REPRESENTATIES DOOR KWADRATISCHE VORMEN

ERIK LEPPEN

16 april 2010

Abstract

In deze scriptie wordt op zoek gegaan naar formules voor het aantal representaties van een getal n door een kwadratische vorm Q, als functie van n. Er wordt gekeken welke voorwaarden er aan de kwadratische vorm moeten worden gesteld om het berekenen van zo'n formule mogelijk te maken, en voor een collectie van zulke kwadratische vormen wordt een expliciete formule gegeven. Om dit in algemeenheid te kunnen doen wordt de theorie van modulaire vormen met karakters opgezet. Via formules voor coëfficiënten van Eisensteinreeksen kunnen we de uiteindelijke representatieformules uitdrukken in termen van specifieke delersommen.

Dankwoord

Allereerst wil ik mijn begeleider Frits Beukers bedanken voor zijn hulp en inzichten over het onderwerp, kennis van de literatuur en de feedback op mijn werk, en Gunther Cornelissen als tweede lezer. Daarnaast staat deze scriptie, net als elke andere, niet op zichzelf, maar is deze het eindresultaat van vijf jaar studie. Gedurende deze periode heb ik veel lol gehad gedurende de samenwerking met mijn medestudenten in de Eigenruimte, in het bijzonder Esther Bod, Marte Koning, Willem Maat, Joachim Schipper, Roeland Warringa, Lotte van der Zalm en anderen. Tot slot gaat mijn dank uit naar mijn ouders en broer, vanwege hun interesse in de vordering van mijn werk.

Inhoudsopgave

Hoofdstuk 1

Inleiding

Kwadratische vormen zijn al vanaf de achttiende eeuw bekende wiskundige objecten. Al in het jaar 1632 dat, volgens Ivan Niven, Albert Girard ontdekte dat een priemgetal te schrijven is als de som van twee kwadraten, dan en slechts dan als het een viervoud plus één is. Dit is in 1747 door Euler bewezen. Later, in 1770, wist Lagrange een bewijs te geven gebruikmakende van kwadratische vormen. Ook liet Lagrange zien dat elk getal te schrijven is als de som van vier kwadraten. Jacobi ging verder en liet in 1834 zien op hoeveel manieren dat kon. Dit staat bekend als Jacobi's vierkwadratenstelling. Wij zijn eveneens geïnteresseerd in de vraag naar het *aantal* oplossingen in gehele getallen van een vergelijking van de vorm $Q(\mathbf{x}) = n$, waarbij Q een kwadratische vorm is. We noemen deze aantallen oplossingen *representatieaantallen*. Dit is een functie van n en we gaan op zoek naar een methode om hier een functievoorschrift voor te vinden en de voorwaarden waaronder deze werkt.
Onderzoek naar kwadratische vormen is overigens geenszins "af". Nog in het jaar 1993 is door Conway en Schneeberger een bewijs gevonden voor de zogeheten *15-stelling*, dat in 2000 door Manjul Bhargava is vereenvoudigd en gepresenteerd in [Bha].

1.1 Samenvatting

We zijn dus uit op formules voor de representatieaantallen van kwadratische vormen. Voordat we hiermee aan de slag kunnen, moeten we echter wat voorbereidend werk doen. Om de onderwerpen goed gescheiden te houden is zo veel mogelijk van dit voorbereidende werk in aparte hoofdstukken geplaatst. Hierdoor komen we pas in hoofdstuk 7 aan de kwadratische vormen toe.

We beginnen in hoofdstuk 2 met Dirichletkarakters. Dit is grotendeels elementair en daarom een goed startpunt. In hoofdstuk 3 bekijken we delersommen. We definiëren een begrip dichtheid dat we verderop gaan gebruiken, en we bepalen de dichtheid van enkele delersommen met Dirichletkarakters.

De volgende drie hoofdstukken gaan over modulaire vormen. Hoofdstuk 4 behandelt ze in het algemeen. We beginnen bij congruentiegroepen en definiëren modulaire vormen daarover, en daarna modulaire vormen met Dirichletkarakter. Ook verdelen we

deze objecten onder in Eisensteinreeksen en spitsvormen. Hoofdstukken 5 en 6 behandelen daarna deze twee typen modulaire vormen verder. In hoofdstuk 7 definiëren we de kwadratische vormen en enkele eigenschappen. Hoofdstuk 8 legt het verband tussen kwadratische vormen en modulaire vormen en geeft het laatste stuk gereedschap om de representatieaantallenformules te kunnen geven. Ook zien we de criteria waaraan kwadatische vormen moeten voldoen om het vinden van zo'n representatieaantallenformule mogelijk te maken. De resultaten van de berekeningen staan in tabellen 10.1 en 10.2.

Wat de originele hoofdvraag betreft zijn we er dan in wezen. Maar er is veel meer te zeggen over representatieaantallenformules. Hoofdstuk 9 legt verbanden tussen verschillende kwadratische vormen, waardoor we ook iets kunnen zeggen over verbanden tussen de representatieaantallen. We geven equivalentierelaties op kwadratische vormen die ze indeelt in geslachten en we geven Siegel's massaformule, die iets zegt over de gemiddelde representatieaantallen over geslachten. Ook definiëren we functies δ_p, die we voor het gemak deltafuncties noemen en die terugkomen in Siegel's formule. Naast representatieaantallenformules geven we dan ook voorschriften voor deltafuncties voor enkele kwadratische vormen. De resultaten van die berekeningen staan in 10.4.

1.2 Notaties

Om verwarring te voorkomen, geven we hier de conventies die worden gebruikt. Allereerst is $\mathbb{N} = \{1, 2, 3, \ldots\}$, oftewel $0 \notin \mathbb{N}$, en $\mathbb{N} \cup \{0\}$ noteren we als $\mathbb{N}_0$. Voor complexe getallen z schrijven we $\Re z$ voor het reële deel en $\Im z$ voor het imaginaire deel.

De inclusie $\subset$ van verzamelingen is niet per se strikt: $A \subset B$ omvat ook de situatie dat $A = B$. Voor ondergroepen gebruiken we $<$. We gebruiken het symbool $\varnothing$ voor de lege verzameling. Het verschil van verzamelingen wordt genoteerd met $A \setminus B$. Afsluiting en inwendige van een verzameling X zijn $\overline{X}$ en X° en cardinaliteit is $|X|$.

Voor de eenhedengroep van een ring R schrijven we R^*. De groep van $n \times n$-matrices over R noteren we met $\mathrm{Mat}_{n\times n}(R)$ en de ondergroep van determinant 1-matrices is $\mathrm{Mat}^1_{n\times n}(R)$. De $n \times n$-identiteitsmatrix noteren we met $\mathbb{I}_{n\times n}$, of $\mathbb{I}$ als de dimensie duidelijk is. Getransponeerde vector of matrix is $\mathbf{x}^{\mathrm{t}}$ of A^{t}. Het getal van Euler e en de imaginaire eenheid i schrijven we rechtop om ze te onderscheiden van variabelen e en i.

Voor een natuurlijk getal n schrijven we $\phi(n)$ voor Euler's totiëntfunctie, oftewel voor het aantal restklassen modulo n dat relatief priem is met n. We hanteren de conventie dat $\phi(1) = 1$. Als we spreken over delers van n of erover sommeren, doelen we op positieve delers.

Hoofdstuk 2

Dirichletkarakters

In dit hoofdstuk definiëren we Dirichletkarakters en bekijken we hun eigenschappen. Later gaan we deze nog uitgebreid nodig hebben. We geven de definitie van het Dirichletkarakter modulo een gegeven natuurlijk getal M. Daarna bekijken we primitieve voortbrengers modulo M om te kijken hoe we Dirichletkarakters eenvoudig kunnen weergeven. We geven het bekendste voorbeeld, het Kroneckersymbool, en we eindigen met Gausssommen en Dirichlet L-functies.

2.1 Definities

We geven hier de basisdefinities van Dirichletkarakters, waaronder modulus, conductor, orde, en geven aan wat primitieve karakters zijn.

Dirichletkarakters

We beginnen met de definitie zelf.

Definitie 2.1.1 (Dirichletkarakter)**.** Een *Dirichletkarakter van modulus* M is een periodieke multiplicatieve afbeelding $\chi : \mathbb{Z} \to \mathbb{C}$ met periode M zodanig dat $|\chi(a)| = 1$ als $\text{ggd}(a, M) = 1$ en $\chi(a) = 0$ als $\text{ggd}(a, M) > 1$.

Periodiciteit wil zeggen dat $\forall a \in \mathbb{Z}$: $\chi(a + M) = \chi(a)$ en multiplicativiteit betekent dat $\forall a, b \in \mathbb{Z}$: $\chi(ab) = \chi(a)\chi(b)$. Uiteraard volgt hieruit dat $\chi(1) = 1$. We weten dankzij Euler dat voor alle $a \in \mathbb{Z}$ relatief priem met M geldt dat $a^{\phi(M)} \equiv 1 \pmod{M}$, en derhalve dat voor zulke a ook $\chi(a)^{\phi(M)} = 1$. Oftewel, $\chi(a)$ is een macht van $\zeta_{\phi(M)}$. Voor een $a \in \mathbb{Z}$ relatief priem met M, definieer t_a als de *orde* van $\chi(a)$; oftewel de kleinste t met de eigenschap $\chi(a)^t = 1$. Dan zijn alle t_a dus delers van $\phi(M)$, en het kleinte gemeenschappelijke veelvoud van alle t_a dus ook. Dit kleinste gemeenschappelijke veelvoud noemen we de *orde* van χ.
Als de orde 1 of 2 is, dan is χ een *reëel karakter*. Als de orde 1 is, dan is χ het *triviale karakter* van modulus M en dit noteren we vaak simpelweg met 1. Merk op dat het triviale karakter modulo M wordt gegeven door het voorschrift $\chi(a) = 1$ als $\text{ggd}\,(a, M) = 1$, 0 anders (dus eigenlijk als de indicatorfunctie $\mathbf{1}_{\text{ggd}\,(a,M)=1}$). Dit voorschrift hangt alleen af van de priemfactoren in M, oftewel alleen van de *radicaal* $R(M)$ van M, dat gedefinieerd is als het product van de priemdelers van M, oftewel de grootste kwadraatvrije deler van M.

Opmerking 2.1.2. Dirichletkarakters kun je zien als een speciaal geval van groepskarakters. Een *karakter* van een groep G is een homomorfisme van G naar $\mathbb{C}\setminus\{0\}$. Dirichletkarakters modulo M zijn dus karakters van de groep $G = (\mathbb{Z}/M\mathbb{Z})^*$, uitgebreid tot heel $\mathbb{Z}$ door ze periodiek te maken en elementen buiten $(\mathbb{Z}/M\mathbb{Z})^*$ op nul af te beelden.

Als χ en ψ twee Dirichletkarakters van dezelfde modulus M zijn, dan is $\chi \cdot \psi : a \mapsto \chi(a)\psi(a)$ eveneens een Dirichletkarakter. Uiteraard geldt $\chi \cdot 1 = \chi = 1 \cdot \chi$. Als χ en ψ twee Dirichletkarakters modulo respectievelijk M en N zijn, dan induceren ze beide een Dirichletkarakter modulo $L = \text{kgv}\, M, N$ en is hun product $\chi \cdot \psi$ een Dirichletkarakter modulo L. Gegeven een Dirichletkarakter χ mod M, kunnen we het karakter $\psi = \overline{\chi}$ definiëren als $a \mapsto \overline{\chi(a)}$. Voor alle $a \in \mathbb{Z}$ relatief priem met M geldt dan dat $\chi(a)\overline{\chi}(a) = |\chi(a)| = 1$, dus $\chi \cdot \overline{\chi} = 1$. We noteren $\overline{\chi}$ daarom ook wel met $1/\chi$. De conclusie is

Propositie 2.1.3. *De verzameling van Dirichletkarakters modulo M is een groep met het triviale karakter 1 als eenheidselement. Deze groep noteren we met $\mathscr{D}(M)$.*

Primitieve karakters

Een Dirichletkarakter χ van modulus M geeft automatisch aanleiding tot (*induceert*) een karakter χ' van modulus cM, voor alle $c \in \mathbb{Z}$, via het voorschrift $\chi'(a) = \chi(a)$ als $\text{ggd}(a, cM) = 1$; 0 anders. Dit inductieproces is transitief: als χ aanleiding geeft tot ψ en ψ tot ω, dan induceert χ eveneens ω.

Voor veel karakters χ bestaat er dus een karakter ψ van lagere modulus dat χ induceert. Dirichletkarakters die niet geïnduceerd worden door karakters van lagere moduli, hebben zogezegd een "minimale" modulus en noemen we *primitief*. Maar ook voor karakters χ die niet primitief zijn is een "minimale" waarde van de modulus aan te geven, dit is de kleinste modulus van een karakter dat χ induceert en deze modulus noemen we de *conductor* van χ. Deze is als volgt gedefinieerd.

Definitie 2.1.4 (Conductor)**.** Voor een karakter χ van modulus M, definieer $\mathscr{M}_\chi$ als de verzameling van alle $m \in \mathbb{N}$ met de volgende eigenschap:

$$(\text{ggd}(n, M) = 1 \text{ en } n \equiv 1 \pmod{m}) \Longrightarrow \chi(n) = 1. \tag{2.1}$$

De *conductor* van χ, genoteerd als f_χ, definiëren we als het kleinste element van $\mathscr{M}_\chi$.

Deze definitie komt overeen met die van Toshitsune Miyake in [Miy].

Opmerking 2.1.5. Andere notaties die je wel ziet voor de conductor van χ zijn m_χ of $\text{cond}(\chi)$.

Voor de verzameling $\mathscr{M}_\chi$ uit definitie 2.1.4 is duidelijk dat $M \in \mathscr{M}_\chi$ en dus weten we dat $\mathscr{M}_\chi \neq \varnothing$ en dat het kleinste element van $\mathscr{M}_\chi$ niet groter is dan M. Bovendien, als $m_1, m_2 \in \mathscr{M}_\chi$, dan zit ook $\text{ggd}\, m_1, m_2 \in \mathscr{M}_\chi$, dus het kleinste element van $\mathscr{M}_\chi$ is een deler van alle andere. We concluderen:

Propositie 2.1.6. *De conductor f_χ van een karakter χ is een deler van zijn modulus*

M.

Opmerking 2.1.7. Het enige karakter mod M met conductor 1 is het triviale karakter mod M.

We kunnen nu zeggen wat het betekent als een Dirichletkarakter primitief is.

Definitie 2.1.8 (Primitief karakter)**.** Een Dirichletkarakter χ van modulus M heet *primitief* als $f_\chi = M$.

Gegeven een $\chi \in \mathscr{D}(M)$ kunnen we een primitief karakter modulo f_χ vinden dat χ induceert, oftewel het "kleinste" Dirichletkarakter dat χ induceert, dat zelf niet geïnduceerd wordt door iets nog kleiners. We definiëren dit karakter als volgt.

Definitie 2.1.9 (Primitief karakter geassocieerd met χ)**.** Zij χ een Dirichletkarakter met modulus M en conductor $f = f_\chi$. Het *primitieve karakter geassocieerd met* χ, genoteerd χ^0, is gedefinieerd als het karakter χ^0 modulo f gegeven door het volgende voorschrift. Als $\gcd a, f = 1$, kies een a' met $\gcd a', M = 1$ en $a' \equiv a \pmod f$, en laat $\chi^0(a) = \chi(a')$. Als $\gcd a, f > 1$, laat $\chi^0(a) = 0$.

Uit deze definitie volgt dat als χ zelf primitief is, dan is $\chi^0 = \chi$.

2.2 Primitieve voortbrengers mod M

We kunnen een Dirichletkarakter uitdrukken aan de hand van een functievoorschrift, maar ook aan de hand van zijn functiewaarden. Omdat Dirichletkarakters multiplicatief zijn, is zodra de waarden in a en b bekend zijn, de waarde in ab automatisch ook bekend. Als we ook de modulus kennen, kunnen we uit alleen $\chi(a)$ en $\chi(b)$ een grote hoeveelheid andere functiewaarden ook vinden, doordat alle mogelijke woorden in $\{a, b\}$ een heleboel restklassen modulo M kunnen opleveren. In feite kunnen we de waarde van χ in ieder woord in $\{a, b\}$ vinden als we $\chi(a)$ en $\chi(b)$ kennen. Hierbij definiëren we een *woord* in een alfabet S als een eindige samensteling van elementen uit S, zo is $a^3b^2a^{-1}$ een voorbeeld van een woord in $\{a, b\}$. Dus als $\chi(a)$ en $\chi(b)$ bekend zijn, dan is $\chi(a^3b^2a^{-1}) = \chi(a)^3\chi(b)^2\overline{\chi(a)}$ dat ook.

Deze observatie leidt tot de vraag of we een minimale verzameling van restklassen g_i modulo M kunnen geven zodanig dat elk karakter χ mod M waarvan we alle $\chi(g_i)$ kennen, geheel vast ligt. Dit is inderdaad mogelijk en we geven hier het antwoord op deze vraag.

Voor oneven priemmachten $M = p^r$ en voor $M = 2, 4$ geeft het volgende lemma dat één functiewaarde genoeg is.

Lemma 2.2.1. *Voor $M = p^r$ een oneven priemmacht en voor $M = 2, 4$ is $(\mathbb{Z}/M\mathbb{Z})^*$ cyclisch.*

Bewijs. Zie [Beu, Stelling 7.4.1] □

Definitie 2.2.2 (Primitieve wortel)**.** Een voortbrenger g van $(\mathbb{Z}/p^r\mathbb{Z})^*$ noemen we een *primitieve wortel* modulo p^r.

Equivalent met deze definitie is het feit dat als g een primitieve wortel modulo p^r is, de machten van g

$$1, g, g^2, g^3, \ldots, g^{\phi(p^r)-1}$$

alle restklassen modulo p^r precies éénmaal aandoen. Tevens is de orde van de primitieve wortel $g \bmod p^r$ uiteraard precies gelijk aan $\phi(p^r)$. Ondanks dat primitieve wortels modulo elk oneven priemgetal bestaan, is er geen algoritme bekend om deze snel te vinden. Men zal achtereenvolgens de kwadraatvrije getallen $2, 3, 5, 6, \ldots$ moeten proberen. Gelukkig zegt een heuristisch argument dat je meestal vrij snel een primitieve wortel te pakken hebt.

Er is een eenvoudig criterium om te testen of een getal een primitieve wortel is.

Lemma 2.2.3. *Een getal g is een primitieve wortel modulo p^r, dan en slechts dan als voor elke priemdeler ℓ van $p(p-1)$ geldt dat*

$$g^{p^{r-1}(p-1)/\ell} \not\equiv 1 \pmod{p}.$$

Bewijs. Schrijf voor het gemak $n = \phi(p^r) = p^{r-1}(p-1)$. Merk op dat $p(p-1)$ dezelfde priemdelers heeft als n. Als er een priemdeler ℓ van n bestaat waarvoor $g^{n/\ell} = 1 \pmod{p}$, dan is g geen primitieve wortel modulo p^r. Andersom, als g geen primitieve wortel is, dan moet $g^d \equiv 1$ voor een echte deler $d \mid n$. Omdat voor elke deler d van een getal n er een priemfactor van n bestaat dat in d tot een kleinere exponent voorkomt dan in n zelf, is elke deler d van n een deler van n/ℓ voor een zekere priemfactor $\ell \mid n$. Als $g^d = 1$, dan moet voor die ℓ, ook $g^{n/\ell} = 1$. □

Voorbeeld 2.2.4. Neem $p = 7$. De priemdelers van $p-1$ zijn 2 en 3. Probeer $g = 2$. Omdat $2^3 \equiv 1$, is 2 geen primitieve wortel. Omdat $3^2 \equiv 2 \not\equiv 1$ en $3^3 \equiv 6 \not\equiv 1$, is 3 wel een primitieve wortel.

Voor de even priemmachten vanaf 2^3 is de structuur van $\mathbb{Z}/2^r\mathbb{Z}$ eveneens bekend.

Lemma 2.2.5. *Voor $p = 2$ en $r \geq 3$ is $(\mathbb{Z}/p^r\mathbb{Z})^*$ het product van twee cyclische groepen, voortgebracht door 5 en -1.*

Voor moduli M met meerdere priemfactoren bestaat de ontbinding

$$(\mathbb{Z}/M\mathbb{Z})^* = (\mathbb{Z}/2^{r_2}\mathbb{Z})^* \times (\mathbb{Z}/3^{r_3}\mathbb{Z})^* \times (\mathbb{Z}/5^{r_5}\mathbb{Z})^* \times \ldots, \tag{2.2}$$

waarbij $M = 2^{r_2}3^{r_3}5^{r_5}\cdots$.

Voor alle $M \in \mathbb{N}$ kunnen we dus een verzameling voortbrengers voor $(\mathbb{Z}/M\mathbb{Z})^*$ geven. Hiertoe gebruiken we ontbinding (2.2) en voor elke factor $(\mathbb{Z}/p^{r_p}\mathbb{Z})^*$ nemen we de kleinste primitieve wortel modulo p^{r_p}, of de twee voortbrengers 5 en -1 voor het

geval $r_2 \geq 3$. Daarna "liften" we elke primitieve voortbrenger g modulo p^r naar dat getal modulo M dat modulo p^r gelijk is aan g, en modulo de andere priemmachten in M tot 1 reduceert. De Chinese reststelling zegt dat dit altijd een unieke restklasse modulo M oplevert. Dat deze methode het juiste element oplevert, is te zien in de uitdrukking (2.2): de voortbrenger van bijvoorbeeld $(\mathbb{Z}/3^{r_3}\mathbb{Z})^*$ wordt dat element van $(\mathbb{Z}/M\mathbb{Z})^*$ dat $(\mathbb{Z}/3^{r_3}\mathbb{Z})^*$ in zijn geheel voortbrengt en triviaal is op de andere factoren. De ordes van de voortbrengers veranderen daarmee niet. Voor $p = 2$ moet iets anders gehandeld worden. Dit omdat er voor $p = 2$ twee voortbrengers zijn als $8 \mid M$, namelijk -1 en 5. Deze voortbrengers worden dan ook gelift naar *twee* restklassen modulo M, namelijk naar de getallen die -1 respectievelijk 5 geven modulo 2^{r_2} en 1 modulo alle andere priemmachten in M. Ook dit geeft twee unieke restklassen modulo M. Tot slot laten we doorgaans de toevoeging "mod M" weg en laten we de primitieve voortbrengers de kleinste positieve representanten van deze klassen in $\mathbb{Z}$ zijn. We kunnen het geheel samenvatten in het volgende algoritme.

Algoritme 2.2.6 (Primitieve voortbrengers modulo N)**.**

(i) Ontbind N in zijn priemfactoren $N = p_1^{r_1} \dots p_t^{r_t}$.

(ii) Bepaal voor iedere factor $p_j^{r_j}$ een primitieve wortel g_j, of in het geval van $p_1 = 2, r_1 \geq 3$, twee voortbrengers g_0 en g_1. Het aantal voortbrengers is dus $t + 1$ als $8 \mid N$ en t anders.

(iii) Met behulp van de Chinese reststelling, "lift" elke voortbrenger g_j over p_j naar die restklasse modulo N die modulo p_j reduceert tot g_j en modulo alle andere priemgetallen reduceert tot 1. Als $8 \mid N$, moet voor $p_1 = 2$ ook g_0 op die manier gelift worden.

(iv) Geef uitvoer $(g_1, \dots, g_t)$, of $(g_0, \dots, g_t)$ als $8 \mid N$.

Voorbeeld 2.2.7. Zij $M = 112 = 2^4 \cdot 7$. Dan is

$$(\mathbb{Z}/112\mathbb{Z})^* = (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*.$$

Omdat $r_2 = 4 \geq 3$, zijn er twee voortbrengers voor $(\mathbb{Z}/16\mathbb{Z})^*$, namelijk $-1 \equiv 15$ en 5. Modulo 7 is er een primitieve wortel, voorbeeld 2.2.4 laat zien dat dat 3 is. De primitieve voortbrengers van $(\mathbb{Z}/112\mathbb{Z})^*$ zijn die drie getallen g_1, g_2 en g_3 waarvoor

$$g_1 \equiv -1 \pmod{16}, \qquad g_1 \equiv 1 \pmod{7}, \tag{2.3}$$
$$g_2 \equiv 5 \pmod{16}, \qquad g_1 \equiv 1 \pmod{7}, \tag{2.4}$$
$$g_3 \equiv 1 \pmod{16}, \qquad g_1 \equiv 3 \pmod{7}, \tag{2.5}$$

en dit geeft de getallen

$$g_1 = 15, \qquad g_2 = 85, \qquad g_3 = 17.$$

Stel nu dat van een Dirichletkarakter χ modulo M de functiewaarden in de primitieve voortbrengers modulo M bekend zijn. Omdat elke inverteerbare restklasse a mod M een woord in deze voortbrengers is, is $\chi(a)$ uit te drukken in de χ-beelden op deze voortbrengers. Oftewel, χ ligt hiermee volledig vast. Omdat we de primitieve voortbrengers modulo M eenduidig vast hebben gelegd (daarom hebben we gekozen om specifiek

de *kleinste* primitieve wortels te nemen), kunnen we een Dirichletkarakter modulo M beschrijven aan de hand van zijn waarden in de primitieve voortbrengers g_i; we noteren χ modulo M als rijtje

$$(\chi(g_1), \chi(g_2), \ldots, \chi(g_n)) \,. \tag{2.6}$$

Daarnaast geldt voor elke primitieve voortbrenger g_i dat de mogelijke waarden voor $\chi(g_i)$ precies de machten zijn van ζ_s, waarbij s de orde van g_i in $(\mathbb{Z}/M\mathbb{Z})^*$ is, oftewel $\phi(p^r)$.

Twee Dirichletkarakters zijn gelijk dan en slechts dan als hun rijtjes (2.6) van beelden op de g_i overeenkomen. Elk rijtje geeft dus een ander Dirichletkarakter en door alle combinaties van machten van ζ_{s_i} te kiezen met s_i de orde van g_i, worden alle Dirichletkarakters precies éénmaal bereikt. We krijgen

Propositie 2.2.8. *De groep $\mathscr{D}(M)$ van Dirichletkarakters modulo M is isomorf met $(\mathbb{Z}/M\mathbb{Z})^*$ via het isomorfisme*

$$g_0^{r_0} g_1^{r_1} \ldots g_n^{r_n} \in (\mathbb{Z}/M\mathbb{Z})^* \longmapsto \left(\zeta_{s_0}^{r_0}, \zeta_{s_1}^{r_1}, \ldots, \zeta_{s_1}^{r_1}\right),$$

waarbij s_i de orde van g_i in $(\mathbb{Z}/M\mathbb{Z})^*$ is.

Gevolg 2.2.9. *De orde van de groep $\mathscr{D}(M)$ is $\phi(M)$.*

De reële karakters komen overeen met de rijtjes

$$(\pm 1, \pm 1, \ldots, \pm 1)$$

en het rijtje $(1, 1, \ldots, 1)$ geeft het triviale karakter mod M.

Voorbeeld

Kies $M = 153 = 3^2 \cdot 17$. De primitieve voortbrenger modulo 9 is 2 en die modulo 17 is 3. De primitieve voortbrengers g_0 en g_1 van $(\mathbb{Z}/153\mathbb{Z})^*$ zijn dus die getallen g_0 en g_1 modulo 153 waarvoor geldt

$$\begin{aligned} g_0 &\equiv 2 \pmod 9, \quad g_0 \equiv 1 \pmod{17}; \\ g_1 &\equiv 1 \pmod 9, \quad g_1 \equiv 3 \pmod{17}. \end{aligned}$$

Dit geeft $g_0 = 137, g_1 = 37$. Een Dirichletkarakter χ mod 153 ligt dus vast als $\chi(137)$ en $\chi(37)$ gegeven zijn en een karakter χ mod 153 wordt genoteerd als

$$\{\chi(137), \chi(37)\} \,.$$

De ordes van $\mathbb{Z}/9\mathbb{Z}$ en $\mathbb{Z}/17\mathbb{Z}$ zijn $\phi(9) = 6$ en $\phi(17) = 16$ en inderdaad hebben 137 en 37 respectievelijk ordes 6 en 16 in $(\mathbb{Z}/153\mathbb{Z})^*$. De $\phi(153) = 96$ producten $137^{e_0}37^{e_1}$ met $0 \le e_0 \le 5$ en $0 \le e_1 \le 15$ zijn precies de 96 inverteerbare restklassen modulo 153. Elk Dirichletkarakter χ modulo 153 is van de vorm

$$\{\zeta_6^{e_0}, \zeta_{16}^{e_1}\} \,,$$

met $0 \leq e_0 \leq 5$ en $0 \leq e_1 \leq 15$, en er zijn dus in totaal $\phi(153) = 96$ Dirichletkarakters modulo 153. Hiervan zijn er vier reëel, namelijk

$$\{1,1\},\ \{1,-1\},\ \{-1,1\},\ \{-1,-1\},$$

en deze hebben respectievelijk conductors 1, 17, 3 en 51. Als $\chi = \{c,d\}$ dan is $\chi(146) = c \cdot d^3$, omdat $146 = 137 \cdot 37^3 \pmod{153}$.

2.3 Het Kroneckersymbool

Het bekendste reële Dirichletkarakter is waarschijnlijk het *Legendresymbool*, ook wel het *kwadraatrestsymbool* genoemd. Het is als volgt gedefinieerd voor een oneven priemgetal p en $a \in \mathbb{N}$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{als } p \mid a, \\ 1 & \text{als } a = x^2 \text{ oplosbaar is mod } p, \\ -1 & \text{als } a = x^2 \text{ niet oplosbaar is mod } p. \end{cases} \tag{2.7}$$

Notatie 2.3.1. Het kwadraatrestsymbool $\left(\frac{a}{p}\right)$ wordt ook wel genoteerd met $(a|p)$.

Dit is inderdaad een Dirichletkarakter [Beu]. In het bijzonder zijn er modulo p precies $\frac{p-1}{2}$ kwadraten en evenzoveel niet-kwadraten.

We kunnen het symbool uitbreiden tot willekeurige oneven getallen door het multiplicatief te verklaren: voor $m = 2^{e_2}3^{e_3}5^{e_5}\ldots$ is

$$\left(\frac{a}{m}\right) = \left(\frac{a}{2}\right)^{e_2}\left(\frac{a}{3}\right)^{e_3}\left(\frac{a}{5}\right)^{e_5}\cdots$$

merk op dat factoren die in het kwadraat in m voorkomen, kunnen worden genegeerd. Dus $\left(\frac{a}{m}\right)$ is alleen afhankelijk van het kwadraatvrije deel van m. Verder definiëren we de speciale gevallen

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{als } 2 \mid a, \\ 1 & \text{als } a \equiv 1,\ 7 \bmod 8, \\ -1 & \text{als } a \equiv 3,\ 5 \bmod 8, \end{cases} \tag{2.8}$$

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{als } a \geq 0, \\ -1 & \text{als } a < 0. \end{cases} \tag{2.9}$$

De uitbreiding wordt het *Kroneckersymbool* genoemd.

Voor het Kroneckersymbool geldt de *wet van kwadratische wederkerigheid* [Beu, Stelling 11.1.6]

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{2.10}$$

Hieruit volgt dat voor oneven positieve a,

$$\left(\frac{-1}{a}\right) = \left(\frac{a}{-1}\right)(-1)^{(a-1)/2} = \begin{cases} 1 & \text{als } a = 1 \bmod 4, \\ -1 & \text{als } a = 3 \bmod 4. \end{cases} \tag{2.11}$$

$$\left(\frac{2}{a}\right) = \left(\frac{a}{2}\right)(-1)^{(a-1)/4} = \begin{cases} 1 & \text{als } a = 1, 3 \bmod 8, \\ -1 & \text{als } a = 5, 7 \bmod 8. \end{cases} \tag{2.12}$$

$$\left(\frac{-2}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{2}{a}\right) = \begin{cases} 1 & \text{als } a \equiv 1, 7 \bmod 8, \\ -1 & \text{als } a \equiv 3, 5 \bmod 8. \end{cases} \tag{2.13}$$

Omdat $\left(\frac{4}{a}\right) = 1$, kunnen we deze drie functies ook schrijven als $\left(\frac{-4}{a}\right)$, $\left(\frac{8}{a}\right)$ en $\left(\frac{-8}{a}\right)$. Uit de kwadratische wederkerigheid volgt ook dat voor oneven p,

$$\left(\frac{a}{p}\right) = \begin{cases} \left(\frac{p}{a}\right) & \text{als } p \equiv 1 \bmod 4, \\ \left(\frac{-p}{a}\right) & \text{als } p \equiv 3 \bmod 4 \end{cases} = \left(\frac{p^*}{a}\right), \tag{2.14}$$

waarbij $p^* = (-1)^{(p-1)/2}p$, oftewel het unieke getal zodanig dat $|p^*| = p$ en $p^* \equiv 1 \bmod 4$.

2.4 Klassificatie van reële primitieve karakters

We laten hier zien dat het Kroneckersymbool in essentie het enige type reële primitieve karakter is.

Karakters modulo priemmachten

We beweren het volgende.

Lemma 2.4.1. *Modulo een oneven priemgetal p is de functie $a \longmapsto \left(\frac{a}{p}\right)$ het enige niet-triviale reële karakter en het is bovendien primitief.*

Bewijs. Zij nu p een oneven priemgetal en veronderstel χ een willekeurig reëel karakter modulo p dat niet het triviale karakter is. We hebben dus $\chi(a) = 1$ of -1 en dus $\chi(a^2) = 1$, mits $p \nmid a$. Alle kwadraten worden dus op 1 afgebeeld. Omdat χ gebalanceerd is, moeten alle niet-kwadraten op -1 afbeelden. Het resultaat is dat χ het kwadraatrestsymbool is. Tot slot impliceert het niet-triviaal zijn van χ dat $f_\chi > 1$ en dus dat $f_\chi = p$. □

Voor oneven priemmachten p^k met $k \geq 2$ kennen we ook alle reële karakters.

Lemma 2.4.2. *Modulo een oneven priemmacht p^k met $k \geq 2$ is de functie $\chi : a \longmapsto \left(\frac{a}{p}\right)$ het enige niet-triviale reële karakter.*

Bewijs. Beschouw de getallen van de vorm $bp^{k-1} + 1$ en neem daarvan het kwadraat:

$$(b\,p^{k-1} + 1)^2 = b^2\,p^{2k-2} + 2\,b\,p^{k-1} + 1 \equiv 2\,b\,p^{k-1} + 1 \pmod{p^k},$$

vanwege $2k - 2 \geq k$. Alle getallen van de vorm $2bp^{k-1} + 1$ zijn dus kwadraten, en vanwege inverteerbaarheid van 2 zijn alle p^{k-1}-vouden plus één dus kwadraten modulo p^k. Voor een willekeurig reëel Dirichletkarakter χ modulo p^k geldt dus dat

$$\chi(b\,p^{k-1} + 1)) = 1.$$

Uit definitie 2.1.4 volgt nu dat $p^{k-1} \in \mathscr{M}_\chi$ en dus $f_\chi \mid p^{k-1} < p^k$. Dus χ is niet primitief en reduceerbaar tot een karakter modulo p^{k-1}. Omdat dit geldt voor alle $k \geq 2$ kunnen we dit procédé herhalen met als eindconclusie dat χ een niet-triviaal karakter modulo p induceert. Lemma 2.4.1 geeft nu dat χ het kwadraatrestsymbool moet zijn. □

Modulo oneven priemmachten zijn er dus weinig reële karakters. Hoe zit dat met even priemmachten? Vanaf 16 blijkt net als voor oneven priemmachten niets te vinden te zijn, maar modulo 4 en 8 bestaan wel primitieve karakters.

Lemma 2.4.3. *Er zijn geen primitieve reële karakters modulo 2^k als $k \geq 4$.*

Bewijs. Kwadrateren van het getal $2^{k-2}+1$ geeft

$$(2^{k-2}+1)^2 = 2^{2k-4} + 2 \cdot 2^{k-2} + 1 \equiv 2^{k-1} + 1 \pmod{2^k},$$

vanwege $2k-4 \geq k$. Dus $2^{k-1}+1$ is een kwadraat. Dit geeft voor willekeurige karakters χ modulo 2^k dat $f_\chi \mid 2^{k-1}$ en dus is χ niet primitief. Ook hier kunnen we door herhaling zien dat χ door een karakter modulo 8 zal worden geïnduceerd. □

Modulo 8 zijn er $\phi(8) = 4$ Dirichletkarakters, met de volgende beelden op de waarden 0, …, 7.

$$\begin{array}{l} \chi_1 : \{0,\ 1,\ 0,\ \ 1,\ 0,\ \ 1,\ 0,\ \ 1\} \\ \chi_2 : \{0,\ 1,\ 0,\ -1,\ 0,\ \ 1,\ 0,\ -1\} \\ \chi_3 : \{0,\ 1,\ 0,\ -1,\ 0,\ -1,\ 0,\ \ 1\} \\ \chi_4 : \{0,\ 1,\ 0,\ \ 1,\ 0,\ -1,\ 0,\ -1\} \end{array} \tag{2.15}$$

Hier is $\chi(1)$ het triviale karakter. Uit $\chi_2(5) = 1$ en $\chi_2(3) = -1$ volgt $f_{\chi_2} = 4$ en uit $\chi_3(5) = \chi_4(5) = -1$ volgt $f_{\chi_3} = f_{\chi_4} = 8$.
Merk op dat

$$\chi_2(a) = \left(\frac{-4}{a}\right), \qquad \chi_3(a) = \left(\frac{-8}{a}\right), \qquad \chi_4(a) = \left(\frac{8}{a}\right), \tag{2.16}$$

de drie karakters (2.11), (2.12) en (2.13) uit paragraaf 2.3.

Willekeurige moduli

We hebben nu alle primitieve reële karakters modulo priemmachten gevonden; we kijken nu naar getallen met verschillende priemfactoren. Het is voldoende om te kijken naar karakters modulo pq met $\gcd(p,q) = 1$. We laten het volgende zien.

Lemma 2.4.4. *Zij $p, q \in \mathbb{N}$ relatief priem, χ_p en χ_q karakters modulo respectievelijk p en q en zij χ_{pq} het karakter modulo pq gegeven door $a \longmapsto \chi_p(a)\chi_q(a)$. Dan geldt dat χ_{pq} primitief is dan en slechts dan als χ_p en χ_q beide primitief zijn.*

Bewijs. Stel dat χ_{pq} niet primitief is. Dan is er een echte deler m van pq met $\chi_{pq}(am+1) = 1$ voor alle a. Met een *echte deler* van een getal n bedoelen we een deler ongelijk aan n zelf. Schrijf $m = p'q'$ met $p' \mid p, q' \mid q$. Dan is $p' \neq p$ of $q' \neq q$. Dit impliceert dat $\mathrm{kgv}(m,p)$ of $\mathrm{kgv}(m,q)$ een echte deler van pq is. Dit op zijn beurt impliceert dat

$$\gcd(q, \mathrm{kgv}(m,p)) \neq q \quad \text{of} \quad \gcd(p, \mathrm{kgv}(m,q)) \neq p. \tag{2.17}$$

Voor χ_p, χ_q en χ_{pq} gelden nu de volgende implicaties.

$$\begin{aligned}
\left\{\begin{array}{rcl}\chi_{pq}(a\,m+1) &=& 1\\ \chi_p(a\,p+1) &=& 1\end{array}\right. &\Longrightarrow \left\{\begin{array}{rcl}\chi_{pq}(a\ \mathrm{kgv}(m,p)+1) &=& 1\\ \chi_p(a\ \mathrm{kgv}(m,p)+1) &=& 1\end{array}\right.\\
&\Longrightarrow \quad \chi_q(a\ \mathrm{kgv}(m,p)+1)=1,\\
\left\{\begin{array}{rcl}\chi_q(a\ \mathrm{kgv}(m,p)+1) &=& 1\\ \chi_q(a\,q+1) &=& 1\end{array}\right. &\Longrightarrow \quad \chi_q(a\ \mathrm{ggd}(q,\mathrm{kgv}(m,p))+1)=1\\
&\Longrightarrow \quad f_{\chi_q} \mid \mathrm{ggd}(q,\mathrm{kgv}(m,p)).
\end{aligned}$$

Door dit te herhalen met p en q verwisseld, verkrijgen we

$$f_{\chi_p} \mid \mathrm{ggd}(p,\mathrm{kgv}(m,q)).$$

Gecombineerd met (2.17) geeft dit dat $f_{\chi_p} \neq p$ of $f_{\chi_q} \neq q$, en dus dat tenminste één van beide niet primitief is.

Andersom geldt dat als, zonder verlies van algemeenheid, χ_p niet primitief is, dan is er een echte deler $m \mid p$ zodanig dat χ_p tot een karakter χ_m modulo m reduceert. Het product χ_{pq} zal dan tot het karakter $\chi_m\chi_q$ modulo mq reduceren, waaruit volgt dat het niet primitief is. □

We kunnen nu de klassificatie geven.

Stelling 2.4.5. *Een reëel primitief Dirichletkarakter heeft de vorm*

$$\rho_m : a \longmapsto \left(\frac{m}{a}\right), \tag{2.18}$$

waarbij $m = tk$ met $k \equiv 1 \mod 4$ en kwadraatvrij en $t = 1, -4, 8$ of -8. Bovendien is $f_{\rho_m} = |m|$.

Merk op dat de verzameling van alle getallen m van de gegeven vorm precies een collectie representanten zijn voor $\mathbb{Q}/\mathbb{Q}^2$. Als we voor iedere $n \in \mathbb{Z}$, het getal $s(n)$ definiëren als de unieke m van de in deze stelling beschreven vorm zodanig dat m/n een kwadraat in $\mathbb{Q}$ is, dan geldt dat $\rho_{n_1}\rho_{n_2} = \rho_{s(n_1n_2)}$. We geven een algoritme om gegeven n de waarde $s(n)$ te vinden.

Algoritme 2.4.6.

(i) Zij j het positieve oneven deel van n. Zij k het kwadraatvrije deel van j. Als $k \equiv 3 \mod 4$, vervang k door $-k$. Dan is k altijd 1 modulo 4.

(ii) Zij $a = n/k$. Dan is $a = \pm 2^u$ voor een $u \in \mathbb{N}_0$.

(iii) Zij b het kwadraatvrije deel van a. Dan is $b = 1, 2, -1$ of -2.

(iv) Zij

$$t = \begin{cases} b & \text{als } b = 1,\\ 4b & \text{als } b = -1, 2 \text{ of } -2.\end{cases}$$

(v) Geef uitvoer $s(n) = tk$ en stop.

De getallen uitgevoerd door dit algoritme worden *discriminanten* genoemd. Merk op dat $s(n)$ de discriminant is van de kwadratische lichaamsuitbreiding $\mathbb{Q}(\sqrt{n})$ van $\mathbb{Q}$. Als n een kwadraat is, dan is $s(n) = 1$. Stelling 2.4.5 heeft een interessant gevolg.

Gevolg 2.4.7. *Zij $n \in \mathbb{Z}$. Het primitieve karakter geassocieerd met $\chi_n : a \mapsto \left(\frac{n}{a}\right)$ is $\rho_{s(n)}$.*

Dit stelt ons in staat om heel snel de primitieve geassocieerde van een willekeurig Kroneckersymbool te vinden.

2.5 Gausssommen

Zij $M \in \mathbb{N}$ en zij $\chi \in \mathscr{D}(M)$ een primitief Dirichletkarakter modulo M. De Gausssom van χ is een gewogen som over de machten van de M-de complexe eenheidswortel $\zeta_M = e^{2\pi i/M}$, met als weegfactor voor ζ_M^a de waarde van χ in a.

Definitie 2.5.1 (Gausssom)**.** Voor $\chi \in \mathscr{D}(M)$ een primitief Dirichletkarakter is de *Gausssom* van χ gedefinieerd als

$$W(\chi) = \sum_{a=0}^{M-1} \chi(a)\mathrm{e}^{2\pi \mathrm{i} a/M}. \tag{2.19}$$

De complexe getallen $e^{2\pi i a/M}$ zijn precies alle machten van de M-de complexe eenheidswortel ζ_M. We definiëren een gerelateerde som die we hier noteren met $W_b(\chi)$ (dit is geen standaardnotatie), als de uitdrukking

$$W_b(\chi) = \sum_{a=0}^{M-1} \chi(a)\mathrm{e}^{2\pi \mathrm{i} ab/M}. \tag{2.20}$$

Een gelijkheid voor Gausssommen die we later gaan gebruiken is het volgende resultaat dat ook wordt genoemd en bewezen in [Miy, Lemma 3.1.1 (1)]).

Lemma 2.5.2. *Voor $\chi \in \mathscr{D}(M)$ primitief en $b \in \mathbb{N}$ geldt dat*

$$W_b(\chi) = \overline{\chi}(b)W(\chi). \tag{2.21}$$

We volgen het bewijs van Toshitsune Miyake in [Miy, Lemma 3.1.1 (1)].

Bewijs. Stel dat $\gcd b, M = 1$. Dan is $\chi(a) = \chi(ab)\overline{\chi}(b)$ en dus

$$W_b(\chi) = \overline{\chi}(b) \sum_{a=0}^{M-1} \chi(ab)\mathrm{e}^{2\pi \mathrm{i} ab/M} = \overline{\chi}(b)W(\chi), \tag{2.22}$$

omdat voor $a = 0, \cdots, M-1$, de waarden van ab precies alle restklassen modulo M doorlopen, zij het in een andere volgorde. Dit werkt echter alleen als $\gcd b, M = 1$. In

het geval dat $\gcd b, M > 1$ is $\overline{\chi}(b) = 0$ en moeten we dus laten zien dat ook $W_b(\chi) = 0$. Schrijf $n = M/\gcd b, M$ en definieer

$$\begin{aligned} H &= \{d \in (\mathbb{Z}/M\mathbb{Z})^*\colon\ d \equiv 1 \pmod{M}\}, \\ Hc &= \{dc \in (\mathbb{Z}/M\mathbb{Z})^*\colon\ d \equiv 1 \pmod{M}\}. \end{aligned}$$

Merk op dat de Hc een partitie van $(\mathbb{Z}/M\mathbb{Z})^*$ vormen.
Voor alle $d \in H$ geldt $n \mid d-1$ en dus $bn \mid bd-b$. Omdat $bn = bM \,/\, \gcd b, M = \operatorname{kgv} b, M$, geldt $M \mid bn$ en dus $M \mid bd - b$. Dit geeft dat

$$bd \,/\, M \equiv b \,/\, M \pmod{1}. \tag{2.23}$$

Er geldt dan

$$\begin{aligned} W_b(\chi) &= \sum_{c=1}^{n-1} \sum_{d \in Hc} \chi(d) \mathrm{e}^{2\pi \mathrm{i} db/M} \\ &= \sum_{c=1}^{n-1} \sum_{d \in H} \chi(cd) \mathrm{e}^{2\pi \mathrm{i} cdb/M} \\ &= \sum_{c=1}^{n-1} \chi(c) \sum_{d \in H} \chi(d) \mathrm{e}^{2\pi \mathrm{i} bc/M}, \end{aligned}$$

waarbij de laatste stap gebruik maakt van (2.23). Dit schrijven we verder om naar

$$\sum_{c=1}^{n-1} \chi(c) \mathrm{e}^{2\pi \mathrm{i} bc/M} \sum_{d \in H} \chi(d). \tag{2.24}$$

Het is nu voldoende om te laten zien dat $\sum_{d \in H} \chi(d) = 0$. Omdat dit een som van karakterwaarden is, is het voldoende om te laten zien dat χ op H niet reduceert ot het triviale karakter. Stel dat het dat wel zou doen, dan geldt $\chi(d) = 1$ voor alle $d \in H$, oftewel

$$(\gcd(d, M) = 1 \text{ en } d \equiv 1 \pmod{n}) \Longrightarrow \chi(d) = 1. \tag{2.25}$$

Dit is dezelfde bewering als (2.1), en dit impliceert dat $n \in \mathscr{M}_\chi$ en dus $f_\chi \mid n$. Maar $f_\chi = M$ per aanname dat χ primitief is. Dit levert $M \mid n$, hetgeen een tegenspraak geeft, omdat $n < M$. Daarom kan χ niet triviaal zijn op H, en moet dus $\sum_{d \in H} \chi(d) = 0$, en uitdrukking (2.24) is dus nul. □

2.6 Dirichlet L-functies

Dirichlet L-functies zijn een veralgemenisatie van Riemann's zetafunctie, en zijn in feite lineaire combinaties van zetafuncties. We geven hier de benodigde definities en geven een speciaal geval waarin de waarde van Dirichlet L-functies voor triviale karakters modulo M kan worden uitgerekend.

Riemann's zetafunctie

Gegeven een Dirichletkarakter, kunnen we daar een functie op $\mathbb{C}$ aan koppelen die een Dirichlet L-functie wordt genoemd. We beginnen met het geven van *Riemann's zetafunctie* ζ:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2.26}$$

Naar deze functie wordt veel onderzoek gedaan en er is veel over bekend. Zo heeft Euler in 1735 laten zien dat

$$\zeta(2) = \frac{\pi^2}{6}. \tag{2.27}$$

Zij $M \in \mathbb{N}$. We kunnen nu alle termen $1/n^s$ verdelen over de restklassen n modulo M:

$$\zeta(s) = \sum_{a=1}^{M} \sum_{n=0}^{\infty} \frac{1}{(Mn+a)^s}. \tag{2.28}$$

De restklasse 0 mod M geeft de term

$$\sum_{n=1}^{\infty} \frac{1}{(Mn)^s} = \frac{1}{M^s}\zeta(s). \tag{2.29}$$

De andere restklassen geven termen die van een vorm zijn die de *Hurwitzzetafunctie* wordt genoemd:

$$\zeta(s,x) = \sum_{n\in\mathbb{N}_0}^{\star} \frac{1}{(n+x)^s}, \qquad x \in \mathbb{R}. \tag{2.30}$$

De $\star$ boven het sommatieteken geeft aan dat eventuele termen met $n + x = 0$ worden weggelaten. Merk op dat de term voor de restklasse a mod M in (2.29) gelijk is aan $M^s\zeta(s, a/M)$. Zo kunnen we $\zeta(s)$ uitdrukken in een som van $\zeta(s, a/M)$ waarbij a de restklassen modulo M doorloopt:

$$\zeta(s) = \frac{1}{M^s}\left(\zeta(s) + \zeta\Big(s, \frac{1}{M}\Big) + \zeta\Big(s, \frac{2}{M}\Big) + \ldots + \zeta\Big(s, \frac{M-1}{M}\Big)\right) \tag{2.31}$$

Dirichlet L-functie

De M termen in de som (2.31) hebben alle coëfficiënt 1. Deze coëfficiënten kunnen we vervangen door de beelden van een Dirichletkarakter χ van modulus M. Het resultaat is een nieuwe functie op $\mathbb{C}$ die bekend staat als de *Dirichlet L-functie* behorend bij χ.

Definitie 2.6.1 (Dirichlet L-functie)**.** Zij χ een Dirichletkarakter van modulus M. De *Dirichlet L-functie* of *Dirichlet L-reeks* behorend bij χ is de functie op $\mathbb{C}$ gedefinieerd door het volgende voorschrift.

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s. \tag{2.32}$$

Opmerking 2.6.2. $L(s,\chi)$ kan net als $\zeta(s)$ worden opgesplitst over de restklassen modulo M. Dit geeft de volgende gelijkheid voor Dirichlet L-functies.

$$L(s,\chi) = \left(\chi(1)\zeta\Big(s,\frac{1}{M}\Big) + \chi(2)\zeta\Big(s,\frac{2}{M}\Big) + \ldots + \chi(M-1)\zeta\Big(s,\frac{M-1}{M}\Big)\right).$$

De waarde in $s = 2$

Laten we bij wijze van voorbeeld het karakter χ modulo 2 bekijken, dat 1 geeft op oneven waarden en 0 op even waarden. We vragen ons af wat $L(2,\chi)$ is. We weten dat voor elke 2-periodieke functie f met beeld a op even getallen en b op oneven getallen,

$$L(2,f) = a\sum_{n=1}^{\infty}\frac{1}{(2n)^2} + b\sum_{n=0}^{\infty}\frac{1}{(2n+1)^2}$$

Als $a = b = 1$, dan staat hier Euler's $\frac{\pi^2}{6}$. Voor $a = 1$ en $b = 0$ staat hier $\frac{1}{2^2}\frac{\pi^2}{6} = \frac{\pi^2}{24}$. Onze situatie is $a = 0$, $b = 1$ en is dus het verschil tussen deze twee waarden. De conclusie is dat

$$L(2,\chi) = \sum_{n=0}^{\infty}\frac{1}{(2n+1)^2} = \frac{\pi^2}{6} - \frac{\pi^2}{24} = \frac{\pi^2}{8}. \tag{2.33}$$

Zij nu χ het primitieve karakter modulo 4. Dan geldt dat

$$L(2,\chi) = \sum_{n=0}^{\infty}\frac{1}{(4n+1)^2} - \sum_{n=0}^{\infty}\frac{1}{(4n+3)^2} = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)^2}.$$

De waarde van deze uitdrukking staat bekend als *de constante van Catalan* [Wol1] welke ongeveer $0,915\,965\,594$ in waarde is [Wol2].

Eulerproducten

Een som $\sum a(n)$ waarvan de termen multiplicatief zijn, kan worden geschreven als *Eulerproduct*. Dit geschiedt door de termen op te splitsen in priemfactoren:

$$a(n) = a(2^{k_2})a(3^{k_3})a(5^{k_5})\ldots \quad \text{voor } n = 2^{k_2}3^{k_3}5^{k_5}\ldots.$$

Omdat elke combinatie van exponenten voorkomt, is het mogelijk om de term $1 + a(2) + a(4) + a(8) + \ldots$ buiten de som te halen; de oneven termen blijven over.

$$\sum_{n\in\mathbb{N}} a(n) = (1 + a(2) + a(4) + a(8) + \ldots)\sum_{2\nmid n} a(n)$$

Men kan op die manier hetzelfde doen voor de andere priemgetallen:

$$\begin{aligned}\sum_{n\in\mathbb{N}} a(n) = {} & (1 + a(2) + a(4) + a(8) + \ldots)\cdot(1 + a(3) + a(9) + a(27) + \ldots) \\ & \cdot(1 + a(5) + a(25) + a(125) + \ldots)\cdot(1 + a(7) + a(49) + a(343) + \ldots)\cdot\ldots\end{aligned}$$

Omdat de $a(p^k) = a(p)^k$, kunnen we elke factor nu schrijven als machtreeks. Priemgetallen waarvoor $a_p = 0$ geven de factor 1 en die vervallen dus. Het resultaat noemen we het Eulerproduct van de reeks.

Lemma 2.6.3. *Zij $a : \mathbb{N} \to \mathbb{C}$ een rij complexe getallen, met de eigenschap dat $a(mn) = a(m)a(n)$ voor alle $m, n \in \mathbb{N}$, en zij $s \in \mathbb{R}$ met $|\Re s| < 1$. Dan geldt*

$$\sum_{n\in\mathbb{N}} a(n) = \prod_{p} \left(1 + a(p) + a(p)^2 + a(p)^3 + \ldots\right) = \prod_{p:a(p)\neq 0} \frac{1}{1 - a(p)}. \tag{2.34}$$

Het product wordt hierbij genomen over alle priemgetallen.

De termen $\chi(n)/n^s$ in de L-reeks (2.32) zijn multiplicatief en dus hebben Dirichlet L-reeksen een Eulerproduct:

$$L(s, \chi) = \prod_{p:\chi(p)\neq 0} \frac{1}{1 - \chi(p)p^{-s}}. \tag{2.35}$$

Voor Riemann's zetafunctie (2.26) is $a(n) = n^{-s}$ en dus is

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

In het bijzonder vinden we dat

$$\prod_{p} \frac{1}{1 - p^{-2}} = \pi^2/6. \tag{2.36}$$

Triviale karakters

Voor het triviale karakter χ modulo M kunnen we $L(2, \chi)$ volledig bepalen, gebruikmakende van het Eulerproduct. Merk op dat voor p priem, $\chi(p) = 0$ als p een deler van M is en 1 anders. Dit betekent voor het Eulerproduct (2.35) dat

$$L(2, \chi) = \prod_{p\nmid n} \frac{1}{1 - p^{-2}}.$$

Voegen we aan beide zijden extra factoren toe voor de priemgetallen p die n delen, en passen we daarna (2.36) toe op het rechterlid, dan vinden we

$$\left(\prod_{p|n} \frac{1}{1 - p^{-2}}\right) L(2, \chi) = \pi^2/6,$$

oftewel

$$L(2, \chi) = \frac{\pi^2}{6} \prod_{p|n} \left(1 - p^{-2}\right). \tag{2.37}$$

Voorbeeld 2.6.4. De L-reeks behorende bij het triviale karakter modulo $77 = 7 \cdot 11$ is

$$L(2, \chi_{77}) = \frac{\pi^2 \cdot 48 \cdot 120}{6 \cdot 49 \cdot 121} = \frac{960}{5\,929}\pi^2.$$

Even karakters

Een reëel Dirichletkarakter χ heet *even* als $\chi(-a) = \chi(a)$ voor alle a. Dit is equivalent met de bewering dat $\chi(-1) = 1$. Als $\chi(-1) = -1$ noemen we χ *oneven*. We kunnen $L(s, \chi)$ herschrijven als s en χ beide even of beide oneven zijn. We nemen hier $s = 2$, aangezien dat geval voor ons belangrijk is.

We gebruiken het volgende.

Lemma 2.6.5. *Voor $z \notin \mathbb{Z}$ geldt dat $\pi^2/(\sin(\pi z))^2 = \sum_{n\in\mathbb{Z}}(n-z)^{-2}$.*

Bewijs. Door in te zien dat beide leden dezelfde nulpuntsverzameling hebben (met multipliciteit geteld) zien we dat beide leden een constant veelvoud van elkaar zijn. We vullen nu een waarde voor z in om aan te tonen dat die constante 1 is. Kies $z = 1/2$.

$$\begin{aligned}
\frac{\pi^2}{(\sin(\pi/2))^2} &= \sum_{n\in\mathbb{Z}} \frac{1}{(n-1/2)^2} \\
\pi^2 &= 2\sum_{n=1}^{\infty} \frac{1}{(n-1/2)^2} \\
\pi^2 &= 8\sum_{n=1}^{\infty} \frac{1}{(2n-1)^2} \\
\pi^2/8 &= L(2,\chi),
\end{aligned}$$

waarbij χ het triviale karakter modulo 2 is. Deze laatste gelijkheid hebben we aangetoond in (2.33). □

Veronderstel χ een even karakter modulo m. Dan is $L(2, \chi)$ gelijk aan

$$\begin{aligned}
\sum_{n=1}^{\infty} \chi(n)/n^2 &= \frac{1}{2}\sum_{n\in\mathbb{Z}}^{\star} \chi(n)/n^2 \\
&= \frac{1}{2}\sum_{a=1}^{m-1}\sum_{n\in\mathbb{Z}} \chi(nm+a)/(nm+a)^2 \\
&= \frac{1}{2}\sum_{a=1}^{m-1} \chi(a)\sum_{n\in\mathbb{Z}} (nm+a)^{-2} \\
&= \frac{1}{2m^2}\sum_{a=1}^{m-1} \chi(a)\sum_{n\in\mathbb{Z}} (n+\frac{a}{m})^{-2} \\
&= \frac{1}{2m^2}\sum_{a=1}^{m-1} \chi(a)\frac{\pi^2}{(\sin(-a\pi/m))^2} \\
&= \frac{\pi^2}{2m^2}\sum_{a=1}^{m-1} \frac{\chi(a)}{(\sin(a\pi/m))^2}.
\end{aligned}$$

Op rationele veelvouden van π geeft de sinusfunctie algebraïsche functiewaarden, dus deze afleiding laat zien dat $L(2, \chi)$ voor even karakters χ een algebraïsch getal is. Voor χ het

niet-triviale karakter modulo 5 kunnen we deze afleiding laten zien, gebruikmakende van de gelijkheden

$$\sin(\pi/5) = \sin(4\pi/5) = \sqrt{5/8 - \sqrt{5}/8}, \qquad \sin(2\pi/5) = \sin(3\pi/5) = \sqrt{5/8 + \sqrt{5}/8}.$$

Nemen we dit aan, dan vinden we dat

$$\begin{aligned}
L(2,\chi) &= \frac{\pi^2}{50} \sum_{a=1}^{4} \frac{\chi(a)}{(\sin(a\pi/5))^2} \\
&= \frac{\pi^2}{50} \left((\sin(\pi/5))^{-2} - (\sin(2\pi/5))^{-2} - (\sin(3\pi/5))^{-2} + (\sin(4\pi/5))^{-2} \right) \\
&= \frac{\pi^2}{25} \left((\sin(\pi/5))^{-2} - (\sin(2\pi/5))^{-2} \right) \\
&= \frac{\pi^2}{25} \left(\frac{1}{5/8 - \sqrt{(}5)/8} - \frac{1}{5/8 + \sqrt{(}5)/8} \right) \\
&= \frac{\pi^2}{25} \frac{(5/8 + \sqrt{5}/8) - (5/8 - \sqrt{5}/8)}{(5/8 - \sqrt{5}/8)(5/8 + \sqrt{5}/8)} \\
&= \frac{\pi^2}{25} \frac{\sqrt{5}/4}{5/16} \\
&= \frac{4\pi^2}{25\sqrt{5}}.
\end{aligned}$$

Hoofdstuk 3

Delersommen

Later gaan we veel gebruik maken van sommen over delers van een getal n en daarom wijden we een afzonderlijk hoofdstuk aan gelijkheden over delers van n. We kijken naar sommen over deelverzamelingen van delers en ook over sommen van delers met Dirichlet-karakters.

3.1 Definities

We definiëren eerst de delersom van een getal $n \in \mathbb{N}$.

Notatie 3.1.1. We schrijven $\sigma_t(n)$ voor de functie die $n \in \mathbb{N}$ stuurt naar de som van de t-de machten van alle positieve delers van n:

$$\sigma_t(n) = \sum_{d|n} d^t. \tag{3.1}$$

De som $\sum_{d|n}$ met n niet geheel beschouwen we als de lege som. Op niet-gehele argumenten geeft σ_t dus de waarde nul. Deze functie is niet gedefinieerd voor $n = 0$. De "gewone" delersom σ_1 schrijven we als σ.

Voorbeeld 3.1.2. $\sigma_t(1) = 1$ voor alle t. $\sigma_0(n)$ is het aantal delers van n. Als p priem is, dan is $\sigma_t(p) = 1 + p^t$.

Lemma 3.1.3. *Voor alle $n \in \mathbb{N}$ geldt dat $\sigma(n) = n\,\sigma_{-1}(n)$.*

Bewijs. Als S de collectie van delers van n is, dan is $\{n/d\colon\ d \in S\} = S$. Dus geldt

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d}.$$

□

Er is het een en ander te zeggen over delersommen over delers die zelf bepaalde deelbaarheidseigenschappen hebben.

Lemma 3.1.4. *Zij p een priemgetal en f een willekeurige functie op $\mathbb{N}$. Dan geldt dat*

$$\sum_{d|n,\, p|d} f(d) = \sum_{d|\frac{n}{p}} f(pd)$$

en

$$\sum_{d|n,\, p|\frac{n}{d}} f(d) = \sum_{d|\frac{n}{p}} f(d).$$

Bewijs. Het is voldoende te bewijzen dat in beide gevallen de som over dezelfde verzameling wordt genomen. Stel $p \mid n$.
In het eerste geval wordt de linkersom genomen over de verzameling $S = \{d \mid n\colon\ p \mid d\}$. Als $p \mid n$, dan is elke deler d van n die een p-voud is, te schrijven als $d = pd'$, waarbij d' een deler van n/p is, en is voor elke deler d' van n/p, het getal dp' een deler van n die een p-voud is. Dus $S = \{pd'\colon\ d' \mid n/p\}$ en de linker- en rechtersom zijn dus gelijk.
De tweede gelijkheid werkt op een vergelijkbaar manier voor $p \mid n$, met de extra factor p weggelaten. Een deler d van n zodanig dat n/d deelbaar is door p is simpelweg een deler van n/p en andersom. Dus het linker- en rechterlid zijn beide de som van $f(d)$ waarbij d de verzameling $S = \{d \mid n\colon\ p \mid n/d\}$ doorloopt.
Als $p \nmid n$, dan zijn alle vier sommen leeg. □

Dichtheid van een functie

We voeren een notatie in voor het gemiddelde van een functie op $\mathbb{N}$ en deelverzamelingen daarvan, als volgt.

Notatie 3.1.5. Voor eindige verzamelingen $X \subset \mathbb{N}$ schrijven we

$$\operatorname*{mean}_{x \in X} f(x) \quad \text{of} \quad \operatorname*{mean}_{X} f \tag{3.2}$$

voor het gemiddelde van de $f(x)$ over alle $x \in X$. Voor oneindige $X \subset \mathbb{N}$ definiëren we dit gemiddelde als limiet:

$$\operatorname*{mean}_{X} f = \lim_{n \to \infty} \operatorname*{mean}_{X \cap \{1,2,\cdots,n\}} f. \tag{3.3}$$

Verder schrijven we

$$f \rightsquigarrow a, \quad \text{of} \quad f(n) \rightsquigarrow a \tag{3.4}$$

voor de bewering dat $\operatorname{mean}_{\mathbb{N}} f = a$ en

$$f \rightsquigarrow_X a, \quad \text{of} \quad f(n) \rightsquigarrow_X a \tag{3.5}$$

voor de bewering dat $\operatorname{mean}_X f = a$.

We voeren ook een notatie in voor een speciaal soort dichtheid van een functie. Als voor een functie f op $\mathbb{N}$ geldt dat $f(n) = O(n)$, dan is $\sum_{j=1}^{n} f(j) = O(n^2)$. Een aantal functies die we later bekijken heeft deze eigenschap en daarom geven we deze dichtheid een aparte naam.

Notatie 3.1.6. Als f een functie op $\mathbb{N}$ is, schrijven we

$$\Delta(f) = \lim_{n\to\infty} \frac{1}{n^2} \sum_{j=1}^{n} f(j) \tag{3.6}$$

Deze uitdrukking noemen we de *dichtheid* van f.

3.2 Gemiddelde waarden van $\sigma(n)$

Eén van de functies waarvoor $f(n) = O(n)$, is $\sigma(n)$, en deze functie heeft dus een goed gedefinieerde dichtheid. Ook van de algemenere functie

$$\sigma_\chi : n \mapsto \sum_{d|n} \chi\Big(\frac{n}{d}\Big) d, \tag{3.7}$$

met χ een Dirichletkarakter, kunnen we de dichtheid bepalen.

Lemma 3.2.1. *De dichtheid van $\sigma_\chi(n)$ is $\Delta(\sigma_\chi) = \frac{1}{2}L(2,\chi)$. In het bijzonder is $\Delta(\sigma) = \pi^2/12$.*

Bewijs. $\Delta(\sigma_\chi)$ is per definitie de limiet $\lim_{n\to\infty} S_n$, waarbij

$$\begin{aligned} S_n &= \frac{1}{n^2} \sum_{j=1}^{n} \sigma_{\chi,1}(j) \\ &= \frac{1}{n^2} \sum_{j=1}^{n} \sum_{d|j} \chi\Big(\frac{j}{d}\Big) d \\ &= \frac{1}{n^2} \sum_{j=1}^{n} \sum_{d|j} \chi(d) \frac{j}{d}. \end{aligned}$$

We willen nu een afschatting voor S_n maken. Verwissel eerst de sommatievolgorde. De voorwaarde "d deelt j" in de som over d wordt overgeplaatst op de som over j:

$$S_n = \frac{1}{n^2} \sum_{d=1}^{n} \sum_{\substack{j=1 \\ d|j}}^{n} \chi(d) \frac{j}{d}.$$

De factoren d in elke j in de binnenste som valt weg tegen de $1/d$ waarover wordt gesommeerd:

$$\begin{aligned} S_n &= \frac{1}{n^2} \sum_{d=1}^{n} \chi(d) \sum_{j=1}^{\lfloor n/d \rfloor} j \\ &= \frac{1}{n^2} \sum_{d=1}^{n} \frac{\chi(d)}{2} \left(\left\lfloor \frac{n}{d} \right\rfloor^2 + \left\lfloor \frac{n}{d} \right\rfloor \right) \\ &= \frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \left\lfloor \frac{n}{d} \right\rfloor^2 + \frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \left\lfloor \frac{n}{d} \right\rfloor \\ &= A_n + B_n. \end{aligned}$$

We bekijken beide delen nu afzonderlijk. Het rechterstuk B_n kunnen we als volgt afschatten.

$$\begin{aligned}
0 &\leq B_n \\
&\leq \frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \frac{n}{d} \\
&= \frac{1}{2n} \sum_{d=1}^{n} \frac{\chi(d)}{d} \\
&\leq \frac{1}{2n} \sum_{d=1}^{n} \frac{|\chi(d)|}{d} \\
&\leq \frac{1}{2n} \sum_{d=1}^{n} \frac{1}{d} \\
&\leq \frac{1}{2n}(1 + \log(n)).
\end{aligned}$$

Voor $n \to \infty$ gaan beide grenzen naar nul, en dus gaat ook B_n naar 0. De som A_n klemmen we ook in tussen twee grenzen, gebruikmakende van het feit dat $x - 1 \leq \lfloor x \rfloor \leq x$:

$$\frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \left(\frac{n}{d} - 1\right)^2 \leq A_n \leq \frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \left(\frac{n}{d}\right)^2.$$

De bovengrens is

$$\frac{1}{2} \sum_{d=1}^{n} \frac{\chi(d)}{d^2}.$$

De ondergrens splitsen we op door het kwadraat uit te schrijven.

$$\frac{1}{2n^2} \sum_{d=1}^{n} \chi(d) \left(\left(\frac{n}{d}\right)^2 - \frac{2n}{d} + 1\right) = \frac{1}{2} \sum_{d=1}^{n} \frac{\chi(d)}{d^2} - \frac{1}{n^2} \sum_{d=1}^{n} \chi(d) \frac{n}{d} + \frac{1}{2n^2} \sum_{d=1}^{n} \chi(d)$$

De derde term wordt van boven begrensd door $1/n$ en gaat dus naar nul. De tweede term is B_n, waarvan we hebben laten zien dat dat naar nul gaat. Dit geeft dat A_n, en dus S_n, dezelfde limiet heeft als $\frac{1}{2} \sum_{d=1}^{n} \chi(d)/d^2$ en de limiet hiervan voor $n \to \infty$ is per definitie gelijk aan $\frac{1}{2} L(2, \chi)$. □

Verdeling van delers over congruentieklassen

We laten hier zien dat voor alle $m \in \mathbb{N}$, elke restklasse a modulo m een ongeveer even grote bijdrage levert aan $\Delta(\sigma_\chi)$. Met andere woorden dat, als we de functie $\sigma_{\chi,a}$ definiëren als

$$n \mapsto \sum_{\substack{d \mid n \\ d \equiv a \mod m}} \chi\left(\frac{n}{d}\right) d,$$

$\Delta(\sigma_{\chi,a})$ niet van a afhangt.

Lemma 3.2.2. *Zij $m \in \mathbb{N}$ en zij a een restklasse modulo m. Dan geldt dat $\Delta(\sigma_{a,m}) = \frac{1}{2m}L(2,\chi)$.*

Bewijs. We beginnen weer met het verwisselen van de sommatievolgorde en het wegstrepen van de factoren $1/d$ en d in de som die dan ontstaat.

$$\begin{aligned} S_n &= \frac{1}{n^2}\sum_{j=1}^{n}\sigma_{\chi,a}(j) \\ &= \frac{1}{n^2}\sum_{j=1}^{n}\sum_{\substack{d|j \\ d\equiv a}}\chi\Big(\frac{j}{d}\Big)d \\ &= \frac{1}{n^2}\sum_{j=1}^{n}\sum_{\substack{d|j \\ j/d\equiv a}}\chi(d)\frac{j}{d} \\ &= \frac{1}{n^2}\sum_{d=1}^{n}\sum_{\substack{j=1 \\ d|j \\ j/d\equiv a}}^{n}\chi(d)\frac{j}{d} \\ &= \frac{1}{n^2}\sum_{d=1}^{n}\chi(d)\sum_{\substack{j=1 \\ j\equiv a}}^{\lfloor n/d\rfloor} j. \end{aligned}$$

Hierbij moeten alle congruenties modulo m worden gelezen.
Het lastigste deel van het bewijs is de bepaling van de binnenste som. De bovengrens $\lfloor n/d\rfloor$ noemen we N en we willen de som $\sum_{j=1,j\equiv a}^{N} j$ nu begrenzen tussen twee waardes met dezelfde grootte-orde. We gebruiken daarbij dat de som van een rekenkundige rij van x termen waarvan de kleinste y en de grootste z is, gelijk is aan $x(y+z)/2$.
De som bevat ten hoogste $(n/d)/m+1$ termen, waarvan de kleinste maximaal m is en de grootste maximaal n/d. De som is dus altijd kleiner dan $(n/(dm)+1)(m+n/d)/2$, wat we als u_n noteren. De som bevat ten minste $(n/d-1)/m$ termen, waarvan de kleinste minimaal 0 is en de grootste maximaal $(n/d-1)-m$. De som is dus altijd groter dan $((n/d-1)/m)((n/d-1)-m)/2$, wat we als ℓ_n noteren. We vinden dat

$$\frac{1}{n^2}\sum_{d=1}^{n}\chi(d)\ell_n \le S_n \le \frac{1}{n^2}\sum_{d=1}^{n}\chi(d)u_n.$$

Merk op dat ℓ_n en u_n polynomen in $r = n/d$ zijn, en dat bovendien de leidende termen gelijk zijn.

$$u_n = \frac{r^2}{2m} + r + \frac{m}{2}, \qquad \ell_n = \frac{r^2}{2m} - \frac{(m+2)r}{2m} + \frac{m+1}{2m}.$$

Zowel bovengrens als ondergrens zijn dus een lineaire combinatie van de drie waarden

$$A_n = \frac{1}{n^2}\sum_{d=1}^{n}\chi(d),$$
$$B_n = \frac{1}{n^2}\sum_{d=1}^{n}\chi(d)\frac{n}{d},$$
$$C_n = \frac{1}{n^2}\sum_{d=1}^{n}\chi(d)\left(\frac{n}{d}\right)^2.$$

$|A_n|$ is van boven begrensd door $1/n$ en heeft dus limiet nul, $|B_n|$ is van boven begrensd door $1/n\sum_{d=1}^{n}1/d$ en gaat dus eveneens naar nul en de limiet van C_n is $L(2,\chi)$. Uit

$$\frac{C_n}{2m} - \frac{(m+2)B_n}{2m} + \frac{(m+1)A_n}{2m} \leq S_n \leq \frac{C_n}{2m} + B_n + \frac{mA_n}{2}$$

volgt nu direct dat $S_n \to \frac{1}{2m}L(2,\chi)$. □

Lemma 3.2.2 heeft een interessant gevolg.

Gevolg 3.2.3. *Zij ψ een niet-triviaal Dirichletkarakter modulo m en zij*

$$\sigma_{\chi,\psi}(n) = \sum_{d|n}\psi(d)\chi\left(\frac{n}{d}\right)d.$$

Dan is $\Delta(\sigma_{\chi,\psi}) = 0$.

Bewijs. $\Delta(\sigma_{\chi,\psi})$ is een lineaire combinatie van de $\Delta(\sigma_{\chi,a})$ met als coëfficiënten de functiewaarden van χ. Omdat $\Delta(\sigma_{\chi,a})$ niet van a afhangt, komt dit neer op $\frac{1}{2m}L(2,\chi)$ maal de som van de functiewaarden van ψ, welke nul is omdat ψ niet triviaal is. □

De voorgaande resultaten combinerend hebben we nu de volgende stelling.

Stelling 3.2.4. *Voor willekeurige Dirichletkarakters χ en ψ geldt dat*

$$\Delta(\sigma_{\chi,\psi}) = \begin{cases} \frac{\pi^2}{12} & \text{als } \chi = \psi = 1, \\ \frac{1}{2}L(2,\chi) & \text{als } \chi \neq 1,\ \psi = 1, \\ 0 & \text{als } \psi \neq 1. \end{cases}$$

3.3 De aritmetische functies g_p, v_p en w_p

We geven een aantal functies op gehele getallen om enkele notaties eenvoudiger te maken. De functies hebben te maken met deelbaarheidseigschappen en priemontbindingen. Daarna leiden we enkele gelijkheden af die voor deze functies gelden, waarin we ook Dirichletkarakters betrekken.

Notatie 3.3.1. Zij p een priemgetal. Schrijf $g_p(n)$ voor de hoogste p-macht die n deelt en $v_p(n)$ voor het omgekeerde. Schrijf $w_p(n)$ voor het p-vrije deel van n.

$$g_p(n) = p^{\mathrm{ord}_p(n)}, \tag{3.8}$$
$$v_p(n) = 1/g_p(n), \tag{3.9}$$
$$w_p(n) = v_p(n)n. \tag{3.10}$$

Voor $n = 0$ definiëren we $g_p(0) = \infty$ en $v_p(0) = 0$. w_p is niet gedefineerd op 0.

Opmerking 3.3.2. De functie v_p staat bekend als de *p-adische valuatie* $|\cdot|_p$, dit is een norm op $\mathbb{Z}$.

De notaties g_p, v_p en w_p zijn geen standaardnotatie.

Voorbeeld 3.3.3. Voor $n = 240 = 2^4 \cdot 3 \cdot 5$ geldt $g_2(n) = 2^4$, $v_2(n) = 2^{-4}$ en $w_2(n) = 3 \cdot 5$.

Notatie 3.3.4. Omdat voor willekeurige priemgetallen $p \neq q$ geldt dat $w_p(w_q(n)) = w_q(w_p(n))$, schrijven we $w_{pq}(n)$ voor deze uitdrukking. Dus voor kwadraatvrije a is $w_a(n)$ de grootste deler van n die relatief priem met a is. Verder definiëren we $g_{pq}(n) = g_p(n)g_q(n)$ en $v_{pq}(n) = v_p(n)v_q(n)$, dan blijven uitdrukkingen 3.8, 3.9, 3.10, gebruikt als definities voor priemgetallen, ook geldig voor willekeurige kwadraatvrije indices.

Gemiddelde waarde van v_p

We kijken kort naar het asymptotische gedrag van v_p. Ter herinnering, als $p^a \mid n$ en $p^{a+1} \nmid n$, dan is $v_p(n) = 1/p^a$. De fractie van $\mathbb{N}$ die voldoet aan deze eigenschap, is $1/p^a - 1/p^{a+1}$. Dat wil zeggen dat de gemiddelde waarde van v_p gelijk is aan

$$\left(1 - \frac{1}{p}\right) 1 + \left(\frac{1}{p} + \frac{1}{p^2}\right) \frac{1}{p} + \left(\frac{1}{p^2} - \frac{1}{p^3}\right) \frac{1}{p^2} + \dots$$

$$= \left(1 - \frac{1}{p}\right) \left(1 + p^{-2} + p^{-4} + \cdots\right) = \frac{p-1}{p} \frac{p^2}{p^2-1} = \frac{p}{p+1}.$$

Vanwege het feit dat $v_p(pn) = v_p(n)/p$, geldt tevens

$$\forall a \in \mathbb{N}_0 : \; v_p \rightsquigarrow_{p^a\mathbb{N}} \frac{p^{1-a}}{p+1}. \tag{3.11}$$

Hierbij is de notatie $\rightsquigarrow_{p^a\mathbb{N}}$ dezelfde als die uit (3.5).

3.4 Gelijkheden voor delersommen

Lemma 3.1.4 gaf uitdrukkingen voor sommen over delers d van n die deelbaar zijn door p. We kunnen ook iets zeggen over sommen van delers d van n die niet deelbaar zijn door p.

Lemma 3.4.1. *Zij p een priemgetal en f een willekeurige functie op $\mathbb{N}$. Dan geldt dat*

$$\sum_{d|n,\, p\nmid d} f(d) = \sum_{d|w_p(n)} f(d)$$

en

$$\sum_{d|n,\, p\nmid \frac{n}{d}} f(d) = \sum_{d|w_p(n)} f(g_p(n)d) = \sum_{d|w_p(n)} f(n/d).$$

Bewijs. Wederom voldoet het om te bewijzen dat de sommen over dezelfde verzamelingen worden genomen.
Een deler d van n die de factor p niet bezit, is deler van $w_p(n)$ en elke deler van $w_p(n)$ is een deler van n die de factor p niet bezit. Dit geeft de eerste gelijkheid. Een deler d van n zodanig dat n/d de factor p niet bezit, moet alle factoren p in n zelf bevatten. Dat betekent dat het deelbaar is door $g_p(n)$. Schrijven we $d = g_p(n)d'$, dan is d' een deler van $n/g_p(n) = w_p(n)$. Daarnaast is elke deler van $w_p(n)$, vermenigvuldigd met $g_p(n)$, een deler van n die alle factoren p uit n bevat. Dit geeft de eerste gelijkheid in de tweede vergelijking. Als d een deler van n is die alle factoren p van n bezit, dan is n/d een deler van n die geen factor p bezit; oftewel een deler van $w_p(n)$. Dit geeft de laatste gelijkheid. □

Merk op dat de eerste bewering van bovenstaand lemma kan worden veralgemeniseerd door p te vervangen door willekeurige kwadraatvrije a:

Gevolg 3.4.2. *Zij $p_1, \ldots, p_r$ een willekeurig aantal verschillende priemgetallen. Dan geldt voor alle $n \in \mathbb{N}$:*

$$\sum_{d|n,\, p_1\nmid d,\ldots,p_r\nmid d} f(d) = \sum_{d|w_{p_1p_2\ldots p_n}(n)} f(d).$$

Bewijsschets. Pas lemma 3.4.1 herhaaldelijk toe op geschikte waarden van p en n. □

We geven hier nog een gelijkheid met betrekking tot $\sigma(w_p(n))$:

Lemma 3.4.3. *Zij $a \in \mathbb{N}$ kwadraatvrij en p een priemgetal dat niet voorkomt in a. Dan geldt voor alle $n \in \mathbb{N}$:*

$$\sigma(w_a(n)) = (p\, g_p(n) - 1)\sigma(w_{ap}(n)).$$

Bewijs. Schrijf $m = w_a(n)$. Omdat p niet voorkomt in a, is $w_{ap}(n) = w_p(m)$. Het linkerlid bevat alle delers van m. De delersom in het rechterlid bevat de delers van m die p niet bevatten. Stel, $m = p^c k$ bevat c factoren p. De delers van m zijn dan altijd van de vorm

$$d = p^b \ell,$$

met $b \leq c$ en $\ell \mid k$. Voor elke deler ℓ van $w_p(m)$ bevat m dus de delers

$$\ell, p\ell, p^2\ell, \ldots, p^c\ell.$$

De conclusie is dat

$$\sigma(m) = \left(1 + p + p^2 + \ldots + p^c\right) \sigma(w_p(m)) = (pg_p(n) - 1)\sigma(w_p(m).$$

□

Gelijkheden voor delersommen en Dirichletkarakters

Lemma 3.4.4. *Zij p een priemgetal en χ een Dirichletkarakter van modulus p. Dan geldt dat*

$$\sum_{d|n} \chi(d)f(d) = \sum_{d|w_p(n)} \chi(d)f(d). \tag{3.12}$$

Bewijs. Voor delers d van n met $p \mid d$ is $\chi(d) = 0$. □

Zij p een priemgetal en χ een *reëel* karakter modulo p. Beschouw de volgende uitdrukking.

$$\sum_{d|n, p\nmid d} \chi(w_p(n)/d)d$$

Dit kunnen we herschrijven als

$$\sum_{d|w_p(n)} \chi(w_p(n))\overline{\chi}(d)d = \chi(w_p(n)) \sum_{d|w_p(n)} \overline{\chi}(d)d = \chi(w_p(n)) \sum_{d|w_p(n)} \chi(d)d,$$

want als χ reëel is, dan is $\chi = \overline{\chi}$. We krijgen de volgende gelijkheden.

Lemma 3.4.5. *Als p priem is en χ een reëel karakter modulo p, dan geldt dat*

$$\sum_{d|n, p\nmid d} \chi(w_p(n)/d)d = \chi(w_p(n)) \sum_{d|w_p(n)} \chi(d)d,$$

$$\chi(w_p(n)) \sum_{d|n, p\nmid d} \chi(w_p(n)/d)d = \sum_{d|w_p(n)} \chi(d)d,$$

Bewijs. De tweede gelijkheid volgt direct uit de eerste door beide zijden te vermenigvuldigen met $\chi(w_p(n))$. □

Hoofdstuk 4

Modulaire vormen

Modulaire vormen zijn een belangrijke klasse functies met toepassingen in allerlei gebieden in de wiskunde. Wij gebruiken ze voor het uitdrukken van representaties door kwadratische vormen. Modulaire vormen leven in het complexe bovenhalfvlak $\mathbb{H}$ en hebben eigenschappen als de onderliggende groep, het niveau, het gewicht en het karakter. We geven definities van elk van deze eigenschappen. We maken onderscheid tussen spitsvormen en Eisensteinreeksen; hoofdstukken 5 en 6 gaan daar verder op in.

4.1 Groepen

We bekijken groepen als verzamelingen van transformaties van het bovenhalfvlak. Alles speelt zich af binnen de speciale lineaire groep $SL_2(\mathbb{Z})$ die we eerst geven. Aan bepaalde ondergroepen, congruentieondergroepen genoemd, is een niveau N te koppelen.

De modulaire groep

De belangrijkste groep voor modulaire vormen is de groep van 2×2-matrices met elementen in $\mathbb{Z}$ van determinant 1, oftewel de *speciale lineaire groep* $SL_2(\mathbb{Z})$:

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \colon\ a, b, c, d \in R, ad - bc = 1 \right\} \tag{4.1}$$

Men kan een *actie* definiëren van $SL_2(\mathbb{Z})$ op het *complexe bovenhalfvlak* $\mathbb{H} = \{z \in \mathbb{C} \colon\ \Im(z) > 0\}$, waarbij $\gamma \in SL_2(\mathbb{Z})$ werkt op $z \in \mathbb{H}$ via het voorschrift

$$\gamma z = \frac{az + b}{cz + d}, \qquad \text{voor} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \tag{4.2}$$

De functie $z \longmapsto \frac{az+b}{cz+d}$ wordt een *fractionele lineaire transformatie* genoemd. Als men $SL_2(\mathbb{Z})$ beschouwt samen met deze actie op $\mathbb{H}$, dan wordt $SL_2(\mathbb{Z})$ de *modulaire groep* genoemd.
Anderen definiëren de modulaire groep als groep van transformaties, in plaats van als matrixgroep, het is dan een groep onder samenstelling van functies. Omdat de matrix $\gamma = -\mathbb{I}_{2\times 2}$ triviaal werkt, namelijk $(-\mathbb{I}_{2\times 2})z = z$ voor alle $z \in \mathbb{H}$, en dus de triviale transformatie oplevert, is de groep van fractionele lineaire transformaties niet isomorf met $SL_2(\mathbb{Z})$, maar met een quotiëntgroep, en wel

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\mathbb{I}_{2\times 2}, -\mathbb{I}_{2\times 2}\}$$

Meestal wordt voor de modulaire groep echter de notatie $SL_2(\mathbb{Z})$ gebruikt, waarbij impliciet bekend wordt verondersteld dat men γ en $-\gamma$ als equivalent beschouwt.

Stelling 4.1.1. *De matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad en \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{4.3}$$

brengen de modulaire groep voort.

Bewijs. Het bewijs is elementair en te vinden in veel literatuur over modulaire vormen, zoals [Iwa, Stelling 1.1]. In [Lan, Stelling 1.1] wordt ook deze stelling genoemd. □

Dit heeft als gevolg dat elke fractionele lineaire transformatie geschreven kan worden als woord in S en T, waarbij

$$Sz = \frac{-1}{z}, \quad Tz = z + 1. \tag{4.4}$$

Het fundamentaalgebied

Als een groep G werkt op een verzameling X, dan ontstaan de *banen* $Gx = \{gx\colon\ g \in G\}$. Banen Gx en Gy zijn gelijk of disjunct, en de collectie X/G van alle banen vormt een partitie van X. Van elke baan kunnen we een representant bekijken. Een fundamentaalgebied is een collectie van representanten voor alle banen.

Definitie 4.1.2 (Fundamentaalgebied)**.** Laat een groep G werken op een verzameling X. Een *fundamentaalgebied* voor deze actie is een deelverzameling $\mathscr{F}$ van X zodanig dat

- elke baan van X een punt in de afsluiting $\overline{\mathscr{F}}$ van $\mathscr{F}$ bevat.
- elk tweetal punten $x, y \in \mathscr{F}^\circ$ in verschillende banen zitten; oftewel: elke baan heeft ten hoogste één punt in $\mathscr{F}^\circ$.

Anders gezegd is een fundamentaalgebied een kleinste verzameling van representanten voor alle banen in X/G.

Een erg bekend resultaat dat we hier zonder bewijs vermelden, is het volgende.

Propositie 4.1.3. *De verzameling*

$$\mathscr{F} = \{z \in \mathbb{H}\colon\ |\Re z| < 1/2, |z| > 1\}.$$

is een fundamentaalgebied voor de actie van $SL_2(\mathbb{Z})$ op $\mathbb{H}$.

Dezelfde stelling is ook te vinden in [Lan, Stelling 1.1]. Om het intuïtief duidelijk te maken, bedenk dat $SL_2(\mathbb{Z})$ wordt voortgebracht door S en T. Via de transformatie T zijn z en $z + 1$ equivalente punten. Het fundamentaalgebied kan dus niet groter zijn dan een verticale strook in $\mathbb{H}$ van breedte 1. De canonieke keuze is de strook met $|\Re z| < 1/2$. Op eenzelfde manier verwisselt $S : z \mapsto -1/z$ de elementen $z \in \mathbb{H}$ met $\|z\| < 1$ met die $z \in \mathbb{H}$ waarvoor $\|z\| > 1$. Het hier genoemde fundamentaalgebied is precies het deel van de centrale strook dat buiten de eenheidscirkel ligt. Het zou volstaan te bewijzen dat deze punten niet equivalent zijn.

Congruentieondergroepen

Voor een $N \in \mathbb{N}_{\geq 2}$, beschouw het groepshomomorfisme $\phi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ dat matrices coëfficiëntsgewijs modulo N reduceert. De kern van dit homomorfisme bestaat uit die matrices die modulo N reduceren tot de identiteitsmatrix en deze verzameling is dus een normaaldeler van $SL_2(\mathbb{Z})$. Deze groep heeft vanwege zijn belang een speciale naam gekregen.

Definitie 4.1.4 (Hoofdcongruentieondergroep)**.** Voor een $N \in \mathbb{N}_{\geq 2}$ is de *hoofdcongruentieondergroep van niveau* N gedefinieerd als de kern $\Gamma(N)$ van het hierboven gedefinieerde homomorfisme ϕ. Oftewel,

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

Naar analogie met deze definitie wordt $SL_2(\mathbb{Z})$ soms genoteerd als $\Gamma(1)$. Het begrip hoofdcongruentieondergroep is een speciaal geval van het algemenere begrip van een *congruentieondergroep*, wat zoiets betekent als "een ondergroep van $SL_2(\mathbb{Z})$ gedefinieerd door congruenties". De officiële definitie is als volgt.

Definitie 4.1.5 (Congruentieondergroep)**.** Een *congruentieondergroep* is een ondergroep Γ van $SL_2(\mathbb{Z})$ waarvoor er een $N \in \mathbb{N}_{\geq 2}$ bestaat zodanig dat dat $\Gamma(N) < \Gamma$. De kleinste N zodanig dat $\Gamma(N) < \Gamma$ is het *niveau* van Γ.

Belangrijk voor ons zijn de congruentieondergroepen $\Gamma_0(N)$ en $\Gamma_0(L, M)$ gedefinieerd door

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \colon c = 0 \pmod{N} \right\}, \tag{4.5}$$

$$\Gamma_0(L, M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \colon b = 0 \pmod{M},\ c = 0 \pmod{L} \right\}. \tag{4.6}$$

Omdat $SL_2(\mathbb{Z}/N\mathbb{Z})$ eindig is, heeft $\Gamma(N)$ eindige index binnen $SL_2(\mathbb{Z})$, en dus hebben alle congruentieondergroepen eindige index binnen $SL_2(\mathbb{Z})$.

4.2 Modulaire vormen over $SL_2(\mathbb{Z})$

Modulaire vormen zijn functies op $\mathbb{H}$ met een speciaal gedrag ten opzichte van de modulaire groep. Ze komen op verschillende plaatsen in de wiskunde terug [Ste, §1.5] en zijn ook hier essentieel. Informeel gezegd zijn modulaire vormen "nette" functies op $\mathbb{H}$ die een soort "invariantie" hebben onder de fractionele lineaire transformaties.

Definitie 4.2.1 (Modulaire vorm)**.** Een *modulaire vorm over* $SL_2(\mathbb{Z})$ is een holomorfe afbeelding f op $\mathbb{H}$ zodanig dat $f(z)$ begrensd blijft als $z \to \mathrm{i}\infty$ en waarvoor er een $k \in \mathbb{N}_0$ bestaat zodanig dat voor alle $z \in \mathbb{H}$ en $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z). \tag{4.7}$$

Deze k heet ook wel het *gewicht* van de modulaire vorm f.

Opmerking 4.2.2. Sommige literatuur hanteert een ruimere definitie van het begrip modulaire vorm (begrensdheid richting i∞ wordt vervangen door polynomiaal groeigedrag) en noemen die modulaire vormen die voldoen aan definitie 4.2.1, *geheel*.

4.3 De q-expansie van een modulaire vorm

Laat f een modulaire vorm zijn van gewicht k. Dan weten we dus dat voor alle $z \in \mathbb{H}, \gamma \in SL_2(\mathbb{Z})$ geldt dat $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$. Zo geldt dit in het bijzonder voor $\gamma = T$:

$$f(z+1) = f(z).$$

Modulaire vormen zijn dus *periodiek* met periode 1 en zijn derhalve te schrijven als Fourierreeks:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n \mathrm{e}^{2\pi \mathrm{i} n z}.$$

Schrijf $q = \mathrm{e}^{2\pi \mathrm{i} z}$. Dan wordt dit een Laurentreeks in q (machtreeks in q en $1/q$):

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n. \tag{4.8}$$

Deze representatie van f noemt men de *q-expansie* van f. Als z naar i∞ neigt, dan zal $2\pi \mathrm{i} z \to -\infty$ en dus $q = \mathrm{e}^{2\pi \mathrm{i} z} \to 0$. Begrensdheid van f voor $z \to \mathrm{i}\infty$ impliceert dus dat de q-expansie begrensd blijft rondom nul. Een term q^n met $n < 0$ geeft een pool in $q = 0$, hetgeen in strijd is met begrensdheid aldaar. De conclusie is dat de q-expansie van een modulaire vorm geen negatieve q-machten kan bevatten. De Laurentreeks (4.8) is dus in feite de machtreeks

$$f(z) = \sum_{n=0}^{\infty} a_n q^n. \tag{4.9}$$

4.4 Spitsvormen

Spitsvormen zijn een subklasse van modulaire vormen, gedefinieerd aan de hand van zeker asymptotisch gedrag. Modulaire vormen die loodrecht staan op spitsvormen noemen we Eisensteinreeksen. De ruimte van modulaire vormen is op deze manier een product van de ruimtes van spitsvormen en Eisensteinreeksen. Alvorens te definiëren wat een spitsvorm is moet eerst de spits worden gedefinieerd.

Spitsen

Omdat modulaire vormen holomorf zijn in $\mathbb{H}$, zijn ze uit te breiden tot een gebied daarbuiten en is de waarde in i∞ en op $\mathbb{Q}$ eenduidig bepaald. Deze randpunten geven samen met $\mathbb{H}$ het *uitgebreide bovenhalfvlak* dat we hier noteren met $\overline{\mathbb{H}}$:

$$\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\} \tag{4.10}$$

Het punt $i\infty$ noteren we doorgaans gewoon met ∞. De fractionele lineaire transformaties $z \longmapsto \frac{az+b}{cz+d}$ breiden zich ook uit naar $\overline{\mathbb{H}}$ als we definieren dat

$$\gamma(-d/c) = \frac{a(-d/c)+b}{c(-d/c)+d} = \infty, \qquad \gamma \cdot \infty = \frac{a \cdot \infty + b}{c \cdot \infty + d} = \frac{a}{c}; \qquad (\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

Merk op dat $\gamma \in SL_2(\mathbb{Z})$ de ruimte $\mathbb{H}$ afbeeldt op $\mathbb{H}$ en de ruimte van randpunten $\mathbb{P}^1(\mathbb{Q})$ afbeeldt op $\mathbb{P}^1(\mathbb{Q})$. Deze eigenschap geldt dus ook voor alle congruentieondergroepen $\Gamma < SL_2(\mathbb{Z})$.

We noemen twee punten $x, y \in \mathbb{P}^1(\mathbb{Q})$ *equivalent* over een groep Γ als er een $\gamma \in \Gamma$ bestaat zodanig dat $\gamma x = y$. Dit is een equivalentierelatie en we noteren met C_Γ de verzameling equivalentieklassen, die $\mathbb{P}^1(\mathbb{Q})$ dus partitioneert. Een element van C_Γ noemen we een *spits*. We geven de volgende beweringen zonder bewijs.

Propositie 4.4.1. *Als $\Gamma < SL_2(\mathbb{Z})$ een congruentieondergroep is, dan is het aantal spitsen $|C_\Gamma|$ altijd eindig.*

Propositie 4.4.2. *Voor het aantal spitsen voor de modulaire groep geldt: $\left|C_{SL_2(\mathbb{Z})}\right| = 1$. Met andere woorden, de actie van $SL_2(\mathbb{Z})$ op $\mathbb{P}^1(\mathbb{Q})$ is transitief, oftewel voor alle $x, y \in \mathbb{P}^1(\mathbb{Q})$ bestaat er een $\gamma \in SL_2(\mathbb{Z})$ zodanig dat $\gamma x = y$.*

Als representant voor de spits in $C_{SL_2(\mathbb{Z})}$ nemen we vaak ∞.

Spitsvormen

Binnen de modulaire vormen is onderscheid te maken of ze al dan niet nul zijn in ∞, dit onderscheid zal later belangrijk worden. Stel dat een modulaire vorm f over $SL_2(\mathbb{Z})$ waarde nul heeft in ∞. Dan geeft de modulariteitseigenschap (4.7) dat

$$f(a/c) = f(\gamma \cdot \infty) = (cz+d)^k f(\infty) = 0$$

Dit laat zien dat elke modulaire vorm over $SL_2(\mathbb{Z})$ die nul is in ∞, ook verdwijnt op de rest van $\mathbb{P}^1(\mathbb{Q})$. Het is dus een modulaire vorm die "verdwijnt op de spits". Dit type modulaire vorm geven we een speciale naam.

Definitie 4.4.3 (Spitsvorm)**.** Een modulaire vorm f over $SL_2(\mathbb{Z})$ heet een *spitsvorm* als f waarde nul heeft op $\mathbb{P}^1(\mathbb{Q})$. Dit is equivalent met de bewering dat in de q-expansie

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

de constante coëfficiënt a_0 nul is.

4.5 Modulaire vormen van niveau N

Tot nog toe hebben we alleen gekeken naar modulaire vormen over $SL_2(\mathbb{Z})$. Het is echter ook mogelijk dat een holomorfe functie f op $\mathbb{H}$ weliswaar modulair gedrag vertoont,

maar slechts voor die γ die bevat zijn in een congruentieondergroep Γ van $SL_2(\mathbb{Z})$. We spreken dan over modulaire vormen over congruentieondergroepen, en net zoals congruentieondergroepen Γ een niveau N hebben, spreken we ook van modulaire vormen van een gegeven niveau N. Ook voor congruentieondergroepen bestaan spitsvormen; dat zijn wederom modulaire vormen die verwdijnen op $\mathbb{P}^1(\mathbb{Q})$. Merk echter op dat er nu meer spitsen zijn en ∞ er daar één van is, waardoor de eigenschap dat $f(\infty) = 0$ niet meer voldoende is om f te laten verdwijnen op $\mathbb{P}^1(\mathbb{Q})$.

Definitie 4.5.1 (Modulaire vorm van niveau N)**.** Zij $N \in \mathbb{N}_{\geq 2}$ en $k \in \mathbb{N}_0$. Een *modulaire vorm van gewicht k en niveau N* (of een modulaire vorm van gewicht k over $\Gamma_0(N)$) is een holomorfe functie f op $\mathbb{H}$ die begrensd blijft voor $z \to \mathbb{P}^1(\mathbb{Q})$ en waarvoor

$$f(\gamma z) = (cz + d)^k f(z) \tag{4.11}$$

voor alle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Een modulaire vorm f van gewicht k en niveau N wordt een *spitsvorm* genoemd als bovendien geldt dat $f(z) = 0$ voor $z \in \mathbb{P}^1(\mathbb{Q})$, oftewel dat f verdwijnt in alle spitsen in $C_{\Gamma_0(N)}$.

4.6 Ruimten van modulaire vormen

We voeren de notatie $\mathfrak{M}$ in voor de verzameling van alle modulaire vormen over $SL_2(\mathbb{Z})$. Deze verdelen we in ruimtes $\mathfrak{M}_k$ voor $k \in \mathbb{N}_0$, voor de ruimtes van modulaire vormen over $SL_2(\mathbb{Z})$ van gewicht k. Voor elk niveau N geven we bovendien de ruimte van alle modulaire vormen van gewicht k over $\Gamma_0(N)$ de naam $\mathfrak{M}_k(\Gamma_0(N))$, of korter, $\mathfrak{M}_k(N)$.

Stel dat f een modulaire vorm van gewicht k en niveau N is. Dan geldt dus per definitie voor alle $\gamma \in \Gamma_0(N)$ dat

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

Voor alle $\lambda \in \mathbb{C}$ geldt dan automatisch dezelfde eigenschap voor $\lambda \cdot f$. Dit laat zien dat $\lambda \cdot f$ ook een modulaire vorm van gewicht k over Γ is. Laat nu ook g een modulaire vorm zijn, van hetzelfde gewicht k, maar van niveau M. Dan geldt dat f en g beide modulair zijn op elke congruentieondergroep die $\Gamma_0(M) \cap \Gamma_0(N)$ bevat, en in het bijzonder dus over $\Gamma_0(\mathrm{kgv}(N, M))$, en dat daardoor ook $f + g$ modulair is van gewicht k en niveau $\mathrm{kgv}(N, M)$. Als $N = M$, dan laat dit zien dat als f en g modulair zijn van gewicht k en niveau N, dat $f + g$ dat dan ook is. De conclusie is

Propositie 4.6.1. *De ruimte $\mathfrak{M}_k(\Gamma_0(N))$ van modulaire vormen van gewicht k en niveau N is een vectorruimte over $\mathbb{C}$.*

Laat nu f een modulaire vorm van gewicht k en niveau N zijn en g een modulaire vorm van gewicht ℓ en niveau M. Dan geldt voor alle $\gamma \in \Gamma_0(\mathrm{kgv}\, N, M)$ dat

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \qquad g\left(\frac{az+b}{cz+d}\right) = (cz+d)^\ell g(z),$$

en dus

$$(f \cdot g)\left(\frac{az+b}{cz+d}\right) = (cz+d)^{k+\ell}(f \cdot g)(z),$$

dus $f \cdot g$ is een modulaire vorm van gewicht $k+\ell$ en niveau $\mathrm{kgv}(N, M)$. Hieruit concluderen we het volgende.

Propositie 4.6.2. *De ruimte $\mathfrak{M}(\Gamma_0(N))$ van alle modulaire vormen van niveau N is een gegradeerde ring:*

$$\mathfrak{M}(\Gamma_0(N)) = \bigoplus_{k\in\mathbb{N}} \mathfrak{M}_k(\Gamma_0(N)).$$

Voor de matrix $\gamma = -\mathbb{I}_{2\times 2} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, die in alle $\Gamma_0(N)$ voorkomt, ziet de modulariteitseigenschap eruit als

$$f(z) = (-1)^k f(z).$$

Dit laat zien dat de enige modulaire vorm van oneven gewicht ten opzichte van de groep $\Gamma_0(N)$ de nulvorm is.

De spitsvormen van gewicht k en niveau N vormen een deelruimte van $\mathfrak{M}_k(\Gamma_0(N))$ en wordt genoteerd met $\mathfrak{S}_k(\Gamma_0(N))$. De keuze voor de letter S is afkomstig van het Duitse "Spitzenform". Het deel van $\mathfrak{M}_k$ dat loodrecht op $\mathfrak{S}_k$ staat, wordt ook wel de ruimte van *Eisensteinreeksen* van gewicht k genoemd en noteren we met $\mathfrak{E}_k$. Hierbij wordt "loodrecht" opgevat ten aanzien van het *Petersson-inproduct*. We hebben dus

$$\mathfrak{M}_k = \mathfrak{E}_k \oplus \mathfrak{S}_k. \tag{4.12}$$

Een willekeurige modulaire vorm vermenigvuldigd met een spitsvorm levert een spitsvorm op, dus ook $\mathfrak{S} = \bigoplus_{k\in\mathbb{N}} \mathfrak{S}_k$ is een gegradeerde ring.

4.7 Modulaire vormen met karakter

Behalve modulaire vormen over $\Gamma_0(N)$ te bekijken, kunnen we ook kijken naar modulaire vormen over de ondergroep $\Gamma_1(N)$ van $\Gamma_0(N)$. Doordat de groep kleiner is, zijn er meer modulaire vormen: $\mathfrak{M}_k(\Gamma_1(N)) \supset \mathfrak{M}_k(\Gamma_0(N))$. Het blijkt dat modulaire vormen voor $\Gamma_1(N)$ ook modulaire vormen zijn over $\Gamma_0(N)$, mits we de definitie van modulaire vorm verruimen door het Dirichletkarakter of *Nebentypus* in te voeren. We definiëren daarom hier de modulaire vormen met karakter; voor ons is dat de ruimste variant van modulaire vormen.

Merk op dat als $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, dan is $c \equiv 0 \bmod N$ en dus $ad \equiv 1 \bmod N$, oftewel $a \equiv d^{-1} \bmod N$. Definieer een karakter ε op $\Gamma_0(N)$ volgens het voorschrift $\varepsilon(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = \varepsilon(d)$.

Definitie 4.7.1 (Modulaire vorm met karakter)**.** Zij $N \in \mathbb{N}$ en $k \in \mathbb{N}_0$, en zij $\varepsilon \in \mathscr{D}(N, \mathbb{C})$ een Dirichletkarakter modulo N. Een holomorfe functie $f : \overline{\mathbb{H}} \longrightarrow \mathbb{C}$ is een

modulaire vorm van niveau N, gewicht k en karakter ε als voor alle $\gamma \in \Gamma_0(N)$ geldt dat

$$f(\gamma z) = \varepsilon(d)(cz+d)^k f(z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Als $f(z) = 0$ voor alle $z \in \mathbb{P}^1(\mathbb{Q})$, is f een spitsvorm. Als f loodrecht staat op de ruimte van spitsvormen dan noemen we f een Eisensteinreeks en schrijven we $f \in \mathfrak{E}_k(N, \varepsilon)$.

We schrijven $\mathfrak{M}_k(N, \varepsilon)$, $\mathfrak{E}_k(N, \varepsilon)$ en $\mathfrak{S}_k(N, \varepsilon)$ voor de ruimte van respectievelijk modulaire vormen, Eisensteinreeksen en spitsvormen van niveau N, gewicht k en karakter ε.

Opmerking 4.7.2. Er geldt dus per definitie dat $\mathfrak{M}_k(N, \varepsilon) = \mathfrak{E}_k(N, \varepsilon) \oplus \mathfrak{S}_k(N, \varepsilon)$.

Als ε het triviale karakter is, dan is $\mathfrak{M}_k(N, \varepsilon) = \mathfrak{M}_k(\Gamma_0(N))$. Ook geldt

$$\mathfrak{M}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon \in \mathscr{D}(N, \mathbb{C})} \mathfrak{M}_k(N, \varepsilon), \tag{4.13}$$

$$\mathfrak{E}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon \in \mathscr{D}(N, \mathbb{C})} \mathfrak{E}_k(N, \varepsilon). \tag{4.14}$$

$$\mathfrak{S}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon \in \mathscr{D}(N, \mathbb{C})} \mathfrak{S}_k(N, \varepsilon), \tag{4.15}$$

Alle ruimtes $\mathfrak{M}_k(N, \varepsilon)$, $\mathfrak{E}_k(N, \varepsilon)$, en $\mathfrak{S}_k(N, \varepsilon)$ zijn $\mathbb{C}$-vectorruimten.

Er bestaan verbanden tussen modulaire vormen over verschillende groepen, hiervan laten we nu een paar voorbeelden zien die we later nodig hebben.

Lemma 4.7.3. *Stel dat f een modulaire vorm van gewicht k en karakter ε is ten opzichte van de groep $\Gamma_0(L, M)$ uit (4.6). Definieer g door $g(z) = f(Mz)$. Dan is g eveneens een gewicht k-modulaire vorm met karakter ε, maar ten opzichte van de groep $\Gamma_0(LM)$.*

Bewijs. In de modulariteitseigenschap (4.7), vervang z door Mz en haal een factor M uit de teller naar voren.

$$f\left(M \frac{az + b/M}{cMz + d}\right) = \varepsilon(d)(cMz+d)^k f(Mz).$$

Kies $c' = Mc$ en $b' = b/M$, dan zal $b' \in \mathbb{Z}$ en $LM \mid c'$, en zal

$$f\left(M \frac{az + b'}{c'z + d}\right) = \varepsilon(d)(c'z+d)^k f(Mz),$$

oftewel

$$g\left(\frac{az + b'}{c'z + d}\right) = \varepsilon(d)(c'z+d)^k g(z).$$

hetgeen precies de modulariteitseigenschap is voor g. We vinden dus dat g modulair is over

$$\left\{ \begin{pmatrix} a & b/M \\ Mc & d \end{pmatrix} \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(L, M) \right\} = \Gamma_0(LM).$$

□

Merk op dat als f geschreven is in zijn q-expansie, en $f(z) = F(q)$, dan is $f(Mz) = F(q^M)$. Het volgende lemma is vergelijkbaar met, en volgt uit, lemma 4.7.3 hierboven.

Lemma 4.7.4. *Stel dat f een modulaire vorm van gewicht k en karakter ε is ten opzichte van de groep $\Gamma_0(M)$. Definieer g door $g(z) = f(tz)$, voor $t \in \mathbb{N}$. Dan is g eveneens een gewicht k-modulaire vorm met karakter ε, maar ten opzichte van de groep $\Gamma_0(tM)$.*

Bewijs. Omdat f modulair is over $\Gamma_0(M)$, is f ook modulair over de kleinere groep $\Gamma_0(t, M)$ en is lemma 4.7.3 van toepassing. □

In het volgende hoofdstuk gaan we enkele Eisensteinreeksen expliciet geven.

Hoofdstuk 5

Eisensteinreeksen

In dit hoofdstuk bekijken we een belangrijk voorbeeld van modulaire vormen over $SL_2(\mathbb{Z})$, namelijk de Eisensteinreeksen. We beginnen bij de standaard Eisensteinreeks G_k, een modulaire vorm over $SL_2(\mathbb{Z})$. Daarna bekijken we meer algemene Eisensteinreeksen over $\Gamma_0(N)$ en Eisensteinreeksen met een karakter ε. We geven de basis van de ruimtes $\mathfrak{E}_k(N,\varepsilon)$ zoals bewezen in [Miy].

5.1 De standaard Eisensteinreeks G_k

We beginnen met de definitie van de standaard Eisensteinreeks van gewicht k en geven daarna de q-expansie hiervan.

Definitie

Voor alle even $k \geq 4$, definieer de functie $G_k : \mathbb{H} \longrightarrow \mathbb{C}$ gegeven door het voorschrift

$$G_k(z) = \sum_{m,n\in\mathbb{Z}}^{\star} \frac{1}{(mz+n)^k}. \tag{5.1}$$

De $\star$ boven het somteken geeft aan dat de som wordt genomen over die $m, n \in \mathbb{Z}$ waarvoor $m+nz$ niet nul is, oftewel alle paren (m,n) met weglating van $(0,0)$. Deze som convergeert absoluut voor $k > 2$ en is 0 voor oneven k. Daarom wordt k even genomen en tenminste 4. De absolute convergentie stelt ons bovendien in staat de sommatievolgorde te veranderen en laat bovendien zien dat G_k holomorf is. Voor G_k gelden de volgende gelijkheden.

$$G_k(z+1) = \sum_{(m,n)}^{\star} \frac{1}{(m(z+1)+n)^k} = \sum_{(m,n)}^{\star} \frac{1}{(mz+(m+n))^k} = \sum_{(m,n')}^{\star} \frac{1}{(mz+n')^k} = G_k(z),$$

$$G_k(-1/z) = \sum_{(m,n)}^{\star} \frac{1}{(m(-1/z)+n)^k} = \sum_{(m,n)}^{\star} \frac{z^k}{(m-nz)^k} = \sum_{(m',n')}^{\star} \frac{z^k}{(m'z+n')^k} = G_k(z).$$

De functie G_k voldoet dus aan de transformaties (4.4) en is dus modulair ten opzichte van $SL_2(\mathbb{Z})$. Voor $z \longrightarrow \infty$ zullen de termen waarbij $n \neq 0$ naar nul dalen waardoor het gedrag in ∞ goed is. De conclusie is dat G_k een gewicht k-modulaire vorm over $SL_2(\mathbb{Z})$ is: $G_k \in \mathfrak{M}_k$.

De q-expansie van G_k

De Eisensteinreeks E_k heeft een elegante q-expansie die we in het vervolg veelvuldig nodig hebben. De afleiding van de q-expansie voor G_k is een bekende in de wereld van modulaire vormen, deze is dan ook terug te vinden in veel boeken over modulairevormtheorie. We volgen hier een aanpak vergelijkbaar met die in [Iwa, §1.4]. De afleiding begint bij een gelijkheid uit de analyse.

Lemma 5.1.1. *Voor $z \in \mathbb{H}$ geldt*

$$\pi \frac{\cos(\pi z)}{\sin(\pi z)} = \lim_{n\to\infty} \sum_{k=-n}^{n} \frac{1}{z-k}. \tag{5.2}$$

Bewijs. Om deze gelijkheid te bewijzen, merk ten eerste op dat beide leden enkelvoudige polen hebben in $\mathbb{Z}$ en enkelvoudige nulpunten op $\mathbb{Z} + 1/2$. Het quotiënt

$$\frac{\pi \cos(\pi z)/\sin(\pi z)}{\lim_{n\to\infty} \sum_{k=-n}^{n} \frac{1}{z-k}}.$$

heeft dus geen polen en nulpunten. Nu willen we laten zien dat de waarde van deze uitdrukking begrensd is op het gebied $\mathbb{H}_\varepsilon = \{z \in \mathbb{C}\colon \varepsilon < \Im z < 1/\varepsilon\}$. Het is voldoende te laten zien dat de teller begrensd is van boven. Merk op dat $z \in \mathbb{H}_\varepsilon$ betekent dat $-1/\varepsilon < \Re(\mathrm{i}z) < -\varepsilon$, en dus

$$\mathrm{e}^{-\pi/\varepsilon} < \left|\mathrm{e}^{\pi \mathrm{i} z}\right| < \mathrm{e}^{-\pi\varepsilon}, \qquad \mathrm{e}^{\pi\varepsilon} < \left|\mathrm{e}^{-\pi \mathrm{i} z}\right| < \mathrm{e}^{\pi/\varepsilon}.$$

Hieruit volgt op zijn beurt dat

$$|\cos(\pi z)| = \left|\mathrm{e}^{\pi \mathrm{i} z} + \mathrm{e}^{-\pi \mathrm{i} z}\right|/2 < \mathrm{e}^{-\pi\varepsilon} + \mathrm{e}^{\pi/\varepsilon}, \qquad |\sin(\pi z)| = \left|\mathrm{e}^{\pi \mathrm{i} z} - \mathrm{e}^{-\pi \mathrm{i} z}\right|/2 > \mathrm{e}^{-\pi/\varepsilon} - \mathrm{e}^{\pi/\varepsilon},$$

hetgeen laat zien dat de teller begrensd is in $\mathbb{H}_\varepsilon$ en dus de hele uitdrukking begrensd. Omdat de uitdrukking holomorf is, is deze nu volgens de stelling van Liouville constant. Gelijkheid kan nu worden aangetoond door de waarden te vergelijken in een willekeurig punt dat geen nulpunt of pool is. Kies $z = 1/4$. Dan is $\pi \cot(\pi z) = \pi$ en

$$\lim_{n\to\infty} \sum_{k=-n}^{n} \frac{1}{1/4 - k} = 4 \sum_{k=1}^{\infty} \frac{(-1)^k}{2k+1}.$$

Deze laatste uitdrukking is de *Madhava−Leibnizreeks* voor π. □

Het linkerlid kan, voor $z \in \mathbb{H}$, ook geschreven worden als

$$\begin{aligned}
\pi\frac{\cos(\pi z)}{\sin(\pi z)} &= \pi\frac{(\mathrm{e}^{\pi \mathrm{i} z}+\mathrm{e}^{-\pi \mathrm{i} z})/2}{(\mathrm{e}^{\pi \mathrm{i} z}-\mathrm{e}^{-\pi \mathrm{i} z})/(2\mathrm{i})} \\
&= \pi\mathrm{i}\frac{\mathrm{e}^{2\pi \mathrm{i} z}+1}{\mathrm{e}^{2\pi \mathrm{i} z}-1} \\
&= \pi\mathrm{i}\left(\frac{\mathrm{e}^{2\pi \mathrm{i} z}-1}{\mathrm{e}^{2\pi \mathrm{i} z}-1}+\frac{2}{\mathrm{e}^{2\pi \mathrm{i} z}-1}\right) \\
&= \pi\mathrm{i}+2\pi\mathrm{i}\frac{1}{\mathrm{e}^{2\pi \mathrm{i} z}-1} \\
&= \pi\mathrm{i}-2\pi\mathrm{i}\sum_{\ell=0}^{\infty}\mathrm{e}^{2\pi \mathrm{i}\ell z} \\
&= -\pi\mathrm{i}-2\pi\mathrm{i}\sum_{\ell=1}^{\infty}\mathrm{e}^{2\pi \mathrm{i}\ell z}.
\end{aligned}$$

Combineren we beide uitwerkingen van $\pi\frac{\cos(\pi z)}{\sin(\pi z)}$ en voegen we aan beide kanten een minteken toe, dan krijgen we

$$\sum_{n\in\mathbb{Z}}\frac{1}{n-z} = \pi\mathrm{i}+2\pi\mathrm{i}\sum_{\ell=1}^{\infty}\mathrm{e}^{2\pi \mathrm{i}\ell z}.$$

Hierbij moet de som over $\mathbb{Z}$ worden gelezen als de limiet van sommen over symmetrische intervallen $[-N, N]$. Differentieer deze gelijkheid nu $k-1$ keer naar z.

$$(k-1)!\sum_{n\in\mathbb{Z}}\frac{1}{(n-z)^k} = 2\pi\mathrm{i}\sum_{\ell=1}^{\infty}(2\pi\mathrm{i}\ell)^{k-1}\mathrm{e}^{2\pi \mathrm{i}\ell z},$$

oftewel

$$\sum_{n\in\mathbb{Z}}\frac{1}{(n+z)^k} = -\frac{(2\pi\mathrm{i})^k}{(k-1)!}\sum_{\ell=1}^{\infty}\ell^{k-1}q^{\ell}. \tag{5.3}$$

Nu nemen we de definitie van de Eisensteinreeks G_k uit definitie 5.1 erbij om met behulp van (5.3) de q-expansie hiervan te bepalen. We maken hierbij gebruik van het feit dat k even is.

$$\begin{aligned}
G_k(z) &= \sum_{m,n\in\mathbb{Z}}^{\star}\frac{1}{(mz+n)^k} \\
&= 2\sum_{n=1}^{\infty}\frac{1}{n^k}+2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^k} \\
&= 2\zeta(k)-2\frac{(2\pi\mathrm{i})^k}{(k-1)!}\sum_{n=1}^{\infty}\sum_{\ell=1}^{\infty}\ell^{k-1}q^{\ell n}.
\end{aligned}$$

Neem nu alle termen met dezelfde waarde m voor ℓn bij elkaar. Als (ℓ, n) alle paren doorloopt met $\ell n = m$, dan doorloopt ℓ alle delers van m. We krijgen dus

$$G_k(z) = 2\zeta(k)-\frac{2(2\pi\mathrm{i})^k}{(k-1)!}\sum_{m=1}^{\infty}\sigma_{k-1}(m)q^m. \tag{5.4}$$

Dit geeft de q-expansie van G_k. Deze gaan we in het vervolg nog uitgebreid nodig hebben. De functie σ_{k-1} is dezelfde als die gedefinieerd in (3.1). Om te voorkomen dat de constanten in deze q-expansie verdere berekeningen onnodig bemoeilijken, definiëren we een genormaliseerde versie E_k van G_k, waarbij we de coëfficiënt voor q gelijk stellen aan 1.

$$E_k(z) := c_k + \sum_{m=1}^{\infty} \sigma_{k-1}(m) q^m, \qquad c_k = -\frac{(k-1)!\,\zeta(k)}{(2\pi i)^k}. \tag{5.5}$$

Deze genormaliseerde Eisensteinreeksen gaan we nog met regelmaat terugzien. Let wel op: de meeste literatuur normaliseert zodat de *constante* coëfficiënt gelijk is aan 1, maar wij stellen dus de *lineaire* coëfficiënt op 1. Merk op dat alle coëfficiënten, met uitzondering van de constante, geheel zijn.

5.2 Eisensteinreeksen met karakter

We beginnen weer bij de som uit definitie 5.1, maar voegen nu Dirichletkarakters toe aan de teller. We definiëren de algemene Eisensteinreeks $G_{k,\chi,\psi}$ als volgt.

Definitie 5.2.1. Zij χ en ψ twee primitieve Dirichletkarakters modulo respectievelijk L en M. De Eisensteinreeks $G_{k,\chi,\psi}$ van gewicht k wordt gegeven door

$$G_{k,\chi,\psi}(z) = \sum_{m,n\in\mathbb{Z}}^{\star} \frac{\chi(m)\psi(n)}{(mz+n)^k}. \tag{5.6}$$

Dan is $G_{k,\chi,\psi}$ modulair ten opzichte van de congruentieondergroep $\Gamma_0(L,M)$ gedefinieerd in (4.6).

Lemma 5.2.2. *De Eisensteinreeks $G_{k,\chi,\psi}$ is een modulaire vorm ten opzichte van de groep $\Gamma_0(L,M)$ met karakter $\varepsilon = \chi/\psi$.*

Bewijs. We volgen hier dezelfde methode als in [Miy, §7.1]. Laat $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(L,M)$ en definieer de functies m' en n' van m en n als $m' = am + cn$ en $n' = bm + dn$. Dan is

$$\chi(m') = \chi(am+cn) = \chi(am) = \chi(a)\chi(m), \quad \text{want } L \mid c, \tag{5.7}$$

$$\psi(n') = \psi(bm+dn) = \psi(dn) = \psi(d)\psi(n), \quad \text{want } M \mid b, \tag{5.8}$$

$$m\gamma z + n = m\frac{az+b}{cz+d} + n = \frac{am+cn}{cz+d} z + bm + dn = (cz+d)^{-1} m' z + n'. \tag{5.9}$$

We gebruiken nu al deze gelijkheden om de modulariteitseigenschap voor $G_{k,\chi,\psi}$ aan te tonen. Hierbij gebruiken we ook het feit dat $(m,n) \longmapsto (m',n')$ een permutatie van $\mathbb{Z}\times\mathbb{Z}$ is, wat ons in staat stelt de sommatie over m,n te vervangen door een sommatie over

m', n'.

$$\begin{aligned} G_{k,\chi,\psi}(\gamma z) &= \sum_{m,n}^{\star} \chi(m)\psi(n)(m\gamma z + n)^{-k} \\ &= \sum_{m,n}^{\star} \frac{\chi(m')}{\chi(a)} \frac{\psi(n')}{\psi(d)} (cz+d)^k (m'z+n')^{-k} \\ &= \chi(a)^{-1}\psi(d)^{-1}(cz+d)^k \sum_{m,n}^{\star} \chi(m')\psi(n')(m'z+n')^{-k} \\ &= \chi(d)/\psi(d)(cz+d)^k \sum_{m',n'}^{\star} \chi(m')\psi(n')(m'z+n')^{-k} \\ &= \varepsilon(d)(cz+d)^k G_{k,\chi,\psi}(z). \end{aligned}$$

Merk op dat we ook hebben gebruikt dat $a \equiv d^{-1}$ modulo LM, wat eenvoudig volgt uit het feit dat $\gamma \in \Gamma_0(L, M)$ en dus $LM \mid bc$. □

Neem nu $\gamma = -\mathbb{I}_{2\times 2} \in \Gamma_0(L, M)$. Dan volgt:

$$G_{k,\chi,\psi}(z) = (\chi/\psi)(-1) \cdot (-1)^k G_{k,\chi,\psi}(z).$$

Dit laat zien dat $G_{k,\chi,\psi}(z) = 0$ zodra $\chi(-1)\psi(-1) \neq (-1)^k$. We mogen dus nu aannemen dat $\chi(-1)\psi(-1) = (-1)^k$.

We willen nu de q-expansie van $G_{k,\chi,\psi}$ afleiden, en maken net als bij de berekening voor G_k gebruik van (5.3). Onderstaande methode is dezelfde als die in [Miy, p. 270].

$$\begin{aligned} G_{k,\chi,\psi}(z) &= \sum_{m,n\in\mathbb{Z}}^{\star} \frac{\chi(m)\psi(n)}{(mz+n)^k} \\ &= C + 2\sum_{m=1}^{\infty} \left(\chi(m) \sum_{n=-\infty}^{\infty} \frac{\psi(n)}{(mz+n)^k} \right) \end{aligned}$$

We splitsen de som in een positief en een negatief deel. Daarna gebruiken we de aanname dat $\chi(-1)\psi(-1) = (-1)^k$ om een factor $\chi(-1)\psi(-1)(-1)^k$ te kunnen wegstrepen in het negatieve deel, waardoor de twee delen gelijk worden. Daarna is $\chi(m)$ uit de som gehaald.

De binnenste som is gelijk aan

$$\begin{aligned}
\sum_{n=-\infty}^{\infty} \psi(n)(mz+n)^{-k} &= \sum_{a=0}^{M-1} \psi(a) \sum_{\ell=-\infty}^{\infty} (mz+(M\ell+a))^{-k} \\
&= M^{-k} \sum_{a=0}^{M-1} \psi(a) \sum_{\ell=-\infty}^{\infty} \left(\frac{mz+a}{M}+\ell\right)^{-k} \\
&= M^{-k} \frac{(-2\pi\mathrm{i})^k}{(k-1)!} \sum_{a=0}^{M-1} \psi(a) \sum_{n=1}^{\infty} n^{k-1} \mathrm{e}^{2\pi\mathrm{i}n\frac{mz+a}{M}} \\
&= \frac{(-2\pi\mathrm{i})^k}{M^k(k-1)!} \sum_{n=1}^{\infty} \left(\sum_{a=0}^{M-1} \psi(a) \mathrm{e}^{2\pi\mathrm{i}na/M} \right) n^{k-1} \mathrm{e}^{2\pi\mathrm{i}nmz/M} \\
&= \frac{(-2\pi\mathrm{i})^k}{M^k(k-1)!} W(\psi) \sum_{n=1}^{\infty} \overline{\psi}(n) n^{k-1} \mathrm{e}^{2\pi\mathrm{i}nmz/M},
\end{aligned}$$

dus de gehele som is een constante maal

$$C + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \chi(m)\overline{\psi}(n) n^{k-1} \mathrm{e}^{2\pi\mathrm{i}nmz/M}. \tag{5.10}$$

Deze constante hebben we niet nodig en vergeten we daarom direct; we stellen $G_{k,\chi,\psi}$ gelijk aan uitdrukking (5.10). Verwisselen we nu de sommatievolgorde door termen met dezelfde waarde voor mn bij elkaar te zetten, dan krijgen we

$$\begin{aligned}
G_{k,\chi,\psi}(z) &= C + \sum_{s=1}^{\infty} \left(\sum_{d|s} \chi(d)\overline{\psi}(s/d) d^{k-1} \right) e^{2\pi i s z/M} \\
&= C + \sum_{s=1}^{\infty} a_s q^{s/M},
\end{aligned} \tag{5.11}$$

waarbij

$$a_n = \sum_{d|n} \chi(d)\overline{\psi}(n/d) d^{k-1}. \tag{5.12}$$

De exacte waarde van de constante C is hieruit afleidbaar, maar hebben we niet nodig en die afleiding laten we daarom achterwege. Merk op dat $a_1 = 1$, omdat $\chi(1) = \psi(1) = 1$, dus deze uitdrukking is genormaliseerd. Er staat wel nog een noemer M in de exponent van q die we liever kwijt zijn. We voeren daarom als we de basis van $\mathfrak{E}_k(N,\varepsilon)$ gaan geven, nieuwe Eisensteinreeksen in waarbij we deze factor $1/M$ in de exponent weglaten. We geven eerst een formule voor de dimensie van de beoogde ruimte.

5.3 Dimensie van ruimtes van Eisensteinreeksen

Ons doel is om een basis te geven van de ruimtes $\mathfrak{E}_k(N,\varepsilon)$ voor willekeurige N en ε. We geven hier eerst een formule voor de dimensie van deze ruimtes; dit is een handige methode om de basis te controleren. We geven hier alleen de formules voor $\varepsilon = 1$. Deze zijn ook te vinden in onder andere [Ste, §6.1].

Stelling 5.3.1. *De dimensie van de ruimte $\mathfrak{E}_2(\Gamma_0(N))$ van gewicht k-Eisensteinreeksen van niveau N en triviaal karakter, is*

$$\dim \mathfrak{E}_k(\Gamma_0(N)) = \sum_{d \mid N} \phi(\mathrm{ggd}(d, N/d)) \quad \textit{als } k \geq 3, \tag{5.13}$$

waarbij we stellen dat $\phi(1) = 1$. In het geval $k = 2$ is er één basisvorm minder:

$$\dim \mathfrak{E}_2(\Gamma_0(N)) = \left(\sum_{d \mid N} \phi(\mathrm{ggd}(d, N/d)) \right) - 1. \tag{5.14}$$

Voor algemene karakters worden de formules een stuk ingewikkelder. Deze geven we daarom hier niet, ze zijn wel te vinden in [Ste, §6.3]. Wel volgt uit de formules het volgende.

Stelling 5.3.2. *Voor alle $k \in \mathbb{N}, N \in \mathbb{N}$ en $\varepsilon \in \mathscr{D}(N, \mathbb{C})$ is de ruimte $\mathfrak{E}_k(N, \varepsilon)$ eindigdimensionaal.*

Onze bases worden derhalve alle eindig.

5.4 De basis van de ruimte van Eisensteinreeksen

We hebben gezien dat $G_{k,\chi,\psi}(z) = C + \sum_n a_n q^{n/M}$ modulair is ten opzichte van $\Gamma_0(L, M)$. We definiëren nu een nieuwe genormaliseerde Eisensteinreeks zonder $1/M$ in de exponent en bewijzen daarvan ook modulariteit, zij het ten opzichte van een andere modulaire groep, namelijk $\Gamma_0(LM)$. We definiëren de genormaliseerde Eisensteinreeks $E_{k,\chi,\psi}$ als volgt als functie van q.

Definitie 5.4.1 (Genormaliseerde Eisensteinreeks)**.** Zij χ en ψ twee primitieve Dirichletkarakters modulo respectievelijk L en M, en zij $k \in \mathbb{N}$. We definiëren de Eisensteinreeks van gewicht k voor de karakters χ en ψ als

$$E_{k,\chi,\psi}(q) = a_0 + \sum_{n=1}^{\infty} a_n q^n, \qquad \text{met } a_n = \sum_{d \mid n} \chi(d)\overline{\psi}(n/d) d^{k-1} \text{ voor } n \geq 1. \tag{5.15}$$

Merk op dat als $E_{k,\chi,\psi}$ opgevat wordt als functie van z, dan geldt dat

$$E_{k,\chi,\psi}(z) = G_{k,\chi,\psi}(Mz). \tag{5.16}$$

We halen nu lemma's 4.7.3 en 4.7.4 aan, die van toepassing zijn op $E_{k,\chi,\psi}$ vanwege (5.16). Lemma 4.7.3 zorgt ervoor dat $E_{k,\chi,\psi}$ modulair is ten opzichte van de groep $\Gamma_0(LM)$, en lemma 4.7.4 geeft dan dat $E_{k,\chi,\psi}(q^t)$ modulair is ten opzichte van $\Gamma_0(tLM)$. We krijgen als resultaat:

Stelling 5.4.2. *Zij χ en ψ twee primitieve Dirichletkarakters modulo $f_\chi = L$ en $f_\psi = M$ en zij $k \in \mathbb{N}$ zodanig dat $\chi(-1)\psi(-1) = (-1)^k$. Zij $t \in \mathbb{N}$. Dan is, behalve als $\chi = \psi = 1, k = 2$,*

$$E_{k,\chi,\psi}(q^t) \in \mathfrak{M}_k(tLM, \chi/\psi). \tag{5.17}$$

Als $\chi = \psi = 1$ en $k = 2$, en $E_2 = E_{k,\chi,\psi}$, dan is

$$E_2(q) - tE_2(q^t) \in \mathfrak{M}_2(\Gamma_0(t)). \tag{5.18}$$

Voor het gemak voeren we een notatie in voor beide van deze vormen. In het geval van reële karakters schrijven we

$$B_{k,\chi,\psi,t}(q) = E_{k,\chi,\psi}(q^t), \tag{5.19}$$
$$B_{2,1,1,t}(q) = E_2(q) - tE_2(q^t). \tag{5.20}$$

De coëfficienten in de q-expansie noemen we $\sigma_{k,\chi,\psi,t}$. Er geldt dus

$$B_{k,\chi,\psi,t}(q) = \sum_{n=0}^{\infty} \sigma_{k,\chi,\psi,t}(n) q^n. \tag{5.21}$$

Als χ en ψ reële primitieve karakters zijn, oftewel van de vorm ρ_m uit stelling 2.4.5, dan vervangen we het subscript ρ_m door m.

De q-expansie van de vorm in (5.18) verdient extra aandacht. De coëfficiënt van q^n in $E_2(q)$ is $\sigma(n)$, en de coëfficiënt in $-tE_2(q^t)$ is

$$\begin{cases} 0 & \text{als } t \nmid n, \\ -t\,\sigma(n/t) & \text{als } t \mid n. \end{cases}$$

De coëfficiënt van $B_{2,1,1,t}$ voor q^n is dus

$$\begin{cases} \sum_{d|n} d & \text{als } t \nmid n, \\ \sum_{d|n} d - \sum_{d|n/t} td = \sum_{d|n} d - \sum_{d|n,\, t|d} d = \sum_{d|n, t\nmid d} d & \text{als } t \mid n. \end{cases}$$

Als $t \nmid n$, geldt $t \nmid d$ voor elke deler d van n, en dus is het niet nodig onderscheid te maken tussen het al dan niet deelbaar zijn door t. De coëfficiënt van q^n in $B_{2,1,1,t}$ is dus gelijk aan

$$\sigma_{2,1,1,t}(n) = \sum_{d\,|\,n,\ t\nmid d} d = \sigma(w_t(n)).$$

Voorbeeld 5.4.3. De coëfficiënt van q^n in $B_{2,1,1,2}$ is de som der oneven delers van n en de coëfficiënt van q^n in $B_{2,1,1,4}$ is de som van die delers van n die geen viervoud zijn. De q-expansies van deze twee vormen zien er dus als volgt uit.

$$B_{2,1,1,2}(q) = 1 + q + \ q^2 + 4q^3 + \ q^4 + 6q^5 + \ 4q^6 + 8q^7 + \ q^8 + 13q^9 + \cdots,$$
$$B_{2,1,1,4}(q) = 1 + q + 3q^2 + 4q^3 + 3q^4 + 6q^5 + 12q^6 + 8q^7 + 3q^8 + 13q^9 + \cdots.$$

Merk op dat een modulaire vorm van een zeker niveau N ook een modulaire vorm is van elk niveau cN met $c \in \mathbb{N}$. Dit geeft ons voor elke denkbare Eisensteinreeks $B_{k,\chi,\psi,t}$ alle ruimten $\mathfrak{E}_k(N,\varepsilon)$ van Eisensteinreeksen waar deze een element van is. Toshitsune Miyake gaat verder en bewijst in zijn boek [Miy, §7.2] een voor ons belangrijk resultaat, ook vermeld in [Ste, §5.3], namelijk dat dit in zekere zin *alle* Eisensteinreeksen zijn.

Stelling 5.4.4. *De modulaire vormen $B_{k,\chi,\psi,t}$ met de eigenschap dat $f_\chi f_\psi t \mid N$ en $\chi/\psi = \varepsilon$, met uitzondering van $B_{2,1,1,1}$, vormen een basis van de ruimte $\mathfrak{E}_k(N,\varepsilon)$.*

De vorm $B_{2,1,1,1}$ is weggelaten omdat dit de nulvorm is. Laten we als voorbeeld een basis geven voor $\mathfrak{E}_2(\Gamma_0(4))$.

Voorbeeld 5.4.5. We hebben $N = 4, k = 2, \varepsilon = 1$. Stelling 5.4.4 geeft dat de basis van $\mathfrak{E}_2(\Gamma_0(4))$ precies die Eisensteinreeksen $B_{2,\chi,\psi,t}$ bevat met de eigenschap dat $\chi/\psi = 1$, oftewel $\chi = \psi$, en $f_\chi f_\psi t \mid 4$. Deze eigenschap impliceert dat $(f_\chi)^2 \mid 4$ en dus $f_\chi = 1$ of 2. Er zijn geen primitieve karakters van modulus 2, en dus moeten χ en ψ het triviale karakter zijn en is $f_\chi = f_\psi = 1$. Dit geeft $t = 1, 2$ of 4, en dat levert de vormen $B_{2,1,1,t}$ voor $t = 2$ en 4 op (want $B_{2,1,1,1} = 0$). De gevonden basis voor $\mathfrak{E}_2(\Gamma_0(4))$ bestaat dus uit de twee vormen

$$E_2(q) - 2E_2(q^2),$$
$$E_2(q) - 4E_2(q^4).$$

De dimensie van $\mathfrak{E}_2(\Gamma_0(4))$ is dus 2. Dit komt overeen met het resultaat van formule (5.14) in stelling 5.3.1 (herinner de conventie dat $\phi(1) = 1$).

$$\dim \mathfrak{E}_2(\Gamma_0(4)) = -1 + \phi(1) + \phi(2) + \phi(1) = 2.$$

Voor algemene niveaus $N \in \mathbb{N}$ en primitieve karakters $\varepsilon \in \mathscr{D}(N)$ kunnen we deze basis uitrekenen met onderstaand algoritme.

Algoritme 5.4.6 (Basisvormen in ruimte $\mathfrak{E}_2(N,\varepsilon)$)**.**

(i) Bepaal de primitieve voortbrengers g_i van $(\mathbb{Z}/N\mathbb{Z})^*$ uit paragraaf 2.2, en de ordes r_i van de g_i in $(\mathbb{Z}/N\mathbb{Z})^*$.

(ii) Schrijf het karakter ε in de vorm (2.6) door $\varepsilon(g_i)$ te bepalen voor alle g_i.

(iii) Maak nu de lijst $\mathscr{X}$ van alle karakters van modulus N. We noteren de karakters zoals in (2.6). Genereer alle producten $\prod_i \zeta_{r_i}^{a_i}$ waarbij voor elke exponent a_i geldt dat $0 \le a_i < r_i$. Dit geeft een lijst van lengte $\phi(N) = \prod_i r_i$.

(iv) Bepaal van elk karakter χ_j de conductor f_j uit definitie 2.1.4.

(v) Maak nu de paren karakters $(\chi_j, \overline{\varepsilon}\chi_j)$ waarbij χ_j de lijst $\mathscr{X}$ doorloopt. Doordat de karakters dezelfde modulus hebben en geschreven zijn als lijstje voortbrengende beelden, gaat het vermenigvuldigen ervan elementsgewijs. Schrijf $\psi_j = \overline{\varepsilon}\chi_j$. Merk op dat $\chi_j/\psi_j = \varepsilon$.

(vi) Verbind met elk paar karakters het product van de conductors $c_j = f_{\chi_j} f_{\psi_j}$.

(vii) We gaan nu de basis van $E_2(N,\varepsilon)$ samenstellen. Begin met de lege lijst $\mathscr{B} = \varnothing$. Voor elk element $\{(\chi,\psi), c\}$, doe het volgende:

- Als $c \nmid N$, doe niets.
- Als $\chi = 1$ en $\psi = 1$, dan voeg voor elke deler t van N/c, behalve $t = 1$, het basiselement $B_{2,1,1,t}$ toe aan de lijst $\mathscr{B}$.

- Als $\chi \neq 1$ of $\psi \neq 1$, dan voeg voor elke deler t van N/c, inclusief $t = 1$, het basiselement $B_{2,\chi,\psi,t}$ toe aan de lijst $\mathscr{B}$.

(viii) Geef uitvoer $\mathscr{B}$ en stop.

5.5 Dichtheid van Eisensteinreeksen

Net zoals we in hoofdstuk 3 voor $\sigma(\chi, \psi)$ hebben gedaan, kunnen we ook voor de Eisensteinreeksen van gewicht 2 een dichtheid definiëren.

Notatie 5.5.1. We schrijven $\Delta(\chi, \psi, t)$ voor de dichtheid van $B_{2,\chi,\psi,t}$.

Oftewel,

$$\Delta(\chi, \psi, t) = \lim_{n\to\infty} \frac{1}{n^2} \sum_{j=1}^{n} \sigma_{2,\chi,\psi,t}(j). \tag{5.22}$$

Voor $t = 1$ zijn dit de functies die in hoofdstuk 3 aan bod kwamen. Een uitzondering geldt als beide karakters triviaal zijn, want $B_{2,1,1,1}$ is de nulvorm. We concluderen het volgende.

Lemma 5.5.2. *Voor willekeurige Dirichletkarakters χ en ψ, niet beide 1, geldt dat*

$$\Delta(\chi, \psi, 1) = \begin{cases} \frac{1}{2}L(2, \chi) & \text{als } \chi \neq 1, \psi = 1, \\ 0 & \text{als } \psi \neq 1. \end{cases}$$

Voor $t > 1$ is $B_{2,1,1,t}$ wel gedefinieerd, de coëfficiënt van q^n is $\sigma(n) - t\sigma(n/t)$. We weten al dat $\sigma(n) \rightsquigarrow \frac{\pi^2}{12}$, dus de vraag is wat de limietwaarde is voor $t\sigma(n/t)$. Merk op dat de waarden van $\sigma(n/t)$ nul zijn als $t \nmid n$. De rij van waarden van $\sigma(n/t)$ tot en met N is dus de rij van waarden van $\sigma(n)$ tot en met N/t met nullen tussengevoegd. De som is dus daaraan gelijk, maar omdat er meer termen zijn ligt de dichtheid lager. Er geldt

$$\sum_{j=1}^{n} \sigma(j/t) \approx \sum_{j=1}^{n/t} \sigma(j),$$

en dus

$$\frac{1}{n^2} \sum_{j=1}^{n} \sigma(j/t) \approx \frac{1}{t^2} \cdot \frac{1}{(n/t)^2} \sum_{j=1}^{n/t} \sigma(j).$$

We concluderen

$$\sigma(n/t) \rightsquigarrow \frac{\pi^2}{12t^2},$$

en dus

$$\Delta(1, 1, t) = \Delta(\sigma(n) - t\sigma(n/t)) = \frac{\pi^2}{12} - \frac{\pi^2}{12t}.$$

Deze redenatie kan ook worden toegepast op $\Delta(\chi, \psi, t)$, omdat op dezelfde manier als hierboven geldt dat

$$\Delta(\sigma_{\chi,\psi}(n/t)) = \frac{1}{t^2}\Delta(\sigma_{\chi,\psi}(n)).$$

We verkrijgen het volgende resultaat.

Lemma 5.5.3. *Voor willekeurige Dirichletkarakters χ en ψ en willekeurige $t \in \mathbb{N}$, niet alledrie gelijk aan* 1*, geldt dat*

$$\Delta(\chi, \psi, t) = \begin{cases} \frac{\pi^2}{12} - \frac{\pi^2}{12t} & \text{als } \chi = 1, \psi = 1, \\ \frac{1}{2t^2} L(2, \chi) & \text{als } \chi \neq 1, \psi = 1, \\ 0 & \text{als } \psi \neq 1. \end{cases}$$

Hoofdstuk 6

Spitsvormen

De ruimtes van Eisensteinreeksen zijn zeer voorspelbaar en daardoor expliciet berekenbaar. Voor spitsvormen is dit een ander verhaal. Er is niet zomaar een formule te geven voor de q-expansies van spitsvormen. Er is wel een dimensieformule, maar ook die is een stuk ingewikkelder dan dimensieformule (5.13) voor Eisensteinreeksen. Daarnaast kunnen we in het die gevallen van gewicht 2 waarin de dimensie 1 is, spitsvormen verbinden aan elliptische krommen en zo toch redelijk snel een paar coëfficiënten van de q-expansie bepalen. We geven eerst de dimensieformule.

6.1 Dimensie van spitsvormruimtes

We beperken ons hier tot gewicht $k = 2$ en triviaal karakter; we geven dus de dimensies van $\mathfrak{S}_2(\Gamma_0(N))$ voor alle $N \in \mathbb{N}$. Hiertoe definiëren we eerst de volgende aritmetische functies van N:

$$\begin{aligned}
\mu_0(N) &= \prod_{p|N} \left(\left(1 + \frac{1}{p}\right) p^{\mathrm{ord}_p(N)} \right), \\
\mu_{0,2}(N) &= \begin{cases} 0 & \text{als } 4 \mid N, \\ \prod_{p|N} \left(1 + \left(\frac{-4}{p}\right)\right) & \text{anders,} \end{cases} \\
\mu_{0,3}(N) &= \begin{cases} 0 & \text{als } 2 \mid N \text{ of } 9 \mid N, \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{anders,} \end{cases} \\
c_0(N) &= \sum_{d|N} \phi(\operatorname{ggd} d, N/d).
\end{aligned}$$

Dan geldt de volgende formule voor de dimensie van $\mathfrak{S}_2(\Gamma_0(N))$. Deze formule is ook te vinden in [Ste, §6.1].

Stelling 6.1.1. *Voor alle $N \in \mathbb{N}$ is de dimensie van $\mathfrak{S}_2(\Gamma_0(N))$ gelijk aan*

$$\dim \mathfrak{S}_2(\Gamma_0(N)) = 1 + \frac{\mu_0(N)}{12} - \frac{\mu_{0,2}(N)}{4} - \frac{\mu_{0,3}(N)}{3} - \frac{c_0(N)}{2}. \tag{6.1}$$

Voor algemene k en ε geven we de formules niet, maar we hebben wel het volgende.

Stelling 6.1.2. *Voor alle $k \in \mathbb{N}, N \in \mathbb{N}$ en $\varepsilon \in \mathscr{D}(N, \mathbb{C})$ is de ruimte $\mathfrak{S}_k(N, \varepsilon)$ eindigdimensionaal.*

In combinatie met stelling 5.3.2 geeft dit

Gevolg 6.1.3. *Voor alle $k \in \mathbb{N}, N \in \mathbb{N}$ en $\varepsilon \in \mathscr{D}(N, \mathbb{C})$ is de ruimte $\mathfrak{M}_k(N, \varepsilon)$ eindigdimensionaal.*

Ook volgt uit (6.1) het volgende.

Propositie 6.1.4. *De dimensie van $\mathfrak{S}_2(\Gamma_0(N))$ is nul dan en slechts dan als*

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}. \tag{6.2}$$

De dimensie van $\mathfrak{S}_2(\Gamma_0(N))$ is 1 dan en slechts dan als

$$N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}. \tag{6.3}$$

6.2 Spitsvormen uit elliptische krommen

In deze paragraaf veronderstellen we dat $k = 2$ en $\varepsilon = 1$.

Er blijkt een relatie te bestaan tussen spitsvormen van gewicht 2 en elliptische krommen. Deze relatie geeft meer specifiek een methode om voor kleine n de coëfficiënten a_n in de q-expansie van spitsvormen te vinden. We definiëren eerst wat wij een elliptische kromme noemen.

Definitie 6.2.1 (Elliptische kromme)**.** Wij beschouwen een *elliptische kromme* als de nulpuntsverzameling C van een vergelijking van de vorm

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{6.4}$$

voor zekere a_1, a_2, a_3, a_4 en $a_6 \in \mathbb{Z}$.

Deze op het eerste gezicht vreemde nummering van de coëfficiënten is standaard. Merk op dat de term $x^\alpha y^\beta$ is vergezeld van de coëfficiënt $a_{6-2\alpha-3\beta}$. Een elliptische kromme C wordt vaak genoteerd in de vorm

$$C = [a_1, a_2, a_3, a_4, a_6]\,. \tag{6.5}$$

Elliptische krommen hebben een *discriminant* D en een *conductor* N. De definities van deze begrippen laten we achterwege, maar een later resultaat is afhankelijk van de waarde van deze conductor.

Zij C een elliptische kromme met coëfficiënten in $\mathbb{Z}$ en zij $K = \mathbb{F}_p$ een eindig lichaam met p priem. Een *rationaal punt van C mod p* is een paar (x, y) van twee elementen van K waarvoor vergelijking (6.4) geldt. Het punt op oneindig, genoteerd ∞, rekenen we ook bij de rationale punten modulo p. We schrijven $\nu_C(p)$ voor het aantal rationale punten van C mod p:

$$\nu_C(p) = \left|\left\{x, y \in \mathbb{F}_p\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\}\right|$$

Als char $K \neq 2, 3$, dan is vergelijking (6.4) door een geschikte transformatie te vereenvoudigen tot $y^2 = x^3 + Ax + B$. Schrijf $R(x) = x^3 + Ax + B \in K$. Als $R(x)$ een kwadraat in K is, dan zijn er voor $y^2 = R(x)$ twee oplossingen te verwachten. Als $R(x)$ geen kwadraat is, dan heeft de vergelijking $y^2 = R(x)$ logischerwijs geen oplossingen. Daarnaast geeft $R(x) = 0$ één oplossing. Laten we veronderstellen dat $R(x)$ uniform verdeeld is over heel K. Nemen we dit aan, dan kunnen we een schatting geven van het aantal rationale punten van C modulo p. In $K = \mathbb{F}_p$ is de helft van de inverteerbare elementen een kwadraatrest, dus dat geeft $2 \cdot \frac{p-1}{2}$ oplossingen. $R(x) = 0$ geeft één oplossing en het punt op oneindig is nog één oplossing. Het verwachte aantal oplossingen is dus $2 \cdot \frac{p-1}{2} + 1 + 1 = p + 1$. We definiëren de afwijking van het werkelijke aantal met deze schatting met $\lambda_C(p)$:

$$\lambda_C(p) = \nu_C(p) - (p + 1).$$

De schatting $p + 1$ is inderdaad nauwkeurig, er is namelijk een bovengrens bekend voor hoeveel deze maximaal afwijkt. Deze ongelijkheid staat bekend als de *Hassegrens*.

Lemma 6.2.2 (Hasse)**.** *Voor alle elliptische krommen C en alle priemgetallen p geldt dat $|\lambda_C(p)| \leq 2\sqrt{p}$.*

Zij C een elliptische kromme. Definieer een rij $a(n)$ als volgt. Voor p priem, definieer

$$a(p) = \lambda_C(p). \tag{6.6}$$

Voor priemmachten $n = p^r$ met $r \geq 2$, definieer $a(n)$ recursief aan de hand van elementen met lagere machten van p als index:

$$a(p^r) = a(p^{r-1})a(p) - p\,a(p^{r-2}). \tag{6.7}$$

Verklaar de rij $a(n)$ vervolgens multiplicatief voor onderling ondeelbare m en n:

$$a(mn) = a(m)a(n) \quad \text{als } \gcd(m, n) = 1. \tag{6.8}$$

We geven de volgende stelling, bekend als de *stelling van Wiles* of *modulariteitsstelling*, dat voordat het in 1995 bewezen werd bekend stond als het *Shimura-Taniyama-Weilvermoeden*, en ook genoemd in [Hof].

Stelling 6.2.3 (Wiles)**.** *Zij C een elliptische kromme met conductor N. Dan bestaat er een spitsvorm $f = \sum a_n q^n$ van gewicht 2, niveau N en karakter 1 waarvoor*

$$a(p) = \lambda_C(p)$$

voor alle priemgetallen p. Als bovendien geldt dat $\dim \mathfrak{S}_2(\Gamma_0(N)) = 1$, dan bestaat er een spitsvorm f waarvoor de coëfficiënten a_n voldoen aan (6.6), (6.7) en (6.8).

De stelling geeft dat als N één van de waarden in (6.3) is, dat de uitdrukkingen (6.6), (6.7) en (6.8) een manier geven om een spitsvorm $f \in \mathfrak{S}_2(\Gamma_0(N))$, en dus de enige

op constanten na, te *construeren* vanuit C, door simpelweg punten te tellen van C op priemlichamen. Voor al deze waarden van N is een elliptische kromme bekend die de basisspitsvorm f van $\mathfrak{S}_2(\Gamma_0(N))$ geeft. Deze staan opgesomd in tabel 6.1 en zijn afkomstig uit [Cre]. De elliptische krommen zijn niet uniek; er zijn meerdere elliptische krommen met dezelfde puntenaantallen en dus dezelfde coëfficiënten. We geven in de tabel steeds de elliptische kromme met de eenvoudigste vergelijking. Tabel 6.2 geeft de eerste twintig coëfficiënten van de spitsvormen van deze niveaus, genormaliseerd op de coëfficiënt voor q.

Bovenstaande stelling wordt doorgaans samengevat als "elliptische krommen zijn modulair". Het omgekeerde is ook waar en staat bekend als *de stelling van Eichler-Shimura*:

Stelling 6.2.4 (Eichler, Shimura)**.** *Zij $f = \sum a_n q^n$ een spitsvorm van gewicht 2, niveau N en karakter 1, zodanig dat de coëfficiënten $a_n \in \mathbb{Z}$ multiplicatief zijn en $a_1 = 1$. Dan bestaat er een elliptische kromme C zodanig dat*

$$a(p) = \lambda_C(p)$$

Als bovendien geldt dat $\dim \mathfrak{S}_2(\Gamma_0(N)) = 1$, dan bestaat er een elliptische kromme C zodanig dat (6.6)*,* (6.7) *en* (6.8) *gelden voor f.*

Voor andere niveau's en gewichten zijn de eerste coëfficiënten van spitsvormen, gegeven genoeg rekencapaciteit, wel te bepalen, maar er bestaan voor coëfficiënten van spitsvormen geen gesloten formules. Het enige eenvoudige geval is dat waarin er geen spitsvormen zijn, voor $\varepsilon = 1$, $k = 2$ zijn de niveaus N waarop dat gebeurt gegeven in (6.2). In het geval dat $\varepsilon = 1$, $k = 2$ en N zoals in (6.3) is het een kwestie van punten tellen op elliptische krommen.

Tabel 6.1: Elliptische krommen behorend bij spitsvormen in dimensie 1-spitsvormruimtes

N	$[a_1,$	$a_2,$	$a_3,$	$a_4,$	$a_6]$	C		
11	$[0,$	$-1,$	$1,$	$0,$	$0]$	$y^2 + y$	$=$	$x^3 - x^2$
14	$[1,$	$0,$	$1,$	$-1,$	$0]$	$y^2 + xy + y$	$=$	$x^3 - x$
15	$[1,$	$1,$	$1,$	$0,$	$0]$	$y^2 + xy + y$	$=$	$x^3 + x^2$
17	$[1,$	$-1,$	$1,$	$-1,$	$0]$	$y^2 + xy + y$	$=$	$x^3 - x^2 - x$
19	$[0,$	$1,$	$1,$	$1,$	$0]$	$y^2 + y$	$=$	$x^3 + x^2 + x$
20	$[0,$	$1,$	$0,$	$-1,$	$0]$	y^2	$=$	$x^3 + x^2 - x$
21	$[1,$	$0,$	$0,$	$1,$	$0]$	$y^2 + xy$	$=$	$x^3 + x$
24	$[0,$	$-1,$	$0,$	$1,$	$0]$	y^2	$=$	$x^3 - x^2 + x$
27	$[0,$	$0,$	$1,$	$0,$	$0]$	$y^2 + y$	$=$	x^3
32	$[0,$	$0,$	$0,$	$-1,$	$0]$	y^2	$=$	$x^3 - x$
36	$[0,$	$0,$	$0,$	$0,$	$1]$	y^2	$=$	$x^3 + 1$
49	$[1,$	$-1,$	$0,$	$-2,$	$-1]$	$y^2 + xy$	$=$	$x^3 - x^2 - 2x - 1$
N	$[a_1,$	$a_2,$	$a_3,$	$a_4,$	$a_6]$	C		

Tabel 6.2: De eerste 20 coëfficiënten van spitsvormen behorend bij de elliptische krommen uit tabel 6.1

N	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}	a_{20}
11	1	−2	−1	2	1	2	−2	0	−2	−2	1	−2	4	4	−1	−4	−2	4	0	2
14	1	−1	−2	1	0	2	1	−1	1	0	0	−2	−4	−1	0	1	6	−1	2	0
15	1	−1	−1	−1	1	1	0	3	1	−1	−4	1	−2	0	−1	−1	2	−1	4	−1
17	1	−1	0	−1	−2	0	4	3	−3	2	0	0	−2	−4	0	−1	1	3	−4	2
19	1	0	−2	−2	3	0	−1	0	1	0	3	4	−4	0	−6	4	−3	0	1	−6
20	1	0	−2	0	−1	0	2	0	1	0	0	0	2	0	2	0	−6	0	−4	0
21	1	−1	1	−1	−2	−1	−1	3	1	2	4	−1	−2	1	−2	−1	−6	−1	4	2
24	1	0	−1	0	−2	0	0	0	1	0	4	0	−2	0	2	0	2	0	−4	0
27	1	0	0	−2	0	0	−1	0	0	0	0	0	5	0	0	4	0	0	−7	0
32	1	0	0	0	−2	0	0	0	−3	0	0	0	6	0	0	0	2	0	0	0
36	1	0	0	0	0	0	−4	0	0	0	0	0	2	0	0	0	0	0	8	0
49	1	1	0	−1	0	0	0	−3	−3	0	4	0	0	0	0	−1	0	−3	0	0
N	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}	a_{20}

6.3 Dichtheid van spitsvormen

Zij $f = \sum_{n=1}^{\infty} a(n)q^n$ een spitsvorm van gewicht 2. De dichtheid van f is gedefinieerd als

$$\Delta(f) = \lim_{n\to\infty} \frac{1}{n^2} \sum_{j=1}^{n} a_j.$$

Wij beweren het volgende.

Lemma 6.3.1. *Als f een gewicht 2-spitsvorm is, dan is $\Delta(f) = 0$.*

Bewijs. Voor het bewijs gebruiken we een resultaat van Robert Rankin uit [Ran], dat zegt dat voor de coëfficiënten a_j van een gewicht k-spitsvorm geldt dat

$$\sum_{j=1}^{n} |a(j)|^2 = O(n^k)$$

In ons geval is $k = 2$. Dit betekent dat, asymptotisch, $|a(n)|^2 + \ldots + |a(2n)|^2$ ongeveer vier keer zo groot is als $|a(n/2)|^2 + \ldots + |a(n)|^2$. Omdat de eerste som twee keer zoveel termen heeft, volgt hieruit dat de gemiddelde term uit de eerste som ongeveer twee keer zo groot is als de gemiddelde term uit de tweede som. Oftewel, $|a(2j)|^2 \sim 2\,|a(j)|^2$. Oftewel,

$$|a(j)|^2 = O(j), \quad \text{en dus} \quad a(j) = O(\sqrt{j}).$$

Dit geeft dat $\sum_{j=1}^{n} a(j) = O(n\sqrt{n})$. De dichtheid van f is nu

$$\begin{aligned}\Delta(f) &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{j=1}^{n} a(j) \\ &= \lim_{n\to\infty} \frac{1}{n^2} O(n\sqrt{n}) \\ &= \lim_{n\to\infty} O(1/\sqrt{n}) \\ &= 0.\end{aligned}$$

□

Hoofdstuk 7

Kwadratische vormen

Kwadratische vormen zijn homogene polynomen van graad 2 in een eindig aantal variabelen. We definiëren hier wat dat precies betekent en geven hun eigenschappen, zoals discriminant, gewicht, niveau en karakter. Dit zijn voor een deel dezelfde eigenschappen als modulaire vormen en dat is niet toevallig. We eindigen met een bekend voorbeeld.

7.1 Definities

We geven eerst alle definities, te beginnen bij de kwadratische vorm zelf.

Kwadratische vormen

Een kwadratische vorm van *rang* r is als volgt gedefinieerd.

Definitie 7.1.1 (Kwadratische vorm)**.** Een *kwadratische vorm in* r *variabelen* is een polynoom Q gedefinieerd op $\mathbb{Z}^r$ gegeven door het voorschrift

$$(x_1, \ldots, x_r) \longmapsto \sum_{i=1}^{r} \sum_{j=1}^{r} a_{i,j} x_i x_j, \tag{7.1}$$

met $a_{i,j} = a_{j,i}$ en $2a_{i,j} \in \mathbb{Z}$ voor alle $1 \leq i, j \leq r$, en bovendien $a_{i,i} \in \mathbb{Z}$. De coëfficiënten $a_{i,i}$ noemen we *diagonaalcoëfficiënten*, de termen $a_{i,i}x_i^2$ zijn de *diagonaaltermen* van Q. De termen die niet op de diagonaal liggen noemen we ook wel *mengtermen*. Een kwadratische vorm waarvan alle mengtermen nul zijn, is een *diagonaalvorm*.

De eenvoudigste kwadratische vorm in r variabelen is de diagonaalvorm $\mathbf{x} \longmapsto x_1^2 + \ldots + x_r^2$.

Definitie 7.1.2 (Gewicht)**.** Het gewicht k van een kwadratische vorm Q definiëren we als de helft van de rang r: $k = r/2$.

Bij een kwadratische vorm kunnen we een coëfficiëntenmatrix opstellen die de kwadratische vorm uniek bepaalt.

Definitie 7.1.3 (Coëfficiëntenmatrix)**.** Zij Q Een kwadratische vorm in r variabelen gegeven door het voorschrift in (7.1). Definieer de *matrix A_Q behorend bij Q* als de $r \times r$-matrix A gegeven door

$$A_{(i,j)} = 2a_{i,j} \tag{7.2}$$

Merk op dat $A_{(i,j)} = A_{(j,i)}$, dus $A = A_Q$ is symmetrisch. De coëfficiënten zijn alle geheel, en de diagonaalcoëfficiënten zijn even. Sommige literatuur definieert A als de helft van (7.2), dan geldt deze eigenschap niet. De matrix behorende bij de kwadratische vorm $\mathbf{x} \longmapsto x_1^2 + \ldots + x_r^2$ is $2\mathbb{I}_{r\times r}$. De diagonaaltermen van de matrix A zijn tweemaal de diagonaalcoëfficiënten van Q. Een kwadratische vorm Q is een diagonaalvorm dan en slechts dan als A_Q een diagonaalmatrix is. Merk op dat

$$Q(\mathbf{x}) = \frac{1}{2}\mathbf{x}\, A_Q\, \mathbf{x}^{\mathrm{t}}. \tag{7.3}$$

Definitie 7.1.4 (Definiteit)**.** Een kwadratische vorm Q is *positief definiet* als $Q(\mathbf{x}) > 0$ voor alle $\mathbf{x} \in \mathbb{Z}^r \setminus \{0\}$. Een kwadratische vorm is negatief definiet als $-Q$ positief definiet is en een kwadratische vorm is indefiniet als deze niet positief of negatief definiet is.

Opmerking 7.1.5. Een kwadratische vorm Q is positief definiet dan en slechts dan als de bijbehorende matrix A_Q positief definiet is; dit per definitie van positief definiteit voor matrices.

Conventie 7.1.6. Vanaf hier beperken we ons tot positief definiete vormen in een even aantal variabelen.

Voor een positief definiete kwadratische vorm Q in $r = 2k$ variabelen definiëren we de determinant van Q als $\det(A_Q)$.

Definitie 7.1.7 (Discriminant)**.** Zij Q een kwadratische vorm met matrix A. De *discriminant D* van Q definiëren we als $(-1)^{r/2} \det A$.

Niveau van een kwadratische vorm

Behalve de discrimimant is er nog een manier om de "grootte" van een kwadratische vorm te bekijken: het *niveau*. Later zal blijken dat het niveau dat we hier definieren voor kwadratische vormen, verband heeft met het niveau dat we in definitie 4.5.1 hebben gedefinieerd voor modulaire vormen. Beschouw een kwadratische vorm Q met matrix $A = A_Q$ van determinant d. Omdat A gehele coëfficiënten heeft, heeft dA^{-1} dat ook. De matrix $2dA^{-1}$ heeft gehele coëfficiënten en noodzakelijkwijs een even diagonaal (want alle coëfficiënten zijn even). Maar soms zijn er kleinere getallen dan $2d$ waarvoor deze eigenschap al geldt.

Definitie 7.1.8 (Niveau)**.** Het *niveau* van een kwadratische vorm Q is de kleinste deler N van $2 \det A_Q$ waarvoor geldt dat NA_Q^{-1} gehele coëfficiënten heeft en bovendien een even diagonaal.

Merk op dat het niveau N van een kwadratische vorm Q een deler is van $2 \det A_Q$.

Er geldt zelfs de iets sterkere bewering dat

Propositie 7.1.9. *Het niveau N van een kwadratische vorm Q is altijd een deler van* $\det A_Q$.

Dit kun je bewijzen door $\det(A_Q)A_Q^{-1}$ te berekenen en te concluderen dat de diagonaalcoëfficiënten altijd even zijn. Er bestaat een sterkere relatie tussen determinant en niveau:

Propositie 7.1.10. *Het niveau N van een kwadratische vorm Q en de determinant van de bijbehorende matrix $A = A_Q$ hebben dezelfde priemfactoren, en er gelden bovendien de volgende grenzen op de verhouding tussen N en* $\det A$*:*

$$N \mid \det A, \qquad \det A \mid N^r. \tag{7.4}$$

Bewijs. Het niveau N voldoet aan de eigenschap dat $NA^{-1} \in \mathbb{Z}^{r\times r} \ni A$. Neem van de triviaal ware gelijkheid

$$NA^{-1} \cdot A = N\mathbb{I}_{r\times r}$$

de determinant:

$$\det(NA^{-1}) \cdot \det A = \det(N\mathbb{I}_{r\times r}) = N^r$$

Dan is duidelijk dat

$$\det A \mid N^r.$$

We hadden al dat

$$N \mid \det A,$$

dus een priemfactor p zit in N dan en slechts dan als deze in $\det A$ zit. □

Nemen we dus een kwadratische vorm van een gegeven determinant $\det A$, dan is een expliciet interval aan te geven waar N in moet vallen, en andersom.

Voorbeeld 7.1.11. Een kwadratische vorm in 2 variabelen van determinant $153 = 3^2\cdot 17$ heeft een niveau N dat de priemfactoren 3 en 17 bevat en een deler is van 153, zodanig dat 153 een deler is van N^2. Dit geeft de mogelijke waarden 51 en 153 voor N. Een kwadratische vorm in 2 variabelen van niveau $153 = 3^2 \cdot 17$ heeft een determinant van de vorm

$$3^a 17^b, \qquad 2 \le a \le 4, \quad 1 \le b \le 2,$$

de mogelijke waarden voor $\det A$ zijn dus

$$153,\ 459,\ 1\,377,\ 2\,601,\ 7\,803,\ 23\,409.$$

Karakter van een kwadratische vorm

Net als een gewicht en een niveau kunnen we aan kwadratische vormen ook een karakter koppelen. We veronderstellen dat $4 \mid r$. Dan is het karakter van een kwadratische vorm als volgt gedefinieerd.

Definitie 7.1.12 (Karakter)**.** Zij Q een kwadratische vorm in $r = 2k$ variabelen, waarbij $4 \mid r$, met matrix A en discriminant $D = \det A$.Het *karakter* $\varepsilon = \varepsilon_Q$ van de kwadratische vorm Q is het primitief geassocieerde van het karakter

$$d \mapsto \left(\frac{D}{d}\right), \tag{7.5}$$

oftewel $\varepsilon = \rho_{s(D)}$, waarbij s de functie is die in algoritme 2.4.6 wordt gegeven.

Gevolg 7.1.13. *Er volgt nu direct dat als de discriminant D van Q een kwadraat is, dan $\varepsilon = 1$.*

Opmerking 7.1.14. Als Q een kwadratische vorm is met karakter $\varepsilon \neq 1$, dan wordt Q ook wel een kwadratische vorm met *Nebentypus* genoemd. Dit in tegenstelling tot kwadratische vormen Q met karakter 1, welke ook wel kwadratische vormen met *Haupttypus* worden genoemd.

7.2 Voorbeeld: de som van vier kwadraten

De eenvoudigste kwadratische vorm in vier variabelen is

$$Q : (r, s, t, u) \longmapsto r^2 + s^2 + t^2 + u^2. \tag{7.6}$$

Dit is een positief definiete kwadratische vorm van rang $r = 4$ en dus gewicht $k = 2$. De matrix A_Q behorend bij Q is

$$A_Q = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} = 2\,\mathbb{I}_{4\times 4},$$

van determinant 16. Dit geeft een discriminant van $D = (-1)^k 16 = 16$. Doordat de discriminant een kwadraat is, is ε_Q het triviale karakter.

De inverse van A_Q is $\frac{1}{2}\mathbb{I}_{4\times 4}$ en het niveau van Q is de kleinste deler N van 16 waarvoor $\frac{N}{2}\mathbb{I}_{4\times 4}$ gehele coëfficiënten en een even diagonaal heeft, oftewel $N = 4$. De kwadratische vorm Q heeft dus

- matrix $A = 2\mathbb{I}_{4\times 4}$ en
- discriminant $D = 16$.
- niveau $N = 4$,
- gewicht $k = 2$,
- karakter $\varepsilon = 1$,

Hoofdstuk 8

Representaties

Omdat coëfficiënten van kwadratische vormen geheel zijn en we ze alleen bekijken op gehele getallen, bestaat het beeld van een kwadratische vorm alleen uit gehele getallen. Het beeld van positief definiete kwadratische vormen Q bevat alleen de niet-negatieve gehele getallen, $\mathbb{N}_0$. Maar hoe wordt dat beeld opgevuld? Hoe vaak komt een getal n voor in het beeld van Q? Oftewel, hoe vaak wordt n *gerepresenteerd* door Q? Deze vraag proberen we hier te beantwoorden. We beginnen bij het bekende resultaat van Jacobi uit 1834. Daarna definiëren we de thetareeks Θ van een kwadratische vorm, dat de koppeling levert met modulaire vormen. Met behulp hiervan kunnen we van kwadratische vormen die aan bepaalde voorwaarden voldoen, de representatieaantallen geven.

8.1 Representatieaantallen

Laten we het aantal representaties van n door Q eerst een naam geven.

Definitie 8.1.1 (Representaties van n door Q)**.** Zij Q een positief definiete kwadratische vorm van rang r en zij $n \in \mathbb{N}_0$. We schrijven $r(n, Q)$ voor het aantal representaties van n door Q, oftewel het aantal argumenten $\mathbf{x} \in \mathbb{Z}^r$ die door Q worden afgebeeld op n. Oftewel,

$$r(n, Q) = \left|\{(x_1, \cdots, x_r) \in \mathbb{Z}^r \colon\ f(x_1, \cdots, x_r) = n\}\right|. \tag{8.1}$$

We noemen de waarden van $r(n, Q)$ *representatieaantallen.*

De som van vier kwadraten

We gaan verder op het voorbeeld van paragraaf 7.2. Het getal $n = 0$ wordt precies één keer gerepresenteerd door Q: $r(0, Q) = 1$; dit geldt voor alle positief definiete kwadratische vormen. Voor $n = 1$ is de enige optie om één van de vier kwadraten 1 te laten zijn en de andere drie 0. Dit geeft de vectoren

$$(\pm 1, 0, 0, 0), \quad (0, \pm 1, 0, 0), \quad (0, 0, \pm 1, 0), \quad (0, 0, 0, \pm 1).$$

Dit geeft $r(1,Q)=8$. Zo kunnen we systematisch nog enkele representatieaantallen vinden voor kleine n.

$$\begin{aligned}
r(0,Q) &= 1\\
r(1,Q) &= 2^1\cdot\frac{4!}{3!1!}=8,\\
r(2,Q) &= 2^2\cdot\frac{4!}{2!2!}=24,\\
r(3,Q) &= 2^3\cdot\frac{4!}{1!3!}=32,\\
r(4,Q) &= 2^4\cdot\frac{4!}{0!4!}+2^1\cdot\frac{4!}{3!0!1!}=24,\\
r(5,Q) &= 2^2\cdot\frac{4!}{2!1!1!}=48,\\
&\vdots
\end{aligned}$$

Hierbij stelt de *multinomiaalcoëfficiënt* $4!/a_0!a_1!a_2!\cdots$ het aantal manieren voor waarop a_0 nullen, a_1 enen, a_2 tweeën, $\cdots$ kunnen worden verdeeld over r, s, t en u. De tweemacht geeft het aantal keuzes voor de tekens aan voor de argumenten, vanwege $x^2=(-x)^2$ voor $x\neq 0$. Hoewel voor kleine n deze methode prima werkt, wordt het voor grotere n een flinke boekhoudklus om alle mogelijke verdelingen van n in kwadraten te vinden en alle aantallen varianten $2^{4-a_0}\frac{4!}{a_0!a_1!a_2!\cdots}$ voor deze verdelingen te bekijken. Daarnaast is het zo dat deze methode alleen goed werkt voor eenvoudige kwadratische vormen zoals $r^2+s^2+t^2+u^2$. Voor kwadratische vormen met minder symmetrie en kwadratische vormen met mengtermen wordt dit ook voor kleine n haast ondoenlijk.

De vraag rijst of het mogelijk is om een *formule* te vinden voor $r(n,Q)$, waarmee voor grotere waarden van n, zoals $n=1\,234$, het aantal representaties meteen kan worden uitgerekend. Voor de kwadratische vorm (7.6) bestaat zo'n formule inderdaad, en deze is al sinds 1834 bekend en staat bekend als *Jacobi's vierkwadratenstelling*.

Stelling 8.1.2 (Jacobi)**.** *Het aantal manieren waarop $n\in\mathbb{N}$ te schrijven is in de vorm $n=Q(r,s,t,u)=r^2+s^2+t^2+u^2$ met $r,s,t,u\in\mathbb{Z}$, bedraagt*

$$r(n,Q)=8\sum_{d\,|\,n,\ 4\nmid d} d. \tag{8.2}$$

Met de kennis dat 617 priem is, vinden we dus bijvoorbeeld razendsnel dat

$$r(1\,234,Q)=8(1+2+617+1\,234)=14\,832.$$

8.2 Bepaling van de representatieaantallen

Ook voor andere kwadratische vormen in vier variabelen bestaan representatieformules soortgelijk aan (8.2). Met behulp van modulaire vormen kunnen we deze formules construeren. Om dit te doen missen we echter nog één belangrijk ingrediënt en dat is de *thetareeks*. Na deze te hebben gedefinieerd, laten we zien hoe formule formule (8.2) is af te leiden.

De thetareeks van een kwadratische vorm

Het sleutelelement in het proces van kwadratische vorm naar formule voor de representaties is de *thetareeks*. Deze thetareeks levert ook de koppeling tussen kwadratische vormen en modulaire vormen, waardoor we de modulairevormtheorie uit voorgaande hoofdstukken kunnen toepassen op kwadratische vormen.

Definitie 8.2.1 (Thetareeks)**.** Zij Q een kwadratische vorm in r variabelen. Definieer de *thetareeks van* Q als de machtreeks in q gegeven door

$$\Theta(q) = \sum_{\mathbf{x}\in\mathbb{Z}^r} q^{Q(\mathbf{x})}.$$

Hersorteren we de som door alle $\mathbf{x}$ met hetzelfde Q-beeld bijelkaar te zetten, dan is duidelijk dat de coëfficiënt voor q^n gelijk is aan het aantal $\mathbf{x}$ met $Q(\mathbf{x}) = n$. We krijgen daarmee een equivalente, maar prettiger definitie voor Θ:

$$\Theta(q) = \sum_{n\in\mathbb{N}_0} r(n, Q)q^n. \tag{8.3}$$

Voorbeeld 8.2.2. Voor $Q(r, s, t, u) = r^2 + s^2 + t^2 + u^2$ is

$$\Theta(q) = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + 48q^5 + \dots$$

De koppeling naar modulaire vormen wordt geleverd door de volgende stelling.

Stelling 8.2.3. *Zij Q een kwadratische vorm van niveau N in $r = 2k$ variabelen en zij ε het karakter van Q. Dan geldt voor de thetareeks Θ van Q dat*

$$\Theta \in \mathfrak{M}_k(N, \varepsilon). \tag{8.4}$$

Het bewijs van deze stelling beslaat meerdere pagina's en is in meerdere boeken reeds te vinden, zij het met een omweg om een grotere algemeenheid te behalen. In [Iwa, pp. 165 . . . 178] geeft Henryk Iwaniec een bewijs, in [Ogg] wijdt Andrew Ogg hoofdstuk VI aan een bewijs van deze stelling en in [Sch] bewijst Bruno Schöneberg dit met het resultaat op pagina 217.

Merk op dat de stelling samen met de ontbinding (4.12) impliceert dat Θ te ontbinden is als som van een Eisensteinreeks E en een spitsvorm F:

$$\Theta = E + F, \quad E \in \mathfrak{E}_k(N, \varepsilon), \quad F \in \mathfrak{S}_k(N, \varepsilon). \tag{8.5}$$

Gegeven een kwadratische vorm Q, zijn de parameters k, N en ε vrij snel uit te rekenen. We kunnen dus precies zien in welke ruimte van modulaire vormen Θ zich bevindt. Van die ruimte kennen we de dimensie, en van de component $\mathfrak{E}_k(N, \varepsilon)$ kennen we ook een basis. Als $k = 2, \varepsilon = 1$ en de component $\mathfrak{S}_k(N, \varepsilon)$ is nul- of ééndimensionaal, dan kennen we de hele ruimte, vanwege stelling 6.2.3 en tabel 6.1.

De thetareeks als lineaire combinatie

Als Θ zich bevindt in een lineaire ruimte waarvan we een basis kennen, dan komt het vinden van een formule voor Θ neer op het vinden van de coëfficiënten waarmee deze basiselementen voorkomen in Θ. We gaan daarom Θ schrijven als lineaire combinatie van de basisvormen.
In eerste instantie gaan we ervan uit dat de q-expansies van alle basisvormen bekend zijn en Θ een onbekende lineaire combinatie daarvan is. We kennen dus de basisvormen $B_1, \ldots, B_m$ en weten dat

$$\Theta = \lambda_1 B_1 + \cdots + \lambda_m B_m, \tag{8.6}$$

voor zekere $\lambda_i \in \mathbb{C}$. De q-expansie van basisvorm B_i schrijven we als volgt:

$$B_i(q) = \sum_{n=0}^{\infty} b_i(n) q^n. \tag{8.7}$$

Herinner uit (8.3) dat $\Theta(q) = \sum_{n=0}^{\infty} r(n, Q) q^n$. We willen nu de λ_i bepalen. Uit (8.6) volgt dat voor alle $n \in \mathbb{N}$,

$$r(n, Q) = \lambda_1 b_1(n) + \cdots + \lambda_m b_m(n). \tag{8.8}$$

Vinden we dus m onafhankelijke vergelijkingen van deze vorm waarbij we $r(n, Q)$ handmatig bepalen, dan geeft dat alle λ_i. Vergelijking (8.8) geeft dan voor alle overige $n \in \mathbb{N}$ een formule voor $r(n, Q)$. Laten we als het voorbeeld $Q(r, s, t, u) = r^2 + s^2 + t^2 + u^2$ bekijken.

Voorbeeld: de som van vier kwadraten

Zij Q de kwadratische vorm gegeven door $Q(r, s, t, u) = r^2 + s^2 + t^2 + u^2$. Uit paragraaf 7.2 weten we dat Q niveau $N = 4$ en gewicht $k = 2$ heeft, dus $\Theta \in \mathfrak{M}_2(\Gamma_0(4))$. Voorbeeld 5.4.3 laat zien dat de basis van $\mathfrak{E}_2(\Gamma_0(4))$ bestaat uit de basisvormen $B_{2,1,1,2}$ en $B_{2,1,1,4}$. Propositie 6.1.4 geeft dat er voor gewicht 2 en niveau 4 geen spitsvormen bestaan. De conclusie is dat

$$\Theta \in \mathfrak{M}_2(\Gamma_0(4)) = \langle B_{2,1,1,2}, B_{2,1,1,4} \rangle,$$

oftewel

$$\Theta = \lambda B_{2,1,1,2} + \mu B_{2,1,1,4}$$

voor zekere $\lambda, \mu \in \mathbb{C}$. De coëfficiënten voor q^n zijn links en rechts dus ook gelijk. Gebruikmakende van (5.22) vinden we dat voor alle $n \in \mathbb{N}$,

$$r(n, Q) = \lambda \sum_{d \mid n,\ 2 \nmid d} d + \mu \sum_{d \mid n,\ 4 \nmid d} d.$$

Voor $n = 1, 2$ geeft dit

$$8 = \lambda + \mu, \qquad 24 = \lambda + 3\mu.$$

De conclusie is dat $\lambda = 0, \mu = 8$, en dus $Q = 8B_{2,1,1,4}$. We vinden dat voor alle $n \in \mathbb{N}$,

$$r(n, Q) = 8 \sum_{d \mid n,\ 4 \nmid d} d,$$

hetgeen precies overeenkomt met de formule die Jacobi in 1834 vond. Om deze berekening te doen hebben we slechts gebruik gemaakt van $r(1,Q)$ en $r(2,Q)$, om alle andere representatieaantallen te vinden. Het aantal representatieaantallen dat we nodig hebben is minimaal de dimensie van de modulairevormruimte waar Θ in zit (meer als er afhankelijke vectoren zijn), maar we weten uit gevolg 6.1.3 dat deze altijd eindig is. Onderstaand algoritme geeft een formule voor de representatieaantallen in de vorm van coëfficiënten voor de basisvormen, onder de aanname dat we een voldoende groot aantal eerste representaties al hebben. Zij $\mathbf{r}$ een m-dimensionale rijvector met de representaties van de getallen $1,\ldots,m$ door Q.

Algoritme 8.2.4 (Representatieaantallen voor een kwadratische vorm)**.**

(i) Bepaal matrix A, discriminant D, niveau N en karakter ε van Q met behulp van de definities uit hoofdstuk 7.

(ii) Bepaal de basis $\mathscr{B} = (B_1, B_2, \ldots, B_d)$ van de ruimte $\mathfrak{E}_2(N,\varepsilon)$ met behulp van algoritme 5.4.6.

(iii) Bereken de q-expansie van elk basiselement $B_\ell \in \mathscr{B}$ uit definitie 5.4.1, tot een precisie van q^m en schrijf deze als rijvector $\mathbf{b}_\ell$. Verwijder de constante coëfficient, die gebruiken we niet. Zij M de matrix met de $\mathbf{b}_\ell$ als rijen. Dan is M een $m \times d$-matrix waarvan het element op plaats i,j de coëfficiënt van q^i in B_j is.

(iv) Kies d lineair onafhankelijke kolommen uit M. Merk op dat m tenminste zo groot moet zijn dat er inderdaad d lineair onafhankelijke kolommen bestaan. Voor deze stap kan een *gretig algoritme* worden gebruikt: bekijk per kolom of deze lineair onafhankelijk is van de reeds gekozen kolommen en zo ja, voeg deze toe aan de lijst reeds gekozen kolommen en ga zo door totdat het aantal gekozen kolommen d is. Als alle kolommen bekeken zijn en er geen d kolommen gevonden worden, is m te laag en moeten er meer representaties worden gegeven en M worden uitgebreid.

(v) Zodra de plaatsen $n_1,\ldots,n_d$ van de d kolommen gevonden zijn, zij M' de $d \times d$-matrix bestaande uit de gekozen kolommen op plaatsen $n_1,\ldots,n_d$. Zij $\mathbf{r}'$ de d-vector bestaande uit de elementen op plaatsen $n_1,\ldots,n_d$ uit $\mathbf{r}$.

(vi) Bepaal de oplossing $\mathbf{x} = (x_1, \cdots, x_d)$ van het lineaire stelsel $\mathbf{x}M' = \mathbf{r}'$.

(vii) Geef als uitvoer $\mathscr{B}$ en $\mathbf{x}$.

Bewijs. Dit algoritme zal altijd eindigen omdat als er geen d lineair onafhankelijke vectoren $\mathbf{x}_n$ zouden bestaan, er een lineaire relatie zou zijn tussen $B_1,\ldots,B_d$, wat in tegenspraak is met de bewering dat $\{B_1,\ldots,B_d\}$ een basis is. □

Een aantal dingen kunnen worden opgemerkt.

- Het bewijs impliceert dat m, het aantal benodigde representaties, eindig is.
- Als er spitsvormen in het spel zijn en daarvan de eerste m termen in de q-expansie bekend zijn, worden met dit algoritme nog steeds de juiste coëfficiënten voor alle basisvormen gevonden, maar is dit niet meer een gesloten formule voor $r(n,Q)$ omdat we geen gesloten formule voor de spitsvormen hebben.

We kunnen het algoritme ook omdraaien. Dan vinden we éérst de basisvormen en de onafhankelijke kolommen $n_1,\ldots,n_d$. Dan bepalen we precies de representaties voor deze d getallen en bepalen daarna $\mathbf{x}$. Op die manier zijn alleen de representaties voor $n_1,\ldots,n_d$ nodig, in plaats van alle representaties tot en met m. Het voordeel is dat we nu $m = n_d$ kunen kiezen.

Bepaling van de eerste representatieaantallen

We hebben het probleem van het bepalen van een representatieformule dus teruggebracht tot het bepalen van de eerste representatieaantallen. Het vinden van deze eerste aantallen is een kwestie van tellen. We beschouwen alle vectoren in het blok

$$\mathscr{B}_B = \{-B, 1-B, \ldots, B\}^4 \subset \mathbb{Z}^4 \tag{8.9}$$

en nemen de Q-waarde op elk ervan. We produceren hiermee de representaties van 1 tot en met m.

Algoritme 8.2.5.

(i) Zij $\mathscr{R}$ een lijst lengte m gevuld met nullen. Deze lijst wordt zo gevuld met de representatieaantallen.

(ii) Voor elke niet-nul vector $(r, s, t, u) \in \mathbb{Z}^4$ met $-a \leq r, s, t, u \leq B$ (dit zijn in totaal $(2B+1)^4 - 1$ vectoren):

- Bepaal $f = Q(r, s, t, u)$.
- Als $f \leq m$, verhoog het f-de element van $\mathscr{R}$ met 1.

(iii) Geef uitvoer $\mathscr{R}$ en stop.

Opmerking 8.2.6. Dit algoritme kan ongeveer een factor 2 sneller worden gemaakt door gebruik te maken van het feit dat $Q(r, s, t, u) = Q(-r, -s, -t, -u)$.

De vraag die nog rest is: welke waarde van B moeten we kiezen om er zeker van te zijn dat alle representaties tot en met m daadwerkelijk gevonden zijn? Om die vraag te beantwoorden kijken we naar vergelijking (7.3),

$$Q(\mathbf{x}) = \frac{1}{2}\mathbf{x}\, A\, \mathbf{x}^{\mathrm{t}}.$$

Verder hebben we aangenomen dat Q positief definiet is, en vanwege opmerking 7.1.5, A dus ook. Verder is de matrix A symmetrisch, en dat betekent dat A *orthogonaal diagonaliseerbaar* is, oftewel, er bestaan een orthogonale matrix U en een diagonaalmatrix D zodanig dat

$$U\, D\, U^{\mathrm{t}} = A$$

Hierbij zijn de diagonaalelementen van D de eigenwaarden van A. Dit geeft

$$Q(\mathbf{x}) = \frac{1}{2}\mathbf{x}\, U D\, U^{\mathrm{t}}\, \mathbf{x}^{\mathrm{t}} \tag{8.10}$$

$$= \frac{1}{2}(\mathbf{x}U)\, D\, (\mathbf{x}U)^{\mathrm{t}}. \tag{8.11}$$

Schrijf $\mathbf{y} = \mathbf{x}U = (y_1, y_2, y_3, y_4)$. Dan geldt

$$2Q(\mathbf{x}) = \mathbf{y}D\mathbf{y}^{\mathrm{t}} \tag{8.12}$$

$$= \begin{pmatrix} y1 & y2 & y3 & y4 \end{pmatrix} \tag{8.13}$$

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix} \begin{pmatrix} y1 \\ y2 \\ y3 \\ y4 \end{pmatrix} \tag{8.14}$$

$$= \lambda_1 y_1^2 + \lambda_2 y_2^2 + \lambda_3 y_3^2 + \lambda_4 y_4^2 \tag{8.15}$$

$$\geq \lambda \left\|\mathbf{y}\right\|^2, \tag{8.16}$$

waarbij $\lambda = \min(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. Omdat U orthogonaal is en $\mathbf{y} = \mathbf{x}U$, geldt dat $\|\mathbf{y}\| = \|\mathbf{x}\|$. Hieruit concluderen we dat

$$Q(\mathbf{x}) \geq \frac{1}{2}\lambda \left\|\mathbf{x}\right\|^2.$$

Ligt de vector $\mathbf{x}$ nu buiten het blok $\mathscr{B}_B$, dan moet $\|\mathbf{x}\| > B$, en dus $Q(\mathbf{x}) > \frac{1}{2}\lambda B^2$. De conclusie is dus de volgende.

Lemma 8.2.7. *Zij Q een kwadratische vorm met matrix A en zij λ de kleinste eigenwaarde van A. Zij B in $\mathbb{N}$ en zij $\mathbf{x} \in \mathbb{Z}^4 \setminus \mathscr{B}_B$. Dan is $Q(\mathbf{x}) > \frac{1}{2}\lambda B^2$.*

Anders gezegd, nemen we alle representaties van Q door de vectoren $\mathbf{x} \in \mathscr{B}_B$, dan zijn de representaties van de getallen $n \geq \frac{1}{2}\lambda B^2$ volledig. Voeren we algoritme 8.2.5 dus uit voor $B \geq \sqrt{2m/\lambda}$, dan vinden we alle representaties door Q van getallen $\leq m$ met de zekerheid dat ze correct zijn. In het geval dat we ook de basis volledig hebben, hetgeen het geval is als er geen spitsvormen zijn, kunnen we nu met algoritme 8.2.4 de representatieformule in zijn geheel bepalen. Dit geeft ons de volgende conclusie.

Conclusie 8.2.8. *Als Q een kwadratische vorm is van triviaal karakter en niveau N waarvoor $\mathfrak{S}_2(\Gamma_0(N)) = 0$, oftewel de niveaus genoemd in* (6.2)*, dan zijn de representatieaantallen van Q formuliseerbaar.*

8.3 De dichtheid van representaties als $r = 4$

We nemen hier aan dat $r = 4$ en dus $k = 2$. We vragen ons af "hoe dicht bij elkaar" de representaties liggen, oftewel, hoeveel vectoren $\mathbf{x}$ er zijn met $Q(\mathbf{x}) \leq n$. Om deze vraag te beantwoorden, definiëren we de cumulatieve representaties $R(n, Q)$ en de dichtheid van de representaties $\Delta(Q)$ volgens de volgende voorschriften.

$$R(n, Q) = r(0, Q) + \ldots + r(n, Q),$$

$$\Delta(Q) = \Delta(\Theta(Q)) = \lim_{n\to\infty} \frac{1}{n^2} \sum_{j=1}^{n} r(n, Q)$$

We weten dat $r(n, Q)$ een lineaire combinatie is van basisvormen:

$$r(n, Q) = \lambda_1 b_1(n) + \lambda_2 b_2(n) + \ldots + \lambda_m b_m(n).$$

De coëfficiënten $\lambda(i)$ hangen niet af van n, wat betekent dat dezelfde lineaire combinatie geldt voor $R(n, Q)$:

$$R(n, Q) = \lambda_1 B_1(n) + \lambda_2 B_2(n) + \ldots + \lambda_m B_m(n),$$

waarbij $B_j(n) = b_j(1) + \ldots + b_j(n)$. Delen we links en rechts door n^2 en nemen we de limiet, dan zien we dat

$$\Delta(Q) = \lambda_1 \Delta(b_1) + \lambda_2 \Delta(b_2) + \ldots + \lambda_m \Delta(b_m).$$

Als voor een $1 \leq j \leq m$ de $b_j(n)$ coëfficiënten van de Eisensteinreeks $B(2, \chi, \psi, t)$ zijn, dan volgt uit lemma 5.5.3 de waarde voor $\Delta(b_j)$. Uit paragraaf 6.3 volgt dat spitsvormen geen bijdrage leveren aan de dichtheid. Dit betekent dat we zodra we $\Theta(Q)$ kennen, we volgens deze methode altijd een formule voor de dichtheid kunnen geven.

Voorbeeld 8.3.1. Voor de kwadratische vorm $Q : (r, s, t, u) \longmapsto r^2 + s^2 + t^2 + u^2$ geldt

$$r(n, Q) = 8\sigma_{2,1,1,4}(n),$$

en dus is

$$\Delta(Q) = 8\Delta(1, 1, 4) = 8\left(\frac{\pi^2}{12} - \frac{\pi^2}{48}\right) = \frac{\pi^2}{2}. \tag{8.17}$$

Er is een andere manier om naar de dichtheid te kijken. In bovenstaand voorbeeld keken we immers naar de cardinaliteit van de verzameling

$$\left\{(r, s, t, u) \in \mathbb{Z}^4 \colon\ r^2 + s^2 + t^2 + u^2 \leq n\right\},$$

oftewel naar

$$\left\{\mathbf{x} \in \mathbb{Z}^4 \colon\ \|\mathbf{x}\| \leq \sqrt{n}\right\},$$

oftewel naar het aantal roosterpunten van het rooster $\mathbb{Z}^4$ in de vierdimensionale bol met straal $\sqrt{n}$. Dit aantal is asymptotisch gelijk aan het volume van deze bol gedeeld door het volume van een roosterblok (het *fundamenteel volume*), oftewel, in dit geval

$$\frac{1}{2}\pi^2(\sqrt{n})^4 \,/\, 1.$$

Dit is inderdaad $O(n^2)$ en als we de n^2 wegdelen houden we, net zoals boven, $\pi^2/2$ over.

We kunnen de dichtheid $\Delta(Q)$ koppelen aan de determinant D van Q, op de volgende manier.

Lemma 8.3.2. *Voor alle positief definiete kwadratische vormen Q geldt dat de dichtheid van $R(n, Q)$ gelijk is aan*

$$\Delta(Q) = 2\pi^2 \,/\, \sqrt{\det A}. \tag{8.18}$$

Bewijs. Voor de kwadratische vorm $Q : (r, s, t, u) \longmapsto r^2 + s^2 + t^2 + u^2$ van determinant 16 hebben we gezien dat de dichtheid inderdaad gelijk is aan $\pi^2/2$. Beschouw nu een

willekeurige diagonaalvorm $Q : (r, s, t, u) \longmapsto ar^2 + bs^2 + ct^2 + du^2$ met matrix

$$A = A_Q = \begin{pmatrix} 2a & 0 & 0 & 0 \\ 0 & 2b & 0 & 0 \\ 0 & 0 & 2c & 0 \\ 0 & 0 & 0 & 2d \end{pmatrix}$$

van determinant $16abcd$. De dichtheid van Q is asymptotisch gelijk aan $1/n^2$ maal het volume van de ellipsoïde

$$\left\{(r, s, t, u) \in \mathbb{R}^4 \colon\ ar^2 + bs^2 + ct^2 + du^2 \leq n\right\},$$

na hernoeming van r, s, t en u gelijk aan de verzameling

$$\left\{\left(\frac{r}{\sqrt{a}}, \frac{s}{\sqrt{b}}, \frac{t}{\sqrt{c}}, \frac{u}{\sqrt{d}}\right) \in \mathbb{R}^4 \colon\ r^2 + s^2 + t^2 + u^2 \leq n\right\},$$

van volume $\frac{1}{\sqrt{abcd}} \frac{\pi^2}{2} \sqrt{n}^4$. Delen we door n^2 en nemen we daarna de limiet, dan vinden we dat

$$\Delta(Q) = 2\pi^2/\sqrt{16abcd}.$$

Dit bewijst het lemma voor diagonaalvormen. We gaan nu voor algemene positief definiete vormen Q met matrix A laten zien dat de verzameling

$$\left\{\mathbf{v} \in \mathbb{R}^4 \colon\ 1/2\mathbf{v}A\mathbf{v}^{\mathrm{t}} \leq n\right\},$$

volume $2\pi^2/\sqrt{\det A}$ heeft. Merk op dat A een symmetrische matrix is, en dus orthogonaal diagonaliseerbaar is. Schrijf $A = UDU^{\mathrm{t}}$ met U een orthogonale matrix en D een diagonaalmatrix. Dan is bovenstaande verzameling gelijk aan

$$\begin{aligned} &\left\{\mathbf{v} \in \mathbb{R}^4 \colon\ 1/2\mathbf{v}UD\mathbf{v}U^{\mathrm{t}} \leq n\right\} \\ &= \left\{\mathbf{w}U^{-1} \in \mathbb{R}^4 \colon\ 1/2\mathbf{w}D\mathbf{w}^{\mathrm{t}} \leq n\right\}. \end{aligned}$$

Een orthogonale matrix is een combinatie van rotaties en reflecties en verandert dus het volume niet. Deze verzameling heeft dus volume $2\pi^2/\sqrt{\det D}$. Maar omdat U determinant 1 of -1 heeft, is $\det D = \det A$, hetgeen het gestelde bewijst. □

Hoofdstuk 9

Siegel's massaformule

Siegel's massaformule legt verbanden tussen de representatieaantallen van verschillende kwadratische vormen. De kwadratische vormen waarvan de representatieaantallen gerelateerd zijn, vertonen zelf ook verbanden met elkaar en die bekijken we daarom eerst. We definiëren equivalentieklassen die bestaan uit één of meer kwadratische vormen en geslachten die bestaan uit één of meer klassen. We geven de massa van een geslacht. We definiëren de lokale representaties modulo M en definiëren functies δ_p die iets zeggen over de representaties modulo machten van p. Siegel's massaformule maakt gebruik van deze functies en na het geven hiervan eindigen we met een voorbeeld van niveau $N = 11$.

Conventie. In dit hoofdstuk zijn alle kwadratische vormen positief definiet en van rang $r = 4$.

9.1 Reductie en equivalentie van kwadratische vormen

Als we de representaties kennen van een kwadratische vorm Q, dan kennen we ze ook voor kwadratische vormen die verkregen worden door Q te transformeren. Op die manier definiëren we equivalentie en beschouwen equivalente kwadratische vormen als "hetzelfde". We geven een reductieproces dat uit elke klasse een gereduceerde vorm geeft, deze beschouwen we als de representant voor die klasse.

Klassen van kwadratische vormen

Zij Q een kwadratische vorm in r variabelen. We kunnen Q dan transformeren door een $r \times r$-matrix M met coëfficiënten in $\mathbb{Z}$ toe te passen op de vector $\mathbf{x}$. Definieer de kwadratische vorm R door $R(\mathbf{x}) = Q(M\mathbf{x})$. Als M inverteerbaar is en M^{-1} is tevens een matrix over $\mathbb{Z}$, dan is $Q(\mathbf{x}) = R(M^{-1}\mathbf{x})$. De kwadratische vormen Q en R zijn dan wezenlijk hetzelfde en verschillen alleen op die transformatie. Bestuderen we Q, dan weten we hetzelfde over R. Twee kwadratische vormen die deze eigenschap hebben, noemen we *equivalent*.

Definitie 9.1.1 (Equivalentie van kwadratische vormen)**.** Twee kwadratische vormen Q en R, beide in r variabelen, noemen we *equivalent*, genoteerd $Q \sim R$, als er een $r \times r$-matrix $M \in SL_r(\mathbb{Z})$ bestaat zodanig dat $R(\mathbf{x}) = Q(M\mathbf{x})$ voor alle $\mathbf{x} \in \mathbb{Z}^r$.

Deze definitie is equivalent met de bewering dat als A en B de matrices van respectievelijk Q en R zijn, dat er dan een matrix U bestaat met elementen in $\mathbb{Z}$ zodanig dat

$$A = U^{\mathrm{t}}BU. \tag{9.1}$$

Dit impliceert dat er een matrix V over $\mathbb{Z}$ bestaat zodanig dat $B = V^{\mathrm{t}}AV$ en dus dat $\det A = \det B$ en $\det U = 1$; oftewel U is een *unimodulaire transformatie*. De relatie $\sim$ is een equivalentierelatie. We kunnen kwadratische vormen dus partitioneren in equivalentieklassen. De equivalentieklasse waar Q in bevat is noemen we de *klasse van* Q. Equivalente kwadratische vormen hebben dezelfde rang, discriminant en niveau. Deze eigenschappen zijn dus *invariant* op equivalentieklassen. We kunnen dus spreken over het niveau of de discriminant van een klasse van kwadratische vormen. Voor een gegeven rang r geven we het aantal klassen van een gegeven discriminant D aan met $h(D)$ en we noemen dit het *klassegetal*. Er geldt het volgende.

Propositie 9.1.2. *Voor alle r en D is $h(D)$ eindig.*

Gereduceerde kwadratische vormen

Er is geen eenvoudige formule voor $h(D)$. Willen we het klassegetal vinden voor een zekere discriminant, dan zouden we een methode moeten hebben die uit elke equivalentieklasse precies één element levert, dat fungeert als representant voor die klasse. We definiëren daartoe het begrip van een *Minkowskigereduceerde*, of simpelweg *gereduceerde* kwadratische vorm, dit is een eigenschap die voor tenminste één element van elke equivalentieklasse geldt. Deze eigenschap wordt gedefinieerd aan de hand van de coëfficiënten zoals gedefinieerd in definitie 7.1.1.

Definitie 9.1.3 (Gereduceerde kwadratische vorm)**.** Zij Q een kwadratische vorm van rang r gegeven door het voorschrift (7.1). We noemen Q *gereduceerd* als

$$0 < a_{1,1} \leq a_{2,2} \leq \ldots \leq a_{r,r} \tag{9.2}$$

en voor alle $i = 2, \ldots, r$,

$$Q(e_1, \ldots, e_{i-1}, 1, 0, \ldots, 0) \geq a_{i,i}, \tag{9.3}$$

voor alle $e_j \in \{-1, 0, 1\}$.

Er geldt dan de volgende eigenschap [Nip].

Lemma 9.1.4. *Voor elke kwadratische vorm Q bestaat er een gereduceerde kwadratische vorm R equivalent met Q.*

Een belangrijk ingrediënt van het bewijs van lemma 9.1.4 is een reductieproces dat een gereduceerde vorm construeert die per constructie equivalent is met Q. Dat proces gaat als volgt.

Algoritme 9.1.5 (Minkowskireductie van kwadratische vormen)**.** Zij een kwadratische vorm Q gegeven. Kies een $\mathbf{e}_1 \in \mathbb{Z}^r \setminus \{0\}$ zodanig dat $Q(\mathbf{e}_1)$ een minimaal element is

van $\{Q(\mathbf{x})\colon \mathbf{x} \in \mathbb{Z}^r \setminus \{0\}\}$. Voor $i = 2, \ldots, r$, kies nu $\mathbf{e}_i$ als een vector van $\mathbb{Z}^r$ zodanig dat $\{\mathbf{e}_1, \ldots, \mathbf{e}_i\}$ uit te breiden is tot een basis van $\mathbb{Z}^r$ en met $Q(\mathbf{e}_i)$ minimaal onder de vectoren die aan die eigenschap voldoen. Definieer M als de matrix met de $\mathbf{e}_1, \ldots, \mathbf{e}_r$ als kolommen en definieer de kwadratische vorm R via het voorschrift

$$R(\mathbf{x}) = Q(M\mathbf{x}). \tag{9.4}$$

We gebruiken rijvector- en kolomvectornotatie door elkaar. Het is evident dat de kwadratische vorm R die algoritme 9.1.5 uitvoert, equivalent is aan de invoer Q. We geven hier enkele lemma's die laten zien dat dit algoritme werkt zoals bedoeld.

Lemma 9.1.6. *Voor elke kwadratische vorm Q als invoer, levert het reductieproces in algoritme 9.1.5 een gereduceerde vorm als uitvoer.*

Bewijs. Zij $Q = \sum_{i,j} a_{i,j}x_ix_j$ de invoer, $R = \sum_{i,j} b_{i,j}x_ix_j$ de uitvoer en M e transformatiematrix van algoritme 9.1.5 (dus $R(\mathbf{x}) = Q(M\mathbf{x})$). De vectoren $\mathbf{e}_i$ zijn zodanig gekozen dat $B = \{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ een basis voor $\mathbb{Z}^r$ is. De matrix M is zodanig dat

$$b_{i,i} = R(0, \ldots, 1, \ldots, 0) = Q(M(0, \ldots, 1, \ldots, 0)) = Q(\mathbf{e}_i),$$

en $\mathbf{e}_i$ heeft onder alle vectoren die samen met $\mathbf{e}_1, \ldots, \mathbf{e}_{i-1}$ uit te breiden is tot een basis van $\mathbb{Z}^r$, het kleinste Q-beeld. Als de vector $\mathbf{w} = e_1\mathbf{e}_1 + \ldots + e_{i-1}\mathbf{e}_{i-1} + \mathbf{e}_i$ samen met $\mathbf{e}_1, \ldots, \mathbf{e}_{i-1}$ eveneens uit te breiden is tot een basis van $\mathbb{Z}^r$, dan moet

$$R(e_1, \ldots, e_{i-1}, 1, \ldots, 0) = Q(e_1\mathbf{e}_1 + \ldots + e_{i-1}\mathbf{e}_{i-1} + \mathbf{e}_i, 0, \ldots, 0) \geq b_{i,i}. \tag{9.5}$$

Het is dus voldoende om te bewijzen dat $\{\mathbf{e}_1, \ldots, \mathbf{e}_{i-1}, \mathbf{w}\}$ inderdaad uit te breiden is tot een basis.

Kies $\mathbf{v} \in \mathbb{Z}^r$ willekeurig. Omdat B een basis is, zijn er λ_i zodanig dat

$$\mathbf{v} = \lambda_1\mathbf{e}_1 + \ldots + \lambda_r\mathbf{e}_r.$$

We herschrijven dit als volgt.

$$\begin{aligned}
\mathbf{v} &= (\lambda_1 - \lambda_i e_i)\mathbf{e}_1 + \ldots + (\lambda_{i-1} - \lambda_i e_{i-1})\mathbf{e}_{i-1} \\
&\quad + \lambda_i(e_1\mathbf{e}_1 + \ldots + e_{i-1}\mathbf{e}_{i-1} + \mathbf{e}_i) \\
&\quad + \lambda_{i+1}\mathbf{e}_{i+1} + \ldots + \lambda_r\mathbf{e}_r \\
&= \mu_1\mathbf{e}_1 + \ldots + \mu_{i-1}\mathbf{e}_{i-1} + \mu_i\mathbf{w} + \mu_{i+1}\mathbf{e}_{i+1} + \ldots + \mu_r\mathbf{e}_r \\
&\in \langle B' \rangle.
\end{aligned}$$

dus $\mathbf{v}$ is uit te drukken in $B' = \{\mathbf{e}_1, \ldots, \mathbf{e}_{i-1}, \mathbf{w}, \mathbf{e}_{i+1}, \ldots, \mathbf{e}_r\}$. Omdat $\mathbf{v}$ willekeurig is, is B' een basis en $\{\mathbf{e}_1, \ldots, \mathbf{e}_{i-1}, \mathbf{w}\}$ is er toe uit te breiden. Dit bewijst (9.5).
Tot slot is de deelverzameling van $\mathbb{Z}^r$ waarover $\mathbf{e}_i$ een minimaal Q-beeld heeft, bevat in de deelverzameling van $\mathbb{Z}^r$ waarover $\mathbf{e}_{i-1}$ een minimaal Q-beeld heeft. Dit impliceert dat $b_{i-1,i-1} \leq b_{i,i}$. Omdat we Q positief definiet veronderstellen is $b_{1,1} > 0$. □

We bewijzen ook dat het reduceren van een gereduceerde vorm niets oplevert.

Lemma 9.1.7. *Als Q een gereduceerde vorm is, dan is de uitvoer R van algoritme 9.1.5 gelijk aan Q. Oftewel, algoritme 9.1.5 is idempotent.*

Voor lemma 9.1.7 hebben we eerst een paar tussenresultaten nodig.

Lemma 9.1.8. *Een positief definiete kwadratische vorm is een convexe functie.*

Lemma 9.1.9. *Als f een convexe functie is in één reële variabele, en a, b en c zijn reële getallen waarvoor geldt dat $a < b < c$ en $f(a) \geq f(b) \leq f(c)$, dan geldt voor alle $x < a$ dat $f(x) \geq f(a)$ en voor alle $x > c$ dat $f(x) \geq f(c)$.*

Bewijs. Stel dat de aannames gelden en de conclusie niet. Dan bestaat er ofwel een $x < a$ met $f(x) \leq f(a) \geq f(b)$, ofwel een $x > c$ met $f(b) \leq f(c) \geq f(x)$. Beide gevallen zijn in strijd met de definitie van convexiteit van f. □

Hieruit volgt dat als f een convexe functie op $\mathbb{Z}$ is en $f(-1) \geq f(0) \leq f(1)$, dan is 0 het globale minimum van f. We bewijzen nu lemma 9.1.7.

Bewijs. Te bewijzen is dat als Q gereduceerd is en R is de Minkowskigereduceerde van Q volgens algoritme 9.1.5, dan $R = Q$. We bewijzen hier dat de transformatiematrix M de identiteitsmatrix is.

Er geldt
- $0 < a_{1,1} \leq a_{2,2} \leq \ldots \leq a_{r,r}$,
- $Q(e_1, \ldots, e_{i-1}, 1, 0, \ldots, 0) \geq a_{i,i}$ voor alle $e_j \in \{-1, 0, 1\}$.

Schrijf $R(\mathbf{x}) = Q(M\mathbf{x})$ met M de matrix met kolommen $\mathbf{e}_1, \ldots, \mathbf{e}_r$. $\mathbf{e}_1$ is de vector met het kleinste Q-beeld. Maar we weten

$$Q(1, 0, \ldots, 0) = a_{1,1} \leq a_{j,j} = Q(0, \ldots, 0, 1, 0, \ldots, 0) \leq Q(e_1, \ldots, e_{i-1}, 1, 0, \ldots, 0); \quad (9.6)$$

dus van alle niet-nul vectoren met elementen -1, 0 en 1 heeft $(1, 0, \ldots, 0)$ de kleinste Q-waarde. De convexiteit van Q impliceert nu dat $(1, 0, \ldots, 0)$ het minimale Q-beeld over heel $\mathbb{Z}^r$ geeft. Dus $\mathbf{e}_1 = (1, 0, \ldots, 0)$.
Dit reduceert het probleem tot dimensie $r - 1$, waarop dezelfde methode toepasbaar is. De conclusie is dat $M = \mathbb{I}_{r \times r}$. □

Zelfequivalentie van een kwadratische vorm

Vergelijking (9.1) geeft de eigenschap van de matrices van equivalente vormen Q en R. Omdat deze equivalentie-eigenschap een equivalentierelatie is, is een kwadratische vorm ook equivalent aan zichzelf. Echter, dat wil niet zeggen dat elke unimodulaire transformatie U zodanig dat $A = U^{\mathrm{t}}AU$ de identiteitsmatrix is. Zo heeft de matrix $-\mathbb{I}_{r \times r}$ ook altijd deze eigenschap. Een unimodulaire transformatie U zodanig dat $A = U^{\mathrm{t}}AU$ noemen we een *automorf* van A. We schrijven $O(A)$ voor de verzameling van deze automorfen:

$$O(A) = \left\{U \in \mathrm{Mat}^1_{2\times 2} \colon\ A = U^{\mathrm{t}} A\, U\right\} \quad (9.7)$$

We schrijven daarnaast $o(A)$ voor het aantal automorfen van A:

$$o(A) = |O(A)|\,. \quad (9.8)$$

We schrijven $o(Q)$ voor het aantal automorfen $o(A_Q)$ van de matrix A_Q behorend bij de kwadratische vorm Q.

9.2 Geslachten van kwadratische vormen

In paragraaf 9.1 hebben we de kwadratische vormen van rang r en discriminant D ingedeeld in klassen. We kunnen de klassen groeperen in *geslachten* via de volgende definitie van Henryk Iwaniec in [Iwa, p. 182].

Definitie 9.2.1 (Geslacht van een kwadratische vorm)**.** De volgende beweringen zijn equivalent en twee kwadratische vormen Q en R zitten in hetzelfde *geslacht* als ze gelden voor Q en R.

- Q en R zijn equivalent over $\mathbb{Z}_p$ voor elk priemgetal p.
- Q en R zijn equivalent over $\mathbb{Z}_p$ voor elke priemdeler p van $2 \det A_Q \det A_R$.
- Q en R zijn equivalent over $\mathbb{Z}$ met vormen die modulo $8 \det A_Q \det A_R$ overeenkomen.

Het geslacht waarin Q zich bevindt noteren we met gen Q.
Uit deze definitie volgt dat een geslacht bestaat uit hele klassen: als Q en R equivalent zijn, zijn bovenstaande beweringen trivialiter waar. Vormen in hetzelfde geslacht hebben dezelfde discriminant en hetzelfde niveau, dus de indeling in geslachten kan per discriminant en niveau bekeken worden. Geslachten bestaan altijd uit eindig veel klassen.

Definitie 9.2.2 (Uniek in het geslacht)**.** Als gen Q slechts de klasse van Q zelf bevat, dan noemen we de kwadratische vorm Q *uniek in zijn geslacht*.

Er bestaan vormen die uniek in hun geslacht zijn, een bekend voorbeeld is de diagonaalvorm $(r, s, t, u) \mapsto r^2 + s^2 + t^2 + u^2$.

Massa's van geslachten

Siegel's massaformule zegt iets over de gemiddelde representatieaantallen over een geslacht. Deze werkt echter alleen met een correct gewogen gemiddelde. Onderstaande definities en beweringen zijn afkomstig van Henryk Iwaniec uit [Iwa, p. 184]. We definiëren eerst de *massa* van een geslacht gen Q:

$$m(\text{gen } Q) = \sum_{R \in \text{ gen } Q} \frac{1}{o(R)} \tag{9.9}$$

Hierbij nemen we de som over de klassen in gen Q; we nemen dus uit elke klasse één representant R. Omdat o een klasse-invariant is, maakt het niet uit welke representant wordt gekozen.

We willen nu het gewogen gemiddelde nemen van de representatieaantallen van de vormen $R \in \text{gen } Q$ met $1/o(R)$ als relatieve weegfactor. De absolute weegfactor wordt dan

$$w(R) = \frac{1}{m(\text{gen } Q)} \frac{1}{o(R)}. \tag{9.10}$$

Dan volgt namelijk direct dat

$$\sum_{R \in \text{gen } Q} w(R) = 1. \tag{9.11}$$

We definiëren de representatieaantallen $r(n, \text{gen } Q)$ over het geslacht gen Q als volgt.

Definitie 9.2.3 (Representatieaantallen over gen Q)**.** Voor het geslacht gen Q zijn de representatieaantallen voor $n \in \mathbb{N}$ gedefinieerd als het gewogen gemiddelde van de representatieaantallen over de afzonderlijke klassen in gen Q, waarbij wordt gewogen volgens de weegfactoren (9.10). Oftewel,

$$r(n, \text{gen } Q) = \sum_{R \in \text{gen } Q} w(R) r(n, R). \tag{9.12}$$

We kunnen ook hier een thetareeks definiëren:

$$\Theta(\text{gen } Q) = \sum_{n=0}^{\infty} r(n, \text{gen } Q) q^n$$

Omdat $r(n, \text{gen } Q)$ een lineaire combinatie is van de $r(n, R)$, is $\Theta(\text{gen } Q)$ een lineaire combinatie van de $\Theta(R)$. Omdat al deze R hetzelfde niveau hebben, zijn al deze $\Theta(R)$ modulaire vormen in dezelfde ruimte en is derhalve ook $\Theta(\text{gen } Q)$ een modulaire vorm van hetzelfde gewicht, niveau en karakter. Merk op dat

$$\Theta(\text{gen } Q) = \sum_{R \in \text{gen } Q} w(R) \Theta(R).$$

Beide leden kunnen we wegens (8.5) ontbinden als

$$E(\text{gen } Q) + F(\text{gen } Q) = \sum_{R \in \text{gen } Q} w(R)(E(R) + F(R)). \tag{9.13}$$

Henryk Iwaniec laat in [Iwa, (11.65)] zien dat

$$E(Q) = \sum_{R \in \text{gen } Q} w(R) \Theta(R).$$

Dit laat zien dat $E(Q)$ niet afhankelijk is van de keuze van de betreffende Q uit dit geslacht. We concluderen:

Propositie 9.2.4. *$E(Q)$ is* invariant *op het geslacht.*

Omdat $E(\text{gen } Q)$ een gewogen gemiddelde is van al deze $E(Q)$, is het er eveneens aan gelijk. Dus

$$E(\text{gen } Q) = \sum_{R \in \text{gen } Q} w(R) \Theta(R). \tag{9.14}$$

Nemen we het verschil tussen de vergelijkingen (9.13) en (9.14), dan vinden we dat $F(\text{gen } Q) = 0$, oftewel dat $\Theta(\text{gen } Q) \in \mathfrak{E}_k(N, \varepsilon)$ en meer specifiek dat $\Theta(\text{gen } Q) = E(Q)$, ongeacht de keuze van de representant Q voor het geslacht gen Q.

Gevolg 9.2.5. *Omdat in* $\Theta(\text{gen } Q)$ *geen spitsvormen voorkomen, is deze een lineaire combinatie van de basiselementen uit stelling 5.4.4 en is* $\Theta(\text{gen } Q)$ *dus volledig formuliseerbaar.*

Als Q uniek in zijn geslacht is, dan moet $\Theta(Q) = \Theta(\text{gen } Q)$ en is dus $\Theta(Q) \in \mathfrak{E}_k(N, \varepsilon)$.

Conclusie 9.2.6. *Als* Q *uniek in zijn geslacht is, dan is* $\Theta(Q)$ *volledig formuliseerbaar.*

We hebben dus nu twee criteria voor kwadratische vormen Q die de zekerheid geven dat we een formule kunnen vinden voor de representatieaantallen: Q heeft triviaal karakter en een "laag niveau", daarmee bedoelen we een niveau dat genoemd is in (6.2) (zodat er geen spitsvormen bestaan), of Q is uniek in zijn geslacht. Maar er is een verband tussen deze twee criteria. Gordon Nipp heeft namelijk het volgende opgemerkt in [Nip, p. 2].

Propositie 9.2.7. *Er bestaan twee niet-equivalente kwadratische vormen van niveau* $N = 1\,729$ *met dezelfde thetareeks, en dit fenomeen komt niet voor bij lagere niveaus.*

Anders gezegd, twee niet-equivalente vormen met een niveau kleiner dan 1 729 hebben een verschillende thetareeks. Hieruit kunnen we het volgende afleiden.

Lemma 9.2.8. *Alle kwadratische vormen van "laag niveau" en triviaal karakter zijn uniek in hun geslacht.*

Bewijs. Merk op dat alle "lage niveaus" kleiner zijn dan 1 729. Zij Q en R twee niet-equivalente kwadratische vormen van een laag niveau N. Dan hebben ze dus verschillende thetareeksen. Omdat $\mathfrak{S}_2(\Gamma_0(N)) = 0$, hebben Q en R dus thetareeksen met verschillende Eisensteincomponenten. Propositie 9.2.4 laat nu zien dat Q en R tot verschillende geslachten behoren. De conclusie is dat elke twee niet-equivalente vormen van laag niveau tot verschillende geslachten behoren, dus alle vormen van laag-niveau zijn uniek in hun geslacht. □

Dit betekent dat we de voorwaarde at Q van laag niveau is kunnen weghalen, omdat de voorwaarde dat Q uniek in zijn geslacht is, deze geheel omvat.

Conclusie 9.2.9. *We weten zeker dat* $\Theta(Q)$ *volledig formuliseerbaar is, dan en slechts dan als* Q *uniek in zijn geslacht is.*

9.3 Lokale representaties en de functies δ_p

Siegel's massaformule doet niet alleen uitspraken over de gezamenlijke representatieaantallen van een aantal kwadratische vormen bij elkaar, maar verbindt deze representatieaantallen ook met lokale representatieaantallen van de vormen in dat geslacht.

Definities

We definiëren de lokale representaties van Q als volgt.

Definitie 9.3.1 (Lokale representaties)**.** Zij Q een kwadratische vorm van rang r en zij $M = p^a$ een priemmacht. Zij $n \in \mathbb{N}$. De lokale dichtheid modulo M van n door Q definiëren we als de genormaliseerde fractie van $\mathbf{x} \in (\mathbb{Z}/M\mathbb{Z})^r$ waarvoor $Q(\mathbf{x}) \equiv n \pmod{M}$:

$$\lambda_M(n, Q) = \frac{|\{\mathbf{x} \in (\mathbb{Z}/M\mathbb{Z})^r \colon Q(\mathbf{x}) \equiv n \pmod{M}\}|}{M^{r-1}}. \tag{9.15}$$

De lokale representatieaantallen modulo p definiëren we als de limiet

$$\delta_p(n, Q) = \lim_{a \to \infty} \lambda_{p^a}(n, Q). \tag{9.16}$$

Merk op dat $\lambda_M(n, Q)$ periodiek is met periode M. Voor δ_p geldt zo'n periodiciteitseigenschap niet.

Zouden we in bovenstaande definitie de noemer vervangen door M^r dan hebben we de normale dichtheid te pakken; de som van $\lambda_M(n, Q)$ over alle restklassen n modulo M is dan 1. De individuele functiewaarden zouden naar nul neigen en de limietfunctie wordt daardoor de nulfunctie. De reden dat we kiezen voor een noemer van M^{r-1} is dat op die manier de de *gemiddelde* waarde van λ_M nu 1 wordt, oftewel $\lambda_M \rightsquigarrow 1$, waardoor de limietfunctie ook gemiddelde waarde 1 heeft. In de volgende subparagraaf geven we een voorbeeld van zo'n lokale representatiefunctie δ_p als functie van n.

De lokale representaties modulo M kunnen we vinden door van alle M^r vectoren $\mathbf{x} \in (\mathbb{Z}/M\mathbb{Z})^4$ de Q-waarde modulo p te reduceren en die te tellen. Zo kan het vinden van bijvoorbeeld δ_2 geschieden door de lokale representaties modulo $M = 2$, 4, 8, 16 en 32 te tellen en in de resultaten een patroon te zoeken. Voor kleine priemgetallen als 2 en 3 is dat goed mogelijk, voor grotere priemgetallen wordt dit helaas onpraktisch omdat voor de representaties modulo M in totaal M^4 stappen nodig zijn.

We definiëren ook de functie δ_∞, op dezelfde manier als Henryk Iwaniec doet in [Iwa, (11.20)], maar specifiek voor het geval $r = 4$. Zij Q een kwadratische vorm met matrix A. We definiëren δ_∞ voor Q als de functie op $\mathbb{N}$ gegeven door het volgende voorschrift.

$$\delta_\infty(n, Q) = \frac{4\pi^2 n}{\sqrt{\det A}}. \tag{9.17}$$

Voorbeeld: $r^2 + s^2 + t^2 + u^2$

We bekijken de kwadratische vorm $Q : (r, s, t, u) \mapsto r^2 + s^2 + t^2 + u^2$ van niveau $N = 4$ en willen $\delta_2(n, Q)$ vinden. Hiertoe bekijken we eerst de lokale dichtheden modulo $2, 4, 8, ...$ en nemen dan de limiet. De lokale dichtheden tellen we met een computer; omdat er vier variabelen zijn hebben we modulo $M = p^a$ een aantal van M^4 tellingen nodig. Dit betekent dat we slechts voor zeer kleine a deze telling kunnen uitvoeren. Hieronder geven we het resultaat van die tellingen. Hierbij schrijven we het resultaat van de telling modulo

M op als een rijtje van lengte M; het i-de element staat voor de lokale representaties van i modulo M; beginnend bij $i = 0$.

$$\begin{array}{lll} M = 2, & 2^4 = 16, & \{8, 8\} \\ M = 4, & 4^4 = 256, & \{32, 64, 96, 64\} \\ M = 8, & 8^4 = 4096, & \{128, 512, 768, 512, 384, 512, 768, 512\} \\ \vdots & & \end{array}$$

We normaliseren dit door te delen door $(p^a)^{r-1} = M^3$:

$$\begin{array}{rl} M = 2 & \{1, 1\} \\ M = 4 & \{\frac{1}{2}, 1, \frac{3}{2}, 1\} \\ M = 8 & \{\frac{1}{4}, 1, \frac{3}{2}, 1, \frac{3}{4}, 1, \frac{3}{2}, 1\} \\ M = 16 & \{\frac{1}{8}, 1, \frac{3}{2}, 1, \frac{3}{4}, 1, \frac{3}{2}, 1, \frac{3}{8}, 1, \frac{3}{2}, 1, \frac{3}{4}, 1, \frac{3}{2}, 1\} \\ \vdots & \end{array}$$

We kunnen zo een vermoeden opstellen over de waarschijnlijke structuur van de limietfunctie $\delta_2(n, Q)$. Het lijkt er namelijk op dat als n oneven is, dan is $\lambda_M(n, Q) = 1$ voor alle $M = 2^a$, en als n even is, dan is voor voldoende grote a de waarde van $\lambda_{2^a}(n, Q)$ gelijk aan $3v_2(n)$. We krijgen de volgende kandidaat-limietfunctie.

Vermoeden 9.3.2. *Voor $Q(r, s, t, u) = r^2 + s^2 + t^2 + u^2$ geldt*

$$\delta_2(n, Q) = \begin{cases} 3v_2(n) & \text{als } 2 \mid n, \\ 1 & \text{als } 2 \nmid n. \end{cases} \tag{9.18}$$

Omdat δ_p een limiet is van functies met gemiddelde waarde 1, heeft het zelf ook gemiddelde waarde 1. Als het door ons gevonden voorschrift voor δ_2 dat ook heeft is dat een aanwijzing dat het voorschrift correct kan zijn. Er geldt voor ons voorschrift van δ_2 dat

$$\begin{aligned} \operatorname*{mean}_{\mathbb{Z}} \delta_2(n, Q) &= \frac{1}{2} \operatorname*{mean}_{2 \mid n} 3v_2(n) + \frac{1}{2} \operatorname*{mean}_{2 \nmid n} 1 \\ &= \frac{1}{2} \cdot 3 \cdot \frac{1}{3} + \frac{1}{2} \\ &= 1, \end{aligned}$$

en dus

$$\delta_2(n, Q) \rightsquigarrow 1 \tag{9.19}$$

9.4 Siegel's massaformule

We hebben nu de ingrediënten om Siegel's massaformule te geven. Deze geeft een andere formule voor $r(n, \text{gen } Q)$, die gebruik maakt van de functies δ_p uit (9.16) en (9.17).

Stelling 9.4.1 (Siegel's massaformule)**.** *Zij Q een kwadratische vorm en* gen Q *het geslacht waar Q in bevat is. Voor de representaties $r(n, \text{gen } Q)$ geldt de volgende formule.*

$$r(n, \text{gen } Q) = \delta_\infty(n, Q) \prod_p \delta_p(n, Q). \tag{9.20}$$

Dit geeft een formule voor de globale representaties over een geslacht als functie van alle lokale representaties van een willekeurige vorm binnen dat geslacht. Dit is een oneindig product, dus we hebben er nog weinig aan, maar het blijkt dat alle behalve eindig veel δ_p samengenomen kunnen worden tot een berekenbare uitdrukking. Het resultaat is de volgende formule.

Stelling 9.4.2. *Zij Q een kwadratische vorm van rang 4 en discriminant D. Zij χ het Dirichletkarakter gegeven door $\chi(a) = \left(\frac{4D}{a}\right)$. Dan geldt*

$$r(n, \text{gen } Q) = \delta_\infty(n, Q) \cdot \Big(\prod_{p \,|\, 2D} \delta_p(n, Q) \Big) \cdot \frac{1}{L(2, \chi)} \cdot \sum_{d \,|\, n} \frac{\chi(d)}{d}. \tag{9.21}$$

Het voorbeeld $r^2 + s^2 + t^2 + u^2$

Laten we met behulp van Siegel's formule (9.21) een uitdrukking voor $r(n, \text{gen } Q)$ vinden voor de kwadratische vorm $Q : (r, s, t, u) \longmapsto r^2 + s^2 + t^2 + u^2$. We gaan ervan uit dat de formule in vermoeden 9.3.2 juist is. Verder gebruiken we dat gen Q uit slechts de vorm Q zelf bestaat. Omdat $r(n, \text{gen } Q)$ een gemiddelde over de representatieaantallen over een geslacht is, moet het zo zijn dat $r(n, \text{gen } Q) = r(n, Q)$ voor deze vorm. We gaan hier kijken of dat inderdaad zo is.

Q heeft discriminant 16 en dus is χ het karakter gegeven door $\chi(a) = \left(\frac{64}{a}\right)$. Omdat 64 een kwadraat is, is dit het triviale karakter mod $R(64) = 2$. Dus $L(2, \chi) = \frac{\pi^2}{8}$. De som van $\chi(d)/d$ over de delers d van n is

$$\sum_{d \,|\, n, 2 \nmid d} \frac{1}{d} \;=\; \sum_{d \,|\, w_2(n)} \frac{1}{d} \;=\; \sigma_{-1}(w_2(n)). \tag{9.22}$$

De determinant is 16, dus vergelijking (9.17) geeft dat $\delta_\infty(n, Q) = \pi^2 n$. Dus

$$\begin{aligned} r(n, \text{gen } Q) &= \pi^2\, n \cdot \delta_2(n, Q) \cdot \frac{8}{\pi^2} \cdot \sigma_{-1}(w_2(n)) \\ &= 8\, n\, \sigma_{-1}(w_2(n)) \cdot \delta_2(n, Q) \\ &= \begin{cases} 24\, n\, v_2(n) \cdot \sigma_{-1}(w_2(n)) & \text{als } 2 \mid n, \\ 8\, n\, \sigma_{-1}(w_2(n)) & \text{als } 2 \nmid n. \end{cases} \end{aligned}$$

Als n oneven is, dan $w_2(n) = n$ en dus $r(n, \text{gen } Q) = 8\sigma(n)$. Oneven n hebben geen delers deelbaar door 4, dus de uitdrukking voor $r(n, \text{gen } Q)$ is in dit geval gelijk aan

$$8 \sum_{d \,|\, n, 4 \nmid d} d.$$

Dan rest het geval waarin n even is. De uitdrukking $nv_2(n)$ is gelijk aan $w_2(n)$, dus als n even is, dan is

$$r(n, \text{gen } Q) = 24\ w_2(n)\ \sigma_{-1}(w_2(n)) = 24\ \sigma(w_2(n)) = 24 \sum_{d \mid n, 2 \nmid d} d.$$

Voor elke oneven deler d van n is $2d$ een deler van n die niet een viervoud is. Nemen we dus de som over de delers niet deelbaar door 4, dan is dat hetzelfde als dat we de som over alle oneven delers van $3d$ nemen. Halen we de factor 3 uit de 24 binnen de som, dan krijgen we dat voor even n,

$$r(n, \text{gen } Q) = 8 \sum_{d \mid n, 4 \nmid d} d.$$

We komen uit op exact dezelfde formule als die in stelling 8.1.2. Dit laat zien dat vermoeden 9.3.2 inderdaad correct is.

Een voorbeeld van niveau $N = 11$

Het kleinste niveau N waarvoor er een geslacht is dat uit meerdere klassen bestaat, is $N = 11$. Het betreft de volgende drie kwadratische vormen van determinant 121.

$$\begin{aligned}
Q_1(r,s,t,u) &= \ r^2 + \ s^2 + 3t^2 + 3u^2 + \ rt + su, \\
Q_2(r,s,t,u) &= \ r^2 + \ s^2 + 4t^2 + 4u^2 + \ rs + rt + ru + su + 4tu, \\
Q_3(r,s,t,u) &= 2r^2 + 2s^2 + 2t^2 + 2u^2 + 2rs + rt + ru + su + 2tu,
\end{aligned}$$

Siegel's massaformule zegt dat

$$r(n, \text{gen } Q) = \frac{4\pi^2 n}{\sqrt{\det A}} \delta_2(n,Q)\delta_{11}(n,Q) \cdot \frac{1}{L(2,\chi)} \cdot \sum_{d \mid n} \chi(d)/d, \tag{9.23}$$

waarbij $\chi(a) = \left(\frac{484}{a}\right)$ het triviale karakter modulo $R(484) = 22$ is. Het bekijken van de lokale representaties modulo 32 geeft het vermoeden dat voor $i = 1, 2, 3$,

$$\delta_2(n, Q_i) = \frac{3}{2} - \frac{3}{4}\, v_2(n), \tag{9.24}$$

en de lokale representaties modulo 11 geven het vermoeden dat

$$\delta_{11}(n, Q_i) = \frac{12}{11}\, v_{11}(n). \tag{9.25}$$

Merk op dat de lokale representaties van Q_1, Q_2 en Q_3 overeenkomen. Dit is vanwege het feit in definitie 9.2.1 dat deze vormen, omdat ze in hetzelfde geslacht zitten, equivalent zijn modulo 2 en 11. Merk op dat voor deze voorschriften voor δ_2 en δ_{11} (gebruik makende van (3.11)) inderdaad geldt dat

$$\delta_2 \rightsquigarrow \frac{3}{2} - \frac{3}{4} \cdot \frac{2}{3} = 1, \qquad \delta_2 \rightsquigarrow \frac{12}{11} \cdot \frac{11}{12} = 1.$$

Omdat 484 een kwadraat is, is χ het triviale karakter modulo $R(484) = 22$. De som $\sum_{d|n} \chi(d)/d$ is dus gelijk aan

$$\sum_{d|n,\, 2\nmid d,\, 11\nmid d} \frac{1}{d} = \sum_{d \,|\, w_{22}(n)} \frac{1}{d}.$$

Betrekken we nu de factor n in deze som, dan krijgen we

$$\sum_{d \,|\, w_{22}(n)} \frac{n}{d} = \frac{n}{w_{22}(n)}\, \sigma(w_{22}(n)).$$

De L-reeks voor χ heeft volgens (2.37) de waarde

$$L(2,\chi) = \frac{\pi^2 \cdot 3 \cdot 120}{6 \cdot 4 \cdot 121} = \frac{15}{121}\pi^2.$$

Dit geeft dat

$$\begin{aligned} r(n, \text{gen } Q) &= \frac{3}{4}\frac{12}{11}\frac{4}{\sqrt{121}}\frac{121}{15}\,(2 - v_2(n)) \cdot v_{11}(n) \cdot g_{22}(n) \cdot \sigma(w_{22}(n)) \\ &= \frac{12}{5}\,(2 - v_2(n)) \cdot v_{11}(n) \cdot g_2(n) \cdot g_{11}(n) \cdot \sigma(w_{22}(n)) \\ &= \frac{12}{5}\,(2g_2(n) - 1) \cdot \sigma(w_{22}(n)). \end{aligned} \tag{9.26}$$

In deze berekening gebruikt de tweede stap de gelijkheid $g_{pq}(n) = g_p(n)g_q(n)$ en de laatste stap de gelijkheid $v_p(n)g_p(n) = 1$.

We hebben gezien dat $r(n, \text{gen } Q) \in \mathfrak{E}_2(\Gamma_0(11))$. Van niveau 11 en triviaal karakter bestaat slechts één basisvorm, te weten $B_{2,1,1,11}$, en $r(n, \text{gen } Q)$ moet hier dus een veelvoud van zijn. Uit de coëfficiënten van q^1 in $B_{2,1,1,11}$ en in $r(n, \text{gen } Q)$ volgt dat

$$\Theta(\text{gen } Q) = \frac{12}{5} B_{2,1,1,11} \tag{9.27}$$

en dus, volgens (5.22),

$$r(n, \text{gen } Q) = \frac{12}{5}\sigma(w_{11}(n)). \tag{9.28}$$

Dit heeft een aantal gevolgen. Uit (9.28) volgt dat

$$\sigma(w_{11}(n)) = (2g_2(n) - 1)\, \sigma(w_{22}(n)),$$

hetgeen precies overeenkomt met lemma 3.4.3 voor $a = 11$ en $p = 2$. Dit laat zien dat de vermoede functievoorschriften voor δ_2 en δ_{11} uit (9.24) en (9.25) correct zijn. Daarnaast volgt dat voor $i = 1, 2, 3$,

$$r(n, Q_i) = \frac{12}{5}\sigma(w_{11}(n)) + F_i, \qquad F_i \in \mathfrak{S}_2(\Gamma_0(11)),$$

en dus ook dat

$$F_i = r(n, Q_i) - r(n, \text{gen } Q) \in \mathfrak{S}_2(\Gamma_0(11)).$$

Volgens propositie 6.1.4 is $\mathfrak{S}_2(\Gamma_0(11))$ ééndimensionaal, en daaruit volgt dat de F_i veelvouden van één en dezelfde spitsvorm zijn. Als we dus voldoende representatieaantallen hebben van een Q_i waarvoor $F_i \neq 0$, kunnen we daaruit evenzoveel coëfficiënten van deze spitsvorm vinden. Ook volgt dat het gewogen gemiddelde van deze F_i nul is:

$$\sum_{i=1}^{3} \frac{1}{o(Q_i)} F_i = 0$$

Uit lemma 6.3.1 blijkt dat spitsvormen dichtheid nul hebben. Voor $i = 1, 2, 3$ is de dichtheid van de representaties van Q_i dus gelijk aan die van $\frac{12}{5} B_{2,1,1,11}$ en die bedraagt $\frac{12}{5}\frac{10}{11}\frac{\pi^2}{12} = \frac{2\pi^2}{11}$.

Hieronder volgt een tabel van representatieaantallen, die voor het gemak vermenigvuldigd zijn met 5 om ervoor te zorgen dat alles geheel blijft.

Tabel 9.1: Representaties van kwadratische vormen van niveau $N = 11$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$5r(n, Q_1)$	20	20	40	100	80	160	80	180	140	200	20	320	200	320	280
$5r(n, Q_2)$	30	0	30	120	90	180	60	180	120	180	30	300	240	360	270
$5r(n, Q_3)$	0	60	60	60	60	120	120	180	180	240	0	360	120	240	300
$12\sigma_{2,1,1,11}(n)$	12	36	48	84	72	144	96	180	156	216	12	336	168	288	288
$5F_1$	8	−16	−8	16	8	16	−16	0	−16	−16	8	−16	32	32	−8
$5F_2$	18	−36	−18	36	18	36	−36	0	−36	−36	18	−36	72	72	−18
$5F_3$	−12	24	12	−24	−12	−24	24	0	24	24	−12	24	−48	−48	12

Hoofdstuk 10

Tabellen

We geven hier de tabellen met resultaten van de berekeningen volgens de theorie in de vorige hoofdstukken. We geven een tabel van representatieformules en een tabel van de functies δ_p voor een aantal kwadratische vormen van rang 4.

10.1 Representaties

Tabellen 10.1, 10.2 en 10.3 bevatten de representatieformules. De tabellen 10.1 en 10.2 bevatten alle kwadratische vormen met discriminant 1 732 of minder die uniek in hun geslacht zijn. Volgens conclusie 9.2.9 bevat de representatieformule voor deze vormen gegarandeerd geen spitsvormen. Deze kwadratische vormen zijn afkomstig uit de tabellen van Gordon Nipp [Nip], welke tot en met discriminant 1 732 gaan. Van alle vormen tot deze discriminant die uniek in hun geslacht zijn, staat de representatieformule in deze tabel gegeven.
Er zijn echter mogelijk nog dergelijke kwadratische vormen van hogere discriminant, dus deze lijst is niet volledig.
Ook van kwadratische vormen die niet aan één van deze eigenschappen voldoen, kan het gebeuren dat de coëfficiënten van alle spitsvormen nul zijn, en dus als het ware "toevallig" spitscomponent nul hebben. Tabel 10.3 bevat vormen van hogere discriminant waarvan de representatieformule geen spitsvormen bevat, maar waarvan we het niet weten of ze uniek in hun geslacht zijn.
De kwadratische vormen worden in de tabel weergegeven als vectoren van coëfficiënten. Hierbij staat de vector $[a, b, c, d, e, f, g, h, i, j]$ voor de kwadratische vorm

$$Q : (r, s, t, u) \mapsto ar^2 + bs^2 + ct^2 + du^2 + ers + frt + gst + hru + isu + jtu$$

met matrix

$$A_Q = \begin{pmatrix} 2a & e & f & h \\ e & 2b & g & i \\ f & g & 2c & j \\ h & i & j & 2d \end{pmatrix}.$$

De verkorte vector $[a, b, c, d]$ staat voor $[a, b, c, d, 0, 0, 0, 0, 0, 0]$, oftewel voor de diagonaalvorm $(r, s, t, u) \mapsto ar^2 + bs^2 + ct^2 + du^2$ van determinant $16abcd$.

De kolom D geeft de discriminant van Q. De kolom g geeft de index van het geslacht uit de tabellen van Gordon Nipp in [Nip]. Dit getal betekent verder niets behalve

dat het elk geslacht uniek nummert, deze kolom is vooral toegevoegd ter referentie. De kolom N geeft het niveau van Q. Kolom j geeft aan wat het karakter van Q is. Omdat dit altijd een reëel primitief karakter is, is het van de vorm ρ_j gedefinieerd in stelling 2.4.5, voor een zekere $j \in \mathbb{Z}$. Deze j wordt in de tabel gegeven. Merk op dat $j = s(D)$ voor de functie s uit algoritme 2.4.6.

Tot slot bevat de laatste kolom de representatieformules. De term $e_{a,b,t}$ in deze formules staat voor de gewicht-2 Eisensteinreeks $B_{2,\rho_a,\rho_b,t}$, waarbij ρ_m in stelling 2.4.5 gegeven is als het karakter $a \mapsto \left(\frac{m}{a}\right)$. Alle representaties in de tabel bevatten alleen modulaire vormen met reële karakters. In feite bevatten tot nu toe zelfs alle *basissen* van de ruimtes $\mathfrak{E}_2(N, \varepsilon)$ met ε reëel, alleen basisvormen met reële karakters, met als enige uitzondering tot nu toe de ruimte van niveau 25 en triviaal karakter, welke ook $B_{2,\chi,\chi,1}$ en $B_{2,\overline{\chi},\overline{\chi},1}$ bevat, waarbij χ het karakter modulo 5 is met $\chi(2) = \mathrm{i}$.

Klassificatie van kwadratische vormen

Zoals gezegd is niet zeker of de tabellen compleet zijn. Er is een methode die alle kwadratische vormen genereert tot een bepaalde discriminant D, beschreven in [Nip]. Vanwege het verband tussen N en D in propositie 7.1.10 is deze methode in principe in staat om alle kwadratische vormen te vinden tot een bepaald niveau. Omdat de niveaus voor welke er geen spitsvormen bestaan, bekend zijn, zie propositie 6.1.4 weten we tot hoever we die methode moeten doorvoeren. Het hoogste niveau waarvoor geen gewicht 2-spitsvormen bestaan is $N = 25$ en de hoogste discriminant die mogelijk tot dat niveau leidt is $D = 25^4 = 390\,625$. Vinden we alle kwadratische vormen tot en met discriminant 390 625, dan bevat die lijst hoe dan ook alle kwadratische vormen van de niveaus tot en met 25.
De tabellen van Gordon Nipp gaan tot $D = 1\,732$, wat in totaal circa 74 000 vormen oplevert. Uit deze lijst blijkt ook dat het aantal vormen van discriminant tot en met D ongeveer evenredig is met D^2. Dit geeft een schatting voor het aantal vormen tot en met 390 625 van circa $(\frac{390625}{1732})^2 \cdot 74\,000 \approx 3\,700\,000\,000$ vormen. Vanwege dit grote aantal is deze methode niet verder uitgewerkt. Merk op dat Gordon Nipp's tabellen zeker weten alle kwadratische vormen tot en met niveau $\left\lfloor \sqrt[4]{1732} \right\rfloor = 6$ bevatten.
Voor diagonaalvormen is het gelukkig makkelijker; het niveau van de diagonaalvorm $[a, b, c, d]$ is $4\,\mathrm{kgv}(a, b, c, d)$, waardoor alle diagonaalvormen voor de betreffende niveaus razendsnel gevonden zijn; dit levert zeven vormen op, te weten

$$[1,1,1,1], [1,1,2,2], [1,1,3,3], [1,1,1,4], [1,1,4,4], [1,2,2,4] \text{ en } [1,4,4,4].$$

10.2 De functies δ_p

De tweede belangrijke tabel is die van de functies δ_p van enkele geslachten van kwadratische vormen van niveaus tot en met 19. De kwadratische vormen zijn hier daarom geordend per geslacht en voor elk geslacht g van niveau N wordt voor elk priemgetal $p \mid 2N$ de functie δ_p gegeven. Verder zijn de geslachten geordend op het niveau N dat in de eerste kolom staat. Dit maakt de lijst compleet tot en met niveau 19. De gegevens over de automorfen en de massa's van de geslachten zijn afkomstig uit [Nip]. De andere kolommen bevatten de geslachtsindex g, de massa $w(g)$ de vormen Q in dat geslacht met

het aantal automorfen $o(Q)$ per vorm en de priemgetallen p en deltafunctie δ_p als functie van n.

Tabel 10.1: Representatieformules van diagonaalvormen met $D \leq 1\,732$

D	g	Q	N	j	$r(Q)$
16	1	$[1,1,1,1]$	4	1	$8e_{1,1,4}$
32	1	$[1,1,1,2]$	8	8	$-2e_{1,8,1} + 8e_{8,1,1}$
48	1	$[1,1,1,3]$	12	12	$-2e_{-4,-3,1} + 3e_{-3,-4,1} - e_{1,12,1} + 6e_{12,1,1}$
64	1	$[1,1,1,4]$	16	1	$2e_{-4,-4,1} + 5e_{1,1,4} - 3e_{1,1,8} + 2e_{1,1,16}$
64	3	$[1,1,2,2]$	8	1	$2e_{1,1,2} - 2e_{1,1,4} + 4e_{1,1,8}$
80	2	$[1,1,1,5]$	20	5	$e_{1,5,1} - 2e_{1,5,2} - 4e_{1,5,4} + 5e_{5,1,1} + 10e_{5,1,2} - 20e_{5,1,4}$
96	4	$[1,1,2,3]$	24	24	$4/3e_{-8,-3,1} - e_{-3,-8,1} - 1/3e_{1,24,1} + 4e_{24,1,1}$
128	3	$[1,1,1,8]$	32	8	$2e_{-8,-4,1} + e_{-4,-8,1} - e_{1,8,1} + e_{1,8,2} - 2e_{1,8,4} + 4e_{8,1,1} + 4e_{8,1,2} - 16e_{8,1,4}$
128	4	$[1,1,2,4]$	16	8	$-2e_{1,8,2} + 4e_{8,1,1}$
128	9	$[1,2,2,2]$	8	8	$-2e_{1,8,1} + 4e_{8,1,1}$
144	4	$[1,1,3,3]$	12	1	$4e_{1,1,2} + 4e_{1,1,3} - 4e_{1,1,4} - 4e_{1,1,6} + 4e_{1,1,12}$
192	5	$[1,1,2,6]$	24	12	$e_{-4,-3,1} + 3e_{-3,-4,2} - e_{1,12,2} + 3e_{12,1,1}$
192	9	$[1,2,2,3]$	24	12	$-e_{-4,-3,1} - 3e_{-3,-4,2} - e_{1,12,2} + 3e_{12,1,1}$
256	7	$[1,1,4,4]$	16	1	$2e_{-4,-4,1} + e_{1,1,2} - e_{1,1,8} + 2e_{1,1,16}$
256	10	$[1,2,2,4]$	16	1	$e_{1,1,2} - e_{1,1,8} + 2e_{1,1,16}$
384	12	$[1,2,2,6]$	24	24	$-2/3e_{-8,-3,1} + e_{-3,-8,1} - 1/3e_{1,24,1} + 2e_{24,1,1}$
432	7	$[1,1,3,9]$	36	12	$2e_{-4,-3,3} + 4/3e_{-3,-4,1} + 3e_{-3,-4,3} - e_{1,12,3} + 8/3e_{12,1,1} - 6e_{12,1,3}$
432	13	$[1,3,3,3]$	12	12	$2e_{-4,-3,1} - e_{-3,-4,1} - e_{1,12,1} + 2e_{12,1,1}$
512	9	$[1,1,4,8]$	32	8	$2e_{-8,-4,1} - 2e_{1,8,4} + 2e_{8,1,1}$
512	12	$[1,2,2,8]$	32	8	$e_{-4,-8,1} - e_{1,8,1} + e_{1,8,2} - 2e_{1,8,4} + 2e_{8,1,1}$
512	13	$[1,2,4,4]$	16	8	$-2e_{1,8,2} + 2e_{8,1,1}$
768	23	$[1,2,4,6]$	48	12	$1/2e_{-4,-3,1} - 3e_{-3,-4,4} - e_{1,12,4} + 3/2e_{12,1,1}$
864	27	$[1,3,3,6]$	24	24	$4/3e_{-8,-3,1} - 1/3e_{-3,-8,1} - 1/3e_{1,24,1} + 4/3e_{24,1,1}$
1024	17	$[1,4,4,4]$	16	1	$e_{-4,-4,1} + 3/2e_{1,1,2} - 5/2e_{1,1,4} + 2e_{1,1,16}$
1296	25	$[1,3,3,9]$	36	1	$e_{-3,-3,1} + 2e_{-3,-3,2} + 4e_{-3,-3,4} + e_{1,1,2} - e_{1,1,4} + e_{1,1,9} - e_{1,1,18} + e_{1,1,36}$
1728	39	$[1,3,6,6]$	24	12	$e_{-4,-3,1} + e_{-3,-4,2} - e_{1,12,2} + e_{12,1,1}$
1728	46	$[2,3,3,6]$	24	12	$-e_{-4,-3,1} - e_{-3,-4,2} - e_{1,12,2} + e_{12,1,1}$
D	g	Q	N	j	$r(Q)$

Tabel 10.2: Representatieformules van niet-diagonaalvormen met $D \leq 1\,732$

D	g	Q	N	j	$r(Q)$
4	1	$[1,1,1,1,0,0,0,1,1,1]$	2	1	$24e_{1,1,2}$
5	1	$[1,1,1,1,1,0,0,1,0,1]$	5	5	$-5e_{1,5,1} + 25e_{5,1,1}$
8	1	$[1,1,1,1,0,0,0,1,1,0]$	8	8	$-2e_{1,8,1} + 16e_{8,1,1}$
9	1	$[1,1,1,1,1,0,0,0,0,1]$	3	1	$12e_{1,1,3}$
12	1	$[1,1,1,2,1,1,0,1,0,0]$	12	12	$4e_{-4,-3,1} - 3e_{-3,-4,1} - e_{1,12,1} + 12e_{12,1,1}$
12	2	$[1,1,1,1,0,0,0,1,0,0]$	12	12	$-4e_{-4,-3,1} + 3e_{-3,-4,1} - e_{1,12,1} + 12e_{12,1,1}$
13	1	$[1,1,1,2,1,1,0,0,1,0]$	13	13	$-e_{1,13,1} + 13e_{13,1,1}$
16	2	$[1,1,1,2,1,1,0,0,0,0]$	8	1	$14e_{1,1,2} - 6e_{1,1,4} + 4e_{1,1,8}$
17	1	$[1,1,1,2,1,0,0,1,0,1]$	17	17	$-1/2e_{1,17,1} + 17/2e_{17,1,1}$
20	1	$[1,1,1,3,1,1,0,1,0,0]$	10	5	$-3e_{1,5,1} - 2e_{1,5,2} + 15e_{5,1,1} - 10e_{5,1,2}$
20	2	$[1,1,1,2,0,0,0,1,1,1]$	10	5	$e_{1,5,1} - 6e_{1,5,2} + 5e_{5,1,1} + 30e_{5,1,2}$
20	3	$[1,1,1,2,1,0,0,1,0,0]$	20	5	$-2e_{1,5,1} + e_{1,5,2} - 4e_{1,5,4} + 10e_{5,1,1} + 5e_{5,1,2} + 20e_{5,1,4}$
21	1	$[1,1,1,2,1,0,0,0,0,1]$	21	21	$-7/2e_{-7,-3,1} + 3/2e_{-3,-7,1} - 1/2e_{1,21,1} + 21/2e_{21,1,1}$
21	2	$[1,1,1,3,1,1,0,0,1,0]$	21	21	$7/2e_{-7,-3,1} - 3/2e_{-3,-7,1} - 1/2e_{1,21,1} + 21/2e_{21,1,1}$
24	2	$[1,1,1,2,0,0,0,1,1,0]$	24	24	$-8/3e_{-8,-3,1} + e_{-3,-8,1} - 1/3e_{1,24,1} + 8e_{24,1,1}$
25	1	$[1,1,2,2,1,1,0,1,1,2]$	5	1	$6e_{1,1,5}$
28	2	$[1,1,2,2,1,1,0,0,1,1]$	28	28	$-7/4e_{-7,-4,1} + e_{-4,-7,1} - 1/4e_{1,28,1} + 7e_{28,1,1}$
32	2	$[1,1,1,3,1,0,0,1,0,0]$	32	8	$2e_{-8,-4,1} - e_{-4,-8,1} - e_{1,8,1} + e_{1,8,2} - 2e_{1,8,4} + 8e_{8,1,1} - 4e_{8,1,2} + 16e_{8,1,4}$
32	3	$[1,1,1,4,1,1,0,0,0,0]$	16	8	$-2e_{1,8,2} + 12e_{8,1,1} - 16e_{8,1,2}$
32	4	$[1,1,2,2,0,0,0,1,1,2]$	16	8	$-2e_{1,8,2} + 4e_{8,1,1} + 16e_{8,1,2}$
32	5	$[1,1,2,2,1,1,0,1,0,0]$	32	8	$-2e_{-8,-4,1} + e_{-4,-8,1} - e_{1,8,1} + e_{1,8,2} - 2e_{1,8,4} + 8e_{8,1,1} - 4e_{8,1,2} + 16e_{8,1,4}$
33	2	$[1,1,2,2,0,1,1,1,0,2]$	33	33	$-11/6e_{-11,-3,1} + 1/2e_{-3,-11,1} - 1/6e_{1,33,1} + 11/2e_{33,1,1}$
36	1	$[1,1,1,5,1,1,0,1,0,0]$	18	1	$3e_{-3,-3,1} + 6e_{-3,-3,2} + 9e_{1,1,2} + 4e_{1,1,3} - 4e_{1,1,6} - 3e_{1,1,9} + 3e_{1,1,18}$
36	2	$[1,1,1,3,0,0,0,1,1,1]$	18	1	$-3e_{-3,-3,1} - 6e_{-3,-3,2} + 9e_{1,1,2} + 4e_{1,1,3} - 4e_{1,1,6} - 3e_{1,1,9} + 3e_{1,1,18}$
36	3	$[1,1,1,3,1,0,0,0,0,0]$	12	1	$6e_{1,1,2} + 8e_{1,1,3} - 4e_{1,1,4} - 6e_{1,1,6} + 4e_{1,1,12}$
36	4	$[1,1,2,2,1,0,0,0,0,2]$	6	1	$6e_{1,1,2} - 6e_{1,1,3} + 6e_{1,1,6}$
36	5	$[1,1,2,2,0,1,1,1,1,1]$	6	1	$-4e_{1,1,2} + 4e_{1,1,3} + 4e_{1,1,6}$
45	1	$[1,1,1,4,1,0,0,0,0,1]$	15	5	$-2e_{1,5,1} - 3e_{1,5,3} + 10e_{5,1,1} - 15e_{5,1,3}$
45	3	$[1,1,2,2,1,0,0,0,0,1]$	15	5	$e_{1,5,1} - 6e_{1,5,3} + 5e_{5,1,1} + 30e_{5,1,3}$
45	4	$[1,1,2,2,0,1,0,0,1,1]$	45	5	$-5/2e_{-15,-3,1} + 1/2e_{-3,-15,1} - 3/2e_{1,5,1} + e_{1,5,3} - 9/2e_{1,5,9} + 15/2e_{5,1,1} + 5e_{5,1,3} + 45/2e_{5,1,9}$
48	3	$[1,1,1,6,1,1,0,0,0,0]$	24	12	$3e_{-4,-3,1} + 4e_{-4,-3,2} + 3e_{-3,-4,2} - e_{1,12,2} + 9e_{12,1,1} - 12e_{12,1,2}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
48	4	$[1,1,2,3,1,1,0,0,1,1]$	48	12	$2e_{-4,-3,1} + e_{-4,-3,2} + 4e_{-4,-3,4} - 3/2e_{-3,-4,1} - 3/2e_{-3,-4,2} - 3e_{-3,-4,4} - 1/2e_{1,12,1} + 1/2e_{1,12,2} - e_{1,12,4} + 6e_{12,1,1} - 3e_{12,1,2} + 12e_{12,1,4}$
48	5	$[1,1,2,2,0,1,1,0,0,0]$	24	12	$e_{-4,-3,1} - 4e_{-4,-3,2} + 3e_{-3,-4,2} - e_{1,12,2} + 3e_{12,1,1} + 12e_{12,1,2}$
48	6	$[1,1,2,2,0,0,0,0,0,2]$	12	12	$2e_{-4,-3,1} - 3e_{-3,-4,1} - e_{1,12,1} + 6e_{12,1,1}$
48	7	$[1,1,2,2,1,0,0,0,0,0]$	24	12	$-3e_{-4,-3,1} - 4e_{-4,-3,2} - 3e_{-3,-4,2} - e_{1,12,2} + 9e_{12,1,1} - 12e_{12,1,2}$
48	8	$[1,2,2,2,0,0,0,1,2,2]$	24	12	$-e_{-4,-3,1} + 4e_{-4,-3,2} - 3e_{-3,-4,2} - e_{1,12,2} + 3e_{12,1,1} + 12e_{12,1,2}$
49	1	$[1,1,2,2,0,1,0,0,1,0]$	7	1	$4e_{1,1,7}$
60	4	$[1,2,2,2,1,0,2,0,1,2]$	60	15	$-5/3e_{-20,-3,1} - 5/4e_{-15,-4,1} + 1/3e_{-4,-15,1} + 1/4e_{-3,-20,1} - 1/12e_{1,60,1} + 5/12e_{5,12,1} - e_{12,5,1} + 5e_{60,1,1}$
64	4	$[1,1,3,3,1,1,0,1,1,3]$	8	1	$9e_{1,1,2} - 9e_{1,1,4} + 6e_{1,1,8}$
64	5	$[1,1,2,3,1,0,0,1,0,0]$	32	1	$-2e_{-4,-4,2} + 7e_{1,1,2} - 3e_{1,1,4} + 5/2e_{1,1,8} - 3/2e_{1,1,16} + e_{1,1,32}$
64	6	$[1,2,2,2,0,0,2,0,2,0]$	16	1	$-2e_{-4,-4,1} + 5e_{1,1,4} - 3e_{1,1,8} + 2e_{1,1,16}$
69	2	$[1,1,2,3,0,1,0,1,1,0]$	69	69	$-23/12e_{-23,-3,1} + 1/4e_{-3,-23,1} - 1/12e_{1,69,1} + 23/4e_{69,1,1}$
80	4	$[1,1,3,3,1,1,0,0,1,1]$	20	5	$-3/2e_{1,5,1} - 3/2e_{1,5,2} - 2e_{1,5,4} + 15/2e_{5,1,1} - 15/2e_{5,1,2} + 10e_{5,1,4}$
80	5	$[1,1,2,3,0,0,0,0,0,2]$	20	5	$-e_{1,5,1} - 4e_{1,5,4} + 5e_{5,1,1} + 20e_{5,1,4}$
80	8	$[1,2,2,2,1,1,0,1,0,0]$	20	5	$-1/2e_{1,5,1} + 3/2e_{1,5,2} - 6e_{1,5,4} + 5/2e_{5,1,1} + 15/2e_{5,1,2} + 30e_{5,1,4}$
81	2	$[1,1,2,4,0,1,1,1,0,2]$	27	1	$-3e_{-3,-3,3} + 13/3e_{1,1,3} - 4/3e_{1,1,9} + e_{1,1,27}$
81	3	$[1,1,3,3,1,0,0,0,0,3]$	9	1	$3e_{-3,-3,1} + 3e_{1,1,9}$
81	4	$[2,2,2,2,1,1,1,2,2,-1]$	9	1	$-3e_{-3,-3,1} + 3e_{1,1,9}$
96	8	$[1,1,2,4,0,1,0,0,0,2]$	96	24	$e_{-24,-4,1} - 4/3e_{-8,-3,1} - 2/3e_{-8,-3,2} - 8/3e_{-8,-3,4} - 1/6e_{-4,-24,1} + 1/2e_{-3,-8,1} + 1/2e_{-3,-8,2} + e_{-3,-8,4} - 1/6e_{1,24,1} + 1/6e_{1,24,2} - 1/3e_{1,24,4} - 1/3e_{8,12,1} + 1/2e_{12,8,1} + 4e_{24,1,1} - 2e_{24,1,2} + 8e_{24,1,4}$
96	9	$[1,1,3,3,0,1,1,1,1,0]$	48	24	$-2e_{-8,-3,1} - 8/3e_{-8,-3,2} - e_{-3,-8,2} - 1/3e_{1,24,2} + 6e_{24,1,1} - 8e_{24,1,2}$
96	10	$[1,2,2,2,0,0,0,1,1,1]$	96	24	$-e_{-24,-4,1} - 4/3e_{-8,-3,1} - 2/3e_{-8,-3,2} - 8/3e_{-8,-3,4} + 1/6e_{-4,-24,1} + 1/2e_{-3,-8,1} + 1/2e_{-3,-8,2} + e_{-3,-8,4} - 1/6e_{1,24,1} + 1/6e_{1,24,2} - 1/3e_{1,24,4} + 1/3e_{8,12,1} - 1/2e_{12,8,1} + 4e_{24,1,1} - 2e_{24,1,2} + 8e_{24,1,4}$
100	3	$[1,1,3,3,0,1,1,1,1,1]$	10	1	$4e_{1,1,2} - 4e_{1,1,5} + 4e_{1,1,10}$
100	5	$[1,2,2,3,1,0,2,0,1,2]$	10	1	$-2e_{1,1,2} + 2e_{1,1,5} + 2e_{1,1,10}$
108	5	$[1,1,2,5,0,1,1,1,1,1]$	36	12	$-4e_{-4,-3,3} - 4/3e_{-3,-4,1} - 3e_{-3,-4,3} - e_{1,12,3} + 16/3e_{12,1,1} - 12e_{12,1,3}$
108	6	$[1,1,3,3,1,0,0,0,0,0]$	12	12	$4e_{-4,-3,1} - e_{-3,-4,1} - e_{1,12,1} + 4e_{12,1,1}$
108	7	$[1,2,2,3,0,0,2,-1,1,-1]$	36	12	$-4e_{-4,-3,3} - 2/3e_{-3,-4,1} + 3e_{-3,-4,3} - e_{1,12,3} + 8/3e_{12,1,1} + 12e_{12,1,3}$
108	8	$[2,2,2,2,2,1,-1,-1,1,-1]$	12	12	$-4e_{-4,-3,1} + e_{-3,-4,1} - e_{1,12,1} + 4e_{12,1,1}$
112	3	$[1,1,2,5,1,0,0,1,0,0]$	56	28	$-7/4e_{-7,-4,2} + 3/4e_{-4,-7,1} - e_{-4,-7,2} - 1/4e_{1,28,2} + 21/4e_{28,1,1} - 7e_{28,1,2}$
112	7	$[1,2,2,3,0,0,2,0,2,0]$	28	28	$-7/4e_{-7,-4,1} + 1/2e_{-4,-7,1} - 1/4e_{1,28,1} + 7/2e_{28,1,1}$
112	8	$[1,2,2,3,1,0,2,0,1,0]$	56	28	$-7/4e_{-7,-4,2} + 1/4e_{-4,-7,1} + e_{-4,-7,2} - 1/4e_{1,28,2} + 7/4e_{28,1,1} + 7e_{28,1,2}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
125	2	$[1,1,2,7,1,1,0,1,1,2]$	25	5	$-5e_{1,5,5}+6e_{5,1,1}-25e_{5,1,5}$
125	3	$[2,2,2,2,1,1,-1,-1,1,1]$	5	5	$-5e_{1,5,1}+5e_{5,1,1}$
125	4	$[1,1,3,4,0,1,1,1,0,3]$	25	5	$-5e_{1,5,5}+4e_{5,1,1}+25e_{5,1,5}$
128	7	$[1,1,3,4,1,1,0,0,0,0]$	32	8	$-2e_{1,8,4}+6e_{8,1,1}-12e_{8,1,2}+16e_{8,1,4}$
128	8	$[1,1,3,5,1,1,0,1,1,3]$	64	8	$-2e_{-8,-4,2}-e_{-4,-8,2}-e_{1,8,2}+e_{1,8,4}-2e_{1,8,8}+6e_{8,1,1}-8e_{8,1,2}+4e_{8,1,4}-16e_{8,1,8}$
128	10	$[1,2,2,4,1,0,2,0,2,0]$	64	8	$-2e_{-8,-4,2}+e_{-4,-8,2}-e_{1,8,2}+e_{1,8,4}-2e_{1,8,8}+2e_{8,1,1}+8e_{8,1,2}-4e_{8,1,4}+16e_{8,1,8}$
128	11	$[1,1,3,3,0,0,0,0,0,2]$	32	8	$2e_{-8,-4,1}-e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+4e_{8,1,1}-4e_{8,1,2}+16e_{8,1,4}$
128	12	$[1,2,2,3,1,1,0,0,1,1]$	32	8	$-2e_{1,8,4}+2e_{8,1,1}+4e_{8,1,2}+16e_{8,1,4}$
128	13	$[1,2,2,3,0,0,0,0,2,2]$	32	8	$-2e_{-8,-4,1}+e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+4e_{8,1,1}-4e_{8,1,2}+16e_{8,1,4}$
128	14	$[2,2,2,3,2,2,0,2,0,0]$	32	8	$-2e_{-8,-4,1}-e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+4e_{8,1,1}+4e_{8,1,2}-16e_{8,1,4}$
144	5	$[1,1,4,4,1,0,0,0,0,4]$	12	1	$9e_{1,1,2}+6e_{1,1,3}-6e_{1,1,4}-9e_{1,1,6}+6e_{1,1,12}$
144	6	$[1,2,2,4,1,1,0,1,2,2]$	12	1	$-e_{1,1,2}+2e_{1,1,3}-2e_{1,1,4}+e_{1,1,6}+2e_{1,1,12}$
144	7	$[1,1,2,5,0,0,0,0,0,2]$	36	1	$e_{-3,-3,1}-4e_{-3,-3,4}+4/3e_{1,1,3}+3e_{1,1,4}-e_{1,1,9}-4/3e_{1,1,12}+e_{1,1,36}$
144	12	$[1,2,2,3,0,0,2,0,0,0]$	12	1	$-2e_{1,1,3}+2e_{1,1,4}+2e_{1,1,12}$
169	1	$[1,2,2,4,1,0,1,1,1,2]$	13	1	$2e_{1,1,13}$
189	5	$[2,2,2,2,1,1,1,1,1,1]$	21	21	$-7/2e_{-7,-3,1}+1/2e_{-3,-7,1}-1/2e_{1,21,1}+7/2e_{21,1,1}$
189	6	$[1,1,3,6,1,0,0,0,0,3]$	21	21	$7/2e_{-7,-3,1}-1/2e_{-3,-7,1}-1/2e_{1,21,1}+7/2e_{21,1,1}$
189	7	$[1,1,4,4,0,1,0,0,1,3]$	63	21	$-7/2e_{-7,-3,3}-2/3e_{-3,-7,1}-3/2e_{-3,-7,3}-1/2e_{1,21,3}+14/3e_{21,1,1}-21/2e_{21,1,3}$
189	8	$[1,2,3,3,0,1,1,1,2,1]$	63	21	$-7/2e_{-7,-3,3}-1/3e_{-3,-7,1}+3/2e_{-3,-7,3}-1/2e_{1,21,3}+7/3e_{21,1,1}+21/2e_{21,1,3}$
192	7	$[1,1,3,7,1,1,0,1,1,3]$	48	12	$3/2e_{-4,-3,1}+3e_{-4,-3,2}+4e_{-4,-3,4}-3e_{-3,-4,4}-e_{1,12,4}+9/2e_{12,1,1}-9e_{12,1,2}+12e_{12,1,4}$
192	13	$[1,1,4,4,0,0,0,0,0,4]$	12	12	$-e_{-4,-3,1}+3e_{-3,-4,1}-e_{1,12,1}+3e_{12,1,1}$
192	16	$[1,2,2,4,0,0,2,0,0,0]$	48	12	$e_{-4,-3,1}-e_{-4,-3,2}-4e_{-4,-3,4}-3/2e_{-3,-4,1}-3/2e_{-3,-4,2}-3e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+3e_{12,1,1}+3e_{12,1,2}-12e_{12,1,4}$
192	18	$[1,2,3,3,1,0,1,0,-1,2]$	48	12	$1/2e_{-4,-3,1}-e_{-4,-3,2}+4e_{-4,-3,4}-3e_{-3,-4,4}-e_{1,12,4}+3/2e_{12,1,1}+3e_{12,1,2}+12e_{12,1,4}$
192	19	$[1,2,3,3,0,0,2,0,2,0]$	48	12	$e_{-4,-3,1}+e_{-4,-3,2}+4e_{-4,-3,4}-3/2e_{-3,-4,1}-3/2e_{-3,-4,2}-3e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+3e_{12,1,1}-3e_{12,1,2}+12e_{12,1,4}$
192	20	$[2,2,2,3,0,0,0,2,2,2]$	12	12	$e_{-4,-3,1}-3e_{-3,-4,1}-e_{1,12,1}+3e_{12,1,1}$
216	8	$[2,2,2,3,2,1,-1,0,0,0]$	24	24	$-8/3e_{-8,-3,1}+1/3e_{-3,-8,1}-1/3e_{1,24,1}+8/3e_{24,1,1}$
240	14	$[1,2,3,3,0,1,0,1,0,0]$	120	15	$-5/4e_{-20,-3,1}-5/3e_{-20,-3,2}-5/4e_{-15,-4,2}+1/4e_{-4,-15,1}-1/3e_{-4,-15,2}-1/4e_{-3,-20,2}-1/12e_{1,60,2}-5/12e_{5,12,2}-3/4e_{12,5,1}-e_{12,5,2}+15/4e_{60,1,1}-5e_{60,1,2}$
240	15	$[1,2,3,3,0,0,0,0,2,0]$	60	15	$5/6e_{-20,-3,1}-5/4e_{-15,-4,1}+1/6e_{-4,-15,1}-1/4e_{-3,-20,1}-1/12e_{1,60,1}-5/12e_{5,12,1}+1/2e_{12,5,1}+5/2e_{60,1,1}$
256	11	$[1,2,2,6,0,0,2,0,2,0]$	64	1	$1/2e_{-8,-8,1}-e_{-4,-4,1}-2e_{-4,-4,4}+5/2e_{1,1,4}-3/2e_{1,1,8}+5/4e_{1,1,16}-3/4e_{1,1,32}+1/2e_{1,1,64}+1/2e_{8,8,1}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
256	12	$[1,2,3,3,0,0,0,0,0,2]$	32	1	$-2e_{-4,-4,2}+e_{1,1,2}-e_{1,1,4}+5/2e_{1,1,8}-3/2e_{1,1,16}+e_{1,1,32}$
256	13	$[1,3,3,3,0,0,2,0,2,-2]$	8	1	$3e_{1,1,2}-7e_{1,1,4}+6e_{1,1,8}$
256	14	$[2,2,3,3,0,2,2,2,2,2]$	16	1	$-2e_{-4,-4,1}+e_{1,1,2}-e_{1,1,8}+2e_{1,1,16}$
256	15	$[2,2,3,3,2,2,0,0,2,0]$	64	1	$-1/2e_{-8,-8,1}-e_{-4,-4,1}-2e_{-4,-4,4}+5/2e_{1,1,4}-3/2e_{1,1,8}+5/4e_{1,1,16}-3/4e_{1,1,32}+1/2e_{1,1,64}-1/2e_{8,8,1}$
297	6	$[2,2,2,5,2,1,-1,1,2,1]$	33	33	$-11/6e_{-11,-3,1}+1/6e_{-3,-11,1}-1/6e_{1,33,1}+11/6e_{33,1,1}$
320	19	$[1,3,3,3,0,0,2,0,2,2]$	20	5	$-1/2e_{1,5,1}-1/2e_{1,5,2}-4e_{1,5,4}+5/2e_{5,1,1}-5/2e_{5,1,2}+20e_{5,1,4}$
324	6	$[1,1,6,6,1,0,0,0,0,6]$	18	1	$3e_{-3,-3,1}+6e_{-3,-3,2}+3e_{1,1,2}+2e_{1,1,3}-2e_{1,1,6}-3e_{1,1,9}+3e_{1,1,18}$
324	7	$[2,2,2,3,1,1,1,0,0,0]$	36	1	$-2e_{-3,-3,1}-3e_{-3,-3,2}-4e_{-3,-3,4}+3/2e_{1,1,2}-e_{1,1,4}+2e_{1,1,9}-3/2e_{1,1,18}+e_{1,1,36}$
324	8	$[2,2,2,5,2,1,-1,-1,1,-1]$	18	1	$-e_{-3,-3,1}+2e_{-3,-3,2}-e_{1,1,2}+e_{1,1,9}+e_{1,1,18}$
324	12	$[1,1,5,5,0,1,1,1,1,1]$	18	1	$4e_{1,1,2}+16/3e_{1,1,3}-16/3e_{1,1,6}-4e_{1,1,9}+4e_{1,1,18}$
324	14	$[1,2,3,5,0,1,2,0,2,1]$	18	1	$2e_{1,1,2}-4/3e_{1,1,3}+4/3e_{1,1,6}-2e_{1,1,9}+2e_{1,1,18}$
324	15	$[1,3,3,4,0,0,0,1,3,3]$	18	1	$e_{-3,-3,1}-2e_{-3,-3,2}-e_{1,1,2}+e_{1,1,9}+e_{1,1,18}$
324	16	$[2,2,3,3,2,0,0,0,0,3]$	18	1	$-3e_{-3,-3,1}-6e_{-3,-3,2}+3e_{1,1,2}+2e_{1,1,3}-2e_{1,1,6}-3e_{1,1,9}+3e_{1,1,18}$
384	11	$[1,1,5,5,0,0,0,0,0,2]$	96	24	$e_{-24,-4,1}+2/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}+1/6e_{-4,-24,1}-1/2e_{-3,-8,1}-1/2e_{-3,-8,2}-e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}+1/3e_{8,12,1}+1/2e_{12,8,1}+2e_{24,1,1}+2e_{24,1,2}-8e_{24,1,4}$
384	26	$[1,3,3,4,1,1,0,0,2,2]$	192	24	$-e_{-24,-4,2}-e_{-8,-3,1}-4/3e_{-8,-3,2}-2/3e_{-8,-3,4}-8/3e_{-8,-3,8}-1/6e_{-4,-24,2}-1/2e_{-3,-8,2}-1/2e_{-3,-8,4}-e_{-3,-8,8}-1/6e_{1,24,2}+1/6e_{1,24,4}-1/3e_{1,24,8}-1/3e_{8,12,2}-1/2e_{12,8,2}+3e_{24,1,1}-4e_{24,1,2}+2e_{24,1,4}-8e_{24,1,8}$
384	27	$[1,3,3,4,1,1,-1,0,-2,2]$	96	24	$-e_{-8,-3,1}-2e_{-8,-3,2}-8/3e_{-8,-3,4}+e_{-3,-8,4}-1/3e_{1,24,4}+3e_{24,1,1}-6e_{24,1,2}+8e_{24,1,4}$
384	28	$[2,2,3,3,0,0,0,2,2,0]$	96	24	$-e_{-24,-4,1}+2/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}-1/6e_{-4,-24,1}-1/2e_{-3,-8,1}-1/2e_{-3,-8,2}-e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}-1/3e_{8,12,1}-1/2e_{12,8,1}+2e_{24,1,1}+2e_{24,1,2}-8e_{24,1,4}$
400	11	$[1,2,3,5,0,0,2,0,0,0]$	20	1	$2e_{1,1,2}-2e_{1,1,4}+2e_{1,1,5}-2e_{1,1,10}+2e_{1,1,20}$
405	5	$[1,1,3,12,1,0,0,0,0,3]$	45	5	$5/2e_{-15,-3,1}+1/2e_{-3,-15,1}+1/2e_{1,5,1}-e_{1,5,3}-9/2e_{1,5,9}+5/2e_{5,1,1}+5e_{5,1,3}-45/2e_{5,1,9}$
405	11	$[2,2,2,5,1,1,1,-2,-2,1]$	45	5	$-5/2e_{-15,-3,1}+1/2e_{-3,-15,1}-1/2e_{1,5,1}-9/2e_{1,5,9}+5/2e_{5,1,1}+45/2e_{5,1,9}$
405	12	$[2,2,3,3,1,0,0,0,0,3]$	45	5	$-5/2e_{-15,-3,1}-1/2e_{-3,-15,1}+1/2e_{1,5,1}-e_{1,5,3}-9/2e_{1,5,9}+5/2e_{5,1,1}+5e_{5,1,3}-45/2e_{5,1,9}$
432	9	$[1,1,5,6,0,1,1,0,0,0]$	72	12	$-3e_{-4,-3,3}-4e_{-4,-3,6}+4/3e_{-3,-4,2}+3e_{-3,-4,6}-e_{1,12,6}+4e_{12,1,1}-16/3e_{12,1,2}-9e_{12,1,3}+12e_{12,1,6}$
432	14	$[2,2,2,6,2,1,-1,0,0,0]$	24	12	$-e_{-4,-3,1}+4e_{-4,-3,2}-e_{-3,-4,2}-e_{1,12,2}+e_{12,1,1}+4e_{12,1,2}$
432	20	$[1,1,6,6,1,0,0,0,0,0]$	24	12	$3e_{-4,-3,1}+4e_{-4,-3,2}+e_{-3,-4,2}-e_{1,12,2}+3e_{12,1,1}-4e_{12,1,2}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
432	23	$[1,2,3,5,0,0,0,0,2,0]$	36	12	$2e_{-4,-3,3}+2/3e_{-3,-4,1}-3e_{-3,-4,3}-e_{1,12,3}+4/3e_{12,1,1}+6e_{12,1,3}$
432	25	$[1,2,3,6,0,1,2,0,0,0]$	72	12	$-3e_{-4,-3,3}-4e_{-4,-3,6}+2/3e_{-3,-4,2}-3e_{-3,-4,6}-e_{1,12,6}+2e_{12,1,1}-8/3e_{12,1,2}+9e_{12,1,3}-12e_{12,1,6}$
432	28	$[1,2,4,5,1,0,2,1,1,2]$	144	12	$-2e_{-4,-3,3}-e_{-4,-3,6}-4e_{-4,-3,12}-2/3e_{-3,-4,1}-2/3e_{-3,-4,2}-3/2e_{-3,-4,3}-4/3e_{-3,-4,4}-3/2e_{-3,-4,6}-3e_{-3,-4,12}-1/2e_{1,12,3}+1/2e_{1,12,6}-e_{1,12,12}+8/3e_{12,1,1}-4/3e_{12,1,2}-6e_{12,1,3}+16/3e_{12,1,4}+3e_{12,1,6}-12e_{12,1,12}$
432	29	$[1,3,4,4,0,1,3,1,3,2]$	24	12	$e_{-4,-3,1}-4e_{-4,-3,2}+e_{-3,-4,2}-e_{1,12,2}+e_{12,1,1}+4e_{12,1,2}$
432	30	$[2,2,2,5,1,1,1,2,2,2]$	48	12	$-2e_{-4,-3,1}-e_{-4,-3,2}-4e_{-4,-3,4}+1/2e_{-3,-4,1}+1/2e_{-3,-4,2}+e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+2e_{12,1,1}-e_{12,1,2}+4e_{12,1,4}$
432	31	$[2,2,3,3,2,0,0,0,0,0]$	12	12	$-2e_{-4,-3,1}+e_{-3,-4,1}-e_{1,12,1}+2e_{12,1,1}$
432	32	$[2,3,3,3,0,0,0,0,3,3]$	24	12	$-3e_{-4,-3,1}-4e_{-4,-3,2}-e_{-3,-4,2}-e_{1,12,2}+3e_{12,1,1}-4e_{12,1,2}$
448	17	$[1,2,3,5,0,0,0,0,0,2]$	56	28	$-7/4e_{-7,-4,2}+1/4e_{-4,-7,1}-1/4e_{1,28,2}+7/4e_{28,1,1}$
448	20	$[2,3,3,3,2,2,0,2,2,0]$	28	28	$-7/4e_{-7,-4,1}+1/4e_{-4,-7,1}-1/4e_{1,28,1}+7/4e_{28,1,1}$
484	5	$[1,2,3,6,0,1,0,0,2,0]$	22	1	$2e_{1,1,2}-2e_{1,1,11}+2e_{1,1,22}$
500	9	$[1,4,4,4,1,1,-2,1,3,3]$	10	5	$e_{1,5,1}-6e_{1,5,2}+e_{5,1,1}+6e_{5,1,2}$
500	11	$[2,2,2,5,1,1,-1,0,0,0]$	20	5	$-2e_{1,5,1}+e_{1,5,2}-4e_{1,5,4}+2e_{5,1,1}+e_{5,1,2}+4e_{5,1,4}$
500	12	$[2,3,3,3,2,2,1,2,1,1]$	10	1	$-3e_{1,5,1}-2e_{1,5,2}+3e_{5,1,1}-2e_{5,1,2}$
512	20	$[1,2,4,5,0,0,0,0,0,4]$	64	8	$-2e_{-8,-4,2}+e_{-4,-8,2}-e_{1,8,2}+e_{1,8,4}-2e_{1,8,8}+2e_{8,1,1}-4e_{8,1,4}+16e_{8,1,8}$
512	22	$[1,3,3,4,0,0,2,0,0,0]$	32	8	$-2e_{1,8,4}+2e_{8,1,1}-4e_{8,1,2}+16e_{8,1,4}$
512	23	$[1,3,3,5,0,0,2,0,-2,2]$	64	8	$-2e_{-8,-4,2}-e_{-4,-8,2}-e_{1,8,2}+e_{1,8,4}-2e_{1,8,8}+2e_{8,1,1}+4e_{8,1,4}-16e_{8,1,8}$
512	24	$[1,4,4,4,0,0,0,0,4,4]$	32	8	$2e_{-8,-4,1}-e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+2e_{8,1,1}-4e_{8,1,2}+16e_{8,1,4}$
512	25	$[2,2,3,3,0,0,0,0,0,2]$	32	8	$-e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+2e_{8,1,1}$
512	26	$[2,2,3,4,0,2,2,0,0,0]$	32	8	$-2e_{-8,-4,1}-2e_{1,8,4}+2e_{8,1,1}$
512	27	$[2,2,3,5,2,2,0,0,0,2]$	128	8	$-e_{-8,-4,1}-2e_{-8,-4,4}-1/2e_{-4,-8,1}-e_{-4,-8,4}-1/2e_{1,8,1}+1/2e_{1,8,2}-e_{1,8,4}+e_{1,8,8}-2e_{1,8,16}+2e_{8,1,1}+2e_{8,1,2}-8e_{8,1,4}+4e_{8,1,8}-16e_{8,1,16}$
512	28	$[2,3,3,3,0,0,2,0,2,-2]$	8	8	$-2e_{1,8,1}+2e_{8,1,1}$
512	29	$[3,3,3,3,2,2,-2,-2,-2,2]$	32	8	$-2e_{-8,-4,1}+e_{-4,-8,1}-e_{1,8,1}+e_{1,8,2}-2e_{1,8,4}+2e_{8,1,1}-4e_{8,1,2}+16e_{8,1,4}$
528	16	$[1,3,3,5,1,1,-1,1,1,0]$	132	33	$-11/12e_{-11,-3,1}-11/4e_{-11,-3,2}-11/3e_{-11,-3,4}+1/4e_{-3,-11,1}+3/4e_{-3,-11,2}+e_{-3,-11,4}-1/12e_{1,33,1}+1/4e_{1,33,2}-1/3e_{1,33,4}+11/4e_{33,1,1}-33/4e_{33,1,2}+11e_{33,1,4}$
540	16	$[2,2,3,5,2,0,0,2,1,3]$	60	15	$-5/3e_{-20,-3,1}+5/12e_{-15,-4,1}-1/3e_{-4,-15,1}+1/12e_{-3,-20,1}-1/12e_{1,60,1}-5/12e_{5,12,1}+1/3e_{12,5,1}+5/3e_{60,1,1}$
576	30	$[1,3,4,4,0,0,0,0,0,4]$	12	1	$3e_{1,1,2}+2e_{1,1,3}-4e_{1,1,4}-3e_{1,1,6}+4e_{1,1,12}$
621	8	$[2,2,3,5,1,0,0,2,2,3]$	69	69	$-23/12e_{-23,-3,1}+1/12e_{-3,-23,1}-1/12e_{1,69,1}+23/12e_{69,1,1}$
625	3	$[1,4,4,4,1,1,-2,-1,-3,2]$	25	1	$e_{1,1,25}+e_{5,5,1}$
625	4	$[2,2,2,7,1,1,-1,1,-1,-1]$	25	1	$e_{1,1,25}-e_{5,5,1}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
729	7	$[2,2,2,8,1,1,1,2,2,-1]$	27	1	$-e_{-3,-3,1}+3e_{-3,-3,3}+1/3e_{1,1,3}-1/3e_{1,1,9}+e_{1,1,27}$
729	8	$[2,2,5,5,2,1,-1,1,2,4]$	27	1	$-e_{-3,-3,1}-3e_{-3,-3,3}+1/3e_{1,1,3}-1/3e_{1,1,9}+e_{1,1,27}$
729	9	$[1,4,4,4,1,1,-1,1,2,2]$	27	1	$e_{-3,-3,1}-3e_{-3,-3,3}+1/3e_{1,1,3}-1/3e_{1,1,9}+e_{1,1,27}$
768	27	$[1,1,8,8,0,0,0,0,0,8]$	24	12	$1/2e_{-4,-3,1}+3/2e_{-3,-4,1}+9/2e_{-3,-4,2}+1/2e_{1,12,1}-3/2e_{1,12,2}+3/2e_{12,1,1}$
768	37	$[1,3,3,7,0,0,2,0,-2,2]$	48	12	$1/2e_{-4,-3,1}+e_{-4,-3,2}+4e_{-4,-3,4}-3e_{-3,-4,4}-e_{1,12,4}+3/2e_{12,1,1}-3e_{12,1,2}+12e_{12,1,4}$
768	38	$[1,4,4,4,0,0,0,0,0,4]$	48	12	$-(1/2)e_{-4,-3,1}-e_{-4,-3,2}-4e_{-4,-3,4}+3/2e_{-3,-4,1}+3/2e_{-3,-4,2}+3e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+3/2e_{12,1,1}-3e_{12,1,2}+12e_{12,1,4}$
768	39	$[1,4,4,5,0,0,0,0,4,4]$	24	12	$-(1/2)e_{-4,-3,1}+3/2e_{-3,-4,1}-3/2e_{-3,-4,2}-1/2e_{1,12,1}-1/2e_{1,12,2}+3/2e_{12,1,1}$
768	40	$[2,2,3,7,0,2,2,2,2,2]$	24	12	$1/2e_{-4,-3,1}-3/2e_{-3,-4,1}+3/2e_{-3,-4,2}-1/2e_{1,12,1}-1/2e_{1,12,2}+3/2e_{12,1,1}$
768	41	$[2,3,3,4,2,2,0,0,0,0]$	48	12	$1/2e_{-4,-3,1}-3/2e_{-3,-4,1}-3/2e_{-3,-4,2}-3e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+3/2e_{12,1,1}$
768	43	$[3,3,3,3,2,2,2,2,2,2]$	48	12	$1/2e_{-4,-3,1}+e_{-4,-3,2}+4e_{-4,-3,4}-3/2e_{-3,-4,1}-3/2e_{-3,-4,2}-3e_{-3,-4,4}-1/2e_{1,12,1}+1/2e_{1,12,2}-e_{1,12,4}+3/2e_{12,1,1}-3e_{12,1,2}+12e_{12,1,4}$
768	44	$[3,3,3,3,2,0,0,2,-2,0]$	24	12	$-(1/2)e_{-4,-3,1}-3/2e_{-3,-4,1}-9/2e_{-3,-4,2}+1/2e_{1,12,1}-3/2e_{1,12,2}+3/2e_{12,1,1}$
784	10	$[1,3,3,8,1,1,-1,0,2,2]$	28	1	$3e_{1,1,2}-2e_{1,1,4}+2e_{1,1,7}-3e_{1,1,14}+2e_{1,1,28}$
864	38	$[2,2,3,5,1,0,0,1,1,0]$	96	24	$-1/3e_{-24,-4,1}-4/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}+1/6e_{-4,-24,1}+1/6e_{-3,-8,1}+1/6e_{-3,-8,2}+1/3e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}+1/3e_{8,12,1}-1/6e_{12,8,1}+4/3e_{24,1,1}-2/3e_{24,1,2}+8/3e_{24,1,4}$
864	39	$[2,2,5,5,1,2,-1,1,1,5]$	96	24	$1/3e_{-24,-4,1}-4/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}-1/6e_{-4,-24,1}+1/6e_{-3,-8,1}+1/6e_{-3,-8,2}+1/3e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}-1/3e_{8,12,1}+1/6e_{12,8,1}+4/3e_{24,1,1}-2/3e_{24,1,2}+8/3e_{24,1,4}$
864	40	$[2,3,3,5,0,0,0,2,3,3]$	48	24	$-2e_{-8,-3,1}-8/3e_{-8,-3,2}-1/3e_{-3,-8,2}-1/3e_{1,24,2}+2e_{24,1,1}-8/3e_{24,1,2}$
960	26	$[2,3,3,6,2,2,0,0,2,2]$	60		$-5/12e_{-20,-3,1}-5/4e_{-15,-4,1}+1/12e_{-4,-15,1}+1/4e_{3,-20,1}-1/12e_{1,60,1}+5/12e_{5,12,1}-1/4e_{12,5,1}+5/4e_{60,1,1}$
972	9	$[1,4,4,6,1,1,-1,0,3,3]$	36	12	$4/3e_{-4,-3,1}-8/3e_{-4,-3,3}-1/3e_{-3,-4,1}-1/3e_{1,12,1}-2/3e_{1,12,3}+4/3e_{12,1,1}$
972	18	$[2,2,5,5,2,1,-1,1,-1,1]$	36	12	$-4/3e_{-4,-3,1}-16/3e_{-4,-3,3}-1/3e_{-3,-4,1}+1/3e_{1,12,1}-4/3e_{1,12,3}+4/3e_{12,1,1}$
1024	20	$[2,2,3,8,0,2,2,0,0,0]$	32	1	$-e_{-4,-4,1}+2e_{-4,-4,2}+1/2e_{1,1,2}-1/2e_{1,1,16}+e_{1,1,32}$
1024	22	$[1,2,6,6,0,0,0,0,0,4]$	64	1	$1/2e_{-8,-8,1}-2e_{-4,-4,4}+1/2e_{1,1,2}-1/2e_{1,1,8}+5/4e_{1,1,16}-3/4e_{1,1,32}+1/2e_{1,1,64}+1/2e_{8,8,1}$
1024	25	$[1,4,5,5,0,0,4,0,4,2]$	32	1	$e_{-4,-4,1}-2e_{-4,-4,2}+1/2e_{1,1,2}-1/2e_{1,1,16}+e_{1,1,32}$
1024	26	$[2,3,3,5,0,0,2,0,-2,2]$	64	1	$-1/2e_{-8,-8,1}-2e_{-4,-4,4}+1/2e_{1,1,2}-1/2e_{1,1,8}+5/4e_{1,1,16}-3/4e_{1,1,32}+1/2e_{1,1,64}-1/2e_{8,8,1}$
1024	27	$[2,3,3,6,2,2,0,0,-2,2]$	64	1	$-e_{-4,-4,1}-2e_{-4,-4,4}+1/2e_{1,1,2}-1/2e_{1,1,8}+5/4e_{1,1,16}-3/4e_{1,1,32}+1/2e_{1,1,64}$
1024	28	$[3,3,3,3,2,0,0,0,0,2]$	32	1	$-e_{-4,-4,1}-2e_{-4,-4,2}+1/2e_{1,1,2}-1/2e_{1,1,16}+e_{1,1,32}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
1024	29	$[3,3,3,4,2,2,-2,0,0,0]$	16	1	$-e_{-4,-4,1}+3/2e_{1,1,2}-5/2e_{1,1,4}+2e_{1,1,16}$
1029	7	$[1,2,7,7,1,0,0,0,0,7]$	21	21	$-1/2e_{-7,-3,1}+3/2e_{-3,-7,1}-1/2e_{1,21,1}+3/2e_{21,1,1}$
1029	8	$[3,3,3,3,1,1,-1,-1,1,1]$	21	21	$1/2e_{-7,-3,1}-3/2e_{-3,-7,1}-1/2e_{1,21,1}+3/2e_{21,1,1}$
1125	14	$[1,4,5,5,1,0,0,0,0,5]$	15	5	$e_{1,5,1}-6e_{1,5,3}+e_{5,1,1}+6e_{5,1,3}$
1125	15	$[2,2,5,5,1,0,0,0,0,5]$	15	5	$-2e_{1,5,1}-3e_{1,5,3}+2e_{5,1,1}-3e_{5,1,3}$
1125	16	$[2,3,3,7,2,2,1,1,3,3]$	45	5	$1/2e_{-15,-3,1}-1/2e_{-3,-15,1}-3/2e_{1,5,1}+e_{1,5,3}-9/2e_{1,5,9}+3/2e_{5,1,1}+e_{5,1,3}+9/2e_{5,1,9}$
1280	39	$[1,4,4,8,0,0,4,0,4,0]$	80	5	$5/4e_{-20,-4,1}-1/4e_{-4,-20,1}-1/4e_{1,5,1}-1/4e_{1,5,2}-3/2e_{1,5,4}+e_{1,5,8}-4e_{1,5,16}+5/4e_{5,1,1}-5/4e_{5,1,2}+15/2e_{5,1,4}+5e_{5,1,8}+20e_{5,1,16}$
1280	43	$[3,3,3,4,2,2,2,0,0,0]$	80	5	$-5/4e_{-20,-4,1}+1/4e_{-4,-20,1}-1/4e_{1,5,1}-1/4e_{1,5,2}-3/2e_{1,5,4}+e_{1,5,8}-4e_{1,5,16}+5/4e_{5,1,1}-5/4e_{5,1,2}+15/2e_{5,1,4}+5e_{5,1,8}+20e_{5,1,16}$
1296	27	$[1,4,5,7,0,1,4,1,0,5]$	108	1	$-3/2e_{-3,-3,3}-9/2e_{-3,-3,6}-6e_{-3,-3,12}+3e_{1,1,2}+13/6e_{1,1,3}-2e_{1,1,4}-13/4e_{1,1,6}-2/3e_{1,1,9}+13/6e_{1,1,12}+e_{1,1,18}+1/2e_{1,1,27}-2/3e_{1,1,36}-3/4e_{1,1,54}+1/2e_{1,1,108}$
1296	31	$[3,3,5,5,3,3,0,3,3,5]$	36	1	$-3/2e_{-3,-3,1}-9/2e_{-3,-3,2}-6e_{-3,-3,4}+9/4e_{1,1,2}-3/2e_{1,1,4}+3/2e_{1,1,9}-9/4e_{1,1,18}+3/2e_{1,1,36}$
1296	34	$[1,3,6,6,0,0,0,0,0,6]$	36	1	$e_{-3,-3,1}-4e_{-3,-3,4}+2/3e_{1,1,3}+e_{1,1,4}-e_{1,1,9}-2/3e_{1,1,12}+e_{1,1,36}$
1296	37	$[2,2,3,9,2,0,0,0,0,0]$	36	1	$-e_{-3,-3,1}+4e_{-3,-3,4}+2/3e_{1,1,3}+e_{1,1,4}-e_{1,1,9}-2/3e_{1,1,12}+e_{1,1,36}$
1296	38	$[2,2,5,5,1,1,1,1,1,-2]$	36	1	$-1/2e_{-3,-3,1}+1/2e_{-3,-3,2}-2e_{-3,-3,4}-1/4e_{1,1,2}-1/2e_{1,1,4}+1/2e_{1,1,9}+1/4e_{1,1,18}+1/2e_{1,1,36}$
1296	39	$[2,3,3,5,0,0,0,2,0,0]$	36	1	$-e_{-3,-3,1}-2e_{-3,-3,2}-4e_{-3,-3,4}+e_{1,1,2}-e_{1,1,4}+e_{1,1,9}-e_{1,1,18}+e_{1,1,36}$
1372	8	$[3,3,3,5,1,1,-1,2,-2,-2]$	28	28	$1/4e_{-7,-4,1}-e_{-4,-7,1}-1/4e_{1,28,1}+e_{28,1,1}$
1500	11	$[1,4,4,9,1,1,-2,1,3,3]$	60	15	$1/3e_{-20,-3,1}-1/4e_{-15,-4,1}+1/3e_{-4,-15,1}-1/4e_{-3,-20,1}-1/12e_{1,60,1}-1/12e_{5,12,1}+e_{12,5,1}+e_{60,1,1}$
1536	50	$[1,4,4,8,0,0,0,0,4,4]$	96	24	$e_{-24,-4,1}-1/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}-1/6e_{-4,-24,1}+1/2e_{-3,-8,1}+1/2e_{-3,-8,2}+e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}-1/3e_{8,12,1}+1/2e_{12,8,1}+e_{24,1,1}-2e_{24,1,2}+8e_{24,1,4}$
1536	56	$[2,4,4,5,0,0,0,0,4,4]$	24	24	$1/3e_{-8,-3,1}-e_{-3,-8,1}-1/3e_{1,24,1}+e_{24,1,1}$
1536	57	$[3,3,3,7,2,2,-2,2,-2,2]$	96	24	$-e_{-24,-4,1}-1/3e_{-8,-3,1}-2/3e_{-8,-3,2}-8/3e_{-8,-3,4}+1/6e_{-4,-24,1}+1/2e_{-3,-8,1}+1/2e_{-3,-8,2}+e_{-3,-8,4}-1/6e_{1,24,1}+1/6e_{1,24,2}-1/3e_{1,24,4}+1/3e_{8,12,1}-1/2e_{12,8,1}+e_{24,1,1}-2e_{24,1,2}+8e_{24,1,4}$
1701	13	$[1,4,6,6,1,0,3,0,3,3]$	63	21	$7/6e_{-7,-3,1}-7/3e_{-7,-3,3}-1/6e_{-3,-7,1}-1/6e_{1,21,1}-1/3e_{1,21,3}+7/6e_{21,1,1}$
1701	18	$[2,5,5,5,1,1,1,2,5,-4]$	63	21	$-7/6e_{-7,-3,1}-14/3e_{-7,-3,3}-1/6e_{-3,-7,1}+1/6e_{1,21,1}-2/3e_{1,21,3}+7/6e_{21,1,1}$
1728	48	$[2,5,5,5,2,2,-2,2,4,4]$	12	12	$-e_{-4,-3,1}+e_{-3,-4,1}-e_{1,12,1}+e_{12,1,1}$
1728	67	$[1,4,5,7,0,1,2,0,4,1]$	144	12	$-3/2e_{-4,-3,3}-3e_{-4,-3,6}-4e_{-4,-3,12}-4/3e_{-3,-4,4}-3e_{-3,-4,12}-e_{1,12,12}+2e_{12,1,1}-4e_{12,1,2}-9/2e_{12,1,3}+16/3e_{12,1,4}+9e_{12,1,6}-12e_{12,1,12}$
D	g	Q	N	j	$r(Q)$

D	g	Q	N	j	$r(Q)$
1728	72	$[2,2,3,12,2,0,0,0,0,0]$	48	12	$-e_{-4,-3,1} + e_{-4,-3,2} + 4e_{-4,-3,4} + 1/2e_{-3,-4,1} + 1/2e_{-3,-4,2} + e_{-3,-4,4} - 1/2e_{1,12,1} + 1/2e_{1,12,2} - e_{1,12,4} + e_{12,1,1} + e_{12,1,2} - 4e_{12,1,4}$
1728	74	$[2,2,5,8,1,1,1,2,2,-4]$	48	12	$-1/2e_{-4,-3,1} + e_{-4,-3,2} - 4e_{-4,-3,4} + e_{-3,-4,4} - e_{1,12,4} + 1/2e_{12,1,1} + e_{12,1,2} + 4e_{12,1,4}$
1728	75	$[2,2,6,7,0,0,0,2,2,6]$	36	12	$-e_{-4,-3,3} - 4/3e_{-3,-4,1} - 3e_{-3,-4,3} - e_{1,12,3} + 4/3e_{12,1,1} - 3e_{12,1,3}$
1728	76	$[2,3,3,10,2,2,0,0,2,2]$	36	12	$-e_{-4,-3,3} - 2/3e_{-3,-4,1} + 3e_{-3,-4,3} - e_{1,12,3} + 2/3e_{12,1,1} + 3e_{12,1,3}$
1728	78	$[2,3,5,5,0,2,0,2,0,4]$	48	12	$-e_{-4,-3,1} - e_{-4,-3,2} - 4e_{-4,-3,4} + 1/2e_{-3,-4,1} + 1/2e_{-3,-4,2} + e_{-3,-4,4} - 1/2e_{1,12,1} + 1/2e_{1,12,2} - e_{1,12,4} + e_{12,1,1} - e_{12,1,2} + 4e_{12,1,4}$
1728	79	$[3,3,4,4,0,0,0,0,0,4]$	12	12	$e_{-4,-3,1} - e_{-3,-4,1} - e_{1,12,1} + e_{12,1,1}$
1728	80	$[3,3,5,5,3,3,0,3,0,2]$	48	12	$-3/2e_{-4,-3,1} - 3e_{-4,-3,2} - 4e_{-4,-3,4} + e_{-3,-4,4} - e_{1,12,4} + 3/2e_{12,1,1} - 3e_{12,1,2} + 4e_{12,1,4}$
D	g	Q	N	j	$r(Q)$

Tabel 10.3: Representatieformules van vormen met $D > 1\,732$

D	g	Q	N	j	$r(Q)$
2000		$[1,5,5,5]$	20	5	$e_{1,5,1} - 2e_{1,5,2} - 4e_{1,5,4} + e_{5,1,1} + 2e_{5,1,2} - 4e5,1,4$
2048		$[1,2,8,8]$	32	8	$e_{-4,-8,1} - 2e_{1,8,4} + e_{8,1,1}$
2048		$[1,4,4,8]$	32	8	$e_{-8,-4,1} - 2e_{1,8,4} + e_{8,1,1} - 2e_{8,1,2} + 8e_{8,1,4}$
3456		$[2,3,6,6]$	24	24	$-(2/3)e_{-8,-3,1} + 1/3e_{-3,-8,1} - 1/3e_{1,24,1} + 2/3e_{24,1,1}$
3888		$[1,3,9,9]$	36	12	$e_{-4,-3,1} + 8/3e_{-4,-3,3} + 1/3e_{-3,-4,1} + 1/3e_{1,12,1} - 4/3e_{1,12,3} + 2/3e_{12,1,1}$
6912		$[2,3,6,12]$	48	12	$-(1/2)e_{-4,-3,1} + e_{-3,-4,4} - e_{1,12,4} + 1/2e_{12,1,1}$
8192		$[1,8,8,8]$	32	8	$1/2e_{-8,-4,1}+1/2e_{-4,-8,1}+1/2e_{1,8,1}-1/2e_{1,8,2}-2e_{1,8,4}+1/2e_{8,1,1}-e_{8,1,2}+4e_{8,1,4}$
D	g	Q	N	j	$r(Q)$

Tabel 10.4: Deltafuncties

N	D	g	$w(g)$	Q	$p : \delta_p$
2	4	1	1/1152	$[1,1,1,1,0,0,0,1,1,1],1152$	$2 : \frac{3}{2}v_2(n)$
3	9	1	1/288	$[1,1,1,1,1,0,0,0,0,1],288$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $3 : \frac{4}{3}v_3(n)$
4	16	1	1/384	$[1,1,1,1,0,0,0,0,0,0],384$	$2 : \begin{cases} 3v_2(n) \text{ als } 2 \mid n, \\ 1 \text{ anders} \end{cases}$
5	5	1	1/240	$[1,1,1,1,1,0,0,1,0,1],240$	$2 : \frac{5}{6} + \frac{5}{12}(-1)^{\mathrm{ord}_2(n)}v_2(n)$ $5 : 1 - \frac{1}{5}\chi_5(w_5(n))v_5(n)$
5	25	1	1/72	$[1,1,2,2,1,1,0,1,1,2],72$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $5 : \frac{6}{5}v_5(n)$
5	125	3	1/240	$[2,2,2,2,1,1,-1,-1,1,1],240$	$2 : \frac{5}{6} + \frac{5}{12}(-1)^{\mathrm{ord}_2(n)}v_2(n)$ $5 : 1 - \chi_5(w_5(n))v_5(n)$
6	36	4	1/144	$[1,1,2,2,1,0,0,0,0,2],144$	$2 : \frac{3}{2}v_2(n)$ $3 : 2 - \frac{4}{3}v_3(n)$
6	36	5	1/64	$[1,1,2,2,0,1,1,1,1,1],64$	$2 : 2 - \frac{3}{2}v_2(n)$ $3 : \frac{4}{3}v_3(n)$
7	49	1	1/32	$[1,1,2,2,0,1,0,0,1,0],32$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $7 : \frac{8}{7}v_7(n)$
8	8	1	1/96	$[1,1,1,1,0,0,0,1,1,0],96$	$2 : 1 - \frac{1}{8}\chi_{8,\{3,5\}}(w_2(n))v_2(n)$
8	16	2	1/96	$[1,1,1,2,1,1,0,0,0,0],96$	$2 : \begin{cases} 3v_2(n) \text{ als } 4 \mid n, \\ 1/2 \text{ als } 2 \parallel n, \\ 3/2 \text{ anders} \end{cases}$
8	32	1	1/96	$[1,1,1,2,0,0,0,0,0,0],96$	$2 : 1 - \frac{1}{4}\chi_{8,\{3,5\}}(w_2(n))v_2(n)$
8	64	3	1/64	$[1,1,2,2,0,0,0,0,0,0],64$	$2 : \begin{cases} 6v_2(n) \text{ als } 4 \mid n, \\ 1 \text{ anders} \end{cases}$
8	64	4	1/72	$[1,1,3,3,1,1,0,1,1,3],72$	$2 : \begin{cases} 6v_2(n) \text{ als } 4 \mid n, \\ 0 \text{ als } 2 \parallel n, \\ \frac{3}{2} \text{ anders} \end{cases}$
8	128	9	1/96	$[1,2,2,2,0,0,0,0,0,0],96$	$2 : 1 - \frac{1}{2}\chi_{8,\{3,5\}}(w_2(n))v_2(n)$
8	256	13	1/96	$[1,3,3,3,0,0,2,0,2,-2],96$	$2 : \begin{cases} 12v_2(n) \text{ als } 4 \mid n, \\ 0 \text{ als } 2 \parallel n, \\ 1 \text{ anders} \end{cases}$
9	81	3	1/144	$[1,1,3,3,1,0,0,0,0,3],144$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $3 : \begin{cases} 4v_3(n) \text{ als } 3 \mid n, \\ 1 + \chi_3(n) \text{ anders} \end{cases}$
9	81	4	1/144	$[2,2,2,2,1,1,1,2,2,-1],144$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $3 : \begin{cases} 4v_3(n) \text{ als } 3 \mid n, \\ 1 - \chi_3(n) \text{ anders} \end{cases}$
10	20	1	1/96	$[1,1,1,3,1,1,0,1,1,0],96$	$2 : \frac{2}{3} + \frac{5}{6}(-1)^{\mathrm{ord}_2(n)}v_2(n)$ $5 : 1 - \frac{1}{5}\chi_5(w_5(n))v_5(n)$
10	20	2	1/96	$[1,1,1,2,0,0,0,1,1,1],96$	$2 : \frac{4}{3} - \frac{5}{6}(-1)^{\mathrm{ord}_2(n)}v_2(n)$ $5 : 1 + \frac{1}{5}\chi_5(w_5(n))v_5(n)$
10	100	3	1/64	$[1,1,3,3,0,1,1,1,1,1],64$	$2 : \frac{3}{2}v_2(n)$ $5 : 2 - \frac{6}{5}v_5(n)$
10	100	5	1/16	$[1,2,2,3,1,0,2,0,1,2],16$	$2 : 2 - \frac{3}{2}v_2(n)$ $5 : \frac{6}{5}v_5(n)$
N	D	g	$w(g)$	Q	$p : \delta_p$

N	D	g	$w(g)$	Q	$p : \delta_p$
11	121	1	25/288	$[1,1,3,3,0,1,0,0,1,0],32;$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$
				$[1,1,4,4,1,1,0,1,1,4],72;$	$11 : \frac{12}{11}v_{11}(n)$
				$[2,2,2,2,2,1,0,1,1,2],24$	
12	12	1	1/96	$[1,1,1,2,1,1,0,1,0,0],96$	$2 : 1 - \frac{1}{4}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 + \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	12	2	1/96	$[1,1,1,1,0,0,0,1,0,0],96$	$2 : 1 + \frac{1}{4}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 - \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	36	3	1/48	$[1,1,1,3,1,0,0,0,0,0),48$	$2 : \begin{cases} \frac{3}{2} - \frac{3}{2}v_2(n) \text{ als } 2 \mid n, \\ 1 \text{ anders} \end{cases}$
					$3 : \frac{4}{3}v_3(n)$
12	48	1	1/96	$[1,1,1,3,0,0,0,0,0,0],96$	$2 : 1 + \frac{1}{2}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 - \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	48	6	1/96	$[1,1,2,2,0,0,0,0,0,2],96$	$2 : 1 - \frac{1}{2}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 + \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	108	6	1/96	$[1,1,3,3,1,0,0,0,0,0],96$	$2 : 1 - \frac{1}{4}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 + (-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	108	8	1/96	$[2,2,2,2,2,1,-1,-1,1,-1],96$	$2 : 1 + \frac{1}{4}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 - (-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	144	4	1/64	$[1,1,3,3,0,0,0,0,0,0],64$	$2 : \begin{cases} 2 - 3v_2(n) \text{ als } 2 \mid n, \\ 1 \text{ anders} \end{cases}$
					$3 : \frac{4}{3}v_3(n)$
12	144	5	1/144	$[1,1,4,4,1,0,0,0,0,4],144$	$2 : \begin{cases} \frac{3}{2} - 3v_2(n) \text{ als } 2 \mid n, \\ \frac{3}{2} \text{ anders} \end{cases}$
					$3 : \frac{4}{3}v_3(n)$
12	144	6	1/16	$[1,2,2,4,1,1,0,1,2,2],16$	$2 : \begin{cases} \frac{5}{2} - 3v_2(n) \text{ als } 2 \mid n, \\ \frac{1}{2} \text{ anders} \end{cases}$
					$3 : \frac{4}{3}v_3(n)$
12	144	12	1/48	$[1,2,2,3,0,0,2,0,0,0],48$	$2 : \begin{cases} 3v_2(n) \text{ als } 2 \mid n, \\ 1 \text{ anders} \end{cases}$
					$3 : \frac{4}{3}v_3(n)$
12	192	13	1/96	$[1,1,4,4,0,0,0,0,0,4],96$	$2 : 1 + (-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 - \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	192	20	1/96	$[2,2,2,3,0,0,0,2,2,2],96$	$2 : 1 - (-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 + \frac{1}{3}(-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	432	31	1/96	$[2,2,3,3,2,0,0,0,0,0],96$	$2 : 1 + \frac{1}{2}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 - (-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
12	432	13	1/96	$[1,3,3,3,0,0,0,0,0,0],96$	$2 : 1 - \frac{1}{2}(-1)^{\mathrm{ord}_2(n)}\chi_4(w_2(n))v_2(n)$
					$3 : 1 + (-1)^{\mathrm{ord}_3(n)}\chi_3(w_3(n))v_3(n)$
13	13	1	1/48	$[1,1,1,2,1,1,0,0,1,0],48$	$2 : \frac{5}{6} + \frac{5}{12}(-1)^{\mathrm{ord}_2(n)}v_2(n)$
					$13 : 1 - \frac{1}{13}\chi_{13}(w_{13}(n))v_{13}(n)$
13	169	1	1/8	$[1,2,2,4,1,0,1,1,1,2],8$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$
					$13 : \frac{14}{13}v_{13}(n)$
14	196	4	9/64	$[1,1,4,4,0,1,1,1,1,1],64;$	$2 : 2 - \frac{3}{2}v_2(n)$
				$[1,2,2,4,1,0,0,0,0,2],16;$	$7 : \frac{8}{7}v_7(n)$
				$[2,2,2,2,1,1,0,0,1,-1),16$	
14	196	5	1/36	$[1,1,5,5,1,1,0,1,1,5],72;$	$2 : \frac{3}{2}v_2(n)$
				$[2,2,3,3,2,2,0,2,2,3],72$	$7 : 2 - \frac{8}{7}v_7(n)$
15	45	1	1/48	$[1,1,1,4,1,0,0,0,0,1],8$	$2 : \frac{5}{6} + \frac{5}{12}(-1)^{\mathrm{ord}_2(n)}v_2(n)$
					$3 : \frac{1}{2} + \frac{5}{6}(-1)^{\mathrm{ord}_3(n)}v_3(n)$
					$5 : 1 - \frac{1}{5}\chi_5(w_5(n))v_5(n)$
N	D	g	$w(g)$	Q	$p : \delta_p$

N	D	g	$w(g)$	Q	$p : \delta_p$
15	45	3	1/48	$[1,1,2,2,1,0,0,0,0,1],8$	$2 : \frac{5}{6} + \frac{5}{12}(-1)^{\mathrm{ord}_2(n)}v_2(n)$ $3 : \frac{3}{2} - \frac{5}{6}(-1)^{\mathrm{ord}_3(n)}v_3(n)$ $5 : 1 + \frac{1}{5}\chi_5(w_5(n))v_5(n)$
15	225	4	1/16	$[1,1,4,4,0,1,0,0,1,0],32$; $[2,2,2,2,1,0,0,0,0,1],32$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $3 : \frac{4}{3}v_3(n)$ $5 : 2 - \frac{6}{5}v_5(n)$
15	225	5	1/9	$[1,1,5,5,1,0,0,0,0,5],144$; $[1,2,2,4,0,0,1,1,0,0],16$; $[2,2,3,3,2,1,-1,1,2,2),24$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $3 : 2 - \frac{4}{3}v_3(n)$ $5 : \frac{6}{5}v_5(n)$
16	32	3	1/96	$[1,1,1,4,1,1,0,0,0,0],96$	$2 : \begin{cases} \frac{1}{2} - \frac{1}{4}\chi_{8_{17}}(w_2(n))v_2(n) \text{ als } 2 \mid n, \\ \frac{3}{2} \text{ anders} \end{cases}$
16	32	4	1/32	$[1,1,2,2,0,0,0,1,1,2],32$	$2 : \begin{cases} \frac{3}{2} - \frac{1}{4}\chi_{8_{17}}(w_2(n))v_2(n) \text{ als } 2 \mid n, \\ \frac{1}{2} \text{ anders} \end{cases}$
16	64	1	1/96	$[1,1,1,4,0,0,0,0,0,0],96$	$2 : \begin{cases} 6v_2(n) \text{ als } 8 \mid n, \\ \frac{3}{2} \text{ als } n \equiv 1,2,5,6 \mod 8, \\ \frac{1}{2} \text{ als } n \equiv 3,4,7 \mod 8 \end{cases}$
16	64	6	1/96	$[1,2,2,2,0,0,2,0,2,0],96$	$2 : \begin{cases} 6v_2(n) \text{ als } 8 \mid n, \\ \frac{3}{2} \text{ als } n \equiv 2,3,6,7 \mod 8, \\ \frac{1}{2} \text{ als } n \equiv 1,4,5 \mod 8 \end{cases}$
16	128	4	1/32	$[1,1,2,4,0,0,0,0,0,0],32$	$2 : \begin{cases} 1 - \frac{1}{2}\chi_{8_{17}}(w_2(n))v_2(n) \text{ als } 2 \mid n, \\ 1 \text{ anders} \end{cases}$
16	256	7	1/64	$[1,1,4,4,0,0,0,0,0,0],64$	$2 : \begin{cases} 12a_2(n) \text{ als } 8 \mid n, \\ 0 \text{ als } n \equiv 3 \mod 4, \\ 2 \text{ als } n \equiv 1 \mod 4, \\ 1 \text{ als } n \equiv 2,4,6 \mod 8 \end{cases}$
16	256	10	1/32	$[1,2,2,4,0,0,0,0,0,0],32$	$2 : \begin{cases} 12a_2(n) \text{ als } 8 \mid n, \\ 1 \text{ anders} \end{cases}$
16	256	14	1/64	$[2,2,3,3,0,2,2,2,2,2],64$	$2 : \begin{cases} 12a_2(n) \text{ als } 8 \mid n, \\ 0 \text{ als } n \equiv 1 \mod 4, \\ 2 \text{ als } n \equiv 3 \mod 4, \\ 1 \text{ als } n \equiv 2,4,6 \mod 8 \end{cases}$
17	17	1	1/24	$[1,1,1,2,1,0,0,1,0,1],24$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $17 : 1 - \frac{1}{17}\chi_{17}(w_{17}(n))v_{17}(n)$
17	289	1	2/9	$[1,1,6,6,1,1,0,1,1,6],72$; $[1,2,3,5,1,0,2,0,1,3),8$; $[2,2,3,3,2,1,0,1,1,3),12$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $17 : \frac{18}{17}v_{17}(n)$
18	36	1	1/96	$[1,1,1,5,1,1,0,1,0,0],96$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{4}{3} - \frac{4}{3}a_3(n) \text{ als } 3 \mid n, \\ 4/3 \text{ als } n \equiv 1 \mod 3, \\ 2/3 \text{ als } n \equiv 2 \mod 3 \end{cases}$
18	36	2	1/96	$[1,1,1,3,0,0,0,1,1,1],96$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{4}{3} - \frac{4}{3}a_3(n) \text{ als } 3 \mid n, \\ 2/3 \text{ als } n \equiv 1 \mod 3, \\ 4/3 \text{ als } n \equiv 2 \mod 3 \end{cases}$
N	D	g	$w(g)$	Q	$p : \delta_p$

N	D	g	$w(g)$	Q	$p : \delta_p$
18	324	6	1/144	$[1,1,6,6,1,0,0,0,0,6], 144$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{5}{3} - v_3(n) \text{ als } 9 \mid n, \\ \frac{2}{3} \text{ als } 3 \parallel n, \\ 2 \text{ als } n \equiv 1 \mod 3, \\ 0 \text{ als } n \equiv 2 \mod 3 \end{cases}$
18	324	12	1/64	$[1,1,5,5,0,1,1,1,1,1], 64$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{4}{3} - 4v_3(n) \text{ als } 3 \mid n, \\ \frac{4}{3} \text{ anders} \end{cases}$
18	324	14	1/16	$[1,2,3,5,0,1,2,0,2,1], 16$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{8}{3} - 4v_3(n) \text{ als } 3 \mid n, \\ \frac{2}{3} \text{ anders} \end{cases}$
18	324	15	1/32	$[1,3,3,4,0,0,0,1,3,3], 32$	$2 : 2 - \frac{3}{2}v_2(n)$ $3 : \begin{cases} 4v_3(n) \text{ als } 3 \mid n, \\ 2 \text{ als } n \equiv 1 \mod 3 \\ 0 \text{ als } n \equiv 2 \mod 3 \end{cases}$
18	324	16	1/144	$[2,2,3,3,2,0,0,0,0,3], 144$	$2 : \frac{3}{2}v_2(n)$ $3 : \begin{cases} \frac{5}{3} - v_3(n) \text{ als } 9 \mid n, \\ \frac{2}{3} \text{ als } 3 \parallel n, \\ 0 \text{ als } n \equiv 1 \mod 3, \\ 2 \text{ als } n \equiv 2 \mod 3 \end{cases}$
19	361	1	9/32	$[1,1,5,5,0,1,0,0,1,0], 32;$ $[1,2,3,6,1,1,0,1,2,3), 8;$ $[2,2,3,3,0,2,1,1,2,1), 8$	$2 : \frac{3}{2} - \frac{3}{4}v_2(n)$ $19 : \frac{20}{19}v_{19}(n)$
N	D	g	$w(g)$	Q	$p : \delta_p$

Bibliografie

[Beu] Frits Beukers. *Getaltheorie voor Beginners*. Epsilon uitgaven, 2005.

[Bha] Manjul Bhargava. On the Conway-Schneeberger Fifteen Theorem. In *Quadratic forms and their applications*, 2000. Zie ook `http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf`.

[Cre] John Cremona. Elliptic Curve Data, 2005. Zie ook `http://modular.fas.harvard.edu/cremona/index.html`.

[Hof] William Hoffman. Topics in Elliptic Curves and Modular Forms. *Unknown*, 2001. Zie ook `http://www.math.lsu.edu/~hoffman/papers/elmod.pdf`.

[Iwa] Henryk Iwaniec. *Topics in Classical Automorphic Forms*, volume 17. American Mathematical Society, 1997.

[Lan] Serge Lang. *Introduction to Modular Forms*. Springer-Verlag, 2001.

[Miy] Toshitsune Miyake. *Modular Forms*. Springer-Verlag, 1989.

[Nip] Gordon Nipp. *Quaternary Quadratic Forms: Computer Generated Tables*. Springer-Verlag, 1991. Voor de tabellen, zie `http://www.research.att.com/~njas/lattices/nipp.html`.

[Ogg] Andrew Ogg. *Modular Forms and Dirichlet Series*. University of California, Berkeley, 1969.

[Ran] Robert Rankin. Contributions to the theory of Ramanujan's function. *Proc. Cambridge Philos. Soc.*, 35:357–372, 1939.

[Sch] Bruno Schöneberg. *Elliptic Modular Functions*. Springer-Verlag, 1974.

[Ste] William Stein. *Modular Forms, a Computational Approach*, volume 79. American Mathematical Society, 2007.

[Wol1] Stephen Wolfram. The Wolfram Functions Site: Catalan constant: Primary definition, 2001. `http://functions.wolfram.com/02.07.02.0001.01`.

[Wol2] Stephen Wolfram. The Wolfram Functions Site: Catalan constant: Specific values, 2001. `http://functions.wolfram.com/02.07.03.0001.01`.

Index