Analytische bewijzen van de kwadratische en de kwartische reciprociteit

Marco Streng

7 augustus 2004 (aangepast 30 november)

Samenvatting

Een uitwerking van de analytische bewijzen uit [7] voor de kwadratische en de kwartische reciprociteitswetten. Deze bewijzen zijn oorspronkelijk afkomstig van Eisenstein.

Deze tekst is geschreven als kleine scriptie aan de Universiteit Utrecht onder begeleiding van Gunther Cornelissen.

Inhoudsopgave

1 Inleiding

De kwadratische residu-symbolen zijn getaltheoretische symbolen die aangeven of een gegeven getal congruent is aan een kwadraat, modulo een gegeven priemgetal. Ongeveer analoog aan de kwadratische residu-symbolen, bestaan er ook kwartische residu-symbolen, die iets zeggen over vierdemachten. In deze tekst geven we een analytisch bewijs van Eisenstein voor de kwadratische reciprociteitswet, die iets zegt over het verband tussen kwadratische residu-symbolen. Het mooiste aan dit bewijs is dat het, met de juiste functie, om te zetten is in een eenvoudig bewijs van de reciprociteitswet voor kwartische residu-symbolen.

We beginnen het eerste hoofdstuk door de kwadratische residu-symbolen in te voeren en er wat theorie over te geven. Daarbij formuleren we de kwadratische reciprociteitswet, maar bewijzen we hem niet. Daarna volgt een toepassing van de kwadratische reciprociteit, die direct een nieuwe vraag oproept. Die vraag wekt extra interesse op voor de kwartische reciprociteit. We gaan dan verder met het invoeren van de kwartische residu-symbolen en formuleren ook de kwartische reciprociteitswet.

In het tweede hoofdstuk geven we het Lemma van Gauss, dat een belangrijk hulpmiddel is bij het bestuderen van residu-symbolen. In het hoofdstuk daarna wordt het analytische bewijs van Eisenstein voor de kwadratische reciprociteit gegeven. En in het daarop volgende hoofdstuk wordt dit omgezet in Eisensteins bewijs voor de kwartische reciprociteit. Daarvoor moet dan wel eerst de theorie van elliptische functies ontwikkeld worden.

In het laatste hoofdstuk wordt het bewijs van de kwartische reciprociteitswet afgerond en kan het probleem uit de toepassing opgelost worden.

1.1 Kwadratische reciprociteit

1.1.1 Legendre-symbolen

Lemma 1.1. *Zij p een oneven priemgetal en a een geheel getal dat niet deelbaar is door p. Dan $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ voor precies één keuze van $\pm$.*

Bewijs. Schrijf $\alpha = a^{\frac{p-1}{2}}$. De kleine stelling van Fermat zegt dat $\alpha^2 = a^{p-1} \equiv 1 \pmod{p}$, dus $0 = \alpha^2 - 1 = (\alpha - 1)(\alpha + 1)$ in het lichaam $\mathbb{Z}/p\mathbb{Z}$. Dus $\alpha \equiv \pm 1 \pmod{p}$. Verder $1 \not\equiv -1 \pmod{p}$, omdat $p > 2$. □

Dit lemma stelt ons in staat het **Legendre-symbool** als volgt te definiëren.

Definitie 1.2. *Zij p een oneven priemgetal en a een geheel getal dat niet deelbaar is door p. Het Legendre-symbool van a modulo p, notatie $(\frac{a}{p})$, is dat element van $\{\pm 1\}$ waarvoor*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Het Legendre-symbool wordt ook wel het kwadratische residu-symbool genoemd. Wat dit symbool te maken heeft met kwadratische residuen wordt duidelijk uit de volgende stelling.

Stelling 1.3. *Zij p een oneven priemgetal en a een geheel getal dat niet deelbaar is door p. De congruentievergelijking $x^2 \equiv a \pmod{p}$ heeft een oplossing $x \in \mathbb{Z}[i]$, precies als $(\frac{a}{p}) = 1$.*

Bewijs. We gaan bewijzen dat de kwadraten modulo p precies de oplossingen a van de vergelijking $a^{(p-1)/2} \equiv 1 \pmod{p}$ zijn.

Als $x^2 \equiv a \pmod{p}$, dan volgt direct uit de Kleine Stelling van Fermat dat $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. Alle kwadraten zijn dus oplossingen van de vergelijking.

Bekijk $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Als $a^2 \equiv b^2 \pmod{p}$, dan volgt $a \equiv \pm b \pmod{p}$ en als bovendien $1 \leq a, b \leq \frac{p-1}{2}$, dan volgt $a = b$. Dit zijn dus $\frac{p-1}{2}$ verschillende kwadraten modulo p.

We hebben nu $\frac{p-1}{2}$ nulpunten gevonden van de veelterm $a^{\frac{p-1}{2}} - 1$ van graad $\frac{p-1}{2}$ in het lichaam $\mathbb{Z}/p\mathbb{Z}$. Dat zijn dus alle nulpunten, dus alle oplossingen van de vergelijking zijn kwadraten modulo p. □

De kwadratische reciprociteitswet is de volgende stelling, die het verband tussen $(\frac{p}{q})$ en $(\frac{q}{p})$ aangeeft.

Stelling 1.4. *Zijn p, q oneven priemgetallen, dan,*

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

Daarnaast gelden de twee supplementaire wetten

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \textit{en} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

De eerste supplementaire wet is niets anders dan de definitie. Voor het bewijs van de rest van deze stelling is wat meer nodig. Een belangrijke stap daarin is het lemma van Gauss, dat in sectie 2.1 wordt geformuleerd. Daar wordt ook een bewijs gegeven voor de tweede supplementaire wet. In sectie 3 volgt een analytisch bewijs van Eisenstein voor de kwadratische reciprociteit zelf.

1.1.2 Jacobi-symbolen

We kunnen de Legendre-symbolen, dankzij unieke factorisatie in priemgetallen, als volgt generaliseren tot de **Jacobi-symbolen**.

Definitie 1.5. *Zijn m, n onderling ondeelbare gehele getallen, en is n bovendien positief en oneven. Dan is het Jacobi-symbool $(\frac{m}{n})$ gedefinieerd door het product*

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_k}\right),$$

waarbij $n = p_1 \cdots p_k$ de factorisatie van n in priemgetallen is.

Stelling 1.6 (Kwadratische reciprociteit)**.** *Zijn n, m onderling ondeelbare oneven positieve gehele getallen, dan,*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Daarnaast gelden de twee supplementaire wetten

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \quad \textit{en} \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Bewijs. Stelling 1.4 zegt dat deze vergelijkingen kloppen voor oneven priemgetallen. Laat $n = p_1 \cdots p_r$ en $m = q_1 \cdots q_s$ de priemontbindingen van n en m zijn. Als k het

aantal indices i is met $p_i \equiv -1 \pmod 4$, dan $\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \equiv k \equiv \frac{n-1}{2} \pmod 2$. Er volgt

$$\begin{aligned}
\left(\frac{-1}{n}\right) &= \prod_{i=1}^{r} (-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{n-1}{2}} \quad \text{en} \\
\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\prod_{i=1}^{r}\left(\frac{m}{p_i}\right)\right)\left(\prod_{j=1}^{s}\left(\frac{n}{q_j}\right)\right) \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{q_j-1}{2}\frac{p_i-1}{2}} \\
&= (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.
\end{aligned}$$

Voor elke i: $p_i^2 \equiv 1, 9 \pmod{16}$ en $9^2 \equiv 1 \pmod{16}$. Als l het aantal indices i is met $p_i^2 \equiv 9 \pmod{16}$, dan $\frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} \equiv l \equiv \frac{n^2-1}{8} \pmod{16}$. Dus volgt ook

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{r}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\frac{n^2-1}{8}}.$$

□

1.2 Toepassing

Neem een oneven getal $q \geq 3$ en stel dat $p = 4q + 1$ een priemgetal is. Laat $S_q = 2^{2q} + 1$, dan heeft S_q de factorisatie

$$S_q = A_q \cdot B_q, \quad A_q = 2^q - 2^{\frac{q+1}{2}} + 1, \quad B_q = 2^q + 2^{\frac{q+1}{2}} + 1.$$

Er geldt $p = 4q + 1 \equiv 5 \pmod 8$, dus met de tweede supplementaire wet van de kwadratische reciprociteit volgt

$$\begin{aligned}
S_q &= 2^{2q} + 1 = 2^{\frac{p-1}{2}} + 1 \equiv \left(\frac{2}{p}\right) + 1 \\
&= (-1)^{\frac{p^2-1}{8}} + 1 = 0 \pmod p,
\end{aligned}$$

oftewel p deelt $S_q = A_q \cdot B_q$. De tweede supplementaire wet van de kwadratische reciprociteit heeft ons dus verteld dat A_q of B_q deelbaar is door p. De vraag is nu, welke?

Als we p schrijven als som van twee kwadraten, $p = a^2 + b^2$ met a oneven en b even, dan hebben we de factorisatie $p = (a + bi)(a - bi)$. We willen weten of $A_q \equiv 0 \pmod p$ of $B_q \equiv 0 \pmod p$, daarom zijn we geïnteresseerd in A_q en B_q modulo $a+bi$ en dus in a en b. Met behulp van een computer kunnen we de volgende

tabel maken.

q	p	$p\vert\cdot$	a	$\frac{b}{2}$
3	13	B	3	1
7	29	B	5	1
9	37	A	1	3
13	53	B	7	1
15	61	A	5	3
25	101	A	1	5
27	109	A	3	5
37	149	A	7	5
39	157	A	11	3
43	173	B	13	1
45	181	A	9	5
49	197	B	1	7
57	229	B	15	1
67	269	A	13	5
69	277	B	9	7
73	293	B	17	1
79	317	B	11	7
87	349	B	5	9

q	p	$p\vert\cdot$	a	$\frac{b}{2}$
93	373	B	7	9
97	389	A	17	5
99	397	A	19	3
105	421	B	15	7
115	461	A	19	5
127	509	A	5	11
135	541	A	21	5
139	557	B	19	7
153	613	B	17	9
163	653	A	13	11
165	661	A	25	3
169	677	A	1	13
175	701	A	5	13
177	709	A	15	11
183	733	B	27	1
189	757	A	9	13
193	773	A	17	11
199	797	A	11	13

Deze tabel leidt tot het volgende vermoeden.

Vermoeden 1.7. *Met de bovenstaande notatie hebben we*

$$p|A_q \iff \frac{b}{2} \equiv \pm 3 \pmod 8 \quad \textit{en} \quad p|B_q \iff \frac{b}{2} \equiv \pm 1 \pmod 8.$$

Om dit vermoeden te bewijzen moeten we onder andere $2^q = 2^{\frac{p-1}{4}}$ bepalen modulo $a + bi$. Hiervoor gaan we de kwartische reciprociteit gebruiken.

1.3 Kwartische reciprociteit

In de eerste paragraaf werden de kwadratische residu-symbolen voor $\mathbb{Z}$ ingevoerd. In deze paragraaf zullen, analoog daaraan, de kwartische residu-symbolen voor $\mathbb{Z}[i]$ ingevoerd worden.

Voordat we daarmee beginnen, zetten we eerst nog wat eigenschappen van $\mathbb{Z}[i]$ op een rij en voeren we de primaire elementen van $\mathbb{Z}[i]$ in. Deze kunnen dan de rol van de positieve oneven getallen overnemen.

1.3.1 Eigenschappen van $\mathbb{Z}[i]$

Is $\alpha = a + bi \in \mathbb{Z}[i]$, dan gebruiken we de notatie $\overline{\alpha} := a - bi$ voor de complex geconjugeerde van α en $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2$ noemen we de norm van α.

In §1.3 en §1.4 van Ireland en Rosen [4] is te zien dat $\mathbb{Z}[i]$ een hoofdideaaldomein (HID) is. Daar wordt ook bewezen dat elk tweetal elementen a, b van een HID R een grootste gemeenschappelijke deler $d = \text{ggd}(a, b)$ heeft en dat de idealen $(a, b) := \{xa + yb \mid x, y \in R\}$ en $(d) := \{zd \mid z \in R\}$ aan elkaar gelijk zijn. Dit betekent dat $d \in (a, b)$, dus dat er $x, y \in R$ zijn zodat $xa + yb = d$. Voor elke $a, b \in \mathbb{Z}[i]$ zijn er dus $x, y \in \mathbb{Z}[i]$ zodat $xa + yb = \text{ggd}(a, b)$.

In dezelfde bron wordt ook bewezen dat elk hoofdideaaldomein een uniekefactorisatiedomein is. Dat wil zeggen dat elke $\alpha \neq 0$ in $\mathbb{Z}[i]$ een unieke factorisatie in irreducibele elementen van $\mathbb{Z}[i]$ heeft, op de volgorde van de factoren en vermenigvuldiging van de factoren met eenheden na.

Lemma 1.8. *De eenheden van $\mathbb{Z}[i]$ zijn precies de elementen u met $N(u) = 1$ en dat zijn precies ± 1 en $\pm i$. Is $\alpha \in \mathbb{Z}[i]$ met $N(\alpha) \geq 5$, dan zijn de vier eenheden verschillend modulo α.*

Bewijs. Uit $\pm 1 \cdot \pm 1 = 1$ en $i \cdot -i = 1$ volgt dat ± 1 en $\pm i$ eenheden zijn. Stel nu dat u een eenheid is, dus dat $uv = 1$ voor een $v \in \mathbb{Z}[i]$. Dan volgt $N(u)N(v) = N(uv) = 1$, dus $N(u) = 1$, waaruit volgt $u = \pm 1$ of $u = \pm i$.

Neem nu $\alpha \in \mathbb{Z}[i]$ met $N(\alpha) \geq 5$ en stel dat u, u' eenheden zijn met $u \equiv u' \pmod{\alpha}$. Uit $u, u' \in \{\pm 1, \pm i\}$, volgt $N(u - u') \in \{0, 2, 4\}$, dus $N(u - u') < 5$. Maar $\alpha | (u - u')$, dus $N(\alpha) | N(u - u')$ met $N(\alpha) \geq 5$. Daaruit volgt $N(u - u') = 0$ en dus $u = u'$. □

Lemma 1.9. *Is p een priemgetal in $\mathbb{Z}$. Dan geldt het volgende:*

1. *Als $p \equiv 1 \pmod 4$, dan $p = \pi\overline{\pi}$ voor een irreducibel element π van $\mathbb{Z}[i]$.*
2. *Als $p \equiv 3 \pmod 4$, dan is p irreducibel in $\mathbb{Z}[i]$.*
3. *$1 + i$ is irreducibel in $\mathbb{Z}[i]$.*

Bewijs. Stel dat $p \equiv 1 \pmod 4$ een priemgetal is. Uit $(\frac{-1}{p}) = (-1)^{(p-1)/2} = 1$ volgt dat er een x is met $x^2 \equiv -1 \pmod p$. Dus $p | (x^2 + 1) = (x + i)(x - i)$. Als p irreducibel is in $\mathbb{Z}[i]$, dan $p | (x + i)$ of $p | (x - i)$, dus $p | i$ en dat kan niet. Daaruit volgt dat p reducibel is. In de factorisatie van p komen dus minstens twee irreducibelen voor. Schrijf $p = \pi\alpha$ met π irreducibel. Omdat π en α beide geen eenheden zijn, geldt $N(\pi), N(\alpha) \neq 1$. Dus uit $N(\pi)N(\alpha) = N(p) = p^2$ volgt $\pi\overline{\pi} = N(\pi) = p$.

Stel nu dat $p \equiv 3 \pmod 4$ priem is in $\mathbb{Z}$, maar reducibel in $\mathbb{Z}[i]$. Schrijf $p = \pi\alpha$ met π irreducibel. Zoals boven al is bewezen volgt nu $N(\pi) = p$. Schrijf $\pi = a + bi$, dan $p = N(\pi) = a^2 + b^2$. Kwadraten zijn 0 of 1 modulo 4, dus dit is in tegenspraak met $p \equiv 3 \pmod 4$.

Stel als laatste dat $1 + i = \alpha\beta$, dan $N(\alpha)N(\beta) = N(1 + i) = 2$, dus $N(\alpha) = 1$ of $N(\beta) = 1$. Dus α of β is een eenheid, $1 + i$ is irreducibel. □

1.3.2 Primaire elementen van $\mathbb{Z}[i]$

Definitie 1.10. *Een element α van $\mathbb{Z}[i]$ heet primair als $\alpha \equiv 1 \pmod{2 + 2i}$.*

Lemma 1.11. *Een element $a + bi$ van $\mathbb{Z}[i]$ is primair, precies als aan één van de volgende voorwaarden is voldaan:*

1. *$a \equiv 1 \pmod 4$ en $b \equiv 0 \pmod 4$.*
2. *$a \equiv 3 \pmod 4$ en $b \equiv 2 \pmod 4$.*

Bewijs.

$$\begin{aligned} a + bi \equiv 1 \pmod{2 + 2i} &\iff \exists x, y \in \mathbb{Z} : a + bi = 1 + (x + yi)(2 + 2i) \\ &\iff \exists x, y \in \mathbb{Z} : a + bi = 1 + 2(x - y) + 2i(x + y) \\ &\iff \exists x, y \in \mathbb{Z} : \begin{cases} a = 1 + 2(x - y) \\ b = 2(x + y) \end{cases} \end{aligned}$$

Voor $x + y$ even is dit equivalent met $a \equiv 1, b \equiv 0 \pmod 4$ en voor $x + y$ oneven met $a \equiv 3, b \equiv 2 \pmod 4$. □

Lemma 1.12. *Zij $\alpha \in \mathbb{Z}[i]$ en stel dat $(1 + i) \nmid \alpha$. Dan is er een unieke eenheid u zodat $u\alpha$ primair is.*

Bewijs. Schrijf $\alpha = a+bi$, dan zijn a en b niet beide even en ook niet beide oneven. Stel namelijk dat a en b beide even zijn, dan volgt $(1+i)(1-i) = 2|(a+bi)$ en dat is in tegenspraak met de aanname dat $(1+i) \nmid \alpha$. Op dezelfde manier leidt ook de aanname dat a en b beide oneven zijn tot een tegenspraak, omdat dan $2|(a+bi+(1+i))$.

Door α indien nodig met i te vermenigvuldigen kan nu aangenomen worden dat a oneven is en b even. Modulo 4 zijn er nu dus vier mogelijkheden voor a en b. Door elk van deze mogelijkheden langs te gaan, en daarbij eventueel te vermenigvuldigen met -1, blijkt dat $a+bi$ voldoet aan de voorwaarden die genoemd zijn in lemma 1.11. Dit bewijst de existentie van u.

Stel nu dat $u\alpha$ en $u'\alpha$ beide primair zijn, dan $u\alpha \equiv 1 \equiv u'\alpha \pmod{2+2i}$, dus $(1+i)^3|(u-u')\alpha$. Omdat $1+i$ irreducibel is en $(1+i) \nmid \alpha$, volgt $(1+i)^3|(u-u')$. Dus $u \equiv u' \pmod{(1+i)^3}$. Maar $N((1+i)^3) = 2^3 \geq 5$, dus uit lemma 1.8 volgt $u = u'$. □

Lemma 1.13. *Elk primair element van $\mathbb{Z}[i]$ is op unieke wijze (op volgorde na) te schrijven als het product van primaire irreducibelen.*

Bewijs. Zij $\alpha \in \mathbb{Z}[i]$ primair. Schrijf $\alpha = u\pi_1 \cdots \pi_t$ met $\pi_1, \cdots, \pi_t$ irreducibel en u een eenheid. Wegens unieke factorisatie in $\mathbb{Z}[i]$ kan dit en is de uitdrukking uniek, afgezien van de volgorde van de factoren en van vermenigvuldiging van de factoren met eenheden. Volgens lemma 1.12 kan elk van de π_j hierin op unieke wijze primair gekozen worden. Dit maakt de uitdrukking uniek op volgorde na. Reduceer hem nu modulo $2+2i$ tot $1 \equiv u \pmod{2+2i}$, zodat, uit lemma 1.8, volgt $u = 1$. □

1.3.3 Kwartische residu-symbolen

Lemma 1.14. *Zij $\alpha \in \mathbb{Z}[i]$ ongelijk aan nul. De ring $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ van restklassen modulo α heeft $N(\alpha)$ elementen. Als α irreducibel is, dan is deze ring een lichaam.*

Bewijs. Stel $\alpha = a+bi \in \mathbb{Z}[i]$ is ongelijk aan nul. Schrijf (a,b) voor de positieve grootste gemeenschappelijke deler van a en b. We zullen bewijzen dat elke restklasse modulo α precies één representant heeft in de verzameling

$$R := \{s+ti \mid 0 \leq s < \frac{a^2+b^2}{(a,b)}, 0 \leq t < (a,b)\}.$$

Daaruit volgt dan dat $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ precies $\frac{a^2+b^2}{(a,b)} \cdot (a,b) = a^2+b^2 = N(\alpha)$ elementen heeft.

Zij $m+ni \in \mathbb{Z}[i]$. We willen laten zien dat er een unieke $s+ti \in R$ is zodat $m+ni \equiv s+ti \pmod{\alpha}$. Met het Euclidische Algoritme kunnen we $x, y \in \mathbb{Z}$ nemen met $xa+yb = (a,b)$. Dan $(y+xi)\alpha = (ya-xb)+(xa+yb)i = (ya-xb)+(a,b)i$, dus $(a,b)i \equiv xb-ya \pmod{\alpha}$. Laat nu t de rest van n bij deling door (a,b) zijn. Met andere woorden, neem q en t met $n = q(a,b)+t$ en $0 \leq t < (a,b)$. Dan volgt $m+ni = m+q(a,b)i+ti \equiv m+q(xb-ya)+ti \pmod{\alpha}$. Er geldt ook $(a^2+b^2)/(a,b) = (a-bi)/(a,b) \cdot (a+bi) \equiv 0 \pmod{\alpha}$. Laat nu s de rest zijn bij deling van $m+q(xb-ya)$ door $(a^2+b^2)/(a,b)$, dan volgt $m+ni \equiv m+q(xb-ya)+ti \equiv s+ti \pmod{\alpha}$ en $s+ti \in R$.

Stel nu dat $s+ti \equiv s'+t'i \pmod{\alpha}$ en $(s+ti), (s'+t'i) \in R$. Er is dan een $\gamma \in \mathbb{Z}[i]$ met $(s-s')+(t-t')i = \gamma(a+bi)$. Daaruit volgt direct $(a,b)|(t-t')$, maar $|t-t'| < (a,b)$, dus $t = t'$ en $s-s' = \gamma(a+bi)$. Vermenigvuldigen met $a-bi$ geeft $(s-s')(a-bi) = \gamma(a^2+b^2)$, oftewel $\gamma = (a-bi)(s-s')/N(\alpha)$. Dus zowel $a(s-s')/N(\alpha)$ als $b(s-s')/N(\alpha)$ is geheel. Met x en y zodat $xa+yb = (a,b)$ volgt dat ook $(s-s')(a,b)/N(\alpha)$ geheel is. Dus $N(\alpha)/(a,b)|(s-s')$, maar $|s-s'| < N(\alpha)/(a,b)$, dus $s = s'$, $s+ti = s'+t'i$. De ring $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ heeft dus $N(\alpha)$ elementen.

Stel nu dat α irreducibel is. Neem $\beta \in \mathbb{Z}[i]$ willekeurig zodat $\alpha \nmid \beta$. Omdat α irreducibel is en $\alpha \nmid \beta$, moet $\text{ggd}(\alpha, \beta) = 1$. Boven lemma 1.8 is bewezen dat er nu γ_1, γ_2 zijn, zodat $\gamma_1\alpha + \gamma_2\beta = 1$, dus $\gamma_2\beta \equiv 1 \pmod{\alpha}$. Daaruit volgt dat $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ een lichaam is. □

Gevolg 1.15. *Zij $\pi \in \mathbb{Z}[i]$ priem. De eenhedengroep $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ is een cyclische groep van orde $N(\pi) - 1$.*

Bewijs. De eenhedengroep van een eindig lichaam is cyclisch. Zie bijvoorbeeld §7.1 van [4] of §VIII.3 van [6]. □

Lemma 1.16. *Zij $\pi \in \mathbb{Z}[i]$ priem en primair. Dan is zijn de eenheden in $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ allen verschillend modulo π. We kunnen daarom $\mathbb{Z}[i]^*$ zien als deelgroep van de abelse groep $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ en daarmee de quotiëntgroep $Q = (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*/\mathbb{Z}[i]^*$ van orde $(N(\pi) - 1)/4$ maken.*

Bewijs. Stel dat twee eenheden in $\{\pm 1, \pm i\}$ congruent zijn modulo π. Het verschil van die eenheden is dan een veelvoud van $1 + i$, maar π is copriem met $1 + i$, want π is primair. □

Lemma 1.17. *Zij π een irreducibel element van $\mathbb{Z}[i]$ en $\alpha \in \mathbb{Z}[i]$, zodat $(1 + i) \nmid \pi$ en $\pi \nmid \alpha$. Dan*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv u \pmod{\pi}$$

voor precies één eenheid $u \in \mathbb{Z}[i]$.

Bewijs. Uit het vorige lemma volgt dat $(N(\pi) - 1)/4$ een geheel getal is. Omdat $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ een groep van orde $N(\pi) - 1$ is, weten we ook $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$. Daaruit volgt dat $\alpha^{(N(\pi)-1)/4}$ een nulpunt is van de veelterm $X^4 - 1$ in het lichaam $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. We weten dat de eenheden $\{\pm 1, \pm i\}$ verschillend zijn in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ en dat het nulpunten zijn van $X^4 - 1$. De eenheden $\{\pm 1, \pm i\}$ zijn dus precies de vier nulpunten van $X^4 - 1$ in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Conclusie $\alpha^{\frac{N(\pi)-1}{4}} \equiv u \pmod{\pi}$ voor precies één eenheid $u \in \{\pm 1, \pm i\} = \mathbb{Z}[i]^*$. □

Dit lemma stelt ons in staat het **kwartische of bikwadratische residu-symbool** als volgt te definiëren.

Definitie 1.18. *Zij $\pi \in \mathbb{Z}[i]$ primair en irreducibel en $\alpha \in \mathbb{Z}[i]$ niet deelbaar door π. Het kwartische residu-symbool van α modulo π, notatie $\left[\frac{\alpha}{\pi}\right]$ of $(\frac{\alpha}{\pi})_4$, is dat element van $\{\pm 1, \pm i\}$ waarvoor*

$$\left[\frac{\alpha}{\pi}\right] \equiv \alpha^{\frac{N(\pi)-1}{4}} \pmod{\pi}.$$

Zoals de Legendre-symbolen iets zeggen over de oplosbaarheid van kwadratische vergelijkingen in $\mathbb{Z}$, zo zeggen de kwartische residu-symbolen iets over de oplosbaarheid van vierdemachtsvergelijkingen in $\mathbb{Z}[i]$. Dat is te zien in de volgende stelling.

Stelling 1.19. *Zij $\pi \in \mathbb{Z}[i]$ primair en irreducibel en $\alpha \in \mathbb{Z}[i]$ niet deelbaar door π. De congruentievergelijking $x^4 \equiv \alpha \pmod{\pi}$ heeft een oplossing $x \in \mathbb{Z}[i]$, precies als $\left[\frac{\alpha}{\pi}\right] = 1$.*

Bewijs. Stel dat $x^4 \equiv \alpha \pmod{\pi}$. Gevolg 1.15 zegt dat $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ een groep is met $N(\pi) - 1$ elementen. Daaruit volgt $\alpha^{(N(\pi)-1)/4} \equiv x^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Stel, voor de andere kant van het bewijs, dat $\left[\frac{\alpha}{\pi}\right] = 1$. Neem een voortbrenger γ van de cyclische groep $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$. Dan is er een k zodat $\alpha \equiv \gamma^k \pmod{\pi}$. Nu geldt $\gamma^{k(N(\pi)-1)/4} = 1$, dus $k(N(\pi) - 1)/4$ is een veelvoud van $\text{ord}(\gamma) = N(\pi) - 1$. Daaruit volgt dat $\frac{k}{4}$ geheel is, dus $x = \gamma^{\frac{k}{4}}$ is een oplossing van de vergelijking. □

Het volgende lemma vertelt hoe de kwartische residu-symbolen zich gedragen met betrekking tot complexe conjugatie.

Lemma 1.20. *Is $\pi \in \mathbb{Z}[i]$ primair en irreducibel en $\alpha \in \mathbb{Z}[i]$ niet deelbaar door π. Dan is ook de complex geconjugeerde $\overline{\pi}$ van π primair en irreducibel en geldt*

$$\left[\frac{\overline{\alpha}}{\overline{\pi}}\right] = \overline{\left[\frac{\alpha}{\pi}\right]} = \left[\frac{\alpha}{\pi}\right]^{-1}.$$

Bewijs. Als $\overline{\pi} = \alpha\beta$, dan $\pi = \overline{\alpha}\overline{\beta}$, dus $\overline{\pi}$ is irreducibel. Verder geldt $\overline{\pi} \equiv \overline{1} \equiv 1 \pmod{\overline{2+2i} = -i(2+2i)}$, dus $\overline{\pi}$ is primair. Uit $[\frac{\alpha}{\pi}] \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}$ volgt dat er een γ is met

$$\overline{\left[\frac{\alpha}{\pi}\right]} = \overline{\alpha^{\frac{N(\pi)-1}{4}} + \gamma\pi} = \overline{\alpha}^{\frac{N(\pi)-1}{4}} + \overline{\gamma\pi} \equiv \overline{\alpha}^{\frac{N(\overline{\pi})-1}{4}} \pmod{\overline{\pi}}$$

Daaruit volgt $[\frac{\overline{\alpha}}{\overline{\pi}}] = \overline{[\frac{\alpha}{\pi}]}$. Verder is $[\frac{\alpha}{\pi}]$ een eenheid en $\overline{i} = i^{-1}$ en $\overline{1} = 1^{-1}$. □

Dankzij lemma 1.13, over unieke factorisatie in primaire irreducibelen, kunnen we de kwartische residu-symbolen op dezelfde manier generaliseren als de Legendre-symbolen.

Definitie 1.21. *Zijn $\alpha, \beta \in \mathbb{Z}[i]$ onderling ondeelbaar en is β primair. Dan is het kwartische residu-symbool $[\frac{\alpha}{\beta}]$ gedefinieerd door het product*

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\pi_1}\right] \cdots \left[\frac{\alpha}{\pi_k}\right],$$

waarbij $\beta = \pi_1 \cdots \pi_k$ de factorisatie van β in primaire irreducibelen is.

Stelling 1.22 (Kwartische reciprociteit)**.** *Zijn $\alpha = a + bi$ en $\beta = c + di \in \mathbb{Z}[i]$ onderling ondeelbaar en primair, dan,*

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right]^{-1} = (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}.$$

Daarnaast gelden de drie supplementaire wetten

$$\left[\frac{i}{\alpha}\right] = i^{\frac{N(\alpha)-1}{4}} = i^{\frac{1-a}{2}}, \quad \left[\frac{1+i}{\alpha}\right] = i^{\frac{a-b-b^2-1}{4}} \quad \text{en} \quad \left[\frac{2}{\alpha}\right] = i^{\frac{-b}{2}}.$$

Bewijs. Net als in het kwadratische geval, stellen we een deel van het bewijs uit. De reciprociteitswet zelf wordt, voor irreducibelen, analytisch bewezen in sectie 4 en de laatste twee supplementaire wetten worden in sectie 5 bewezen.

We beginnen nu met de eerste supplementaire wet. Is $\pi \in \mathbb{Z}[i]$ irreducibel en primair, dan volgt direct uit de definitie dat $[\frac{i}{\pi}] = i^{(N(\pi)-1)/4}$. Laat α_1 en α_2 willekeurige primaire elementen van $\mathbb{Z}[i]$ zijn. Schrijf $k_j = (N(\alpha_j)-1)/4$, dan volgt

$$\begin{aligned}
\frac{N(\alpha_1\alpha_2)-1}{4} &= \frac{(4k_1+1)(4k_2+1)-1}{4} \\
&= \frac{16k_1k_2 + 4(k_1+k_2)}{4} \equiv k_1 + k_2 \pmod 4 \\
&\equiv \frac{N(\alpha_1)-1}{4} + \frac{N(\alpha_2)-1}{4} \pmod 4.
\end{aligned}$$

Is $\alpha = \pi_1 \cdots \pi_n \in \mathbb{Z}[i]$ de ontbinding van α in primaire irreducibelen, dan volgt uit het bovenstaande,

$$\left[\frac{i}{\alpha}\right] = \prod_{k=1}^{n}\left[\frac{i}{\pi_k}\right] = \prod_{k=1}^{n} i^{\frac{N(\pi_k)-1}{4}} = i^{\frac{N(\alpha)-1}{4}}.$$

Volgens lemma 1.11 geldt $a \equiv 1, b \equiv 0 \pmod 4$ of $a \equiv 3, b \equiv 2 \pmod 4$. Als $a = 4k+1$, dan $a^2 + b^2 - 1 \equiv a^2 - 1 = 16k^2 + 8k \equiv 8k \equiv -8k = 2(1-a) \pmod{16}$ en als $a = 4k+3$, dan $a^2 + b^2 - 1 \equiv a^2 + 4 - 1 = 16k^2 + 24k + 12 \equiv 8k + 12 \equiv -8k - 4 = 2(1-a) \pmod{16}$. In beide gevallen geldt dus $\frac{N(\alpha)-1}{4} \equiv \frac{1-a}{2} \pmod 4$, waaruit volgt $\left[\frac{i}{\alpha}\right] = i^{(N(\alpha)-1)/4} = i^{(1-a)/2}$.

In sectie 4 zal bewezen worden dat voor ongelijke primaire irreducibelen $\pi, \lambda \in \mathbb{Z}[i]$ geldt,

$$\left[\frac{\pi}{\lambda}\right]\left[\frac{\lambda}{\pi}\right]^{-1} = (-1)^{\frac{N(\pi)-1}{4}\frac{N(\lambda)-1}{4}}.$$

Met de tussenresultaten die ook bij $\left[\frac{i}{\alpha}\right]$ gebruikt zijn, volgt dan,

$$\begin{aligned}
\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right]^{-1} &= \prod_{k=1}^{m}\left[\frac{\alpha}{\lambda_k}\right]\prod_{j=1}^{n}\left[\frac{\beta}{\pi_j}\right]^{-1} \\
&= \prod_{j=1}^{n}\prod_{k=1}^{m}\left[\frac{\pi_j}{\lambda_k}\right]\left[\frac{\lambda_k}{\pi_j}\right]^{-1} \\
&= \prod_{j=1}^{n}\prod_{k=1}^{m}(-1)^{\frac{N(\pi_j)-1}{4}\frac{N(\lambda_k)-1}{4}} \\
&= (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}} = (-1)^{\frac{1-a}{2}\frac{1-c}{2}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}}.
\end{aligned}$$

Omdat α en β primair zijn, volgt uit lemma 1.11, $a - 1 \equiv b, c - 1 \equiv d \pmod 4$. Daarom geldt ook $(-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}$. □

2 Lemma van Gauss

Een belangrijk stuk gereedschap bij het bestuderen van residu-symbolen is het Lemma van Gauss. In de eerste helft van deze sectie wordt de kwadratische versie van dit lemma geformuleerd. Daarna zal analoog daaraan de kwartische versie geformuleerd worden.

2.1 Kwadratisch

Definitie 2.1. *Zij p een oneven priemgetal en A een verzameling van $\frac{p-1}{2}$ verschillende gehele getallen die niet deelbaar door p zijn. A heet een half-systeem modulo p als elk getal $a \not\equiv 0 \pmod p$ congruent is aan $\pm\alpha$ voor precies één $\alpha \in A$.*

Een voorbeeld van een half-systeem modulo een oneven priemgetal p is $\{1, 2, \ldots, \frac{p-1}{2}\}$. Er bestaat dus altijd een half-systeem.

Lemma 2.2 (Lemma van Gauss)**.** *Zij p een oneven priemgetal en $a \not\equiv 0 \pmod p$. Stel dat A een half-systeem modulo p is. Laat μ het aantal $\alpha \in A$ zijn waarvoor $a\alpha \equiv -\alpha' \pmod p$ voor een $\alpha' \in A$. Dan*

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

Bewijs. Omdat A een half-systeem is, is er voor elke $\alpha \in A$ precies één $\sigma(\alpha) \in A$ zodat $a\alpha \equiv \pm\sigma(\alpha) \pmod p$. Dit definiëert een functie $\sigma : A \to A$. Die functie is injectief, want als $a\alpha \equiv \pm a\alpha' \pmod p$, dan $\alpha \equiv \pm\alpha' \pmod p$ en dus $\alpha = \alpha'$ omdat A een half-systeem is. Dus σ is een permutatie van A en

$$\prod_{\alpha\in A} a\alpha \equiv \prod_{\alpha\in A} \pm\sigma(\alpha) \equiv (-1)^\mu \prod_{\alpha\in A} \sigma(\alpha) \equiv (-1)^\mu \prod_{\alpha\in A} \alpha \pmod p.$$

Door wegdelen van de gemeenschappelijke factoren volgt $a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod p$ □

Met dit lemma kunnen we de tweede supplementaire wet van de kwadratische reciprociteit bewijzen: Voor elk oneven priemgetal p geldt $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.

Bewijs. Kies het half-systeem $A = \{1, 2, \ldots, \frac{p-1}{2}\}$ en pas het lemma van Gauss toe.

$$\begin{aligned}
\mu &= \#\{1 \le n \le \frac{p-1}{2} \mid 2n \textit{ is niet congruent aan een element van } A\} \\
&= \#\{n \mid \frac{p+1}{2} \le 2n \le p-1\} \\
&= \#\{n \mid \frac{p+1}{4} \le n \le \frac{p-1}{2}\}.
\end{aligned}$$

Vervang n door $\frac{p+1}{2} - n$, dan volgt

$$\begin{aligned}
\mu &= \#\{n \mid 1 \le n \le \frac{p+1}{4}\} \\
&= \left\lfloor \frac{p+1}{4} \right\rfloor.
\end{aligned}$$

Nu hoeft alleen nog bewezen te worden dat dit even is, precies als $\frac{p^2-1}{8}$ even is. Dit doen we door onderscheid te maken tussen $p \equiv \pm 1$ en $p \equiv \pm 3$ (modulo 8). Als $p = 8k \pm 1$, dan

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = k(8k \pm 2) = 2k(4k \pm 1)$$

en

$$\mu = \left\lfloor \frac{p+1}{4} \right\rfloor = \left\{ \begin{array}{ll} & \lfloor 2k + \frac{1}{2} \rfloor \\ of & \lfloor 2k \rfloor \end{array} \right\} = 2k,$$

dus dan zijn beide even. Als $p = 8k \pm 3$, dan

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8} = \frac{(8k \pm 4)(8k \pm 2)}{8} = (2k \pm 1)(4k \pm 1)$$

en

$$\mu = \left\lfloor \frac{p+1}{4} \right\rfloor = \left\{ \begin{array}{ll} & \lfloor 2k + 1 \rfloor \\ of & \lfloor 2k - \frac{1}{2} \rfloor \end{array} \right\} = 2k \pm 1,$$

dus dan zijn beide oneven. □

2.2 Kwartisch

Gegeven een primaire irreducibele $\pi \in \mathbb{Z}[i]$.

Definitie 2.3. *Een $\frac{1}{4}$-**systeem** modulo π is een deelverzameling van $\mathbb{Z}[i]$ die precies één representant bevat van elk element van $Q = (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*/\mathbb{Z}[i]^*$ uit lemma 1.16.*

Een $\frac{1}{4}$-systeem modulo π is dus een verzameling A met $(N(\pi)-1)/4$ elementen, zodat voor elke $\alpha \in \mathbb{Z}[i]$ er een uniek paar $\alpha' \in A, u \in \mathbb{Z}[i]^*$ is met $\alpha \equiv u\alpha' \pmod{\pi}$. Voor elke π is bestaat er een $\frac{1}{4}$-systeem modulo π.

Lemma 2.4 (Lemma van Gauss)**.** *Zij $\pi \in \mathbb{Z}[i]$ primair en irreducibel en $\alpha \not\equiv 0 \pmod{\pi}$. Stel dat $\{\alpha_1, \ldots, \alpha_m\}$, met $\alpha_j \neq \alpha_l$ voor $j \neq l$, een $\frac{1}{4}$-systeem modulo π is. Dan is er voor elke j precies één $\sigma(j)$, zodat $\alpha\alpha_j \equiv i^{k(j)}\alpha_{\sigma(j)} \pmod{\pi}$. Laat $\mu = \sum_{j=1}^{m} k(j)$, dan*

$$\left[\frac{\alpha}{\pi}\right] = i^{\mu}.$$

Bewijs. Uit de definitie van een $\frac{1}{4}$-systeem volgt dat er, voor elke j, precies één $\sigma(j)$ is. De functie $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$, die daardoor gedefinieerd wordt, is injectief. Stel namelijk dat $\sigma(j) = \sigma(l)$. Dan is er een k zodat $\alpha\alpha_j \equiv i^k\alpha\alpha_l \pmod{\pi}$. Deel α weg, dan volgt $\alpha_j \equiv i^k\alpha_l \pmod{\pi}$ en, omdat A een $\frac{1}{4}$-systeem is, $\alpha_j = \alpha_l$, dus $j = l$. Dus σ is een permutatie van $\{1, 2, \ldots, m\}$ en

$$\prod_{j=1}^{m} \alpha\alpha_j \equiv \prod_{j=1}^{m} i^{k(j)}\alpha_{\sigma(j)} \equiv i^{\mu} \prod_{j=1}^{m} \alpha_{\sigma(j)} \equiv i^{\mu} \prod_{j=1}^{m} \alpha_j \pmod{\pi}.$$

Door wegdelen van de gemeenschappelijke factoren, volgt $\alpha^{(N(\pi)-1)/4} = \alpha^m \equiv i^{\mu} \pmod{\pi}$. □

In het kwadratische geval was er een eenvoudig bewijs van de tweede supplementaire wet, dat heel direct gebruik maakte van het Lemma van Gauss. Daarbij werd het half-systeem $\{1, \ldots, \frac{p-1}{2}\}$ gebruikt. Zo'n handig $\frac{1}{4}$-systeem hebben we hier niet, dus dat bewijs is niet zomaar om te zetten in een bewijs van de kwartische supplementaire wetten. Die supplementaire wetten zullen daarom pas aan het eind van deze tekst bewezen worden.

3 Analytisch bewijs van de kwadratische reciprociteit

De basis voor dit analytische bewijs van de kwadratische reciprociteit is het volgende gevolg van het Lemma van Gauss.

Lemma 3.1. *Zij p een oneven priemgetal en A een half-systeem modulo p. Stel dat f een $\mathbb{Z}$-periodieke oneven functie is en dat $f(\frac{a}{p}) \neq 0$ als $a \not\equiv 0 \pmod{p}$. Dan geldt voor alle gehele $a \not\equiv 0 \pmod{p}$,*

$$\left(\frac{a}{p}\right) = \prod_{\alpha \in A} \frac{f(\frac{a\alpha}{p})}{f(\frac{\alpha}{p})}.$$

Bewijs. Neem $\alpha \in A$ willekeurig. Kies $\sigma(\alpha) \in A$ zodat $a\alpha \equiv \pm\sigma(\alpha) \pmod{p}$. Dan

$$f(\frac{a\alpha}{p}) = f(\frac{\pm\sigma(\alpha) + kp}{p}) = \pm f(\frac{\sigma(\alpha)}{p}).$$

Omdat σ, net als in het bewijs van het Lemma van Gauss, een permutatie van A is, volgt

$$\prod_{\alpha \in A} f(\frac{a\alpha}{p}) = \prod_{\alpha \in A} \pm f(\frac{\sigma(\alpha)}{p}) = (-1)^{\mu} \prod_{\alpha \in A} f(\frac{\alpha}{p}),$$

waarbij μ is als in het Lemma van Gauss. Deel nu beide zijden door $\prod_{\alpha \in A} f(\frac{\alpha}{p})$ en pas het Lemma van Gauss toe, zodat volgt

$$\prod_{\alpha \in A} \frac{f(\frac{a\alpha}{p})}{f(\frac{\alpha}{p})} = (-1)^{\mu} = \left(\frac{a}{p}\right).$$

□

Zij p een oneven priemgetal en q een oneven getal dat niet deelbaar is door p. Passen we het bovenstaande lemma toe met $f(z) = \sin(2\pi z)$, dan volgt

$$\left(\frac{q}{p}\right) = \prod_{\alpha \in A} \frac{\sin(\frac{2\pi}{p} q\alpha)}{\sin(\frac{2\pi}{p}\alpha)}. \tag{1}$$

Daarom bekijken we $\sin(qz)$.

Lemma 3.2. *Er bestaat een veelterm P van graad $q-1$, met kopcoëfficiënt $(-4)^{(q-1)/2}$, waarvoor*

$$\sin qz = \sin z \cdot P(\sin z).$$

Bewijs.

$$\begin{aligned}
\sin(qz) &= \operatorname{Im}(e^{iqz}) = \operatorname{Im}((\cos z + i \sin z)^q) \\
&= \operatorname{Im}(\sum_{k=0}^{q} \binom{q}{k} \cos^k(z) i^{q-k} \sin^{q-k}(z)) \\
&= \sum_{m=0}^{\frac{q-1}{2}} \binom{q}{2m} \cos^{2m}(z) (-1)^{\frac{q-2m-1}{2}} \sin^{q-2m}(z) \\
&= \sin(z) \sum_{m=0}^{\frac{q-1}{2}} \binom{q}{2m} (1 - \sin^2(z))^m (-1)^{\frac{q-1}{2}-m} \sin^{q-1-2m}(z) \\
&=: \sin(z) P(\sin z).
\end{aligned}$$

Hierin is P een veelterm van graad $\leq q-1$ en de coëfficiënt van X^{q-1} in $P(X)$ is

$$\begin{aligned}\sum_{m=0}^{\frac{q-1}{2}} \binom{q}{2m}(-1)^m(-1)^{\frac{q-1}{2}-m} &= \frac{1}{2}(-1)^{\frac{q-1}{2}}\sum_{m=0}^{q}\binom{q}{m} \\ &= \frac{1}{2}(-1)^{\frac{q-1}{2}}(1+1)^q = (-4)^{\frac{q-1}{2}}.\end{aligned}$$

□

Er is dus een monische veelterm ψ van graad $q-1$ zodat

$$\frac{\sin(qz)}{\sin(z)} = (-4)^{\frac{q-1}{2}}\psi(\sin(z)). \tag{2}$$

Lemma 3.3. *Is B een half-systeem modulo q, dan bestaat $\{\pm\sin(\frac{2\pi}{q}\beta) \mid \beta \in B\}$ uit $q-1$ verschillende nulpunten van de veelterm ψ.*

Bewijs. De verzameling $\{\pm\frac{2\pi}{q}\beta \mid \beta \in B\}$ bestaat uit nulpunten van $\frac{\sin(qz)}{\sin(z)}$, dus $\{\pm\sin(\frac{2\pi}{q}\beta) \mid \beta \in B\}$ bestaat uit nulpunten van ψ. Omdat B een half-systeem is en de sinus 2π-periodiek is, kunnen we B vervangen door $\{1, 2, \ldots, \frac{q-1}{2}\}$. De verzameling $\{\pm\sin(\frac{2\pi}{q}\beta) \mid \beta \in B\}$ is dus gelijk aan

$$\{\pm\sin(\frac{\pi}{q}2b) \mid 1 \leq b \leq \frac{q-1}{4}\} \cup \{\pm\sin(\frac{\pi}{q}2b) \mid \frac{q+1}{4} \leq b \leq \frac{q-1}{2}\}.$$

Vervang nu b door $\frac{q+1}{2} - b$ in de tweede helft. Uit $\sin(z) = \sin(\pi - z)$, volgt $\sin(\frac{\pi}{q}(q+1-2b)) = \sin(\frac{\pi}{q}(2b-1))$. De verzameling is dus gelijk aan

$$\begin{aligned}&\{\pm\sin(\tfrac{\pi}{q}2b) \mid 1 \leq b \leq \tfrac{q-1}{4}\} \\ &\quad \cup \{\pm\sin(\tfrac{\pi}{q}(2b-1)) \mid 1 \leq b \leq \tfrac{2q+2}{4} - \tfrac{q+1}{4} = \tfrac{q+1}{4}\} \\ &= \{\pm\sin(\tfrac{\pi}{q}c) \mid 1 \leq c \leq \tfrac{q-1}{2}\}.\end{aligned}$$

Uit het feit dat de sinusfunctie strikt monotoon stijgt op het interval $[-\frac{1}{2}\pi, \frac{1}{2}\pi]$, volgt dat deze verzameling $q-1$ elementen heeft. □

We kunnen ψ dus schrijven als

$$\psi(X) = \prod_{\beta\in B}\left(X \pm \sin(\frac{2\pi}{q}\beta)\right) = \prod_{\beta\in B}\left(X^2 - \sin^2(\frac{2\pi}{q}\beta)\right).$$

Vullen we $X = \sin z$ in, dan volgt met (2),

$$\frac{\sin(qz)}{\sin(z)} = (-4)^{\frac{q-1}{2}}\prod_{\beta\in B}\left(\sin^2(z) - \sin^2(\frac{2\pi}{q}\beta)\right).$$

Kies daarin $z = \frac{2\pi}{p}\alpha$. Het Legendre-symbool van q modulo p wordt, volgens (1), gegeven door

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{\alpha\in A}\frac{\sin(\frac{2\pi}{p}q\alpha)}{\sin(\frac{2\pi}{p}\alpha)} = \prod_{\alpha\in A}(-4)^{\frac{q-1}{2}}\prod_{\beta\in B}\left(\sin^2(\frac{2\pi}{p}\alpha) - \sin^2(\frac{2\pi}{q}\beta)\right) \\ &= (-4)^{\frac{q-1}{2}\frac{p-1}{2}}\prod_{\alpha\in A}\prod_{\beta\in B}\left(\sin^2(\frac{2\pi}{p}\alpha) - \sin^2(\frac{2\pi}{q}\beta)\right).\end{aligned}$$

Stel nu dat q ook een priemgetal is. Verwisselen van p en q geeft dezelfde uitdrukking voor $(\frac{p}{q})$ op $|A|\cdot|B|$ factoren (-1) na, dus

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

Hiermee is de kwadratische reciprociteitswet bewezen. □

4 Analytisch bewijs van de kwartische reciprociteit

4.1 Gauss

Op dezelfde manier als in het kwadratische geval kunnen we, met behulp van het lemma van Gauss, een analytische uitdrukking voor $\left[\frac{\nu}{\pi}\right]$ maken.

Lemma 4.1. *Is $\pi \in \mathbb{Z}[i]$ primair en is A een $\frac{1}{4}$-systeem modulo π. Stel dat f een $\mathbb{Z}[i]$-periodieke functie is met*

1. $f(iz) = if(z)$,
2. $f(\frac{\alpha}{\pi}) \neq 0$ *voor alle* $\alpha \in \mathbb{Z}[i]$ *met* $\pi \nmid \alpha$.

Dan geldt voor alle $\nu \not\equiv 0 \pmod{\pi}$,

$$\left[\frac{\nu}{\pi}\right] = \prod_{\alpha \in A} \frac{f(\frac{\nu\alpha}{\pi})}{f(\frac{\alpha}{\pi})}.$$

Bewijs. Neem $\alpha \in A$ willekeurig. Kies $\sigma(\alpha) \in A$ zodat $\nu\alpha \equiv i^k\sigma(\alpha) \pmod{p}$. Dan

$$f(\frac{\nu\alpha}{\pi}) = f(\frac{i^k\sigma(\alpha) + \gamma\pi}{\pi}) = i^k f(\frac{\sigma(\alpha)}{\pi}).$$

Omdat σ, net als in het bewijs van het Lemma van Gauss, een permutatie van A is, volgt

$$\prod_{\alpha \in A} f(\frac{\nu\alpha}{\pi}) = \prod_{\alpha \in A} i^k f(\frac{\sigma(\alpha)}{\pi}) = i^\mu \prod_{\alpha \in A} f(\frac{\alpha}{\pi}),$$

waarbij μ is als in het Lemma van Gauss. Deel nu beide zijden door $\prod_{\alpha \in A} f(\frac{\alpha}{\pi})$ en pas het Lemma van Gauss toe, zodat volgt

$$\prod_{\alpha \in A} \frac{f(\frac{\nu\alpha}{\pi})}{f(\frac{\alpha}{\pi})} = i^\mu = \left[\frac{\nu}{\pi}\right].$$

□

Met de juiste functie kan het analytische bewijs uit het vorige hoofdstuk nu omgezet worden in een bewijs voor de kwartische reciprociteit. Om zo'n functie te construeren gebruiken we de theorie van elliptische functies.

4.2 Elliptische functies

4.2.1 Roosters

Definitie 4.2. *Zijn $\omega_1, \omega_2 \in \mathbb{C}$ lineair onafhankelijk over $\mathbb{R}$. Het* ***rooster*** *opgespannen door ω_1, ω_2 is de verzameling van alle complexe getallen van de vorm*

$$m\omega_1 + n\omega_2 \quad met \quad m, n \in \mathbb{Z}.$$

Definitie 4.3. *Is $z_0 \in \mathbb{C}$ en is Λ een rooster, dan heet de verzameling*

$$\mathcal{F} = \{z_0 + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_j < 1\}$$

een ***fundamenteel parallellogram*** *voor het rooster Λ.*

Opmerking 4.4. *Elke $z \in \mathbb{C}$ is congruent modulo Λ aan precies één element van $\mathcal{F}$.*

Bewijs. We bewijzen het eerst voor het fundamentele parallellogram met $z_0 = 0$. Omdat ω_1 en ω_2 lineair onafhankelijk over $\mathbb{R}$ zijn, geldt $\omega_1\mathbb{R} + \omega_2\mathbb{R} \cong \mathbb{R}^2$, dus $\omega_1\mathbb{R} + \omega_2\mathbb{R} = \mathbb{C}$. Daarom zijn er $a, b \in \mathbb{R}$ met $z = a\omega_1 + b\omega_2$. Laat $t_1 = a - \lfloor a \rfloor, t_2 = b - \lfloor b \rfloor$, dan $0 \leq t_j < 1$ en

$$z = a\omega_1 + b\omega_2 \equiv t_1\omega_1 + t_2\omega_2 \pmod{\Lambda}.$$

Stel aan de andere kant dat

$$t_1\omega_1 + t_2\omega_2 \equiv s_1\omega_2 + s_2\omega_2 \pmod{\Lambda} \quad \text{met} \quad 0 \leq t_j, s_j < 1.$$

Er zijn dan $m, n \in \mathbb{Z}$ met $(t_1 - s_1 - m)\omega_1 + (t_2 - s_2 - n)\omega_2 = 0$, maar ω_1 en ω_2 zijn lineair onafhankelijk, dus $t_1 - s_1 = m, t_2 - s_2 = n$. Omdat $|t_j - s_j| < 1$, volgt $t_1 = s_1$, $t_2 = s_2$.

Als $z_0 \neq 0$, dan kan dit bewijs toegepast worden op $z - z_0$. □

De torus $\mathbb{C}/\Lambda$, die ontstaat door punten in $\mathbb{C}$ te identificeren als hun verschil in Λ zit, staat dus in bijectief verband met elk fundamenteel parallellogram. Daarnaast volgt ook dat er in elk fundamenteel parallellogram precies één roosterpunt zit. De roosterpunten zijn namelijk de punten die nul zijn modulo Λ. We kunnen nu het volgende zeggen over de verdeling van de roosterpunten over het vlak.

Lemma 4.5. *Geef met A_n de verzameling $\{z \in \mathbb{C} \mid n - 1 \leq |z| < n\}$ aan. Dan is er een $C > 0$ zodat, voor elke $n \geq 1$, het aantal roosterpunten λ dat in A_n ligt, kleiner is dan Cn.*

Bewijs. Neem $d > 0$ groter dan de diameter van een fundamenteel parallellogram. Bekijk de fundamentele parallellogrammen met roosterpunten als hoekpunten, die A_n snijden. Noem het aantal dergelijke parallellogrammen k_n. Deze parallellogrammen zijn onderling disjunct en elk ervan ligt binnen de verzameling

$$\{z \in \mathbb{C} \mid n - 1 - d \leq |z| \leq n + d\}$$

met oppervlakte hooguit

$$\pi((n+d)^2 - (n-1-d)^2) = an + b \leq C_1 n.$$

Er liggen hoogstens k_n roosterpunten in A_n en $k_n \cdot \text{opp}(\mathcal{F}) \leq C_1 n$. □

Uit dit lemma volgt onmiddellijk dat het aantal roosterpunten in een begrensde verzameling eindig is. Verder kunnen we nu het volgende zeggen over de convergentie van reeksen over Λ.

Lemma 4.6. *Is $q > 2$, dan convergeert de reeks*

$$\sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{|\lambda|^q}.$$

Bewijs.

$$\sum_{\lambda} \frac{1}{|\lambda|^q} = \sum_{n=1}^{\infty} \sum_{\lambda \in A_n} \frac{1}{|\lambda|^q}.$$

Het aantal roosterpunten in A_1 is eindig en

$$\sum_{n=2}^{\infty} \sum_{\lambda \in A_n} \frac{1}{|\lambda|^q} \leq C \sum_{n=2}^{\infty} \frac{n}{(n-1)^q} \leq C \sum_{n=2}^{\infty} \frac{2(n-1)}{(n-1)^q} \leq 2C \sum_{m=1}^{\infty} \frac{1}{m^{q-1}} < \infty.$$

□

4.2.2 Elliptische functies

Definitie 4.7. *Is Λ een rooster. Een **elliptische functie** met betrekking tot Λ is een Λ-periodieke meromorfe functie op $\mathbb{C}$.*

Als f en g elliptische functies zijn, en g is niet de nulfunctie, dan zijn $f+g$, $f-g$, fg, f/g en f' ook meromorf op $\mathbb{C}$ en Λ-periodiek, dus elliptisch.

Lemma 4.8. *Een niet-constante elliptische functie heeft eindig veel nulpunten en polen op $\mathbb{C}/\Lambda$.*

Bewijs. Gegeven een niet-constante elliptische functie f. De verzameling S van polen en nulpunten van f is gesloten en discreet. Beperk S tot de (compacte) afsluiting $\overline{\mathcal{F}}$ van een fundamenteel parallellogram $\mathcal{F}$. De verzameling S is dan compact en discreet, dus eindig. □

Hieruit volgt dat er, door verschuiving, altijd een fundamenteel parallellogram te vinden is dat geen nulpunten of polen van f op zijn rand heeft. Dat maakt het mogelijk om over de rand van $\mathcal{F}$ te integreren. Daarnaast kunnen we nu de volgende definitie geven.

Definitie 4.9. *Is Λ een rooster. Een **deler** is een eindige formele som van elementen van $\mathbb{C}/\Lambda$. Hierbij mogen ook negatieve coëfficiënten voorkomen. In het bijzonder is de deler van een elliptische functie f gedefinieerd als*

$$(f) = \sum_{\alpha \in \mathcal{F}} ord_\alpha f \ (\alpha).$$

Merk op dat voor Λ-elliptische f en g geldt, $(fg) = (f) + (g)$ en $(1/f) = -(f)$.

Definitie 4.10. *Is $D = \sum_{j=1}^{r} n_j(u_j)$ een deler. De **graad** van D wordt gegeven door*

$$\deg D = \sum_{j=1}^{r} n_j.$$

Voor een Λ-elliptische functie f is $\deg(f)$ dus het verschil tussen het aantal nulpunten en het aantal polen op $\mathbb{C}/\Lambda$, beide geteld met multipliciteiten.

Stelling 4.11. *Zijn f en g niet-constante elliptische functies met betrekking tot hetzelfde rooster, dan geldt het volgende.*

1. *Elliptische functies zonder polen zijn constant en als $(f) = (g)$, dan is er een constante $c \in \mathbb{C}$ met $f = c \cdot g$.*
2. *De som van de residuen van f op $\mathbb{C}/\Lambda$ is 0 en f heeft minstens twee polen op $\mathbb{C}/\Lambda$.*
3. *$\deg(f) = 0$. Met andere woorden, f heeft evenveel nulpunten als polen op $\mathbb{C}/\Lambda$ (geteld met multipliciteit).*

Bewijs. 1. Stel dat f een elliptische functie zonder polen is. De functie f is dan holomorf, dus continu, waaruit volgt dat hij begrensd is op de afsluiting van een fundamenteel parallellogram. Uit de periodiciteit van f volgt dan dat f begrensd is op $\mathbb{C}$. De stelling van Liouville ([5] §III.7) zegt dat begrensde geheel holomorfe functies constant zijn, dus f is constant.

Als $(f) = (g)$, dan is de functie f/g een elliptische functie met deler 0. Die functie heeft geen polen en is dus constant.

2. Kies een fundamenteel parallellogram $\mathcal{F}$ dat geen polen van f op zijn rand heeft. De rand van $\mathcal{F}$ bestaat uit de vier zijden van het parallellogram. Door de

periodiciteit is de waarde van f op twee overliggende zijden gelijk. De richting van het pad is op de overliggende zijden tegengesteld, dus de som van de integralen over twee overliggende zijden is nul. Dit geeft

$$\int_{\partial\mathcal{F}} f = 0.$$

De residuenformule ([5], §VI.1) zegt dat de som van de residuen op $\mathcal{F}$ gelijk is aan

$$\frac{1}{2\pi i}\int_{\partial\mathcal{F}} f = 0.$$

Stel dat f een elliptische functie is met hooguit één pool. Als f geen polen heeft, dan is f constant volgens het vorige onderdeel. Neem daarom aan dat f precies één enkelvoudige pool heeft in een punt α Het residu van f in α is dan ongelijk aan nul, maar dat is in tegenspraak met wat hierboven bewezen is.
3. De functie f' is Λ-elliptisch en de logaritmische afgeleide f'/f van f dus ook. Uit ([5],§VI.1) volgt $\mathrm{res}_\alpha f'/f = \mathrm{ord}_\alpha f$, dus dit onderdeel volgt uit het vorige. □

Stelling 4.12. *Is f een elliptische functie met deler $(f) = \sum_{j=1}^r n_j(u_j)$, dan geldt*

$$\sum_{j=1}^r n_j u_j \equiv 0 \pmod{\Lambda}.$$

Bewijs. Uit ([5],§VI.1) volgt

$$\mathrm{res}_\alpha\ z\frac{f'(z)}{f(z)} = \alpha\ \mathrm{res}_\alpha \frac{f'(z)}{f(z)} = \alpha\ \mathrm{ord}_\alpha f,$$

dus

$$\int_{\partial\mathcal{F}} z\frac{f'(z)}{f(z)}dz = 2\pi i \sum_{\alpha\in\mathcal{F}} \mathrm{res}_\alpha z\frac{f'(z)}{f(z)} = 2\pi i\sum_{j=1}^r n_j u_j.$$

Daarom integreren we de functie $zf'(z)/f(z)$ over de rand van $\mathcal{F}$. De integraal over twee overliggende zijden is (mogelijk met een ander teken),

$$\int_{z_0}^{z_0+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{z_0+\omega_2}^{z_0+\omega_2+\omega_1} z\frac{f'(z)}{f(z)}dz.$$

Substitueren van $u = z-\omega_2$ in de tweede integraal en gebruiken van de periodiciteit van f, geeft

$$\int_{z_0}^{z_0+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{z_0}^{z_0+\omega_1} (u+\omega_2)\frac{f'(u)}{f(u)}du = -\omega_2\int_{z_0}^{z_0+\omega_1}\frac{f'(u)}{f(u)}du.$$

Om het lijnstukje tussen z_0 en $z_0+\omega_1$ kunnen we een enkelvoudig samenhangende open verzameling vinden waarop f geen polen en nulpunten heeft. Daarop kunnen we een logaritme L_f van f definiëren door $f'(z)/f(z)$ te integreren (zie [5], §III.6). Er geldt $e^{L_f(z_0+\omega_1)} = f(z_0+\omega_1) = f(z_0) = e^{L_f(z_0)}$, dus

$$\int_{z_0}^{z_0+\omega_1}\frac{f'(u)}{f(u)}du = \omega_2(L_f(z_0+\omega_1) - L_f(z_0)) = \omega_2 2\pi k i$$

voor een geheel getal k. Dit kan herhaald worden voor het andere paar van zijden. □

4.2.3 Weierstrass

Om elliptische functies met gegeven polen en nulpunten te kunnen construeren, willen we holomorfe functies met gegeven nulpunten door elkaar delen. De eerste stap daarin is het maken van een functie die enkelvoudige nulpunten heeft op het rooster Λ. De functie $z\prod_{\lambda\in\Lambda\setminus\{0\}}(1-z/\lambda)$ zou zo'n functie zijn, maar het product convergeert niet. Voor $z>0$, $\Lambda=\mathbb{Z}+\alpha\mathbb{Z}$ heeft het bijvoorbeeld een deelproduct $\prod_{n=1}^{\infty}(1+z/n)\geq 1+\sum_{n=1}^{\infty}z/n=\infty$.

Weierstrass had het idee om elk van de factoren te vermenigvuldigen met een factor zonder nulpunten die het product convergent zou maken. Het resultaat van dat idee is de theorie van Weierstrass producten, waarover meer te lezen is in [5], hoofdstuk XIII. Het product dat wij nodig hebben is de **σ-functie van Weierstrass**,

$$\sigma(z)=z\prod_{\lambda\in\Lambda\setminus\{0\}}\left(1-\frac{z}{\lambda}\right)e^{z/\lambda+\frac{1}{2}(z/\lambda)^2}.$$

Lemma 4.13. *Het bovenstaande product convergeert en definieert een geheel holomorfe functie σ met enkelvoudige nulpunten op het rooster Λ en verder geen nulpunten. De logaritmische afgeleide van σ noemen we de **ζ-functie van Weierstrass** en deze wordt gegeven door de reeks*

$$\zeta(z)=\frac{1}{z}+\sum_{\lambda\in\Lambda\setminus\{0\}}\left(\frac{1}{z-\lambda}+\frac{1}{\lambda}+\frac{z}{\lambda^2}\right).$$

Deze reeks convergeert absoluut uniform op elke compacte verzameling die geen roosterpunten bevat.

Bewijs. Laat $E_n(z)=(1-z)\exp(z+\frac{z^2}{2}+\cdots+\frac{z^{n-1}}{n-1})$. Omdat $\lim_{z\to 0}E_n(z)=1$, is er een omgeving van 0 waarop $|E_n(z)-1|<\frac{1}{2}$. Op het schijfje $B(1,\frac{1}{2})\subset\mathbb{C}$ kunnen we het logaritme definiëren. Ontwikkelen we de machtreeks van het logaritme in 1, dan volgt, voor z in een omgeving van 0,

$$\begin{aligned}\log(E_n(z)) &= \log(1-z)+z+\frac{z^2}{2}+\cdots+\frac{z^{n-1}}{n-1}\\ &= \sum_{k=n}^{\infty}-\frac{z^k}{k}.\end{aligned}$$

De eerste n termen van de machtreeks vallen dus weg. Door ook te eisen dat $|z|<\frac{1}{2}$, kunnen we de volgende afschatting geven.

$$|\log(E_n(z))|\leq\sum_{k=n}^{\infty}\frac{|z|^k}{k}\leq|z|^n\sum_{k=0}^{\infty}|z|^k\leq 2|z|^n.$$

Is n vast, kies dan $M>0$ zodat het bovenstaande geldt voor alle z met $|z|<1/M$. Laat $g_\lambda(z)=E_n(z/\lambda)$. Dat is een geheel holomorfe functie met alleen een enkelvoudig nulpunt in λ. We zijn daarom geïnteresseerd in een product van de vorm $\prod_\lambda g_\lambda(z)$.

Neem $R>0$ willekeurig. We gaan de convergentie van het product bekijken op $B(0,R)$. Voor roosterpunten λ met $|\lambda|>RM$ geldt $|z/\lambda|<1/M$. Voor die λ kunnen we dus de holomorfe functie f_λ op $B(0,R)$ definiëren door $f_\lambda(z)=\log(g_\lambda(z))=\log(E_n(z/\lambda))$. Er geldt

$$|f_\lambda(z)|=|\log(E_n(z/\lambda))|\leq 2|z/\lambda|^n\leq 2R^n\frac{1}{|\lambda|^n}.$$

Bekijk, voor $z \in B(0,R)$, de reeks

$$\sum_{\lambda} f_\lambda(z), \tag{3}$$

waarbij gesommeerd wordt over alle roosterpunten λ met $|\lambda| > RM$. Er geldt,

$$\sum_{\lambda} |f_\lambda(z)| \leq 2R^n \sum_{\lambda} \frac{1}{|\lambda|^n}.$$

Als $n > 2$, dan convergeert deze laatste reeks volgens lemma 4.6. Daarom kiezen we nu $n = 3$. De reeks uit (3) convergeert dan absoluut uniform op $B(0,R)$. Noem de limiet $f(z)$, dan is f een holomorfe functie en $f'(z) = \sum_\lambda f'_\lambda(z)$, waarbij ook de convergentie van deze laatste reeks absoluut uniform is op K (zie [5], §V.1). Omdat f holomorf is op $B(0,R)$, is de functie $e^{f(z)}$ een holomorfe functie zonder nulpunten op $B(0,R)$. Er volgt

$$\begin{aligned}
\sigma(z) &= z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) e^{z/\lambda + \frac{1}{2}(z/\lambda)^2} \\
&= z \prod_{0<|\lambda|\leq RM} g_\lambda(z) \prod_{|\lambda|>RM} g_\lambda(z) \\
&= z \prod_{0<|\lambda|\leq RM} g_\lambda(z) \exp\Big(\sum_{|\lambda|>RM} f_\lambda(z)\Big) \\
&= z \prod_{0<|\lambda|\leq RM} g_\lambda(z) \exp(f(z)).
\end{aligned}$$

Omdat er eindig veel λ zijn met $|\lambda| \leq RM$, definieert dit een holomorfe functie σ op op $B(0,R)$, die alleen enkelvoudige nulpunten in de roosterpunten heeft.

Dit geldt voor alle R, dus σ is een geheel holomorfe functie met enkelvoudige nulpunten in de roosterpunten en verder geen nulpunten. Bovendien geldt voor $z \in B(0,R)$,

$$\begin{aligned}
\frac{\sigma'(z)}{\sigma(z)} &= \frac{1}{z} + \sum_{0<|\lambda|\leq RM} \frac{g'_\lambda(z)}{g_\lambda(z)} + f'(z) \\
&= \frac{1}{z} + \sum_{0<|\lambda|\leq RM} \frac{g'_\lambda(z)}{g_\lambda(z)} + \sum_{|\lambda|>RM} f'_\lambda(z),
\end{aligned} \tag{4}$$

waarbij de laatste som absoluut uniform convergeert. Zij K een compacte deelverzameling van $\mathbb{C}$, die geen roosterpunten bevat. Neem dan R zo dat $K \subset B(0,R)$. De eerste som in (4) is een eindige som van continue functies op K en de tweede som convergeert absoluut uniform op K, dus de hele som convergeert absoluut uniform op K. Omdat $f'_\lambda(z) = g'_\lambda(z)/g_\lambda(z)$, is (4) hetzelfde als

$$\frac{1}{z} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{g'_\lambda(z)}{g_\lambda(z)},$$

waarbij

$$\frac{g'_\lambda(z)}{g_\lambda(z)} = \frac{-1}{\lambda(1 - \frac{z}{\lambda})} + (\frac{1}{\lambda} + \frac{z}{\lambda^2}) = \frac{1}{z-\lambda} + \frac{1}{\lambda} + \frac{z}{\lambda^2}.$$

□

Omdat de reeks voor de ζ-functie absoluut uniform convergeert op compacte deelverzamelingen van $\mathbb{C} \setminus \Lambda$, kunnen we de afgeleide termsgewijs uitrekenen ([5], §V.1). De **$\wp$-functie van Weierstrass** wordt gegeven door,

$$\wp(z) = -\zeta'(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Door weer termsgewijs te differentiëren volgt

$$\wp'(z) = -2\frac{1}{z^3} + \sum_{\lambda \in \Lambda \setminus \{0\}} -2\frac{1}{(z-\lambda)^3} = -2\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}.$$

Daar is direct aan te zien dat $\wp'$ een Λ-periodieke functie is. De functie $\wp(z+\omega_j) - \wp(z)$ heeft dus afgeleide nul voor $j \in \{1,2\}$ en is dus constant. Het punt $\omega_j/2$ is geen roosterpunt, dus $\wp$ is er holomorf. We kunnen dus $\omega_j/2$ invullen om de constante te bepalen. Aan de reeksnotatie is te zien dat $\wp$ een even functie is, dus de constante is $\wp(\omega_j/2) - \wp(-\omega_j/2) = 0$. De Weierstrass $\wp$-functie is dus Λ-periodiek. Het is dus een elliptische functie.

Omdat de $\wp$-functie Λ-periodiek is, weten we dat de afgeleide van de functie $\zeta(z+\lambda) - \zeta(z)$, nul is voor elke $\lambda \in \Lambda$. Daaruit volgt dat er een constante $\eta(\lambda)$ is met $\zeta(z+\lambda) - \zeta(z) = \eta(\lambda)$. Voor deze constante geldt,

$$\begin{aligned}
\eta(\lambda_1 + \lambda_2) &= \zeta(z+\lambda_1+\lambda_2) - \zeta(z) \\
&= \zeta(z+\lambda_1+\lambda_2) - \zeta(z+\lambda_1) + \zeta(z+\lambda_1) - \zeta(z) \\
&= \eta(\lambda_1) + \eta(\lambda_2), \\
\eta(n\lambda) &= \sum_{k=0}^{n-1} \zeta(z+(k+1)\lambda) - \zeta(z+k\lambda) \\
&= n\eta(\lambda),
\end{aligned}$$

dus η is $\mathbb{Z}$-lineair in λ.

Lemma 4.14. *Voor de Weierstrass σ-functie geldt de volgende relatie,*

$$\frac{\sigma(z+\lambda)}{\sigma(z)} = \psi(\lambda) e^{\eta(\lambda)(z+\lambda/2)}$$

waarbij

$$\psi(\lambda) = \begin{cases} 1 & \text{als} \quad \lambda/2 \in \Lambda, \\ -1 & \text{als} \quad \lambda/2 \notin \Lambda. \end{cases}$$

Bewijs. Neem λ vast en laat $f(z) = \sigma(z+\lambda)/\sigma(z)$. Bekijk de logaritmische afgeleide van f,

$$\frac{f'(z)}{f(z)} = \frac{\sigma'(z+\lambda)}{\sigma(z+\lambda)} - \frac{\sigma'(z)}{\sigma(z)} = \zeta(z+\lambda) - \zeta(z) = \eta(\lambda).$$

De functies f en $g(z) = e^{\eta(\lambda)z}$ zijn dus twee meromorfe functies met gelijke logaritmische afgeleide, dus de logaritmische afgeleide van $h = f/g$ is,

$$\frac{h'(z)}{h(z)} = \frac{f'(z)}{f(z)} - \frac{g'(z)}{g(z)} = 0.$$

Daaruit volgt $h'(z) = 0$, dus h is constant, f is een constant veelvoud van g. Er is dus een $\psi(\lambda)$ met

$$\frac{\sigma(z+\lambda)}{\sigma(z)} = \psi(\lambda) e^{\eta(\lambda)(z+\lambda/2)}.$$

Als $\lambda/2 \notin \Lambda$, dan kunnen we $z = -\lambda/2$ kiezen in de vorige vergelijking. Omdat σ oneven is, volgt dan

$$\psi(\lambda) = \sigma(\lambda/2)/\sigma(-\lambda/2) = -1.$$

Als $\lambda/2 \in \Lambda$, dan kan dat niet, omdat $\sigma(-\lambda/2)$ dan nul is. Bekijk

$$\frac{\sigma(z+2\lambda)}{\sigma(z)} = \frac{\sigma(z+2\lambda)}{\sigma(z+\lambda)}\frac{\sigma(z+\lambda)}{\sigma(z)}.$$

Dat geeft

$$\psi(2\lambda)e^{2\eta(\lambda)(z+\lambda)} = \psi(\lambda)e^{\eta(\lambda)(z+\lambda+\lambda/2)}\psi(\lambda)e^{\eta(\lambda)(z+\lambda/2)},$$

dus $\psi(2\lambda) = \psi(\lambda)^2$. Als $\lambda/2 \in \Lambda$, dan geeft dit $\psi(\lambda) = \psi(\lambda/2)^2$. We blijven door twee delen tot we een $\lambda' \in \Lambda$ krijgen met $\lambda'/2 \notin \Lambda$. Dan volgt $\psi(\lambda') = (-1)^2 = 1$, dus $\psi(\lambda) = 1$. □

Voor elke $a \in \mathbb{C}$ hebben we nu

$$\frac{\sigma(z+a+\lambda)}{\sigma(z+a)} = \psi(\lambda)e^{\eta(\lambda)(z+\lambda/2)}e^{\eta(\lambda)a}. \tag{5}$$

Stelling 4.15 (Abel)**.** *Is Λ een rooster. Gegeven $u_1, \ldots, u_r \in \mathbb{C}$ en gehele getallen $n_1, \ldots, n_r$, is er een Λ-elliptische functie met deler $D = \sum_{j=1}^r n_j(u_j)$, dan en slechts dan als*

$$\sum_{j=1}^r n_j = 0 \quad \textit{en} \quad \sum_{j=1}^r n_j u_j \equiv 0 \pmod{\Lambda}. \tag{6}$$

Bewijs. In stellingen 4.11 en 4.12 is bewezen dat de deler van een elliptische functie moet voldoen aan de relaties in (6).

Stel nu dat D een willekeurige deler is die aan deze relaties voldoet. Schrijf $D = \sum_{j=1}^n (a_j) - \sum_{j=1}^n (b_j)$, dan geldt $\sum_{j=1}^n a_j - \sum_{j=1}^n b_j \in \Lambda$. Door a_1 te verschuiven, kunnen we van deze som nul maken en blijft de deler D hetzelfde op $\mathbb{C}/\Lambda$. Laat nu

$$f(z) = \frac{\prod_{j=1}^n \sigma(z-a_j)}{\prod_{j=1}^n \sigma(z-b_j)}$$

De functie f is meromorf en

$$\begin{aligned}
\frac{f(z+\lambda)}{f(z)} &= \prod_{j=1}^n \frac{\sigma(z-a_j+\lambda)}{\sigma(z-a_j)} \prod_{j=1}^n \frac{\sigma(z-b_j)}{\sigma(z-b_j+\lambda)} \\
&= \prod_{j=1}^n \psi(\lambda)e^{\eta(\lambda)(z+\lambda/2)}e^{-\eta(\lambda)a_j} \prod_{j=1}^n \psi(\lambda)^{-1}e^{-\eta(\lambda)(z+\lambda/2)}e^{\eta(\lambda)b_j} \\
&= \exp(\eta(\lambda)(\sum_{j=1}^n b_j - \sum_{j=1}^n a_j)) \\
&= 1
\end{aligned}$$

Daaruit volgt dat f periodiek is met perioderooster Λ. Uit de constructie van f is af te lezen dat f precies deler D heeft. □

4.3 Het bewijs

Met deze laatste stelling kunnen we elliptische functies construeren met gegeven delers. Kies deler $D = (0) + (\frac{1+i}{2}) - (\frac{1}{2}) - (\frac{i}{2})$ voor het rooster $\Lambda = \mathbb{Z} + \mathbb{Z}i$. Er geldt $1+1-1-1 = 0$ en $0 + \frac{1+i}{2} - \frac{1}{2} - \frac{i}{2} = 0$, dus uit de stelling volgt dat er een elliptische functie ϕ is met deler $(\phi) = D$. We hebben nu dus een elliptische functie ϕ met

perioderooster $\mathbb{Z}[i]$, enkelvoudige nulpunten in 0 en $\frac{1+i}{2}$ en enkelvoudige polen in $\frac{1}{2}$ en $\frac{i}{2}$. Door met een constante te vermenigvuldigen, kan deze functie zo gekozen worden dat $\phi(\frac{1+i}{4}) = 1$.

Lemma 4.16. *$\phi(iz) = i\phi(z)$ en $\phi(z)\phi(z - \frac{1}{2}) = i$.*

Bewijs. De functie $\phi(iz)$ heeft dezelfde deler als ϕ, want $i\frac{1+i}{2} \equiv \frac{1+i}{2} \pmod{\Lambda}$, $i\frac{1}{2} = \frac{i}{2}$ en $i\frac{i}{2} \equiv \frac{1}{2} \pmod{\Lambda}$. Volgens stelling 4.11 is er dus een constante $c \in \mathbb{C}$ met $\phi(iz) = c\phi(z)$. Taylorontwikkeling in 0 geeft

$$\phi(z) = \sum_{n\geq 0} a_n z^n, \quad \phi(iz) = \sum_{n\geq 0} a_n i^n z^n.$$

Dus als $a_n \neq 0$, dan $c = i^n$. De functie ϕ heeft een enkelvoudig nulpunt in 0, dus $a_1 \neq 0$, $c = i$.

De deler van $\phi(z - \frac{1}{2})$ is min de deler van ϕ, want $\frac{1+i}{2} + \frac{1}{2} \equiv \frac{i}{2} \pmod{\Lambda}$, $\frac{1}{2} + \frac{1}{2} \equiv 0 \pmod{\Lambda}$, $\frac{i}{2} + \frac{1}{2} = \frac{1+i}{2}$ en $0 + \frac{1}{2} = \frac{1}{2}$. Uit stelling 4.11 volgt dus dat $\phi(z)\phi(z - \frac{1}{2})$ constant is. Vul $z = \frac{1+i}{4}$ in, dan blijkt dat de constante gelijk is aan $\phi(\frac{1+i}{4})\phi(\frac{-1+i}{4}) = i\phi(\frac{1+i}{4})^2 = i$. □

In de deler van ϕ komen alleen termen van de vorm $\frac{\gamma}{2}$ voor, dus als $\frac{\alpha}{\pi}$ een nulpunt of een pool is, dan is er een $\gamma \in \mathbb{Z}[i]$ met $\frac{\alpha}{\pi} = \frac{\gamma}{2}$, oftewel $2\alpha = \pi\gamma$. Als $\pi, \alpha \in \mathbb{Z}[i]$ en π is primair, dan volgt $\pi|\alpha$. De functie ϕ heeft dus geen nulpunten en polen van de vorm $\frac{\alpha}{\pi}$ met π primair en $\pi \nmid \alpha$.

We kunnen ϕ dus gebruiken met lemma 4.1 om de volgende uitdrukking voor $[\frac{\nu}{\pi}]$ te krijgen. Is A een $\frac{1}{4}$-systeem modulo π, dan

$$\left[\frac{\nu}{\pi}\right] = \prod_{\alpha\in A} \frac{\phi(\frac{\nu\alpha}{\pi})}{\phi(\frac{\alpha}{\pi})}. \tag{7}$$

De teller kan verder uitgeschreven worden met de volgende stelling.

Stelling 4.17. *Is $\nu \in \mathbb{Z}[i]$ willekeurig en niet deelbaar door $(1 + i)$ en is R een volledige verzameling representanten van $\mathbb{Z}[i]/\nu\mathbb{Z}[i]$, dan*

$$\phi(\nu z) = \epsilon_\nu \prod_{\alpha\in R} \phi(z - \frac{\alpha}{\nu}), \tag{8}$$

waarbij ϵ_ν een eenheid is met $\epsilon_\nu \equiv \nu \pmod{2 + 2i}$.

Bewijs. De functie $\phi(z - \frac{\alpha}{\nu})$ heeft deler

$$\left(\frac{\alpha}{\nu}\right) + \left(\frac{\alpha}{\nu} + \frac{1+i}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{1}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{i}{2}\right).$$

De deler van de $\mathbb{Z}[i]$-elliptische functie $\chi(z) := \prod_{\alpha\in R} \phi(z - \frac{\alpha}{\nu})$ is dus

$$\sum_{\alpha\in R} (\left(\frac{\alpha}{\nu}\right) + \left(\frac{\alpha}{\nu} + \frac{1+i}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{1}{2}\right) - \left(\frac{\alpha}{\nu} + \frac{i}{2}\right)).$$

De termen in deze deler zijn allemaal verschillend, want als $\frac{\alpha_1}{\nu} + \frac{\gamma_1}{2} \equiv \frac{\alpha_2}{\nu} + \frac{\gamma_2}{2} \pmod{\mathbb{Z}[i]}$, dan $\nu|2(\alpha_1 - \alpha_2) + \nu(\gamma_1 - \gamma_2)$, dus $\nu|(\alpha_1 - \alpha_2)$, dus $\alpha_1 = \alpha_2$. De functie χ heeft dus alleen enkelvoudige polen en nulpunten.

De functie $\psi(z) := \phi(\nu z)$ is ook een $\mathbb{Z}[i]$-elliptische functie, want $\psi(z + \beta) = \phi(\nu z + \nu\beta) = \phi(\nu z) = \psi(z)$ voor $\beta \in \mathbb{Z}[i]$. Deze functie heeft ook alleen enkelvoudige polen en nulpunten. Om te laten zien dat ψ en χ dezelfde deler hebben, hoeven

we dus alleen te laten zien dat ze dezelfde nulpunten en polen hebben. Schrijf $\nu = a + bi$. Omdat $(1+i) \nmid \nu$, geldt $a \not\equiv b \pmod 2$.

Stel dat $z = \frac{\alpha}{\nu} + \gamma$ voor $\gamma \in \{0, \frac{1+i}{2}, \frac{1}{2}, \frac{i}{2}\}$, $\alpha \in R$, dan geldt $\nu z = \alpha + \nu\gamma \equiv \nu\gamma \pmod{\mathbb{Z}[i]}$. Als $\gamma = 0$, dan is het direct duidelijk dat νz een nulpunt van ϕ is, dus dat z een nulpunt van ψ is. Als $\gamma = \frac{1+i}{2}$, dan $\nu\gamma = \frac{a-b}{2} + \frac{a+b}{2}i \equiv \frac{1+i}{2} \pmod{\mathbb{Z}[i]}$, dus ook dan is z een nulpunt van ψ. Als $\gamma = \frac{1}{2}$, dan $\nu\gamma = \frac{a+bi}{2} \equiv \frac{1}{2}$ of $\frac{i}{2} \pmod{\mathbb{Z}[i]}$. Dus als $\gamma = \frac{1}{2}$ of $\frac{i}{2}$, dan is z een pool van ψ. Alle nulpunten van χ zijn dus ook nulpunten van ψ en alle polen van χ zijn ook polen van ψ.

Stel dat z een pool of een nulpunt van ψ is, dan $\nu z \equiv \gamma' \pmod{\mathbb{Z}[i]}$ met $\gamma' = 0$ of $\frac{1+i}{2}$ als het een nulpunt is en $\frac{1}{2}$ of $\frac{i}{2}$ als het een pool is. Zoals in het voorgaande al bewezen is, geldt $\gamma' \equiv \nu\gamma \pmod{\mathbb{Z}[i]}$ voor een γ, waarbij $\gamma \in \{0, \frac{1+i}{2}\}$ als $\gamma' \in \{0, \frac{1+i}{2}\}$ en $\gamma \in \{\frac{1}{2}, \frac{i}{2}\}$ als $\gamma' \in \{\frac{1}{2}, \frac{i}{2}\}$. Daaruit volgt $\nu z \equiv \nu\gamma \pmod{\mathbb{Z}[i]}$, dus er is een $\alpha' \in \mathbb{Z}[i]$ met $z = \gamma + \frac{\alpha'}{\nu}$. Kies $\alpha \in R$ met $\alpha \equiv \alpha' \pmod{\nu}$, dan geldt $z \equiv \frac{\alpha}{\nu} + \gamma \pmod{\mathbb{Z}[i]}$. Dus elk nulpunt van ψ is een nulpunt van χ en elke pool van ψ is een pool van χ.

De functies ψ en χ hebben dus dezelfde deler. Volgens stelling 4.11 verschillen ze daarom met een constante factor. Om deze factor te bepalen vullen we $\gamma = \frac{1+i}{4}$ in. Er geldt $\phi(\gamma) = 1$ en

$$\begin{aligned}
\phi(\gamma + \frac{\alpha}{\nu})\phi(\gamma - \frac{i\alpha}{\nu}) &= -i\phi(\gamma + \frac{\alpha}{\nu})\phi(i\gamma + \frac{\alpha}{\nu}) \\
&= -i\phi(\gamma + \frac{\alpha}{\nu})\phi(\gamma + \frac{\alpha}{\nu} - \frac{1}{2}) \\
&= 1.
\end{aligned}$$

Voor elke $\alpha \in R$ is er ook een $\beta \in R$ met $\beta \equiv i\alpha \pmod{\nu}$, dus we kunnen R opdelen in paren, zodat volgt $\chi(\gamma) = 1$.

Volgens lemma 1.12 is er een unieke eenheid u zodat $u\nu \equiv 1 \pmod{2+2i}$. Laat $\epsilon_\nu = u^{-1}$, dan volgt $\epsilon \equiv \nu \pmod{2+2i}$ en

$$\psi(\gamma) = \phi(\nu\gamma) = \phi(\epsilon_\nu\gamma + (\nu - \epsilon_\nu)\gamma) = \phi(\epsilon_\nu\gamma) = \epsilon_\nu\phi(\gamma) = \epsilon_\nu.$$

□

Is B een $\frac{1}{4}$-systeem modulo ν, dan krijgen we een verzameling representanten van $\mathbb{Z}[i]/\nu\mathbb{Z}[i]$ door elk element van B met elke eenheid te vermenigvuldigen en er de nul bij te doen. De vorige stelling geeft dan

$$\phi(\nu z) = \epsilon_\nu\phi(z) \prod_{\beta\in B}\prod_{k=1}^{4} \phi(z - i^k\frac{\beta}{\nu}).$$

De uitdrukking voor $\left[\frac{\nu}{\pi}\right]$ uit (7) kan nu verder uitgeschreven worden tot

$$\left[\frac{\nu}{\pi}\right] = \prod_{\alpha\in A} \frac{\phi(\frac{\nu\alpha}{\pi})}{\phi(\frac{\alpha}{\pi})} = \prod_{\alpha\in A} \epsilon_\nu \prod_{\beta\in B}\prod_{k=1}^{4} \phi(\frac{\alpha}{\pi} + i^k\frac{\beta}{\nu}).$$

Stel nu dat π en λ willekeurige onderling ondeelbare primaire irreducibelen in $\mathbb{Z}[i]$ zijn. Laat A een $\frac{1}{4}$-systeem modulo π zijn en B een $\frac{1}{4}$-systeem modulo λ. Omdat λ primair is, geldt $\epsilon_\lambda = 1$. De uitdrukking voor het residu-symbool wordt nu

$$\left[\frac{\lambda}{\pi}\right] = \prod_{\alpha\in A}\prod_{\beta\in B} P\left(\frac{\alpha}{\pi}, \frac{\beta}{\lambda}\right), \quad \text{waarbij} \quad P(x,y) = \prod_{k=1}^{4} \phi(x + i^k y).$$

Er geldt ook

$$\begin{aligned} P(x,y) &= \phi(x+y)\phi(x+iy)\phi(x-y)\phi(x-iy) \\ &= \phi(y+x)\phi(i(y-ix))\phi(-(y-x))\phi(-i(y+ix)) \\ &= i(-1)(-i)\phi(y+x)\phi(y-ix)\phi(y-x)\phi(y+ix) \\ &= -P(y,x). \end{aligned}$$

Door π en λ te verwisselen krijgen we er dus $\frac{N(\pi)-1}{4}\frac{N(\lambda)-1}{4}$ factoren (-1) bij, waaruit volgt

$$\left[\frac{\pi}{\lambda}\right] = (-1)^{\frac{N(\pi)-1}{4}\frac{N(\lambda)-1}{4}}\left[\frac{\lambda}{\pi}\right].$$

En dat is precies de kwartische reciprociteitswet. □

5 De supplementaire wetten van de kwartische reciprociteit

5.1 Bewijs

De supplementaire wetten van de kwartische reciprociteit zeggen dat voor primaire $\alpha = a + bi \in \mathbb{Z}[i]$ geldt,

$$\left[\frac{i}{\alpha}\right] = i^{\frac{N(\alpha)-1}{4}} = i^{\frac{1-a}{2}}, \quad \left[\frac{1+i}{\alpha}\right] = i^{\frac{a-b-b^2-1}{4}} \quad en \quad \left[\frac{2}{\alpha}\right] = i^{\frac{-b}{2}}.$$

De eerste supplementaire wet hebben we al bewezen. De tweede bewijzen we eerst voor $\alpha = a \in \mathbb{Z}$ primair. Uit lemma 1.11 volgt dat $a \equiv 1 \pmod 4$ als $a \in \mathbb{Z}$ primair is, dus we willen het volgende bewijzen.

Lemma 5.1. *Voor $a \in \mathbb{Z}$ met $a \equiv 1 \pmod 4$ geldt*

$$\left[\frac{1+i}{a}\right] = i^{\frac{a-1}{4}}.$$

Bewijs. Factoriseer a in priemgetallen tot $a = (-1)^k p_1 \cdots p_r q_1 \cdots q_s$, waarbij $p_j \equiv 1 \pmod 4$ en $q_j \equiv -1 \pmod 4$, dan is $(s+k)$ even, waardoor we a kunnen schrijven als

$$a = p_1 \cdots p_r (-q_1) \cdots (-q_s).$$

Als $a_1 = 4k_1+1, a_2 = 4k_2+1$, dan $a_1 a_2 \equiv 4(k_1+k_2)+1 \pmod{16}$, dus $i^{(a_1-1)/4} i^{(a_2-1)/4} = i^{k_1+k_2} = i^{(a_1 a_2-1)/4}$. Het is dus genoeg om het lemma te bewijzen voor p_j en $-q_j$.

Is q een priemgetal met $q \equiv -1 \pmod 4$, dan is q, volgens lemma 1.9, irreducibel in $\mathbb{Z}[i]$, dus $-q$ is primair en irreducibel. Nu geldt $(1+i)^q \equiv 1 + i^q \equiv 1 + i^{-1} \equiv 1 - i \pmod q$ en dus $(1+i)^{q-1} \equiv \frac{1-i}{1+i} = -i \pmod q$. Daaruit volgt

$$\begin{aligned} \left[\frac{1+i}{-q}\right] &\equiv (1+i)^{\frac{q^2-1}{4}} = ((1+i)^{q-1})^{\frac{q+1}{4}} \\ &\equiv (-i)^{\frac{q+1}{4}} = i^{\frac{-q-1}{4}} \pmod q. \end{aligned}$$

Is p een priemgetal met $p \equiv 1 \pmod 4$, dan is er volgens lemma 1.9 een irreducibele π met $p = \pi\overline{\pi}$. Volgens lemma 1.12 kan deze π primair gekozen worden, zodat volgt

$$\left[\frac{1+i}{p}\right] = \left[\frac{1+i}{\pi}\right]\left[\frac{1+i}{\overline{\pi}}\right].$$

Met lemma 1.20 wordt dit

$$\begin{aligned} \left[\frac{1+i}{p}\right] &= \left[\frac{1+i}{\pi}\right]\left[\frac{1-i}{\pi}\right]^{-1} = \left[\frac{i}{\pi}\right]\left[\frac{1-i}{\pi}\right]\left[\frac{1-i}{\pi}\right]^{-1} \\ &= i^{\frac{N(\pi)-1}{4}} = i^{\frac{p-1}{4}}. \end{aligned}$$

□

Nu gaan we bewijzen dat hieruit de tweede supplementaire wet van de kwartische reciprociteit volgt. Neem een willekeurige primaire $\alpha = a + bi \in \mathbb{Z}[i]$. Laat $\lambda = (1+i)^3 = -2 + 2i$, dan

$$\left[\frac{\lambda}{\alpha}\right] = \left[\frac{1+i}{\alpha}\right]^3 = \left[\frac{1+i}{\alpha}\right]^{-1}.$$

We bekijken daarom $[\frac{\lambda}{\alpha}]$. Er geldt,

$$\left[\frac{\lambda}{\alpha}\right] = \left[\frac{\lambda-\alpha}{\alpha}\right] = \left[\frac{-1}{\alpha}\right]\left[\frac{\alpha-\lambda}{\alpha}\right]$$

en $\alpha - \lambda$ is primair, omdat $\lambda \equiv 0 \pmod{2+2i}$. We kunnen dus de kwartische reciprociteitswet toepassen zodat we krijgen,

$$\left[\frac{\alpha-\lambda}{\alpha}\right] = (-1)^{\frac{a-1}{2}\frac{a-2-1}{2}}\left[\frac{\alpha}{\alpha-\lambda}\right].$$

Omdat $\frac{a-1}{2}$ of $\frac{a-1}{2}-1$ even is en $\alpha \equiv \lambda \pmod{\alpha-\lambda}$, geeft dit

$$\left[\frac{\alpha-\lambda}{\alpha}\right] = \left[\frac{\alpha}{\alpha-\lambda}\right] = \left[\frac{\lambda}{\alpha-\lambda}\right].$$

Uit de eerste supplementaire wet van de kwartische reciprociteit volgt bovendien

$$\left[\frac{-1}{\alpha}\right] = \left[\frac{i}{\alpha}\right]^2 = i^{1-a} = (-1)^{\frac{1-a}{2}}.$$

Nu is $\frac{1-a}{2}$ even precies als $a \equiv 1 \pmod 4$ en volgens lemma 1.11 is dat precies als $b \equiv 0 \pmod 4$, dus precies als $\frac{b}{2}$ even is. Dit geeft

$$\left[\frac{-1}{\alpha}\right] = (-1)^{\frac{b}{2}}.$$

We hebben nu dus

$$\left[\frac{\lambda}{\alpha}\right] = (-1)^{\frac{b}{2}}\left[\frac{\lambda}{\alpha-\lambda}\right].$$

We kunnen α schrijven als $c + d\lambda$ met c en d in $\mathbb{Z}$. Laat namelijk $c = a + b$ en $d = \frac{b}{2}$, dan geldt $c + d\lambda = a + b + \frac{b}{2}(-2+2i) = a + bi$. Met die notatie hebben we de relatie

$$\left[\frac{\lambda}{\alpha}\right] = (-1)^{d}\left[\frac{\lambda}{\alpha-\lambda}\right].$$

Herhaald toepassen van deze relatie geeft

$$\begin{aligned}
\left[\frac{\lambda}{\alpha}\right] &= (-1)^{d}\left[\frac{\lambda}{\alpha-\lambda}\right] = (-1)^{d+(d-1)}\left[\frac{\lambda}{\alpha-2\lambda}\right] \\
&= \cdots = (-1)^{d+(d-1)+\cdots+1}\left[\frac{\lambda}{\alpha-d\lambda}\right] \\
&= (-1)^{\frac{d(d+1)}{2}}\left[\frac{\lambda}{c}\right] \quad \text{als} \quad d > 0, \\
\left[\frac{\lambda}{\alpha}\right] &= (-1)^{(d+1)}\left[\frac{\lambda}{\alpha+\lambda}\right] = (-1)^{(d+1)+(d+2)}\left[\frac{\lambda}{\alpha+2\lambda}\right] \\
&= \cdots = (-1)^{(d+1)+(d+2)+\cdots+0}\left[\frac{\lambda}{\alpha-d\lambda}\right] \\
&= (-1)^{\frac{-d(d+1)}{2}}\left[\frac{\lambda}{c}\right] \quad \text{als} \quad d < 0.
\end{aligned}$$

Er geldt dus

$$\left[\frac{\lambda}{\alpha}\right] = (-1)^{\frac{d(d+1)}{2}}\left[\frac{\lambda}{c}\right].$$

Gebruiken we nu $[\frac{\lambda}{\alpha}] = [\frac{1+i}{\alpha}]^{-1}$, dan krijgen we

$$\begin{aligned}\left[\frac{1+i}{\alpha}\right] &= (-1)^{\frac{-d(d+1)}{2}}\left[\frac{1+i}{c}\right] = i^{-d(d+1)}\left[\frac{1+i}{c}\right] \\ &= i^{\frac{-b^2-2b}{4}} i^{\frac{a+b-1}{4}} = i^{\frac{a-b-b^2-1}{4}}.\end{aligned}$$

En dat is de tweede supplementaire wet van de kwartische reciprociteit.

Voor $[\frac{2}{\alpha}]$ geldt nu

$$\begin{aligned}\left[\frac{2}{\alpha}\right] &= \left[\frac{i}{\alpha}\right]^{-1}\left[\frac{1+i}{\alpha}\right]^2 = i^{\frac{a-1}{2}} i^{\frac{a-b-b^2-1}{2}} \\ &= i^{\frac{-b}{2}+a-1-\frac{b^2}{2}},\end{aligned}$$

dus om de derde supplementaire wet te bewijzen hoeven we alleen nog te laten zien dat $a-1-\frac{b^2}{2} \equiv 0 \pmod 4$. Volgens lemma 1.11 geldt

$$\begin{aligned} & a = 4k+1, \qquad b = 4l \\ \text{of} \quad & a = 4k+3, \qquad b = 4l+2.\end{aligned}$$

In het eerste geval geldt $a-1-\frac{b^2}{2} = 4k-8l^2 \equiv 0 \pmod 4$ en in het tweede geval $a-1-\frac{b^2}{2} = 4k+2-8l^2-8l-2 \equiv 0 \pmod 4$. Hiermee zijn dus alle supplementaire wetten van de kwartische reciprociteit bewezen. □

5.2 Toepassing

We hebben nu genoeg theorie om het vermoeden uit paragraaf 1.2 te bewijzen. Neem een oneven $q \geq 3$ zodat $p = 4q+1$ een priemgetal is en laat $S_q = 2^{2q}+1$, $A_q = 2^q - 2^{\frac{q+1}{2}} + 1$ en $B_q = 2^q + 2^{\frac{q+1}{2}} + 1$. We hadden het vermoeden dat

$$p|A_q \iff \frac{b}{2} \equiv \pm 3 \pmod 8 \quad \text{en} \quad p|B_q \iff \frac{b}{2} \equiv \pm 1 \pmod 8.$$

als we p schrijven als $p = a^2+b^2$ met a oneven en b even.

We weten $p \equiv 5 \pmod 8$ en p is een priemgetal, dus lemma 1.9 zegt dat er een irreducibele π is zodat $p = \pi\overline{\pi}$. Wegens unieke factorisatie is deze π uniek, op complexe conjugatie en vermenigvuldiging met eenheden na. Schrijf $\pi = a+bi$, dan zijn a en b dus uniek op verwisseling en tekens na. Van a en b is er één even en één oneven, want p is oneven. Door te eisen dat b even is, wordt de keuze van a en b uniek, op tekens na, en de tekens van a en b spelen geen rol in het vermoeden.

Er geldt nu $b \equiv 2 \pmod 4$. Stel namelijk dat $b \equiv 0 \pmod 4$, dan $p = a^2+b^2 \equiv a^2 \pmod 8$, maar $p \equiv 5 \pmod 8$ en 5 is geen kwadraat modulo 8. Omdat a oneven is, kunnen we het teken van a zo kiezen dat $a \equiv -1 \pmod 4$. Uit lemma 1.11 volgt dan dat π primair is.

Het volgende lemma zegt dat het voldoende is om A_q en B_q modulo π te bekijken.

Lemma 5.2. *Als $A \equiv 0 \pmod \pi$ in $\mathbb{Z}[i]$ voor een $A \in \mathbb{Z}$, dan geldt $A \equiv 0 \pmod p$ in $\mathbb{Z}$.*

Bewijs. We bewijzen eerst $\gcd(\pi, \overline{\pi}) = 1$. Stel dat π en $\overline{\pi}$ een gemeenschappelijke deler hebben die geen eenheid is. Omdat π irreducibel is, impliceert dit $\pi|\overline{\pi}$, waaruit volgt $\pi|(\pi - \overline{\pi}) = (1+i)^2 b$. Als $\pi|(1+i)$, dan $(1+i)|\pi$, maar dat is in tegenspraak met π primair. Er volgt $\pi|b$ en dat betekent $N(\pi) \leq N(b)$ of $b = 0$. In het eerste geval geldt $a^2+b^2 = N(\pi) \leq N(b) = b^2$, dus $a = 0$ en in het tweede geval hebben we al $b = 0$. Er volgt nu $p = b^2$ of $p = a^2$ en dat is in tegenspraak met p priem.

Stel nu $A \equiv 0 \pmod \pi$ in $\mathbb{Z}[i]$, dan volgt direct door complexe conjugatie, $A \equiv 0 \pmod{\overline{\pi}}$. We hebben dan $\pi|A$, $\overline{\pi}|A$ en $\gcd(\pi, \overline{\pi}) = 1$, dus $p|A$ in $\mathbb{Z}[i]$. Daaruit volgt $p|A$ in $\mathbb{Z}$. □

We gaan nu A_q en B_q bekijken modulo π. Uit de derde supplementaire wet van de kwartische reciprociteit volgt

$$2^q = 2^{\frac{p-1}{4}} \equiv \left[\frac{2}{\pi}\right] = i^{-\frac{b}{2}} \pmod{\pi}.$$

Voor de tweede term, $2^{\frac{q+1}{2}}$ geldt

$$\frac{2^{\frac{q+1}{2}}}{1+i} = \frac{2^{\frac{p+3}{8}}}{1+i} = (-i)^{\frac{p+3}{8}} \frac{(1+i)^{\frac{p+3}{4}}}{1+i} = i^{-\frac{p+3}{8}}(1+i)^{\frac{p-1}{4}}.$$

Met de tweede kwartische supplementaire wet krijgen we

$$(1+i)^{\frac{p-1}{4}} \equiv \left[\frac{1+i}{\pi}\right] = i^{\frac{a-b-b^2-1}{4}} \pmod{\pi}.$$

Schrijven we $a = 4k-1, b = 4l+2$, dan krijgen we

$$\begin{aligned}
-\frac{p+3}{8} &= -\frac{a^2+b^2+3}{8} \\
&= -\frac{16k^2-8k+1+16l^2+16l+4+3}{8} \\
&= -2k^2+k-2l^2-2l-1, \\
\frac{a-b-b^2-1}{4} &= \frac{4k-1-4l-2-16l^2-16l-4-1}{4} \\
&= k-l-4l^2-4l-2 \\
&\equiv k-l-2 \pmod{4}.
\end{aligned}$$

Samen is dit

$$\begin{aligned}
-\frac{p+3}{8} + \frac{a-b-b^2-1}{4} &\equiv -2k^2+k-2l^2-2l-1+k-l-2 \\
&= -2k(k-1)-2l(l+1)-3-l \\
&\equiv 1-l \\
&= \frac{3-(2l+1)}{2} \\
&= \frac{3-\frac{b}{2}}{2} \pmod{4}.
\end{aligned}$$

Dus

$$\frac{2^{\frac{q+1}{2}}}{1+i} \equiv i^{\frac{3-\frac{b}{2}}{2}} \pmod{\pi}.$$

We hebben nu

$$\begin{aligned}
A_q &\equiv i^{-\frac{b}{2}} - (1+i)i^{\frac{3-\frac{b}{2}}{2}} + 1 \pmod{\pi}, \\
B_q &\equiv i^{-\frac{b}{2}} + (1+i)i^{\frac{3-\frac{b}{2}}{2}} + 1 \pmod{\pi}.
\end{aligned}$$

We onderscheiden de volgende gevallen

1. $\frac{b}{2} \equiv 1 \pmod 8$, dan $B_q \equiv i^{-1} + (1+i)i + 1 \equiv 0 \pmod{\pi}$
2. $\frac{b}{2} \equiv 3 \pmod 8$, dan $A_q \equiv i^{-3} - (1+i) + 1 \equiv 0 \pmod{\pi}$
3. $\frac{b}{2} \equiv -3 \pmod 8$, dan $A_q \equiv i^3 - (1+i)i^3 + 1 \equiv 0 \pmod{\pi}$
4. $\frac{b}{2} \equiv -1 \pmod 8$, dan $B_q \equiv i + (1+i)i^2 + 1 \equiv 0 \pmod{\pi}$

Dankzij lemma 5.2 is nu één kant ($\Leftarrow$) van de implicaties in het vermoeden bewezen. Omdat $B_q - A_q = 2 \cdot 2^{\frac{q+1}{2}}$ een tweemacht is, kan p niet tegelijkertijd A_q en B_q delen. Daardoor volgt ook direct de andere kant van de implicaties en is het vermoeden bewezen. $\square$

5.3 Opmerkingen

De reciprociteitswetten zijn ook vanuit computationeel oogpunt erg interessant. In Beukers [1] en [2] staat bijvoorbeeld een algoritme dat kwadratische residu-symbolen uitrekent met behulp van de kwadratische reciprociteitswet.

Meer over reciprociteitswetten kan gevonden worden in Lemmermeyer [7]. Daar zijn bijvoorbeeld algemenere residu-symbolen en reciprociteitswetten te vinden, maar ook meer verschillende bewijzen en veel over de geschiedenis van de reciprociteitswetten.

Over elliptische functies en Weierstrass sommen is meer te vinden in Lang [5].

Referenties

[1] Frits Beukers, *Elementary Number Theory*, Mathematisch Instituut Universiteit Utrecht, 2003

[2] Frits Beukers, *Getaltheorie voor Beginners*, Epsilon Uitgaven, 2000

[3] David A. Cox, *Primes of the Form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, 1989

[4] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, second edition, Springer, 1990

[5] Serge Lang, *Complex Analysis*, fourth edition, Springer, 1999

[6] Serge Lang, *Undergraduate Algebra*, second edition, Springer, 1990

[7] Franz Lemmermeyer, *Reciprocity Laws, From Euler to Eisenstein*, Springer, 2000

Index