Het tellen van krommen op het product van twee projectieve lijnen over een eindig lichaam

Bas van Rooij
4155572

Begeleider: Prof. dr. C.F. Faber

Universiteit Utrecht

17 juni 2016

Universiteit Utrecht

Inhoudsopgave

1 Introductie

In de algebraïsche meetkunde worden algebraïsche variëteiten bestudeerd. Een algebraïsche variëteit is een nulpuntsverzameling van een aantal polynomen. Een algebraïsche variëteit heeft een dimensie en de variëteiten van dimensie 1 heten krommen. Deze krommen spelen een belangrijke rol in de algebraïsche meetkunde.

Een niet-singuliere, projectieve, irreducibele algebraïsche kromme heeft een geslacht g. Het geslacht van een kromme is een geheel getal ≥ 0. Het geslacht van een kromme is invariant onder isomorfie.

Het doel van deze scriptie is het tellen van bepaalde krommen van geslacht 4 over eindige lichamen. Hiervoor heb ik een computerprogramma ontwikkeld dat de krommen telt. De krommen die geteld worden zijn de krommen van type $(3,3)$ op het product van twee projectieve lijnen ($\mathbb{P}^1 \times \mathbb{P}^1$) over een eindig lichaam. Er is een stelling [1, V, p.362, Ex 1.5.2] die zegt dat voor krommen van type (a,b) op $\mathbb{P}^1 \times \mathbb{P}^1$ het geslacht gelijk is aan $(a-1)(b-1)$. Hieruit volgt dat de krommen van type $(3,3)$ inderdaad geslacht 4 hebben. De reden om geslacht 4 te tellen is dat over krommen van geslacht ≤ 3 al veel bekend is.

Als we de krommen over een eindig lichaam k tellen, worden ze op de k-isomorfismen na geteld. Van elke isomorfieklasse wordt het aantal punten op de kromme geteld en vervolgens gedeeld door het aantal k-automorfismen. In het bijzonder gaat het programma voor een aantal kleine eindige lichamen k voor alle isomorfieklassen het aantal k-automorfismen tellen en het aantal punten op de kromme over k, k_2, k_3 en k_4. Hier zijn k_2, k_3 en k_4 uitbreidingslichamen van graad $2, 3$ en 4.

De reden om op deze manier te tellen is dat we zo de punten tellen over een eindig lichaam van een deel van de moduliruimte M_4 van gladde krommen van geslacht 4. Dit geeft veel informatie over de cohomologie van M_4. De moduliruimten M_g spelen een zeer belangrijke rol in de algebraïsche meetkunde.

Het tellen van het aantal punten geeft informatie voor het corresponderende deel van de modulieruimte $M_{4,n}$ van n-gepunte krommen van geslacht 4. Een berekening die we kunnen maken met behulp van deze lijst zijn de volgende sommen over eindige lichamen k.

$$\sum_{C \in (3,3)} \frac{1}{|Aut_k(C)|} |C(k_i)|$$

met k_i een uitbreidingslichamen van k van graad i. De som gaat over alle isomorfieklasse van gladde krommen C van het type $(3,3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$. Hier is $|C(k_i)|$ het aantal punten op de kromme over k_i. Deze sommen geven informatie over het corresponderende deel van de moduliruimte $M_{4,1}$. Op eenzelfde manier kunnen we sommen voor de deelruimte $M_{4,2}$ berekenen. Dit zijn de krommen met twee punten en berekenen we door te tellen met $|C(k_i)||C(k_i) - 1|$. Het tweede punt kan alles zijn behalve het eerste punt.

2 Algebraïsche achtergrond

2.1 Lichamen

Hier volgt een korte samenvatting van theorie en definities over lichamen die in het vervolg gebruikt worden. Het is grotendeels gebaseerd op het boek *Fundamental Concepts of Abstract Algebra* van *Gertrude Ehrlich* [2].

We beginnen met de definitie van een **lichaam**.

Definitie 1. *Een lichaam is een commutatieve ring met een eenheid niet gelijk aan* 0*, waarin alle niet-nul elementen een multiplicatieve inverse hebben.*

Lichamen kunnen bevat zijn in een groter lichaam met dezelfde operatoren, in dit geval spreekt men van een **deellichaam**. Het grotere lichaam is een **uitbreidingslichaam**.

Definitie 2. *Een deelring k van een lichaam K heet een deellichaam van K als k een lichaam vormt onder de operaties van K. Andersom heet K een uitbreidingslichaam van k.*

In ons geval zijn we vooral geïnteresseerd in **eindige lichamen**. Dit zijn lichamen met een eindig aantal elementen. Een voorbeeld van veelgebruikte eindige lichamen zijn de lichamen $\mathbb{Z}/p\mathbb{Z}$ met p een priemgetal. Deze lichamen hebben p elementen.

Lichamen hebben een **karakteristiek**.

Definitie 3. *Voor een lichaam k is het kleinste getal n de karakteristiek van k, als de eenheid van k een n aantal keer bij zichzelf opgeteld gelijk aan* 0 *is. Dit wordt genoteerd met $char(k) = n$. Als er geen zodanige n bestaat, is de karakteristiek gelijk aan* 0*.*

De karakteristiek is altijd gelijk aan 0 of aan een priemgetal p. Voor de eindige lichamen $\mathbb{Z}/p\mathbb{Z}$ is de karakteristiek gelijk aan p. In het bijzonder geldt dat voor elk eindig lichaam de karakteristiek gelijk aan een priemgetal p is.

Voor eindige lichamen gelden de volgende stellingen.

Stelling 1. *Voor een eindig lichaam k bestaat er een priemgetal p en een getal $n \in \mathbb{Z}_{\geq 1}$ zodat $|k| = p^n$.*

Stelling 2. *Voor elk priemgetal p en elke $n \in \mathbb{Z}_{\geq 1}$ bestaat er een eindig lichaam k met p^n elementen.*

Stelling 3. *Als twee eindige lichamen k en k' hetzelfde aantal elementen bevatten, dan zijn k en k' isomorf.*

Voor de bewijzen, zie [2].

Uit Stelling 3 volgt dat alle eindige lichamen met een gegeven aantal elementen isomorf zijn. Hierdoor kunnen we spreken over een eindig lichaam $\mathbb{F}_q$ waar q het aantal elementen van het lichaam is.

In het vervolg hebben we ook nog de volgende stellingen nodig.

Stelling 4. *Voor een eindig lichaam k en een eindig uitbreidingslichaam K geldt dat het aantal elementen van K altijd een macht van het aantal elementen van k is.*

Stelling 5. *Voor elk priemgetal p en elke $n, m \in \mathbb{Z}_{\geq 1}$ met $n|m$ geldt dat er voor het eindige lichaam $\mathbb{F}_{p^n}$ een uitbreidingslichaam $\mathbb{F}_{p^m}$ bestaat.*

We gaan verder veelvuldig gebruik maken van **polynomen** over lichamen.

Definitie 4. *Een polynoom f over een lichaam k is een polynoom met coëfficiënten in k. Een polynoom in de variabele X heeft de volgende vorm*

$$f = a_n X^n + \ldots + a_1 X + a_0$$

*met $a_n, \ldots, a_0 \in k$. Als $a_n \neq 0$, dan is de **graad** van f gelijk aan n. De ring van alle polynomen over k wordt genoteerd met $k[X]$.*

Polynomen van graad n heten **monisch** als de coëfficiënt van X^n gelijk aan 1 is. Polynomen kunnen ook **multivariant** zijn. Dit zijn polynomen in meer dan één variabele. De verzameling van polynomen met n variabelen over een lichaam k wordt genoteerd met $k[X_1, \ldots, X_n]$. Hier zijn $X_1, \ldots, X_n$ de variabelen van de polynomen.

In het vervolg gaan we het vaak hebben over **nulpunten** van een polynoom.

Definitie 5. *Zij k een lichaam en $f \in k[X_1, \ldots, X_n]$ een polynoom. Een punt $p = (p_1, \ldots, p_n)$ is een nulpunt van f als $f(p) = 0$.*

Er zijn lichamen k waarvoor niet alle polynomen $f \in k[X]$ een nulpunt in k hebben. Echter, voor elk lichaam k bestaat er een uitbreidingslichaam K waarin een polynoom $f \in k[X]$ een nulpunt heeft. In het vervolg gaan we gebruik maken van de volgende stelling hierover.

Stelling 6. *Zij $k = \mathbb{F}_q$ een eindig lichaam. Een irreducibel polynoom $f \in k[x]$ splitst volledig in lineaire factoren over het uitbreidingslichaam $K = k[x]/fk[x]$.*

Een minimaal uitbreidingslichaam waarin elk polynoom $f \in k[X]$ een nulpunt heeft wordt de **algebraïsche afsluiting** van k genoemd. Voor elk lichaam bestaat er een algebraïsche afsluiting [2, p. 249].

2.2 Krommen

De volgende sectie geeft een inleiding over krommen. De inhoud is grotendeels gebaseerd op het boek *Algebraic Curves* van *William Fulton* [3].

Definitie 6. *Een **vlakke affiene algebraïsche kromme** is de verzameling van alle nulpunten van een niet-constant polynoom f in twee variabelen over een lichaam k.*

Het polynoom f waardoor zo'n kromme C bepaald is, wordt ook wel de **vergelijking** van C genoemd.

Wij zijn geïnteresseerd in krommen op $\mathbb{P}^1 \times \mathbb{P}^1$ over een eindig lichaam. Voor we zulke krommen kunnen definiëren, moeten we eerst kijken naar de **affiene ruimten** $\mathbb{A}^n(k)$ over een lichaam k.

Definitie 7. *Voor een lichaam k is $\mathbb{A}^n(k)$ de verzameling n-tupels met elementen uit k. We noemen $\mathbb{A}^n(k)$ de affiene n-ruimte over k.*

Als het lichaam k duidelijk is, wordt dit weggelaten in de notatie en schrijven we alleen $\mathbb{A}^n$. Elementen van $\mathbb{A}^n$ worden *punten* genoemd.

Aan de verzamelingen $\mathbb{A}^n$ kunnen we punten in het oneindige toevoegen. Deze nieuwe ruimten heten de **projectieve ruimten** en worden genoteerd met $\mathbb{P}^n$.

Definitie 8. *De projectieve ruimte $\mathbb{P}^n(k)$ over een lichaam k is de verzameling lijnen in $\mathbb{A}^{n+1}(k)$ door het punt $(0, \dots, 0) \in \mathbb{A}^{n+1}(k)$.*

De lijnen kunnen gerepresenteerd worden door punten in $\mathbb{A}^{n+1}\backslash\{0\}$. Elk punt $(p_1, \dots, p_{n+1}) \in \mathbb{A}^{n+1}\backslash\{0\}$ definieert de lijn $(\lambda p_1, \dots, \lambda p_{n+1})$ door het punt $0 \in \mathbb{A}^{n+1}$. Hieruit volgt dat de punten $(a_0, \dots, a_n), (b_0, \dots, b_n) \in \mathbb{P}^n$ dezelfde lijn representeren als een $\lambda \neq 0$ bestaat zodat $(a_0, \dots, a_n) =$
$(\lambda b_0, \dots, \lambda b_n)$. Dit heeft tot gevolg dat we voor de punten waarvan de eerste coördinaat niet 0 is, een λ kunnen vinden zodat deze punten gerepresenteerd worden door de punten $(1, p_1, \dots, p_n) \in \mathbb{A}^{n+1}$. Deze punten in $\mathbb{P}^n$ worden dus gegeven door de punten $(p_1, \dots, p_n) \in \mathbb{A}^n$. De punten met de eerste coördinaat gelijk aan 0 kun je beschouwen als de punten in oneindig. Deze punten kunnen gerepresenteerd worden door de punten $(p_1, \dots, p_n) \in \mathbb{P}^{n-1}$, waarbij elk punt correspondeert met het punt $(0, p_1, \dots, p_n) \in \mathbb{P}^n$. Nu zien we dat $\mathbb{P}^n$ een disjuncte vereniging van $\mathbb{A}^n$ en $\mathbb{P}^{n-1}$ is.

In het vervolg gaan wij alleen werken op $\mathbb{P}^1$ over een eindig lichaam k. Deze verzameling ziet er als volgt uit:

$$\mathbb{P}^1(k) = \{[x : 1] | x \in k\} \cup \{(1 : 0)\}$$

Een polynoom heet **homogeen** als alle eentermen een gelijke totale graad hebben. Een voorbeeld is het polynoom $f(x, y, z) = x^4y + xyz^3 + x^2z^3$. De som van de machten in elke eenterm is gelijk aan 5.

Nu kunnen we krommen van type $(3, 3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ over een eindig lichaam definiëren.

Definitie 9. *Een kromme C van type $(3, 3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ over een lichaam k is een kromme met als vergelijking een niet-constant bihomogeen polynoom van orde $(3, 3)$ in $((x_0 : x_1), (y_0 : y_1)) \in \mathbb{P}^1 \times \mathbb{P}^1$ met coëfficiënten in k.*

Een voorbeeld is een kromme gedefinieerd over $k = \mathbb{Z}/5\mathbb{Z}$ door het polynoom $f((x_0 : x_1), (y_0 : y_1)) = x_1^3y_0^3 + 2x_0x_1^2y_0y_1^2 + 4x_0^3y_1^3$.

In het vervolg zullen we het altijd hebben over krommen op $\mathbb{P}^1 \times \mathbb{P}^1$ over een eindig lichaam, tenzij anders vermeld.

2.3 Aantal krommen op $\mathbb{P}^1 \times \mathbb{P}^1$

Nu we de definitie van krommen van type $(3, 3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ over een eindig lichaam $\mathbb{F}_q$ hebben, kunnen we gaan bepalen hoeveel verschillende krommen er bestaan over een gegeven eindig lichaam $\mathbb{F}_q$. Het totaal aantal krommen van type $(3, 3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ over een gegeven eindig lichaam $\mathbb{F}_q$ is gevat in het volgende lemma:

Lemma 1. *Het aantal krommen bihomogeen van orde* $(3,3)$ *op* $\mathbb{P}^1 \times \mathbb{P}^1$ *over een eindig lichaam* $\mathbb{F}_q$ *is gelijk aan* $\frac{q^{16}-1}{q-1}$.

Bewijs. Een homogene kromme van orde 3 op $\mathbb{P}^1$ heeft 4 mogelijkheden voor eentermen, namelijk $x_0^3, x_0^2x_1, x_0x_1^2$ en x_1^3. Dit geeft voor een bihomogene kromme van orde $(3,3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ in totaal 16 mogelijkheden voor eentermen. Elke eenterm heeft q mogelijkheden voor de coëfficiënt, namelijk alle elementen van $\mathbb{F}_q$. Dit geeft q^{16} mogelijke krommen. Hier valt het nulpolynoom onder. De kromme met als vergelijking het nulpolynoom wordt buiten beschouwing gelaten, deze trekken we ervan af en we houden $q^{16}-1$ krommen over. Krommen zijn nulpuntsverzamelingen van polynomen. Als twee polynomen een scalair van elkaar zijn, hebben ze dezelfde nulpunten en zijn de krommen gelijk. We moeten nog de scalairen eruit halen. Voor een eindig lichaam $\mathbb{F}_q$ geldt dat er $q-1$ scalairen zijn. Dit betekent dat elke kromme $q-1$ scalairen heeft. Het totaal aantal krommen is dus het totaal aantal mogelijke polynomen gedeeld door alle mogelijke scalairen, ofwel $\frac{q^{16}-1}{q-1}$. □

2.4 Gladde krommen

Voor het tellen kijken we alleen naar gladde krommen. Voor de definitie van een gladde kromme moeten we eerst weten wat een singulier punt is. Hiervoor moeten we de partiële afgeleide van een polynoom over een lichaam definiëren.

Definitie 10. *Zij* k *een lichaam en* $f \in k[X_1, \ldots, X_n]$ *een polynoom. Voor de partiële afgeleiden van* f *naar de variabele* X_i*, beschouwen we* f *als*

$$f = a_n X_i^n + \ldots + a_1 X_i + a_0$$

met $a_n, \ldots, a_0 \in k[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$*. De partiële afgeleide naar* X_i *wordt genoteerd met* $\frac{\partial f}{\partial X_i}$ *en is gelijk aan*

$$\frac{\partial f}{\partial X_i} = \sum_{j \geq 1} j a_j X_i^{j-1}$$

Definitie 11. *Een punt* P *is een singulier punt van een vlakke algebraïsche kromme* C *als* P *een punt op* C *is en als* P *een nulpunt van alle partiële afgeleides van de vergelijking van* C *is.*

Merk hier op dat voor een lichaam k en een kromme C op $\mathbb{P}^1 \times \mathbb{P}^1$ een singulier punt niet over k gedefinieerd hoeft te zijn. Zoals al eerder vermeld is, hoeven de nulpunten van een polynoom niet over het lichaam zelf gedefinieerd te zijn. Een singulier punt is wel over de algebraïsche afsluiting van k gedefinieerd.

Nu we singuliere punten kennen, kunnen we een gladde kromme definiëren.

Definitie 12. *Als een kromme* C *een singulier punt bevat, is* C *een singuliere kromme. Als* C *niet singulier is, is* C *een gladde kromme.*

In de volgende sectie gaan we kijken hoe het programma kan berekenen of een kromme glad is.

3 Bepalen van gladheid en automorfismen

3.1 Bepalen van de gladheid van krommen

3.1.1 Affiene overdekking van een kromme

Voor het bepalen of een kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ glad is of niet, moeten we bepalen of de kromme een singulier punt bevat. Om hier achter te komen gaan we gebruik maken van affiene overdekkingen van $\mathbb{P}^1 \times \mathbb{P}^1$.

De ruimte $\mathbb{P}^1 \times \mathbb{P}^1$ is te overdekken met vier kopieën van $\mathbb{A}^1 \times \mathbb{A}^1$. Om dit in te zien definiëren we eerst $U_i = \{(x_1, \ldots, x_{n+1}) \in \mathbb{P}^n | x_i \neq 0\}$. Dit zijn de verzamelingen van punten in $\mathbb{P}^n$ waarvan de i'de coördinaat niet nul is. De punten kunnen gerepresenteerd worden door de punten met $x_i = 1$. We kunnen $\mathbb{P}^n$ schrijven als $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$. Als we nu kijken naar de afbeelding $\phi_i : \mathbb{A}^n \to U_i$ gedefinieerd door

$$\phi_i : (a_1, \ldots, a_n) \to (a_1, \ldots, a_{i-1}, 1, a_i, \ldots, a_n),$$

dan zien we dat dit een 1-op-1 relatie is tussen $\mathbb{A}^n$ en U_i. We zien nu dat $\mathbb{P}^n$ overdekt is met $n+1$ keer de ruimte $\mathbb{A}^n$. Voor het geval $\mathbb{P}^1$ zien we dat er twee kopieën van $\mathbb{A}^1$ zijn die samen $\mathbb{P}^1$ volledig overdekken. Voor $\mathbb{P}^1 \times \mathbb{P}^1$ geeft dit vier kopieën van $\mathbb{A}^1 \times \mathbb{A}^1$.

Wij kunnen de overdekking maken door achtereen $x_0 = y_0 = 1$, $x_0 = y_1 = 1$, $x_1 = y_0 = 1$ en $x_1 = y_1 = 1$ in de vergelijking van een kromme te nemen. Op deze manier houden we vier affiene krommen over in twee variabelen. Met het volgende lemma kunnen we gebruik maken van de affiene overdekking.

Lemma 2. *Als een kromme C op $\mathbb{P}^1 \times \mathbb{P}^1$ een singulier punt P heeft, bestaat er een affiene overdekking met een singulier punt.*

Bewijs. Stel een kromme C op $\mathbb{P}^1 \times \mathbb{P}^1$ heeft een singulier punt $P = ((x_0 : x_1), (y_0 : y_1))$. Stel, zonder verlies van generaliteit, dat $x_1, y_1 \neq 0$. Nu bestaat er een λ zodat we P kunnen herschrijven in de vorm $P = ((\lambda x_0 : 1), (\lambda y_0 : 1))$. Dit punt ligt op de affiene kromme met $x_1 = y_1 = 1$ en is nog steeds een singulier punt van C. Dit betekent dat de partiele afgeleides naar x_0 en y_0 van C nog steeds 0 zijn. Deze twee partiele afgeleides van C, voor $x_1 = y_1 = 1$, zijn precies alle partiële afgeleides van de affiene kromme. Hieruit volgt dat het punt $(\lambda x_0, \lambda y_0)$ op de affiene kromme ligt en dat alle partiële afgeleides van de affiene kromme 0 zijn in het punt. Ofwel, $(\lambda x_0, \lambda y_0)$ is een singulier punt van de affiene kromme met $x_1 = y_1 = 1$. □

Dit lemma stelt ons in staat om de kromme C te overdekken met vier affiene vlakke krommen en te controleren of een van deze krommen een singulier punt bevat. Voor het vervolg beschouw ik de vergelijking van een affiene kromme op $\mathbb{A}^1 \times \mathbb{A}^1$ als polynoom in de twee variabelen x en y.

3.1.2 Het bepalen van de gladheid van een affiene kromme

We gaan nu kijken hoe we kunnen bepalen of een affiene kromme op $\mathbb{A}^1 \times \mathbb{A}^1$ een singulier punt bevat. Een manier om dit te doen is met behulp van **resultanten**. De resultante is een operatie waarmee gekeken kan worden of twee polynomen een gemeenschappelijk nulpunt hebben. Voor de definitie van resultanten hebben we eerst de volgende definities nodig.

Definitie 13. *Een univariant polynoom is een polynoom in een variabele.*

Definitie 14. *Zij $f(x)$ en $g(x)$ twee univariante niet-constante polynomen. Stel $f(x) = a_n x^n + \ldots + a_0$ met graad n en $g(x) = b_m x^m + \ldots + b_0$ met graad m en stel $n > m$. De Sylvester matrix $S_{f,g}$ van de polynomen f en g is als volgt gedefinieerd*

$$S_{f,g} = \begin{pmatrix} a_n & a_{n-1} & \ldots & a_0 & 0 & & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_0 & 0 & \ldots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & & & 0 & a_n & a_{n-1} & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_0 & 0 & & \ldots & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_0 & 0 & \ldots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & & & 0 & b_m & b_{m-1} & \ldots & b_0 \end{pmatrix}$$

Definitie 15. *De resultante van twee univariante niet-constante polynomen f en g is gelijk aan de determinant van de Sylvester matrix $S_{f,g}$. Dit wordt genoteerd met $Res_{f,g}$.*

Door het volgende lemma kunnen we gebruik maken van resultanten.

Lemma 3. *Zij $f(x)$ en $g(x)$ twee niet-constante polynomen. De resultante $Res_{f,g}$ is 0 dan en slechts dan als f en g een gemeenschappelijk nulpunt hebben.*

Voor het bewijs, zie [4, p203, IV §8, Corollary 8.4]

Dit lemma kunnen we als volgt gebruiken. Voor een singulier punt P van een affiene kromme C op $\mathbb{A}^1 \times \mathbb{A}^1$ met vergelijking $f(x, y)$ geldt

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Aangezien P een gemeenschappelijk nulpunt is van de vergelijking van de kromme C en beide partiële afgeleides, moeten volgens Lemma 3 de resultanten van de kromme en zijn partiële afgeleides nul zijn.

Merk hier op dat de Sylvester matrix gebruik maakt van twee univariante polynomen en dat de vergelijking van de affiene kromme en zijn partiële afgeleides niet univariant zijn. We kunnen echter deze polynomen opvatten als een univariant polynoom in een van de twee variabelen, met als coëfficienten polynomen in de andere variabele. Op deze manier kunnen we een resultante nemen in een specifieke variabele. Dit is de variabele ten opzichte waarvan we de kromme als univariant polynoom beschouwen. Dus als we twee polynomen $P(x, y)$ en $Q(x, y)$ hebben, is de resultante $Res_{P,Q}(x)$ gelijk aan de determinant van de Sylvester matrix $S_{P,Q}$ waarbij P en Q opgevat worden als univariante polynomen in x met als coëfficienten polynomen in y. De resultante levert in dit geval een polynoom in y op.

We kijken, zonder verlies van generaliteit, naar de resultanten naar x. Er zijn drie resultanten die we kunnen nemen, namelijk $Res_{f,\frac{\partial f}{\partial x}}(x)$, $Res_{f,\frac{\partial f}{\partial y}}(x)$ en $Res_{\frac{\partial f}{\partial x},\frac{\partial f}{\partial y}}(x)$. Deze resultanten leveren allemaal een polynoom in y op. De y coördinaat van een singulier punt is een gemeenschappelijk nulpunt van alle drie

de resultanten. Met het volgende lemma kunnen we het stelsel vergelijkingen vereenvoudigen. Hiervoor hebben we eerst de volgende stelling nodig.

Stelling 7. *Laat $f \in k[x]$ een polynoom met positieve graad over een lichaam k zijn. Als f een nulpunt $x_0 \in k$ heeft, bestaat er een $g \in k[x]$ zodat $f = (x - x_0)g$.*

Lemma 4. *Stel $f, g \in k[x]$ zijn twee polynomen over een lichaam k met een gemeenschappelijk nulpunt x_0. Dan heeft de $ggd(f, g)$ ook x_0 als nulpunt.*

Bewijs. Stel $f, g \in k[x]$ zijn twee polynomen over een lichaam k met een gemeenschappelijk nulpunt x_0. Uit Stelling 7 volgt dat de polynomen te schrijven zijn als $f = (x - x_0)h$ en $g = (x - x_0)l$ met $h, l \in k[x]$. Hieruit volg dat de ggd een factor $(x - x_0)$ bevat en x_0 als nulpunt heeft. □

Met behulp van dit lemma is het genoeg om te kijken naar de nulpunten van de ggd van de resultanten. Als wij alle nulpunten van de ggd vinden, hebben we alle mogelijke y waardes voor een singulier punt P. We kunnen hetzelfde doen voor de resultanten naar y en vinden alle mogelijkheden voor x. Het enige wat nog rest is het controleren van alle mogelijke punten op singulariteit in de oorspronkelijke kromme C.

Het is belangrijk om hier op te merken dat, zoals al eerder vermeld, de mogelijke x en y waardes van een singulier punt niet over k gedefinieerd hoeven te zijn. De ggd's kunnen een irreducibele factor over het oorspronkelijke lichaam k bevatten. We moeten de mogelijke x en y waardes zien als elementen van een uitbreidingslichaam K van k. We gaan een uitbreidingslichaam maken met nulpunten van de ggd's en proberen de nulpunten in de kromme over het uitbreidingslichaam K.

We kijken eerst naar het geval dat de ggd van de resultanten naar x of y constant is. Er zijn twee gevallen te onderscheiden, ondergebracht in de volgende lemma's.

Lemma 5. *Als de ggd van resultanten naar een variabele van een affiene kromme C op $\mathbb{A}^1 \times \mathbb{A}^1$ gelijk aan een constante ongelijk aan 0 is, is de kromme C glad.*

Bewijs. Stel, zonder verlies van generaliteit, dat de ggd van een kromme C naar x gelijk aan een constante ongelijk aan 0 is. Voor een singulier punt P van C geldt dat de ggd, voor de y waarde van P, gelijk aan nul is. Echter, voor een constante ongelijk aan 0 bestaat er geen enkele y zodat de constante 0 wordt. Er kan dus geen singulier punt bestaan en C is glad. □

Lemma 6. *Als de ggd van alle resultanten naar een variabele van een affiene kromme C op $\mathbb{A}^1 \times \mathbb{A}^1$ gelijk aan 0 is, is de kromme singulier.*

Bewijs. Stel, zonder verlies van generaliteit, dat de ggd van alle resultanten van de vergelijking $f(x, y)$ van een kromme C naar x gelijk aan 0 is. Dit is alleen mogelijk als alle afzonderlijke resultanten 0 zijn. In het bijzonder geldt $Res_{f, \frac{\partial f}{\partial x}}(x) = 0$. We beschouwen f en $\frac{\partial f}{\partial x}$ als polynomen in x met coëfficienten in $k[y]$. We gaan twee gevallen onderscheiden.

Voor het eerste geval nemen we aan dat de partiële afgeleide $\frac{\partial f}{\partial x}$ identiek 0 is. In dit geval is elk gemeenschappelijk nulpunt van f en $\frac{\partial f}{\partial y}$ een singulier punt. Er geldt dat $f(x, y)$ van orde $(3, 3)$ is en $\frac{\partial f}{\partial y}$ van orde $(3, 2)$. Deze twee krommen

hebben 15 snijpunten [1, V, §1] en dat zijn in het bijzonder singuliere punten van de kromme.

Het tweede geval is als $\frac{\partial f}{\partial x}$ niet identiek 0 is. Omdat $Res_{f,\frac{\partial f}{\partial x}}(x) = 0$, hebben f en $\frac{\partial f}{\partial x}$ een gemeenschappelijk nulpunt α in de algebraïsche afsluiting $\overline{k(y)}$. Het minimale polynoom p over $k(y)$ van het nulpunt α deelt $\frac{\partial f}{\partial x}$ en f. Er geldt $0 \neq p \in k(y)[x]$. Het minimale polynoom p is niet van het type $(0, 0$ en de partiële afgeleide $\frac{\partial f}{\partial y}$ is van het type $(3, 2)$. In het bijzonder hebben ze een gemeenschappelijk nulpunt [1, V, §1]. Dit gemeenschappelijke nulpunt is een singulier punt van de kromme C. □

In een van deze twee gevallen weten we direct of een kromme glad is. We beschouwen nu de ggd's met graad > 0. We splitsen eerst beide ggd's in irreducibele factoren over k en nemen van beide ggd's een irreducibele factor. Noem de factoren $P(y)$ voor de ggd naar x en $Q(x)$ voor de factor van de ggd naar y. Met behulp van het volgende lemma kunnen we een uitbreidingslichaam maken dat alle nulpunten van factoren $P(y)$ en $Q(x)$ bevat.

Lemma 7. *Zij k een eindig lichaam. Stel $f(x), g(x) \in k[x]$ zijn twee irreducibele polynomen. Stel $f(x)$ heeft graad n en $g(x)$ heeft graad m. De polynomen $f(x)$ en $g(x)$ splitsen volledig over het uitbreidinglichaam $k[x]/pk[x]$ met $p \in k[x]$ een irreducibel polynoom van graad $kgv(n, m)$.*

Bewijs. Uit Stelling 6 volgt dat het uitbreidingslichaam $k[x]/fk[x]$ alle nulpunten van $f(x)$ bevat en dat het uitbreidingslichaam $k/gk[x]$ alle nulpunten van $g(x)$ bevat. We zoeken nu een uitbreidingslichaam dat de nulpunten van beide polynomen bevat. Omdat $k[x]/fk[x]$ een eindig lichaam is, is het isomorf aan $\mathbb{F}_{q^n}$. Hetzelfde geldt voor het lichaam $k[x]/gk[x]$ met $\mathbb{F}_{q^m}$. Uit Stelling 4 volgt dat het aantal elementen van een uitbreidingslichaam altijd een macht is van het aantal elementen van het deellichaam. Dit betekent dat ons gezochte uitbreidingslichaam minstens $q^{kgv(m,n)}$ elementen moet bevatten. Uit Stelling 2 volgt dat er een eindig lichaam met zoveel elementen bestaat. Uit Stelling 5 volgt dat er voor zowel $\mathbb{F}_{q^n}$ als $\mathbb{F}_{q^m}$ altijd een uitbreidingslichaam met dit aantal elementen bestaat. Uit Stelling 3 volgt als laatste dat beide uitbreidingslichamen isomorf zijn aan elkaar. We mogen nu zelf een lichaam met $q^{kgv(n,m)}$ elementen creëren, want dit is volgens Stelling 3 ook isomorf aan beide uitbreidingslichamen. Wij maken het lichaam $k[x]/pk[x]$ met $p \in k[X]$ een irreducibel polynoom van graad $kgv(n, m)$. Dit lichaam bevat $q^{kgv(m,n)}$ elementen en bevat alle nulpunten van de polynomen f, g. □

Nu nemen we een irreducibel polynoom van graad $kgv(n, m)$ over k en we construeren het uitbreidinglichaam $K = k[x]/pk[x]$. Volgens Lemma 7 splitsen $P(y)$ en $Q(x)$ volledig over K. We proberen nu alle combinaties met nulpunten van $P(y)$ als y waarden en alle nulpunten van $Q(x)$ als x waarden als singuliere punten van de kromme C op $\mathbb{A}^1 \times \mathbb{A}^1$. Zodra we een singulier punt gevonden hebben, weten we dat de kromme singulier is. Als deze kopie van $\mathbb{A}^1 \times \mathbb{A}^1$ geen singuliere punten bevat, proberen we de andere drie kopieën op dezelfde manier. Als geen van deze affiene krommen singulier is, is de originele kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ glad.

3.2 Automorfismen van krommen

Elke isomorfieklasse willen we tellen met één gedeeld door $\#Aut_k(C)$. We bedoelen hier het aantal k-automorfismen van C op $\mathbb{P}^1 \times \mathbb{P}^1$. Om dit te berekenen gaan we eerst kijken naar de isomorfismen van C.

Hiervoor gaan we eerst kijken naar de automorfismen van $\mathbb{P}^1$. De automorfismen van $\mathbb{P}^1(k)$ worden gegeven door $PGL_2(k)$. Voor de definitie van $PGL_2(k)$ hebben we eerst de volgende definitie nodig.

Definitie 16. *Voor een lichaam k bestaat de groep $GL_n(k)$ uit de inverteerbare n bij n matrices over k. De operatie van $GL_n(k)$ is standaard matrix vermenigvuldiging.*

Voor het vervolg is het belangrijk om te weten hoeveel elementen $GL_n(k)$ geeft. Wij zijn alleen geïnteresseerd in het aantal elementen over de eindige lichamen $\mathbb{F}_q$.

Lemma 8. *De groep $GL_n(\mathbb{F}_q)$ bevat*

$$\prod_{i=0}^{n-1}(q^n - q^i)$$

elementen.

Bewijs. Voor een inverteerbare matrix moeten de kolommen onafhankelijk zijn. We gaan voor elke kolom het aantal mogelijkheden tellen. De eerste kolom mag alles behalve de nulvector zijn. Dit geeft ons $q^n - 1$ mogelijkheden. Voor de tweede kolom hebben we alle mogelijkheden min de veelvouden van de eerste kolom, dit zijn er $q^n - q$. De derde kolom heeft alle mogelijkheden min de veelvouden van de eerste en tweede kolom, ofwel $q^n - q^2$. Dit kan herhaald worden voor alle kolommen en geeft voor de i'de kolom $q^n - q^{i-1}$ aantal mogelijkheden. Hieruit volgt dat het totaal aantal mogelijkheden gelijk aan $\prod_{i=0}^{n-1}(q^n - q^i)$ is. □

Definitie 17. *Voor een lichaam k is de groep $Z_n(k)$ is de groep van niet-nul scalairen van de n bij n identiteitsmatrix. De operatie van $Z(k)$ is matrix vermenigvuldiging.*

Voor een eindig lichaam $\mathbb{F}_q$ bevat $Z_n(\mathbb{F}_q)$ precies $q - 1$ elementen.

Met behulp van $GL_n(k)$ en $Z_n(k)$ kunnen we $PGL_n(k)$ definieren.

Definitie 18. *Voor een lichaam k is de groep $PGL_n(k)$ gedefinieerd door $PGL_n(k) = GL_n(k)/Z_n(k)$.*

Wij gebruiken in het vervolg alleen $PGL_2(\mathbb{F}_q)$. Het aantal elementen van $PGL_2(\mathbb{F}_q)$ is gelijk aan $\frac{(q^2-1)(q^2-q)}{q-1} = q^3 - q$. De elementen van de groep PGL_2 geven de automorfismen van $\mathbb{P}^1$.

Lemma 9. *Voor een lichaam k zijn de automorfismen van $\mathbb{P}^1(k)$ gegeven door de elementen van de groep $PGL_2(k)$.*

Voor het bewijs, zie [1, p. 151, II, Example 7.1.1].

De isomorfismen van een kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ worden gegeven door $PGL_2 \times PGL_2$. Voor bihomogene krommen met graad $(a, a), a \in \mathbb{Z}_{\geq 1}$ geldt nog een extra bewerking. Dit komt overeen met het 'wisselen' van de $\mathbb{P}^1$'s. Dit wordt gedaan door het omwisselen van de x en y variabelen in de vergelijking van de kromme C op $\mathbb{P}^1 \times \mathbb{P}^1$.

Om het aantal k-automorfismen van een kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ te berekenen, kunnen we alle mogelijke isomorfismen berekenen en tellen hoeveel automorfismen er zijn. Op deze manier moeten er voor krommen van het type (a, a) per isomorfieklasse $2(q^3 - q)^2$ isomorfismen berekend worden. Het berekenen kan sneller als je de automorfismen splitst in twee isomorfismen.

Een automorfisme $(A \times B) \in (PGL_2 \times PGL_2)$ kunnen we als volgt schrijven.

$$(A \times B) = (A \times I) \circ (I \times B) \tag{1}$$

met $I \in PGL_2$ de identiteitsmatrix. We kunnen dit gebruiken om sneller het aantal automorfismen te berekenen. Met behulp van het volgende lemma kunnen het aantal automorfismen van een isomorfieklasse berekend worden.

Lemma 10. *Zij C een kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ over een eindig lichaam k. Zij n het aantal automorfismen van C van de vorm $(I \times B)$ en m het aantal isomorfismen van de vorm $(A \times I)$ die gelijk zijn aan een isomorfismen van de vorm $(I \times D)$. Het aantal k-automorfismen van C wordt gegeven door $Aut_k(C) = nm$.*

Bewijs. Stel C is een kromme op $\mathbb{P}^1 \times \mathbb{P}^1$ en n is het aantal automorfismen van de vorm $(I \times B)$. Er geldt $n \geq 1$, omdat de identiteit $(I \times I)$ meetelt. Stel m is het aantal isomorfismen van de vorm $(A \times I)$ die gelijk zijn aan $(I \times D)$, ofwel $(A \times I)(C) = (I \times D)(C)$. Voor elk zo'n isomorfisme geldt dat $(A^{-1} \times D)(C) = C$ een automorfisme geeft. Maar we kunnen eventueel meer automorfismen hieruit afleiden. Voor elke automorfismen van de vorm $(I \times E)$ geldt

$$(A^{-1} \times D) \circ (I \times E)(C) = (A^{-1} \times DE)(C) = C.$$

Hieruit volgt dat voor elk isomorfismen van de vorm $(A \times I)$ er n automorfismen te maken zijn.

Op deze manier worden alle automorfismen geteld. Stel we hebben een automorfisme $(F \times G)$. Dit is te schrijven als $(F \times I) \circ (I \times G)$. In het bijzonder geldt dat $(F \times I)(C) = (I \times G^{-1})(C)$. Merk op dat deze combinatie berekend wordt en meegeteld wordt als automorfisme.

□

Door dit lemma is het genoeg om alle isomorfismen van de vorm $(A \times I)$ en $(I \times B)$ te berekenen. Hieruit kan vervolgens het aantal k-automorfismen van C worden berekend. Dit geeft dat we $2(q^3 - q)$ isomorfismen moeten berekenen per isomorfieklasse.

Voor de extra bewerking op krommen van het type (a, a) moeten we de berekening nog een keer doen nadat we de variabelen x en y hebben omgedraaid. In dit geval berekenen we $4(q^3 - q)$ isomorfismen per isomorfieklasse.

4 Programma

In deze sectie kijken we naar de werking van het programma en waarom bepaalde keuzes gemaakt zijn. Hier wordt vooral beschreven hoe de losse berekeningen die hierboven beschreven zijn samenwerken.

Deze scriptie is gefocused op het tellen over eindige lichamen. We beginnen met het kijken hoe het programma met deze lichamen werkt. Als we over een lichaam $\mathbb{F}_p$ willen werken met p een priemgetal, gebruikt het programma het eindige lichaam $\mathbb{Z}/p\mathbb{Z}$. Als we over een eindig lichaam $\mathbb{F}_{p^n}$ werken, met p een priemgetal en $n \in \mathbb{Z}_{\geq 1}$, construeert het programma een uitbreidingslichaam van graad n over $k = \mathbb{Z}/p\mathbb{Z}$. Hiervoor neemt het een irreducibel polynoom $f \in k[x]$ van graad n en construeert het uitbreidingslichaam $k[x]/pk[x]$. Dit is een eindig lichaam met p^n elementen.

Voor het tellen van de krommen gaat het programma een lijst met krommen af. Voor elke kromme in de lijst bepaalt het programma eerst of de kromme isomorf is aan een voorafgaande kromme. Om dit te berekenen worden de isomorfismen in $(PGL_2 \times PGL_2)$ gesplitst zoals in vergelijking 1. In het bijzonder zijn twee krommen C_1 en C_2 isomorf als er twee isomorfismen $(A \times I), (I \times B) \in (PGL_2 \times PGL_2)$ bestaan zodat $(A \times I)(C_1) = (I \times B)(C_2)$. Hieruit volgt dat het isomorfisme $(A \times B^{-1})$ een isomorfisme van C_1 naar C_2 is. Voor de extra bewerking van krommen van orde (a, a) wordt deze berekening nog een keer gedaan nadat de variabelen x en y omgedraaid zijn. Om te kijken of twee krommen isomorf zijn, moeten er dus maximaal $4(q^3 - q)$ isomorfismen worden berekend.

Zoals net genoemd, wordt per kromme in de lijst gekeken of deze isomorf is aan een van de voorafgaande krommen. Het is niet efficiënt om per voorafgaande kromme dit individueel te berekenen. In plaats daarvan wordt het per isomorfieklasse berekend. Per isomorfieklasse wordt voor een representant alle $(A \times I)$ isomorfismen berekend en in een lijst opgeslagen. Voor elke nieuwe kromme worden alle $(I \times B)$ isomorfismen berekend en per isomorfie wordt gekeken of deze gelijk is aan een kromme in de lijst van linker isomorfismen van alle getelde isomorfieklassen. Zodra dit het geval is, behoort de kromme tot een isomorfieklasse die al geteld is. Anders behoort de kromme tot een isomorfieklasse die nog niet is geteld. Op deze manier kan met maar $(q^3 - q)$ isomorfismen berekend worden of een willekeurige kromme tot een isomorfieklasse behoort die al geteld is.

Zodra het programma een kromme tegenkomt die niet tot een isomorfieklasse hoort die al geteld is, berekent het programma de automorfismen van de kromme en daarna controleert het programma of de kromme glad of singulier is. Als de kromme singulier is, gaat het programma door naar de volgende kromme. Als de kromme glad is, gaat het programma het aantal punten over k, k_2, k_3 en k_4 tellen. Het aantal punten op de kromme en het aantal k-automorfismen wordt opgeslagen en het programma gaat door naar de volgende kromme.

Hier kan opgemerkt worden dat het niet voor de hand ligt om eerst het aantal automorfismen te berekenen en daarna pas te kijken of de kromme glad is. In het geval dat de kromme singulier zou zijn, gaan we direct door naar de volgende kromme en daarmee zou je onnodige berekeningen uitvoeren, namelijk het tellen van de automorfismen. De reden om toch eerst de automorfismen te berekenen, is omdat voor het tellen over kleine lichamen het sneller is om te berekenen of twee krommen isomorf zijn dan het bepalen of een kromme glad is. Om de automorfismen te tellen, worden de linker isomorfismen van de isomor-

fieklasse berekend. In het bijzonder wordt dus de isomorfieklasse toegevoegd aan de lijst isomorfieklassen die al geteld zijn. Hierdoor zullen de volgende singuliere krommen in dezelfde isomorfieklasse al afvallen omdat ze tot een isomorfieklasse behoren die al geteld is. Als je niet eerst de automorfismen telt, blijft de isomorfieklasse voor het programma als niet-geteld. Hierdoor zullen de volgende singuliere krommen in de isomorfieklasse elke keer als een nieuwe isomorfieklasse worden bestempeld, waarna opnieuw bepaald wordt of de kromme glad of singulier is. Aangezien het bepalen of een kromme glad is over een klein eindig lichaam langer duurt dan het bepalen of de kromme isomorf is aan een voorafgaande kromme, is het efficiënter om eerst de automorfismen te tellen.

We hebben nu besproken hoe het programma alle berekeningen uitvoert. Hierboven werd genoemd dat het programma een lijst met krommen afgaat. Het is mogelijk om de lijst met alle mogelijke krommen af te gaan, maar met behulp van normaalvormen is het mogelijk om de lijst een stuk korter te maken.

Het principe is gebaseerd op het feit dat voor een polynoom $f(x, y) = ax^3y^3 + bx^2y^3 + \dots$ met $a \neq 0$, de coëfficient a gelijk aan 1 gemaakt kan worden. Dit komt omdat scalairen van een vergelijking hetzelfde polynoom voorstelt. Vervolgens kan met de substitutie $x \to x - \frac{b}{3}$ de term x^2 gelijk aan 0 gemaakt worden. Omdat we delen door 3, kan dit niet gebruikt worden voor lichamen van $char(k) = 3$. Voor lichamen van $char(k) \neq 2$ is het mogelijk om dit te doen met de term x^2. In dit geval verdwijnt de term x. Het programma heeft alleen over de lichamen $\mathbb{F}_2, \mathbb{F}_3$ en $\mathbb{F}_4$ geteld. Voor de lichamen met karakteristiek 2 heeft het programma de volgende normaalvorm gebruikt. Voor gladde krommen geldt dat de coëfficient van $x_0^3y_0^3$ niet gelijk aan 0 is. Deze kunnen we vervolgens gelijk aan 1 maken. Met behulp van de substitie van hierboven naar zowel x_0 als y_0 kunnen we de termen $x_0^2x_1y_0^3$ en $x_0^3y_0^2y_1$ gelijk aan 0 maken. Op deze manier liggen 3 van de 16 termen vast en bestaat de lijst uit nog maar q^{13} krommen. Voor het lichaam $\mathbb{F}_3$ was het programma nog snel genoeg zonder normaalvormen.

5 Resultaten

Het programma heeft de isomorfieklassen over $\mathbb{F}_2$ en $\mathbb{F}_3$ kunnen tellen. Het tellen over $\mathbb{F}_4$ is een te grote berekening om binnen afzienbare tijd uit te rekenen op één computer. Voor $\mathbb{F}_4$ wilde ik het programma op een rekencluster laten draaien.

Hiervoor was eerst een kleine aanpassing aan het programma nodig. Een rekencluster werkt door het programma op meerdere cores tegelijkertijd te laten draaien. Hierdoor kan het programma parallel vele berekeningen uitvoeren. Het is nog niet gelukt om het programma volledig parallel te maken. In Sectie 4 staat dat het programma gelijk het aantal punten op de krommen over de lichamen k, k_2, k_3 en k_4 telt als het een nieuwe gladde isomorfieklasse tegenkomt. Het tellen van het aantal punten neemt de meeste tijd in beslag van alle berekeningen en dit deel van het programma is wel goed te paralelliseren. Voor $\mathbb{F}_4$ heeft het programma eerst een lijst van representanten van de isomorfieklasse berekend zonder gelijk de punten op de kromme te tellen. Hierna heb ik het programma zo aangepast dat hij parallel voor alle de representanten de punten over de lichamen telt. Ik heb het programma op een rekencluster gestart. Op het moment van schrijven draait het programma nog en daardoor zijn de resultaten nu nog niet beschikbaar.

Onderaan de pagina staat een tabel met de sommen uit de introductie over $\mathbb{F}_2$ en $\mathbb{F}_3$. De sommen gaan over de gladde krommen C van het type $(3,3)$ op $\mathbb{P}^1 \times \mathbb{P}^1$.

Naast het tellen van de isomorfieklassen, heeft het programma ter controle gladde krommen van andere ordes geteld. Het tellen van deze krommen gaat op dezelfde manier als de krommen van type $(3,3)$. Alleen het wisselen van de $\mathbb{P}^1$'s hangt af van de orde. In het bijzonder heeft het de gladde krommen van het type $(1,a)$ op $\mathbb{P}^1 \times \mathbb{P}^1$ geteld. Van deze krommen is bekend hoeveel gladde krommen er zijn. Dit is bevat in het volgende lemma.

Lemma 11. *Het aantal gladde krommen van type* $(1,a), a \in \mathbb{Z}_a$ *op* $\mathbb{P}^1 \times \mathbb{P}^1$ *over een eindig lichaam* $\mathbb{F}_q$ *is gelijk aan* $q^{2a}(q-1)$.

In appendix A staat de tabel waarin het aantal gladde krommen van verschillende types.

De code van het programma is te vinden op

$$https://git.science.uu.nl/S.B.vanRooij/smoothCurveCounter$$

	$\sum_C \frac{\lvert C(k)\rvert}{\lvert Aut_k(C)\rvert}$	$\sum_C \frac{\lvert C(k_2)\rvert}{\lvert Aut_k(C)\rvert}$	$\sum_C \frac{\lvert C(k_3)\rvert}{\lvert Aut_k(C)\rvert}$	$\sum_C \frac{\lvert C(k_4)\rvert}{\lvert Aut_k(C)\rvert}$
$\mathbb{F}_2$	858	1821	2603,5	4459
$\mathbb{F}_3$	46644	136484	300964	844792
$\mathbb{F}_4$				

6 Discussie

Met het programma gaat het waarschijnlijk niet lukken om binnen afzienbare tijd de sommen voor $\mathbb{F}_5$ te berekenen. Hiervoor is het programma op dit moment te langzaam. In deze sectie bespreek ik eventuele verbeterpunten voor het programma.

Als eerste kan de specifieke implementatie van het programma sneller. Vooral het tellen van het aantal punten op de krommen kan sneller. In het programma gebeurt dit op de *brute force* manier door simpelweg alle mogelijke punten te proberen. Voor het lichaam $k = \mathbb{F}_4$ geeft dit al $256^2 = 65536$ punten over k_4.

Daarnaast is het programma niet geheel parallel. Dit betekent dat je zelfs met een rekencluster waarschijnlijk niet ver komt. Voor het tellen over $\mathbb{F}_4$ op één computer was het niet-parallel gedeelte van het programma nog net snel genoeg om het uit te rekenen. Deze berekening duurde echter ruim 30 uur. Voor $\mathbb{F}_5$ zal het programma er ruim 60 dagen over doen. Ik denk echter wel dat het mogelijk is om het programma volledig parallel te maken.

Als laatste kan waarschijnlijk nog snelheid gehaald worden als het programma herschreven wordt in een andere programmeertaal. Ik heb gekozen voor $C\#$, maar met een lagere taal zoals C kan je het waarschijnlijk een stukje sneller krijgen. De reden waarom ik toch voor $C\#$ heb gekozen is omdat ik hier meer ervaring in heb. Ik heb nog nooit in C geprogrammeerd en verwachtte niet dat ik in de tijd van de scriptie genoeg ervaring zou opdoen om alles uit C te halen wat erin zit.

Appendix A

Lichaam	type	Totaal aantal krommen	Aantal singulieren krommen	Aantal gladden krommen
$\mathbb{F}_2$	(1,2)	63	39	24
	(1,3)	255	159	96
	(1,4)	1023	639	384
	(2,2)	511	367	144
	(2,3)	4095	2979	1116
	(3,3)	65535	49515	16020
	(3,4)	1048575	790599	257976
$\mathbb{F}_3$	(1,2)	364	148	216
	(1,3)	3280	1336	1944
	(1,4)	29524	12028	17496
	(2,2)	9841	4657	5184
	(2,3)	265720	126328	139392
	(3,3)	21523360	10608160	10915200
$\mathbb{F}_4$	(1,2)	1365	405	960
	(1,3)	21845	6485	15360
	(2,2)	87381	29781	57600
	(2,3)	5592405	1909605	3682800
	(3,3)	1431655765	502700965	928954800
$\mathbb{F}_5$	(1,2)	3906	906	3000
	(1,3)	97656	22656	75000
	(2,2)	488281	128281	360000
	(2,3)	61035156	16049556	44985600
$\mathbb{F}_7$	(1,2)	19608	3144	16464
	(1,3)	960800	154064	806736
	(2,2)	6725601	1193697	5531904
$\mathbb{F}_{11}$	(1,2)	177156	17436	159720
$\mathbb{F}_{13}$	(1,2)	402234	33138	369096

References

[1] Robin Hartshorne, *Algebraic Geometry*, Springer, New York, 1977

[2] Gertrude Ehrlich, *Fundamental Concepts of Abstract Algebra -Dover ed.*, Dover Publications, Mineola, New York, 1st edition, 2011.

[3] William Fulton, *Algebraic Curves,* Bejamin Publishing Company, New York, 1969

[4] Serge Lang, *Algebra*, Springer, New York, revised third edition, 2002