

Gehele punten op elliptische krommen

M de Leeuw

20 oktober 2003

Inhoudsopgave

1	Inleiding	2
1.1	Notaties	2
2	Isomorfismes	4
2.1	Isomorfisme tussen $E(\mathbb{C})$ en \mathbb{C}/Λ	4
2.2	Isomorfisme tussen $E_0(\mathbb{R})$ en \mathbb{R}/\mathbb{Z}	9
3	Hoogtes	11
3.1	Hoogtes	11
3.2	De Canonieke Hoogtes	16
3.3	Het verschil tussen de Weil-hoogte en de canonieke hoogte	18
4	Ongelijkheden	26
4.1	Elementaire ongelijkheden	26
4.2	De uiteindelijke ongelijkheid	28
5	Het Lenstra, Lenstra, Lovász-algoritme	30
5.1	Gereduceerde bases	30
5.2	Het algoritme	31
5.2.1	Voorbeeld	33
5.3	Toepassing	34
6	Voorbeeld	35
7	Literatuurlijst	39

Hoofdstuk 1

Inleiding

In het begin van de twintigste eeuw bewees Siegel dat er slechts eindig veel gehele punten op elliptische krommen waren. Hij bewees dit m.b.v diophantische approximatie. In deze scriptie zal ik ook op zoek gaan naar alle gehele punten op elliptische krommen. Dit doe ik echter niet net als Siegel met diophantische approximatie, maar met het afschatten van lineaire vormen in elliptische logaritmes. Ik zal dit doen aan de hand van een artikel geschreven door R.J. Stroeker en N. Tzanakis ([ST]). Voor het vinden van de bovengrens voor deze punten is aardig wat afschatwerk nodig en ik wens de lezer de nodige sterkte toe in sommige taaie en soms saaie bewijzen. Ik ga er van uit dat de lezer ongeveer als voorkennis het boek Rational Points on Elliptic Curves, J.H. Silverman en J. Tate heeft. Ik zal in de volgende paragraaf eerst wat notatie doornemen. Het eerste hoofdstuk gaat over het isomorfisme tussen $E(\mathbb{C})$ en \mathbb{C}/Λ . Dit isomorfisme blijkt nodig als we elliptische logaritmes gaan bekijken. In het tweede hoofdstuk wordt er dan nader in gegaan op het begrip hoogtes. Bij het afschatten wordt namelijk veel gebruik gemaakt van eigenschappen van de canonicke hoogte, de Weil-hoogte en het verschil tussen beide. Het hoofdstuk wat hierop volgt zal de verkregen theorie uit voorgaande hoofdstukken gebruiken bij uiteindelijk construeren van een bovengrens. Deze bovengrens is echter vaak nog te groot om alle gehele punten hieruit te verkrijgen. Dit probleem kan worden opgelost m.b.v het zogenaamde LLL-algoritme wat de verkregen bovengrens behoorlijk kan reduceren. Aan het eind van de scriptie zal ik de behandelde theorie in praktijk gaan brengen en alle gehele punten vinden op de kromme die gegeven wordt door:

$$\frac{1}{2}y^2 + \frac{1}{2}y = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x.$$

Gehele punten op deze kromme corresponderen met getallen x, y zodat de som van de eerste y getallen gelijk is aan de som van de eerste x kwadraten. Aan het eind van deze scriptie is ook nog een literatuurlijst te vinden. Hierin staan niet alleen boeken waarnaar verwezen wordt in de tekst, maar ook boeken die gebruikt zijn bij het maken van de tekst.

1.1 Notaties

We willen expliciet alle oplossingen $(X, Y) \in \mathbb{Z}$ vinden van de volgende vergelijking:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

met $a_i \in \mathbb{Z}$. Deze vergelijking definieert een elliptische kromme E over \mathbb{Q} , tenminste als deze een discriminant ongelijk 0 heeft. Als we nu een geschikte getallen $u, v, w, z \in \mathbb{Q}, u \neq 0$ kiezen en we nemen

$$X = u^2x + v, \quad Y = u^3y + wu^2x + z, \tag{1.2}$$

dan krijgen we een vergelijking voor E van de volgende vorm:

$$y^2 = x^3 + ax + b = f(x). \tag{1.3}$$

Hierin heeft $f(x)$ een discriminant ongelijk 0. Laatstgenoemde vorm is het makkelijkst te gebruiken. Een geheel punt $P = (X(P), Y(P))$ is een punt met gehele coördinaten die aan formule 1.1 voldoet. Het daarmee corresponderende punt $(x(P), y(P))$ hoeft dus geen geheel punt te zijn. Verder noteren we de rang van de elliptische kromme met r . We zijn alleen geïnteresseerd in het geval $r \geq 1$ omdat je voor het geval $r = 0$ alle punten al kent (d.m.v. Lutz-Nagell). We weten vanwege Mordell-Weil dat de groep van rationale punten van de volgende vorm is:

$$E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r.$$

De voortbrengers van het niet torsie gedeelte van de groep worden genoteerd met $\{P_1, \dots, P_r\}$. Er geldt dus dat ieder punt $P \in E(\mathbb{Q})$ te schrijven is als:

$$P = m_1 P_1 + \dots + m_r P_r + T \tag{1.4}$$

met $m_i \in \mathbb{Z}$ en $T \in E_{tors}$. Nu wordt in de rest van het artikel aangenomen dat de voortbrengers bekend zijn.

Hoofdstuk 2

Isomorfismes

In dit hoofdstuk zullen een aantal isomorfismes worden behandeld die nodig zijn bij het bestuderen van elliptische krommen.

2.1 Isomorfisme tussen $E(\mathbb{C})$ en \mathbb{C}/Λ

In deze paragraaf zal een isomorfisme van een elliptische kromme met de complexe getallen worden behandeld.

Zij E een elliptische kromme gedefinieerd over \mathbb{C} . Stel nu dat we een afbeelding proberen te definiëren:

$$\begin{aligned} E(\mathbb{C}) &\longrightarrow \mathbb{C} \\ P &\mapsto \int_O^P \frac{dx}{y} \end{aligned}$$

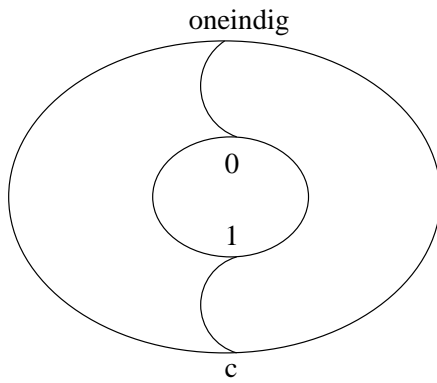
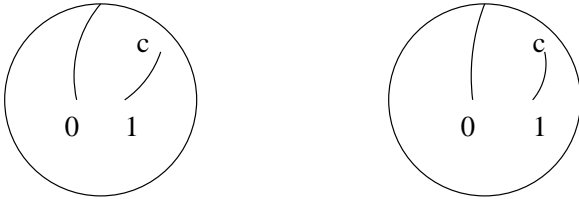
waar de integraal een langs een pad is dat O met P verbindt. Er doen zich vrij snel problemen voor, omdat de uitkomst van de integraal niet padonafhankelijk is. Er horen namelijk bij een x -waarde twee y -waardes. Verder hebben we dat een elliptische kromme voldoet aan een vergelijking van de vorm $y^2 = x^3 + ax + b$ (na wat coördinatentransformaties). We verkrijgen dus de y -waarde bij een zekere x m.b.v. wortels. Nu is in het complexe vlak worteltrekken alleen goed gedefinieerd als we daar bijvoorbeeld de negatieve reële as uit weglaten. Dit komt doordat worteltrekken is gedefinieerd met de complexe logaritme. We zien dus dat bovenstaande integraal alleen goed is gedefinieerd als we uit het complexe vlak de twee lijnen weglaten waarop $x^3 + ax + b$ negatief is.

Om de integraal goed uit te rekenen moeten we dus twee kopieën van het complexe vlak met daaruit twee lijnen weggelaten bekijken. Het complexe vlak is feitelijk homeomorf met een bol met als polen 0 en ∞ (via de stereografische projectie). Als we nu deze bollen wat uitrekken langs de lijnen en we plakken ze vervolgens aan elkaar, dan krijgen we een torus (figuur 2.1 op de volgende pagina). Hierop moet bovenstaande integraal dus bekeken worden. In onderstaand figuur is een kromme genomen die wordt beschreven door de vergelijking $y^2 = x(x-1)(x-c)$. Dit is echter geen probleem omdat je een kromme altijd op die vorm kan brengen (zie [Si1] III,1.7).

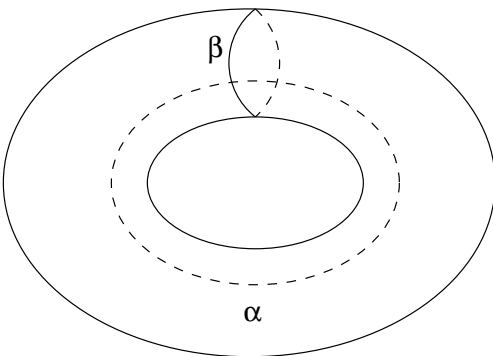
Omdat in een torus alle lussen worden voortgebracht door twee onafhankelijke paden α en β (figuur 2.2), geldt dat alle paden van O naar P padhomotoop zijn op iets homotoop met $n\alpha + m\beta$ na.

We hebben dus dat de integraal welgedefinieerd is (volgt m.b.v. de integraalstelling Cauchy en het lineair zijn van integralen) modulo constantes ω_1 en ω_2 . Waar deze constantes worden gegeven door:

$$\begin{aligned} \omega_1 &= \int_\alpha \frac{dx}{y}, \\ \omega_2 &= \int_\beta \frac{dx}{y}. \end{aligned}$$



Figuur 2.1: De vorming van de torus



Figuur 2.2: Paden op de torus

We gaan nu aantonen dat we hiermee een isomorfisme kunnen construeren door eerst naar een andere functie te gaan kijken.

Beschouw nu een rooster Λ in \mathbb{C} voorgebracht door twee complexe getallen ω_1 en ω_2 (deze notatie geen toeval m.b.t bovenstaande, zoals later zal blijken). We kunnen nu de volgende functie bekijken:

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

Deze functie wordt de Weierstrass-p-functie genoemd en hij heeft de volgende eigenschappen ([La hoofdstuk XIV]):

$$\wp'(z)^2 = 4\wp(z)^3 + g_2\wp(z) + g_3, \quad (2.1)$$

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) - \frac{1}{4} \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}. \quad (2.2)$$

Hierin zijn g_2 en g_3 bepaalde machtreeksen die afhangen van Λ , namelijk $g_2 = 60 \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-4}$ en $g_3 = 140 \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-6}$. Aangezien g_2 en g_3 alleen afhangen van het rooster schrijven we ook wel $g_2(\omega_1, \omega_2)$ en $g_3(\omega_1, \omega_2)$. Er volgt dus dat \wp de volgende elliptische kromme parametrizeert

$$y^2 = 4x^3 + g_2x + g_3 =: f_1(x) \quad (2.3)$$

d.m.v. het volgende groepsisomorfisme ψ tussen de elliptische kromme $y^2 = 4x^3 + g_2x + g_3$ en \mathbb{C}/Λ , dat gegeven wordt door:

$$\begin{aligned} \psi : \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ \psi : z &\mapsto [\wp(z), \wp'(z), 1]. \end{aligned}$$

Dit is een isomorfisme omdat eigenschap 2.2 er voor zorgt dat optelling behouden wordt. En verder geldt dat deze functie bijectief is. Eerst maar injectiviteit controleren. Stel we hebben dat $\psi(z_1) = \psi(z_2)$. Eerst nemen we aan dat $2z_1$ niet in Λ ligt. Er volgt nu dat de functie $\wp(z) - \wp(z_1)$ drie nulpunten heeft, namelijk $z_1, -z_1, z_2$ (\wp is even). Verder heeft deze functie orde twee en dus moeten we hebben dat $z_2 = \pm z_1 \pmod{\Lambda}$. Bekijken we nu \wp' , dan krijgen we $\wp'(z_1) = \wp'(z_2) = \pm \wp'(z_1)$ en dus volgt $z_1 = z_2 \pmod{\Lambda}$. ($\wp' \neq 0$ omdat de wortels allen verschillend zijn). Als nu wel $2z_1 \in \Lambda$ dan zien we dat $\wp(z) - \wp(z_1)$ een dubbel nulpunt heeft op z_1 en ook nul is op z_2 . We concluderen dus weer injectiviteit.

Nu surjectiviteit. Stel nu $(x, y) \in E$ en bekijk de functie $\wp - x$. Dit is een niet-constante elliptische functie en dus heeft deze een nulpunt ([Si1], VI prop 2.1), zeg $z = a$. Uit de vergelijking voor E volgt nu dat $\wp'^2(a) = y^2$. Hieruit volgt natuurlijk $\wp'(a) = \pm y$, omdat \wp' nu oneven is kunnen we dus krijgen dat $\wp'(a) = y$ door a door $-a$ te vervangen als dat nodig is.

We kunnen ons nu afvragen of er bij iedere niet-singuliere elliptische kromme wel een rooster bestaat. Het antwoord hierop is ja. Dit zal in het komende gedeelte bewezen worden.

Lemma 2.1.1 *Zij $\rho = e^{\frac{2\pi i}{3}}$ dan hebben we:*

$$g_2(1, \rho) = 0, \quad g_3(1, i) = 0.$$

Bewijs. Er geldt $\rho^3 = 1$ en $\rho^2 + \rho + 1 = 0$. We krijgen nu dus de volgende gelijkheden:

$$\begin{aligned} \frac{1}{60}g_2(1, \rho) &= \sum_{n, m \in \mathbb{Z}} \frac{1}{(m + n\rho)^4} = \sum_{n, m \in \mathbb{Z}} \frac{1}{(m\rho^3 + n\rho)^4} \\ &= \frac{1}{\rho^4} \sum_{n, m \in \mathbb{Z}} \frac{1}{(m\rho^2 + n)^4} = \frac{1}{\rho} \sum_{n', m' \in \mathbb{Z}} \frac{1}{(m' + n'\rho)^4} \\ &= \frac{1}{60\rho}g_2. \end{aligned}$$

En dus volgt het gestelde. Het bewijs voor de tweede identiteit gaat volledig analoog, alleen wordt er nu gebruik gemaakt van $i^2 = -1$.

q.e.d.

Stelling 2.1.2 Gegeven twee complexe getallen a_2 en a_3 z.d.d. $a_2^3 - 27a_3^2 \neq 0$ dan zijn er complexe getallen ω_1, ω_2 met $\frac{\omega_1}{\omega_2}$ niet reëel zodat $g_2(\omega_1, \omega_2) = a_2$ en $g_3(\omega_1, \omega_2) = a_3$.

Bewijs. In dit bewijs onderscheiden we 3 gevallen.

Geval 1 $a_2 = 0$. In dit geval volgt dus dat $a_3 \neq 0$. Kies nu een complex getal ω_1 zodat dit getal voldoet aan:

$$\omega_1^6 = \frac{g_3(1, \rho)}{a_3}.$$

Neem vervolgens $\omega_2 = \rho\omega_1$, dan volgt onmiddellijk (m.b.v bovenstaand lemma):

$$\begin{aligned} g_2(\omega_1, \omega_2) &= g_2(\omega_1, \rho\omega_1) = \frac{1}{\omega_1^4} g_2(1, \rho) = 0 = a_2 \\ g_3(\omega_1, \omega_2) &= g_3(\omega_1, \rho\omega_1) = \frac{1}{\omega_1^6} g_3(1, \rho) = a_3. \end{aligned}$$

Geval 2 $a_3 = 0$. Dit keer volgt dus dat $a_2 \neq 0$. Kies nu een complex getal ω_1 zodat dit getal voldoet aan:

$$\omega_1^4 = \frac{g_2(1, i)}{a_2}.$$

Neem vervolgens $\omega_2 = i\omega_1$, dan volgt onmiddellijk (weer m.b.v. bovenstaand lemma):

$$\begin{aligned} g_2(\omega_1, \omega_2) &= g_2(\omega_1, i\omega_1) = \frac{1}{\omega_1^4} g_2(1, i) = a_2 \\ g_3(\omega_1, \omega_2) &= g_3(\omega_1, i\omega_1) = \frac{1}{\omega_1^6} g_3(1, i) = 0 = a_3. \end{aligned}$$

Nu het laatste geval.

Geval 3 $a_2 a_3 \neq 0$. Kies dit keer een complex getal τ dat voldoet aan:

$$J(\tau) := \frac{g_2^3(1, \tau)}{g_2^3(1, \tau) - 27g_3^2(1, \tau)} = \frac{a_2^3}{a_2^3 - 27a_3^2}.$$

Er geldt nu dat $J(\tau) \neq 0$ en er geldt ook dat

$$\frac{J(\tau) - 1}{J(\tau)} = \frac{27a_3^2}{a_2^3}. \quad (2.4)$$

Kiezen dan we nu ω_1 zo dat deze voldoet aan:

$$\omega_1^2 = \frac{a_2 g_3(1, \tau)}{a_3 g_2(1, \tau)}$$

en $\omega_2 = \tau\omega_1$, dan volgt er:

$$\frac{g_2(\omega_1, \omega_2)}{g_3(\omega_1, \omega_2)} = \frac{\omega_1^{-4} g_2(1, \tau)}{\omega_1^{-6} g_3(1, \tau)} = \frac{a_2}{a_3}.$$

Uit de definitie van $J(\tau)$ volgt in combinatie met voorgaande formule tenslotte dat

$$\frac{J(\tau) - 1}{J(\tau)} = \frac{27g_3^2}{g_2^3} = 27 \frac{a_3^2 g_2^2}{a_2^3 g_3^3}. \quad (2.5)$$

Als we nu 2.4 en 2.5 vergelijken volgt onmiddellijk dat $g_2(\omega_1, \omega_2) = a_2$ en daarmee volgt ook direct dat $g_3(\omega_1, \omega_2) = a_3$.

q.e.d.

In bovenstaand bewijs is gebruikt dat er een τ is met de eigenschap dat $J(\tau) = a$ voor zekere a . Dat deze τ inderdaad bestaat kan bewezen worden m.b.v modulaire functies, zie bijv. [S11] Appendix C paragraaf 12.

We hebben nu dus dat er voor iedere kromme een rooster is zodat

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

Na dit uitstapje kunnen we nu onze integraal uit het begin van dit hoofdstuk gebruiken om een isomorfisme te definiëren. Als we nu een elliptische kromme E en bijbehorend rooster Λ bekijken, neem dan:

$$\begin{aligned} \phi : E(\mathbb{C}) &\longrightarrow \mathbb{C}/\Lambda \\ \phi(P) &\equiv \begin{cases} 0 \pmod{\Lambda} & (\text{als } P = O) \\ \int_{x(P)}^O \frac{dx}{y} \pmod{\Lambda} & (\text{als } y(P) \geq 0) \\ -\varphi(-P) \pmod{\Lambda} & (\text{als } y(P) < 0) \end{cases} \end{aligned} \quad (2.6)$$

Aangezien ψ van \mathbb{C}/Λ naar $E(\mathbb{C})$ een bijectie is, kunnen we de volgende variabelensubstitutie gebruiken: $x(P) = \wp(z), y(P) = \wp'(z)$. Gebruiken we dit, dan zien we al snel dat $\phi(\psi(z)) = z$ voor alle $z \in \mathbb{C}/\Lambda$. Hieruit volgt dus dat ϕ ook een isomorfisme is, omdat het de inverse van ψ (ook een isomorfisme) is.

Het enige wat nu nog rest is te bepalen of $\Lambda = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}$ (met ω_1 en ω_2 de integralen van het begin). Dit is inderdaad zo. We moeten nu eerst opmerken dat ψ niet alleen een isomorfisme is, maar ook een homeomorfisme. We hebben namelijk niet alleen dat ψ continu is, maar zijn inverse ook.

Stelling 2.1.3 *Zij E een elliptische kromme, Λ het bijbehorende rooster en α en β als boven, dan hebben we dat ω_1 en ω_2 een basis vormen voor Λ .*

Bewijs. We hebben dat α en β een basis vormen voor $H_1(E)$ en dus volgt ook dat $\phi \circ \alpha$ en $\phi \circ \beta$ een basis vormen voor $H_1(\mathbb{C}/\Lambda)$. Voorts geldt dat $H_1(\mathbb{C}/\Lambda) \cong \Lambda$ via het isomorfisme $f : \gamma \mapsto \int_\gamma dz$ (Deze functie f is duidelijk bijectief. Verder geldt triviaal dat $f(\gamma + \delta) = f(\gamma) + f(\delta)$ aangezien $\gamma(t) + \delta(t) = \gamma(2t)$ als $0 \leq t \leq \frac{1}{2}$ en $\gamma(t) + \delta(t) = \delta(2t - 1)$ als $\frac{1}{2} \leq t \leq 1$). We komen nu tot de conclusie dat:

$$\omega_1 = \int_\alpha \frac{dx}{y} = \int_{\phi \circ \alpha} dz, \quad \omega_2 = \int_\beta \frac{dx}{y} = \int_{\phi \circ \beta} dz$$

(variabelensubstitutie). En dus vormen ω_1 en ω_2 een basis voor Λ .

q.e.d.

We kunnen nu de volgende expliciete uitdrukkingen vinden voor ω_1 en ω_2 ([AS] blz. 641). Als $\Delta > 0$ dan hebben we:

$$\omega_1 = \int_{e_1}^{\infty} \frac{dt}{\sqrt{f_1(t)}} \quad (2.7)$$

$$\omega_2 = i \int_{-\infty}^{e_3} \frac{dt}{\sqrt{|f_1(t)|}}. \quad (2.8)$$

Als echter $\Delta < 0$ dan hebben we:

$$\omega_1 = \int_{e_1}^{\infty} \frac{dt}{\sqrt{f_1(t)}} + i \int_{-\infty}^{e_1} \frac{dt}{\sqrt{|f_1(t)|}} \quad (2.9)$$

$$\omega_2 = \overline{\omega_1}. \quad (2.10)$$

Nu nog een opmerking over het rooster. We kunnen een rooster zo kiezen dat, als we $\tau = \frac{\omega_1}{\omega_2}$ nemen, dat

$$|\tau| \geq 1, \quad \text{Im}(\tau) > 0, \quad -\frac{1}{2} < \text{Re}(\tau) \leq \frac{1}{2}, \quad |\tau| = 1 \Rightarrow \text{Re}(\tau) \geq 0. \quad (2.11)$$

2.2 Isomorfisme tussen $E_0(\mathbb{R})$ en \mathbb{R}/\mathbb{Z}

In deze paragraaf wordt het isomorfisme uit de vorige paragraaf gebruikt om het isomorfisme uit de titel te vinden. Dit isomorfisme zal later nodig blijken te zijn.

Stel, we hebben een elliptische kromme die beschreven wordt als (1.1) uit paragraaf 1.1. Als we nu eens γ de grootste reële wortel van $f(x)$ (weer in de notatie van paragraaf 1.1) nemen dan is het duidelijk dat alle gehele punten $X(P) \leq u^2\gamma + v$ gemakkelijk gevonden kunnen worden. Het is dus alleen nodig om de component van E te bekijken die naar oneindig gaat, namelijk:

$$E_0(\mathbb{R}) = \{P \in E \cap \mathbb{R}^2 \mid x(P) \geq \gamma\} \cup \{O\}.$$

We hebben nu een groepsisomorfisme tussen $E_0(\mathbb{R})$ en \mathbb{R}/\mathbb{Z} . Als we nu even ω nemen als

$$\omega = 2 \int_{\gamma}^{\infty} \frac{dt}{\sqrt{f(t)}},$$

dan wordt het isomorfisme gegeven door:

$$\begin{aligned} \varphi : E_0(\mathbb{R}) &\longrightarrow \mathbb{R}/\mathbb{Z} \\ \varphi(P) &\equiv \begin{cases} 0 \pmod{1} & (\text{als } P = O) \\ \frac{1}{\omega} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{f(t)}} \pmod{1} & (\text{als } y(P) \geq 0) \\ -\varphi(-P) \pmod{1} & (\text{als } y(P) < 0) \end{cases} \end{aligned} \quad (2.12)$$

Nu moet natuurlijk bewezen worden dat dit een isomorfisme is. Dit doen we door gebruik te maken van het isomorfisme uit de vorige paragraaf. Aangezien ψ een isomorfisme is tussen $E(\mathbb{C})$ en \mathbb{C}/Λ is het verstandig te kijken naar de beperking $\psi|_{\mathbb{R} \cap (\mathbb{C}/\Lambda)}$. Met $\mathbb{R} \cap (\mathbb{C}/\Lambda)$ bedoel ik het reële gedeelte van \mathbb{C}/Λ . We hebben dan natuurlijk dat

$$\mathbb{R} \cap (\mathbb{C}/\Lambda) \cong \text{Im}(\psi(\mathbb{R} \cap (\mathbb{C}/\Lambda)))$$

omdat ψ hierop nog steeds bijectief is en voldoet aan de optelregels. Aan de expliciete formules voor het rooster, behorende bij een elliptische kromme, kunnen we zien dat $\mathbb{R} \cap (\mathbb{C}/\Lambda)$ gelijk is aan $\mathbb{R}/2\omega\mathbb{Z}$. Als we nu kunnen laten zien dat $\psi(a) \in \mathbb{R}^2$ als $a \in \mathbb{R}$ dan hebben we dat het beeld van $\mathbb{R}/2\omega\mathbb{Z}$ inderdaad $E_0(\mathbb{R})$ is. Dit is zo omdat ψ een continue functie is. Er geldt daarom dat omdat $[0, 2\omega[$ samenhangend is, ook het beeld onder ψ samenhangend is. Verder geldt dat $\wp(\frac{\omega}{2})$ een nulpunt is van $f(x)$ (punt van orde 2) en $\psi(0) = O$. We zoeken dus een samenhangende deelverzameling van $E(\mathbb{R}) \cup \{O\}$ die een nulpunt bevat en O . Verder hebben we dat voor een $x \in [0, 2\omega[$ zowel $(\wp(x), \wp'(x))$ als $(\wp(x), -\wp'(x))$ erin zitten (we hebben immers vanwege het feit dat \wp even is en \wp' oneven dat $\wp'(x) = -\wp'(x + \omega)$ en $\wp(x) = \wp(x + \omega)$). De enige deelverzameling van $E(\mathbb{R}) \cup \{O\}$ die hieraan voldoet is $E_0(\mathbb{R})$.

Er moet dus nog bewezen worden dat \wp en \wp' reële getallen op reële getallen afbeeld. Voor het rooster dat we boven hebben gekregen zien we dat als $\omega \in \Lambda$ dan ook $\bar{\omega} \in \Lambda$. Omdat we voor complexe getallen a en b hebben dat

$$\overline{a + b} = \bar{a} + \bar{b}, \quad \overline{\frac{1}{a^2}} = \frac{1}{\bar{a}^2}$$

kunnen we voor $z \in \mathbb{R}$ \wp ook schrijven als:

$$\wp = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0, \text{Im}\omega > 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} + \overline{\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}} \right) + \sum_{\omega \in \Lambda, \omega \neq 0, \text{Im}\omega = 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

wat natuurlijk een reëel getal is. Voor \wp' hebben we de ontwikkeling:

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

Het gestelde volgt nu op analoge wijze. We hebben nu dus dat

$$\mathbb{R}/\mathbb{Z} \cong E_0(\mathbb{R})$$

met als isomorfisme de beperking van ψ . Er volgt nu dat φ dus precies de beperking van de ϕ uit de vorige paragraaf en is dus ook een isomorfisme.

Hoofdstuk 3

Hoogtes

Bij het bepalen van een bovengrens voor de gehele punten spelen hoogtes een belangrijke rol. In de eerste paragraaf zullen wat algemene eigenschappen van hoogtes op elliptische krommen worden afgeleid. Vervolgens zal de canonieke hoogte besproken worden. Tot slot zal nader worden ingegaan op het verschil tussen de Weil-hoogte en de canonieke hoogte.

3.1 Hoogtes

Allereerst een paar definities:

Definitie 3.1.1 *De verzameling absolute waarden op \mathbb{Q} , genoteerd met $M_{\mathbb{Q}}$, wordt gegeven door:*

1. $|x|_{\infty}$ (ook wel $|x|$). Dit is de normale absolute waarde.
2. Voor een priemgetal $p \in \mathbb{Z}$ bevat $M_{\mathbb{Q}}$ een niet archimedische absolute waarde (p -adische norm) gegeven door:

$$\left| p^n \frac{a}{b} \right|_p = p^{-n}. \quad (3.1)$$

Al deze absolute waarden voldoen aan de driehoeksongelijkheid. De p -adische norm voldoet zelfs aan wat sterkers omdat dit een niet-Archimedische absolute waarde is. We kunnen dit samenvatten als

$$|a_1 + \dots, a_n| \leq n^{\varepsilon(v)} \max_{0 \leq i \leq n} \{|a_i|_v\}.$$

Waarin $\varepsilon(v) = 0$ bij een niet-Archimedische norm v en $\varepsilon(v) = 1$ bij een Archimedische norm v .

Definitie 3.1.2 *De hoogte van een punt $P = [x_0, \dots, x_N]$ in de projectieve ruimte $\mathbb{P}^N(\mathbb{Q})$ wordt gegeven door:*

$$H(P) = \prod_{v \in M_{\mathbb{Q}}} \max\{|x_0|_v, \dots, |x_N|_v\}. \quad (3.2)$$

Het is niet direct duidelijk of dit wel een welgedefinieerd begrip is omdat bij een punt meerdere keuzes van homogene coördinaten mogelijk zijn. Hierover geeft het volgende lemma uitsluitsel.

Lemma 3.1.3 *De hoogte van een punt hangt niet af van de keuze van homogene coördinaten.*

Bewijs. Stel dat we een andere set coördinaten hebben. Dit is dan van de vorm: $[\lambda x_0, \dots, \lambda x_n]$ met $\lambda \in \mathbb{Q}^*$. Er geldt nu:

$$\begin{aligned} H([\lambda x_0, \dots, \lambda x_n]) &= \prod_{v \in M_{\mathbb{Q}}} \max_{0 \leq i \leq N} \{|\lambda x_i|_v\} \\ &= \prod_{v \in M_{\mathbb{Q}}} |\lambda|_v \prod_{v \in M_{\mathbb{Q}}} \max_{0 \leq i \leq N} \{|x_i|_v\}. \end{aligned}$$

Uit priemfactorisatie van teller en noemer volgt nu onmiddellijk dat $\prod_{priem} \left| \frac{a}{b} \right|_p = \frac{b}{a}$ (hier natuurlijk wel $a \neq 0$). Er volgt dus dat voor $a \in \mathbb{Q}^*$ dat $\prod_{v \in M_{\mathbb{Q}}} a = 1$ en dus volgt onmiddellijk uit bovenstaande dat $H([\lambda x_0, \dots, \lambda x_N]) = H([x_0, \dots, x_N])$.

q.e.d.

Voorts gebruiken we de notatie voor $x \in \mathbb{Q}$

$$H(x) := H([x, 1]). \quad (3.3)$$

We zien dat de hoogte in dit geval gegeven wordt door het maximum van de teller en noemer van x . Merk op dat onmiddellijk uit deze definitie volgt dat $H(P) \geq 1$.

Definitie 3.1.4 Een morfisme van graad d tussen twee projectieve ruimtes is een functie $F : \mathbb{P}^N \rightarrow \mathbb{P}^M$ met

$$F(P) = [f_0(P), \dots, f_M(P)]. \quad (3.4)$$

Hierin zijn de $f_i \in \overline{\mathbb{Q}}[X_0, \dots, X_N]$ en ze zijn homogene polynomen van graad d . Verder hebben deze polynomen geen gemeenschappelijk nulpunt op $X_0 = \dots = X_N = 0$ na. Het morfisme heet gedefinieerd over K als de coëfficiënten van de polynomen in K zitten.

De definitie van een morfisme hebben we nodig in het bewijs van wat afschattingen. De eerste zien we terug in de nu volgende stelling.

Stelling 3.1.5 Zij $F : \mathbb{P}^N \rightarrow \mathbb{P}^M$ een morfisme van graad d gedefinieerd over \mathbb{Q} . Dan zijn er positieve constanten C_1 en C_2 zodat voor alle $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ volgt:

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d. \quad (3.5)$$

Bewijs. Gebruik de driehoeksongelijkheid en het feit dat een f_i maximaal N^d termen heeft, dan volgt onmiddellijk:

$$|f_i(P)|_v \leq (N^d)^{\varepsilon(v)} D_i \max_{1 \leq k \leq N} \{|x_k|_v\}^d.$$

Hierin staat de D_i voor het maximum van de gebruikte absolute waarde van de coëfficiënten. Aangezien dit nu voor iedere f_i geldt volgt onmiddellijk dat

$$\max_{1 \leq i \leq M} \{|f_i(P)|_v\} \leq (N^d)^{\varepsilon(v)} \max_i \{D_i|_v\} \max_{1 \leq k \leq N} \{|x_k|_v\}^d.$$

We hebben dus nu:

$$\begin{aligned} H(F(P)) &= \prod_{v \in M_{\mathbb{Q}}} \max_{1 \leq i \leq M} \{|f_i|_v\} \\ &\leq C_1 H(P)^d. \end{aligned}$$

Waar C_1 gegeven wordt door N^d maal de hoogte van $[D_1, \dots, D_M]$.

Nu gaan we de ondergrens afleiden. Bekijk het ideaal A in $\mathbb{Q}[X_0, \dots, X_N]$ voortgebracht door bovengenoemde f_i . Omdat F een morfisme is weten we dat het enige gemeenschappelijke nulpunt van de polynomen $[0, \dots, 0]$ is. Aangezien ieder polynoom X_i hierop ook nul is, volgt met de Nullstellensatz (S.Lang, Algebra blz. 256) dat er een $e \in \mathbb{N}$ is zodat $X_i^e \in A$. Ofwel, we hebben:

$$X_i^e = \sum_{j=0}^M g_{ij} f_j, \quad g_{ij} \in \mathbb{Q}[X_0, \dots, X_N].$$

We kunnen aannemen dat de g_{ij} homogeen zijn van graad $e - d$. Met de driehoeksongelijkheid volgt nu onmiddellijk dat voor alle i :

$$\begin{aligned} \max_{0 \leq i \leq N} \{|x_i|_v^e\} &= \max_{0 \leq i \leq N} \left\{ \left| \sum_{j=0}^M g_{ij}(P) f_j(P) \right|_v \right\} \\ &\leq C_2^{\varepsilon(v)} \max_{0 \leq i \leq N} \{|g_{ij}(P) f_j(P)|_v\} \\ &\leq C_2^{\varepsilon(v)} \max_{0 \leq i \leq N, 0 \leq j \leq M} \{|g_{ij}(P)|_v\} \max_{0 \leq i \leq N} \{|f_j(P)|_v\}. \end{aligned}$$

Als we nu met m het maximum van de coëfficiënten van alle g_{ij} 's noteren volgt m.b.v de driehoeksongelijkheid:

$$|g_{ij}(P)|_v \leq C_3^{\varepsilon(v)} m |P|_v^{e-d}.$$

Waarin $|P|_v$ staat voor $\max_i \{|x_i|_v\}$. Merk op dat de C 's in dit bewijs alleen afhankelijk zijn van de g_{ij} en e , maar deze zijn alleen afhankelijk van N, M en F en dus kunnen ze ook in termen van deze dingen worden begrensd. Substitueren we dit nu in de bovenstaande afchatting, dan volgt als we ook nog links en rechts met $|P|_v^{d-e}$ vermenigvuldigen en het product over alle $v \in M_{\mathbb{Q}}$ nemen dat:

$$H(P)^d \leq C_4 H(F(P)).$$

En dus hebben we ook de ondergrens verkregen.

q.e.d.

Lemma 3.1.6 Zij $f(T) = T^d + a_1 T^{d-1} + \dots + a_d = (T - \alpha_1) \dots (T - \alpha_d)$ met $\alpha_i \in \mathbb{Q}$, dan geldt de volgende ongelijkheid:

$$2^{-d} \prod_{j=1}^d H(\alpha_j) \leq H([a_0, \dots, a_d]) \leq 2^{d-1} \prod_{j=1}^d H(\alpha_j). \quad (3.6)$$

Waarin $a_0 = 1$ is genomen.

Bewijs. We gebruiken hier inductie op d voor de volgende afchatting:

$$(2^{\varepsilon(v)})^{-d} \prod_{j=1}^d \max\{|\alpha_j|_v, 1\} \leq \max_{0 \leq i \leq d} \{|a_i|_v\} \leq (2^{\varepsilon(v)})^{d-1} \prod_{j=1}^d \max\{|\alpha_j|_v, 1\}.$$

Als we hebben $d = 1$ dan volgt de ongelijkheid onmiddellijk, immers:

$$\frac{1}{2} |\alpha_1|_v \leq |\alpha_1|_v \leq |\alpha_1|_v.$$

Stel nu dat het geldt voor $d - 1$. Kies nu de index k die hoort bij de wortel $\alpha_k = \max_{1 \leq i \leq d} \{\alpha_i\}$ en definieer het polynoom $g(T)$ als volgt:

$$\begin{aligned} g(t) &= (T - \alpha_1) \dots (T - \alpha_{k-1})(T - \alpha_{k+1}) \dots (T - \alpha_d) \\ &= T^{d-1} + b_1 T^{d-2} + \dots + b_{d-1}. \end{aligned}$$

Aangezien $f(T) = (T - \alpha_k)g(T)$ volgt voor de coëfficiënten dat:

$$a_i = b_i - \alpha_k b_{i-1}.$$

Hier moet dan wel $b_{-1} = 0$ en $b_d = 0$ gekozen worden. Nu eerst de bovengrens. Er geldt:

$$\begin{aligned}
\max\{|a_0|_v, \dots, |a_d|_v\} &= \max_{0 \leq i \leq d} \{|b_i - \alpha_k b_{i-1}|_v\} \\
&\leq 2^{\varepsilon(v)} \max_{0 \leq i \leq d} \{|b_i|_v, |\alpha_k b_{i-1}|_v\} \\
&\leq 2^{\varepsilon(v)} \max_{0 \leq i \leq d} \{|b_i|_v\} \max_{0 \leq i \leq d} \{|\alpha_k|_v, 1\} \\
&\leq (2^{\varepsilon(v)})^{d-1} (\max\{|\alpha_k|_v, 1\}) \prod_{j=1, j \neq k}^d \max\{|\alpha_j|_v, 1\} \\
&= (2^{\varepsilon(v)})^{d-1} \prod_{j=1}^d \max\{|\alpha_j|_v, 1\}.
\end{aligned}$$

In bovenstaande is in stap 2 de driehoeksongelijkheid gebruikt en in stap 4 de inductiehypothese toegepast op g .

Voor de ondergrens maken we onderscheid tussen 2 gevallen, nl. $|\alpha_k|_v \leq 2^{\varepsilon(v)}$ en $|\alpha_k|_v > 2^{\varepsilon(v)}$. Stel nu dus eerst dat $|\alpha_k|_v \leq 2^{\varepsilon(v)}$. We hebben nu, aangezien $\alpha_0 = 1$, dat:

$$\begin{aligned}
(2^{\varepsilon(v)})^{-d} \prod_{j=1}^d \max\{|\alpha_j|_v, 1\} &\leq (2^{\varepsilon(v)})^{-d} \max\{|\alpha_j|_v, 1\}^d \\
&\leq 1 \\
&\leq \max_{0 \leq i \leq d} \{|a_i|_v\}.
\end{aligned}$$

En dus geldt de ondergrens als $|\alpha_k|_v \leq 2^{\varepsilon(v)}$.

Stel nu $|\alpha_k|_v > 2^{\varepsilon(v)}$. We hebben nu de volgende afschattingen als v Archimedisches ($2^{\varepsilon(v)} = 2$):

$$\begin{aligned}
\max_{0 \leq i \leq d} \{|a_i|_v\} &= \max_{0 \leq i \leq d} \{|b_i - \alpha_k b_{i-1}|_v\} \\
&\geq (|\alpha_k|_v - 1) \max_{0 \leq i \leq d-1} \{|b_i|_v\} \\
&> \frac{|\alpha_k|_v}{2} \max_{0 \leq i \leq d-1} \{|b_i|_v\} \\
&= 2^{-d} \max\{|\alpha_k|_v, 1\} \prod_{i=1, i \neq k}^d \max\{|\alpha_i|_v, 1\} \\
&= 2^{-d} \prod_{j=1}^d \max\{|\alpha_j|_v, 1\}.
\end{aligned}$$

Hierin is in stap 3 de inductiehypothese, toegepast op g , gebruikt. Als v niet-Archimedisches ($2^{\varepsilon(v)} = 1$) is dan hebben we

$$\begin{aligned}
\max_{0 \leq i \leq d} \{|a_i|_v\} &= \max_{0 \leq i \leq d} \{|b_i - \alpha_k b_{i-1}|_v\} \\
&\geq \max_{0 \leq i \leq d-1} \{|b_i|_v\} \max\{|\alpha_k|_v, 1\}.
\end{aligned}$$

Hier kunnen we weer de inductiehypothese op toepassen. We hebben nu dus de hypothese bewezen en als we nu links en rechts producten nemen over v dan volgt de ongelijkheid 3.6.

q.e.d.

Nu gaan we deze resultaten gebruiken om hoogtes op elliptische krommen te definiëren. We kunnen nu de volgende hoogte nemen:

Definitie 3.1.7 De logaritmische hoogte $h(P)$ (of Weil-hoogte) van een punt P op de elliptische kromme wordt gegeven door:

$$h(P) = \log H(x(P)). \quad (3.7)$$

Vanwege de definitie van $H(x)$ is het duidelijk dat $h(P) \geq 0$.

Van deze hoogte hebben we een aantal eigenschappen nodig die we later zullen gebruiken bij de canonieke hoogte. De eerste eigenschap heeft te maken met het optellen van punten.

Stelling 3.1.8 Zij $E : y^2 = x^3 + Ax + B$, een elliptische kromme, dan geldt voor alle $P, Q \in E(\mathbb{Q})$ de volgende relatie:

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1).$$

Bewijs. Aangezien $h(O) = 0$ volgt onmiddellijk dat de relatie geldt als $P = O$ of $Q = O$. Stel nu dus $P, Q \neq O$. Voor verkort schrijfwerk introduceren we:

$$\begin{aligned} x(P) &= [x_1, 1], & x(Q) &= [x_2, 1] \\ x(P + Q) &= [x_3, 1], & x(P - Q) &= [x_4, 1]. \end{aligned}$$

Uit de optelformule voor punten op een elliptische kromme volgen de volgende relaties:

$$\begin{aligned} x_3 + x_4 &= \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}, \\ x_3x_4 &= \frac{2(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}. \end{aligned}$$

Definieer nu een functie $g : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ als volgt:

$$g([u, v, t]) = [u^2 - 4tv, 2u(At + v) + 4Bt^2, (v - At)^2 - 4Btu].$$

Als we nu t, u, v zien als $1, x_1 + x_2, x_1x_2$ dan zien we dat $g([t, u, v]) = [1, x_3 + x_4, x_3x_4]$. Nu gaan we bewijzen dat g een morfisme van graad twee is om op die manier stelling 1.1.3 te kunnen gebruiken. Alle polynomen van g zijn inderdaad homogeen en van graad 2 en nu moet er dus gekeken worden of er geen gemeenschappelijke nulpunten zijn op $[0, 0, 0]$ na. Stel nu dat $g([t, u, v]) = [0, 0, 0]$ en dat $t = 0$ dan zien we onmiddellijk dat $t = u = v = 0$. Stel nu dan $g([t, u, v]) = [0, 0, 0]$ en dat $t \neq 0$. Als we nu $\alpha = \frac{u}{2t}$ nemen en we delen het tweede en derde polynoom van g door t^2 dan krijgen we:

$$\begin{aligned} 4Ax + 4x\frac{v}{t} + 4B &= 0 \\ \left(\frac{v}{t}\right)^2 - 2\frac{Av}{t} + A^2 - 8Bx &= 0. \end{aligned}$$

Uit de het eerste polynoom halen we vervolgens $x^2 = \frac{v}{t}$ waardoor we de volgende vergelijkingen krijgen:

$$\begin{aligned} \varphi(x) &:= 4x^3 + 4Ax + 4B = 0 \\ \psi(x) &:= x^4 - 2Ax^2 - 8Bx + A^2 = 0. \end{aligned}$$

Er geldt:

$$(12x^2 + 16A)\varphi(x) - (3x^3 - 5Ax - 27B)\psi(x) = 4(4A^3 + 27B^2) \neq 0.$$

Dit is omdat we te maken hebben met een niet singuliere kromme (we herkennen de discriminant in de laatste term). Hieraan zien we ook dat de polynomen geen gemeenschappelijke wortel hebben anders zou er uit bovenstaande ongelijkheid geen constante ongelijk 0 uit kunnen komen. Dus g is een morfisme. We hebben nu een commutatief diagram:

$$\begin{array}{ccccc}
E & \times & E & \xrightarrow{G} & E \times E \\
\downarrow & & \downarrow & & \\
\sigma & \mathbb{P}^1 & \times & \mathbb{P}^1 & \mathbb{P}^1 \times \mathbb{P}^1 & \sigma \\
\downarrow & & \downarrow & & \\
\mathbb{P}^2 & & \xrightarrow{g} & & \mathbb{P}^2.
\end{array}$$

Gebruiken we nu dus het feit dat het diagram commutatief is en stelling 3.1.5, dan volgt:

$$\begin{aligned}
h(\sigma(P+Q, P-Q)) &= h(\sigma \circ G(P, Q)) \\
&= h(g \circ \sigma(P, Q)) \\
&= 2h(\sigma(P, Q)) + O(1).
\end{aligned} \tag{3.8}$$

Er geldt nu voor punten X, Y op E dat als $X = O$ of $Y = O$ $h(\sigma(X, Y)) = h(X) + h(Y)$. Stel nu dus dat $X, Y \neq O$ en schrijf dan $x(X) = [a, 1]$ en $x(Y) = [b, 1]$. Dan volgt dat $h(\sigma(X, Y)) = h([1, a+b, ab])$ en $h(X) + h(Y) = h(a) + h(b)$. Passen we nu lemma 3.1.6 toe op het polynoom $(T+a)(T+b)$ dan krijgen we dat

$$h(\sigma(X, Y)) = h(X) + h(Y) + O(1).$$

Passen we dit nu toe op het linkerlid en het uiteindelijke rechterlid van formule 3.8 dan volgt onmiddellijk:

$$h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1).$$

q.e.d.

Nu zullen we deze stelling nog toepassen in een laatste lemma voordat we naar de canonieke hoogte gaan kijken.

Lemma 3.1.9 *Zij E een elliptische kromme, $m \in \mathbb{Z}$ en $P \in E(\mathbb{Q})$, dan geldt:*

$$h(mP) = m^2 h(P) + O(1) \tag{3.9}$$

Bewijs. We hoeven alleen maar $m \geq 0$ te kiezen omdat $h(-mP) = h(mP)$. Verder geldt dit resultaat duidelijk voor $m = 0$ en $m = 1$. We gaan nu dit bewijs met inductie afmaken. Stel 3.9 geldt voor $m, m-1$. Kieszen we nu $P = mP$ en $Q = P$ en passen we stelling 3.1.8 toe dan volgt er:

$$\begin{aligned}
h((m+1)P) &= -h((m-1)P) + 2h((m)P) + 2h(P) + O(1) \\
&= -(m-1)^2 + 2m^2 + 2)h(P) + O(1) \\
&= (m+1)^2 h(P) + O(1).
\end{aligned}$$

q.e.d.

3.2 De Canonieke Hoogtes

We komen nu toe aan de canonieke hoogte. In de vorige paragraaf is in alle relaties tussen de hoogtes van punten een $O(1)$ te vinden. De canonieke hoogte is zo geconstrueerd dat de relaties uit bijv. stelling 3.1.8 exact worden. De eersten die deze hoogte hebben gevonden waren Néron en Tate. De canonieke hoogte is als volgt gedefinieerd:

Definitie 3.2.1 *De canonieke hoogte \hat{h} is de functie $\hat{h} : E(\mathbb{Q}) \rightarrow \mathbb{R}$ gedefinieerd door:*

$$\hat{h} = \lim_{N \rightarrow \infty} 4^{-N} h(2^N P). \tag{3.10}$$

De eerste vraag die nu rijst is of deze limiet wel bestaat. Het antwoord hierop is ja en het is een gevolg van het volgende lemma.

Stelling 3.2.2 *De reeks $\{4^{-N}h(2^N)\}_{N=0}^{\infty}$ is Cauchy en dus convergeert deze.*

Bewijs. Uit lemma 3.1.9 volgt dat er een constante C is zodanig dat voor alle $Q \in E(\mathbb{Q})$ geldt dat

$$|h(2Q) - 4h(Q)| \leq C. \quad (3.11)$$

Neem nu N, M twee gehele getallen groter dan 0 en $N > M$. Er geldt:

$$\begin{aligned} |4^{-N}h(2^N P) - 4^{-M}h(2^M P)| &= \left| \sum_{n=M}^{N-1} 4^{-n-1}h(2^{n+1}P) - 4^{-n}h(2^n P) \right| \\ &\leq \sum_{n=M}^{N-1} 4^{-n-1}|h(2^{n+1}P) - 4h(2^n P)| \\ &\leq \sum_{n=M}^{N-1} 4^{-n-1}C \\ &\leq C4^{-M}. \end{aligned} \quad (3.12)$$

Hierin is gebruik gemaakt van 3.11 met $Q = 2^n P$. Er volgt dus dat deze reeks Cauchy is.

q.e.d.

De nu volgende stelling is van belang voor de afschattingen die ik ga gebruiken om een bovengrens voor gehele punten af te leiden. Het is een stelling die erg op de stelling 3.1.8 en lemma 3.1.9 lijkt. Deze stellingen worden dan ook in het bewijs gebruikt.

Stelling 3.2.3 *Zij E een elliptische kromme. Voor alle $P, Q \in E(\mathbb{Q})$ en $m \in \mathbb{Z}$ geldt dan:*

1. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$
2. $\hat{h}(mP) = m^2\hat{h}(P)$
3. *De relatie $\langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is bilineair en \hat{h} is even*
4. $\hat{h}(P) = 0 \Leftrightarrow P$ is een torsiepoint
5. $\hat{h} = h + O(1)$.

Bewijs. Voor 1 en 2 gebruiken we stelling 3.1.8 en lemma 3.1.9. We nemen in deze stellingen $P = 2^N P$ en $Q = 2^N Q$ en vermenigvuldigen links en rechts met 4^{-N} . Laten we nu N naar oneindig gaan, dan krijgen we het gewenste resultaat. Nu onderdeel 3. We zien uit 1 dat \hat{h} even is (neem immers $P = O$). Vanwege de symmetrie in \langle, \rangle is het voldoende te bewijzen dat

$$\langle P+R, Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle.$$

Gebruiken we nu 1 vier keer en het feit dat \hat{h} even is, dan volgt er:

$$\begin{aligned} \hat{h}(P+R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P+R) - 2\hat{h}(Q) &= 0 \\ \hat{h}(P-R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P) - 2\hat{h}(R-Q) &= 0 \\ \hat{h}(P-R+Q) + \hat{h}(P+R+Q) - 2\hat{h}(P+Q) - 2\hat{h}(Q) &= 0 \\ 2\hat{h}(R+Q) + \hat{h}(R-Q) - 4\hat{h}(R) - 4\hat{h}(Q) &= 0. \end{aligned}$$

Tellen we vergelijking 1 en 3 op en halen we hier dan vergelijking 2 en 4 van af, dan volgt er:

$$\hat{h}(P+R+Q) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(R+Q) + \hat{h}(P) + \hat{h}(R) + \hat{h}(Q) = 0.$$

Wat hetzelfde is als $\langle P+R, Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle$. Nu zal eerst 5 bewezen worden. Als we in formule 3.12 $M = 0$ kiezen en N naar oneindig laten gaan, volgt m.b.v behoud van ongelijkheid bij limieten dat

$$|\hat{h}(P) - h(P)| \leq \frac{C}{4}.$$

Tot slot nog onderdeel 4. Stel dat P een torsiepoint is, ofwel $mP = O$ voor zekere $m \neq 0$. Dan volgt de ene implicatie via 2 onmiddellijk. Stel nu dat $\hat{h}(P) = 0$. Uit 5 volgt onmiddellijk dat er een C is z.d.d. voor alle $m \in \mathbb{Z}$ geldt:

$$h(mP) = |\hat{h}(mP) - h(mP)| \leq \frac{C}{4}.$$

Er geldt dus dat de verzameling $\{P, 2P, \dots\}$ bevat is in de verzameling $\{Q \in E(\mathbb{Q}) : h(Q) \leq C\}$ maar dit is een eindige verzameling (want je weet dat de hoogte niet afhangt van de keuze van homogene coördinaten (kies dan degene met gehele getallen) en je weet dat er slechts eindig veel gehele getallen zijn kleiner dan een bepaald getal (in dit geval $e^{C/4}$)) en dus is P een torsiepoint.

q.e.d.

3.3 Het verschil tussen de Weil-hoogte en de canonieke hoogte

Het verschil tussen de canonieke hoogte en Weil-hoogte is ook van belang bij de afschattingen. Dit verschil zal worden bepaald aan de hand van een artikel van Silverman ([Si2]). In dit artikel wordt dit gedaan m.b.v zogenaamde lokale hoogtes. Dit zijn functies op elliptische krommen die aan bepaalde eigenschappen voldoen. In het artikel staan de belangrijkste van de lokale hoogtes eigenschappen vermeld. Als de lezer het artikel bekijkt, houdt er dan rekening mee dat lemma 5.2.a onjuist is.

Er zijn nu een aantal lemma's die van pas zullen komen. Als er in deze paragraaf log staat, betekent dit de 10 log. Verder staat $\log^+ a$ voor $\log \max\{1, a\}$.

Lemma 3.3.1 *Voor alle reële getallen $a, b > 0$ geldt de volgende relatie:*

$$-\log^+(b^{-1}) \leq \log^+\left(\frac{a}{b}\right) - \log^+(a) + \log(b) \leq \log^+(b).$$

Bewijs. Er geldt na wat uitschrijven dat

$$\log^+\left(\frac{a}{b}\right) - \log^+(a) + \log(b) = \log\left(\frac{\max\{a, b\}}{\max\{a, 1\}}\right).$$

Als we nu alle mogelijke ordeningen controleren volgt het gestelde.

q.e.d.

Eerst nu wat notaties,

1. $\tau, z \in \mathbb{C}, \quad \text{Im}(\tau) > 0,$
2. $q = e^{2\pi i\tau}, \quad u = e^{2\pi iz},$
3. $\alpha = \frac{z}{\tau} = \frac{\log|u|}{\log|q|}.$

Verder zullen we soms een of beide van de volgende condities opleggen:

- * $|q| \leq e^{-\pi\sqrt{3}},$
- ** $0 \leq \alpha \leq \frac{1}{2}.$

Lemma 3.3.2 Voor een complex getal w met $|w| < 1$ hebben we de volgende ongelijkheid:

$$\frac{-|w|}{1-|w|} \leq \log|1-w| \leq |w|.$$

Bewijs. Schrijf $w = re^{i\varphi}$ met $r \in [0, 1[$, $\varphi \in [0, 2\pi[$. Bekijken we nu eerste de laatste ongelijkheid. In deze notatie zien we dat het rechterlid r wordt en het linkerlid gegeven wordt door $\frac{1}{2} \log(r^2 - 2r \cos(\varphi) + 1)$. Deze is maximaal als $\varphi = \pi$ en dus hebben we:

$$\log|1-w| \leq \log(1+r).$$

Dus we hoeven alleen nog te bewijzen dat $0 \leq 10^r - r - 1$. Differentiëren geeft dat dit een monotoon stijgende functie is en verder geldt $0 \leq 0$ en dus geldt de laatste ongelijkheid voor alle $0 \leq |w| < 1$. Nu de andere ongelijkheid. We zien nu dat $\log|1-w|$ minimaal is bij $\varphi = 0$ en dus krijgen we nu de volgende afchatting:

$$\log(1-r) \leq \log|1-w|.$$

Dus nu is te bewijzen dat

$$0 \leq \log(1-r) - \frac{-r}{1-r}.$$

Differentiëren geeft weer dat dit een monotoon stijgende functie is en aangezien voor $r = 0$ inderdaad geldt dat $0 \leq \log(1-r) - \frac{-r}{1-r}$ geldt de afchatting dus altijd voor $0 \leq r < 1$.

q.e.d.

Lemma 3.3.3 Zij $t \in \mathbb{C}$ z.d.d. $|qt| < 1$ dan geldt:

$$\frac{-|qt|}{(1-|q|)(1-|qt|)} \leq \sum_{n \geq 1} \log|1-q^n t| \leq \frac{|qt|}{1-|q|}.$$

Bewijs. Gebruik voorgaand lemma voor $w = q^n t$ (deze voldoet duidelijk aan de aanname omdat $|q^n t| \leq |qt| < 1$). De bovengrens verkrijgen we door te sommeren over $n \geq 1$. Als we dan in het rechterlid een factor $|qt|$ buiten de som halen herkennen we een meetkundige rij en hierdoor wordt de bovengrens verkregen. Nu de ondergrens. We hebben dat $\frac{1}{1-|q^n t|} \geq \frac{1}{1-|qt|}$ en dus krijgen we na toepassing van bovenstaand lemma

$$\sum_{n \geq 1} \log|1-q^n t| \geq - \sum_{n \geq 1} \frac{|q^n t|}{1-|q^n t|} \geq - \frac{1}{1-|qt|} \sum_{n \geq 1} |q^n t|.$$

Hier herkennen we weer de meetkundige reeks en dus volgt analoog aan boven ook de onderste afchatting.

q.e.d.

Deze lemma's zullen we nodig hebben bij de afchattingen die gaan komen. Zoals in de inleiding is gezegd zal het verschil tussen de Weil-hoogte en de canonicke hoogte bepaald m.b.v. lokale hoogtes λ_v . Er geldt namelijk dat:

$$\hat{h}(P) = \sum_{v \in M_Q} \lambda_v(P). \quad (3.13)$$

We kunnen deze relatie dan gaan gebruiken door eerst het verschil tussen de lokale hoogtes en het bijbehorende gedeelte van de Weil-hoogte te bepalen en vervolgens over de lokale hoogtes sommeren. We moeten nu onderscheidt maken tussen Archimedische en niet-Archimedisch lokale hoogtes. Allereerst een stelling over de niet-Archimedische hoogtes ([Si2] stelling 4.1).

Stelling 3.3.4 *Zij K een volledig lichaam t.o.v. een niet-Archimedische absolute waarde v en zij E/K een elliptische kromme met Weierstrass-vergelijking:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

zo dat alle coëfficiënten v -geheel zijn. Als nu Δ de discriminant is van bovenstaande vergelijking en j de j -invariant van E , dan hebben we voor alle $P \in E(K)$:

$$-\frac{1}{24} \log^+ |j|_v \leq \lambda_v(P) - \frac{1}{2} \log^+ |x(P)|_v \leq \frac{1}{12} v(\Delta).$$

Als we ook nog hebben dat $\text{ord}_v(j) = -1$ en $\text{ord}_v(c_4) = 0$, dan kan de ondergrens in de afchatting vervangen worden door $\frac{1}{12} \log^+ |j|_v$.

We gaan dan nu verder met de Archimedische lokale hoogtes.

Lemma 3.3.5 *Stel dat (*) geldt dan hebben we dat*

$$\begin{aligned} -5,695 &\leq \log^+ |j(\tau)| + \log |q| \leq 2,304 \\ -0,105 &\leq \log \left| \frac{1}{(2\pi)^{12}} \frac{\Delta(\tau)}{q} \right| \leq 0,1045. \end{aligned}$$

Bewijs. Eerst de tweede afchatting. We hebben dat $\Delta(\tau) = (2\pi)^{12} q \prod_{n \geq 1} (1 - q^n)^{24}$ (zie [Si1] Appendix C, paragraaf 12). We zien nu dus dat:

$$\log \left| \frac{1}{(2\pi)^{12}} \frac{\Delta(\tau)}{q} \right| = 24 \sum_{n \geq 1} \log |1 - q^n|.$$

We verkrijgen nu de afchatting door lemma 3.3.3 toe te passen en te gebruiken dat $|q| \leq e^{-\pi\sqrt{3}}$. Dan nu de eerste afchatting. We hebben $j(\tau) = \frac{(12g_2(\tau))^3}{\Delta(\tau)}$. Als we nu even Γ definiëren als $\Gamma = \frac{12}{(2\pi)^4} g_2(\tau)$, dan zien we dat we kunnen schrijven (gebruik weer [Si1] zelfde paragraaf): $\log |j(\tau)q| = 3 \log \Gamma(\tau) - 24 \log \prod_{n \geq 1} (1 - q^n)$. We gaan nu eerst $\log \Gamma(\tau)$ afschatten. De volgende afchatting geldt namelijk:

$$|\Gamma(\tau)| \leq 1 + \frac{240}{1 - |q|} \sum_{n \geq 1} n^3 |q^n| = 1 + 240|q| \frac{1 + 4|q| + |q|^2}{(1 - |q|)^5} \leq 2,0813.$$

Waarin in de laatste stap * is gebruikt. Verder geldt ook nog het volgende:

$$\begin{aligned} \log \left| \prod_{n \geq 1} (1 - q^n) \right| &\geq \sum_{n \geq 1} \log(1 - |q|^n) \geq \sum_{n \geq 1} \frac{-|q|^n}{1 - |q|^n} \\ &\geq -(1 - |q|)^{-1} \sum_{n \geq 1} |q|^n = \frac{-|q|}{(1 - |q|)^2} \geq -0,00472. \end{aligned}$$

In stap 2 is lemma 3.3.2 gebruikt. Combineren we nu deze afchattingen dan volgt de bovengrens onmiddellijk. Verder hebben we $-\log |q| > 0$ waardoor we in de uiteindelijke afchatting \log door \log^+ mogen vervangen. Nu de ondergrens. Er geldt voor Γ :

$$|\Gamma(\tau)| \geq 1 - \frac{240}{1 - |q|} \sum_{n \geq 1} n^3 |q^n| = 1 - 240|q| \frac{1 + 4|q| + |q|^2}{(1 - |q|)^5}.$$

Verder volgt met lemma 3.3.3 onmiddellijk dat

$$-24 \log \prod_{n \geq 1} |1 - q^n| \geq -24 \frac{|q|}{1 - |q|}.$$

We krijgen nu dus:

$$\begin{aligned} \log^+ |j(\tau)| + \log |q| &= \max\{\log |qj(\tau)|, \log |q|\} \\ &\geq \max\left\{3 \log \left(1 - 240|q| \frac{1 + 4|q| + |q|^2}{(1 - |q|)^5}\right) - 24 \frac{|q|}{1 - |q|}, \log |q|\right\}. \end{aligned}$$

Nu kunnen we numeriek kijken waar het maximum van deze uitdrukking zit, en deze blijkt te zitten bij $|q| = 0,0034153$ en dat geeft een ondergrens van $-5,67948$.

q.e.d.

Lemma 3.3.6 *Stel dat * en ** gelden, dan hebben we de volgende afschattingen:*

1. $|\frac{1}{(2\pi i)^2} \wp(z, \tau) - \frac{u}{(1-u)^2}| < 0,1682$
2. $-0,0506 \leq \log^+ |\frac{1}{(2\pi i)^2} \wp(z, \tau)| + 2 \log |1 - u| \leq 2 \log(1 + |q|^\alpha)$
3. $-0,0665 \leq \lambda(z) + \frac{1}{2} B_2(\alpha) \log |q| + \log |1 - u| \leq 0,071$.

Bewijs. De Weierstrass \wp -functie heeft de volgende ontwikkeling ([Si1], prop. 12.6):

$$\frac{1}{(2\pi i)^2} \wp(z, \tau) = \frac{u}{(1-u)^2} + \frac{1}{12} + \sum_{n \geq 1} \left(\frac{q^n u}{(1 - q^n u)^2} + \frac{q^n u^{-1}}{(1 - q^n u^{-1})^2} + \left(\frac{q^n}{(1 - q^n)^2} \right) \right).$$

Als we nu $t \in \mathbb{C}$ weer nemen z.d.d. $|qt| < 1$ dan krijgen we analoog aan de eerdere afschattingen dat:

$$\left| \sum_{n \geq 1} \frac{q^n t}{(1 - q^n t)^2} \right| \leq \frac{1}{(1 - |qt|)^2} \sum_{n \geq 1} |q^n t| = \frac{|qt|}{1 - |q|(1 - |qt|)^2}. \quad (3.14)$$

Passen we nu 3.14 toe met $t = u, t = u^{-1}, t = 1$ dan krijgen we dat:

$$\begin{aligned} \left| \frac{1}{(2\pi i)^2} \wp(z, \tau) - \frac{u}{(1-u)^2} \right| &\leq \frac{1}{12} + \frac{1}{1 - |q|} \left\{ \frac{|q|^{1+\alpha}}{(1 - |q|^{1+\alpha})^2} \right. \\ &\quad \left. + \frac{|q|^{1-\alpha}}{(1 - |q|^{1-\alpha})^2} + 2 \frac{|q|}{(1 - |q|)^2} \right\}. \end{aligned}$$

Differentiëren we dit nu naar α dan krijgen we dat de term tussen haken als functie van α monotoon stijgend is en dus is deze maximaal bij $\alpha = \frac{1}{2}$ vanwege **. Nemen we dan dus $\alpha = \frac{1}{2}$ en gebruiken we * dan volgt uiteindelijk:

$$\left| \frac{1}{(2\pi i)^2} \wp(z, \tau) - \frac{u}{(1-u)^2} \right| \leq \frac{1}{12} + 0,08482 \dots \leq 0,1682.$$

Dan gaan we nu verder met de tweede afschatting. Als we nu even als $F(z, \tau)$ als volgt kiezen

$$F(z, \tau) = \left| \frac{1}{(2\pi i)^2} \wp(z, \tau) - \frac{u}{(1-u)^2} \right|,$$

dan krijgen we dat

$$\log^+ \left| \frac{1}{(2\pi i)^2} \wp(z, \tau) \right| + 2 \log |1 - u| = \log \max\{|u + (1-u)^2 F|, |1-u|^2\}.$$

De eerste afschatting geeft ons dat $|F| \leq 0,1682$. Hieruit volgt:

$$|u + (1-u)^2 F| \leq |u| + 0,1682(1 + |u|)^2 \leq (1 + |u|)^2.$$

Vanwege de driehoeksongelijkheid hebben we ook dat $|1-u|^2 \leq (1+|u|)^2$ en dus volgt de bovengrens als we gebruiken dat $|u| = |q|^\alpha$. Nu dus de ondergrens in deze afchatting. We hebben dit keer:

$$\begin{aligned} |u + (1-u)^2 F| &\geq 1 - |1-u| - F|1-u|^2 \\ &\geq 1 - |1-u| - 0,1682|1-u|^2. \end{aligned}$$

Hieruit volgt onmiddellijk:

$$\begin{aligned} \max\{|u + (1-u)^2 F|, |1-u|^2\} &\geq \max\{1 - |1-u| - 0,1682|1-u|^2, |1-u|^2\} \\ &\geq 0,34976. \end{aligned}$$

In de laatste stap is gebruikt dat deze twee parabolen elkaar snijden op $|1-u| = 0,5914\dots$ en we zien dat op dit punt het minimum van $\max\{1 - |1-u| - 0,1682|1-u|^2, |1-u|^2\}$ wordt aangenomen met een waarde van $0,34976$. Nemen we dan wat logaritmes, dan volgt de ongelijkheid onmiddellijk. Nu nog de laatste afchatting. De lokale hoogte $\lambda(z)$ wordt gegeven door ([Si2] formule 25):

$$\lambda(z) = -\frac{1}{2}B_2(\alpha) \log|q| - \log|1-u| - \sum_{n \geq 1} \log|(1-q^n u)(1-q^n u^{-1})|.$$

Splitsen we m.b.v. de gebruikelijke regels voor het optellen van logaritmen de som in de definitie op in twee sommen en passen we op ieder van die sommen lemma 3.3.3 (een keer met $t = u$ en een keer met $t = u^{-1}$) toe, dan volgt:

$$\begin{aligned} -\frac{1}{1-|q|} \left\{ \frac{|q|^{1+\alpha}}{1-|q|^{1+\alpha}} + \frac{|q|^{1-\alpha}}{1-|q|^{1-\alpha}} \right\} &\leq \sum_{n \geq 1} \log|(1-q^n u)(1-q^n u^{-1})| \leq \\ &\frac{1}{1-|q|} \{|q|^{1+\alpha} + |q|^{1-\alpha}\}. \end{aligned}$$

We vinden weer dat beide zijden een extremum hebben op $\alpha = \frac{1}{2}$ en dus volgt de gewenste afchatting.

q.e.d.

We gaan nu verder met nog wat meer afchattingen.

Lemma 3.3.7 *Er geldt:*

$$-0,973 - \frac{1}{8} \log^+ |j(\tau)| \leq \lambda(z) - \frac{1}{2} \log^+ \left| \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} \right| \leq 1,07 + \frac{1}{12} \log^+ |j(\tau)|.$$

Bewijs. Vanwege $SL_2(\mathbb{Z})$ -invariantie van $j(\tau)$ en $\frac{\wp(z, \tau)^6}{\Delta(\tau)}$ kunnen we * aannemen. We kunnen namelijk altijd een lineaire transformatie loslaten op τ . Verder mogen we z modulo $\mathbb{Z} + \tau\mathbb{Z}$ kiezen, zo dat:

$$-\frac{1}{2} \leq \alpha(z) = \frac{\text{Im}(z)}{\text{Im}(\tau)} \leq \frac{1}{2}.$$

Omdat λ en \wp even functies zijn kunnen we nu dus ook ** altijd aannemen.

Beschouw nu:

$$a = \left| \frac{1}{(2\pi i)^{12}} \wp(z, \tau)^6 \right|, \quad b = \left| \frac{1}{(2\pi)^{12}} \Delta(\tau) \right|.$$

We zien dat uit lemma 3.3.5 (tweede afchatting) en * volgt dat

$$\log b \leq \log|q| + 0,1045 \leq -\pi\sqrt{3} + 0,1045 < 0.$$

We hebben dus dat $|b| < 1$. Gebruiken we nu lemma 3.3.1 met a, b als boven, dan krijgen we:

$$0 \leq \log^+ \frac{a}{b} - \log^+ a \leq -\log b.$$

Als we deze ongelijkheid met $-\frac{1}{12}$ vermenigvuldigen, we tellen er de derde ongelijkheid van lemma 3.3.6 bij op en we halen er de helft van de tweede ongelijkheid van 3.3.6 er van af dan houden we na wat wegstrepen de volgende termen over:

$$\begin{aligned} & -0,0665 - \log(1 + |q|^\alpha) + \frac{1}{12} \log \left| \frac{1}{(2\pi)^{12}} \Delta \right| \\ & \leq \lambda(z) - \frac{1}{12} \log^+ \left| \frac{\wp(z, \tau)^6}{\Delta} \right| + \frac{1}{2} B_2 \log |q| \leq 0,5964. \end{aligned}$$

Als we nu in het laatste gedeelte van de eerste term een $\frac{\Delta}{|q|}$ er in forceren door $\log |q| - \log |q|$ bij deze term op te tellen, dan kunnen we nu 3.3.5 gebruiken om $\frac{1}{12} \log \left| \frac{\Delta}{q(2\pi)^{12}} \right|$ te vervangen door 0,105. Als we nu dan de term met $B_2(\alpha) = \alpha^2 - \alpha + \frac{1}{6}$ van de afchatting af trekken, dan krijgen we tenslotte:

$$\begin{aligned} & -0,1715 + \frac{\alpha(1-\alpha)}{2} \log |q| - \log(1 + |q|^\alpha) \leq \\ & \lambda(z) - \frac{1}{12} \log^+ \left| \frac{\wp(z, \tau)^6}{\Delta(\tau)} \right| \leq 0,5964 - \frac{1}{2} B_2(\alpha) \log |q|. \end{aligned} \quad (3.15)$$

Als we nu de bovengrens bekijken en we gebruiken dat $B_2(\alpha) \leq \frac{1}{6}$, wat geldig is voor $1 \leq \alpha \leq 1$ en lemma 3.3.5, dan volgt:

$$\begin{aligned} 0,5964 - \frac{1}{2} B_2(\alpha) \log |q| & \leq 0,5964 - \frac{1}{12} \log |q| \\ & \leq 1,0697 + \frac{1}{12} \log^+ |j(\tau)|. \end{aligned}$$

Merk op dat deze afchatting goed gaat omdat * geldt ($\log |q| < 0$). De bovengrens uit het lemma krijgen we nu door dit in te vullen in 3.15. Nu moet de ondergrens nog bewezen worden. Voor de ondergrens gebruiken we nu * en lemma 3.3.5. We krijgen namelijk als we ze gebruiken:

$$\begin{aligned} \frac{\alpha(1-\alpha)}{2} \log |q| & \geq -2,28898\alpha(1-\alpha) - \frac{1}{8} \log^+ |j(\tau)|, \\ -\log(1 + |q|^\alpha) & \geq -\log(1 + e^{-\pi\sqrt{3}\alpha}). \end{aligned}$$

Stoppen we nu deze afchattingen in de ondergrens van 3.15 dan krijgen we als ondergrens:

$$-0,1715 - \frac{1}{8} \log^+ |j(\tau)| - 2,8898\alpha(1-\alpha) - \log(1 + e^{-\pi\sqrt{3}\alpha}).$$

Er geldt nu dat

$$-2,8898\alpha(1-\alpha) - \log(1 + e^{-\pi\sqrt{3}\alpha}) \geq -0,8010883.$$

Als we dit nu substitueren, dan verkrijgen we de gevraagde ondergrens.

q.e.d.

Stelling 3.3.8 *Zij E/\mathbb{C} een elliptische kromme gegeven door de vergelijking:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Neem nu Δ de discriminant van E , j zijn j -invariant. Beschouw verder $b_2 = a_1^2 + 4a_2$ en $2^* = 2$ als $b_2 \neq 0$ en $2^* = 1$ anders. Voor alle $P \in E(\mathbb{C})$ geldt dan:

$$\begin{aligned} & -\frac{1}{12} \log^+ |\Delta| - \frac{1}{8} \log^+ |j| - \frac{1}{2} \log^+ \left| \frac{b_2}{12} \right| - \frac{1}{2} \log 2^* + 1, 07 \\ \leq & \lambda(P) - \frac{1}{2} \log^+ |x(P)| \\ \leq & \frac{1}{12} \log^+ |\Delta^{-1}| + \frac{1}{12} \log^+ |j| + \frac{1}{2} \log^+ \left| \frac{b_2}{12} \right| + \frac{1}{2} \log 2^* + 1, 07. \end{aligned}$$

Bewijs. Kies een τ met $j(\tau) = j(E)$ (dat zo'n τ bestaat is het zelfde probleem als in het bewijs van stelling 2.1.2). En bekijk de kromme E' die wordt gegeven door:

$$E' : Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau).$$

We hebben nu dus een isomorfisme (zie paragraaf 2.1):

$$\frac{\mathbb{C}}{\mathbb{Z}\tau + \mathbb{Z}} \xrightarrow{\sim} E'(\mathbb{C}), \quad z \mapsto (\wp(z, \tau), \wp'(z, \tau)).$$

Kies nu een $c \in \mathbb{C}^*$ en $r, s, t \in \mathbb{C}$ zodanig dat de afbeelding:

$$x = c^2 X + r, \quad y = \frac{1}{2} c^3 Y + s c^2 X + t$$

een isomorfisme geeft tussen $E'(\mathbb{C})$ en $E(\mathbb{C})$. Zij nu $z \in \frac{\mathbb{C}}{\mathbb{Z}\tau + \mathbb{Z}}$ het punt dat correspondeert met het punt $P \in E(\mathbb{C})$, dan geldt:

$$\lambda(P) - \frac{1}{2} \log^+ |x(P)| = \lambda(z) - \frac{1}{2} \log^+ |c^2 \wp(z, \tau) + r|.$$

Gebruiken we nu de coördinatentransformatie uit [Si1] (hoofdstuk 3 paragraaf 1), dan volgt:

$$\lambda(P) - \frac{1}{2} \log^+ |x(P)| = \lambda(z) - \frac{1}{2} \log^+ \left| \Delta^{\frac{1}{6}} \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} - \frac{b_2}{12} \right|. \quad (3.16)$$

Verder geldt dat:

$$\begin{aligned} & \frac{\max \left\{ \left| \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} \right|, 1 \right\}}{\max \{ |\Delta^{-\frac{1}{6}}|, 1 \} \cdot 2^* \cdot \max \left\{ \left| \frac{b_2}{12} \right|, 1 \right\}} \leq \max \left\{ \left| \Delta^{\frac{1}{6}} \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} - \frac{b_2}{12} \right|, 1 \right\} \leq \\ & \max \{ |\Delta^{-\frac{1}{6}}|, 1 \} \cdot 2^* \cdot \max \left\{ \left| \frac{b_2}{12} \right|, 1 \right\} \cdot \max \left\{ \left| \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} \right|, 1 \right\}. \end{aligned}$$

Als we nu logaritmes nemen en we vullen het resultaat in in 3.16, dan krijgen we:

$$\begin{aligned} & -\frac{1}{12} \log^+ |\Delta| - \frac{1}{2} \log 2^* - \frac{1}{2} \log^+ \left| \frac{b_2}{12} \right| \\ \leq & \left\{ \lambda(P) - \frac{1}{2} \log^+ |x(P)| \right\} - \left\{ \lambda(z) - \frac{1}{2} \log^+ \left| \frac{\wp(z, \tau)}{\Delta(\tau)^{\frac{1}{6}}} \right| \right\} \\ \leq & \frac{1}{12} \log^+ |\Delta^{-1}| + \frac{1}{2} \log 2^* + \frac{1}{2} \log^+ \left| \frac{b_2}{12} \right|. \end{aligned}$$

Als we hier dan lemma 3.3.7 op toepassen, verkrijgen we het gestelde resultaat.

q.e.d.

Nu komt de uiteindelijke stelling die in de later zal worden gebruikt.

Stelling 3.3.9 *Zij E een elliptische kromme over \mathbb{Q} , beschreven door de Weierstrass-vergelijking:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

met de $a_i \in \mathbb{Z}$. Neem nu Δ, j, b_2 en 2^ als boven. Definieer nu een soort van hoogte E als volgt:*

$$\mu(E) = \frac{1}{12}h(\Delta) + \frac{1}{12}h_\infty(j) + \frac{1}{2}h_\infty\left(\frac{b_2}{12}\right) + \frac{1}{2}\log^+ 2^*$$

(hierin geldt $h_\infty(a) := \log^+ |a|$). Dan hebben we voor alle punten $P \in E(\mathbb{Q})$ de volgende relatie:

$$-\frac{1}{24}h(j) - \mu(E) - 0,973 \leq \hat{h}(P) - \frac{1}{2}h(x(P)) \leq \mu(E) + 1,07.$$

Bewijs. In de ondergrens van stelling 3.3.8 gebruiken we $\frac{1}{8}\log^+ |j| = \frac{1}{24}\log^+ |j| + \frac{1}{12}\log^+ |j|$. Sommeren we nu stelling 3.3.7 en stelling 3.3.4 en gebruiken we formule 3.13, dan krijgen we:

$$-\frac{1}{24}h(j) - \mu(E) - 0,973 \leq \hat{h}(P) - \frac{1}{2}h(x(P)) \leq \mu(E) + 1,07.$$

Hierin is in de bovengrens gebruikt dat $h(\Delta) = h(\Delta^{-1})$. Verder is in de ondergrens gebruikt dat $h_\infty(\Delta) = h(\Delta)$.

q.e.d.

Hoofdstuk 4

Ongelijkheden

In dit hoofdstuk zullen alle ongelijkheden worden behandeld die nodig zijn voor de bovengrens voor de gehele punten op een elliptische kromme.

4.1 Elementaire ongelijkheden

In deze paragraaf zullen alle ongelijkheden behandeld worden die nodig zijn voor de uiteindelijke bovengrens.

We bekijken eerst de zogenaamde Néron-Tate paring, gedefinieerd als in stelling 3.2.3:

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Gebruiken we nu de eigenschappen van de canonieke hoogte uit stelling 3.2.3 en schrijven we P als in formule (1.4) dan volgt:

$$\begin{aligned} 2\hat{h}(P) &= \langle P, P \rangle \\ &= \langle T + \sum_{i=1}^r m_i P_i, T + \sum_{i=1}^r m_i P_i \rangle \\ &= \langle \sum_{i=1}^r m_i P_i, \sum_{i=1}^r m_i P_i \rangle \\ &= \sum_{1 \leq i, j \leq r} m_i m_j \langle P_i, P_j \rangle. \end{aligned} \tag{4.1}$$

Het heeft nu dus zin om de volgende matrix te definiëren:

$$\mathcal{H}_{ij} = \frac{1}{2} \langle P_i, P_j \rangle.$$

Ongelijkheid 4.1.1 *We hebben voor een punt $P = \sum_{i=1}^r m_i P_i + T \in E(\mathbb{Q})$ de volgende afchatting:*

$$\hat{h}(P) \geq c_1 \max_{1 \leq i \leq r} \{m_i^2\}$$

met c_1 de kleinste eigenwaarde van de matrix \mathcal{H} .

Bewijs. Vanwege 4.1 hebben we dat

$$\hat{h}(P) = \vec{m}^T \mathcal{H} \vec{m}$$

met \vec{m} de kolomvector met componenten m_i . Er geldt nu dat \mathcal{H} een symmetrische matrix is en dus is deze diagonaliseerbaar. Er bestaan dus matrices C, D z.d.d.

$$\mathcal{H} = C^T D C$$

met C orthogonaal en D op diagonaalvorm. Nemen we nu c_1 de kleinste eigenwaarde van \mathcal{H} dan volgt:

$$\begin{aligned}\hat{h}(P) &= \vec{m}^T C^T D C \vec{m} \\ &= \sum_{i=1}^r \lambda_i (C \vec{m})_i^2 \\ &\geq c_1 \vec{m}^T C^T C \vec{m} \\ &= c_1 \vec{m}^T \vec{m} \\ &\geq c_1 \max_{1 \leq i \leq r} \{m_i^2\}.\end{aligned}$$

q.e.d.

Ongelijkheid 4.1.2 *Zij $\gamma, \gamma', \gamma''$ de wortels van $f(x)$ en neem $c_2 = 2 \max\{|\gamma|, |\gamma'|, |\gamma''|\}$. Dan hebben we voor alle $x \geq c_2$ de volgende afchatting:*

$$\left| \int_x^\infty \frac{dt}{\sqrt{f(t)}} \right| \leq 4\sqrt{2}(x^{-\frac{1}{2}}).$$

Bewijs. Voor $t \geq x \geq c_2$ hebben we dat $0 < f(t) = t^3 + at + b = |t - \gamma||t - \gamma'| |t - \gamma''|$. Verder krijgen we via de omgekeerde driehoeksongelijkheid en m.b.v. de definitie van c_2 dat $|t - \gamma| \geq t - |\gamma| \geq \frac{t}{2}$ (idem voor γ' en γ''). We krijgen nu dus voor een $N > x$ dat

$$\int_x^N \frac{dt}{\sqrt{f(t)}} \leq \int_x^N 2^{\frac{3}{2}} t^{-\frac{3}{2}} dt = 4\sqrt{2}(x^{-\frac{1}{2}} - N^{-\frac{1}{2}})$$

Nemen we nu de limiet voor N gaat naar oneindig dan volgt de ongelijkheid.

q.e.d.

Ongelijkheid 4.1.3 *Zij u, v, γ als eerder. Zij X_0 een geheel getal groter dan v . Neem:*

$$\begin{aligned}c_0 &= \begin{cases} \log |u|, & \text{als } v \leq 0 \\ \log |u| + \frac{1}{2}v(X_0 - v)^{-1}, & \text{als } v > 0 \end{cases} \\ c_3 &= c_0 + \frac{1}{12} \log |\Delta| + \frac{1}{12} \log^+ |j| + \frac{1}{2} \log^+ \left| \frac{b_2}{12} \right| + \frac{1}{2} \log 2^* + 1, 07.\end{aligned}$$

Hierin is alles als in paragraaf 3.3. Dan hebben we voor alle gehele punten $P \in E(\mathbb{Q})$ met $X(P) \geq X_0$ dat $x(P) > 0$ en

$$\hat{h}(P) - \frac{1}{2} \log x(P) \leq c_3.$$

Bewijs. We hebben dat $x(P) = u^{-2}(X(P) - v) > 0$. Verder volgt onmiddellijk uit stelling 3.3.9 dat

$$\hat{h}(P) - \frac{1}{2} h(X(P)) \leq c_3 - c_0. \quad (4.2)$$

Aangezien $X(P)$ een geheel punt is, volgt er dat $h(X(P)) = \log X(P)$. We krijgen nu dus:

$$h(X(P)) = \log(u^2 x(P) + v) = 2 \log |u| + \log x(P) + \log \left(1 + \frac{v}{u^2 x(P)} \right). \quad (4.3)$$

Als $v \leq 0$ dan is de laatste logaritme negatief en klopt de afchatting. Als v positief is, dan hebben we de volgende afchatting:

$$\log \left(1 + \frac{v}{u^2 x(P)} \right) < \frac{v}{u^2 x(P)} = \frac{v}{X(P) - v} \leq \frac{v}{X_0 - v}.$$

Als we dit nu combineren met 4.2 en 4.3 (we werken met een kromme met gehele coëfficiënten), dan volgt de gestelde ongelijkheid.

q.e.d.

Voor de uiteindelijke afchatting hebben we een boven-en ondergrens nodig. De ongelijkheden die hier boven zijn afgeleid, zijn nodig voor de bovengrens. Voor de ondergrens hebben we de stelling van David nodig. Het is een speciaal geval van de stelling uit [Da] Théorème 2.1. Eerst zullen we wat notatie in moeten voeren. Zoals we in paragraaf 1.1 hebben gezien kan men aan een elliptische kromme een rooster toekennen. Beschouw nu de kromme

$$y^2 = x^3 + ax + b = f(x).$$

Zij nu $u_0, \dots, u_r \in \mathbb{C}$ zo danig dat voor alle i , $R_i = (4\wp(u_i), 4\wp'(u_i)) \in E(\mathbb{Q}) \cup O$. Kies nu ω_1 en ω_2 zo dat ze het bijbehorende rooster voortbrengen en aan 2.11 voldoen. Als we nu als de lineaire vorm nemen $L = \frac{b_0}{t}u_0 + b_1u_1 + \dots + b_ru_r$, dan krijgen we de volgende afchatting:

Stelling 4.1.4 (David) *Als $L \neq 0$ dan hebben we de volgende ondergrens voor $|L|$:*

$$|L| \geq e^{-c_4(\log B + \log K)(\log \log B + \log K + h_E)^{r+2}}.$$

In deze formule worden de constantes gegeven door:

1. $c_4 = 2 \cdot 10^{7r+15} \left(\frac{2}{e}\right)^{2(r+1)^2} (r+2)^{4r^2+18r+14} (\log K)^{-2r-3} \prod_{i=0}^r A_i$
2. $h_E = \max\{1, h(\frac{a}{4}, \frac{b}{16}), h(j_E)\}$
3. B is een geheel getal met $B \geq \max\{A_0, \dots, A_r, t, |b_0|, \dots, |b_r|, 16\}$
4. $A_i, i = 0, \dots, r$ zijn getallen die voldoen aan

$$A_i \geq \max\left\{\hat{h}(R_i), h_E, \frac{3\pi u_i^2}{|\omega_1|^2 \text{Im}(\tau)}\right\}$$

5. K is een getal dat voldoet aan:

$$e \leq K \leq \min_{0 \leq i \leq r} \left\{ \frac{e|\omega_1| \sqrt{A_i \text{Im}(\tau)}}{|u_i| \sqrt{3\pi}} \right\}.$$

4.2 De uiteindelijke ongelijkheid

We gaan nu een bovengrens voor $M = \max_{1 \leq i \leq r} \{|m_i|\}$ afleiden. We gebruiken hierbij het isomorfisme φ uit paragraaf 2.2. Aangezien φ een isomorfisme is, geldt de volgende relatie:

$$\varphi(P) \equiv m_1\varphi(P_1) + \dots + m_r\varphi(P_r) + \varphi(T) \pmod{1}.$$

Er bestaat dus een geheel getal m_0 zodat

$$\varphi(P) = m_0 + m_1\varphi(P_1) + \dots + m_r\varphi(P_r) + \varphi(T).$$

Als we nu aannemen dat $\varphi(P) \in [0, 1[$ dan volgt dus

$$m_0 < |m_1| + \dots + |m_r| + 1 \leq rM + 1. \quad (4.4)$$

Merk nu wel op dat de voortbrengers niet in $E_0(\mathbb{R})$ hoeven te zitten. Als er zulke voortbrengers P_s, \dots, P_t zijn, neem dan als nieuwe voortbrengers $P_s + R, \dots, P_t + R$ met $R = (0, \gamma)$ en pas T dan aan.

Als T nu een torsiepoint van orde t is dan volgt dat $\varphi(T)$ van de vorm $\frac{s}{t}$ met $s \leq t$ (want $\varphi(P) \in [0, 1[$) is. We hebben dus:

$$\varphi(P) = \left(m_0 + \frac{s}{t}\right) + m_1\varphi(P_1) + \dots + m_r\varphi(P_r).$$

We willen nu de ongelijkheden uit de vorige sectie gaan toepassen. Om dit te doen zullen we alleen naar punten kijken met $X(P) \geq X_0$ met $X_0 = \lfloor \max\{c_2, v, u^2\gamma + v\} \rfloor$. Ongelijkheden 4.1.1 en 4.1.3 geven dat

$$\log x(P) \geq 2(\hat{h}(P) - c_3) \geq 2(c_1M^2 - c_3).$$

We hebben dus dat $|x(P)|^{-\frac{1}{2}} = (x(P))^{-\frac{1}{2}} \leq e^{(c_3 - c_1M^2)}$ We hebben nu dus vanwege 4.1.2 dat:

$$\begin{aligned} |\varphi(P)| &= \frac{1}{\omega} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{f(t)}} \\ &\leq \frac{4\sqrt{2}}{\omega} |x(P)|^{-\frac{1}{2}} \\ &\leq \frac{4\sqrt{2}}{\omega} e^{(c_3 - c_1M^2)}. \end{aligned} \tag{4.5}$$

Definiëren we nu:

$$L(P) := \omega\varphi(P),$$

dan zien we dat 4.5 een bovengrens geeft voor $L(P)$. We kunnen nu de stelling van David gebruiken om een ondergrens te geven voor $|L(P)|$. We hebben dat $B \geq \max\{A_0, \dots, A_r, t, |b_0|, \dots, |b_r|, 16\} \geq \max\{M, t, m_0t + s\}$ (immers b_i komt overeen met m_i). De ondergrens van David levert in dit geval dan:

$$|L(P)| > e^{-c_4(\log M' + c_5)(\log \log M' + c_6)^{r+2}} \tag{4.6}$$

met $\log M' := \max\{\log M, h(m_0 + \frac{s}{t})\}$, $c_5 = \log K$ en $c_6 = \log K + h_E$. Als we nu t_0 de grootste orde van punten uit de torsiegroep nemen, dan hebben we dat $M \leq t_0(rM + 1) + t_0 - 1$. Vanwege Mazur hebben we dat $t_0 \leq 12$ en dus is t_0 wel begrensd. Verder hebben we dat, als $m_0 \geq 1$:

$$\begin{aligned} h(m_0 + \frac{s}{t}) &= \log \max\{|tm_0 + s|, t\} \\ &= \log(|tm_0 + s|) \\ &\leq \log(t(rM + 1) + s) \\ &\leq \log(t(rM + 1) + t - 1) \\ &\leq \log(t_0(rM + 1) + t_0 - 1). \end{aligned}$$

Waarin in stap 2 gebruikt is dat als $m_0 \geq 2$, dan $|tm_0 + s| \geq t|m_0| - s \geq t$ omdat $t - 1 \geq s$. Verder is in stap 3 formule 3.4 gebruikt. Als $m_0 = 0$, dan geldt de uiteindelijke afchatting ogenblikkelijk. We kunnen nu dus $\log M'$ op de volgende manier afschatten:

$$\log M' \leq \log(t_0(rM + 1) + t_0 - 1)$$

Vullen we dit nu in ongelijkheid 4.6 in en combineren we dit met 4.5 dan volgt de volgende ongelijkheid voor M :

$$M^2 < c_3c_1^{-1} + c_1^{-1} \log(4\sqrt{2}) + c_4c_1^{-1}(\log(t_0(rM + 1) + t_0 - 1) + c_5)(\log \log(t_0(rM + 1) + t_0 - 1) + c_6)^{r+2}. \tag{4.7}$$

Aangezien alle constantes bekend zijn, geeft dit dus een expliciete bovengrens voor M en dus kunnen we hiermee alle gehele punten op de elliptische kromme vinden.

Hoofdstuk 5

Het Lenstra, Lenstra, Lovász-algoritme

We hebben nu een bovengrens verkregen voor M , maar deze kan nog erg groot zijn. In dit hoofdstuk zal een manier besproken worden om die bovengrens te verlagen. Dit gebeurt m.b.v. het LLL-algoritme (Lenstra, Lenstra, Lovász). Zij gebruikten het algoritme oorspronkelijk bij het factoriseren van polynomen (zie [LLL]), maar het blijkt ook bij dit onderwerp erg nuttig te zijn.

5.1 Gereduceerde bases

Het LLL-algoritme maakt van een basis van een rooster een zogenaamde gereduceerde basis. In dit hoofdstuk zal uitgelegd worden wat een gereduceerde basis is en er zal een afschatting worden behandeld die nodig is bij het reduceren van de bovengrens.

Zij nu n een positief geheel getal. Een deelverzameling van \mathbb{R}^n noemen we een rooster als er een basis $\{b_i\}$ is met $b_i \in \mathbb{R}^n$ zodat:

$$L = \left\{ \sum_{i=1}^n r_i b_i : r_i \in \mathbb{Z} \right\}.$$

We noemen n nu de rang van L .

Zij nu b_1, \dots, b_n lineair onafhankelijke vectoren in \mathbb{R}^n . We kunnen hier nu een orthogonale basis uit verkrijgen door het Gram-Schmidt-procédé toe te passen. De orthogonale basis $\{b_1^*, \dots, b_n^*\}$ die dan verkregen wordt, is met inductie gedefinieerd als:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \tag{5.1}$$

$$\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \tag{5.2}$$

met \langle, \rangle het standaard inproduct op \mathbb{R}^n .

We noemen nu een basis $\{b_1, \dots, b_n\}$ gereduceerd als we hebben dat:

$$|\mu_{ij}| \leq \frac{1}{2}, \quad 1 \leq j < i \leq n \tag{5.3}$$

$$|b_i^* + \mu_{ii-1} b_{i-1}^*| \geq \frac{3}{4} |b_{i-1}^*|^2, \quad 1 < i \leq n. \tag{5.4}$$

Nu een lemma over een gereduceerde basis:

Lemma 5.1.1 *Zij $\{b_1, \dots, b_n\}$ een gereduceerde basis voor een rooster L in \mathbb{R}^n en neem b_1^*, \dots, b_n^* de bijbehorende orthonormale basis (als in 5.1), dan hebben we*

$$|b_j|^2 \leq 2^{i-1} |b_i^*|^2, \quad 1 \leq j \leq i \leq n. \quad (5.5)$$

Bewijs. Met de driehoeksongelijkheid en formules 5.3 en 5.4 volgt er

$$\begin{aligned} |b_i^*|^2 &\geq \left(\frac{3}{4} - \mu_{ii-1}^2\right) |b_{i-1}^*|^2 \\ &\geq \frac{1}{2} |b_{i-1}^*|^2. \end{aligned}$$

Als we dit nu herhalen tot aan een $j \leq i$ dan krijgen we

$$|b_j|^2 \leq 2^{i-j} |b_i^*|^2, \quad 1 \leq j \leq i \leq n.$$

Ook volgt m.b.v. 5.1 en 5.2 en de orthogonaliteit van de b_i^* dat

$$\begin{aligned} |b_i|^2 &= |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 \\ &\leq |b_i^*|^2 + \sum_{j=1}^{i-1} \frac{1}{4} 2^{i-j} |b_j^*|^2 \\ &= \left(1 + \frac{1}{4}(2^i - 2)\right) |b_i^*|^2 \\ &\leq 2^{i-1} |b_i^*|^2. \end{aligned}$$

We hebben nu dus dat

$$|b_j|^2 \leq 2^{j-1} |b_j^*|^2 \leq 2^{i-1} |b_i^*|^2.$$

q.e.d.

Nu komt de afchatting die gebruikt zal worden bij het terugbrengen van de bovengrens:

Ongelijkheid 5.1.2 *Zij $L \subset \mathbb{R}^n$ een rooster met een gereduceerde basis $\{b_1, \dots, b_n\}$. Dan geldt voor alle $x \in L, x \neq 0$:*

$$|b_1|^2 \leq 2^{n-1} |x|^2.$$

Bewijs. We hebben $x = \sum_{i=1}^n r_i b_i = \sum_{i=1}^n r_i^* b_i^*$ met $r_i \in \mathbb{Z}, r_i^* \in \mathbb{R}$. Als i de grootste index is met $r_i \neq 0$, dan $r_i = r_i^*$. We hebben dus:

$$|x|^2 \geq r_i^* |b_i^*|^2 \geq |b_i^*|^2.$$

Uit voorgaand lemma halen we voorts dat $|b_1|^2 \leq 2^{i-1} |b_i^*|^2 \leq 2^{n-1} |b_i^*|^2$ wat het lemma dus bewijst.

q.e.d.

5.2 Het algoritme

Deze paragraaf gaat over hoe we een basis kunnen reduceren. Dit gebeurt dus met het LLL-algoritme. Het werkt als volgt. Het algoritme begint met het uitvoeren van het Gram-Schmidt-proces. We zullen een teller k introduceren. We beginnen met $k = 2$. We zullen nu een aantal iteraties uitvoeren waarbij we altijd in de volgende situatie zitten:

$$|\mu_{ij}| \leq \frac{1}{2}, \quad 1 \leq j < i < k \quad (5.6)$$

$$|b_i^* + \mu_{ii-1} b_{i-1}^*|^2 \geq \frac{3}{4} |b_{i-1}^*|^2, \quad 1 < i < k. \quad (5.7)$$

Aan bovenstaande situatie is voldaan als $k = 2$. Als we dus hebben dat $k = n + 1$ is de basis gereduceerd en stopt het algoritme.

Stel nu dat $k \leq n$. We moeten nu voor elkaar krijgen dat

$$|\mu_{kk-1}| \leq \frac{1}{2} \quad (5.8)$$

als $k > 1$. Stel het geldt niet. Beschouw dan het gehele getal r dat het dichtst bij μ_{kk-1} en vervang dan b_k door $b_k - rb_{k-1}$. De getallen μ_{kj} met $j < k - 1$ worden dan vervangen door $\mu_{kj} - r\mu_{k-1j}$ en μ_{kk-1} door $\mu_{kk-1} - r$. Alle andere μ_{ij} en b_i^* blijven ongewijzigd. Nu is wel aan 5.8 voldaan. Nu onderscheiden we twee gevallen:

Geval1. Stel dat $k \geq 2$ en we hebben dat $|b_k^* + \mu_{kk-1}b_{k-1}^*| < \frac{3}{4}|b_{k-1}^*|^2$. In dit geval verwisselen we de b_k en b_{k-1} en laten de rest van de b_i ongewijzigd. Hierna veranderen $b_{k-1}^*, b_k^*, \mu_{kk-1}, \mu_{k-1j}, \mu_{kkj}, \mu_{ik-1}, \mu_{ik}$ voor $j < k - 1$ en $i > k$. Deze worden verkregen door op de nieuwe basis het Gram-Schmidt-procédé weer toe te passen. Vervolgens vervangen we k door $k - 1$. We zitten nu dus weer in de situatie van 5.6 en 5.7 en we gaan weer verder met het algoritme.

Geval2. Stel dat $k = 1$ of we hebben dat $|b_k^* + \mu_{kk-1}b_{k-1}^*| \geq \frac{3}{4}|b_{k-1}^*|^2$. In dit geval zorgen we er eerst voor dat

$$|\mu_{kj}| \leq \frac{1}{2} \quad (5.9)$$

met $1 \leq j \leq k - 1$. Stel dit geldt niet. Kies dan l de grootste index met $|\mu_{kl}| > \frac{1}{2}$ en kies r het gehele getal zijn dat het dichtst bij μ_{kl} ligt. Vervang nu weer b_k door $b_k - rb_l$. Hieruit volgt dan dat μ_{kj} ($j < l$) vervangen wordt door $\mu_{kj} - r\mu_{lj}$ en μ_{kl} door $\mu_{kl} - r$ wat natuurlijk aan 5.9 voldoet. Vervolgens herhalen we dit tot 5.9 geldt voor alle $j \leq k - 1$. Tot slot vervangen we k door $k + 1$ en gaan weer verder met het algoritme.

Merk op dat de basis in de stappen weliswaar veranderd wordt, maar het blijft wel een basis.

Schematisch gezien ziet het er dus als volgt uit:

- Begin :
- $b_i^* := b_i$
 - $B_i := \langle b_i^*, b_i^* \rangle$
 - $\mu_{ij} := \frac{\langle b_i^*, b_j^* \rangle}{B_j}, \quad j = 1, \dots, i - 1$
 - $b_i^* := b_i^* - \mu_{ij}b_j^*, \quad j = 1, \dots, i - 1$
 - $k := 2$
- Stap1
- Voer (*) uit voor $l = k - 1$
 - als $B_k < (\frac{3}{4} - \mu_{kk-1}^2)B_{k-1}$ ga naar Stap 2
 - voer (*) uit voor $l = k - 2, k - 3, \dots, 1$
 - als $k = 1$ eindig dan
 - $k := k + 1$
 - ga naar Stap1
- Stap2
- $\mu := \mu_{kk-1}; B := B_k + \mu^2 B_{k-1}; \mu_{kk-1} = \frac{\mu B_{k-1}}{B}$
 - $B_k := \frac{B_{k-1} B_k}{B}; B_{k-1} := B$
 - $\begin{pmatrix} b_{k-1} \\ b_k \end{pmatrix} := \begin{pmatrix} b_k \\ b_{k-1} \end{pmatrix}$
 - $\begin{pmatrix} \mu_{k-1j} \\ \mu_{kj} \end{pmatrix} := \begin{pmatrix} \mu_{kj} \\ \mu_{k-1j} \end{pmatrix}, \quad j = 1, 2, \dots, k - 2$
 - $\begin{pmatrix} \mu_{ik-1} \\ \mu_{ik} \end{pmatrix} := \begin{pmatrix} 1 & \mu_{kk-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{kj} \\ \mu_{k-1j} \end{pmatrix}, \quad i = k + 1, k + 2, \dots, n$
 - als $k > 2$ dan $k := k - 1$

- ga naar Stap1
- * · als $|\mu_{kl}| > \frac{1}{2}$ dan:

$$\begin{cases} r := \text{gehele getal dichtst bij } \mu_{kl}; & b_k := b_k - rb_l \\ \mu_{kj} := \mu_{kj} - r\mu_{lj}, & j = 1, 2, \dots, l-1 \\ \mu_{kl} := \mu_{kl} - r \end{cases}$$

Het kan bewezen worden dat dit een eindig algoritme is (zie [LLL] blz 521). De formules die voorkomen in bovenstaand schema komen in feite van het Gram-Schmidt-proces. Je zou ook iedere keer als basis veranderd is dit proces gewoon uit kunnen voeren.

5.2.1 Voorbeeld

Nu even een voorbeeld om te zien hoe dit algoritme werkt. Bekijk de volgende basis.

$$\begin{aligned} b_1 &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \\ b_2 &= \begin{pmatrix} 3 \\ 4 \end{pmatrix}. \end{aligned}$$

Passen we hier de Gram-Schmidt-procedure op toe, dan krijgen we:

$$\begin{aligned} b_1^* &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \\ b_2^* &= \begin{pmatrix} \frac{4}{5} \\ -\frac{2}{5} \end{pmatrix} \\ \mu_{21} &= \frac{11}{5}. \end{aligned} \tag{5.10}$$

We zien dus onmiddellijk dat deze basis niet gereduceerd is. We beginnen nu bij stap 1 en we hebben $k = 2$. We moeten nu dus (*) volgen ($l = 1$) en krijgen $r = 2$. We krijgen nu dus de basis:

$$\begin{aligned} b_1 &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \\ b_2 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{aligned}$$

Na Gram-Schmidt krijgen we weer 5.10, op μ_{21} na. Deze is nu $\frac{1}{5}$ geworden. Vervolgens zien we dat $B_k (= \frac{4}{5}) < (\frac{3}{4} - \mu_{kk-1}^2)B_{k-1} (= \frac{71}{20})$ en dus moeten we verder naar stap 2. Hierin worden b_1 en b_2 omgedraaid en passen we hier Gram-Schmidt weer op toe, dan volgt er:

$$\begin{aligned} b_1^* &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ b_2^* &= \begin{pmatrix} 0 \\ 2 \end{pmatrix} \\ \mu_{21} &= 1. \end{aligned}$$

We gaan nu weer terug naar stap 1. Nu moeten we (*) dus weer uitvoeren we krijgen dit keer $r = 1$. Als nieuwe basis hebben we nu dus:

$$\begin{aligned} b_1 &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ b_2 &= \begin{pmatrix} 0 \\ 2 \end{pmatrix}. \end{aligned} \tag{5.11}$$

Deze vectoren zijn orthogonaal en dus blijven ze na Gram-Schmidt onveranderd. We gaan weer terug naar Stap 1. We hoeven dit keer niet naar stap 2 en dus is het algoritme klaar. We hebben 5.11 dus als gereduceerde basis.

5.3 Toepassing

In deze paragraaf zal besproken worden hoe de bovengrens die we in hoofdstuk 4 hebben afgeleid terug kan worden gebracht.

We kunnen nu de afschattingen die we hebben verkregen in sectie 4.2 verkort schrijven als:

$$|\varphi(P)| < K_1 e^{-K_2 M^2}, \quad M < K_3. \quad (5.12)$$

In het algemeen zal K_3 erg groot zijn. Beschouwen we dan nu het rooster voortgebracht door de kolommen van de volgende matrix:

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ [K_0\varphi(P_1)] & [K_0\varphi(P_2)] & \dots & [K_0\varphi(P_r)] & [K_0] \end{pmatrix}.$$

Hierin is K_0 een geheel getal groter dan K_3^{r+1} en staat $[a]$ voor a afgerond richting 0. Kies nu $(m_1, \dots, m_r, m_0) \in \mathbb{Z}^{r+1}$ met $|m_i| < K_3$ en beschouw het roosterpunt:

$$l = A \begin{pmatrix} tm_1 \\ \vdots \\ tm_r \\ tm_0 + s \end{pmatrix} = \begin{pmatrix} tm_1 \\ \vdots \\ tm_r \\ \lambda \end{pmatrix}.$$

met $\lambda := tm_1[K_0\varphi(P_1)] + \dots + tm_r[K_0\varphi(P_r)] + (tm_0 + s)K_0$. Omdat we hebben dat $|\lambda - K_0 t \varphi(P)| \leq rtM \leq rtK_3$ volgt dus dat:

$$|l|^2 = t^2(m_1^2 + \dots + m_r^2) + \lambda^2 \leq rt^2K_3^2 + t^2(K_0|\varphi(P)| + rK_3)^2 \quad (5.13)$$

Als we nu de basis van het rooster via het LLL-algoritme reduceren, dan krijgen een nieuwe basis $\{b_1, \dots, b_{r+1}\}$ en via ongelijkheid 5.1.2 krijgen we ook:

$$|b_1|^2 \leq 2^r |l|^2.$$

Combineren we dit nu met 5.13, dan krijgen we

$$K_0|\varphi(P)| \geq \sqrt{t^{-2}2^{-r}|b_1|^2 - rK_3^2} - rK_3$$

Gebruiken we dan de eerste ongelijkheid van formule 5.12, dan komen we tot de volgende nieuwe bovengrens voor M :

$$M^2 \leq K_2^{-1}(\log(K_0K_1) - \log(\sqrt{t^{-2}2^{-r}|b_1|^2 - rK_3^2} - rK_3)) \quad (5.14)$$

Dit geldt natuurlijk mits:

$$|b_1| > 2^{\frac{r}{2}} t K_3 \sqrt{r^2 + r} \quad (5.15)$$

We moeten dus K_0 zo kiezen dat aan 5.15 is voldaan om de nieuwe afschatting in 5.14 te krijgen. In de praktijk komt het er dan meestal op neer dat je K_0 groter moet kiezen dan $(2^{\frac{r}{2}} t K_3 \sqrt{r^2 + r})^{r+1}$. De nieuwe afschatting geeft een bovengrens in de orde van grootte $\log K_3$ en dat is dus een forse reductie van de eerder verkregen bovengrens.

Hoofdstuk 6

Voorbeeld

In dit hoofdstuk zal de theorie die is behandeld worden toegepast op een voorbeeld.

Als we bijvoorbeeld kijken wanneer de eerste b gehele getallen en de eerste a kwadraten opgeteld hetzelfde opleveren, dan levert dat de volgende vergelijking op:

$$E : \frac{1}{2}b^2 + \frac{1}{2}b = \frac{1}{3}a^3 + \frac{1}{2}a^2 + \frac{1}{6}a.$$

Ik ga in dit hoofdstuk alle gehele punten van deze vergelijking vinden. Eerst moet even gekeken worden of de kromme wel een elliptische kromme is. Deze vergelijking beschrijft in ieder geval een kubiek. De kromme met gehele coëfficiënten die met deze kromme correspondeert wordt gegeven door (neem $6a = w$, $18b = z$):

$$E' : z^2 + 18z = w^3 + 9w^2 + 18w.$$

We brengen nu de kromme in Weierstrass-normaalvorm door de volgende transformaties uit te voeren:

$$a = \frac{1}{6}x - \frac{1}{2}, \quad b = \frac{1}{18}y - \frac{1}{2}. \quad (6.1)$$

De kromme die ons dit oplevert is:

$$E'' : y^2 = x^3 - 9x + 81.$$

In de notatie van de inleiding levert ons dit dat $u = 1$, $v = -3$, $z = -6$. We zien aan deze vergelijking dat de kromme niet singulier is en we hebben ook een rationaal punt, namelijk bijvoorbeeld $(0, \pm 9)$. Deze kromme is dus een elliptische kromme.

Er geldt nu:

$$(a, b) \in E(\mathbb{Z}) \Leftrightarrow (6a, 18b) \in E'(\mathbb{Z})$$

We moeten dus alle gehele punten zoeken van E' en hier alle punten van de vorm $(6a, 18b)$ uit halen.

Met behulp van MWRank en Pari rekenen we nu de torsiegroep en rang uit. De Torsiegroep blijkt triviaal en de rang blijkt 2 te zijn. De voortbrengers van de groep van rationale punten zijn $(9, 27)$ en $(-\frac{15}{4}, \frac{63}{8})$. De rang en de voortbrengers werden door MWRank onconditioneel gegeven. We hebben dus $t_0 = 1$, $s = 0$. Verder is de discriminant van deze kromme $\Delta = 174231$.

De kromme die we gekregen hebben heeft maar 1 reële wortel, namelijk $x = -3^{\frac{2}{3}} \left(\frac{2}{27 - \sqrt{717}} \right)^{\frac{1}{3}} - \left(\frac{3}{2}(27 - \sqrt{717}) \right)^{\frac{1}{3}}$.

We moeten nu een aantal eigenschappen van de kromme bepalen die nodig zijn bij het invullen van alle formules uit voorgaande paragrafen. Invullen van de formules geeft ons:

$$\omega \approx 4,24975$$

$$\begin{aligned}
c_2 &\approx 10,0302 \\
\varphi(P_1) &\approx 0,157375 \\
\varphi(P_2) &\approx 0,431702 \\
u_1 &\approx 0,668802 \\
u_2 &\approx 1,83462 \\
b_2 &= 36 \\
\Delta &= -2787696 \\
j_E &= -\frac{6912}{239}.
\end{aligned}$$

Uit deze gegevens kunnen we afleiden dat

$$\begin{aligned}
c_0 &= 0 \\
c_3 &\approx 2,117946562.
\end{aligned}$$

Nu zullen we het rooster gaan bekijken dat bij de elliptische kromme hoort.

$$\begin{aligned}
\omega_1 &\approx 2,12487 + 1,11118i \\
\omega_2 &= \overline{\omega_1} \\
\tau &= \frac{\omega_1}{\omega_2} \approx 0,57052 + 0,821284i
\end{aligned}$$

Deze basis voldoet echter niet aan 2.11. Wat combineerwerk geeft nu een basis:

$$\begin{aligned}
\omega'_1 &= -\omega_2 \\
\omega'_2 &= \omega_1 - \omega_2 \\
\tau' &= \frac{\omega'_1}{\omega'_2} \approx \frac{1}{2} + 0,956137i.
\end{aligned}$$

Deze voldoet wel aan 2.11. We beschouwen dus de volgende lineaire vorm:

$$L(P) = m_0\omega + m_1u_1 + m_2u_2.$$

In de notatie van de stelling van David hebben we nu dus:

$$\begin{aligned}
R_0 &= O \\
R_1 &= P_1 \\
R_2 &= P_2 \\
r &= 2 \\
j_E &= -\frac{6912}{239} \\
h_E &\approx 4,394449155.
\end{aligned}$$

We kiezen $K = e$. en verder $A_0 = 9, A_1 = 5, A_2 = 7$. Hieruit volgt: $c_4 \approx 1,37 \cdot 10^{70}$.

We kunnen nu Pari gebruiken om de canonieke hoogtes te berekenen. Hieruit volgt:

$$\begin{aligned}
\hat{h}(P_1) &\approx 0,456266250485050524793862761 \\
\hat{h}(P_2) &\approx 1,168856325634384324776937512 \\
\hat{h}(P_1 + P_2) &\approx 0,2303858627991179521527112702
\end{aligned}$$

M.b.v deze gegevens kunnen we c_1 uitrekenen.

We nemen nu dus:

$$\begin{aligned}
c_1 &= 0,294 \\
c_2 &= 10,03 \\
c_3 &= 2,118 \\
c_4 &= 1,37 \cdot 10^{70}.
\end{aligned}$$

De ongelijkheid die we nu krijgen is:

$$M^2 < 13, 2 + 4, 7 \cdot 10^{70}(\log(2M + 1) + 1)(\log \log(2M + 1) + 5, 4)^4.$$

Grafisch oplossen met Mathematica geeft ons nu $M < 2, 1 \cdot 10^{38}$. Nu moeten we deze bovengrens gaan reduceren. Als we even de notatie van paragraaf 5.3 aanhouden, kunnen we nemen: $K_1 = 12$, $K_2 = 0, 294$ en $K_3 = 2, 1 \cdot 10^{38}$. Een goede keuze voor K_0 lijkt 10^{120} te zijn. Dit levert m.b.v. Mathematica:

$$\begin{aligned} [K_0\varphi(P_1)] &= 1573745639561788195439117719810161 - \\ &2155247409082829646876957539989252878877862920430180482993 - \\ &6704336186037931517758039262 \\ [K_0\varphi(P_2)] &= 4317018545263020064860043772983681 - \\ &0465737312187996257836825678821612197169061584984664015998 - \\ &8710126312103287794826485798. \end{aligned}$$

De gereduceerde basis wordt dan gegeven door:

$$\begin{aligned} b_1 &= \begin{pmatrix} 6115286738902238657899046545875322378200 \\ 3565267481259182871387982668040011947545 \\ -4083999028312654005151062614890923645690 \end{pmatrix} \\ b_2 &= \begin{pmatrix} 7401794820873550185010712892913792700322 \\ -6634086298642993305600231889576329059597 \\ 6104511756100099460987587432897459938958 \end{pmatrix} \\ b_3 &= \begin{pmatrix} 1218164689673954435026210361552777707615 \\ -4968883109383298484465801949049215089502 \\ -10018045766291824884688229823623175512466 \end{pmatrix}. \end{aligned}$$

Deze heb ik uitgerekend met Mathematica. Bij Mathematica zit een commando dat heet LatticeReduce, deze reduceert een basis. Verder heb ik nog gecontroleerd of de basis LLL-gereduceerd is m.b.v. een programma dat dr. van der Kallen heeft geschreven (staat op zijn website: www.math.uu.nl/people/vdkallen). We zien dat b_1 voldoet aan 5.15. Dit levert ons een nieuwe bovengrens van $M \leq 25$. Deze bovengrens is al stukken beter, maar we kunnen hem proberen te verbeteren door nog een keer het LLL-algoritme toe te passen. Dan moeten we nemen $K_3 = 26$. Een goede keuze lijkt nu $K_0 = 10^7$ te zijn. Dit levert ons de volgende getallen:

$$\begin{aligned} [K_0\varphi(P_1)] &= 1573745 \\ [K_0\varphi(P_2)] &= 4317018. \end{aligned}$$

Mathematica levert nu

$$b_1 = \begin{pmatrix} 74 \\ -115 \\ 60 \end{pmatrix}, b_2 = \begin{pmatrix} -139 \\ 97 \\ 191 \end{pmatrix}, b_3 = \begin{pmatrix} -285 \\ -93 \\ 1 \end{pmatrix}.$$

Dit levert ons nu de volgende bovengrens $M \leq 7$. Tot slot hebben we nog $X_0 = 11$. Alle gehele punten met $w \leq X_0$ op E' zijn:

$$\begin{aligned} &(-8, -10), (-8, -8), (-6, -18), (-6, 0), (-3, -18), (-3, 0), \\ &(0, -18), (0, 0), (4, -28), (4, 10), (6, -36), (6, 18). \end{aligned}$$

We zien onmiddellijk dat alle gehele punten van E'' ook gehele punten zijn van E' . Alle gehele punten van E'' die we verkrijgen door de afchatting van M zijn:

$$\begin{aligned} &(-3, \pm 9), (513, \pm 11619), (3, \pm 9), (7, \pm 19), (24, \pm 117), (0, \pm 9), \\ &(-5, \pm 1), (39, \pm 243), (33, \pm 189). \end{aligned}$$

Deze punten leveren met de volgende punten op E' :

$$\begin{aligned} &(-6, 0), (510, 11610), (0, 0), (4, 10), (21, 108), (-3, 0), \\ &\qquad\qquad\qquad (-8, -8), (36, 234), (30, 180) \\ &(-6, -18), (510, -11628), (0, -18), (4, -28), (21, -126), (-3, -18), \\ &\qquad\qquad\qquad (-8, -10), (36, -252), (30, -198) \end{aligned}$$

Om nu alle gehele punten te vinden van E moeten we nu dus bekijken welke punten van de vorm $(6a, 18b)$ zijn. Dit levert ons tenslotte de volgende gehele punten van E :

$$\begin{aligned} &(-1, -1), (-1, 0), (0, -1), (0, 0), (1, -2), (1, 1), (5, -11), (5, 10), \\ &\qquad\qquad\qquad (6, -14), (6, 13), (85, -646), (85, 645). \end{aligned}$$

In de vraag wanneer de som van de eerste b getallen gelijk is aan de som van de eerste a kwadraten is gebruik gemaakt van formules die alleen gelden voor getallen groter dan nul. We zien dus dat het uiteindelijke antwoord de volgende paren (a, b) bevat:

$$(0, 0), (1, 1), (5, 10), (6, 13), (85, 645).$$

Hoofdstuk 7

Literatuurlijst

1. [Ap] T. Apostolos, *Modular Functions and Dirichlet Series in Number Theory*, Springer Verlag, 1976.
2. [AS] M. Abramowitz and I. Stegun (eds.), *Handbook of Mathematical Functions*, Dover, New York, 1964.
3. [Da] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Publ. Math Univ. Pierre et Marie Curie 106, Problèmes diophantiens 1991-1992, exposé no.3.
4. [La] S. Lang, *Complex Analysis*, Springer Graduate texts in mathematics nr. 103.
5. [LLL] A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515-534
6. [Si1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer, New York, 1986.
7. [Si2] J.H. Silverman, *The difference between the Weil height and the canonical height of elliptic curves*, Math. Comp. 55 (1990), 723-743.
8. [ST] R.J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arithmetica LXVII.2(1994), 177-196.