



Universiteit
Leiden
The Netherlands

Counting curves and their rational points

Spelier, P.

Citation

Spelier, P. (2024, June 12). *Counting curves and their rational points*.
Retrieved from <https://hdl.handle.net/1887/3762227>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3762227>

Note: To cite this publication please use the final published version (if applicable).

Samenvatting

Een belangrijke focus van wiskunde door de millenia heen is het bestuderen van oplossingen van vergelijkingen. In ongeveer 1800 v.Chr. bestudeerden de Babyloniërs [BPS11] bijvoorbeeld geheeltallige oplossingen van

$$x^2 + y^2 = z^2,$$

die nu bekend staan als Pythagorese drietallen. Er zijn vanzelfsprekend zeer veel voorbeelden van vergelijkingen: de vergelijking

$$y = x^2,$$

wiens oplossingen een parabool vormen, of $xy = z$, wiens oplossingen een oppervlak vormen in een driedimensionale ruimte. Of

$$y^2 = x^3 + x,$$

wat een zogeheten elliptische kromme geeft, een concept uit de 19e eeuw dat de basis vormt van een groot gedeelte van de moderne cryptography [Mil86, Kob87], en dat veel verbanden heeft met getaltheorie [Sil94, Sil09].

In dit proefschrift bestuderen we krommen, *algebraïsche krommen* om precies te zijn. Dit zijn een-dimensionale meetkundige objecten gegeven door polynomiale vergelijkingen. De studie naar ruimtes gedefinieerd door polynomiale vergelijkingen heet algebraïsche meetkunde, precies omdat het de talen van algebra en meetkunde combineert. Algebraïsch gezien hebben we vergelijkingen, wiens verzameling van oplossingen we interpreteren als meetkundige objecten die *variëteiten* heten; algebraïsch gezien hebben we oplossingen, die we in de meetkundige wereld interpreteren als punten op de variëteit. Bijvoorbeeld, de vergelijking $y = x^2$ correspondeert met de parabool, een voorbeeld van een

variëteit, en de oplossing $9 = 3^2$ correspondeert met het punt $(3, 9)$ op de parabool. Voor een verwijzing naar een simpele uiteenzetting over algebraïsche krommen, zie bijvoorbeeld [Sil09, Chapters 1-2].

We behandelen twee problemen over krommen. Als eerste, het *tellen van krommen*, deel van een gebied genaamd *enumeratieve meetkunde*. Het doel van dit gebied is het tellen van krommen met bepaalde eigenschappen, zoals krommen door een bepaalde verzameling punten. Bijvoorbeeld, er is een unieke lijn door twee punten in het vlak, en er is een unieke kegelsnede (een kromme gegeven door een polynomiale vergelijking in x en y van graad 2) door vijf punten in het vlak. En er zijn exact twaalf kubische krommen (een kromme gegeven door een polynomiale vergelijking in x en y van graad 3) die zichzelf in één punt doorsnijden en door acht punten in het vlak gaan. Dit vakgebied heeft diepe verbanden met natuurkunde en met partiële differentiaalvergelijkingen [DZ01, BR21]. Een samenvatting van dit vakgebied kan men vinden in [KV07] of [Vak08].

Het tweede probleem is het daadwerkelijk oplossen van vergelijkingen, oftewel, het vinden van alle punten op de kromme. Wij zijn geïnteresseerd in het vinden van de rationale punten, de punten met coördinaten in $\mathbb{Q}$. Dit probleem is een speciaal geval van de zeer brede klasse van *diofantische* vergelijkingen. Onder bepaalde voorwaarden op de kromme zijn er maar eindig veel rationale punten, maar het is een lastige taak om ze allemaal te vinden, en een bewijs te geven dat er geen andere zijn. Voor een uiteenzetting van dit vakgebied, zie [MP12, BM20, BDM⁺21].

De volgende twee secties van de samenvatting behandelen deze twee onderwerpen. Ze zijn bedoeld om op zichzelf te staan.

Krommen tellen

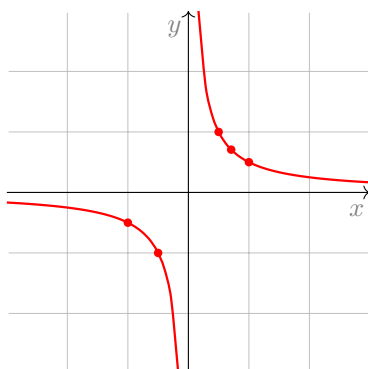
We duiken eerst in een specifiek geval, namelijk het geval van een kegelsnede door 5 punten in het vlak. Voor elk vijftal punten, is er een unieke kegelsnede die ze bevat. Beschouw bijvoorbeeld het vijftal punten

$$S_t = \{(1, t), (t, 1), (-1, -t), (-t, -1), (\sqrt{t}, \sqrt{t})\},$$

voor een reëel getal $t > 0$. De hyperbool

$$C_t : xy = t$$

gaat dan door deze vijf punten, zie Figuur 1. Er doet zich een interessant fenomeen voor als t dichter en dichter bij 0 komt: de hyperbool wordt scherper



Figuur 1: De hyperbool $xy = \frac{1}{2}$, die door de vijf punten $(1, \frac{1}{2})$, $(\frac{1}{2}, 1)$, $(-1, -\frac{1}{2})$, $(-\frac{1}{2}, -1)$, $(\sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}})$ gaat.

en scherper rond $(0, 0)$, en wordt uiteindelijk de kromme

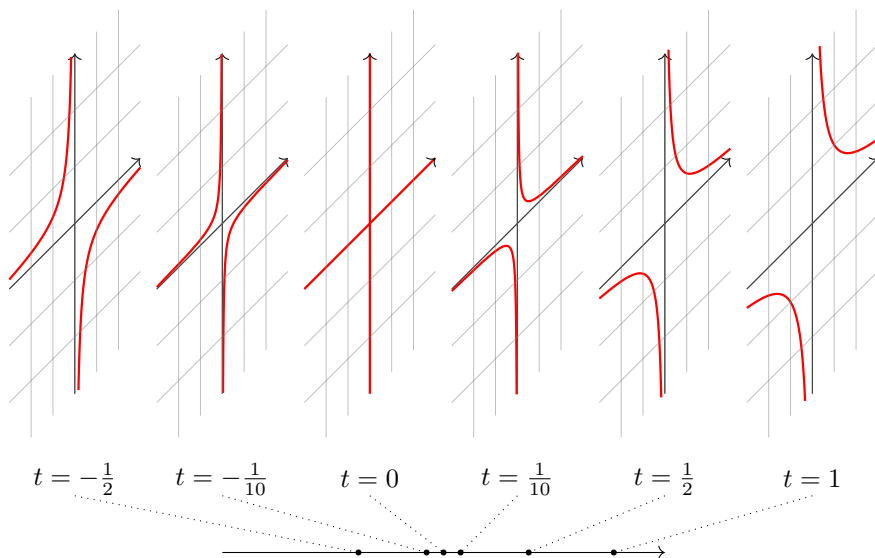
$$C_0 : xy = 0.$$

Deze degeneratie wordt afgebeeld in Figuur 2. Deze kromme C_0 is niet *glad*, betekenend dat het er lokaal niet uit ziet als een lijn, in tegenstelling tot het geval $t \neq 0$, waar C_t altijd glad is. Omdat C_0 er lokaal uit ziet als het snijpunt van twee lijnen, heet C_0 een *nodale* kromme.

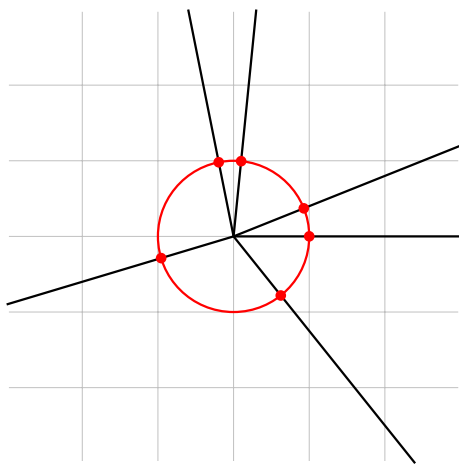
Veel fijne eigenschappen van gladde krommen gelden niet voor nodale krommen. Desondanks bestuderen mensen vaak nodale kromme, zelfs als ze gladde krommen willen tellen. Waarom? De verklaring ligt in het begrip van de *moduliruimte van krommen*. Dat is een verzameling die alle krommen bevat, en op miraculeuze wijze zelf een meetkundig object is.

Voor een voorbeeld van dit fenomeen, beschouw de verzameling halflijnen vanuit de oorsprong, afgebeeld in Figuur 3. Dit is een verzameling van meetkundige objecten, maar het is ook zelf een meetkundig object, namelijk een cirkel! Voor nog een voorbeeld, kijken we opnieuw naar Figuur 2. De verzameling krommen vormt hier op een natuurlijke wijze een lijn met coördinaat t , en de verzameling gladde krommen vormt een lijn met een gat, aangezien het punt $t = 0$ ontbreekt.

Het bestuderen van moduliruimtes is een buitengewoon krachtig hulpmiddel voor het beantwoorden van vragen over krommen. Echter, als deze moduliruimten gaten hebben, oftewel niet *compact* zijn, dan kunnen veel van de



Figuur 2: De kromme $xy = t$ voor enkele t . De kromme is glad voor $t \neq 0$.



Figuur 3: De verzameling halflijnen vanuit de oorsprongt correspondeert op een natuurlijke wijze met een cirkel (rood). Elke halflijn correspondeert met de doorsnede van de halflijn met de cirkel.

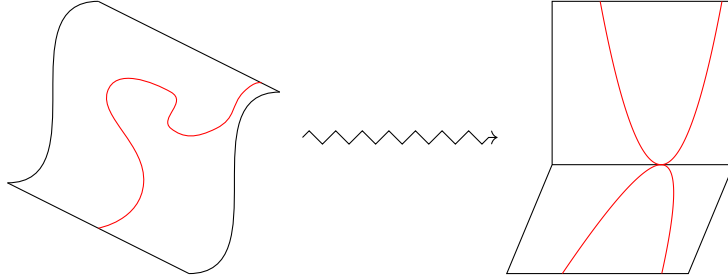
meetkundige technieken niet toegepast worden. De moduli-ruimte van gladde krommen $\mathcal{M}$ heeft veel gaten, en de *compactificatie* $\overline{\mathcal{M}}$, de moduli-ruimte van nodale krommen, heeft er geen. Heden ten dage spelen moduli-ruimten een centrale rol in veel gebieden binnen de algebraïsche meetkunde. We raden [Beh14] aan voor een prachtige inleiding tot dit onderwerp via de moduli-ruimte van driehoeken. Voor een klassieke, algebraïsche versie, zie bijvoorbeeld [Vak08] of [Sch20].

In Hoofdstuk 2 gebruiken we dit moduli-ruimtenperspectief voor de studie van de *dubbele vertakkingscykel* $\mathrm{DR}(A)$, die afhangt van een vector $A \in \mathbb{Z}^n$ met som 0. Deze telt krommen met oneindige symmetriën, en extra voorwaarden gegeven door A . Dit object, gedefinieerd in [GV03, MW20, Hol21] heeft veel verbanden met andere gebieden in de wiskunde [BR21, RK23]. In [JPPZ17] formuleerden ze het vermoeden dat $\mathrm{DR}(A)$ polynomiaal is in A , en kondigden ze een bewijs hiervan aan. Recent gaf Pixton een bewijs van deze stelling [Pix23]. Wij geven een alternatief bewijs, in Theorem A.

Het degenereren van gladde krommen naar nodale krommen kan nuttig zijn voor het bestuderen van gladde krommen. Maar een kromme is slechts een speciaal geval van een variëteit, aangezien een variëteit een willekeurige meetkundige ruimte gedefinieerd door polynomiale vergelijkingen is. In feite kunnen we elke variëteit degenereren, en dit kan een sterk gereedschap zijn. Men kan een gladde variëteit degenereren naar eenvoudiger bouwstenen, op dezelfde manier als we $xy = 1$ hebben gedegenerereerd naar $xy = 0$, de vereniging van de twee lijnen $x = 0$ en $y = 0$. De krommen in de variëteit degenereren dan naar krommen op de bouwstenen. Voor een voorbeeld, zie Section 7.7.6. Vaak kunnen vragen over de oorspronkelijke variëteit vertaald worden naar vragen over de bouwstenen. Bijvoorbeeld, de *degeneratieformule* vertelt hoe je krommen in X kan tellen als je weet hoe je krommen in de bouwstenen kan tellen [KLR18, ACGS20b, RK23].

De sleutel voor het samen laten werken van de meetkunde en de combinatoriek van de degeneraties is de taal van *logaritmische meetkunde*, een uitbreiding van algebraïsche meetkunde. Een *log variëteit* is een variëteit met wat extra structuur, een *log structuur*. Wij behandelen voornamelijk *log gladde log varieties* X , waar de log structuur een representatie is van X als een degeneratie van een gladde variëteit. Bijvoorbeeld, Figuur 2 induceert een log gladde log structuur op C_0 , door het te representeren als een degeneratie van $xy = t$ waar t naar 0 gaat.

Het blijkt dat elke nodale kromme een canonieke log gladde log structuur heeft, en dus kunnen we $\overline{\mathcal{M}}$ ook interpreteren als de moduli-ruimte van log gladde



Figuur 4: Een degeneratie van een variëteit. De krommen in de variëteit degenereren naar krommen die raken aan de doorsnede.

krommen. Dit induceert ook een log structuur op $\overline{\mathcal{M}}$. Het feit dat alle log krommen log glad zijn zorgt ervoor dat alles zich ongeveer hetzelfde gedraagt als in het geval van gladde krommen, met het voordeel dat we een compacte moduli ruimte hebben. Veel resultaten in algebraïsche meetkunde zijn bewezen door een log analoog te beschouwen, stellingen over de log analoog te bewijzen, en ten slotte algebraïsche resultaten te deduceren [HPS19, HMOP23, RK23]. Voor enkele voorbeelden waar *tropische meetkunde*, het combinatorische gedeelte van log meetkunde, gebruikt wordt om algebraïsche resultaten te bewijzen, zie bijvoorbeeld [KRZB16, FJP23]. Echter, het vinden van de correcte log analoog, en het bewijzen van de corresponderende log stellingen, is niet een simpele taak.

In Hoofdstuk 3 beschouwen we een voorbeeld hiervan. Met behulp van logaritmische methoden versimpelen we resultaten van [BH19], en beantwoorden we enkele open vragen van [BH19].

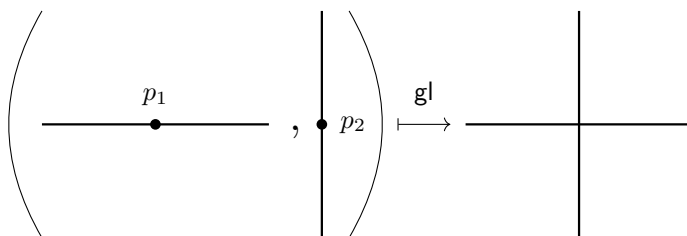
In Hoofdstuk 4, gezamenlijk werk met David Holmes, bestuderen we een ander voorbeeld, het *lijmen* van krommen. Klassiek werkt dit als volgt. Zij $\overline{\mathcal{M}}_1$ de moduli ruimte van paren (C, p) waar C een kromme is, en p een punt op C . Gegeven twee paren $(C_1, p_1), (C_2, p_2) \in \overline{\mathcal{M}}_1$, kunnen we de punten p_1 en p_2 aan elkaar lijmen om een andere kromme C^{gl} te krijgen. Formeel hebben we

$$C^{\text{gl}} = (C_1 \sqcup C_2) / \sim$$

met $p_1 \sim p_2$. Voor een voorbeeld, zie Figuur 5 waar we C_0 construeren als de lijming van twee lijnen.

Dit definieert een lijmafbeelding

$$\text{gl} : \overline{\mathcal{M}}_1 \times \overline{\mathcal{M}}_1 \rightarrow \overline{\mathcal{M}}.$$



Figuur 5: De lijming van twee lijnen.

Het beeld ligt in de rand $\overline{\mathcal{M}} \setminus \mathcal{M}$ van nodale krommen, en het is deze lijmafbeelding waardoor we recursief de rand kunnen begrijpen. Deze lijmafbeeldingen zijn de basis geweest voor veel theorieën, stellingen en formules in klassieke algebraïsche meetkunde. Bijvoorbeeld, de eerdergenoemde kromme-aantallen voldoen aan recursieve relaties met betrekking tot de lijmafbeeldingen.

Echter, men kan bewijzen dat log krommen niet te lijmen zijn. Dat betekent dat veel klassieke constructies die de lijmafbeelding gebruiken niet gegeneraliseerd konden worden naar de logaritmische wereld. Samen met David Holmes hebben we dit opgelost, door zogeheten *log gepunte krommen* te definiëren. Dit geeft een log moduli-ruimte $\mathbb{M}_1$, met een zekere log structuur. We hebben de volgende stelling bewezen.

Stelling (Theorem F). *De onderliggende variëteit van $\mathbb{M}_1$ is $\overline{\mathcal{M}}_1$. Er is een logaritmische lijmafbeelding*

$$\text{gl} : \mathbb{M}_1 \times \mathbb{M}_1 \rightarrow \overline{\mathcal{M}}.$$

Hierdoor hebben we log analogen van meerdere klassieke constructies kunnen produceren, in het bijzonder logaritmische cohomologische veldentheorieën, zekere collecties van functies die op een zekere manier compatibel zijn met de logaritmische lijmafbeeldingen. We hebben een belangrijke stelling in de klassieke wereld [BR21] gegeneraliseerd naar de log versie Theorem G. Dit artikel opent ook een nieuwe onderzoekslijn, over welke constructies en stellingen over de klassieke lijmafbeeldingen gegeneraliseerd kunnen worden naar de log wereld.

Rationale punten

Een van de eerste abstracte wiskundige problemen was het oplossen van *diofantische* vergelijkingen, polynomiale vergelijkingen waar het doel is om alle rationale punten te vinden. Bijvoorbeeld, de vergelijking $x^2 + y^2 = 1$, de vergelijking van een cirkel, heeft de rationale oplossing $(x, y) = (\frac{3}{5}, \frac{4}{5})$.

Door de millenia heen zijn er veel strategieën en stellingen gebruikt om allerlei soorten diofantische vergelijkingen op te lossen. Wij focussen op het specifieke geval van krommen. Gegeven een polynoom in x, y , bijvoorbeeld $x^2 + y^2 = 1$, of

$$y^2 + (x^3 + x + 1)y = x^5 - x$$

vormt de verzameling van complexe oplossingen een meetkundige kromme die makkelijk te beschrijven is. De rationale oplossingen corresponderen dan met rationale punten op de kromme, en ze vormen een deelverzameling die vaak lastig te vinden is. Voor een kromme C noteren we de rationale punten als $C(\mathbb{Q})$. Wellicht het meest bekend is de Fermat-kromme F_n , gegeven door $x^n + y^n = 1$ voor een zekere $n \geq 3$. Andrew Wiles heeft bewezen dat deze alleen de rationale punten $(0, \pm 1)$ en $(\pm 1, 0)$ heeft, en heeft daarmee Fermats Laatste Stelling bewezen, over de geheeltallige oplossingen $a^n + b^n = c^n$ [Wil95, TW95].

Een kromme C heeft een belangrijke invariant genaamd het geslacht $g \in \mathbb{Z}_{\geq 0}$, en het gedrag van de kromme C en de rationale punten $C(\mathbb{Q})$ hangt sterk af van het geslacht. Er is slechts één kromme van geslacht 0, namelijk de lijn, en de lijn heeft oneindig veel rationale punten¹³.

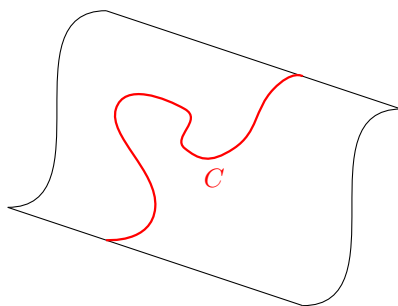
Krommen van geslacht 1 heten *elliptische krommen*. Dit is een zeer speciaal soort kromme die op een natuurlijke manier de structuur heeft van een abelse groep. Anders gezegd, je kan twee punten optellen om een derde punt te krijgen. Rationale punten vormen een ondergroep, en zelfs een eindig voortgebrachte groep. Voor een specifieke elliptische kromme is het vinden van voortbrengers en relaties voor deze groep normaal goed te doen.

Voor krommen van geslacht $g \geq 2$, het onderwerp van de tweede helft van dit proefschrift, formuleerde Mordell in 1922 het vermoeden dat er altijd slechts eindig veel rationale punten zijn. Hoewel er gedeeltelijke voortgang geboekt was, werd dit vermoeden pas bewezen in 1983, door Faltings. Tegenwoordig staat het bekend als Faltings' stelling. Dit was een enorme doorbraak, maar helaas is dit resultaat niet *effectief*, wat betekent dat het niet helpt met het

¹³In deze sectie maken we de technische aanname dat C minstens één rationaal punt heeft, om de uitleg te versimpelen

daadwerkelijk berekenen van de verzameling rationale punten

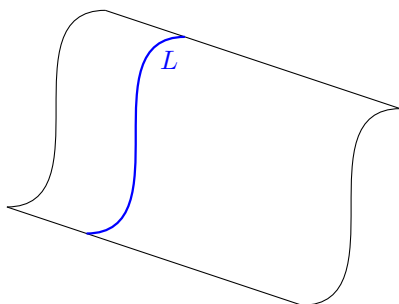
Een manier om het in zekere gevallen effectief te maken, is met behulp van een stelling van Chabauty uit 1941 [Cha41], die een specifiek geval van Faltings' stelling bewees. Bij elke kromme C van geslacht g hoort een ruimte van dimensie g , de Jacobiaan van C . Deze noteren we als $J = J(C)$. Net zoals een elliptische kromme is deze meetkundige ruimte ook een abelse groep. Er hoort een afbeelding $C \rightarrow J$ bij, genaamd de Abel–Jacobi-afbeelding, die een inbedding is voor $g \geq 1$, en men kan J interpreteren als de abelse groepificatie van C . Een incarnatie hiervan is bijvoorbeeld dat de fundamenteaalgroep van J de abelianisatie is van de fundamenteaalgroep van C . Zie Figuur 6 voor een voorbeeld van hoe deze inbedding eruit kan zien als $g = 2$.



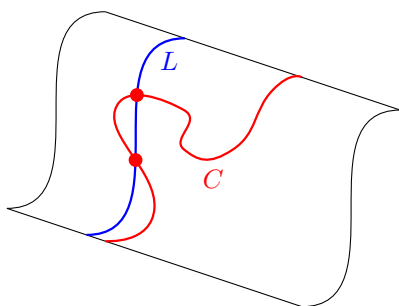
Figuur 6: De inbedding van de geslacht 2 kromme C (rood) naar de Jacobiaan J (zwart), een oppervlak.

Voor een elliptische kromme C is de Jacobiaan J gelijk aan C , en is de afbeelding naar de Jacobiaan simpelweg de identiteit. In het algemeen heeft J veel weg van een elliptische kromme. Bijvoorbeeld, de verzameling rationale punten $J(\mathbb{Q})$ vormen een abelse groep die eindig voortgebracht is, van een bepaalde rang r . Zie Figuur 7 voor een voorbeeld waar $r = 1$, en we de lijn hebben geplot die de verzameling $J(\mathbb{Q})$ bevat.

Nu zien we Chabauty's truc verschijnen als we deze twee inbeddingen $C \rightarrow J$ en $J(\mathbb{Q}) \rightarrow J$ over elkaar leggen, in Figuur 8. We weten dat de rationale punten in $C(\mathbb{Q})$ in C liggen, en naar $J(\mathbb{Q})$ worden afgebeeld onder de Abel–Jacobi-afbeelding. Dan liggen ze ook in de doorsnede $J(\mathbb{Q}) \cap C \subset J$. En met de cruciale aanname $r < g$, verwachten we dat deze doorsnede eindig is wegens de dimensies. Dit is inderdaad wat Chabauty bewezen heeft: als $r < g$, dan is $C(\mathbb{Q})$ eindig.



Figuur 7: Een lijn L (blauw) die de rationale punten van de Jacobiaan bevat.



Figuur 8: Chabauty's methode: de doorsnede van L en C bevat alle rationale punten van C en is eindig.

Een kleine technische opmerkingen: de afbeelding suggereert dat we deze doorsnede nemen binnen de $\mathbb{R}$ -punten van J . Echter, dat werkt niet, en in plaats daarvan nemen we de doorsnede $C(\mathbb{Q}_p) \cap J(\mathbb{Q})$ binnen $J(\mathbb{Q}_p)$, waar $\mathbb{Q}_p$ de p -adische getallen zijn voor een zeker priemgetal p . Dit is een andere, niet-archimedische vervollediging van $\mathbb{Q}$, die veel van de convergentieproblemen van $\mathbb{R}$ vermijdt.

Het heeft nog 44 jaar geduurd voordat er een effectieve versie van Chabauty's methode kwam. In 1985 gaf Coleman [Col85a] een methode om (een licht grotere verzameling dan) $\overline{J(\mathbb{Q})} \cap C \subset J$ te berekenen, waar $\overline{J(\mathbb{Q})}$ de afsluiting van $J(\mathbb{Q})$ in J is. Hij deed dit door met bepaalde vectorruimte geassocieerd aan C en J te berekenen, zogeheten *cohomologiegroepen*.

Heden ten dage zijn er veel variaties van deze methode, en het spel is om methodes te vinden die werken voor steeds meer en meer krommen, en steeds

kleinere en kleinere verzamelingen punten produceren (die nog steeds alle rationale punten bevatten).

In 2009 generaliseerde Kim de Chabauty–Coleman naar een veel sterkere vorm [Kim09]. In plaats van met de abelianisatie van de fundamenteaalgroep $G = \pi_1(C)$ te werken, werkte Kim met niet-abelse quotiënten van de fundamenteaalgroep G . Kim definieerde een rijtje van quotiënten

$$G \rightarrow \cdots \rightarrow G_n \rightarrow G_{n-1} \rightarrow \cdots \rightarrow G_2 \rightarrow G_1 = G^{\text{ab}} = \pi_1(J)$$

en voor elke G_n een deelverzameling C_n van C (niet noodzakelijk eindig) die de rationale punten bevat, op zo een manier dat we een rijtje

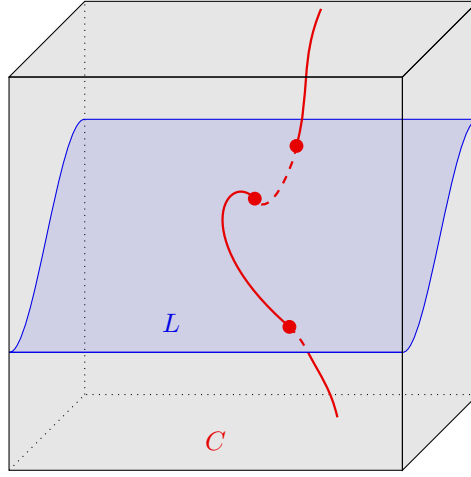
$$C(\mathbb{Q}) \subset \cdots \subset C_n \subset C_{n-1} \subset \cdots \subset C_2 \subset C_1$$

krijgen.

Net zoals Coleman, definieerde Kim deze verzamelingen met behulp van cohomologiegroepen. En inderdaad, voor de abelianisatie G_1 krijgt Kim dezelfde verzameling als Coleman vindt. Deze generalisatie zou enorme gevolgen kunnen hebben; er is het vermoeden dat voor elke kromme C van geslacht minstens 2, ongeacht de waarde van r , het rijtje $C_1, C_2, \dots$ uiteindelijk eindig is, en sterker nog, dat er altijd een n is met $C_n = C(\mathbb{Q})$. Helaas blijkt het berekenen van deze verzameling lastig voor $n > 1$. De beste methode tot nu toe is (*cohomologische*) *kwadratische Chabauty*. Dit gebruikt een groep G_{Coh} met $G_2 \rightarrow G_{\text{Coh}} \rightarrow G_1$, en geeft een verzameling punten C_{Coh} met $C_2 \subset C_{\text{Coh}} \subset C_1$. Zij ρ de Néron–Severi-rang van J (een bepaald getal in $\mathbb{Z}_{\geq 1}$ geassocieerd aan J). Dan is C_{Coh} eindig als $r < g + \rho - 1$. Deze methode is effectief gemaakt door Balakrishnan, Dogra en Müller for $r = g, \rho > 1$ [BBM16, BD18, BD21, BDM⁺21]. Één van de belangrijkste prestaties van deze methode is het berekenen van de rational punten op de “vervloekte kromme” $X_s(13)$ [BDM⁺19].

Recent hebben Edixhoven en Lido een meer meetkundige aanpak voor effectieve Chabauty-berekeningen geïntroduceerd. Hun methode staat bekend als *meetkundige kwadratische Chabauty* [EL21]. Ze vervangen de Abel–Jacobi-afbeelding $C \rightarrow J$ met een andere afbeelding $C \rightarrow T$, en ze bewijzen dat de doorsnede $C \cap T(\mathbb{Q}) \subset T$ eindig is als $r < g + \rho - 1$. Een visualisatie voor $r = g = \rho = 2$ is te zien in Figuur 9. Er werd vermoed dat de meetkunde kwadratische Chabauty-methode te vergelijken is met de cohomologische kwadratische Chabauty-methode, maar dit was een open probleem.

In mijn masterscriptie [Spe20] gebruikte ik de meetkundige methodes van [EL21] om de map $C \rightarrow J$ te bestuderen, in een methode genaamd *meet-*



Figuur 9: Een visualisatie van de meetkundige kwadratische Chabauty-methode voor $r = g = \rho = 2$: de rationale punten $T(\mathbb{Q})$ liggen op een oppervlak (blauw) in T (zwart), en de kromme C (rood) doorsnijdt dit oppervlak in een eindige verzameling. Deze doorsnede $C \cap T(\mathbb{Q})$ bevat de rationale punten van C , en dus is de verzameling rationale punten $C(\mathbb{Q})$ eindig.

kundige lineaire Chabauty. Het vermoeden was dit te vergelijken was met de Chabauty–Coleman-methode.

Samen met Sachi Hashimoto hebben we in Hoofdstuk 5 de volgende stelling bewezen.

Stelling (Theorem 5.5.1). *De meetkundige lineaire Chabauty-methode presteert beter dan de Chabauty–Coleman-methode, op de volgende manier. Zij C_{CC} de verzameling punten gevonden door de Chabauty–Coleman-methode, en C_{GLC} de verzameling punten gevonden door de meetkundige lineaire Chabauty-methode. Dan hebben we inclusies*

$$C(\mathbb{Q}) \subset C_{CC} \subset C_{GLC},$$

en er is een expliciete karakterisatie van $C_{GLC} \setminus C_{CC}$.

En samen met Juanita Duque-Rosero en Sachi Hashimoto hebben we in Hoofdstuk 6 de volgende stelling over kwadratische Chabauty bewezen.

Stelling (Theorem H). *De meetkundige kwadratische Chabauty-methode presteert beter dan de cohomologische kwadratische Chabauty-methode, op de vol-*

gende manier. Zij C_{Coh} de verzameling punten gevonden door de cohomologische kwadratische Chabauty-methode, en C_{Geo} de verzameling punten gevonden door de meetkundige kwadratische Chabauty-methode. Dan hebben we inclusies

$$C(\mathbb{Q}) \subset C_{\text{Coh}} \subset C_{\text{Geo}},$$

en er is een expliciete karakterisatie van $C_{\text{Geo}} \setminus C_{\text{Coh}}$.

In Hoofdstuk 7 focussen we op een specifiek ingrediënt van kwadratische Chabauty (zowel cohomologische als meetkundige), namelijk *lokale hoogtes* (om precies te zijn, de lokale hoogtes weg van p als we de p -adische getallen $\mathbb{Q}_p$ aan het gebruiken zijn). Deze vormen een eindige set getallen geassocieerd aan de kromme. In de literatuur zijn veel voorbeelden gekozen zodanig dat de lokale hoogtes 0 zijn, om te zorgen dat er geen niet-triviale lokale hoogtes berekend hoeven te worden. Samen met Alex Betts, Juanita Duque-Rosero en Sachi Hashimoto geven we een algoritme om de lokale hoogtes te berekenen. We gebruiken dit om te bewijzen dat de kromme met vergelijking

$$y^2 = x^6 + 18/5x^4 + 6/5x^3 + 9/5x^2 + 6/5x + 1/5$$

precies 10 rationale punten heeft (Theorem I). Dit is het eerste voorbeeld van de kwadratische Chabauty-methode toegepast op een kromme met twee niet-triviale lokale hoogtes.

