DE GESCHIEDENIS VAN

DE VERGELIJKING VAN PELL

Afstudeerscriptie van
L. M. Hugenholtz
Onder begeleiding van
J. Hogendijk en R. Tijdeman

Inhoudsopgave

Hoofdstuk 1

Inleiding

Deze scriptie behandelt de vergelijking van Pell, haar geschiedenis, en de verschillende methoden om haar op te lossen. Er is al veel gepubliceerd over deze vergelijking. Het is als relatief makkelijk probleem populair in boeken over getaltheorie, en vooral de diverse oplossingen uit het Europa van de zeventiende eeuw zijn goed gedocumenteerd, en een dankbaar onderwerp van studie.

Er is daarentegen nog geen werk dat alles dat er aan de vergelijking van Pell is gedaan samenvat. Het dichtst daarbij komt een boek uit 1901 van H.Konen geheten "*Geschichte der Gleichung* $t^2 - Du^2 = 1$", maar dit boek besteedt nauwelijks aandacht aan historische achtergrond. Deze scriptie is bedoeld om dit gat op te vullen.

Over een periode van tenminste tweeduizend jaar is er in verschillende culturen aan de vergelijking van Pell gewerkt, en het is bijzonder interessant de verschillende oplossingen naast elkaar te leggen. Door de eeuwen zien we de voorwaarden van het probeem aangescherpt worden, zien we de aannames veranderen, en zien we het wiskundig inzicht vooruitgaan, doordat men voortbouwt op wat al bewezen is. We zullen ook bewijzen dat de op het oog verschillende oplossingen meer met elkaar te maken hebben dan op het eerste gezicht duidelijk is.

Na een korte introductie van het probleem zelf in Hoofdstuk 2 zullen we in Hoofdstukken 3, 4, 5 en 6 de verschillende manieren bekijken waarop de vergelijking van Pell (gedeeltelijk) is opgelost. In Hoofdstuk 6 behandelen we de moderne methode, die gebruik maakt van kettingbreuken. Daarna zullen we in Hoofdstuk 7 de overeenkomsten tussen de verschillende methoden laten zien. Tenslotte behandelen we in Hoofdstuk 8 een algebraïsche manier om naar de vergelijking te kijken en het oplossen van de vergelijking $x^2 - Ay^2 = k$, met k een geheel getal.

Hoofdstukken 3, 4, 5 en 6 vallen elk uiteen in drie delen. In het eerste deel wordt achtergrondinformatie gegeven over het tijdperk en de betrokken wiskundigen. In het tweede deel volgt een behandeling van het werk dat de desbetreffende wiskundigen hebben bijgedragen aan het oplossen van de vergelijking van Pell. Het laatste stuk zal steeds bestaan uit een omzetting naar moderne notatie, en het interpreteren van de oude resultaten in termen van onze huidige wiskundige kennis. Vaak vinden we resultaten die niet in het desbetreffende tijdperk gevonden zijn, maar die wel belangrijk zijn om correctheid aan te tonen, of om de ene methode met de andere te kunnen vergelijken.

Het eerste deel van zo'n hoofdstuk is grotendeels op basis van secundaire literatuur, zoals de diverse 'History of Number Theory' boeken, en de Dictionary of Scientific Biography. Het tweede deel is zo veel mogelijk op basis van primaire literatuur. Het derde deel is eigen werk, vaak geholpen door berekeningen of voorbeelden uit de secundaire literatuur. Hoofdstukken 2 en 7 zijn mijn eigen werk.

De moeilijkheidsgraad van deze scriptie wisselt. De inleidingen en letterlijke behandelingen van het werk uit vroeger tijden zouden te volgen moeten zijn voor een enthousiaste middelbare scholier; dat is in ieder geval mijn bedoeling. De wiskundige analyses en de hoofdstukken over kettingbreuken zijn daarentegen een stuk moeilijker, en enige bekendheid met universitair wiskundige werkwijze wordt hier dan ook verondersteld. Het is echter prima mogelijk deze hoofdstukken of secties over te slaan, en zodoende een overzicht te krijgen van wat er de afgelopen tweeduizend jaar is gedaan op het gebied van de vergelijking van Pell.

1.1 Een woord over notatie

In dit hele werk zal ik refereren aan 'de vergelijking van Pell'. Technisch gezien is deze naam om meerdere redenen incorrect. Het spreekt bijvoorbeeld vanzelf dat Indiase wiskundigen uit de achtste eeuw het niet over 'de vergelijking van Pell' hadden, aangezien Pell een Engels wiskundige uit de Renaissance was. Bovendien lijkt de toeschijving aan Pell op een misverstand te berusten.[1]

Echter, 'de vergelijking van Pell' is tegenwoordig de standaard naam voor dit probleem. Het leest ook een stuk prettiger dan de formele definitie uit het volgende hoofdstuk. Ik zal in de historische hoofdstukken dan ook voor zover mogelijk de historisch correcte naam noemen, maar daarna de moderne naam gebruiken.

Dit verschil is nog duidelijker in de gebruikte wiskundige notatie. Er is in tweeduizend jaar veel vooruitgang geboekt op dit gebied. Het gebruik van va-

[1] zie hoofdstuk 6

riabelen voor bekende grootheden en het gebruik van indices voor iteratie zijn twee bijzonder handige dingen die bijvoorbeeld de Indiërs niet tot hun beschikking hadden. Ook hier geldt dat ik de originele notatie zo goed mogelijk zal weergeven, maar het meeste van mijn wiskundige analyses in moderne notatie zal doen. Niet alleen is dit een stuk prettiger voor de lezer, maar bovendien is een belangrijk onderwerp van deze scriptie het vergelijken van verschillende algoritmes, en daarvoor is het noodzakelijk dat ze in vergelijkbare notatie staan.

Ik heb als gevolg hiervan in een aantal citaten de namen van variabelen veranderd. Waar ik dit gedaan heb zal ik het aangeven. Dit is enkel om deze citaten beter leesbaar te maken in hun context; het is bijvoorbeeld bijzonder vervelend als een citaat een variabele n heeft die naar iets anders verwijst dan de variabele n die ik gebruik in de rest van de desbetreffende sectie.

Een notatieconventie die ik meteen maar zal noemen is dat kleine letters typisch staan voor onbekende grootheden, en hoofdletters voor bekende grootheden. Als ik bijvoorbeeld $p^2 + Q = R$ opschrijf is dat een familie vergelijkingen waarbij Q en R gegeven zijn, en er een p wordt gezocht die aan de vergelijking voldoet. Dit zal uiteraard overal netjes gedefiniëerd worden, maar het is een conventie die makkelijk leest.

1.2 Literatuur

Deze scriptie is gedeeltelijk een geschiedkundig werk. Als zodanig is bronvermelding erg belangrijk. Achterin staat een overzicht van de boeken die ik gebruikt heb, met een beschrijving van ieder boek. Verwijzingen in de tekst staan meestal in voetnoten, en zijn verkort tot '*achternaam auteur - titel*', of 'het boek van *achternaam auteur*'.

De meeste makkelijk te vinden literatuur bestaat helaas uit overzichtswerken. Vaak zijn deze onvolledig op historisch gebied, of maken ze zelfs fouten. Het opzoeken van oorspronkelijke teksten is daarentegen tijdrovend, en het kost vaak veel moeite het stuk te vinden dat je nodig hebt. Ik heb dan ook een paar keer iets aangenomen uit een secundaire bron die naar een primaire bron verwijst, zonder dit zelf te controleren. Waar dit is gebeurd zal het in de tekst aangeven.

Tenslotte merk ik op dat directe citaten worden weergegeven in *dit lettertype.*

1.3 Dankwoord

Ik wil graag van deze gelegenheid gebruik maken om mijn afstudeerdocenten, prof. Jan Hogendijk en prof. Rob Tijdeman te bedanken voor hun begeleiding en feedback. Het is een voorrecht dat ik heb mogen werken met twee mensen die zo goed zijn in hun vakgebied, en elkaar zo goed aanvullen. Hetzelfde geldt voor prof. Hendrik Lenstra, mijn derde lezer.

Daarnaast gaat mijn dank uit naar de studentassisstenten in kamer 205 van het Snellius gebouw, die mij nooit uit hun kamer hebben gezet.

Hoofdstuk 2

De vergelijking van Pell

2.1 $x^2 - Ay^2 = 1$

Het oplossen van de vergelijking van Pell is een probleem uit de getaltheorie. Getaltheorie is de tak van wiskunde die zich onder andere bezighoudt met gehele getallen.

Kies een positief geheel getal A, dat geen kwadraat is. De vergelijking van Pell luidt nu:

$$x^2 - Ay^2 = 1$$

Gevraagd wordt om gehele x en y die aan deze vergelijking voldoen.

Omdat je A van te voren kiest kun je zeggen dat de vergelijking van Pell een *familie* van problemen is, één probleem voor iedere mogelijke waarde van A.

Stel dat we de vergelijking van Pell op willen lossen voor $A = 12$, dan zouden we met een beetje puzzelen kunnen bedenken dat $x = 7$, $y = 2$ een oplossing is. Immers $7^2 - 12 \cdot 2^2 = 49 - 48 = 1$. Willen we daarentegen de vergelijking voor $A = 61$ oplossen, dan halen we dat niet met puzzelen en proberen alleen: de kleinste oplossing is $x = 1766319049$, $y = 226153980$. De rest van deze scriptie zal diverse manieren laten zien om dergelijk grote oplossingen te vinden, en zal aantonen dat deze manieren sterk op elkaar lijken. Vooralsnog gaan we eerst goed naar het probleem zelf kijken.

2.2 Een eerste analyse

Allereerst kunnen we opmerken dat als we 0 zouden toestaan voor x of y, we ieder Pell probleem op kunnen lossen door $x = 1$ en $y = 0$ te kiezen. Dit is de zogeheten *triviale oplossing*. Daarom eisen we dat x en y groter zijn dan 0.

Het is makkelijk om aan te tonen dat als we reële getallen toestaan, we zonder moeite voor iedere gegeven $x, |x| > 1$ een antwoord kunnen vinden:

$x^2 - Ay^2 = 1$, dus $y = \sqrt{\frac{x^2-1}{A}}$. Het vinden van een oplossing in reeële getallen is dus triviaal.[1]

Ook in rationale getallen bestaat altijd een oplossing, hoewel je iets meer moeite moet doen om die te vinden. Kies een willekeurig positief geheel getal p, en definieer $q = p^2 - A$. Kies nu $x = \frac{p^2+A}{p^2-A}$, $y = \frac{2p}{q}$. Nu volgt:

$$x^2 - Ay^2 = \frac{(p^2+A)^2}{q^2} - \frac{4Ap^2}{q^2} = \frac{p^4-2Ap^2+A^2}{q^2} = 1.$$

Het is mogelijk dat x of y negatief is. Deze variabelen komen in de vergelijking echter alleen als kwadraten voor, en daarom is het mogelijk om eventuele negatieve variabelen met -1 te vermenigvuldigen zonder dat dit invloed heeft op de berekening. Dit maakt in hedendaagse wiskunde niet uit, maar was belangrijk in de tijd dat negatieve getallen niet als 'echte' getallen werden beschouwd.

Zo blijkt dat de vergelijking van Pell in rationale getallen ook niet bijzonder moeilijk is.[2]

Het wordt wel lastig als we eisen dat x en y gehele getallen zijn. Zoals we net al hebben opgemerkt komen x en y alleen voor als kwadraten. Als (x, y) een oplossing is zijn $(\pm x, \pm y)$ allemaal oplossingen. We mogen daarom aannemen dat x en y positief zijn.[3]

We eisen dat $A > 0$, omdat als $A = 0$ we $x = \pm 1$ kunnen kiezen, en alle y dan mogelijk zijn. Immers, $1 - 0 \cdot y^2 = 1$.

Als A een kwadraat is, is alleen de triviale oplossing mogelijk. Stel dat A een kwadraat is, bijvoorbeeld $A = b^2, b \neq 0$, dan geldt dat $x^2 - b^2y^2 = 1$. Omdat

[1] Als $|x| = 1$ volgt de triviale oplossing. Als $|x| < 1$ krijgen we een oplossing waarbij y een complex getal is.

[2] De Engelse wiskundigen Wallis en Brouncker hebben hier en groot conflict over gehad met de Franse wiskundige Fermat, zie daarvoor Hoofdstuk 5.

[3] Het is de moeite waard op te merken dat het een tijd geduurd heeft tot negatieve getallen werden toegestaan als oplossingen voor dit soort vergelijkingen. Zie bijvoorbeeld de constructies van Wallis en Brouncker in Hoofdstuk 5.

$x^2 - b^2y^2 = (x - by) \cdot (x + by)$ moet gelden dat $(x - by) = (x + by) = \pm 1$. Door de twee termen bij elkaar op te tellen volgt dat $2x = \pm 2$, dus $x = \pm 1$. Daaruit volgt dat $y = 0$.

2.3 Toepassingen van de vergelijking van Pell

Hoe komt een wiskundige er op de vergelijking van Pell te bestuderen? Het ziet er op het eerste gezicht niet uit als iets dat praktisch toepasbaar is. Toch heeft Pell's vergelijking raakvlakken met veel interessante onderwerpen binnen de getaltheorie.

Een oplossing (x, y) van de vergelijking van Pell voor een gegeven A levert een goede benadering van $\sqrt{A}$, zeker als x en y groot zijn. Immers, $x^2 - Ay^2 \approx 0$, dus $x \approx y\sqrt{A}$ en $\sqrt{A} \approx \frac{x}{y}$. Aangezien wortels veelvuldig voorkomen in vlakke meetkunde (en toepassingen daavan, zoals berekeningen over architectuur en landmeetkunde) is het nuttig om breuken te hebben die wortels goed benaderen. We zullen dit verband uitgebreid bespreken in Hoofdstuk 6, waar we ook zullen quantiseren hoe 'goed' deze benaderingsbreuken zijn.

De vergelijking van Pell maakt het mogelijk sommige getallen snel in factoren te ontbinden. Dit gaat via het volgende principe:

Stel we hebben voor een gegeven A twee bekende vergelijkingen: $x_1^2 - Ay_1^2 = k$ en $x_2^2 - Ay_2^2 = k$. Dan geldt dat $(x_1x_2 - Ay_1y_2)^2 - A(x_1y_2 - x_2y_1)^2 = (x_1^2 - Ay_1^2)(x_2^2 - Ay_2^2) = k^2$, en daarmee dat $(x_1x_2 - Ay_1y_2)^2 - k^2 = A(x_1y_2 - x_2y_1)^2$.

De linkerkant van deze laatste vergelijking is te ontbinden in $(x_1x_2 - Ay_1y_2 - k)(x_1x_2 - Ay_1y_2 + k)$. In veel gevallen verdelen de priemfactoren van A zich over deze twee factoren: in dat geval kunnen we $x_1y_2 - x_2y_1$ uitdelen aan beide kanten, en hebben we een factorisatie $A = \frac{x_1x_2 - Ay_1y_2 - k}{x_1y_2 - x_2y_1} \cdot \frac{x_1x_2 - Ay_1y_2 + k}{x_1y_2 - x_2y_1}$. In het geval dat $x_1^2 - Ay_1^2 = 1$ kunnen we dee eerste stappen zelfs overslaan, en meteen herschikken tot $x_1^2 - 1 = Ay_1^2$.

Een triviaal voorbeeld: $5^2 - 6 \cdot 2^2 = 1$. Dus $(5 - 1)(5 + 1) = 5^2 - 1^2 = 6 \cdot 2^2$. Hieruit volgt dat $6 = \frac{4}{2} \cdot \frac{6}{2} = 2 \cdot 3$.

Snelle factorisatie is belangrijk in het breken van moderne cryptografische codes, die vaak gebruik maken van vermenigvulgingen van twee zeer grote priemgetallen. Zie voor meer informatie over het verband tussen factoriseren en de vergelijking van Pell *Solving the Pell equation* van H. Lenstra.

Hoofdstuk 3

Griekse wiskundigen en de vergelijking van Pell

3.1 Theon van Smyrna

De eerste behandeling van de vergelijking van Pell vinden we in het werk van Theon van Smyrna, een wiskundige van rond 100 na Christus. In zijn werk *Over wiskunde die nuttig is voor het begijpen van het werk van Plato* behandelt hij de vergelijking die wij tegenwoordig zouden schrijven als $x^2 - 2y^2 = \pm 1$. [1]

Theon van Smyrna was een wiskundige in de traditie van de Pythagoreërs, de wiskundigen uit de school die gesticht werd door Pythagoras *($\pm$582 v.C. - $\pm$507 v.C.)*. Veel wiskunde uit de oudheid wordt toegeschreven aan Pythagoras en zijn volgelingen; dit is in een aantal gevallen incorrect.[2] We hebben echter te weinig bronnen om precies te weten wat er te danken is aan Pythagoras en zijn school, wat daarvoor is gedaan door bijvoorbeeld de Mesopotamiërs en de Egyptenaren, en welk werk later door op Pythagoras geïnspireerde wiskundigen is verricht. Wat dit onderwerp betreft is het werk van Theon van Smyrna het oudst bekende, dus zullen we zijn naam aanhouden. Het is echter waarschijnlijk dat de methode ouder is. Niet alleen presenteert Theon van Smyrna zijn werk als een overzichtswerk in plaats van als onderzoek, maar Plato zelf verwijst al naar de hierondergenoemde 'diagonale getallen' in zijn *Politeia.*[3]

[1] Theon van Smyrna behandelt alleen het geval $A = 2$, en kijkt nergens naar het gegeneraliseerde probleem.

[2] Een goed voorbeeld is dat de zogeheten 'Pythagoreëische tripels', getallen a, b, c zodat $a^2 + b^2 = c^2$, gevonden zijn op een kleitablet uit het Babylonië van 1800 v.C.

[3] Zie Konen, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, blz 2-18 voor een uitgebreidere

De behandeling van het werk van Theon van Smyrna is gebaseerd op het eerste hoofdstuk van deel 1 van het boek *Geschichte der Gleichung* $t^2 - Du^2 = 1$ van H. Konen. Ik heb niet de gelegenheid gehad het werk van Theon zelf te bekijken. Omdat Konen alle wiskunde in moderne notatie geeft, kan ik hier niet de oorspronkelijke notatie laten zien.

In zijn behandeling definieert Theon een reeks paren van zogenaamde 'zijdegetallen' en 'diagonaalgetallen'. Ieder paar is dan een oplossing van $x^2 - 2y^2 = \pm 1$. Het eerste paar in de reeks is $(1, 1)$, en ieder volgend paar wordt berekend uit het vorige volgens de regel hieronder; uit het eerste paar volgt het tweede, uit het tweede het derde, enzovoorts. In moderne notatie noemen we de 'zijdegetallen' z_i en de 'diagonaalgetallen' d_i, en schrijven we Theon van Smyrna's methode als volgt:

Initialisatie:

- $z_1 = 1$
- $d_1 = 1$

Definitie van de nieuwe getallen in termen van de oude:

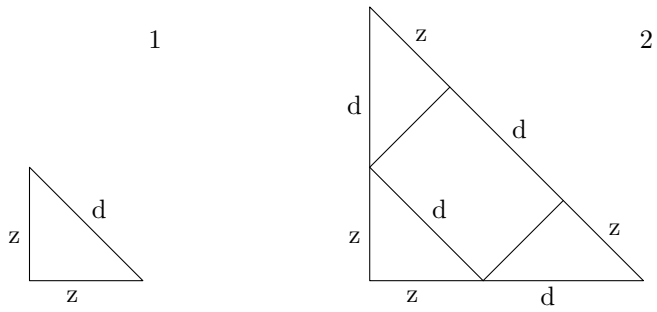
- $z_{i+1} = z_i + d_i$
- $d_{i+1} = 2z_i + d_i$

Theon claimt ook dat (in moderne notatie) ieder van deze paren een oplossing is voor $x^2 - 2y^2 = \pm 1$, maar bewijst dit nergens.

De wiskundige P. Bergh geeft een plausibele verklaring voor deze methode en haar naamgeving.[4] Zie de 'zijdegetallen' als de zijden van een driehoek, en de 'diagonaalgetallen' als *benaderingen* van de diagonaal van diezelfde driehoek. De eerste driehoek is in feite een gelijkzijdige driehoek (alle drie de hoeken zijn 1 lang), maar kan worden gezien als een (slechte) benadering van een rechthoekige driehoek met zijden $1, 1$ en $\sqrt{2}$. Een nieuwe benadering van een dergelijke driehoek volgt dan uit de onderstaande constructie (plaatje te danken aan P. Bergh)

behandeling van dit vermoeden, en de meningen van diverse historici.

[4] P. Bergh, *Seiten und Diametralzahlen bei den Griechen*. Ik heb deze verwijzing uit het boek van Konen, en heb het werk van Bergh zelf niet bekeken.



Theon doet dus alsof de driehoek die hij heeft rechthoekig is, en maakt een grotere driehoek. Deze driehoek heeft zijden $z+d$ en diagonaal $2z+d$. We zullen straks aantonen dat deze driehoek een betere benadering is van een rechthoekige driehoek.

Deze uitleg geeft ook een waarschijnlijke reden waarom de wiskundigen in de Oudheid geïnteresseerd waren in het oplossen van $x^2 - 2y^2 = 1$: Iedere oplossing geeft een benadering $\frac{d_i}{z_i}$ voor $\sqrt{2}$ die beter wordt naarmate de oplossing groter is (we zullen dit ook hieronder bewijzen). Het meetkundig nut van goede benaderingen van $\sqrt{2}$ moge duidelijk zijn.

De eerste drie paren (s, d) zijn $(1, 1)$, $(2, 3)$ en $(5, 7)$, wat leidt tot de benaderingen 1, 1.5 en 1.4. Gegeven dat $\sqrt{2} \approx 1.4142$ wordt het verschil (in absolute waarde) steeds kleiner: 0.4142, 0.0858 respectievelijk 0.0142. Het is eenvoudig te bewijzen dat dit algemeen geldig is, en zelfs dat geldt:

Stelling 3.1. $|\sqrt{2} - \frac{d_{i+1}}{z_{i+1}}| < \frac{1}{3} \cdot |\sqrt{2} - \frac{d_i}{z_i}|$

Bewijs. Gegeven d_i en z_i schrijven we $\alpha_i = z_i\sqrt{2} - d_i$. Daarmee geldt dat $\sqrt{2} - \frac{d_i}{z_i} = \frac{\alpha_i}{z_i}$. We weten dat $|\frac{\alpha_1}{z_1}| < 1$, daarom mogen we gebruiken dat $|\frac{\alpha_i}{z_i}| < 1$.

We schrijven nu $|\sqrt{2} - \frac{d_{i+1}}{z_{i+1}}| = |\sqrt{2} - \frac{2z_i+d_i}{z_i+d_i}| = |\frac{(\sqrt{2}-2)z_i+(\sqrt{2}-1)d_i}{z_i+d_i}| = |\frac{(\sqrt{2}-1)\alpha_i}{(1+\sqrt{2})z_i-\alpha_i}|$

Dit is als volgt af te schatten: $|\frac{(\sqrt{2}-1)\alpha_i}{(1+\sqrt{2})z_i-\alpha_i}| < \frac{\sqrt{2}-1}{\sqrt{2}} \cdot \frac{|a_i|}{z_i} < \frac{|a_i|}{3z_i}$. □

Per iteratie wordt onze foutterm dus minstens een factor drie kleiner.

We zullen de relatie tussen oplossingen van de vergelijking van Pell met coëfficient A en benaderingen voor $\sqrt{A}$ nader bekijken in Hoofdstuk 6.

Het bewijs dat de op deze manier gegenereerde getallen allemaal oplossingen zijn van de vergelijking van Pell is voor ons niet bijzonder moeilijk:

Stelling 3.2. $z_i^2 - 2d_i^2 = \pm 1$

Bewijs. Met volledige inductie:
$1^2 - 2 \cdot 1^2 = -1$
Als geldt dat $z_i^2 - 2d_i^2 = \pm 1$, dan volgt dat

$$\begin{aligned} d_{i+1}^2 - 2z_{i+1}^2 &= (2z_i + d_i)^2 - 2(z_i + d_i)^2 \\ &= 4z_i^2 + 4z_i d_i + d_i^2 - 2z_i^2 - 4z_i d_i - 2d_i^2 \\ &= -(d_i^2 - 2z_i^2) = \mp 1 \end{aligned}$$

□

Merk op dat het teken van de 1 steeds wisselt.

De twee bovenstaande stellingen zijn modern werk. Ze zijn makkelijk direct te bewijzen (zoals ik hier heb gedaan), of af te leiden uit de eigenschappen van kettingbreuken.

Wanneer ik 'makkelijk' zeg is het belangrijk op te merken dat dat voor ons zo is, omdat wij efficiënte notatie en gevorderde wiskunde kennen. Wij kunnen gebruik maken van indices en bewijs door volledige inductie, terwijl de oude Grieken geen van beide kenden.

Voor zover bekend hebben de Pythagoreërs zich alleen bezig gehouden met dit specifieke geval van de vergelijking van Pell. Er is geen werk gevonden over een dergelijke vergelijking met een andere constante dan 2. Waarschijnlijk de eerste die dat wel doet is de Siciliaanse wiskundige Archimedes *(287 v.C. - 212 v.C.)*. Het is de moeite waard om op te merken dat Archimedes breuken gebruikt die een bijzonder goede benadering zijn voor $\sqrt{3}$, namelijk $\frac{265}{153}$ en $\frac{1351}{780}$.[5] Het is niet onwaarschijnlijk dat deze berekend zijn via een proces dat lijkt op het bovenstaande, maar dan met 3 als coëfficient. De twee benaderingen voldoen namelijk aan de volgende vergelijkingen:

- $265^2 - 3 \cdot 153^2 = -2$
- $1351^2 - 3 \cdot 780^2 = 1$

Waarschijnlijk is het ook Archimedes die het zogenaamde 'veestapelprobleem' heeft gesteld, dat we in de volgende sectie zullen behandelen.

[5] Dit wordt zonder directe verwijzing genoemd in Heath, *Diophantus of Alexandria*, op pagina 278.

3.2 De veestapel van de Zon

Het 'veestapelprobleem' ('cattle problem' in het Engels) is een probleem dat bij nadere bestudering oplosbaar blijkt wanneer we de vergelijking van Pell kunnen oplossen. Het staat in een brief die waarschijnlijk door Archimedes aan onbekende wiskundigen in de stad Alexandrië is gestuurd. Het is een ingewikkeld raadsel in dichtvorm over de veestapel van de zonnegod; de lezer wordt geacht met behulp van aanwijzingen het correcte aantal van iedere soort stier en koe te vinden.[6][7]

In iedere kudde waren stieren, groot in aantal volgens deze verhoudingen:

Als u ijverig en wijs bent, o vreemdeling, bereken dan de grootte van de Zon's veestapel, die ooit graasde op de velden van het driehoekige eiland Sicilië, verdeeld in vier kudden van verschillende kleuren, één melkwit, een ander glanzend zwart, een derde geel en de laatste gevlekt.

Begrijp, vreemdeling, dat de witte stieren [in aantal] gelijk waren aan de helft en een derde van de zwarte samen met het geheel van de gele, terwijl de zwarte gelijk waren aan een kwart van de gevlekte plus een vijfde, samen met, wederom, het geheel van de gele. Merk verder op dat de overgebleven stieren, de gevlekte, gelijk zijn [in aantal] aan een zesde van de witte en een zevende, tezamen met al de gele.

Dit zijn de verhoudingen van de koeien: de witte waren precies gelijk aan een derde en een vierde van de gehele zwarte kudde terwijl de zwarte gelijk waren aan wederom een kwart van de gevlekte en een vijfde wanneer alle, inclusief de stieren, naar de wei gingen. De gevlekte in vier delen waren nu gelijk in getal aan een vijfde en een zesde van de gele kudde. Ten slotte waren de gele gelijk in getal aan een zesde deel en een zevende van de witte kudde.

Als u, o vreemdeling, de grootte van de veestapel van de Zon correct

[6] vertaald naar het Nederlands uit de Engelse vertaling in *Greek Mathematical works vol. II* van Ivor Thomas, pagina 203-205

[7] Merk op dat omdat het hier over een aantal stuks vee gaat, het voor de Grieken meteen duidelijk is dat een oplossing in gehele getallen gevraagd wordt.

kunt vertellen met afzonderlijk [aan de ene kant] het aantal weldoorvoede stieren, en aan de andere kant de wijfjes per kleur zou u niet onkundig of onwetend op het gebied van getallen genoemd worden, maar u zult nog niet gerekend worden onder de wijzen.

Maar kom, begrijp ook deze eisen die aan de veestapel van de zon gesteld worden. Wanneer de witte stieren zich mengden met de zwarte, stonden zij stevig, gelijk in diepte en breedte, en de velden van het driehoekige land, wijd uitgestrekt, waren vol van hun aantal. Opnieuw, wanneer de gele en gevlekte stieren in één kudde waren samengevoegd stonden zij op zulk een wijze dat hun aantal, beginnend bij één langzaam toenam tot het een driehoeksfiguur vormde, zonder dat er stieren van een andere kleur in hun midden waren, of één van hen ontbrak.

Als u in staat bent, o vreemdeling, al deze dingen uit te vinden en in uw geest samen te voegen, daarbij alle relaties gevend, zult u vertrekken gekroond met glorie, en wetend dat u binnen dit ras bent beoordeeld als zijnde perfect in wijsheid.

De beschrijving bestaat uit drie delen: een deel dat de verhoudingen van de stieren onderling beschrijft, een deel dat de hoeveelheid koeien relateert aan de hoeveelheid stieren, en een laatste deel dat twee extra eisen stelt. We zullen de delen stuk voor stuk oplossen. Daartoe voeren we de volgende notatie in:

- W is het aantal witte stieren
- Z is het aantal zwarte stieren
- G is het aantal gele stieren
- V is het aantal gevlekte stieren
- W' is het aantal witte koeien
- Z' is het aantal zwarte koeien
- G' is het aantal gele koeien
- V' is het aantal gevlekte koeien

De derde alinea van het raadsel beschrijft de verhoudingen tussen de stieren:

- $W = \frac{5}{6}Z + G$
- $Z = \frac{9}{20}V + G$
- $V = \frac{13}{42}W + G$

Oftewel: $W - \frac{5}{6}Z = Z - \frac{9}{20}V = V - \frac{13}{42}W = G$.

Een oplossing voor deze vergelijking in gehele getallen is gemakkelijk te vinden.[8] De kleinst mogelijke oplossing is $W = 2226, Z = 1602, V = 1580, G = 891$. Merk op dat het vermenigvuldigen van alle termen met een constante factor een nieuwe oplossing levert, omdat het raadsel het alleen heeft over de verhoudingen tussen de verschillende kleuren stieren. Er zijn dus oneindig veel oplossingen mogelijk, en al deze oplossingen hebben de vorm $W = m{\cdot}2226, Z = m{\cdot}1602, V = m \cdot 1580, G = m \cdot 891$, met m een positief geheel getal.

De vierde alinea legt de aantallen koeien vast. In onze hedendaagse notatie staat er het volgende:

- $W' = \frac{7}{12}(Z + Z')$
- $Z' = \frac{9}{20}(V + V')$
- $V' = \frac{11}{30}(G + G')$
- $G' = \frac{13}{42}(W + W')$

Met enig rekenwerk dat we hier achterwege zullen laten valt te berekenen dat voor $W = n{\cdot}4657{\cdot}2226, Z = n{\cdot}4657{\cdot}1602, V = n{\cdot}4657{\cdot}1580, G = n{\cdot}4657{\cdot}891$ de andere vier variabelen (die te berekenen zijn door vier lineaire vergelijkingen in vier onbekenden op te lossen) uitkomen op gehele getallen. Hier is n een positief geheel getal, dat we zelf mogen kiezen. Voor de kleinst mogelijke oplossing kunnen we $n = 1$ nemen, maar er zijn oneindig veel verschillende oplossingen mogelijk. (We kunnen ook zeggen dat de m die we vonden in de oplossing voor alleen stieren gelijk moet zijn aan $n \cdot 4657$).

We hebben nu volgens het raadsel de opperste wijsheid nog niet bereikt. Daarvoor moeten we ook nog aan de eisen in de één na laatste alinea voldoen. Hoewel deze eisen op het eerste gezicht een beetje cryptisch lijken, is er best wijs uit te worden:

Wanneer de witte stieren zich mengden met de zwarte, stonden zij stevig, gelijk in diepte en breedte, en de velden van het driehoekige land, wijd uitgestrekt,

[8] Stel bijvoorbeeld dat $G = 1$, en bereken dan V, W en Z (je hebt immers drie lineaire vergelijkingen in drie onbekenden). Vermenigvuldig daarna met een constante factor die groot genoeg is om alle getallen geheel te maken.

waren vol van hun aantal. Gegeven $W + Z$ stieren moeten we deze in een vierkant ("gelijk in diepte en breedte") op kunnen stellen. $W + Z$ moet dus een kwadraat zijn.

Opnieuw, wanneer de gele en gevlekte stieren in één kudde waren samengevoegd stonden zij op zulk een wijze dat hun aantal, beginnend bij één langzaam toenam tot het een driehoeksfiguur vormde, zonder dat er stieren van een andere kleur in hun midden waren, of één van hen ontbrak. Gegeven $G + V$ stieren kunnen we dezen in een driehoek opstellen. $G+V$ is dus een zogeheten driehoeksgetal. Het is een eenvoudig te controleren feit dat driehoeksgetallen van de vorm $\frac{1}{2}n(n+1)$ zijn, met n een positief geheel getal.

Als u in staat bent, o vreemdeling, al deze dingen uit te vinden en in uw geest samen te voegen, daarbij alle relaties gevend, zult u vertrekken gekroond met glorie, en wetend dat u binnen dit ras tot perfect in wijsheid bent beoordeeld. Dat is geen understatement; bij de kleinst mogelijke oplossing van het probleem met de twee extra eisen is iedere groep stieren orde van grootte 10^{206547}, een getal met 206548 cijfers

(In de jaren zestig hebben wiskundigen een computerprogramma geschreven om het anwoord uit te rekenen. Nadat een supercomputer meer dan zeven dagen had staan rekenen, is het antwoord helaas weggegooid. Pas in 1981, na een tweede berekening op een snellere supercomputer, werd het kleinst mogelijke antwoord gepubliceerd. Dit kostte 47 pagina's).

Dit antwoord op het probleem van Archimedes past niet in deze scriptie. We zijn eigenlijk ook niet zozeer geïnteresseerd in het antwoord, maar meer in de structuur van het probleem. Dit is waar we voor het eerst de vergelijking van Pell tegen zullen komen.

Een oplossing van de moeilijke versie van het probleem moet nog steeds voldoen aan alle eisen die we al hebben, dat wil zeggen dat $W = n \cdot 4657 \cdot 2226, Z = n \cdot 4657 \cdot 1602, V = n \cdot 4657 \cdot 1580, G = n \cdot 4657 \cdot 891$.

Hieruit volgt dat $W + Z = n \cdot 4657 \cdot 3828 = n \cdot 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657$. Dit laatste is de ontbinding in priemfactoren. Volgens de eerste extra eis moet $W + Z$ een kwadraat zijn. Dat kan alleen als $n = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot Y^2$, met Y een positief getal naar keuze.

Als $G + V$ een driehoeksgetal is, is er een gehele en positieve p zodat $G + V = \frac{1}{2}p(p+1)$. Hieruit volgt dat $8 \cdot (G+V)+1$ gelijk is aan $4p^2+4p+1 = (2p+1)^2$. Tegelijkertijd geldt dat $G+V = n \cdot 4657 \cdot 2471 = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot Y^2 \cdot 4657 \cdot 2471$.

Definieer nu $X := 2p + 1$, dan volgt uit $8(G + V) + 1 = (2p + 1)^2$ dat $X^2 - 8(G + V) = 1$, oftewel dat:
$X^2 - 8 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot 4657 \cdot 2471 \cdot Y^2 = 1$, dat wil zeggen

$$X^2 - 410286423278424 \cdot Y^2 = 1.$$

Dit is de vergelijking van Pell voor $A = 410286423278424$. Als we eenmaal een X en een Y hebben die aan deze voorwaarden voldoen, kunnen we de hoeveelheden stieren berekenen:

- $W = 2226 \cdot 4657 \cdot n = 2226 \cdot 4657^2 \cdot 3828 \cdot Y^2 = 184803233148072 \cdot Y^2$
- $Z = 1602 \cdot 4657 \cdot n = 1602 \cdot 4657^2 \cdot 3828 \cdot Y^2 = 132998553235944 \cdot Y^2$
- $G = 891 \cdot 4657 \cdot n = 891 \cdot 4657^2 \cdot 3828 \cdot Y^2 = 73971105451452 \cdot Y^2$
- $V = 1580 \cdot 4657 \cdot n = 1580 \cdot 4657^2 \cdot 3828 \cdot Y^2 = 131172106187760 \cdot Y^2$

De kleinst mogelijke waarde voor Y heeft 103266 cijfers. Bovenstaande variabelen komen dan rond de 206547 cijfers uit.

Voor het uitgebreide probleem is geen oplossing uit de Oudheid bekend (voor de makkelijke versie ook niet, hoewel het waarschijnlijk is dat wiskundigen uit die tijd in staat waren dit op te lossen). Hoewel sommigen, zoals de Franse wiskundige Paul Tannery, van mening waren dat Archimedes in staat moet zijn geweest dit probleem op te lossen[9], wordt algemeen aangenomen dat niemand daar destijds toe in staat was, al was het maar omdat een berekening met de hand ondoenlijk lang zou zijn. Waarom Archimedes een probleem opgaf dat hij zelf (naar alle waarschijnlijkheid) niet op kon lossen is niet duidelijk.

Het genoemde antwoord dat berekend was door een computer is de eerste keer dat het probleem in zijn volle glorie is opgelost. Wel is er een werk uit 1880 waarin de Duitse wiskundige A. Amthor berekent hoeveel cijfers het antwoord zou moeten hebben, en dat de eerste vier cijfers 7766 zouden moeten zijn.[10] Helaas was het vierde van deze cijfers fout, omdat de logaritmetabellen die Amthor gebruikte niet nauwkeurig genoeg waren. Een interessante moderne publicatie over de snelheid van het berekend van dit probleem (en varianten van de Pell vergelijking voor grote A in het algemeen) is Lenstra, *Solving the Pell Equation.*

Naast het veestapelprobleem duikt de vergelijking van Pell nog een paar keer op in Griekse geschriften als manier om een goede benadering voor $\sqrt{n}$ te geven. De wiskundige Diophantus gebruikt een Lemma[11] dat (in moderne notatie) zegt dat gegeven twee getallen x en y zodat $x^2 - Ay^2$ een kwadraat is, het mogelijk is

[9] Ik heb dit gegeven uit Weil's *Number Theory*, pagina 19. Weil geeft geen expliete verwijzing, en ik heb niet de tijd gehad Tannery's gehele werk door te nemen om het te controleren.

[10] Amthor, *Das Problema Bovinum des Archimedes*

[11] het Lemma bij Stelling 15 van Boek 6

grotere getallen met dezelfde eigenschap te vinden. Het is echter bijna zeker dat Diophantus hier, zoals in de rest van zijn werk, genoegen neemt met oplossingen in breuken. Het is bijzonder opmerkelijk dat Fermat, wanneer hij de getaltheorie nieuw leven in wil blazen,[12] claimt voort te bouwen op het werk van Diophantus, aangezien deze vrijwel al zijn problemen oploste in positieve breuken. De term 'Diophantische vergelijking' voor een vergelijking die in gehele getallen opgelost dient te worden is feitelijk dan ook incorrect.

Diophantus' idee om uit gegeven oplossingen voor vergelijkingen die op die van Pell lijken nieuwe te maken lijkt op het werk van Indiase wiskundigen in het volgende hoofdstuk. Uiteindelijk vinden die een methode om de vergelijking van Pell in gehele getallen op te lossen.

[12] zie Hoofdstuk 5

Hoofdstuk 4

De Indiase methode

India kent een rijke wiskundige traditie, die terug te traceren is tot vóór de klassieke Griekse wiskunde. Voor zover bekend is er geen verband tussen die twee, hoewel er soms gespeculeerd wordt dat beide groepen contact met elkaar zouden hebben gehad. De Indiase wiskundige traditie is grotendeels mondeling, bestaande uit lange gedichten in het Sanskriet, die van meester op leerling werden doorgegeven. Losse verzen worden *Stanzas* genoemd. In een wiskundig werk bevat één zo'n Stanza meestal een wiskundige stelling of een voorbeeld.

Ondanks deze traditie zijn er een aantal geschreven werken uit de oud-Indiase wiskunde gevonden. Vaak zijn deze geschreven door één wiskundige, en later (soms tientallen jaren later) becommentarieerd door andere wiskundigen, die passages verduidelijken, of zelfs theorie toevoegen.

Wij zullen hier het werk van twee Indiase wiskundigen behandelen, namelijk van Brahmagupta ($\pm$*598-668*) en Bhaskara (*1114-1185*). Beiden hebben gewerkt aan de vergelijking van Pell of varianten daarvan: Brahmagupta laat zien hoe je van oplossingen voor $x^2 - Ay^2 = k$ er meer kunt maken, en in sommige gevallen een oplossing voor $k = 1$ kunt construeren. Vijfhonderd jaar later geeft Bhaskara zelfs een algoritme om de vergelijking van Pell op te lossen.

Brahmagupta en Bhaskara leefden rond respectievelijk het begin en het einde van de bloeiperiode van de Indiase wiskunde. In deze periode ontdekken Indiase geleerden onder andere het positiesysteem om getallen te schrijven, de nul, en de differentiaalrekening, en werken ze aan veel problemen in rationale en gehele getallen. Deze wiskunde is voornamelijk gemotiveerd door sterrenkunde. Het berekenen van de banen van hemellichamen was belangrijk voor navigatie, maar vooral ook om religieuze redenen, aangezien volgens de Indiërs de stand van de hemellichamen een bijzonder sterke invloed had op het dagelijks leven,

en hier zeker rekening mee moest worden gehouden bij het nemen van belangrijke beslissingen. De religieuze kaste hield zich dan ook mede bezig met het bedrijven van sterrenkunde, en onder deze religieus geïnspireerde wiskundigen waren Brahmagupta en Bhaskara.

Alle citaten in dit hoofdstuk komen uit het boek *Brahmegupta* (sic) *and Bhaskara - Algebra with arithmetic and mensuration* van H.T. Colebrooke, dat voor het eerst verscheen in 1817. Aanvullingen [tussen vierkante haken] zijn van hem, toevoegingen van mijn kant zijn aangegeven met voetnoten. Van Brahmagupta behandel ik het eerste deel van Sectie 7 van zijn *Brahma-sidd'hánta*, namelijk Stanza's 65-75 op pagina 363-367. Van Bhaskara behandel ik Hoofdstuk 3 van zijn *Víja-gańita*, te weten Stanza's 75-99 op pagina 170-184.

4.1 Brahmagupta

Brahmagupta schreef een belangrijk werk over astronomie, de *Brahma-sidd'hánta*. Naast astronomie behandeld dit werk ook wiskunde. Hoofdstuk achttien gaat over algebra (*Cuťťaca* in het Sanskriet), en in het zevende deel van dit hoofdstuke behandelt Brahmagupta wat hij noemt "kwadraten beïnvloed door een coëficiënt", problemen die neerkomen op de vergelijking van Pell zowel voor $k = 1$ als voor $k \neq 1$.

Nu schrijven de Indiërs niet $x^2 - Ay^2 = k$. Hun notatie maakt niet eens gebruik van letters als variabelen, maar geeft iedere variabele en constante een naam, die duidelijk maakt welke functie de desbetreffende term vervult. Het bovenstaande probleem bijvoorbeeld, zou Brahmagupta ongeveer als volgt beschrijven:

Het kwadraat van de 'laatste wortel' (*Jyéshť'ha* of *antya*) is gelijk aan het product van het kwadraat van de 'eerste wortel' (*Canishť'ha* of *ádya*) met de 'vermenigvuldiger' (*Pracrĭti*) opgeteld bij de 'vermeerderaar' (*Cshépa*[1]) of de 'verminderaar' (*Sód'haca*). Oftewel:

'laatste wortel'	$= x$
'eerste wortel'	$= y$
'vermenigvuldiger'	$= A$
'vermeerderaar' of 'verminderaar'	$= k$, afhankelijk van of k positief of negatief is.

In zijn hoofdstuk over dit soort vergelijkingen bewijst Brahmagupta een aantal nuttige resultaten om gevallen van de vergelijking van Pell op te lossen. Hij begint met aantonen dat als hij twee oplossingen heeft voor wat wij nu $x^2 - Ay^2 = k$ noemen (deze twee oplossingen mogen dezelfde zijn), hij daarmee een

[1] ook wel *Cshipti* of *Cshipticá*

derde kan construeren:[2]

Stanzas 65-66: Stellingen 39-40: *"Een wortel [wordt] tweemaal [neergezet]: en [een andere wortel afgeleid] van het aangenomen kwadraat vermenigvuldigd met de vermenigvuldiger, en vermeerderd of verminderd met de aangenomen hoeveelheid. Het product van het eerste [paar] samen genomen met de vermenigvuldiger, met het product van het laatste paar toegevoegd, is een 'laatste wortel'. De som van de kruiselingse vermenigvuldigingen is een 'eerste wortel'. De vermeerdering is het product van de desbetreffende vermeerderende of verminderende hoeveelheden. De wortels [die zo gevonden zijn], gedeeld door de [oorspronkelijke] vermeerdering of vermindering zijn wortels voor de positieve eenheid."*

Dit lijkt op het eerste gezicht onbegrijpelijk, maar dat is voornamelijk een kwestie van terminologie en manier van spreken. De Indiërs hadden een minder vergevorderde wiskundige notatie dan wij tegenwoordig hebben: ze hebben bijvoorbeeld geen tekens als '+' en '·' voor optellen en vermenigvuldigen, en gebruiken namen voor hun onbekenden in plaats van letters (x of y). Dit komt door hun traditie van het mondeling overdragen van kennis. Als we een beetje moeite doen om de door Brahmagupta gebruikte termen om te zetten in een notatie die gebruik maakt van symbolen is deze tekst best te begrijpen.

Wat Brahmagupta vertelt in Stanzas 65-66 is dat als hij twee oplossingen $x_1^2 - Ay_1^2 = k, x_2^2 - Ay_2^2 = k$ heeft, hij door samenstelling een nieuwe oplossing kan maken. Hij zet twee wortels neer (x_1, x_2) (dit mogen twee verschillende wortels zijn), en hij zet ook de twee daarvan af te leiden wortels neer (y_1, y_2), "vermenigvuldigd met de vermenigvuldiger"(zo weten we dat dit onze y_i zijn). De vermenigvuldiging van de 'eerste wortels' (y_i), vermenigvuldigd met de 'vermenigvuldiger' (A) en opgeteld bij de vermenigvuldiging van de twee 'laatste wortels' (x_i) is een nieuwe 'laatste wortel'. Tegenwoordig zouden we schrijven: $x_3 := x_1x_2 + Ay_1y_2$.

Brahmagupta vervolgt: "De som van de kruiselingse vermenigvuldigingen (*Vajrabad'ha*) is een eerste wortel". Met 'kruiselingse vermenigvuldigingen' wordt bedoeld het met elkaar vermenigvuldigen van de *verschillende* wortels uit de twee gegeven vergelijkingen. Hier staat dus $y_3 = x_1y_2 + x_2y_1$.

"De vermeerdering is het product van de desbetreffende vermeerderde of ver-

[2]Het is niet precies duidelijk of Brahmagupta eist dat beide 'vermeerderingen' hetzelfde zijn. Dit kan te wijten zijn aan onduidelijkheid in de oorspronkelijke tekst, of aan een incomplete vertaling. Ik ben zelf van mening dat Brahmagupta er van uitgaat dat beide 'vermeerderaars' hetzelfde zijn, omdat de inhoud van Stanza 68 anders triviaal zou zijn.

minderde hoeveelheden". Dit betekent dat $k_3 = k^2$.

Tenslotte merkt Brahmagupta op "De wortels [die zo gevonden zijn], gedeeld door de [oorspronkelijke] vermeerdering of vermindering zijn wortels voor de positieve eenheid." We kunnen de hele vergelijking delen door k^2, en dan krijgen we de vergelijking $(\frac{x_3}{k})^2 - A(\frac{y_3}{k})^2 = 1$. (Merk op dat $\frac{x_3}{k}$ en $\frac{y_3}{k}$ niet per sé geheeltallig hoeven te zijn. Deze kruisvermenigvuldiging levert dan ook in het algemeen geen geheeltallige oplossing voor de vergelijking van Pell).

Wat Brahmagupta hier zegt klopt. Het paar (x_3, y_3) is inderdaad een geldige oplossing voor de vergelijking $x^2 - Ay^2 = k^2$, want:

$$\begin{aligned} x_3^2 - Ay_3^2 &= (x_1x_2 + Ay_1y_2)^2 - A(x_1y_2 + x_2y_1)^2 \\ &= x_1^2x_2^2 + 2Ax_1x_2y_1y_2 + A^2y_1^2y_2^2 - Ax_1^2y_2^2 - 2Ax_1x_2y_1y_2 - Ax_2^2y_1^2 \\ &= x_1^2(x_2^2 - Ay_2^2) - Ay_1^2(x_2^2 - Ay_2^2) \\ &= k \cdot k = k^2 \end{aligned}$$

Brahmagupta bewijst nog aanzienlijk meer:

Stanza 68: Stelling 41: *"Nadat achtereenvolgens de wortels voor de positieve eenheid onder de wortels voor de gegeven vermeerderaar of verminderaar zijn geplaatst dienen 'eerste' en 'laatste' wortels [vanaf daar afgeleid door compositie] voor de gegeven vermeerderaar of verminderaar."*

Gegeven een bepaalde vermeerderaar of verminderaar en een oplossing daarvoor, kunnen we de methode uit Stanzas 65 en 66 gebruiken om een nieuwe oplossing voor dezelfde k te maken. Als we namelijk samenstellen met een oplossing van $x^2 - Ay^2 = 1$ volgt uit de vermenigvuldiging dat de berekende x_3 en y_3 ook oplossingen zijn van $x^2 - Ay^2 = k$.

Brahmagupta is dus duidelijk in staat om nieuwe oplossingen te maken uit oplossingen die hij al heeft, en hij kan oplossingen samenstellen. In zijn volgende regel laat hij zien dat het mogelijk is om uit oplossingen voor sommige k oplossingen voor $k = 1$ te maken.

Stanza 69: Stelling 42: *"Wanneer de vermeerderaar vier is, is het kwadraat van de laatste wortel, verminderd met drie, gehalveerd en vermenigvuldigd met de laatste, een laatste wortel, en het kwadraat van de laatste wortel, min één, gedeeld door twee en vermenigvuldigd met de eerste is een eerste wortel [voor de positieve eenheid]."*

Als Brahmagupta een oplossing (x_1, y_1) heeft voor $x^2 - Ay^2 = 4$ ("wanneer

de vermeerderaar vier is"), vervaardigd hij hieruit een oplossing voor $k = 1$. Kwadrateer x_1, haal er drie van af, halveer en vermenigvuldig met x_1. Het resultaat is dan x_2. Om y_2 te berekenen doen we bijna hetzelfde: we trekken één van x_1 af, vermenigvuldigen met y_1, en halveren het resultaat. Is (x_2, y_2) een oplossing voor $x^2 - Ay^2 = 1$?

$$\begin{aligned} x_2^2 - Ay_2^2 &= (\tfrac{x_1(x_1^2-3)}{2})^2 - A(\tfrac{y_1(x_1^2-1)}{2})^2 \\ &= \tfrac{x_1^6-6x_1^4+9x_1^2}{4} - A\tfrac{x_1^4y_1^2-2x_1^2y_1^2+y_1^2}{4} \\ &= \tfrac{x_1^4(x_1^2-Ay_1^2)-2x_1^2(x_1^2-Ay_1^2)+(x_1^2-Ay_1^2)-4x_1^4+8x_1^2}{4} \\ &= \tfrac{4x_1^4-4x_1^4+8x_1^2-8x_1^2+4}{4} = 1 \end{aligned}$$

Ja, het is inderdaad een geldige oplossing. Vervolgens wordt hetzelfde gedaan met een oplossing voor $k = -4$:

Stanza 71: Stelling 42: *"Wanneer vier de verminderaar is, wordt het kwadraat van de laatste wortel twee maal neergezet, met in het ene geval drie en in het andere geval één toegevoegd: de helft van het product van deze optellingen wordt apart gezet, en hetzelfde min één. Dit, vermenigvuldigd met de vorige, min één is de 'laatste wortel'. De andere, vermenigvuldigd met het product van de wortels is de 'eerste wortel' die behoort bij die 'laatste'."*

Met de eerste zin definiëert Brahmagupta twee getallen: $\frac{(x^2+3)(x^2+1)}{2}$ en $\frac{(x^2+3)(x^2+1)}{2} - 1$, oftwel $\frac{x^4+4x^2+3}{2}$ en $\frac{x^4+4x^2+1}{2}$. De laatste van die twee, vermenigvuldigd met de oorspronkelijke 'laatste wortel', min één wordt de nieuwe 'laatste wortel': $\frac{x^5+4x^3+x-2}{2}$. De eerste, vermenigvuldigd met het product van de twee vorige wortels, is de nieuwe 'eerste' wortel: $\frac{x^5y+4x^3y+3xy}{2}$.

Hier maakt Brahmagupta een fout. In het algemeen geldt niet dat de twee gevonden getallen een oplossing zijn voor $x^2 - Ay^2 = 1$. Kijk wat er gebeurt als we ze invullen:

$$\begin{aligned} x_2^2 - Ay_2^2 &= (\tfrac{x^5+4x^3+x-2}{2})^2 - A(\tfrac{x^5y+4x^3y+3xy}{2})^2 \\ &= \tfrac{x^{10}+8x^8+18x^6-4x^5+8x^4-16x^3+x^2-4x+4}{4} - A\tfrac{y^2(x^{10}+8x^8+22x^6+24x^4+9x^2)}{4} \\ &= \tfrac{(8x^8+22x^6+24x^4+9x^2)(x^2-Ay^2)+x^{10}y^2-7x^{10}-14x^8-6x^6-4x^5-x^4-16x^3+x^2-4x+4}{4} \\ &= \tfrac{x^{10}y^2-7x^{10}-46x^8-94x^6-4x^5-97x^4-16x^3-35x^2-4x+4}{4} \end{aligned}$$

Deze laatste term is in het algemeen niet gelijk aan één.

Er is wel een oplossing voor dit probleem, en die lijkt erg op die van Brahmagupta. We houden $y_2 = \frac{x^5y+4x^3y+3xy}{2}$, maar in plaats van $x_2 = \frac{x((x^2+1)(x^2+3)-1)-1}{2}$

kiezen we $x_2 = \frac{x^2(x^2+3)^2+1}{2}$. Dit levert wel een geldige oplossing:

$$\begin{aligned} x_2^2 - Ay_2^2 &= (\tfrac{x^2(x^2+3)^2-2}{2})^2 - A(\tfrac{(x^2+1)(x^2+3)(xy)}{2})^2 \\ &= \tfrac{x^{12}+12x^{10}+54x^8+112x^6+105x^4+36x^2+4}{4} - A\tfrac{y^2(x^{10}+8x^8+22x^6+24x^4+9x^2)}{4} \\ &= \tfrac{(x^{10}+8x^8+22x^6+24x^4+9x^2)(x^2-Ay^2)+4x^{10}+32x^8+88x^6+96x^4+36x^2+4}{4} \\ &= \tfrac{4x^{10}-4x^{10}+32x^8-32x^8+88x^6-88x^6+96x^4-96x^4+36x^2-36x^2+4}{4} = 1 \end{aligned}$$

Brahmagupta had de waarde van de eerste wortel (y) dus goed, maar heeft een fout gemaakt in het berekenen van zijn laatste wortel (x). Het is niet precies duidelijk waar deze fout vandaan komt. Omdat de tekst bijzonder compact en moeilijk te interpreteren is kan het aan de vertaling hebben gelegen. Aan de andere kant staat er een commentaar bij de tekst dat deze exacte (foute) uitleg geeft. Colebrooke zelf schrijft niets over deze fout, hoewel hij wel (terecht) opmerkt dat er een fout staat in het voorbeeld dat deze stelling moet illustreren door te zeggen dat 'er iets niet klopt in het manuscript'.

Stanza 73: Stelling 43: *"Wanneer een kwadraat de vermenigvuldiger is, neem dan de vermeerderaar [of verminderaar] gedeeld door een [willekeurig] getal, en nadat het er bij is opgeteld en afgetrokken en het [in beide gevallen] gehalveerd is, is de eerste een 'laatste wortel' en de laatste, gedeeld door de wortel van de vermenigvuldiger, is een 'eerste wortel'."*

Deze Stanza lost $x^2 - Ay^2 = k$ op als A een kwadraat is. Om dat te doen beginnen we met het vinden van een deler l van k. Dan definiëren we de laatste wortel: $x = (\frac{k}{l} + l) \cdot \frac{1}{2} = \frac{k+l^2}{2l}$ en de eerste wortel: $y = (\frac{k}{l} - l) \cdot \frac{1}{2} \cdot \frac{1}{\sqrt{A}} = \frac{k-l^2}{2\sqrt{A}l}$. Dit invullen levert de gevraagde oplossing:

$$\begin{aligned} x^2 - Ay^2 &= (\tfrac{k+l^2}{2l})^2 - A((\tfrac{k-l^2}{2\sqrt{A}l})^2 \\ &= \tfrac{k^2+2kl^2+q^4}{4l^2} - A\tfrac{k^2-2kl^2+q^4}{4Al^2} \\ &= \tfrac{4kl^2}{4l^2} = k. \end{aligned}$$

Merk op dat de stelling geldig is als we $l = 1$ invullen (we eindigen dan met $\frac{4k}{4}$). Merk ook op dat als $k = \pm 1$ de enige mogelijke deler bestaat uit $l = 1$, en daaruit volgt dat $x = 1, y = 0$. Dit is logisch, want we hebben in hoofdstuk 2.2 laten zien dat alleen de triviale oplossing mogelijk is als A een kwadraat is.

Merk ook op dat als k negatief is de volgorde moet worden omgedraaid: dan is degene waar wordt afgetrokken de 'laatste wortel', en degene waar wordt opgeteld de 'eerste wortel'. Brahmagupta gebruikt dit zelf in een voorbeeld dat hij uitwerkt.[3]

[3] De tweede opgave in Stanza 74

Stanza 75: Stelling 45: *"Als de vermenigvuldiger [precies] gedeeld wordt door een kwadraat, dan [wordt] de 'eerste wortel' gedeeld door de wortel van de deler."*

Wanneer we een oplossing hebben voor $x^2 - \frac{A}{p^2}y^2$ ('de vermenigvuldiger gedeeld door een kwadraat'), dan kunnen we een oplossing vinden voor $x^2 - Ay^2$ door de y uit de vorige oplossing te delen door p.

Diverse secundaire bronnen[4] maken er melding van dat Brahmagupta op de hoogte zou zijn van manieren om oplossingen voor $k = \pm 2$ en $k = -1$ om te zetten in oplossingen voor $k = 1$. Hier wordt in de *Brahma-sidd'hánta* niets over gezegd. Het is goed mogelijk dat Brahmagupta op de hoogte was van dergelijke methoden, omdat ze makkelijker zijn dan de methoden voor $k = \pm 4$, die hij wel behandelt. Bewijs daarvoor hebben we echter niet.

Voor de volledigheid zullen we de genoemde regels hier geven, in moderne notatie.

Wanneer we een paar (x, y) hebben zodat $x^2 - Ay^2 = -1$, dan kunnen we beide kanten van de vergelijking kwadrateren.

$$\begin{aligned} (x^2 - Ay^2)^2 &= (-1)^2 \\ x^4 - 2Ax^2y^2 + A^2y^4 &= 1 \\ (x^2 + Ay^2)^2 - A(2xy)^2 &= 1. \end{aligned}$$

We hebben nu dus de oplossing $(x^2 + Ay^2, 2xy)$ geconstrueerd voor $x^2 - Ay^2 = 1$.

Wanneer voor (x, y) geldt dat $x^2 - Ay^2 = \pm 2$, kunnen we ook een oplossing voor $k = 1$ construeren:

We hebben $(x^2 - Ay^2)^2 = (\pm 2)^2$, uitgewerkt levert dit $x^4 - 2Ax^2y^2 + A^2y^4 = 4$. Dit is om te schrijven naar $(x^2 + Ay^2)^2 - A(2xy)^2 = 4$. Nu geldt er (wegens de beginvoorwaarde) dat $2|x^2 - Ay^2$, en dus dat $4|(x^2 - Ay^2)^2$. Dan moet ook gelden dat $4|(x^2 + Ay^2)^2 - 4x^2y^2$, en omdat duidelijk is dat $4|(2xy)^2$ moet volgen dat $4|(x^2 + Ay^2)^2$. Dan is $\frac{x^2+Ay^2}{2}$ een geheel getal, en is $(\frac{x^2+Ay^2}{2}, xy)$ een oplossing voor $x^2 - Ay^2 = 1$.

4.2 Bhaskara, en de volledige cirkelmethode

De volgende grote stap in het oplossen van de vergelijking van Pell wordt vijfhonderd jaar na Brahmagupta gezet door Bhaskara II, een andere Indiase wis-

[4] Weil, *Number Theory*, pagina 21 en Edwards, *Fermat's Last Theorem*, pagina 29

kundige.[5] Hij besteedt Hoofdstuk 3 van zijn werk over Algebra, de *Vîja-gańita* aan het oplossen van de vergelijking van Pell of zoals het heet in het Indiaas, het probleem 'kwadratisch van aard' (*Varga-pracrĭti* of *Crĭti-pracrĭti*).[6]

In hoofdstuk 3 van de *Vîja-gańita* geeft Bhaskara II eerst een kort overzicht dat lijkt op het werk van Brahmagupta. Hij laat hier kort zien hoe je uit oplossingen van de *Varga-pracrĭti* met diverse waarden van *Cshépa* (k) nieuwe oplossingen kunt maken, en dat je in sommige gevallen de *Cshépa* kunt uitdelen. Daarna geeft hij in Sectie II de methode die de vergelijking van Pell oplost door slim gebruik te maken van deze identiteiten. Sectie III bevat enkele losse opmerkingen.

We zullen Bhaskara's tekst in zijn geheel behandelen. Wederom werken we op basis van de vertaling in het boek van Colebrooke.

Sectie I, Stanza 75 *Laat een getal aangenomen worden, en de 'kleinste wortel'*[7] *genoemd worden. Dat getal dat, opgeteld bij of afgetrokken van het product van haar*[8] *kwadraat met de gegeven coëfficient, maakt dat de som een vierkantswortel levert noemen wiskundigen de positieve of negatieve vermeerderaar; en ze noemen deze wortel de 'grootste'.*

Deze definitie van het probleem lijkt sterk op die van Brahmagupta, en gebruikt dezelfde termen. Wel vallen een aantal details in de notatie op.

Zo staat Bhaskara toe dat de 'vermeerderaar' negatief is, in plaats van (zoals Brahmagupta) een negatieve term een geheel andere naam te geven. Dit is des te opvallender omdat beiden het zelfde woord, *Cshépa*, gebruiken voor deze term.

Verder definiëert Bhaskara expliciet zijn probleem, op een manier die lijkt op onze huidige manier van schrijven. Hij benoemt als zijn variabelen en zegt van te voren in welke relatie ze tot elkaar staan. Dit in tegenstelling to Brahmagupta, die aanneemt dat de lezer weet waar hij het over heeft en meteen begint te rekenen.

[5] Er zijn aanwijzingen dat een eerdere Indiase wiskundige, Jayadeva, ook van deze methode op de hoogte was. Het werk waarin dit wordt beschreven, *Gaṇita* van Shukla heb ik echter niet kunnen inzien.

[6] *varga* of *crĭti* betekent kwadraat, *pracrĭti* betekent 'aard' of 'natuur'

[7] Colebrooke noemt deze wortel in dit werk consequent de 'kleinste' wortel, en in het werk van Brahmagupta consequent de 'eerste' wortel, hoewel beide wiskundigen gedeeltelijk dezelfde term (*Canishť'ha*) gebruiken.

[8] 'haar' slaat op de 'kleinste wortel', niet op 'dat getal dat...'

Stanza 76 *"Nadat de 'kleinste' en 'grootste' wortels en de vermeerderaar zijn neergezet, en nadat onder hen dezelfden of anderen in dezelfde volgorde zijn geplaatst, is het mogelijk veel wortels te vinden door compositie. Daarvoor zullen hun samenstellingen worden voorgelegd."*

Vergelijk dit met het begin van Stanza 65-66 in Brahmagupta's werk. Bhaskara gaat ons uitleggen hoe we uit oplossingen $x_1^2 - Ay_1^2 = k_1$ en $x_1^2 - Ay_2^2 = k_2$ nieuwe oplossingen kunnen maken. Merk weer op hoe netjes Bhaskara definieert, en hoe hij van tevoren zegt welk probleem hij aan gaat pakken.

Net als Brahmagupta wordt de wiskunde hier beschreven in practische, bijna fysieke termen. De lezer wordt geïnstrueerd om het ene rijtje getallen onder het andere te zetten, waar wij tegenwoordig alleen zouden zeggen wat er met de getallen moet gebeuren, en de lezer zelf zijn notatie zouden laten kiezen. Voor de wiskundige correctheid maakt notatie immers niet uit. De Indiase schrijfwijze is meer gericht op het daadwerkelijke uitvoeren van het proces.

Stanza 77 *"De 'grootste' en 'kleinste' wortels moeten kruiselings vermenigvuldigd worden, en de som van de producten moet genomen worden als 'kleinste wortel'. Het product van de twee [originele] 'kleinste' wortels vermenigvuldigd met de gegeven coëfficient en het product van de 'grootste' wortels hieraan toegevoegd, deze som is de bijbehorende 'grootste' wortel; en het product van de vermeerderaren zal de nieuwe vermeerderaar zijn."*

Dit zegt dat $(x_1x_2 + Ay_1y_2)^2 - A \cdot (x_1y_2 + x_2y_1)^2 = k_1k_2$.

Stanza 78 *"Of het verschil van de producten van de kruiselingse vermenigvuldiging van 'kleinste' en 'grootste' wortels kan worden genomen als 'kleinste' wortel, en het verschil tussen het product van de twee [oorpronkelijke] 'kleinste' wortels samen vermenigvuldigd en in de coëfficiënt genomen, en het product van de 'grootste' wortel samen vermenigvuldigd, zal de bijbehorende 'grootste wortel' zijn: en ook hier zal de vermeerderaar het product van de twee [oorspronkelijke] vermeerderaars zijn."*

Deze regel lijkt sterk op de bovenstaande. Bhaskara zegt dat $(x_1x_2 - Ay_1y_2, x_1y_2 - x_2y_1)$ ook een oplossing is voor $k = 1$.

$$
\begin{aligned}
(x_1x_2 - Ay_1y_2)^2 - A(x_1y_2 - x_2y_1)^2 &= x_1^2x_2^2 - 2Ax_1x_2y_1y_2 + A^2y_1^2y_2^2 \\
&\quad -A(x_1^2y_2^2 - 2x_1x^2y_1y_2 + x_2^2y_1^2) \\
&= x_1^2x_2^2 - Ax_1^2y_2^2 - Ax_2^2y_1^2 + A^2y_1^2y_2^2 \\
&= (x_1^2 - Ay_1^2)(x_2^2 - Ay_2^2) = k_1k_2
\end{aligned}
$$

Dat klopt dus.

Stanza 79 *"Laat de vermeerderaar gedeeld door het kwadraat van een aangenomen getal een nieuwe vermeerderaar zijn; en de wortels, gedeeld door dat aangenomen getal, zullen de bijbehorende wortels zijn. Of, als de vermeerderaar vermenigvuldigd wordt [met het kwadraat], dan moeten de wortels op dezelfde manier vermenigvuldigd worden [met het aangenomen getal]"*

Vergelijk dit met Brahmagupta, Stanza 75, maar merk op dat Bhaskara naast deling ook vermenigvuldiging toestaat.

Stanza 80-81 *"Of deel het dubbele van een aangenomen getal door het verschil van dat kwadraat van dat getal met de gegeven coëfficiënt; en laat het quotient genomen worden als 'kleinste' wortel, wanneer één de vermeerderaar is, en vind vanaf daar de 'grootste' wortel. Hier [zijn de oplossingen] oneindig, zowel door [verscheidenheid van] aannamen als door [diversiteit van] compositie."*

Wanneer de vermeerderaar één is, kiezen we een willekeurige n, en we stellen $y = \frac{2n}{n^2-A}$. Volgens Bhaskara kunnen we nu een passende x uitrekenen.

$$
\begin{aligned}
x^2 - A \cdot (\tfrac{2n}{n^2-A})^2 &= 1 = \tfrac{(n^2-A)^2}{(n^2-A)^2}, \text{ na vermenigvuldiging met } (n^2-A) \text{ staat hier:} \\
x^2(n^2-A)^2 &= 4An^2 + (n^2-A)^2, \text{ oftewel:} \\
x &= \tfrac{(n^2+A)}{(n^2-A)}
\end{aligned}
$$

Het lijkt alsof Bhaskara hier in één klap de vergelijking van Pell oplost, maar er is geen enkele garantie dat de genoemde getallen geheel zijn, in plaats van breuken. Op deze manier vind je gegarandeerd een *rationale* oplossing, maar dat zegt niets over een oplossing in gehele getallen.

Na deze rekenregels geeft Bhaskara eerst een uitgebreid voorbeeld in Stanza 82, dat we over zullen slaan. Stanza's 83 tot en met 86 bevatten de *Chacraválа*, wat we het beste kunnen vertalen als 'cyclische methode' of 'cirkelmethode' [9], de

[9] '*Chacraválа*' betekent letterlijk 'cirkel'. De methode is naar de cirkel genoemd omdat het bestaat uit het steeds herhalen van dezelfde stappen; je zou je kunnen voorstellen dat deze stappen punten zijn op een cirkel die je steeds weer doorloopt.

manier waarop de Indiërs er uiteindelijk in slaagden om de vergelijking van Pell voor gehele getallen op te lossen. We zullen deze methode stapje voor stapje doorlopen.

Bhaskara gaat er van uit dan hij een x, y en k kan vinden zodat $x^2 - Ay^2 = k$. (Het is niet moeilijk zo'n vergelijking te maken: kies bijvoorbeeld $x = \lfloor\sqrt{A}\rfloor + 1$, en $y = 1$.) Met behulp van deze gelijkheid gaat hij een nieuwe gelijkheid van hetzelfde type maken: $x'^2 - Ay'^2 = k'$. De hoop is dat deze nieuwe gelijkheid hem dichterbij een oplossing voor $k = 1$ brengt.

Stanza 83-86 *"Regel voor de cyclische methode: nadat we van de 'kleinste' en 'grootste' wortels en de vermeerderaar een teller, vermeerderaar en noemer hebben gemaakt is op deze manier de vermenigvuldiger te vinden. "*

Dit is wat moeilijk te begrijpen zonder enige uitleg. Bhaskara zoekt een nieuwe 'vermenigvuldiger' (wij zullen dit getal r noemen). Hij gaat ervan uit dat hij deze al heeft, en beschrijft dan een breuk waarin y een teller is en x vermeerderaar, en k een noemer; deze breuk komt neer op $\frac{yr+x}{k}$.

Voor de methode is het noodzakelijk dat deze breuk een geheel getal is. Waarschijnlijk definiëert Bhaskara hier dan ook niet zozeer de breuk zelf (hoewel die later ook nog nuttig zal blijken te zijn), maar probeert hij te zeggen wat wij nu als volgt schrijven:

"Er is een vermenigvuldiger r, zodanig dat $\frac{yr+x}{k}$ een geheel getal is".

"Na de vermindering van de gegeven coëfficiënt met het kwadraat van deze vermenigvuldiger, of van de vermindering van het kwadraat van de vermenigvuldiger met de coëfficiënt (zodanig dat het overblijfsel klein is), is het overblijvende gedeeld door de originele vermeerderaar een nieuwe vermeerderaar; die wordt geïnverteerd als de aftrekking [het kwadraat] van de coëfficiënt [afhaalt]."

Bhaskara definieert hier een verschil tussen r^2 en A, dat wij s zullen noemen. Dit moet zó gedaan worden dat s zo klein mogelijk is (we zullen straks zien waarom). Merk op dat het Bhaskara niet uitmaakt of r^2 groter of kleiner is dan A, als $|r^2 - A|$ maar zo klein mogelijk is. Hij zegt wel dat 'als de aftrekking [het kwadraat] van de coëfficiënt [afhaalt]' het antwoord 'geïnverteerd' moet worden. Een commentaar van Ráma Crishńa, een andere wiskundige, maakt duidelijk dat dit betekent dat het teken moet worden omgewisseld.

Wat Bhaskara hier zegt is: zoek r zodat je de kleinst mogelijke $|r^2 - A|$ hebt. Als

dit kleinste resultaat van de vorm $A - r^2$ is, zet dan een min voor dit resultaat. In hedendaagse termen definiëren we s als $r^2 - A$ en eisen we dat $|r^2 - A|$ minimaal is.

Merk op dat er drie eisen aan r zijn, die het getal uniek vastleggen. r moet geheeltallig zijn, de breuk $\frac{yr+x}{k}$ moet geheeltallig zijn, en $|r^2 - A|$ moet minimaal zijn. De mogelijkheid dat er geen r bestaat die aan de drie voorwaarden voldoet (in het bijzonder de tweede), wordt besproken in sectie 4.4.

Vergeleken met de Engelse wiskundigen die dit probleem aanpakken valt op dat Bhaskara er geen probleem mee heeft negatieve getallen te gebruiken, iets waar Westerse wiskundigen vierhonderd jaar later aanmerkelijk meer bezwaren tegen hebben.

Als we s eenmaal hebben vinden we volgens Bhaskara k', een nieuwe vermeerderaar, door $k' = \frac{s}{k}$.

"De breuk behorend bij de vermenigvuldiger [en erbij gevonden] zal de 'kleinste wortel' zijn, waarvandaan de 'grootste wortel' kan worden afgeleid."

Onze nieuwe 'kleinste wortel', y', is gedefinieerd als $\frac{yr+x}{k}$. Daarmee kunnen we x' uitrekenen.

$x'^2 - Ay'^2 = k'$, dus
$x'^2 = \frac{r^2-A}{k} + A\frac{y^2r^2+2rxy+x^2}{k^2}$, en
$x'^2 = \frac{r^2x^2+2Arxy+Ay^2}{k^2}$, en daarmee
$x' = \frac{rx+Ay}{k}$

"Met deze [nieuwe getallen] wordt de onderneming herhaald, door de vroegere wortels en vermeerderaar opzij te zetten."

We hebben nu een nieuwe vergelijking, $x'^2 - Ay'^2 = k'$. We kunnen hier uiteraard hetzelfde proces op toepassen, en zo de 'cirkel' compleet maken.

"Deze methode noemen wiskundigen degene van de cirkel. Zo worden gehele wortels gevonden met vier, twee, of één [of een ander getal] als vermeerderaar: en compositie dient om wortels af te leiden voor de positieve eenheid uit diegenen die een oplossing zijn voor twee of vier [of een ander getal]."

Bhaskara raadt ons aan door te gaan tot we uitkomen op een vermeerderaar van

1,2 of 4, en dan eventueel met behulp van 'compositie' (zoals de vergelijkingen van Brahmagupta) een oplossing voor 1 te vinden. Bhaskara zegt hier niets over het teken van k (k zou bijvoorbeeld gelijk kunnen zijn aan -4), maar één van zijn commentatoren, *Crĭshńa*, merkt op dat het hier gaat om 'vier, twee of één positief of negatief, of een of ander ander getal'. Wat er wordt bedoeld met dit 'andere getal' is niet geheel duidelijk, Bhaskara geeft in ieder geval geen regels voor andere getallen dan één twee en vier.

Stanza 87 bevat een uitgebreid voorbeeld dat we later zullen behandelen. Na deze beschrijving van de cirkelmethode geeft Bhaskara een sectie met 'diverse regels'.

Stanza 88-89: *"Regel: als de vermenigvuldiger [dat wil zeggen: de coëfficient voor de 'kleinste' wortel] niet de som van [twee] kwadraten is, wanneer de eenheid aftrekkend is, dan is het voorgestelde imperfect."*

Volgens commentaar van de wiskundigen Chrĭshńa en Súryadása betekent 'imperfect' hier 'onoplosbaar'. Bhaskara geeft verder geen toelichting bij zijn bewering. Zijn bewering is correct, zie ook [het hoofdstuk over $k \neq 1$].

"Als het probleem correct is gesteld, laat dan de eenheid twee maal neergezet gedeeld worden door de wortels van de [deel-]kwadraten[10]*: en laten de quotiënten genomen worden als twee 'kleinste' wortels voor de negatieve eenheid: daarvandaan kunnen de overeenkomstige 'grootste' wortels worden beredeneerd. Of twee wortels voor de negatieve eenheid kunnen worden gevonden op de manier die al is laten zien".*

Als $A = b^2 + c^2$, en we vullen in dat $y = \frac{1}{b}$ (of $y = \frac{1}{c}$, dat maakt niet uit), dan volgt dat $x^2 - (b^2 + c^2)\frac{1}{b^2}) = -1$, daaruit volgt weer dat $x = c$ (als we beginnen met $y = \frac{1}{c}$ volgt $x = b$).

Het is bijzonder opvallend dat Bhaskara hier plotseling rationale oplossingen goedkeurt, in plaats van alleen geheeltallige. Het is niet duidelijk waarom hij dit doet. Wel is het zo dat er voor gehele getallen niet altijd een oplossing bestaat, zelfs niet als geldt dat $A = b^2 + c^2$.

Stanza's 90 en 91 zijn voorbeelden. Dan vervolgt hij:

Stanza 92: *"Voor een positief of negatief getal kunnen [op diverse*

[10] dat wil zeggen, de twee kwadraten die optellen tot A

wijzen] bijbehorende wortels worden gevonden volgens eigen inzicht [van de uitvoerende]: en uit hen kan een oneindig aantal worden afgeleid, door samenstelling met wortels voor de positieve eenheid. "

Dit lijkt op wat aan het begin van het hoofdstuk wordt gezegd. De uitspraak dat er wortels kunnen gevonden is niet geheel correct; er zijn namelijk mogelijkheden die niet oplosbaar zijn. Waarschijnlijk bedoelt Bhaskara hier dat het mogelijk is veel oplossingen te vinden, en dat gegeven zo'n oplossing en een oplossing voor $k = 1$ het mogelijk is oneindig veel nieuwe oplossingen te maken. Ook in het licht van Stanza's 88-89 is het onrealistisch er van uit te gaan dat Bhaskara hier zegt dat ieder probleem van de vorm $x^2 - Ay^2 = k$ oplosbaar is.

Stanza 93 *"Regel: Wanneer de vermenigvuldiger [coëfficient] gedeeld wordt door een kwadraat [en de bijbehorende wortels gevonden worden], deel dan de 'kleinste' wortel door de wortel van dit kwadraat."*

(Stanza 94 is een bijbehorend voorbeeld).

Vergelijk het behandelde werk van Brahmagupta, Stanza 75 op pagina 28.

Stanza 95 *"Regel: de vermeerderaar, gedeeld door een aangenomen hoeveelheid wordt twee keer neergezet en de aangenomen hoeveelheid wordt er in het ene geval van afgetrokken, en in het andere geval bij opgeteld: ieder wordt gehalveerd en de eerste wordt gedeeld door de wortel van de vermenigvuldiger [coëfficient]. De resultaten zijn de 'kleinste' en 'grootste' wortel, in die volgorde."*

Vergelijk het behandelde werk van Brahmagupta, Stanza 73 op pagina 27.

Hierna volgen nog drie voorbeelden in Stanzas 96, 97 en 98, en dan het slot van het hoofdstuk:

Stanza 99 *"Deze berekening, waarlijk toepasbaar op algebraïsch onderzoek, is kort uitgelegd. Nu zal ik algebra voorleggen die voldoening zal schenken aan wiskundigen."*

(Het volgende hoofdstuk gaat over het oplossen van lineaire vergelijkingen).

We zullen hier nog een keer de 'cirkelmethode' samenvatten, voor we hem in een volgend hoofdstuk wiskundig analyseren. We beginnen met het vinden van een kloppende vergelijking $x_1^2 - Ay_1^2 = k_1$. Bhaskara zelf gebruikt als eerste vergelijking $x_1 = \lfloor\sqrt{A}\rfloor, y_1 = 1$, waaruit k eenvoudig te berekenen is. Gegeven

deze vergelijking kiezen we een r_1, die moet voldoen aan de volgende eisen:

- r_1 moet positief zijn.
- k_1 moet $x_1 + y_1 r_1$ delen.
- $|s_1| := |r_1^2 - A|$ moet minimaal zijn.

Als we deze r_1 hebben, berekenen we x_2, y_2 en k_2 als volgt:[11]

- $x_2 = \frac{x_1 r_1 + A y_1}{|k_1|}$
- $y_2 = \frac{x_1 + y_1 r_1}{|k_1|}$
- $k_2 = \frac{s_1}{k_1}$

Dit leidt tot een nieuwe kloppende gelijkheid:

$$\begin{aligned} x_2^2 - A y_2^2 &= (\tfrac{x_1 r_1 + A y_1}{|k_1|})^2 - A(\tfrac{x_1 + y_1 r_1}{|k_1|})^2 \\ &= \tfrac{x_1^2 r_1^2 + 2A x_1 y_1 r_1 + A^2 y_1^2}{k_1^2} - \tfrac{A x_1^2 + 2A x_1 y_1 r_1 + A y_1^2 r_1^2}{k_1^2} \\ &= \tfrac{(x_1^2 - A y_1^2)(r_1^2 - A)}{k_1^2} = \tfrac{s_1}{k_1} = k_2 \end{aligned}$$

We herhalen het proces startend met deze nieuwe vergelijking. We gaan net zo lang door totdat we een vergelijking vinden waar hetzij $k = 1$, hetzij $k = -1, \pm 2$, of ± 4 (in welk geval we de bekende formules kunnen gebruiken om een oplossing voor $k = 1$ te construeren).

Om dit alles te illustreren zullen we nu eerst Bhaskara's eigen voorbeeld behandelen, en tevens vertalen naar de bovenstaande moderne notatie. Daarna zullen we in detail behandelen of dit algoritme altijd uitvoerbaar is.

4.3 Een voorbeeld voor $A = 67$

Om de cirkelmethode te illustreren zullen we een voorbeeld laten zien dat ook door Bhaskara zelf behandeld wordt. We zullen Bhaskara's methode niet precies volgen, omdat sommige van Bhaskara's berekeningen heel anders zijn dan die van tegenwoordig, en het uitvoerige uitleg zou kosten om duidelijk te maken wat hij precies doet. Het voegt weinig toe hier uitgebreid aandacht aan te

[11] We mogen het teken van x_i en y_i kiezen. Door te delen door $|k_i|$ zijn x_i en y_i altijd positief. Zie voor rechtvaardiging ook het voorbeeld in hoofdstuk 4.3.

besteden. We zullen dan ook sommige stukken letterlijke berekening overslaan of samenvatten.

Stanza 87 *"Voorbeeld: Wat is het kwadraat, dat, vermenigvuldigd met zevenenzestig, en met één opgeteld bij het product, een kwadraat oplevert? En welk is het dat, vermenigvuldigd met eenenzestig, met de eenheid aan het product toegevoegd, hetzelfde zal doen? Verklaar dit, vriend, als de methode kwadratisch van aard grondig verspreid is over uw geest, zoals een klimplant over een boom."*

Bhaskara vraagt ons oplossingen voor $x^2 - 67y^2 = 1$ en voor $x^2 - 61y^2 = 1$.

"Verklaring van het eerste voorbeeld: (Door de eenheid te zetten voor de 'kleinste' wortel, en drie negatief voor de vermeerderaar)
$C\,67\ L\,1\ G\,8\ A\,\dot{3}.$ "[12] [13]

We beginnen met de 'kleinste' wortel (y) op één te zetten, en -3 te kiezen voor de vermeerderaar (k). Hieruit is het eenvoudig te berekenen dat de 'grootste' wortel (x) 8 moet zijn. Merk op deze waarden zo gekozen zijn dat $|k|$ minimaal is.

Wij hebben het voordeel dat we moderne notatie kunnen gebruiken. In het bijzonder kunnen we de waarden uit iedere iteratie van elkaar onderscheiden door middel van indices. We beginnen nu dan ook met:

- $x_1 = 8$
- $y_1 = 1$
- $k_1 = -3$

In het hierop volgende gedeelte gaat Bhaskara de vergelijking $\frac{x+ry}{k}$ oplossen. Hij doet dit met een algoritme dat verwant is aan het algoritme van Euclides. We zullen dit hier verder niet uitleggen; het voldoet dat de r die hij vindt correct is.

De r zodanig dat $3|(8 + r)$ zijn $r = 1, 4, 7, 10, ...$ Het is eenvoudig te zien dat $r_1 = 7$ de minimale $|s_1|$ levert, namelijk $s_1 = -18$.

[12] $\dot{a}$ is de indiase notatie voor $-a$

[13] Het is mij niet geheel duidelijk of deze notatie met letters voor de variabelen van Colebrooke is, of van Bhaskara zelf. In het laatste geval duidt dat er op dat Bhaskara een hoger niveau van abstractie beheerste dan algemeen wordt aangenomen.

"...een nieuwe vermenigvuldiger wordt gevonden: 7. Diens kwadraat 49 afgetrokken van de coëfficient 67, is het overblijvende 18 gedeeld door de oorspronkelijke deler $\dot{3}$ levert $\dot{6}$, het teken waarvan wordt omgedraaid, omdat het kwadraat van de coëfficiënt werd afgehaald."

Net als wij vindt Bhaskara $r_1 = 7$. Hiermee berekent hij $s_1 = 18$; merk op dat hij eerst het resultaat van de aftreksom opschrijft als een positief getal, daarmee k_2 berekent, en dan pas kijkt naar het teken dat de uitkomst zou moeten hebben.

"Het quotiënt behorend bij deze vermenigvuldiger, 5, is de 'kleinste' wortel. Het maakt voor de rest van het werk niet uit of dit negatief of positief is. Het wordt daarom opgeschreven als 5 positief. Diens kwadraat vermenigvuldigd met de coëfficiënt en 6 opgeteld bij het product, en de wortel getrokken, is de uitkomst van de 'grootste' wortel 41."

De 'kleinste' wortel (y_2) wordt de uitkomst van de deelsom: 5. Bhaskara merkt terecht op dat het teken van dit getal niet uitmaakt (het komt alleen nog als kwadraat voor), en dat hij het daarom positief mag *kiezen*. Technisch gezien is y_2 negatief, omdat de teller van de breuk positief is, en de noemer negatief.

Na de berekening van y_2 en k_2 wordt x_2 afgeleid. Bhaskara geeft geen formule voor de x_i, maar leidt ze steeds ter plekke af uit y_i en k_i.

We eindigen de eerste ronde langs de cirkel met de vergelijking $41^2 - 67 \cdot 5^2 = 6$.

Nu moeten we r_2 vinden. De eis is dat $6|(41 + 5r_2)$. Mogelijke waarden van r_2 die hier aan voldoen zijn 5, 11, 17, enzovoorts. Hiervan geeft $r_2 = 5$ de kleinst mogelijke s_2, namelijk $s_2 = -42$. Hieruit berekenen we:

- $x_3 = \frac{41 \cdot 5 + 67 \cdot 5}{6} = 90$
- $y_3 = \frac{41 + 5 \cdot 5}{6} = 11$
- $k_3 = \frac{-42}{6} = -7$

Deze getallen stellen weer eisen aan r_3: $7|(90 + 11r_3)$. De optimale waarde van r_3 is 9, zodat $s_3 = 14$. Dit geeft de volgende nieuwe getallen:

- $x_4 = \frac{90 \cdot 9 + 67 \cdot 11}{7} = 221$
- $y_4 = \frac{90 + 11 \cdot 9}{6} = 27$

- $k_4 = \frac{14}{-7} = -2$

Tot dusver hebben we geen idee hoe goed of slecht het gaat met onze methode, en hoe dicht we bij een oplossing zitten. Als we gewoon door zouden gaan met het uitvoeren van het algoritme moeten we nog 5 stappen doen, met steeds grotere getallen. Bhaskara zelf gaf echter al aan op pagina 33 dat zijn methode moet worden uitgevoerd tot een k_i van $\pm 1, \pm 2$ of ± 4 bereikt is. Daarna kan het uiteindelijke antwoord gevonden worden door compositie. Dit is precies wat Bhaskara nu gaat doen:

"Vanaf deze[14]*, zijn andere af te leiden door combinatie van gelijksoortige groepen.*

Verklaring: $L \quad 27 \quad G \quad 221 \quad A \quad \dot{2}$
$l \quad 27 \quad g \quad 221 \quad a \quad \dot{2}$

Door te doen zoals is aangegeven vinden we de wortels L *11934,* G *97684,* A *4. Deze wortels gedeeld door de wortel van positief vier geven wortels die een antwoord zijn voor de positieve eenheid:* L *5967,* G *48842,* A *1."*

(Bhaskara vervolgt met de uitwerking van het voorbeeld voor $A = 61$, een voorbeeld dat hij waarschijnlijk heeft uitgekozen om haar moeilijkheid. De kleinste y zodat $Ay^2 + 1$ een kwadraat is, is 226153980).

Met 'doen wat is aangegeven' bedoelt Bhaskara het vermenigvuldigen van de twee vergelijkingen volgens de door hem (en eerder door Brahmagupta) gegeven regel. Zie hiervoor Stanza's 76 en 77.

De uitkomst is dus $48842^2 - 67 \cdot 5967^2 = 1$. Dit is een correct antwoord.

We zullen in het volgende hoofdstuk laten zien dat de cirkelmethode om de vergelijking van Pell op te lossen altijd uitgevoerd kan worden.

[14] ...gevonden wortels...

4.4 Wiskundige onderbouwing van de cirkelmethode

Deze en de volgende sectie zijn geheel mijn eigen werk. Ik zal hierin de cirkelmethode zoals beschreven in de literatuur[15] overzetten naar moderne notatie, en haar correctheid bewijzen. Ook zal de de zogeheten 'versimpelde cirkelmethode' uitleggen, een variant die functioneel equivalent is, maar handiger zal blijken in een latere vergelijking met kettingbreuken.

Om te beginnen zullen we de cirkelmethode wat anders opschrijven. We beginnen met de vergelijking $x_1^2 - A \cdot y_1^2 = k_1$, die we als volgt invullen:

- $x_1 := 1$
- $y_1 := 0$
- $k_1 := x_1^2 - A \cdot y_1^2 = 1$

Voor iedere set x_i, y_i, k_i berekenen we r_i en s_i:

- r_i voldoet aan de eisen:
  - r_i is positief.
  - $|k_i|$ deelt $(x_i + y_i \cdot r_i)$.
  - $|r_i^2 - A|$ is minimaal.
- $s_i := r_i^2 - A$

Uit x_i, y_i, k_i, r_i en s_i berekenen we de volgende generatie: x_{i+1}, y_{i+1} en k_{i+1}.

- $x_{i+1} := \frac{x_i r_i + A y_i}{|k_i|}$.
- $y_{i+1} := \frac{x_i + r_i y_i}{|k_i|}$.
- $k_{i+1} := \frac{s_i}{k_i}$

We stoppen op het moment dat $k_i = 1$. Immers, dan hebben we een vergelijking $x_i^2 - A y_i^2 = 1$, en dan is (x_i, y_i) een oplossing van de vergelijking van Pell.

[15] Weil, *Number Theory*, Hoofdstuk 1.9 en Edwards, *Fermat's Last Theorem*, Hoofdstuk 1.9

Dit is de manier waarop wij tegenwoordig de cirkelmethode op zouden schrijven. Het is een verdere formalisatie van wat we aan het eind van Hoofdstuk 4.2 hebben opgeschreven. In plaats van te beginnen met een 'willekeurige' oplossing van $x^2 - Ay^2 = k$ beginnen we met de triviale oplossing. Hiermee kunnen we later een symmetrie laten zien in de ontwikkeling van de k_i en de r_i. Merk op dat $x_2 = \lfloor\sqrt{A}\rfloor$ of $x_2 = \lceil\sqrt{A}\rceil$, en $y_2 = 1$, en dat Bhaskara zijn voorbeeld inderdaad begint met $x_2 = 8 = \lfloor\sqrt{67}\rfloor$.

Het grote voordeel van deze notatie is dat het stukken makkelijker is om uitspraken te doen over bijvoorbeeld alle x_i en y_i die in het algoritme voorkomen:

Stelling 4.1. *De x_i en y_i zijn altijd copriem. Dat wil zeggen, ze hebben nooit een gemene deler die groter is dan 1.*

Bewijs. x_1 en y_1 zijn duidelijk copriem. Stel nu dat x_i en y_i copriem zijn, en bekijk de volgende vergelijking:

$$x_i y_{i+1} - x_{i+1} y_i = \frac{x_i(x_i + r_i y_i)}{|k_i|} - \frac{y_i(x_i r_i + A y_i)}{|k_i|} = \frac{x_i^2 - A y_i^2}{|k_i|} = \frac{k_i}{|k_i|} = \pm 1.$$

Elke gemene deler van x_{i+1} en y_{i+1} deelt dus ± 1. Dan moet de grootste gemene deler van x_{i+1} en y_{i+1} dus 1 zijn, en zijn x_{i+1} en y_{i+1} copriem. □

Stelling 4.2. *y_i en k_i zijn copriem voor alle i.*

Bewijs. We weten dat $x_i^2 - Ay_i^2 = k_i$. Als $a|y_i$ en $a|k_i$, dan geldt dat $a|k_i + Ay_i^2 = x_i^2$. Omdat x_i en y_i copriem zijn, moet gelden dat $a = \pm 1$. Hieruit volgt dat y_i en k_i copriem zijn. □

Stelling 4.3. *Er is een positieve r_i te vinden zodat $k_i|(x_i + r_i y_i)$.*

Bewijs. y_i en k_i zijn copriem. Er is dus een a_i zodat $a_i y_i \equiv -x_i \bmod k_i$. Voor gehele waarden van n geldt dan ook dat $(nk_i + a_i)y_i \equiv x_i \bmod k_i$. Door nu n groot genoeg te maken is een r_i te vinden die positief is, en waarvoor $r_i y_i \equiv -x_i \bmod k_i$. □

Stelling 4.4. $k_i | x_i r_i + A y_i$.

Bewijs. Bekijk $y_i \cdot (x_i r_i + A y_i) = x_i^2 - k_i + x_i r_i y_i = x_i(x_i + r_i y_i) - k_i$. Omdat r_i zo gekozen is dat $k_i|(x_i + y_i r_i)$, is $x_i(x_i + r_i y_i) - k_i$ en daarmee $y_i \cdot (x_i r_i + A y_i)$ deelbaar door k_i. Omdat y_i en k_i copriem zijn volgt dat $k_i | x_i r_i + A y_i$. □

Gevolg 4.1. $k_i^2 | (x_i r_i + A y_i)^2$.

We hebben hiermee laten zien dat x_{i+1} en y_{i+1} geheeltallig zijn. We weten al uit het eind van sectie 4.2 dat $x_{i+1}^2 - Ay_{i+1}^2 = \frac{(x_i^2 - Ay_i^2)(r_i^2 - A)}{k_i^2} = \frac{s_i}{k_i}$. Omdat de linkerkant van deze vergelijking geheeltallig is moet de rechterkant dat ook zijn, en daarmee weten we dat $k_i|(r_i^2 - A)$.

Uit deze stellingen blijkt dat de cirkelmethode altijd voortgezet kan worden. We kunnen altijd een getal A kiezen dat geen kwadraat is en gaan rekenen, en als het algoritme stopt geeft het ons een oplossing voor de vergelijking van Pell.

We weten nu nog niet of er altijd een oplossing *is*, en of de cirkelmethode altijd een oplossing vindt als er één bestaat. Het is immers theoretisch mogelijk dat er voor een bepaalde A wel een oplossing bestaat, maar dat het algoritme oneindig lang doorgaat en de oplossing nooit vindt. Het aantonen van deze eigenschappen is niet eenvoudig; we zullen dit later doen door de cirkelmethode te vergelijken met Lagrange's algoritme, dat gebruik maakt van kettingbreuken.

Als laatste is het nuttig om twee kleine stellingen te bewijzen, die samen aantonen dat je voor het berekenen van de k_i en r_i de x_i en y_i niet nodig hebt. We zullen hier later gebruik van maken bij het vergelijken van de cirkelmethode met de kettingbreuk van $\sqrt{A}$.

Stelling 4.5. $k_{i+1}|(x_{i+1} - r_i y_{i+1})$.

Bewijs. $x_{i+1} - r_i y_{i+1} = \frac{x_i r_i + A y_i}{|k_i|} - \frac{r_i(x_i + r_i y_i)}{|k_i|} = \frac{A y_i - r_i^2 y_i}{|k_i|} = \frac{-s_i y_i}{|k_i|} = \pm y_i k_{i+1}$. □

Stelling 4.6. $k_{i+1}|(r_i + r_{i+1})$.

Bewijs. We weten dat $k_{i+1}|x_{i+1} + r_{i+1}y_{i+1}$ per het algoritme. Uit Stelling 4.5 volgt dat $x_{i+1} \equiv r_i y_{i+1} \bmod k_{i+1}$. Dan geldt dus dat $k_{i+1}|(r_i + r_{i+1})y_{i+1}$. Omdat volgens Stelling 4.2 y_{i+1} en k_{i+1} copriem zijn, moet gelden dat $k_{i+1}|(r_i + r_{i+1})$. □

Omgekeerd geldt dat als algemeen geldt dat $k_{i+1}|(r_i + r_{i+1})$, dat dan algemeen geldt dat $k_i|x_i + r_i y_i$:

Stelling 4.7. *Als* $k_{i+1}|(r_i + r_{i+1})$ *voor alle* i*, dan* $k_i|x_i + r_i y_i$ *voor alle* i*.*

Bewijs. Met inductie:
$x_1 = 1$, $y_1 = 0$, $k_1 = 1$, dus $k_1|x_1 + r_1 y_1$. Als $k_i|(x_i + r_i y_i)$ en $k_{i+1}|(r_i + r_{i+1})$ geldt:
$k_i k_{i+1}|(x_i + r_i y_i)(r_i + r_{i+1})$, dus
$k_i k_{i+1}|x_i r_i + x_i r_{i+1} + r_i^2 y_i + r_i r_{i+1} y_i)$, dus

$k_{i+1} | \frac{x_i r_i + A y_i}{|k_i|} + r_{i+1} \frac{x_i + r_i y_i}{|k_i|} + \frac{s_i y_i}{|k_i|}$, en daarmee
$k_{i+1} | x_{i+1} + r_{i+1} y_{i+1}$ (omdat $s_i = k_i k_{i+1}$). □

Als we alleen geïnteresseerd zijn in de k_i en r_i kunnen we dus het volgende, simplere algoritme volgen:

Initialisatie:

- $r_1 = \lfloor \sqrt{A} \rfloor$.
- $k_1 = 1$.

Iteratie:

- $s_i = r_i^2 - A$
- $k_{i+1} = \frac{s_i}{k_i}$.
- Kies r_{i+1} zó dat
  - r_{i+1} is positief.
  - $|k_{i+1}|$ deelt $(r_i + r_{i+1})$.
  - $|r_{i+1}^2 - A|$ is minimaal.

Ga door met itereren todat $k_i = 1$.

Als we de k_i en r_i eenmaal hebben, kunnen we één voor één de x_i en y_i berekenen. x_2 en y_2 hangen alleen van x_1, y_1, k_1 en r_1, en die zijn allemaal bekend. Daarna heb je voldoende gegevens om x_3 en y_3 te berekenen, en zo ga je door tot je aangekomen bent bij $k_i = 1$.

4.5 De versimpelde cirkelmethode

We zullen nu een extra eis stellen bij de keuze van r_{i+1}, namelijk dat $r_{i+1} < \sqrt{A}$. Dan volgt dat we kunnen eisen dat $A - r_{i+1}^2$ minimaal is, in plaats van $|r_{i+1}^2 - A|$. Merk op dat in dit geval $s_i = r_i^2 - A$ altijd negatief is, en dat de tekens van k_i en k_{i+1} daardoor altijd tegengesteld zijn.[16]

[16] Het verband tussen de twee cirkelmethoden en verschillende typen kettingbreuken zal worden behandeld in hoofdstuk 7

We zullen in dit hoofdstuk de resulterende r_i van deze 'versimpelde' cirkelmethode aangeven met r'_i. Deze r'_i leidt tot x'_{i+1}, y'_{i+1} en k'_{i+1}, en aan de hand daarvan vinden we weer een r'_{i+1}.

We moeten natuurlijk aantonen dat het altijd mogelijk om een r'_i te vinden zodat $0 < r'_i < \sqrt{A}$ en $|k'_i|$ deelt $(r'_{i-1} + r'_i)$. We doen dit met volledige inductie.[17]

Stelling 4.8. *Het is altijd mogelijk om een r'_i te vinden zodat $0 < r'_i < \sqrt{A}$ en zodat $|k'_i|$ een deler is van $(r'_{i-1} + r'_i)$.*

Bewijs. We zullen door middel van inductie twee ongelijkheden bewijzen waar duidelijk uit blijkt dat r'_i positief moet zijn:
$k'_i + 2r'_i + k'_{i+1} > 0$
$k'_i - 2r'_i + k'_{i+1} < 0$.

Deze ongelijkheden gelden voor k_1, k_2, r_1:
$k'_1 + 2r'_1 + k'_2 \quad = 1 + 2\lfloor\sqrt{A}\rfloor + \lfloor\sqrt{A}\rfloor^2 - A = (\lfloor\sqrt{A}\rfloor + 1)^2 - A > 0,$
$k'_1 - 2r'_1 + k'_2 \quad = 1 - 2\lfloor\sqrt{A}\rfloor + \lfloor\sqrt{A}\rfloor^2 - A = (\lfloor\sqrt{A}\rfloor - 1)^2 - A < 0.$

Nu volgt de inductiestap, waarin we aannemen dat
$k_i + 2r'_i + k'_{i+1} > 0$
$k_i - 2r'_i + k'_{i+1} < 0$.
Hieruit bewijzen we eerst dat:
$(r'_{i+1} - |k'_{i+1}|)^2 < A$.
$(r'_{i+1} + |k'_{i+1}|)^2 > A$.

Neem aan dat $k'_{i+1} < 0$. Dan $k_i k'_{i+1} + 2r'_i k'_{i+1} + k'^2_{i+1} < 0$, dus
$r'^2_{i+1} - A + 2r'_i k'_{i+1} + k'^2_{i+1} < 0$, en daarmee $(-r'_{i+1} - k'_{i+1})^2 < A$ waaruit volgt dat $(r'_{i+1} - |k'_{i+1}|)^2 < A$.

Als daarentegen $k'_{i+1} > 0$, dan geldt $k_i k'_{i+1} - 2r'_i k'_{i+1} + k'^2_{i+1} < 0$, dus
$r'^2_{i+1} - A - 2r'_i k'_{i+1} + k'^2_{i+1} < 0$ en daarmee $(-r'_{i+1} + |k'_{i+1}|)^2 < A$ waaruit volgt dat ook $(r'_{i+1} - |k'_{i+1}|)^2 < A$.

Aan de andere kant is uit de definitie van r'_{i+1} duidelijk dat $(r'_{i+1} + |k'_{i+1}|)^2 > A$.
We hebben dus aangetoond dat:
$(r'_{i+1} - |k'_{i+1}|)^2 < A$, en $(r'_{i+1} + |k'_{i+1}|)^2 > A$.

Uit $(r'_{i+1} - |k'_{i+1}|)^2 < A$ volgt dat $r'^2_{i+1} - 2r'_{i+1}|k'_{i+1}| + k'^2_{i+1} < A$. Via $k'_{i+2} = \frac{r'^2_{i+1} - A}{k'_{i+1}}$ komen we uit op $k'_{i+1}(k'_{i+2} - 2r'_{i+1} \cdot \frac{|k'_{i+1}|}{k'_{i+1}} + k'_{i+1}) < 0$.
Als k'_{i+1} negatief is levert dit $k'_{i+2} + 2r'_{i+1} + k'_{i+1} > 0$, en als k'_{i+1} positief is $k'_{i+2} - 2r'_{i+1} + k'_{i+1} < 0$.

[17] De bewijzen in dit hoofdstuk zijn mijn uitwerkingen van de opgaven achterin Hoofdstuk 1.9 van Edwards, *Fermat's Last Theorem*

Op analoge wijze volgt uit $(r'_{i+1}+|k'_{i+1}|)^2 > A$ dat $r'^2_{i+1}+2r'_{i+1}|k'_{i+1}|+k'^2_{i+1} > A$. Via $k'_{i+2} = \frac{r'^2_{i+1}-A}{k_{i+1}}$ krijgen we:
$k'_{i+1}(k'_{i+2} + 2r'_{i+1} \cdot \frac{|k'_{i+1}|}{k'_{i+1}} + k'_{i+1}) > 0$.
Als k'_{i+1} negatief is levert dit $k'_{i+2} - 2r'_{i+1} + k'_{i+1} < 0$, en als k'_{i+1} positief is $k'_{i+2} + 2r'_{i+1} + k'_{i+1} > 0$.

Hiermee is de inductiestap voltooid, en is Stelling 4.8 bewezen.

□

De r'_i die gevonden worden door de 'versimpelde' cirkelmethode zijn altijd kleiner dan of gelijk aan de r_i die gevonden worden met de 'traditionele' cirkelmethode. Het verschil tussen de twee methodes maakt alleen uit als de traditionele methode een r_i vindt die groter is dan $\sqrt{A}$. De versimpelde methode vindt dan $r'_i = r_i - |k_i|$. Merk op dat de twee antwoorden door de minimaliteitseis precies $|k_i|$ uit elkaar liggen.

We zullen hieronder bewijzen in Stellingen 4.9 en 4.10 dat de 'versimpelde' cirkelmethode alle tussenresultaten (x_i, y_i, k_i) van de 'oorspronkelijke' cirkelmethode ook behaalt, maar mogelijk met tussenstappen. Met andere woorden, de 'oorspronkelijke' cirkelmethode snijdt soms een stukje van de berekening van de 'versimpelde' af. We zullen in Stelling 4.11 bewijzen dat de resultaten die het 'oorspronkelijke' algoritme overslaat nooit oplossingen zijn.

Merk op dat we in de berekeningen hieronder ervan uitgaan dat het 'traditionele' algoritme de kleinst mogelijke oplossing kiest als er twee r_i zijn waarvoor $|r_i^2 - A|$ minimaal is. Uit Stelling 4.11 volgt dat als dat niet zo is het mogelijk is dat dit algoritme oplossingen overslaat.

Stelling 4.9. [18] *Wanneer $r_i \neq r'_i$, geldt dat $r'_{i+1} = -r'_i + |k'_{i+1}|$.*

Bewijs. We weten dat $k_i k'_{i+1} = r'^2_i - A$. We doen de gevallen waarin k_i positief is en die waarin k_i negatief is apart. In beide gevallen zullen we laten zien dat $0 < -r'_i + |k'_{i+1}| < \sqrt{A}$, maar $-r'_i + 2|k'_{i+1}| > \sqrt{A}$, zodat duidelijk is dat $r'_{i+1} = -r'_i + |k'_{i+1}|$.

Stel $k_i < 0$. Dan geldt dat $k'_{i+1} > 0$. Dit impliceert:

$$\begin{aligned}(-r'_i + k'_{i+1})^2 - A &= r'^2_i - 2r'_i k'_{i+1} + k'^2_{i+1} - A \\ &= k_i k'_{i+1} - 2r'_i k'_{i+1} + k'^2_{i+1} \\ &= k'_{i+1}(k_i - 2r'_i + k'_{i+1}).\end{aligned}$$

[18] In deze en de volgende stellingen wordt 'k_i' opzettelijk zonder accent geschreven. We beginnen namelijk op het eerste punt dat $r_i \neq r'_i$, zodat daarvoor alle resultaten hetzelfde zijn, ook $k_i = k'_i$.

Deze laatste term heeft het zelfde teken als $k_i - 2r'_i + k'_{i+1}$, omdat $k'_{i+1} > 0$. Er geldt $k_i - 2r'_i + k'_{i+1} = \frac{k_i^2 - 2r'_i k_i + r'^2_i - A}{k_i} = \frac{(r'_i - k_i)^2 - A}{k_i} = \frac{(r'_i + |k_i|)^2 - A}{k_i}$.
Deze term is negatief omdat $r_i \neq r'_i$ en $k_i < 0$, en dus is $(-r'_i + k'_{i+1})^2 - A$ negatief.

Anderzijds geldt dat $(-r'_i + 2k'_{i+1})^2 - A = r'^2_i - A - 4r'_i k'_{i+1} + 4k'^2_{i+1}$
$= k'_{i+1}(k_i - 4r'_i + 4k'_{i+1})$.
We zullen bewijzen dat $k'_{i+1}(k_i - 4r'_i + 4k'_{i+1})$ positief is door eerst te bewijzen dat $k_i - 2r'_i + 2k'_{i+1}$ positief is.

Er geldt: $k_i(k_i - 2r'_i + 2k'_{i+1}) = k_i^2 - 2r'_i k_i + 2r'^2_i - 2A = (r'_i + |k_i|)^2 - A + (r'^2_i - A))$.

Als het 'traditionele' algoritme een ander getal vindt dan de versimpelde, weten we dat $0 < r_i^2 - A = (r'_i + |k_i|)^2 - A < A - r'^2_i$. Er volgt dat $k_i - 2r'_i + 2k'_{i+1}$ positief is. Wegens $k_i < 0$ vinden we dat $k'_{i+1} > r'_i$.

De combinatie van $k_i - 2r'_i + 2k'_{i+1} > 0$ en $k'_{i+1} > r'_i$ levert dat $k_i - 4r'_i + 4k'_{i+1} > 0$, en omdat $k'_{i+1} > 0$ concluderen we dat $k'_{i+1}(k_i - 4r'_i + 4k'_{i+1}) > 0$. Dan volgt dat $(-r'_i + 2k'_{i+1})^2 - A > 0$. Omdat $(r'_i + k'_i)^2 - A < 0$, geldt $r'_{i+1} = -r'_i + |k'_{i+1}|$.

De redenering voor $k_i > 0$ gaat analoog. Als k_i negatief is, geldt

$$\begin{aligned}(-r'_i - k'_{i+1})^2 - A &= r'^2_i + 2r'_i k'_{i+1} + k'^2_{i+1} - A \\ &= k_i k'_{i+1} + 2r'_i k'_{i+1} + k'^2_{i+1} \\ &= k'_{i+1}(k_i + 2r'_i + k'_{i+1}).\end{aligned}$$

Deze laatste term heeft het tegengestelde teken van $k_i + 2r'_i + k'_{i+1}$, omdat $k'_{i+1} < 0$. Merk op dat $k_i + 2r'_i + k'_{i+1} = \frac{(r'_i + k_i)^2 - A}{k_i} = \frac{(r'_i + |k_i|)^2 - A}{k_i}$.
Deze term is positief omdat $r_i^2 > A$ en $k_i > 0$. We concluderen dat $(-r'_i - k'_{i+1})^2 - A$ negatief is.

Anderzijds geldt dat $(-r'_i - 2k'_{i+1})^2 - A = r'^2_i - A + 4r'_i k'_{i+1} + 4k'^2_{i+1}$
$= k'_{i+1}(k_i + 4r'_i + 4k'_{i+1})$. Het teken hiervan is te bepalen via:

$k_i(k_i + 4r'_i + 4k'_{i+1}) = k_i^2 + 4r'_i k_i + 4r'^2_i - 4A < 2k_i^2 + 4r'_i k_i + 2r'^2_i - 2A + 2(r'^2_i - A) =$
$2 \cdot ((r'_i + |k_i|)^2 - A + (r'^2_i - A))$.

Deze laatste term is negatief, waaruit blijkt dat $k'_{i+1}(k_i + 4r'_i + 4k'_{i+1})$ positief is. Dan volgt weer dat $(-r'_i - 2k'_{i+1})^2 - A > 0$, en dus dat $r'_{i+1} = -r'_i + |k'_{i+1}|$.

Dus $r'_{i+1} = -r'_i + |k'_{i+1}|$.

□

Stelling 4.10. *$k'_{i+2} = k_{i+1}$, $y'_{i+2} = y_{i+1}$ en $x'_{i+2} = x_{i+1}$.*

Bewijs.

$$\begin{aligned}
k'_{i+2} &= \tfrac{r'^2_{i+1}-A}{k'_{i+1}} \\
&= \tfrac{r'^2_i - A - 2r'_i|k'_{i+1}| + k'^2_{i+1}}{k'_{i+1}} \\
&= k_i - 2r'_i \cdot \tfrac{|k_{i+1}|}{k_{i+1}} + k'_{i+1} \\
&= k_i + 2r'_i \cdot \tfrac{|k_i|}{k_i} + k'_{i+1} \\
&= \tfrac{r'^2_i - A + k_i^2 + 2r'_i \cdot |k_i|}{k_i} \\
&= \tfrac{(r'_i + |k_i|)^2 - A}{k_i} \\
&= \tfrac{(r_i)^2 - A}{k_i} = k_{i+1}
\end{aligned}$$

$$\begin{aligned}
y'_{i+2} &= \tfrac{x'_{i+1} + r'_{i+1} y'_{i+1}}{|k'_{i+1|}} \\
&= \left(\tfrac{x_i r'_i + A y_i}{|k_i|} + \tfrac{(x_i + y_i r'_i)(-r'_i + |k'_{i+1}|)}{|k_i|}\right) \cdot \tfrac{|k_i|}{A - r'^2_i} \\
&= \tfrac{A y_i - y_i r'^2_i + x_i |k'_{i+1}| + y_i r'_i |k'_{i+1}|}{A - r'^2_i} \\
&= y_i + \tfrac{x_i + y_i r'_i}{|k_i|} \\
&= \tfrac{x_i + y_i r_i}{|k_i|} = y_{i+1}
\end{aligned}$$

Als k'_{i+2} en y'_{i+2} bekend zijn ligt x'_{i+2} vast, deze moet dus gelijk zijn aan x_{i+1}. □

Stelling 4.11. *Als $r_i \neq r'_i$, dan $k'_{i+1} \neq \pm 1$.*

Bewijs. Volgens Stelling 4.9 geldt $r'_{i+1} = -r'_i + |k'_{i+1}|$. Omdat $r'_i \geqslant 1$ en $r'_{i+1} \geqslant 1$ moet gelden dat $|k'_{i+1}| > 1$. □

Hieruit volgt dat geen van de stappen die we overslaan met de 'traditionele' methode oplossingen zijn. Als we er daarentegen niet van uitgaan dat het 'traditionele' algoritme de kleinst mogelijke oplossing kiest als er twee r_i zijn waarvoor $|r_i^2 - A|$ minimaal is, is het mogelijk dat dit wel gebeurt. Er geldt dan niet meer per definitie dat $r'_{i+1} = -r'_i + |k'_{i+1}|$, en het bewijs is niet meer geldig.

We weten nu dat we met het gebruiken van de versimpelde cirkelmethode hoogstens extra stappen doen: alle resultaten van de 'traditionele' cirkelmethode komen ook voor in de versimpelde. Bovendien is geen van de extra stappen een oplossing.

De versimpelde cirkelmethode wordt nu:

Initialisatie:

- $r_1 = \lfloor \sqrt{A} \rfloor$.

- $k_1 = 1$.

Iteratie:

- $s_i = r_i^2 - A$
- $k_{i+1} = \frac{s_i}{k_i}$.
- Kies r_{i+1} als het grootse getal dat voldoet aan:
  $0 < r_{i+1} < \sqrt{A}$, $|k_{i+1}|$ deelt $r_i + r_{i+1}$.

Ga door met itereren todat $k_i = 1$.

Met alle extra informatie die we nu hebben kunnen we vrij gemakkelijk bewijzen dat de cirkelmethode na verloop van tijd een oplossing zal vinden.

Stelling 4.12. *De cirkelmethode vindt een paar x, y zodat $x^2 - Ay^2 = 1$*

Bewijs. We kunnen vrij makkelijk aantonen dat $|k_i|$ begrensd is. Immers, $|k_i|$ deelt $r_{i-1} + r_i$. Omdat $0 < r_j < \sqrt{A}$ volgt dat $|k_i| < 2\sqrt{A}$.

Er zijn dus maar eindig veel verschillende k_i mogelijk. Omdat de cirkelmethode eindeloos herhaald kan worden is er dus minstens één k waarvoor oneindig veel paren (x_i, y_i) met $x_i^2 - Ay_i^2 = k$ voorkomen in de resultaten van de cirkelmethode.

We splitsen al deze oplossingen in k^2 equivalentieklassen volgens de equivalentierelatie $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 \equiv x_2 \bmod k$, $y_1 \equiv y_2 \bmod k$.

Er zijn oneindig veel oplossingen en maar eindig veel equivalentieklassen dus minstens één van de klassen bevat oneindig veel oplossingen. Kies twee oplossingen (x_1, y_1) en (x_2, y_2) uit dezelfde equivalentieklasse.

Uit $k|x_1^2 - Ay_1^2 \equiv x_1x_2 - Ay_1y_2 \bmod k$ volgt $k|x_1x_2 - Ay_1y_2$.
Uit $0 = x_1y_1 - x_1y_1 \equiv x_1y_2 - x_2y_1 \bmod k$ volgt $k|x_1y_2 - x_2y_1$.

Definieer $x := \frac{x_1x_2 - Ay_1y_2}{k}$ en $y := \frac{x_1y_2 - x_2y_1}{k}$. Nu geldt:
$x^2 - Ay^2 = \frac{(x_1x_2 - Ay_1y_2)^2}{k^2} - A\frac{(x_1y_2 - x_2y_1)^2}{k^2} = \frac{1}{k^2}(x_1^2 - Ay_1^2)(x_2^2 - Ay_2^2) = \frac{k^2}{k^2} = 1$.

Hieruit volgt direct dat $x^2 > 0$. Mocht het zo zijn dat x of y negatief is, dan vervangen we x door $-x$, respectievelijk y door $-y$. In het geval dat $y = 0$ volgt dat $x_1y_2 = x_2y_1$. Uit Resultaat 6.2 weten we dat x_n en y_n altijd copriem zijn, dus volgt dat $x_1|x_2$ én $x_2|x_1$, zodat $x_1 = x_2$, wat in tegenspraak is met onze aanname. Dus zijn x en y beide positieve gehele getallen. □

Merk op dat dit bewijs meteen aantoont dat er altijd een oplossing bestaat.

Zoals al is opgemerkt heeft Bhaskara nooit bewezen dat zijn methode correct is, en heeft hij zich ook nooit bezig gehouden met bepalen of er altijd een oplossing mogelijk is (hij toont nergens aan dat zijn methode ooit stopt). De zogenaamde 'versimpelde' cirkelmethode is een moderne constructie en komt nergens in de Indiase teksten voor; dit bewijs is dan ook geheel modern werk. Toch verdienen Brahmagupta en Bhaskara veel lof voor hun werk, dat ver vooruitliep op Europese resultaten. Deze prestaties zijn lange tijd onopgemerkt gebleven in het Westen. Het boek van Colebrooke is het eerste werk waarin de werken van Brahmagupta en Bhaskara aan bod komen, en dat stamt uit 1817.

Westerse wiskundigen zelf zijn pas geïnteresseerd geraakt in dit probleem toen Fermat in de zeventiende eeuw de getaltheorie opnieuw als tak van wiskunde op de kaart zette. Dit heeft er toe geleid dat de Engelse wiskundigen Wallis en Brouncker een methode ontwikkelen die verwant is aan de Indiase, zonder dat ze het werk van Brahmagupta of Bhaskara ooit gezien hebben.

Hoofdstuk 5

De methode van Wallis en Brouncker

5.1 Wallis, Brouncker en Fermat

De vergelijking die later de vergelijking van Pell zou gaan heten duikt in de Westerse wiskunde pas weer op in de zeventiende eeuw. Er was in die tijd geen sprake van een coherent gestructureerde wiskunde zoals we die nu kennen, of zelfs van een gemeenschappelijke definitie van wat wiskunde nu precies inhield. Wiskunde werd door heel verschillende mensen om heel verschillende redenen beoefend [1].

Wiskunde werd beoefend door geprivilegeerde mensen die het een interessante hobby vonden, handelaars en bankiers die moesten boekhouden en rentetarieven moesten kunnen berekenen, zogeheten 'rekenmeesters' die les gaven en te huur waren om problemen op te lossen, en astrologen en mystici, die probeerden door middel van ingewikkelde modellen het heelal en de mens te doorgronden.

Hoewel er in het Westen zeker was gewerkt aan wiskunde in gehele getallen, zoals de reeks van Fibonacci, het construeren van magische vierkanten, en het werk van de reeds genoemde getallenmystici, was er geen getaltheoretische wetenschappelijke traditie. Deze was er wel voor onderwerpen als klassiek Griekse meetkunde, het oplossen van tweede-, derde- en hogeregraads vergelijkingen, en wat wij tegenwoordig analyse noemen.

De Fransman Pierre de Fermat wordt vaak genoemd als grondlegger van onze

[1] Zie voor een uitgebreidere beschrijving hoofdstuk 1 van Mahoney, *Pierre de Fermat*

moderne getaltheorie. Fermat heeft bijdragen geleverd aan bijna alle takken van wiskunde, maar had een duidelijke passie voor wiskunde in gehele getallen. Hij heeft gecorrespondeerd met wiskundigen uit heel Europa, en moedigde hen aan getaltheoretische problemen te onderzoeken. Het is zijn correspondentie met de Engelse wiskundigen John Wallis en Lord William Brouncker die uiteindelijk leidt tot het eerste westerse algoritme om $x^2 - Ay^2 = 1$ op te lossen.

Pierre de Fermat *(1601-1665)* was een Frans rechtsgeleerde en wiskundige. Hoewel hij zijn hele leven lang gerechtlijk ambtenaar in dienst van de stad Toulouse was, herinneren we hem nu om zijn baanbrekende werk in de wiskunde, die hij als hobby bedreef. Fermat heeft bijdragen geleverd aan de analyse, kansrekening en analytische meetkunde.

Weinig bekend is dat Fermat de analytische meetkunde ongeveer tegelijk uitvond met Descartes, zonder ooit diens werk te hebben gelezen. Descartes publiceerde zijn werk echter meteen als bijlage bij zijn bijzonder invloedrijke *Discourse de la méthode*, terwijl Fermat om onduidelijke redenen zijn werk nooit gepubliceerd heeft. Fermat heeft in zijn hele leven eigenlijk nooit iets gepubliceerd, hoogstens heeft hij andere toegestaan brieven van hem op te nemen in hun werk (zoals John Wallis deed in zijn *Commercium epistolicum*).

Zoals hierboven al is gezegd was Fermat's grote liefde echter de getaltheorie. Hij heeft veel geproduceerd op dit gebied (hij heeft zelfs meer geproduceerd dan we kennen, maar een gedeelte van zijn werk is verloren gegaan na zijn dood)[2]. Om een idee te geven van deze productiviteit: tegenwoordig kennen we in de getaltheorie Fermat's kleine stelling, Fermats laatste stelling, Fermat getallen en Fermat pseudopriemen, en dit zijn alleen de dingen die daadwerkelijk naar hem vernoemd zijn.

Naast wiskundig werk uitte Fermat's interesse in getaltheorie zich ook in zijn pogingen veel van zijn tijdgenoten in dit vakgebied te interesseren via correspondentie en wiskundige uitdagingen. Zo kwam het dat Fermat op 3 januari 1657 een brief schreef aan de wiskundige Digby, waarin hij hem vroeg 'Wallis en andere Engelse wiskundigen' twee getaltheoretische problemen voor te leggen. Deze zelfde problemen werden voorgelegd aan de Franse wiskundige Frénicle de Bessy, en de brief meldde dat 'als de oplossing niet geleverd zou worden door Engeland, door Belgisch Frankrijk of door Keltisch Frankrijk (waar Frénicle de Bessy woonde), dat zij dan geleverd zou worden door de streek rondom Narbonne' (Fermat woonde in Toulouse, in de buurt van de destijds belangrijke havenstad Narbonne).[3] We zullen zien dat deze correspondentie de Engelse wiskundigen er toe brengt het eerste Westerse algoritme voor de oplossing van de vergelijking van Pell te geven.

[2] Zie voor een uitgebreide beschijving van wat er met Fermat's werk is gebeurd na zijn dood Mahoney, *Pierre de Fermat*, Appendix II.

[3] *Dictionary of Scientific Biography*

John Wallis *(1616-1703)* was één van de grootste wiskundigen uit zijn tijd. Hoewel hij zijn carrière begon als dominee, en nauwelijks wiskunde bedreven had tijdens zijn studie, raakte hij in het onderwerp geïnteresseerd bij het lezen van studiemateriaal van zijn jongere broer, die een opleiding tot handelaar volgde. Later kwam Walli in aanraking met de groep Engelse wetenschappers die de aanzet zou vormen tot de beroemde Royal Society (waar Wallis één van de oprichters van was), en kreeg hij de gelegenheid zich meer in wiskunde te verdiepen.

In 1649 werd Wallis benoemd tot professor in de meetkunde aan de universiteit van Oxford. Deze positie had hij niet zozeer te danken aan zijn wetenschappelijk werk tot dan toe (hij had nauwelijks gepubliceerd), maar aan het cryptografisch werk dat hij deed voor de toenmalige puriteinse regering in hun strijd tegen de royalisten. Eenmaal benoemd bleek Wallis echter een wiskundige van formaat.

Tegenwoordig worden de uitdrukking van $\frac{4}{\pi}$ als het oneindige product $\frac{3}{2} \cdot \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{5}{6} \cdot \frac{7}{6} \cdot \frac{7}{8} \cdot ...$, een uitgebreide behandeling van kegelsneden, en het generaliseren van machten van gehele (x^2) naar rationale getallen ($x^{\frac{2}{3}}$) als Wallis' belangrijkste wiskundige verdiensten gezien. In zijn eigen tijd werd hij gewaardeeerd om zijn *Arithmetica Infinitorum*, waarin hij werkte aan de theorie van limieten en uitbreidde op Descartes' wiskundig werk. Ook heeft hij gewerkt aan analyse, meetkunde en het berekenen van zwaartepunten en zwaartekracht.

Naast zijn wiskundig werk was Wallis actief in de linguisitiek en de theologie. Hij was een pioneer in het ontwikkelen van een manier om doven te leren spreken.

De correspondentie tussen Fermat en Wallis liep via Digby en Lord Brouncker, ook iemand met aanzienlijk wiskundig talent. Hoewel Wallis degene is die de uiteindelijke oplossing naar Fermat stuurt, schrijft hij haar toe aan Brouncker.

Lord William Brouncker II *(1620-1684)* was een Engels edelman en geleerde. Naast zijn werk voor de Engelse regering (hij was onder meer parlementslid, vlootcommandant en beheerder van de schatkist) was hij een van de oprichters van de Royal Society, en haar eerste president, van 1660 tot 1677. Hij was de eerste Engelse wiskundige die zich bezig hield met kettingbreuken, die in 1613 door Cataldi geïntroduceerd waren.[4] Hij heeft diverse ontdekkingen gedaan, waaronder een beschijving van $\frac{4}{\pi}$ als kettingbreuk, en werk aan $\int \frac{dx}{1+x}$, maar deze nooit zelf gepubliceerd; zijn wiskundig werk is alleen de vinden in de boeken van John Wallis.

Dit is een vaker voorkomend thema in Brouncker's wiskundig werk: het lijkt er op dat hij zich alleen met wiskunde bezighield als hem een probleem voorgelegd werd door een ander, en dat hij niet of nauwelijks uit eigen beweging onderzoek deed. Daar staat tegenover dat hij in correspondentie met anderen zeker resul-

[4] In diens *Trattato del modo brevissimo di trovar la radice quadra delli numeri (1613)*

taten in de wiskunde heeft geboekt. Brouncker had een levendige interesse in muziektheorie, en het enige werk dat hij zelf gepubliceerd heeft is een vertaling van Descartes' 'Musicae Compendium' naar het Engels, met aantekeningen die zo lang zijn als het werk zelf.

Door Fermat's uitdaging ontstond een levendige correspondentie (in totaal 44 brieven) tussen Fermat aan de ene en Wallis en Brouncker aan de andere kant[5]. Deze liep via Kenelm Digby, een katholieke Engelse wiskundige die het grootste deel van de tijd in Frankrijk verbleef, uit onvrede met de toenmalige protestantse regering. Hij stuurde brieven van Fermat en Frénicle de Bessy naar Thomas White, een (katholieke) priester en natuurfilosoof, die bevriend was met Brouncker (beiden woonden in Londen). Het lijkt er op dat White de brieven uit het Latijn en Frans naar het Engels heeft vertaald. Brouncker stuurde de vertaalde brieven, vaak vergezeld van eigen berekeningen, naar Wallis, die professor was aan de universiteit van Oxford. Antwoorden van Wallis gingen dan via Brouncker en Digby terug naar Fermat. Omdat Fermat geen Engels sprak liet hij de brieven vertalen door 'een jonge Engelsman, die hier woont en weinig van deze [wiskundige] zaken weet'.[6]

Het zal niet verwonderlijk zijn dat deze correspondentie enige tijd in beslag nam, en er zijn een paar gevallen waarin Digby of Fermat reageert op een geschrift dat inmiddels achterhaald is. Veel van de 44 brieven gaan over eerdere opgaven, ander wiskundig onderzoek van Wallis (die bijvoorbeeld claimt een kwadratuur van de cirkel te hebben gevonden), of betreffen slechts het uitwisselen van beleefdheden. We zullen hier alleen de brieven behandelen die relevant zijn voor de vergelijking van Pell. Citaten in dit stuk zijn mijn eigen vertalingen van Franstalige passages uit Fermats *Oeuvres*.

Op 3 januari 1657 stuurde Fermat zijn eerste uitdaging.[7] Deze omvat twee getaltheoretische opgaven, te weten:

- Vind een derdemacht zodat de som van deze derdemacht en zijn delers een kwadraat is.
- Vind een kwadraat zodat de som van dit kwadraat en zijn delers een derdemacht is.[8]

Deze uitdaging is nog maar nauwelijks bij Wallis aangekomen als Brouncker al een tweede brief ontvangt, waarin Fermat vertelt dat hij al een oplossing van

[5] De hele correspondentie is te vinden in *Oeuvres*, Fermats volledig werk, delen 2 en 3. Alle citaten in dit hoofdstuk komen uit dat boek, en zijn uit het Frans naar het Nederlands vertaald.

[6] uit een Brief van Fermat aan Digby, 6/7/1657. *Oeuvres*, deel 2, pg 341-342

[7] *Oeuvres* deel 2, pg 332-333 (Latijn),*Oevres* deel 3, pg 311-312 (Franse vertaling)

[8] Merk op dat met 'delers' *wel* 1, maar *niet* het getal zelf wordt bedoeld.

Frénicle de Bessy heeft gekregen, en waarin hij een nieuw probleem onder de aandacht van de Engelsen wil brengen. Nadat hij zich eerst heeft beklaagd dat niemand meer in problemen in gehele getallen geïnteresseerd is zegt hij dat nodig is deze tak van wiskunde te ontwikkelen of opnieuw uit te vinden, en dat hij Wallis en Brouncker daarom een nieuw theorema voor wil leggen:[9]

"Gegeven een willekeurig getal dat geen kwadraat is, zijn er oneindig veel kwadraten vastgelegd[10] *zodat als men de eenheid optelt bij het product van één van hen met het gegeven getal men weer een kwadraat heeft.*

Men geeft bijvoorbeeld 3, een getal dat geen kwadraat is.

- *3 x 1 + 1 = 4 (een kwadraat)*
- *3 x 16 + 1 = 49 (een kwadraat)*

In plaats van de kwadraten 1 en 16 kan men oneindig veel andere kwadraten vinden die voldoen aan de gestelde eis, maar ik vraag een algemene regel, die toepasbaar is op elk willekeurig niet-kwadraat dat maar gegeven kan worden.

Men vraagt bijvoorbeeld een kwadraat zodat men bij het optellen van de eenheid bij zijn product met 149, of met 109, of met 433 een kwadraat heeft".

Oftewel, dat wat later de vergelijking van Pell zal worden genoemd.

In zijn motivatie voor wiskunde in gehele getallen haalt Fermat Diophantus aan als voorbeeld van een groot Grieks getaltheoreticus. Dit is des te opvallender omdat Diophantus (zoals we al eerder zagen) de vergelijking van Pell alleen in breuken heeft behandeld, en ook in zijn andere werk meer bezig was met rationale dan met gehele getallen.

Het duurt even voordat Fermat's nieuwe uitdaging bij Wallis aankomt; hoewel de oorspronkelijke brief geschreven is in februari 1657 hoort Wallis er pas over in augustus van dat jaar, en krijgt hij hem pas in september. Brouncker stuurt hem Fermat's brief, met zijn eigen oplossing bijgevoegd.[11] Brounckers werk wordt ook naar Fermat gestuurd.

[9] *Oeuvres* deel 2, pg 334-335 (Latijn),*Oevres* deel 3, pg 312-313 (Franse vertaling)
[10] *'dantur'* in het Latijn, '*déterminés'* in het Frans
[11] *Oeuvres*, deel 3, pg 416-417

Brouncker's oplossing is echter in rationale getallen. Zoals we in de inleiding al hebben laten zien is het oplossen van de vergelijking van Pell in rationale getallen niet bijzonder moeilijk, en Fermat is dan ook niet tevreden. Er volgt een levendige discussie waarin Wallis en Brouncker Fermat ervan beschuldigen dat hij het door hen opgeloste probleem onder hun neus verandert, en waarin Fermat (en later Frénicle de Bessy) zeggen dat zelfs *a quodlibet de trivio arithmetico*[12], 'de willekeurige minste rekenaar', een oplossing in breuken had kunnen vinden, en dat het dus duidelijk zou moeten zijn dat een oplossing in gehele getallen gevraagd werd.

We kunnen de Engelsen op zijn minst verwijten dat ze de uitdaging niet goed hebben gelezen, omdat Fermat zijn 'tweede uitdaging' begint met een lofzang op de wiskunde in gehele getallen, en zijn voornemen noemt deze tak van wiskunde nieuw leven in te blazen. Omdat de door hen ingestuurde oplossing dan ook nog eens vrij weinig werk is, hadden Wallis en Brouncker volgens mij ook zelf kunnen bedenken dat Fermat misschien een moeilijker probleem bedoelde. Ook merkt Wallis bij zijn behandeling van het probleem op dat zijn oplossing ook zou werken in het geval n wel een kwadraat zou zijn; dit had ook een indicatie kunnen zijn dat hij het verkeerde probleem aan het oplossen was.

Interessanter is hoe voornamelijk Wallis probeert om de oude oplossing te repareren. Hij begint met een brief aan Digby, waarin hij zowel Brouncker's als zijn eigen methode nog eens uitlegt 'omdat het er op lijkt dat deze slecht voor meneer Fermat vertaald is'. Wallis beschrijft Brouncker's methode als volgt:[13][14]

Zij n een willekeurig gegeven getal (kwadraat of niet, geheel of een breuk); q een ander willekeurig kwadraat (geheel of een breuk) waarvan de wortel r is. Laat d ten slotte het verschil zijn tussen q en n, te weten hetzij $q - n$, hetzij $n - q$.

Het maakt niet uit welke van de twee definities voor d we gebruiken, want d komt alleen als kwadraat voor. Waarschijnlijk gaf Wallis beide definities om te laten zien dat het altijd mogelijk is om d positief te kiezen. Westerse wiskundigen in de zeventiende eeuw zagen negatieve getallen niet 'in de natuur' (bijvoorbeeld als een aantal appels), en concludeerden daarom dat negatieve getallen 'absurd' waren, en geen geldige getallen om wiskunde mee te doen.

De grote uitzondering hierop was de handelswiskunde die gebruikt werd door kooplieden en bankiers. Hier kon een negatieve hoeveelheid geld worden opgevat als een schuld of tekort. Dit verschil in aanpak is een goed voorbeeld van de

[12] *Oeuvres*, deel 2, pg 341-342

[13] *Oeuvres*, deel 3, pg 317-319

[14] Ik heb dezelfde variabelen gebruikt als Wallis zelf, behalve dat hij al zijn variabelen als hoofdletters schrijft. Daarentegen gebruikt hij 'Q' en 'q' door elkaar, de logica hierachter is niet duidelijk.

fragmentatie van de wiskunde gedurende deze periode.

Wallis vervolgt:

Regel: $\frac{4q}{d^2} = (\frac{2r}{d})^2$ *is een kwadraat, waarvan het product met* n*, verhoogd met de eenheid, een kwadraat geeft,* $n\frac{4q}{d^2} + 1 = \frac{4qn+d^2}{d^2}$.

Inderdaad:
$\frac{4qn+d^2}{d^2} = \frac{4qn+q^2-2qn+n^2}{q^2-2qn+n^2} = \frac{q^2+2qn+n^2}{q^2-2qn+n^2} = (\frac{q+n}{q-n})^2$.

Daarna geeft hij zijn eigen vergelijking:

De tweede regel, die van mij afkomstig is, is een beetje algemener dan de vorige, maar komt op hetzelfde neer met betrekking tot het vinden van oplossingen. Zij n *een willekeurig gegeven getal;* a *een willekeurig gekozen getal;* q *een willekeurig kwadraat en* m *diens quotiënt door* a*; en ten slotte* d *het verschil (in absolute waarde)*[15] *tussen* $\frac{ma}{4p}$ *en* pn.

Regel: $\frac{ma}{d^2}$ *is een kwadraat waarvan het product met* n*, verhoogd met de eenheid, een kwadraat geeft,* $n\frac{ma}{d^2} + 1 = \frac{man+d^2}{d^2}$.

Inderdaad:
$\frac{man+d^2}{d^2} = \frac{\frac{m^2a^2}{16p^2}+\frac{1}{2}man+p^2n^2}{\frac{m^2a^2}{16p^2}-\frac{1}{2}man+p^2n^2} = (\frac{\frac{ma}{4p}+pn}{\frac{ma}{4p}-pn})^2$.

Iets later krijgt Wallis een brief terug van Brouncker,[16] waarin deze schrijft dat hij een nieuwe brief van Fermat heeft gehad waarin Fermat duidelijk maakt dat hij zijn eerdere problemen opgelost wil zien in gehele getallen. Brouncker merkt op dat dit 'Iets' is 'dat hij eerder niet had geëist'. We mogen ons dus afvragen of Wallis en Brouncker de introductie van Fermats tweede probleem wel goed hebben gelezen, want die doelt vrij duidelijk op een oplossing in gehele getallen.

In eerste instantie gooit Wallis ook dit op een slechte vertaling en probeert hij de vraag op de makkelijke manier op te lossen:[17]

Wat er ook geschreven is zal slecht vertaald zijn voor Fermat, zo-

[15] Merk op dat Wallis hier de term 'differentia duorum' gebruikt, die het best te vertalen is met 'absolute waarde'. Kennelijk was Wallis bekend met dit concept, ondanks dat hij dit niet heeft gebruikt in zijn vorige definite van d hierboven.

[16] *Oeuvres*, deel 3, pg 419-420

[17] *Oeuvres*, deel 3, pg 427-428

als u gezegd heeft, het zijn geschriften die ik nooit gezien heb en waarover ik geenszins kan oordelen. Mijn oplossingen zijn zodanig, volgens mij, dat zij zeer precies voldoen aan de eisen. Ik voelde mij dus verplicht me er meteen mee bezig te houden, nadat ik ze naar het Latijn had vertaald, zodat een verkeerde interpretatie niemand meer zal verwarren.

Wallis beschrijft vervolgens Brounckers oplossingen voor Fermat's eerste uitdaging, en herhaalt beide methoden om de vergelijking van Pell in breuken op te lossen. Na een lange tirade waarin hij Fermat beschuldigt van onredelijkheid en volhoudt dat er geen enkele manier was dat hij kon weten dat hij geacht werd het probleem in gehele getallen op te lossen, vervolgt hij met de mededeling dat het allemaal niet zo veel uitmaakt, omdat zijn methode ook oneindig veel gehele oplossingen kan vinden:[18]

Laten we f^2 *kiezen als een kwadraat met de gewenste eigenschap, we hebben dan dat* $nf^2 + 1 = l^2$.

Laat ons nu $r = \frac{l \mp 1}{f}$ *nemen, ik zeg dat* f^2 *[gelijk aan]* $\frac{4q}{d^2}$ *zal zijn, hetgeen de regel hieronder geeft. We hebben inderdaad:* $q = r^2 = \frac{l^2 \mp 2l + 1}{f^2}$. *Maar* $nf^2 + 1 = l^2$. *Dus* $l^2 - 1 = nf^2$ *en* $n = \frac{l^2 - 1}{f^2}$.

Als gevolg daarvan: $d = |q - n| = |\frac{l^2 \mp 2l + 1}{f^2} - \frac{l^2 - 1}{f^2}| = \frac{2l \mp 1}{f^2}$.

En vervolgens, omdat $2r = \frac{2l \mp 1}{f}$, $2r = \frac{2l \mp 1}{f} : 2r = \frac{2l \mp 1}{f^2} = f = \frac{2r}{d}$ *oftewel* $f^2 = \frac{4q}{d^2}$.

(...)

Het moet nu ook zo zijn dat $\frac{4q}{d^2} = f$ *geheel is, en ik moet oneindig veel van dergelijke kwadraten leveren. Om dit te bereiken kan men uit de oneindige oplossingen die de regel geeft er willekeurig een kiezen die voldoet aan de gestelde eis, en die men ook op een andere manier kan vinden; dankzij dit ene kwadraat kan men oneindig veel andere leveren, als volgt:*

[18] *Oeuvres*, deel 3, pg 433-435

Zij f bijvoorbeeld dit kwadraat; dan geldt $f^2 + 1 = l^2$. Dan zal $2dl$ de wortel zijn van een ander kwadraat dat voldoet aan de voorgestelde, etcetera, tot in het oneindige.

Wat Wallis hier schrijft is geen antwoord op de vraag; hij heeft niet eens laten zien dat er überhaupt een oplossing in gehele getallen bestaat, noch dat zijn manier om de vergelijking in breuken op te lossen er één vindt. Hij ontwijkt de vraag gewoon door te stellen dat er vast wel één zal; zijn, en die hypothetische oplossing gebruikt hij om er oneindig veel meer te maken.

Wallis gaat niet verder in op zijn meest interessante bewering, namelijk dat als $nf^2 + 1 = l^2$, dat dan $2fl$ de wortel is van een nieuwe oplossing. Dit blijkt te kloppen:

Stel $l^2 - nf^2 = 1$, dan ook
$l^4 + 2nf^2l^2 + n^2f^2 = 4nf^2l^2 + 1$, en dus geldt dat
$(l^2 + nf^2)^2 = n(2fl)^2 + 1$.

Omdat we f en l positief kiezen, en beiden $\geqslant 1$ zijn volgt dat $2fl > f$.

Het was dus duidelijk voor de Engelsen dat ze maar één oplossing hoefden te berekenen; het is immers mogelijk daaruit oneindig veel andere te maken.

De 'andere methode' die Wallis noemt wordt in die brief niet meer genoemd, wel stuurt hij hem later ter verduidelijking aan Brouncker.[19] Deze methode komt op niets anders neer dan één voor één alle mogelijkheden afgaan, gekoppeld aan een tabel om alles bij te houden. Hij gebruikt 7 als voorbeeld:

- $7 \cdot 1^2 = 7 = 3^2 - 2$
- $7 \cdot 2^2 = 28 = 6^2 - 8$
- $7 \cdot 3^2 = 63 = 9^2 - 18 = 8^2 - 1$
- $7 \cdot 4^2 = 112 = 12^2 - 32 = 11^2 - 9$
- ...
- $7 \cdot n^2 = (3 \cdot n)^2 - 2 \cdot n^2$, en vervolgens kun je net zo lang 1 van de voorste kwadraatterm af halen tot er $l^2 - m$ staat, met $m < 2l$.

Je vindt nu een oplossing zodra $m = 1$ (in dit geval dus al in de derde regel). Iedere kolom van deze methode betaat uit veelvouden van kwadraten; omdat de verschillen tussen kwadraten relatief makkelijk te berekenen zijn, is dit een

[19] *Oeuvres*, deel 3, pg 457-480

vereenvoudiging van het rekenwerk. Wiskundig gezien blijft het echter gewoon uitproberen.

Pas na een uitgebreide analyse van deze methode meldt Wallis in een postscriptum:

Ik had al het andere al geschreven toen het idee me inviel om uw methode om het eerste kwadraat te vinden toe te voegen, in een vorm geheel verschillend van die hierboven. Zij bijvoorbeeld voorgesteld het niet-kwadraat 13*, en laat* a^2 *het gezochte kwadraat zijn zodat* $13a^2 + 1$ *een kwadraat is.*[20] *Dan hebben we:*

$$13a^2 + 1 = 9a^2 + 6ab + b^2, \textit{ oftewel}$$
$$4a^2 + 1 = 6ab + b^2; \textit{ en daarom}$$
$$2b > a > b, \textit{ dus } a = b + c \textit{ en vervolgens:}$$

$$4b^2 + 8bc + 4c^2 + 1 = 6b^2 + 6bc + b^2, \textit{ oftewel}$$
$$2bc + 4c^2 + 1 = 3b^2;$$
$$2c > b > c$$

$$b = c + d:$$

$$2c^2 + 2cd + 4c^2 + 1 = 3c^2 + 6cd + 3d^2$$
$$3c^2 + 1 = 4cd + 3d^2;$$
$$2d > c > d$$

$$c = d + e:$$

$$3d^2 + 6de + 3e^2 + 1 = 4d^2 + 4de + 3d^2$$
$$2de + 3e^2 + 1 = 4d^2;$$
$$2e > d > e$$

$$d = e + f:$$

$$2e^2 + 2ef + 3e^2 + 1 = 4e^2 + 8ef + 4f^2$$

[20] Wallis stelt dit kwadraat hier gelijk aan $3a + b$. We zullen later uitgebreid uitleggen waar deze en de volgende afschattingen op gebaseerd zijn. Voorlopig is het voldoende op te merken dat $(3a)^2 < 13a^2 + 1 < (4a)^2$.

$$e^2 + 1 = 6ef + 4f^2;$$
$$7f > e > 6f$$

$$e = 6f + g:$$

$$36f^2 + 12fg + g^2 + 1 = 36f^2 + 6fg + hf$$
$$6fg + g^2 + 1 = 4f^2;$$
$$2g > f > g$$

$$f = g + h:$$

$$6g^2 + 6gh + g^2 + 1 = 4g^2 + 8gh + 4h^2$$
$$3g^2 + 1 = 2gh + 4h^2;$$
$$2h > g > h$$

$$g = h + i:$$

$$3h^2 + 6hi + 3i^2 + 1 = 2h^2 + 2hi + 4h^2$$
$$4hi + 3i^2 + 1 = 3h^2$$

$$2i = h, i = 1.$$

Als gevolg daarvan: $i = 1, h = 2, g = 3, f = 5, 3e = 33, d = 38, c = 71, b = 109, a = 180.$
Men kan dit zelfde uitvoeren voor ieder niet-kwadratisch getal.

Dit algoritme, dat later bekend zal worden als 'de methode van Wallis en Brouncker', werkt. Hoewel Wallis niet bewijst dat het altijd werkt en/of stopt, is dit een manier om voor iedere A een oplossing te vinden. Merk overigens op dat Wallis nergens bewijst of er voor iedere A überhaupt een oplossing bestaat.

Hoe Wallis aan zijn afschattingen komt legt hij verder niet uit, maar ze zijn vrij makkelijk met de hand te controleren. We zullen in hoofdstuk 5.2 uitleggen hoe de methode precies werkt, en waarom er altijd een geldig antwoord uitkomt.

Merk op dat Wallis hier 'uw methode' schrijft, hoewel er geen enkele aanwijzing is dat Brouncker er de bedenker van is. Een brief waarin Brouncker dit idee uitlegt aan Wallis, of zelfs maar een aanwijzing tot het bestaan van zo'n brief, is nooit gevonden. Wanneer Wallis later de briefwisseling publiceert schrijft hij de methode weer toe aan Brouncker. Het is niet helemaal duidelijk waarom

hij dit doet; gespeculeerd wordt dat Wallis probeerde in de gunst te komen bij Brouncker, die een adelijke titel had en meer prestige genoot dan Wallis zelf.

Aan het begin van 1658 stuurt Wallis deze methode opnieuw naar Brouncker, maar dan netter uitgewerkt en voorzien van commentaar.[21] Brouncker stuurt de brief via Digby door naar Fermat. Fermat verklaart in een brief aan Digby vervolgens dat dit algoritme aan zijn eisen voldoet, en schrijft zelfs:[22]

Dat de zeer vermaarde heren Graaf Brouncker en John Wallis eindelijk legitieme oplossingen voor mijn opgaven hebben gegeven zal ik grif toegeven; sterker nog, ik ben er bijzonder blij mee. Echter, uw eminente correspondentiegenoten hebben niet willen toegeven dat deze vragen hen ook maar een enkel moment in de verlegenheid gebracht hebben. Ik had liever gehad had dat zij van te voren wilden toegeven dat deze onderwerpen in Engeland het bestuderen waard zijn; hun triomf zou nog groter zijn geweest naarmate de strijd moeilijker was.[23]

Hieruit blijkt weer Fermat's motivatie voor het insturen van zijn opgaven: zijn doel is om getaltheorie erkend te zien als een serieuze tak van wiskunde.

Later verandert Fermat van mening: hij merkt in een brief aan Huygens op dat Wallis en Brouncker 'er niet in waren geslaagd een algemeen bewijs te geven'.[24] Fermat was van mening dat een goed bewijs alleen te leveren was met wat hij 'oneindige afdaling' noemt. Dit is een techniek die Fermat een aantal keer aanhaalt. De precieze details zijn niet bekend, omdat zo weinig van Fermat's werk bewaard is gebleven, maar het is te reconstrueren tot een vorm van volledige inductie. Om precies te zijn: de variant waar, gegeven een oplossing voor een probleem, een kleinere oplossing wordt geconstrueerd. Dit kan worden gebruikt om aan te tonen dat er geen kleinste oplossing bestaat, hetgeen voor een probleem in positieve gehele getallen impliceert dat er geen oplossing bestaat.

Hoewel Fermat er in zijn 'tweede uitdaging' melding van maakt dat hij de opgaven zelf op kan lossen is zijn eigen algoritme nooit gepubliceerd, of zelfs maar teruggevonden. We weten zelfs niet zeker of hij de oplossingen van zijn eigen opgaven $A = 109$ en $A = 433$ ooit heeft opgeschreven. Echter, deze twee voorbeelden zijn bijzonder moeilijk. De kleinste oplossing voor $A = 109$ is bijvoorbeeld $y = 15140424455100$, terwijl voor $A = 433$ de kleinste oplossing 19

[21] *Oeuvres*, deel 3, pg 490-503

[22] *Oeuvres*, deel 2, pg 402 (Latijn), deel 3, pg 314 (Franse vertaling)

[23] De volgorde van de woorden in de laatste zin is veranderd en enkele woorden zijn toegevoegd ten bate van een leesbare vertaling.

[24] *Oeuvres*, deel 2, pg 433

cijfers heeft. Omdat voor deze waarden van A de kleinste oplossingen bijzonder groot zijn is het waarschijnlijk dat Fermat een werkende methode had om de vergelijking van Pell op te lossen, en dat hij met opzet twee moeilijke voorbeelden heeft opgegeven.

Helaas heeft Fermat zijn werkelijke doel nooit bereikt; na zijn dood werd er nauwelijks onderzoek gedaan naar getaltheorie, todat Euler in de achtiende eeuw geïnteresseerd raakte in het onderwerp. Euler is een belangrijk figuur in de geschiedenis van de vergelijking van Pell; we zullen zijn rol bespreken in het volgende hoofdstuk.

5.2 De methode zelf

Net als de Indiërs ontwikkelden de Engelsen een iteratieve methode, die net zo lang door gaat tot een antwoord gevonden is. In plaats van telkens de vergelijking om te schrijven door vermenigvuldiging drukken Wallis en Brouncker de variabelen van iedere vergelijking steeds in elkaar uit, om op die manier op een nieuwe vergelijking te komen.

Kies als voorbeeld weer $A = 55$, dan zoeken we een oplossing voor $x^2 - 55y^2 = 1$. Stel dat we zo'n oplossing (x, y) hebben, dan weten we dat $x = \sqrt{55y^2 + 1}$. Hiermee kunnen we afschatten dat als (x, y) een geheeltallige oplossing is, dat dan $\lfloor\sqrt{55}\rfloor y < x < \lceil\sqrt{55}\rceil y$. Omdat $\lfloor\sqrt{55}\rfloor = 7$ kunnen we x schrijven als $7y+z$, met $0 < z < y$ geheeltallig.

Door nu $7y + z$ in te vullen voor x krijgen we een nieuwe vergelijking in y en z, die lijkt op de vorige:

$(7y + z)^2 - 55y^2 = 1$
$49y^2 + 14yz + z^2 - 55y^2 = 1$
$-6y^2 + 14yz + z^2 = 1$

Met behulp van deze vergelijking is het mogelijk y af te schatten in termen van z, net zoals we eerder x hebben afgeschat in termen van y. Wallis zelf doet in zijn brief naar Fermat deze afschattingen ieder voor zich, maar Euler (die een hoofdstuk van zijn *Algebra* aan de vergelijking van Pell heeft gewijd) laat zien dat dit ook kan met de a, b, c - of Wortelformule, die gebruikt wordt om tweedegraadsvergelijkingen op te lossen.

Los op: $-6y^2 + 14yz + z^2 = 0$ *(Let op! We hebben de 1 aan de rechterkant hier weggelaten, we zullen later uitleggen waarom dit mag.)*
Uit $6y^2 - 14yz - z^2 = 0$ volgt $y_{1,2} = \frac{7z \pm \sqrt{55z^2}}{6}$.

We hebben al opgemerkt dat $\sqrt{55} > 7$. Dus hebben we een positieve en een negatieve y. Omdat we alleen geïnteresseerd zijn in *positieve* gehele getallen mogen we de oplossing met de negatieve wortel weglaten, zodat we uitkomen op $y = \frac{7z+\sqrt{55z^2}}{6}$.

Nu kunnen we y afschatten in termen van z. We weten dat $7 < \sqrt{55} < 8$, dus $\frac{14z}{6} < y < \frac{15z}{6}$. Schrijf nu $y = 2z + a$, met $0 \leqslant a < 1$. Dit kunnen we invullen in onze vergelijking:

$-6(2z + a)^2 + 14(2z + a)z + z^2 = 1$, wat we kunnen uitwerken tot
$5z^2 - 10za - 6a^2 = 1$

We hebben nu weer een vergelijking van hetzelfde type als eerst, en dus kunnen we de wortelformule weer toepassen. Merk op dat deze vergelijking ook weer een positief en een negatief nulpunt heeft, en dat we het negatieve weer weg kunnen laten:

Uit $5z^2 - 10za - 6a^2 = 0$ volgt $z = \frac{5a+\sqrt{55a^2}}{5}$
Dus $z = 2a + b$, met $0 \leqslant b < 1$. Invullen levert:
$5(2a + b)^2 - 10(2a + b)a - 6a^2 = 1$, wat we kunnen uitwerken tot
$-6a^2 + 10ab + 5b^2 = 1$

Itereer:

Uit $6a^2 - 10ab - 5b^2 = 0$ volgt $a = \frac{5b+\sqrt{55b^2}}{6}$
Dus $a = 2b + c$, met $0 \leqslant c < 1$. Invullen levert:
$-6(2b + c)^2 + 10(2b + c)b + 5b^2 = 1$, wat we kunnen uitwerken tot
$b^2 - 14bc - 6c^2 = 1$

En die laatste vergelijking kunnen we bijzonder makkelijk oplossen door de triviale oplossing $b = 1$, $c = 0$ te kiezen.

Gegeven dat je b en c weet, kan je achtereenvolgens berekenen dat $a = 2$, $z = 5$, $y = 12$ en $x = 89$. Dit is dezelfde uitkomst als die van het Indiase algoritme.

De methode van Wallis en Brouncker komt er dus op neer dat je de vergelijking om blijft schrijven door steeds de ene variabele in de andere uit te drukken, tot je op een vergelijking uitkomt die je kunt oplossen met de triviale oplossing (1,0). Daarna kun je door terugrekenen een (niet triviale) oplossing vinden voor je oorspronkelijke probleem.

Om zeker te weten dat de methode altijd uitvoerbaar is, en altijd een oplossing van de vergelijking van Pell levert, moeten we nog wel het een en ander bewijzen. Daarvoor zal het nuttig blijken om ook deze methode op te schrijven als een

iteratief proces.

5.3 Wiskundige onderbouwing van de methode van Wallis en Brouncker

In dit hoofdstuk zal ik de methode van Wallis en Brouncker verder analyseren, en bewijzen dat áls er een antwoord is, dit altijd gevonden wordt. Ik doe dat grotendeels met moderne notatie en concepten, zoals het schrijven van indices bij variabelen (bijvoorbeeld a_2), en bewijs door volledige inductie. Het is belangrijk te beseffen dat dit historisch gezien totaal niet accuraat is: driehonderd jaar geleden beschikten wiskundigen niet over onze notatie en niveau van abstractie, en ze hadden in het algemeen minder precieze ideeën over wat een bewijs is [25].

Het werk in deze en de hieropvolgende secties is schatplichtig aan Edwards' *Fermat's Last Theorem* en vooral aan Weil's *Number Theory*, waaruit ik het begrip 'gereduceerd tripel' heb overgenomen. Weil is echter bijzonder beknopt en Edwards gebruikt in zijn notatie geen indices, zodat alle notatie en een aantal van de stellingen en bewijzen van mijzelf afkomstig zijn.

Net als de cirkelmethode werkt de methode van Wallis en Brouncker iteratief: we beginnen met een vergelijking in een bepaalde 'standaard-vorm', en schrijven deze om tot een nieuwe vergelijking in die vorm. We herhalen dit proces tot we een vergelijking krijgen die we makkelijk op kunnen lossen (door de triviale oplossing $(1, 0)$ in te vullen), en daarna rekenen we terug om een niet-triviale oplossing te vinden voor de oorspronkelijke vergelijking.

De basis van deze methode ligt in de observatie dat als x_0 en x_1 positief zijn en $x_0^2 - Ax_1^2 = 1$, x_0 groter moet zijn dan x_1. Dan is het mogelijk om x_0 te schrijven als $t_1x_1 + x_2$ (met t_1 positief en geheel), en $0 < x_2 < x_1$. Door nu $t_1x_1 + x_2$ voor x_0 in te vullen in de oorspronkelijk vergelijking ontstaat een nieuwe vergelijking van vergelijkbare vorm, in x_1 en x_2. Omdat we al hebben bepaald dat $x_2 < x_1$ kunnen we x_1 schrijven als $t_2x_2 + x_3$. We zullen verderop aantonen dat het mogelijk is deze substitutie te herhalen totdat we een oplossing voor de vergelijking van Pell hebben gevonden.

Alle vergelijking die we gebruiken zijn te schrijven als
$B_ix_i^2 - 2C_ix_ix_{i+1} - D_ix_{i+1}^2 = (-1)^i$. De beginvergelijking $x_0^2 - Ax_1^2 = 1$ bijvoorbeeld, wordt $1 \cdot x_0^2 - 2 \cdot 0 \cdot x_0x_1 - Ax_1^2 = (-1)^0$.

We zullen aantonen dat na een substitutie $x_i \to (t_{i+1}x_{i+1} + x_{i+2})$ in $B_ix_i^2 -$

[25] Vergelijk Wallis' eerste poging om de vergelijking van Pell op te lossen in gehele getallen op bladzijde 57.

$2C_i x_i x_{i+1} - D_i x_{i+1}^2 = (-1)^i$ de nieuwe vergelijking te schrijven is als $B_{i+1}x_{i+1}^2 - 2C_{i+1}x_{i+1}x_{i+2} - D_{i+1}x_{i+2}^2 = (-1)^{i+1}$. In deze vergelijking kunnen we uiteraard weer x_{i+1} uitdrukken in x_{i+2} en een nieuw te introduceren x_{i+3}, zodat de substitutieprocedure door kan gaan.

We zullen echter ook aantonen dat er na verloop van tijd altijd een vergelijking onstaat van het type $x_n^2 - 2C_n x_n x_{n+1} - D_n x_{n+1}^2 = 1$. Deze vergelijking kunnen we oplossen met de triviale oplossing $x_n = 1, x_{n+1} = 0$. Gegeven dat we x_n en x_{n+1} weten kunnen we x_{n-1} berekenen, die immers gelijk is aan $t_n x_n + x_{n+1}$. Vervolgens kunnen we op dezelfde manier x_{n-2} berekenen, en zo terugrekenen tot x_1 en x_0. Omdat alle $t_i \geqslant 1$ is $x_1 > 0$, en is de gevonden oplossing voor $x_0^2 - Ax_1^2 = 1$ niet de triviale oplossing.

Let's get started. Wat gebeurt er als we beginnen met $B_i x_i^2 - 2C_i x_i x_{i+1} - D_i x_{i+1}^2 = (-1)^i$, en daarin $x_i = (t_{i+1}x_{i+1} + x_{i+2})$ substitueren?

Uit $B_i x_i^2 - 2C_i x_i x_{i+1} - D_i x_{i+1}^2 = B_i(t_{i+1}x_{i+1} + x_{i+2})^2 - 2C_i(t_{i+1}x_{i+1} + x_{i+2})x_{i+1} - D_i x_{i+1}^2 = (-1)^i$ volgt dat
$(-B_i t_{i+1}^2 + 2C_i t_{i+1} + D_i)x_{i+1}^2 - 2(B_i t_{i+1} - C_i)x_{i+1}x_{i+2} - (B_i)x_{i+2}^2 = (-1)^{i+1}$.

Oftewel, we hebben een vergelijking van de gevraagde standaardvorm, met:

- $B_{i+1} = -(B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i)$
- $C_{i+1} = B_i t_{i+1} - C_i$
- $D_{i+1} = B_i$

Het enige wat we nu nog moeten doen is het vastleggen van t_{i+1}. Daarvoor hebben we een hulpstelling nodig:

Stelling 5.1. *$C_i^2 + B_i D_i = A$ voor alle i.*

Bewijs. Voor $i = 0$ geldt: $0^2 + 1 \cdot A = A$. Stel nu dat $C_n^2 + B_n D_n = A$. Dan volgt dat $C_{n+1}^2 + B_{n+1}D_{n+1} = B_n^2 t_{n+1}^2 - 2B_n C_n t_{n+1} + C_n^2 - B_n^2 t_{n+1}^2 + 2B_n C_n t_{n+1} + B_n D_n = C_n^2 + B_n D_n = A$. □

Opmerking 5.1. *Dit impliceert dat $C_i = \sqrt{A - B_i D_i}$ voor alle i.*

Hoe bepalen we nu de t_{i+1}? We moeten uit de vergelijking $B_i x_i^2 - 2C_i x_i x_{i+1} - D_i x_{i+1}^2 = (-1)^i$ iets concluderen over de verhouding tussen x_i en x_{i+1}. We doen dit door de vergelijking op te vatten als een kwadratische vergelijking in x_i, en de a, b, c - of Wortelformule toe te passen.

We hebben $B_i x_i^2 - 2C_i x_i x_{i+1} - D_i x_{i+1}^2 = (-1)^i$. Als functie van x_i is dit: $B_i x_i^2 - (2C_i x_{i+1})x_i - (D_i x_{i+1}^2 + (-1)^i) = 0$. De Wortelformule levert nu $x_i = \frac{C_i x_{i+1} \pm \sqrt{A x_{i+1}^2 + (-1)^i}}{B_i}$ als nulpunten.

Uit de opmerking onder Stelling 5.1 volgt dat $\sqrt{A x_{i+1}^2 + (-1)^i}$ groter is dan $C_i x_{i+1}$. De vergelijking heeft dan ook een positief en een negatief nulpunt. We zijn alleen in het positieve nulpunt geïnteresseerd; we zoeken immers een verhouding tussen twee positieve variabelen. We concluderen dat

$$x_i = \frac{C_i x_{i+1} + \sqrt{A x_{i+1}^2 + (-1)^i}}{B_i} = x_{i+1} \cdot \frac{(C_i + \sqrt{A + \frac{(-1)^i}{x_{i+1}^2}})}{B_i}.$$

Het blijkt dat de wortel in deze uitdrukking een heel eind vereenvoudigd kan worden:

Stelling 5.2. *We mogen bij de berekening van t_i gebruikt maken van $\sqrt{A}$ in plaats van $\sqrt{A + \frac{(-1)^i}{x_{i+1}^2}}$.*

Bewijs. We weten dat de term $\frac{(-1)^i}{x_{i+1}^2} \leqslant 1$, omdat alle x_i die gebruikt worden groter dan of gelijk aan 1 zijn. De enige uitzondering hierop is de x_{n+1} die op 0 wordt gezet in de triviale oplossing aan het eind van het algoritme, maar deze komt nooit voor in een wortel. We hoeven dus alleen te bewijzen dat er óf geen verschil is tussen $\lfloor\sqrt{A}\rfloor$ en $\lfloor\sqrt{A \pm 1}\rfloor$, óf dat dit verschil niet uitmaakt voor de berekening.

We weten dat A geen kwadraat is, dus $\lfloor\sqrt{A}\rfloor = \lfloor\sqrt{A-1}\rfloor$. Daarnaast geldt dat als $x_{i+1} > 1$, dan $\lfloor\sqrt{A}\rfloor = \lfloor\sqrt{A + \frac{1}{x_{i+1}^2}}\rfloor$. De enige situatie die overblijft is wanneer $x_{i+1} = 1$, i even is, en er een geheeltallige n bestaat zodat $A = n^2 - 1$. Dan volgt dat $\lfloor\sqrt{A + \frac{1}{x_{i+1}^2}}\rfloor = \lfloor\sqrt{A}\rfloor + 1$.

In dit geval leidt het weglaten van de +1 echter één iteratie later ook tot een goede oplossing:

- $x_0^2 - (n^2-1)x_1^2 = 1$. Kies de 'foute' $t_1 : t_1 = \lfloor\frac{0+\sqrt{A}}{1}\rfloor = n-1$. Dan volgt $D_1 = 1, C_1 = n-1, B_1 = n^2 - 1 - (n-1)^2 = 2(n-1)$. Dit leidt tot de nieuwe vergelijking:
- $2(n-1)x_1^2 - 2(n-1)x_1x_2 - x_2^2 = -1$. Het berekenen van t_2 (wederom op de 'foute' manier) geeft $t_2 = \lfloor\frac{n-1+\sqrt{A}}{2(n-1)}\rfloor = 1$, en daarmee vinden we $B_2 = 1, C_2 = n-1, D_2 = 2(n-1)$. Dit geeft een vergelijking die triviaal oplosbaar is met $x_2 = 1, x_3 = 0$, waaruit volgt dat $x_1 = 1, x_0 = n$.

In het enige geval waar de +1 uit zou kunnen maken geeft de methode dus nog steeds een oplossing. We kunnen in het vervolg dus veilig $t_{i+1} = \lfloor \frac{C+\sqrt{A}}{B} \rfloor$ stellen.

□

Nu is ons iteratief systeem compleet. Samenvattend: We werken met vergelijkingen van het type $B_i x_i^2 - 2C_i x_i x_{i+1} - D_i x_{i+1}^2 = (-1)^i$. Als startwaarden kiezen we:

- $B_0 = 1$
- $C_0 = 0$
- $D_0 = A$

Voor iedere B_i, C_i, D_i berekenen we t_{i+1}:

- $t_{i+1} = \lfloor \frac{C_i+\sqrt{A}}{B_i} \rfloor$

Uit t_{i+1}, B_i, C_i en D_i berekenen we B_{i+1}, C_{i+1} en D_{i+1}:

- $B_{i+1} = -(B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i)$
- $C_{i+1} = B_i t_{i+1} - C_i$
- $D_{i+1} = B_i$

Zo vinden we na één stap de waarden van B_1, C_1 en D_1, die we nodig zullen hebben voor latere bewijzen:

- $B_1 = A - \lfloor \sqrt{A} \rfloor^2$
- $C_1 = \lfloor \sqrt{A} \rfloor$
- $D_1 = 1$

We gaan door met dit proces totdat we een n vinden waarvoor geldt dat n even is, en $B_n = 1$. Dit geeft een vergelijking van de vorm $x_n^2 - 2C_n x_n x_{n+1} - D_n x_{n+1}^2 = 1$. Deze vergelijking is triviaal op te lossen met $x_n = 1, x_{n+1} = 0$. Daarna gebruiken we deze x'en en de t_n om terug te rekenen naar x_1 en x_0,

waarmee we een oplossing hebben gevonden voor de vergelijking van Pell voor A.

We zullen nu een aantal dingen bewijzen over $B_i x^2 - 2C_i x - D_i$, om te laten zien dat de methode inderdaad altijd uitkomt op een vergelijking waarvoor de bovenstaande eisen gelden.

$B_i x^2 - 2C_i x - D_i$ heeft nulpunten $x_{1,2} = \frac{C_i \pm \sqrt{C_i^2 + B_i D_i}}{B_i} = \frac{\sqrt{A - B_i D_i} \pm \sqrt{A}}{B_i}$. Hieruit kunnen we opmaken dat er altijd één positief en één negatief nulpunt is.

Merk op dat omdat B_i, C_i en D_i altijd positief zijn (dit zullen we hieronder bewijzen), $B_i x^2 - 2C_i x - D_i$ een dalparabool is. Een andere manier om t_{i+1} te beschrijven is dus dat het het grootste gehele getal is dat kleiner is dan het positieve nulpunt van deze tweedegraadsfunctie.

Definitie: Een tripel van drie positieve gehele getallen (B, C, D) heet *gereduceerd* als het grootste nulpunt van de vergelijking $Bx^2 - 2Cx - D$ groter is dan 1, en het kleinste nulpunt groter is dan -1.[26]

Stelling 5.3. *(B, C, D) is gereduceerd $\Leftrightarrow |B - D| < 2C$.*

Bewijs. Het negatieve nulpunt van $Bx^2 - 2Cx - D$ is groter dan -1 dan en slechts dan als $\frac{\sqrt{A - BD} - \sqrt{A}}{B} > -1$. Er geldt

$$\begin{array}{lll}
\frac{\sqrt{A - BD} - \sqrt{A}}{B} & > -1 & \Leftrightarrow \\
\sqrt{A - BD} + B & > \sqrt{A} & \Leftrightarrow \\
(\sqrt{A - BD} + B)^2 = A - BD + B^2 + 2B\sqrt{A - BD} & > A & \Leftrightarrow \\
B(B - D + 2\sqrt{A - BD}) & > 0 & \Leftrightarrow \\
B - D + 2C & > 0 & \Leftrightarrow \\
D - B & < 2C. &
\end{array}$$

Op dezelfde manier geldt dat het positieve nulpunt groter is dan 1 dan en slechts dan als $\sqrt{A - BD} + \sqrt{A} > B$. Er geldt

$$\begin{array}{lll}
\sqrt{A - BD} + \sqrt{A} & > B & \Leftrightarrow \\
B - \sqrt{A - BD} & < \sqrt{A} & \Leftrightarrow \\
B^2 + A - BD - 2B\sqrt{A - BD} & < A & \Leftrightarrow \\
B(B - D - 2C) & < 0 & \Leftrightarrow \\
B - D - 2C & < 0 & \Leftrightarrow \\
B - D & < 2C. &
\end{array}$$

Uit dit alles samen volgt dat (B, C, D) gereduceerd is dan en slechts als $|B - D| < 2C$. □

Opmerking 5.2. *(D, C, B) is dan ook gereduceerd.*

[26] Deze definitie van een 'gereduceerd' tripel heb ik uit Weil's boek *Number Theory and its History*, het is een standaardterm uit de theorie van binaire kwadratische vergelijkingen.

Stelling 5.4. *(B_1, C_1, D_1) is gereduceerd.*

Bewijs. $B_1 = A - \lfloor\sqrt{A}\rfloor^2$, $C_1 = \lfloor\sqrt{A}\rfloor$, $D_1 = 1$. Omdat $A \geqslant \lfloor\sqrt{A}\rfloor^2 + 1$ mogen we de absolute waarde strepen in $|B-D|$ weglaten. Stel nu dat $A - \lfloor\sqrt{A}\rfloor^2 - 1 \geqslant 2\lfloor\sqrt{A}\rfloor$. Dan geldt dat $\lfloor\sqrt{A}\rfloor^2 + 2\lfloor\sqrt{A}\rfloor + 1 \leqslant A$, en dus dat $(\lfloor\sqrt{A}\rfloor + 1)^2 \leqslant A$. Tegenspraak. Dus (B_1, C_1, D_1) is gereduceerd. □

Stel nu dat (B_i, C_i, D_i) gereduceerd is. Dan liggen er minstens twee gehele getallen (0 en 1) tussen het negatieve nulpunt en het positieve nulpunt van $B_i x^2 - 2C_i x - D_i$. Omdat de x-waarde waar $B_i x^2 - 2C_i x - D_i$ een minimum aanneemt op het gemiddelde van de twee nulpunten ligt, ligt er minstens één geheeltallig punt tussen deze x-waarde en het positieve nulpunt. De afgeleide van deze functie in t_{i+1} is dus positief, want we hebben op bladzijde 67 t_{i+1} gedefinieerd als $\lfloor\frac{C_i+\sqrt{A}}{B_i}\rfloor$, het grootste gehele getal kleiner dan het positieve nulpunt van $B_i x^2 - 2C_i x - D_i$. Hieruit volgt dat $B_i t_{i+1} - C_i$ positief is.

Stelling 5.5. *Als (B_i, C_i, D_i) gereduceerd is, en B_i, C_i en D_i positief zijn, zijn B_{i+1}, C_{i+1} en D_{i+1} positief.*

Bewijs.

- $B_{i+1} = -(B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i)$, is positief, omdat $(B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i)$ negatief is per hoe t_{i+1} gekozen wordt.
- $C_{i+1} = B_i t_{i+1} - C_i > 0$.
- $D_{i+1} = B_i > 0$.

□

Stelling 5.6. *Als (B_i, C_i, D_i) gereduceerd is, is $(B_{i+1}, C_{i+1}, D_{i+1})$ gereduceerd.*

Bewijs. Volgens de keuze van t_{i+1} geldt:

- $B_i(t_{i+1} - 1)^2 - 2C_i(t_{i+1} - 1) - D_i < 0$
- $B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i < 0$
- $B_i(t_{i+1} + 1)^2 - 2C_i(t_{i+1} + 1) - D_i > 0$

Daaruit berekenen we:

$$\begin{aligned} B_{i+1} - D_{i+1} - 2C_{i+1} &= -B_i t_{i+1}^2 + 2C_i t_{i+1} + D_i - B_i + 2C_i - B_i t_{i+1} \\ &= -B_i(t_{i+1} + 1)^2 + 2C_i(t_{i+1} + 1) + D_i < 0, \\ D_{i+1} - B_{i+1} - 2C_{i+1} &= B_i + B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i + 2C_i - B_i t_{i+1} \\ &= B_i(t_{i+1} - 1)^2 - 2C_i(t_{i+1} - 1) - D_i < 0. \end{aligned}$$

Dus $|B_{i+1} - D_{i+1}| < 2C_{i+1}$. □

Uit Stellingen 5.1 tot en met 5.6 volgt dat alle tripels (B_i, C_i, D_i) gereduceerd zijn.

Het algoritme van Wallis en Brouncker berekent steeds nieuwe vergelijkingen. We hebben nu aangetoond dat we deze op twee manieren kunnen vinden: hetzij door de (B_i, C_i, D_i) om te schrijven, hetzij door $x_i = t_{i+1}x_{i+1} + x_{i+2}$ in te vullen en de vergelijking te vermenigvuldigen met -1. Immers:

$$\begin{aligned}(-1)^i &= B_{i+1}x_{i+1}^2 - 2C_{i+1}x_{i+1}x_{i+2} - D_{i+1}x_{i+2}^2 \\ &= -(B_i t_{i+1}^2 - 2C_i t_{i+1} - D_i)x_{i+1}^2 - 2(B_i t_{i+1} - C_i)x_{i+1}x_{i+2} - B_i x_{i+2}^2 \\ &= -B_i(t_{i+1}x_{i+1} + x_{i+2})^2 + 2C_i(t_{i+1}x_{i+1} + x_{i+2})x_{i+1} + D_i x_{i+1}^2.\end{aligned}$$

We hebben eerder opgemerkt dat als (B, C, D) gereduceerd is, (D, C, B) ook gereduceerd is. Met behulp van bovenstaande identiteit kunnen we dit echter aanscherpen:

Stelling 5.7. *Als (B_i, C_i, D_i) gereduceerd is dan zijn (D_i, C_i, B_i) en $(D_{i+1}, C_{i+1}, B_{i+1})$ gereduceerd. Bovendien is $(D'_{i+1}, C'_{i+1}, B'_{i+1})$, de uitkomst van het substitutieproces op $(D_{i+1}, C_{i+1}, B_{i+1})$, gelijk aan (D_i, C_i, B_i).*

Bewijs. De gereduceerdheid hebben we al bewezen, de andere uitspraak is interessanter. Kies voor s het grootste gehele getal zodat $D_{i+1}s^2 - 2C_{i+1}s - B_{i+1}$ nog negatief is, oftewel:

$$s = \lfloor \frac{C_{i+1} + \sqrt{C_{i+1}^2 + B_{i+1}D_{i+1}}}{D_{i+1}} \rfloor = \lfloor \frac{B_i t_{i+1} - C_i + \sqrt{A}}{B_i} \rfloor = t_{i+1} + \lfloor \frac{-C_i + \sqrt{A}}{B_i} \rfloor.$$

We zullen hieronder in Lemma 5.1 laten zien dat $\sqrt{A} - C_i < B_i$. Daaruit volgt dat
$\lfloor \frac{-C_i + \sqrt{A}}{B_i} \rfloor < 1$, en daarmee dat $s = t_{i+1}$.

Dan, volgens de gebruikelijke substitutie:

- $D'_{i+1} = -D_{i+1}s^2 + 2C_{i+1}s + B_{i+1} = -B_i t_{i+1}^2 + 2B_i t_{i+1}^2 - C_i t_{i+1} - B_i t_{i+1}^2 + 2C_i t_{i+1} + D_i = D_i$
- $C'_{i+1} = D_{i+1}s - C_{i+1} = B_i t_{i+1} - B_i t_{i+1} + C_i = C_i$
- $B'_{i+1} = D_{i+1} = B_i$

□

Gevolg 5.1. *i keer het substitutieproces toepassen op (D_i, C_i, B_i) resulteert in (D_0, C_0, B_0).*

Lemma 5.1. *Als (B, C, D) een gereduceerd tripel is, geldt dat $(C + B)^2 > C^2 + BD$.*

Bewijs. Als $B \geqslant D$, dan volgt $(C + B)^2 = C^2 + 2BC + B^2 > C^2 + BD$. Als $D > B$, dan geldt $D < 2C + B$ wegens gereduceerdheid, en dus $(C + B)^2 = C^2 + (2C + B)B > C^2 + DB$. □

Gevolg 5.2. *Uit $C^2 + BD = A$ volgt dat $\sqrt{A} - C = \sqrt{C^2 + BD} - C < \sqrt{(C + B)^2} - C = B$.*

Opmerking 5.3. *Wegens $B_iD_i = A - C_i^2$, geldt $B_i = \frac{A-C_i^2}{D_i} = \frac{A-C_i^2}{B_{i-1}}$*

We hebben in Stelling 5.1 bewezen dat $C_i^2 + B_iD_i = A$ voor alle i. Omdat B_i, C_i en D_i altijd positief zijn zijn er maar eindig veel tripels (B_i, C_i, D_i) mogelijk. We hebben bewezen dat we het algoritme van Wallis en Brouncker zo lang kunnen uitvoeren als we willen; er volgt dus dat na we verloop van tijd een tripel (B_j, C_j, D_j) moeten krijgen dat we al hebben gehad:

Stel dat $(B_{i+p}, C_{i+p}, D_{i+p}) = (B_i, C_i, D_i)$, voor i en p positief en geheel. Dan dus ook $(D_{i+p}, C_{i+p}, B_{i+p}) = (D_i, C_i, B_i)$. Het i keer uitvoeren van de substitutie op (D_i, C_i, B_i) geeft (D_0, C_0, B_0). Dus geldt dat i keer substitueren op $(D_{i+p}, C_{i+p}, B_{i+p})$ tot (D_p, C_p, B_p) leidt. Hieruit volgt dat $(D_p, C_p, B_p) = (D_0, C_0, B_0)$. Dus ook $(B_p, C_p, D_p) = (B_0, C_0, D_0)$.

Oftewel, we bereiken gegarandeerd een situatie waarin $B_p = 1, C_p = 0, D_p = A$. De bijbehorende vergelijking is $B_px_p^2 - 2C_px_py_{p+1} - D_py_{p+1}^2 = (-1)^p$. Als p oneven is, kunnen we de redenering herhalen: $(B_{2p}, C_{2p}, D_{2p}) = (B_p, C_p, D_p) = (B_0, C_0, D_0)$. We komen dus altijd uit op een vergelijking van de vorm $x_q^2 - 2C_qx_qy_{q+1} - D_qy_{q+1}^2 = 1$. Deze vergelijking heeft de triviale oplossing $x_q = 1, x_{q+1} = 0$.

We hebben al laten zien dat iedere x_i uit te drukken is als lineaire combinatie van x_{i+1} en x_{i+2}. Daarom kunnen we met x_q en x_{q+1} terugrekenen naar x_{q-1}, en daarna naar x_{q-2}, enzovoorts, tot we x_0 en x_1 bepaald hebben, die een oplossing vormen van het oorspronkelijke probleem. Omdat alle getallen positief en geheel zijn is dit niet de triviale oplossing.

Merk op dat, omdat dit een constructief bewijs is, het meteen bewijst dat er voor iedere A een oplossing bestaat.

Wallis noch Brouncker heeft ooit een bewijs gegeven dat deze methode werkt. Net als Bhaskara gaan ze ook niet in op de mogelijkheid dat er een A zou kunnen bestaan waarvoor geen oplossing voor $x^2 - Ay^2 = 1$ gevonden kan worden, in welk geval hun algoritme niet zou werken. Zij hebben Fermat alleen een

uitwerking van zijn opgaven gestuurd, met de opmerking dat zij ieder dergelijk probleem met hun methode op zouden kunnen lossen.

Het eerste *bewijs* van de werking van een algoritme voor het oplossen van de vergelijking van Pell komt toe aan Lagrange, die haar oplost met behulp van kettingbreuken. Lagrange is voor zover ik heb kunnen vinden ook de eerste die indices gebruikt bij het oplossen van de vergelijking van Pell. Zijn bewijs staat in Hoofdstuk 7.3.

Hoofdstuk 6

Kettingbreuken en de vergelijking van Pell

6.1 Lagrange

De volgende twee belangrijke ontwikkelingen op het gebied van de vergelijking van Pell staan in de Franse vertaling van Leonhard Euler's *Anleitung zur Algebra*[1] [2]door Joseph Lagrange.

Leonhard Euler *(1707-1783)* wordt vaak genoemd als de grootste wiskundige uit zijn tijd. Hij werd geboren in Basel, Zwitserland, maar heeft zijn leven doorgebracht als professor in Sint Petersburg en Berlijn.

Euler heeft bijdragen geleverd aan iedere tak van de wiskunde, en wordt algemeen gezien als de eerste die grafentheorie bedreef. Hij is misschien wel de meest productieve wiskundige ooit: er is ooit geschat dat iemand die acht uur per dag bezig zou zijn met het overschrijven van Euler's volledig werk daar vijftig jaar voor nodig zou hebben[3]. Zijn tomeloze productie is des te indrukwekkender als men bedenkt dat hij op latere leeftijd blind werd (waarschijnlijk door experimenten waarbij hij naar de zon keek zonder oogbescherming), en de helft van zijn werk heeft moeten dicteren aan assistenten.

[1] Dit boek staat in de literatuurlijst als 'Elements of Algebra', omdat ik een Engelse vertaling gebruikt heb.

[2] De *Dictionary of Scientific Biogrpahy* meldt dat het originele werk van Euler in het Russisch geschreven is (Euler doceerde destijds in Sint Petersburg), maar ook dat Lagrange de Duitse titel vertaalde. Het is dus goed mogelijk dat er nog een vertaling tussen Euler en Lagrange in zit.

[3] *Dictionary of Scientific Biography*

Euler schreef niet alleen artikelen maar wisselde brieven uit met vele topwiskundigen uit zijn tijd, zoals Goldbach, Lagrange en de familie Bernoulli. Er zijn meer dan 300 verschillende wiskundigen bekend waar Euler mee gecorrespondeerd heeft.[4] Daarnaast is Euler ook verantwoordelijk voor een groot aantal lesboeken, die tegenwoordig nog zeer goed leesbaar zijn. Deze boeken hebben ertoe geleid dat Euler zonder twijfel de meest gelezen wiskundige uit zijn tijd is.

Anleitung zur Algebra gaat (in tegenstelling tot de moderne betekenis van 'algebra') voornamelijk over het oplossen van lineaire en polynomiale vergelijkingen, waarbij Euler uitgebreid stilstaat bij het vinden van oplossingen in gehele getallen. Hij bespreekt in Hoofdstuk 7 van Deel II de methode van Wallis en Brouncker voor het oplossen van de vergelijking van Pell, met twee wijzigingen. Één daarvan is wiskundig: in plaats van met de hand de waarden van x_i en y_i af te schatten gebruikt Euler de wortelformule. De andere wijziging is historisch van aard: in plaats van aan Lord Brounkcer of John Wallis schrijft Euler het algoritme toe aan John Pell. John Pell heeft weinig tot niets te maken gehad met de naar hem vernoemde vergelijking; het enige dat hij gedaan heeft is het publiceren van Wallis' algoritme in zijn boek *Translation of Rizonius's Algebra*.

Als gevolg van Euler's bekendheid bleef zijn toeschrijving echter hangen, en kennen we $x^2 - Ay^2 = 1$ tegenwoordig als 'de vergelijking van Pell'. Een term als 'de vergelijking van Fermat', 'de vergelijking van Wallis (en Brouncker)' of zelfs 'de vergelijking van Archimedes' of 'de vergelijking van Brahmagupta en Bhaskara' zou de geschiedenis van deze vergelijking beter weerspiegelen.

Joseph Louis Lagrange *(1736-1813)* is de andere wiskundige die vaak wordt genoemd als grootste van de achttiende eeuw. Hoewel de familie Lagrange in Turijn woonde was ze van Franse afkomst. Lagrange gebruikte dan ook vanaf jonge leeftijd al de Franse spelling van zijn naam. Tijdens de studie rechten (die hij volgde op aanraden van zijn vader) begon Lagrange zelfstandig wiskunde te studeren, en bleek hij hiervoor aanzienlijk talent te hebben.

Het leven van Lagrange valt op te delen in drie delen, die samenvallen met de plaatsen waar hij geleefd heeft: van 1736 tot 1766 in Turijn, waar hij op zijn negentiende benoemd werd tot professor aan de Koninklijke School voor Artillerie in Turijn,[5] van 1766 tot 1787 als professor in Berlijn, en van 1788 tot zijn dood in 1813 in Parijs, als inmiddels genaturaliseerd Frans staatsburger.

Lagrange heeft binnen de analyse gewerkt aan het berekenen van maxima en minima, golfvergelijkingen (deels als onderdeel van natuurkundig werk over geluidsgolven) en de middelwaardestelling (die hij geformuleerd heeft). Ook heeft

[4] *Dictionary of Scientific Biography*

[5] In de achttiende en negentiende eeuw waren militaire academies belangrijke werkgevers voor wiskundigen en fysici, omdat die in staat waren de banen van kanonskogels en dergelijke te berekenen.

hij de klassieke mechanica hergeformuleerd in termen van kinetische en potentiële energie in plaats van krachten, wat het makkelijker maakt sommige problemen te berekenen. Ook heeft hij zich, vooral in zijn Berlijnse periode, bezig gehouden met getaltheorie. Tenslotte heeft hij werk geleverd op het gebied van groepentheorie, astronomie en analytische meetkunde.

Lagrange heeft vanaf jonge leeftijd met Euler gecorrespondeerd. Zijn eerste artikel stuurde hij aan Euler, en diens aanbeveling leidde in 1755 tot de publicatie van Lagrange's oplossing voor een probleem dat vijftig jaar onopgelost was gebleven.[6] Hun relatie was langdurig (hoewel niet bijzonder vriendschappelijk), en leidde er toe dat Lagrange in 1772 Euler's *Anleitung zur Algebra* naar het Frans vertaalde Hierbij voegde hij een lang stuk eigen werk als uitbreiding, onder de naam *Additions*, 'toevoegingen'.

Additions is een uitgebreide kennismaking met kettingbreuken, de daarvan afgeleide convergenten, en hun toepassingen. In zijn behandeling van kettingbreuken noemt Lagrange ook de vergelijking van Pell, en werkt hij uit hoe je die met kettingbreuken op kunt lossen. Lagrange gebruikt de afschat-eigenschappen van kettingbreuken om voor het eerst aan te tonen *dat* er überhaupt een oplossing voor de vergelijking van Pell bestaat. Daarnaast geeft hij een eenvoudige manier om zo'n oplossing te vinden. We zullen in dit hoofdstuk laten zien hoe deze methode werkt, en in het volgende hoofdstuk bewijzen dat ze equivalent is aan de methoden uit Hoofdstukken 4 en 5.

Kettingbreuken zelf waren in het Westen bekend sinds de werken van de wiskundigen Bombelli *(±1530-?)* en Cataldi *(1548-1628)* uit Bologna. (Daarnaast zijn er aanwijzingen dat zowel de oude Grieken als de oude Indiërs specifieke kettingbreuken hebben gebruikt om bepaalde problemen op te lossen). Er is aan kettingbreuken gewerkt door onder anderen lord Brouncker, Christiaan Huygens *(1629-1695)*, en Euler. Hoewel lord Brouncker zich met kettingbreuken heeft beziggehouden (hij is de eerste die $\frac{4}{\pi}$ als een kettingbreuk schreef), heeft hij nooit ingezien dat ze ook van toepassing waren op het probleem dat Fermat hem opgaf.

6.2 Kettingbreuken

Ik zal in dit hoofdstuk een korte introductie in kettingbreuken geven. Ik leg hier kort uit wat kettingbreuken zijn, en geef een aantal resultaten die we nodig zullen hebben voor het uitleggen van de moderne manier om de vergelijking van Pell op te lossen, en het bewijs dat deze equivalent is aan de Indiase en Engelse algoritmes. We zullen deze resultaten niet bewijzen, omdat ik ketting-

[6] Voor geïnteresseerden: het betreft hier het isoperimetrisch probleem, dat te maken heeft met het maximaliseren van de oppervlakte van een kromme met vaste lengte.

breuken alleen wil behandelen in het kader van de vergelijking van Pell. Voor de geïnteresseerde lezer zijn de bewijzen zelf uit te vinden, of op te zoeken in het dictaat *Getaltheorie* van R. Tijdeman. Het materiaal in deze sectie is voldoende voor het begrijpen van de wiskunde in de volgende twee hoofdstukken.

Deze uitleg van kettingbreuken is consistent met die van Lagrange, maar niet direct op zijn werk gebaseerd, omdat hij het grondiger opbouwt dan we nodig zullen hebben. In plaats daarvan heb ik een gedeelte van hoofdstuk 6 van het bovengenoemde dictaat samengevat, en een stuk over negatieve en andere kettingbreuken toegevoegd op basis van *Die Lehre von den Kettenbrüchen* van O. Perron.

We kunnen een rationaal getal beschrijven als de *ratio* tussen twee gehele getallen. Dit werkt echter niet voor niet-rationale reële getallen. Een kettingbreuk is een manier om een dergelijk reeël getal tot op willekeurige nauwkeurigheid te benaderen, alleen gebruik makend van gehele getallen.

Zij gegeven een reeël getal α. We kunnen α schrijven als $a_0 + \alpha_1$, met $a_0 \in \mathbb{Z}$ en $0 \leqslant \alpha_1 < 1$. Wegens deze laatste voorwaarde geldt óf dat $\alpha_1 = 0$ óf dat $\frac{1}{\alpha_1} > 1$. In het eerste geval is α een geheel getal, in het tweede geval moet $\frac{1}{\alpha_1}$ te schrijven zijn als $a_1 + \alpha_2$, met $a_1 \in \mathbb{Z}$ en $0 \leqslant \alpha_2 < 1$. Op vergelijkbare wijze is α_2 óf gelijk aan 0, in welk geval de kettingbreuk afbreekt, óf $\alpha_2 > 1$, en is het te schrijven als $a_2 + \alpha_3$, met $a_2 \in \mathbb{Z}$ en $0 \leqslant \alpha_3 < 1$. We kunnen oneindig lang doorgaan met dit proces, tenzij een van de gevonden α_i gelijk is aan 0.

De oorspronkelijke α is nu te schrijven als $a_0 + \alpha_1 = a_0 + \frac{1}{\frac{1}{\alpha_1}} = a_0 + \frac{1}{a_1 + \alpha_2}$. Dit is verder te expanderen:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \alpha_3}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ldots}}}}}$$

De term 'kettingbreuk' moge duidelijk zijn.

De gebruikelijke notatie van een kettingbreuk[7] is $\alpha = [a_0; a_1, a_2, a_3, ...]$. We noemen de a_i de *wijzergetallen* van α. Voor $i > 0$ geldt $a_i \in \mathbb{N}$.

Stelling 6.1. *De kettingbreuk van α breekt af $\Leftrightarrow \alpha \in \mathbb{Q}$*

Bewijs. $\Rightarrow$ Als $\alpha = [a_0; a_1, a_2, ..., , a_{k-1}]$, dan

[7] Een andere notatie die wel voorkomt is $\alpha = [a_0; a_1, a_2, a_3, ..., , a_{k-1} + \alpha_k]$. Ook wordt de puntkomma na a_0 wel eens geschreven als een komma.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots a_{k-1}}}} \in \mathbb{Q}.$$

$\Leftarrow$ Zij $\alpha \in \mathbb{Q}$. Schrijf $\alpha = \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N}$, met de grootste gemene deler van p en q gelijk aan 1. Volgens het algoritme van Euclides bestaan er nu $c_k, d_k \in \mathbb{Z}$ met $q > d_1 > d_2 > .... > d_{k-1} > d_k > 0$ zodat

- $p = c_0 q + d_0$
- $q = c_1 d_0 + d_1$
- ...
- $1 = c_k d_{k-1} + d_k$

Het is gemakkelijk in te zien dat bij een kettingbreukexpansie van α de c_i, $0 \leqslant i \leqslant k$, de wijzergetallen a_i worden, en dat de resulterende kettingbreuk dus eindig is. □

Iedere eindige kettingbreuk komt dus overeen met precies één rationaal getal. Omgekeerd zijn er voor ieder rationaal getal *twee* kettingbreuken: $[a_0; a_1, ..., a_k]$ en $[a_0; a_1, ..., a_k - 1, 1]$. De eerste hiervan wordt gevonden door de hierbovengenoemde methode. Merk op dat bij de tweede geldt dat $\alpha_{k+1} > 1$. Er zijn dan ook definities van kettingbreuken (vooral oudere) die '1' als laatste getal uitsluiten, zodat er een één op één relatie is tussen rationale getallen en eindige kettingbreuken.

Gegeven een kettingbreuk voor α kunen we voor ieder bestaand wijzergetal a_i beslissen de kettingbreuk 'af te kappen' en $[a_0; a_1, a_2, ..., a_i + \alpha_{i+1}]$ te vervangen door $[a_0; a_1, a_2, ..., a_i]$. Als α irrationaal is geeft dit een rij breuken $\{\frac{p_i}{q_i}\}_{i=1}^{\infty}$, die α benaderen. Als α rationaal is eindigt de rij met α zelf. Deze breuken worden de *convergenten* van α genoemd. Ze hebben diverse nuttige eigenschappen, waarvan we een aantal in een lijstje resultaten zullen geven.

Door de eindige kettingbreuk uit te werken kunnen we deze p_i en q_i ook directer definiëren.

Resultaat 6.1. *Voor i positief en geheel zijn p_i en q_i als volgt inductief te berekenen:*

- $p_{-1} = 0$, $p_0 = 1$, $p_i = a_{i-1} p_{i-1} + p_{i-2}$

- $q_{-1} = 1$, $q_0 = 0$, $q_i = a_{i-1}q_{i-1} + q_{i-2}$

Omdat $a_i \geqslant 1$ geldt vanaf $i = 1$ dat $p_{i+1} > p_i$, en vanaf $i = 2$ dat $q_{i+1} > q_i$.

Resultaat 6.2. $p_i q_{i-1} - p_{i-1} q_i = (-1)^i$.

Resultaat 6.3. $[a_0; a_1, ..., a_{i-1}, x] = \frac{x p_i + p_{i-1}}{x q_i + q_{i-1}}$

Resultaat 6.4. *De rij* $\{\frac{p_i}{q_i}\}_{i=1}^{\infty}$ *convergeert naar* α.

Resultaat 6.5. $|\alpha - \frac{p_i}{q_i}| \leqslant \frac{1}{q_i^2}$ *voor alle positieve en gehele* i.

Resultaat 6.6. *Iedere* $\frac{p_i}{q_i}$ *is een beste benaderingsbreuk van* α. *Dit wil zeggen dat er geen breuk* $\frac{r}{s} \neq \frac{p_i}{q_i}$ *met* $s \leqslant q_i$ *bestaat zodat* $|\alpha - \frac{r}{s}| < |\alpha - \frac{p_i}{q_i}|$.

Resultaat 6.7. *(Legendre) Zij* $\alpha \in \mathbb{R}$. *Als* $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, *dan is* $\frac{p}{q}$ *een convergent van* α.

Technisch gezien heet wat we hier gedefiniëerd hebben de *versimpelde kettingbreuk*. Het is namelijk mogelijk om kettingbreuken te generaliseren tot de vorm

$$\alpha = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{a_4 + \cfrac{b_5}{\ddots}}}}}.$$

waarbij (voor i positief en geheel) de a_i positief en geheel zijn, en de b_i geheel, maar niet per se positief. In dit geval vervalt natuurlijk de eigenschap dat er precies één kettingbreuk per (niet-rationaal) reeël getal is.

Een deelverzameling van deze gegeneraliseerde kettingbreuken zijn de zogenaamde *half-regelmatige* kettingbreuken. Deze voldoen aan drie extra eisen: $|b_i| = 1$, $a_i \geqslant 1$, en $a_i + b_{i+1} \geqslant 1$. Het is te bewijzen[8] dat alle half-regelmatige kettingbreuken convergeren, oftwel dat $\lim_{i\to\infty} a_0 + \cfrac{\pm 1}{a_1 + \cfrac{\pm 1}{a_2 + \cfrac{\pm 1}{\ddots\, a_{i-1} + \frac{\pm 1}{a_i}}}} = \alpha$.

Twee interessante half-regelmatige kettingbreuken zijn de 'negatieve' kettingbreuken en de 'afgeronde' kettingbreuken.

[8] Zie voor een duidelijk bewijs Perron, *Die Lehre von den Kettenbrüchen*, Hoofdstuk 5 op pagina 135

In het geval van de negatieve kettingbreuken wordt b_k altijd als -1 te gekozen. In vergelijking met de versimpelde kettingbreuken zijn alle plustekens vervangen door mintekens, en zijn alle a_k omhoog in plaats van omlaag afgerond.

De 'afgeronde' variant gebruikt zowel positieve als negatieve b_i. Steeds wordt a_k zo gekozen dat $|a_k - \alpha_k|$ minimaal is. Het teken van b_k is dan afhankelijk van of α_k omhoog of omlaag wordt afgerond.

Beide varianten voldoen duidelijk aan de eerste twee eisen voor half-regelmatigheid. Omdat $\alpha_i < 1$ geldt dat de a_i van de negatieve kettingbreuk altijd $\geqslant 2$ zijn. Op vergelijkbare wijze volgt voor de 'afgeronde' kettingbreuk uit $|\alpha_i| \leqslant \frac{1}{2}$, dat $a_i \geqslant 2$. Dus geldt in beide gevallen dat $a_i + b_{i+1} \geqslant 1$.

Er is een interessante parallel tussen de versimpelde kettingbreuk versus de 'afgeronde' kettingbreuk, en de 'versimpelde' cirkelmethode versus de 'originele' kettingbreuk waar we in Hoofdstuk 7 uitgebreid op terug zullen komen.

6.3 Het gebruik van convergenten om Pell's vergelijking op te lossen

Het lijkt op het eerste gezicht vreemd dat een getaltheoretisch probleem als de vergelijking van Pell iets met kettingbreuken te maken heeft. Tenslotte worden kettingbreuken gebruikt voor het maken van nauwkeurige benaderingen van irrationale getallen, en is de vergelijking van Pell een zoektocht naar twee getallen die voldoen aan een kwadratische vergelijking.

Het verband is dat een oplossing van de vergelijking van Pell een goede benadering geeft voor $\sqrt{A}$. Immers, als geldt dat $x^2 = Ay^2 + 1$, en x en y zijn redelijk groot dan geldt $x^2 \approx Ay^2$, en daarmee $\sqrt{A} \approx \frac{x}{y}$. Vergelijk de benaderingen van $\sqrt{2}$ door de Pythagoreërs in Hoofdstuk 3.1.

We kunnen bewijzen dat iedere oplossing (x, y) van de vergelijking van Pell een breuk $\frac{x}{y}$ geeft, die een beste benaderingsbreuk is van $\sqrt{A}$.

We kunnen dit nog iets algemener stellen:

Stelling 6.2. *Zij A een positief geheel getal, dat geen kwadraat is. Zij k een geheel getal zodat $0 < |k| < \sqrt{A}$. Als nu (x, y) een geheeltallige oplossing is van $x^2 - Ay^2 = k$, dan is $\frac{x}{y}$ een convergent van $\sqrt{A}$.*

Bewijs. Merk op dat $k = x^2 - Ay^2 = (x + \sqrt{A}y)(x - \sqrt{A}y)$. Als (x, y) een oplossing is, zijn $(\pm x, \pm y)$ allemaal oplossingen. We mogen dus aannemen dat

x en y positief zijn. We behandelen $k > 0$ en $k < 0$ apart.

Als $k > 0$ geldt $x + \sqrt{A}y > 0$. Er geldt ook dat $x - \sqrt{A}y = \frac{k}{x+\sqrt{A}y} > 0$. Hieruit volgt dat $\frac{x}{y} - \sqrt{A} > 0$. Nu volgt:
$0 < x - \sqrt{A}y = \frac{k}{x+\sqrt{A}y} < \frac{\sqrt{A}}{x+\sqrt{A}y} = \frac{1}{y} \cdot \frac{1}{1+\frac{x}{y\sqrt{A}}}$.
Dus $0 < \frac{x}{y} - \sqrt{A} = \frac{\frac{k}{x+\sqrt{A}y}}{y} < \frac{1}{y^2(1+\frac{x}{\sqrt{A}y})} < \frac{1}{2y^2}$, immers, $\frac{x}{\sqrt{A}y} > 1$. Nu weten we dat $\frac{x}{y}$ een convergent is volgens Resultaat 6.7.

Als $k < 0$ geldt $x + \sqrt{A}y > 0$ en $x - \sqrt{A}y = \frac{k}{x+\sqrt{A}y} < 0$. Dus $\frac{x}{y} < \sqrt{A}$. Wegens $y^2 - \frac{x^2}{A} = \frac{-k}{A}$ en $-k < \sqrt{A}$ geldt
$0 < \frac{y}{x} - \frac{1}{\sqrt{A}} = \frac{1}{x}(y - \frac{x}{\sqrt{A}}) = \frac{1}{x} \cdot \frac{\frac{-k}{A}}{y+\frac{x}{\sqrt{A}}} = \frac{1}{x^2} \cdot \frac{\frac{-k}{A}}{\frac{y}{x}+\frac{1}{\sqrt{A}}} < \frac{1}{x^2} \cdot \frac{\frac{1}{\sqrt{A}}}{\frac{y}{x}+\frac{1}{\sqrt{A}}}$.

Uit $\frac{x}{y} < \sqrt{A}$ volgt $\frac{\frac{1}{\sqrt{A}}}{\frac{y}{x}+\frac{1}{\sqrt{A}}} < \frac{1}{2}$. Daarom geldt dat $\frac{1}{x^2} \cdot \frac{\frac{1}{\sqrt{A}}}{\frac{y}{x}+\frac{1}{\sqrt{A}}} < \frac{1}{2x^2}$.

Volgens Resultaat 6.7 is $\frac{y}{x}$ nu een convergent van $\frac{1}{\sqrt{A}}$. Zij $\sqrt{A} = [a_0; a_1, ...]$. Dan $a_0 \geqslant 1$, en $\frac{1}{\sqrt{A}} = [0; a_0, a_1, ...]$. Dus er bestaat een n zó dat $\frac{y}{x} = [0; a_0, a_1, ..., a_n] = \frac{1}{[0,a_0,a_1,...,a_n]}$. Dan is $\frac{x}{y} = [a_0; a_1, ..., a_n]$ een convergent van $\sqrt{A}$.

□

Op het geval dat k ongelijk is aan 1 zullen we in hoofdstuk 8.2 terugkomen.

Stelling 6.3. *Voor elk positief geheel getal A dat geen kwadraat is heeft de vergelijking $x^2 - Ay^2 = 1$ een oplossing x_0, y_0 in natuurlijke getallen.*[9]

Bewijs. Laat $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, $\frac{p_3}{q_3}$,... de rij van convergenten van $\sqrt{A}$ zijn. Uit Resultaat 6.5 volgt nu dat $|\sqrt{A} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$.
Omdat $\frac{p_n}{q_n} = \sqrt{A} + \epsilon$, $|\epsilon| < \frac{1}{q_n^2}$ geldt dat $\sqrt{A} + \frac{p_n}{q_n} < 2\sqrt{A} + 1 < 3\sqrt{A}$.
Dus $|p_n^2 - Aq_n^2| = q_n^2|\frac{p_n}{q_n} - \sqrt{A}||\frac{p_n}{q_n} + \sqrt{A}| < |\frac{p_n}{q_n} + \sqrt{A}| < 3\sqrt{A}$.

Bekijk nu de oneindig lange rij $\{p_n^2 - Aq_n^2\}_{n=1}^{\infty}$. Ieder element van deze rij is begrensd door $3\sqrt{A}$. Er is dus minstens één $k < 3\sqrt{A}$ geheel en positief zodat de vergelijking $x^2 - dy^2 = k$ oneindig veel oplossingen (p_n, q_n) heeft. We splitsen al deze oplossingen in k^2 equivalentieklassen volgens de equivalentierelatie $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 \equiv x_2 \bmod k$, $y_1 \equiv y_2 \bmod k$.

[9]Merk op dat dit bewijs op de details van de afschatting na hetzelfde is als dat van Stelling 4.12

Er zijn oneindig veel oplossingen en maar eindig veel equivalentieklassen dus minstens één van de klassen bevat oneindig veel oplossingen. Kies twee oplossingen (x_1, y_1) en (x_2, y_2) uit dezelfde equivalentieklasse. Dan geldt modulo k:

$$\begin{array}{lll} x_1x_2 - Ay_1y_2 & \equiv x_1^2 - Ay_1^2 & \equiv 0\ . \\ x_1y_2 - x_2y_1 & \equiv x_1y_1 - x_1y_1 & = 0. \end{array}$$

Definieer $x := \frac{x_1x_2 - Ay_1y_2}{k}$ en $y := \frac{x_1y_2 - x_2y_1}{k}$. Dan volgt
$x^2 - Ay^2 = \frac{(x_1x_2 - Ay_1y_2)^2}{k^2} - A\frac{(x_1y_2 - x_2y_1)^2}{k^2} = \frac{1}{k^2}(x_1^2 - Ay_1^2)(x_2^2 - Ay_2^2) = 1.$

Hieruit volgt direct dat $x^2 > 0$. Mocht het zo zijn dat x of y negatief is, dan vervangen we x door $-x$, respectievelijk y door $-y$. In het geval dat $y = 0$ volgt dat $x_1y_2 = x_2y_1$. Uit Resultaat 6.2 weten we dat x_n en y_n copriem zijn, daarom volgt dat $x_1|x_2$ én $x_2|x_1$, zodat $x_1 = x_2$, wat in tegenspraak is met onze aanname. Dus is (x, y) een positieve geheeltallige oplossing van $x^2 - Ay^2 = 1$. □

Het blijkt dat we met behulp van de afschat-eigenschappen van convergenten kunnen laten zien dat er altijd een oplossing bestaat van $x^2 - Ay^2 = 1$. Helaas geeft de bovenstaande stelling ons niet een concrete oplossing; ze bewijst alleen *dat er een antwoord is*. We kunnen een antwoord construeren door één voor één de convergenten van $\sqrt{A}$ af te gaan, die op te delen in equivalentieklassen en dit te herhalen tot we een equivalentieklasse hebben waar er twee in zitten. Met die twee equivalente convergenten kunnen we dan een oplossing voor Pell's vergelijking maken.

Dit is nogal wat werk. In het volgende stuk zullen we laten zien dat er een makkelijkere manier is om een convergent $\frac{p_n}{q_n}$ te vinden die snel een oplossing (p_n, q_n) levert van $x^2 - Ay^2 = 1$. We doen dit met behulp van een regelmaat in de kettingbreukontwikkeling van $\sqrt{A}$. Deze regelmaat zal ons ook helpen om de verbanden tussen de cirkelmethode, de Engelse methode en de kettingbreukontwikkeling van $\sqrt{A}$ te laten zien.

6.4 De kettingbreuk van een vierkantswortel.

In principe is het mogelijk van ieder reëel getal de kettingbreuk te berekenen. In de praktijk is dit voor willekeurige getallen vaak lastig, vooral als ze een oneindige decimale expansie hebben. Vierkantswortels uit gehele getallen [10] daarentegen hebben een periodieke kettingbreuk. We zullen dat in dit hoofdstuk

[10] In de rest van deze scriptie zal ik het woord 'wortel' gebruiken voor 'vierkantswortel'.

bewijzen, en het vervolgens gebruiken om de vergelijking van Pell eenvoudig op te lossen.

Wat in dit hoofdstuk staat is is algemeen bekend, en grotendeels gebaseerd op het dictaat van R. Tijdeman. Ik heb het darentegen zelf opnieuw geformuleerd als een iteratief proces, omdat dat een vergelijking met de cirkelmethode en de Engelse methode mogelijk maakt.

We beginnen met een voorbeeld. Kies een getal, bijvoorbeeld 55. Omdat $7^2 < 55 < 8^2$, schrijven we $\sqrt{55} = 7 + \alpha_1$ met $\alpha_1 < 1$. We moeten nu $\frac{1}{\alpha_1}$ bepalen.

$\alpha_1 = \sqrt{55} - 7 \rightarrow \frac{1}{\alpha_1} = \frac{1}{\sqrt{55}-7} = \frac{1}{\sqrt{55}-7} \cdot \frac{\sqrt{55}+7}{\sqrt{55}+7} = \frac{\sqrt{55}+7}{6}$.
$\frac{14}{6} < \frac{\sqrt{55}+7}{55-49} < \frac{15}{6} \rightarrow \frac{1}{\alpha_1} = 2 + \frac{\sqrt{55}-5}{6} = 2 + \alpha_2$. $(a_1 = 2)$.

$\alpha_2 = \frac{\sqrt{55}-5}{6} \rightarrow \frac{1}{\alpha_2} = \frac{6}{\sqrt{55}-5} = \frac{6}{\sqrt{55}-5} \cdot \frac{\sqrt{55}+5}{\sqrt{55}+5} = \frac{6(\sqrt{55}+5)}{30}$.
$\frac{12}{5} < \frac{\sqrt{55}+5}{5} < \frac{13}{5} \rightarrow \frac{1}{\alpha_2} = 2 + \frac{\sqrt{55}-5}{5} = 2 + \alpha_3$. $(a_2 = 2)$.

$\alpha_3 = \frac{\sqrt{55}-5}{5} \rightarrow \frac{1}{\alpha_3} = \frac{5}{\sqrt{55}-5} = \frac{5}{\sqrt{55}-5} \cdot \frac{\sqrt{55}+5}{\sqrt{55}+5} = \frac{5(\sqrt{55}+5)}{30}$.
$\frac{12}{6} < \frac{\sqrt{55}+5}{6} < \frac{13}{6} \rightarrow \frac{1}{\alpha_3} = 2 + \frac{\sqrt{55}-7}{6} = 2 + \alpha_4$. $(a_3 = 2)$.

$\alpha_4 = \frac{\sqrt{55}-7}{6} \rightarrow \frac{1}{\alpha_3} = \frac{6}{\sqrt{55}-7} = \frac{6}{\sqrt{55}-7} \cdot \frac{\sqrt{55}+7}{\sqrt{55}+7} = \frac{6(\sqrt{55}+7)}{6}$.
$14 < \sqrt{55} + 7 < 15 \rightarrow \frac{1}{\alpha_4} = 14 + \sqrt{55} - 7 = 2 + \alpha_5$. $(a_4 = 14)$.

$\alpha_5 = \sqrt{55} - 7$... hé, die kennen we al. Het blijkt dat $\alpha_5 = \alpha_1$. Omdat α_6 alleen van α_5 afhangt, moet gelden dat $\alpha_6 = \alpha_2$, en op die manier herhaalt de serie zich eindeloos. We krijgen een rij getallen met periode 4:
$a_0 = 7, a_1 = 2, a_2 = 2, a_3 = 2, a_4 = 14, a_5 = a_1 = 2, a_6 = a_2 = 2$, enzovoorts.
We schrijven $\sqrt{55} = [7; \overline{2, 2, 2, 14}]$.

Laten we het geheel samenvatten als een iteratief systeem, voor het vinden van de kettingbreuk van de wortel van A. Hiervoor schrijven we $\alpha_i = \frac{\sqrt{A}-b_i}{c_i}$. Nu geldt dat $\frac{1}{\alpha_i} = \frac{c_i}{\sqrt{A}-b_i} = \frac{c_i}{\sqrt{A}-b_i} \cdot \frac{\sqrt{A}+b_i}{\sqrt{A}+b_i} = \frac{c_i(\sqrt{A}+b_i)}{A-b_i^2}$. Hieruit volgt dat $a_i = \lfloor \frac{c_i(\sqrt{A}+b_i)}{A-b_i^2} \rfloor$ en $\alpha_{i+1} = \frac{c_i(\sqrt{A}+b_i)}{A-b_i^2} - \lfloor \frac{c_i(\sqrt{A}+b_i)}{A-b_i^2} \rfloor = \frac{c_i(\sqrt{A}+b_i)}{A-b_i^2} - a_i = \frac{\sqrt{A}+b_i-a_i \cdot \frac{A-b_i^2}{c_i}}{\frac{A-b_i^2}{c_i}}$.

Hieruit berekenen we dat $b_{i+1} = -b_i + a_i \cdot \frac{A-b_i^2}{c_i}$ en $c_{i+1} = \frac{A-b_i^2}{c_i}$. Dit leidt tot het volgende algoritme:

Beginwaarden:

- $a_0 = \lfloor\sqrt{A}\rfloor$, $b_1 = \lfloor\sqrt{A}\rfloor$, $c_1 = 1$

Iteratieregels:

- $a_{i+1} = \lfloor\frac{c_{i+1}(\sqrt{A}+b_{i+1})}{(A-b_{i+1}^2)}\rfloor$
- $b_{i+1} = \frac{a_{i+1}(A-b_i^2)}{c_i} - b_i$
- $c_{i+1} = \frac{(A-b_i^2)}{c_i}$

Merk op dat $b_{i+1} = a_{i+1}c_{i+1} - b_i$, en dat uit de definitie van c_{i+1} volgt dat $b_i^2 + c_i c_{i+1} = A$.

Om aan te tonen dat dit systeem uitvoerbaar is moeten we nog bewijzen dat $c_i|(A-b_i^2)$ voor alle i. Daarnaast willen we graag aantonen dat de wijzergetallen periodiek zijn.

Stelling 6.4. *Voor alle i geldt in het bovenstaande algoritme dat* $c_i|(A - b_i^2)$.

Bewijs. We gebruiken volledige inductie. Het is duidelijk dat $1|A - (\lfloor\sqrt{A}\rfloor)^2$, waarmee de stelling bewezen is voor $i = 0$. Stel nu dat $c_n|(A - b_n^2)$. Het invullen van b_{n+1} levert $A - b_{n+1}^2 = A - b_n^2 - a_{n+1}^2 c_{n+1}^2 + 2a_{n+1}c_{n+1}b_n$. Uit de iteratieregel voor c_{i+1} maken we op dat $A - b_n^2 = c_n c_{n+1}$. Het is dus duidelijk dat $c_{n+1}|(A - b_{n+1}^2)$. □

Voordat we kunnen bewijzen dat de kettingbreuk van een wortel periodiek is hebben we eerst een Lemma nodig:

Lemma 6.1. *Zij* $\sqrt{A} = [a_0; a_1, ..., a_{n-1}, x_n]$. *Dan geldt:*
$\frac{1}{x_n} = \frac{-p_{n-1}p_n + Aq_{n-1}q_n}{p_{n-1}^2 - Aq_{n-1}^2} + \frac{(-1)^{n-1}\sqrt{A}}{p_{n-1}^2 - Aq_{n-1}^2}$.

Bewijs. Uit Resultaat 6.3 volgt $\sqrt{A} = \frac{x_n p_n + p_{n-1}}{x_n q_n + q_{n-1}}$. We lossen x_n hieruit op:
$x_n = \frac{p_{n-1} - q_{n-1}\sqrt{A}}{q_n\sqrt{A} - p_n}$
Dus $\frac{1}{x_n} = \frac{q_n\sqrt{A} - p_n}{p_{n-1} - q_{n-1}\sqrt{A}} = \frac{-p_n p_{n-1} + Aq_n q_{n-1} - p_n q_{n-1}\sqrt{A} + p_{n-1}q_n\sqrt{A}}{p_{n-1}^2 - Aq_{n-1}^2}$.
Omdat Resultaat 6.2 zegt dat $p_n q_{n-1} - p_{n-1}q_n = (-1)^n$ volgt
$\frac{1}{x_n} = \frac{-p_n p_{n-1} + Aq_n q_{n-1} + (-1)^{n-1}\sqrt{A}}{p_{n-1}^2 - Aq_{n-1}^2}$. □

Opmerking 6.1. *We kunnen het resultaat van dit lemma ook schrijven als* $\frac{1}{x_n} = r_n + s_n\sqrt{A}$, *waarbij*
$r_n = \frac{-p_{n-1}p_n + Aq_{n-1}q_n}{p_{n-1}^2 - Aq_{n-1}^2}$ *en* $s_n = \frac{(-1)^{n-1}}{p_{n-1}^2 - Aq_{n-1}^2}$.

Stelling 6.5. *Zij* $\sqrt{A} = [a_0, a_1, ...]$. *Dan bestaat een* h *zodat* $\sqrt{A} = [a_0, \overline{a_1, ..., a_h}]$.

Bewijs. Volgens Stelling 6.3 is er een oplossing (p_n, q_n) van $x^2 - Ay^2 = 1$, en volgens Stelling 6.2 zijn p_n en q_n dan convergenten van $\sqrt{A}$. Kies h het kleinste getal zo dat $|p_h^2 - Aq_h^2| = 1$. Uit [verwijzing] volgt dat $(-1)^{h-1}(\sqrt{A} - \frac{p_h}{q_h}) > 0$ en dus $p_h^2 - Aq_h^2 = (-1)^h$. Met behulp van Lemma 6.1 vinden we dat r_{h+1} een geheel getal is, en dat $s_{h+1} = 1$. Omdat $0 < \frac{1}{x_{h+1}} < 1$ (volgens de constructie van kettingbreuken) geldt $0 < r_{h+1} + \sqrt{A} < 1$. Hieruit volgt $r_{h+1} = -\lfloor \sqrt{A} \rfloor = -a_0$. Dus $x_{h+1} = \frac{1}{r_{h+1} + s_{h+1}\sqrt{A}} = \frac{1}{\sqrt{A} - a_0} = [a_1, a_2, ...] = x_1$. Zo vinden we achtereenvolgens $a_{h+1} = a_1$, $x_{h+2} = x_2$, $a_{h+2} = a_2$, enzovoorts. Dus $\sqrt{A} = [a_0, a_1, a_2, ..., a_h, a_1, a_2, ..., a_h, a_1, a_2, ...,] =: [a_0, \overline{a_1, ..., a_h}]$. □

Stelling 6.6. *De in het bewijs van Stelling 6.5 gedefinieerde* h *is minimaal: er is geen kleinere* k *waarvoor geldt dat* $\sqrt{A} = [a_0, \overline{a_1, ..., a_k}]$.

Bewijs. Stel er bestaat een k met $k < h$ en $\sqrt{A} = [a_0, \overline{a_1, ..., a_k}]$. Omdat $\sqrt{A}$ geen rationaal getal is volgt uit Lemma 6.1 dat ook $\{s_n\}_{n=1}^{\infty}$ en dus $\{(-1)^{n-1}(p_{n-1}^2 - Aq_{n-1}^2)\}_{n=2}^{\infty}$ periodiek is met periodelengte k. Dus is er onder de $\{(p_{n-1}^2 - Aq_{n-1}^2)\}_{n=2}^{k+1}$ minstens één met absolute waarde 1. Volgens de definitie van h moet dan gelden dan $k = h$. Hieruit volgt dat h minimaal is.

□

Opmerking 6.2. *De rij* $\{(-1)^{n-1}(p_{n-1}^2 - Aq_{n-1}^2)\}_{n=2}^{\infty}$ *is periodiek met periodelengte* h *en de getallen* n *met* $|(p_n^2 - Aq_n^2)| = 1$ *zijn de veelvouden van* h.

Opmerking 6.3. *Als de hierboven gekozen* h *even is, geldt* $p_h^2 - Aq_h^2 = 1$ *en is* (p_h, q_h) *de* fundamentaaloplossing*; dat wil zeggen de oplossing van* $x^2 - Ay^2 = 1$ *met de kleinste* y *(en daarmee automatisch de kleinste* x*). Als* h *oneven is, dan geldt* $p_h^2 - Aq_h^2 = -1$*, en is* (p_{2h}, q_{2h}) *de fundamentaaloplossing.*

We hadden al bewezen dat *als* er een oplossing bestaat voor $x^2 - Ay^2 = 1$, er oneindig veel dergelijke oplossingen bestaan. We zullen nu bewijzen dat al deze oplossingen te formuleren zijn in termen van de fundamentaaloplossing (x_0, y_0).

Stelling 6.7. *Een paar gehele getallen* (x, y) *is een oplossing voor* $x^2 - Ay^2 = 1$ *dan en slechts dan als er een* $n \in \mathbb{Z}$ *bestaat zodat*

$$x + y\sqrt{A} = \pm(x_0 + y_0\sqrt{A})^n.$$

Bewijs. We beginnen met aantonen dat alle (x, y) die aan bovengenoemde voorwaarde voldoen inderdaad oplossingen zijn. Dit doen we met volledige inductie. We zullen het '$\pm$' teken weglaten, omdat het argument voor positieve getallen triviaal veranderd kan worden in een argument voor negatieve getallen.

Voor $n = 0$ levert de eis de triviale oplossing, en voor $n = 1$ de fundamentaal-oplossing.

Stel dat we voor $n > 0$ een oplossing (x_n, y_n) hebben waarvoor $x_n + y_n\sqrt{A} = (x_0 + y_0\sqrt{A})^n$.

Dan volgt $x_{n+1} + y_{n+1}\sqrt{A} = (x_0 + y_0\sqrt{A})^n(x_0 + y_0\sqrt{A}) = (x_n + y_n\sqrt{A})(x_0 + y_0\sqrt{A})$. Hieruit volgt $x_{n+1} = x_n x_0 + A y_n y_0$, en $y_{n+1} = x_n y_0 + x_0 y_n$. Zoals we weten uit Stanza 65 en 66 van het werk van Brahmagupta op bladzijde 24 is dit een geldige nieuwe oplossing.

Voor negatieve n definiëren we $m = -n$, en krijgen we:

$x_n + y_n\sqrt{A} = \frac{1}{(x_0+y_0\sqrt{A})^m} = (x_0 - y_0\sqrt{A})^m$. Omdat we weten dat $(x_0, -y_0)$ ook een oplossing is, kunnen we het argument voor positieve n hier ook op toepassen.

Nu moeten we nog aantonen dat iedere oplossing van $x^2 - Ay^2 = 1$ in gehele getallen van de gevraagde vorm is. Hiertoe merken we eerst op dat:

- $x + y\sqrt{A} = 1 \Leftrightarrow x = 1, y = 0$
- $x + y\sqrt{A} > 1 \Leftrightarrow x > 0, y > 0$

De eerste regel is duidelijk, de tweede volgt uit de volgende observaties:

- $x > 0, y < 0 \rightarrow x - y\sqrt{A} > 1 \rightarrow x + y\sqrt{A} = (x - y\sqrt{A})^{-1} < 1.$
- $x \leqslant 0, y > 0 \rightarrow x - y\sqrt{A} < 0 \rightarrow x + y\sqrt{A} < 0.$
- $x \leqslant 0, y < 0 \rightarrow x + y\sqrt{A} < 0.$

Zij $\alpha = x_0 + y_0\sqrt{A}$. Omdat x_0 en y_0 minimaal zijn volgt uit de tweede opmerking dat er geen oplossingen (x, y) zijn met $1 < x + y\sqrt{A} < \alpha$. Verder geldt

$x_0 - y_0\sqrt{A} = \frac{1}{x_0+y_0\sqrt{A}} = \alpha^{-1}$.

Zij (x', y') een willekeurige geheeltallige oplossing van $x^2 - Ay^2 = 1$. Als $x' + y'\sqrt{A} < 0$ beschouwen we $(-x', -y')$, dus mogen we aannemen dat $x' + y'\sqrt{A} > 0$. Kies nu $n \in \mathbb{Z}$ zó dat $\alpha^n \leqslant x' + y'\sqrt{A} < \alpha^{n+1}$.

Definieer nu (x'', y'') door $x'' + y''\sqrt{A} = (x' + y'\sqrt{A})(x_0 - y_0\sqrt{A})^n$.

Nu volgt dat $1 \leqslant x'' + y''\sqrt{A} < \alpha$, en dus volgt uit de opmerking hierboven dat $x'' + y''\sqrt{A} = 1$. We concluderen dat $x'' = 1, y'' = 0$. Dus $x' + y'\sqrt{A} = \frac{1}{(x_0-y_0\sqrt{A})^n} = (x_0 + y_0\sqrt{A})^n$ □

We kunnen op deze manier alle oplossingen van de vergelijking van Pell voor gegeven A in één formule geven. Deze formule is zelfs uit te breiden naar het geval $x^2 - Ay^2 = k$.

Stelling 6.8. *Zij A een natuurlijk getal, geen kwadraat en $k \in \mathbb{Z}, k \neq 0$. Stel (a_1, b_1), (a_2, b_2),...,(a_i, b_i) zijn de oplossingen van $x^2 - Ay^2 = k$ waarvoor geldt dat $1 \leqslant a_j + b_j\sqrt{A} < \alpha = x_0 + y_0\sqrt{A}$ (met (x_0, y_0) de fundamentaaloplossing). Dan is elke oplossing (a, b) van $x^2 - Ay^2 = k$ op precies één manier te schrijven als*

$$a + b\sqrt{A} = \pm(a_j + b_j\sqrt{A})(x_0 + y_0\sqrt{A})^n,\ j \in \{1, 2, ..., i\},\ n \in \mathbb{Z}.$$

Tevens zijn al deze uitdrukkingen oplossingen.

We hebben in dit hoofdstuk de eerste bewezen methode behandeld om alle oplossingen van $x^2 - Ay^2 = 1$ te vinden. In het hoofdstuk hierna zullen we laten zien dat de drie methoden die we tot nu toe gezien hebben equivalent zijn. Daarna behandelen we in Hoofdstuk 8 later werk over de vergelijking van Pell, en gaan we dieper in op hte geval $k \neq 1$.

Hoofdstuk 7

Equivalentie van de verschillende methoden

We hebben tot nu toe de vergelijking van Pell op drie manieren opgelost:

- De cirkelmethode uit het oude India begint met de oplossing van een vergelijking die bijna goed is, en veranderd die steeds in de oplossing van een andere vergelijking. Uiteindelijk wordt zo een oplossing gevonden voor $x^2 - Ay^2 = 1$.
- De methode van Wallis en Brouncker beschrijft aan welke eisen een oplossing van de vergelijking van Pell moet voldoen, en breidt die eisen net zo lang uit tot ze makkelijk in te willigen zijn.
- De moderne methode toont aan dat een oplossing van $x^2 - Ay^2 = 1$ te veranderen is in een convergent van $\sqrt{A}$, en gebruikt de kettingbreukontwikkeling van $\sqrt{A}$ om een dergelijke convergent te vinden.

De oplettende lezer zal al gemerkt hebben dat sommige rijtjes getallen in de voorbeelden overeenkomen. Dit is geen toeval: de drie algoritmen zijn wiskundig gezien equivalent. Wat dit betekent zal ik in dit hoofdstuk uitleggen.

Diverse boeken over de geschiedenis van de getaltheorie, zoals Weil's *Number Theory - an approach through History* en Edwards' *Fermat's Last Theorem* merken op dat de methode van de oude Indiërs en die van de Engelse wiskundigen vierhonderd jaar later op hetzelfde neerkomen. Geen van die boeken werkt dit echter uit. Uitzoeken dat deze methodes altijd hetzelfde resultaat geven, en waarom dat zo is, is niet triviaal, en is een van de twee hoofddoelen van deze

scriptie. Zelfs het boek van H. Konen over dit onderwerp bevat geen volledige berekening.

Dit hoofdstuk is dan ook geheel mijn eigen werk, waarin ik de vorige hoofdstukken aan elkaar knoop. Ik heb wat terminologie overgenomen uit andere boeken, en in sommige gevallen opzettelijk de variabelen veranderd, maar al het denken schrijfwerk is van mijzelf.

Ik zal beginnen aan te tonen dat Bhaskara in zijn werk impliciet de kettingbreuk van $\sqrt{A}$ uitrekent.

7.1 Equivalentie van de cirkelmethode en de methode op basis van kettingbreuken

We hebben in hoofdstuk 4.5 de 'versimpelde' cirkelmethode laten zien. Deze methode berekent alleen de k_i en r_i. We zullen laten zien dat de x_i (en daarmee de y_i) eenvoudig te berekenen zijn uit k_i en r_i, en dat dit leidt tot een recursieve betrekking die gelijk is aan die van de convergenten van een kettingbreuk. Via twee hulpvariabelen kunnen we de kettingbreuk daarna geheel uitdrukken in termen van k_i en r_i.

Nog even een lijstje om het geheugen op te frissen. De volgende relaties gelden voor i positief en geheel:

$k_1 = 1.$	$k_{i+1} = \frac{r_i^2 - A}{k_i}$.
$r_1 = \lfloor \sqrt{A} \rfloor.$	r_{i+1} is het grootste getal dat voldoet aan $0 < r_{i+1} < \sqrt{A}$ en k_{i+1} deelt $r_i + r_{i+1}$.
$x_1 = 1.$	$x_{i+1} = \frac{x_i r_i + A y_i}{\lvert k_i \rvert}$.
$y_1 = 0.$	$y_{i+1} = \frac{x_i + r_i y_i}{\lvert k_i \rvert}$

Stelling 7.1. *Definieer* $l_i = \frac{r_i + r_{i+1}}{|k_{i+1}|}$ *voor* $i \geqslant 1$. *Dan geldt voor* $i \geqslant 2$ *dat* $x_{i+1} = l_{i-1}x_i + x_{i-1}$ *en* $y_{i+1} = l_{i-1}y_i + y_{i-1}$.

Bewijs. Er geldt

$$\begin{aligned} |k_i| x_{i+1} &= x_i r_i + A y_i \\ &= x_i(r_{i-1} + r_i) + A y_i - r_{i-1} x_i \\ &= l_{i-1} x_i \cdot |k_i| + A y_i - r_{i-1} x_i. \end{aligned}$$

Daaruit volgt dat

$$\begin{aligned} x_{i+1} &= l_{i-1}x_i + \tfrac{Ay_i - r_{i-1}x_i}{|k_i|} \\ &= l_{i-1}x_i + \tfrac{A(x_{i-1}+r_{i-1}y_{i-1}) - r_{i-1}(r_{i-1}x_{i-1}+Ay_{i-1})}{|k_{i-1}|\cdot|k_i|} \\ &= l_{i-1}x_i + \tfrac{x_{i-1}(A-r_{i-1}^2)}{A-r_{i-1}^2} \\ &= l_{i-1}x_i + x_{i-1}. \end{aligned}$$

Ook geldt

$$\begin{aligned} |k_i|y_{i+1} &= x_i + r_i y_i. \\ &= y_i(r_{i-1}+r_i) + x_i - r_{i-1}y_i \\ &= l_{i-1}y_i \cdot |k_i| + x_i - r_{i-1}y_i. \end{aligned}$$

Daaruit volgt dat

$$\begin{aligned} y_{i+1} &= l_{i-1}y_i + \tfrac{x_i - r_{i-1}y_i}{|k_i|} \\ &= l_{i-1}y_i + \tfrac{r_{i-1}x_{i-1} + Ay_{i-1} - r_{i-1}(x_{i-1}+r_{i-1}y_{i-1})}{|k_{i-1}|\cdot|k_i|} \\ &= l_{i-1}y_i + \tfrac{y_{i-1}(A-r_{i-1}^2)}{A-r_{i-1}^2} \\ &= l_{i-1}y_i + y_{i-1}. \end{aligned}$$

□

Naast l_i definieren we $g_i := \frac{\sqrt{A}+r_i}{|k_{i+1}|}$.

Stelling 7.2. *Er geldt dat* $g_i = l_i + \frac{1}{g_{i+1}}$.

Bewijs.

$$\begin{aligned} g_i &= \tfrac{\sqrt{A}+r_i}{|k_{i+1}|} \\ &= \tfrac{\sqrt{A}+l_i|k_{i+1}|-r_{i+1}}{|k_{i+1}|} \\ &= l_i + \tfrac{\sqrt{A}-r_{i+1}}{|k_{i+1}|} \\ &= l_i + \tfrac{A-r_{i+1}^2}{(\sqrt{A}+r_{i+1})|k_{i+1}|} \\ &= l_i + \tfrac{|k_{i+2}|}{\sqrt{A}+r_{i+1}} \\ &= l_i + \tfrac{1}{g_{i+1}} \end{aligned}$$

□

Het is duidelijk dat $g_1 = \frac{\sqrt{A}+\lfloor\sqrt{A}\rfloor}{|k_2|}$. Het getal l_0 bestaat volgens onze huidige definitie niet, maar dat definiëren we als $\frac{0+r_1}{|k_1|} = \lfloor\sqrt{A}\rfloor$.

Voor j positief en geheel vervullen de getallen l_j en g_j de rol van a_j respectievelijk $\frac{1}{\alpha_j}$ in de kettingbreuk van $\sqrt{A}$:

Stelling 7.3. *Voor j positief en geheel gelden de volgende twee gelijkheden:*

$$a_j = l_j = \frac{r_j + r_{j+1}}{|k_{j+1}|} \text{ en } \frac{1}{\alpha_j} = g_j = \frac{\sqrt{A} + r_j}{|k_{j+1}|}.$$

De getallen r_j, r_{j+1} en k_{j+1} komen uit de 'versimpelde' cirkelmethode, de getallen g_j en l_j zijn hierboven gedefinieerd, de a_j zijn de wijzergetallen van $\sqrt{A}$ en de α_j zijn de resten die ontstaan bij het maken van een kettingbreuk zoals in Hoofdstuk 6.

Bewijs. We bewijzen dit met volledige inductie. De eerste stap is makkelijk: $\sqrt{A} = \lfloor\sqrt{A}\rfloor + (\sqrt{A} - \lfloor\sqrt{A}\rfloor) = l_0 + \frac{A - \lfloor\sqrt{A}\rfloor^2}{\sqrt{A} + \lfloor\sqrt{A}\rfloor} = l_0 + \frac{|k_2|}{\sqrt{A} + \lfloor\sqrt{A}\rfloor} = l_0 + \frac{1}{g_1}$.
Gegeven dat $\sqrt{A} = [l_0; l_1, ..., l_{i-1} + g_i]$ kunnen we Stelling 7.2 gebruiken om aan te tonen dat $\sqrt{A} = [l_0; l_1, ..., l_{i-1}, l_i + g_{i+1}]$ □

De wijzergetallen van $\sqrt{A}$ zijn dus uit te drukken in getallen uit de 'versimpelde' cirkelmethode. We hebben in Stelling 7.1 aangetoond dat voor de getallen x_i en y_i dezelfde recurrente betrekking geldt als voor de p_i en q_i uit de kettingbreuk methode.[1] Omdat $x_1 = 1 = p_1$, $x_2 = \lfloor\sqrt{A}\rfloor = p_2$, $y_1 = 0 = q_1$ en $y_2 = 1 = q_2$ zien we dat de convergenten (p_i, q_i) die geleverd worden door de het ontwikkelen van de kettingbreuk van $\sqrt{A}$ precies de oplossingen (x_i, y_i) zijn die de 'versimpelde' kettingbreukmethode genereert.

We moeten nu alleen nog aantonen dat beide methoden op hetzelfde moment stoppen. De cirkelmethode stopt zodra $k_i = 1$, de moderne methode stopt na n stappen, waar n het kleinste gemene veelvoud is van 2 en de periode van de kettingbreukontwikkeling van $\sqrt{A}$.

Wanneer $k_i = 1$ wordt vanzelf voldaan aan de eis '$|k_i|$ deelt $r_{i-1} + r_i$'. De waarde die r_i dan aanneemt is de grootste mogelijke waarde die kleiner is dan $\sqrt{A}$. Dus $r_i = \lfloor\sqrt{A}\rfloor$. Als we hierna door zouden gaan met het algoritme volgt $k_{i+1} = A - \lfloor\sqrt{A}\rfloor^2 = k_2$, $r_{i+1} = r_2$, enzovoorts. Op vergelijkbare wijze volgt uit $k_i = -1$ dat $k_{i+1} = -k_2$. In dit geval volgt dus ook dat $k_{2i} = 1 = k_1$, en $k_{2i+1} = k_2$. Het is dus duidelijk dat de k_i (en daarmee de r_i) periodiek zijn met periodelengte $i - 1$ als $k_i = 1$ en periodelengte $2i - 1$ als $k_i = -1$. In het bewijs van Stelling 4.12 was dit ook al bewezen.[2]

Om aan te tonen dat de periodes gelijk zijn gebruiken we Stelling 7.2, waaruit blijkt dat $\frac{1}{\alpha_i} = g_i = \frac{\sqrt{A} + r_i}{|k_{i+1}|}$. We weten uit Stelling 6.5 dat er een g_i bestaat

[1] Zie Resultaat 6.1 op bladzijde 77

[2] Merk op dat in de versimpelde methode het teken van het getal k_j steeds het tegengestelde is van dat van k_{j-1}. We weten dus dat $k_i = 1$ als i even is, en dat $k_i = -1$ als i oneven is.

zodat $c_i = g_1$. Dan $\frac{\sqrt{A}+r_i}{|k_{i+1}|} = \frac{\sqrt{A}+r_1}{|k_2|}$. Omdat $\sqrt{A}$ irrationaal is moet dan volgen dat $r_i = r_1$, $|k_{i+1}| = |k_2|$.

We concluderen:

Stelling 7.4. *De periode van de wijzergetallen van $\sqrt{A}$ is gelijk de kleinste i waarvoor $|k_i| = 1$. Net als in de moderne kettingbreukmethode betekent dit dat de fundamentaaloplossing gevonden wordt in $i-1$ stappen als $k_i = 1$, en in $2i-1$ stappen als $k_i = -1$.*

We hebben in Hoofdstuk 4.5 al bewezen dat de 'traditionele' en de 'versimpelde' cirkelmethode dezelfde oplossingen vinden, en dat de 'traditionele' methode hoogstens stappen van de 'versimpelde' overslaat. We kunnen echter ook een kettingbreuk definiëren aan de hand van de getallen uit de 'traditionele' methode. Ik noem voor de duidelijkheid de x_i, y_i, r_i en k_i uit de traditionele methode x'_i, y'_i, r'_i en k'_i.

Definieer net als in het begin van dit hoofdstuk $l'_i := \frac{r'_i+r'_{i+1}}{|k'_{i+1}|}$ en $g'_i := \frac{\sqrt{A}+r'_i}{|k'_{i+1}|}$. Definieer voor $i > 0$ daarnaast $b'_i := \frac{-k'_{i+1}k'_{i+2}}{|k'_{i+1}||k'_{i+2}|}$. Bij het versimpelde algoritme weten we dat $k_{i+1}k_{i+2}$ negatief is. Wanneer de 'tradionele' methode een stap overslaat is $r'_{i+1} > \sqrt{A}$ en is $k_{i+1}k_{i+2}$ positief. We definiëren b_i om in dat geval bij het berekenen van de wijzergetallen van de kettingbreuk omhoog in plaats van omlaag af te ronden.

Voor de getallen l'_i en g'_i geldt bijna hetzelfde als voor l_i en g_i, en de bewijzen van onderstaande twee feiten gaan dan ook volledig analoog aan die van Stellingen 7.1 en 7.2.

- $x'_{i+1} = l'_{i-1}x'_i + x'_{i-1}$
- $c'_i = l'_i + \frac{b'_i}{g'_{i+1}}$

We definiëren nu de 'aangepaste afgeronde' kettingbreuk. Dit is een gegeneraliseerde kettingbreuk (zie bladzijde 78), met $a_i = l'_i$, $\frac{1}{\alpha_i} = g'_i$ en $b_i = b'_i$. Het is duidelijk dat net als in Stelling 7.3 geldt dat $\sqrt{A} = l'_0 + \frac{1}{g'_1}$. We gebruiken de inductiestap uit diezelfde stelling om te bewijzen dat $a_0 + \cfrac{\pm 1}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{\ddots\, a_{i-1} + \frac{b_i}{\alpha_i}}}}$ voor alle i gelijk is aan $\sqrt{A}$.

Er geldt duidelijk dat $|b_i| = 1$ en $a_i \geqslant 1$. Ook geldt dat $a_0 + b_1 \geqslant 1$, en $a_i + b_{i+1} \geqslant 1$ voor $i > 0$ volgt uit dezelfde redenering als voor de gewone

'afgeronde' kettingbreuk. De 'aangepaste afgeronde' kettingbreuk voldoet dus aan de drie eisen van half-regelmatigheid op bladzijde 78.

We hebben in Hoofdstuk 4.5 bewezen dat de 'traditionele' en 'versimpelde' cirkelmethoden dezelfde oplossingen geven voor de vergelijking van Pell. Ook hebben we bewezen dat de 'versimpelde' cirkelmethode dezelfde oplossingen geeft als het bekijken van de convergenten die geleverd worden door de simpele kettingbreuk. Hieruit volgt dat de convergenten die geleverd worden door de 'aangepaste afgeronde' kettingbreuk dezelfde oplossingen geven als de convergenten die geleverd worden door de simpele. Een iets zwakker resultaat is ook direct te bewijzen. Op bladzijde 151 geeft *Die Lehre von den Kettenbrüchen* van O. Perron de volgende stelling:

Stelling 7.5. *Iedere convergent afgeleid van een half-regelmatige kettingbreuk komt ook voor in de rij convergenten die kunnen worden afgeleid van de bijbehorende versimpelde kettingbreuk.*[3]

Bewijs. Omdat dit bewijs veel voorbereidend werk vereist zal ik het hier niet geven. Geïnteresseerden kunnen het nalezen in het werk van Perron. □

7.2 Equivalentie van de methode van Wallis en Brouncker en de methode op basis van kettingbreuken

Het bewijs dat de methode van Wallis en Brouncker equivalent is met de moderne methode is bijna analoog aan het bewijs voor de cirkelmethode. Weer definiëren we een hulpvariabele die afhangt van de gebruikte variabelen, en gebruiken we deze om de kettingbreuk van $\sqrt{A}$ uit te drukken. Het verschil is dat we de a_i al hebben, in de vorm van t_i.

Nu definiëren we $u_{i+1} := \frac{C_i+\sqrt{A}}{B_i}$.

Stelling 7.6. $u_i = t_i + \frac{1}{u_{i+1}}$.

Bewijs. Er geldt op grond van Opmerking 5.3 dat $\frac{1}{u_{i+1}} = \frac{B_i}{C_i+\sqrt{A}} = \frac{A-C_i^2}{B_{i-1}(\sqrt{A}+C_i)}$. Dus vinden we (zie bladzijde 67) dat $\frac{1}{u_{i+1}} = \frac{\sqrt{A}-C_i}{B_{i-1}} = \frac{\sqrt{A}-B_{i-1}t_i+C_{i-1}}{B_{i-1}} = -t_i + \frac{C_{i-1}+\sqrt{A}}{B_{i-1}} = u_i - t_i$. Nu volgt dat $u_i = t_i + \frac{1}{u_{i+1}}$. □

[3] Merk op dat deze stelling geen uitspraken doet over of oplossingen van de vergelijking van Pell kunnen worden overgeslagen.

Stelling 7.7. *De t_i zijn de wijzergetallen van $\sqrt{A}$. Preciezer, $t_i = a_{i-1}$.*

Bewijs. We bewijzen dit met volledige inductie naar de wijzergetallen van $\sqrt{A}$. Merk op dat $t_1 = \lfloor\sqrt{A}\rfloor$. Merk ook op dat $\sqrt{A} = t_1 + (\sqrt{A} - \lfloor\sqrt{A}\rfloor) = t_1 + \frac{A-(\lfloor\sqrt{A}\rfloor)^2}{\sqrt{A}+\lfloor\sqrt{A}\rfloor}$. Uit de definities op bladzijde 67 volgt dat $\sqrt{A} = t_1 + \frac{B_1}{C_1+\sqrt{A}} = t_1 + \frac{1}{u_2}$.

Als $\sqrt{A} = [t_0; t_1, ..., t_{i-1} + u_i]$ volgt uit Stelling 7.6 dat $\sqrt{A} = [t_0; t_1, ..., t_i + u_{i+1}]$ □

We moeten nu ook nog laten zien dat beide stopcondities equivalent zijn, om zo te bewijzen dat de beide algoritmes tegelijk stoppen. Om dit te bereiken bewijzen we eerst het een en ander over de methode van Wallis en Brouncker.

Lemma 7.1. *Als $B_n = 1$, dan geldt dat $C_n = \lfloor\sqrt{A}\rfloor$ en $D_n = A - (\lfloor\sqrt{A}\rfloor)^2$.*

Bewijs. Stel $B_n = 1$. Volgens Stelling 5.1 geldt $B_n D_n + C_n^2 = A$, en volgens Stelling 5.3 geldt $D_n - 1 < 2C_n$. Uit $B_n = 1$ volgt $C_n^2 < A < C_n^2 + 2C_n + 1$, wat impliceert dat $C_n = \lfloor\sqrt{A}\rfloor$, $D_n = \frac{A-C_n^2}{B_n} = A - (\lfloor\sqrt{A}\rfloor)^2$. □

Gevolg 7.1. *Als je na $B_n = 1$ te hebben gevonden door zou gaan met het algoritme van Wallis en Brouncker zou gelden dat:*

- $t_{n+1} = \lfloor\lfloor\sqrt{A}\rfloor + \sqrt{A}\rfloor = 2\lfloor\sqrt{A}\rfloor$
- $B_{n+1} = -4\lfloor\sqrt{A}\rfloor^2 + 2 \cdot \lfloor\sqrt{A}\rfloor \cdot 2\lfloor\sqrt{A}\rfloor + A - (\lfloor\sqrt{A}\rfloor)^2 = A - (\lfloor\sqrt{A}\rfloor)^2 = B_1$
- $C_{n+1} = 2\lfloor\sqrt{A}\rfloor - \lfloor\sqrt{A}\rfloor = \lfloor\sqrt{A}\rfloor = C_1$
- $D_{n+1} = 1 = D_1$.

Omdat de $t_{n+2}, B_{n+2}, C_{n+2}, D_{n+2}$ alleen afhangen van $t_{n+1}, B_{n+1}, C_{n+1}, D_{n+1}$ hebben de betreffende rijen periode n.

Gevolg 7.2. *De n waarbij de methode van Wallis en Brouncker stopt (d.w.z. de kleinste even n waarvoor geldt dat $B_n = 1$) is dezelfde n die je vindt met de kettingbreuk-methode. Dit volgt uit het feit dat beide volledig worden bepaald door de reeks van t_i of a_i.*

Gevolg 7.3. *De oplossing (x_0, x_1) die je vindt met de methode van Wallis en Brouncker is een convergent $\frac{x_0}{x_1}$ van $\sqrt{A}$ die dus een beste benaderingsbreuk is. Als $x_0, x_1, x_2, ..., x_{n+1}$ de getallen zijn uit het algoritme van Wallis en Brouncker, zodat voor $0 < j \leqslant n$ geldt dat $x_{j-1} = t_j x_j + x_{j+1}$ en $x_n = 1, x_{n+1} = 0$, dan zijn $x_n, x_{n-1}, ...x_0$ opeenvolgende noemers van convergenten die gegenereerd worden door de 'afgeronde' kettingbreukontwikkeling van $\sqrt{A}$.*

We concluderen hieruit dat het Engelse algoritme en de kettingbreuk-methode op hetzelfde neerkomen: Wallis en Brouncker berekenen in feite de convergenten van $\sqrt{A}$, en gebruiken die voor het berekenen van (p_n, q_n) die een oplossing levert van de vergelijking van Pell; dit is dezelfde (p_n, q_n) die gevonden wordt door het kettingbreukalgoritme.

7.3 Het bewijs van Lagrange

Lagrange heeft in zijn Appendix bij het werk van Euler zelf een bewijs gegeven van de equivalentie van 'zijn' kettingbreukmethode en de methode van Wallis en Brouncker.[4] Interessant genoeg verwijst hij zelf wel degelijk naar deze twee wiskundigen in plaats van naar John Pell. Ondanks dat Lagrange ook de vertaler is van Eulers werk heeft hij het daar niet verbeterd of becommentarieerd. We zullen het bewijs hier verkort herhalen.

Net als wij heeft Lagrange eerder al bewezen[5] dat voor iedere geheeltallige oplossing (p, q) van $x^2 - Ay^2 = 1$ de breuk $\frac{p}{q}$ een convergent is van $\sqrt{A}$. Hij schrijft[6]:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{... + \cfrac{1}{a_i}}}}}$$

Hij eist hierbij dat de a_i onderafschattingen van de α_i zijn, net zoals Wallis en Brouncker eisen dat hun oplossingen altijd positief zijn.

Het is nu duidelijk dat $a_0 = \lfloor \frac{p}{q} \rfloor$, dat $a_1 = \lfloor \frac{q}{p \mod q} \rfloor$, enzovoorts, volgens het Euclidisch algoritme. In de notatie uit Hoofdstuk 5 schrijven we $x_0 = p$ en $x_1 = q$ en voor $1 < j \leqslant i$ schrijven we $x_j = x_{j-2} \mod x_{j-1}$. Dan geldt $a_j = \lfloor \frac{x_j}{x_{j+1}} \rfloor$. Het laatste positieve getal dat gegenereerd wordt door het Euclidisch algortime is x_{i+1}. Dit moet gelijk zijn aan 1 want, zo meldt ook Lagrange, p en q zijn copriem. Daarmee is a_i een geheel getal.

Omdat de wijzergetallen van $\sqrt{A}$ gelijk zijn aan de coëfficienten van de x_i in de Engelse methode kan Lagrange nu het werk van Wallis en Brouncker gebruiken om de kettingbreuk van $\sqrt{A}$ uit te rekenen, en dat is precies wat hij doet.

[4] Euler, *Algebra*, Additions Hoofdstuk 8.

[5] Euler, *Algebra*, Additions Hoofdstuk 2, Gevolg 4 op pagina 518

[6] Technisch gezien gebruikt Lagrange μ, μ', μ'' als variabelen in plaats van mijn a_i. Ik heb mijn eigen variabelen aangehouden om de verbanden met de rest van de scriptie duidelijk te maken.

De rest van zijn hoofdstuk besteedt Lagrange aan een opmerking dat de a_i ook bovenafschattingen zouden mogen zijn. Hij geeft een voorbeeld waarin, door eerst een bovenafschatting te kiezen en dan alleen maar onderafschattingen, een kettingbreuk wordt gegenereerd die alleen maar convergenten levert die geen oplossing geven voor $x^2 - Ay^2 = 1$. Hij schrijft deze opmerking toe aan Wallis, maar er is geen enkele aanwijzing waarom hij dit doet. Wallis maakt nergens in zijn uitgave van zijn correspondentie met Fermat (de *Commercium Epistolicum*) een dergelijke opmerking, en doet juist zijn best om al zijn oplossingen positief te houden.

Lagrange meldt dat de kettingbreuk van een wortel periodiek is in *Additions*, maar gebruikt dit niet in zijn bewijs. Uit zijn werk valt niet op te maken dat hij het verband ziet tussen de periode van de kettingbreuk van $\sqrt{A}$, en het aantal stappen dat gezet moet worden in de Engelse methode.

7.4 Een voorbeeld voor $A = 55$

Om het voorgaande hoofdstuk wat duidelijker te maken zal ik een voorbeeld geven voor $A = 55$.

Allereerst construeren we een oplossing voor $x^2 - 55y^2 = 1$ met de 'versimpelde' cirkelmethode. Het uitvoeren van het algoritme op bladzijde 47 levert de volgende reeks vergelijkingen:

- $1^2 - 55 \cdot 0^2 = 1$.
- $7^2 - 55 \cdot 1^2 = -6$.
- $15^2 - 55 \cdot 2^2 = 5$.
- $37^2 - 55 \cdot 5^2 = -6$.
- $89^2 - 55 \cdot 12^2 = 1$.

Alle variabelen staan in de volgende tabel, samen met de twee extra variabelen die we hebben gedefinieerd in hoofdstuk 7.

i	x_i	y_i	k_i	r_i	s_i	l_i	g_i
1	1	0	1	7	- 6	2	$\frac{\sqrt{55}+7}{6}$
2	7	1	-6	5	-30	2	$\frac{\sqrt{55}+5}{5}$
3	15	2	5	5	-30	2	$\frac{\sqrt{55}+5}{6}$
4	37	5	-6	7	- 6	14	$\frac{\sqrt{55}+7}{1}$
5	89	12	1	7	- 6	-	-

We hebben in Hoofdstuk 5.2 de methode van Wallis en Brouncker al toegepast op $x^2-55y^2=1$. We zullen de resultaten hier kort herhalen. We zoeken (x_0,x_1) zodat $x_0^2-55x_1^2=1$. We herschrijven dit een aantal keer.

$$\begin{array}{lrll} x_0^2-55x_1^2=1 & \text{is equivalent aan} & -6x_1^2+14x_1x_2+x_2^2=1 & \text{na} \quad x_0=7x_1+x_2,\\ & \text{is equivalent aan} & 5x_2^2-10x_2x_3-6x_3^2=1 & \text{na} \quad x_1=2x_2+x_3,\\ & \text{is equivalent aan} & -6x_3^2+10x_3x_4+5x_4^2=1 & \text{na} \quad x_2=2x_3+x_4,\\ & \text{is equivalent aan} & x_4^2-14x_4x_5-6x_5^2=1 & \text{na} \quad x_3=2x_4+x_5. \end{array}$$

We vullen nu voor (x_4,x_5) de getallen $(1,0)$ in, en berekenen daarmee x_3,x_2,x_1, en x_0

Op bladzijde 64 schrijven we de vergelijkingen als $B_ix_i^2-2C_ix_ix_{i+1}-D_ix_{i+1}=(-1)^i$ en de substituties als $x_i=t_{i+1}x_{i+1}+x_{i+2}$. We zetten al deze variabelen samen met de in Hoofdstuk 7.2 gedefinieerde u_i in een tabel.

i	x_i	t_i	B_i	C_i	D_i	u_i
0	89	-	1	0	55	$\frac{\sqrt{55}+0}{1}$
1	12	7	6	7	1	$\frac{\sqrt{55}+7}{6}$
2	5	2	5	5	6	$\frac{\sqrt{55}+5}{5}$
3	2	2	6	5	5	$\frac{\sqrt{55}+5}{6}$
4	1	2	1	7	6	$\frac{\sqrt{55}+7}{1}$

Tot slot hebben we de kettingbreukontwikkeling van $\sqrt{55}$. Volgens het voorbeeld op bladzijde 82 geldt $\sqrt{55}=[7;\overline{2,2,2,14}]$. Ook hier kunnen we een tabel maken van de variabelen.

i	a_i	b_i	c_i	α_i	$\frac{1}{\alpha_i}$	p_i	q_i
0	7	-	-	-	-	1	0
1	2	7	1	$\frac{\sqrt{55}-7}{1}$	$\frac{\sqrt{55}+7}{6}$	7	1
2	2	5	6	$\frac{\sqrt{55}-5}{6}$	$\frac{\sqrt{55}+5}{5}$	15	2
3	2	5	5	$\frac{\sqrt{55}-5}{5}$	$\frac{\sqrt{55}+5}{6}$	37	5
4	14	7	6	$\frac{\sqrt{55}-7}{6}$	$\frac{\sqrt{55}+7}{1}$	89	12

Met behulp van deze overzichten kunnen we de stellingen uit dit hoofdstuk illustreren.

Stelling 7.3 zegt dat de getallen l_i en g_i uit de 'versimpelde' cirkelmethode gelijk zijn aan respectievelijk de getallen a_i en $\frac{1}{\alpha_i}$ uit de kettingbreukontwikkeling van $\sqrt{A}$. Dit is in het voorbeeld te controleren.

Stelling 7.7 zegt dat de getallen t_i uit de methode van Wallis en Brouncker gelijk zijn aan de getallen a_i uit de kettingbreukontwikkeling van $\sqrt{A}$. Dit is

ook in het voorbeeld te controleren.

Naast deze twee stellingen kunnen we nog meer identiteiten vinden, zoals $|k_i|$ (cirkelmethode) $= D_i$ (engelse methode) $= c_i$ (kettingbreukontwikkeling) voor $i > 0$, en r_i (cirkelmethode) $= C_i$ (engelse methode) $= b_i$ (kettingbreukontwikkeling) voor $i > 0$. Merk ook op dat de reeks van getallen x_i uit de Engelse methode overeenkomt met de *omgekeerde* reeks y_i uit de 'versimpelde' cirkelmethode (op x_0 na), en dat de paren (x_i, y_i) uit de 'versimpelde' cirkelmethode gelijk zijn aan de convergenten (p_i, q_i) die geconstrueerd worden uit de kettingbreukontwikkeling van $\sqrt{A}$.[7]

Deze en andere identiteiten kunnen zonder veel moeite bewezen worden met behulp van Stellingen 7.3 en 7.7 en de definities van de getallen l_i, c_i (cirkelmethode) en u_i (Engelse methode).

[7] Zoals opgemerkt op bladzijde 90

Hoofdstuk 8

Diverse onderwerpen

8.1 Onderzoek aan de Pellvergelijking na Lagrange

Na het werk van Lagrange zijn er meer ontdekkingen gedaan op het gebied van de vergelijking van Pell. Ik noem daarvan slechts twee belangrijke.

De eerste komt van C.F. Gauss, die in zijn behandeling van $x^2 - Ay^2 = m^2$ gebruikt maakt van de eigenschappen van tripels (A, B, C) om kwadratische functies te beschrijven. Het bewijs in Hoofdstuk 5 dat de methode van Wallis en Brouncker werkt is gebaseerd op dit werk. Gauss beschrijft hier de 'gereduceerde tripels' voor het eerst, hoewel ik niet zeker weet of hij de term ook gebruikt.

In 1837 ontdekken de wiskundigen C.G.J. Jacobi en J.P.G.L. Dirichlet onafhankelijk van elkaar dat de vergelijking van Pell op te lossen is met behulp van de theorie van cyclotomische lichamen. Ik zal de rest van deze sectie besteden aan een uitleg van hoe dit werkt.[1] Kennis van algebra (voornamelijk het begrip 'lichaamsuitbreiding') is noodzakelijk om dit te kunnen volgen.

Definitie: Een *getallenlichaam* is een eindige uitbreiding van het lichaam $\mathbb{Q}$ van rationale getallen. Een *getallenring* is een deelring van een getallenlichaam.

De getallenringen waarin wij geïnteresseerd zijn zijn $\mathbb{Z}[\sqrt{A}] = \{a + b\sqrt{A} : a, b \in \mathbb{Z}\}$. In een dergelijke ring geldt $x^2 - Ay^2 = (x + \sqrt{A}y)(x - \sqrt{A}y)$, en hoeven we dus alleen $(x + \sqrt{A}y)(x - \sqrt{A}y) = 1$ op te lossen. Iedere oplossing van de

[1] Deze uitleg is gebaseerd op het dictaat *Number Rings* van P.Stevenhagen. De vergelijking van Pell wordt behandeld op bladzijde 4.

vergelijking van Pell voor A levert dus een eenheid in de ring $\mathbb{Z}[\sqrt{A}]$.

We bekijken de norm-functie $N : \mathbb{Z}[\sqrt{A}] \to \mathbb{Z}$, gedefinieerd door $N(a+b\sqrt{A}) = (a+b\sqrt{A})(a-b\sqrt{A}) = a^2 - Ab^2$. Het is eenvoudig te bewijzen dat $N(xy) = N(x)N(y)$ voor $x, y, \in \mathbb{Z}[\sqrt{A}]$. De norm is een geheel getal, dus eenheden van $\mathbb{Z}[\sqrt{A}]$ hebben een norm van ± 1. De functie N geeft dan ook een homomorfisme tussen deze twee groepen. Een element $a+b\sqrt{A}$ met norm 1 levert getallen a, b zodat $a^2 - Ab^2 = 1$, en een element met norm -1 levert getallen a, b zodat $a^2 - Ab^2 = -1$. Er zijn dus eenheden die geen oplossing voor de vergelijking van Pell zelf leveren.

Op deze manier wordt het oplossen van ons getaltheoretisch probleem gereduceerd tot het vinden van de goede eenheden in een algebraische lichaamsuitbreiding. Het is aan te tonen dat er altijd een eenheid bestaat die overeenkomt met een oplossing van de vergelijking van Pell, en zelfs dat dit zo kan dat deze eenheid samen met -1 de hele groep $\mathbb{Z}[\sqrt{A}]^*$ genereert.[2]

8.2 $x^2 - Ay^2 = k, k \neq 1$

De vergelijking van Pell laat zich gemakkelijk generaliseren naar wat we eerder een 'Pell-achtige' vergelijking hebben genoemd: de vergelijking $x^2 - Ay^2 = k$, voor een gegeven geheeltallige A en k. In tegenstelling tot A hoeft k niet positief te zijn.[3]

We hebben eerder in stelling 6.2 gezien dat als $|k| < \sqrt{A}$ iedere oplossing van $x^2 - Ay^2 = k$ een convergent is van $\sqrt{A}$. We zullen laten zien dat we gegeven een oplossing van $x^2 - Ay^2 = 1$ (die we inmiddels hebben) oplossingen kunnen construeren voor $x^2 - Ay^2 = k$, of dat we kunnen aantonen dat er geen oplossing bestaat. Om te beginnen kunnen we bewijzen dat het mogelijk is om oplossingen $x_1^2 - Ay_1^2 = k_1$ en $x_2^2 - Ay_2^2 = k_2$ samen te stellen tot een nieuwe oplossing $x_3^2 - Ay_3^2 = k_3$.

Stelling 8.1. *Stel dat voor x_i, y_i, k_i en A positief en geheel, A geen kwadraat geldt dat $x_1^2 - Ay_1^2 = k_1$ en $x_2^2 - Ay_2^2 = k_2$. Definieer nu $x_3 = x_1x_2 + Ay_1y_2$, $y_3 = x_1y_2 + x_2y_1$. Dan geldt dat $x_3^2 - Ay_3^2 = k_1k_2$.*

Bewijs. We kunnen dit makkelijk bewijzen met behulp van de hierboven gedefiniëerde normfunctie. Het is duidelijk dat $x_3 + y_3\sqrt{A} = (x_1 + y_1\sqrt{A})(x_2 + y_2\sqrt{A})$. De normeigenschap zegt nu dat $N(x_3 + y_3\sqrt{A}) = N(x_1 + y_1\sqrt{A})N(x_2 + y_2\sqrt{A}) = k_1k_2$.

[2] Zie opgaven 9-11 in Hoofdstuk 1 van het dictaat van Stevenhagen.

[3] De wiskunde in deze sectie is gebaseerd op het dictaat *Getaltheorie* van R.Tijdeman, bladzijde 49-51.

□

Als we dus een oplossing zoeken voor en bepaalde k, en we hebben oplossingen voor de elementen van een ontbinding van k, dan kunnen we de nieuwe oplossing direct berekenen.

Nog een mooi gevolg is dat als we een oplossing hebben van $x^2 - Ay^2 = k$ en een oplossing voor $x^2 - Ay^2 = 1$ we oneindig veel nieuwe oplossingen voor $x^2 - Ay^2 = k$ kunnen maken door herhaaldelijk oplossingen samen te stellen met de oplossing voor $k = 1$. We kunnen op deze manier zelfs alle oplossingen van een Pell(-achtige) vergelijking vinden als we beginnen met de fundamenaaloplossing (x_0, y_0).

Stelling 8.2. *Zij A een geheel getal, geen kwadraat. Dan is een paar (x, y) een oplossing voor $x^2 - Ay^2 = 1$ dan en slechts dan er een $n \in \mathbb{Z}$ bestaat zodat $x + y\sqrt{A} = \pm(x_0 + y_0\sqrt{A})^n$.*

Bewijs. Eerst bewijzen we dat al deze (x, y) daadwerkelijk oplossingen zijn. Als (x_0, y_0) de fundamentaaloplossing is heeft $x_0 + y_0\sqrt{A}$ norm 1. Volgens Stelling 8.1 hebben alle machten van $x_0+y_0\sqrt{A}$ ook norm 1, en volgens Sectie 8.1 is iedere (x, y) waarvoor geldt dat $x+y\sqrt{A} = \pm(x_0+y_0\sqrt{A})^n$ dan een oplossing van de Pellvergelijking.

Rest te bewijzen dat *iedere* oplossing (x, y) van de gevraagde vorm is. Hiertoe merken we eerst twee feiten op over deze oplossingen (x, y):

- $x + y\sqrt{A} = 1 \iff x = 1, y = 0.$
- $x + y\sqrt{A} > 1 \iff x > 0, y > 0.$

De eerste bewering is direct duidelijk. De tweede bewering is gemakkelijk af te leiden:

- Als $x > 0, y < 0 \to x - y\sqrt{A} > 1 \to x + y\sqrt{A} = (x - y\sqrt{A})^{-1} < 1$
- Als $x \leqslant 0, y > 0 \to x - y\sqrt{A} < 0 \to x + y\sqrt{A} < 0$
- Als $x \leqslant 0, y < 0 \to x + y\sqrt{A} < 0$

Zij (x_0, y_0) de fundamentaaloplossing. Dan volgt uit de minimaliteit van de fundamentaaloplossing en de feiten hierboven dat er geen oplossingen (x, y) bestaan zodat $1 < x + y\sqrt{A} < x_0 + y_0\sqrt{A}$. Verder geldt dat $x_0 - y_0\sqrt{A} = (x_0 + y_0\sqrt{A})^{-1}$.

Zij (x', y') een willekeurige andere oplossing van $x^2 - Ay^2 = 1$. Mocht het zo zijn dat $x' + y'\sqrt{A} < 0$, dan kiezen we de oplossing $(-x', -y')$; we mogen dus aannemen dat $x' + y'\sqrt{A} > 0$. Kies $n \in \mathbb{Z}$ zó dat $(x_0 + y_0\sqrt{A})^n \leqslant x' + y'\sqrt{A} < (x_0 + y_0\sqrt{A})^{n+1}$. Definiëer nu de oplossing (x'', y'') door $x'' + y''\sqrt{A} = (x + y\sqrt{A})(x_0 - y_0\sqrt{A})^n$. Nu geldt dat $1 \leqslant x'' + y''\sqrt{A} < x_0 + y_0\sqrt{A}$, en dus volgens de gemaakte opmerking $x'' + y''\sqrt{A} = 1$. Daaruit volgt $x'' = 1, y'' = 0$. Dus $x' + y'\sqrt{A} = \frac{1}{(x_0 - y_0\sqrt{A})^n} = (x_0 + y_0\sqrt{A})^n$.

□

Alle oplossingen van de vergelijking van Pell zijn dus terug te voeren op de fundamentaaloplossing. De claim van Wallis dat hij alle mogelijke antwoorden kon geven blijkt dus te kloppen. Wallis zelf heeft echter nooit meer gedaan dan de losse opmerking maken 'dat hij door vermenigvuldiging alle oplossingen zou kunnen vinden'; een degelijk bewijs heeft hij nooit geleverd.

We kunnen op eenzelfde manier alle oplossingen van $x^2 - Ay^2 = k$ karakteriseren. Gegeven dat we voor een zekere k alle oplossingen hebben die kleiner zijn dan de fundamentaaloplossing van $x^2 - Ay^2 = 1$ kunnen we een formule geven waaraan alle oplossingen voor de gevraagde k aan moeten voldoen. Iedere uitkomst van de formule is dan ook zo'n oplossing. Merk op dat nergens een methode wordt gegeven om alle oplossingen kleiner dan de fundamentaaloplossing te genereren, en dat dit dus geen algoritme is.

Stelling 8.3. *Zij A een natuurlijk getal, geen kwadraat en $k \in \mathbb{Z}$, $k \neq 0$. Stel $(a_1, b_1), (a_2, b_2), ..., (a_l, b_l)$ zijn de oplossingen van $x^2 - Ay^2 = k$ waarvoor geldt dat $1 \leqslant a_i + b_i\sqrt{A} < x_0 + y_0\sqrt{A}$ (waarbij (x_0, y_0) de fundamentaal oplossing is). Dan is elke oplossing van $x^2 - Ay^2 = k$ op precies één manier te schrijven als $a + b\sqrt{A} = \pm(a_i + b_i\sqrt{A})(x_0 + y_0\sqrt{A})^n$, $n \in \mathbb{Z}$. Tevens zijn alle (a, b) die hieraan voldoen oplossingen.*

Bewijs. Omdat we a en b positief kunnen kiezen mogen we veronderstellen dat $a + b\sqrt{A} > 0$. Kies $n \in \mathbb{Z}$ zó dat $(x_0 + y_0\sqrt{A})^n \leqslant a + b\sqrt{A} < (x_0 + y_0\sqrt{A})^{n+1}$
Dan volgt dat $1 \leqslant (a + b\sqrt{A})(x_0 - y_0\sqrt{A})^n < (x_0 + y_0\sqrt{A})$. Dus $(a + b\sqrt{A})(x_0 - y_0\sqrt{A})^n = (a_i + b_i\sqrt{A})$ voor een zekere i. Hieruit volgt dat $a + b\sqrt{A} = (a_j + b_j\sqrt{A})(x_0 + y_0\sqrt{A})^n)$.
Deze representatie is éénduidig, omdat $a_j + b_j\sqrt{A} = (a_i + b_i\sqrt{A})(x_0 + y_0\sqrt{A})^n$ en $1 \leqslant a_i + b_i\sqrt{A} < x_0 + y_0\sqrt{A}$, $1 \leqslant a_j + b_j\sqrt{A} < x_0 + y_0\sqrt{A}$ impliceren dat $n = 0$, en dus moet gelden dat $a_j = a_i, b_j = b_i$.
Volgens stellingen 8.1 en 8.2 zijn alle paren (a, b) die we op deze manier kunnen maken geldige oplossingen van $x^2 - Ay^2 = k$. □

Opmerking 8.1. *Als $|k| < \sqrt{A}$ kunnen we (a_i, b_i) bepalen met behulp van de methoden uit Hoofdstuk 6.3.*

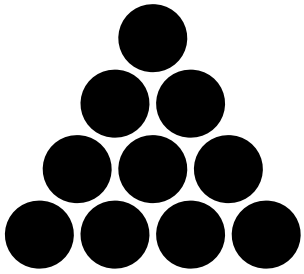
Zoals we gezien hebben in hoofdstuk 4 was Brahmagupta al in staat uit oplossingen van 'Pell-achtige' vergelijkingen nieuwe oplossingen te maken, op dezelfde manier als in stelling 8.1. Oplossingen voor $k = \pm 1, \pm 2$ of ± 4 leveren zelfs een manier om een antwoord op $x^2 - Ay^2 = 1$ te geven. Van Brahmagupta zijn ook werken gevonden waarin hij $x^2 - Ay^2 = k$ uitvoerig behandelt.

Wallis en Brouncker claimen in eerste instantie $x^2 - Ay^2 = k$ op te kunnen lossen voor willekeurige k en A, maar hebben het dan nog over een oplossing in rationale getallen. Als eenmaal duidelijk is dat de oplossing geheeltallig moet zijn, schrijven ze er niet meer over. Fermat zelf laat de optie $k \neq 1$ geheel links liggen, en schrijft er (voor zover we weten) nergens over.

Bijlage A

Gebruikte notatie en uitleg van termen

- $|a|$: de absolute waarde van a. Dat wil zeggen: a als $a \geqslant 0$, $-a$ als $a < 0$.
- $a|b$: a deelt b.
- a, b copriem: de grootste gemene deler van a en b is 1, oftewel er bestaat geen getal groter dan 1 dat èn a èn b deelt.
- $a := 2b$: definiëer a als $2b$.
- $a \equiv b \bmod c$. ("a is equivalent aan b modulo c"). De rest na deling van a door c is gelijk aan de rest na deling van b door c. Een voorbeeld is $8 \equiv 3 \bmod 5$.
- (B, C, D) is gereduceerd: $|B - D| < 2C$.
- Een positief geheel getal a is een driehoeksgetal als er een positieve geheeltallige n bestaat zodat $a = \frac{1}{2}n(n+1)$. Dan is a te schrijven als de som van de getallen 1 tot en met n. Als a een driehoeksgetal is, zijn a knikkers altijd precies in een gelijkzijdige driehoek neer te leggen. Zie het onderstaande plaatje voor $a = 10 = 1 + 2 + 3 + 4$.



Bijlage B

Bibliografie

Voor het schrijven van deze scriptie heb ik gebruik gemaakt van veel primaire en secundaire literatuur, die ik hier per onderwerp zal bespreken. Boeken zijn in het Engels, tenzij anders aangeduid.

B.1 Algemeen

Edwards, H. M. - *Fermat's last theorem, a genetic introduction to algebraic number theory*
Springer Verlag, New York etc., 1977 Hoofdstuk 1.9

- Dit boek behandeld algebraïsche getaltheorie op een historische wijze. Hoofdstuk 1.9 bevat een uitgebreide behandeling van de vergelijking van Pell, inclusief een vergelijking van de cirkelmethode met de Engelse methode (hoewel die laatste niet in haar oorspronkelijke vorm wordt gegeven). De opgaven aan het eind van dit hoofdstuk zijn gebruikt voor de bewijzen in Hoofdstuk 4.5.

Gillespie, C. C. & Holmes, F. L. (Editors in chief) - *Dictionary of Scientific Biography* Scribner, New York, 1970-1990

- Het belangrijkste overzicht van historische wetenschappers.

Konen, H. - *Geschichte der Gleichung* $t^2 - Du^2 = 1$
Verlag von S. Hirzel, Leipzig, 1901

- Dit is een historische behandeling van de geschiedenis van de vergelijking van

Pell, inclusief de Griekse, Indiase en Engelse oplossingen. Ook besteedt Konen uitgebreid aandacht aan de behandeling van het probleem *na* de oplossing van Lagrange door onder andere Gauss en Dirichlet. Het boek richt zich voornamelijk op de wiskundige details, en minder op de historische context. Geschreven in het Duits.

Ore, O - *Number Theory, and its History*
McGraw-Hill, New York etc., 1948

- Compact boek over de geschiedenis van de getaltheorie, geordend per onderwerp. Dit is een goed referentiewerk, voornamelijk door de uitgebreide bibliografie. De vergelijking van Pell wordt niet met naam genoemd, zodat het nut van dit boek met betrekking tot deze scripte beperkt is.

Weil, A - *Number Theory, an Approach though History*
Birkhäuser, Boston, 1983

- Dit boek behandelt naar eigen zeggen de geschiedenis van de getaltheorie 'From Hammurapi to Legendre'. Het is zeer compleet, maar slechts in grote lijnen uitgewerkt, en laat veel over aan de lezer. De indeling is niet helemaal logisch, vooral het eerste hoofdstuk springt van de ene naar de andere tijdsperiode.

Young, L - *Mathematicians and their times*
North-Holland, Amsterdam etc., 1981

- In theorie een overzicht van historische wiskundigen en de tijd waarin ze leefden, in de praktijk voornamelijk gevuld met meningen van de auteur in plaats van feitelijke informatie.

B.2 Griekse wiskunde

Amthor, A. en Rumbiegel, B.K. - *Das Problema Bovinum des Archimedes*
Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik 25, 121-136, 153-171. Leipzig, 1880

- Het werk waarin Amthor een afschatting geeft van de grootte van de oplossing van het 'veestapelprobleem'.

Bergh, P. - Seiten und Diametralzahlen bei den Griechen
Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik 31
Leipzig, 1886

- Bevat uitleg over de 'zijdegetallen' en 'diagonaalgetallen' in oud Grieks werk.

Ik heb dit artikel niet zelf ingezien, maar de gegevens (en het plaatje) overgenomen uit Konen, *Geschichte der Gleichung* $t^2 - Du^2 = 1$.

Heath, T.H. - *Diophantus of Alexandria - a study in the history of Greek algebra*
Cambridge University Press, Cambridge (UK), 1910

- Behandelt Diophantus' leven en de eerste vijf boeken van zijn *Arithmetica* in detail, en bevat een beschijvinng van wat er later met Diophantus' werk is gedaan door onder andere Fermat en Euler.

Thomas, I - *Greek mathematical works*
Harvard University Press, Cambridge (USA), 1968
Volume II

- Behandelt diverse Griekse wiskunde. Ik heb dit boek alleen gebruikt om het 'veestapelprobleem' uit te vertalen.

B.3 Indiase wiskunde

Brahmegupta (sic) **and Bhaskara** - *Algebra with arithmetic and mensuration*
(vertaald door H. T. Colebrooke)
John Murray, London, 1817 (onveranderde herdruk uit 1973, uitgegeven door Walluf bei Wiesbaden)

- Vertaling van selecte stukken van het werk van Brahmagupta en Bhaskara, inclusief commentaar daarop van latere Indiase wiskundigen. Dit boek is vrij moeilijk te lezen, omdat de Indiase notatie zo ver van de onze af staat. Alle directe citaten in hoofstuk 4 zijn vertaald uit dit boek.

B.4 Engelse wiskunde

Fermat, P. de - *Oeuvres de Fermat (publ. par Paul Tannery et Charles Henry)*
Parijs, 1891-1922
Delen 2 en 3

- Fermat's volledig werk bevat niet alleen zijn correspondentie met Wallis en Brouncker, maar ook alle brieven die tussen Brouncker, Wallis en Digby zijn geschreven. Deze twee delen zijn de bron van alle citaten in Hoofdstuk 5. Geschreven in het Frans en Latijn (alle brieven in het Latijn staan vertaald naar

het Frans in Deel 3).

Mahoney, M.S. - *The Mathematical career of Pierre de Fermat*
Princeton University Press, Princeton, 1973

- Uitgebreide biografie van Fermat, met bijzonder veel wiskunde voor een biografie. Bevat een uitstekende inleiding over zeventiende eeuwse wiskunde, en de wiskundigen die invloed hadden op Fermat.

Wallis, J - *The correspondence of John Wallis* (editors P. Beeley en C. J. Scriba)
Oxford university Press, New York, 2003
Volume I

- Bevat alle correspondentie van Wallis. Bijna alle brieven zijn in het Latijn (een enkele is in het Engels). Alle brieven met betrekking tot de uitdagingen van Fermat staan ook in diens *Oeuvres*.

B.5 Lagrange en verder

Euler, L - *Elements of algebra* (vertaald door Rev. J. Hewlett)
Springer Verlag, New York etc, 1972

- *Elements of algebra* bevat zowel Eulers samenvatting van het werk van Wallis en Brouncker, als een appendix van Lagrange. In Eulers samenvatting legt hij duidelijk uit dat het afschatten in Wallis' methode gedaan kan worden met de wortelformule. In zijn appendix legt Lagrange uit hoe kettingbreuken werken, toont hij voor het eerst het verband tussen kettingbreuken en de vergelijking van Pell aan, en bewijst hij dat deze vergelijking met behulp van kettingbreuken op te lossen is. Daarnaast is dit het geschrift waarin voor het eerst wordt bewezen dat de vergelijking van Pell voor iedere positieve niet-kwadratische A een oplossing heeft.

Virey, J - *Précis historique sur la vie et la mort de Joseph-Louis Lagrange*
Parijs, 1813

- Korte (20 pagina's) biografie van Lagrange. Bevat uitgebreide feitelijke data, maar is tamelijk ophemelend.

B.6 Modern werk

Lenstra, H W - Solving the Pell Equation
Notices of the American Mathematical Society, vol 49, Number 2, pg. 182-192

- Een behandeling van de vergelijking van Pell in moderne wiskunde, die zich richt op een zo snel mogelijke oplossing. Bevat ook een stuk over het 'cattle problem' van Archimedes.

Stevenhagen, P - *Number Rings*
Mathematisch Instituut Leiden, 2000

- Dictaat bij het vak 'Algebraïsche Getaltheorie'. Het eerste hoofdstuk behandelt het oplossen van de vergelijking van Pell met behulp van lichamen.

Tijdeman, R - *Collegedictaat Getaltheorie*
Mathematisch Instituut Leiden, 2000

- Aantekeningen bij het vak Getaltheorie. Bevat hoofdstukken over kettingbreuken en de moderne methode om kettingbreuken op te lossen. Veel van het werk in hoofdstuk 6 is hierop gebaseerd.

Index