On the computation of norm residue symbols

Bouw, J.

Samenvatting

1. Het Legendresymbool

In zijn "Essai sur la théorie des nombres" uit 1798 introduceerde de Franse wiskundige Legendre (1752–1833) het kwadratisch restsymbool dat ook wel Legendresymbool wordt genoemd. Dit symbool wordt voor een priemgetal $p > 2$ en een geheel getal a dat niet deelbaar is door p genoteerd als $(\frac{a}{p})$. Het symbool heeft de waarde 1 wanneer de congruentie $x^2 \equiv a \bmod p$ opgelost kan worden en de waarde -1 wanneer dit niet het geval is. Met het Legendresymbool wordt in feite een functie

$$\{a \in \mathbf{Z} : p \nmid a\} \longrightarrow \{-1, 1\}$$

gegeven die gedefinieerd wordt door

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

Uit de congruentie $a^{p-1} \equiv 1 \bmod p$ volgt, dat

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p$$

dus $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ of $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Leonhard Euler (1707–1783) bewees dat beide definities gelijkwaardig zijn door aan te tonen dat de congruentie $x^2 \equiv a \bmod p$ kan worden opgelost wanneer geldt $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ en dat dit niet het geval is als $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Door zijn compactheid en de mogelijkheid om het op eenvoudige wijze aan te passen om er zo machtsrestsymbolen van hogere orde mee te noteren is het Legendresymbool een succesvolle notatie gebleken die het onderzoek naar de eigenschappen van kwadratische resten zeker heeft gestimuleerd.

We geven een voorbeeld van de berekening van een Legendresymbool. Kies $p = 17$ en bereken de kwadratische resten modulo 17. Dit zijn

$$1^2 \equiv 1 \bmod 17,\ 2^2 \equiv 4 \bmod 17,\ 3^2 \equiv 9 \bmod 17,\ 4^2 \equiv 16 \bmod 17,$$

$$5^2 \equiv 8 \bmod 17,\ 6^2 \equiv 2 \bmod 17,\ 7^2 \equiv 15 \bmod 17,\ 8^2 \equiv 13 \bmod 17.$$

De kwadraten van andere gehele getallen geven geen nieuwe kwadratische resten modulo 17, want er geldt

$$a^2 \equiv (17 - a)^2 \bmod 17$$

zodat $1^2 \equiv 16^2$, $2^2 \equiv 15^2$ enzovoorts. Een kwadratische rest modulo 17 is dus een element van de verzameling

$$R = \{1, 2, 4, 8, 9, 13, 15, 16\}.$$

Omdat 12 geen kwadratische rest is modulo 17, geldt $(\frac{12}{17}) = -1$. De congruentie $x^2 \equiv 12 \bmod 17$ heeft dan ook geen oplossing. Maar $\left(\frac{15}{17}\right) = 1$, want $15 \in R$ en de congruentie $x^2 \equiv 15 \bmod 17$ is oplosbaar. De oplossingen zijn $x \equiv 7 \bmod 17$ en $x \equiv 10 \bmod 17$.

2. Kwadratische reciprociteit

Er bestaat een verband tussen een Legendresymbool en, in zekere zin, het omgekeerde symbool. Dit verband wordt beschreven door de kwadratische reciprociteitswet en luidt als volgt:

als p en q verschillende, oneven priemgetallen zijn, dan geldt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^{-1} = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 4 \text{ of } q \equiv 1 \bmod 4, \\ -1, & \text{als } p \equiv 3 \bmod 4 \text{ en } q \equiv 3 \bmod 4. \end{cases}$$

De kwadratische reciprociteitswet is een opmerkelijk resultaat, omdat het oplossen van kwadratische congruenties modulo een priemgetal p op het eerste gezicht niets te maken heeft met het oplossen van kwadratische congruenties modulo een ander priemgetal q.

De kwadratische reciprociteitswet heeft een tweetal aanvullingswetten:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 4, \\ -1, & \text{als } p \equiv 3 \bmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 8 \text{ of } p \equiv -1 \bmod 8, \\ -1, & \text{als } p \equiv 3 \bmod 8 \text{ of } p \equiv -3 \bmod 8. \end{cases}$$

Legendre slaagde er niet in om een correct bewijs van de kwadratische reciprociteitswet te geven. Het eerste volledige bewijs werd in 1801 gegeven door de Duitse wiskundige Carl Friedrich Gauss (1777–1855), die in de loop der jaren zelfs op zijn minst zes verschillende bewijzen gaf.

De gevalsonderscheidingen modulo 4 en modulo 8 laten de kwadratische reciprociteitswet en zijn aanvullingswetten er niet bijzonder elegant uitzien. We kunnen hier wat aan doen door de invoering van het *Jacobisymbool* en een tweetal *normrestsymbolen*. Deze symbolen zullen ons in staat stellen alle genoemde wetten door een enkele formule uit te drukken. Een extra voordeel is dat deze herformulering ook goed werkt voor de zogenaamde "hogere" reciprociteitswetten uit de algebraïsche getaltheorie.

3. Jacobisymbolen

Voor gehele getallen $a, b \in \mathbf{Z}\backslash\{0\}$ die relatief priem zijn, kan het Jacobisymbool $\left(\frac{a}{b}\right)$ worden gedefinieerd, dat een product is van Legendresymbolen:

$$\left(\frac{a}{b}\right) = \prod_{p \text{ priem},\, p \neq 2,\, p \mid b} \left(\frac{a}{p}\right)^{\operatorname{ord}_p b}$$

waarbij $\operatorname{ord}_p b$ het aantal factoren p in de priemfactorisatie van b aangeeft. Dit symbool moet overigens niet verward worden met het zogenaamde Kroneckersymbool!

Het oorspronkelijke Jacobisymbool was beperkt tot het geval dat b positief en oneven is. In bovenstaande uitbreiding van het Jacobisymbool voor algemene b worden factoren 2 in b bij het product in het rechterlid genegeerd. Het is gebruikelijk om voor de uitgebreide definitie van het Jacobisymbool te kiezen, omdat de reciprociteitswet zich dan eenvoudig laat uitdrukken.

Met het Jacobisymbool kan een belangrijke uitbreiding worden gegeven aan de kwadratische reciprociteitswet en de beide aanvullingswetten. Deze wetten gelden namelijk niet alleen voor Legendresymbolen met oneven priemtallen p en q, maar ook voor Jacobisymbolen als a en b oneven zijn. Er geldt namelijk voor oneven, gehele getallen $a, b \in \mathbf{Z} \setminus \{0\}$ die copriem zijn en waarvoor bovendien geldt dat $a > 0$ of $b > 0$:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \begin{cases} 1, & \text{als } a \equiv 1 \bmod 4 \text{ of } b \equiv 1 \bmod 4, \\ -1, & \text{als } a \equiv 3 \bmod 4 \text{ en } b \equiv 3 \bmod 4. \end{cases}$$

En bovendien, als $b > 0$, dat

$$\left(\frac{-1}{b}\right) = \begin{cases} 1, & \text{als } b \equiv 1 \bmod 4, \\ -1, & \text{als } b \equiv 3 \bmod 4. \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1, & \text{als } b \equiv 1 \bmod 8 \text{ of } b \equiv -1 \bmod 8, \\ -1, & \text{als } b \equiv 3 \bmod 8 \text{ of } b \equiv -3 \bmod 8. \end{cases}$$

We berekenen als voorbeeld het Jacobisymbool $\left(\frac{5}{24}\right)$. Omdat factoren 2 uit de priemfactorontbinding van het getal 24 worden weggelaten, geldt dat $\left(\frac{5}{24}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$, want 2 is geen kwadratische rest modulo 3. Een ander voorbeeld: $\left(\frac{7}{45}\right) = \left(\frac{7}{5}\right)^1 \cdot \left(\frac{7}{3}\right)^2 = \left(\frac{2}{5}\right) = -1$.

4. Normrestsymbolen

We gaan nu voor rationale getallen $a, b \in \mathbf{Q} \setminus \{0\}$ een tweetal normrestsymbolen definiëren, namelijk het symbool $(a, b)_\infty$ en het symbool $(a, b)_2$.

Het eerstgenoemde symbool is bijzonder eenvoudig. Schrijf $H_\infty = \mathbf{Q}_{>0}$, de verzameling van de positieve rationale getallen. Er geldt dat H_∞ een ondergroep is van $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$. De quotiëntgroep $\mathbf{Q}^*/H_\infty$ heeft precies twee elementen want $\mathbf{Q}^*$ is te schrijven als de vereniging van de twee disjuncte nevenklassen H_∞ en $-H_\infty$.

We definiëren nu het normrestsymbool $(a, b)_\infty$ voor $a, b \in \mathbf{Q}^*$ met $a \in (-1)^{a_0} \cdot H_\infty$ en $b \in (-1)^{b_0} \cdot H_\infty$ waarbij $a_0, b_0 \in \{0, 1\}$:

$$(a, b)_\infty = (-1)^{a_0 \cdot b_0}.$$

Kennelijk geldt dat:

$$(a, b)_\infty = \begin{cases} -1, & \text{als } a < 0 \text{ en } b < 0, \\ 1, & \text{anders.} \end{cases}$$

Bovendien is het symbool *bimultiplicatief*. Dit betekent dat

$$(a \cdot a', b)_\infty = (a, b)_\infty \cdot (a', b)_\infty$$

$$(a, b \cdot b')_\infty = (a, b)_\infty \cdot (a, b')_\infty$$

waarbij $a, a', b, b' \in \mathbf{Q}^*$. Ook is eenvoudig in te zien dat het symbool *symmetrisch* is:

$$(a, b)_\infty = (b, a)_\infty.$$

Met de definitie is het niet moeilijk na te gaan dat bijvoorbeeld $(3\frac{1}{2}, -5)_\infty = 1$ en dat $(-2, -\frac{1}{3})_\infty = -1$.

Het tweede normrestsymbool is op analoge wijze gedefinieerd. Dit symbool wordt voor elk tweetal elementen $a, b \in \mathbf{Q}^*$ genoteerd als $(a, b)_2$. De multiplicatieve groep $\mathbf{Q}^*$ heeft $H_2 = \{4^l \cdot \frac{1+8n}{1+8m} : l, m, n \in \mathbf{Z}\}$ als ondergroep. De quotiënt groep $\mathbf{Q}^*/H_2$ heeft precies acht elementen, want $\mathbf{Q}^*$ is te schrijven als vereniging van de disjuncte nevenklassen $(-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3} \cdot H_2$, waarbij $a_i \in \{0, 1\}$ voor $i = 1, 2$ en 3.
Voor $a, b \in \mathbf{Q}^*$ definiëren we nu het normrestsymbool $(a, b)_2$ als volgt:
als $a \in (-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3} \cdot H_2$ en $b \in (-1)^{b_1} \cdot 2^{b_2} \cdot 5^{b_3} \cdot H_2$ dan is

$$(a, b)_2 = (-1)^{a_1 \cdot b_1 + a_2 \cdot b_3 + a_3 \cdot b_2}.$$

Eenvoudig is in te zien dat ook dit symbool symmetrisch en bimultiplicatief is.

We geven enkele voorbeelden. Stel, we willen het normrestsymbool $(29, 14)_2$ berekenen. Er geldt $29 = 5 \cdot \frac{145}{25} \in 5 \cdot H_2$, omdat 145 en 25 elementen van H_2 zijn. Daaruit volgt dat $a_1 = a_2 = 0$ en $a_3 = 1$. Verder hebben we $14 \in -1 \cdot 2 \cdot -7 \in -1 \cdot 2 \cdot H_2$, dus $b_1 = b_2 = 1$ en $b_3 = 0$. Als we de definitie toepassen, volgt dat $(29, 14)_2 = -1$.

5. Normrestsymbolen en de kwadratische reciprociteitswet

We kunnen nu voor coprieme getallen $a, b \in \mathbf{Z} \setminus \{0\}$ de kwadratische reciprociteitswet en de beide aanvullingswetten met één enkele formule weergeven:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = (b, a)_\infty \cdot (b, a)_2.$$

We geven enkele voorbeelden. Neem $a = 29$ en $b = 14$. Er geldt $(29, 14)_\infty = 1$ en $(29, 14)_2 = -1$. Verder is $(\frac{29}{14}) = (\frac{1}{14}) = 1$ en $(\frac{14}{29}) = -1$ want eenvoudig is door berekening na te gaan dat 14 geen kwadratische rest modulo 29 is omdat de kwadratische resten modulo 29 de getallen $1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25$ en 28 zijn. Eenvoudig volgt dan de juistheid van de kwadratische reciprociteitswet in dit geval.

Als voorbeeld controleren we verder nog de tweede aanvullingswet. Stel nu dat voor het oneven priemgetal p geldt dat $p \in (-1)^{b_1} \cdot 2^{b_2} \cdot 5^{b_3} \cdot H_2$, dan onderscheiden we vier verschillende gevallen voor p en berekenen in elk van die gevallen het normrestsymbool $(p, 2)_2$. Dit geeft de onderstaande tabel.

$p \bmod 8$	b_1	b_2	b_3	$(p, 2)_2$
1	0	0	0	1
3	1	0	1	-1
5	0	0	1	-1
7	1	0	0	1.

Het resultaat is als volgt samen te vatten:

$$(p,2)_2 = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 8 \text{ of } p \equiv -1 \bmod 8, \\ -1, & \text{als } p \equiv 3 \bmod 8 \text{ of } p \equiv -3 \bmod 8. \end{cases}$$

Als we nu de kwadratische reciprociteitswet toepassen, dan krijgen we

$$\left(\frac{2}{p}\right)\left(\frac{p}{2}\right)^{-1} = (p,2)_\infty \cdot (p,2)_2.$$

Omdat $\left(\frac{p}{2}\right) = \left(\frac{1}{2}\right) = 1$ en $(p,2)_\infty = 1$ volgt er dat

$$\left(\frac{2}{p}\right) = (p,2)_2.$$

6. Reële en 2-adische getallen

De definitie van $(a,b)_\infty$ die we in paragraaf 4 gegeven hebben, hangt alleen af van het teken van a en b en kan daarom zonder verandering ook voor reële getallen a en b ongelijk nul gegeven worden. De rol van $H_\infty = \mathbf{Q}_{>0}$ wordt dan overgenomen door $\mathbf{R}_{>0}$, die samenvalt met de verzameling kwadraten $(\mathbf{R}^*)^2$ van elementen van $\mathbf{R}^*$.

Merk op dat geldt $H_\infty = \mathbf{Q}^* \cap (\mathbf{R}^*)^2$ en dat de functie

$$\mathbf{R}^* \times \mathbf{R}^* \longrightarrow \{-1,1\}, \quad (a,b) \mapsto (a,b)_\infty$$

in de gebruikelijke topologie continu is.

Wat zojuist is gezegd voor $(a,b)_\infty$, is ook van toepassing op het symbool $(a,b)_2$, wanneer we het lichaam $\mathbf{R}$ vervangen door het lichaam van de 2-*adische getallen*, waarvan we straks de constructie zullen schetsen. Er zal dan blijken dat geldt $H_2 = \mathbf{Q}^* \cap (\mathbf{Q}_2^*)^2$ en dat $(a,b)_2$ ook gedefinieerd kan worden voor $a,b \in \mathbf{Q}_2^*$. De functie

$$\mathbf{Q}_2^* \times \mathbf{Q}_2^* \longrightarrow \{-1,1\}, \quad (a,b) \mapsto (a,b)_2$$

is dan continu in de 2-*adische topologie*.

Het lichaam $\mathbf{Q}_2$ van de 2-adische getallen wordt precies zo geconstrueerd als het lichaam $\mathbf{R}$ van de reële getallen, namelijk door naar Cauchyrijen van rationale getallen te kijken, met als enige verschil dat Cauchyrijen nu gedefinieerd worden ten opzichte van de 2-*adische metriek*, die als volgt wordt verkregen. Definieer

$$|x|_2 = 2^{-k}$$

voor

$$x = 2^k \cdot \frac{1+2l}{1+2m} \in \mathbf{Q}^*$$

met $k,l,m \in \mathbf{Z}$, en $|0|_2 = 0$, dan is de 2-adische afstand van de rationale getallen x en y gelijk aan $|x-y|_2$. In de 2-adische metriek geldt bijvoorbeeld $\lim_{n\to\infty} 2^n = 0$. Het lichaam $\mathbf{Q}_2$ wordt de *completering* van $\mathbf{Q}$ genoemd ten opzichte van de 2-adische metriek.

7. Rekenen met 2-adische getallen

Net zoals men een reëel getal meestal door middel van zijn decimale ontwikkeling representeert, gebruikt men voor een 2-adisch getal a doorgaans een binaire schrijfwijze. Deze ziet er als volgt uit:

$$a = \sum_{n \in \mathbf{Z}} c_n 2^n$$

met alle $c_n \in \{0, 1\}$, zodanig dat er een $m \in \mathbf{Z}$ is met $c_n = 0$ voor alle $n < m$. Omgekeerd definieert elke dergelijke rij $\{c_n\}_{n \in \mathbf{Z}}$ een 2-adisch getal, namelijk de limiet van

$$\sum_{n=m}^{m+h} c_n 2^n$$

voor $h \to \infty$.

Voor $a \in \mathbf{Z}_{\geq 0}$ is dit de gebruikelijke schrijfwijze van a in het tweetallig stelsel, met $c_n = 0$ voor $n < 0$ en ook voor n voldoende groot.

Voor $a = -1 = \lim_{n \to \infty}(2^n - 1)$ krijgen we

$$-1 = 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \ldots$$

en in het algemeen geldt voor $a \in \mathbf{Z}_{<0}$, dat $c_n = 0$ voor $n < 0$ en $c_n = 1$ voor n voldoende groot.

Elementen van $\mathbf{Q}_2$ kunnen worden opgeteld, afgetrokken en vermenigvuldigd op de manier waarop in het tweetallig stelsel wordt gerekend. Als bijvoorbeeld $c = 1 + 2 + 2^3 + 2^4 + 2^6$ en $d = 2 + 2^2 + 2^5 + 2^7$ dan is

$$c + d \equiv 1 \bmod 2^8,$$

$$c \cdot d \equiv 2 \bmod 2^8.$$

Het is ook mogelijk om door elementen van $\mathbf{Q}_2^* = \mathbf{Q}_2 \setminus \{0\}$ te delen. Daarbij kan gebruik gemaakt worden van een alternatieve staartdeling, waarbij 2-adische getallen genoteerd worden als som van machten van twee, waarvan de exponenten van links naar rechts toenemen. Een voorbeeld:

$$\frac{c}{d} = 2^{-1} + 2^2 + 2^3 + 2^5 + 2^6 \bmod 2^7.$$

Rationale getallen zijn ook 2-adische getallen en kunnen dus binair worden geschreven als een som van machten van 2. Dit kunnen er eindig veel zijn, zoals $\frac{3}{4} = 2^{-2} + 2^{-1}$, of oneindig veel, zoals

$$\frac{3}{7} = 1 - \frac{4}{7} = 1 + \frac{4}{1-8} = 1 + 4(1 + 8 + 8^2 + 8^3 + \ldots) = 1 + 2^2 + 2^5 + 2^8 + \ldots.$$

Er kan worden aangetoond dat een element van $\mathbf{Q}_2^*$ een kwadraat is, dan en slechts dan als het van de vorm

$$4^k \cdot (1 + \sum_{l \geq 3} c_l 2^l)$$

is, met $c_l \in \{0, 1\}$ en $k \in \mathbf{Z}$. Uiteraard zijn machten van 4 kwadraten in $\mathbf{Q}_2$, maar ook getallen $x \in \mathbf{Q}_2^*$ waarvoor geldt dat $x \equiv 1 \bmod 8$ zijn kwadraten, en ook producten van beide. Zo is bijvoorbeeld het getal -7 een kwadraat in $\mathbf{Q}_2$, want $-7 \equiv 1 \bmod 8$.

De getallen $\sqrt{-7}$ en $-\sqrt{-7}$ behoren dus tot $\mathbf{Q}_2$. Het oplossen van de congruentie $x^2 \equiv -7 \bmod 2$ geeft $x \equiv 1 \bmod 2$. Vervolgens kan de oplossing verfijnd worden door de congruentie $x^2 \equiv -7$ op te lossen modulo hogere machten van 2. Zo vinden we $\sqrt{-7} \equiv 1+2^2+2^4+2^6+2^7 \bmod 2^8$ en $-\sqrt{-7} \equiv 1+2+2^3+2^5 \bmod 2^8$. Dit voorbeeld illustreert dat $\mathbf{Q}_2$ een ander lichaam is dan het lichaam van de reële getallen.

8. Normrestsymbolen van 2-adische getallen

De definitie van H_2 zoals we die in paragraaf 4 hebben gegeven, lijkt op de definitie van de verzameling $(\mathbf{Q}_2^*)^2$. Het is niet moeilijk om met deze beschrijving van de kwadraten in $\mathbf{Q}_2^*$ aan te tonen dat $H_2 = \mathbf{Q}^* \cap (\mathbf{Q}_2^*)^2$ en dat $\mathbf{Q}^*/H_2$ isomorf is met $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$. Opnieuw bevat elke nevenklasse van $\mathbf{Q}_2^*$ modulo $(\mathbf{Q}_2^*)^2$ precies één element van de vorm

$$(-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3}$$

met alle $a_i \in \{0, 1\}$. De quotiëntgroep $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$ heeft dus acht elementen. Daarmee is duidelijk dat het normrestsymbool $(a, b)_2$ met $a, b \in \mathbf{Q}_2^*$ kan worden gedefinieerd zoals in paragraaf 4 voor elementen van $\mathbf{Q}^*$.

We geven enkele voorbeelden van de berekening van normrestsymbolen in $\mathbf{Q}_2^*$. Voor het normrestsymbool $(a, b)_2$ met

$$a = 1 + 2^2 + 2^3 + 2^4 + \ldots$$

en

$$b = 2 + 2^2 + 2^3 + 2^5 + \ldots$$

geldt dat $a \in 5 \cdot H_2$ en $b \in -1 \cdot 2 \cdot H_2$.

Merk op dat bij de beantwoording van de vraag tot welke nevenklasse de elementen van $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$ in het normrestsymbool behoren, het niet van belang is welke termen met hogere machten van 2 in de representatie van a en b op de plaats van de puntjes staan. Het 2-adische normrestsymbool is dan ook continu in beide argumenten: wanneer a of b wordt vervangen door een 2-adisch getal dat er in de 2-adische metriek dichtbij ligt, verandert de waarde van het symbool niet.

Voor de genoemde elementen a en b geldt dat $(a_1, a_2, a_3) = (0, 0, 1)$ en $(b_1, b_2, b_3) = (1, 1, 0)$. Daaruit volgt, dat $(a, b)_2 = (-1)^{a_1 \cdot b_1 + a_2 \cdot b_3 + a_3 \cdot b_2} = -1$.

Een ander voorbeeld. Als

$$a = 1 + 2 + 2^2 + 2^5 + \ldots$$

en

$$b = 2 + 2^4 + 2^9 + 2^{11} + \ldots$$

dan geldt dat $a \in -1 \cdot H_2$ en $b \in 2 \cdot H_2$. Dus $(a_1, a_2, a_3) = (1, 0, 0)$ en $(b_1, b_2, b_3) = (0, 1, 0)$. Daaruit volgt $(a, b)_2 = 1$.

9. Hogere machtsrestsymbolen

In de eerste paragraaf van deze samenvatting hebben we de oplosbaarheid besproken van de kwadratische congruentie $x^2 \equiv a \bmod p$, waarbij p een oneven priemgetal is en het gehele getal a niet deelbaar is door p. De congruentie is oplosbaar wanneer het Legendresymbool $(\frac{a}{p}) = 1$ en er is geen oplossing wanneer $(\frac{a}{p}) = -1$. De waarde van

het Legendresymbool is dus een oplossing van de vergelijking $x^2 = 1$. Ook kan het m-de machtsrestsymbool gedefinieerd worden, waarbij het gehele getal m groter is dan twee. De uitkomst van het m-de machtsrestsymbool is een oplossing van de vergelijking $x^m = 1$. Deze vergelijking heeft in een geschikt gekozen lichaam m verschillende oplossingen, die m-de eenheidswortels worden genoemd. De m-de eenheidswortels zijn machten van een zogenaamde primitieve m-de eenheidswortel, die we aangeven met het symbool ζ_m. De oplossingen van de vergelijking $x^m = 1$ zijn dus de elementen van

$$\{(\zeta_m)^i : i \in \mathbf{Z}, 0 \leq i \leq m-1\}.$$

Voor $m > 2$ zijn deze oplossingen niet allemaal elementen van $\mathbf{Q}$. Als we m-de machtsrestsymbolen willen definiëren waarbij $m > 2$, dan ligt het voor de hand om te rekenen in een lichaam dat niet alleen de rationale getallen maar ook de m-de eenheidswortels bevat. Zo'n lichaam is het getallenlichaam $\mathbf{Q}(\zeta_m)$.

Als voorbeeld van hogere machtsrestsymbolen kiezen we het vierde machtsrestsymbool, waarbij de vierde eenheidswortels

$$\langle \mathrm{i} \rangle = \{\mathrm{i}^k : k \in \mathbf{Z}, 0 \leq k \leq 3\}$$

de mogelijke uitkomsten zijn.

De getallen die in het vierde machtsrestsymbool voorkomen, zijn getallen uit de zogenaamde ring van gehelen $\mathbf{Z}[\mathrm{i}] = \{a + b \cdot \mathrm{i}; a, b \in \mathbf{Z}\}$ van het lichaam $\mathbf{Q}(\mathrm{i})$. Wanneer $P = (\pi)$ een priemideaal is van de ring $\mathbf{Z}[\mathrm{i}]$, met π een irreducibel element, dan definieert men de norm van P, die genoteerd wordt als $N(P)$, als het aantal elementen van de eindige quotiëntring $\mathbf{Z}[\mathrm{i}]/P$. Er geldt dat $N(P) = \pi \cdot \bar{\pi}$ waarbij $\bar{\pi}$ de geconjugeerde is van π.

Het lichaam waarin we werken is

$$\mathbf{Q}(\mathrm{i}) = \{a + b \cdot \mathrm{i}; a, b \in \mathbf{Q}\}.$$

Het vierde machtsrestsymbool is voor $\alpha \in \mathbf{Z}[\mathrm{i}]$ en een priemideaal $P \neq (1+i)$, waarbij bovendien geldt dat $2 \notin P$ en $\alpha \notin P$, gedefinieerd als de vierde eenheidswortel $\left(\frac{\alpha}{P}\right)_4$, waarvoor geldt

$$\left(\frac{\alpha}{P}\right)_4 \equiv \alpha^{\frac{N(P)-1}{4}} \bmod P.$$

Merk op dat deze definitie veel lijkt op de definitie van kwadratische resten uit het begin van deze samenvatting. Volgens de kleine stelling van Fermat geldt $\alpha^{N(P)-1} \equiv 1 \bmod P$, waaruit volgt voor $\alpha \notin P$ dat

$$\alpha^{N(P)-1} - 1 = \prod_{j=0}^{3} (\alpha^{\frac{N(P)-1}{4}} - \mathrm{i}^j).$$

Voor precies één waarde $j \in \{0, 1, 2, 3\}$ geldt

$$\alpha^{\frac{N(P)-1}{4}} \equiv \mathrm{i}^j \bmod P.$$

We geven een voorbeeld:

$$\left(\frac{1+\mathrm{i}}{3+2\mathrm{i}}\right)_4 \equiv (1+\mathrm{i})^{\frac{13-1}{4}} \bmod (3+2\mathrm{i})$$

want $N(3+2\mathrm{i}) = 3^2 + 2^2 = 13$. Bovendien is $\mathbf{Z}[\mathrm{i}]/(3+2\mathrm{i})$ een eindig lichaam van dertien elementen dat isomorf is met $\mathbf{Z}/13\mathbf{Z}$. Het isomorfisme stuurt $3+2\mathrm{i}$ naar 0, en $2\mathrm{i}$ naar $-3 \equiv 10 \bmod 13$ en dus i naar 5. Daaruit volgt dat 5 een vierde eenheidswortel is in $\mathbf{Z}/13\mathbf{Z}$. Het isomorfisme geeft $\overline{a+b\mathrm{i}} \to a+5b \bmod 13$ en $1+\mathrm{i} \to 6$. Daaruit volgt dat $(1+\mathrm{i})^3 \to 6^3 \equiv 8 \bmod 13$. Omdat $8 \equiv 5^3 \bmod 13$ geldt dat

$$\left(\frac{1+\mathrm{i}}{3+2\mathrm{i}}\right)_4 = \mathrm{i}^3 = -\mathrm{i}.$$

Op een analoge wijze kunnen m-de machtsrestsymbolen worden gedefinieerd voor $m > 2$, waarbij we werken in een getallenlichaam $K \supset \mathbf{Q}(\zeta_m)$.

10. Hogere normrestsymbolen

In de vorige paragraaf gaven we een voorbeeld van een m-de machtsrestsymbool waarbij $m > 2$. Er kan ook een Jacobisymbool voor hogere machtsresten worden gedefinieerd. De analogie met het Legendresymbool beperkt zich niet tot definities, maar geldt ook voor de eigenschappen van hogere machtsrestsymbolen. Zo geldt er een reciprociteitswet die een generalisatie is van de reciprociteitswet van Legendresymbolen.

Voor algemene K en m is, anders dan voor $K = \mathbf{Q}$ en $m = 2$, de reciprociteitswet van de m-de machtsrestsymbolen niet goed te formuleren zonder gebruik te maken van normrestsymbolen. Hogere normrestsymbolen zijn door Hilbert (1862–1943) uitgevonden om er zijn reciprociteitswet voor hogere machtsrestsymbolen mee te kunnen formuleren.

Normrestsymbolen worden gedefinieerd in bepaalde completeringen van een lichaam K, zoals we eerder kwadratische normrestsymbolen definieerden in completeringen van $\mathbf{Q}$ zoals $\mathbf{R}$ en $\mathbf{Q}_2$. Zulke completeringen heten *lokale lichamen* en normrestsymbolen worden dan ook gedefinieerd in lokale lichamen. De introductie van *p-adische lichamen* door Hensel (1861–1941) en de ontwikkeling van de klassenlichamentheorie door o.a. Furtwängler (1869–1940) en Takagi (1875–1960), die de reciprociteitswet voor hogere machtsrestsymbolen bewees, maakte het mogelijk om reciprociteit te formuleren in de terminologie van deze theorie.

Het belangrijkste resultaat van dit proefschrift is een algoritme om in polynomiale tijd normrestsymbolen te berekenen in een lokaal lichaam dat een geschikte eenheidswortel bevat. Het belang van de algoritme is tweeërlei. In de eerste plaats is er een theoretisch belang, namelijk dat het mogelijk is om de waarde van normrestsymbolen uit te rekenen. In de tweede plaats is de algoritme onmisbaar wanneer men de reciprociteitswet van hogere machtsrestsymbolen praktisch wil toepassen voor getallenlichamen. Koen de Boer, promovendus bij het CWI te Amsterdam, gebruikt de algoritme om er hogere machtsrestsymbolen mee te berekenen.

Net als bij berekeningen in de numerieke analyse is er bij alle algoritmen in lokale lichamen steeds weer het probleem van de precisie waarmee moet worden gerekend om een voldoende nauwkeurig en correct resultaat te krijgen. Men kan immers niet rekenen met getallen die gerepresenteerd worden door een som van oneindig veel termen, maar elementen van lokale lichamen worden meestal wel op die manier gegeven.

Een stimulans voor dit onderzoek was een stelling van Moore over zwak continue Steinbergsymbolen uit de K-theorie. Normrestsymbolen zijn dergelijke symbolen en

de waarde van zulke symbolen wordt bepaald door de bimultiplicatieve eigenschap en de eigenschap dat een symbool waarvan beide argumenten som 1 hebben de waarde 1 heeft. Tenslotte is de exacte waarde van het normrestsymbool het resultaat van een normalisatie door toepassing van een stelling uit de klassenlichamentheorie. De eenvoud van deze feiten was een uitdaging om op zoek te gaan naar een algoritme die de exacte waarde van normrestsymbolen berekent in polynomiale tijd.