K. S. Baak

Het vermoeden van Birch en Swinnerton-Dyer

Bachelorscriptie

Scriptiebegeleider: dr. P. J. Bruin

juni 2016

Universiteit Leiden

Mathematisch Instituut, Universiteit Leiden

Notatie

(i) We gebruiken de notatie $\mathbb{N}$ voor de verzameling niet-negatieve gehele getallen.

(ii) Voor een priemgetal p is $\mathbb{Q}_p$ het lichaam der p-adische getallen.

(iii) Voor een priemgetal p is $\mathbb{Z}_p$ de ring van p-adische gehelen.

(iv) Voor een priemgetal p is $\mathbb{F}_p$ het lichaam dat bestaat uit p elementen.

(v) De lijn op oneindig in het projectieve vlak noteren we met L_∞.

(vi) Een algebraïsche afsluiting van een lichaam K noteren we als $\overline{K}$.

(vii) De eenhedengroep van een ring R noteren we als $R^\times$.

(viii) Het quotiëntenlichaam van een domein R noteren we als $\kappa(R)$.

Inhoudsopgave

1 Inleiding

Heel informeel is een elliptische kromme E over $\mathbb{Q}$ de oplossingsverzameling van een vergelijking $y^2 = x^3 + Ax + B$ met $A, B \in \mathbb{Q}$ en $4A^3 + 27B^2 \neq 0$. Deze laatste voorwaarde garandeert dat de kromme "glad" of "niet-singulier" is. De vraag die men hierbij meteen stelt is "Bestaan er $\mathbb{Q}$-rationale punten op E?", dat wil zeggen, bestaan er (x, y) die aan $y^2 = x^3 + Ax + B$ voldoen met $x, y \in \mathbb{Q}$. Als we de situatie bekijken in het projectieve vlak, krijgt de verzameling $E(\mathbb{Q})$ van alle $\mathbb{Q}$-rationale punten op E een abelse groepsstructuur. De beroemde stelling van Mordell vertelt ons dat $E(\mathbb{Q})$ eindig voortgebracht is en uit de structuurstelling voor eindig voortgebrachte abelse groepen volgt nu $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus A$ voor een zekere $r \in \mathbb{N}$ en een eindige groep A. Het natuurlijke getal r wordt de algebraïsche rang van E genoemd.

Voor een elliptische kromme is ook het begrip van een analytische rang gedefinieerd. Gegeven een elliptische kromme, kunnen we een functie $L(E, s)$ aan E verbinden. De functie $L(E, s)$ is een holomorfe functie van een complexe variabele s en wordt de L-functie van E genoemd. Na het definiëren van deze functie kan men vrij makkelijk laten zien dat het inderdaad een holomorfe functie is op het rechterhalfvlak van het complexe vlak gedefinieerd door $\mathrm{Re}(s) > 3/2$. Al in 1952 werd voor het eerst vermoed dat $L(E, s)$ analytisch kan worden voortgezet tot een functie op het gehele complexe vlak. Dit werd echter pas in 2001 bewezen als gevolg van de modulariteitsstelling. Een specifiek geval van deze stelling werd al in 1995 bewezen door Andrew Wiles die er daarmee in slaagde de laatste stelling van Fermat te bewijzen, een open probleem sinds 1637. Nu we weten dat de L-functie van E op heel $\mathbb{C}$ gedefinieerd is, kunnen we de analytische rang van E definiëren als de verdwijnorde van E in het punt $s = 1$. De eerste versie van het vermoeden van Birch en Swinnerton-Dyer publiceerden Bryan Birch en Peter Swinnerton-Dyer in 1965. Dit is de versie zoals we hem nu kennen.

Vermoeden. *Zij E een elliptische kromme over $\mathbb{Q}$. De algebraïsche rang en de analytische rang van E zijn gelijk.*

Dit vermoeden is tot de dag van vandaag een open probleem in de wiskunde en werd in 2000 door het Clay Mathematics Institute uitgeroepen tot één van de zeven millenniumproblemen. Dit houdt in dat het instituut een prijs van $1.000.000 biedt aan degene die een oplossing weet te vinden.

Er is tevens een sterke variant van het vermoeden van Birch en Swinnerton-Dyer. Dit sterke vermoeden zegt dat de algebraïsche en analytische rang van E gelijk zijn en geeft een uitdrukking voor de leidende term van $L(E, s)$ in het punt $s = 1$.

$$\lim_{s \to 1} L(E, s)(s-1)^{-r} = \frac{\Omega(E) \left(\prod_p c_p \right) \mathrm{Reg}(E) \#Ш(E)}{\left(\#(E(\mathbb{Q})^{\mathrm{tor}}) \right)^2}.$$

Het doel van deze scriptie is om de termen in het sterke vermoeden van Birch en Swinnerton-Dyer te definiëren. In het eerste hoofdstuk zullen we beginnen met een grote hoeveelheid theorie over elliptische krommen. Het tweede hoofdstuk zal de reële periode $\Omega(E)$, de Tamagawa-getallen c_p en de regulator $\mathrm{Reg}(E)$ bespreken. In het laatste hoofdstuk zullen we de Tate-Shafarevich-groep $Ш(E)$ bespreken en een voorbeeld geven van een elliptische kromme met niet-triviale $Ш(E)$.

2 Elliptische krommen

2.1 Affiene en projectieve krommen

Voordat we elliptische krommen definiëren, zullen we kort een aantal meetkundige termen bespreken. Voor een lichaam K is de affiene n-dimensionale ruimte $\mathbb{A}^n(K)$ de verzameling $K^n = \{(x_1, ..., x_k) : x_i \in K\}$. In het geval $n = 1$ spreken we over de affiene lijn en in het geval $n = 2$ over het affiene vlak. Naast affiene ruimtes is ook het begrip van een projectieve ruimte belangrijk. Voor een lichaam K is de projectieve n-dimensionale ruimte $\mathbb{P}^n(K)$ gelijk aan $(\mathbb{A}^{n+1}(K) \setminus (0, ..., 0))/\sim$, waarbij $\sim$ de equivalentierelatie is gegeven door

$$(x_1, ..., x_{n+1}) \sim (y_1, ..., y_{n+1}) \iff \exists \lambda \in K : (x_1, ..., x_{n+1}) = (\lambda y_1, ..., \lambda y_{n+1}).$$

De equivalentieklassen van $\sim$ noteren we met $(x_1 : x_2 : ... : x_{n+1})$ en noemen we homogene coördinaten voor $\mathbb{P}^n(K)$. Wederom spreken we in de gevallen $n = 1$ en $n = 2$ over respectievelijk de projectieve lijn en het projectieve vlak. Elementen van zowel affiene als projectieve ruimtes worden in het vervolg punten genoemd. We zullen nu het begrip kromme definiëren.

Definitie 2.1. Zij K een lichaam. Een *vlakke (algebraïsche) affiene kromme* over K is een deelverzameling

$$C_f = \{(x, y) \in \mathbb{A}^2(\overline{K}) : f(x, y) = 0\} \subseteq \mathbb{A}^2(\overline{K})$$

waarbij $f \in K[X, Y]$ niet-constant en kwadraatvrij over $\overline{K}$ is. We noemen de kromme C_f de vlakke affiene kromme gedefinieerd door het polynoom f of door de vergelijking $f = 0$.

Merk op dat de polynoomring in n variabelen over een lichaam K een ontbindingsring is en we kunnen elk polynoom dus ontbinden in irreducibele factoren. We zeggen dat een polynoom $f \in K[X_1, ..., X_n]$ kwadraatvrij is als het geen irreducibele factor met macht 2 of hoger bevat. Voor de definitie van een projectieve kromme moeten we iets voorzichtiger zijn. Immers, de kromme mag niet afhangen van de representanten die we voor punten in $\mathbb{P}^2(\overline{K})$ kiezen. We zijn dus geïnteresseerd in de polynomen F in $K[X, Y, Z]$ waarvoor geldt $F(a, b, c) = 0 \implies F(\lambda a, \lambda b, \lambda c) = 0$ voor alle $\lambda \in \overline{K}$. Dit zijn precies de homogene polynomen.

Definitie 2.2. Zij K een lichaam. Een polynoom $F \in K[X_1, X_2, ..., X_n]$ heet homogeen van graad d als het een K-lineaire combinatie van monomen in $K[X_1, X_2, ..., X_n]$, alle van graad d, is.

We kunnen nu projectieve krommen definiëren.

Definitie 2.3. Zij K een lichaam. Een *vlakke (algebraïsche) projectieve kromme* over K van graad d is een deelverzameling

$$C_F = \{(x : y : z) \in \mathbb{P}^2(\overline{K}) : F(x, y, z) = 0\} \subseteq \mathbb{P}^2(\overline{K})$$

waarbij $F \in K[X, Y, Z]$ een niet-constant homogeen polynoom van graad d is dat kwadraatvrij is over $\overline{K}$. We noemen de kromme C_F de vlakke projectieve kromme gedefinieerd door het polynoom F of door de vergelijking $F = 0$.

In deze scriptie zullen we het adjectief “vlakke" weglaten en hebben we het kortweg over affiene of projectieve krommen. We sluiten de paragraaf af met een aantal opmerkingen en definities omtrent krommen.

Opmerking 2.4. Om aan te geven dat een kromme C gedefinieerd is over een lichaam K, schrijven we ook wel C/K.

Opmerking 2.5. Zij $F \in K[X,Y,Z]$ een niet-constant homogeen polynoom dat kwadraatvrij is over $\overline{K}$ met een irreducibele factor g. Als $(x:y:z) \in \mathbb{P}^2(\overline{K})$ aan de vergelijking $g(x,y,z) = 0$ voldoet, dan geldt er ook meteen $F(x,y,z) = 0$. Met andere woorden $C_g \subseteq C_F$. Als we F in irreducibele factoren ontbinden, $F = \alpha p_1 ... p_n$ met $\alpha \in K^\times$ en $p_1, ..., p_n$ irreducibel in $K[X,Y,Z]$, dan geldt er $C_F = \bigcup_{i=1}^n C_{p_i}$. De componenten C_{p_i} noemen we *irreducibele componenten* van de kromme C_F. Als F zelf irreducibel is, spreken we van een *irreducibele kromme*.

Opmerking 2.6. Zij K een lichaam en F en G twee verschillende polynomen in $K[X,Y,Z]$ die dezelfde projectieve kromme definiëren. Ontbinden we F en G over $\overline{K}$ in irreducibele factoren, dan krijgen we $F = \alpha p_1 \cdots p_n$ en $G = \beta q_1 \cdots q_m$ met $\alpha, \beta \in \overline{K}^\times$ en $p_1, ..., p_n, q_1, ..., q_m \in \overline{K}[X,Y,Z]$ irreducibel. Omdat F en G beide kwadraatvrij zijn over $\overline{K}$ geldt er $p_i \neq p_j$ en $q_i \neq q_j$ voor alle $i \neq j$. We concluderen $p_1 \cdots p_n = q_1 \cdots q_n$ en dus $F = \alpha\beta^{-1}G$. Twee polynomen definiëren dus dezelfde kromme dan en slechts dan als ze op vermenigvuldiging met een element uit $K^\times$ na gelijk zijn.

Definitie 2.7. Een kromme gedefinieerd door een lineair polynoom wordt een *lijn* genoemd.

Merk op dat we voor elk lichaam K een natuurlijke inclusie $\mathbb{P}^2(K) \to \mathbb{P}^2(\overline{K})$ hebben.

Definitie 2.8. Zij K_0 een lichaam en C/K_0 een vlakke projectieve kromme. We definiëren de verzameling $C(K_0) = C \cap \mathbb{P}^2(K_0)$. Voor elke lichaamsuitbreiding $K_0 \subseteq K$ kunnen we C opvatten als kromme over K en de verzameling $C(K)$ bestuderen. De punten in $\mathbb{P}^2(K)$ noemen we K-rationaal en de verzameling $C(K)$ bestaat dus uit alle K-rationale punten op C.

De projectieve n-ruimte over een lichaam K kent nog een andere bekende constructie. We maken $\mathbb{P}^n(K)$ door aan elke richting in de affiene n-ruimte over K een punt op oneindig toe te voegen. Een richting in $\mathbb{A}^n(K)$ kunnen we identificeren met een lijn door de oorsprong in $\mathbb{A}^n(K)$, i.e. een punt in $\mathbb{P}^{n-1}(K)$. We hebben daarom $\mathbb{P}^n(K) = \mathbb{A}^n(K) \coprod \mathbb{P}^{n-1}(K)$. Dat de twee genoemde constructies van de projectieve ruimte equivalent zijn, zullen we hier niet bewijzen. Een duidelijke toelichting kan gevonden worden in Appendix A van [8, p. 265 - 270]. Wel geven we nog de volgende bijectie

$$\begin{aligned}(\mathbb{A}^{n+1}(K) \setminus (0,...,0))/\sim &\longrightarrow \mathbb{A}^n(K) \coprod \mathbb{P}^{n-1}(K) \\ (x_1 : ... : x_{n+1}) &\longmapsto \begin{cases} (x_1/x_{n+1}, ..., x_n/x_{n+1}) \in \mathbb{A}^n(K) & \text{als } x_{n+1} \neq 0 \\ (x_1 : ... : x_n) \in \mathbb{P}^{n-1}(K) & \text{als } x_{n+1} = 0 \end{cases}\end{aligned}$$

met de bijbehorende inverse

$$\begin{aligned}\mathbb{A}^n(K) \coprod \mathbb{P}^{n-1}(K) &\longrightarrow \mathbb{A}^{n+1}(k) \setminus (0,...,0))/\sim \\ (x_1, ..., x_n) &\longmapsto (x_1 : ... : x_n : 1) \\ (x_1 : ... : x_n) &\longmapsto (x_1 : ... : x_n : 0).\end{aligned}$$

Punten $(a:b:c)$ in het projectieve vlak $\mathbb{P}^2(K)$ met $c = 0$ noemen we dus punten op oneindig en punten met $c \neq 0$ zien we als punten in $\mathbb{A}^2(K)$. Dit is niets meer dan een conventie en we hadden er evengoed voor kunnen kiezen de punten met $a = 0$ of $b = 0$ de punten op oneindig te noemen. De lijn in het projectieve vlak gedefinieerd door de vergelijking $Z = 0$ bestaat uit alle punten op oneindig en wordt daarom de lijn op oneindig L_∞ genoemd. We hebben gezien dat we de affiene ruimte als deelverzameling van de projectieve ruimte kunnen zien en dit leidt tot de vraag of we een affiene kromme ook kunnen zien als deel van een projectieve kromme. Dit is inderdaad het geval. Als $F \in K[X,Y,Z]$ een homogeen polynoom is, dan noemen we het polynoom $f(x,y) := F(x,y,1) \in K[X,Y]$ de

dehomogenisatie van F. Omgekeerd kunnen we een polynoom $f \in K[X,Y]$ tot een homogeen polynoom in $K[X,Y,Z]$ maken door elk monoom van f met Z^d te vermenigvuldigen voor een geschikte waarde van d. Het verkregen polynoom noemen we de homogenisatie van f. Zo is de homogenisatie van het polynoom $f := \alpha + \beta X^3Y + \gamma Y + \delta XY^2$ bijvoorbeeld $\alpha Z^4 + \beta X^3Y + \gamma YZ^3 + \delta XY^2Z$. Merk op dat als we laatst genoemd polynoom in z'n geheel met Z^m vermenigvuldigen we ook een homogeen polynoom in $K[X,Y,Z]$ verkrijgen waarvan de dehomogenisatie f is. We spreken echter af dat dé homogenisatie van een polynoom f in $K[X,Y]$ het homogene polynoom F in $K[X,Y,Z]$ is met dehomogenisatie f en waarvoor geldt $Z \nmid F$.

Als $(a : b : c) \in \mathbb{P}^2(K)$ met $c \neq 0$ voldoet aan het homogene polynoom $F \in K[X,Y,Z]$, dan geldt er $F\left(\frac{a}{c}, \frac{b}{c}, 1\right) = 0$ en $\left(\frac{a}{c}, \frac{b}{c}\right)$ voldoet dus aan de dehomogenisatie van F. Als $(a,b) \in \mathbb{A}^2(K)$ voldoet aan een polynoom $f \in K[X,Y]$ dan voldoet $(a,b,1) \in \mathbb{A}^3(K)$ aan zijn homogenisatie in $K[X,Y,Z]$. We concluderen dat het geven van punten $(a : b : c)$ in $\mathbb{P}^2(K)$ die voldoen aan een homogeen polynoom $F \in K[X,Y,Z]$ equivalent is met het geven van punten $(a,b) \in \mathbb{A}^2(K)$ die voldoen aan de dehomogenisatie van F samen met het geven van alle punten op oneindig in $\mathbb{P}^2(K)$ die aan F voldoen. Als F een homogeen polynoom ongelijk aan Z in $K[X,Y,Z]$ is met dehomogenisatie $f \in K[X,Y]$, dan noemen we de affiene kromme C_f het affiene deel van de projectieve kromme C_F. Merk op dat de dehomogenisatie van het polynoom $Z \in K[X,Y,Z]$ een constante is en dus geen affiene kromme definieert.

2.2 Elliptische krommen en de Weierstrass-vorm

Een elliptische kromme is een niet-singuliere projectieve kromme gegeven door een specifieke vergelijking. In deze paragraaf zal dit precies worden gemaakt. We zullen beginnen met het definiëren van het begrip niet-singulier.

Definitie 2.9. Zij C een vlakke projectieve kromme over een lichaam K gedefinieerd door $F \in K[X,Y,Z]$. Een *singulier punt* op C is een punt $(x : y : z) \in C$ waarvoor geldt

$$\frac{\partial F}{\partial X}(x,y,z) = \frac{\partial F}{\partial Y}(x,y,z) = \frac{\partial F}{\partial Z}(x,y,z) = 0.$$

Een projectieve kromme zonder singuliere punten wordt *niet-singulier* genoemd.

De vergelijking van een elliptische kromme over een lichaam K heeft de volgende vorm

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2.1}$$

Een vergelijking als deze heet een vergelijking in de *(lange) Weierstrass-vorm* of een *(lange) Weierstrass-vergelijking*. De notatie van de coëfficiënten van vergelijking (2.1) is standaard voor een Weierstrass-vergelijking en als we het in het vervolg over een Weierstrass-vergelijking hebben, gaan we er impliciet van uit dat de coëfficiënten a_1, a_2, a_3, a_4, a_6 zijn. Gegeven een vergelijking in Weierstrass-vorm, definiëren we een aantal bijbehorende constanten.

Definitie 2.10. Zij K een lichaam en laat $a_1, a_2, a_3, a_4, a_6 \in K$ de coëffciënten zijn van een

Weierstrass-vergelijking over K (als in (2.1)). We definiëren

$$\begin{aligned}
b_2 &:= a_1^2 + 4a_2 \\
b_4 &:= 2a_4 + a_1a_3 \\
b_6 &:= a_3^2 + 4a_6 \\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &:= b_2^2 - 24b_4 \\
c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 - 9b_2b_4b_6
\end{aligned}$$

De constante Δ wordt de *discriminant* van de vergelijking genoemd.

In deze scriptie zullen we niet in gaan op wat de morfismen tussen krommen zijn en daardoor kunnen we ook niet herkennen wanneer twee krommen isomorf zijn. In paragraaf 4.2 zullen we dit grotendeels oplossen door de categorie van functielichamen te bestuderen, die equivalent is met de categorie van niet-singuliere projectieve krommen. De volgende propositie zal echter goed van pas komen en we nemen hem daarom aan zonder bewijs.

Propositie 2.11. *Zij K een lichaam en C_1/K en C_2/K projectieve krommen gegeven door Weierstrass-vergelijkingen. Noteer de variabelen van de vergelijking die C_1, respectievelijk C_2, definieert als X, Y, Z, respectievelijk X', Y', Z'. De krommen C_1 en C_2 zijn isomorf dan en slechts dan als er een $u \in K^\times$ en $r, s, t \in K$ bestaan zodanig dat de vergelijking voor C_2 uit de vergelijking voor C_1 verkregen kan worden met de coördinaattransformatie*

$$\begin{aligned}
X &= u^2X' + r \\
Y &= u^3Y' + su^2X' + t \\
Z &= Z'.
\end{aligned} \tag{2.2}$$

Bewijs. Zie [7, p. 59] □

Een coördinaattransformatie zoals beschreven in 2.11 zullen we vanaf nu een *toegelaten coördinaattransformatie* noemen.

Opmerking 2.12. Bekijk de coördinaattransformatie (2.2) tussen een Weierstrass-vergelijking met coëfficiënten a_1, a_2, a_3, a_4, a_6 en een met coëfficiënten $a_1', a_2', a_3', a_4', a_6'$. Na wat uitschrijfwerk vinden we dat er geldt $u^{12}\Delta' = \Delta$. Geldt er $r, s, t = 0$, dan vinden we $u^i a_i' = a_i$ voor $i = 1, 2, 3, 4, 6$. Dit verklaart de nummering van de coëfficiënten van een Weierstrass-vergelijking, die op het eerste oog willekeurig kan lijken.

Opmerking 2.13. Zij C/K een projectieve kromme gegeven door een Weierstrass-vergelijking. Als er geldt $\mathrm{char}(K) \neq 2$, dan levert de toegelaten coördinaattransformatie $X = X',\ Y = Y' - (a_1X' + a_3)/2,\ Z = Z'$ de Weierstrass-vergelijking

$$Y^2Z = X^3 + \frac{b_2}{4}X^2Z + \frac{b_4}{2}XZ^2 + \frac{b_6}{4}Z^3$$

voor C. Is het karakteristiek van K ook ongelijk aan 3, dan kunnen we vervolgens de toegelaten coördinaattransformatie $X = X' - b_2/12,\ Y = Y',\ Z = Z'$ uitvoeren om de Weierstrass-vergelijking

$$Y^2Z = X^3 - \frac{c_4}{48}XZ^2 - \frac{c_6}{864}$$

voor C te krijgen. Als C dus een projectieve kromme over een lichaam K met $\mathrm{char}(K) \neq 2, 3$ is gegeven door een Weierstrass-vergelijking, dan bestaat er een Weierstrass-vergelijking van de vorm $Y^2Z = X^3 + AXZ^2 + BZ^3$ met $A, B \in K$ voor C.

We zullen nu onderzoeken onder welke voorwaarde een kromme gegeven door een Weierstrass-vergelijking niet-singulier is.

Propositie 2.14. *Zij C/K een vlakke projectieve kromme gegeven door een vergelijking in de Weierstrass-vorm. De lijn op oneindig L_∞ snijdt C op precies één punt en dit snijpunt is een niet-singulier punt van C.*

Bewijs. Een punt $(x : y : z)$ op L_∞ voldoet aan $z = 0$. We stellen Z gelijk aan 0 in (2.1) en vinden $X^3 = 0$. Het enige punt van L_∞ op C is dus $\mathcal{O} := (0 : 1 : 0)$. Nemen we de partiële afgeleide van het polynoom dat bij (2.1) hoort naar Z, dan vinden we $Y^2 + a_1XY + 2a_3Y - a_2X^2 - 2a_4XZ - 3a_6Z^2$. Invullen van $(0 : 1 : 0)$ geeft $1 \neq 0$. We concluderen dat $(0 : 1 : 0)$ geen singulier punt is. □

Het unieke punt op oneindig op een kromme gegeven door een Weierstrass-vergelijking zullen we $\mathcal{O}$ noemen. Uit propositie 2.14 volgt dat het voldoende is om naar het affiene deel van een Weierstrass-vergelijking te kijken om te kunnen bepalen of de kromme niet-singulier is. Vaak wordt dan ook alleen het affiene deel van een Weierstrass-vergelijking gegeven, zo hebben we het bijvoorbeeld over de kromme (over $\mathbb{Q}$) gegeven door $y^2 = x^3 - 2x + 2$, waar we eigenlijk de kromme gegeven door $Y^2Z = X^3 - 2XZ^2 + 2Z^3$ bedoelen. De volgende stelling doet een uitspraak over wanneer een projectieve kromme gedefinieerd door een Weierstrass-vergelijking niet-singulier is.

Stelling 2.15. *Zij K een lichaam en C/K een vlakke projectieve kromme gegeven door een vergelijking in de Weierstrass-vorm. De kromme C heeft een singulier punt dan en slechts dan als er geldt $\Delta = 0$.*

Bewijs. Voor het gemak nemen we aan dat er geldt $\mathrm{char}(K) \neq 2$. Voor een bewijs in het geval $\mathrm{char}(K) = 2$, zie [5, p. 62]. Wegens propositie 2.14 is het voldoende te bewijzen dat het affiene deel van C een singulier punt heeft dan en slechts dan als er geldt $\Delta = 0$. Met opmerking 2.13 vinden we dat

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

een Weierstrass-vergelijking voor C is. Een punt $P = (x : y : 1)$ op C is singulier als er geldt $2y = 0$ en $3x^2 + b_2x/2 + b_4x/2 = 0$. De eerste voorwaarde geeft $y = 0$ en er volgt dat x zowel een nulpunt moet zijn van f als van f' waarbij f het polynoom $X^3 + b_2X^2/4 + b_4X/2 + b_6 \in K[X]$ is. We weten dat x een nulpunt is van zowel f als f' als de discriminant d van f gelijk is aan 0 (voor de definitie van de discriminant van een polynoom in $K[X]$ en een methode om deze te berekenen, zie [9, p. 53]). De discriminant van een derdegraads polynoom $\sum_{i=0}^{3} c_iX^i$ is gelijk aan $c_2^2c_1^2 - 4c_3c_1^3 - 4c_2^3c_0 - 27c_3^2c_0^2 + 18c_0c_1c_2c_3$. Rekenen we nu de gewenste discriminant d uit (dit wordt een stuk minder uitschrijf werk als we gebruiken dat $4b_8 = b_2b_6 - b_4^2$), dan vinden we $d = \Delta/16$. We concluderen dat C een singulier punt heeft dan en slechts dan als $d = 0$ dan en slechts dan als $\Delta = 0$. □

We sluiten deze pargraaf af met de definitie van een elliptische kromme.

Definitie 2.16. Zij K een lichaam. Een *elliptische kromme* over K is een niet-singuliere vlakke projectieve kromme over K gedefinieerd door een vergelijking in Weierstrass-vorm.

2.3 Snijpunten en multipliciteiten

In de volgende paragraaf zullen we een groepsstructuur op de verzameling $E(K)$ van K-rationale punten op een elliptische kromme E/K leggen. Deze groepsstructuur berust op een aantal feiten over het snijden van krommen en lijnen. We zullen deze feiten in deze paragraaf noemen en bewijzen. We hebben hierbij veelvuldig de volgende propositie nodig.

Propositie 2.17. *Zij K een lichaam. Zij $F \in K[X,Y]$ een homogeen polynoom van graad n. Over $\overline{K}$ ontbindt F zich in lineaire factoren*

$$F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

met zekere $\alpha_i, \beta_i \in K$ voor alle $1 \leq i \leq n$.

Bewijs. Omdat F homogeen van graad n is, geldt er $F(X,Y) = Y^n F(X/Y, 1)$. Het polynoom $F(X/Y,1) \in K[X/Y]$ is homogeen van graad $d \leq n$. Over $\overline{K}$ geldt er

$$F(X/Y,1) = \prod_{i=1}^{d}(c_i X/Y - d_i)$$

voor zekere $c_i, d_i \in \overline{K}$. We vinden

$$F(X,Y) = Y^n F(X/Y,1) = Y^n \prod_{i=1}^{d}(c_i X/Y - d_i) = Y^{n-d}\prod_{i=1}^{d}(c_i X - d_i Y) = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

met $\alpha_i = c_i$ voor $i = 1,...,d$, $\alpha_i = 0$ voor $i = d,...,n$, $\beta_i = d_i$ voor $i = 1,...,d$ en $\beta_i = -1$ voor $i = d,...,n$. □

Zij C/K een projectieve kromme gegeven door een polynoom $F \in K[X,Y,Z]$ die niet de lijn op oneindig L_∞ bevat. We bekijken de snijpunten van C met L_∞. De lijn op oneindig is gegeven door $Z = 0$ en voor alle punten $(x : y : z)$ op $C \cap L_\infty$ geldt dus $z = 0$. Er geldt tevens $F(x,y,z) = 0$ en dus $F(x,y,0) = 0$. Als het polynoom Z een irreducibele factor is van F, bevat C de lijn op oneindig. We hebben aangenomen dat dit niet het geval is en er geldt dus $Z \nmid F$. Er volgt dat $G(X,Y) := F(X,Y,0)$ een homogeen polynoom van graad n in $K[X,Y]$ is ongelijk aan 0. Met propositie 2.17 volgt er

$$G(X,Y) = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

voor zekere $\alpha_i, \beta_i \in \overline{K}$. Voor alle $i \in \{1,...,n\}$ is $(\beta_i, \alpha_i) \in \overline{K}^2$ dus een nulpunt van G en we concluderen dat $(\beta_i : \alpha_i : 0)$ een snijpunt is van C en L_∞. Omgekeerd bestaat er voor elk snijpunt $(x : y : 0) \in C \cap L_\infty$ een $i \in \{1,...,n\}$ zodanig dat $(x : y : 0) = (\beta_i : \alpha_i : 0)$. Dit geeft aanleiding tot de volgende definitie.

Definitie 2.18. Zij K een lichaam en C/K een projectieve kromme van graad n gedefinieerd door $F \in K[X,Y,Z]$ die niet de lijn op oneindig bevat. Zij $P = (a : b : 0) \in C$ een snijpunt van C en de lijn op oneindig L_∞. De *multipliciteit* van P is het maximale natuurlijke getal $m \geq 1$ zodanig dat er $\alpha_1,...,\alpha_{n-m}, \beta_1,...,\beta_{n-m} \in \overline{K}$ bestaan met

$$F(X,Y,0) = (bX - aY)^m \prod_{i=1}^{n-m}(\alpha_i X - \beta_i Y)$$

Zij C/K een projectieve kromme en L/K een lijn die niet bevat is in C. We voeren een lineaire coördinaattransformatie uit die L naar L_∞ brengt en definiëren de multipliciteit van L en C als de multipliciteit van het snijpunt na de coördinatentransformatie.

De volgende twee opmerkingen volgen meteen uit propositie 2.17.

Opmerking 2.19. Zij K een lichaam, L/K een lijn en C/K een projectieve kromme van graad n die L niet als irreducibele component heeft. Als we multipliciteiten tellen, snijden L en C in precies n punten.

Opmerking 2.20. Zij K een lichaam, L/K een lijn en C/K een projectieve kromme van graad 3 die L niet als irreducibele component heeft. Als twee van de drie, niet noodzakelijk verschillende snijpunten van L en C in $C(K)$ liggen, dan ook het derde.

2.4 De groep $E(K)$

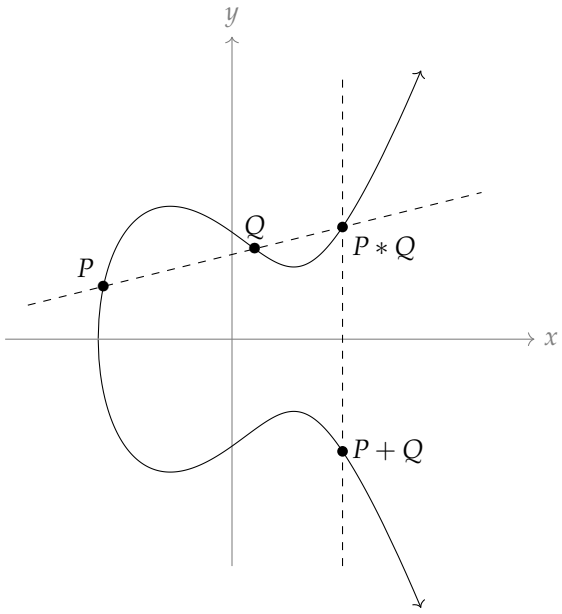
Zij E/K_0 een elliptische kromme en $K_0 \subseteq K$ een lichaamsuitbreiding. Zoals aangekondigd, zullen we in deze paragraaf een groepsstructuur op de verzameling $E(K)$ van K-rationale punten op E leggen. We beginnen met een bewerking $* : E(K) \times E(K) \to E(K)$. Gegeven twee verschillende punten $P, Q \in E(K)$, kunnen we een lijn L/K definiëren waar zowel P als Q opliggen. De lijn L en de elliptische kromme E snijden in precies drie punten (waarbij we multipliciteiten tellen). Twee van de drie snijpunten zijn P en Q, laat R het derde snijpunt zijn. Propositie 2.20 geeft $R \in E(K)$. Voor alle $P, Q \in E(K)$ definiëren we dus $P * Q = R$ waarbij R het derde snijpunt is van de lijn door P en Q en E. Kiezen we $P = Q$, dan laten we L de raaklijn van P aan E zijn. Het bestaan van deze raaklijn wordt gegarandeerd door het feit dat de kromme E niet-singulier is. De bewerking $*$ definieert nog geen groepsstructuur op de verzameling $E(K)$. We definiëren nog een bewerking op $E(K)$.

$$\begin{aligned} + : E(K) \times E(K) &\longrightarrow E(K) \\ (P, Q) &\longmapsto (P * Q) * \mathcal{O}. \end{aligned}$$

Stelling 2.21. *Zij E/K een elliptische kromme. Het paar $(E(K), +)$ is een abelse groep.*

Bewijs. Merk allereerst op dat de commutativiteit van $+$ meteen volgt uit de commutativiteit van $*$.
We bewijzen dat $\mathcal{O}$ het eenheidselement van $E(K)$ is. Zij $P \in E(K)$. Het punt $P * \mathcal{O}$ is het derde snijpunt van de lijn door P en $\mathcal{O}$ en E. Het punt $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O}$ is het derde snijpunt van de lijn door $P * \mathcal{O}$ en $\mathcal{O}$ en E. Dit moet dus wel P zijn. Er geldt $P + \mathcal{O} = P$.
We bewijzen nu dat elk punt in $E(K)$ een inverse heeft voor $+$. Zij $P \in E(K)$. We bekijken het punt $P * \mathcal{O}$. Er geldt $P + (P * \mathcal{O}) = (P * (P * \mathcal{O})) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$. Een punt $P \in E(\mathbb{Q})$ heeft dus inverse $-P = P * \mathcal{O}$.
De associativiteit van $+$ vereist heel wat meer werk, en zullen we hier niet bewijzen. Zie bijvoorbeeld [6, p. 27-19]. □

De bewerking $+$ wordt intuïtief duidelijk als de situatie wordt geschetst, zie figuur 1.



Figuur 1: Een schets van de bewerking $+$ op de elliptische kromme gegeven door de vergelijking $y^2 = x^3 - 2x + 2$.

In het geval $K = \mathbb{Q}$ hebben we de volgende beroemde stelling.

Stelling 2.22 (Mordell)**.** *Zij E een elliptische kromme over $\mathbb{Q}$. De groep $E(\mathbb{Q})$ is eindig voortgebracht.*

Bewijs. Zie [5, p. 402] of [8, p. 95]. □

Voor eindig voortgebrachte abelse groepen hebben we de structuurstelling. Deze stelling zegt dat een eindig voortgebrachte abelse groep A isomorf is met

$$A^{\text{tor}} \oplus \mathbb{Z}^r$$

voor zekere $r \geq 0$. Deze r wordt de rang van A genoemd. Verder is de torsie-ondergroep A^{tor} van A eindig. De rang van $E(\mathbb{Q})$ wordt de algebraïsche rang van de elliptische kromme E genoemd. Het zwakke vermoeden van Birch en Swinnerton-Dyer stelt dat deze rang gelijk is aan de analytische rang van E. Om deze rang te definiëren, moeten we de L-functie van E definiëren en hiertoe bestuderen we eerst de reductie van E modulo priemgetallen.

2.5 Reductie modulo priemen

Laat E in deze hele pargraaf een elliptische kromme over $\mathbb{Q}$ zijn. Als c het kleinst gemeenschappelijk veelvoud is van de noemers van de coëfficiënten a_1, a_2, a_3, a_4, a_6, kunnen we de toegelaten coördinaattransformatie $x = x'/c^2$, $y = y'/c^3$ uitvoeren. De verkregen vergelijking is

$$\frac{1}{c^6}Y^2Z + \frac{a_1}{c^5}XYZ + \frac{a_3}{c^3}YZ^2 = \frac{1}{c^6}X^3 + \frac{a_2}{c^4}X^2Z + \frac{a_4}{c^2}XZ^2 + a_6Z^3.$$

Modulo vermenigvuldiging met een constante is deze vergelijking gelijk aan de Weierstrass-vergelijking

$$Y^2Z + ca_1XYZ + c^3a_3YZ^2 = X^3 + c^2a_2X^2Z + c^4a_4XZ^2 + c^6a_6Z^3. \tag{2.3}$$

Aangezien we c gelijk hadden genomen aan het kleinste gemeenschappelijke veelvoud van de noemers van alle a_i, is (2.3) een Weierstrass-vergelijking met coëfficiënten in $\mathbb{Z}$ voor E. In het vervolg zullen we ervan uitgaan dat de Weierstrass-vergelijking van een elliptische kromme over $\mathbb{Q}$ coëfficiënten in $\mathbb{Z}$ heeft.

Zij p nu een priemgetal. Gegeven een Weierstrass-vergelijking met coëfficiënten in $\mathbb{Z}$ voor E, kunnen we alle coëfficiënten modulo p nemen om een een Weierstrass-vergelijking over $\mathbb{F}_p$ te krijgen. De projectieve kromme over $\mathbb{F}_p$ die deze vergelijking definieert is echter niet altijd niet-singulier. Laten we de gereduceerde kromme $\tilde{E}_p$ noemen. Hoewel we deze definitie later zullen verfijnen, zeggen we voor nu dat een elliptische kromme $E/\mathbb{Q}$ *goede reductie* modulo p heeft, als $\tilde{E}_p$ ook elliptisch is. Op het eerste gezicht lijken we de volgende methode te hebben om te bepalen of E een goede of slechte reductie modulo p heeft. Stelling 2.15 geeft dat $\tilde{E}_p$ niet-singulier is dan en slechts dan als $\tilde{\Delta} = 0$. Er geldt duidelijk $\Delta \equiv \tilde{\Delta} \mod p$ en $\tilde{E}_p$ is dus niet-singulier dan en slechts dan als $p|\Delta$. Dit lijkt simpel, maar we moeten toch wat voorzichtiger zijn. Bekijk bijvoorbeeld de elliptische kromme E gegeven door $y^2 = x^3 - 625x$. We berekenen $\Delta = -15625000000$. Uit de voorgaande redenatie heeft E duidelijk een slechte reductie modulo 5. Echter, bekijk nu de toegestane coördinaattransformatie $x = 25x'$, $y = 125y'$. De nieuwe Weierstrass-vergelijking voor E is $y^2 = x^3 - x$ met discriminant $\Delta = 16$. Nu moeten we concluderen dat E wel goede reductie modulo 5 heeft. We lossen dit probleem op door $\tilde{E}_p$ te definiëren als de projectieve kromme over $\mathbb{F}_p$ gedefinieerd door de reductie van een minimale Weierstrass-vergelijking voor E. Laat $\mathcal{D}$ de verzameling van de discriminanten

van alle Weierstrass-vergelijkingen voor E met gehele coëfficiënten zijn. We zeggen dat een Weierstrass-vergelijking p-minimaal is als $\mathrm{ord}_p(\Delta) \leq \mathrm{ord}_p(\Delta')$[1] voor alle $\Delta' \in \mathcal{D}$. Als een Weierstrass-vergelijking p-minimaal is voor alle priemgetallen p noemen we de vergelijking een *(globale) minimale Weierstrass-vergelijking* voor E. De discriminant van een minimale Weierstrass-vergelijking noemen we de *minimale discriminant* van E. Stelling 2.23 garandeert dat een elliptische kromme over $\mathbb{Q}$ altijd een minimale Weierstrass-vergelijking heeft. Merk op dat een elliptische kromme over $\mathbb{Q}$ wel een unieke minimale discriminant heeft maar niet altijd een unieke minimale Weierstrass-vergelijking.

Stelling 2.23. *Zij $E/\mathbb{Q}$ een elliptische kromme, dan heeft E een globale minimale Weierstrass-vergelijking.*

Bewijs. Leg een Weierstrass-vergelijking voor E vast. We zullen een toegelaten coördinatentransformatie beschrijven die een globale minimale Weierstrass-vergelijking voor E geeft. Voor alle priemgetallen p met $p \nmid \Delta$ is de huidige vergelijking al p-minimaal. Zij p een priemgetal met $p \mid \Delta$. Laat $u_p \in \mathbb{Q}^\times$ en $r_p, s_p, t_p \in \mathbb{Q}$ een toegelaten coördinaattransformatie definiëren zodanig dat de nieuwe Weierstrass-vergelijking p-minimaal is. Zij Δ_p de discriminant van deze p-minimale Weierstrass-vergelijking voor E en laat $a_{i,p}$ met $i = 1, 2, 3, 4, 6$ de coëfficiënten zijn. Definieer $\alpha_p = \mathrm{ord}_p(u_p)$ en merk op dat er geldt $\mathrm{ord}_p(\Delta_p) = \mathrm{ord}_p(\Delta u_p^{-12}) = \mathrm{ord}_p(\Delta) - 12\alpha_p$. We definiëren nu

$$u = \prod_{p \mid \Delta} p^{\alpha_p}.$$

Laat nu $d_p \in \mathbb{Z}$ en $m_p, n_p \in \mathbb{Z}$ met $\mathrm{ord}_p(m_p) = \mathrm{ord}_p(n_p) = 0$ zodanig zijn dat $r_p = p^{d_p} m_p / n_p$. Laat $\beta_p = \max_{i=1,2,3,4,6} \mathrm{ord}_p(u^i a_{i,p})$. Laat n_p^{-1} de inverse van n_p zijn modulo p^{β_p}. Wegens de Chinese reststelling bestaat er een $r \in \mathbb{Z}$ zodanig dat $r \equiv p^{d_p} m_p n_p^{-1} \mod p^{\beta_p}$ voor alle $p \mid \Delta$. Er volgt $n_p r - p^{d_p} m_p \equiv 0 \mod p^{\beta_p}$ en dus $\mathrm{ord}_p(r - r_p) = \mathrm{ord}_p(n_p r - p^{d_p} m_p) \geq \beta_p$. Analoog kunnen we $s, t \in \mathbb{Z}$ vinden met $\mathrm{ord}_p(s - s_p) \geq \beta_p$ en $\mathrm{ord}_p(t - t_p) \geq \beta_p$ voor alle $p \mid \Delta$. We bekijken nu de toegelaten coördinaattransformatie gedefinieerd door u, r, s en t (als in 2.11). Laat Δ' de discriminant van de nieuwe Weierstrass-vergelijking zijn. Voor elk priemgetal $p \mid \Delta$ hebben we

$$\begin{aligned}\mathrm{ord}_p(\Delta') &= \mathrm{ord}_p(\Delta u^{-12}) = \mathrm{ord}_p(\Delta) + \mathrm{ord}_p(u^{-12}) \\ &= \mathrm{ord}_p(\Delta) - 12\,\mathrm{ord}_p(u) = \mathrm{ord}_p(\Delta) - 12\alpha_p = \mathrm{ord}_p(\Delta_p).\end{aligned}$$

We concluderen dat de nieuwe Weierstrass-vergelijking p-minimaal is voor alle priemgetallen p. Het resteert te bewijzen dat de nieuwe Weierstrass-vergelijking coëfficiënten in $\mathbb{Z}$ heeft. Laat a_i' de coëfficiënten van de nieuwe Weierstrass-vergelijking zijn. Na wat uitschrijfwerk kunnen we vergelijking voor a_i' in termen van $a_1, a_2, a_3, a_4, a_6, u, r, s, t$ vinden. Merk op dat een rationaal getal $a \in \mathbb{Q}$ geheel is als er geldt $\mathrm{ord}_p(a) \geq 0$ voor alle priemgetallen p. Met behulp van de verkregen vergelijkingen voor a_i' kunnen we nu checken dat er inderdaad geldt $\mathrm{ord}_p(a_i') \geq 0$ voor alle p. We zullen het hier alleen helemaal uitwerken voor $i = 2$. Zij p een priemgetal, we hebben

$$\begin{aligned}\mathrm{ord}_p(u^2 a_2') &= \mathrm{ord}_p(a_2 - s a_1 + 3r - s^2) \\ &= \mathrm{ord}_p((a_2 - s_p a_1 + 3r_p - s_p^2) + (s_p - s)a_1 + 3(r - r_p) + s^2 - s_p^2) \\ &= \mathrm{ord}_p(u_p^2 a_{2,p} - (s - s_p)a_1 + 3(r - r_p) + (s - s_p)(s + s_p)) \\ &\geq \min\{\mathrm{ord}_p(u_p^2 a_{2,p}), \mathrm{ord}_p((s - s_p)a_1), \mathrm{ord}_p(3(r - r_p)), \mathrm{ord}_p((s - s_p)(s + s_p))\} \\ &\geq \min\{\mathrm{ord}_p(u_p^2 a_{2,p}), \beta_p\} \\ &= \mathrm{ord}_p(u_p^2 a_{2,p}).\end{aligned}$$

[1] Voor een priemgetal p en een geheel getal $a \in \mathbb{Z} \setminus \{0\}$ is $\mathrm{ord}_p(a)$ de maximale $m \in \mathbb{N}$ zodanig dat $p^m \mid a$. Voor een rationaal getal $a = x/y$ met $x, y \in \mathbb{Z}$ definiëren we $\mathrm{ord}_p(a) = \mathrm{ord}_p(x) - \mathrm{ord}_p(y)$.

Er geldt $\mathrm{ord}_p(u^2) = \mathrm{ord}_p(u_p^2)$ en dus $\mathrm{ord}_p(a_2') \geq \mathrm{ord}_p(a_{2,p}) \geq 0$. □

We definiëren de reductie modulo p van E dus als de kromme $\tilde{E}_p$ over $\mathbb{F}_p$ gedefinieerd door de reductie van een minimale Weierstrass-vergelijking voor p.

Definitie 2.24. Zij $E/\mathbb{Q}$ een elliptische kromme. Zij p een priemgetal. We zeggen dat E *goede reductie* modulo p heeft als $\tilde{E}_p$ een elliptische kromme is. Is $\tilde{E}_p$ geen elliptische kromme, dan heeft E *slechte reductie* modulo p.

Nu hebben we wel de volgende methode om te bepalen of E een goede reductie modulo p heeft.

Opmerking 2.25. Een elliptische kromme $E/\mathbb{Q}$ heeft een goede reductie modulo een priemgetal p dan en slechts dan als p de minimale discriminant van E deelt. Merk op dat hier meteen uit volgt dat er maar eindig veel priemen p zijn waarbij E slechte reductie heeft.

De L-functie van een elliptische kromme $E/\mathbb{Q}$, die we in de volgende paragraaf zullen bespreken, bevat informatie over de reductie van E bij alle priemgetallen p. Deze informatie is bevat in getallen die we zullen noteren met a_p.

Definitie 2.26. Zij $E/\mathbb{Q}$ een elliptische kromme en p een priemgetal. We definiëren

$$a_p = p + 1 - \#\tilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p).$$

Hierbij is $\tilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)$ de verzameling van alle niet-singuliere $\mathbb{F}_p$-rationale punten op $\tilde{E}_p$.

2.6 L-functies van elliptische krommen

Het vermoeden van Birch en Swinnerton-Dyer heeft betrekking tot de L-functie van een elliptische kromme. In deze pargraaf zullen we dit begrip definiëren. Een L-functie is een bepaald Eulerproduct. Zij $f : D \to \mathbb{C}$ met $D \subseteq \mathbb{C}$ open een holomorfe functie die we op z'n domein kunnen schrijven als

$$f(s) = \prod_{p \text{ priem}} \frac{1}{f_p(p^{-s})} \tag{2.4}$$

met $f_p \in \mathbb{C}[T]$ een polynoom met staartcoëfficiënt 1 voor alle priemgetallen p. De uitdrukking aan de rechterkant van (2.4) noemen we een *Euler product*.

Voor de complexe variabele s gebruiken we traditiegetrouw $\mathrm{Re}(s) = \sigma$ en $\mathrm{Im}(s) = t$. Het meest bekende voorbeeld van een Eulerproduct is de Riemann-zetafunctie. De Riemann-zetafunctie is gedefinieerd door $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Merk op dat er voor alle $\delta > 1$ geldt $|n^{-s}| = n^{-\sigma} \leq n^{-\delta}$ en de som $\sum_{n=1}^{\infty} n^{-s}$ convergeert dus absoluut en uniform in het rechterhalfvlak $\{z \in \mathbb{C} : \mathrm{Re}(z) \geq \delta\} \subseteq \mathbb{C}$. We concluderen dat ζ een holomorfe functie $\{z \in \mathbb{C} : \mathrm{Re}(z) > 1\} \to \mathbb{C}$ is. Euler liet zien dat de Riemann-zetafunctie op z'n domein gelijk is aan het Eulerproduct

$$\prod_{p \text{ priem}} \frac{1}{1 - p^{-s}}.$$

Definitie 2.27. De *L-functie* van een elliptische kromme $E/\mathbb{Q}$ is gedefinieerd als het Eulerproduct

$$L(E, s) = \prod_{p \text{ priem}} \left(1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}\right)^{-1}$$

met a_p als in definitie 2.26, $s \in \mathbb{C}$ en

$$\varepsilon(p) = \begin{cases} 1 & E \text{ heeft een goede reductie modulo } p \\ 0 & E \text{ heeft een slechte reductie modulo } p. \end{cases}$$

De L-functie van een elliptische kromme convergeert absoluut en uniform in het rechterhalfvlak van $\mathbb{C}$ gedefinieerd door $\sigma > 3/2$ en is dus een holomorfe functie $\{z \in \mathbb{C} : \mathrm{Re}(z) > 3/2\} \to \mathbb{C}$. Het bewijs hiervan maakt gebruik van de stelling van Hasse.

Stelling 2.28 (Hasse)**.** *Zij $E/\mathbb{Q}$ een elliptische kromme en a_p als in definitie 2.26. Voor alle priemgetallen p geldt*

$$|a_p| \leq 2\sqrt{p}.$$

Bewijs. [7, p. 138]. □

Propositie 2.29. *De L-functie van een elliptische kromme $E/\mathbb{Q}$ convergeert absoluut en uniform in het rechterhalfvlak $\{z \in \mathbb{C} : \mathrm{Re}(z) > \delta\}$ voor alle $\delta > 3/2$.*

Bewijs. Zij $\delta > 3/2$, $s \in \{z \in \mathbb{C} : \mathrm{Re}(z) > \delta\}$ en p een priemgetal. Beschouw het polynoom $f_p := 1 - a_p T + pT^2 \in \mathbb{C}[T]$ en laat $\alpha_p, \beta_p \in \mathbb{C}$ de inversen van de nulpunten van f_p zijn. Dus $f_p = (1 - \alpha_p T)(1 - \beta_p T)$. De discriminant van f_p is gelijk aan $d = a_p^2 - 4p$. Uit de Stelling van Hasse volgt $d \leq 0$. Als er geldt $d = 0$, dan hebben we $a_p^2 = 4p$ en er volgt dat p een kwadraat is. Dit is in tegenspraak met het feit dat p een priemgetal is en er volgt $d < 0$. Het polynoom f_p heeft dus twee complexe nulpunten die elkaars geconjungeerde zijn en er geldt $\alpha_p = \overline{\beta_p}$. Er volgt $|\alpha_p| = |\beta_p|$ en omdat $\alpha_p \beta_p = p$ concluderen we $|\alpha_p| = |\beta_p| = p^{1/2}$.

Merk op dat er geldt $|1 - \alpha_p p^{-s}| \geq 1 - |\alpha_p p^{-s}| = 1 - p^{1/2-\sigma}$. Er volgt

$$\frac{1}{|1 - \alpha_p p^{-s}|} \leq \frac{1}{1 - p^{1/2-\sigma}} \leq \frac{1}{1 - p^{1/2-\delta}}.$$

We hebben hetzelfde voor β_p en concluderen

$$\frac{1}{|1 - a_p p^{-s} + p^{1-2s}|} = \frac{1}{|(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})|} \leq \frac{1}{(1 - p^{1/2-\sigma})^2} \leq \frac{1}{(1 - p^{1/2-\delta})}.$$

Nu vinden we

$$\begin{aligned} |L(E,s)| &= \prod_p \frac{1}{|1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}|} \\ &= \prod_{p \text{ slecht}} \frac{1}{|1 - a_p p^{-s}|} \prod_{p \text{ goed}} \frac{1}{|1 - a_p p^{-s} + p^{1-2s}|} \\ &\leq \prod_{p \text{ slecht}} \frac{1}{1 - p^{1/2-\delta}} \prod_{p \text{ goed}} \frac{1}{(1 - p^{1/2-\delta})^2} \\ &= \prod_{p \text{ slecht}} \frac{(1 - p^{1/2-\delta})^2}{1 - p^{1/2-\delta}} \prod_p \frac{1}{(1 - p^{1/2-\delta})^2} \\ &= \left(\prod_{p \text{ slecht}} \frac{1}{1 - p^{1/2-\delta}} \right) \zeta(\delta - 1/2)^2 \end{aligned}$$

Het eerste product is eindig en convergeert dus altijd. We weten dat de Riemann-zetafunctie absoluut en uniform convergeert op het rechterhalfvlak gedefinieerd door $\sigma > 1$ en $\zeta(\delta - 1/2)$ convergeert dus absoluut en uniform voor $\delta > 3/2$. We concluderen dat $L(E,s)$ absoluut en uniform convergeert in het rechterhalfvlak $\{z \in \mathbb{C} : \mathrm{Re}(z) > \delta\}$. □

2.7 Het vermoeden van Birch en Swinnerton-Dyer

Het zwakke vermoeden van Birch en Swinnerton-Dyer stelt dat de algebraïsche rang van een elliptische kromme $E/\mathbb{Q}$ gelijk is aan de analytische rang van E.

Definitie 2.30. Zij $E/\mathbb{Q}$ een elliptische kromme. De *analytische rang* van E is de verdwijnorde[2] van $L(E,s)$ in het punt $s=1$.

Het vermoeden van Birch en Swinnerton-Dyer doet dus een uitspraak over de L-functie van E in het punt $s=1$. Stelling 2.29 geeft dat $L(E,s)$ een holomorfe functie $\{z \in \mathbb{C} : \mathrm{Re}(z) > 3/2\} \to \mathbb{C}$ is en $L(E,s)$ is dus nog niet gedefinieerd in het punt $s=1$. Het feit dat de L-functie van een elliptische kromme analytisch kan worden voortgezet tot het gehele complexe vlak is een gevolg van de modulariteitsstelling. Deze stelling werd in 2001 volledig bewezen. De eerste versie van deze stelling, een specifiek geval van de stelling zoals die nu bekend is, werd in 1995 bewezen door Andrew Wiles die daarmee een bewijs gaf voor de laatste stelling van Fermat. Nu we weten dat de L-functie van een elliptische kromme in het punt $s=1$ is gedefinieerd, kunnen we het (zwakke) vermoeden van Birch en Swinnerton-Dyer formuleren. Dit is de versie van het vermoeden van Birch en Swinnerton-Dyer die in 2000 door het Clay Mathematics Institute werd uitgeroepen tot één van de zeven millenniumproblemen, een probleem waarvan het oplossen een prijs van een miljoen dollar oplevert.

Vermoeden 2.31 (Birch en Swinnerton-Dyer)**.** *Zij $E/\mathbb{Q}$ een elliptische kromme. Er geldt*

$$\operatorname*{ord}_{s=1} L(E,s) = \mathrm{rk}(E(\mathbb{Q})).$$

In deze scriptie zullen we het tevens sterke vermoeden van Birch en Swinnerton-Dyer formuleren. Dit vermoeden geeft een uitdrukking voor de leidende term van de L-functie in het punt $s=1$.

Vermoeden 2.32 (Sterke vermoeden van Birch en Swinnerton-Dyer)**.** *Zij $E/\mathbb{Q}$ een elliptische kromme. Er geldt*

(i)

$$\operatorname*{ord}_{s=1} L(E,s) = \mathrm{rk}(E(\mathbb{Q})).$$

(ii)

$$\lim_{s\to 1} L(E,s)(s-1)^{-\mathrm{rk}(E(\mathbb{Q}))} = \frac{\Omega(E)\,\mathrm{Reg}(E)\left(\prod_p c_p\right)\#Ш(E)}{(\#E(\mathbb{Q})^{\mathrm{tor}})^2}. \tag{2.5}$$

In hoofdstuk 4 zullen we term $Ш(E)$ in (2.5) bespreken; de Tate-Shafarevich-groep. De regulator $\mathrm{Reg}(E)$, de Tamagawa getallen c_p en de reële periode $\Omega(E)$ zullen we in hoofdstuk 3 bespreken.

[2]De verdwijnorde van een holomorfe functie $f : D \to \mathbb{C}$ in een punt $s \in D \subseteq \mathbb{C}$ is gelijk aan het getal $m \in \mathbb{N}$ zodanig dat er een holomorfe functie $g : D \to \mathbb{C}$ bestaat met $f(z) = (z-s)^m g(z)$ en $g(s) \neq 0$.

3 Termen in het BSD-vermoeden

In dit hoofdstuk zullen we een groot aantal termen uit het sterke vermoeden van Birch en Swinnerton-Dyer definiëren. De Tate-Shafarevich-groep $Ш(E)$ bewaren we voor hoofdstuk 4. Laat, gedurende het hele hoofdstuk, E een elliptische kromme over $\mathbb{Q}$ zijn.

We beginnen met de definitie van de reële periode. Zoals de naam doet verwachten, bevat $\Omega(E)$ informatie over de $\mathbb{R}$-rationale punten op E.

Definitie 3.1. Zij $E/\mathbb{Q}$ een elliptische kromme gegeven door een minimale Weierstrass-vergelijking. De *reële periode* van E is

$$\Omega(E) = \int_{E(\mathbb{R})} \left| \frac{1}{2y + a_1 x + a_3} \right| \, dx.$$

Propositie 3.2. *De reële periode is welgedefinieerd, i.e. onafhankelijk van de gekozen minimale Weierstrass-vergelijking.*

Bewijs. Laat $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ en $a_1', a_2', a_3', a_4', a_6' \in \mathbb{Z}$ de coëfficiënten van twee minimale Weierstrass-vergelijking voor E zijn. Propositie 2.11 geeft dat de twee vergelijkingen uit elkaar verkregen kunnen worden met een toegelaten coördinatentransformatie. Merk op dat de twee discriminanten Δ en Δ' beide p-minimaal zijn voor alle priemgetallen p en er moet dus gelden $\Delta = \Delta'$. We hebben $\Delta = u^{12}\Delta'$ en er volgt $u = 1$. Uitschrijfwerk levert nu op

$$\frac{dx}{2y + a_1 x + a_3} = \frac{dx'}{u(2y' + a_1' x' + a_3)} = \frac{dx'}{2y' + a_1' x' + a_3}.$$

□

3.1 De regulator

Zij $E/\mathbb{Q}$ een elliptische kromme van rang n en $\{P_1, ..., P_n\}$ een $\mathbb{Z}$-basis voor $E(\mathbb{Q})/E(\mathbb{Q})^{\text{tor}}$. De regulator $\text{Reg}(E)$ van E is gedefinieerd als de determinant van de matrix $(\langle P_i, P_j \rangle_{NT})_{i,j}$ waarbij $\langle ., . \rangle_{NT}$ de *Néron-Tate paring* is op $E(\mathbb{Q})/E(\mathbb{Q})^{\text{tor}}$. Deze bilineaire paring is gedefinieerd met behulp van de hoogte functie op $E(\mathbb{Q})$.

Definitie 3.3. Zij $E/\mathbb{Q}$ een elliptische kromme. De *naïeve hoogte* is de afbeelding

$$\begin{aligned} h : E(\mathbb{Q}) &\longrightarrow \mathbb{R} \\ (x : y : 1) &\longmapsto \log \max\{|a|, |b|\} \\ \mathcal{O} &\longmapsto 0 \end{aligned}$$

waarbij $x = a/b$ met $a, b \in \mathbb{Z}$ copriem.

De naïeve hoogte heeft twee belangrijke eigenschappen. De bewijzen van deze eigenschappen vereisen veel uitschrijf- en rekenwerk en zullen we hier niet geven.

Lemma 3.4. *Zij $E/\mathbb{Q}$ een elliptische kromme. Er bestaat een $c_1 \in \mathbb{R}$ zodanig dat (3.1) voor alle $P \in E(\mathbb{Q})$ geldt. Tevens bestaat er een $c_2 \in \mathbb{R}$ zodanig dat (3.2) geldt voor alle $P, Q \in E(\mathbb{Q})$.*

$$|h(2P) - 4h(P)| \leq c_1 \tag{3.1}$$

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + c_2 \tag{3.2}$$

Bewijs. Voor (3.1) zie [5, p. 95]. Voor (3.2) zie [7, p.235]. □

We zeggen dat een functie f van een abelse groep A naar $\mathbb{R}$ aan de parallellogram-wet voldoet als er geldt $f(x+y)+f(x-y)=2f(x)+2f(y)$ voor alle $x,y\in A$. Functies $A\to\mathbb{R}$ die aan deze wet voldoen induceren bilineaire vormen $A\times A\to\mathbb{R}$. Een bewijs van dit feit is ingesloten in het bewijs van propositie 3.8. Lemma 3.4 geeft dat de naïeve hoogte op $E(\mathbb{Q})$ "bijna" aan de parallellogram-wet voldoet. We definiëren nu de kanonieke hoogte op E.

Definitie 3.5. Zij $E/\mathbb{Q}$ een elliptische kromme. De *kanonieke hoogte* op E is de afbeelding

$$\begin{aligned}\hat{h}: E(\mathbb{Q}) &\longrightarrow \mathbb{R}\\ P &\longmapsto \lim_{n\to\infty}\frac{h(2^nP)}{4^n}.\end{aligned}$$

Stelling 3.6. *De kanonieke hoogte op een elliptische kromme $E/\mathbb{Q}$ is welgedefinieerd.*

Bewijs. We moeten bewijzen dat de limiet $\lim_{n\to\infty}4^{-n}h(2^nP)$ bestaat voor alle $P\in E(\mathbb{Q})$. We zullen dit doen door aan te tonen dat het rijtje $\{4^{-n}h(2^nP)\}_{n=0}^{\infty}$ Cauchy is voor alle $P\in E(\mathbb{Q})$. Lemma 3.4 geeft dat er een constante $c\in\mathbb{R}$ bestaat met $|h(2P)-4h(P)|\leq c$. Zij $N>M\geq 0$. We vinden

$$\begin{aligned}|4^{-N}h(2^NP)-4^{-M}h(2^MP)| &= \left|\sum_{i=M}^{N-1}\left(4^{-(i+1)}h(2^{i+1}P)-4^{-i}h(2^iP)\right)\right|\\ &= \left|\sum_{i=M}^{N-1}4^{-i-1}\left(h(2^{i+1}P)-4h(2^iP)\right)\right|\\ &\leq \left|\sum_{i=M}^{N-1}4^{-i-1}c\right|\\ &\leq c\sum_{i=M}^{N-1}4^{-i-1}\\ &\leq c4^{-M}.\end{aligned}$$

En dus $|4^{-N}h(2^NP)-4^{-M}h(2^MP)|\to 0$ als $M\to\infty$. We concluderen dat $\{4^{-n}h(2^nP)\}_{n=0}^{\infty}$ een Cauchy-rijtje is en dus convergeert. □

De kanonieke hoogte op $E(\mathbb{Q})$ geeft aanleiding tot de volgende definitie.

Definitie 3.7. Zij $E/\mathbb{Q}$ een elliptische kromme. De *Néron-Tate-paring* op E is de bilineaire paring

$$\begin{aligned}\langle .,.\rangle_{\mathrm{NT}}: E(\mathbb{Q})\times E(\mathbb{Q}) &\longrightarrow \mathbb{R}\\ (P,Q) &\longmapsto \langle P,Q\rangle_{\mathrm{NT}}=\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).\end{aligned}$$

Propositie 3.8. *De Néron-Tate-paring is bilineair.*

Bewijs. Zij $n\in\mathbb{N}$. Lemma 3.4 geeft dat er een $c_n\in\mathbb{R}$ bestaat met

$$h(2^nP+2^nQ)+h(2^nP-2^nQ)=2h(2^nP)+2h(2^nQ)+c_n.$$

Delen door 4^n en de de limiet $n\to\infty$ nemen, geeft

$$\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q)+\lim_{n\to\infty}\frac{c_n}{4^n}=2\hat{h}(P)+2\hat{h}(Q). \tag{3.3}$$

Merk op dat er geldt $\hat{h}(\mathcal{O}) = 0$ en met (3.3) vinden we $\hat{h}(-Q) = \hat{h}(Q)$ voor alle $Q \in E(\mathbb{Q})$. Veelvuldig van deze identiteit en (3.3) gebruik maken, geeft de vier vergelijkingen

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

Nemen we de alternerende som van deze vergelijkingen dan vinden we

$$\hat{h}(P+Q+R) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(Q+R) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R) = 0. \tag{3.4}$$

De linkerkant van (3.4) is gelijk aan $\langle P+R, Q\rangle_{\mathrm{NT}} - \langle P, Q\rangle_{\mathrm{NT}} - \langle R, Q\rangle_{\mathrm{NT}}$. We concluderen $\langle P+R, Q\rangle_{\mathrm{NT}} = \langle P, Q\rangle_{\mathrm{NT}} + \langle R, Q\rangle_{\mathrm{NT}}$ en $\langle ., .\rangle_{\mathrm{NT}}$ is dus bilineair. □

Nu we de Néron-Tate-paring op $E(\mathbb{Q})$ hebben gedefinieerd, kunnen we bijna de regulator van een elliptische kromme definiëren. Het rest op te merken dat de Néron-Tate-paring een bilineaire paring op $E(\mathbb{Q})/E(\mathbb{Q})^{\mathrm{tor}}$ induceert. Immers, zij $P \in E(\mathbb{Q})$ en $Q \in E(\mathbb{Q})^{\mathrm{tor}}$ met $nQ = \mathcal{O}$. Er geldt

$$\langle P, Q\rangle_{\mathrm{NT}} = \frac{1}{n}\langle P, nQ\rangle_{\mathrm{NT}} = \frac{1}{n}\langle P, \mathcal{O}\rangle_{\mathrm{NT}} = \frac{1}{n}\left(\hat{h}(P+\mathcal{O}) - \hat{h}(P) - \hat{h}(\mathcal{O})\right) = 0.$$

Als $P, R \in E(\mathbb{Q})$ en $Q \in E(\mathbb{Q})^{\mathrm{tor}}$, dan geldt er dus $\langle P+Q, R\rangle_{\mathrm{NT}} = \langle P, R\rangle_{\mathrm{NT}} + \langle Q, R\rangle_{\mathrm{NT}} = \langle P, R\rangle_{\mathrm{NT}}$ en we concluderen dat $\langle ., .\rangle_{\mathrm{NT}}$ inderdaad een bilineaire paring op $E(\mathbb{Q})/E(\mathbb{Q})^{\mathrm{tor}}$ induceert. Deze paring zullen we tevens noteren met $\langle ., .\rangle_{\mathrm{NT}}$.

Definitie 3.9. Zij $E/\mathbb{Q}$ een elliptische kromme. Zij $\{P_1, ..., P_r\}$ een basis voor $E(\mathbb{Q})/(E(\mathbb{Q}))^{\mathrm{tor}}$ met $r = \mathrm{rk}(E(\mathbb{Q}))$. De regulator van E is

$$\mathrm{Reg}(E) = \det\left((\langle P_i, P_j\rangle_{\mathrm{NT}})_{i,j}\right)$$

Dat de regulator welgedefinieerd is, volgt uit de volgende propositie.

Propositie 3.10. *Zij A een vrije abelse groep van rang r en $f : A \times A \to \mathbb{R}$ een bilineaire paring. Zij $S = \{s_1, ..., s_r\}$ en $T = \{t_1, ..., t_r\}$ twee $\mathbb{Z}$-bases voor A. Er geldt* $\det((f(s_i, s_j))_{i,j}) = \det((f(t_i, t_j))_{i,j})$.

Bewijs. Laat $M = (f(s_i, s_j))_{i,j}$ en $N = (f(t_i, t_j))_{i,j}$. Het is makkelijk te zien dat voor $x = \sum_{i=1}^r x_i s_i \in A$ en $y = \sum_{i=0}^r y_i s_i \in A$ geldt $f(x, y) = (x_1, ..., x_r)M(y_1, ..., y_r)^\top$. Zij P een basistransformatiematrix van S naar T. Zij $x = \sum_{i=1}^r x_i s_i = \sum_{i=1}^r x_i' t_i \in A$ en $y = \sum_{i=1}^r y_i t_i = \sum_{i=1}^r y_i' t_i \in A$. We vinden

$$\begin{aligned}
(x_1, ..., x_r)M(y_1, ..., y_r)^\top &= (x_1', ..., x_r')N(y_1', ..., y_r')^\top \\
&= P(x_1, ..., x_r)^\top NP(y_1, ..., y_r)^\top \\
&= (x_1, ..., x_r)P^\top NP(y_1, ..., y_r)^\top.
\end{aligned}$$

Dus $M = P^\top NP$. De matrix P is een basistransformatiematrix en dus inverteerbaar. Een inverteerbare matrix met coëfficiënten in $\mathbb{Z}$ heeft determinant ± 1 en we concluderen $\det(M) = \det(P)^2 \det(N) = \det(N)$. □

3.2 De Tamagawa-getallen

Het Tamagawa-getal c_p waarbij p een priemgetal is, bevat informatie over de p-adische punten op E. We zullen beginnen met het beschrijven van de reductie afbeelding $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$. We brengen hiertoe de volgende propositie over p-adische getallen in herinnering.

Propositie 3.11. *Zij p een priemgetal. Elk p-adisch getal $\alpha \in \mathbb{Q}_p$ kunnen we op een unieke manier schrijven als*

$$\alpha = \sum_{i=-n}^{\infty} \alpha_i p^i$$

met $0 \leq \alpha_i \leq p-1$ en $n \in \mathbb{N}$ waarbij n afhankelijk is van α. Tevens geldt er $\alpha \in \mathbb{Z}_p$ dan en slechts dan als $n = 0$

Bewijs. Als we de theorie over p-adische getallen opbouwen door de p-adische gehelen te definiëren als de projectieve limiet van het systeem $(\mathbb{Z}/p^n\mathbb{Z})_{n=1}^{\infty}$ met voor alle $n \leq m$ de afbeelding $a \mod p^m \mapsto a \mod p^n$ (voor de definitie van een projectieve limiet en een projectief systeem, zie [10, p. 102]) en $\mathbb{Q}_p$ te definiëren als $\kappa(\mathbb{Z}_p)$, dan is de uitspraak triviaal. Als we de de theorie over p-adische getallen opbouwen met equivalentieklassen van Cauchy-rijtjes met respect tot de p-adische norm, dan kan een bewijs worden gevonden in [4, p. 67, 68]. □

Als α een p-adisch getal is, kunnen we dus met een geschikte macht van p vermenigvuldigen om een element uit $\mathbb{Z}_p$ te krijgen. Elementen uit $\mathbb{Z}_p$ hebben een natuurlijke reductie modulo p; als $\alpha = \sum_{i=0}^{\infty} \alpha_i p^i$ een p-adisch geheel getal is, is de reductie modulo p van α gelijk aan α_0. Zij $(x_1 : x_2 : x_3)$ nu een punt uit het projectieve vlak over $\mathbb{Q}_p$. Zij m het minimale natuurlijke getal zodanig dat $p^{m_i} x_i$ allen in $\mathbb{Z}_p$ liggen. Er geldt $(x_1 : x_2 : x_3) = (p^m x_1 : p^m x_2 : p^m x_3)$ en we hebben een representant van $(x_1 : x_2 : x_3)$ gevonden met coördinaten in $\mathbb{Z}_p$. Merk op dat er voor minstens één i geldt $p^m x_i \in \mathbb{Z}_p^{\times}$ en er bestaat dus minstens één i zodanig dat $p^m x_i$ niet gelijk is aan 0 modulo p. We krijgen de afbeelding

$$\begin{aligned} \mathbb{P}^2(\mathbb{Q}_p) &\longrightarrow \mathbb{P}^2(\mathbb{F}_p) \\ (x : y : z) &\longmapsto (x_0 : y_0 : z_0) \end{aligned}$$

waarbij $x, y, z \in \mathbb{Z}_p$ met $x = \sum_{i=0}^{\infty} x_i p^i$, $y = \sum_{i=0}^{\infty} y_i p^i$, $z = \sum_{i=0}^{\infty} z_i p^i$. Voor een punt $P \in \mathbb{P}^2(\mathbb{Q}_p)$ noteren we de reductie modulo p als $\tilde{P}$.

Als $\tilde{E}_p$ de reductie modulo p van E is als in paragraaf 2.5 en P is een $\mathbb{Q}_p$-rationaal punt op E, dan is $\tilde{P}$ een punt op $\tilde{E}_p$. We hebben dus een geïnduceerde afbeelding

$$\begin{aligned} \Phi : E(\mathbb{Q}_p) &\longrightarrow \tilde{E}_p(\mathbb{F}_p) \\ P &\longmapsto \tilde{P}. \end{aligned}$$

Voor de Tamagawa-getallen speelt de deelverzameling van $E(\mathbb{Q}_p)$ een rol die bestaat uit alle punten die door de reductie afbeelding naar een niet-singulier punt van $\tilde{E}_p$ worden gestuurd. Deze verzameling is een ondergroep van $E(\mathbb{Q}_p)$.

Definitie 3.12. Zij $E/\mathbb{Q}$ een elliptische kromme en p een priemgetal. We definiëren de verzameling

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \Phi(P) \in \tilde{E}_p^{\mathrm{ns}}(\mathbb{F}_p)\}.$$

Propositie 3.13. *Zij p een priemgetal, $E/\mathbb{Q}_p$ een elliptische kromme en $L/\mathbb{Q}_p$ een lijn. Als er geldt dat P_1, P_2, P_3 de niet noodzakelijk verschillende snijpunten van L en E zijn, dan zijn $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ de niet noodzakelijk verschillende snijpunten van $\tilde{E}_p$ en $\tilde{L}_p$.*

Bewijs. Laat $P_i = (a_1^i : a_2^i : a_3^i)$. Zonder verlies van algemeenheid mogen we stellen dat $a_j^i \in \mathbb{Z}_p$ voor alle $i, j \in I := \{1, 2, 3\}$ en dat er voor alle $i \in I$ een $j \in I$ is met $a_j^i \in \mathbb{Z}_p^{\times}$. Zij L gegeven door $\alpha X + \beta Y + \gamma Z = 0$ en stel ook hier zonder verlies van algemeenheid dat

α, β, γ elementen zijn van $\mathbb{Z}_p$ en dat $\gamma \in \mathbb{Z}_p^\times$. Voor alle $i \in I$ hebben we $\alpha a_1^i + \beta a_2^i + \gamma a_3^i = 0$ en dus $\tilde{\alpha}\tilde{a}_1^i + \tilde{\beta}\tilde{a}_2^i + \tilde{\gamma}\tilde{a}_3^i = 0$. Als er geldt $\tilde{a}_1^i = \tilde{a}_2^i = 0$ dan impliceert $\tilde{\gamma} \neq 0$ dat er tevens geldt $\tilde{a}_3^i = 0$ en we vinden een tegenspraak met het feit dat er een $j \in I$ bestaat met $a_j^i \in \mathbb{Z}_p^\times$. Voor alle $i \in I$ hebben we dus $\neg\left(\tilde{a}_1^i = \tilde{a}_2^i = 0\right)$. Zij $F \in \mathbb{Q}_p[X, Y, Z]$ het homogene polynoom dat E definieert. Voor alle $i \in I$ geldt $F(a_1^i, a_2^i, -\gamma^{-1}\alpha a_1^i - \gamma^{-1}\beta a_2^i) = 0$ en propositie 2.17 geeft

$$F(X, Y, -\gamma^{-1}\alpha X - \gamma^{-1}\beta Y) = c(a_2^1 X - a_1^1 Y)(a_2^2 X - a_1^2 Y)(a_2^3 X - a_1^3 Y) \tag{3.5}$$

voor zekere $c \in \mathbb{Z}_p^\times$. De snijpunten van $\tilde{E}_p$ en $\tilde{L}_p$ zijn duidelijk de nulpunten van de reductie van het polynoom $F(X, Y, -\gamma^{-1}\alpha X - \gamma^{-1}\beta Y)$ modulo p en omdat er voor alle i geldt $(\tilde{a}_1^i, \tilde{a}_2^i) \neq (0, 0)$, kunnen we met (3.5) duidelijk zien dat $(\tilde{a}_1^i, \tilde{a}_2^i)$ nulpunten zijn. We concluderen dat $(\tilde{a}_1^i : \tilde{a}_2^i : \tilde{a}_3^i) = \tilde{P}_i$ een snijpunt is van $\tilde{E}_p$ en $\tilde{L}_p$ voor alle $i \in I$. □

Gevolg 3.14. *Zij $E/\mathbb{Q}$ een elliptische kromme en p een priemgetal. De verzameling $E_0(\mathbb{Q}_p)$ is een ondergroep van $E(\mathbb{Q}_p)$.*

Bewijs. Merk allereerst op dat de reductie van $\mathcal{O} = (0 : 1 : 0)$ gelijk is aan $(0 : 1 : 0)$ voor elk priemgetal p en het eenheidselement van $E(\mathbb{Q}_p)$ zit dus zeker in $E_0(\mathbb{Q}_p)$. Zij $P, Q \in E_0(\mathbb{Q}_p)$. Zij $L/\mathbb{Q}_p$ de lijn door P en Q. Het derde snijpunt van $\tilde{L}_p$ en $\tilde{E}_p$ is wegens propositie 3.13 gelijk aan $\widetilde{P * Q}$. Als er geldt $\widetilde{P * Q} \neq \tilde{P}, \tilde{Q}$, dan moet $\widetilde{P * Q}$ wel een snijpunt van $\tilde{L}_p$ en $\tilde{E}_p$ met multipliciteit 1 zijn en dus een niet-singulier punt van $\tilde{E}_p$. Als $\widetilde{P * Q}$ gelijk is aan minstens één van de punten $\tilde{P}, \tilde{Q}$, dan is $\widetilde{P * Q}$ niet-singulier. Immers, $P, Q \in E_0(\mathbb{Q}_p)$. We concluderen $P * Q \in E_0(\mathbb{Q}_p)$. Er volgt nu $P + Q = (P * Q) * \mathcal{O} \in E_0(\mathbb{Q}_p)$. In het bewijs van 2.21 hebben we laten zien dat $-P = P * \mathcal{O}$ en er geldt dus ook $P \in E_0(\mathbb{Q}_p) \implies -P \in E_0(\mathbb{Q}_p)$. □

Het Tamagawa-getal c_p is nu gedefinieerd als de index van $E_0(\mathbb{Q}_p)$ in $E(\mathbb{Q}_p)$. De term die in het vermoeden van Birch en Swinnerton-Dyer voor komt is $\prod_{p \text{ priem}} c_p$ en het is dus noodzakelijk dat dit product convergeert. We merken op dat als E goede reductie modulo p heeft, er geldt $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$ en dus $c_p = 1$. Er zijn maar eindig veel priemgetallen waarvoor E slechte reductie heeft en als voor deze priemen geldt dat de index $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ eindig is, convergeert het product. In het bewijs van het feit dat $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ eindig is, maken we gebruik van de compactheid van $\mathbb{P}^2(\mathbb{Q}_p)$.

Lemma 3.15. *Zij p een priemgetal. Het projectieve vlak $\mathbb{P}^2(\mathbb{Q}_p)$ is compact.*

Bewijs. De quotiëntafbeelding $\pi : \mathbb{Q}_p^3 \setminus \{0\} \to \mathbb{P}^2(\mathbb{Q}_p)$ is continu. Merk op dat

$$\pi(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p^\times) \cup \pi(\mathbb{Z}_p \times \mathbb{Z}_p^\times \times \mathbb{Z}_p) \cup \pi(\mathbb{Z}_p^\times \times \mathbb{Z}_p \times \mathbb{Z}_p) = \mathbb{P}^2(\mathbb{Q}_p).$$

Bewijzen we dat $\mathbb{Z}_p$ en $\mathbb{Z}_p^\times$ compact zijn, dan geeft de stelling van Tychonoff het gewenste resultaat. De verzameling $\mathbb{Z}_p$ is de projectieve limiet $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, i.e. de deelverzameling

$$\{(a_n)_{n=1}^\infty \in \prod_n \mathbb{Z}/p^n\mathbb{Z} : a_n \equiv a_{n-1} \mod p^{n-1} \text{ voor alle } n \geq 2\} \subseteq \prod_n \mathbb{Z}/p^n\mathbb{Z}.$$

De verzameling $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ is wegens de stelling van Tychonoff compact als product van compacte verzamelingen. We zullen bewijzen dat $\mathbb{Z}_p$ gesloten is in $\prod_n \mathbb{Z}/p^n\mathbb{Z}$. Laat f_i^j de reductie afbeeldingen $\mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ zijn en merk op dat de grafieken $G_{i,j}$ van f_i^j gesloten zijn in $\mathbb{Z}/p^j\mathbb{Z} \times \mathbb{Z}/p^i\mathbb{Z}$. Definieer nu $C_n := G_{n,n+1} \times \prod_{i \neq n,n+1} \mathbb{Z}/p^i\mathbb{Z}$ en merk op dat deze verzameling tevens gesloten is. We hebben $\mathbb{Z}_p = \cap_{n=0}^\infty C_n$ en concluderen dat $\mathbb{Z}_p$ inderdaad gesloten is in $\prod_n \mathbb{Z}/p^n\mathbb{Z}$. We concluderen dat $\mathbb{Z}_p$ compact is en omdat $\mathbb{Z}_p^\times$ gesloten is in $\mathbb{Z}_p$ is het lemma bewezen. □

Stelling 3.16. *Zij $E/\mathbb{Q}$ een elliptische kromme en p een priemgetal. De index $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is eindig.*

Bewijs. Allereerst bewijzen we dat de groep $E(\mathbb{Q}_p)$ gesloten is in $\mathbb{P}^2(\mathbb{Q}_p)$. Zij $(P_n)_{n=1}^{\infty}$ een convergent rijtje in $E(\mathbb{Q}_p)$ met limiet P. Zij $F \in \mathbb{Q}[X, Y, Z]$ het homogene polynoom dat de kromme E definieert. Er geldt $F(P) = F(\lim_{n\to\infty} P_n) = \lim_{n\to\infty} F(P_n) = \lim_{n\to\infty} 0 = 0$ en dus $P \in E(\mathbb{Q}_p)$. Elk convergent rijtje in $E(\mathbb{Q}_p)$ heeft z'n limiet in $E(\mathbb{Q}_p)$ en $E(\mathbb{Q}_p)$ is dus een gesloten deelverzameling van $\mathbb{P}^2(\mathbb{Q}_p)$. Gesloten deelverzamerlingen van compacte ruimtes zijn compact en we concluderen dat $E(\mathbb{Q}_p)$ een compacte ruimte is.
Merk op dat deelverzameling $E_0(\mathbb{Q}_p)$ open is in $E(\mathbb{Q}_p)$. Immers, zij $P \in E_0(\mathbb{Q}_p)$ en ε klein genoeg. Alle punten in de verzameling $U := \{Q \in \mathbb{Q}_p^3 : |P - Q|_p < \varepsilon\}$ hebben dezelfde reductie modulo p als P. Het beeld U' van U in $\mathbb{P}^2(\mathbb{Q}_p)$ is open en de verzameling $U' \cap E(\mathbb{Q}_p)$ is een open deelverzameling van $E(\mathbb{Q}_p)$ die bevat is in $E_0(\mathbb{Q}_p)$. Voor alle $P \in E_0(\mathbb{Q}_p)$ is er een open $U' \subseteq E(\mathbb{Q}_p)$ met $P \in U'$ en $U' \subseteq E_0(\mathbb{Q}_p)$ en we concluderen dat $E_0(\mathbb{Q}_p)$ open is.
Er volgt nu dat de nevenklassen van $E_0(\mathbb{Q}_p)$ in $E(\mathbb{Q}_p)$ open zijn en we hebben dus de open overdekking

$$E(\mathbb{Q}_p) = \bigcup_{P \in E(\mathbb{Q}_p)} P + E_0(\mathbb{Q}_p).$$

Omdat $E(\mathbb{Q}_p)$ compact is, heeft elke open overdekking een eindige deeloverdekking. Er bestaan dus $P_1, ..., P_n \in E(\mathbb{Q}_p)$ zodanig dat $E(\mathbb{Q}_p) = \bigcup_{i=1}^{n} P_i + E_0(\mathbb{Q}_p)$ en we concluderen dat $E_0(\mathbb{Q}_p)$ eindig veel nevenklassen heeft in $E(\mathbb{Q}_p)$. □

Definitie 3.17. Zij $E/\mathbb{Q}$ een elliptische kromme en p een priemgetal. Het *Tamagawa-getal* van E voor p is

$$c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)].$$

4 De Tate-Shafarevich-groep

4.1 De groep $Ш(E)$

In het vorige hoofdstuk hebben we veel van de termen uit het sterke vermoeden van Birch en Swinnerton-Dyer besproken. De regulator van E en de torsie-ondergroep van $E(\mathbb{Q})^{\text{tor}}$ bevatten beide globale informatie over E; informatie over de $\mathbb{Q}$-rationale punten op E. De regulator bevat informatie over het vrije deel van $E(\mathbb{Q})$ en de torsie-ondergroep $E(\mathbb{Q})^{\text{tor}}$ bevat alle $\mathbb{Q}$-rationale punten op E met eindige orde in $E(\mathbb{Q})$. De Tamagawa-getallen en de reële periode van E bevatten lokale informatie over E; informatie over de $\mathbb{Q}_p$-rationale punten op E met p een priemgetal of ∞ en $\mathbb{Q}_\infty := \mathbb{R}$. Voor elk priemgetal p is het Tamagawa-getal c_p de index van een ondergroep van $E(\mathbb{Q}_p)$ en $\Omega(E)$ bevat informatie over alle $\mathbb{R}$-rationale punten op E. In dit hoofdstuk zullen we de Tate-Shafarevich-groep definiëren. Deze groep meet in hoeverre een elliptische kromme niet aan het Hasse-principe te voldoet. We zeggen dat een polynoom, een stelsel polynomen of een klasse van polynomen met bepaalde eigenschappen aan het Hasse-principe voldoet als er geldt dat er lokale niet-triviale oplossingen bestaan dan en slechts dan als er globale niet-triviale oplossingen bestaan. Een algebraïsche kromme (over $\mathbb{Q}$) voldoet aan het Hasse-principe als het $\mathbb{Q}_p$-rationale punten heeft voor alle p dan en slechts dan als het $\mathbb{Q}$-rationale punten heeft, waarbij p een priemgetal is of ∞. De elementen van de Tate-Shafarevich-groep $Ш(E)$ zijn isomorfieklassen van projectieve krommen die over $\overline{\mathbb{Q}}$ isomorf zijn E en $\mathbb{Q}_p$-rationale punten hebben voor alle priemgetallen p en ∞. De groepsstructuur van E komt van een bijectie tussen $Ш(E)$ en een groep uit de Galois cohomologie. Verder kan men laten zien dat een element in $Ш(E)$ triviaal is dan en slechts dan als het aan het Hasse-principe voldoet. De niet-triviale elementen uit de Tate-Shafarevich-groep van E zijn dus isomorfieklassen van projectieve krommen over $\mathbb{Q}$ die over een algebraïsche afsluiting $\overline{\mathbb{Q}}$ isomorf zijn met E en die niet aan het Hasse-principe voldoen. De projectieve krommen hoeven hier niet vlak te zijn en mogen dus in hoger dimensionale projectieve ruimten liggen. In deze scriptie hebben we het begrip van een niet-vlakke projectieve kromme niet geïntroduceerd en tevens zijn we niet ingegaan op wat de morfismen tussen projectieve krommen zijn. Veel van de hier genoemde feiten over de Tate-Shafarevich-groep zullen we in deze scriptie niet bewijzen.

Definitie 4.1. Zij $E/\mathbb{Q}$ een elliptische kromme. De Tate-Shafarevich-groep $Ш(E)$ van E is

$$Ш(E) = \{\text{projectieve krommen } C/\mathbb{Q} : C \text{ heeft } \mathbb{Q}_p\text{-rationale punten voor alle priemgetallen } p \text{ en } \infty \text{ en } C \text{ is over } \overline{\mathbb{Q}} \text{ isomorf met } E\}.$$

In het vermoeden van Birch en Swinnerton-Dyer komt de orde van de Tate-Shafarevich-groep voor en willen we dat het sterke vermoeden van Birch en Swinnerton-Dyer een nuttige uitspraak is, dan moet er dus gelden dat $Ш(E)$ eindig is. Dit is tot op de dag van vandaag niet bewezen.

Vermoeden 4.2. *Zij $E/\mathbb{Q}$ een elliptische kromme. De Tate-Shafarevich-groep $Ш(E)$ is eindig.*

In de rest van dit hoofdstuk zullen we laten zien dat er elliptische krommen over $\mathbb{Q}$ bestaan met niet-triviale Tate-Shafarevich-groep. We moeten dus een elliptische kromme E vinden en een projectieve kromme C zodanig dat C niet aan het Hasse-principe voldoet en isomorf is met E over een algebraïsche afsluiting $\overline{\mathbb{Q}}$. We hebben hiertoe eerst een notie van isomorfe krommen nodig.

4.2 Krommen en functielichamen

Het wordt een stuk eenvoudiger te bepalen of twee projectieve krommen isomorf zijn als we gebruik maken van functielichamen.

Definitie 4.3. Zij K een lichaam. Een functielichaam F over K is een lichaam dat K bevat en voldoet aan

1. F is eindig voortgebracht over K.
2. F heeft transcendentiegraad 1 over K.
3. K is algebraïsch afgesloten in F, i.e. elk element $\alpha \in F$ dat algebraïsch is over K is bevat in K.

Dankzij de volgende stelling kunnen we functielichamen gebruiken om na te gaan of twee niet-singulier projectieve krommen isomorf zijn. De morfismen in de categorie van niet-singulier projectieve krommen worden *dominante morfismen* genoemd.

Stelling 4.4. *De categorie van niet-singuliere projectieve krommen over K met dominante morfismen is equivalent met de categorie van functielichamen over K met K-ringhomomorfismen.*

We zullen hieronder aan tonen hoe we uit een vlakke niet-singuliere projectieve kromme over K een functielichaam over K krijgen.

Definitie 4.5. Zij K een lichaam en C/K een vlakke affiene kromme gedefinieerd door een irreducibel polynoom $f \in K[X,Y]$. Het functielichaam van C definiëren we als $K(C) = \kappa(K[X,Y]/(f))$. Zij C/K een vlakke niet-singuliere projectieve kromme gedefinieerd door een homogeen polynoom $F \in K[X,Y,Z]$. Zij f een dehomogenisatie van F en C' de vlakke affiene kromme gedefinieerd door f. We definiëren het functielichaam van C als $K(C) = K(C')$.

Propositie 4.6. *Zij K een lichaam. Het functielichaam van een irreducibele affiene kromme C/K is inderdaad een functielichaam. Het functielichaam van een projectieve kromme is onafhankelijk van de keuze voor de dehomogenisatie en dus goed gedefinieerd.*

Bewijs. Zij C/K gedefinieerd door $f \in K[X,Y]$ irreducibel. Het is duidelijk dat $K(C)$ aan de voorwaarden 1 en 3 uit definitie 4.3 voldoet. Om in te zien dat $K(C)$ transcendentiegraad 1 over K heeft, merken we op de uitbreiding $K \subseteq K(x)$ transcendentiegraad 1 heeft en dat de uitbreiding $K(x) \subseteq \kappa(K(x)[y]/(f))$ algebraïsch is.

Zij C/K nu een projectieve kromme gegeven door een homogeen polynoom $F \in K[X_1,X_2,X_3]$. Het is duidelijk dat er geldt $K[X_1,X_2,X_3]/(X_1) \cong K[X_1,X_2,X_3]/(X_2) \cong K[X_1,X_2,X_3]/(X_3)$. Stel dat er geldt $F \neq X_i$ voor alle $i = 1,2,3$. De drie affiene delen van F zijn de affiene krommen gedefinieerd door

$$\begin{aligned} f_1 &= F(1, X_2/X_1, X_3/X_1) \in K[X_2/X_1, X_3/X_1] \\ f_2 &= F(X_1/X_2, 1, X_3/X_2) \in K[X_1/X_2, X_3/X_1] \\ f_3 &= F(X_1/X_3, X_2/X_3, 1) \in K[X_1/X_3, X_2/X_3] \end{aligned}$$

De verzameling $A_i := K[X_j/X_i, X_k/X_i]/(f_i)$, met $i,j,k \in \{1,2,3\}$ verschillend, wordt voortgebracht door $\{\frac{x_j}{x_i}, \frac{x_k}{x_i}\}$. Als er geldt $\frac{x_i}{x_j} = 0$ in A_j dan moet er gelden $x_i = 0$ voor alle $(x_1 : x_2 : x_3) \in C_{f_j}$. Er volgt $C_{f_i} = \emptyset$, wat onmogelijk is. We concluderen $x_i/x_j \neq 0$ in A_j en dus $(x_k/x_j)/(x_i/x_j) = x_k/x_i \in \kappa(A_j)$. We concluderen $A_i \subseteq \kappa(A_j)$ en dus $K(C_{f_i}) = \kappa(A_i) \subseteq \kappa(A_j) = K(C_{f_j})$. Wegens symmetrie geldt de omgekeerde inclusie ook en daarmee hebben we het gewenste bewezen. □

Twee niet-singuliere projectieve krommen C_1 en C_2 over een lichaam K_0 zijn nu isomorf als de bijbehorende functielichamen isomorf zijn. Als $K_0 \subseteq K$ een lichaamsuitbreiding is, zeggen we dat C_1 en C_2 isomorf zijn over K als de functielichamen van de krommen, gezien als krommen over K, isomorf zijn.

We geven het volgende voorbeeld.

Propositie 4.7. *De projectieve kromme over $\mathbb{Q}$ waarvan het affiene deel is gegeven door $2y^2 = x^4 - 17$ is over $\overline{\mathbb{Q}}$ isomorf met de elliptische kromme $E/\mathbb{Q}$ gegeven door de Weierstrass-vergelijking $y^2 = x^3 - 17x$.*

Bewijs. Een expliciet isomorfisme tussen $\overline{\mathbb{Q}}[x,y]/(y^2 - x^3 + 17x)$ en $\overline{\mathbb{Q}}[u,v]/(2v^2 - u^4 + 17)$ wordt gegeven door

$$\begin{aligned} \overline{\mathbb{Q}}[x,y]/(y^2 - x^3 + 17x) &\longrightarrow \overline{\mathbb{Q}}[u,v]/(2v^2 - u^4 + 17) \\ x &\longmapsto i\sqrt{-17}\frac{u + \sqrt[4]{17}}{u - \sqrt[4]{17}} \\ y &\longmapsto \frac{\sqrt{68}\sqrt{i}\sqrt[4]{-17}v}{(u - \sqrt[4]{17})^2}. \end{aligned}$$

□

4.3 Het Hasse-principe

Het is niet meteen duidelijk dat er elliptische krommen over $\mathbb{Q}$ bestaan waarvan de Tate-Shafarevich-groep niet triviaal is. In deze paragraaf zullen we een voorbeeld geven. Het gaat om de projectieve kromme $C/\mathbb{Q}$ waarvan het affiene deel is gegeven door $2y^2 = x^4 - 17$. We zagen in propositie 4.7 al dat deze kromme over $\overline{\mathbb{Q}}$ isomorf is met de elliptische kromme $y^2 = x^3 - 17x$. De projectieve kromme C is een kromme in de 3-dimensionale projectieve ruimte en wordt gedefinieerd door het stelsel

$$\begin{cases} 2Y^2 &= X^2 - 17Z^2 \\ XZ &= W^2 \end{cases} \tag{4.1}$$

Het stelsel (4.1) voldoet niet aan het Hasse-principe, iets wat voor het eerst bewezen werd door Reichardt en Lind. In ons bewijs zullen we gebruik maken van de wet van de kwadratische reciprociteit. Deze beroemde stelling van Gauss heeft betrekking op het Legendre symbool. Een bewijs van de stelling kan bijvoorbeeld gevonden worden in [10, p. 53].

Definitie 4.8. Zij p een oneven priemgetal en $a \in \mathbb{Z}$. Het *Legendre-symbool* (a/p) is gedefinieerd als

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \mod p \\ 1 & a \not\equiv 0 \mod p \text{ en } a \text{ is een kwadraat modulo } p \\ -1 & a \not\equiv 0 \mod p \text{ en } a \text{ is geen kwadraat modulo } p. \end{cases}$$

Stelling 4.9 (De wet van de kwadratische reciprociteit)**.** *Zij p, q verschillende oneven priemgetallen. Er geldt*

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

Naast de wet van de kwadratische reciprociteit zal in ons bewijs ook de volgende propositie meerdere malen van pas komen.

Propositie 4.10 (Criterium van Euler)**.** *Zij p een oneven priemgetal en $a \in \mathbb{Z}$ niet deelbaar door p. Er geldt*

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

Bewijs. De kleine stelling van Fermat geeft $a^{(p-1)} \equiv 1 \mod p$ en er geldt dus $a^{(p-1)/2} \equiv \pm 1 \mod p$. Het is nu voldoende aan te tonen dat er geldt $a^{(p-1)/2} \equiv 1 \mod p$ dan en slechts dan als $(a/p) = 1$. Stel dat er geldt $a^{(p-1)/2} \equiv 1 \mod p$. Zij b een voortbrenger van de cyclische groep $\mathbb{F}_p^\times$. Er bestaat een $1 \leq n \leq p-1$ zodanig dat $a \equiv b^n \mod p$ en er volgt $b^{n(p-1)/2} = 1$ in $\mathbb{F}_p^\times$. Het element b heeft orde $p-1$ en er volgt dat $n(p-1)/2$ een veelvoud van $p-1$ moet zijn. Het getal $n/2$ is dus geheel en we concluderen dat $a \equiv (b^{n/2})^2 \mod p$, ofwel $(a/p) = 1$. Voor de ander implicatie nemen we aan dat er geldt $(a/p) = 1$ en er bestaat dus een $c \in \mathbb{F}_p$ met $a \equiv c^2 \mod p$. We vinden $a^{(p-1)/2} \equiv c^{p-1} \mod p$ en met de kleine stelling van Fermat $a^{(p-1)/2} \equiv 1 \mod p$. □

Een belangrijk ingrediënt in het bewijzen dat (4.1) lokaal oplosbaar is, is Hensels lemma. We zullen het nu bewijzen, gevolgd door een bewijs van het feit dat (4.1) niet aan het Hasse-principe voldoet.

Lemma 4.11. *Zij R een commutatieve ring, $I \subseteq R$ een ideaal en $f \in R[X]$ een polynoom. In R/I^2 geldt $f(r+i) = f(r) + f'(r)i$ voor alle $r \in R$ en $i \in I$.*

Bewijs. Schrijf $f = \sum_{j=0}^n c_j X^j$ voor zekere $c_0, ..., c_n \in R$. In een commutatieve ring kunnen we het binomium van Newton gebruiken en we hebben dus

$$f(r+i) = \sum_{j=0}^n c_j (r+i)^j = \sum_{j=0}^n c_j \left(\sum_{k=0}^j \binom{j}{k} r^{j-k} i^k \right).$$

In R/I^2 geldt $i^k = 0$ voor alle $k \geq 2$ en in R/I^2 vinden we dus

$$\begin{aligned} f(r+i) &= \sum_{j=0}^n c_j \left(\binom{j}{0} r^j + \binom{j}{1} r^{j-1} i \right) \\ &= \sum_{j=0}^n c_j (r^j + j r^{j-1} i) \\ &= f(r) + i f'(r). \end{aligned}$$

□

Lemma 4.12 (Hensels lemma)**.** *Zij R een commutatieve ring, $\mathfrak{m}$ een maximaal ideaal en $f \in R[X]$ een polynoom. Als er een $a \in R$ bestaat met $f(a) = 0$ in $R/\mathfrak{m}$ en $f'(a) \neq 0$ in $R/\mathfrak{m}$, dan bestaat er een nulpunt van f in de projectieve limiet $\varprojlim_n R/\mathfrak{m}^n$.*

Bewijs. We zullen een rijtje $(a_1, a_2, ...)$ definiëren met $a_{n+1} \equiv a_n \mod \mathfrak{m}^n$ en $f(a_n) \equiv 0 \mod \mathfrak{m}^n$ voor alle $n \geq 1$. Definieer $a_1 = a$ en $a_{n+1} = a_n + f(a_n)/f'(a_n)$ voor alle $n \geq 1$. We bewijzen dat dit rijtje aan de gewenste eigenschappen voldoet met inductie.

Bekijk het geval $n = 1$. Er geldt $f(a) = 0$ in $R/\mathfrak{m}$ per aanname. We hebben

$$\begin{aligned} a_2 &= a_1 + f(a_1)/f'(a_1) \\ &\equiv a_1 + 0 \mod \mathfrak{m}. \end{aligned}$$

en we concluderen dat er aan de gewenste eigenschappen wordt voldaan voor $n = 1$.
Stel nu dat de uitspraken gelden voor alle $1 \leq d \leq n$ en bekijk het geval $n+1$. Merk op dat de inductiehypothese geeft dat $f'(a_n) = f'(a_1)$ in $R/\mathfrak{m}$ en $f'(a_n)$ is dus een eenheid in $R/\mathfrak{m}$. Er volgt dat $f'(a_n)$ een eenheid is in $R/\mathfrak{m}^m$ voor alle $m \geq 1$. Met lemma 4.11 vinden we dat er in $R/\mathfrak{m}^{2n}$ geldt

$$f(a_{n+1}) = f(a_n) + f(a_n) f'(a_n)/f'(a_1) = f(a_n)(1 - f'(a_n)/f'(a_n)) = 0.$$

Er geldt dus $f(a_{n+1}) \equiv 0 \mod \mathfrak{m}^{2n}$ en omdat er geldt $2n \geq n+1$ voor alle $n \geq 1$ volgt er $f(a_{n+1}) \equiv 0 \mod \mathfrak{m}^{n+1}$. Nu volgt meteen er $a_{n+1} \equiv a_{n+1} \mod \mathfrak{m}^{n+1}$. □

Lemma 4.13. *Zij p een oneven priemgetal en $\alpha, \beta \in \mathbb{F}_p^\times$. Er bestaan $x, y \in \mathbb{F}_p$ zodanig dat $\alpha x^2 + \beta y^2 = 1$.*

Bewijs. Stel dat (x, y) zijn zoals gewenst. Er geldt dus dat (x, y) een oplossing is van de vergelijking $Y^2 = f(X)$ met $f(X) = \beta^{-1} - \beta^{-1}\alpha X^2 \in \mathbb{F}_p[X]$ en we hebben $(f(x)/p) \in \{0, 1\}$. Stel omgekeerd dat er een $c \in \mathbb{F}_p$ bestaat met $(f(c)/p) \in \{0, 1\}$. Geldt er $(f(c)/p) = 0$ dan hebben we $\beta^{-1} = \beta^{-1}\alpha c^2$ en dus $\alpha c^2 = 1$ en $(x, y) = (c, 0)$ voldoet. Als er geldt $(f(c)/p) = 1$, dan voldoet $(x, y) = (c, f(c))$. We concluderen dat de gewenste x en y bestaan dan en slechts dan als er een $c \in \mathbb{F}_p$ bestaat met $(f(c)/p) \in \{0, 1\}$.

Stel dat er niet zo'n c bestaat. Uit het criterium van Euler volgt nu dat er voor alle $c \in \mathbb{F}_p$ geldt $f(c)^{(p-1)/2} = -1$. We concluderen dat het polynoom $f^{(p-1)/2} + 1$ elk element van $\mathbb{F}_p$ als nulpunt heeft. Echter, $f^{(p-1)/2} + 1$ heeft graad $p - 1$ en heeft dus niet meer dan $p - 1$ nulpunten. Tegenspraak. □

Lemma 4.14. *Zij p een oneven priemgetal. Zij $f, g \in \mathbb{F}_p[X]$ twee polynomen van graad kleiner dan of gelijk aan 2. Als er voor alle $t \in \mathbb{F}_p$ geldt $(f(t)/p) = -(g(t)/p)$ dan bestaat er een $c \in \mathbb{F}_p$ zodanig dat $f = cg$.*

Bewijs. Stel dat er voor alle $t \in \mathbb{F}_p$ geldt $(f(t)/p) = -(g(t)/p)$. Het criterium van Euler geeft dat er voor alle $t \in \mathbb{F}_p$ geldt $f(t)^{(p-1)/2} = -g(t)^{(p-1)/2}$. Het polynoom $f^{(p-1)/2} + g^{(p-1)/2}$ heeft graad kleiner dan of gelijk aan $p - 1$ en p nulpunten. We concluderen dat $f^{(p-1)/2} + g^{(p-1)/2}$ het nulpolynoom is en dus $f^{(p-1)/2} = -g^{(p-1)/2}$. Omdat $\mathbb{F}_p[T]$ een ontbindingsring is volgt er dat er een $c \in \mathbb{F}_p$ bestaat met $f = cg$. □

Stelling 4.15. *Het stelsel (4.1) voldoet niet aan het Hasse-principe.*

Bewijs. We bewijzen eerst dat (4.1) lokaal oplosbaar is. Over $\mathbb{R}$ hebben we de oplossing $(w, x, y, z) = (\sqrt[4]{17}, \sqrt{17}, 0, 1)$. Zij $p \neq 2, 17$ een priemgetal, we zullen nu bewijzen dat (4.1) een oplossing heeft over $\mathbb{Q}_p$. We doen dit door eerst aan te tonen dat (4.1) een oplossing heeft modulo p. Vermenigvuldigen van de eerste vergelijking met $2^{-1} \in \mathbb{F}_p$ levert de vergelijking $Y^2 = \alpha X^2 - \beta Z^2$ met $\alpha = 2^{-1}$ en $\beta = 17/2 \mod p$. Definieer nu de volgende polynomen in $\mathbb{F}_p[T]$

$$\begin{aligned} q_1(T) &= \beta x T^2 - 2\beta y T - \alpha x \\ q_2(T) &= -\beta y T^2 - 2\alpha x T + \alpha y \\ q_3(T) &= \beta T^2 + \alpha. \end{aligned}$$

waarbij $x, y \in \mathbb{F}_p$ zodanig zijn dat er geldt $\alpha x^2 + \beta y^2 = 1$. Het bestaan van dergelijke x, y wordt gegarandeerd door lemma 4.13. Na wat uitschrijfwerk en veelvuldig gebruik van de gelijkheid $\alpha x^2 + \beta y^2 = 1$ vinden we dat er geldt $\alpha q_1^2 + \beta q_2^2 = q_3^2$. Stel nu dat er een $c \in \mathbb{F}_p$ bestaat met $q_1 = cq_2$, er volgt $(\alpha + \beta c^2)q_1^2 = q_3^2$. Omdat $\mathbb{F}_p[T]$ een ontbindingsring is, volgt er dat er een $c' \in \mathbb{F}_p$ bestaat met $c'q_1 = q_3$. Er volgt dat de lineaire term in q_1 gelijk is aan 0 en omdat $q_2 = cq_1$, is ook de lineaire term van q_2 gelijk aan 0. Maar nu zijn αx en βy beide 0 en dat levert een tegenspraak op met $\alpha x^2 + \beta y^2 = 1$. Er bestaat dus geen $c \in \mathbb{F}_p$ met $q_1 = cq_2$ en uit lemma 4.14 volgt dat er een $t \in \mathbb{F}_p$ bestaat zodanig dat $(q_1(t)/p) \neq -(q_2(t)/p)$. Nu volgt dat $q_1(t)$ en $q_2(t)$ niet beide gelijk zijn aan 0 en $(q_1(t)q_2(t)/p) = 1$. Er bestaat dus een $s \in \mathbb{F}_p$ met $q_1(t)q_2(t) = s^2$. We concluderen dat $(w, x, y, z) = (s, q_1(t), q_2(t), q_3(t))$ een niet-triviale oplossing is van (4.1) modulo p.

Het stelsel (4.1) heeft dus een niet-triviale oplossing (w, x, y, z) modulo p. Merk op dat als x en z beide 0 zijn, dan geldt $(w, x, y, z) = (0, 0, 0, 0)$ en de oplossing is triviaal. Er geldt dus dat minstens één van de elementen x en z ongelijk aan 0 is. Stel, zonder verlies van

algemeenheid, dat er geldt $x \neq 0$. Er geldt nu dat x een eenheid is in $\mathbb{F}_p$ en het viertal $(w', x', y', z') = (wx^{-1}, 1, yx^{-1}, zx^{-1})$ is een oplossing van (4.1) modulo p. De tweede vergelijking van het stelsel (4.1) geeft $z' \equiv w'^2 \mod p$ en er volgt $2y'^2 \equiv 1 - 17z'^4 \mod p$. We onderscheiden nu twee gevallen.
Als er geldt $y' \equiv 0 \mod p$, dan is $z' \in \mathbb{F}_p$ een nulpunt van het polynoom $f := 1 - 17S^4 \in \mathbb{Z}[S]$ modulo p. Er geldt $f'(z') = -4 \cdot 17z'^3$. Merk op dat er geldt $z' \not\equiv 0 \mod p$. Immers, z' is een nulpunt van $f \mod p$ en er geldt dus $-17z'^4 \equiv 1 \mod p$. We hebben aangenomen dat er geldt $p \neq 2, 17$ en er geldt dus $-4 \cdot 17 \not\equiv 0 \mod p$. Er volgt $f'(z') = -4 \cdot 17z'^3 \not\equiv 0 \mod p$. We kunnen nu Hensels lemma gebruiken om te concluderen dat f een nulpunt $\zeta \in \mathbb{Z}_p$ heeft. Er bestaat dus een $\zeta \in \mathbb{Z}_p$ met $17\zeta^4 = 1$ en $(\zeta, 1, 0, \zeta^2) \in \mathbb{Z}_p^4$ is nu een niet triviale oplossing van (4.1).
Stel nu dat er geldt $y' \not\equiv 0 \mod p$. Er geldt nu dat y' een nulpunt is van het polynoom $g := 2S^2 - 1 + 17z'^4 \in \mathbb{Z}[S]$ modulo p. Er geldt $g'(y') = 4y' \not\equiv 0 \mod p$, waarbij we weer gebruiken dat $p \neq 2$. Hensels lemma geeft ons weer een nulpunt $\zeta \in \mathbb{Z}_p$ van het polynoom g en we vinden de niet-triviale oplossing $(z', 1, \zeta, z'^2) \in \mathbb{Z}_p^4$ van (4.1).
We concluderen dat (4.1) niet-triviale oplossingen heeft over $\mathbb{R}$ en $\mathbb{Q}_p$ voor $p \neq 2, 17$.

We bekijken $p = 2$. Definieer het polynoom $f := X^4 - 17 \in \mathbb{Z}[X]$. Merk op dat 1 een nulpunt van f is modulo 2 en dat er geldt $f'(1) = -13 \not\equiv 0 \mod 2$. Hensels lemma geeft nu dat er een nulpunt $\zeta \in \mathbb{Z}_2$ van f bestaat. Er bestaat dus een $\zeta \in \mathbb{Z}_2$ met $\zeta^4 = 17$ en er volgt dat $(\zeta, \zeta^2, 0, 1) \in \mathbb{Z}_2^4$ een niet-triviale oplossing is van (4.1). We bekijken nu $p = 17$. Definieer het polynoom $g := 2X^2 - X^4 + 17 \in \mathbb{Z}[X]$. Merk op dat 6 een nulpunt van g is modulo 17 en dat er geldt $g'(6) = -840 \not\equiv 0 \mod 17$. Hensels lemma geeft nu dat er een nulpunt $\zeta \in \mathbb{Z}_{17}$ van g bestaat. Er bestaat dus een $\zeta \in \mathbb{Z}_{17}$ met $2\zeta^2 = \zeta^4 - 17$ en we concluderen dat $(\zeta, \zeta^2, \zeta, 1)$ een niet-triviale oplossing van (4.1) is in $\mathbb{Z}_{17}^4$. We concluderen dat (4.1) lokaal oplosbaar is.

Het rest te bewijzen dat (4.1) niet globaal oplosbaar is. Stel dat er wel een niet triviale oplossing $(w, x, y, z) \in \mathbb{Q}^4$ van (4.1) bestaat. Vanwege de homogeniteit van de vergelijkingen mogen we aannemen dat w, x, y, z geheel zijn en grootste gemeenschappelijke deler 1 hebben. Merk op dat als p een priemgetal is dat x en z deelt, dan geldt er $p \mid w$ en $p^2 \mid 2y^2$ en dus $p \mid y$. Dit is in tegenspraak met de aanname dat w, x, y, z grootst gemeenschappelijke deler 1 hebben en we concluderen dat x en z geen gemeenschappelijke priemfactoren hebben. Uit volstrekt analoge redeneringen concluderen we dat x en y geen gemeenschappelijke priemfactoren hebben en dat y en z geen gemeenschappelijke priemfactoren hebben. Merk ook op dat er geldt $x^2z^2 = w^4$ en omdat x en z geen gemeenschappelijke priemfactoren hebben, geldt dat x^2 een vierde macht is. Ook geldt er $17 \nmid x$. Immers, anders geldt er $17 \mid y$ en hebben x en y een gemeenschappelijk priemfactor. We concluderen dat x^2 een vierde macht is modulo 17 ongelijk aan 0. Zij p nu een oneven priemfactor van y. We hebben $x^2 \equiv 17z^2 \mod p$. We wisten al dat y en z geen gemeenschappelijke priemfactoren hebben en z is dus een eenheid modulo p. We hebben nu $17 \equiv x^2z^{-2} \mod p$. Er volgt $(17/p) = 1$. Uit de wet van de kwadratische reciprociteit volgt nu $(p/17) = 1$. Voor elk oneven priemgetal $p|y$ hebben we dus $(p/17) = 1$ en omdat er modulo 17 geldt $2 = 6^2$ hebben we tevens $(2/17) = 1$ en we concluderen dat er voor elk priemgetal p geldt $(p/17) = 1$. Modulo 17 geldt er tevens $4^2 = 16 = -1$ en dus $(-1/17) = 1$. Ontbinden van y in priemfactoren en gebruik maken van de multiplicativiteit van het Legendre symbool geeft $(y/17) = 1$. We weten nu dat y^2 modulo 17 een vierde macht is ongelijk aan 0. Modulo 17 geldt er $x^2 = 2y^2$ en dus $x^2y^{-2} = 2$. Nu zijn x^2 en y^{-2} beide vierde machten modulo 17 en er volgt dat 2 ook een vierde macht is modulo 17. We kunnen simpelweg elk element in $\mathbb{F}_{17}$ tot de macht 4 verheffen en zo te weten komen dat 2 geen vierde macht is modulo 17. Tegenspraak. We concluderen dat (4.1) niet globaal oplosbaar is.
We hebben bewezen dat (4.1) lokaal oplosbaar is maar niet globaal, daarmee voldoet (4.1) inderdaad niet aan het Hasse-principe. □

Referenties

[1] Aitken, W. and Lemmermeyer, F. (2011). Counterexamples to the Hasse principle. *Am. Math. Mon.*, 118(7):610–628.

[2] Cassels, J. W. S. (1991). *Lectures on Elliptic Curves*. Cambridge University Press, Cambridge.

[3] Goldschmidt, D. M. (2003). *Algebraic Functions and Projective Curves*. Springer, New York.

[4] Gouvêa, F. Q. (1997). *p-adic Numbers*. Springer, Berlin, Heidelberg, 2nd edition.

[5] Knapp, A. W. (1992). *Elliptic Curves*. Princeton University Press, Princeton.

[6] Milne, J. S. (2006). *Elliptic Curves*. BookSurge Publishers.

[7] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Springer, New York, 2nd edition.

[8] Silverman, J. H. and Tate, J. T. (2015). *Rational Points on Elliptic Curves*. Springer, 2nd edition.

[9] Stevenhagen, P. (2010). *Algebra II*. Universiteit Leiden.

[10] Stevenhagen, P. (2012). *Algebra III*. Universiteit Leiden.

[11] Stevenhagen, P. (2014). *Algebra I*. Universiteit Leiden.