rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Maximale elliptische krommen over eindige lichamen

Bacheloronderzoek Wiskunde

Augustus 2009

Student: Peter Doetjes

Begeleider: Prof.dr. Jaap Top

Maximale elliptische krommen over eindige lichamen

Peter Doetjes

31 augustus 2009

Inleiding

We behandelen hier elliptische krommen over een eindig lichaam $\mathbb{F}_q$, deze krommen zijn van de vorm: $C : y^2 = x^3 + ax^2 + bx + c$, als q oneven is en waarbij het rechterlid geen meervoudige nulpunten heeft. Als q even is nemen we als vergelijking $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, met a_i in $\mathbb{F}_q$ en de eis dat het stelsel

$$\begin{cases} a_1x + a_3 = 0 \\ a_1y = x^2 + a_4 \\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \end{cases}$$ geen oplossingen heeft.

Van deze krommen kennen we de Hasse-Weil ongelijkheid:

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Deze ongelijkheid geeft aan hoeveel punten er op de kromme kunnen liggen, dit zijn naast de oplossingen ook nog *een punt op oneindig*. Dit punt op oneindig wordt gebruikt om van de oplossingen samen met dit punt een groep te maken (zie [1]).

Als we de Hasse-Weil ongelijkheid toepassen op de uitbreiding $\mathbb{F}_{q^n}$ van $\mathbb{F}_q$, dan volgt $\#C(\mathbb{F}_{q^n}) \leq q^n + 1 + 2\sqrt{q^n}$. Dus omdat het linkerlid een geheel getal is, is ook $\#C(\mathbb{F}_{q^n}) \leq q^n + 1 + \lfloor 2\sqrt{q^n} \rfloor$. In deze scriptie kijken we naar de vraag of er bij een gegeven C over $\mathbb{F}_q$ een n is zodat de ongelijkheid een gelijkheid wordt.

Hoofdstuk 1

Een belangrijke stelling

In dit korte hoofdstuk behandelen we een stelling en drie gevolgen ervan. Overal geven we met E een elliptische kromme aan.

Stelling 1.1 *$\forall E/\mathbb{F}_q, \exists \alpha \in \mathbb{C}$ met $|\alpha| = \sqrt{q}$ zodat voor elke $m \geq 1$ geldt:*

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 - \alpha^m - \overline{\alpha}^m.$$

Voor het bewijs verwijzen we naar [3], §2 van hoofdstuk 5. In hoofdstuk 2 zullen we een speciaal geval gaan behandelen.

Gevolg 1.2 *De α van stelling 1.1 is een nulpunt van $x^2 + ax + q$, voor zekere $a \in \mathbb{Z}$ met de eigenschap $a^2 - 4q \leq 0$*

Bewijs:
Neem $a = -\alpha - \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1 \in \mathbb{Z}$. Dan is $\alpha^2 + a\alpha + q = \alpha^2 - \alpha(\alpha + \overline{\alpha}) + \alpha\overline{\alpha} = 0$. Als $\alpha \in \mathbb{R}$ dan is $a^2 - 4q = (-\alpha - \overline{\alpha})^2 - 4\alpha\overline{\alpha} = (-2\alpha)^2 - 4\alpha^2 = 0$. Als $\alpha \notin \mathbb{R}$, dan is de discriminant van $x^2 + ax + q$ negatief. Dua is in alle gevallen $a^2 - 4q \leq 0$.

Gevolg 1.3 $\#E(\mathbb{F}_{q^m}) \leq q^m + 1 + 2|\alpha|^m = q^m + 1 + 2\sqrt{q}^m$

Dit volgt rechtstreeks uit de stelling.

Definitie 1.4 *Een elliptische kromme die voldoet aan $\#E(\mathbb{F}_q) = q + 1 + 2|\alpha| = q + 1 + \lfloor 2\sqrt{q} \rfloor$ noemen we maximaal over $\mathbb{F}_q$.*

Voorbeeld 1.5 *Voorbeelden van elliptische krommen die maximaal zijn:*

$\mathbb{F}_q$	*kromme*
$\mathbb{F}_5$	$y^2 = x^3 + 3x$
$\mathbb{F}_7$	$y^2 = x^3 + 3$
$\mathbb{F}_{11}$	$y^2 = x^3 + 3x + 1$
$\mathbb{F}_{13}$	$y^2 = x^3 + 4$
$\mathbb{F}_{17}$	$y^2 = x^3 + 3x$

Gevolg 1.6 *Heb je eenmaal* $a = -\alpha - \overline{\alpha} = \#E(\mathbb{F}_q) - q - 1$, *dan voldoen* $b_n = \alpha^n + \overline{\alpha}^n$ *aan* $\begin{cases} b_0 = 2 \\ b_1 = -a \\ b_n = -ab_{n-1} - qb_{n-2} \end{cases}$

Bewijs:
We kunnen Gevolg 1.6 bewijzen met inductie naar n. Een bewijs langs deze weg laten we aan de lezer over.

Een iets meer conceptueel bewijs gaat als volgt. De rijen $(\alpha^n)_{n\geq 0}$ en $(\overline{\alpha}^n)_{n\geq 0}$ behoren tot de lineaire ruimte bestaande uit alle rijen $(c_n)_{n\geq 0}$ met de eigenschap $c_n = -ac_{n-1} - qc_{n-2}$. Dus zit ook de som van deze twee rijen in deze ruimte, en die som is $(b_n)_{n\geq 0}$. □

$\#E(\mathbb{F}_{q^n})$ is dus te schrijven als $q^n + 1 - b_n$ en dat is makkelijk te berekenen via de recursie van Gevolg 1.6. Een voorbeeld wordt gegeven in Hoofdstuk 3.

Hoofdstuk 2

Speciaal geval: $y^2 = x^3 - n^2x$

2.1 Zeta-functie van E

Om het aantal punten te berekenen van een elliptische kromme E, gedefiniëerd over een eindig lichaam, kunnen we gebruik maken van de zeta-functie, wat dit precies is laten we later zien. We volgen [1] Hoofdstuk II, §2. We vergelijken eerst het aantal punten op de kromme $E_n : y^2 = x^3 - n^2x$ met het aantal punten op de kromme $E'_n : u^2 = v^4 + 4n^2$. Stel (u, v) is een punt op E'_n, dan ligt $(x, y) = (\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2))$ op E_n. Als (x, y) op E_n ligt en $x \neq 0$, dan volgt dat $(u, v) = (2x - \frac{y^2}{x^2}, \frac{x}{y})$ op E'_n ligt. De twee afbeeldingen zijn inverse van elkaar, als we $E_n - \{0, 0\}$ nemen in plaats van E_n. Het aantal punten op E'_n noemen we N'. De punten die op E_n liggen zijn dan (0,0), het punt op oneindig en N' punten die corresponderen met de punten op E'_n. We krijgen dus: $\#E_n(\mathbb{F}_q) = N' + 2$. Om N' te berekenen maken we gebruik van de Gauss en Jacobi sommen over eindige lichamen.

Definitie 2.1.1 *Het spoor* Tr *van* $\mathbb{F}_q$ *naar* $\mathbb{F}_p$*, voor* $q = p^n$ *is de afbeelding* Tr*:* $x \mapsto x^{p^{n-1}} + ... + x^p + x$*.*

We zien dat Tr(x) $\in \mathbb{F}_p$, want $\mathrm{Tr}(x)^p = x^{p^n} + ... + x^p = x^{p^{n-1}} + ... + x^p + x = \mathrm{Tr}(x)$. En Tr is lineair over $\mathbb{F}_p$, want $\mathrm{Tr}(\lambda x + y) = (\lambda x + y)^{p^{n-1}} + ... + (\lambda x + y)^p + \lambda x + y = (\lambda x)^{p^{n-1}} + ...\lambda x + y^{p^{n-1}} + ... + y + p \cdot (...) = \lambda x^{p^{n-1}} + \lambda x^{p^{n-2}} + ... + \lambda x + \mathrm{Tr}(y) + 0 = \lambda \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

Het spoor is een niet-triviale afbeelding doordat $x^{p^{n-1}} + ... + x^p + 1$ hooguit p^{n-1} nulpunten heeft en er dus $\exists y \in \mathbb{F}_{p^n}$ zodat y geen nulpunt is.

Definitie 2.1.2 *Het additief karakter* ψ *wordt gedefiniëerd als het homomorfisme* $\psi : \mathbb{F}_q \to \mathbb{C}^*$*,* $\psi(x) = \xi^{\mathrm{Tr}\ x}$ *waarbij* $\xi = e^{\frac{2\pi i}{p}}$ *en* Tr *het spoor van* $\mathbb{F}_q$ *naar* $\mathbb{F}_p$ *is.*

Omdat het spoor een niet-triviale afbeelding is, is ψ niet triviaal, met andere woorden, $\exists x$ zodat $\psi(x) \neq 1$. Verder geldt voor deze afbeelding $\psi(xy) = \psi(x)\psi(y)$, met andere woorden ψ is een homomorfisme. Ook is $\sum_{x\in\mathbb{F}_q} \psi(x) = 0$. Want als we een $y \in \mathbb{F}_q$ nemen, zodat $a := \psi(y) \neq 1$, en we noemen de som b, dan krijgen we: $ab = \psi(y) \sum_{x\in\mathbb{F}_q} \psi(x) = \sum_{x\in\mathbb{F}_q} \psi(x+y) = \sum_{x\in\mathbb{F}_q} \psi(x) = b$, maar $a \neq 1$, dus moet b nul zijn.

Definitie 2.1.3 *Een multiplicatief karakter is een homomorfisme $\chi : {\mathbb{F}_q}^* \to \mathbb{C}^*$, dat we uitbreiden tot $\chi : \mathbb{F}_q \to \mathbb{C}$, door $\chi(0)$ nul te stellen.*
Een voorbeeld hiervan is $\chi_{triv} : \mathbb{F}_q \to \mathbb{C}$, gegeven door $\chi_{triv}(x) = 1$ als $x \neq 0$ en $\chi_{triv}(0) = 0$

Met hetzelfde argument als bij ψ geldt ook hier:

$$\sum_{x\in\mathbb{F}_q} \chi(x) = 0, \text{als } \chi \neq \chi_{\text{triv}}$$

Definitie 2.1.4 *Voor een multiplicatief karakter χ, definiëren we de Gauss-som op de volgende manier:*

$$g(\chi) = \sum_{x\in\mathbb{F}_q} \chi(x)\psi(x).$$

Definitie 2.1.5 *We definiëren de Jacobi-som, bij twee multiplicatieve karakters χ_1 en χ_2, op de volgende manier:*

$$J(\chi_1, \chi_2) = \sum_{x\in\mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

Eigenschappen 2.1.6 *Elementaire eigenschappen*

1. $g(\chi_{triv}) = -1$. *Immers:* $g(\chi_{triv}) = \sum_{x\in{\mathbb{F}_q}^*} \psi(x) = (\sum_{x\in\mathbb{F}_q} \psi(x)) - \psi(0) = -1$.
2. $J(\chi_{triv}, \chi_{triv}) = q-2$, *want* $\chi_{triv}(x)\chi_{triv}(1-x) = 0$ *voor* $x = 0$ *en* $x = 1$ *en* $\chi_{triv}(x)\chi_{triv}(1-x) = 1$, *voor de overige* $q-2$ *waarden van* x.
3. $$J(\chi_{triv}, \chi) = \sum_{x\in\mathbb{F}_q} \chi_{triv}(x)\chi(1-x) = \sum_{x\in\mathbb{F}_q^*} \chi(1-x) =$$
$$(\sum_{x\in\mathbb{F}_q} \chi(1-x)) - \chi(1) = -\chi(1) = -1, \text{ als } \chi \neq \chi_{triv}.$$

4. *Voor* $\chi \neq \chi_{triv}$ *geldt*

$$J(\chi, \overline{\chi}) = \sum_{x \in \mathbb{F}_q} \chi(x)\overline{\chi(1-x)} = \sum_{x \in \mathbb{F}_q} \chi(1-x)\overline{\chi(x)} = \sum_{x \neq 0} \chi(1-x)\frac{1}{\chi(x)} =$$

$$\sum_{x \neq 0} \chi(1-x)\chi(\frac{1}{x}) = \sum_{x \neq 0} \chi(\frac{1}{x} - 1) = \chi(-1) \cdot \sum_{x \neq 0} \chi(1 - \frac{1}{x}) =$$

$$\chi(-1) \cdot \sum_{x \neq 1} \chi(x) = \chi(-1) \cdot \left(-\chi(1) + \sum_{x \in \mathbb{F}_q} \chi(x) \right) = -\chi(-1).$$

5. $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$.

6.

$$g(\chi) \cdot g(\overline{\chi}) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) \sum_{y \in \mathbb{F}_q} \overline{\chi(y)}\psi(y) =$$

$$\sum_{\substack{x,y \in \mathbb{F}_q \\ y \neq 0}} \chi(\frac{x}{y})\psi(x+y) = \sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q^*} \chi(\frac{z-y}{y})\psi(z) =$$

$$\chi(-1) \sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q^*} \chi(1 - zy^{-1})\psi(z).$$

Voor $z = 0$ *hebben we:*

$$\sum_{y \in \mathbb{F}_q^*} \chi(1) = q - 1.$$

Voor $z \neq 0$, *doorloopt* zy^{-1} *de groep* $\mathbb{F}_q^*$ *als* y *ook* $\mathbb{F}_q^*$ *doorloopt en* $1 - zy^{-1}$ *dus* $\mathbb{F}_q - \{1\}$. *Dus* $\sum_{y \in \mathbb{F}_q^*} \chi(1 - zy^{-1}) = (\sum_{y \in \mathbb{F}_q^*} \chi(1 - zy^{-1})) - \chi(1) = -1$, *op voorwaarde dat* $\chi \neq \chi_{triv}$. *Dus:*

$$\sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q^*} (\chi(1 - zy^{-1})\psi(z) = q - 1 + \sum_{z \in \mathbb{F}_q^*} (-\psi(z)) = q, \textit{ als } \chi \neq \chi_{triv}.$$

Dus:

$$g(\chi) \cdot g(\overline{\chi}) = \chi(-1)q, \textit{ als } \chi \neq \chi_{triv}.$$

7. *Voor* $\chi \neq \chi_{triv}$ *geldt* $|g(\chi)| = \sqrt{q}$. *Immers, uit de vorige eigenschap leiden we af:*

$$q = \chi(-1)g(\chi)g(\overline{\chi}) = g(\chi) \sum_{x \neq 0} (\chi(-x^{-1})\psi(x)) \overset{y=-x}{=} g(\chi) \sum_{y \neq 0} \chi(y^{-1})\psi(-y) =$$

$$g(\chi) \sum \overline{\chi(y)\psi(y)} = g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Dus: $|g(\chi)| = \sqrt{q}$.

8. $J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$ *indien* $\chi_2 \neq \overline{\chi_1}$.

Immers, $J(\chi_1, \chi_2)g(\chi_1\chi_2) = \sum_{x\in\mathbb{F}_q} \chi_1(x)\chi_2(1-x) \sum_{y\in\mathbb{F}_q} \chi_1(y)\chi_2(y)\psi(y) = \sum_{x,y\in\mathbb{F}_q} \chi_1(xy)\chi_2(y-xy)\psi(x+y)$.

Vanaf de andere kant: $g(\chi_1)g(\chi_2) = \sum_{x\in\mathbb{F}_q} \chi_1(x)\psi(x) \sum_{y\in\mathbb{F}_q} \chi_2(y)\psi(y) = \sum_{x,y\in\mathbb{F}_q} \chi_1(x)\chi_2(y)\psi(x+y)$.
We gaan nu transformaties doen:

$$\sum_{x,y\in\mathbb{F}_q} \chi_1(xy)\chi_2(y-xy)\psi(x+y) \overset{z=xy}{=} \sum_{\substack{x,z\in\mathbb{F}_q \\ x,z\neq 0}} \chi_1(z)\chi_2(\frac{z}{x}-z)\psi(z+\frac{z}{x}), \text{ met } y = \frac{z}{x}.$$

En vanaf de andere kant:

$$\sum_{a,b\in\mathbb{F}_q} \chi_1(a)\chi_2(b)\psi(a+b) \overset{w=a+b}{=} \sum_{a,w\in\mathbb{F}_q} \chi_1(a)\chi_2(w-a)\psi(w), \text{ met } b = w-a.$$

We kiezen nu: $\frac{z}{x} = w, a = z$ *en we krijgen:*

$$\sum_{\substack{x,z\in\mathbb{F}_q \\ x,z\neq 0}} \chi_1(z)\chi_2(\frac{z}{x}-z)\psi(z+\frac{z}{x}) = \sum_{\substack{x,z\in\mathbb{F}_q \\ x,z\neq 0}} \chi_1(z)\chi_2(w-z)\psi(z+w).$$

Met deze definities zullen we nu N', het aantal paren $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ die voldoen aan $u^2 = v^4 + 4n^2$, proberen uit te rekenen.

Lemma 2.1.7 *Voor* $a \in \mathbb{F}_q^*$ *en* $m|(q-1)$ *het aantal oplossingen* $x \in \mathbb{F}_q$ *van de vergelijking* $x^m = a$ *wordt gegeven door:*

$$\#\{x \in F_q^* | x^m = a\} = \sum_{\chi^m = \chi_{triv}} \chi(a),$$

waarbij de som wordt genomen over alle multiplicatieve karakters χ *waarvan de* m*-de macht het triviale karakter is. Dit aantal is* m *indien* a *een* m*-de macht in* $\mathbb{F}_q$ *is en anders gelijk aan 0.*

Bewijs:
We weten dat $\mathbb{F}_q^*$ een cyclische groep is. Het karakter $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ wordt vastgelegd door $\chi(b)$ waarin b een voortbrenger van $\mathbb{F}_q^*$ is. Omdat $1 = \chi(1) = \chi(b^{q-1}) = \chi(b)^{q-1}$, moet b een oplossing van $x^{q-1} - 1 = 0$ zijn. Er zijn $q-1$ oplossingen, dus $q-1$ verschillende karakters.

Als a geen m-de macht is, dan is $\#x \in \mathbb{F}_q | x^m = a = 0$, als a wel een m-de macht is; $a = c^m$, dan zijn alle $b^k c$, waarbij k een veelvoud is van $\frac{q-1}{m}$, oplossingen. Dat

zijn er precies m.

Als $\chi^m = \chi_{\text{triv}}$, dan moet $\chi(b)^m = 1$, dus $x = \chi(b)$ een nulpunt van $x^m - 1$. Omdat $m|(q-1)$ voldoet elk nulpunt ook aan $x^{q-1} = 1$, dus er zijn m zulke nulpunten.

Indien $q \equiv 3(\text{mod}4)$ dan heeft de E_n precies $q+1$ punten ($N' = q-1$). In dit geval zijn er vier punten van orde 2, het punt op oneindig, het punt (0,0) en de punten $(\pm n,\ 0)$. De overige punten (x, y) met $x \neq 0, n, -n$ tellen we in paren. We verdelen de paren in x en $-x$. Omdat $f(x) = x^3 - n^2x$ een oneven functie is en $-1(\equiv 3(\text{mod}4))$ geen kwadraat in $\mathbb{F}_q$ is, is een van $f(x)$ of $f(-x) = -f(x)$, een kwadraat in $\mathbb{F}_q$.Voor elke x krijgen we twee punten: $(x, \pm\sqrt{f(x)})$ of $(-x, \pm\sqrt{f(-x)})$. Dus hebben we $\frac{q-3}{2}$ paar punten, dus $q-3$ punten in totaal. Samen met de 4 punten van orde 2 hebben we voor het geval $q \equiv 3(\text{mod}4)$ dus: $N_1 = q+1$ of $N' = q-1$.

Nu nemen we aan dat $q \equiv 1(\text{mod}4)$. Nu tellen we de paren met u of v is 0. Dat maakt:

$$N' = \#\{u \in \mathbb{F}_q | u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} + \#\{u, v \in \mathbb{F}_q{}^* | u^2 = v^4 + 4n^2\}.$$

De eerste term in deze vergelijking is 2, want alleen $u = \pm 2n$ voldoet aan $u^2 = 4n^2$. Voor de tweede term gebruiken we de formule

$$\#\{x^m = a\} = \sum_{\chi^m = \chi_{\text{triv}}} \chi(a).$$

Kies $g \in \mathbb{F}_q^*$ van orde $q-1$ en definiëer $\chi_4 : F_q^* \to \mathbb{C}^*$ door $\chi_4(g^k) = i^k$. Dit is een karakter van orde 4. Bovendien als een karakter $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ voldoet aan $\chi^4 = \chi_{\text{triv}}$ dan is $\chi(g)^4 = 1$, dus $\chi(g) = i^n$, met $n = 0, 1, 2$ of 3. Conclusie: $\chi = \chi_4^m$. Hieruit volgt de tweede term:

$$\#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} = \sum_{j=1}^{4} \chi_4^j(-4n^2) = 2 + 2\chi_4(-4n^2).$$

Immers, $\chi_4^2(-4n^2) = \chi_2(-4n^2) = \chi_2(-4) = 1$ en dus $\chi_4^3(-4n^2) = \chi_2(-4n^2)\chi_4(-4n^2) = \chi_4(-4n^2)$.

Voor de derde term nemen we $\chi_2 (= \chi_4^2)$, het niet triviale multiplicatieve karakter van orde 2. Opnieuw gebruik makend van

$$\#\{x^m = a\} = \sum_{\chi^m = 1} \chi(a),$$

krijgen we:

$$\#\{u,v\in {\mathbb{F}_q}^*|u^2=v^4+4n^2\}=\sum_{\substack{a,b\in {\mathbb{F}_q}^*\\ a=b+4n^2}}\#\{u^2=a\}\cdot\#\{v^4=b\}=$$

$$\sum_{a\in {\mathbb{F}_q}^*,a-4n^2\neq 0}\sum_{\substack{j=1,2,3,4\\ k=1,2}}\chi_2^k(a)\chi_4^j(a-4n^2).$$

Nu nemen we de substitutie $c=\frac{a}{4n^2}$, in de eerste sommatie aan de onderste regel en verwisselen we de sommatie:

$$\sum_{\substack{j=1,2,3,4\\ k=1,2}}\chi_4^j(-4n^2)\sum_{c\in {\mathbb{F}_q}^*}\chi_2^k(c)\chi_4^j(-4n^2)J(\chi_2^k,\chi_4^j).$$

Nu brengen we de drie sommen weer samen en maken we gebruik van de eigenschap van Jacobi sommen dat als $J(\chi_2^2,\chi_4^4)=J(\chi_{\text{triv}},\chi_{\text{triv}})=q-2$ of $J(\chi_2^2,\chi_4^4)=J(\chi_{\text{triv}},\chi_4^j)=-1$ (als $j=1,2,3$), dan krijgen we:

$$N'=4+2\chi_4(-4n^2)+\sum_{j=1,3}\chi_4^j(-4n^2)J(\chi_2,\chi_4^j)+q-2+3\cdot -1+2\chi_4(-4n^2)\cdot -1=$$

$$q-1+\chi_4(-4n^2)(J(\chi_2,\chi_4)+J(\chi_2,\overline{\chi_4})).$$

$q\equiv 1(\text{mod}4)$, dus $4|(q-1)$. Dus, omdat $\mathbb{F}_q^*$ cyclisch is, bestaat er een $\alpha\in\mathbb{F}_q^*$, die orde 4 heeft. Dan heeft α^2 orde 2, dus $\alpha^2=-1$. En $(1+\alpha)^4=(1+2\alpha+\alpha^2)^2=(2\alpha)^2=-4$. Dus: $\chi_4(-4)=\chi_4((1+\alpha)^4)=(\chi_4(1+\alpha))^4=1$, want $\chi_4(1+\alpha)\in\pm 1,\pm i$.

Daaruit volgt dat $\chi_4(-4n^2)=\chi_4(n^2)=\chi_2(n)$. Daarmee definiëren we:

$$\alpha=\alpha_{n,q}=-\chi_2(n)J(\chi_2,\chi_4),(1.1)$$

en schrijven we N_1 als:

$$\#E_n(\mathbb{F}_q)=q+1-\alpha-\overline{\alpha}.(1.2)$$

Er geldt dat α (en dus ook $\overline{\alpha}$) $\in\mathbb{Z}[i]$, omdat de waarden van χ_2 en χ_4 in de definitie van $J(\chi_2,\chi_4)$ alleen ± 1 of $\pm i$ kunnen zijn. We schrijven α als $a+bi$,

voor de gevallen $q = p \equiv 1 \text{mod} 4$ of $q = p^2$, waarbij $p \equiv 3 \text{mod} 4$. Uit een van de eigenschappen van de Jacobisom volgt:

$$\alpha = -\chi_2(n)J(\chi_2, \chi_4) = -\chi_2(n)\frac{g(\chi_2)g(\chi_4)}{g(\overline{\chi_4})}.$$

En omdat $|-\chi_2(n)| = 1$ en $|g(\chi_2)| = |g(\chi_4)| = |g(\overline{\chi_4})| = \sqrt{q}$, volgt $|\alpha| = \sqrt{q}$, dus $a^2 + b^2 = |\alpha|^2 = q$.

Daaruit volgt dat er in de twee gevallen slecht een beperkt aantal mogelijkheden zijn voor α. In het geval van $p \equiv 1$ zijn er acht mogelijkheden: $\pm a, \pm bi, \pm b$, of $\pm ai$. En in het andere geval vier $\pm p$ of $\pm pi$. Om te kunnen bepalen welke de juist is maken we gebruik van het volgende lemma:

Lemma 2.1.8 *Als $q \equiv 1(\text{mod}4)$, laat dan χ_2 en χ_4 karakters van, resp., exacte orde 2 en 4 zijn. Dan gelden de volgende drie dingen:*

1. $J(\chi_2, \chi_4) \in \mathbb{Z}[i]$.
2. $J(\chi_2, \chi_4)\overline{J(\chi_2, \chi_4)} = q$
3. $1 + J(\chi_2, \chi_4)$ *is deelbaar door* $2 + 2i$

Bewijs:
Eerst vergelijken we $J(\chi_2, \chi_4)$ en $J(\chi_4, \chi_4)$ via Gauss-sommen. Met de laatste eigenschap van de Jacobi- en Gauss-sommen krijgen we:

$$J(\chi_2, \chi_4) = J(\chi_4, \chi_4)\frac{g(\chi_2)^2}{g(\chi_4)g(\overline{\chi_4})} = \chi(-1)J(\chi_4, \chi_4).$$

Nu schrijven we $J(\chi_4, \chi_4)$ volgens de definitie:

$$J(\chi_4, \chi_4) = \sum \chi_4(x)\chi_4(1-x) = \chi_4^2(\frac{p+1}{2}) + 2\sum \chi_4(x)\chi_4(1-x),$$

waarbij de tweede som over $\frac{q-3}{2}$ elementen is, een voor elk paar $\{x, 1-x\} \subset \mathbb{F}_q^*$ met $x \neq 1-x$. Omdat $\chi_4(x)$ een macht van i is, is het congruent aan 1 modulo $1+i$ in $\mathbb{Z}[i]$. Dus is $2\chi_4(x)\chi_4(1-x) \equiv 2(\text{mod}(2+2i))$. Door modulo $2+2i$ te werken hebben we $J(\chi_4, \chi_4) \equiv q - 3 + \chi_4^2(\frac{p+1}{2}) \equiv 2 + \chi_4(4)$. Als we dit invullen in $1 + J(\chi_2, \chi_4)$ krijgen we

$$1 + \chi_4(-1)J(\chi_4, \chi_4) \equiv 1 + \chi_4(-4) + 2\chi_4(-1)(\text{mod}2 + 2i).$$

Omdat $\chi_4(-4) = 1$ en $\chi_4(-1) = \chi_4(\alpha^2) = \pm 1$, (voor $\alpha \in \mathbb{F}_q^*$ van orde 4), volgt: $1 + \chi_4(-4) + 2\chi_4(-1) = 0$ of 4. Daaruit volgt dat $1 + J(\chi_2, \chi_4)$ deelbaar is door $2 + 2i$ en dat is wat we wilden bewijzen. □

We gaan nu stelling 1.1 bewijzen voor het speciale geval van de kromme E_n : $y^2 = x^3 - n^2x$ over $\mathbb{F}_p$.

Stelling 2.1.9 *Laat E_n een eliptische kromme van de vorm $y^2 = x^3 - n^2x$ over $\mathbb{F}_p$ zijn. Dan is er een $\alpha \in \mathbb{C}$ zodat:*

$$\#E_n(\mathbb{F}_{p^r}) = p^r + 1 + \alpha^r + \overline{\alpha}^r.$$

Voor $p \equiv 3(\text{mod}4)$ voldoet $\alpha = i\sqrt{p}$ en voor $p \equiv 1(\text{mod}4)$ moet α een element van $\mathbb{Z}[i]$ met $|\alpha|^2 = p$ zijn, die congruent is aan $\chi_2(n)$ modulo $2 + 2i$.

Voor de keuze van α, bij $p \equiv 1(\text{mod}4)$ zijn er precies twee mogelijkheden α en $\overline{\alpha}$, die voldoen aan $|\alpha|^2 = p$ en $\alpha \equiv \chi_2(n)\text{mod}(2 + 2i)$.

Bewijs:
We laten eerst de macht van p variëren, we bepalen $N_r = \#E_n(\mathbb{F}_{p^r})$ voor $p \equiv 1(\text{mod}4)$ en $N_{2r} = \#E_n(\mathbb{F}_{q^r})$ voor $p \equiv 3(\text{mod}4), q = p^2$ (omdat we weten dat $N_r = p^r + 1$ voor oneven r, in dit geval) We stellen q vast op p voor het eerste geval en op p^2 voor het tweede geval. In beide gevallen is $q \equiv 1(\text{mod}4)$. Waar we eerder, voor de formule $\#E_n(\mathbb{F}_q), q \equiv 1(\text{mod}4)$, q schreven, vervangen we deze nu door q^r in de berekeningen.
Omdat we r variëeren, moeten we aangeven welke χ_2 en χ_4 we bedoelen, oftewel van welke eindige lichamen zij een multiplicatief karakter zijn. Laat $\chi_{2,1} = \chi_2$ het unieke niet-triviale karakter van $\mathbb{F}_q^*$ van orde 2 zijn en laat $\chi_{4,1} = \chi_4$ een vast karakter van $\mathbb{F}_q^*$ van exacte orde 4 (hiervan zijn er twee, de andere is $\overline{\chi_4}$). Dan, door χ_2 of χ_4 met de norm van $\mathbb{F}_{q^r}$ naar $\mathbb{F}_q$ samen te stellen, krijgen we een karakter van $\mathbb{F}_{q^r}^*$ van, resp., exacte orde 2 of 4. We noteren deze karakters als $\chi_{2,r}$ en $\chi_{4,r}$. Als g bijvoorbeeld een generator is van $\mathbb{F}_q^*$, zodat $\chi_4(g) = i$ en als g_r een generator van $\mathbb{F}_{q^r}^*$ waarvan de norm g is, oftewel $(g_r)^{1+q+\ldots+q^{r-1}} = g$, dan hebben we $\chi_{4,r}(g_r) = i$. Als we de norm van $\mathbb{F}_{q^r}^*$ naar $\mathbb{F}_q^*$ schrijven als: $\mathbb{N}_r$, dan kunnen we onze definities schrijven als

$$\chi_{4,r} = \chi_4 \circ \mathbb{N}_r, \chi_{2,r} = \chi_2 \circ \mathbb{N}_r.$$

Met deze definities, kunnen we, gebruikmakend van (1.1) en (1.2), het volgende schrijven:

$$\#E_n(\mathbb{F}_{q^r}) = q^r + 1 - \alpha_{n,q^r} - \overline{\alpha_{n,q^r}}, (1.3)$$

$$\text{waar } \alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\overline{\chi_{4,r}})}.(1.4)$$

Nu gebruiken we de Hasse-Davenport relatie voor Gauss-sommen:

$$-g(\chi \circ \mathbb{N}_r) = (-g(\chi))^r.$$

Het bewijs komt na dit bewijs. Als we deze relatie toepassen op de drie Gauss-sommen in (1.4), met de wetenschap dat $\chi_{2,r}(n) = \chi_2(n^r) = \chi_2(n)^r$, dan volgt de

volgende relatie:

$$\alpha_{n,q^r} = \alpha_{n,q}^r. (1.5)$$

Neem aan dat $p \equiv 1(\text{mod}4)$, als we nu (1.1) en lemma 1.8 nemen, dan vinden we dat $\alpha = \alpha_{n,p}$ eem geheel getal van Gauss met norm p is congruent aan $\chi_2(n)$ modulo $(2+2i)$ en uit (1.3) en (1.5) volgt

$$N_r = p^r + 1 - \alpha^r - \overline{\alpha^r}.$$

Hiermee is de stelling voor het geval $p \equiv 1(\text{mod}4)$ bewezen.

Neem nu aan dat $p \equiv 3(\text{mod}4), q = p^2$. Dan is $\chi_2(n) = 1$, omdat alle elementen van $\mathbb{F}_p$ kwadraten zijn in $\mathbb{F}_{p^2}$. Lemma 1.8 vertelt ons dat $\alpha_{n,q}$ een geheel getal van Gauss met norm q is, die congruent is aan 1 mod $2+2i$. Van de vier gehele getallen van Gauss $i^j p, j = 0, 1, 2, 3$, die norm q hebben, voldoet alleen $\alpha_{n,q} = -p$ aan de congruentieconditie. Door (1.2) en (1.5) concluderen we dat we voor een even r hebben:

$$N_r = \#E_n(\mathbb{F}_{q^{\frac{1}{2}r}}) = p^r + 1 - (-p)^{\frac{r}{2}} - (-p)^{\frac{r}{2}}.$$

Omdat $N_r = p^r + 1$ voor oneven r, hebben we voor elke r:

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r.$$

Hiermee is stelling 1.9 bewezen.

Bewijs van de Hasse-Davenport relatie:
(Het bewijs volgt uit de opgaven 10-17 op pagina 62-63 van [1])

Gegeven is een multiplicatief karakter $\chi : \mathbb{F}_q^* \to \mathbb{C}*$. We gaan eerst kijken naar de verzameling S, van alle monische polynomen in $\mathbb{F}_q[x]$. We gebruiken de notatie S^{irr} om de verzameling van irreducibele monische polynomen te beschrijven. Het subscript geeft aan van welke graad de polynomen zijn. We schrijven:

$$x^{q^r} - x = \prod_{\alpha \in \mathbb{F}_{q^r}} (x - \alpha)$$

en

$$\prod_{\alpha \in \mathbb{F}_{q^r}} (x - \alpha) = \prod_{f \in S_d^{irr}, d|r} f.$$

Het bewijs volgt uit stelling 9.3.2 van [2].

Vervolgens schrijven we $f \in S$ als $f(x) = x^d - c_1 x^{d-1} + ... + (-1)^d c_d$ en we definiëren de afbeelding $\lambda : S \to \mathbb{C}$ door $\lambda(f) = \chi(c_d)\psi(c_1)$ en voor $f = 1$ nemen we $\lambda(1) = 1$. We kijken nu naar $\lambda(f_1 f_2)$. $f_1 f_2 = x^{d_1+d_2} - (c_{1,1} + c_{2,1})x^{d_1+d_2-1} + ... + (-1)^{d_1+d_2} c_{1,d_1} c_{2,d_2}$. Dus $\lambda(f_1 f_2) = \chi(c_{1,d_1} c_{2,d_2})\psi(c_{1,1} + c_{2,1}) = \chi(c_{1,d_1})\chi(c_{2,d_2})\psi(c_{1,1})\psi(c_{2,1}) = \lambda(f_1)\lambda(f_2)$. We zien dat deze vergelijking ook geldt als f_1 of $f_2 = 1$, dus kunnen we zeggen $\lambda(f_1 f_2) = \lambda(f_1)\lambda(f_2)$.

In de volgende stap gaan we de Gauss som herschrijven in termen van labda's:

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) = \sum_{f \in S_1} \chi(c_1)\psi(c_1) = \sum_{f \in S_1} \lambda(f).$$

Nu nemen we aan dat $\alpha \in \mathbb{F}_q$ voldoet aan een monisch irreducibel polynoom $f \in S_d^{irr}$, waarbij $d|r$. Dan, $\lambda(f)^{\frac{r}{d}} = (\chi(c_d)\psi(c_1))^{\frac{r}{d}} = \chi(c_d)^{\frac{r}{d}}\psi(c_1)^{\frac{r}{d}} = \chi_r(\alpha)\psi_r(\alpha)$, waarbij het subscript r aangeeft de karakters van $\mathbb{F}_{q^r}$ verkregen zijn door samen te stellen met de norm van $\mathbb{F}_{q^r}$ naar $\mathbb{F}_q$ (in geval van het multiplicatieve karakter) of met het spoor van $\mathbb{F}_{q^r}$ naar $\mathbb{F}_q$ in geval van het additief karakter.

Op basis hiervan kunnen we zeggen dat

$$g(\chi_r) = \sum_{d|r} \sum_{f \in S_d^{irr}} d\lambda(f)^{\frac{r}{d}}. \quad (1.5)$$

Vervolgens gaan we kijken naar de machtreeks eigenschap

$$\sum_{f \in S} \lambda(f) T^{gr(f)} = \prod_{f \in S^{irr}} (1 - \lambda(f) T^{gr(f)})^{-1}$$

.

Als $d > 1$ dan $\sum_{f \in S_d} \lambda(f) = 0$.

Als we van beide kanten van de machtreeks eigenschap de logaritmische afgeleide nemen krijgen we:

$$(-1)^{r-1} g(\chi)^r = \sum_{d|r} \sum_{f \in S_d^{irr}} d\lambda(f)^{\frac{r}{d}}.$$

Deze laatste vergelijking samen met vergelijking 1.5 geeft:

$$g(\chi \circ \mathbb{N}_r) = (-1)^{r-1} g(\chi)^r.$$

De Hasse-Davenport vergelijking volgt nu door beide zijden met -1 te vermenigvuldigen.

2.2 Voorbeelden

We nemen bij deze voorbeelden $y^2 = x^3 - x$ en gaan $\#E(\mathbb{F}_p)$ voor enkele $p \equiv 1 \bmod 4$ bepalen.

We beginnen met $p = 5$. Met de hand tellen we 8 punten:

$$(0,0), (\pm 1, 0), (2, \pm 1), (-2, \pm 2)$$

en het punt op oneindig. Met de formule vinden we: $\#E(\mathbb{F}_5) = 6 - \alpha - \overline{\alpha} = 6 + \chi_2(1)(J(\chi_2, \chi_4) + \overline{J(\chi_2, \chi_4)}) = 6 + J(\chi_2, \chi_4) + \overline{J(\chi_2, \chi_4)} = 6 + \chi_2(2)\chi_4(4) + \chi_2(3)\chi_4(3) + \chi_2(4)\chi_4(2) + \chi_2(2)\chi_4(4) + \chi_2(3)\chi_4(3) + \chi_2(4)\chi_4(2) = 6 - \chi_4(4) - \chi_4(3) + \chi_4(2) - \chi_4(4) + \chi_4(3) - \chi_4(2) = 6 + 1 - 2i + 1 + 2i = 8$.
Nu nemen we $p = 13$. Met de hand vinden we er eveneens 8:

$$(0,0), (\pm 1, 0), (5, \pm 4), (-5, \pm 6)$$

en het punt op oneindig. We gaan nu het aantal bepalen via Lemma 2. In dit geval moeten we naar de Jacobisom zoeken die een absolute waarde heeft van $\sqrt{13}$ en waarvoor geldt $J + 1$ is deelbaar door $2 + 2i$ in de ring $\mathbb{Z}[i]$. De mogelijkheden voor J is dan op basis van de eerste eis: $\pm 2 + \pm 3i$ of $\pm 3 + \pm 2i$. De tweede eis zegt dat $\Re(1 + J)$ deelbaar moet zijn door 2, daaruit volgt als enige mogelijkheid: $J = -3 \pm 2i$, natuurlijk had deze Jacobisom ook gevonden kunnen worden via de definitie. De formule geeft dan: $\#E(\mathbb{F}_{13}) = 14 + J + \overline{J} = 14 - 6 = 8$. Tot slot proberen we $p = 137$. Dit gaan we natuurlijk niet met de blote hand doen. We maken weer gebruik van Lemma 2. De mogelijkheden voor J zijn dan $\pm 4 + \pm 11i$ en $\pm 11 + \pm 4i$, waarbij het imaginaire deel even moet zijn, dus houden we alleen de mogelijkheden $\pm 11, \pm 4i$ over. Aan de deelbaarheids eis voldoet enkel $J = 11 + 4i$. Dus : $\#E(\mathbb{F}_{137}) = 138 + J + \overline{J} = 138 + 22 = 160$.

Voor $p \equiv 3 (\bmod 4)$ hebben de vergelijkingen van de $E_n : y^2 = x^3 - n^2 x$, $p + 1$ punten met coördinaten in $\mathbb{F}_p$.
Bijvoorbeeld voor $p = 3$, liggen er 4 punten op de kromme $y^2 = x^3 - x$. namelijk $(0,0), (\pm 1, 0)$ en het punt op oneindig. Voor $p = 7$ liggen er 8 punten op deze kromme:

$$(0,0), (1,0), (6,0), (4, \pm 2), (5, \pm 1)$$

en het punt op oneindig. Voor $p = 11$ ten slotte liggen er 12 punten op deze kromme:

$$(0,0), (1,0), (4, \pm 4), (6, \pm 1), (8, \pm 3), (9, \pm 4), (10, 0)$$

en het punt op oneindig.

Hoofdstuk 3

$E(\mathbb{F}_{2^m})$

Als $q = 2$ dan geldt de volgende stelling:

Stelling 3.1 *Voor elke E over $\mathbb{F}_2$, is er een m zodat $E(\mathbb{F}_{2^m})$ maximaal is.*

Bewijs:
Om dit te bewijzen is het voldoende om voor iedere a een kromme te vinden die maximaal is:

a	kromme	m
-2	$y^2 + y = x^3 + x + 1$	1
-1	$y^2 + xy = x^3 + x + 1$	5
0	$y^2 + y = x^3$	2
1	$y^2 + xy = x^3 + 1$	3
2	$y^2 + y = x^3 + x$	4

Berekening voor $E : y^2 + xy = x^3 + x + 1$. Punten in $E(\mathbb{F}_2)$: Voor $x = 0$ moet y voldoen aan $y^2 = 1$, dus $y = 1$: $(0, 1)$. Voor $x = 1$, voldoet $(1, y)$ als $y^2 + y = 1$. Dit heeft geen oplossingen in $\mathbb{F}_2$, dus $\#E(\mathbb{F}_2) = 2$ en de α in Gevolg 1.2 is: $\alpha = \#E(\mathbb{F}_2) - 2 - 1 = -1$. De α en $\overline{\alpha}$ in stelling 1.1 en Gevolg 1.2 zijn dus nulpunten van $x^2 - x + 2$.
Uit Gevolg 1.6 volgt $\alpha^5 + \overline{\alpha}^5 = b_n = b_4 - 2b_3 = b_3 - 2b_2 - 2(b_2 - 2b_1) = -3b_2 + 2b_1 = -b_1 - 6b_0 = -1 + 12 = 11$. $\lfloor 2\sqrt{32} \rfloor = \lfloor \sqrt{128} \rfloor = 11$, dus inderdaad is deze kromme maximaal bij $m = 5$.

□

Alle a met $a^2 \leq 8$ komen ook daadwerkelijk voor.

Hoofdstuk 4

reële α

Als α reëel is volgt dat q een kwadraat is, immers: $|\alpha| = \sqrt{q}$. Als α reëel is, volgt dat $\alpha + \overline{\alpha} = 2\sqrt{q}$ een geheel getal is, dus q is een kwadraat.
Of er uitbredingen zijn waarover een kromme maximaal wordt is afhankelijk van α; als α positief dan zijn er geen uitbreidingen waarover de kromme maximaal wordt, als α negatief dan zijn er wel uitbreidingen mogelijk waarover een kromme maximaal wordt.
Namelijk, stel $\alpha > 0$, dan is het aantal punten over $\mathbb{F}_{q^m}$ gelijk aan $q^m + 1 - 2\alpha^m$ en dat is niet gelijk aan $q^m + 1 + 2\lfloor 2\sqrt{q^m} \rfloor$, er is dus geen $m > 0$ zodat de kromme maximaal wordt over $\mathbb{F}_{q^m}$.
Als nu $\alpha < 0$, dus $\alpha = \sqrt{q}$. Dan is het aantal punten over $\mathbb{F}_{q^m}$ gelijk aan $q^m + 1 - 2(-\sqrt{q})^m = q^m + 1 + (-1)^{m+1} 2\sqrt{q^m}$. Dus wordt de kromme maximaal als α negatief en $m \equiv 1 \pmod 2$.

Als voorbeeld nemen we $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, waarbij ω voldoet aan $\omega^2 = \omega + 1$ en $y^2 + y = x^3$ en $y^2 + y = x^3 + \omega$. In het eerste voorbeeld zien we dat α negatief is en dus zijn er uitbreidingen waarover de kromme maximaal is. In het tweede geval is α negatief en zijn er geen uitbreidingen waarover de kromme maximaal wordt, namelijk voor oneven m.

Hoofdstuk 5

q is kwadraat

Stelling 5.1 *Als q een kwadraat is en $E/\mathbb{F}_q$ wordt maximaal over een uitbreiding, dan geldt voor de α bij E dat: $\alpha \in \{-\sqrt{q}, (\frac{1}{2} \pm \frac{1}{2}\sqrt{-3})\sqrt{q}, \pm i\sqrt{q}\}$*

Bewijs:
Als er $E/\mathbb{F}_{q^m}$ maximaal wordt voor zekere $m \geq 1$, dan geldt $q^m + 1 + 2r^m = \#E(\mathbb{F}_{q^m}) = q^m + 1 - \alpha^m - \overline{\alpha}^m$, waarbij $r = \sqrt{q}$. Dus, moet gelden $\alpha^m + \overline{\alpha}^m = -2r^m$. We weten ook dat $|\alpha| = \sqrt{q} = r$. Dus kunnen we α ook schrijven als $\alpha = r\beta$, waarbij β verkregen wordt door α te normaliseren., dus $|\beta| = 1$. Dan volgt dat $\beta^m + \overline{\beta}^m = -2$. Als we dit met β^m vermenigvuldigen krijgen we:

$$\beta^{2m} + 1 + 2\beta^m = (\beta^m + 1)^2 = 0,$$

daaruit volgt dus dat $\beta^m = -1$. We weten uit hoofdstuk 1 dat α voldoet aan de vergelijking $\alpha^2 + a\alpha + q = 0$, dus $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$. Nu is $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, dus ook $[\mathbb{Q}(\beta) : \mathbb{Q}] \leq 2$. Schrijf je $n = orde(\beta)$ (in de groep $\mathbb{C}^*$) omdat $\beta^{2m} = 1$ geldt dat $n|2m$.
Voor de rest verwijzen we door naar stelling 5.2 en 5.3. De α van deze ordes zijn dus $a \in \{-\sqrt{q}, \pm i\sqrt{q}, (\frac{1}{2} \pm \sqrt{3}i)\sqrt{q}\}$.

□

Stelling 5.2 *De volgende drie gevallen voldoen niet voor de orde van n voor β:*

1. *Als n deelbaar door priemgetal $p \geq 5$.*
2. *Als n deelbaar door 8*
3. *Als n deelbaar door 9*

Bewijs:
We gaan de drie gevallen afzonderlijk bekijken.

Geval 1 Omdat n deelbaar is door p kunnen we het schrijven als $n = p\ l$ en $\beta^l \neq 1$. We hebben $\mathbb{Q} \subset \mathbb{Q}(\beta^l) \subset \mathbb{Q}(\beta)$ met $\beta^l = \xi$ zodat $\xi^p = 1$ en $\xi \neq 1$ en $p - 1 \geq 4$. Dan is $\frac{\xi^p - 1}{\xi - 1} = \xi^{p-1} + ... + 1 = 0$. En deze is irreducibel in $\mathbb{Q}[x]$ Deze heeft minimaal graad 4 en voldoet dus niet aan $[\mathbb{Q}(\beta) : \mathbb{Q}] \leq 2$.

Geval 2 In dit geval is de orde van $\beta^l = \xi$ 8. $x^8 - 1$ kan gereduceerd worden tot $(x^4 - 1)(x^4 + 1)$, ξ moet voldoen aan $x^4 + 1 = 0$ welke irreducibel is in $\mathbb{Q}[x]$. Maar deze heeft graad 4 en voldoet dus niet.

Geval 3 In dit geval kijken we naar het polynoom $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$. β^l is een nulpunt van $x^6 + x^3 + 1$, welke irreducibel is en heeft dus graad 6 en voldoet dus ook niet.

□

Stelling 5.3 *De orde n van β is 2, 4 of 6.*

Bewijs:
Uit stelling 5.2 volgt dat $n = 2^{e_1} \cdot 3^{e_2}$, met $e_1 \leq 2, e_2 \leq 1$. De mogelijke combinaties voor n zijn dus $n = 1, 2, 3, 4, 6, 12$. // $n = 1$ valt direct af, omdat $\beta \neq 1$
$n = 2$ is wel mogelijk. Je hebt dan $\beta = -1$ en deze voldoet als $m \equiv 1(\text{mod}2)$.
$n = 3$ voldoet niet. Je hebt dan twee waarden voor β namelijk $\beta = -\frac{1}{2} \pm \sqrt{3}i$, zodat $b^m + \overline{b}^m \neq -1$, voor alle $m \geq 1$.
$n = 4$ voldoet wel, je krijgt dan $\beta = \pm i$, de m die dan gekozen moet worden is $m \equiv 2(\text{mod}4)$.
$n = 6$ voldoet ook, je krijgt dan de punten $\beta = \frac{1}{2} \pm \sqrt{3}i$, de m die voldoen zijn $m \equiv 3(\text{mod}6)$.
$n = 12$ voldoet niet, β zou dan een nulpunt moeten zijn van $x^{12} - 1 = (x^6 - 1)(x^2 + 1)(x^4 - x^2 + 1)$ en β voldoet aan $x^4 - x^2 + 1$, maar deze is irreducibel en heeft graad 4 en kan dus niet de orde van β zijn.
Dus, n = 2, 4 of 6.

□

Als voorbeeld nemen we weer $q = 4$. In dit geval moet de α dus $-2, 1 \pm \sqrt{-3}$ of $\pm 2i$ zijn en dus $\#E(\mathbb{F}_4) = 9, 3$ of 5. Voor elk van deze α nemen we nu een voorbeeld. Voor de vergelijking $y + y^2 = x^3$, hebben we, voor $q = 4$, 9 punten: $(0,0), (0,1), (1,\omega), (1,1+\omega), (\omega,\omega), (\omega,1+\omega), (1+\omega,\omega), (1+\omega,1+\omega)$ en het punt op oneindig en de α is in dit geval dus -2 ($\beta = -1$). Dus wordt deze kromme maximaal voor alle uitbreidingen F_{4^m} van $\mathbb{F}_4$ met oneven $m \in \mathbb{N}$. We zien het hier al gebeuren voor $m = 1$.
Voor de vergelijking $y^2 + y = x^3 + x$ hebben we 5 oplossingen $(0,0), (0,1), (1,0), (0,1)$

en het punt op oneindig, we hebben hier dus te maken met een $\alpha = \pm 2i$. In dit geval voldoet $m \equiv 2(\text{mod}4)$, zie ook tabel van hoofdstuk 3.
Als laatste voorbeeld nemen we de vergelijking $y^2 + \omega y = x^3$, deze levert drie punten $(0, 0)$, $(0, \omega)$ en het punt op oneindig. Deze heeft dus een α van orde 6 en wordt maximaal over een uitbreiding $\mathbb{F}_{4^m}$, met $m \equiv 3(\text{mod}6)$, bij voorbeeld over $\mathbb{F}_{64}$.

Hoofdstuk 6

$E(\mathbb{F}_{3^m})$

Voor $q = 3$ blijken niet alle a, die aan de voorwaarde van gevolg 1.2, te werken. Voor vijf a, vinden we een m, zodat een kromme die bij die a hoort over $\mathbb{F}_{3^m}$ maximaal wordt maar voor de andere twee keuzes van a worden de bijbehorende krommes niet maximaal over $\mathbb{F}_{3^m}$, voor $m < 1.000.000$.

Stelling 6.1 *Voor alle E over $\mathbb{F}_3$, waarvan $a = \alpha + \overline{\alpha} \in \{-3, -1, 0, 2, 3\}$, is er een m zodat $E(\mathbb{F}_{3^m})$ maximaal is.*

Bewijs:
Om dit te bewijzen is het voldoende om voor ieder van deze a een kromme te vinden, die maximaal wordt:

a	kromme	m
-3	$y^2 = x^3 - x + 1$	1
-1	$y^2 = x^3 + x$	5
0	$y^2 = x^3 - x$	2
2	$y^2 = x^3 + x^2 - 1$	3
3	$y^2 = x^3 - x - 1$	6

□

Nu blijft we nog over met $a = -2$ en $a = 1$. We maken voor een elliptische kromme waarbij $a = 1$ een tabel voor de eerste 10 m:

m	b_m	$\lfloor 2\sqrt{3^m} \rfloor$
1	-1	3
2	-5	6
3	8	10
4	7	18
5	-31	31
6	10	54
7	83	93
8	-113	162
9	-136	280
10	475	486

Er zijn dus geen $m \leq 10$ die voldoet. Het is aan te tonen dat er voor $m < 1.000.000$ geen m te vinden is die voldoet. We gaan nu kijken naar de voorwaarden waaraan een m moet voldoen als deze zou bestaan.

Stelling 6.2 *Als m voor $a = -2$ of $a = 1$ bestaat moet deze oneven zijn.*

Bewijs:
Voor even m zien we dat $6 \mid \lfloor 2\sqrt{3^m} \rfloor$, als we de recursie voor b_m modulo 3 nemen, zien we dat $b_m \equiv -b_{m-1} (\text{mod} 3) \equiv b_{m-2} (\text{mod} 3)$. We weten dat $b_2 \equiv 1 (\text{mod} 3)$, daaruit volgt dat b_m niet deelbaar is door 6 en daaruit volgt dat m niet even kan zijn.

□

Daarom zullen we het dus over een andere boeg moeten gooien. We proberen het eerst met convergenten van de $\frac{\theta}{\pi}$ waarbij θ geldt: $\alpha = -\sqrt{p^n} e^{-in\theta}$.

6.1 kettingbreuken en convergenten

Convergenten worden gevormd uit äfgekapte"kettingbreuken.

Nu volgen twee definities (zie ook [4], pagina 129 en 139):

Definitie 6.3 *Een kettingbreuk van $g \in \mathbb{R}$ worden als volgt gedefiniëerd:*

$$g = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \frac{1}{b_3 + \cdots}}}$$

$$\text{met} \quad b_0 \in \mathbb{Z} \quad \text{en} \quad b_j \in \mathbb{N}, j \neq 0.$$

Voor $g \in \mathbb{Q}$ is deze breuk "eindig", voor niet-rationale reële oplossingen van tweede graats vergelijkingen is de breuk "oneindig", maar wel (uiteindelijk) periodiek,

oftewel: $b_n = b_{n+m}$, voor alle n en een vaste $m \geq 1$, (zie [4], pagina 144). Voor overige reële getallen is de breuk ook "oneindig", maar niet (uiteindelijk) periodiek.

Om te voorkomen dat de breuk onleesbaar wordt schrijven we:

$$b_0 + \frac{1}{b_1+}\frac{1}{b_2+}\frac{1}{b_3+}...$$

Definitie 6.4 *Zij $g \in \mathbb{R}$, dan wordt zijn $n$de convergent c_n gedefinieërd door:*

$$c_n(g) = b_0 + \frac{1}{b_1+}\frac{1}{b_2+}...\frac{1}{b_n}$$

Oftewel, de afgekapte kettingbreuk bij b_n.

Voorbeeld 6.5 *Het meest geëigende voorbeeld vormt de gulden snede $\phi = \frac{1}{2} + \sqrt{\frac{5}{4}}$.*
Haar convergenten zijn: $c_k = \frac{f_{k+2}}{f_{k+1}}$, waarbij f_k het kde fibonaccigetal is.

Maar wat zijn deze convergenten? En wat hebben we aan convergenten? Daarvoor hebben we de volgende stelling (stelling 181-182 op pagina 151 in [4]), waarbij we c_n schrijven als $\frac{p_n}{q_n}$:

Stelling 6.6 *Als $n > 1, 0 < q \leq q_n$, en $\frac{p}{q} \neq \frac{p_n}{q_n}$, dan gelden de volgende twee uitspraken:*

$$|\frac{p_n}{q_n} - x| < |\frac{p}{q} - x|$$

$$|p_n - q_n x| < |p - qx|$$

Bewijs: Uit stelling 171 van [4] volgt dat $|p_n - q_n x| < |p_{n-1} - q_{n-1}x|$, het volledige bewijs volgt dan uit inductie. Neem aan dat $q = q_n$. Dan:

$$|\frac{p_n}{q_n} - \frac{p}{q_n}| \geq \frac{1}{q_n},$$

als $p \neq p_n$. Maar:

$$|\frac{p_n}{q_n} - x| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n},$$

volgens stelling 171 en 156 van [4]. Dus:

$$|\frac{p_n}{q_n} - x| < |\frac{p}{q_n} - x|.$$

Neem nu aan dat $q_{n-1} < q < q_n$, zodat $\frac{p}{q}$ niet gelijk is aan $\frac{p_{n-1}}{q_{n-1}}$ of $\frac{p_n}{q_n}$. Als we

$$\mu p_n + \nu p_{n-1} = p, \mu q_n + \nu q_{n-1} = q$$

schrijven, dan:

$$\mu(p_n q_{n-1} - p_{n-1} 1_n) = pq_{n-1} - qp_{n-1},$$

zodat

$$\mu = \pm(pq_{n-1} - qp_{n-1})$$

en

$$\nu = \pm(pq_n - qp_n)$$

. Dus, μ en ν zijn gehele getallen ongelijk aan 0. Omdat $q = \mu q_n + \nu q_{n-1} < q_n$, moeten μ en ν van teken verschillen. Uit stelling 171 van [4] volgt dan dat:

$$p_n - q_n x, p_{n-1} - q_{n-1} x$$

verschillende tekens hebben. Dus:

$$\mu(p_n - q_n x), \nu(p_{n-1} - q_{n-1} x),$$

hebben hetzelfde teken. Maar,

$$p - qx = \mu(p_n - q_n x) + \nu(p_{n-1} - q_{n-1} x),$$

dus:

$$|p - qx| > |p_{n-1} - q_{n-1} x| > |p_n - q_n x|.$$

Convergenten zijn dus zeer sterke benaderingen rationale benaderingen voor een reëel getal. Omgekeerd blijken alle voldoende goede rationele benaderingen van een reëel getal x convergenten te zijn, (Stelling 184 op pagina 153 van [4]):

Stelling 6.7 *Als*

$$|\frac{p}{q} - x| < \frac{1}{2q^2},$$

dan is $\frac{p}{q}$ *een convergent.*

Voor het bewijs verwijzen we naar [4].

We gaan nu kijken hoe we deze theorie kunnen toepassen op het vinden van een goede m.

Stelling 6.8 *Als* $q \geq 3$ *geen kwadraat is en* $E/\mathbb{F}_q$ *is maximaal over* $\mathbb{F}_{q^m}$ *en bovendien,* $ggd(q, \#E(\mathbb{F}_q) - 1) = 1$, *en tenslotte* $\theta \in \mathbb{R}$ *met* $0 \leq \theta < \pi$ *is zo dat voor elke* n *geldt* $\#E(\mathbb{F}_{q^n}) = q^n + 1 + \sqrt{q^n} \cdot \left(e^{i\theta n} + e^{-i\theta n}\right)$, *dan is* m *oneven en* m *is de noemer van een convergent* $\frac{k}{m}$ *van* $\frac{\theta}{\pi}$, *waarbij ook* k *oneven is.*

Bewijs. Definieer $b_0 = 2$ en $b_1 = q + 1 - \#E(\mathbb{F}_q)$ en $b_{n+2} = b_1 b_{n+1} - q b_n$ (als $n \geq 0$). Vanwege Gevolg 1.6 geldt dan $\#E(\mathbb{F}_{q^n}) = q^n + 1 + b_n$.

Als m even zou zijn, dan was dus $q^m + 1 + b_m = q^m + 1 + 2 \cdot q^{m/2}$, dus $b_m \equiv 0 \bmod q$. Nu geldt voor elke n dat $b_{n+1} \equiv b_1 b_n \bmod q$. Omdat

$$1 = \text{ggd}(q, \#E(\mathbb{F}_q) - 1) = \text{ggd}(q, q + 1 - \#E(\mathbb{F}_q)) = \text{ggd}(q, b_1),$$

zou volgen dat $0 \equiv b_m \equiv b_1^m \not\equiv 0 \bmod q$, een tegenspraak. Dus inderdaad geldt dat m oneven is.

Onze m moet voldoen aan $1 + q^m - \alpha^m - \overline{\alpha}^m = 1 + q^m + \lfloor 2\sqrt{q^m} \rfloor$, dus aan $2\sqrt{q}^m \cos(m\theta) = \alpha^m + \overline{\alpha}^m = -\lfloor 2\sqrt{q}^m \rfloor$, dus omdat $2\sqrt{q}^m - 1 < \lfloor 2\sqrt{q}^m \rfloor < 2\sqrt{q}^m$, (want m oneven)

$$\cos(m\theta) < \frac{1-x}{x} = -1 + \frac{1}{x}, \text{waarbij } x = 2\sqrt{q^m},$$

oftewel:

$$\cos(m\theta) + 1 < \frac{1}{2\sqrt{q}^m}.$$

We schrijven $m\theta = k\pi + \epsilon$, $-\frac{1}{2}\pi \leq \epsilon \leq \frac{1}{2}\pi$, dan omdat $\cos m\theta < 0$, is k oneven.

Er geldt $1 + \cos(m\theta) = 1 + \cos(k\pi + \epsilon) = 1 + \cos(\pi + \epsilon) = \frac{1}{2}\epsilon^2 + \frac{1}{24}\epsilon^4\delta < \frac{1}{2\sqrt{q^m}}$, met $\delta \in [-1, 1]$. Dus:

$$\epsilon^2(1 + \frac{1}{12}\epsilon^2\delta) < \frac{1}{\sqrt{q}^m},$$

ofwel

$$\epsilon^2 < \frac{1}{1 + \frac{1}{12}\epsilon^2\delta} \frac{1}{\sqrt{q}^m},$$

want $1 + \frac{1}{12}\epsilon^2\delta > 0$: immers, we hebben $q \geq 3$ en $m \geq 1$, dus voor de hoek $\alpha = m\theta$ geldt:

$$\cos\alpha < -1 + \frac{1}{2\sqrt{3}},$$

daaruit volgt (modulo 2π) dat $2,36 < \alpha < 3,93$, dus $2,36 - \pi < \epsilon < 3,93 - \pi$, oftewel $-0,78 < \epsilon < 0,78$ en daarmee $1 + \frac{1}{12}\epsilon^2\delta > 1 - \frac{1}{12}\epsilon^2 > 0,94 > 0$.

Er volgt: $|m\theta - \pi k| = |\epsilon| < \sqrt{\left(1 + \frac{1}{12}\epsilon^2\delta\right)^{-1}} \frac{1}{q^{\frac{1}{4}m}} < \frac{1,03}{q^{\frac{1}{4}m}}$ en dus

$$|\frac{\theta}{\pi} - \frac{k}{m}| < \frac{1,03}{\pi} \frac{1}{mq^{\frac{1}{4}m}} < \frac{0,33}{mq^{\frac{1}{4}m}} \leq \frac{0,33}{m \cdot 3^{\frac{1}{4}m}}.$$

Voor $m > 0$ kan dit worden afgeschat met $\frac{1}{2m^2}$. Dus is $\frac{k}{m}$ een convergent van $\frac{\theta}{\pi}$, op basis van stelling 6.7. Dit bewijst de stelling. □

Met behulp van Mathematica is het bepalen van zulke convergenten erg gemakkelijk. De θ die we gebruiken voldoet aan $\cos\theta = \frac{q+1-\#E(\mathbb{F}_q)}{2\sqrt{q}}$. Voor bijvoorbeeld $q = 3$ en $\#E(\mathbb{F}_3) = 6$ leveren onderstaande regels de eerste 50 convergenten.

```
theta = ArcCos[-1/Sqrt[3]]
Convergents[theta/Pi, 50]
```

Al na 17 ervan is de noemer groter dan 10^6, en slechts 5 van die eerste 17 hebben zowel teller als noemer oneven. Zo kan je heel efficient bepalen dat er voor $m < 1.000.000$ geen maximale kromme wordt gevonden voor de twee openstaande gevallen bij $q = 3$.

Er blijkt zelfs dat voor de door deze convergenten gegeven m, het verschil tussen $3^m + 1 + 2\sqrt{3^m}$ en $\#E(\mathbb{F}_{3^m})$ steeds groter wordt. Dit brengt ons tot het vermoeden dat er geen m bestaat zodat de kromme over $\mathbb{F}_3$ met 6 (of met 3) punten, over $\mathbb{F}_{3^m}$ maximaal is.

Hoofdstuk 7

conclusies

We vinden dat voor $q = 2$, alle elliptische krommen over $\mathbb{F}_q$ maximaal worden over $\mathbb{F}_{q^m}$ voor zekere m.
Voor $q = 3$ vinden we dat een elliptische kromme E over $\mathbb{F}_q$ maximaal wordt over een of andere uitbreiding $\mathbb{F}_{q^m}$ voor zekere m, als $\#E(\mathbb{F}_3) = 7, 5, 4, 2, 1$.

Voor $q = 3$ en $\#E(\mathbb{F}_3) = 6$ of 3, hebben we een aantal voorwaarden op m kunnen leggen. We hebben echter geen m kunnen vinden zodat de elliptische kromme maximaal wordt over $\mathbb{F}_3^m$, en zelfs lijkt de afstand tussen het gewenste en het werkelijke aantal punten te groeien. Daarom vermoeden we dat er in deze gevallen geen m zal bestaan zodat deze elliptische krommen over $\mathbb{F}_3^m$ maximaal worden.

Voor q een kwadraat, hebben we een volledige beschrijving van welke krommen over $\mathbb{F}_q$ over een uitbreiding maximaal zijn, en welke uitbreiding(en) dat dan zijn.

Voor $q > 3$ met q geen kwadraat verwachten we dat de situatie analoog is aan het geval $q = 3$. Verder suggereren onze voorbeelden, dat als de kromme maximaal wordt de bijbehorende m 'klein' zal zijn. In alle voorbeelden waar een m gevonden werd, bleek zelfs $m \leq 6$.

Hoofdstuk 8

referenties

[1] N.Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

[2] B. Van Geemen, H.W. Lenstra Jr., F. Oort, *College dictaat Algebra: Ringen, Lichamen*, RuG, 1997.

[3] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[4] G.H. Hardy, E.M. Wright, *Introduction to the Theory of Numbers*, Oxford University Press, 1954.