Ron Hoogwater

Potentieel goede reductie van elliptische krommen met een gegeven periodenrooster

Bachelorscriptie, 25 juni 2010

Scriptiebegeleider: Dr. R.S. de Jong

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

Inleiding

Beschouw de nulpuntsverzameling van de vergelijking

$$E : y^2 = 4x^3 - Ax - B \quad A, B \in K, \tag{1}$$

waarbij K een lichaam is van karakteristiek niet 2 of 3, en de coëfficiënten A en B voldoen aan $\Delta = A^3 - 27B^2 \neq 0$. Krommen van dit type worden veelvuldig bestudeerd in de wiskunde. Als we de vergelijking (1) bekijken in het projectieve vlak $\mathbb{P}^2(K)$, dan definieert dit een elliptische kromme. Elliptische krommen worden bijvoorbeeld gebruikt bij het berekenen van de booglengte van een ellips, in Lenstra's algoritme voor het factoriseren in priemfactoren of in een bewijs van de laatste stelling van Fermat. Er ligt bovendien een groepsstructuur op de punten van een elliptische kromme die gebruikt wordt in cryptografische protocollen.

In deze scriptie worden alleen elliptische krommen van de vorm (1) bekeken. De volledige definitie van een elliptische kromme vergt veel algebraïsche meetkunde die niet nodig is voor het bestuderen van krommen van de vorm (1), en zullen we daarom niet geven.

Als we vergelijking (1) modulo een priemgetal bekijken, kunnen we ons afvragen of dit nog steeds een elliptische kromme definieert. We zeggen dat E goede reductie heeft als dit het geval is. Dit proces van *reductie modulo p*, alsmede een goede definitie van het priemgetal p, wordt uiteengezet in hoofdstuk 3.

Als E geen elliptische kromme is 'modulo p', dan kunnen we reductie modulo p proberen toe te passen in een uitbreiding van K. De vraag is nu welke uitbreiding $K \subset K'$ resulteert in goede reductie in K'. Op het eerste gezicht lijkt deze uitbreiding alleen impliciet te vinden, maar voor complexe elliptische krommen blijkt ook een expliciete beschrijving te zijn. Bovendien blijkt deze uitbreiding te werken voor alle priemen p die niet 2 of 3 delen. In deze scriptie werken we toe naar deze beschrijving.

In deze beschrijving wordt gebruik gemaakt van het feit dat een complexe elliptische kromme als Riemann-oppervlak isomorf is met een complexe torus. Dit is een mooi resultaat op zich, en wordt in detail uiteengezet in hoofdstuk 2. Als gevolg van dit isomorfisme vinden we een equivalentie van categorieën tussen roosters in $\mathbb{C}$ en elliptische krommen over $\mathbb{C}$.

Maar eerst zullen we in hoofdstuk 1 de definities introduceren die we in deze scriptie zullen gebruiken.

1 Elliptische krommen

Elke elliptische kromme over een lichaam K in $\mathbb{P}^2(K)$ kan geschreven worden als de nulpuntsverzameling van een Weierstrass-vergelijking [SIL, p. 63]. Als ook geldt dat $\operatorname{char} K \neq 2, 3$ reduceert deze vergelijking tot:

$$E : y^2 = 4x^3 - Ax - B \quad A, B \in K \tag{2}$$

met $\Delta = A^3 - 27B^2 \neq 0$. We noemen Δ de *discriminant* van E. We zullen in deze scriptie vergelijking (2) als definitie van een elliptische kromme nemen. We noteren het punt van E op oneindig met O.

Beschouw nu een elliptische kromme E over een lichaam K met $\operatorname{char} K \neq 2, 3$ en stel dat deze wordt gegeven door vergelijking (2). De enige coördinatentransformatie die vergelijking (2) invariant laat is:

$$x \mapsto u^2 x \qquad y \mapsto u^3 y \qquad u \in K^*. \tag{3}$$

Hiermee gaat de kromme over in

$$E' : y^2 = 4x^3 - A'x - B',$$

met $A' = u^{-4}A$ en $B' = u^{-6}B$. De kromme E' is isomorf met E en omgekeerd kunnen alle K-isomorfe krommen in de vorm (2) verkregen worden door deze transformatie toe te passen.

We kunnen een functie op A en B definiëren die invariant blijft onder deze transformatie.

Definitie. De *j-invariant* van de elliptische kromme E van vergelijking (2) wordt gegeven door

$$j(E) = j(A, B) = 1728\frac{A^3}{A^3 - 27B^2}$$

Propositie 1.1. Twee elliptische krommen zijn isomorf over $\bar{K}$ dan en slechts dan als ze dezelfde j-invariant hebben.

Bewijs. Als twee elliptische krommen isomorf zijn over $\bar{K}$ wordt het isomorfisme gegeven door de coördinatentransformatie (3) voor een bepaalde $u \in \bar{K}^*$. Dan volgt dat ze dezelfde j-invariant hebben.
Laat nu E en E' twee elliptische krommen zijn met dezelfde j-invariant. Stel dat ze gegeven worden door de volgende vergelijkingen:

$$E : y^2 = 4x^3 - Ax - B$$
$$E' : y^2 = 4x^3 - A'x - B'.$$

Nu is het voldoende te bewijzen dat: $\exists u \in \bar{K}^* : A' = u^{-4}A, \quad B' = u^{-6}B$. Omdat E en E' dezelfde j-invariant hebben geldt:

$$\frac{A^3}{A^3 - 27B^2} = \frac{A'^3}{A'^3 - 27B'^2}.$$

Uitwerken geeft de gelijkheid:

$$A^3 B'^2 = A'^3 B^2. \tag{4}$$

Beschouw nu de volgende drie mogelijkheden:

1. Stel $A = 0$ (dus $j = 0$). Dan is $B \neq 0$ (want $\Delta \neq 0$), dus volgt dat $A' = 0$. Er geldt $B' \neq 0$ en het nemen van een $u \in \bar{K}$ zodat $u^6 = B/B'$ geeft een isomorfisme van de gewenste vorm.

2. Stel $B = 0$ (dus $j = 1728$). Dan is $A \neq 0$ en volgt $B' = 0$ en $A' \neq 0$. Neem een $u \in \bar{K}$ zodat $u^4 = A/A'$.

3. Als $AB \neq 0$ (dus $j \neq 0, 1728$), dan geldt $A'B' \neq 0$ (vanwege vergelijking (4) en $\Delta' \neq 0$). Neem u zo dat $u^2 = \frac{B/B'}{A/A'}$. Dan geldt

$$u^6 B' = \frac{(B/B')^3}{(B/B')^2} B' = B \qquad u^4 A' = \frac{(A/A')^3}{(A/A')^2} A' = A$$

□

Soms kan het handig zijn om de Weierstrass-vergelijking van E op een andere manier te schrijven.

Definitie. Een elliptische kromme E/K is in *Legendre-vorm* als hij isomorf is over K met de kromme

$$y^2 = x(x-1)(x-\lambda) \qquad \text{met } \lambda \in K, \lambda \neq 0, 1$$

We noemen λ ook wel de λ-invariant.

Propositie 1.2. Elke elliptische kromme E/K is isomorf over $\bar{K}$ met een kromme E_λ in Legendre-vorm

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

waar $\lambda \in \bar{K}$ en $\lambda \neq 0, 1$. De j-invariant en de discriminant van E_λ zijn respectievelijk

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \qquad \Delta = 16\lambda^2(\lambda - 1)^2. \tag{5}$$

Bewijs. Schrijf de vergelijking van E in de vorm van vergelijking (2). Het toepassen van de coördinatentransformatie $(x, y) \to (1/4\, x, 1/4\, y)$ en vervolgens factoriseren in lineaire factoren geeft de vergelijking

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{met } e_1, e_2, e_3 \in \bar{K}$$

Omdat $\Delta \neq 0$ zijn de nulpunten e_1, e_2 en e_3 verschillend. Pas de volgende coördinatentransformatie toe:

$$x = (e_2 - e_1)x' + e_1 \qquad y = (e_2 - e_1)^{3/2} y'.$$

Uitwerken geeft een vergelijking in Legendrevorm met

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \bar{K},$$

en er geldt $\lambda \neq 0, 1$ omdat de e_i verschillend zijn.

Voor de berekening van j is het handig om de definitie van de j-invariant te gebruiken bij een algemenere vorm van de Weierstrass vergelijking dan (2), [SIL, p. 46]. De berekening van j en Δ geven we hier niet. □

2 Complexe tori

In dit hoofdstuk beperken we ons tot elliptische krommen over $\mathbb{C}$. We zullen aantonen dat deze elliptische krommen geparametriseerd kunnen worden met de Weierstrass $\wp$-functie en zijn afgeleide. In het bijzonder zal dan blijken dat elke elliptische kromme over $\mathbb{C}$ als Riemann-oppervlak isomorf is met een complexe torus. De Weierstrass $\wp$-functie moet een welgedefinieerd beeld op een complexe torus hebben, dus hij moet periodiek zijn. Functies met deze periodiciteit zijn elliptische functies. Nadat we de benodigde theorie over complexe tori en elliptische functies hebben behandeld kunnen we een definitie geven voor de Weierstrass $\wp$-functie. Met deze theorie kunnen we toewerken naar de genoemde parametrisatie. Dit hoofdstuk besluit met een equivalentie van categorieën van elliptische krommen over $\mathbb{C}$ en roosters.

Definitie. Een *rooster* Λ in $\mathbb{C}$ is een verzameling

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\},$$

met (ω_1, ω_2) een $\mathbb{R}$-basis voor $\mathbb{C}$.

Als we $\mathbb{C}$ uitdelen naar een rooster Λ, dan correspondeert elk punt $w \in \mathbb{C}$ met de punten $w + \omega_1$ en $w + \omega_2$, waarbij ω_1 en ω_2 $\mathbb{R}$-lineair onafhankelijk zijn. De quotiëntruimte $\mathbb{C}/\Lambda$ is dus een torus. We zijn geïnteresseerd in de meromorfe functies op de torus $\mathbb{C}/\Lambda$. Dit zijn in feite meromorfe functies op $\mathbb{C}$ die periodiek zijn ten opzichte van ω_1 en ω_2.

Definitie. Een *elliptische functie* ten opzichte van een rooster Λ is een meromorfe functie $f(z)$ op $\mathbb{C}$ met

$$f(z) = f(z + \omega) \quad \text{voor alle } \omega \in \Lambda, z \in \mathbb{C}$$

Met $\mathbb{C}(\Lambda)$ geven we de verzameling van alle elliptische functies ten opzichte van Λ aan. Het is eenvoudig na te gaan dat $\mathbb{C}(\Lambda)$ een lichaam is.

Definitie. Een *fundamenteel parallellogram* in een rooster Λ is een verzameling

$$D = \{a + s\omega_1 + t\omega_2 : 0 \leq s < 1,\ 0 \leq t < 1\}$$

met $a \in \mathbb{C}$ en ω_1, ω_2 een basis voor Λ.

Met $\bar{D}$ noteren we de compacte afsluiting van D. De afbeelding $D \to \mathbb{C}/\Lambda$ is bijectief, dus $x \in D$ is een goede representant voor $\bar{x} \in \mathbb{C}/\Lambda$.

Voor een meromorfe functie f noteren we met $\mathrm{ord}_w(f)$ de exponent van de eerste term in de Laurentreeks van f rond w. Dus als w een nulpunt is, dan is $\mathrm{ord}_w(f)$ de multipliciteit van het nulpunt, en als w een pool van orde k is, dan is $\mathrm{ord}_w(f) = -k$. Dit wordt ook wel de orde van verdwijnen van f genoemd. Met $\sum_{w \in \mathbb{C}/\Lambda}$ noteren we de som over $w \in D$, met D een fundamenteel parallellogram in Λ.

Propositie 2.1. Laat $f \in \mathbb{C}(\Lambda)$. Dan is binnen een fundamenteel parallellogram het aantal nulpunten geteld met multipliciteiten gelijk aan het aantal polen geteld met multipliciteiten. Ofwel

$$\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0.$$

Bewijs. Laat D een fundamenteel parallellogram zijn in Λ zó dat er geen nulpunten of polen op de rand ∂D van D liggen. Uit [GRE, §5.1] volgt dat

$$\sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f) = \frac{1}{2\pi i}\oint_{\partial D} \frac{f'(z)}{f(z)}\,\mathrm{d}z.$$

Maar uit de periodiciteit van f volgt dat de integralen over de overliggende zijden van D tegen elkaar wegvallen. Dus de totale integraal over ∂D is nul. □

Propositie 2.2. Een elliptische functie $f \in \mathbb{C}(\Lambda)$ zonder polen (of nulpunten) is constant.

Bewijs. Laat $f \in \mathbb{C}(\Lambda)$ een elliptische functie zonder polen zijn en D een fundamenteel parallellogram in Λ. Vanwege de periodiciteit van f geldt:

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in D} |f(z)|.$$

Maar f is continu en $\bar{D}$ is compact, dus f is begrensd op $\bar{D}$, en vanwege bovenstaande identiteit is f begrensd op heel $\mathbb{C}$. De stelling van Liouville zegt nu dat f constant moet zijn [GRE, th. 3.4.3, p. 86].

Nemen we $f \in \mathbb{C}(\Lambda)$ zonder nulpunten, dan geldt bovenstaande redenering voor $1/f$ en volgt ook dat f constant is. □

Voor een $f \in \mathbb{C}(\Lambda)$ is de *orde* van f gedefinieerd als het aantal nulpunten (of polen) van f, geteld met multipliciteiten, in een fundamenteel parallellogram van Λ. Uit bovenstaande resultaten blijkt dat we voor interessante elliptische functies moeten kijken naar functies van orde minimaal 2. We kunnen nu een definitie geven voor de Weierstrass $\wp$-functie. Tevens geven we een definitie van een reeks die we verder in de theorie zullen tegenkomen.

Definitie. De *Weierstrass $\wp$-functie* ten opzichte van Λ wordt gegeven door:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Definitie. De *Eisensteinreeks* van orde k is de machtreeks:

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-2k}.$$

Stelling 2.3. De Weierstrass $\wp$-functie is een even elliptische functie.

Bewijs. De reeks in de Weierstrass $\wp$-functie is uniform convergent op elke compacte deelverzameling van $\mathbb{C}\setminus\Lambda$. Voor een deel van het bewijs, zie [SIL, p. 154]. Dus $\wp(z)$ is een holomorfe functie op $\mathbb{C}\setminus\Lambda$, en uit de definitie zien we dat $\wp(z)$ een dubbele pool heeft op elk roosterpunt.

We zien dat $\wp(z) = \wp(-z)$ door ω in de som te vervangen door $-\omega$, dus $\wp(z)$ is even. De afgeleide kunnen we berekenen door termsgewijs differentiëren:

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

Aan deze uitdrukking zien we dat $\wp'$ een elliptische functie is en er volgt

$$\wp(z+\omega) = \wp(z) + c(\omega) \qquad \text{voor alle } \omega \in \Lambda, z \in \mathbb{C},$$

met $c(\omega) \in \mathbb{C}$ een functie die onafhankelijk is van z. Nemen we $z = -\omega/2$, dan volgt uit het feit dat $\wp(z)$ even is dat $c(\omega) = 0$. □

Propositie 2.4. De Laurentreeks van $\wp(z)$ rond $z = 0$ is:

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

Bewijs. Voor $|z| < |\omega|$ geldt

$$\frac{1}{(1-\frac{z}{\omega})} = \sum_{n=0}^{\infty} \frac{z^n}{\omega^n}.$$

Als we dit differentiëren en vermenigvuldigen met ω^{-1} kunnen we dit gebruiken om het deel van $\wp(z)$ dat onder de som staat uit te werken:

$$\begin{aligned}(z-\omega)^{-2} - \omega^{-2} &= \omega^{-2}\left((1-\tfrac{z}{w})^{-2} - 1\right) \\ &= \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}}\end{aligned}$$

Als we dit invullen in de definitie van de Weierstrass $\wp$-functie en de sommen omwisselen krijgen we

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-n-2}.$$

Omdat $\wp(z)$ een even functie is kan $n = 2k$ genomen worden, waarbij de som over $k \in \mathbb{Z}_{>0}$ loopt. Dit geeft het gewenste resultaat. □

Propositie 2.5. Voor alle $z \in \mathbb{C}$ met $z \notin \Lambda$ geldt:

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\,\wp(z) - 140G_6$$

Bewijs. Schrijf de Laurentreeksen rond $z = 0$ van de verschillende functies uit:

$$\begin{aligned}\wp(z) &= z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots \\ \wp(z)^3 &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \dots \\ \wp'(z)^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \dots\end{aligned}$$

We zien dat de functie

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\,\wp(z) + 140G_6$$

holomorf is rond $z = 0$ omdat na invullen van de Laurentreeksen de termen met negatieve machten van z tegen elkaar wegvallen. Op dezelfde manier zien we dat $f(0) = 0$. Maar f is elliptisch ten opzichte van Λ en vanwege stelling 2.3 holomorf op heel $\mathbb{C} \setminus \Lambda$. Dus f is een holomorfe elliptische functie en uit stelling 2.2 volgt dat f constant is. Er volgt dat $f(z) = 0$. □

Het is standaardnotatie om te schrijven

$$g_2 = g_2(\Lambda) = 60G_4 \quad \text{en} \quad g_3 = g_3(\Lambda) = 140G_6.$$

De gevonden algebraïsche relatie tussen $\wp(z)$ en $\wp'(z)$ stelt ons in staat een isomorfisme tussen elliptische krommen over $\mathbb{C}$ en complexe tori te maken.

Stelling 2.6. Laat g_2 en g_3 de getallen behorende bij het rooster $\Lambda \subset \mathbb{C}$. Laat $E/\mathbb{C}$ de kromme

$$E : y^2 = 4x^3 - g_2x - g_3. \tag{6}$$

Dit is een elliptische kromme. De afbeelding

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\longrightarrow E \qquad \text{gegeven door} \\ z &\longmapsto [\wp(z) : \wp'(z) : 1], \end{aligned}$$

voor $z \neq 0$ en door $\phi(0) = O$ is een isomorfisme van Riemann-oppervlakken.

Bewijs. Vergelijking (6) is van de vorm (2). Bewijzen we nu dat $f(x) = 4x^3 - g_2x - g_3$ geen dubbele nulpunten heeft, dan volgt dat $\Delta \neq 0$ en is E een elliptische kromme. Laat (ω_1, ω_2) een basis zijn voor Λ, en zij $\omega_3 = \omega_1 + \omega_2$. Omdat $\wp'(z)$ een oneven functie is volgt dat, voor $i \in \{1, 2, 3\}$,

$$\wp'\left(\tfrac{1}{2}\omega_i\right) = -\wp'\left(-\tfrac{1}{2}\omega_i\right) = -\wp'\left(\tfrac{1}{2}\omega_i\right).$$

Omdat $wp'(z)$ van orde 3 is, hebben we hiermee precies alle nulpunten van $\wp'$ gevonden: $\wp'\left(\frac{1}{2}\omega_i\right) = 0$. Uit stelling 2.5 volgt dat $f(x)$ nulpunten heeft in elke $x = \wp\left(\frac{1}{2}\omega_i\right)$, dus het is voldoende te laten zien dat deze drie waarden verschillend zijn. Dit zal volgen uit een deel van het bewijs van de injectiviteit van ϕ.

Merk eerst op dat het beeld van ϕ bevat is in E, vanwege stelling 2.5, dus de afbeelding is welgedefinieerd.

We bewijzen nu de injectiviteit. Neem aan dat $\wp(z_1) = \wp(z_2)$. Beschouw de functie $h(z) = \wp(z) - \wp(z_1)$. Dit is een elliptische functie met een pool van orde twee, dus h heeft 2 nulpunten vanwege propositie 2.1. Omdat h even is, heeft h nulpunten in z_1, $-z_1$ en z_2. Enkele van deze nulpunten moeten dus gelijk zijn; dit zullen we in detail uitwerken.

Als $2z_1 \in \Lambda$, ofwel $z_1 \equiv -z_1 \mod \Lambda$, dan heeft h een dubbel nulpunt in z_1 omdat h even is. Dit is in te zien door op te merken dat $h(-z + z_1) = h(-z - z_1) = h(z + z_0)$, Dus $h(z + z_1)$ is even, waardoor de Taylor-expansie van h rond z_1 alleen even termen bevat. Daarom is z_1 een dubbel nulpunt van h en zijn er geen andere nulpunten. Er volgt dat $z_2 \equiv z_1 \mod \Lambda$, waarmee een deel van de injectiviteit bewezen is.

Hiermee zijn we in staat het resterende deel van het eerste deel van het bewijs af te maken. Voor $z_1 = \frac{1}{2}\omega_i$ en $z_2 = \frac{1}{2}\omega_j$ kunnen we concluderen dat

$$\wp\left(\tfrac{1}{2}\omega_i\right) = \wp\left(\tfrac{1}{2}\omega_j\right) \quad \Rightarrow \quad \omega_i = \omega_j,$$

waarmee bewezen is dat f geen dubbele nulpunten heeft.

Als $2z_1 \notin \Lambda$ dan zijn z_1 en $-z_1$ twee verschillende nulpunten, en dus de enige. Er geldt $z_2 \equiv \pm z_1 \mod \Lambda$. Hieruit volgt, samen met de aanname $\wp(z_1) = \wp(z_2)$ en het feit dat $\wp'$ oneven is, dat

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1).$$

Er geldt $z_1 \neq \frac{1}{2}\omega_i$, dus $\wp'(z_1) \neq 0$, dus volgt $z_2 \equiv z_1 \mod \Lambda$. Dit bewijst dat ϕ injectief is.

Vervolgens bewijzen we de surjectiviteit. Laat hiervoor $[x : y : 1] \in E$. De elliptische functie $\wp(z) - x$ is niet constant, en heeft dus een nulpunt vanwege propositie 2.2. Noemen we dit nulpunt $z = a$, dan is $\wp'(a)^2 = y^2$. Door eventueel a door $-a$ te vervangen krijgen we $\phi(a) = [x : y : 1]$.

Om aan te tonen dat ϕ een holomorf isomorfisme is, kunnen we kijken naar zijn effect op de coraakruimte. We zullen hier alleen een schets van een bewijs geven. In elk punt van E is $\mathrm{d}x/y$ een niet-verdwijnende holomorfe differentiaal. De differentiaal

$$\phi^*(\mathrm{d}x/y) = \mathrm{d}\wp(z)/\wp'(z) = \mathrm{d}z$$

is ook holomorf, en zonder polen en nulpunten op elk punt van $\mathbb{C}/\Lambda$. Dus ϕ is lokaal een isomorfisme. Omdat ϕ bijectief is op heel $\mathbb{C}/\Lambda$, is ϕ ook globaal een isomorfisme. □

Omdat vergelijking (6) een elliptische kromme voorstelt kunnen we bij elk rooster Λ in $\mathbb{C}$ een elliptische kromme vinden, en stelling 2.6 vertelt ons dat deze kromme isomorf is met de complexe torus $\mathbb{C}/\Lambda$. We kunnen deze theorie formuleren in termen van categorieën. Hiervoor gebruiken we de volgende notatie.

Definitie. We noemen EC de categorie van elliptische krommen over $\mathbb{C}$. De morfismen zijn de complexe holomorfe afbeeldingen die O naar O afbeelden.

We noemen LA de categorie van roosters $\Lambda \subset \mathbb{C}$. De morfismen zijn de groepshomomorfismen van Λ_1 naar Λ_2, voor $\Lambda_1, \Lambda_2 \in$ LA.

Stelling 2.6 geeft zelfs aanleiding tot een functor van LA naar EC, die we hier verder zullen uitwerken. We kunnen ons afvragen hoe de morfismen van LA door zo'n functor worden afgebeeld op die van EC . Beschouw hiervoor eerst de holomorfe afbeeldingen tussen elliptische krommen in EC . De beelden van de morfismen van LA onder deze functor corresponderen met holomorfe functies tussen complexe tori. Het blijkt dat deze een betrekkelijk eenvoudige vorm hebben.

Laat Λ_1 en Λ_2 roosters zijn in $\mathbb{C}$. Zij $\alpha \in \mathbb{C}$ met de eigenschap $\alpha\Lambda_1 \subset \Lambda_2$. Dan is vermenigvuldiging met α

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \qquad \phi_\alpha(z) \equiv \alpha z \mod \Lambda_2$$

een holomorfe functie. De volgende stelling laat zien dat dit alle holomorfe functies zijn die we nodig hebben.

Stelling 2.7. Laat Λ_1 en Λ_2 roosters zijn in $\mathbb{C}$. De onderstaande afbeelding is een bijectie.

$$\begin{aligned} \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} &\longrightarrow \left\{ \begin{array}{c} \text{holomorfe afbeeldingen } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \text{met } \phi(0) = 0 \end{array} \right\} \\ \alpha &\longmapsto \phi_\alpha \end{aligned}$$

Bewijs. Stel dat $\phi_\alpha = \phi_\beta$, dan geldt voor alle $z \in \mathbb{C}$ dat $\alpha z \equiv \beta z \mod \Lambda$. Dus de afbeelding f gegeven door $f(z) = (\alpha - \beta)z$ stuurt $\mathbb{C}$ naar Λ_2. Omdat Λ_2 discreet is volgt dat f constant is. Dus $\alpha = \beta$.

Laat $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ een holomorfe afbeelding met $\phi(0) = 0$. Omdat $\mathbb{C}$ enkelvoudig samenhangend is kunnen we ϕ liften naar een afbeelding $f : \mathbb{C} \to \mathbb{C}$ met $f(0) = 0$ zodat het volgende diagram commuteert:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

We zien dat voor elke $z \in \mathbb{C}$ en $\omega \in \Lambda_2$ geldt $f(z+\omega) - f(z) \in \Lambda_2$. Omdat Λ_2 discreet is, is $f(z+\omega) - f(z)$ onafhankelijk van z. Dus

$$f'(z+\omega) = f'(z) \qquad \text{voor alle } z \in \mathbb{C}, \omega \in \Lambda_2,$$

ofwel f' is elliptisch. Maar f is ook holomorf, dus f is constant (propositie 2.2). Er volgt dat $f(z) = \alpha z + \gamma$ voor zekere $\alpha, \gamma \in \mathbb{C}$. Uit $\phi(0) = 0$ volgt dat $\gamma = 0$, en $f(\Lambda_1) \subset \Lambda_2$ impliceert $\alpha\Lambda_1 \subset \Lambda_2$. Dus met de notatie uit de stelling is $\phi = \phi_\alpha$.

□

Definieer nu een functor $\mathcal{F} : \underline{\text{LA}} \to \underline{\text{EC}}$ door elk rooster in $\mathbb{C}$ naar een elliptische kromme te sturen:

$$\mathcal{F} : \Lambda \longmapsto E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{7}$$

Noteren we een afbeelding van Λ_1 naar Λ_2 met α, zodat $\alpha\Lambda_1 \subset \Lambda_2$, dan stuurt $\mathcal{F}$ deze afbeelding naar ϕ_α zoals in stelling 2.7. Er geldt $\mathcal{F}(\alpha\beta) = \phi_{\alpha\beta} = \phi_\alpha \circ \phi_\beta$, en als $\Lambda_1 = \Lambda_2$ geldt $\mathcal{F}(1) = \mathrm{id}_{\mathcal{F}(\Lambda_1)}$, dus de functor $\mathcal{F}$ is welgedefinieerd.

De inverse van $\mathcal{F}$ stuurt een kromme $E \in \underline{\text{EC}}$ in de vorm

$$E : y^2 = 4x^3 - Ax - B$$

naar het periodenrooster op $\frac{\mathrm{d}x}{y}$ door alle pad-integralen over deze vorm te nemen. Schematisch ziet dit er uit als

$$\mathcal{F}^{-1} : E \longmapsto \Lambda_E = \left\{ \begin{array}{c} \text{periodenrooster} \\ \text{op } \frac{\mathrm{d}x}{y} \end{array} \right\} = \left\{ \int_\gamma \frac{\mathrm{d}x}{y} : \gamma \in \pi_1(E) \right\} \tag{8}$$

Het zou te ver voeren om in deze scriptie te bewijzen dat vergelijking (8) de inverse definieert van $\mathcal{F}$. We laten het daarom bij de opmerking dat elke elliptische kromme geschreven kan worden in de vorm (6) met een rooster Λ en de categorieën $\underline{\text{EC}}$ en $\underline{\text{LA}}$ equivalent zijn.

Gegeven een elliptische kromme E over $\mathbb{C}$ kan men isomorfe krommen verkrijgen door de de coördinatentransformatie

$$x \mapsto u^2 x \qquad y \mapsto u^3 y \qquad u \in \mathbb{C}^* \tag{9}$$

toe te passen. Deze transformatie wordt vastgelegd door een $u \in \mathbb{C}^*$. Dit kunnen we opvatten als een werking van $\mathbb{C}$ op de krommen in $\underline{\text{EC}}$. Ook in $\underline{\text{LA}}$ vinden we een natuurlijke $\mathbb{C}^*$-werking. Deze twee werkingen zijn compatibel. Laat E een elliptische kromme zijn in de vorm (2), dus deze wordt vastgelegd door coefficiënten A en B. Dan kunnen we de bovengenoemde werkingen opschrijven als

$$\text{in } \underline{\text{EC}}: \quad u \cdot E \longmapsto E : y^2 = 4x^3 - u^{-4}Ax - u^{-6}B \tag{10}$$

$$\text{in } \underline{\text{LA}}: \quad u \cdot \Lambda \longmapsto u\Lambda. \tag{11}$$

We noteren met E_Λ de kromme verkregen verkregen uit een rooster met $\mathcal{F}(\Lambda)$. Het is snel in te zien dat geldt $E_{u\cdot\Lambda} = u \cdot E_\Lambda$ door op te merken dat

$$g_2(u\Lambda) = u^{-4} \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-4} \qquad g_3(u\Lambda) = u^{-6} \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-6}.$$

Omgekeerd, tussen E en $E' = u \cdot E$ is er een isomorfisme van de vorm (9), en geldt voor $(x', y') \in E'$ dat

$$\frac{\mathrm{d}x'}{y'} = \frac{u^{-2}\mathrm{d}x}{u^{-3}y} = u\frac{\mathrm{d}x}{y},$$

dus $\mathcal{F}^{-1}(u \cdot E) = \Lambda_{E'} = u\Lambda_E$. Naar aanleiding hiervan geven we de volgende definitie.

Definitie. Twee roosters Λ_1 en Λ_2 in $\mathbb{C}$ zijn *homotheet* als er een $u \in \mathbb{C}^*$ is zodat $\Lambda_1 = u\Lambda_2$.

3 Reductie modulo priemen

In dit hoofdstuk bekijken we elliptische krommen over een lichaam K met een discrete valuatie ν op K. De formele definitie van een discrete valuatie hebben we in deze scriptie voornamelijk nodig voor propositie 3.1. Voor een meer intuitieve benadering, zie vergelijking (12).

Definitie. Een *discrete valuatie* op een lichaam K is een afbeelding ν van K naar $\mathbb{Z} \cup \{\infty\}$ zodat voor $x, y \in K$ geldt:

1. $\nu(xy) = \nu(x) + \nu(y)$
2. $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$
3. $\nu(0) = +\infty$

We noteren de valuatiering van K behorende bij ν met $R = \{x \in K^* : \nu(x) \geq 0\}$. Met p noteren we een uniformiserend element, dus (p) is het unieke maximale ideaal van R. Verder nemen we aan dat ν genormeerd is, dus $\nu(p) = 1$ [ATI].

Samengevat kunnen we elk element x van K^* schrijven als

$$x = a\, p^{\nu(x)} \quad \text{met } a \in R^*. \tag{12}$$

Als geldt $x \in R$ dan noemen we x geheel bij ν of bij p. Voor $x \in R$ kunnen we $\nu(x)$ opvatten als het aantal factoren p in x.

Laat nu E een elliptische kromme zijn over K, met $\operatorname{char} K \neq 2, 3$, gegeven door de vergelijking

$$E : y^2 = 4x^3 - Ax - B.$$

We zijn geïnteresseerd in een vergelijking met gehele coëfficiënten, omdat we dan naar een vergelijking modulo p kunnen gaan kijken. Met het toepassen van een coördinatentransformatie die (x, y) door $(u^{-2}x, u^{-3}y)$ vervangt, waarbij $u \in K^*$ deelbaar is door een grote macht van p, kunnen we een vergelijking krijgen met $A \in R$ en $B \in R$. Vervolgens kunnen we ons afvragen of er een minimale keuze is voor A en B. Als we een $u \in R$ vinden waarvoor geldt dat $u^{12} \mid \Delta$, dan kunnen we controleren of $u^4 \mid A$ en $u^6 \mid B$. Immers, zo'n u geeft aanleiding tot een transformatie die een vergelijking geeft met een A en B met minder factoren u. Een goed criterium is dus om te kijken naar een vergelijking met minimale Δ.

Definitie. Een vergelijking van E heet *minimaal* als, gegeven dat $A, B \in R$, $\nu(\Delta)$ minimaal is.

Er zijn verschillende manieren om te kijken of een vergelijking minimaal is. Als bijvoorbeeld geldt dat $\nu(\Delta) < 12$, dan is er geen $u \in R$ die deelbaar is door p zodat $u^{12} \mid \Delta$, en is de vergelijking minimaal.

Nu kunnen we kijken naar "reductie modulo p". Voor $x \in R$ noteren we $\tilde{x} \equiv x \mod p \in R/pR$. Merk op dat R/pR een lichaam is omdat pR een maximaal ideaal is. Het reduceren van de minimale vergelijking van een elliptische kromme E geeft een volgende kromme met de volgende vergelijking:

$$\tilde{E} : y^2 = 4x^3 - \tilde{A}x - \tilde{B}.$$

We noemen de kromme $\tilde{E}$ de reductie van E modulo p. De punten van E worden afgebeeld op $\tilde{E}$ door de reductie-afbeelding:

$$\begin{aligned} E(K) &\longrightarrow \tilde{E}(R/pR) \\ P &\longrightarrow \tilde{P}. \end{aligned}$$

Laat hiervoor $P \in E(K)$. Dan kunnen we homogene coördinaten $P = [x : y : z]$ vinden met $x, y, z \in R$ en tenminste een van x, y, z in R^*. Het gereduceerde punt $\tilde{P} = [\tilde{x} : \tilde{y} : \tilde{z}]$ zit in $\tilde{E}(R/pR)$.

Merk op dat de discriminant van $\tilde{E}$, genoteerd met $\tilde{\Delta}$, niet altijd ongelijk aan nul is. Als $\tilde{\Delta} = 0$ is noemen we de kromme $\tilde{E}$ *singulier* en is $\tilde{E}$ geen elliptische kromme.

Definitie. Laat E een elliptische kromme zijn en zij $\tilde{E}$ de gereduceerde kromme bij een minimale vergelijking van E. E heeft *goede reductie* bij ν of p als $\tilde{E}$ niet-singulier is.

Dus E heeft goede reductie als $\tilde{\Delta} \not\equiv 0 \mod p$. Dit is het geval als $p \nmid \Delta$. Om te bewijzen dat E goede reductie heeft is het daarom voldoende te controleren dat $\nu(\Delta) = 0$ of $\Delta \in R^*$.

Als E geen goede reductie heeft over K, dan is het mogelijk dat in een uitbreiding van K wel een minimale vergelijking is met $\nu(\Delta) = 0$. Hiermee zijn we aangekomen bij de definitie van potentieel goede reductie.

Definitie. Laat E/K een elliptische kromme. E heeft *potentieel goede reductie* over K, bij ν, als er een eindige uitbreiding van $K \subset K'$ bestaat zó dat E goede reductie heeft over K' bij een w boven ν.

We noteren de valuatie op een uitbreiding K' van K boven ν in het vervolg met w. De valuatiering van K' behorende bij w noteren we met R'. Deze situatie is samen te vatten in het volgende schema:

$$\begin{array}{ccccccc} (q) & \subset & R' & \subset & K' & \ni x = a\,q^{w(x)} & a \in R'^* \\ \cup & & \cup & & \cup & & \\ (p) & \subset & R & \subset & K & \ni x = b\,p^{\nu(x)} & b \in R^* \end{array} \tag{13}$$

In de context van een uitbreiding van ringen $R \subset R'$ kunnen we een verwante definitie geven van het geheel zijn van een element in R'.

Definitie. Zij R een ring en $\bar{K}$ de algebraïsche afsluiting van het quotiëntenlichaam van R. Een $x \in \bar{K}$ is *algebraïsch geheel over* R als x voldoet aan

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

met $a_i \in R$ en $n \in \mathbb{N}$.

Met de notatie uit schema (13) vinden we het volgende verband tussen de begrippen algebraïsch geheel en geheel bij q.

Propositie 3.1. Laat $x \in K'$ algebraïsch geheel over R. Dan is $x \in R'$. Met andere woorden: x is geheel bij w en $w(x) \geq 0$.

Bewijs. Voor dit bewijs gebruiken we de volgende uitspraak:

$$w(y) \neq w(z) \Rightarrow w(y+z) = \min\{w(y), w(z)\}, \tag{14}$$

met $y, z \in K'$. Neem hiervoor zonder verlies van algemeenheid aan dat $w(y) = \min\{w(y), w(z)\}$. Schrijf vervolgens $y = a\,q^{e_y}$ en $z = b\,q^{e_z}$, met $a, b \in R'$. Dus er geldt $e_y = w(y)$ en $e_z = w(z)$. Uitschrijven van $y + z$ geeft

$$y + z = q^{e_z}\left(a\,q^{e_y - e_z} + b\right),$$

waar $e_y - e_z \geq 0$. Als $e_y \neq e_z$ dan is $a\,q^{e_y - e_z} + b \in R'^*$, en volgt $w(y+z) = e_z$.

Het bewijs van propositie 3.1 gaat uit het ongerijmde. Stel dat niet geldt $w(x) \geq 0$, en schrijf $w(x) = -b$ met $b > 0$. Er geldt

$$\begin{aligned} w(x^n) &= -nb \\ w(a_{n-1}x^{n-1}) &\geq -(n-1)b > -nb \\ &\vdots \\ w(a_0) &> -nb. \end{aligned}$$

Dus uit (14) volgt dat $w(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = -nb$. Dit geeft een tegenspraak met $w(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = w(0) = +\infty$. Dus er geldt $w(x) \geq 0$.

□

De volgende stelling zegt of een elliptische kromme potentieel goede reductie heeft.

Stelling 3.2. Laat E/K een elliptische kromme. E heeft potentieel goede reductie bij ν dan en slechts dan als de j-invariant van E geheel is bij ν (dwz $j(E) \in R$).

Bewijs. $\Rightarrow$ Laat $K \subset K'$ een eindige uitbreiding zijn zó dat E goede reductie heeft over K'. Neem een minimale vergelijking voor E/K' en noteer deze als

$$y^2 = 4x^3 - A'x - B'.$$

Zij Δ' de discriminant bij deze vergelijking. Er geldt $A' \in R$ en $\nu(\Delta') = 0$, dus $\Delta' \in R^*$. Nu volgt dat

$$j = 2^6 3^3 \frac{A'^3}{\Delta'} \in R'.$$

Maar $j \in K$, want E is over K gedefinieerd, dus $j \in R$.

$\Leftarrow$ Neem aan dat $j \in R$. Doe een uitbreiding $K \subset K'$ zó dat er een $\lambda \in K'$ is waarmee na een coördinatentransformatie de vergelijking van E in de volgende Legendre-vorm verandert:

$$E : y^2 = x(x-1)(x-\lambda), \quad \lambda \neq 0, 1. \tag{15}$$

Uit (5) volgt het volgende verband tussen λ en j:

$$(1 - \lambda(1-\lambda))^3 - j\lambda^2(1-\lambda)^2 = 0. \tag{16}$$

Uit proposititie 3.1 volgt dat $\lambda \in R'$, dus de Weierstrass-vergelijking van E heeft gehele coëfficiënten bij w. Beschouwen we vergelijking (16) modulo een q boven p, dan is af te lezen dat $\lambda \not\equiv 0, 1 \mod q$. Er geldt $\Delta' \equiv 16\lambda^2(\lambda-1)^2$, en we zien dat $\Delta' \in R^*$, dus E heeft goede reductie over K'. □

Stelling 3.2 geeft al veel informatie over uitbreidingen die leiden tot goede reductie van een elliptische kromme E/K met potentieel goede reductie. Er volgt bijvoorbeeld dat het adjungeren van een λ uit vergelijking (15) aan K voldoende is. Vergelijking (16) vertelt ons dat deze uitbreiding van graad maximaal 6 is.

Echter deze λ wordt alleen impliciet gegeven door vergelijking (16). De resultaten van de volgende paragraaf kunnen gebruikt worden om expliciet zo'n uitbreiding te vinden.

3.1 Complexe elliptische krommen

Gegeven een rooster Λ zodat $j(\Lambda) = j\left(g_2(\Lambda), g_3(\Lambda)\right) \in R$, met $R \subset \mathbb{C}$ een discrete valuatiering, kunnen we ons afvragen of we ook reductie kunnen toepassen op de geassocieerde elliptische kromme E_Λ, gegeven door de functor $\mathcal{F}$ uit vergelijking (7). Echter nu hebben we het probleem dat de coëfficiënten $g_2(\Lambda)$ en $g_3(\Lambda)$ van de vergelijking van de verkregen kromme E_Λ zelfs transcendent kunnen zijn over R, en in het bijzonder niet geheel hoeven te zijn. Merk wel op dat E_Λ potentieel goede reductie heeft omdat $j(E_\Lambda) = j(\Lambda) \in R$. Het artikel [GUA] geeft een $u \in \mathbb{C}^*$ zodat de kromme $u \cdot E_\Lambda$ de volgende eigenschappen heeft:

- De vergelijking van $u \cdot E_\Lambda$ heeft algebraïsch gehele coëfficiënten over R.
- De kromme $u \cdot E_\Lambda$ heeft goede reductie bij een w boven ν.

Voor de theorie die volgt wordt meestal aangenomen dat het rooster Λ van de vorm $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$ is, met $\tau \in \mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. We beschouwen daarom de volgende natuurlijke afbeelding, met $\mathcal{S}$ de verzameling van roosters in $\mathbb{C}$.

$$\begin{aligned} \mathbb{H} &\longrightarrow \mathcal{S} \\ \tau &\longmapsto \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau. \end{aligned}$$

Een $\tau \in \mathbb{H}$ definieert dus een rooster. Omgekeerd is een rooster gegeven door $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$ hetzelfde als een rooster gegeven door

$$\mathbb{Z}\cdot(c\tau + d) + \mathbb{Z}\cdot(a\tau + b), \qquad \text{met } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Dit is vervolgens na draaiing en schaling gelijk aan $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\frac{a\tau+b}{c\tau+d}$. Dit induceert een bijectie

$$\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H} \xrightarrow{\cong} \mathbb{C}^* \setminus \mathcal{S},$$

waarbij de werking van $\mathrm{SL}_2(\mathbb{Z})$ op $\mathbb{H}$ gegeven wordt door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \longmapsto \frac{a\tau + b}{c\tau + d}.$$

Met E_τ noteren we kromme die via $\mathcal{F}$ geassocieerd is met het rooster $\Lambda = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$. We zullen de u van hierboven geven met behulp van de volgende twee

definities. We definiëren eerst de zogenoemde theta-factoren van E_τ in termen van *Thetanullwerte*. Thetanullwerte zijn functies $\theta_i(\tau)$ op $\mathbb{H}$. De definitie van Thetanullwerte zullen we hier niet geven.

Definitie. De theta-factoren van E_τ zijn

$$\rho_2(\tau) = \pi\theta_3(\tau)\theta_4(\tau), \quad \rho_3(\tau) = e^{\pi i/4}\theta_2(\tau)\theta_4(\tau), \quad \rho_4(\tau) = \pi\theta_2(\tau)\theta_3(\tau).$$

Definitie. Laat ρ_r een theta-factor zijn, met $r \in \{2,3,4\}$. De *algebraïsche Eisenstein-functies* en de *algebraïsche discriminant* zijn dan:

$$\begin{aligned}
\mathcal{G}_{2,r}(\tau) &= \frac{6^2}{\rho_r(\tau)^4} g_2(\tau) \\
\mathcal{G}_{3,r}(\tau) &= \frac{6^3}{\rho_r(\tau)^6} g_3(\tau) \\
\mathcal{D}_r(\tau) &= \frac{6^6}{\rho_r(\tau)^{12}} \Delta(\tau) = \mathcal{G}_{2,r}(\tau)^3 - 27\mathcal{G}_{3,r}(\tau)^2
\end{aligned}$$

De algebraïsche Eisenstein-functies zijn in feite de coëfficienten in de vergelijking van $u \cdot E_\lambda$. In de definitie vinden we dat $u = \frac{6}{\rho_r(\tau)}$.

De reden voor de term *algebraïsch* in deze definitie wordt duidelijk in stelling 3.4 hieronder, die een direct gevolg is van de volgende propositie. Het bewijs van propositie 3.3 wordt uiteengezet in [GUA].

Propositie 3.3. De genoemde invarianten voldoen aan de volgende relaties. Ten behoeve van de leesbaarheid is de afhankelijkheid van τ weggelaten en schrijven we $k = j(\tau) - 1728$.

1. $\mathcal{G}_{2,r}{}^3 - 3^2 j\, \mathcal{G}_{2,r} + 2^4 3^3 j = 0$;
2. $\mathcal{G}_{3,r}{}^6 + 2^4 3k\, \mathcal{G}_{3,r}{}^4 + k^2(j - 2^8 3)\, \mathcal{G}_{3,r}{}^2 + 2^{12} k^3 = 0$;
3. $\mathcal{D}_r{}^3 + 2^{10} 3^7\, \mathcal{D}_r{}^2 - 2^{12} 3^{12}(j - 2^8 3)\, \mathcal{D}_r + 2^{30} 3^{18} = 0$.

Stelling 3.4. De invarianten $\mathcal{G}_{2,r}(\tau)$, $\mathcal{G}_{3,r}(\tau)$ en $\mathcal{D}_r(\tau)$ zijn algebraïsch geheel over $\mathbb{Z}[j(\tau)]$, respectievelijk van graad maximaal 3, 6 en 3.

Laat Λ een rooster in $\mathbb{C}$ zijn van de vorm $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$. Laat E_τ een geassocieerde elliptische kromme over $K \subset \mathbb{C}$. Als E_τ potentieel goede reductie heeft bij een discrete valuatie ν op K, kunnen we nu met propositie 3.3 expliciet een vergelijking geven voor een kromme over $K' \supset K$ die goede reductie heeft bij w boven ν. Stelling 3.4 vertelt ons dat de uitbreiding $K \subset K'$ van een niet al te grote graad is.

Stelling 3.5. Laat E een elliptische kromme over een lichaam $K \subset \mathbb{C}$, met een geassocieerd rooster Λ, zodat E goede reductie heeft bij een valuatie ν op K. Laat p een uniformiserend element zijn van ν.

De vergelijking

$$\mathcal{E} : y^2 = 4x^3 - \mathcal{G}_{2,r}x - \mathcal{G}_{3,r} \tag{17}$$

is minimaal bij een w boven ν. In het bijzonder zijn $\mathcal{G}_{2,r}$ en $\mathcal{G}_{3,r}$ geheel bij ν. Als p niet 2 of 3 deelt, dan heeft de kromme $\mathcal{E}$ goede reductie over $L = K(\mathcal{G}_{2,r}, \mathcal{G}_{3,r})$ bij w boven ν.

Bewijs. Uit stelling 3.2 volgt dat $j(E)$ geheel is bij ν, en $\mathcal{G}_{2,r}$, $\mathcal{G}_{3,r}$ zijn algebraisch geheel over $\mathbb{Z}[j]$. Uit propositie 3.1 volgt dat ze geheel zijn bij ν.

De discriminant van $\mathcal{E}$ is een nulpunt $\mathcal{D}_r$ van vergelijking 3 uit propositie 3.3. Hieruit volgt dat de norm van $\mathcal{D}_r$ gelijk is aan $|\mathcal{D}_r| = 2^{30}3^{18}$. Met andere woorden, $\nu(\mathcal{D}_r) = 0$ als p niet 2 of 3 deelt. Er volgt dat vergelijking (17) minimaal is en dat $\mathcal{E}$ goede reductie heeft bij w. □

Als $j(E)$ algebraïsch geheel is over $\mathbb{Z}$, dan heeft E potentieel goede reductie bij iedere valuatie op K. Stelling 3.5 geeft nu een vergelijking die minimaal is bij bijna elke valuatie op K. Alleen bij valuaties met een uniformiserend element dat 2 of 3 deelt heeft $\mathcal{E}$ mogelijk geen goede reductie.

Stelling 3.2 geeft slechts impliciet een uitbreiding om goede reductie te verkrijgen voor een enkele valuatie. Maar met stelling 3.5 hebben we expliciete coëfficiënten gevonden voor een vergelijking met goede reductie. Sterker nog, de gevonden vergelijking heeft goede reductie voor potentieel goede reductie bij alle valuaties met een uniformiserend element dat niet 2 of 3 deelt. Stelling 3.5 is dus een globale benadering.

Achter het bewijs van stelling 3.5 zit veel complexe analyse, terwijl de uitspraken in de stelling enkel algebraïsch van aard zijn. Een interessante vraag is dus of er een meer algebraïsche benadering bestaat.

Referenties

[GUA] J. Guàrdia, *Jacobi Thetanullwerte, periods of elliptic curves and minimal equations,* Mathematical Research Letters 11 (2004), p. 115-123.

[SIL] J. Silverman, *The arithmetic of elliptic curves.* Graduate texts in Mathematics 106, Springer-Verlag, 1986.

[ATI] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[GRE] Steven G. Kantz, Robert E. Greene, *Function Theory of One Complex Variable.* American Mathematical Society, 3 edition, 2006.

[EKE] Torsten Ekedahl, *One Semester of Elliptic Curves.* EMS Series of Lectures in Mathematics, European Mathematical Society, 2006.

Contactgegevens

Ron Hoogwater
email: ronhoogwater@gmail.com
Kaiserstraat 22-D
2311 GR Leiden