$ en $(H,\cdot)$ twee abelse groepen. Laat $f: G \to H$ een afbeelding tussen G en H zijn waarvoor geldt dat voor elk drietal $P,Q,R \in G$ geldt dat*

(i) $f(-P)=f(P)^{-1}$

(ii) Als $P+Q+R=0$*, dan* $f(P)f(Q)f(R)=1$

Dan is de afbeelding f een groepshomomorfisme.

Bewijs. Zij $P,Q \in G$. Dan bestaat er altijd een $R \in G$ zodat $P+Q+R=0$. Dan zien we dat $P+Q=-R$. Voor deze drie elementen zien we dat door (ii) geldt dat $f(R)^{-1}=f(P)f(Q)$. Dan volgt dat

$$f(P+Q)=f(-R)=f(R)^{-1}=f(P)f(Q).$$

Nu zien we dat de afbeelding f een groepshomomorfisme is. □

Lemma 4.3. *Zij E een elliptische kromme over $\mathbb{Q}$ gegeven door*

$$y^2=(x-\alpha)(x-\beta)(x-\gamma)=x^3+ax^2+bx+c$$

met $\alpha,\beta,\gamma \in \mathbb{Q}$. Voor $(x',y') \in E(\mathbb{Q})$ bestaat er een punt $(x,y) \in E(\mathbb{Q})$ met $2(x,y)=(x',y')$ dan en slechts dan als $x'-\alpha, x'-\beta$ en $x'-\gamma$ kwadraten zijn.

Bewijs. De vergelijking $2(x,y) = (x',y')$ heeft een oplossing op $E(\mathbb{Q})$ dan en slechts dan als de vergelijking $2(x,y) = (0,y')$ een oplossing heeft op de kromme gegeven door

$$y^2 = (x+x'-\alpha)(x+x'-\beta)(x+x'-\gamma).$$

Hierdoor wordt het probleem teruggebracht om het lemma te bewijzen voor een speciaal punt $(0,y')$. In ons geval is dat $y'^2 = -\alpha\beta\gamma$. Als $2(x,y) = (0,y')$ dan heeft de raaklijn in het punt (x,y) op de kromme E een vergelijking in de vorm $y = \lambda x + \nu$. Wanneer we dit invullen krijgen we dat

$$(\lambda x+\nu)^2 = x^3 + ax^2 + bx + c.$$

We zien dat $\nu = y'$ en $\nu^2 = y'^2 = -\alpha\beta\gamma - c$. Dan krijgen we de vergelijking

$$0 = x(x^2 + (a-\lambda^2)x + (b-2\lambda\nu)).$$

Omdat $y = \lambda x + \nu$ een raaklijn is in (x,y) weten we dat x een nulpunt is met multipliciteit 2. Hieruit volgt dat de vergelijking $x^2 + (a-\lambda^2)x + (b-2\lambda\nu)$ een discriminant heeft van nul. Hieruit volgt dat

$$(\lambda^2 - a)^2 = 4(b - 2y'\lambda).$$

Dit is een kwadratische vergelijking voor λ. Deze vergelijking van λ gaan we oplossen door beide kanten een kwadraat te maken. Hiervoor gebruiken we een $u \in \mathbb{Q}$. Dan zien we dat

$$(\lambda - a + u)^2 = 2u\lambda - 8\lambda y' + (u^2 + 4b - 2ua).$$

Hierbij is de rechterkant een kwadraat dan en slechts dan als de discriminant weer nul is. Dit geeft ons

$$0 = 64c - 8u(u^2 + 4b - 2ua).$$

Dit is equivalent met

$$0 = u^3 - 2ua + 4bu - 8c.$$

Om deze vergelijking op te lossen voor u maken we de substitutie $u = -2v$. dit geeft ons de vergelijking

$$0 = -8(v^3 + av^2 + bv + c).$$

Wat weer de vergelijking van de kromme geeft. We zien dat de oplossing van deze vergelijking worden gegeven door $v = \alpha, \beta, \gamma$. Dit geeft ons de oplossing van de derde graads vergelijking van u, namelijk $u = -2\alpha, -2\beta, -2\gamma$. Nu substitueren we $u = -2\alpha$ in de kwadratische vergelijking van λ. Dan zien we dat moet gelden $-a = \alpha + \beta + \gamma, \quad b = \alpha\beta + \beta\gamma + \gamma\alpha$ en $c = -\alpha\beta\gamma$. Dus de vergelijking van λ wordt dan

$$(\lambda^2 + \alpha + \beta + \gamma - 2\alpha)^2 = -4\alpha\lambda^2 - 8y'\lambda + (4a^2 + 4(\alpha\beta + \beta\gamma + \gamma\alpha) - 4\alpha(\alpha + \beta + \gamma)).$$

Laat nu $\alpha'^2 = -\alpha, \beta'^2 = -\beta$ en $\gamma'^2 = -\gamma$. Dan wordt de vergelijking

$$\begin{aligned}(\lambda^2 + \alpha + \beta + \gamma - 2\alpha)^2 &= -4\alpha\lambda^2 - 8y'\lambda + 4\beta\gamma \\ &= 4(\alpha'\lambda - \beta'\gamma')^2.\end{aligned}$$

Wanneer we nu de wortel nemen van allebei de kanten krijgen we

$$\lambda^2 + \beta + \gamma - \alpha = \pm 2(\alpha'\lambda - \beta'\gamma').$$

Dit is gelijk aan de vergelijking

$$\lambda^2 \mp 2\alpha'\lambda - \alpha = -\beta \mp 2\beta'\gamma' - \gamma.$$

Dit is weer equivalent aan

$$(\lambda \mp \alpha')^2 = (\beta' \mp \gamma')^2.$$

Wanneer we nu de wortel nemen van beide kanten zien we dat er 4 oplossingen vinden voor λ. Dus er bestaat een $\lambda \in \mathbb{Q}$ die de richting van de raaklijn in het punt (x,y). Ook zien we dat er een punt (x,y) bestaat zodat $2(x,y) = (0,y')$. Dit geeft ons het resultaat van dit lemma. □

Om te zien welke punten op de geïnduceerde krommen een oplossing van $(*)$ geven, kijken we naar de volgende stelling [6].

Stelling 4.4. *De $x-$coördinaat van een punt $T \in E(\mathbb{Q})$ voldoet aan $(*)$ dan en slechts dan als $T-P \in 2E(\mathbb{Q})$.*

Bewijs. We definiëren $E' : y^2 = (x+bc)(x+ac)(x+ab)$, deze kromme krijgen we door in de kromme E de transformatie $(x,y) \mapsto (\frac{x}{abc}, \frac{y}{abc})$ toe te passen. Voor een punt $X = (x,y) \in E(\mathbb{Q})$ definiëren wij $X' = (xabc, yabc) \in E'(\mathbb{Q})$. Nu kunnen we de volgende afbeelding $\varphi_a : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ definiëren,

$$\varphi_a(X') = \begin{cases} (x+bc)\mathbb{Q}^{*2}, & \text{als } X' = (x,y) \neq \mathscr{O}, A' \\ (ac-bc)(ab-bc)\mathbb{Q}^{*2}, & \text{als } X' = A' \\ (1)\mathbb{Q}^{*2}, & \text{als } X' = \mathscr{O} \end{cases}$$

De verzameling $\mathbb{Q}^{*2}$ is hier de verzameling van kwadraten in $\mathbb{Q}$. Dit geeft ons dat $\mathbb{Q}^*/\mathbb{Q}^{*2}$ de groep van rationale getallen is waarbij we alle kwadraten gelijk stellen aan één met betrekking tot de gebruikelijke vermenigvuldiging. Verder is het punt $A' = (-bc, 0)$ gegeven. Op dezelfde manier kunnen we ook de afbeeldingen φ_b en φ_c definiëren. We gaan aantonen dat de afbeelding φ_a een homomorfisme is. Hiervoor maken we gebruik van lemma 4.2. We gaan eerst de eisen van het lemma langs. Eerst merken we op dat de groepen $E'(\mathbb{Q})$ en $\mathbb{Q}/\mathbb{Q}^{*2}$ abelse groepen zijn.

We zien voor een punt $P = (x,y) \in E'(\mathbb{Q})$ dat $-P = (x,-y)$. Omdat de afbeelding φ_a onafhankelijk is van de $y-$coördinaat zien we dat $\varphi_a(-P) = \varphi_a(P)$. We zien dan dat $\varphi_a(P)\varphi_a(P) = \varphi_a(P)^2 = (1)\mathbb{Q}^{*2}$. Hieruit volgt dat $\varphi_a(-P) = \varphi_a(P)^{-1}$. Nu moeten we nog aantonen dat als $P+Q+R = \mathscr{O}$, dan $\varphi_a(P)\varphi_a(Q)\varphi_a(R) = 1$. Dit doen we door een gevalsonderscheiding te maken. Wanneer $P+Q+R = \mathscr{O}$ dan moeten deze punten op een lijn liggen.

Neem aan dat $P,Q,R \neq A'$ en $P,Q,R \neq \mathscr{O}$. Stel dat de lijn door P,Q en R gegeven wordt door de vergelijking $y = \lambda x + \nu$. Nu noemen we de $x-$coördinaten van de punten P,Q en R respectievelijk x_P, x_Q en x_R. We zien dat x_P, x_Q en x_R de nulpunten zijn van de vergelijking

$$(\lambda x + \nu)^2 = (x+bc)(x+ac)(x+ab).$$

Wanneer we dit omschrijven krijgen we

$$0 = x^3 + (ab+ac+bc-\lambda^2)x^2 + (a^2bc+ab^2c+abc^2-2\lambda\nu)x + a^2b^2c^2 - \nu^2.$$

Omdat x_P, x_Q en x_R hier de nulpunten van zijn krijgen we dat

$$\begin{aligned} 0 &= x^3 + (ab+ac+bc-\lambda^2)x^2 + (a^2bc+ab^2c+abc^2-2\lambda\nu)x + a^2b^2c^2 - \nu^2 \\ &= (x-x_P)(x-x_Q)(x-x_R) \\ &= x^3 + (-x_P-x_Q-x_R)x^2 + (x_Px_Q + x_Px_R + x_Qx_R)x - x_Px_Qx_R \end{aligned}$$

Hieruit volgt dat

$$\begin{aligned} x_P + x_Q + x_R &= \lambda^2 - (ab+ac+bc) \\ x_Px_Q + x_Px_R + x_Qx_R &= a^2bc + ab^2c + abc^2 - 2\lambda\nu \\ x_Px_Qx_R &= \nu^2 - (abc)^2 \end{aligned}$$

Daaruit volgt dat

$$\begin{aligned} \varphi(P)\varphi(Q)\varphi(R) &= (x_P+bc)(x_Q+bc)(x_R+bc) \\ &= x_px_Qx_R + (x_Px_Q + x_Px_R + x_Qx_R)bc + (x_P+x_Q+x_R)(bc)^2 + (bc)^3 \\ &= \nu^2 - (abc)^2 + (a^2bc+ab^2c+abc^2-2\lambda\nu)bc + (\lambda^2 - ab - ac - bc)(bc)^2 + (bc)^3 \\ &= \nu^2 - (abc)^2 + (abc)^2 + ab^3c^2 + ab^2c^3 - 2\lambda\nu bc + (\lambda bc)^2 - ab^3c^2 - ab^2c^3 - (bc)^3 + (bc)^3 \\ &= \nu^2 - 2\lambda\nu bc + (\lambda bc)^2 \\ &= (\lambda bc - \nu)^2 \\ &= (1)\mathbb{Q}^{*2} \end{aligned}$$

We hebben nu de eis van lemma 4.2 aangetoond wanneer de punten P,Q en R allemaal niet $\mathscr{O}$ of A' zijn. Nu gaan we kijken naar de andere gevallen. Wanneer een van de drie punten gelijk is aan $\mathscr{O}$, stel $R=\mathscr{O}$, dan zien we dat voor de andere punten moet gelden dat $P=-Q$, anders liggen ze niet op een lijn. Omdat $\varphi(-P)=\varphi_a(P)^-1$ volgt dat $\varphi(P)\varphi(Q)\varphi(R)=\varphi(\mathscr{O})=(1)\mathbb{Q}^{*2}$. Wanneer we zonder verlies van algemeenheid aannemen dat $P=Q=\mathscr{O}$, dus twee punten gelijk aan $\mathscr{O}$, dan moet ook gelden dat $R=\mathscr{O}$. Hieruit volgt $\varphi(P)\varphi(Q)\varphi(R)=(1)\mathbb{Q}^{*2}$. We moeten nu nog het lemma aantonen in de gevallen dat één of twee punten gelijk zijn aan A'.

Wanneer één van de punten gelijk is aan A', zeg $P=A'$ en $Q,R\neq A'$, dan weten we dat $x_P=-bc$. Ook hier kunnen we de vergelijking van de lijn $y=\lambda x+\nu$ nemen waar al onze punten op liggen. Omdat het punt $A'=(-bc,0)$ op deze lijn ligt dan zien we dat $\nu=\lambda bc$. Dan krijgen we dat

$$(\lambda x+\lambda bc)^2=(x+bc)(x+ac)(x+ab).$$

Dit omschrijven geeft

$$0=x^3+(ab+ac+bc-\lambda^2)x^2+bc(a^2+ab+ac-2\lambda^2)x+b^2c^2(a^2-\lambda^2).$$

Verder moet er gelden dat

$$\begin{aligned}0&=x^3+(ab+ac+bc-\lambda^2)x^2+bc(a^2+ab+ac-2\lambda^2)x+b^2c^2(a^2-\lambda^2)\\&=(x-bc)(x-x_Q)(x-x_R)\\&=x^3-(x_Q+x_R+bc)x^2+(bcx_Q+bcx_R+x_Qx_R)x-bcx_Qx_R\end{aligned}$$

Nu zien we dat moet gelden

$$\begin{aligned}x_Q+x_R&=\lambda^2-(ab+ac)\\x_Qx_R+bcx_Q+bcx_R&=bc(a^2+ab+ac-2\lambda^2)\\x_Qx_R&=bc(a^2-\lambda^2)\end{aligned}$$

Hieruit volgt dat

$$\begin{aligned}\varphi(A')\varphi(Q)\varphi(R)&=(ac-bc)(ab-bc)(x_Q+bc)(x_R+bc)\\&=(a^2bc-ab^2c-abc^2+b^2c^2)(x_Qx_R+bcx_R+bcx_Q+b^2c^2)\\&=b^4c^4+(x_Q+x_R-ac-ab)b^3c^3+(a^2bc-acx_Q-acx_R-abx_Q-abx_R+x_Qx_R)b^2c^2\\&+(a^2bcx_Q+a^2bcx_R-acx_Qx_R-abx_Qx_R)bc+a^2bcx_Qx_R\\&=b^4c^4+(\lambda^2-2ac-2ab)b^3c^3+(4a^2bc-ac\lambda^2-ab\lambda^2+a^2b^2+a^2c^2-\lambda^2bc)b^2c^2\\&+(a^2bc\lambda^2+ab^2c\lambda^2+abc^2\lambda^2-2a^3b^2c-2a^3bc^2)bc+a^4b^2c^2-a^2b^2c^2\lambda^2\\&=b^2c^2(a^4-2a^3c+a^2c^2-2a^3b+4a^2bc-2abc^2+a^2b^2-2ab^2c+b^2c^2+a^2b^2-2ab^2c+b^2c^2)\\&=b^2c^2(a^2-2ab+b^2)(a^2-2ac+c^2)\\&=b^2c^2(a-b)^2(a-c)^2\\&=(1)\mathbb{Q}^{*2}\end{aligned}$$

Tot slot hebben we het geval dat Wanneer twee punten gelijk zijn aan A', zeg $P=Q=A'$ dan zien we dat $R=\mathscr{O}$, dit komt doordat A' orde 2 heeft dus $P+Q+R=\mathscr{O}+R=R$, wanneer dit gelijk moet zijn aan $\mathscr{O}$ moet dus gelden dat $R=\mathscr{O}$. Hieruit volgt dat $\varphi(P)\varphi(Q)\varphi(R)=\varphi(A')^2=(1)\mathbb{Q}^{*2}$. We hebben nu alle mogelijke situaties van de punten P,Q en R behandeld. Hierdoor kunnen we nu lemma 4.2 toepassen. We concluderen nu dat de afbeelding φ_a een groepshomomorfisme is. Op dezelfde manier kunnen we nu aantonen dat de afbeeldingen ϕ_b en ϕ_c ook groepshomomorfismen zijn.

Voor het punt $P'=(0,abc)$ zien we dat $\varphi_a(P')=(bc)\mathbb{Q}^{*2},\varphi_b(P')=(ac)\mathbb{Q}^{*2}$ en $\varphi_c(P')=(ab)\mathbb{Q}^{*2}$. Zij $T\in E(\mathbb{Q})$. Dan volgt per definitie dat $T'\in E'(\mathbb{Q})$. Dan volgt dat T_x voldoet aan $(*)$ dan en slechts dan als

$$\varphi_a(T')=\varphi_a(P'),\quad \varphi_b(T')=\varphi_b(P'),\quad \varphi_c(T')=\varphi_c(P').$$

Dit is equivalent met

$$\varphi_a(T'-P') = \varphi_b(T'-P') = \varphi_c(T'-P') = (1)\mathbb{Q}^{*2}.$$

We gaan nu aantonen dat dit geldt dan en slechts dan als $X' = P' - T' \in 2E'(\mathbb{Q})$, of in andere woorden dat er een $X'' \in E'(\mathbb{Q})$ bestaat zodat $X' = 2X''$. Dit komt overeen met de bewering dat voor de afbeelding

$$\varphi : E'(\mathbb{Q}) \to (\mathbb{Q}/\mathbb{Q}^{*2})^3 \quad \text{met} \quad X' \mapsto (\varphi_a(X'), \varphi_b(X'), \varphi_c(X'))$$

geldt dat $\mathrm{Ker}(\varphi) = 2E'(\mathbb{Q})$.

Laat $Y \in 2E'(\mathbb{Q})$. Dan bestaat er een $Z \in E'(\mathbb{Q})$ zodanig dat $Y = 2Z$. Dan zien we dat

$$\varphi(Y) = \varphi(2Z) = \varphi(Z+Z) = (\varphi_a(Z+Z), \varphi_b(Z+Z), \varphi_c(Z+Z)) = (\varphi_a(Z)^2, \varphi_b(Z)^2, \varphi_c(Z)^2).$$

We zien dus dat $Y \in \mathrm{Ker}(\varphi)$. Hieruit volgt dat $2E'(\mathbb{Q}) \subseteq \mathrm{Ker}(\varphi)$. Laat nu $Y \in \mathrm{Ker}(\varphi)$. Dan geldt dat $\varphi_a(Y) = \varphi_b(Y) = \varphi_c(Y) = (1)\mathbb{Q}^{*2}$. We zien dan dat $Y_x + bc, Y_x + ab$ en $Y_x + ac$ allemaal kwadraten zijn. Nu volgt met lemma 4.3 dat $Y \in 2E'(\mathbb{Q})$. Nu concluderen wij dat $\mathrm{Ker}(\phi) = 2E'(\mathbb{Q})$. Dit geeft ons het resultaat van de stelling. □

4.2 Uitbreiding naar een vijftal

Voor de geïnduceerde kromme $E : y^2 = (ax+1)(bx+1)(cx+1)$ voor een diophantisch drietal $\{a,b,c\}$ weten we dat de punten

$$S = (\frac{1}{abc}, \frac{rst}{abc}), \quad R = (\frac{rs+rt+st+1}{abc}, \frac{(r+s)(r+t)(s+t)}{abc}) \quad \text{en} \quad P = (0,1)$$

op deze kromme liggen. Omdat geldt dat $S = 2R$ zien we dat $S \in 2E(\mathbb{Q})$. Nu volgt uit stelling 4.4 dat de $x-$coördinaat van het punten $P+S$ en $P-S$ een oplossing zijn van $(*)$. We gaan nu $(P+S)_x$ en $(P-S)_x$ berekenen. Voor de lijn tussen P en S zien we dat deze gegeven wordt door de vergelijking $y = (rst - abc)x + 1$. Wanneer we dit in de vergelijking van de krommen invullen dan krijgen we

$$((rst-abc)x+1)^2 = (ax+1)(bx+1)(cx+1).$$

Dit is equivalent met

$$(rst-abc)^2x^2 + 2(rst-abc)x + 1 = abcx^3 + (ab+ac+bc)x^2 + (a+b+c)x + 1.$$

Omdat we al twee nulpunten weten van deze vergelijking kunnen we gemakkelijk de vergelijking ontbinden en vinden we dat

$$0 = x(x - \frac{1}{abc})(x - (a+b+c+2abc-2rst)).$$

We zien nu dus dat $(P+S)_x = a+b+c+2abc-2rst$. Met een dezelfde berekening vinden we dat $(P-S)_x = a+b+c+2abc+2rst$. Nu zien we dat $(P-S)_x = d_+$ zoals we die in hoofdstuk 2 gedefinieerd hebben. Een ander interessant resultaat zien we in de volgende stelling

Stelling 4.5. *Als de x-coördinaat van een punt $T = (p,q) \in E(\mathbb{Q})$ voldoet aan $(*)$ dan geldt voor de punten $T \pm S = (u,v)$ dat $pu+1$ een kwadraat is.*

Bewijs. Laat $T = (p,q) \in E(\mathbb{Q})$ waarbij p voldoet aan $(*)$. Eerst kijken we naar $T+S$, hier zien we dat de punten T en S op de lijn liggen met de vergelijking

$$y = \lambda x + q - p\lambda \quad \text{met} \quad \lambda = \frac{qabc - rst}{pabc - 1}.$$

Wanneer we dit invullen in de vergelijking van de kromme dan krijgen we

$$y = (\lambda x + q - p\lambda)^2 = (ax+1)(bx+1)(cx+1).$$

Dit is equivalent met

$$\begin{aligned}
0 &= abcx^3 + (ab+ac+bc-\lambda^2)x^2 + (a+b+c-2\lambda p+2\lambda^2 p)x + 1 - p^2 + 2p^2\lambda - p^2\lambda^2 \\
&= abcx^3 + (ab+ac+bc-(\frac{qabc-rst}{pabc-1})^2)x^2 + (a+b+c-2\frac{qabc-rst}{pabc-1}p \\
&+ 2(\frac{qabc-rst}{pabc-1})^2 p)x + 1 - p^2 + 2p^2\frac{qabc-rst}{pabc-1} - p^2(\frac{qabc-rst}{pabc-1})^2 \\
&= abc(x-p)(x-\frac{1}{abc})(x-\frac{(a+b+c+p)(pabc+1+2abc+2abp+2acp+2bcp+2rst\sqrt{ap+1}\sqrt{bp+1}\sqrt{cp+1})}{(pabc-1)^2})
\end{aligned}$$

Omdat p een oplossing is van $(*)$ zien wij nu dat

$$u = \frac{(a+b+c+p)(pabc+1+2abc+2abp+2acp+2bcp+2rst\sqrt{ap+1}\sqrt{bp+1}\sqrt{cp+1})}{(pabc-1)^2} \in \mathbb{Q}.$$

Om dezelfde manier vinden wij voor $T-S$ dat

$$u = \frac{(a+b+c+p)(pabc+1+2abc+2abp+2acp+2bcp-2rst\sqrt{ap+1}\sqrt{bp+1}\sqrt{cp+1})}{(pabc-1)^2}.$$

We noteren nu

$$u = \frac{(a+b+c+p)(pabc+1+2abc+2abp+2acp+2bcp\pm 2rst\sqrt{ap+1}\sqrt{bp+1}\sqrt{cp+1})}{(pabc-1)^2}.$$

Nu zien we dat

$$pu+1 = \frac{(p\sqrt{ap+1}\sqrt{bp+1}\sqrt{cp+1}\pm rst)^2}{(pabc-1)^2}.$$

Hiermee is de stelling bewezen. □

Omdat u in dit bewijs symmetrisch is ten opzichten van de getallen a,b,c en p zien we dat ook $au+1, bu+1$ en $cu+1$ ook kwadraten zijn.

Stelling 4.6. *Elk diophantisch viertal $\{a,b,c,d\}$ kan uitgebreid worden tot een rationaal diophantisch vijftal $\{a,b,c,d,u\}$ waarvoor geldt dat $u<1$.*

Bewijs. In stelling 4.5 zien we dat wanneer we een diophantisch viertal $\{a,b,c,d\}$ hebben dat er dan een getal u bestaat zodat $\{a,b,c,d,u\}$ een diophantisch vijftal is. We gaan nu aantonen dat $u<1$ [5]. Hieruit volgt dat $u \in \mathbb{Q}\backslash\mathbb{Z}$. Voor het diophantisch viertal $\{a,b,c,d\}$ geldt dat

$$u = \frac{(a+b+c+d)(abcd+1+2abc+2abd+2acd+2bcd+2rst\sqrt{ad+1}\sqrt{bd+1}\sqrt{cd+1})}{(abcd-1)^2}.$$

Dan noteren wij

$$\begin{aligned}
\sigma_1 &= a+b+c+d \\
\sigma_2 &= ab+ac+ad+bc+bd+cd \\
\sigma_3 &= abc+abd+acd+bcd \\
\sigma_4 &= abcd \\
X &= \sigma_1\sigma_4+2\sigma_3+\sigma_1 \\
Y &= rst\sqrt{ad+1}\sqrt{bd+1}\sqrt{cd+1}
\end{aligned}$$

Dan zien wij dat

$$u = \frac{X+2Y}{(\sigma_4-1)^2}.$$

Zonder verlies van algemeenheid kunnen wij aannemen dat $a<b<c<d$. Wanneer $a=1$ dan zien we dat $b \neq 2$ want $2\cdot 1+1 = 3 \notin \mathbb{Q}^{*2}$. Hieruit volgt dat $b \geq 3, c \geq 4$ en $d \geq 5$. Daaruit volgt dat $\sigma_1 \geq 13$ en

$\sigma_4 \geq 60$. Wanneer $a \neq 1$ dan zien we dat σ_4 groter wordt omdat de termen gelijk blijven of groter worden. We zien dus dat $\sigma_4 \geq 60$. Dan volgt dat

$$\frac{\sigma_1}{\sigma_4} = \frac{1}{abc} + \frac{1}{abd} + \frac{1}{acd} + \frac{1}{bcd} \leq \frac{13}{60} < \frac{1}{4}.$$

Dan zien we dat $52 \leq 4\sigma_1 < \sigma_4$. Op dezelfde manier vinden we dat $59 \leq \sigma_2 < \sigma_4$ en $107 \leq \sigma_3 < 2\sigma_4$. Dan voglt dat

$$(\sigma_4 - 1)^2 - 2X > \sigma_4^2 - 2\sigma_4 + 1 - \frac{\sigma_4^2}{2} - 8\sigma_4 - \frac{\sigma_4}{2} = \frac{1}{2}(\sigma_4^2 - 21\sigma_4 + 2) > 0.$$

Het laatste gedeelte is groter dan nul omdat $\sigma_4 \geq 60$. We zien dus dat $2X < (\sigma_4 - 1)^2$.

Verder zien we dat

$$\begin{aligned} Y^2 &= (ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1) \\ &= \sigma_4^3 + \sigma_2\sigma_4^2 - \sigma_4^2 + \sigma_1\sigma_3\sigma_4 + \sigma_1^2\sigma_4 - 2\sigma_2\sigma_4 + \sigma_3^2 - \sigma_4 + \sigma_1\sigma_3 + \sigma_2 + 1 \\ &< \sigma_4^3 + \sigma_4^3 - \sigma_4^2 + \frac{\sigma_4^3}{2} + \frac{\sigma_4^3}{16} - 118\sigma_4 + 4\sigma_4^2 - \sigma_4 + \frac{\sigma_4^2}{2} + \sigma_4 + 1 \\ &= \frac{14}{16}\sigma_4^3 + \frac{7}{2}\sigma_4^2 - 118\sigma_4 + 1. \end{aligned}$$

Hieruit volgt dat

$$\begin{aligned} (\sigma_4 - 1)^4 - 16Y^2 &> \sigma_4^4 - 4\sigma_4^3 + 6\sigma_4^2 - 4\sigma_4 + 1 - 41\sigma_4^3 - 56\sigma_4^2 + 1888\sigma_4 - 16 \\ &= \sigma_4^4 - 45\sigma_4^3 - 50\sigma_4^2 + 1888\sigma_4 - 15 > 0. \end{aligned}$$

We zien nu dat $4Y < (\sigma_4 - 1)^2$. Nu concluderen wij dat

$$u = \frac{X + 2Y}{(\sigma_4 - 1)^2} < \frac{(\sigma_4 - 1)^2}{(\sigma_4 - 1)^2} = 1.$$

Hiermee hebben we aangetoond dat het vijftal $\{a, b, c, d, u\}$ een rationaal diophantisch vijftal is waarvoor geldt dat $u < 1$. □

Actuele ontwikkelingen

Wij hebben nu een aantal resultaten gezien in de theorie van de diophantische $m-$tupels en in het bijzonder het verband met de theorie van de elliptische krommen. Tegenwoordig wordt er ook nog onderzoek gedaan naar diophantische $m-$tupels.

Zo zien wij dat er in [8] gekeken wordt naar diophantische $m-$tupels over het eindige lichaam $\mathbb{F}_p$. Hierbij wordt er ook een formule gegeven voor het aantal diophantische $m-$tupels in $\mathbb{F}_p$. En ander resultaat in dit artikel is dat er minstens één diophantisch $m-$tupel bestaat in $\mathbb{F}_p$ wanneer geldt dat $p > 2^{2m-2}m^2$.

Verder wordt er in [7] gekeken naar de torsiegroep van een geïnduceerde elliptische krommen. Ook wordt hier aangetoond dat er oneindig veel diophantische drietallen over een kwadratisch lichaam bestaan als de geïnduceerde krommen een bepaalde torsiegroep heeft.

We hebben in deze scriptie gezien dat we elk diophantisch drietal kunnen uitbreiding naar een viertal. In [3] word er gekeken of deze uitbreiding uniek is. Dit artikel ondersteunt het vermoeden dat de uitbreiding uniek is.

Referenties

[1] Joseph Arkin, Verner E. Hoggatt, Jr., and Ernst G. Straus. On Euler's solution of a problem of Diophantus. *Fibonacci Quart.*, 17(4):333–339, 1979.

[2] Alan Baker and Harold Davenport. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math. Oxford Ser. (2)*, 20:129–137, 1969.

[3] Mihai Cipu, Andrej Dujella, and Yasutsugu Fujita. Diophantine triples with largest two elements in common. *Period. Math. Hungar.*, 82(1):56–68, 2021.

[4] Leonard Eugene Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[5] Andrej Dujella. On Diophantine quintuples. *Acta Arith.*, 81(1):69–79, 1997.

[6] Andrej Dujella. Diophantine m-tuples and elliptic curves. volume 13, pages 111–124. 2001. 21st Journées Arithmétiques (Rome, 2001).

[7] Andrej Dujella, Mirela Jukić Bokun, and Ivan Soldo. On the torsion group of elliptic curves induced by Diophantine triples over quadratic fields. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 111(4):1177–1185, 2017.

[8] Andrej Dujella and Matija Kazalicki. Diophantine m-tuples in finite fields and modular forms. *Res. Number Theory*, 7(1):Paper No. 3, 24, 2021.

[9] Leonard Euler. *Opuscula Analytica I*. 1783.

[10] Philip Gibbs. Some rational Diophantine sextuples. *Glas. Mat. Ser. III*, 41(61)(2):195–203, 2006.

[11] Bo He, Alain Togbé, and Volker Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, 371(9):6665–6709, 2019.

[12] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.