Radboud Universiteit Nijmegen

Geschikte Getallen

Bachelorscriptie Wiskunde

Auteur: Erik Mulder

Studentnummer: s4628640

Begeleider: Dr. Wieb Bosma

Tweede lezer: Dr. Arne Smeets

Juli 2018

Inhoudsopgave

Abstract

Euler maakte gebruik van zogeheten geschikte getallen, want hij kon er grote priemgetallen mee vinden. Onlangs heeft Hagedorn laten zien dat de geschikte getallen ook vanuit een heel ander oogpunt bekeken kunnen worden. Hij geeft namelijk een meetkundige invalshoek, waar hij gebruik maakt van een resultaat van Minkowski over convexe verzamelingen. Gauss kwam ook de geschikte getallen tegen, namelijk in zijn werk over binaire kwadratische vormen, en in het bijzonder de geslachtstheorie. Tot slot laten we zien dat er een verband is tussen het aantal klassen in een genus bij een vaste discriminant, en of een getal geschikt is of niet.

1 Inleiding

Rond 1778 had Euler een manier gevonden om door middel van getallen met een specifieke eigenschap grote priemgetallen te vinden. Niet elk getal heeft deze eigenschap, daarom noemde hij ze *numeri idonei*, oftewel geschikte getallen (idoneal numbers in het Engels).
Hieronder geven we een definitie die veel lijkt op die van Euler. In welke zin, en waarom deze definitie verschilt van die van Euler, gaan we straks verder op in.

Definitie 1.1 Een geheel getal $n \geq 1$ heet *geschikt* als de volgende uitspraak waar is: als $m \in \mathbb{N}_{>1}$ te schrijven is als $m = x^2 + ny^2$ met m oneven, $\text{ggd}(x, ny) = 1$, en bovendien de vergelijking $m = a^2 + nb^2$ precies één oplossing heeft met $a, b \in \mathbb{Z}_{\geq 0}$, dan is m een priemgetal.

Dit is al direct een rare definitie, dus laten we eerst eens goed kijken wat er staat.

Voorbeeld 1.2
Stel dat we weten dat $n = 2$ een geschikt getal is. Bekijk dan bijvoorbeeld $17 = 3^2 + 2 \cdot 2^2$. We zien dat $\text{ggd}(3, 4) = 1$, en bovendien zien we door andere waarden van $x, y \in \mathbb{Z}_{\geq 0}$ in te vullen dat $x = 2$ en $y = 3$ de enige oplossing van de vergelijking $m = x^2 + ny^2$ is. Dat laatste gaat redelijk snel, omdat x en y in ieder geval begrensd worden door $0 < x, y < \sqrt{17}$. De definitie van een geschikt getal geeft ons nu dat 17 een priemgetal is, en dat lijkt te kloppen!

We bekijken nog een voorbeeld om een subtiliteit aan te duiden. Stel dat we nog steeds weten dat $n = 2$ een geschikt getal is. Dan is $m = 27$ op een unieke manier te schrijven als $m = x^2 + 2y^2$, *met* $\text{ggd}(x, 2y) = 1$, namelijk door $x = 5$ en $y = 1$ te nemen. Maar 27 is duidelijk geen priemgetal. Dit is gelukkig niet in strijd met de definitie, want de vergelijking $m = a^2 + 2b^2$ heeft namelijk nog wel een extra oplossing: $a = 3$, $b = 3$. Nu geldt natuurlijk niet dat $\text{ggd}(a, 2b) = 1$, maar voor a en b eisen we dat ook niet, dus is er geen tegenspraak.

Een voor de hand liggende vraag is nu: hoe bepaal je of een getal n geschikt is of niet? In deze scriptie gaan we deze vraag via verschillende invalshoeken proberen te beantwoorden. Euler was de eerste die een definitie gaf van een geschikt getal, dus laten we eerst kijken wat hij er mee deed.

Zoals al eerder was aangeven, was de oorspronkelijke definitie van Euler iets anders dan de bovenstaande definitie. De reden daarvoor is dat zijn definitie eigenlijk niet erg duidelijk is, Steinig [16] heeft dit geprobeerd op te helderen. Eulers definitie is een variant op Definitie 1.1, hij eist namelijk niet dat m oneven moet zijn, en ook niet dat $\text{ggd}(m, n) = 1$. Hierdoor hoeft m niet per se priem te zijn, ook al voldoet hij mogelijk wel aan de andere eisen van de definitie.
Het verwarrende is nu dat Euler in die situatie nog steeds beweert dat m een priemgetal moet zijn. Echter, hierboven zien we dat dat duidelijk niet waar is. Euler had dit ook in de gaten, en hij loste dit probleem op door simpelweg een andere definitie te geven van een priemgetal. Om het nog ingewikkelder te maken, gebruikte hij soms ook weer varianten op deze definitie. Een definitie die Euler gaf voor een priemgetal (met betrekking tot $x^2 + ny^2$), is dat het van de vorm tp^r is, met $r \in \mathbb{N}$, $t \mid 2n$ en p een priemgetal, zoals wij die kennen. Steinig [16] liet zien dat het voldoende is om alle getallen van de vorm tp, tp^2 of $t2^r$, met $t \mid 2n$, te zien als priemgetallen (met betrekking tot $x^2 + ny^2$).

Als we nu wel weer eisen dat m oneven moet zijn, dan houden voor m we de mogelijkheden $t'p$, $t'p^2$ en $t'2^0$ over, met $t' \mid n'$, waar $p > 2$ en n' het oneven deel van n is. Als we nu ook weer de eis $\text{ggd}(x, ny) = 1$ erbij nemen, dan houden we alleen nog de gevallen $m = p$ en $m = p^2$

over ($m > 1$). We hoeven nu alleen nog in te zien dat $m = p^2$ niet kan. Stel dat m is schrijven is als $m = x^2 + ny^2 = p^2$ met $\text{ggd}(x, ny) = 1$. Merk nu op dat door $a = p$ en $b = 0$ te nemen, we ook een oplossing krijgen voor de vergelijking $m = a^2 + nb^2$. Dit is een andere oplossing dan de eerste, omdat voor deze oplossing geldt dat $\text{ggd}(a, nb) \neq 1$. Dus heeft de vergelijking geen unieke oplossing, en kunnen we het geval $m = p^2$ ook uitsluiten.
We concluderen dat $m = p$ de enige mogelijkheid die overblijft als m oneven is, $\text{ggd}(x, ny) = 1$, en vergelijking $m = a^2 + nb^2$ een unieke oplossing heeft. Nu zijn we waar we willen, want dit is precies Definitie 1.1.

Het is op zich fijn dat, alhoewel Euler niet helemaal precies was, we toch nog in principe met zijn definitie kunnen werken. Een mogelijke reden voor de slordigheid van Euler is dat hij toentertijd al elf jaar blind was. Hij deed veel van zijn werk samen met assistenten, die bijvoorbeeld brieven voor hem schreven en oplazen. Ondanks dat zijn gezichtsvermogen achteruit ging, ging zijn productiviteit juist omhoog. Of beter gezegd, in de woorden van Euler zelf: "Nu zal ik minder afleiding hebben." (Euler's Gem [15]).

We hebben nu alleen nog geen antwoord gegeven op de vraag hoe Euler bepaalde of een getal n geschikt is of niet. Mogelijk komt dit doordat Eulers methode weer in het thema past van "niet erg nauwkeurig zijn". Euler gebruikte een "criterium" , zonder een sluitend bewijs te geven, en bovendien is het nog niemand in de tussentijd gelukt om het te bewijzen. Euler kreeg met dit criterium wel dezelfde getallen als andere wiskundigen (zoals Gauss), die methoden gebruikten die wel bewezen zijn. Eulers intuïtie lijkt dus wel te kloppen, maar of het onderstaande criterium waar is voor alle getallen n, is nog een open probleem.

Criterium 1.3 (Euler) *Een geheel getal $n \geq 1$ is geschikt dan en slechts dan als we voor alle $0 < k < \sqrt{3n}$ met $ggd(k, n) = 1$ hebben dat $n + k^2 = p$, p^2, $2p$ of 2^s, waar p een oneven priemgetal is (in de standaard definitie) en $s \in \mathbb{N}_{>1}$.*

Grube [8, p. 497-503] bekritiseerde Eulers "bewijs" en corrigeerde het deels. Grube kon wel laten zien dat een geschikt getal n altijd aan de bovenstaande eis voldoet, maar de omkering kon hij niet bewijzen.

Grube [8, p. 510,511] gaf ook twee alternatieve criteria, samen met een bewijs. Deze criteria geven we hieronder, maar voor een bewijs verwijzen we naar Kani [11, p. 9].

Criteria 1.4 (Grube)

a. *Een geheel getal $n \geq 1$ is geschikt dan en slechts dan als voor alle $0 < k < \sqrt{\frac{n}{3}}$ en voor elke factorisatie*
$$n + k^2 = ac, \quad \text{waar } c \geq a \geq 2k,$$
geldt dat $a = c$ of $a = 2k$.

b. *Stel dat $n \geq 1$ kwadraatvrij is en $n \neq 3, 7, 15$. Dan is n geschikt dan en slechts dan als voor alle $0 < k < \sqrt{\frac{n}{3}}$ geldt dat $n + k^2 = tp$, tp^2, of $2tp$, waar p een oneven priemgetal is en $t \mid n$.*

Kani heeft de criteria van Euler en Grube ook in zijn artikel staan, maar maakt bij die van Euler wel een fout. Hij zegt namelijk dat de eis van Criterium 1.3 voor alle $0 < k < \sqrt{\frac{n}{3}}$ nagegaan moet worden, de verwarring komt waarschijnlijk doordat dat bij de criteria van Grube dat wel het geval is.

In deze scriptie gaan we de geschikte getallen vanuit meerdere oogpunten bekijken. Deze verschillende invalshoeken geven ook verschillende manieren om de geschikte getallen te karakteriseren. In tegenstelling tot de criteria van Grube, gaan we die andere karakterisaties wel (grotendeels) bewijzen.

Euler kon dus met de geschikte getallen grote priemgetallen vinden. In het volgende hoofdstuk gaan we kort bekijken hoe hem dat dan lukte, daarna bekijken een aantal rekenkundige uitspraken over de geschikte getallen.

2 Rekenen met geschikte getallen

Criterium 1.3 is dus nooit volledig bewezen, maar Euler heeft er wel veel mee gewerkt. Hij liet zien dat van alle $1 \leq n \leq 10000$, de volgende getallen aan zijn criterium voldoen:

$$\begin{array}{rrrrrrrrrrrrr,} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 12, & 13, & 15, \\ 16, & 18, & 21, & 22, & 24, & 25, & 28, & 30, & 33, & 37, & 40, & 42, & 45, \\ 48, & 57, & 58, & 60, & 70, & 72, & 78, & 85, & 88, & 93, & 102, & 105, & 112, \\ 120, & 130, & 133, & 165, & 168, & 177, & 190, & 210, & 232, & 240, & 253, & 273, & 280, \\ 312, & 330, & 345, & 357, & 385, & 408, & 462, & 520, & 760, & 840, & 1320, & 1365, & 1848. \end{array} \tag{2.1}$$

Euler wist dus dat $n = 1848$ geschikt is. Ook zag hij dat $18.518.809 = 197^2 + 1848 \cdot 100^2$ de enige oplossing van de vergelijking $18.518.809 = x^2 + 1848y^2$ met $x, y \in \mathbb{Z}$ is, waar bovendien geldt dat $\text{ggd}(197, 1848 \cdot 100) = 1$. Dus wist Euler dat 18.518.809 een priemgetal is! Dit was toentertijd op $2^{31} - 1 = 2.147.483.647$ na, het grootste bekende priemgetal. Dat dit grotere priemgetal ook door Euler gevonden is, komt mogelijk niet als een verrassing.

Euler bepaalde dus dat $18.518.809 = x^2 + 1848y^2$ maar één oplossing in $\mathbb{Z}$ heeft. Dit kun je doen door eerst de vergelijking om te schrijven naar: $18.518.809 - 1848y^2 = x^2$, en daarna na te gaan dat voor alle

$$0 \leq y \leq \sqrt{\frac{18.518.809}{1848}} < 101$$

er precies één waarde $y \in \mathbb{Z}$ is zodat $18.518.809 - 1848y^2$ een kwadraat is.

Euler had natuurlijk geen computer tot zijn beschikking, maar voor 101 waarden een bepaalde eis nagaan (die niet heel moeilijk is), is nog wel te doen. Het is redelijk simpel om deze test te programmeren, dus is het interessant om te kijken wat voor getallen we er vandaag de dag mee kunnen vinden.

Zo heb ik gevonden dat $m = 615500020594646084114977$ priem is, omdat

$$615500020594646084114977 = 1825^2 + 1848 \cdot 18250007718^2 \tag{2.2}$$

de unieke manier is om m in die vorm te schrijven, en $\text{ggd}(1825, 1848 \cdot 18250007718) = 1$. Bovendien heb ik gevonden dat $m = 615499651294845300709177$ te schrijven is als:

$$1825^2 + 1848 \cdot 18250002243^2 = m = 438861168415^2 + 1848 \cdot 15127533707^2, \tag{2.3}$$

waardoor de we via de definitie van de geschikte getallen geen uitspraak kunnen doen over de primaliteit van m.

Maar Euler kon toch nog wat leuks doen in deze situatie. Als je namelijk twee manieren vindt om m zo te schrijven, dan is er een algoritme waarmee je factoren van m kunt vinden. Het algoritme dat Euler gaf was weer niet helemaal netjes, maar gelukkig doen Blecksmith, Brillhart en Decaro [2] dat beter. Daarnaast geeft Brillhart in de stelling hieronder een ander algoritme, die in deze situatie erg gemakkelijk factoren van m geeft. Voor een bewijs, zie [3].

Stelling 2.4 (Brillhart)
Stel dat $m > 1$ een oneven getal is, en op twee manieren te schrijven is als:

$$m = aw^2 + bx^2 = ay^2 + bz^2,$$

waar $a, b, w, x, y, z \in \mathbb{Z}_{>0}, x < z$, en $ggd(aw, bx) = ggd(ay, bz) = 1$. Dan is:

$$m = ggd(m, wz - xy) \cdot \frac{m}{ggd(m, wz - xy)} \tag{2.5}$$

een niet-triviale factorisatie van m.

Vergelijking (2.5) is in zekere zin niet heel spannend, hij is namelijk altijd waar. Waar het vooral om gaat is dat het niet-triviale factoren van m oplevert. Als we deze stelling nu toepassen op de getallen van vergelijking (2.3), dan krijgen we de volgende factorisatie van $m = 615499651294845300709177$:

$$615499651294845300709177 = 346103613143 \cdot 1778368176239.$$

Deze factorisatie is tevens ook de priemfactorisatie van m. Als we deze factoren zouden proberen te vinden door naïef te kijken of er een geheel getal $2 \leq x \leq \sqrt{m}$ is, zodat $x \mid m$, dan zou de computer er heel lang over gedaan hebben. Er moet wel bij gezegd worden dat het alsnog ongeveer 5 uur duurde om de getallen uit (2.3) te berekenen. Daarnaast zijn er tegenwoordig andere algoritmes die deze factoren in hoogstens een paar seconden hadden kunnen vinden. Verder is $2^{77.232.917} - 1$ op dit moment (juli 2018) het grootste bekende priemgetal. Dit getal heeft 23.249.425 cijfers. Het priemgetal in (2.2) heeft er bijna een factor miljoen minder. Gelukkig is dit niet het einde van de geschikte getallen, want ook al is het misschien niet de beste manier om priemgetallen te vinden, gaan we toch in deze scriptie zien dat de geschikte getallen in ieder geval veel theoretische waarde hebben.

Opmerking 2.6
In Stelling 2.4 moet gelden dat $\text{ggd}(aw, bx) = \text{ggd}(ay, bz) = 1$. Maar als

$$d = \max\{\text{ggd}(aw, bx),\ \text{ggd}(ay, bz)\} > 1,$$

dan vinden we alsnog een niet-triviale factor van m, namelijk d. Om factoren van m te vinden is het dus voldoende om twee manieren te vinden om m in die vorm te schrijven. Daarom kunnen we geschikte getallen ook op de volgende manier definiëren.
Een geheel getal $n \geq 1$ heet *geschikt* als de volgende uitspraak waar is: als $m \in \mathbb{N}_{>1}$ te schrijven is als $m = x^2 + ny^2$ met m oneven, $\text{ggd}(x, ny) = 1$, dan heeft de vergelijking $m = a^2 + nb^2$ precies één oplossing voor $a, b \in \mathbb{Z}_{\geq 0}$ dan en slechts dan als m een priemgetal is.

Euler kon boven de 1848 geen geschikte getallen vinden. Dat kwam hem eerst wel als een verrassing, maar later stelde hij toch het volgende vermoeden op:

Vermoeden 2.7 (Euler)
Er is geen geschikt getal groter dan 1848.

Het is al ruim 200 jaar geleden dat Euler zijn 65 geschikte getallen vond, en in de tussentijd hebben we geen één andere kunnen vinden. In 1934 liet Chowla [4] zien dat maar eindig veel getallen geschikt zijn. Hij gebruikte daarvoor de theorie van de *kwadratische vormen*, waar wij in Hoofdstuk 6 en 7 naar gaan kijken. In 2006 lieten Jacobson, Ramachandran en Williams [10] zien dat er geen geschikt getal is onder $\frac{10^{11}}{4}$.

Met hulp van een computer heb ik voor alle $0 < n \leq 10^9$ gekeken of ze aan Criterium 1.3 voldeden, wat dus niet bewezen is. Naast de getallen die Euler vond zaten er geen andere tussen, waardoor de correctheid van Criterium 1.3 een open probleem blijft.

Verder geeft Kani [11, Cor. 23], door resultaten van Weinberger [17] te gebruiken, de volgende stelling:

Stelling 2.8 *Er is hoogstens één kwadraatvrij geschikt getal $n > 1848$, verder is precies één van de volgende uitspraken waar:*

1. *Er is geen geschikt getal groter dan 1848.*
2. *Er is precies één geschikt getal $n > 1848$, en in dat geval is n kwadraatvrij en $n \equiv 1 \bmod 4$.*
3. *Er zijn nog precies twee geschikte getallen $n_1 > n_2 > 1848$, en in dat geval is n_2 kwadraatvrij, $n_2 \equiv 2 \bmod 4$ en $n_1 = 4n_2$.*

Verder, als de gegeneraliseerde Riemann-hypothese (GRH) waar blijkt te zijn, dan is mogelijkheid 1 correct.

Naast Euler hebben ook andere wiskundigen met de geschikte getallen gewerkt, maar soms wel in een hele andere context. In de rest van deze scriptie gaan we twee manieren zien om de geschikte getallen te karakteriseren. In Hoofdstuk 6 en 7 geven we een interpretatie van Gauss, maar eerst geven we in Hoofdstuk 4 en 5 een recentere invalshoek via het werk van Hagedorn [9, 2011].

Voordat we net als Hagedorn in een meetkundig opzicht kunnen praten over de geschikte getallen, hebben we eerst een aantal uitspraken nodig over het *Legendre Symbool*. In het volgende hoofdstuk gaan we bekijken wat dit symbool is, en hoe we er mee kunnen werken.

3 Kwadratische Reciprociteit

De wet van de kwadratische reciprociteit is een belangrijke stelling binnen de getaltheorie die gebruik maakt van het Legendre symbool. Als $a \in \mathbb{Z}$ en $p > 2$ een priemgetal is, dan definiëren we:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{als } a \text{ een niet-nul kwadraat mod } p \text{ is,} \\ -1, & \text{als } a \text{ geen kwadraat mod } p \text{ is,} \\ 0, & \text{als } a \equiv 0 \bmod p. \end{cases}$$

Zo is bijvoorbeeld $\left(\frac{2}{7}\right) = 1$, want $4^2 \equiv 2 \bmod 7$.
Voor de hand liggende eigenschappen van het Legendre symbool zijn bijvoorbeeld: $\left(\frac{ab}{p}\right) =$

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, en als $a \equiv b \bmod p$, dan $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. We gaan nu wat extra eigenschappen van dit symbool bewijzen, want die we kunnen we later goed gebruiken om te bewijzen dat een geschikt getal inderdaad geschikt is.

Een bekend resultaat over het Legendre symbool is het criterium van Euler:

Lemma 3.1 *Als $a \in \mathbb{Z}$ en $p > 2$ een priemgetal, dan*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.
2. *In het bijzonder* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 4, \\ -1, & \text{als } p \equiv 3 \bmod 4. \end{cases}$
3. *Bovendien geldt dat* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{als } p \equiv \pm 1 \bmod 8, \\ -1, & \text{als } p \equiv \pm 3 \bmod 8. \end{cases}$

Bewijs
1. We mogen zonder verlies van algemeenheid aannemen dat $a \neq 0$. Want als $a = 0$, dan is $\left(\frac{a}{p}\right) = 0$ en $a^{\frac{p-1}{2}} = 0$.
Als $x^2 \equiv 1 \bmod p$, dan $(x-1)(x+1) \equiv 0 \bmod p$, maar p is een priemgetal, waardoor $p \mid x-1$ of $p \mid x+1$, dus $x \equiv \pm 1 \bmod p$. Bovendien zegt de kleine stelling van Fermat dat $a^{p-1} \equiv 1 \bmod p$. Samen impliceren deze twee uitspraken dat $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. Daarom is het voldoende om $\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$ te bewijzen.
Stel $\left(\frac{a}{p}\right) = 1$, dan $\exists b$ zodanig dat $b^2 \equiv a \bmod p$. Uit de kleine stelling van Fermat weten we dan dat $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod p$.
Stel $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. $(\mathbb{Z}/p\mathbb{Z})^*$ is een cyclische groep (zie [1, p. 22-24]), dus bestaat er een x met orde $p-1$ en een m zodanig dat $x^m \equiv a \bmod p$. Dan is $x^{m\frac{p-1}{2}} \equiv 1 \bmod p$, dus $p-1 \mid m\frac{p-1}{2}$, dus m is deelbaar door 2. Maar dan hebben we dat $a \equiv x^m \equiv \left(x^{m/2}\right)^2 \bmod p$, dus $\left(\frac{a}{p}\right) = 1$.
2. Uit *1.* weten we dat $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$, maar het mod p gedeelte kunnen we weglaten, omdat $\left(\frac{-1}{p}\right)$ en $(-1)^{\frac{p-1}{2}}$ beide ± 1 zijn, en $p > 2$.
3. Hiervoor verwijzen we naar [1, p. 28,29]. □

Stelling 3.2 *De wet van de kwadratische reciprociteit.*
Als p en q verschillende oneven priemgetallen zijn, dan:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Voor een bewijs van deze stelling verwijzen we naar [6, Prop 1.10].

Een herformulering van deze uitspraak is: $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \iff p \equiv q \equiv 3 \bmod 4$. Dat wil zeggen: Als $p \bmod q$ een kwadraat is, dan is $q \bmod p$ dat ook, tenzij ze beide 3 mod 4 zijn.

Met al deze rekenregels is het hoog tijd voor een voorbeeld.

Voorbeeld 3.3
We bepalen of 19 een kwadraat is modulo 37:

$$\left(\frac{19}{37}\right) \overset{3.2}{=} (-1)^{\frac{19-1}{2}\frac{37-1}{2}} \frac{1}{\left(\frac{37}{19}\right)} = (-1)^{9\cdot 18}\left(\frac{37}{19}\right) = \left(\frac{-1}{19}\right) \overset{3.1}{=} (-1)^{\frac{19-1}{2}} = (-1)^9 = -1.$$

We zien dat er *geen* geheel getal x is zodat $x^2 \equiv 19 \bmod 37$.

Bij het bestuderen van de geschikte getallen kijken we naar priemgetallen p die van de vorm $p = x^2 + ny^2$ zijn. In Gevolg 3.5 van Lemma 3.4 hieronder doen we al een aantal uitspraken over priemen van deze vorm.

Lemma 3.4 *Als $p \nmid n$ en $p > 2$ priem, dan:*

$$\left(\frac{-n}{p}\right) = 1 \iff p \mid x^2 + ny^2, \text{ voor zekere } x, y \in \mathbb{Z} \text{ met } ggd(x, y) = 1.$$

Bewijs
Stel $\left(\frac{-n}{p}\right) = 1$, dan $\exists x$ zodanig dat $-n \equiv x^2 \bmod p$, dus $x^2 + n \equiv 0 \bmod p$. Hieruit volgt dat $p \mid x^2 + n \cdot 1^2$, waar natuurlijk geldt dat $\text{ggd}(x, 1) = 1$.

Anderzijds, stel dat $p \mid x^2 + ny^2$ met $\text{ggd}(x, y) = 1$, dan $x^2 \equiv -ny^2 \bmod p$. Stel $p \mid y$, dan $0 \equiv x^2 + ny^2 \equiv x^2 \bmod p$, dus $p \mid x$. Maar dan is $\text{ggd}(x, y) \geq p > 1$ ↯. Dus $y \not\equiv 0 \bmod p$, waardoor y een inverse heeft mod p. Daaruit volgt dat $x^2(y^{-1})^2 \equiv -n \bmod p$, waardoor $\left(\frac{-n}{p}\right) = 1$. □

Gevolg 3.5 *Als $n \in \mathbb{Z}_{\geq 1}$, en $p > 2$ priem is, zodanig dat $p \nmid n$ en $p = x^2 + ny^2$. Dan:*

a. $\left(\frac{-n}{p}\right) = 1$ *en* $\left(\frac{p}{q}\right) = 1$ *voor elke priem $q > 2$ met $q \mid n$.*

b. Als $n \equiv 0, 1 \bmod 4$, dan $p \equiv 1 \bmod 4$.

c. Als $n \equiv 0 \bmod 8$, dan $p \equiv 1 \bmod 8$.

Bewijs
a. $p = x^2 + ny^2$, dus $\text{ggd}(x, y) = 1$, want p is priem. Dus uit Lemma 1.3 weten we dat $\left(\frac{-n}{p}\right) = 1$. Verder zien we dat $p \equiv x^2 \bmod q$, dus $\left(\frac{p}{q}\right) = 1$.
b. Alle kwadraten mod 4 uitschrijven geeft dat $x^2, y^2 \equiv 0, 1 \bmod 4$. Dus $p = x^2 + ny^2 \equiv 0, 1, 2 \bmod 4$. Maar $p \equiv 0, 2 \bmod 4$ kunnen niet, want p is priem en bovendien groter dan 2. Dus $p \equiv 1 \bmod 4$.
c. Gaat hetzelfde als *b.* Alleen merken we nu op dat voor elk oneven getal x geldt dat $x^2 \equiv 1 \bmod 8$. □

Voordat we verder gaan met het Legendre symbool, geven we eerst een aantal stellingen van Fermat. Deze stellingen vormen een inleiding voor een alternatieve (en equivalente) definitie van de geschikte getallen.

Stelling 3.6 (Fermat)
Zij p een priemgetal, dan:

$$\exists x, y \in \mathbb{Z} : p = x^2 + y^2 \iff p = 2 \text{ of } p \equiv 1 \bmod 4.$$

Deze uitspraak zegt dus iets over wanneer een priemgetal in een bepaalde vorm geschreven kan worden. Zo weten we bijvoorbeeld dat 37 een priemgetal is, en bovendien dat $37 \equiv 1 \bmod 4$. De stelling zegt nu dat er $x, y \in \mathbb{Z}$ moeten bestaan zodat $37 = x^2 + y^2$, en dat klopt, want we zien bijvoorbeeld dat $37 = 6^2 + 1^2$.

In dezelfde trant gaf Fermat ook nog de volgende resultaten. Als p een priemgetal is, dan:

$$\exists x, y \in \mathbb{Z} : p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8,$$
$$\exists x, y \in \mathbb{Z} : p = x^2 + 3y^2 \iff p = 3 \text{ of } p \equiv 1 \bmod 3.$$

We zien dus dat p in een bepaalde vorm te schrijven is, precies wanneer p aan bepaalde congruenties voldoet (op een paar uitzonderingen na). Een logische vraag is nu of we dit kunnen generaliseren naar het geval dat p in de vorm $x^2 + ny^2$ geschreven kan worden. Dit blijkt precies een alternatieve karakterisering te zijn van de geschikte getallen!

Stelling 3.7 *Een geheel getal $n \geq 1$ is geschikt dan en slechts dan als de volgende uitspraak waar is: er bestaan getallen $N_n, k \in \mathbb{N}$, een verzameling uitzonderingen S en congruentieklassen $c_1, ..., c_k \bmod N_n$, zodat voor alle priemgetallen $p \notin S$:*

$$\exists x, y \in \mathbb{Z} : p = x^2 + ny^2 \iff p \equiv c_1, \ldots, c_k \bmod N_n.$$

We hadden dus in plaats van Definitie 1.1, ook Stelling 3.7 kunnen nemen als de definitie van een geschikt getal. Maar Euler bestudeerde als eerste de geschikte getallen, dus gingen we uit van zijn definitie (of tenminste een die er veel op leek). Het probleem is nu dat deze stelling niet gemakkelijk te bewijzen is. Je hebt er bijvoorbeeld klassenlichaamtheorie voor nodig, en dat valt buiten de scope van deze scriptie. Daarom gaan we deze stelling niet bewijzen. Maar hij is wel belangrijk, want de meetkunde der getallen (Hoofdstuk 4) blijkt goed toepasbaar te zijn op deze karakterisering van de geschikte getallen.

Met Stelling 3.7 en de resultaten van Fermat zien we dat $n = 1, 2, 3$ alle drie geschikt zijn. Voor de andere geschikte getallen uit (2.1) willen we nu graag congruenties vinden zodanig dat ze aan de eis van Stelling 3.7 voldoen. Maar, dat bij Stelling 3.6 moet gelden dat p congruent aan 1 mod 4 moet zijn, kan je nog wel gokken door veel priemen te bekijken die te schrijven zijn als de som van twee kwadraten. Maar bij een uitspraak als Propositie 5.8:

$$\exists x, y \in \mathbb{Z} : p = x^2 + 133y^2$$
$$\iff$$
$$p \equiv \left[\begin{array}{c} 1, 9, 25, 81, 85, 93, 121, 137, 149, 169, 177, 197, 225, 233, 253, \\ 277, 289, 305, 309, 365, 389, 429, 457, 473, 501, 505, 529 \end{array} \right] \bmod 532.$$

is dat natuurlijk een stuk moeilijker. Daarom is het handig als we voor een getal n een manier zouden hebben om van de uitspraak: $\exists x, y \in \mathbb{Z} : p = x^2 + ny^2 \iff p \equiv c_1, ..., c_k \bmod N_n$ te bepalen wat de c_i en N_n zijn.
In de volgende propositie laten we zien hoe we deze waarden kunnen halen uit de drie uitspraken van Gevolg 3.5. Voordat we die propositie gaan bewijzen, geven we eerst een generalisatie van het Legendre symbool: het Jacobi Symbool.

Het verschil tussen het Jacobi Symbool en het Legendre symbool is dat het Jacobi symbool $\left(\frac{P}{Q}\right)$ gedefinieerd is voor alle getallen $P, Q \in \mathbb{Z}$, waar Q oneven is, maar niet per se priem.

Laat $P = \prod_i p_i^{n_i}$ en $Q = \prod_j q_j^{m_j}$ de priemfactorisaties van P en Q zijn. Definieer:

$$\left(\frac{P}{Q}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)^{n_i m_j},$$

waar aan de linkerkant dus het Jacobi Symbool staat, en waar aan de rechterkant het Legendre symbool gebruikt wordt.
Door deze generalisatie verliezen we wel wat eigenschappen van het Legendre symbool. Als $\left(\frac{P}{Q}\right) = -1$, dan is P net als bij het Legendre symbool geen kwadraat mod Q, maar de omkering is niet meer altijd waar. Gelukkig geldt de reciprociteitswet (Stelling 3.2) wel nog steeds. Dit kun je bewijzen door de multiplicativiteit van het Jacobi symbool te gebruiken, samen met het feit dat de reciprociteitswet geldt voor het Legendre symbool. Daarom kan het soms toch nog handig zijn om het Jacobi symbool te gebruiken.

Propositie 3.8 *Gegeven $n \geq 1$, bestaan er $k = k_n$, N_n en $c_1, ..., c_k \bmod N_n$, die de eigenschap hebben dat een oneven priemgetal p voldoet aan $p \equiv c_1, ..., c_k \bmod N_n$ dan en slechts dan als p aan de uitspraken van Gevolg 3.5 voldoet:*

a. $\left(\frac{-n}{p}\right) = 1$ en $\left(\frac{p}{q}\right) = 1$ voor elke priem $q > 2$ met $q \mid n$.

b. Als $n \equiv 0, 1 \bmod 4$, dan $p \equiv 1 \bmod 4$.

c. Als $n \equiv 0 \bmod 8$, dan $p \equiv 1 \bmod 8$.

Omdat we de expliciete uitdrukking van N_n en de c_i later nodig hebben, verwijzen we naar ze met Propositie 3.8 α en Propositie 3.8 β respectievelijk.

Bewijs
We beginnen met de ($\Leftarrow$) implicatie, waarin we k_n, N_n en de c_i gaan construeren.
Stel dat p voldoet aan de bovenstaande uitspraken. We willen inzien welke congruentie relaties op p gelegd worden door deze uitspraken. Laten we beginnen met het tweede deel van a: $\left(\frac{p}{q}\right) = 1$ voor elke priem $q > 2$ met $q \mid n$. Er zijn precies $\frac{q-1}{2}$ niet-nul kwadraatresten modulo een priemgetal $q > 2$. Immers, als $x^2 \equiv y^2 \bmod q$, dan $x \equiv \pm y \bmod q$. Schrijf $n = 2^s m$ met m oneven, en laat $\prod_q q^{r_q}$ de priemfactorisatie van m zijn. Definieer:

$$k_n^* = \prod_q \left(\frac{q-1}{2}\right) \text{ en } N_n^* = \prod_q q.$$

Volgens de Chinese reststelling bestaan er k_n^* restklassen $c = c_1^*, \ldots, c_{k_n^*}^* \in N_n^*$, zodat $\left(\frac{c}{q}\right) = 1$ voor alle priemdelers q van m.

Dit zegt nog niet iets over de even delers van n, daarvoor kunnen we bijvoorbeeld naar het eerste deel van a kijken (we gebruiken hieronder ook dat $\left(\frac{p}{q}\right) = 1$, voor $q \mid n$ en $q > 2$).

Door de reciprociteit van het Jacobi symbool te gebruiken krijgen we:

$$\begin{aligned}
1 = \left(\frac{-n}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2^s}{p}\right)\left(\frac{m}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{2^s}{p}\right)\left(\frac{p}{m}\right)(-1)^{\frac{p-1}{2}\frac{m-1}{2}} \\
&= (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^s}{p}\right)\prod_q\left(\frac{p}{q^{r_q}}\right) = (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2}{p}\right)^s\prod_q\left(\frac{p}{q}\right)^{r_q} \\
&= (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2}{p}\right)^s = (-1)^{\frac{p-1}{2}\frac{m+1}{2}}(-1)^{s\frac{p^2-1}{8}} \\
&= (-1)^{\frac{p-1}{2}\frac{m+1}{2}+s\frac{p^2-1}{8}}.
\end{aligned}$$

Merk op dat het nu niet erg is dat we tussendoor het Jacobi symbool hebben gebruikt, want we begonnen links met het Legendre symbool. Dus voldoet p aan eigenschap a wanneer $\left(\frac{p}{q}\right) = 1$ voor elke priem $q > 2$ met $q \mid n$, en:

$$(-1)^{\frac{p-1}{2}\frac{m+1}{2}+s\frac{p^2-1}{8}} = 1. \tag{3.9}$$

We gaan nu een paar waarden voor $n \bmod 8$ testen, door te kijken wat $p \bmod 8$ dan moet zijn, en wat de bijbehorende waarden N_n en k_n worden.
Stel dat $n \equiv 1 \bmod 8$, dan is $s = 0$ en $m \equiv 1 \bmod 8$. De vergelijking (3.9) wordt dan: $(-1)^{\frac{p-1}{2}\frac{m+1}{2}} = 1$, waardoor $p \equiv 1 \bmod 4$. We krijgen dus een extra eis voor $p \bmod 4$. Hierdoor is $N_n = 4N_n^*$. Verder is $k_n = k_n^*$, omdat p in precies 1 restklasse mod 4 valt. Dit is anders in het volgende voorbeeld.
Stel dat $n \equiv 2 \bmod 8$, dan is $s = 1$ en $m \equiv 1 \bmod 4$. De vergelijking (3.9) wordt nu: $(-1)^{\frac{p-1}{2}\frac{m+1}{2}+\frac{p^2-1}{8}} = 1$. Door waarden voor $p \bmod 8$ in te vullen zien we dat $p \equiv 1, 3 \bmod 8$. Daarom is in dit geval $N_n = 8N_n^*$ en $k_n = 2k_n^*$, omdat p nu in 2 verschillende restklassen mod 8 kan vallen.

Door dit nu voor elke mogelijke waarde van $n \bmod 8$ uit te schrijven, krijgen we de volgende resultaten (waar nog steeds $m = \prod_q q^{r_q}$).

$$N_n = 2^t\prod_q q, \text{ met } t = \begin{cases} 0, & \text{als } n \equiv 3 \bmod 4 \\ 2, & \text{als } n \equiv 1, 4, 5 \bmod 8 \\ 3, & \text{als } n \equiv 0, 2, 6 \bmod 8 \end{cases} \tag{α}$$

$$k_n = u\prod_q\left(\frac{q-1}{2}\right), \text{ met } u = \begin{cases} 1, & \text{als } n \equiv 0, 1, 3 \bmod 4 \\ 2, & \text{als } n \equiv 2 \bmod 4 \end{cases}$$

Tot slot de extra congruenties waar c mogelijk ook nog aan moet voldoen (naast $\left(\frac{c}{q}\right) = 1$ voor alle priemdelers q van m):

$$\begin{array}{ll}
c \equiv 1 \bmod 4, & \text{als } n \equiv 1, 4, 5 \bmod 8, \\
c \equiv 1 \bmod 8, & \text{als } n \equiv 0 \bmod 8, \\
c \equiv 1, 3 \bmod 8, & \text{als } n \equiv 2 \bmod 8, \\
c \equiv 1, 7 \bmod 8, & \text{als } n \equiv 6 \bmod 8, \\
\text{geen extra eis}, & \text{als } n \equiv 3, 7 \bmod 8.
\end{array} \tag{β}$$

Hoe maken we het bewijs (van de ($\Leftarrow$) implicatie) nu af? We gebruiken weer de Chinese reststelling om in te zien dat er k_n restklassen $c = c_1, \ldots, c_{k_n} \in N_n$ bestaan, zodat $\left(\frac{c}{q}\right) = 1$ voor alle priemdelers q van m, en zodat c aan de eisen van (β) voldoet. Per constructie hebben we dan dat $p \equiv c_1, \ldots, c_{k_n} \bmod N_n$, als de uitspraken *a,b* en *c* gelden voor p. We gebruiken de uitspraken b en c alleen voor het geval dat $n \equiv 0 \bmod 4$, omdat we dan te weinig informatie over m hebben.
Stel bijvoorbeeld dat $n \equiv 4 \bmod 8$. Dan is $s = 2$ en $m \equiv 1 \bmod 2$, uit vergelijking (3.9) volgt dan dat $(-1)^{\frac{p-1}{2}\frac{m+1}{2}} = 1$. Maar omdat $m \equiv 1 \bmod 2$, kunnen we nu geen uitspraak doen over wat p moet zijn. Gelukkig redt uitspraak b ons dan uit de brand.

Nu nog de ($\Rightarrow$) implicatie. Omdat we de c_i, k_n en N_n al geconstrueerd hebben is het meeste werk al gedaan. Door deze getallen te gebruiken, kunnen we op een analoge manier als bij de vorige implicatie de uitspraken *a, b* en *c* bewijzen. We doen dit door het weer voor elke waarde van $n \bmod 8$ na te gaan, precies zoals we daarnet ook deden. Maar omdat we de expliciete constructies al gemaakt hebben, is dit bijna geen moeite meer. Daarmee is het bewijs afgerond. □

Door Gevolg 3.5 en Propositie 3.8 samen te voegen krijgen we:

Propositie 3.10 *Gegeven $n \geq 1$, bestaan er $k = k_n$, N_n en $c_1, ..., c_k \bmod N_n$ zodat als $\exists x, y \in \mathbb{Z} : p = x^2 + ny^2$, waar $p > 2$ priem is en $p \nmid n$, dan $p \equiv c_1, \ldots, c_k \bmod N_n$.*

In de volgende twee hoofdstukken laten we zien dat voor alle getallen n uit (2.1), de omkering van deze uitspraak ook waar is. De volgende uitspraak volgt dan uit Stelling 3.7.

Hoofdstelling 3.11 *Alle getallen uit* (2.1) *zijn geschikt.*

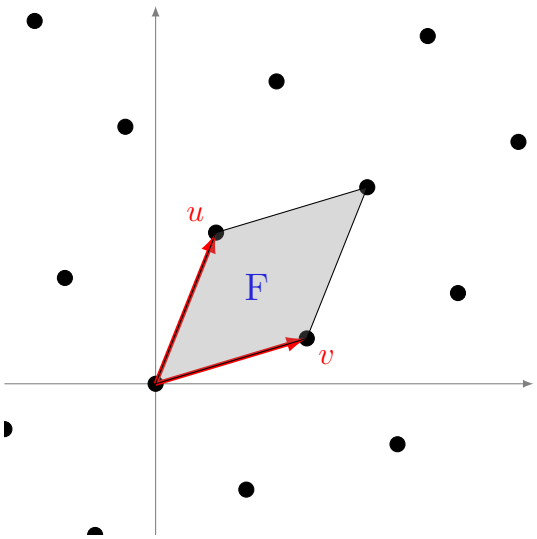
4 Meetkunde der Getallen

Het vorige hoofdstuk over kwadratische reciprociteit is een veelvoorkomend onderwerp bij boeken en artikelen over geschikte getallen. Het recente artikel van Hagedorn [9, 2011] is daar ook geen uitzondering op, maar wat de methode van Hagedorn interessant maakt, is dat het een meetkundige benadering geeft. Zo is er een mooie stelling van Minkowski die een brug vormt tussen de meetkunde en de getaltheorie. Maar voordat we het daar over gaan hebben, hebben we eerst wat terminologie nodig.

Een deelverzameling A van $\mathbb{R}^2$ is *symmetrisch* als $x \in A \iff -x \in A$. A is *convex* als $\forall x, y \in A$ het lijnstuk tussen x en y volledig binnen A ligt. Gegeven twee lineair onafhankelijke vectoren $u, v \in \mathbb{R}^2$ kun je een *rooster* $R \subset \mathbb{R}^2$ maken door alle combinaties $au + bv$ te nemen met $a, b \in \mathbb{Z}$. Het *fundamentaalgebied* $F \subset \mathbb{R}^2$ van een rooster R wordt gemaakt door alle combinaties $ru + sv$ te nemen met $r, s \in \mathbb{R}$ en $0 \leq r, s < 1$. R is een discrete ondergroep van $\mathbb{R}^2$. Dat betekent dat $\forall x \in R : \exists U \subset \mathbb{R}^2$ zodat $U \cap R = \{x\}$. Informeel betekent dat de punten van R dus niet heel erg dicht bij elkaar liggen.

Het fundamentaalgebied F kun je opvatten als het opgevulde parallellogram in $\mathbb{R}^2$ dat opgespannen wordt door de vectoren u en v.

Als $u, v \in \mathbb{Z}^2$, dan is de oppervlakte van F gelijk aan de index (van groepen) $[\mathbb{Z}^2 \colon R]$. Uit de lineaire algebra weten we namelijk dat $\mathrm{opp}(F) = \det(u, v) = [\mathbb{Z}^2 \colon R]$, waar we met (u, v) de matrix met als kolommen de vectoren u en v bedoelen. Bovendien kan elk punt $(x, y) \in \mathbb{R}^2$



Figuur 1: Een rooster met fundamentaalgebied F.

naar F getransleerd worden, door er een element van R bij op te tellen. Dit komt doordat je om elk punt (x, y) een fundamentaalgebied heen kunt tekenen.

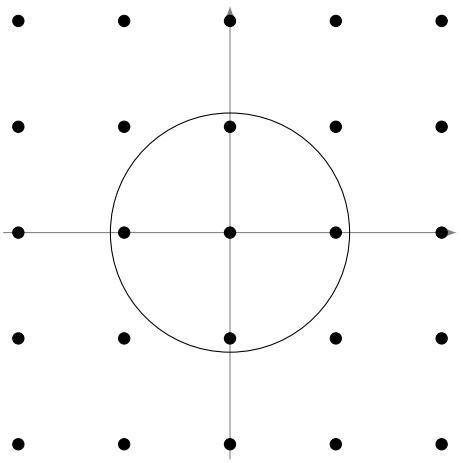
De volgende stelling van Minkowski vormt de basis van de meetkunde der getallen. Wij geven hem hier voor willekeurige m, waar m de exponent bij $\mathbb{R}^m$ is, maar we bewijzen hem alleen voor $m = 2$, omdat we daar steeds in gaan werken.

Stelling 4.1 *Zij R een rooster in $\mathbb{R}^m$, waarvan de oppervlakte van het fundamentaalgebied F gelijk aan V is. Als $A \subseteq \mathbb{R}^m$ convex en symmetrisch is met opp$(A) > 2^m V$, dan bevat A een niet-nul element van R.*

Bewijs (*voor het geval $m = 2$*)
Bekijk het rooster $2R = \{(2x, 2y) \mid (x, y) \in R\}$. Daarvoor geldt dat $[2R\colon R] = 2^2 = 4$, waardoor de oppervlakte van het fundamentaalgebied $2F$ van $2R$ gelijk aan $4V$ is. We weten dat we elk punt $a \in A$ naar $2F$ kunnen transleren met een element uit $2R$. $\mathrm{Opp}(A) > 4V = \mathrm{Opp}(2F)$, dus zijn er twee punten $a \neq b \in A$ die naar hetzelfde element getransleerd worden, dat wil zeggen $a + 2r_1 = b + 2r_2$, voor $r_1, r_2 \in R$. R is een additieve groep, dus $2r_2 - 2r_1 = 2r$ voor een $0 \neq r \in R$. A is symmetrisch, dus $-b \in A$. A is ook convex dus ligt het lijnstuk tussen $-b$ en $a = b + 2r$ binnen A. In het bijzonder ligt het middelpunt $\frac{-b+b+2r}{2} = r$ in A. Dus bevat A een niet-nul element van ons rooster R. □

Om vertrouwd te raken met de nieuwe definities en concepten bekijken we een simpel voorbeeld.

Voorbeeld 4.2
Neem als rooster $R = \mathbb{Z}^2$. De oppervlakte van het fundamentaalgebied van R is $[\mathbb{Z}^2\colon \mathbb{Z}^2] = 1$. We gaan berekenen hoe groot de straal r van een cirkel C moet zijn zodat de stelling Minkowski garandeert dat er een niet-nul element van R binnen de cirkel ligt. Een cirkel is in ieder geval convex en symmetrisch. Bovendien geldt dat $\mathrm{Opp}(C) = \pi r^2$, dit willen we groter dan $4V = 4$ hebben. Oplossen naar r geeft dat $r > \sqrt{\frac{4}{\pi}} \approx 1.13$ moet zijn.



Figuur 2: Een cirkel met straal $r = \sqrt{\frac{4}{\pi}}$ in het rooster $\mathbb{Z}^2$.

Deze straal is maar net iets groter dan de benodigde straal 1, Minkowski geeft daarom een redelijk goede ondergrens voor de straal. Dit zullen we ook nog later terug zien in Opmerking 5.10, waar we Minkowski kort gaan vergelijken met alternatieve methoden.

Hagedorn zag in dat de stelling van Minkowski de mogelijkheid geeft om op een mooie manier uitspraken te doen over geschikte getallen. De ellips $x^2 + ny^2 = p$ is namelijk convex en symmetrisch. Als eerste voorbeeld daarvan bekijken we hier $n = 2$.

Propositie 4.3 *Als $p > 2$ priem is, dan:*

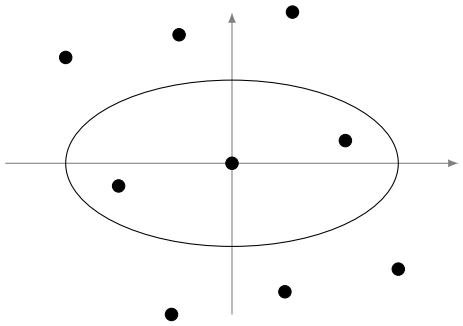
$$\exists x, y \in \mathbb{Z} : p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8.$$

Bewijs
($\Rightarrow$): In Propositie 3.8 hebben we erg veel moeite gedaan, maar daar kunnen we nu de vruchten van plukken. Er geldt dat $n \equiv 2 \bmod 8$, dus volgt uit Propositie 3.8 α, β dat $N_n = 8$ en $p \equiv 1, 3 \bmod 8$.
($\Leftarrow$): Bij deze implicatie komt onze kennis over het Legendre symbool goed van pas. Claim: $\exists u \in \mathbb{Z}$ zodat $u^2 \equiv -2 \bmod p$. Immers: de aanname dat $p \equiv 1, 3 \bmod 8$, is precies de relatie die Propositie 3.8 β ook geeft. Dus geeft Propositie 3.8 a dan dat $\left(\frac{-2}{p}\right) = 1$.

Maar wat hebben we daar nou aan? We kunnen nu een rooster maken zodat de punten van dat rooster ons informatie geven over het bestaan van een oplossing voor $p = x^2 + 2y^2$. Definieer $R = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv ub \bmod p\}$. Dan is R een rooster, want R wordt opgespannen door $v = (u, 1)$ en $w = (p, 0)$. Immers, als $(a, b) \in R$, dan $(a, b) \equiv (ub, b) = bv$. Anderzijds, als $c, d \in \mathbb{Z}$, dan $cv + dw = (cu + dp, c) \in R$, omdat $uc \equiv cu + dp \equiv a \bmod p$. Daarnaast heeft R index p in $\mathbb{Z}^2$. Want er zijn p verschillende paren (a, b) in R met $0 \leq a, b \leq p - 1$, namelijk: $(0, 0), (u, 1), (2u, 2), \ldots, ((p-1)u, p-1)$ (als $iu \geq p$, reduceer het dan mod p). Maar er zijn in totaal p^2 verschillende paren (a, b) in $\mathbb{Z}^2$ met $0 \leq a, b \leq p - 1$, dus $[\mathbb{Z}^2 \colon R] = \frac{p^2}{p} = p$, waardoor de oppervlakte van het fundamentaalgebied van R gelijk aan p is.

Nu we al deze informatie hebben over ons rooster, kunnen we er de stelling van Minkowski op toepassen. Laat E_k het gebied zijn dat ingesloten wordt door de ellips $x^2 + 2y^2 = k$. Uit de calculus weten we dat de oppervlakte van de standaard ellips: $(x/A)^2 + (y/B)^2 = 1$

gelijk aan $AB\pi$ is. Onze ellips kunnen we herschrijven als $(x/\sqrt{k})^2 + (y/\sqrt{k/2})^2 = 1$. Dus is $\text{Opp}(E_k) = \frac{\pi k}{\sqrt{2}} > 2.3k$. Als we nu $k = 1.8p$ nemen, dan is $\text{Opp}(E_k) > 4p$. Dan geeft Minkowski ons dus dat E_k een niet-nul element (a, b) van onze R bevat. Verder zien we dat $a^2 + 2b^2 \equiv (ub)^2 + 2b^2 \equiv -2b^2 + 2b^2 \equiv 0 \bmod p$, dus $p \mid a^2 + 2b^2$. Maar E_k is gedefinieerd als de punten (x, y) met $x^2 + 2y^2 \leq 1.8p$, dus moet wel $a^2 + 2b^2 = p$. Dus hebben we een oplossing voor $p = x^2 + 2y^2,\ x, y \in \mathbb{Z}$ gevonden. □



Figuur 3: De ellips $x^2 + y^2 = 1.8p$ in een rooster.

Voor het geval dat $n = 2$ is het ons nu dus gelukt om te laten zien dat n geschikt is. Een belangrijke vraag is of we een soortgelijk bewijs kunnen geven voor de andere 64 getallen uit (2.1). In de volgende propositie nemen we $n = 5$, waar we gaan zien dat we op sommige plekken wat meer werk moeten doen. We konden bijvoorbeeld daarnet onze k zó kiezen zodat $a^2 + b^2 = p$ de enige mogelijkheid was, maar wat als $k \geq 2p$?

Propositie 4.4 *Als $p \neq 5$ priem is, dan:*

$$\exists x, y \in \mathbb{Z} : p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20.$$

Bewijs
($\Rightarrow$): Uit Propositie 3.8 α, β weten we dat $p \equiv 1 \bmod 4$ en $\left(\frac{p}{5}\right) = 1$. Door alle mogelijkheden af te gaan, of door de Chinese reststelling te gebruiken, zien we dat $p \equiv 1, 9 \bmod 20$.
($\Leftarrow$): We gaan weer hetzelfde proberen te doen als bij $n = 2$. Laten we beginnen door na te gaan dat -5 een kwadraat is mod p: de relatie $p \equiv 1, 9 \bmod 20$ is weer dezelfde die je krijgt als uit Propositie 3.8 β, dus volgt uit Propositie 3.8 a dat $\left(\frac{-5}{p}\right) = 1$. Dus bestaat er een $u \in \mathbb{Z}$, zodat $u^2 \equiv -5 \bmod p$.
We kunnen nu weer een rooster R maken, met $R = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv ub \bmod p\}$. Als ellips nemen we dit keer $x^2 + 5y^2 = k$, waardoor $\text{Opp}(E_k) = \frac{\pi k}{\sqrt{5}} > 1.4k$, dus nemen we $k = 2.9p$, zodat $\text{Opp}(E_k) > 4p$. Uit de stelling van Minkowski volgt dan dat $p \mid a^2 + 5b^2 \leq 2.9p$, waardoor $x^2 + 5y^2 = p$ of $x^2 + 5y^2 = 2p$ (of beide!) een oplossing heeft (of hebben).

In zekere zin komen we er nog goed van af, omdat we nog net het geval $3p = x^2 + 5y^2$ ontwijken. Laten we dan maar eens bekijken wat er gebeurt als $2p = x^2 + 5y^2$. Dan geldt dat $2p \equiv x^2 \bmod 5$, maar de enige niet-nul kwadraten mod 5 zijn 1 en 4, daaruit volgt dat $p \equiv 2, 3 \bmod 5$. Onze aanname is dat $p \equiv 1, 9 \bmod 20$, waardoor $p \equiv 1, 4 \bmod 5$ ↯. De andere optie dat $p = x^2 + 5y^2$ een oplossing heeft, geldt daardoor wel. □

Ook al was $k \geq 2$, lukte het ons toch nog om de propositie te bewijzen, door gebruik te maken dat maar een deel van de getallen mod n een kwadraat is.

We kunnen nu een (voorlopig) algemeen stappenplan geven:
Voor de ($\Rightarrow$) implicatie gebruiken we Propositie 3.8 α, β, om de congruentie relaties op p vast te leggen.
Voor de ($\Leftarrow$) implicatie doen we de volgende 3 stappen:

1. Gebruik Propositie 3.8 a zodat we weten dat $\left(\frac{-n}{p}\right) = 1$.
2. Gebruik de stelling van Minkowski om te laten zien dat $x^2 + ny^2 = dp$ een oplossing heeft voor een $d \leq B_n \stackrel{\text{def}}{=} 4\sqrt{n}/\pi$.
3. Ga voor elke $2 \leq d \leq B_n,\ d \in \mathbb{N}$ na dat $x^2 + ny^2 = dp$ niet mogelijk is.

Merk op dat B_n gedefinieerd is zodat de oppervlakte van de ellips $x^2 + ny^2 = B_n p$ precies $4p$ is, zodat Minkowski's stelling van toepassing is.

5 Bewijs van Hoofdstelling 3.11

Het is nog niet helemaal duidelijk of het inderdaad gaat lukken om stap 3 voor elke optredende d te bewijzen. In dit hoofdstuk geven we een aantal lemma's waarmee we uitspraken kunnen doen over deze getallen d. Het volgende lemma is er een die we veel gaan gebruiken.

Lemma 5.1 *Laat p en q twee verschillende priemen zijn. Stel dat $\left(\frac{p}{q}\right) = 1$, $q \mid n$ en $\left(\frac{d}{q}\right) = -1$. Dan heeft de vergelijking $x^2 + ny^2 = dp$ geen oplossingen in $\mathbb{Z}$.*

Bewijs
Stel dat $x^2 + ny^2 = dp$ wel een oplossing heeft voor zekere $x, y \in \mathbb{Z}$. Dan is $x^2 \equiv dp \not\equiv 0 \bmod q$, waardoor $\left(\frac{dp}{q}\right) = 1$. Maar $\left(\frac{dp}{q}\right) = \left(\frac{d}{q}\right)\left(\frac{p}{q}\right) = (-1) \cdot 1 = -1$ $\lightning$. □

In de volgende propositie bekijken we het geval $n = 10$, waar we ons alleen gaan focussen op stap 3 van de ($\Leftarrow$) implicatie. We gaan zien dat het bovenstaande lemma erg handig is, maar niet voldoende is om $x^2 + ny^2 = dp$ voor alle geschikte getallen n tot $x^2 + ny^2 = p$ te reduceren.

Propositie 5.2 *Als p een priemgetal is, dan:*

$$\exists x, y \in \mathbb{Z} : p = x^2 + 10y^2 \iff p \equiv 1, 9, 11, 19 \bmod 40.$$

Bewijs
$B_n \leq 4.1$, dus bekijken we alle $2 \leq b \leq 4$. Uit lemma 5.1 volgt dat $x^2 + 10y^2 = dp$ voor $d = 2, 3$ niet kan, omdat $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = 1$ (Propositie 3.8 a) en $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$.
Dus rest ons nu alleen nog het geval $d = 4$. Merk op dat $\left(\frac{4}{5}\right) = 1$, waardoor we het lemma hier niet op kunnen toepassen. Stel dat $x^2 + 10y^2 = 4p$ een oplossing heeft. Dan is $x^2 + 2y^2 \equiv 0 \bmod 4$. Hieruit volgt dat x of y even moet zijn, maar daaruit volgt dat de ander ook even is. Dus is $(x/2)^2 + (y/2)^2 = p$ een oplossing voor de oorspronkelijke vergelijking. Dus als $x^2 + 10y^2 = 4p$ een oplossing heeft, dan heeft $x^2 + 10y^2 = p$ ook een oplossing.

We zien bij elke d dat ofwel $x^2 + 10y^2 = dp$ geen oplossing heeft, ofwel als hij wel een oplossing heeft, dan heeft $x^2 + 10y^2 = p$ ook een oplossing. □

We vinden het op zich niet erg als $x^2 + 10y^2 = dp$ een oplossing heeft voor een $d > 1$, zolang we er maar uiteindelijk uit kunnen concluderen dat $x^2 + 10y^2 = p$ een oplossing heeft. Daarom passen we stap 3 uit het stappenplan aan en voeren we het volgende begrip in.

Definitie 5.3 Gegeven n, laat $c_1, ..., c_k \bmod N_n$ de restklassen van Propositie 3.8 α, β zijn. Dan heet d *regulier voor* n als de volgende uitspraak waar is: als p priem is met $p \equiv c_1, ..., c_k \bmod N_n$ en de vergelijking $x^2 + ny^2 = dp$ een oplossing in $\mathbb{Z}$ heeft, dan bestaat er een $d' \in \mathbb{Z}$ met $0 < d' < d$ zodat $x^2 + ny^2 = d'p$ ook een oplossing in $\mathbb{Z}$ heeft.

Opmerking 5.4
Als we voor een bepaalde d concluderen dat $x^2+ny^2 = dp$ *geen* oplossing in $\mathbb{Z}$ heeft, dan is die d regulier voor n. Daarom veranderen we stap 3 in het stappenplan (van de ($\Leftarrow$) implicatie) in het volgende:
3. Ga voor elke $2 \leq d \leq B_n,\ d \in \mathbb{N}$ na dat d regulier is voor n.
Dit is immers voldoende om te bewijzen dat $x^2 + ny^2 = p$ een oplossing heeft.

De technieken die we daarnet in Propositie 5.2 gebruikten kunnen we ook in algemene vorm opschrijven.

Lemma 5.5 *In de volgende gevallen is d regulier voor n.*

1. $4 \mid d$ *en* $n \equiv 1, 2 \bmod 4$.
2. *Laat p en q twee verschillende priemen zijn. Stel dat* $\left(\frac{p}{q}\right) = 1$, $q \mid n$ *en* $\left(\frac{d}{q}\right) = -1$.

Bewijs
1. Het geval dat $n \equiv 2 \bmod 4$ hebben we net in Propositie 5.2 gezien. Stel $n \equiv 1 \bmod 4$, dan hebben we dat $x^2 + y^2 \equiv 0 \bmod 4$. Daar volgt uit dat x en y weer even zijn, waardoor $(x/2)^2 + n(y/2)^2 = (d/4)p$ ook een oplossing heeft. Hieruit volgt dat d regulier is voor n.
2. Dit is Lemma 5.1. □

We hebben er nu weer een paar technieken bij gekregen die ons gaan helpen om (hopelijk) uiteindelijk een lijst te kunnen geven, die bij elke optredende d aangeeft dat d regulier is. Dadelijk gaan we een groot voorbeeld bekijken. Daar gaan we alle huidige technieken in actie zien komen, maar deze technieken blijken wederom niet voldoende te zijn om van alle optredende waarden d te laten zien dat d regulier is. Daarom geven we eerst nog twee extra lemma's.

Lemma 5.6 *Veronderstel dat d een oneven priemdeler q heeft met $ggd(n, q) = 1$ en* $\left(\frac{-n}{q}\right) = -1$. *Dan is d regulier voor n.*

Bewijs
Stel dat $x^2 + ny^2 = dp$ een oplossing heeft voor zekere $x, y \in \mathbb{Z}$. Dan is $x^2 \equiv -ny^2 \bmod q$. Maar $\left(\frac{-n}{q}\right) = -1$, dus $x \equiv y \equiv 0 \bmod q$, waardoor $dp \equiv x^2 + ny^2 \equiv 0 \bmod q^2$. Uit Propositie 3.8 *a* volgt dat $\left(\frac{-n}{p}\right) = 1 \neq \left(\frac{-n}{q}\right)$, dus $p \neq q$. Daarom volgt nu uit $dp \equiv 0 \bmod q^2$ dat $q^2 \mid d$. Hierdoor heeft de vergelijking $(x/q)^2 + n(y/q)^2 = (d/q^2)p$ ook een oplossing. Dus is d regulier voor n. □

Lemma 5.7 *Laat q een oneven priem zijn en laat r het grootste getal zijn zodat $q^r \mid ggd(n, d)$. Als r oneven is en* $\left(\frac{n/q^r}{q}\right) \neq \left(\frac{d/q^r}{q}\right)$, *dan is d regulier voor n.*

Bewijs
Stel dat $x^2 + ny^2 = dp$ een oplossing heeft, en schrijf $n = q^r n_0$, $d = q^r d_0$ en $r = 2m + 1$, zodat $x^2 + q^r n_0 y^2 = q^r d_0 p$. Dan is $x^2 \equiv 0 \bmod q^r$, maar r is oneven, dus $q^{m+1} \mid x$, waardoor we x

kunnen schrijven als $x = q^{m+1}x_0$. Als we de vergelijking $x^2 + ny^2 = dp$ delen door q^r krijgen we $qx_0^2 + n_0y^2 = d_0p$. Hieruit volgt dat $n_0y^2 \equiv d_0p \bmod q$.
Stel dat $y \not\equiv 0 \bmod q$, dan is $\left(\frac{y^2}{q}\right) = \left(\frac{p}{q}\right) = 1$, want Propositie 3.8 *a* is dankzij $q \mid n$ hier van toepassing. Merk op dat $q \nmid n_0$ *of* $q \nmid d_0$, want r was de grootste macht. Maar $y \not\equiv 0 \bmod q$ samen met $n_0y^2 \equiv d_0p \bmod q$ geeft dat $q \nmid n_0$ *en* $q \nmid d_0$.
Stel $\left(\frac{n_0}{q}\right) = 1$, dan is ook $\left(\frac{d_0}{q}\right) = 1$, maar dat is in tegenspraak met de aanname. Als $\left(\frac{n_0}{q}\right) = -1$ krijgen we op dezelfde manier een tegenspraak.
Dus $y \equiv 0 \bmod q$, waardoor $q^2 \mid y^2$. Maar $x = q^{m+1}x_0$, dus ook $q^2 \mid x^2 = dp$, waardoor $q^2 \mid x^2 + ny^2$. We weten nog steeds dat $\left(\frac{p}{q}\right) = 1$, dus $p \neq q$. Hieruit volgt dat $q^2 \mid d$, waardoor de vergelijking $(x/q)^2 + n(y/q)^2 = (d/q^2)p$ ook een oplossing heeft. Dus kunnen we concluderen dat d regulier is voor n. □

Propositie 5.8 *Als p een priemgetal is, dan:*

$$\exists x, y \in \mathbb{Z} : p = x^2 + 133y^2$$
$$\Longleftrightarrow$$
$$p \equiv \left[\begin{array}{c} 1, 9, 25, 81, 85, 93, 121, 137, 149, 169, 177, 197, 225, 233, 253, \\ 277, 289, 305, 309, 365, 389, 429, 457, 473, 501, 505, 529 \end{array}\right] \bmod 532.$$

Bewijs
We gaan ons weer alleen focussen op het gedeelte waar we van elke $d \in \mathbb{N}$ met $1 < d \leq B_n \leq 14.7$ moeten laten zien dat hij regulier is. Dit zijn er redelijk veel, maar door op te merken dat $133 = 7 \cdot 19$, en door $\left(\frac{d}{7}\right)$ en $\left(\frac{d}{19}\right)$ te bekijken, geeft Lemma 5.1 direct al dat $d = 2, 3, 5, 6, 8, 10, 12, 13$ en 14 allemaal regulier zijn. We hoeven dus nu alleen nog de gevallen $d = 4, 7, 9$ en 11 te bekijken.
Er geldt dat $n \equiv 1 \bmod 4$, dus kunnen we dankzij Lemma 5.5 het geval $d = 4$ ook afstrepen.
Voor $d = 7$ kunnen we ons nieuwe Lemma 5.7 gebruiken, want $7^1 \mid \text{ggd}(133, 7)$ en $\left(\frac{19}{7}\right) = -1 \neq 1 = \left(\frac{1}{7}\right)$.
Voor $d = 9$ en 11 is Lemma 5.6 toepasbaar, omdat $\left(\frac{-133}{3}\right) = \left(\frac{-133}{11}\right) = -1$.
Dus hebben we laten zien dat elke $d \in \mathbb{N}$ met $1 < d \leq B_n$, regulier is. □

Het lijkt er nu wel op dat er soort van kat-en-muisspel ontstaat, waar we steeds de nieuwe problemen oplossen, maar dat er ook steeds weer een nieuwe situatie lijkt te zijn waar het toch weer mis gaat. Dat gezegd hebbende, als we alle optredende waarden d bij alle 65 bekende geschikte getallen zouden afgaan, dan blijkt het dat we toch wel aardig in de buurt komen van een complete lijst van lemma's. De enige situaties waar we nu nog soms geen oplossing voor hebben is wanneer n of d even is. Vooral omdat veel van de lemma's draaien om *oneven* priemdelers. In de volgende stelling geven we een lijst van situaties zodat elke optredende d aan een van de eisen voldoet. Deze lijst lijkt veel op de lijst van Hagedorn [9, Prop. 19], alleen staan de gevallen c en f hier in een algemenere vorm.

Stelling 5.9 *In de volgende gevallen is d regulier voor n.*

a. Er bestaat een oneven priem q met $q \mid n$ en $\left(\frac{d}{q}\right) = -1$.

b. Er bestaat een oneven priem q met $q \mid d$, $ggd(q, n) = 1$ en $\left(\frac{-n}{q}\right) = -1$.

c. $n \equiv 1, 2 \bmod 4$ en $4 \mid d$.

d. Er bestaat een oneven priem q zodat het grootste getal r, waarvoor geldt dat $q^r \mid ggd(n,d)$, oneven is, en bovendien $\left(\frac{n/q^r}{q}\right) \neq \left(\frac{d/q^r}{q}\right)$.

e. Het grootste getal k, waarvoor geldt dat $2^k \mid ggd(n,d)$, is oneven, en $2^{k+1} \mid n$ of $2^{k+1} \mid d$.

f. $n \equiv 3 \bmod 4$ *en* $d \equiv 2 \bmod 4$.

g. $d = 4$ *en* $n \equiv 7 \bmod 8$, $n \equiv 8, 12 \bmod 16$, *of* $n \equiv 16 \bmod 32$.

h. $4 \mid n$ *en* $d \equiv 3 \bmod 4$.

i. $8 \mid n$ *en* $d \equiv 5 \bmod 8$.

j. $(n,d) \equiv (3 \cdot 4^a, 4^a) \bmod 4^{a+1}$, *voor een* $a \geq 1$.

k. $(n,d) \equiv (2 \cdot 9^a, 9^a) \bmod 3^{2a+1}$, *voor een* $a \geq 1$.

Bewijs
De gevallen a tot en met d hebben we al bewezen. Hagedorn bewijst alle andere gevallen niet, ik sla alleen degene over die veel op een ander geval lijken. We veronderstellen steeds dat p voldoet aan de congruenties van Propositie 3.8 α, β. Die eigenschappen komen hier erg goed van pas.
e. Analoog aan *d*, zie Lemma 5.7.
f. Er geldt dat $x^2+3y^2 \equiv 2p \bmod 4$. Kwadraten mod 4 uitschrijven geeft dat $x^2 \equiv 0,1 \bmod 4$ en $3y^2 \equiv 0,3 \bmod 4$. Maar $2p$ is even, dus alleen $x^2 \equiv 0 \bmod 4$ en $3y^2 \equiv 0 \bmod 4$ *of* $x^2 \equiv 1 \bmod 4$ en $3y^2 \equiv 3 \bmod 4$ kunnen. In beide gevallen geldt dat $4 \mid 2p$. Dit is in tegenspraak met $p > 2$ (want $n \geq 3$) en dat p een priemgetal is.
g, h, i. Analoog aan *f*.
j. We zien dat $x^2 \equiv 0 \bmod 4^a$, waardoor $x^2 \equiv i \cdot 4^a \bmod 4^{a+1}$, voor $i = 0,1,2$ *of* 3. Uit $x^2 \equiv 0,1 \bmod 4$ volgt dat i alleen 0 of 1 kan zijn.
Stel dat $x^2 \equiv 0 \bmod 4^{a+1}$, dan $3 \cdot 4^a y^2 \equiv 4^a p \bmod 4^{a+1}$. Hieruit volgt dat $4^a(3y^2 - p) \equiv 0 \bmod 4^{a+1}$, waardoor $3y^2 - p \equiv 0 \bmod 4$. Uit Propositie 3.8 *b* weten we dat $p \equiv 1 \bmod 4$ (want $4 \mid n$), terwijl $3y^2 \equiv 0,3 \bmod 4$ $\lightning$.
Dus $x^2 \equiv 4^a \bmod 4^{a+1}$. Dan is $4^a + 3 \cdot 4^a y^2 \equiv 4^a p \bmod 4^{a+1}$, waardoor $4^a(1 + 3y^2 - p) \equiv 0 \bmod 4^{a+1}$, dus $1 + 3y^2 - p \equiv 0 \bmod 4$. We hebben weer dat $p \equiv 1 \bmod 4$, waardoor $3y^2 \equiv 0 \bmod 4$, en $2 \mid y$. Nu zien we dat $(x/2)^2 + n(y/2)^2 = (d/4)p$ ook een oplossing geeft, want x^2, y^2 en d zijn allen deelbaar door 4. Dus is d regulier voor n.
k. Analoog aan *j*.

Bewijs Hoofdstelling 3.11
Dit bewijs stelt in principe nu niet veel meer voor. Aan het eind van dit document staan een aantal tabellen waarin we kunnen zien dat elk voorkomend paar (n,d) onder (minstens) een van de gevallen van Stelling 5.9 valt. Dus, bij alle 65 bekende geschikte getallen is elke optredende d regulier. Daarmee is de hoofdstelling bewezen. □

Opmerking 5.10
Er zijn ook andere manieren, die veel lijken op die van Hagedorn, om van de getallen uit (2.1) te laten zien dat ze geschikt zijn. Deze andere methoden laten namelijk ook eerst zien dat $\left(\frac{-n}{p}\right) = 1$, en geven daarna een andere bovengrens voor d in de vergelijking: $x^2+ny^2 = dp$. Het

principe is hetzelfde, want bij die andere methoden wordt de vergelijking ook gereduceerd tot $d = 1$. Clark geeft in [5, p. 3] het volgende lijstje methoden, en hun bijbehorende bovengrenzen voor d.

- Lemma van Thue: $d \leq n$.
- Lemma van Vinogradov: $d < 2\sqrt{n}$.
- Stelling van Minkowski: $d \leq \frac{4}{\pi}\sqrt{n}$.

Hier zien we dat Minkowski de beste bovengrens voor d geeft (die wij kennen).

Hiermee zijn we al weer bij het einde gekomen van de interessante invalshoek van Hagedorn van de geschikte getallen. Maar dit is zeker niet het laatste wat er te vertellen valt over deze getallen. Zo kwam Gauss ook de geschikte getallen tegen in zijn werk, maar wel in een andere context, namelijk bij het bestuderen van *kwadratische vormen*. Er is een mooi en interessant verband tussen de geschikte getallen en bepaalde kwadratische vormen. Dit verband gaan we in de volgende twee hoofdstukken bestuderen. We volgen voor een redelijk groot deel Hoofdstuk 2 en 3 van Cox [6].

6 Binaire kwadratische vormen

Definitie 6.1 Een *binaire kwadratische vorm* is een veelterm f in twee variabelen van de vorm:

$$f(x, y) = ax^2 + bxy + cy^2.$$

In deze tekst nemen wij steeds $a, b, c \in \mathbb{Z}$. We noemen een (binaire) kwadratische vorm *primitief* als $\text{ggd}(a, b, c) = 1$.

Omdat we vaak x en y ook in $\mathbb{Z}$ nemen, zien we f als functie van $\mathbb{Z}^2$ naar $\mathbb{Z}$. In het algemeen is f niet surjectief, daarom voeren we het volgende begrip in.

Definitie 6.2 We zeggen dat $m \in \mathbb{Z}$ *gerepresenteerd* wordt door een kwadratische vorm f als er $x, y \in \mathbb{Z}$ bestaan zodat $m = f(x, y)$. Verder zeggen we dat dat m *proper gerepresenteerd* wordt door f als er bovendien geldt dat $\text{ggd}(x, y) = 1$.

Opmerking 6.3
Stel dat m door f gerepresenteerd wordt. Als m kwadraatvrij is, dan is elke representatie van m door f proper. Immers, stel dat $f(x, y) = m$ met $\text{ggd}(x, y) = d > 1$, dan $d^2 \mid m$ $\lightning$.
De omkering is niet altijd waar. Neem bijvoorbeeld $f(x, y) = x^2 + 2xy + y^2$, dan wordt $f(1, 1) = 4 = 2^2$ proper gerepresenteerd.

Het volgende begrip helpt ons om twee kwadratische vormen met elkaar te vergelijken.

Definitie 6.4 Twee kwadratische vormen f en g heten *equivalent* als er $p, q, r, s \in \mathbb{Z}$ bestaan met $ps - qr = 1$ zodat:

$$\forall x, y \in \mathbb{Z} : f(x, y) = g(px + qy, rx + sy).$$

In dat geval schrijven we $f \sim g$.

De volgende propositie komt misschien niet geheel onverwachts, maar hij is wel belangrijk.

Propositie 6.5 *Equivalentie van kwadratische vormen is een equivalentie relatie. Bovendien geldt: als $f \sim g$, dan wordt m gerepresenteerd door f dan en slechts dan als m gerepresenteerd wordt door g.*

Bewijs.
Merk op dat we de eis van Definitie 6.4 ook als volgt kunnen schrijven: er bestaat een matrix

$$A = \left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right), \text{ met } p,q,r,s \in \mathbb{Z}, \ \det(A) = 1 \text{ en } \forall x,y \in \mathbb{Z} : f(x,y) = g((x,y)\cdot A). \tag{6.6}$$

Dan is $f \sim f$ duidelijk, want neem voor A de identiteitsmatrix.
Stel nu dat $f \sim g$, dan is er een matrix A zodat (6.6) geldt. Om nu $g \sim f$ te bewijzen, nemen we de inverse matrix: $A^{-1} = \left(\begin{smallmatrix} s & -r \\ -q & p \end{smallmatrix}\right)$. Dit werkt, omdat nog steeds geldt dat $\det(A^{-1}) = 1$, en uit $f(x,y) = g((x,y)\cdot A)$ volgt dat $g(x,y) = f((x,y)\cdot A^{-1})$.
Nu is transitiveit ook niet erg moeilijk meer: als $f \sim g$, dan geeft (6.6) een bijbehorende matrix A, en als $g \sim h$, dan geeft (6.6) ook een matrix B. Door de matrix AB te nemen zien we nu dat $f \sim h$.

De tweede uitspraak is duidelijk, want als er $x,y \in \mathbb{Z}$ bestaan zodat $f(x,y) = m$, dan hebben we ook dat $g(px+qy, rx+sy) = m$. De omkering gaat natuurlijk net zo, omdat we net hebben bewezen dat $\sim$ een equivalentierelatie is. □

Het volgende lemma is, zoals de meeste lemma's, een uitspraak die later nog goed van pas gaat komen.

Lemma 6.7 *Een geheel getal m wordt door een kwadratische vorm f proper gepresenteerd dan en slechts dan als f equivalent is met de vorm $g(x,y) = mx^2 + Bxy + Cy^2$, voor zekere $B, C \in \mathbb{Z}$.*

Bewijs
($\Rightarrow$): We nemen aan dat er $p,q \in \mathbb{Z}$ bestaan zodat $\gcd(p,q) = 1$ en $f(p,q) = m$. Met behulp van het algoritme van Euclides vinden we $r,s \in \mathbb{Z}$ zodat $ps - qr = 1$.
Schrijf f als $f(x,y) = ax^2 + bxy + cy^2$, dan volgt uit een soortgelijke berekening als in Lemma 6.5 dat:

$$\begin{aligned} f(px+ry, qx+sy) &= f(p,q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r,s)y^2 \\ &= mx^2 + Bxy + Cy^2 = g(x,y). \end{aligned}$$

Dus geldt dat $f \sim g$.
($\Leftarrow$): Neem $p = 1$ en $q = 0$. Dan geldt zeker dat $\gcd(p,q) = 1$, bovendien hebben we dat $g(p,q) = m$. □

Definitie 6.8 Laat $f(x,y) = a^2 + bxy + cy^2$ een kwadratische vorm zijn. Dan noemen we:

$$D = b^2 - 4ac$$

de *discriminant* van f.

Opmerking 6.9
Stel dat $f \sim g$, en dat D_f en D_g de discriminanten van respectievelijk f en g zijn. Door de definities uit te schrijven kun je dan nagaan dat $D_f = D_g$.
Verder zien we ook dat $D \equiv 0, 1 \bmod 4$, want $D \equiv b^2 \bmod 4$.

Propositie 6.10 *Stel dat voor een $D \in \mathbb{Z}$ geldt dat $D \equiv 0, 1 \bmod 4$, en laat m een oneven getal zijn met $ggd(m, D) = 1$. Dan wordt m proper gerepresenteerd door een primitieve kwadratische vorm f met discriminant D dan en slechts dan als D een niet-nul kwadraatrest modulo m is.*

Bewijs
($\Rightarrow$): Uit Lemma 6.7 weten we dat f equivalent is met de vorm $mx^2 + Bxy + Cy^2$, voor zekere $B, C \in \mathbb{Z}$. De discriminant van deze vorm (en dus ook van f) is: $D = B^2 - 4mC$, waardoor $D \equiv B^2 \bmod m$. Let op: we zijn nog niet klaar, want $B \equiv 0 \bmod m$ zou namelijk kunnen, maar omdat $\gcd(m, D) = 1$ gaat het toch goed.
($\Leftarrow$): Stel dat $D \equiv B^2 \bmod m$, voor een $B \in \mathbb{Z} \setminus \{0\}$. B kan zowel even als oneven zijn, en $D \equiv 0, 1 \bmod 4$ zegt hetzelfde over D. Maar m is oneven, dus als we

$$B' = \begin{cases} B & \text{als } B \equiv D \bmod 2 \\ B + m & \text{als } B \not\equiv D \bmod 2 \end{cases}$$

definiëren, dan geldt dat D en B' beide ofwel even, ofwel oneven zijn. Sterker nog: in beide geval hebben we dat $D \equiv (B')^2 \bmod 4$. Samen met $D \equiv (B')^2 \bmod m$ geeft dit dat $D \equiv (B')^2 \bmod 4m$, want m is oneven, dus is $\gcd(m, 4) = 1$.
Dit betekent dat $D = (B')^2 - 4mC$, voor een zekere $C \in \mathbb{Z}$. Bekijk $f(x, y) = mx^2 + B'xy + Cy^2$. We zien dat m proper gerepresenteerd wordt door f: neem $(x, y) = (1, 0)$, bovendien is de discriminant van f precies D. Tot slot is f ook primitief, want $1 = \gcd(m, D) = \gcd(m, (B')^2)$, waardoor $\gcd(m, B', C) = 1$. □

Gevolg 6.11 *Gegeven $n \in \mathbb{Z}$ en een oneven priemgetal p met $p \nmid n$. Dan is $\left(\frac{-n}{p}\right) = 1$ dan en slechts dan als p gerepresenteerd wordt door een primitieve kwadratische vorm met discriminant $-4n$.*

Bewijs
Merk op dat $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)\left(\frac{2^2}{p}\right) = \left(\frac{-n}{p}\right)$. Het resultaat volgt nu uit Propositie 6.10. □

Dit is op zich een mooi resultaat, maar de uitspraak: *een primitieve kwadratische vorm met discriminant $-4n$*, kunnen we iets specifieker maken, door te laten zien dat zo'n vorm equivalent is met een simpelere vorm.

Voordat we daar wat zinnigs over kunnen zeggen, maken we eerst een paar opmerkingen over de discriminant.

Opmerking 6.12
Stel dat $f(x, y) = ax^2 + bxy + cy^2$ een kwadratische vorm is met discriminant D. Dan geldt dat:

$$4af(x, y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - Dy^2.$$

Als $D > 0$, dan zien we dat f zowel positieve als negatieve getallen representeert. Maar als $D < 0$ dan representeert f alleen maar niet-negatieve getallen (0 kun je altijd maken), of

alleen maar niet-positieve getallen, afhankelijk van het teken van a. Om hier onderscheid in te maken, voeren we het volgende begrip in.

Definitie 6.13 Laat $f(x,y) = ax^2 + bxy + cy^2$ een kwadratische vorm zijn met discriminant D. Stel dat $D < 0$, als $a > 0$, dan noemen we f *positief definiet*, als $a < 0$, dan noemen we f *negatief definiet*. Als $D > 0$, dan noemen we f *indefiniet*.

We kunnen het nu gaan hebben over de "simpelere" vormen, waar we net erg vaag over waren.

Definitie 6.14 *Een primitieve positief definiete vorm $ax^2 + bxy + cy^2$ heet gereduceerd als:*

$$|b| \leq a \leq c, \text{ en als } |b| = a \text{ òf } a = c, \text{ dan } b \geq 0.$$

Merk op dat de kwadratische vorm $x^2 + ny^2$ als $n > 0$ altijd gereduceerd is.

We kunnen nu ons resultaat van Gevolg 6.11 (in het geval dat $n > 0$) verbeteren, met behulp van de volgende stelling.

Stelling 6.15 *Elke primitieve positief definiete kwadratische vorm is equivalent met een unieke gereduceerde kwadratische vorm.*

Bewijs
We laten eerst zien dat zo'n primitieve positief definiete vorm g equivalent is met *een* gereduceerde vorm, de uniciteit komt daarna.
Pak van al de vormen die equivalent zijn met g, de $f(x,y) = ax^2 + bxy + cy^2$ zodat $|b|$ zo klein mogelijk is.

Stel dat $a < |b|$. Voor elk getal $m \in \mathbb{Z}$ geldt dat:

$$h(x,y) = f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$$

equivalent is met f (en dus ook met g), de transformatiematrix $\left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)$ heeft namelijk determinant 1. Merk nu op dat er een $m \in \mathbb{Z}$ is zodat $|2am + b| < |b|$, want $a < |b|$. Dit is in tegenspraak met onze aanname over f en g. Dus geldt dat $a \geq |b|$.
Verder kunnen we ook aannemen dat $c \geq a$. Want als $a > c$, dan draaien we a en c om door middel van de equivalentie:

$$h(x,y) = f(-y,x) = cx^2 + -bxy + ay^2.$$

Dus krijgen we een vorm waarvoor geldt dat $|b| \leq a \leq c$.

Die vorm is niet gereduceerd als $b < 0$ en $a = -b$, of $b < 0$ en $a = c$. Maar in die twee gevallen is $ax^2 - bxy + cy^2$ in ieder geval wel gereduceerd, dus laten we zien dat de twee vormen $ax^2 \pm bxy + cy^2$ equivalent zijn.

Als $a = -b$: doe dan $(x,y) \mapsto (x + y, y)$, zodat $(ax^2 - axy + cy^2) \sim (ax^2 + axy + cy^2)$.

Als $a = c$: doe dan $(x,y) \mapsto (-y,x)$, zodat $(ax^2 + bxy + ay^2) \sim (ax^2 - bxy + ay^2)$.

Dus is elke primitieve positief definiete vorm equivalent met een gereduceerde vorm.

We gaan nu laten zien dat er tot op equivalentie na ook maar één mogelijkheid is. We doen dit door te bewijzen dat verschillende gereduceerde vormen niet equivalent kunnen zijn. Stel dat $f(x,y) = ax^2 + bxy + cy^2$ gereduceerd is. Dan:

$$ax^2 + bxy + cy^2 \geq (a - |b| + c)\min(x^2, y^2).$$

Immers: als $bxy \geq 0$, dan is het duidelijk waar, en als bijvoorbeeld $x \geq y \geq 0$, en $b \leq 0$, dan:

$$ax^2 + bxy = ax^2 - |b|xy \geq ax^2 - |b|x^2 \geq (a - |b|)y^2, \text{ want } |b| \leq a \leq c,$$

waaruit volgt dat:

$$ax^2 + bxy + cy^2 \geq (a - |b| + c)y^2 = (a - |b| + c)\min(x^2, y^2).$$

Als $y \geq x \geq 0$, dan kunnen we hetzelfde als hierboven doen, maar dan met $bxy + cy^2$. De andere gevallen gaan ongeveer hetzelfde. Als bijvoorbeeld $x \leq 0 \leq y$ en $b \leq 0$, dan kunnen we door onderscheid te maken in of $x^2 \geq y^2$ of $y^2 \geq x^2$ geldt, weer in een van de twee gevallen hierboven terecht komen.

Stel nu eerst dat $|b| < a < c$, daarna bekijken we weer de randgevallen.
Als $xy \neq 0$, dan $f(x, y) \geq a - |b| + c$. Door dit te combineren met $|b| < a < c$ krijgen we dat $a = f(1, 0)$ de kleinste niet-nul waarde is die proper gerepresenteerd wordt door f, daarna komt $c = f(0, 1)$. Immers, als $x = 0$, dan mag voor een propere niet-nul representatie alleen gelden dat $y = \pm 1$, en als $y = 0$, dan alleen $x = \pm 1$. We zien dus dat de buitenste twee coëfficienten van een gereduceerde vorm precies de kleinste waarden zijn die proper gerepresenteerd worden door die vorm.
Merk nu op dat $a < c < a - |b| + c$, en dat $a - |b| + c$ de derde in de lijst van kleinste getallen is die *proper* door f gerepresenteerd worden. Hieruit volgt dat:

$$\begin{aligned} f(x, y) = a \text{ en } \gcd(x, y) = 1 &\iff (x, y) = \pm(1, 0), \\ f(x, y) = c \text{ en } \gcd(x, y) = 1 &\iff (x, y) = \pm(0, 1). \end{aligned} \tag{6.16}$$

Stel nu dat $g(x, y) = a'x^2 + b'xy + c'y^2$ equivalent is met f, en net als f gereduceerd is. Dan zien we op dezelfde manier als hierboven dat a' het kleinste niet-nul getal is dat door g wordt gerepresenteerd. Uit $f \sim g$ volgt nu dat $a = a'$. Bovendien krijgen we ook weer op dezelfde manier dat $c' = a$, of $c' = c$ (we eisen niet voor g dat de ongelijkheden uit Definitie 6.14 strikt zijn).
Als $c' = a$, dan wordt a door g op vier manieren proper gerepresenteerd: $(x, y) = \pm(1, 0)$ en $(x, y) = \pm(0, 1)$. Maar f doet dat maar op twee manieren: $(x, y) = \pm(1, 0)$ $\lightning$, dus $c' = c$. Nu gaan we gebruiken dat voor de discriminanten geldt dat: $b^2 - 4ac = (b')^2 - 4a'c'$, waardoor $b' = \pm b$. We zien dus dat $g(x, y) = ax^2 \pm bxy + cy^2$.
Verder geeft $f \sim g$ dat $g(x, y) = f(px + qy, rx + sy)$, voor zekere $p, q, r, s \in \mathbb{Z}$ met $ps - qr = 1$. Dan geldt dat $\gcd(p, r) = \gcd(q, s) = 1$, en dat $a = g(1, 0) = f(p, r)$ en $c = g(0, 1) = f(q, s)$ propere representaties zijn. Maar dan volgt uit (6.16) en $ps - qr = 1$ dat $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Hier volgt nu uit dat $f(x, y) = g(x, y)$.

We hoeven nu alleen nog de gevallen te bekijken dat $a = c$ of $a = |b|$.
Stel dat $a = c$, dan volgt uit Definitie 6.14 dat $a \neq |b|$. We krijgen dan weer op dezelfde manier als hierboven dat $a = a'$. Voor c' krijgen we nu dat $c' = a$ of $c' = 2a - |b|$. Stel dat $c' = 2a - |b|$. We zien dat f op vier manieren a proper representeert, en dat dit keer g dat maar op twee manieren doet $\lightning$, dus $c' = a$. Om dit keer in te zien dat $b = b'$ merken we op dat uit Definitie 6.14 volgt dat $b, b' \geq 0$, en door nu weer de discriminanten te vergelijken krijgen we dat $f(x, y) = g(x, y)$.
Bekijk tot slot het geval dat $a = |b|$. We krijgen weer dat $a = a'$. Stel nu dat $a' \neq |b'|$, dan geldt ofwel $|b'| < a' < c'$, ofwel $|b'| < a' = c'$. Als we nu de rollen van f en g omdraaien, dan zien we dat we deze gevallen hierboven al gedaan hebben. Dus kunnen we aannemen dat $a' = |b'|$. Door weer de discriminanten te vergelijken, en Definitie 6.14 te gebruiken, zien we wederom dat $f(x, y) = g(x, y)$. □

Gevolg 6.17 *Gegeven $n \in \mathbb{N}_{>0}$ en een oneven priemgetal p met $p \nmid n$. Dan is $\left(\frac{-n}{p}\right) = 1$ dan en slechts dan als p proper gerepresenteerd wordt door een unieke gereduceerde kwadratische vorm met discriminant $-4n$.*

Bewijs
De discriminant is negatief, want $n > 0$. Bovendien is p positief, dus als een vorm p representeert, dan volgt uit Opmerking 6.12 dat die vorm positief definiet is. Het resultaat volgt nu uit Gevolg 6.11 samen met Stelling 6.15. □

Een vraag die door Stelling 6.15 en Gevolg 6.17 mogelijk bij je opkomt is: hoeveel gereduceerde vormen zijn er voor een specifieke discriminant? Om antwoord te geven op die vraag voeren we eerst een nieuw begrip in, waar we daarna een sterke uitspraak over gaan bewijzen.

Definitie 6.18 *Twee kwadratische vormen zitten in dezelfde klasse als $f \sim g$. Bovendien definiëren we het klassengetal $h(D)$ als het aantal klassen van primitieve positief definiete vormen met discriminant D.*

Stelling 6.19 *Neem $D < 0$ vast. Dan is $h(D)$ eindig, en $h(D)$ is gelijk aan het aantal gereduceerde vormen van discriminant D.*

Bewijs
Stel dat $f(x, y) = ax^2 + bxy + cy^2$ een gereduceerde vorm is met discriminant $D < 0$. Dan:

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2, \text{ want } b^2 \leq a^2 \text{ en } c \geq a.$$

Hieruit volgt dat $a \leq \sqrt{-D/3}$.
Dit impliceert dat we voor een vaste D maar eindig veel keuzes hebben voor f. Immers, $|b| \leq a$ en $a \leq \sqrt{-D/3}$ geeft dat er maar eindig veel keuzes voor zijn a en b. Merk nu op dat hetzelfde ook voor c geldt, want $D = b^2 - 4ac$ (en D is vast).

Uit Stelling 6.15 volgt nu dat $h(D)$ gelijk is aan het aantal gereduceerde vormen van discriminant D, daaruit volgt dat $h(D)$ eindig is. □

Opmerking 6.20
Het bovenstaande bewijs laat niet alleen zien dat er maar eindig veel van dat soort vormen f zijn, het geeft zelfs een manier om te bepalen hoeveel het er zijn. Voor kleine waarden van D kun je op deze manier redelijk gemakkelijk het klassengetal $h(D)$ bepalen. Voor grotere waarden kun je ook een computer gebruiken.

Hieronder geven een tabel met daarin alle gereduceerde vormen voor een paar vaste waarden van D. Deze voorbeelden komen uit Cox [6, (2.14)].

Aan het eind van Hoofdstuk 5 werd aangekondigd dat er een verband zou zijn tussen de geschikte getallen van Euler en bepaalde kwadratische vormen. Tot nu toe hebben we daar alleen nog niet veel van gezien, maar daar gaat in het volgende hoofdstuk verandering in komen. We hebben alleen nog wel meer kennis nodig over de theorie van de kwadratische vormen, en in het bijzonder over de zogeheten *geslachtstheorie*.

D	$h(D)$	Alle gereduceerde vormen van discriminant D
-4	1	x^2+y^2
-8	1	x^2+2y^2
-12	1	x^2+3y^2
-20	2	x^2+5y^2, $2x^2+2xy+3y^2$
-28	1	x^2+7y^2
-56	4	x^2+14y^2, $2x^2+7y^2$, $3x^2\pm 2xy+5y^2$

Tabel 1: De gereduceerde vormen voor een paar waarden van de discriminant D.

7 Geslachtstheorie en Compositie

Het idee van geslachtstheorie is het volgende. We nemen een discriminant $D<0$ vast. Uit Stelling 6.19 weten we dat er maar eindig veel gereduceerde kwadratische vormen van discriminant D zijn. De geslachtstheorie gaat nu dit groepje gereduceerde vormen weer onderling van elkaar onderscheiden.

Definitie 7.1 Gegeven een discriminant $D<0$, zeggen we dat twee primitieve positief definiete kwadratische vormen *in hetzelfde genus liggen*, als ze dezelfde waarden representeren in $(\mathbb{Z}/D\mathbb{Z})^*$.

Deze nieuwe definitie wordt waarschijnlijk duidelijker als we een paar voorbeelden bekijken, dus laten we dat maar direct gaan doen.

Voorbeeld 7.2
1. Bekijk $D=-20$. In Tabel 1 zien we dat er twee gereduceerde vormen zijn bij deze discriminant: $f(x,y)=x^2+5y^2$ en $g(x,y)=2x^2+2xy+3y^2$.
We zien dat $f(x,y)\equiv x^2 \bmod 5$. Alle kwadraten mod 5 uitschrijven geeft dat $f(x,y)\equiv 0,1,4 \bmod 5$. Verder is $f(x,y)\equiv x^2+y^2 \bmod 4$, waardoor $f(x,y)\equiv 0,1,2 \bmod 4$. Door nu de Chinese reststelling te gebruiken, of door alle mogelijkheden af te lopen, zien we dat f alleen de waarden 1 en 9 representeert in $(\mathbb{Z}/D\mathbb{Z})^*$. Hier hebben we dus de waarden weggelaten die ggd $\neq 1$ hebben met 20.
Dit kunnen we ook soortgelijk doen van g, alleen is het daar mogelijk iets meer werk. Straks in Propositie 7.3 hieronder geven we een gemakkelijkere manier om deze getallen te bepalen. Dadelijk zien we in Opmerking 7.4 dat g de waarden 3 en 7 in $(\mathbb{Z}/D\mathbb{Z})^*$ representeert.
We zien dus dat f en g niet in hetzelfde genus liggen. Verder zien we dat alle genera maar uit één klasse bestaan, want f en g waren de enige gereduceerde vormen bij deze discriminant.
2. Bekijk nu $D=-56$. Op een soortgelijke manier als hierboven krijgen we dat de twee gereduceerde vormen x^2+14y^2 en $2x^2+7y^2$ de getallen 1, 9, 15, 23, 25 en 39 in $(\mathbb{Z}/D\mathbb{Z})^*$ representeren. De andere twee: $3x^2\pm 2xy+5y^2$ representeren 3, 5, 13, 19, 27, 45 in $(\mathbb{Z}/D\mathbb{Z})^*$. Hier zien we dus dat er weer twee genera zijn, maar dit keer bestaan ze allebei uit twee klassen.

Propositie 7.3 *Gegeven een negatief getal $D\equiv 0,1 \bmod 4$, en laat $f(x,y)=ax^2+bxy+cy^2$ een vorm zijn met discriminant D. Dan geldt dat:*

1. *De waarden die door de hoofdvorm van discriminant D:*

$$x^2 - \frac{D}{4}y^2 \qquad \text{als } D \equiv 0 \bmod 4,$$
$$x^2+xy + \frac{1-D}{4}y^2 \qquad \text{als } D \equiv 1 \bmod 4.$$

   worden gerepresenteerd in $(\mathbb{Z}/D\mathbb{Z})^*$ vormen een ondergroep $H \subset (\mathbb{Z}/D\mathbb{Z})^*$.

2. *De waarden in $(\mathbb{Z}/D\mathbb{Z})^*$ die door f gerepresenteerd worden vormen een nevenklasse van H in $(\mathbb{Z}/D\mathbb{Z})^*$. Als bovendien geldt dat $ggd(a, D) = 1$, dan wordt deze nevenklasse gegeven door $[a]^{-1}H$.*

Bewijs
Zie Cox [6, p. 31, 32]. □

Opmerking 7.4
We kunnen nu de waarden van g uit het eerste deel van Voorbeeld 7.2 gemakkelijk bepalen. Merk wel op dat $\text{ggd}(2, 20) \neq 1$, maar omdat $g(x, y) = 2x^2 + 2xy + 3y^2$ en $h(x, y) = 3x^2 + 2xy + 2y^2$ dezelfde waarden representeren, kunnen we net zo goed h bekijken. Bij h geldt wel dat $\text{ggd}(3, 20) = 1$, waardoor Propositie 7.3 nu wel van toepassing is. We zagen dat de hoofdvorm $f(x, y) = x^2 + 5y^2$ de waarden 1 en 9 representeert. Verder is $3^{-1} \equiv 7 \bmod 20$, waardoor g de waarden 7 en $7 \cdot 9 \equiv 3 \bmod 20$ representeert in $(\mathbb{Z}/D\mathbb{Z})^*$.

Met behulp van de geslachtstheorie kunnen we dus uitspraken doen over primitieve positief definiete vormen met een vaste discriminant $D < 0$. In het volgende stuk gaan we weer deze vormen bekijken, maar nu gaan we er iets heel anders mee doen. We gaan namelijk bekijken wat het betekent om twee vormen samen te stellen. We gaan zien dat dit niet de "normale" samenstelling is van functies: $f \circ g$. Wat we er dan wel mee bedoelen gaan we nu bekijken.

Definitie 7.5 (Lagrange en Gauss)
Gegeven twee primitieve positief definiete vormen f en g met discriminant D, is de samenstelling van f en g *een* vorm F met discriminant D, mits de volgende gelijkheden gelden:

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)), \text{ waar}$$
$$B_i(x, y; z, w) = a_ixz + b_ixw + c_iyz + d_iyw, \text{ voor } i = 1, 2.$$

Waar de B_1 en B_2 bilineaire vormen zijn in de variabelen x, y en z, w.

Voorbeeld 7.6
Voor $n \in \mathbb{Z}$ geldt de volgende vergelijking:

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2 \tag{7.7}$$

Hiermee zien we dat *een* samenstelling van $f(x, y) = x^2 + 5y^2$ met zichzelf weer $x^2 + 5y^2$ is.

We hebben het hier steeds over *een* samenstelling, dat komt doordat de manier waarop we een samenstelling gedefinieerd hebben, de mogelijkheid geeft voor meerdere opties. Zo laat Cox [6, p. 38] zien dat de vormen $14x^2 + 10xy + 21y^2$ en $9x^2 + 2xy + 30y^2$ op 4 manieren samengesteld kunnen worden. Daarom willen we definitie scherper maken, zodat het samenstellen van gereduceerde vormen (tot op equivalentie na!) welgedefinieerd is.

Cox, of eigenlijk Gauss, liet zien dat voor de vormen B_i bij Definitie 7.5 het volgende geldt:

$$a_1b_2 - a_2b_1 = \pm f(1,0) \text{ en } a_1c_2 - a_2c_1 = \pm g(1,0). \tag{7.8}$$

Bovendien liet Gauss zien dat door te eisen dat beide $\pm$ tekens + tekens worden, de samenstelling dan wel welgedefinieerd is. Als dat het geval is, dan noemen we de samenstelling de *directe samenstelling*.

We gaan nu een een variant bekijken op de directe samenstelling die minder algemeen is. Desondanks gaat deze variant goed van pas komen voor onze doeleinden.

Definitie 7.9 (Dirichlet)
Laat $f(x,y) = ax^2 + bxy + cy^2$ en $g(x,y) = a'x^2 + b'xy + c'y^2$ twee primitieve positief definiete kwadratische vormen van discriminant $D < 0$ zijn, waar bovendien voor geldt dat $\text{ggd}(a, a', (b+b')/2) = 1$. Dan is de *Dirichlet samenstelling* van f en g:

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

waar B een geheel getal is, zodat:

$$B \equiv b \bmod 2a, \quad B \equiv b' \bmod 2a', \quad B^2 \equiv D \bmod 4aa'.$$

De Dirichlet samenstelling voldoet gelukkig aan allemaal fijne eigenschappen die we samenvatten in de volgende propositie. Het bewijs van deze propositie slaan we over, zodat we ons sneller kunnen gaan richten op ons uiteindelijke doel: stellingen bewijzen over geschikte getallen! Zie Cox [6, p. 43-45] voor een (gedeeltelijk) bewijs. In Voorbeeld 7.13 gaan we nog wel bekijken hoe deze samenstelling werkt, zodat we nog wel weten waar we mee bezig zijn.

Propositie 7.10 *Neem f en g als in Definitie* 7.9*. Dan is het getal B uit die definitie uniek bepaald* mod $2aa'$*. Verder is de Dirichlet samenstelling F van f en g een primieve positief definiete vorm met discriminant D. Tot slot is F een directe samenstelling, in de zin van Definitie* 7.5 *en vergelijking* (7.8)*.* □

Door te eisen dat $\text{ggd}(a, a', (b+b')/2) = 1$, zien we dat deze samenstelling inderdaad minder algemeen is dan de directe samenstelling uit Definitie 7.5. Maar, de volgende stelling laat zien dat de Dirichlet samenstelling wel erg handig is onze setting. We geven wel eerst een nieuwe definitie, waar het klassengetal weer naar voren komt.

Definitie 7.11 Gegeven een discriminant $D < 0$, noemen we $C(D)$ de verzameling van klassen van primitieve positief definiete vormen met discriminant D. Uit Stelling 6.19 volgt dat $|C(D)| = h(D)$ eindig is.

De volgende stelling geeft aan wat de structuur van de klassengroep is. Voor het bewijs van deze stelling moet erg veel uitgeschreven worden, dus verwijzen we naar Cox [6, p. 46]. Om het goed te maken doen we straks Voorbeeld 7.13, zodat we wel weten hoe we met de klassengroep kunnen werken.

Stelling 7.12 *Stel dat $D \equiv 0, 1 \bmod 4$ negatief is. Dan induceert de Dirichlet samenstelling een welgedefinieerde binaire bewerking op $C(D)$, dit maakt $C(D)$ een eindige abelse groep van orde $h(D)$. Verder is het eenheidselement van $C(D)$ de klasse die de hoofdvorm bevat:*

$$\begin{aligned} x^2 - \frac{D}{4}y^2 & \qquad \text{als } D \equiv 0 \bmod 4, \\ x^2 + xy + \frac{1-D}{4}y^2 & \qquad \text{als } D \equiv 1 \bmod 4. \end{aligned}$$

Tot slot is de inverse van de klasse die de vorm $ax^2 + bxy + cy^2$ bevat, de klasse die $ax^2 - bxy + cy^2$ bevat.

Voorbeeld 7.13
Bekijk $f(x, y) = 2x^2 + 2xy + 3y^3$. We gaan de Dirichlet samenstelling van f met zichzelf berekenen. Als $a = 2$, $b = 2$ en $c = 3$, dan is $\text{ggd}(a, a, (b + b)/2) = 2 \neq 1$, dus kunnen we hier de Dirichlet samenstelling niet op toepassen. Maar merk nu op dat $(x, y) \mapsto (-y, x)$ een equivalentie van kwadratische vormen geeft (bekijk bijvoorbeeld de bijbehorende transformatiematrix).

Neem $g(x, y) = f(-y, x) = 3x^2 - 2xy + 2y^2$, dan is $f \sim g$, en dat is voldoende, omdat we alles toch tot op equivalentie na bekijken. We krijgen nu dat $a' = 3$, $b' = -2$, $c' = 2$, waardoor gelukkig aan $\text{ggd}(a, a', (b + b')/2) = 1$ voldaan wordt, zodat we de Dirichlet samenstelling van f en g kunnen berekenen.

De volgende stap is het getal $B \bmod 2aa'$ bepalen. Merk op dat $D = -20$, we zien dat:

$$B \equiv 2 \bmod 4, \quad B \equiv 4 \bmod 6, \quad B^2 \equiv 4 \bmod 24.$$

Er geldt dat $2aa' = 12$, en door alle waarden $\bmod 12$ te bekijken zien we dat $B \equiv 10 \bmod 12$. Hieruit volgt dat $F(x, y) = 6x^2 + 10xy + 5y^2$ de Dirichlet samenstelling van f met zichzelf is.

Bekijk nu de transformatie: $(x, y) \mapsto (-x, x - y)$, dit geeft ook weer een equivalentie van kwadratische vormen. Door deze transformatie op F toe te passen, krijgen we $G(x, y) = x^2 + 5y^2$. Maar dan is G volgens Stelling 7.12 precies het eenheidselement van de klassengroep $C(-20)$! De lezer is hier mogelijk minder enthousiast over dan de auteur, in Tabel 1 zagen we namelijk dat $h(-20) = 2$, waardoor de orde van onze f in de klassengroep hoogstens 2 is.

In Stelling 7.17 gaan we de verschillende onderwerpen waar we het in dit hoofdstuk over gehad hebben terug zien. Voordat we het bewijs daarvan kunnen geven, hebben we nog wel eerst een lemma nodig.

Lemma 7.14 *Zij $D \equiv 0, 1 \bmod 4$ een negatief getal. Dan gelden de volgende uitspraken:*

1. *Alle genera bij discriminant D bestaan uit hetzelfde aantal klassen.*
2. *Er bestaan $2^{\mu-1}$ genera bij discriminant D, waar*

$$\mu = \begin{cases} r & \text{als } n \equiv 3 \bmod 4, \\ r + 1 & \text{als } n \equiv 1, 2, 4, 5, 6 \bmod 8, \\ r + 2 & \text{als } n \equiv 0 \bmod 8, \end{cases}$$

en r het aantal verschillende oneven priemdelers van D is.

3. *Het genus die de hoofdvorm bevat heet het hoofdgenus, en bestaat uit de klassen van $C(D)^2$. Dat wil zeggen: elke vorm in het hoofdgenus is de Dirichlet samenstelling van een bepaalde vorm met zichzelf.*

Bewijs
Cox [6, Cor. 3.14, Thm. 3.15]. □

Stelling 7.15 *Gegeven $n \in \mathbb{N}_{>0}$, zijn volgende uitspraken equivalent:*

1. *Elke genus van vormen van discriminant $-4n$ bestaat uit een enkele klasse.*
2. *Elk element van de klassengroep $C(-4n)$ heeft orde ≤ 2.*
3. *Het klassengetal $h(-4n)$ is gelijk aan $2^{\mu-1}$.*

Bewijs
(1) $\Rightarrow$ (2) : Als we *1* aannemen, dan bestaat in het bijzonder het hoofdgenus ook maar uit een enkele klasse. Hieruit volgt dat $C(D)^2 = \{1\}$, waardoor elk element in de klassengroep orde ≤ 2 heeft.
(2) $\Rightarrow$ (3) : Merk op dat $C(D)^2 < C(D)$ een ondergroep is, want het bevat het eenheidselement, en het is gesloten onder de groepsbewerking. Daarom kunnen we het hebben over de index van groepen: $[C(D) : C(D)^2]$. We weten dat $C(D)$ en $C(D)^2$ eindige groepen zijn (Stelling 6.19), dus $[C(D) : C(D)^2] = \frac{|C(D)|}{|C(D)^2|}$. Door nu alle drie de uitspraken van Lemma 7.14 te gebruiken, krijgen we dat: $[C(D) : C(D)^2] = 2^{\mu-1}$. Hieruit volgt (zonder nog de aanname te gebruiken) dat:

$$h(-4n) = |C(D)| = [C(D) : C(D)^2] \cdot |C(D)^2| = 2^{\mu-1}|C(D)^2|. \tag{7.16}$$

Onze aanname is dat elk element in $C(D)$ orde ≤ 2 heeft, dus is $C(D)^2 = \{1\}$. We kunnen nu concluderen dat $h(-4n) = 2^{\mu-1}$.
(3) $\Rightarrow$ (1) : Uit *3* en (7.16) volgt dat $|C(D)^2| = 1$. Dit betekent dat het hoofdgenus maar uit één klasse bestaat. Lemma 7.14.1 geeft nu dat elke genus maar uit één klasse bestaat. □

Het lijkt erop dat het moment nu eindelijk is aangebroken waar we het verband tussen de geschikte getallen en de kwadratische vormen gaan zien. Gauss kwam namelijk met de volgende stelling.

Stelling 7.17 *Een getal $n \in \mathbb{N}_{>0}$ is geschikt dan en slechts dan als voor de primitieve positief definiete vormen van discriminant $-4n$ geldt dat elke genus uit een enkele klasse bestaat.*

Voorbeeld 7.18
In Voorbeeld 7.2.1 zagen we dat bij $n = 5$ alle genera maar uit een enkele klasse bestaan. Dus als we de bovenstaande stelling hebben bewezen, kunnen we concluderen dat 5 een geschikt getal is.

Omdat we dit moment even willen koesteren geven we eerst een paar lemma's, deze gaan we wel allemaal bewijzen.

Lemma 7.19 *Laat m een positief oneven getal zijn dat relatief priem is met $n > 1$. Het aantal oplossingen modulo m van de vergelijking $x^2 \equiv -n \bmod m$ wordt gegeven door:*

$$\prod_{p|m} \left(1 + \left(\frac{-n}{p}\right)\right).$$

Bewijs
We gaan de volgende toepassing van de Chinese reststelling gebruiken: stel dat $\text{ggd}(r, s) = 1$, en dat voor een polynoom $f(x)$ geldt dat er a oplossingen zijn voor de vergelijking $f(x) \equiv 0 \bmod r$, en b voor de vergelijking $f(x) \equiv 0 \bmod s$, dan zijn er ab oplossingen voor de vergelijking $f(x) \equiv 0 \bmod rs$. Laat $m = \prod_i q_i^{e_i}$ de priemfactorisatie van m zijn. Dan is het voldoende om het aantal oplossingen van $f(x) \equiv 0 \bmod q_i^{e_i}$ te bepalen voor elke i.

Stel dat $\left(\frac{-n}{q_i}\right) = -1$. Dan heeft $x^2 \equiv -n \bmod q_i^{e_i}$ geen oplossing, want stel dat $z \in \mathbb{Z}$ een oplossing van die vergelijking is, dan is z ook een oplossing van de vergelijking $x^2 \equiv -n \bmod q_i$ ↯. Dit is overeenstemming met de uitspraak van het lemma, want $1 + \left(\frac{-n}{q_i}\right) = 0$.

Stel dat $\left(\frac{-n}{q_i}\right) = 1$. Dan is er dus een $c \in \mathbb{Z}$ zodat $c^2 \equiv -n \bmod q_i$. We kunnen nu deze oplossing via *Hensel's lemma* "liften" naar een oplossing $z \bmod q_i^{e_i}$, zie [14, p. 43]. Claim: naast $x = z$ en $x = -z$ heeft de vergelijking $x^2 \equiv -n \bmod q_i^{e_i}$ geen oplossingen. Neem namelijk een oplossing y van die vergelijking. Dan is $z^2 \equiv y^2 \bmod q_i^{e_i}$, waardoor $(z - y)(z + y) \equiv 0 \bmod q_i^{e_i}$. In het geval dat $e_i = 1$ zien we dat $y \equiv \pm z \bmod q_i^{e_i}$, waardoor we de oplossingen z en $-z$ weer krijgen. Stel daarom dat $e_i > 1$.
Er geldt dat $q_i^{e_i} \mid (z - y)(z + y)$, stel dat er een $0 < k < e_i$ is zodat:

$$q_i^{e_i - k} \mid (z - y) \text{ en } q_i^k \mid (z + y).$$

Dan deelt q_i de som: $q_i \mid (z - y + z + y) = 2z$. Merk op dat $\text{ggd}(m, n) = 1$ impliceert dat $\text{ggd}(q_i, n) = 1$. Verder geeft $z^2 \equiv -n \bmod q_i^{e_i}$ dat $z^2 = -n + l \cdot q_i^{e_i}$ voor een $l \in \mathbb{Z}$, waardoor $q_i \nmid z$ ↯.
Dus hebben we dat ofwel $q_i^{e_i} \mid (z - y)$, ofwel $q_i^{e_i} \mid (z + y)$. In beide gevallen krijgen we weer dat $y \equiv \pm z \bmod q_i^{e_i}$, dus zijn dat inderdaad de enige twee oplossingen van de vergelijking $x^2 \equiv -n \bmod q_i^{e_i}$.
Dit is ook weer in overeenstemming met de uitspraak van het lemma, want $1 + \left(\frac{-n}{q_i}\right) = 2$.

Uit onze eerdere opmerking over de Chinese reststelling volgt nu dat de vergelijking $x^2 \equiv -n \bmod m$ precies

$$\prod_{p|m} \left(1 + \left(\frac{-n}{p}\right)\right)$$

oplossingen heeft. □

Lemma 7.20 *Laat m een positief en oneven getal zijn dat relatief priem is met $n > 1$. Het aantal manieren waarop m proper gerepresenteerd wordt door een gereduceerde vorm van discriminant $-4n$ is:*

$$2 \prod_{p|m} \left(1 + \left(\frac{-n}{p}\right)\right).$$

Bewijs
We volgen de stappen van opgave 3.20 van Cox [6], onderdeel a was Lemma 7.19.

Nu komt onderdeel b. Bekijk de kwadratische vormen g met discriminant $-4n$ van de vorm:

$$g(x,y) = mx^2 + 2bxy + cy^2, \text{ waar } 0 \leq b < m. \tag{7.21}$$

We gaan laten zien dat de afbeelding die zo'n vorm g stuurt naar $[b] \in (\mathbb{Z}/m\mathbb{Z})^*$, een bijectie induceert tussen de g die aan (7.21) voldoen, en de oplossingen van de vergelijking $x^2 \equiv -n \bmod m$.
De discriminant van g is $4b^2 - 4mc = -4n$, waardoor $-n = b^2 - mc$. Merk nu op dat c volledig en uniek door b wordt bepaald, want m en n liggen vast. Daarom is er een bijectie tussen de oplossingen b van $-n = b^2 - mc$ en $-n \equiv b^2 \bmod m$. Dit geeft een bijectie tussen de g die aan (7.21) voldoen, en de oplossingen van $x^2 \equiv -n \bmod m$, want de b uit (7.21) zit tussen 0 en m.

Nu komt onderdeel c van de opgave van Cox. Neem een gereduceerde $f(x,y) = ax^2 + bxy + cy^2$ met discriminant $-4n$, en laat $f(u,v) = m$ een propere representatie zijn. Neem r_0 en s_0 zodat $us_0 - vr_0 = 1$, dit kunnen we doen met behulp van het algoritme van Euclides. Maak nu $r = r_0 + uk$ en $s = s_0 + vk$. Dan zien we dat voor elke $k \in \mathbb{Z}$ geldt dat: $us - vr = us_0 + uvk - vr_0 - vuk = us_0 - vr_0 = 1$. Definieer nu:

$$g(x,y) = f(ux + ry, vx + sy), \tag{7.22}$$

zodat $g \sim f$. We gaan laten zien dat er een unieke $k \in \mathbb{Z}$ is zodat g voldoet aan de eis van (7.21). Door de definitie van g uit te schrijven krijgen we:

$$\begin{aligned} g(x,y) &= (au^2 + buv + cv^2)x^2 + \big(2(aur + cvs) + b(us + vr)\big)xy + (ar^2 + brs + cs^2)y^2 \\ &= mx^2 + Bxy + f(r,s)y^2. \end{aligned}$$

We willen onze k nu zo gaan kiezen zodat $0 < B/2 < m$. Merk op dat B even is, want $D = b^2 - 4mc$ is even, waardoor b even is, waar weer uit volgt dat B even is.
Laten we eerst goed kijken wat B precies is:

$$\begin{aligned} B &= 2\big(au(r_0 + uk) + cv(s_0 + vk)\big) + b\big(u(s_0 + vk) + v(r_0 + uk)\big) \\ &= 2aku^2 + 2bkuv + 2ckv^2 + 2aur_0 + 2cvs_0 + bus_0 + bvr_0. \end{aligned} \tag{7.23}$$

Als we in deze vergelijking de waarde van k met 1 verhogen, dan komt er

$$2(au^2 + buv + cv^2) = 2m$$

bij. Daardoor gaat elke keer dat we de waarde van k met 1 verhogen, de waarde van $B/2$ in stapjes van m omhoog. Daarom is er een unieke waarde $k \in \mathbb{Z}$ zodat g aan (7.21) voldoet. Noem $g_{u,v}(x,y)$ de vorm die g met die specifieke waarde van k wordt.

We zijn nu bij onderdeel d van Cox aangekomen. Bekijk de afbeelding ϕ die een propere representatie $f(u,v) = m$ stuurt naar de vorm $g_{u,v}(x,y)$, waar f een gereduceerde vorm van discriminant $-4n$ is. Deze afbeelding is surjectief. Immers, neem een $g_{u,v}(x,y)$, dan weten we de unieke k zodat $g_{u,v}$ aan (7.21) voldoet. Met deze k kunnen we r en s bepalen, waardoor we kunnen achterhalen welke f bij $g_{u,v}$ hoort, want $g_{u,v}(x,y) = f(ux + ry, vx + sy)$ geeft dat $f(x,y) = g_{u,v}(sx - ry, -vx + uy)$. Op die manier krijgen we de $m = f(u,v)$ zodat ϕ deze representatie naar $g_{u,v}(x,y)$ stuurt.

Nu komt onderdeel e van de opgave. Stel dat $g_{u,v}(x,y) = g_{u',v'}(x,y)$, en definieer

$$A = \begin{pmatrix} u & v \\ r & s \end{pmatrix}, \quad B = \begin{pmatrix} u' & v' \\ r' & s' \end{pmatrix}, \quad C = B^{-1}A.$$

We gaan laten zien dat daaruit volgt dat $C = \pm I$.
Merk op dat uit (7.22) impliceert dat:

$$g_{u,v}(x,y) = f((x,y)\cdot A) \text{ en } g_{u',v'}(x,y) = f((x,y)\cdot B).$$

Hieruit volgt dat $f(x,y) = g_{u',v'}((x,y)\cdot B^{-1})$. We krijgen nu dat:

$$f(x,y) = g_{u',v'}((x,y)\cdot B^{-1}) = g_{u,v}((x,y)\cdot B^{-1}) = f((x,y)\cdot B^{-1}A) = f((x,y)\cdot C).$$

Als we nu op dezelfde manier te werk gaan als in het bewijs van de uniciteit van Stelling 6.15, dan krijgen we dat $C = \pm I$.

We zijn bij onderdeel f van de opgave aangekomen. We gaan tot slot laten zien dat de afbeelding ϕ uit onderdeel d een twee-op-een afbeelding is. Claim:

$$g_{u,v}(x,y) = g_{u',v'}(x,y) \iff (u,v) = \pm(u',v'). \tag{7.24}$$

Opmerking:

$$C = \pm I \iff A = \pm B \iff (u,v) = \pm(u',v').$$

De laatste implicatie van rechts naar links is waar, want als $(u,v) = (u',v')$, dan geldt zeker dat $(r,s) = (r',s')$, en als $(u,v) = -(u',v')$, dan is de implicatie nog steeds waar. Immers: we vinden s_0 en r_0 zodat $us_0 - vr_0 = 1$, dan is $u's_0' - v'r_0' = 1$, met $(s_0', r_0') = -(s_0, r_0)$. Als we nu de waarde van B uit (7.23) bekijken voor $g_{u,v}$ en $g_{u',v'}$, dan zien we dat ze dezelfde waarde van k gebruiken. Hiermee zien we dat:

$$r = r_0 + uk = -(r_0' + u'k) = -r' \text{ en } s = s_0 + vk = -(s_0' + v'k) = -s',$$

waardoor $(r,s) = -(r',s')$, en $A = -B$.
De ($\Rightarrow$) implicatie van (7.24) volgt nu uit onderdeel e. We gaan nu de omkering bewijzen. We hoeven alleen te laten zien dat $(u,v) = -(u',v')$ impliceert dat $g_{u,v}(x,y) = g_{v',u'}(x,y)$, want in het andere geval is de uitspraak duidelijk waar. We hebben net laten zien dat in deze situatie geldt dat $(r,s) = -(r',s')$, waardoor:

$$\begin{aligned} g_{-u,-v}(x,y) &= f(-(ux+ry), -(vx+sy)) \\ &= a(ux+ry)^2 + b(ux+ry)(vx+sy) + c(vx+sy)^2 \\ &= f(ux+ry, vx+sy) = g_{u,v}(x,y). \end{aligned}$$

Daarmee is (7.24) bewezen.
Door nu (7.24) met onderdeel d samen te voegen, zien we dat ϕ een twee-op-een afbeelding is.

We kunnen nu het bewijs van dit lemma afronden. Door Lemma 7.19 en onderdeel b te gebruiken zien we dat het aantal vormen g dat aan (7.21) voldoet precies $\prod_{p|m}\left(1 + \left(\frac{-n}{p}\right)\right)$ is. Uit de onderdelen c en f volgt nu dat:

$$2\prod_{p|m}\left(1 + \left(\frac{-n}{p}\right)\right)$$

het aantal manieren is dat m door een gereduceerde vorm proper gerepresenteerd wordt. $\square$

Gevolg 7.25 *Neem $n > 0$. Stel dat m proper gerepresenteerd wordt door een primitieve positief definiete vorm f met discriminant $-4n$, en stel dat m oneven en relatief priem met n is. Als r het aantal priemdelers van m is, dan wordt m op precies 2^{r+1} manieren proper gerepresenteerd door een gereduceerde vorm in het genus van f.*

Bewijs
Uit Stelling 6.15 volgt dat f equivalent is met een gereduceerde vorm g. Dan representeert g dus ook m, waardoor Lemma 7.3.2 geeft dat f en g in hetzelfde genus liggen, want hun waarden in $(\mathbb{Z}/4n\mathbb{Z})^*$ zijn niet disjunct, terwijl verschillende nevenklassen dat wel zijn.
We willen nu laten zien dat $\left(\frac{-n}{p}\right) = 1$ voor alle priemdelers p van m. Dan volgt namelijk uit 7.20 dat m op $2 \cdot 2^r = 2^{r+1}$ manieren proper gerepresenteerd wordt door een gereduceerde vorm in de de genus van f (niet alle 2^{r+1} manieren hoeven van dezelfde f af te komen).

Neem een willekeurige priemdeler p van m. Als $f(x,y) = ax^2 + bxy + cy^2$ en $f(u,v) = m$, dan $au^2+buv+cv^2 \equiv 0 \bmod p$. Deze uitdrukking kunnen we op de volgende manier ontbinden:

$$\begin{aligned}
&\frac{1}{a}\left(au - \frac{v(-b+\sqrt{b^2-4ac})}{2}\right)\left(au - \frac{v(-b-\sqrt{b^2-4ac})}{2}\right)\\
&= \frac{1}{a}\left(a^2u^2 - \frac{av(-b-\sqrt{b^2-4ac}) + av(-b+\sqrt{b^2-4ac})}{2} + \frac{v^2\big(b^2-(b^2-4ac)\big)}{4}\right)\\
&= au^2 - \frac{-2buv}{2} + \frac{4cv^2}{4} = au^2 + buv + cv^2 \equiv 0 \bmod p.
\end{aligned}$$

Hieruit volgt dat $1 = \left(\frac{b^2-4ac}{p}\right) = \left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$. □

Bewijs Stelling 7.17
Stel eerst dat elke genus maar uit een enkele klasse bestaat.
Stel dat m proper gerepresenteerd wordt door $x^2 + ny^2$, en dat de vergelijking $m = x^2 + ny^2$ een unieke oplossing heeft als $x, y \geq 0$. We moeten nu bewijzen dat m priem is.
Laat r het aantal priemdelers van m zijn, dan geeft Gevolg 7.25 dat m op 2^{r+1} manieren door x^2+ny^2 gerepresenteerd wordt, want x^2+ny^2 is volgens onze aanname de enige gereduceerde vorm in zijn genus. Merk nu op dat een oplossing van $m = x^2 + ny^2$ ook direct drie andere oplossingen geeft: $(x,-y)$, $(-x,y)$ en $(-x,y)$. Hieruit volgt dat voor 2^{r-1} van de 2^{r+1} manieren dat m proper door $x^2 + ny^2$ gerepresenteerd wordt, geldt dat $x, y \geq 0$. Onze aanname geeft nu dat $2^{r-1} = 1$, waardoor $r = 1$. Maar dan heeft m maar één priemdeler, dus is m een priemmacht: $m = p^a$. Als we laten zien dat $a = 1$, dan zijn we klaar, want dan is m priem.

Stel dat $a \geq 2$, dan volgt uit het argument dat we in Gevolg 7.25 gebruikten dat $\left(\frac{-n}{p}\right) = 1$. Als $a = 2$, dan volgt uit Lemma 7.20 dat p^{a-2} op twee manieren proper gerepresenteerd wordt door een gereduceerde vorm, want dan is het product leeg. Als $a > 2$, dan wordt p^{a-2} op vier manieren proper gerepresenteerd. Dus in het geval dat $a \geq 2$ heeft p^{a-2} minstens twee representaties. Zeg $p^{a-2} = f(u,v)$, voor een gereduceerde vorm $f(x,y)$, dan is $f(pu,pv) = p^a = m$. Uit Lemma 7.3.2 volgt nu dat x^2+ny^2 en f in hetzelfde genus liggen. Onze aanname geeft nu dat $f(x,y) = x^2 + ny^2$. Maar dan is dus $m = f(pu,pv) = (pu)^2 + n(pv)^2$, en we kunnen de tekens van pu en pv zo kiezen zodat $pu, pv \geq 0$. Dit geeft een oplossing van de vergelijking $m = x^2 + ny^2$, die ook nog eens anders is dan de degene waarmee we begonnen, want nu hebben we dat $\gcd(pu,pv) \neq 1$. Dit is in tegenspraak met de aanname, dus is $a = 1$.

Anderzijds, stel dat n een geschikt getal is. Laat f een gereduceerde vorm zijn van discriminant $-4n$, en laat g de Dirichlet samenstelling van f met zichzelf zijn. Uit Propositie

7.10 weten we dat g primitief en positief definiet is. Dankzij Stelling 6.15 kunnen we zonder verlies van algemeenheid aannemen dat ook g gereduceerd is. We gaan bewijzen dat $g(x,y) = x^2+ny^2$, want dan heeft elk element van de klassengroep orde ≤ 2, waardoor uit Stelling 7.15 volgt dat elke genus uit een enkele klasse bestaat.
Stel dat $g(x,y) \neq x^2+ny^2$. Laat p en q verschillende oneven priemgetallen zijn die n niet delen en door f gerepresenteerd worden. Dit kunnen we doen, omdat Cox in [6, Thm. 9.12] laat zien dat f oneindig veel priemgetallen representeert. Deze stelling gaan we hier niet bewijzen, omdat daar een paar hoofdstukken voor nodig zijn. Definitie 7.5 geeft dat pq ook door g gerepresenteerd wordt, want g is de Dirichlet samenstelling van f met zichzelf. De middelste coëfficiënt van $f = ax^2+2bxy+cy^2$ is even, want de discriminant van f is even. Nu volgt uit:

$$(ax^2+2bxy+cy^2)(az^2+2bzw+cw^2) = (axz+bxw+byz+cyw)^2+n(xw-yz)^2$$

dat x^2+ny^2 ook pq representeert. Deze representatie is zelfs proper, omdat pq anders niet kwadraatvrij zou zijn.
Gevolg 7.25 geeft nu dat pq op precies $2^3 = 8$ manieren proper gerepresenteerd wordt door gereduceerde vormen van discriminant $-4n$. Ten minste één van die representaties komt van g af, waardoor er nog hoogstens zeven overblijven voor x^2+ny^2. Maar dan heeft $x^2+ny^2 = m$ precies één oplossing met $x,y \geq 0$, want als er nog een andere oplossing $u^2+nv^2 = m$ was met $(x,y) \neq (\pm u, \pm v)$, dan hadden we acht oplossingen gekregen, wat er te veel zijn.
We krijgen dus dat $m = x^2+ny^2$ maar één oplossing heeft, met de eigenschappen: $\text{ggd}(x,y) = 1$ en $x,y \geq 0$. Dit is in tegenspraak met de aanname dat n geschikt is, want pq is duidelijk niet een priemgetal. □

Opmerking 7.26
In Opmerking 6.20 lieten we zien dat we het klassengetal van een gegeven discriminant $D<0$ redelijk makkelijk kunnen berekenen. Dit geeft een manier om geschikte getallen te vinden, want Stelling 7.15 en Stelling 7.17 geven een verband tussen de klassengetallen en de geschikte getallen.

Met behulp van de kennis van de afgelopen twee hoofdstukken kunnen we (2.1) nu ook op de volgende manier weergeven.

$h(-4n)$	Geschikte getallen n
1	$1,2,3,4,7$
2	$5,6,8,9,10,12,13,15,16,18,22,25,28,37,58$
4	$21,24,30,33,40,42,45,48,57,60,70,72,78,85,$ $88,93,102,112,130,133,177,190,232,253$
8	$105,120,165,168,210,240,273,280,312,$ $330,345,357,385,408,462,520,760$
16	$840,1320,1365,1848$

Tabel 2: De 65 bekende geschikte getallen, gesorteerd op het bijbehorende klassengetal.

8 Referenties

[1] Baker, A. *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

[2] Blecksmith, R., Brillhart, J. en Decaro, M. *The completion of Euler's factoring formula*, Rocky Mountain J. Math. **43.3** (2013), 755-762.

[3] Brillhart, J. *A Note on Euler's Factoring Problem*, Amer. Math. Monthly **116** (2009), 928-931.

[4] Chowla, S. en Briggs, W. E. *On discriminants of binary quadratic forms with a single class in each genus*, Canadian J. Math. **6** (1954), 463–470.

[5] Clark, P. L. (2011), *Thue-Vinogradov and integers of the form* $x^2 + Dy^2$, geraadpleegd op 20 juli 2018, `http://math.uga.edu/~pete/thuelemmav6.pdf`.

[6] Cox, D. A. *Primes of the form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, tweede editie, 2013.

[7] Gauss, C. F. *Disquisitiones Arithmeticae*, 1801, Engelse vertaling door Arthur A. Clarke en William C. Waterhouse, Springer, 1986.

[8] Grube, F. *Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen*, Zeitschrift Mathematik und Physik **19** (1874), 492-519.

[9] Hagedorn, T. R. (2011), *Primes of the form* $x^2 + ny^2$ *and the geometry of (convenient) numbers*, geraadpleegd op 1 juli 2018, `http://math.uga.edu/~pete/Hagedorn11.pdf`.

[10] Jacobson, M. J., Ramachandran, S. en Williams, H. C. *Numerical Results on Class Groups of Imaginary Quadratic Fields*, in: Algorithmic Number Theory, Lect. Notes in Comp. Sci. **4076** (2006), 87–101.

[11] Kani, E. (2011), *Idoneal Numbers and some Generalizations*, geraadpleegd op 1 juli 2018, `http://www.mast.queensu.ca/~kani/papers/idoneal-f.pdf`.

[12] Kaplan, J. (2014), *Binary Quadratic Forms, Genus Theory, and Primes of the Form* $p = x^2 + ny^2$, geraadpleegd op 1 juli 2018, `http://math.uchicago.edu/~may/REU2014/REUPapers/Kaplan.pdf`.

[13] Krzyzanowski, R. (2008), *Euler's Convenient Numbers*, geraadpleegd op 21 juni 2018, `http://homepages.math.uic.edu/~robertk/files/number_theory_project2.pdf`.

[14] Lang, S. *Algebraic Number Theory*, Springer Science, tweede editie, 1994.

[15] Richeson, D. S. *Euler's Gem: The Polyhedron Formula and the Birth of Topology*, Princeton University Press, 2008.

[16] Steinig, J. *On Euler's idoneal numbers*, Elem. Math. **21** (1966), 73–88.

[17] Weinberger, P. *Exponents of the class groups of complex quadratic fields*, Acta Arith., **22** (1973), 117–124.

9 Tabellen

De letter in het vakje (i, j) correspondeert met de eerste methode uit de lijst van Stelling 5.9 (van boven naar beneden gelezen), die werkt bij het geval $n = j$ en $d = i$. Als er geen letter in staat bedoelen we daarmee dat deze d groter is dan B_n, waardoor we er niet naar hoeven te kijken.

d \ n	1	2	3	4	5	6	7	8	9	10	12	13	15	16	18	21	22	24	25
2	-	-	a	e	a	a	f	e	a	a	a	a	a	e	a	a	a	a	a
3	-	-	-	-	-	d	a	h	d	a	h	b	a	b	d	a	b	d	a
4	-	-	-	-	-	-	-	-	-	c	g	c	g	g	c	c	c	g	c
5	-	-	-	-	-	-	-	-	-	-	-	-	-	i	a	a	b	a	d
6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	e	b

d \ n	28	30	33	37	40	42	45	48	57	58	60	70	72	78	85	88
2	e	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
3	a	a	d	b	a	a	a	h	a	a	a	a	d	d	a	b
4	g	c	c	c	g	c	c	g	c	c	g	c	g	c	c	g
5	a	a	a	a	d	a	a	a	a	b	a	a	a	a	a	b
6	a	d	a	a	b	a	d	d	d	b	e	a	d	a	a	a
7	-	-	a	b	a	d	a	h	b	b	a	a	b	a	a	a
8	-	-	-	-	a	a	a	a	a	a	a	a	a	a	a	a
9	-	-	-	-	-	-	-	-	d	b	d	b	k	d	b	b
10	-	-	-	-	-	-	-	-	-	-	-	a	b	b	a	a
11	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	d

d \ n	93	102	105	112	120	130	133	165	168	177	190	210	232	240
2	a	a	a	e	a	a	a	a	a	a	a	a	a	a
3	a	a	a	a	a	a	a	a	a	d	a	a	a	a
4	c	c	c	g	g	c	c	c	g	c	c	c	g	g
5	a	a	a	a	a	a	a	a	a	a	d	a	b	a
6	a	a	a	a	d	a	a	a	a	a	b	a	b	e
7	b	a	a	h	a	a	d	a	d	b	a	a	b	a
8	a	a	a	e	a	a	a	a	a	a	a	a	a	a
9	d	d	d	b	d	b	b	d	d	d	b	d	b	d
10	b	a	a	a	d	d	a	a	a	a	a	a	a	e
11	a	a	a	h	a	a	b	a	a	a	b	a	a	a
12	a	a	a	a	a	a	a	a	a	c	a	a	a	a
13	-	-	a	a	a	a	a	a	a	a	a	a	b	a
14	-	-	-	-	-	b	a	a	a	a	a	a	a	a
15	-	-	-	-	-	-	-	d	b	b	a	d	a	h
16	-	-	-	-	-	-	-	c	e	c	c	c	e	j
17	-	-	-	-	-	-	-	-	-	-	a	a	a	a
18	-	-	-	-	-	-	-	-	-	-	-	a	a	a
19	-	-	-	-	-	-	-	-	-	-	-	-	a	h

d \ n	253	273	280	312	330	345	357	385	408	462	520	760	840	1320	1365	1848
2	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
3	b	a	a	d	a	a	a	a	a	a	a	a	a	a	a	a
4	c	c	g	g	c	c	c	c	g	c	g	g	g	g	c	g
5	a	a	a	a	a	a	a	a	a	a	a	d	a	a	a	a
6	a	a	a	a	a	d	a	a	a	a	a	b	a	a	a	a
7	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
8	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
9	b	d	b	d	d	d	d	b	d	d	b	b	d	d	d	d
10	a	a	a	b	a	a	a	a	a	a	d	a	a	a	a	a
11	a	a	b	a	a	a	a	d	a	a	a	b	a	a	a	a
12	b	a	a	d	a	a	a	a	a	a	a	a	a	a	a	a
13	a	a	a	d	a	a	a	a	b	a	a	a	a	a	a	a
14	a	a	d	a	a	a	a	d	a	a	b	a	a	a	a	a
15	a	a	b	a	d	a	b	b	b	b	a	a	d	d	a	b
16	c	c	e	e	c	c	c	c	e	c	e	e	e	e	c	e
17	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
18	a	a	a	a	a	a	d	a	d	a	a	a	a	a	a	a
19	a	a	a	a	a	a	a	a	b	a	a	d	a	a	a	a
20	a	a	a	a	a	a	a	a	a	a	a	d	a	a	a	a
21	-	a	b	a	a	a	d	a	b	a	a	a	d	a	a	a
22	-	-	-	b	a	a	a	a	a	d	a	a	a	a	a	d
23	-	-	-	-	a	a	a	a	a	a	a	a	a	a	a	a
24	-	-	-	-	-	-	a	a	a	a	a	b	a	a	a	a
25	-	-	-	-	-	-	-	-	b	b	d	d	d	d	d	b
26	-	-	-	-	-	-	-	-	-	a	d	b	a	a	a	a
27	-	-	-	-	-	-	-	-	-	a	a	a	a	a	a	a
28	-	-	-	-	-	-	-	-	-	-	a	a	a	a	a	a
29	-	-	-	-	-	-	-	-	-	-	b	a	a	a	a	a
30	-	-	-	-	-	-	-	-	-	-	-	b	d	a	d	a
31	-	-	-	-	-	-	-	-	-	-	-	a	a	b	a	a
32	-	-	-	-	-	-	-	-	-	-	-	a	a	a	a	a
33	-	-	-	-	-	-	-	-	-	-	-	a	a	a	a	a
34	-	-	-	-	-	-	-	-	-	-	-	a	a	b	a	a
35	-	-	-	-	-	-	-	-	-	-	-	b	a	a	a	a
36	-	-	-	-	-	-	-	-	-	-	-	-	d	d	c	d
37	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	b
38	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
39	-	-	-	-	-	-	-	-	-	-	-	-	-	a	d	a
40	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
41	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
42	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	d
43	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
44	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
45	-	-	-	-	-	-	-	-	-	-	-	-	-	d	a	a
46	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a	a
47	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a	a
48	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a
49	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	d
50	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a
51	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a
52	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a
53	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a
54	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	a