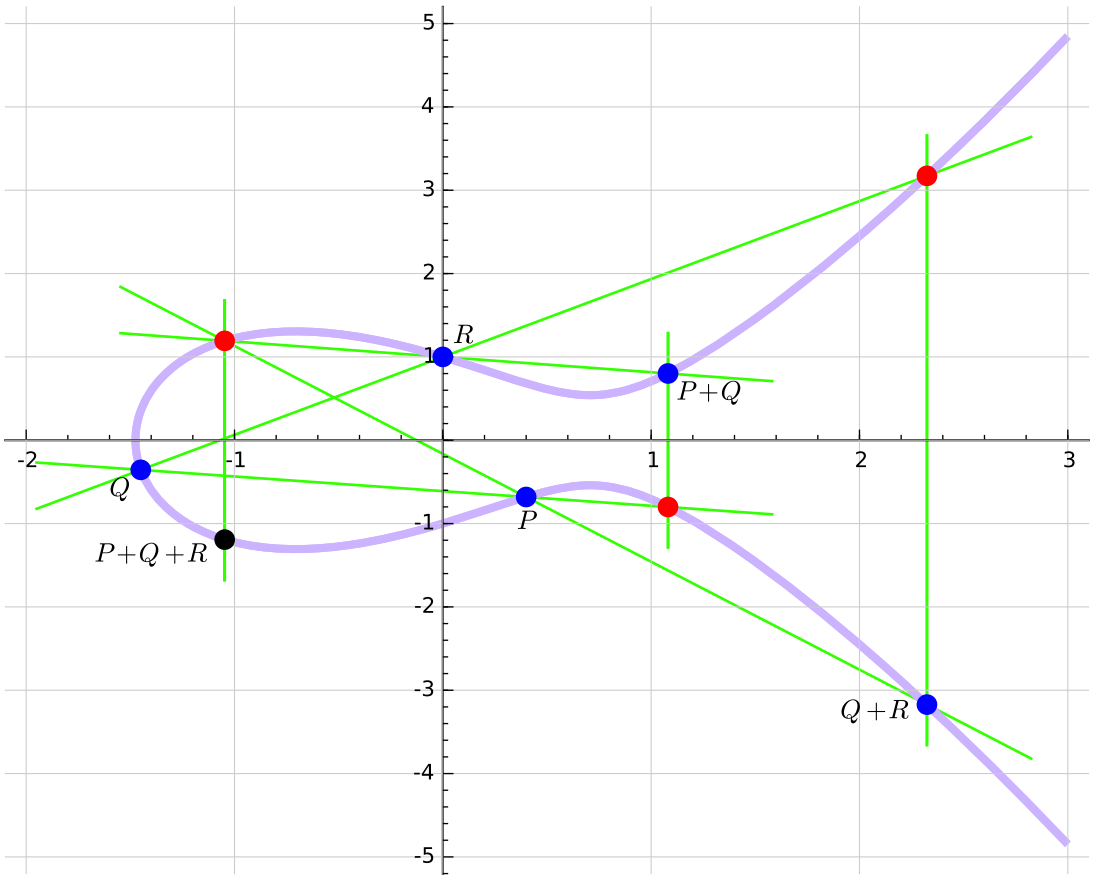
Elliptische krommen

Computerproject Wiskunde — projectopgave 2

2015–2016



Opmerking: In tegenstelling tot project 1 staan de opgaven niet noodzakelijk in volgorde van moeilijkheid. Het is ook niet altijd zo dat je alle voorgaande opgaven moet gemaakt hebben om een zekere opgave te kunnen. De opgaven in sectie 3 bijvoorbeeld staan los van sectie 2. Er zijn 8 opgaven, maar je krijgt reeds alle punten als je 7 opgaven correct maakt (het maakt niet uit welke). Schrijf voor de duidelijkheid expliciet op je werkblad als je een opgave niet maakt.

1 Definities

Zij K een veld, voorlopig mag je gerust denken aan $K = \mathbb{R}$.

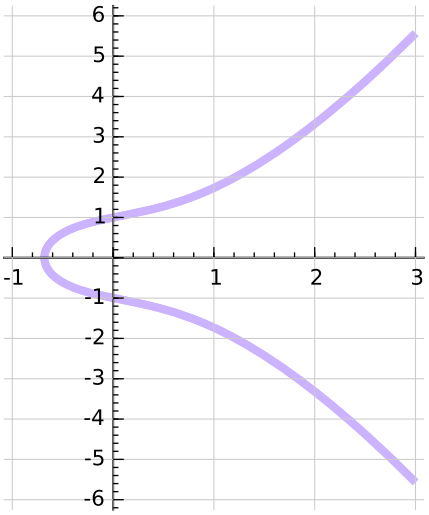
Een *elliptische kromme* over K is een vlakke kromme gegeven door een vergelijking van de vorm

$$Y^2 = X^3 + aX + b, \tag{1}$$

waarbij a en b parameters zijn in K. Bovendien eisen we dat de *discriminant*, gedefinieerd als $D = -16 \cdot (4a^3 + 27b^2)$, niet 0 is.

Merk op dat elliptische krommen niet onmiddellijk iets te maken hebben met ellipsen[1], dat zijn andere krommen!

Hiernaast zie je een voorstelling van de elliptische kromme $Y^2 = X^3 + X + 1$.



Figuur 1: $Y^2 = X^3 + X + 1$

Opgave 1. *Teken 6 krommen met een vergelijking van de vorm* (1)*: teken er twee met $D > 0$, twee met $D = 0$ en twee met $D < 0$ (merk op dat slechts 4 van deze 6 een elliptische kromme zijn). Welk verband zie je tussen het teken van D en de vorm van de figuur?*

2 Optellingswet

Elliptische krommen hebben altijd een punt "op oneindig" dat we noteren met de letter O. Je kan dit zien als het punt dat we krijgen als we Y naar $\pm\infty$ en X naar $+\infty$ laten gaan. Er is slechts één punt op oneindig, dus de keuze $Y \to +\infty$ of $Y \to -\infty$ maakt niet uit.

We definiëren de verzameling van K-punten op E, gegeven door (1), als

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}. \tag{2}$$

Als $a = b = 1$, dan zien we bijvoorbeeld dat $(1, \sqrt{3}) \in E(\mathbb{R})$ en $(-2, 3\mathrm{i}) \in E(\mathbb{C})$.

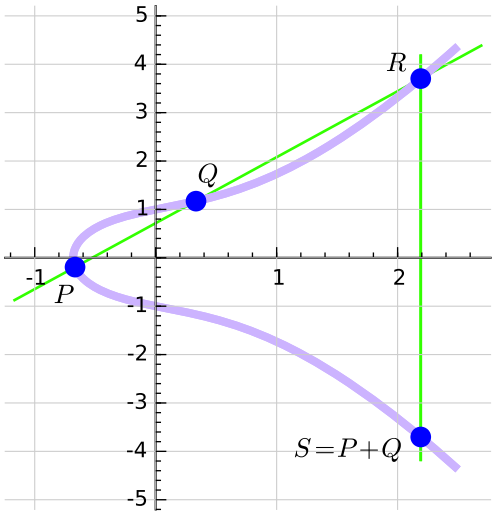
[1] Het verband tussen ellipsen en elliptische krommen wordt gegeven door *elliptische integralen*, maar daar gaan we hier niet verder op in.

Het blijkt nu dat we een optellingswet kunnen definiëren op $E(K)$ en dat $E(K)$ zo een abelse groep wordt.

Neem twee punten P en Q in $E(K) \setminus \{O\}$ met een verschillende x-coördinaat. Teken de rechte door P en Q en noem R het derde snijpunt van de rechte met de elliptische kromme (doordat de vergelijking van de kromme graad 3 heeft, zullen er inderdaad juist 3 snijpunten zijn). Spiegel dan het punt R rond de x-as en noem het resultaat S. Dan definiëren we de som $P + Q$ als het punt S.

We definiëren verder ook $P + O = O + P = P$ voor eender welke $P \in E(K)$.

Het tegenstelde van een punt P, genoteerd als $-P$, is zijn spiegelbeeld rond de x-as. Bovendien definiëren we de som van twee tegengestelde punten als O. Dus bijvoorbeeld $R = -S$ en $R + S = O$.



Figuur 2: $P + Q = S$

Met bovenstaande regels kunnen we elke twee punten op $E(K)$ optellen, behalve een punt met zichzelf. Opgave 3 zal een oplossing geven voor dit probleem.

Door de constructie is het duidelijk dat $P + Q = Q + P$ voor alle $P, Q \in E(K)$. Het is ook een feit dat de optellingswet associatief is: $(P+Q)+R = P+(Q+R)$. Dit is echter niet eenvoudig te controleren. Alles samen concluderen we dat $E(K)$ een abelse groep vormt voor deze optelling, met O als neutraal element.

In de volgende twee opgaven ga je een formule opstellen om de som van twee punten op een willekeurige elliptische kromme uit te rekenen. Het is de bedoeling dat je met algemene krommen werkt, a en b zijn dus parameters. Om de formules zo algemeen mogelijk te maken, werken we over $K = \mathbb{C}$.

Opgave 2. *Stel een formule op voor de som van twee punten P en Q, waarbij je mag aannemen dat P en Q een verschillende x-coördinaat hebben. In principe is dit een berekening die met de hand kan gedaan worden, maar voor deze opgave is het de bedoeling dat je Sage gebruikt.*

Hint: voor een derdegraadsveelterm $f(X) = X^3 + pX^2 + qX + r$ is de som van de drie nulpunten van f gelijk aan $-p$.

Opgave 3. *Stel een formule op voor de som $P + P$. Je kan dit doen door gebruik te maken van de formule $P + P = (P + Q) + (P - Q)$. Zorg dat je antwoord niet van Q afhangt.*

Hint: gebruik voor Q een zo eenvoudig mogelijk punt op $E(\mathbb{C})$.

Opgave 4. *Associativiteit in het algemeen nagaan is lastig, maar we kunnen het wel nagaan op een concreet voorbeeld. De figuur op het voorblad toont aan dat $(P + Q) + R = P + (Q + R)$ op het voorbeeld. Maak zo'n figuur na.*

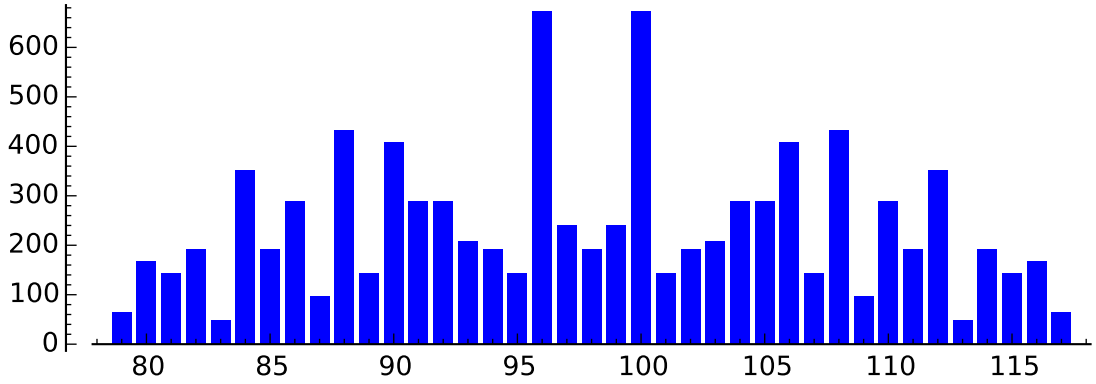
Hint: tekst tekenen doe je in Sage bijvoorbeeld met `text("$f(x)$", (0.5, 1.7))`*. Dit zal de tekst "$f(x)$" tekenen op positie* $(0.5, 1.7)$*. De dollartekens zorgen ervoor dat de tekst met LaTeX wordt getekend.*

3 Punten tellen

We beschouwen nu elliptische krommen over een eindig veld. Voor een elliptische kromme E over een eindig veld $\mathbb{F}_q$ kunnen we het aantal punten op $E(\mathbb{F}_q)$ tellen. We nemen altijd aan dat q oneven is (voor q even geldt namelijk altijd $D = 0$).

Opgave 5. *Schrijf een functie om het aantal punten van* $E(\mathbb{F}_q)$ *te tellen. Deze functie heeft als invoer het eindig veld en de parameters* a *en* b*. Hoeveel punten heeft de elliptische kromme* $Y^2 = X^3 + X + 1$ *over* $\mathbb{F}_5$*?*

Hint: schrijf een lus die alle x*-waarden in* $\mathbb{F}_q$ *probeert en die telt hoeveel mogelijke* y*-waarden er zijn voor elke* x*. Vergeet ook het punt* O *niet.*



Figuur 3: Histogram van $\#E(\mathbb{F}_{97})$

Voor een gegeven eindig veld $\mathbb{F}_q$ kunnen we nu een histogram maken van het aantal punten op $E(\mathbb{F}_q)$, waarbij we alle mogelijke elliptische krommen E nemen. In Figuur 3 hebben we van alle elliptische krommen over $\mathbb{F}_{97}$ geteld hoeveel punten ze bevatten. Op het histogram zetten we dan op waarde n een balkje met hoogte h, waarbij h het aantal krommen is met n punten.

Opgave 6. *Maar zelf zulke histogrammen voor* $q = 17$ *en* $q = 125$*.*

Als E een elliptische kromme is over $\mathbb{F}_q$, dan kunnen we ook het aantal punten tellen over grotere eindige velden, bijvoorbeeld over $\mathbb{F}_{q^2}$.

Opgave 7. *Tel voor alle elliptische krommen* E *over* $\mathbb{F}_7$ *zowel het aantal punten in* $E(\mathbb{F}_7)$ *als in* $E(\mathbb{F}_{49})$*. Maak een plot die het verband weergeeft tussen* $E(\mathbb{F}_7)$ *en* $E(\mathbb{F}_{49})$*.*

4 Punten van eindige orde

Tenslotte beschouwen we elliptische krommen over $\mathbb{Q}$. Als P een punt is op een elliptische kromme en $n \in \mathbb{N}$, dan schrijven we $n \cdot P$ voor de som $P + P + \cdots + P$ (n termen).

Een punt $P \in E(\mathbb{Q})$ noemen we een punt van *eindige orde* als $n \cdot P = O$ voor een zeker positief natuurlijk getal n.

Je mag volgende stelling aannemen:

Stelling. *Beschouw een elliptische kromme $Y^2 = X^3 + aX + b$ met $a, b \in \mathbb{Z}$. Als $P = (x, y) \in E(\mathbb{Q})$ een punt is van eindige orde, dan geldt*

1. *x en y zijn gehele getallen.*
2. *$y = 0$ of $y^2 \mid 4a^3 + 27b^2$.*
3. *$n \cdot P = O$ voor een $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.*

Opgave 8. *Gebruik bovenstaande stelling om alle punten van eindige orde op te sommen op de elliptische kromme $Y^2 = X^3 - 348X + 2497$ over $\mathbb{Q}$.*