Split Jacobians and Lower Bounds on Heights

Djukanovic, M.

Samenvatting

Dit proefschrift behandelt eigenschappen van Jacobianen van krommen van geslacht twee die elliptische krommen overdekken.

Zij E een kromme in het vlak, gegeven door een vergelijking $y^2 = F(x)$, waarbij $F(x) = x^3 + a_2x^2 + a_1x + a_0$ een polynoom is met rationale coëfficiënten en met drie verschillende nulpunten. Om historische redenen wordt een dergelijke kromme een *elliptische kromme* genoemd. Het is bekend dat elke elliptische kromme kan worden voorzien van een commutatieve groepsstructuur – haar punten kunnen bij elkaar worden opgeteld en van elkaar worden afgetrokken. Een punt O „op oneindig", dat bevat is in alle verticale lijnen (lijnen van de vorm $x = c$), is het neutrale element. De groepsstructuur wordt vastgelegd door de voorwaarde dat drie punten $P, Q, R \in E$ voldoen aan $P + Q + R = O$ dan en slechts dan als zij op één lijn liggen. Oppervlakken met een commutatieve groepsstructuur worden *abels* genoemd. Bijvoorbeeld is een product van twee elliptische krommen $E_1 \times E_2$ op de voor de hand liggende wijze een abels oppervlak.

Vervolgens beschouwen we een vlakke kromme C gegeven door een vergelijking $y^2 = G(x)$, waarbij $G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ een polynoom is met rationale coëfficiënten en zes verschillende nulpunten. De kromme C wordt *hyperelliptisch* genoemd en heeft geen groepsstructuur. Toch kunnen we, op een natuurlijke wijze, eraan een abels oppervlak $\mathrm{Jac}(C)$ toekennen, dat de *Jacobiaan* van C wordt genoemd. Voorts kunnen we C hierin inbedden. Sommige hyperelliptische krommen van de vorm $y^2 = G(x)$ zoals hierboven zijn bijzonder omdat zij elliptische krommen overdekken. Bijvoorbeeld, beschouw een kromme C gegeven door $y^2 = x^6 + ax^4 + bx^2 + c$, zodat alleen even machten van x optreden. Als (x, y) een punt is op deze kromme dan is $(-x, y)$ dat ook en we kunnen een algebraïsche afbeelding $f\colon (x, y) \mapsto (x^2, y)$

definiëren die van graad 2 is, d.w.z. 2-op-1. Het punt $(X, Y) = (x^2, y)$ ligt op de elliptische kromme E gegeven door $Y^2 = X^3 + aX^2 + bX + c$ en we zeggen dat C een dubbele overdekking is van E.

Als E een elliptische kromme is, C een hyperelliptische kromme, en $C \to E$ een n-op-1 overdekking die niet een samenstelling is van overdekkingen, dan kunnen we E inbedden in het oppervlak $\mathrm{Jac}(C)$ als ondergroep. Bovendien bestaat er een andere elliptische kromme $\widetilde{E}$ en een n-op-1 overdekking $C \to \widetilde{E}$. Voorts heeft het oppervlak $\mathrm{Jac}(C)$ een bijzondere eigenschap – het kan worden verkregen als een quotiënt van het oppervlak $E \times \widetilde{E}$ naar een eindige ondergroep.

Het eerste hoofdstuk van dit proefschrift behandelt de meetkundige aspecten van deze situatie. We onderzoeken welke krommen in deze bijzondere verhouding tot elkaar kunnen staan en we concentreren ons hoofdzakelijk op de gevallen $n = 2$ en $n = 3$, die al in de literatuur zijn onderzocht. We verkrijgen ook enig inzicht in het algemene geval, maar een volledige beschrijving blijkt vanuit computationeel oogpunt zeer moeilijk te zijn.

Het tweede hoofdstuk behandelt de aritmetische aspecten van de situatie, met behulp van de theorie van *hoogtes*, die een zeer bruikbaar hulpmiddel vormen bij het beantwoorden van vragen rond rationale punten op krommen en oppervlakken. Voor elk rationaal getal $x = a/b$, waarbij a en b gehele getallen zijn die relatief priem zijn, kan men de hoogte $h(x)$ definiëren, op een heel precieze manier, als een maat voor diens aritmetische complexiteit – de hoogte vertelt ons min of meer hoeveel cijfers er nodig zijn om de gehele getallen a en b op te schrijven. Op eenzelfde manier zegt de hoogte van een rationaal punt op een kromme of oppervlak ons iets over het aantal cijfers van zijn coördinaten. Bijvoorbeeld zijn $(3, 5)$ en $(1749/1331, -1861/1331)$ twee rationale punten van behoorlijk verschillende complexiteit op de kromme $y^2 = x^3 - x + 1$. Anderzijds is $(2, \sqrt{7})$ geen rationaal punt. Het is ook mogelijk om een hoogte toe te kennen aan een elliptische kromme of een abels oppervlak om zodoende diens aritmetische complexiteit als geheel te meten. Er wordt een precies verband tussen de twee hoogtes vermoed, en we onderzoeken dit vermoeden in de context van de situatie zoals boven geschetst. We bewijzen dat het vermoede verband geldt voor $E \times \widetilde{E}$ dan en slechts dan als het geldt voor $\mathrm{Jac}(C)$.