

Priemgetallen van de vorm $x^2 + ny^2$

Een klassiek probleem met een moderne oplossing

Sander Bessels

23 november 2005

Inhoudsopgave

1	Van Fermat tot Gauss	2
2	n groter dan 3	7
3	Het Hilbert klassenlichaam	9
4	De ideaalklassengroep	12
5	De oplossing voor ∞ veel n	14
6	Expliciete oplossing voor n=14	18

Hoofdstuk 1

Van Fermat tot Gauss

“Welke priemgetallen zijn te schrijven als de som van twee kwadraten”

Met deze vraag is het allemaal lang geleden begonnen. Even proberen: 5, 13, 17, 29, 37, 41 zijn allemaal te schrijven als som van twee kwadraten (s.v.t.k.), maar 3, 7, 11, 19, 23, 31 niet. Pierre de Fermat (1601-1665) zag hier in 1640 regelmaat in en zo ontstond het eerste resultaat over dit probleem:

Voor een oneven priemgetal p en $x, y \in \mathbb{N}$ (deze variabelen houden we ook in het vervolg als zodanig aan) geldt:

Stelling 1.1 $p = x^2 + y^2 \iff p = 1 \pmod{4}$.

Als Fermat het bij dit resultaat had gelaten, was wellicht één van de mooiste en invloedrijkste problemen van de getaltheorie onopgemerkt gebleven. Hij vond echter nog twee resultaten:

Stelling 1.2 $p = x^2 + 2y^2 \iff p = 1 \pmod{8}$ of $p = 3 \pmod{8}$.

en

Stelling 1.3 $p = x^2 + 3y^2 \iff p = 3$ of $p = 1 \pmod{3}$.

Deze resultaten zijn op zich al heel mooi, maar het maakt wel heel nieuwsgierig naar wat er gebeurt voor priemgetallen van de vorm $x^2 + 5y^2$, $x^2 + 6y^2$ etc.. Het lijkt dus redelijk om te stellen dat Fermat de eerste was die zich bezighield met het probleem in haar meest algemene vorm:

Hoofdvraag 1.4 *Welke priemgetallen kunnen, gegeven $n \in \mathbb{N}$, worden geschreven in de vorm $p = x^2 + ny^2$?*

Hiermee is het startschot gegeven voor een eeuwenlange zoektocht naar een oplossing. Fermat's werk was echter, met het formuleren van het probleem en deze eerste drie resultaten, gedaan, want zoals we van Fermat gewend zijn: schitterende stellingen, maar geen bewijzen. Althans, hij gaf wel een soort van "bewijs" van 1.1, namelijk via oneindige descent, wat neerkomt op het volgende: Stel dat we een priemgetal hebben dat $1 \pmod{4}$ is, dat *geen* s.v.t.k. is, dan kunnen we een kleiner priemgetal vinden dat ook $1 \pmod{4}$ is en ook geen s.v.t.k.. Dit herhaal je net zolang tot je bij 5 bent aanbeland, maar 5 is *wel* een s.t.v.k.. Tegenspraak, q.e.d.. Hij gaf echter geen manier om dit kleinere priemgetal te vinden.

Het eerste volledige bewijs van 1.1 is van de hand van Euler (1707-1783), die er zijn levenswerk van maakte om de bewijzen te vinden voor Fermat's stellingen. In 1749 had Euler het bewijs voor 1.1 rond en in 1772, 40 jaar nadat hij voor het eerst van het probleem gehoord had, voltooid hij ook de bewijzen van 1.2 en 1.3. Hij gebruikte voor zijn bewijzen een afdalingsargument in twee stappen (dat volgens Weil waarschijnlijk overeen kwam met wat Fermat deed):

Reciprociteit: Als $p \equiv 1 \pmod{4}$, dan $\exists x, y$ zodat $p \mid x^2 + y^2$, $\gcd(x, y) = 1$.

Afdaling: Als $p \mid x^2 + y^2$, $\gcd(x, y) = 1$, dan kan p geschreven worden als $x^2 + y^2$.

Eulers bewijzen van deze stappen komen in beknopte vorm neer op ongeveer twee pagina's rekenwerk en die zal ik hier achterwege laten.

Deze stappen kunnen overigens eenvoudig geformuleerd worden voor het algemene geval:

Reciprociteit: Als *een voorwaarde in termen van een simpel na te gane voorwaarde voor p^* , dan $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$

Afdaling: Als $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$, dan kan p geschreven worden als $x^2 + ny^2$

Helaas gaat het bij de afdalingsstap al mis voor $n = 5$, bijvoorbeeld: $3 \mid 21 = 1 + 5 * 2^2$, maar $3 \neq x^2 + 5y^2$. Euler en Fermat wisten dit, maar het zou nog lang duren, voordat de wiskunde ver genoeg was om dit probleem op te lossen. De reciprociteitsstap blijkt echter wel in de uiteindelijke oplossing een rol te spelen, zij het in een iets modernere vorm. De reciprociteitsstap kan namelijk korter geschreven worden m.b.v. het Legendre symbool dat als

volgt gedefinieerd is voor een natuurlijk getal n en een oneven priemgetal p .

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{als } n \text{ een kwadratisch residu is mod } p. \\ -1 & \text{als } n \text{ geen kwadratisch residu is mod } p. \\ 0 & \text{als } p|n. \end{cases} \quad (1.1)$$

Het volgende lemma laat zien dat de voorwaarde $p|x^2 + ny^2$, $\gcd(x, y) = 1$ in de reciprociteitsstap eigenlijk hetzelfde is als de voorwaarde dat $-n$ een kwadraat moet zijn modulo p , oftewel $\left(\frac{-n}{p}\right) = 1$.

Lemma 1.5 $\exists x, y \ p|x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1$.

Bewijs: Merk op dat als $x^2 + ny^2 = 0 \pmod{p}$, en $\gcd(x, y) = 1$, dat dan $\gcd(y, p)$ ook 1 moet zijn, want anders zou $p|y$ en dus zou $ny^2 = 0 \pmod{p}$ en dus $x^2 = 0 \pmod{p}$, waaruit volgt dat $x = y = 0 \pmod{p}$, wat in tegenspraak is met $\gcd(x, y) = 1$. Dus zijn y en p relatief priem, wat betekent dat er een a moet zijn zodat $ay = 1 \pmod{p}$. Als we nu de uit de aanname afgeleide vergelijking $-ny^2 = x^2 \pmod{p}$ met a^2 vermenigvuldigen, krijgen we $-n * a^2 y^2 = (ax)^2 \pmod{p}$ en dus $-n = (ax)^2$ wat hetzelfde betekent als $\left(\frac{-n}{p}\right) = 1$. \square

De argumenten in dit lemma zijn feitelijk vrij elementair, maar voor Euler was dit niet zo eenvoudig. Het duurde jaren voor hij zich realiseerde hoe belangrijk kwadratische residuen zijn voor de oplossing van het probleem. Je kan dit goed zien aan de notatie die hij gebruikt. In 1744 schrijft hij nog *priemdelers van van getallen van de vorm $aa - Nbb$* , in 1747 verandert dit in *residuen die voortkomen uit de deling van kwadraten door het priemgetal p* en in 1751 is de vertaling voltooit; Euler gebruikt vanaf dan de termen *residu* en *niet-residu*, met kwadratisch als bekend verondersteld.

Tegenwoordig is er een veel korter en eleganter bewijs van 1.1. bekend, dat ook wel aardig is om nu te geven:

Bewijs:

\Rightarrow : Stel $p = x^2 + y^2$, dan geldt dat p niet 0 of 2 mod 4 kan zijn (p was immers per definitie oneven) en omdat kwadraten altijd 0 of 1 mod 4 zijn (simpel na te gaan), kan p ook niet 3 mod 4 zijn, dus $p = 1 \pmod{4}$. Deze kant op is duidelijk niet het probleem.

\Leftarrow : Stel $p = 1 \pmod{4}$. Bereken het Legendresymbool $\left(\frac{-1}{p}\right)$ met de formule van Euler:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \quad (1.2)$$

Hiermee is eenvoudig in te zien dat -1 een kwadraat is modulo p . De congruentievergelijking $x^2 = -1 \pmod{p}$ heeft dus een oplossing, zeg x_0 . Laten we nu gaan werken in de ring $\mathbb{Z}[i]$ en unieke factorisatie (op eenheden na) gebruiken. We weten $p|(x_0^2 + 1)$, dus $p|(x_0 + i)(x_0 - i)$ (beide factoren zijn geen eenheid). Als p een Gaussisch priemgetal is, dan deelt p precies één van deze twee, maar vanwege complexe conjugatie ook de andere, tegenspraak. Dus p is samengesteld, zeg $p = \alpha\beta$ met $N\alpha, N\beta > 1$. Neem aan allebei de kanten de norm, dan krijg je $p^2 = N\alpha N\beta$. Omdat $N\alpha, N\beta > 1$ volgt hieruit eenvoudig dat $p = N\alpha$ en dus de som van twee kwadraten. \square

We zien dus dat de eigenschap dat p te schrijven is als som van kwadraten iets te maken heeft met het splijten van p in $\mathbb{Z}[i]$, een mooie vooruitblik op de moderne oplossing van het gehele probleem.

We gaan weer even terug in de geschiedenis. Aan de hand van de resultaten van Fermat en Euler werd er hard gewerkt aan dit nieuwe fenomeen van kwadratische residuen. Dit resulteerde in een aantal voor ons probleem belangrijke stellingen (in sommige gevallen voor hem nog vermoedens) van Euler:

$$\begin{aligned} \left(\frac{-1}{p}\right) &= 1 \iff p \equiv 1 \pmod{4} \\ \left(\frac{-2}{p}\right) &= 1 \iff p \equiv 1, 3 \pmod{8} \\ \left(\frac{-3}{p}\right) &= 1 \iff p \equiv 1, 7 \pmod{12} \\ \left(\frac{-5}{p}\right) &= 1 \iff p \equiv 1, 3, 7, 9 \pmod{20} \\ \left(\frac{-7}{p}\right) &= 1 \iff p \equiv 1, 9, 11, 15, 23, 25 \pmod{28} \\ \left(\frac{1}{p}\right) &= 1 \\ \left(\frac{2}{p}\right) &= 1 \iff p \equiv \pm 1, \pm 3 \pmod{8} \\ \left(\frac{3}{p}\right) &= 1 \iff p \equiv \pm 1 \pmod{12} \\ \left(\frac{5}{p}\right) &= 1 \iff p \equiv \pm 1, \pm 11 \pmod{20} \\ \left(\frac{7}{p}\right) &= 1 \iff p \equiv \pm 1, \pm 3, \pm 9 \pmod{28} \end{aligned}$$

Die uiteindelijk geleid hebben tot de ontdekking van kwadratische reciprociteit:

Stelling 1.6 *Zij p en q verschillende oneven priemmen, dan*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}. \quad (1.3)$$

Of anders geformuleerd: $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, tenzij $p \equiv q \equiv -1 \pmod{4}$, want dan geldt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Handig voor het berekenen van kwadratische restklassen is ook de volgende regel:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \quad (1.4)$$

We hebben nu genoeg gereedschap om de reciprociteitsstappen voor $n = 1$ en 3 te bewijzen. Voor $n = 2$ gaat de stelling over kwadratische reciprociteit niet op (hij geldt alleen voor oneven priemgetallen) en dus is er een ander truukje nodig om $\left(\frac{-2}{p}\right)$ te berekenen. Dit kan bijvoorbeeld met Gauss' lemma. Voor meer informatie, zie het dictaat *Elementaire Getaltheorie* van F. Beukers.

$n = 1$: Een priemgetal p deelt, voor zekere x, y , $x^2 + y^2$, $\gcd(x, y) = 1$ is volgens lemma 1.5 equivalent met $\left(\frac{-1}{p}\right) = 1$. Uit 1.2 volgt nu dat dit betekent dat $(-1)^{\frac{p-1}{2}} = 1$, wat neerkomt op $p = 1 \pmod{4}$.

$n = 3$: Een priemgetal p deelt voor zekere x, y , $x^2 + 3y^2$, $\gcd(x, y) = 1$ is equivalent met $\left(\frac{-3}{p}\right) = 1$. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$. Dit is 1 als $p = 1 \pmod{3}$ en -1 als $p = -1 \pmod{3}$.

Het bewijs dat Euler gevonden had voor de afdalingsstap voor $n = 1$ kan (na een kleine aanpassing) ook gebruikt worden voor de afdalingsstappen van $n = 2$ en 3 , dus daarmee had Euler in ieder geval de eerste drie gevallen van het probleem volledig onder controle (ik vermoed dat hij ook $\left(\frac{-2}{p}\right)$ wel uit kon rekenen, ook al lukt het niet met kwadratische reciprociteit).

Hoofdstuk 2

n groter dan 3

Het bleef Euler fascineren wat er gebeurde voor $n > 3$. In 1744 schreef Euler een artikel waarin hij een aantal vermoedens opstelde over priemgetallen van de vorm $x^2 + 5y^2$ en $x^2 + 14y^2$.

$$\begin{aligned} p &= x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20} \\ 2p &= x^2 + 5y^2 \iff p \equiv 3, 7 \pmod{20} \end{aligned}$$

We weten dat $p|x^2 + 5y^2$ precies als $p = 1, 3, 7, 9 \pmod{20}$. We zien dat deze vier congruentieklassen uiteen vallen in twee groepen: 1, 9 en 3, 7, die andere eigenschappen hebben. Dit is een nieuw fenomeen dat niet voorkwam voor $n \leq 3$. Voor $n = 14$ is zelfs nog ingewikkelder:

$$\begin{aligned} p = x^2 + 14y^2 \text{ of } 2x^2 + 7y^2 &\iff p = 1, 9, 15, 23, 25, 39 \pmod{56} \\ 3p = x^2 + 14y^2 &\iff p = 3, 5, 13, 19, 27, 45 \pmod{56} \end{aligned}$$

Net als bij $n = 5$ geeft de vereniging van deze twee groepen precies de equivalentieklassen waarvoor $(-14/p) = 1$. Het verrassende element is hier dat we $2x^2 + 7y^2$ en $x^2 + 14y^2$ niet lijken te kunnen scheiden. Dit komt doordat ze hetzelfde geslacht hebben en daardoor niet gescheiden kunnen worden met congruentieklassen. Het begrip geslacht, dat ontdekt is door Lagrange, zal in deze scriptie niet behandeld worden. Voor meer informatie verwijs ik naar het boek “Primes of the form $x^2 + ny^2$ ” van David A. Cox.

Ook is het vooralsnog een raadsel waarom bij $n = 5$ $2p$ voorkomt en bij $n = 14$ $3p$. Dit raadsel blijft in deze scriptie eveneens onopgelost. Voor meer

informatie, zie wederom het boek van Cox.

Ten slotte kan je je afvragen welke voorwaarde dan *wel* voldoende is om te garanderen dat $p = x^2 + 14y^2$. Hierop zal ik uitgebreid ingaan. De oplossing ligt diep verscholen in de wiskunde en er zijn moderne technieken nodig om het op te lossen. De oplossing maakt namelijk gebruik van het Hilbert klassenlichaam van $\mathbb{Q}(\sqrt{-14})$.

Voordat ik verder ga met de moderne wiskunde van Hilbert klassenlichamen, wil ik nog even de aandacht vestigen op twee andere zeer belangrijke vermoedens van Euler, die geleid hebben tot het verder ontwikkelen van de theorie van bikwadratische en kubische restklassen door Gauss.

$p = x^2 + 27y^2 \iff p = 1 \pmod{3}$ en 2 is een kubisch residu modulo p .

$p = x^2 + 64y^2 \iff p = 1 \pmod{4}$ and 2 is een bikwadratisch residu modulo p .

We zien dat, mede dankzij Euler's uitzonderlijke vermogen om patronen te herkennen, het probleem $p = x^2 + ny^2$ tot in de twintigste eeuw enorme impulsen heeft gegeven aan de gehele getaltheorie. De weg naar de oplossing ligt bezaaid met pareltjes als kwadratische, kubische en bikwadratische reciprociteit, kwadratische vormen, de theorie van geslachten en klassenlichamentheorie. Laten we nu verder gaan met het behandelen van één van die pareltjes: het Hilbert klassenlichaam.

Hoofdstuk 3

Het Hilbert klassenlichaam

Vanaf dit hoofdstuk wordt de lezer verondersteld bekend te zijn met de basisbegrippen van de algebraïsche getaltheorie.

Om het belang van het Hilbert klassenlichaam aan te geven, nodig ik de lezer uit te kijken naar deze stelling:

Stelling 3.1 *Zij $n \in \mathbb{N}$ kwadraatvrij en niet $3 \pmod{4}$, dan is er een monisch irreducibel polynoom $f_n(x) \in \mathbb{Z}[x]$ van graad $h(-4n)$ zodat als een oneven priemgetal p noch n , noch de discriminant van $f_n(x)$ deelt, dan:*

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ en} \\ f_n(x) \equiv 0 \pmod{p} \text{ heeft een gehele oplossing.} \end{cases}$$

Verder geldt dat je voor $f_n(x)$ het Galoispolynoom kan nemen van de uitbreiding van $K = \mathbb{Q}(\sqrt{-n})$ naar het Hilbertklassenlichaam $L = K(\alpha)$, waar α een reëel algebraïsch geheel getal is.

Dit geeft dus meteen voor ∞ veel n een oplossing voor het probleem! Het enige dat nog onduidelijk is, is wat $h(-4n)$ voorstelt en hoe je f_n berekent. $h(-4n)$ is het aantal elementen van de ideaalklassengroep van \mathcal{O}_K , waarop we later nog uitgebreid zullen terugkomen.

We spitsen ons nu toe op het proberen te begrijpen van het Hilbert klassenlichaam. Het Hilbert klassenlichaam L van een getallenlichaam K is de maximale onvertakte Abelse Galoisuitbreiding. Wat betekent dit?

Abels is makkelijk: de Galoisgroep moet Abels zijn.

Onvertakt is wat lastiger. Een uitbreiding van K naar L is onvertakt als enerzijds alle priemidealen van K onvertakt zijn in L en als anderzijds geen enkele reële inbedding $\sigma : K \rightarrow \mathbb{R}$ een complexe uitbreiding naar L heeft. De priemidealen van \mathcal{O}_K worden *eindige priemen* genoemd, de inbeddingen van K in \mathbb{R} *reële oneindige priemen* en paren complexe inbeddingen $\sigma, \bar{\sigma} : K \rightarrow \mathbb{C}$ *complexe oneindige priemen*. Een oneindige priem is dus vertakt als hij ofwel complex is, ofwel een complexe uitbreiding in L heeft. Bijvoorbeeld: De oneindige priem in \mathbb{Q} is onvertakt in $\mathbb{Q}(\sqrt{2})$, maar vertakt in $\mathbb{Q}(\sqrt{-2})$.

Tot slot de term maximaal. Om uit te leggen wat dit betekent, gebruik ik het volgende resultaat uit de klassenlichamentheorie:

Stelling 3.2 *Gegeven een getallenlichaam K , bestaat er een eindige Galois uitbreiding L van K zodanig dat:*

1. L is een onvertakte Abelse uitbreiding van K .
2. Elke onvertakte Abelse uitbreiding van K ligt in L .

Een onvertakte Abelse uitbreiding die aan 2. voldoet noemen we *maximaal*. Het lichaam L heet het *Hilbert klassenlichaam* en het is duidelijk dat het uniek is.

Het Hilbert klassenlichaam L van een getallenlichaam K heeft de volgende eigenschappen:

1. E is Galois over K
2. $[E : K] = h_K$ met h_K het klassengetal van K
3. De ideaalklassengroep $C(\mathcal{O}_K)$ is isomorf met de Galoisgroep van L over K .
4. Elk ideaal van \mathcal{O}_K is een hoofdideaal in \mathcal{O}_L .
5. Elk priemideaal \wp van \mathcal{O}_K valt uiteen in het product van $\frac{h_K}{f}$ priemidealen in \mathcal{O}_L , waar f de orde is van \wp in de ideaalklassengroep van \mathcal{O}_E .

Deze 5 eigenschappen samen zijn equivalent met: L is een maximale Abelse onvertakte uitbreiding van K , en zijn dus een andere manier om het Hilbert klassenlichaam te definiëren.

We zien hier duidelijk de belangwekkendheid van de ideaalklassengroep van K . Dit lijkt genoeg reden om eens nader bij deze groep stil te staan.

Hoofdstuk 4

De ideaalklassengroep

We zullen ons toespitsen op het zoeken naar de oplossing van $p = x^2 + ny^2$ voor $n = 14$. Dit is het kleinste geval waarin eenvoudige methoden (zoals kwadratische, kubische of bikwadratische reciprociteit, kwadratische vormen of geslachten) geen uitkomst bieden en er echt klassenlichamentheorie nodig is.

Laten we dus de ideaalklassengroep van $\mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$ maar eens berekenen. Hiertoe kijken we eerst maar eens hoe priemidealen van \mathbb{Z} splijten in $\mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$.

We weten dat $\mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$ gelijk is aan $\mathbb{Z}(\sqrt{-n})$ als $n \not\equiv 3 \pmod{4}$ en anders $\mathbb{Z}(\frac{1+\sqrt{-n}}{2})$. Dit is ook precies de reden dat in de bovengenoemde stelling de voorwaarde $n \not\equiv 3 \pmod{4}$ gebruikt wordt. $14 \not\equiv 3 \pmod{4}$, dus de ring van gehelen van $\mathbb{Q}(\sqrt{-14})$ is $\mathbb{Z}(\sqrt{-14})$.

Zij d_K de discriminant van een kwadratisch getallenlichaam K , p een priem in \mathbb{Z} en $(p) = p\mathcal{O}_K$ een ideaal in \mathcal{O}_K . De priemen splijten dan als volgt:

Stelling 4.1

1. Als $(d_K/p) = 0$ dan $(p) = \wp^2$ voor een zeker priemideaal \wp in \mathcal{O}_K .
2. Als $(d_K/p) = 1$ dan $(p) = \wp\wp'$ met $\wp \neq \wp'$.
3. Als $(d_K/p) = -1$ dan is (p) priem.

In het geval dat $K = \mathbb{Q}(\sqrt{-14})$ betekent dit voor de eerste paar priemmen:

$$\begin{aligned} (2) &= (2, \sqrt{-14})^2 \\ (3) &= (3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14}) \\ (5) &= (5, 2 + \sqrt{-14})(5, 2 - \sqrt{-14}) \\ (7) &= (7, \sqrt{-14})^2 \\ (11) &\text{ is priem} \\ (13) &= (13, 5 + \sqrt{-14})(13, 5 - \sqrt{-14}) \\ (17) &\text{ is priem} \\ (19) &= (19, 9 + \sqrt{-14})(19, 9 - \sqrt{-14}) \\ (23) &= (23, 3 - \sqrt{-14})(23, 3 + \sqrt{-14}) \end{aligned}$$

Een stelling van Minkowski vertelt ons dat alle ideaalklassen van $\mathbb{Z}(\sqrt{-14})$ een ideaal bevatten met norm kleiner dan $\frac{4\sqrt{52}}{\pi} \approx 9,18$, dus we hoeven niet verder dan (7) te kijken in het bovenstaande lijstje.

Verder weten we dat $(3, 1 + \sqrt{-14})$ en $(3, 1 - \sqrt{-14})$ in dezelfde klasse zitten, evenals $(5, 2 + \sqrt{-14})$ en $(5, 2 - \sqrt{-14})$, omdat ze slechts een hoofdideaal van elkaar verschillen.

En omdat $N(a + b\sqrt{-14}) = a^2 + 14b^2$ weten we dat $N(1 + \sqrt{-14}) = 15$, dus liggen de priemfactoren van het hoofdideaal $(1 + \sqrt{-14})$ over (3) en (5) (want voor zo'n priemfactor P moet $\|P\|$, $\|(1 + \sqrt{-14})\|$ delen, dus $\|P\| = 3$ of 5). Dus ook $(3, 1 + \sqrt{-14})$ en $(5, 2 + \sqrt{-14})$ liggen in dezelfde klasse.

We houden dan 4 klassen over:

1. de hoofdideaalklasse,
2. $(2, \sqrt{-14})$,
3. $(3, 1 + \sqrt{-14})$ en
4. $(7, \sqrt{-14})$.

Omdat $N(2, \sqrt{-14})$, $N(3, 1 + \sqrt{-14})$ en $N(7, \sqrt{-14})$ geen kwadraten zijn, zijn geen van de drie laatste klassen de hoofdideaalklasse. Verder weten we dat alle drie de klassen verschillend zijn en van orde 2. Daarom is de ideaalklassengroep gelijk aan $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Hoofdstuk 5

De oplossing voor ∞ veel n

De oplossing komt neer op het bewijzen van stelling 3.1.

Het eerste wat we gaan doen is het relateren van $p = x^2 + ny^2$ aan het volledig splijten van (p) in het Hilbert klassenlichaam.

Stelling 5.1 *Zij L het Hilbert klassenlichaam van $K = \mathbb{Q}(\sqrt{-n})$. Neem aan dat $n \in \mathbb{N}$ kwadraatvrij en niet $3 \pmod{4}$ is. Als nu p een oneven priemgetal is dat niet n deelt, dan geldt:*

$$p = x^2 + ny^2 \iff (p) \text{ splijt volledig in } L.$$

Bewijs: n is niet $3 \pmod{4}$, dus $\mathcal{O}_K = \mathbb{Z}(\sqrt{-n})$ en $d_K = -4n$. Omdat p een oneven priem is die niet n deelt, weten we dat $p \nmid d_K$, dus dat $(d_K/p) \neq 0$. Uit stelling uit stelling 4.1 volgt nu dat (p) onvertakt is.

Ik zal de volgende equivalenties laten zien:

$$\begin{aligned} p = x^2 + ny^2 &\iff (p) = \wp\bar{\wp}, \wp \neq \bar{\wp} \text{ en } \wp \text{ is hoofdideaal in } \mathcal{O}_K. \\ &\iff (p) = \wp\bar{\wp}, \wp \neq \bar{\wp} \text{ en } \wp \text{ splijt volledig in } L. \\ &\iff (p) \text{ splijt volledig in } L. \end{aligned}$$

De eerste equivalentie: Stel dat $p = x^2 + ny^2 = (x + \sqrt{-ny})(x - \sqrt{-ny})$. Neem $\wp = (x + \sqrt{-ny})$, dan moet $(p) = \wp\bar{\wp}$ dus wel de priemfactorisatie zijn van (p) in \mathcal{O} . Merk op dat $\wp \neq \text{bar}\wp$ omdat (p) onvertakt is. Dat \wp een hoofdideaal is, is evident. Omgekeerd: stel dat $(p) = \wp\bar{\wp}$, met \wp hoofdideaal, dan kunnen we, omdat $\mathcal{O} = \mathbb{Z}(\sqrt{-n})$, $\wp = (x + \sqrt{-ny})$ schrijven. Dit impliceert

dat $(p) = (x^2 + ny^2)$ en dus $p = x^2 + ny^2$.

In het bijzonder betekent dit voor het geval $n = 14$, dat $(23) = \wp\bar{\wp}$, met $\wp \neq \text{bar}\wp$ en \wp een hoofdideaal, omdat $23 = 3^2 + 14 \cdot 1^2$. We hadden in het vorige hoofdstuk gevonden dat $(23) = (23, 3 - \sqrt{-14})(23, 3 + \sqrt{-14})$, dus dat betekent dat $(23, 3 + \sqrt{-14})$ een hoofdideaal moet zijn en wel het hoofdideaal $(3 + \sqrt{-14})$. Dit klopt ook, want even zoeken levert op dat $23 = -(3 + \sqrt{-14})^2 + 6(3 + \sqrt{-14})$.

De tweede equivalentie is een resultaat uit de klassenlichamentheorie: Priemidealen die hoofdideaal zijn in K , zijn precies de idealen die volledig splijten in L .

Omdat we weten (uit de eigenschappen van L) dat L Galois is over K is de laatste equivalentie niet moeilijk meer.

$$(p) = \wp\bar{\wp}, \quad \wp \neq \bar{\wp} \text{ en } \wp \text{ splijt volledig in } L$$

zegt dat (p) volledig splijt in K en dat \wp , die over (p) ligt, volledig splijt in L , maar omdat L Galois is over \mathbb{Q} splijt dan ook zijn complex geconjugeerde $\bar{\wp}$ en dus splijt (p) volledig in L . \square

Wat we nu nog moeten doen is het volledig splijten van (p) in L koppelen aan de voorwaarden uit stelling ???. Dit komt neer op het bewijzen van de volgende stelling:

Stelling 5.2 *Zij K een imaginair kwadratisch lichaam en L een eindige uitbreiding van K die Galois is over \mathbb{Q} , dan geldt*

1. *Er bestaat een reëel algebraïsch geheel getal α zodanig dat $L = K(\alpha)$.*
2. *Gegeven zo'n α , laat $f(x) \in \mathbb{Z}[x]$ zijn monisch minimaalpolynoom zijn. Als p een priemgetal is dat niet de discriminant van $f(x)$ deelt, dan*

$$(p) \text{ splijt volledig in } L \iff \begin{cases} (d_K/p) = 1 \text{ en } f(x) = 0 \pmod{p} \\ \text{heeft een gehele oplossing} \end{cases} \quad (5.1)$$

Bewijs: Omdat we weten dat L Galois is over \mathbb{Q} , hebben we het volgende diagram

$$= \begin{array}{ccc} & 2 & \\ L \cap \mathbb{R} & - & L \\ | & & | \\ \mathbb{Q} & - & K \\ & 2 & \end{array} =$$

en kunnen we concluderen dat $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$. Dus hebben we voor een reële α in L dat

$$L \cap \mathbb{R} = \mathbb{Q}(\alpha) \iff L = K(\alpha).$$

Dus als $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ voldoet aan $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$, dan is α een reëel algebraïsch geheel primitief element van L over K , met een monisch minimaalpolynoom $f(x) \in \mathbb{Z}[x]$. Aangezien $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$ is $f(x)$ ook het minimaalpolynoom van α over K .

Om het tweede deel van de stelling te laten zien, zij p een priemgetal dat niet de discriminant van $f(x)$ deelt. We weten dan (uit Marcus) dat het volledig splijten van (p) in K (dus $(p) = \wp \bar{\wp}$, $\wp \neq \bar{\wp}$) equivalent is met $(d_K/p) = 1$. Wat we dan nog moeten laten zien, is dat het splijten van \wp in L equivalent is met $f(x) = 0 \pmod p$ voor een gehele x .

We weten uit Marcus dat het splijten van f modulo \wp (oftewel het hebben van een nulpunt in \mathcal{O}_K modulo \wp), equivalent is met het splijten van \wp in L . Om het even wat duidelijker te zeggen:

$$\wp \text{ splijt volledig in } L \iff f(x) \equiv 0 \pmod \wp \text{ is oplosbaar in } \mathcal{O}_K.$$

Verder weten we, omdat p volledig splijt in K , dat $\mathbb{Z}/p\mathbb{Z} \simeq \mathcal{O}_K/\wp$, dus geldt:

$$f(x) \equiv 0 \pmod \wp \text{ is oplosbaar in } \mathcal{O}_K \iff f(x) \equiv 0 \pmod p \text{ is oplosbaar in } \mathbb{Z}.$$

Waarmee de stelling bewezen is. \square

Als we nu 5.1 en 5.2 combineren, zien we dat we ons hoofddoel bereikt hebben. We hebben het probleem welke priemgetallen te schrijven zijn als $x^2 + ny^2$ opgelost voor oneindig veel n . Een schitterend resultaat waar Gauss jaloers op zou zijn. Een aantal vragen blijven nog wel staan, zoals wat er gebeurt als $n = 3 \pmod 4$ (en dus de ring van gehele niet meer $\mathbb{Z}(\sqrt{-n})$ is) en

hoe je precies het Galoispolynoom f_n vindt en waarom dit polynoom graad $h(-4n)$ heeft. Ook deze problemen zijn voor de mensheid geen geheim meer en de nieuwsgierige lezer verwijs ik dan ook naar het boek van David A. Cox.

Tot slot wil ik het probleem nog expliciet oplossen voor $n = 14$.

Hoofdstuk 6

Expliciete oplossing voor $n=14$

Om het probleem voor $n = 14$ op te lossen, hebben we het Galoispolynoom f_14 van het Hilbertklassenlichaam L over $K = \mathbb{Q}(\sqrt{-14})$ nodig. Aangezien we nog geen methode hebben om dit polynoom te vinden, zullen we aannemen dat we het "bij toeval" gevonden hebben. Het goede antwoord is $L = K(\alpha)$ met $\alpha = \sqrt{2\sqrt{2}-1}$. Het oplossen van het probleem $p = x^2 + ny^2$ komt dus neer op het bewijzen van de volgende stelling:

Stelling 6.1 *Het Hilbertklassenlichaam van $K = \mathbb{Q}(\sqrt{-14})$ is $L = K(\alpha)$ met $\alpha = \sqrt{2\sqrt{2}-1}$.*

Bewijs: Aangezien $h(-4n) = 4$, zoals we in hoofdstuk 4 hebben kunnen zien, heeft het Hilbertklassenlichaam graad 4 over K . Dus $L = K(\alpha)$ is het Hilbertklassenlichaam zodra we hebben laten zien dat $K \subset L$ een onvertakte Abelse uitbreiding van graad 4 is. Aangezien K imaginair kwadratisch is, zijn de oneindige priemenvolgen automatisch onvertakt.

Merk op dat $\alpha^2 = 2\sqrt{2} - 1$, dus $\sqrt{2} \in L$. Als we nu $K_1 = K(\sqrt{2})$ stellen, kunnen we de uitbreiding $K \subset L$ opdelen in twee tweedegraads uitbreidingen

$$K \subset K_1 \subset L,$$

waarmee we meteen hebben laten zien dat de uitbreiding Abels en van graad 4 is. Het is nu voldoende om te laten zien dat $K \subset K_1$ en $K_1 \subset L$ onvertakt zijn. Aangezien beide uitbreidingen verkregen zijn door het toevoegen van een wortel ($K_1 = K(\sqrt{2})$ en $L = K_1(\mu, \mu = 2\sqrt{2} - 1)$), is het handig om een algemeen lemma over deze situatie te bewijzen.

Lemma 6.2 *Zij $L = K(u)$ een kwadratische uitbreiding met $u \in \mathcal{O}_K$ en zij \wp een priem in \mathcal{O}_K .*

1. *Als $2u \notin \wp$ onvertakt is in L .*
2. *Als $2 \in \wp, u \notin \wp$ en $u = b^2 - 4c$ voor zekere $b, c \in \mathcal{O}_K$, dan is \wp onvertakt in L .*

Bewijs: (i) Merk op dat de discriminant van $x^2 - u$ gelijk is aan $4u \notin \wp$. Dit betekent dat $x^2 - u$ splijt modulo \wp en dus is \wp onvertakt in L .

(ii) Merk op dat $L = K(\beta)$, waar $\beta = (-b + \sqrt{u})/2$ een wortel is van $x^2 + bx + c$. De discriminant is $b^2 - 4c = u \notin \wp$, dus \wp is wederom onvertakt.

Nu kunnen we het bewijs voltooien. Eerst de uitbreiding $K \subset K_1$. Aangezien $K_1 = K(\sqrt{2})$ kunnen we voor een priem $\wp \in \mathcal{O}_K$ onderdeel (i) van het lemma gebruiken om in te zien dat \wp onvertakt is als $2 \notin \wp$. Nu de situatie dat 2 wel in \wp zit. Eerst merken we op dat, omdat $\sqrt{-14} \in K$ en $\sqrt{2} \in K_1$, ook $\sqrt{-7} \in K_1$ en dus dat $K_1 = K(\sqrt{7})$. Omdat $-7 \notin \wp$ en $-7 = 1^2 - 4 \cdot 2$ zien we nu met behulp van onderdeel (ii) van het lemma in dat \wp ook in dit geval onvertakt is.

Tot slot de uitbreiding $K_1 \subset L$. We weten dat $L = K_1(\sqrt{\mu})$, $\mu = 2\sqrt{2} - 1$. Zij $\mu' = -2\sqrt{2} - 1$. Uit $\sqrt{\mu\mu'} = \sqrt{-7}$ volgt dat ook $\sqrt{\mu'} \in L$ en dus dat $L = K_1(\sqrt{\mu}) = K_1(\sqrt{\mu'})$.

Laat nu \wp een priem zijn in K_1 . Als $2 \notin \wp$, dan volgt uit $\mu + \mu' = -2$ dat ofwel $\mu \notin \wp$ ofwel $\mu' \notin \wp$ en dus is \wp in dat geval onvertakt. En als 2 wel in \wp zit, dan $\mu \notin \wp$ aangezien $\mu = 2\sqrt{2} - 1$. Ook hebben we dat $\mu = (1 + \sqrt{2})^2 - 4$, dus volgt uit onderdeel (ii) van het lemma dat \wp onvertakt is.

Dit voltooit het bewijs dat $K \subset L$ een onvertakte Abelse uitbreiding van graad 4 is, dus moet L wel het Hilbertklassenlichaam zijn. \square

Nu kunnen we stelling 5.1 toepassen om een eenvoudig na te gaan criterium te geven voor wanneer priemgetallen te schrijven zijn als $x^2 + 14y^2$.

De oplossing: Als p een oneven priemgetal ongelijk aan 7 is, dan geldt:

$$p = x^2 + 14y^2 \iff (-14/p) = 1 \text{ en } (x^2 + 1)^2 \equiv 8 \pmod{p}$$

heeft een gehele oplossing.

Bibliografie

- [1] Cox, David A., *Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication*
- [2] Marcus, Daniel A., *Number Fields*
- [3] Beukers, F., *Dictaat Elementaire Getaltheorie* Universiteit Utrecht
- [4] <http://planetmath.org/encyclopedia/HilbertClassField.html>