Elliptische Kurven und ihre Anwendung in der Kryptographie

DMK-Weiterbildung vom 8. September 2022

Philipp Habegger
Departement Mathematik und Informatik
Universität Basel
philipp.habegger@unibas.ch

Revision vom 6. September 2022 um 15:02

Inhaltsverzeichnis

0. Vorwort

Der Inhalt dieses Skripts bildet die Grundlage der Weiterbildungsveranstaltung der Deutschschweizerische Mathematik-Kommission vom 8. September 2022, welche ich an der Universität Basel gehalten habe.
Ich bin dankbar um die Meldung von Fehlern und Ungenauigkeiten an meine Email-Adresse auf der Titelseite.
Hier ist eine Liste von weiterführender Literatur und Ressourcen.

- Dieses Skript sowie ein paar Beispielprogramme, implementiert in SageMath, sind auf `https://github.com/philipphabegger/ElliptischeKurvenDMK` zu finden.
- Das Buch von Silverman und Tate [ST15] ist ein guter Einstieg in die Theorie elliptischer Kurve. Das Buch enthält einen Beweis vom Satz von Mordell (unten zitiert als Satz 2.20) in einem wichtigen Spezialfall.
- Das Buch von Silverman [Sil86] ist weiter fortgeschritten. Etwas Vertrautheit mit algebraischer Geometrie und algebraischer Zahlentheorie wird vorausgesetzt. Es gibt eine Fortsetzung, ebenfalls von Silverman [Sil94], welche Themen wie "komplexe Multiplikation" behandelt.
- Die Online-Datenbank "The L-functions and modular forms database" `https://www.lmfdb.org/` enthält zur Zeit Informationen zu über 3 Millionen elliptische Kurven über $\mathbb{Q}$.
- Eine (ausführliche) Übersicht über elliptische Kurven ihre Anwendungen in der und Kryptographie bietet der Band von Cohen, Frey, et. al. [CFA+06].

0.1. Notation

Wir verwenden die folgenden Konventionen.

- Die Menge der natürlichen Zahlen ist $\mathbb{N} = \{1, 2, 3, \ldots\}$. Die Menge der positiven rationalen Zahlen ist $\mathbb{Q}_{>0}$.
- Wir wählen eine Nullstelle von $X^2 + 1$ in $\mathbb{C}$ und bezeichnen sie mit $\sqrt{-1}$.

1. Kongruente Zahlen

Definition 1.1. *Eine natürliche Zahl $n \in \mathbb{N}$ heisst **kongruente Zahl**, falls n die Fläche eines rechtwinkligen Dreiecks mit rationalen Seitenlängen ist.*

Bemerkung 1.2. *Per Definition ist n genau dann eine kongruente Zahl, wenn es positive $a, b, c \in \mathbb{Q}$ gibt, so dass $a^2 + b^2 = c^2$ und $n = ab/2$.*

Beispiele 1.3.

(i) Die Zahl $n = 6$ ist kongruent, da es ein rechtwinkliges Dreieck mit Seitenlängen $a = 3, b = 4, c = 5$ gibt und da $6 = 3 \cdot 4/2$.

(ii) Für jede kongruente Zahl n und jede rationale Zahl $\lambda \neq 0$ ist $\lambda^2 n$ eine kongruente Zahl, sofern es eine ganze Zahl ist. Um das zu beweisen, dürfen wir $\lambda > 0$ annehmen. Nach Voraussetzung ist $n = ab/2$ mit $a^2 + b^2 = c^2$. Also $a'^2 + b'^2 = c'^2$, wobei $a' = \lambda a, b' = \lambda b, c' = \lambda c$ wiederum rational. Die Fläche des entsprechenden rechtwinkligen Dreiecks ist $a'b'/2 = \lambda^2 ab/2 = \lambda^2 n$. Diese Zahl ist kongruent, falls sie ganz ist. Aus diesem Grund sind vor allem die quadratfreien Zahlen hinsichtlich der Kongruenzbedingung interessant.

(iii) Aus (i) und (ii) folgt, dass es unendlich viele kongruente Zahlen gibt, denn $\{6\lambda^2 : \lambda \in \mathbb{N}\}$ besteht aus kongruente Zahlen. Weiterhin ist jede kongruente Zahl ein rationales Vielfaches einer quadratfreien kongruenten Zahl.

(iv) Es gilt $(3/2)^2 + (20/3)^2 = (41/6)^2$ und damit ist $n = 5 = (3/2) \cdot (20/3)/2$ kongruent.

(v) Auch $n = 7$ ist kongruent wegen $(35/12)^2 + (24/5)^2 = (337/60)^2$.

Für jedes Tripel (a, b, c) mit a, b, c positive rationalen Zahlen mit $a^2 + b^2 = c^2$ existieren $u > v > 0$ rational mit $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$. Hieraus können wir auf systematische Art alle kongruente Zahlen produzieren. Es gilt folgt folgende Aussage.

Lemma 1.4. *Die Menge der kongruenten Zahlen ist*

$$\{n \in \mathbb{N} : \text{ es gibt } u > v > 0 \text{ in } \mathbb{Q} \text{ mit } n = (u^2 - v^2)uv \}.$$

Ist $n = 1$ eine kongruente Zahl? Die Antwort ist nein und dies wurde von Pierre de Fermat bewiesen.

Satz 1.5 (Fermat)**.** *Eins ist keine kongruente Zahl.*

Beweis. Wir nehmen das Gegenteil an und zeigen einen Widerspruch. Dann gibt es ein rechtwinkliges Dreieck mit rationalen Seiten und Fläche 1. Nach geeigneter Streckung erhalten wir ein neues rechwinkliges Dreieck dessen Seitenlängen natürliche Zahlen sind und dessen Quadrat eine Quadratzahl ist.
Daher gibt es ein entsprechendes Dreieck mit minimaler Flächen. D.h. es gibt $a, b, c \in \mathbb{N}$, so dass $a^2 + b^2 = c^2$ und $\frac{ab}{2} = d^2$ mit $d \in \mathbb{N}$ und es gibt kein rechtwinkliges Dreieck mit Seitenlängen in $\mathbb{N}$ und Fläche strikt kleiner als d^2. Insbesondere besitzt das Tripel (a, b, c) kein gemeinsamer Primteiler.
Aus der Theorie pythagoreischer Tripel ist bekannt, dass es $u, v \in \mathbb{N}$ gibt, so dass

$$a = u^2 - v^2, \quad b = 2uv, \quad , c = u^2 + v^2$$

wobei $\mathrm{ggT}(u, v) = 1, v < u$ und $2 \mid uv$.
Behauptung: Die Zahlen $u, v, u + v, u - v$ sind paarwise teilerfremd. Ist p bspw. ein gemeinsamer Primteiler von u und v, dann teilt p alle Einträge von (a, b, c). Dies ist unmöglich. Falls p ein gemeinsamer Primteiler von $u + v$ und $u - v$ ist, dann teilt p die Summe $(u + v) + (u - v) = 2u$ und die Differenz $(u + v) - (u - v) = 2v$. Wie eben gesehen muss $p = 2$ sein. Aber wir wissen, dass u oder v gerade ist. Daher müssen u und v beide Gerade sein. Auch das ist unmöglich. Die Behauptung folgt, da die anderen Fälle allesamt ähnlich sind.
Es gilt $2d^2 = ab = (u^2 - v^2)2uv$, also $d^2 = (u + v)(u - v)uv$. Alle vier Faktoren rechts sind paarweise teilerfremd und deren Produkt ist eine Quadratzahl. Aufgrund der Eindeutigkeit der Primfaktorzerlegung sind die vier Faktoren $u, v, u + v, u - v$ allesamt Quadratzahlen. Also existieren $x, y, z, t \in \mathbb{N}$, so dass

$$u + v = x^2, \quad u - v = y^2, \quad u = z^2, \quad v = t^2.$$

Es gilt $x > y$ und

$$(x + y)^2 + (x - y)^2 = 2x^2 + 2y^2 = 2(u + v) + 2(u - v) = 4u = (2z)^2.$$

Also existiert ein rechwinkliges Dreieck mit Seitenlängen $x + y, x - y, 2z$, allesamt in $\mathbb{N}$, dessen Fläche

$$\frac{(x + y)(x - y)}{2} = \frac{x^2 - y^2}{2} = \frac{(u + v) - (u - v)}{2} = v = t^2$$

eine Quadratzahl ist. Aber $d^2 = (u + v)(u - v)uv \geq 2v$ da $u + v \geq 2, u - v \geq 1$ und $u \geq 1$. Also $t^2 = v < d^2$ und dies widerspricht der Minimalität von d^2. □

Korollar 1.6. *Die reelle Zahl $\sqrt{2}$ ist irrational.*

Beweis. Es gilt $a^2 + b^2 = 2^2$ und $ab/2 = 1$ für $a = b = \sqrt{2}$. Aber 1 ist nicht eine kongruente Zahl wegen Fermats Satz. Damit kann $\sqrt{2}$ nicht rational sein. □

Eine klassische Fragestellung ist das folgende Problem.

Problem 1.7. *Gegeben sei eine natürliche Zahl n. Ist n eine kongruente Zahl oder nicht?*

Es ist heute kein Algorithmus bekannt, der entscheidet, ob eine gegebene natürliche Zahl kongruent ist oder nicht. Daher kennen wir keinen systematischen Zugang zu der Frage oben.

Lemma 1.8. *Sei $n \in \mathbb{N}$.*

1. *Seien $a, b, c \in \mathbb{Q}$ mit $a^2 + b^2 = c^2, a \neq c$ und $n = ab/2$. Wir definieren*

$$x = \frac{nb}{c-a} \quad \text{und} \quad y = \frac{2n^2}{c-a}.$$

   Dann gilt $y^2 = x^3 - n^2 x$ und $y \neq 0$.

2. *Seien $x, y \in \mathbb{Q}$ mit $y^2 = x^3 - n^2 x$. Falls $y \neq 0$, dann ist n eine kongruente Zahl.*

Beweis. Teil (i) ist eine direkt Rechnung. Es gilt

$$y^2 = \frac{4n^4}{(c-a)^2} = \frac{a^4 b^4}{4(c-a)^2}$$

und

$$\begin{aligned} x^3 - n^2 x &= n^3 \frac{b^3}{(c-a)^3} - n^3 \frac{b}{c-a} = n^3 \frac{b}{c-a}\left(\frac{b^2}{(c-a)^2} - 1\right) \\ &= n^3 b \frac{b^2 - (c-a)^2}{(c-a)^3} = \frac{a^3 b^4}{8} \frac{b^2 - (c-a)^2}{(c-a)^3}. \end{aligned}$$

Weiterhin gilt

$$y^2 - (x^3 - n^2 x) = \frac{a^3 b^4}{8(c-a)^3}\left(2a(c-a) - b^2 + (c-a)^2\right) = \frac{a^3 b^4}{8(c-a)^3}(c^2 - a^2 - b^2) = 0,$$

was für (i) zu zeigen.
Für den Beweis von (ii) setzen wir

$$a = \left|\frac{n^2 - x^2}{y}\right|, \quad b = \left|\frac{2nx}{y}\right|, \quad \text{und} \quad c = \left|\frac{n^2 + x^2}{y}\right|. \tag{1.1}$$

Eine direkt Rechnung zeigt $a^2 + b^2 = c^2$. Weiterhin gilt

$$\frac{ab}{2} = \frac{|(n^2 - x^2)(2nx)|}{2y^2} = \frac{2n|n^2 x - x^3|}{2y^2} = \frac{n|-y^2|}{y^2} = n.$$

Da a, b, c nicht negative rationale Zahlen sind, reicht es zu zeigen, dass $abc \neq 0$. Es gilt $c = (n^2 + x^2)/|y| \geq n^2/|y| > 0$.
Es gilt $y^2 = (x^2 - n^2)x \neq 0$. Daraus folgt $x^2 - n^2 \neq 0$ und $x \neq 0$. Also folgt $a \neq 0$ und $b \neq 0$.
Es folgt, dass n eine kongruente Zahl ist. □

Für jede natürliche Zahl $n \in \mathbb{N}$ definiert die Lösungsmenge der kubischen Gleichung

$$Y^2 = X^3 - n^2 X \tag{1.2}$$

eine Kurve in der reelle (oder komplexen) Ebene. Von besonderem Interesse sind die **rationalen Punkte** dieser Kurve, d.h. Punkte, deren Koordinaten rational sind.
Die Punkte $(0,0), (\pm n, 0)$ liegen augenscheinlich auf der Kurve für jedes n. Man nennst sie daher auch die trivialen (rationalen) Lösungen. Gibt es mindestens ein weiterer rationaler Punkt, d.h. ein Punkt dessen Ordinate nicht verschwindet, so ist n eine kongruente Zahl. Weiterhin ist die Umkehrung auch wahr.

Beispiel 1.9. *Die Zahl $n = 103$ ist kongruent. Die kleinste nicht-triviale rationale Lösung von $Y^2 = X^3 - 101^2 X$ mit positiver Ordinate ist*

$$\left(\frac{16332534559428025}{11928893315329}, \frac{2081363685506152106939880}{41200286097029552767} \right).$$

Dieser Punkt entsammt der LMFDB. Nach (1.1) erhalten wir die Seitenlängen des rechtwinkligen Dreiecks:

$$\begin{aligned} a &= \frac{16286253110943816}{441394452081515} \\ b &= \frac{45463628564396045}{8143126555471908} \\ c &= \frac{1341306649380472283747020010796 97}{359433088418295739422370858062 0}. \end{aligned}$$

Die Gleichung (1.2) ist ein Spezialfall einer Weierstrass-Gleichung, welche in grösserer Allgemeinen eine elliptische Kurve definiert.
Den Satz von Fermat, Satz 1.5, lässt sich wie folgt umformulieren.

Satz 1.10 (Fermat – Version 2)**.** *Die rationalen Punkten der Lösungsmenge von $Y^2 = X^3 - X$ in der Ebene ist*

$$\{(0,0), (\pm 1, 0)\}.$$

2. Elliptische Kurven

In diesem Abschnitt werden elliptische Kurven ad hoc eingeführt. Teil des Datums einer elliptischen Kurve ist der Grundkörper K. Dies ist a priori ein beliebiger Körper. Aber für uns sind die wichtigsten Wahlen von Grundkörper die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$. Für Anwendungen in der Kryptographie spielen die endlichen Körper eine zentrale Rolle.
Es sei angemerkt, dass die Theorie elliptische Kurven im arithmetischen Fall, d.h. für den $K = \mathbb{Q}$ und verwandte Körper, ihre volle Tiefe entfaltet. Falls der Grundkörper, so wie $\mathbb{C}$, algebraisch abgeschlossen ist, verschwinden viele arithmetische Aspekte.

2.1. Definition der elliptischen Kurve

Definition 2.1. *Sei K wie oben ein Körper. Eine **Weierstrass-Gleichung** ist eine Gleichung vom Typ*

$$E : Y^2 = X^3 + aX + b \tag{2.1}$$

mit Unbekannten X, Y und Koeffizienten $a, b \in K$, welche die Bedingung

$$\Delta_E = -2^4(4a^3 + 27b^2) \neq 0 \tag{2.2}$$

*erfüllt. Wir bezeichnen E auch als **elliptische Kurve** definiert über K. Die Grösse Δ_E, ein Element aus K, heisst **Diskriminante** der Weierstrass-Gleichung E. Zur Weierstrass-Gleichung E gehört das **Weierstrass-Polynom**[1] $Y^2 - (X^3 + aX + b)$.*

Beispiele 2.2.

(i) In (1.2) hatten wir die Gleichung $Y^2 = X^3 - n^2X$ für $n \in \mathbb{N}$ betrachtet. Es handelt sich um eine Weierstrass-Gleichung E_n, für $K = \mathbb{Q}$ (oder jeden Körper, der $\mathbb{Q}$ enthält) ist $\Delta_{E_n} = -2^4 3^3 n^4 \neq 0$.

(ii) Die Gleichung

$$Y^2 = X^3,$$

definiert keine Weierstass-Gleichung, da (2.2) nicht erfüllt ist.

Bemerkung 2.3. *Sei K ein Körper der Charakteristik 2, z.B. $K = \mathbb{F}_2$, und $a, b \in K$. Dann ist $Y^2 = X^3 + aX + b$ keine Weierstrass-Gleichung, da (2.2) nicht erfüllt ist. In K gilt $1 + 1 = 0$.*

[1] Diese Bezeichnung ist nicht Standard.

Das ist etwas unbefriedigend, da für Anwendung in der Kryptographie endliche Körper der Charakteristik 2 wichtig sind. Weiterhin ist es auch theoretischer Sicht wichtig, einen sinnvollen Begriff von elliptischen Kurven über alle Körper zu haben. Um Charakteristik 2 (und auch 3) abzudecken, muss man die Definition von Weierstrass-Gleichung verallgemeinern. Wir werden dies hier nicht tun, da es etwas technisch ist. Kurzum reicht es mit den sogenannten langen Weierstrass-Gleichungen vom Typ

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

mit entsprechender (aber kompliziertere) Diskriminanten-Bedingung

$$\begin{aligned}
&- a_6a_1^6 + a_4a_3a_1^5 + ((-a_3^2 - 12a_6)a_2 + a_4^2)a_1^4 + (8a_4a_3a_2 + (a_3^3 + 36a_6a_3))a_1^3 \\
&+ ((-8a_3^2 - 48a_6)a_2^2 + 8a_4^2a_2 + (-30a_4a_3^2 + 72a_6a_4))a_1^2 \\
&+ (16a_4a_3a_2^2 + (36a_3^3 + 144a_6a_3)a_2 - 96a_4^2a_3)a_1 \\
&+ ((-16a_3^2 - 64a_6)a_2^3 + 16a_4^2a_2^2 + (72a_4a_3^2 + 288a_6a_4)a_2 \\
&+ (-27a_3^4 - 216a_6a_3^2 + (-64a_4^3 - 432a_6^2))) \neq 0.
\end{aligned}$$

zu arbeiten.
In Charakteristik $\neq 2$ und $\neq 3$ kann man jede lange Weierstrass-Gleichung mittels quadratisch und kubischem Ergänzen durch eine affine lineare Transformation auf eine Weierstrass-Gleichung umformen.

Nun wollen wir die Bedingung (2.2) rechtfertigen. Die partiell Ableitung eines Polynoms ist formal über jedem Körper definiert, es ist kein Grenzwertbegriff notwendig.

Lemma 2.4. *Sei F das Weierstrass-Polynom einer Weierstrass-Gleichung (2.1). Sei $(x, y) \in K^2$ mit $F(x, y) = 0$. Dann gilt*

$$\frac{\partial F}{\partial X}(x, y) \neq 0 \quad \textit{oder} \quad \frac{\partial F}{\partial Y}(x, y) \neq 0.$$

Beweis. Es gilt $F = Y^2 - X^3 - aX - b$ und $-2^4(4a^3 + 27b^2) \neq 0$. Insbesondere gilt $2 \neq 0$ in K. Weiterhin

$$\frac{\partial F}{\partial Y} = 2Y.$$

Sicher ist diese Ableitung $\neq 0$ an jedem Punkt (x, y) mit $y \neq 0$. Es reicht also zu zeigen, dass $\frac{\partial F}{\partial X}(x, 0) \neq 0$, falls $F(x, 0) = 0$.
Nun gilt

$$\underbrace{(X^3 + aX + b)}_{=-F(X,0)}(288aX - 432b) + \underbrace{(-3X^2 - a)}_{=-\partial F/\partial X}(96aX^2 - 144bX + 64a^2) = -2^4(4a^3 + 27b^2) = \Delta_E \neq 0$$

nach Voraussetzung. Wir substituieren X durch x und finden $\frac{\partial F}{\partial X}(x, 0) \neq 0$ da $F(x, 0) = 0$. □

Bemerkung 2.5. *Im Fall $K = \mathbb{R}$ können wir dieses letzte Lemma geometrisch wie folgt interpretieren. Sei $(x, y) \in \mathbb{R}^2$ eine Nullstelle von F, dem Weierstrass-Polynom einer Weierstrass-Gleichung. Wir setzen*

$$\alpha = -\frac{\partial F}{\partial Y}(x, y) \quad \textit{und} \quad \beta = \frac{\partial F}{\partial X}(x, y).$$

Dann ist (α, β) nicht der Nullvektor.
Aus dem Satz von der impliziten Funktion folgt, dass wir die Nullstellenmenge von F in $\mathbb{R}^2$ in der Nähe von (x, y) durch den Graph einer glatten Funktion (nach einem möglichen Koordinatentausch) ausdrücken können.
Weiterhin ist die Menge

$$T = \{(x + \alpha t, y + \beta t) : t \in \mathbb{R}\}$$

eine Gerade durch (x, y). Wir definieren $f(t) = F(x + t\alpha, y + t\beta)$ für alle $t \in \mathbb{R}$. Dann gilt

$$\frac{d\gamma}{dt}(t) = \underbrace{F(x, y)}_{=0} + \left(\underbrace{\alpha \frac{\partial F}{\partial X}(x, y) + \beta \frac{\partial F}{\partial Y}(x, y)}_{=0} \right) t + \textit{(Terme der Ordnung} \geq 2 \textit{ in } t\textit{)}.$$

Also hat $t \mapsto F(x + t\alpha, y + t\beta)$ eine mehrfache Nullstelle bei $t = 0$. Dies bedeutet, dass T die Tangente an der Nullstellenmenge von F ist.
Zusammengefasst: die Gerade durch (x, y) mit Richtungsvektor

$$\left(-\frac{\partial F}{\partial Y}(x, y), \frac{\partial F}{\partial X}(x, y) \right)$$

liegt tangential an der Nullstellenmenge von F.

Die Schlussfolgerung von Lemma 2.4 besagt, dass die Nullstellenmenge einer Weierstrass-Gleichung an jedem Punkt einer Bedingung genügt, welche sich zumindest im reellen Fall als "Glattheitsbedingung" verstehen lässt.

Definition 2.6. *Sei F das Weierstrass-Polynom einer Weierstrass-Gleichung. Falls $(x, y) \in K$ und $F(x, y) = 0$ mit $y \neq 0$, dann heisst*

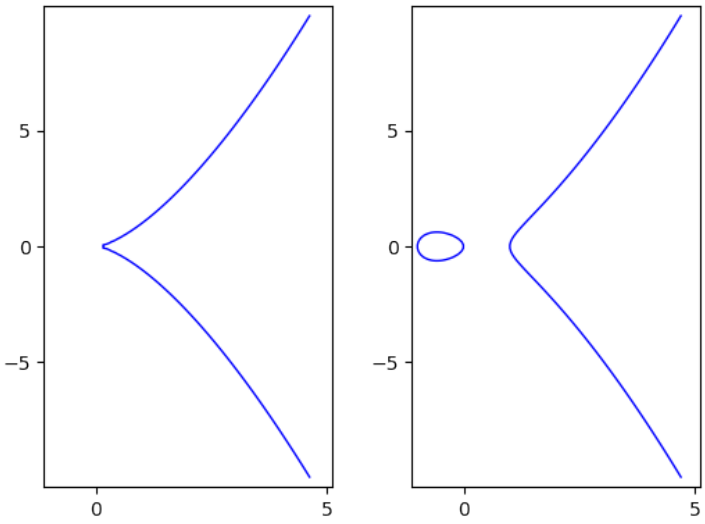
$$\frac{\frac{\partial F}{\partial X}}{-\frac{\partial F}{\partial Y}}(x, y) = \frac{3x^2 + a}{2y}$$

Tangentensteigung *an (x, y).*

Sei m die Tangentensteigung an (x, y). So wie in Beispiel 2.5 zeigt man, dass $F(x+t, y+mt)$ bei $t = 0$ eine Nullstelle der Ordnung ≥ 2 hat.

Beispiel 2.7. *Die Lösungsmenge von $Y^2 = X^3$ hat bei $(0, 0)$ eine "Spitze". Die Nullstellenmenge ist an diesem Punkt nicht glatt, vgl. Abbildung 2.1 links.*
In der gleichen Abbildung rechts ist eine glatte Kurve zu sehen.

Abbildung 2.1.: Lösungsmenge von $Y^2 = X^3$ (links) und $Y^2 = X^3 - X$ (rechts)



2.2. Das Gruppengesetz

In diesem Abschnitt werden wir zeigen, wie man auf der Lösungsmenge einer Weierstrass-Gleichung zusammen mit einem zusätzlichen Punkt, eine Gruppenstruktur definieren kann. Die Konstruktion kann man rein geometrisch veranschaulichen. Wie oben bezeichnet K ein Körper in dem sich alles abspielt (sofern nicht anders vermerkt).

Definition 2.8. *Sei $Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung E. Wir definieren*

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

*wobei $\mathcal{O}$ zunächst ein weiteres Element ist, welches nicht in K^2 liegt. Man nennt $E(K)$ die **Menge der K-rationalen Punkten von** E.*

Beispiel 2.9. *Für die Weierstrass-Gleichung E gegeben durch $Y^2 = X^3 - X$ und für $K = \mathbb{Q}$ besagt der Satz von Fermat, Satz 1.10, dass*

$$E(\mathbb{Q}) = \{(0, 0), (\pm 1, 0), \mathcal{O}\}.$$

aus vier Elementen besteht.

Beispiel 2.10. *Sei $E : Y^2 - (X^3 + aX + b)$ eine Weierstrass-Gleichung mit a, b Elemente eines Körpers K.*

(i) Für $K = \mathbb{R}$ und für alle hinreichend grosse $x \in \mathbb{R}$ gibt es $y \in \mathbb{R}$ mit $y^2 = x^3 + ax + b$. Folglich ist $E(\mathbb{R})$ stets überabzählbar unendlich.

(ii) Für $K = \mathbb{C}$ und für alle $x \in \mathbb{C}$ gibt es $y \in \mathbb{C}$ mit $y^2 = x^3 + ax + b$. Dabei verwenden wir, dass jede komplexe Zahl eine komplexe Quadratwurzel besitzt (oder dass $\mathbb{C}$ algebraisch abgeschlossen ist). Also ist $E(\mathbb{C})$ überabzählbar unendlich.

Wir werden zeigen, dass wir $E(K)$ mit der Struktur einer abelschen Gruppe verstehen können. Dazu müssen wir

- eine Verknüpfung $E(K) \times E(K) \to E(K)$,
- eine Inversionsabbildung $E(K) \to E(K)$,
- sowie ein neutrales Element in $E(K)$ definieren.

Danach muss man überprüfen, dass alle Bedingungen der Definition einer abelschen Gruppe erfüllt sind.

2.2.1. Die Verknüpfung

Sei E eine Weierstrass-Gleichung gegeben durch $Y^2 = X^3 + aX + b$ mit $a, b \in K$. In einem ersten Schritt werden wir eine Verknüpfung

$$+ \colon E(K) \times E(K) \to E(K)$$

definieren. Es ist üblich, die Verknüpfung mit "+" zu bezeichnen.
Seien P und Q Elemente von $E(K)$. Wir werden bereits in der Konstruktion überprüfen, dass die Verknüpfung + die Bedingung

$$P + Q = Q + P \quad \text{für alle} \quad P, Q \in E(K)$$

erfüllt. Hieraus werden wir folgern, dass die Gruppe $E(K)$ abelsch ist.
Es folgt eine Aufspaltung in verschiedene Fälle.

Fall 1: Die Menge $\{P, Q, \mathcal{O}\}$ hat drei Elemente. In diesem Fall gilt $P = (x_1, y_1)$ und $Q = (x_2, y_2)$. Weiterhin haben wir $P \neq Q$. Daher gibt es genau eine Gerade G durch P und Q.
Wir unterscheiden zwei Unterfälle.
Unterfall 1a. Es gilt $x_1 \neq x_2$. In diesem Fall hat die Gerade G (endliche) Steigung $m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. In anderen Worten, sie lässt sich durch die Abszisse parametrisieren

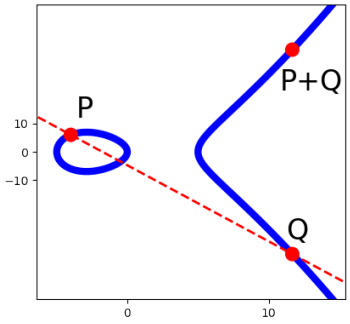
$$G = \{(x, mx + q) : x \in K\}$$

wobei $q = y_1 - mx_1$. Vgl. Abbildung 2.2 darin ist G gestrichelt.
Daher sind P und Q Schnittpunkte der Gerade G mit der Menge $E(K) \setminus \{\mathcal{O}\}$. Mit Vielfachheiten gezählt hat die Gerade G jedoch drei Schnittpunkte mit der Lösungsmenge von $Y^2 = X^3 + aX + b$. Wir können dies wie folgt direkt überprüfen. Dazu definieren wir das Polynom

$$A = (mX + q)^2 - (X^3 + aX + b) = -X^3 + m^2 X + (\text{Terme von Grad} \leq 1 \text{ in } X) \in K[X].$$

Das Polynom A hat Grad 3 und wir kennen bereits zwei verschiedene Nullstellen: $x_1, x_2 \in K$. Daher lässt sich A durch $X - x_1$ und $X - x_2$ teilen. Es gilt also $A = -(X -$

Abbildung 2.2.: $E : Y^2 = X^3 - 5^2X, P = (-4, 6), Q = (\frac{1681}{144}, -\frac{62279}{1728})$



$x_1)(X - x_2)(X - x_3)$, dabei muss x_3 als wiederum ein Element in K sein, denn es gilt $x_1 + x_2 + x_3 = m^2$, also

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1.$$

Nach Konstruktion ist das Paar (x_3, y_3) mit $y_3 = mx_3 + q$ eine Nullstelle von $Y^2 - (X^3 + aX + b)$. Weiterhin ist auch $(x_3, -y_3)$ eine Nullstelle.
In Unterfall 1a definieren wir

$$P + Q = (x_3, -y_3) \in E(K) \setminus \{\mathcal{O}\}.$$

Sind wir in Unterfall 1a, so ist auch das Paar (Q, P) in Unterfall 1a. Es gilt $P+Q = Q+P$, da die Gerade und sowohl (m, q) unabhängig von der Reihenfolge von P, Q ist.
Unterfall 1b. Es gilt $x_1 = x_2$. Nun liegt die Gerade G senkrecht zur Abszisse, vgl. Abbildung 2.3. Es gilt

$$y_1^2 = x_1^3 + ax_1 + b = x_2^3 + ax_2 + b = y_2^2$$

und daher $y_1 = -y_2$ da $P \neq Q$. Nun stehen wir vor einem Dilemma, die Gerade G hat keine weiteren Schnittpunkte mit $E(K)$ in der Ebene K^2. Jetzt kommt uns der Punkt $\mathcal{O}$ zur Hilfe.
In Unterfall 1b definieren wir

$$P + Q = \mathcal{O} \in E(K).$$

Vertauscht man P, Q so bleiben wir in Unterfall 1b und es gilt trivialerweise $P + Q = Q + P$.

Fall 2: Die Menge $\{P, Q, \mathcal{O}\}$ hat zwei Elemente. Auch hier gibt es mehrere Unterfälle.
Unterfall 2a: Es gilt $P = Q \neq \mathcal{O}$ und $P = (x, y)$ mit $y \neq 0$.
Die Gerade, welche in Fall 1 konstruiert wurde, ist nun nicht eindeutig bestimmt.
Etwas Intuition schafft die folgende Überlegung. Wir versetzen uns in die reelle Welt und ersetzen den Punkte Q durch eine Folge von Punkten $(Q_n)_{n\in\mathbb{N}}$ aus $E(\mathbb{R}) \setminus \{Q, \mathcal{O}\}$,

Abbildung 2.3.: $E : Y^2 = X^3 - 5^2X, P = (-4, 6), Q = (-4, -6)$

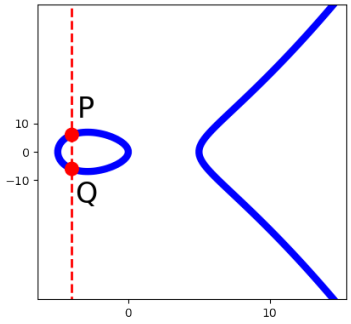
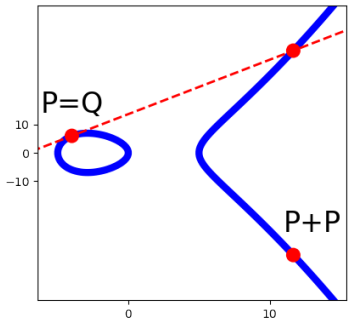


Abbildung 2.4.: $E : Y^2 = X^3 - 5^2X, P = Q = (-4, 6)$



dessen Koordinaten für $n \to \infty$ gegen $Q = P$ konvergieren. Die Gerade G_n durch P und Q_n ist wohldefiniert und die Summe $P + Q_n$ lässt sich mit der Vorschrift aus Fall 1 bestimmen. Anschaulich nähert sich die Gerade G_n der Tangente an $E(\mathbb{R}) \setminus \{\mathcal{O}\}$ durch den Punkte P. Vgl. Abbildung 2.4.
Für einen allgemeinen Körper können wir zwar nicht mit Grenzwertbegriffen argumentieren, aber wir haben dank Bemerkung 2.5 und Definition 2.6 eine algebraische Version der Tangente gefunden.
Für $y \neq 0$ dürfen wir Definition 2.6 anwenden. Das weitere Vorgehen ist vergleichbar mit Unterfall 1a. Wir setzen

$$m = \frac{3x^2 + a}{2y} \in K \quad \text{und} \quad q = y - mx \in K.$$

Das Polynom

$$A = (mX + a)^2 - (X^3 + aX + b) \in K[X]$$

hat eine Nullstelle der Ordnung ≥ 2 in x. Dies lässt sich rein formal mit Hilfe der Definition von m überprüfen. Also gilt $A = -(X - x)^2(X - x')$ für ein $x' \in K$. Dabei gilt

$$x' = m^2 - 2x = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x.$$

Der Punkt (x', y') mit $y' = mx' + q$ liegt in $E(K)$. Wie in Unterfall 1a liegt $(x', -y')$ auch in $E(K)$. In Unterfall 2a definieren wir

$$P + Q = P + P = (x', -y').$$

Trivialerweise gilt $P + Q = Q + P$ in diesem Unterfall.
Unterfall 2b: Es gilt $P = Q \neq \mathcal{O}$ und $P = (x, 0)$. Im Fall $y = 0$ ist die Tangente durch P and $E(K)$ parallel zur Ordinate. Wir definieren

$$P + Q = P + P = (x, 0) + (x, 0) = \mathcal{O}.$$

Trivialerweise gilt $P + Q = Q + P$ in diesem Unterfall.
Unterfall 2c: Es gilt $P = \mathcal{O} \neq Q$. Wir definieren

$$P + Q = \mathcal{O} + Q = Q.$$

Unterfall 2d: Es gilt $P \neq \mathcal{O} = Q$. Dieser Fall ist analog zu Unterfall 2b, wir definieren hier

$$P + Q = P + \mathcal{O} = P.$$

Vergleicht man Unterfälle 2b und 2c, so sehen wir $P + Q = Q + P$, falls $P = \mathcal{O}$ oder $Q = \mathcal{O}$.

Fall 3: Die Menge $\{P, Q, \mathcal{O}\}$ hat ein Elemente. Es gilt $P = Q = \mathcal{O}$ und wir definieren

$$P + Q = \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

Trivialerweise gilt $P + Q = Q + P$.

2.2.2. Die Inversionsabbildung

Sei $P \in E(K)$. Hier gibt es nur zwei Fälle.
Fall 1. Es gilt $P \neq \mathcal{O}$. In diesem Fall ist $P = (x, y)$. Wegen $y^2 = x^3 + ax + b$ ist auch $(x, -y)$ eine Lösung der Weierstrass-Gleichung. Wir definieren

$$-P = (x, -y) \in E(K) \setminus \{\mathbb{Q}\}.$$

Fall 2. Es gilt $P = \mathcal{O}$. Wir definieren

$$-P = \mathcal{O} \in E(K).$$

2.2.3. Das neutral Element

Es sollte nun nicht überraschen, dass wir $\mathcal{O}$ als das neutrale Element designieren.

2.3. Überprüfung der Gruppenaxiome

Satz 2.11. *Sei E eine Weierstrass-Gleichung mit Koeffizienten in einen Körper K. Sei $+$ die Verknüpfung auf $E(K)$ aus Abschnitt 2.2.1. Das Tripel $(E(K), \mathcal{O}, +)$ ist eine abelsche Gruppe.*

Die Abbildung $+\colon E(K) \times E(K) \to E(K)$ ist wohldefiniert. Seien $P, Q \in E(K)$ beliebig. Wir haben bereits überprüft, dass $P + Q = Q + P$. Also ist $(E(K), \mathcal{O}, +)$ eine abelsche Gruppe, sofern es eine Gruppe ist. Weiterhin überprüfen wir mit der Hilfe von den Unterfällen 1b, 2b und Fall 3 der Konstruktion, dass

$$(-P) + P = \mathcal{O}$$

für alle $P \in E(K)$ gilt.
Weiterhin ist $\mathcal{O} + P = P$ für alle $P \in \mathcal{O}$, dies folgt aus den Unterfällen 2c, 2d und Fall 3 in der Konstruktion.
Schliesslich muss noch die Assoziativität der Verknüpfung gezeigt werden. Dies läuft auf die Gleichung

$$P + (Q + R) = (P + Q) + R$$

für alle $P, Q, R \in E(K)$ hinaus.
Das ist ein nicht-trivialer Schritt den wir hier nicht beweisen werden. Es gibt mehrere Ansätze die Assoziativität zu zeigen. Naheliegend ist es, die Gleichheit mit der Definition direkt zu überprüfen. Das ist im Prinzip möglich. Dazu müssen jedoch die vier Verknüpfungen $Q + R, P + (Q + R), P + Q$ und $(P + Q) + R$ gebildet werden. Pro Verknüpfung gibt es 7 Fälle zu unterscheiden. D.h. insgesamt gibt es $7^4 = 2041$ Fälle. Obwohl einige Fälle trivialerweise stimmen, ist ein systematisches Arbeiten mit viel Aufwand verbunden.
Es gibt einen weiteren Zugang zur Assoziativität über die sogenannte **Picard-Gruppe**, einem Objekt der algebraischen Geometrie welches man einer sog. glatten projektiven Kurve zuordnen kann. Die Picard-Gruppe ist aus theoretischen Überlegungen *a priori* eine abelsche Gruppe. Die Idee ist nun, eine bijektive Abbildung zwischen $E(K)$ und der Picard-Gruppe zu konstruieren, welche die oben dargestellte Verknüpfung mit dem Gruppengesetz der Picard-Gruppe in Verbindung setzt. Ein wichtiges Hilfsmittel bei diesem Ansatz ist der Satz von Riemann-Roch.
Wie in jeder Gruppe kann man Elemente mit ganzen Zahlen "multiplizieren". Seien E und K wie oben und weiterhin $P \in E(K)$ ein Punkt. Für eine ganze Zahl $a \geq 1$ schreiben wir

$$a \cdot P = \underbrace{P + P + \cdots + P}_{a\text{-mal}} \in E(K). \tag{2.3}$$

Also $2 \cdot P = P + P, 3 \cdot P = P + P + P$, etc. Z.T. lassen wir den Punkt $\cdot$ in der Schreibweise weg. Für eine negative ganze Zahl $a < 0$ definieren wir

$$a \cdot P = (-a) \cdot P.$$

Schliesslich definiert man

$$0 \cdot P = \mathcal{O}.$$

Damit ist $a \cdot P$ für alle $a \in \mathbb{Z}$ definiert. Es gilt eine Variante der Assoziativität

$$a \cdot (b \cdot P) = (ab) \cdot P \tag{2.4}$$

für alle $a, b \in \mathbb{Z}$.[2] Auch diese Gleichung gilt in allen Gruppen.

Bemerkung 2.12. *Die Verknüpfung $E(K) \times E(K) \to E(K)$ sowie die Inversion $E(K) \to E(K)$ werden mit der Hilfe von Quotienten von Polynomen mit Koeffizienten in K beschrieben.*
Ist K' eine Körpererweiterung von K, dann ist $E(K)$ eine Teilmenge von $E(K')$. Da die Verknüpfung algebraisch ist, ist $E(K)$ eine Untergruppe von $E(K')$.

Lemma 2.13. *Sei $E : Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung mit $a, b \in K$. Sei $P = (x, y) \in E(K) \setminus \{0\}$. Dann gilt $P \in E(K)$ hat Ordnung 2 genau dann, wenn $y = 0$ und $x^3 + ax + b = 0$.*

Beweis. Ist P der Ordnung zwei, so gilt $P + P = \mathcal{O}$. Wir durchsuchen die sieben Fälle in der Konstruktion der Verknüpfung. Nur Unterfall 2b ergibt $\mathcal{O}$ als Summe, daher muss $P = (x, 0)$ sein und $x^3 + ax + b = 0$.
Die Umkehrung der Aussage folgt auf ähnliche Art, wiederum müssen wir in Unterfall 2b sein. □

Korollar 2.14. *Sei $n \in \mathbb{N}$ und $E_n : Y^2 = X^3 - n^2 X$. Dann gilt*

$$\begin{aligned} n \text{ ist eine kongruente Zahl} \quad &\Leftrightarrow \quad E_n(\mathbb{Q}) \supsetneq \{(0,0), (\pm n, 0), \mathcal{O}\} \\ &\Leftrightarrow \quad E_n(\mathbb{Q}) \text{ besitzt ein Punkt der Ordnung} \neq 1, 2. \end{aligned}$$

Beweis. Das Korollar folgt aus Lemma 1.8 und 2.13. □

2.4. Explizite Formeln der Verknüpfung

In diesem kurzen Abschnitt fassen wir explizite Formeln für die Summenbildung zusammen. Sie lassen sich mit der oben beschrieben Vorschrift herleiten und sind nützlich für Anwendungen. Es gibt auch ein paar aus theoretischer Sicht interessante Beobachtungen.
Wir haben die übliche Ausgangslagen. Mit K bezeichnen wir einen Körper und $E : Y^2 = X^3 + aX + b$ ist eine Weierstrass-Gleichung mit $a, b \in K$. Per Definition erfüllt die Diskriminante $\Delta_E \neq 0$, wobei $\Delta_E = -2^4(4a^3 + 27b^2) \neq 0$.
Seien $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ zwei Punkte in $E(K)$. Wir schreiben $Q = P_1 + P_2$.

Angenommen $x_1 \neq x_2$. Dann sind wir in Unterfall 1a, also $Q \neq \mathcal{O}$ und somit $Q = (x, y)$

[2] Es ist zu beachten, dass hier zwei Verknüpfung auftauchen. Einerseits die gerade eben definierte Verknüpfung $\mathbb{Z} \times E(K) \to E(K)$ und andererseits für ab die Multiplikation auf $\mathbb{Z}$.

mit $x, y \in K$. Hier gilt

$$x = \frac{-x_1^3 + x_1^2 x_2 + x_1 x_2^2 + y_1^2 - 2y_1 y_2 - x_2^3 + y_2^2}{(x_2 - x_1)^2},$$
$$y = \frac{-x_1^3 y_1 + 2x_1^3 y_2 - 3x_1^2 x_2 y_2 + 3x_1 y_1 x_2^2 + y_1^3 - 3y_1^2 y_2 - 2x_2^3 y_1 + 3y_1 y_2^2 + x_2^3 y_2 - y_2^3}{(x_2 - x_1)^3}.$$

In diesem Fall hängen die Formeln für die Summenbildung **nicht** von den Parameter a und b der Weierstrass-Gleichung E ab.

Angenommen $P_1 = P_2$ **und** $y_1 \neq 0$**.** Wir sind in Unterfall 2a. Es geht darum, den Punkt P_1 zu verdoppeln. Auf hier gilt wieder $Q = P_1 + P_2 \neq \mathcal{O}$ und damit $Q = (x, y)$ mit $x, y \in K$. Die Tangentenkonstruktion ergibt

$$\begin{aligned} x &= \frac{9x_1^4 + 6ax_1^2 - 8x_1 y_1^2 + a^2}{4y_1^2} = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3 + ax_1 + b)}, \\ y &= \frac{-27x_1^6 - 27ax_1^4 + 36x_1^3 y_1^2 - 9a^2 x_1^2 + 12ax_1 y_1^2 - 8y_1^4 - a^3}{8y_1^3} \\ &= \frac{x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2 x_1^2 - 4abx_1 - a^3 - 8b^2}{8y_1^3} \end{aligned} \tag{2.5}$$

dabei wurde jeweils in der zweiten Gleichung y_1^2 durch $x_1^3 + ax_1 + b$ ersetzt. Diese Formeln nennt man auch **Verdoppelungsformeln**, da sie den Punkt $2 \cdot P = P + P$ in Funktion von P beschreibt.
In der Verdoppelungsformel tauchen die Parameter a und b nun auf. Ein interessanter Aspekt der Verdoppelungsformel ist die Tatsache, dass der Ausdruck für x nur von der ersten Koordinate x_1 von P abhängt. In vielen Anwendungen "rechnet" man ausschliesslich mit der ersten Koordinate, um den Aufwand zu minimieren. Man verliert dabei die Information der zweiten Koordinate. Für jede Wahl von x sind die möglichen y mit $y^2 = x^3 + ax + b$ bis auf das Vorzeichen eindeutig bestimmt. Grob gesagt "enthält" die Verdoppelungsformel der ersten Koordinate die gesamte Information der elliptischen Kurve selber.

Übungsaufgabe 2.A. *Überprüfen sie die zwei Formeln anhand der Konstruktion in Unterfall 1a und 1b.*

2.5. Die Projektive Ebene

Die Hinzunahme des Punktes $\mathcal{O}$ erscheint zunächst künstlich. Arbeitet man mit projektiver Geometrie, so taucht $\mathcal{O}$ natürlich auf.

Definition 2.15. *Die* K***-Punkte der projektiven Ebene*** *sind die Geraden in* K^3*, welche den Nullpunkt enthalten. Wir bezeichnen diese Punkte mit* $\mathbb{P}^2(K)$*.*

Bemerkung 2.16. *Ein Element von $\mathbb{P}^2(K)$ entspricht einer Gerade $G \subseteq K^3$, also*

$$G = \{(\lambda x, \lambda y, \lambda z) : \lambda \in K\}$$

für ein Tripel $(x, y, z) \in K^3 \smallsetminus \{0\}$. Zwei Tripel $(x, y, z), (x', y', z') \in K^3 \smallsetminus \{0\}$ definieren die gleiche Gerade genau dann, wenn $(x, y, z) = (\lambda x', \lambda y', \lambda z')$ für ein $\lambda \in K \smallsetminus \{0\}$. In diesem Fall schreiben wir $(x, y, z) \sim (x', y', z')$. Dabei definiert $\sim$ eine Äquivalenzrelation auf $K^3 \smallsetminus \{0\}$.
Die K-Punkte der projektiven Ebene sind die Äquivalenzklassen dieser Äquivalenzrelation, d.h.

$$\mathbb{P}^2(K) = (K^3 \smallsetminus \{0\})/\sim .$$

Wir bezeichnen Punkte in $\mathbb{P}^2(K)$ mit $[x : y : z]$, wobei $(x, y, z) \in K^3 \smallsetminus \{0\}$. In dieser Schreibweise gilt

$$[x : y : z] = [\lambda x : \lambda y : \lambda z].$$

Achtung: *Die Koordinaten (x, y, z) heissen* ***projektive Koordinaten*** *des Punkts $P = [x : y : z]$. Sie sind i.A. nicht durch den Punkt $[x : y : z]$ bestimmt.*
Die Abbildung

$$K^2 \ni (x, y) \to [x : y : 1] \tag{2.6}$$

ist injektiv. Also können wir vermöge dieser Abbildung K^2 als Teilmenge von $\mathbb{P}^2(K)$ betrachten.

Sei $E : Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung mit Weierstrass-Polynom $F = Y^2 - (X^3 + aX + b)$. Wir führen eine dritte Unbekannte Z ein und **homogenisieren** das Polynom F, d.h.

$$F^{\text{hom}} = F(X/Z, Y/Z)Z^3 = Y^2Z - X^3 - aXZ^2 - bZ^3. \tag{2.7}$$

Für ein Tripel $(x, y, z) \in K^3 \smallsetminus \{0\}$ gilt

$$F^{\text{hom}}(\lambda x, \lambda y, \lambda z) = \lambda^3 F^{\text{hom}}(x, y, z).$$

Hieraus folgt, dass die folgenden Aussagen für alle $P \in \mathbb{P}^2(K)$ äquivalent sind.

(i) Für eine Wahl von projektiven Koordinaten (x, y, z) von P gilt $F^{\text{hom}}(x, y, z) = 0$.

(ii) Für jede Wahl von projektiven Koordinaten (x, y, z) von P gilt $F^{\text{hom}}(x, y, z) = 0$.

Ist eine dieser Aussagen erfüllt, so schreiben wir $F^{\text{hom}}(P) = 0$. Obwohl die projektive Koordinaten von P nicht eindeutig bestimmt sind, ist der Ausdruck $F^{\text{hom}}(P) = 0$ wohldefiniert. Wir betrachten die "Nullstellenmenge"

$$E^{\text{hom}}(K) = \{P \in \mathbb{P}^2(K) : F^{\text{hom}}(P) = 0\}$$

als Teilmenge von $\mathbb{P}^2(K)$.
Sei P ein Punkt dieser Menge und (x, y, z) eine Wahl von projektiven Koordinaten von P. Es gilt zwei Fälle.

Fall 1. Es gilt $z \neq 0$. In diesem Fall gilt $[x : y : z] = [x/z : y/z : 1]$. Wir nehmen o.B.d.A. an, dass $z = 1$, also $P = [x : y : 1]$. Die Bedingung $F^{\text{hom}}(P) = 0$ ist gleichbedeutend mit $F(x, y) = 0$. Daraus folgt $(x, y) \in E(K) \setminus \{\mathcal{O}\}$.
Fall 2. Es gilt $z = 0$. Die Bedingung $F^{\text{hom}}([x : y : 0]) = 0$ impliziert $x = 0$ wegen (2.7). Also $P = [0 : y : 0]$. Aber dann muss $y \neq 0$ sein, denn P entspricht einer Gerade mit Richtungsvektor $(0, y, 0)$. Es folgt $P = [0 : 1 : 0]$.
Ist umgekehrt $(x, y) \in E(K) \setminus \{\mathcal{O}\}$, so liegt $[x : y : 1]$ in $E^{\text{hom}}(K)$.
Vermöge der Abbildung (2.6) haben wir die natürliche Bijektion

$$E^{\text{hom}}(K) \to E(K),$$

wobei $[0 : 1 : 0]$ auf $\mathcal{O}$ abgebildet wird.
In dieser Anschauung wirken auch einige Fälle der Konstruktion der Verknüpfung natürlicher. So liegen in Unterfall 2b die zwei Punkte $P = Q, [0 : 1 : 0]$ auf einer projektiven Gerade in $\mathbb{P}^2(K)$, welche E "mit Vielfachheit 2" im Punkt P schneidet.

2.6. Die Struktur der Gruppe $E(\mathbb{Q})$

In diesem Abschnitt beschäftigen wir uns mit der Struktur von $E(\mathbb{Q})$ als Gruppe, wobei E durch eine Weierstrass-Gleichung mit rationalen Koeffizienten beschrieben wird.

Beispiel 2.17. *Sei E_n durch $Y^2 = X^3 - n^2X$ definiert mit $n \in \mathbb{N}$. Die Menge $H = \{(0, 0), (\pm 1, 0), \mathcal{O}\}$ ist unter der Verknüpfung $+$ abgeschlossen und ebenfalls unter der Inversion. Es handelt sich um eine Untergruppe von $E_n(\mathbb{Q})$. Alle Punkte P dieser Untergruppe erfüllen $P + P = \mathcal{O}$. Also ist H zur Kleinschen Vierergruppe $(\mathbb{Z}/2\mathbb{Z})^2$ isomorph ist.*
Im Fall $n = 1$ folgt aus Beispiel 2.9, bzw. aus dem Satz von Fermat, Satz 1.10, dass $E_1(\mathbb{Q}) = H = \{(0, 0), (\pm 1, 0), \mathcal{O}\}$.

Übungsaufgabe 2.B. *Sei E eine Weierstrass-Gleichung über einem Körper K und $H = \{P \in E(K) : 2 \cdot P = \mathcal{O}\}$.*

(i) Zeigen Sie, dass H eine Untergruppe von $E(K)$ ist.

(ii) Zeigen Sie, dass $\#H \in \{1, 2, 4\}$.

(iii) Zeigen Sie, dass H zur trivialen Gruppe, zu $\mathbb{Z}/2\mathbb{Z}$ oder zu $(\mathbb{Z}/2\mathbb{Z})^2$ isomorph ist.

Beispiel 2.18. *Sei E durch $Y^2 = X^3 - 5^2X$ definiert und $P = (-4, 6) \in E(\mathbb{Q})$. Wir berechnen*

$$\begin{aligned}
2 \cdot P = P + P &= \left(\frac{1681}{144}, \frac{62279}{1728}\right), \\
3 \cdot P = P + P + P &= \left(\frac{-2439844}{5094049}, \frac{-39601568754}{11497268593}\right), \\
4 \cdot P = P + P + P + P &= \left(\frac{11183412793921}{2234116132416}, -\frac{1791076534232245919}{3339324446657665536}\right).
\end{aligned}$$

Die Vielfache $k \cdot P$ von P haben weiterhin rationale Koeffizienten, das ist keine Überraschung angesichts der Konstruktion des Gruppengesetzes. Gleichzeitig sehen wir, dass $k \cdot P$ für $k > 1$ nicht notwendigerweise ganze Koordinaten besitzt, falls der Ausgangspunkt P es tut.
Nun stellt sich die natürliche Frage. Ist $\{k \cdot P : k \geq 1\}$ eine endliche oder unendliche Menge? Die Berechnung legt nahe, dass $k \cdot P$ für wachsendes k zunehmend "kompliziert wird". Wir werden aus dem Satz von Lutz–Nagell (siehe Satz 2.21 unten) folgern, dass $2P$ unendliche Ordnung hat. Das gleiche muss für P folgen.
Insbesondere ist $E(\mathbb{Q})$ eine unendliche Menge.

Lemma 2.19. *Sei $n \neq 0$ in $\mathbb{Q}$ und $E_n : Y^2 = X^3 - n^2X$. Sei $P \in E(\mathbb{Q})$, dann hat P nicht Ordnung 4 und nicht Ordnung 3.*

Beweis. Wir dürfen annehmen, dass P nicht Ordnung 1 oder 2 hat. Also gilt $P = (x, y)$ mit $y \neq 0$ wegen Lemma 2.13. Wir schreiben $2 \cdot P = (x', y')$ mit $x', y' \in \mathbb{Q}$.
Mit Hilfe von (2.5) berechnen wir

$$2 \cdot P = P + P = \left(*, \frac{x^6 - 5n^2x^4 - 5n^4x^2 + n^6}{8y^3} \right)$$

dabei interessiert uns die Abszisse nicht. Wir faktorisieren

$$x^6 - 5n^2x^4 - 5n^4x^2 + n^6 = (x^2 + n^2)(x^2 - 2nx - n^2)(x^2 + 2nx - n^2).$$

Die Polynome $X^2 \pm 2nX - n^2$ haben Diskriminante $8n^2$. Aber $8n^2$ ist nicht das Quadrat einer rationalen Zahl. Also hat $X^2 \pm 2nX - n^2$ keine Nullstelle in $\mathbb{Q}$. Auch $X^2 + n^2$ hat keine Nullstelle in $\mathbb{Q}$ da es in $\mathbb{R}$ keine Nullstelle besitzt. Folglich ist $x^6 - 5n^2x^4 - 5n^4x^2 + n^6 \neq 0$, also $y' \neq 0$. Damit hat $2P$ nicht Ordnung 2, vgl. Lemma 2.13. Also hat P nicht Ordnung 4.
Um zu zeigen, dass P nicht Ordnung 3 hat, müssen wir $2 \cdot P + P \neq \mathcal{O}$ zeigen. Sicher gilt $2 \cdot P \neq P$ (da $P \neq \mathcal{O}$). Wegen Unterfall 1a reicht es zu zeigen, dass $x \neq x'$. Wir nehmen $x = x'$ an und folgern einen Widerspruch. Es muss $y \neq y'$ gelten, also $y = -y'$. Mit Hilfe der Verdoppelungsformel oben erhalten wir

$$\begin{aligned} 0 &= x^6 - 5n^2x^4 - 5n^4x^2 + n^6 + 8y^4 = x^6 - 5n^2x^4 - 5n^4x^2 + n^6 + 8(x^3 - n^2x)^2 \\ &= 9x^6 - 21n^2x^4 + 3n^4x^2 + n^6 = (3x^2 - n^2)(3x^4 - 6n^2x^2 - n^4). \end{aligned}$$

Aber $3X^2 - n^2$ hat keine rationalen Nullstelle und $3X^2 - 6n^2X - n^4$ ebenfalls nicht. In beiden Fällen ist die Diskriminante kein Quadrat in $\mathbb{Q}$. Es folgt aus der zweiten Aussage, dass $3X^4 - 6n^2X^2 - n^4$ keine rationale Nullstelle besitzt. Also haben wir den gesuchten Widerspruch. □

Ein zentrale Satz in der arithmetischen Theorie elliptische Kurven ist der Satz von Mordell.

Satz 2.20 (Mordell (1922))**.** *Sei $E : Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung mit $a, b \in \mathbb{Q}$. Dann existiert $r \geq 0$ in $\mathbb{Z}$ und eine endliche Gruppe G, so dass $E(\mathbb{Q})$ zu $G \times \mathbb{Z}^r$ isomorph ist.*

Die Gruppe G in Mordells Satz kann mit den Elementen in $E(\mathbb{Q})$ endlicher Ordnung identifiziert werden. Der Satz von Lutz–Nagell ermöglicht es uns G explizit zu berechnen, falls $a, b \in \mathbb{Z}$.

Satz 2.21 (Lutz (1937), Nagell (1935))**.** *Sei $E : Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung mit $a, b \in \mathbb{Z}$. Falls $P = (x, y) \in E(\mathbb{Q})$ ein Element endlicher Ordnung ist, so gilt $x, y \in \mathbb{Z}$. Weiterhin gilt entweder $y = 0$ oder $y^2 \mid 4a^3 + 27b^2$.*

Ein tiefes Resultat von Barry Mazur legt die Gruppe G bis auf ein paar wenige Möglichkeiten fest.

Satz 2.22 (Mazur (1978))**.** *In der Notation von Mordells Satz ist G zu einer der folgenden Gruppen isomorph:*

$$\mathbb{Z}/n\mathbb{Z} \quad \text{für ein} \quad n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2n)\mathbb{Z} \quad \text{für ein} \quad n \in \{1, 2, 3, 4\}.$$

Satz 2.23. *Sei $n \in \mathbb{N}$ und $E_n : Y^2 = X^3 - n^2X$. Dann ist n genau dann eine kongruente Zahl, wenn E_n positiven Rang besitzt.*

Beweis. Besitzt E_n positiven Rang, so existiert wegen Lemma 2.13 ein $(x, y) \in E_n(\mathbb{Q})$ mit $y \neq 0$. Wegen Korollar 2.14 ist n eine kongruente Zahl.
Sei umgekehrt n eine kongruente Zahl. Wegen Korollar 2.14 existiert $(x, y) \in E_n(\mathbb{Q})$ mit $y \neq 0$. Wir werden ausschliessen, dass (x, y) ein Punkt endlicher Ordnung ist. Daraus wird folgen, dass der Rang positiv ist.
A priori ist $H = \{(0, 0), (\pm n, 0), \mathcal{O}\}$ eine Untergruppe von $E_n(\mathbb{Q})$ die zu $(\mathbb{Z}/2\mathbb{Z})^2$ isomorph ist, vgl. Beispiel 2.17. Die Untergruppe H ist ebenfalls eine Untergruppe von G wie in Mazurs Satz. Folglich ist $G = H$ oder G ist zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2n)\mathbb{Z}$ isomorph mit $n \in \{2, 3, 4\}$. Im zweiten Fall hätte $E_n(\mathbb{Q})$ ein Element der Ordnung 4 (in den Fällen $n = 2$ und $n = 4$) oder der Ordnung 6 (im Fall $n = 3$). Aber das ist wegen Lemma 2.19 ausgeschlossen. Also muss $G = H$. Weil (x, y) nicht in G liegt, hat (x, y) unendliche Ordnung. Also ist der Rang von E_n positiv. □

Man kann diesen letzten Satz auch ohne den tiefen Satz von Mazur beweisen.
Der Exponent r in Mordells Satz heisst **Rang** von $E(\mathbb{Q})$ oder E. Diese Invariante liegt tiefer und bleibt mysteriös. Die folgende Fragestellung ist 2022 ein offenes Problem.

Problem 2.24. *Entwickeln Sie einen Algorithmus der den Rang r aus einer Weierstrass-Gleichung mit rationalen Koeffizienten berechnet.*

Hier ist der aktuelle Weltrekord bzgl. dem Rang.

Satz 2.25 (Elkies (2006))**.** *Es gibt eine Weierstrass-Gleichung mit rationalen Koeffizienten und Rang ≥ 28.*[3]

[3]Eine lange Weierstrass-Gleichung für das entsprechende Beispiel ist $Y^2 + XY +$

Frage 2.26. *Gibt es eine universelle obere Schranke für den Rang in Mordells Satz?*

Auch diese Frage zum Rang ist offen. Es gibt eine Heuristik von Park, Poonen, Voight, und Matchett Wood, welche nahelegt, dass der Rang gegen oben beschränkt ist.

$Y = X^3 - X^2 - 20067762415575526585033208209338542750930230312178956502X + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429.$

3. Anwendungen

In diesem Abschnitt untersuchen wir die folgenden zwei Anwendungen der Theorie elliptischer Kurven:

- Der Diffie-Hellman Schlüsselaustausch mit elliptischen Kurven
- Lenstras (probabilistisches) Faktorisierungsverfahren für natürliche Zahlen

Für beide Anwendungen arbeiten wir nicht, wie in den ersten Abschnitten, mit elliptischen Kurven über dem Körper $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$. Sondern wir werden mit elliptischen Kurven über einem endlichen Körper oder gar einem endlichen Ring arbeiten.

3.1. Diffie-Hellman Schlüsselaustausch

Der Diffie-Hellman Schlüsselaustausch liefert eine Lösung für das folgende Problem.
Zwei Personen, hier A und B genannt, können nur über einem offenen (und unsicheren!) Kanal miteinander kommunizieren. Dies könnte z.B. eine nicht-abhörsichere Telefonleitung sein oder die beiden kommunizieren über Postkarten. Beide möchten sich auf ein gemeinsames Geheimnis einigen. In den Anwendungen ist dieses gemeinsame Geheimnis z.B. der Schlüssel für ein symmetrisches Verschlüsselungsverfahren wie AES. Sobald dieser gemeinsame Schlüssel beiden vorliegt, können A und B verschlüsselt miteinander kommunizieren. Beim Bilden des gemeinsamen Schlüssels müssen A und B davon ausgehen, dass Unbekannte zuhören. Es soll schlussendlich verhindert werden, dass diese keinen Rückschlüsse auf das Geheimnis machen können.
Der Schlüsselaustausch funktioniert wie folgt.

Schritt 1. A und B legen a priori eine grosse Primzahl p und damit einen endlichen Körper $\mathbb{F}_p$ fest. Sie einigen sich weiterhin auf eine elliptische Kurve

$$E : Y^2 = X^3 + aX + b$$

wobei $a, b \in \mathbb{F}_p$ und auf einen Punkt $P \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$. Die Sicherheit wird gewährleistet, wenn p "gross" ist und wenn die Ordnung von P als Element der abelschen Gruppe auch eine grosse Primzahl. [1] Die gesamte Information (p, E, P) ist an dieser Stelle rein

[1] Der einfachheitshalber arbeiten wir hier mit nicht mit langen Weierstrass-Gleichungen. In Anwendungen kommt z.B. die Primzahl $p = 2^{255} - 19$ und die elliptische Kurve $E : Y^2 = X^3 + 486662X^2 + X$ mit langer Weierstrass-Gleichung vor. Der rationale Punkt P hat die Form $(9, *)$. Er erzeugt eine Untergruppe von $E(\mathbb{F}_p)$ dessen Ordnung die Primzahl $\#E(\mathbb{F}_p)/8$ ist.

öffentlich. A und B müssen davon ausgehen, dass dritte Zugriff auf diese Information haben. Es gibt standardisierte Wahlen für dieses Tripels in den Implementationen.

Schritt 2. In diesem Schritt wählt A per Zufall eine natürliche Zahl a, die optimalerweise teilerfremd zur Ordnung von P ist. **Die Zahl a muss geheim bleiben**, nur A kennt sie. A berechnet nun den Punkt

$$a \cdot P = \underbrace{P + P + P + \cdots + P}_{a \text{ mal}}$$

als Element von $E(\mathbb{F}_p)$.
Diese Berechnung lässt sich wie folgt effizient gestalten. Ist die Entwicklung von a zur Basis 2 durch $\sum_i a_i 2^i$ mit $a_i \in \{0, 1\}$ gegeben, so gilt

$$a \cdot P = \sum_{i:a_i=1} 2^i \cdot P.$$

Also lässt sich $a \cdot P$ rein aus der Addition $E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ und Iterationen der Verdoppelungsabbildung $2\colon E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ bestimmen. Die Anzahl Rechenschritte ist in der Grössenordnung $\log a$. Da a von Grössenordnung p ist, sind das $O(\log p)$ Rechenschritte.

Schritt 3. B macht das gleiche und wählt eine geheime natürliche Zahl b. Daraufhin berechne B den Punkt $b \cdot P \in E(\mathbb{F}_p)$.

Schritt 4. Bis an hin wurde noch keine Information zwischen A und B ausgetauscht (bis auf die Wahl von (p, E, P) die öffentliche Information ist.) In Schritt 4 schickt A den Punkt $a \cdot P$ an B. Gleichzeitig schickt B den Punkt $b \cdot P$ an A. Dieser Informationsaustausch geschieht auf dem öffentlichen und unsicheren Kanal.

Schritt 5. Zu diesem Zeitpunkt besitzt A die Information a und $b \cdot P$ und B besitzt die Information b und $a \cdot P$.
Nun berechnet A den neuen Punkt

$$a \cdot (b \cdot P) \in E(\mathbb{F}_p).$$

Auf der anderen Seite des Kanals berechnet B den Punkt

$$b \cdot (a \cdot P) \in E(\mathbb{F}_p).$$

Nun sind wir am Ziel. Da $E(\mathbb{F}_p)$ eine Gruppe ist, gilt

$$a \cdot (b \cdot P) = (ab) \cdot P = (ba) \cdot P = b \cdot (a \cdot P),$$

diese Gleichung wurde bereits in (2.4) angesprochen.
Das gemeinsame Geheimnis ist der Punkt $(ab) \cdot P$. Dieses kann als Grundlage für die Festlegung eines Schlüssel für ein symmetrisches Verfahren genutzt werden.

Dieses Verfahren ist zur Zeit sicher, da es keinen effizienten Weg gibt, den Wert a (modulo $\mathrm{ord}(P)$) aus $a \cdot P$ zu rekonstruieren. Diese Problem nennt sich **diskreter Logarithmus**. In der Praxis ist $\mathrm{ord}(P)$ von der Grössenordnung p und damit in Anwendungen ca. 2^{256}. Einfaches "Absuchen" von a ist nicht praktikabel.
Dennoch ist es nicht ausgeschlossen, dass es einen noch unbekannten und effizienten Zugang zum diskreten Logarithmus gibt. Dabei bedeutet "effizient" ein Algorithmus der mit hoher Wahrscheinlichkeit a produziert und zwar in $O((\log p)^C)$ Rechenschritt für eine Konstante C.
Im Jahr 1994 hat Peter Shor [Sho94] einen "Quantum-Algorithmus" entwickelt, welcher den Diffie-Hellman Schlüsselaustausch unsicher macht, sollte ein hinreichend mächtiger Quantencomputer zur Verfügung stehen. Kurzum, die zukünftige Bedeutung des Diffie-Hellman Schlüsselaustausches ist offen.
Eine einfache Implementation des Diffie-Hellman Schlüsselaustausches ist als SageMath Skript auf der GitHub repository in

`sage/diffie-hellman-schluesselaustausch.ipynb`

zu finden.

3.2. Lenstras Verfahren

Gegeben sei eine natürliche zusammengesetzte Zahl $n \geq 2$. Die Sicherheit des kryptographischen Verfahren RSA beruht auf der (angeblichen) Schwierigkeit einen Primfaktor von n zu finden.[2]
Da n zusammengesetzt ist, besitzt n einen Primzahl p, so dass $p \leq \sqrt{n}$. Durch simples ausprobieren kann man mit ca. $\sqrt{n}$ ggT-Operationen p finden. Aber für $n \cong 2^{2048}$ sind das ca. $2^{1024} > 10^{300}$ Operationen.
Lenstras Faktorisierungsverfahren ist ein probabilistischer Algorithmus, um in Laufzeit ca. $e^{\sqrt{2 \log n} \sqrt{\log \log n}}$ einen Primfaktor von n zu finden. "Probabilistisch" bedeutet, dass der Algorithmus mit "grossen Wahrscheinlich" zum Ziel führt. D.h. es ist nicht mathematisch gesichert, dass der gesuchte Faktor gefunden wird. Aber dennoch ist es aus sicherheits-theoretischen Überlegungen wichtig, solche Algorithmen bei der Wahl eines kryptographischen Systems zu berücksichtigen.
In der gleichen Arbeit [Sho94] hat Shor gezeigt, dass das Faktorisierungsproblem für einen hinreichen starken Quantencomputer in polynomialer Zeit (in $\log n$) bewältigbar ist.
Lentsras Faktorisierungsverfahren beruht auf der Theorie elliptischer Kurven. Nun müssen wir jedoch einen Schritt weiter gehen als bis an hin. Wir betrachten Weierstrass-Gleichungen mit Koeffizienten in einem Ring, hier typischerweise $\mathbb{Z}/n\mathbb{Z}$. Da n in der Problemstellung gerade keine Primzahl ist, ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper, es ist ein kommutativer Ring mit (nicht-trivialen) Nullteiler. Wir werden nicht die Theorie elliptischer Kurven über

[2] Im konkreten Fall von RSA ist n ein Produkt pq aus zwei verschiedenen Primzahlen der Grössenordnung 2^{2048}.

einem Ring entwickeln,[3] sondern *ad hoc* so rechnen, wie wir das in Abschnitt 2 über einem Körper beschrieben haben. Dabei sind einige Vorkehrungen nötig, um Nullteiler zu berücksichtigen. Es sind aber gerade die Nullteiler von $\mathbb{Z}/n\mathbb{Z}$, welche Rückschlüsse auf die Primfaktoren von n schliessen lassen.
Wir werden die folgende Notation verwenden. Gegeben sei $n \in \mathbb{N}$. Eine ganze Zahl $a \in \mathbb{Z}$ repräsentiert eine Nebenklasse

$$\overline{a} = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}.$$

Also verwenden wir $\overline{a}$ um die Nebenklasse zu beschreiben.
Gegeben seien $a, b \in \mathbb{Z}$ und die Gleichung $E : Y^2 = X^3 + \overline{a}X + \overline{b}$ mit Koeffizienten in $\mathbb{Z}/n\mathbb{Z}$. Wir können die Diskriminante

$$\Delta_E = \overline{-2^4(4a^3 + 27b^2)} \in \mathbb{Z}/n\mathbb{Z}$$

definieren. Aber die Bedingung $\Delta_E \neq 0$ reicht in dieser Situation nicht aus, um E als "elliptische Kurve" bezeichnen zu dürfen, den $\mathbb{Z}/n\mathbb{Z}$ besitzt Nullteiler. Wir brauchen die stärkere Bedingung $\Delta_E \in (\mathbb{Z}/n\mathbb{Z})^\times$, dabei bezeichnet $(\mathbb{Z}/n\mathbb{Z})^\times$ die Elemente in $\mathbb{Z}/n\mathbb{Z}$ die sich multiplikativ invertieren lassen.[4]
Die in Abschnitt 2 beschrieben Vorschrift definiert nur eine partielle Verknüpfung auf

$$E(\mathbb{Z}/n\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 : y^2 = x^3 + \overline{a}x + \overline{b}\} \cup \{\mathcal{O}\}.$$

Es gilt

$$\Delta_E \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \mathrm{ggT}(-2^4(4a^3 + 27b^2), n) = 1. \tag{3.1}$$

In der Praxis lässt sich der ggT sehr effizient mittels Teilung mit Rest berechnen. Sollte Δ_E **keine** Einheit sein, dann haben die "nicht reduzierte" Diskriminante $-2^4(4a^3+27b^2)$ und n einen gemeinsamen Teiler $d > 1$. Nun gibt es zwei Fälle:

- **Fall 1: Es gilt** $d = n$**.** In diesem Fall haben wir leider nichts gewonnen
- **Fall 2: Es gilt** $d < n$**.** Dann ist d ein echten Teiler von n. Um ein Primfaktor von n zu finden, reicht es, einen Primfaktor von d zu finden. Da $d \leq n/2$ hat sich das Problem durch diesen Schritt exponentiell vereinfacht. Ist $n = pq$ das Produkt verschiedener Primzahlen p und q (wie in RSA), so gilt sogar $d = p$ oder $d = q$ und wir sind im Ziel.

Nun beschreiben wir eine vereinfachte Version von Lentras Verfahren. Gegeben sie $n = pq \in \mathbb{N}$ das Produkt zweier Primzahlen $p \neq q$.

Schritt 1. Wir wählen zufällig $a, x, y \in \{0, \ldots, n-1\}$. Diese repräsentieren $\overline{a}, \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$. Dann definieren wir

$$b = y^2 - x^3 - ax \in \mathbb{Z}.$$

[3] Solche Objekte heissen **elliptische Schemata** oder **abelsche Schemata**
[4] Für n eine Primzahl ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper und die Bedingung ist mit $\Delta_E \neq 0$ gleichbedeutend.

Das Paar $(\overline{x}, \overline{y})$ ist eine Nullstelle von $Y^2 - (X^3 + \overline{a}X + \overline{b})$.

Schritt 2. Wir berechnen $\Delta = -2^4(4a^3 + 27b^2) \in \mathbb{Z}$. Falls $\mathrm{ggT}(\Delta, n) > 1$, d.h. $\overline{\Delta}$ ist **keine** Einheit in $\mathbb{Z}/n\mathbb{Z}$, so verwenden wir die Überlegung direkt unterhalb von (3.1). Im (unwahrscheinlichen) Fall 1 kehren wir zurück zu Schritt 1 und wählen eine neue Kurve. Alternativ kann man Fall 1 a priori ausschliessen, wenn man die Repräsentanten $a, x, y \in \{0, \ldots, n\}$ klein genug in Funktion von n wählt, um $|\Delta| < n$ zu erzwingen.
Im Fall 2 muss $d = p$ oder $d = q$ gelten. Wir sind fertig, da ein Primfaktor von n berechnet wurde. Hier ist entscheidend, dass sich der ggT schnell berechnen lässt.
Also können wir für das weitere Vorgehen annehmen, dass $\Delta_E \in (\mathbb{Z}/n\mathbb{Z})^\times$. Damit definiert $E : Y^2 = X^3 + \overline{a}X + \overline{b}$ eine (verallgemeinerte) elliptische Kurve mit Koeffizienten in $\mathbb{Z}/n\mathbb{Z}$.

Schritt 3. Wir betrachten das Paar $(\overline{x}, \overline{y})$ als Punkt P in $E(\mathbb{Z}/n\mathbb{Z})$. Die in Abschnitt 2, Abschnitt 2.2.1, beschriebene Verknüpfung kann man ad hoc auf die Punkte in $E(\mathbb{Z}/n\mathbb{Z})$ anzuwenden. Unser Ziel ist es, ein Vielfaches $B \cdot P$ zu berechnen, dabei ist $B = k! \in \mathbb{N}$ eine natürliche Zahl. Konkret werden wir $2 \cdot P, 6 \cdot P, 24 \cdot P$ bis zu $B \cdot P$ ausrechnen.
Um das effizient zu gestalten, entwickeln wir k, wie beim Diffie-Hellman Schlüsselaustausch, zur Basis 2. D.h. wir schreiben $k = \sum_i k_i 2^i$ mit $k_i \in \{0, 1\}$. Wir möchten

$$\sum_{i:k_i=1} 2^i \cdot Q$$

für $Q \in E(\mathbb{Z}/n\mathbb{Z})$ bestimmen.
Insgesamt müssen wir auf $E(\mathbb{Z}/n\mathbb{Z})$ zwei Punkte addieren können. Da aber $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist, darf nicht durch ein Element ungleich Null dividiert werden. Es gibt Nullteiler. Z.B. im Unterfall 1a wird bei der Konstruktion der Steigung m durch die Differenz $x_1 - x_2$. Oder im Unterfall 2a, bei der Verdoppelung, wird durch $2y$ geteilt.
Teilen ist jedoch nur erlaubt, wenn das entsprechende Element in $(\mathbb{Z}/n\mathbb{Z})^\times$ liegt. D.h. bei jeder Teilung müssen wir überprüfen, dass der ggT eines Repräsentanten in $\mathbb{Z}$, von $x_1 - x_2$ oder $2y$, zu n gleich 1 ist. Ist der ggT gleich 1, so dürfen wir teilen und die Berechnung durchführen. Ist der ggT jedoch > 1 so sind wir wieder in einer Fallunterscheidungen wie unterhalb von (3.1).
Sollte $d = n$ gelten, so haben wir "Pech". Wir müssen das Verfahren wieder bei Schritt 1 mit einer neuen Wahl von $\overline{a}, \overline{x}, \overline{y}$ starten. Es scheint schwierig, diesen unglücklichen Ausgang a priori auszuschliessen. Deshalb ist dieser Algorithmus "probabilistisch".
Gilt jedoch $1 < d < n$, so muss (da $n = pq$) $d = p$ oder $d = q$ gelten. In diesem Fall sind wir fertig, da ein Primfaktor gefunden wurde.

Die genaue Wahl von B spielt für die Analyse des Algorithmus eine wichtig Rolle auf die wir hier nicht eingehen werden. Anstatt einer Fakultät, stellt sich als vorteilhaft heraus, für B ein Produkt von vielen "kleinen" Primzahlen zu wählen.
Eine einfache Implementation dieses Verfahrens ist als SageMath Skript auf der GitHub repository in

`sage/primfaktorisierung_lenstra.ipynb`

zu finden. Hier wurde $B = 10!$ festgelegt.

4. Elliptische Kurven über den komplexen Zahlen

Nachdem wir elliptischen Kurven mittels einer Weierstrass-Gleichung definiert haben, beschäftigen wir uns in diesem Kapitel über den Spezialfall des Grundkörpers $K = \mathbb{C}$. Hier gibt es einen Zugang zu elliptischen Kurven über komplexe Analysis und Gitter in $\mathbb{C}$. Einen detaillierten Zugang zu diesen Überlegungen ist in Kapitel VI von Silvermans Buch [Sil86] zu finden.

Definition 4.1. *Ein **Gitter in** $\mathbb{C}$, ist eine Teilmenge der Form*

$$\Omega = \{\lambda_1\omega_1 + \lambda_2\omega_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\}$$

wobei $\omega_1, \omega_2 \in \mathbb{C}$ nicht auf einer Gerade durch den Nullpunkt liegen.

Die Bedingung an ω_1, ω_2 schliesst aus, dass $\omega_1\omega_2 = 0$ und dass es $\lambda \in \mathbb{R}$ gibt, so dass $\omega_1 = \lambda\omega_2$.

Übungsaufgabe 4.A. *Zeigen Sie, dass $\omega_1, \omega_2 \in \mathbb{C}$ genau dann auf einer Gerade durch den Nullpunkt liegen, wenn*

$$\det \begin{pmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{pmatrix} = 0,$$

dabei bezeichnet $\bar{\cdot}$ komplexe Konjugation.

Ein Gitter in $\mathbb{C}$ ist abgeschlossen unter der Addition auf $\mathbb{C}$ und unter Multiplikation mit -1. Es ist eine Untergruppe der additive Gruppe des Körpers $\mathbb{C}$.
Das Paar (ω_1, ω_2) nennt man auch Basis von Ω. Die Basis ist nie eindeutig durch das Gitter festgelegt.
Die folgende Notation ist naheliegende: $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

Beispiel 4.2. *Das Gitter in $\mathbb{C}$ mit Basis $(1, e^{2\pi\sqrt{-1}/6})$ ist in Abbildung 4.1 dargestellt.*

Gegeben sei ein Gitter Ω in $\mathbb{C}$, wir können dazu eine Funktion konstruieren. Für $z \in \mathbb{C} \smallsetminus \Omega$ definieren wir

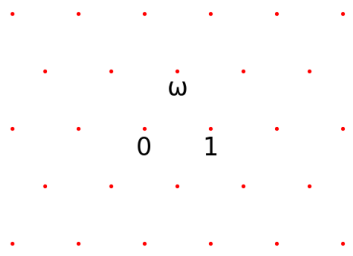
$$\wp_\Omega(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{4.1}$$

Bemerkung 4.3. *Die Reihe (4.1) konvergiert absolut für alle $z \in \mathbb{C} \smallsetminus \Omega$. Für $\omega \neq 0$ und $\omega \neq z$ ist der Absolutbetrag von*

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2 - (z-\omega)^2}{(z-\omega)^2\omega^2} = \frac{-z^2 + 2z\omega}{(z-\omega)^2\omega^2}$$

höchstens $C(z)/|\omega|^3$, wobei $C(z) > 0$ von ω unabhängig ist.

Abbildung 4.1.: Das Gitter $\mathbb{Z} + \omega\mathbb{Z}$ in $\mathbb{C}$ mit $\omega = e^{2\pi\sqrt{-1}/6}$



Ohne Beweis halten wir die folgenden Fakten fest. Die Abbildung $z \mapsto \wp_\Omega(z)$ ist wohldefiniert und komplex differenzierbar auf $\mathbb{C} \setminus \Omega$. Sie ist eine sogenannte meromorphe Funktion mit einer doppelten Polstelle an jedem Punkt auf Ω. Man nennt $\wp_\Omega$ die zu Ω gehörige **Weierstrass-$\wp$ Funktion**.

Lemma 4.4. *Sei Ω eine Gitter in $\mathbb{C}$ und $\wp_\Omega$ die Funktion oben. Für alle $z \in \mathbb{C} \setminus \Omega$ erfüllt die Ableitung*

$$\wp'_\Omega(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}. \tag{4.2}$$

Für alle $z \in \mathbb{C} \setminus \Omega$ und alle $\omega \in \Omega$ gilt $\wp_\Omega(z+\omega) = \wp_\Omega(z)$ und $\wp'_\Omega(z+\omega) = \wp'_\Omega(z)$.

Beweis. Die Formel für die Ableitung folgt aus (4.1), man darf summandenweise Ableitung, da die Reihe absolut konvergiert. Es gilt $\wp'_\Omega(z+\omega) = \wp'_\Omega(z)$ wie im zweiten Teil der Aussage, da die Summe (4.2) invariant unter Translation von z wieder in Ω list. Es folgt damit

$$\wp_\Omega(z+\omega) = \wp_\Omega(z) + c(\omega)$$

wobei $c(\omega)$ nur von ω aber nicht von z abhängt. Wir setzen $z = -\omega/2$ ein und finden $\wp_\Omega(\omega/2) = \wp_\Omega(-\omega/2) + c(\omega)$. Aber man kann sich aus (4.1) davon überzeugen, dass $\wp_\omega(z) = \wp_\omega(-z)$ gilt, d.h. $\wp_\omega$ ist eine gerade Funktion. Es folgt $c(\omega) = 0$. □

Bemerkung 4.5. *Sowohl $\wp_\Omega$ wie auch $\wp'_\Omega$ sind **doppelperiodische Funktionen**. Deshalb werden die Elemente aus Ω auch Perioden genannt.*

Ohne Beweis erwähnen wir, dass $\wp_\Omega$ eine wichtige Differentialgleichung erfüllt. Genauer, es gibt $g_2 = g_2(\Omega), g_3 = g_3(\Omega) \in \mathbb{C}$, so dass

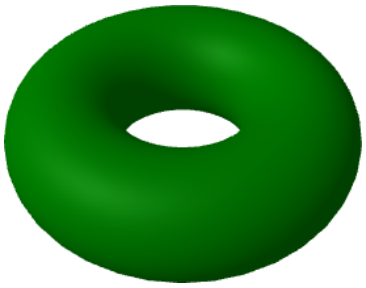
$$g_2^3 - 27g_3^2 \neq 0 \tag{4.3}$$

und

$$\wp'^2_\Omega = 4\wp^3_\Omega - g_2\wp_\Omega - g_3. \tag{4.4}$$

Bis auf den Faktor 4 liegen die Werte des Paars $(\wp_\Omega, \wp'_\Omega)$ auf einer elliptischen Kurve. Die Bedingung (4.3) entspricht dabei der Bedingung (2.2).
Der Faktor 4 ist harmlos, wir können die gesamten Überlegungen aus Kapitel 2 auf die

Abbildung 4.2.: Ein Torus



modifizierte Weierstrass-Gleichung

$$Y^2 = 4X^3 - g_2X - g_3 \quad \text{wobei} \quad g_2^3 - 27g_3^2 \neq 0 \tag{4.5}$$

anwenden und ein Gruppengesetz auf $E(\mathbb{C})$ definieren.
Wir definieren eine Abbildung

$$\Psi\colon \mathbb{C} \to E(\mathbb{C})$$

durch

$$\Psi(z) = \begin{cases} (\wp_\Omega(z), \wp'_\Omega(z)) & : z \notin \Omega, \\ \mathcal{O} & : z \in \Omega. \end{cases}$$

Wegen der Doppelperiodizität von $\wp_\Omega$ und $\wp'_\Omega$ gilt $\Psi(z+\omega) = \Psi(z)$ für alle $z \in \mathbb{C}$ und alle $\omega \in \Omega$.
Weiterhin, und dies ist nicht trivial, ist Ψ ein Gruppenhomomorphismus, wobei wir $\mathbb{C}$ als additive Gruppe des Körpers der komplexen Zahlen verstehen. Schliesslich ist Ψ auch eine surjektive Abbildung. Aus diesen Überlegungen folgt, dass

$$\mathbb{C}/\Omega \quad \text{und} \quad E(\mathbb{C}) \quad \text{vermöge } \Psi \text{ als Gruppen isomorph sind.}$$

Weiterhin können trägt $E(\mathbb{C})$ wegen der Interpretation aus Abschnitt 2.5 die Struktur eines topologischen Raums. Aus topologischer Sicht sind $\mathbb{C}/\Omega$ und $E(\mathbb{C})$ ununterscheidbar.

Bemerkung 4.6. *Aus topologischer Sicht ist $\mathbb{C}/\Omega$ nichts anderes als ein Torus, vgl. Abbildung 4.2. Topologisch gesehen sehen alle elliptischen Kurven über $\mathbb{C}$ gleich aus. Aber die elliptische Kurve selber trägt zusätzliche Struktur, da sie schlussendlich von einer Weierstrass-Gleichung kommt. Diese Struktur ist feiner als die Topologie.*

Bemerkung 4.7. *Sei Ω ein Gitter in $\mathbb{C}$ mit Basis (ω_1, ω_2) Die Halbperioden $\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$ repräsentieren Elemente der Ordnung 2 in $\mathbb{C}/\Omega$. Wie für die übliche Weierstrass-Gleichung, ohne den Faktor 4, kann man zeigen, dass die Ordinate eines Punktes der Ordnung 2 verschwindet. Folglich gilt*

$$\wp'_\Omega\left(\frac{\omega_1}{2}\right) = \wp'_\Omega\left(\frac{\omega_2}{2}\right) = \wp'_\Omega\left(\frac{\omega_1+\omega_2}{2}\right) = 0.$$

Es folgt, dass

$$\wp_\Omega(z) \text{ eine Nullstelle von } 4X^3 - g_2(\Omega)X - g_3(\Omega) \text{ ist für alle } z \in \left\{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\right\}.$$

Also kann man kubische Gleichungen mit der Hilfe von der Weierstrass-$\wp$ Funktion lösen.

Eine modifizierte Weierstrass-Gleichung (4.5) legt ein Gitter Ω in $\mathbb{C}$ fest, für welches (4.4) gilt. Die "Perioden" in Ω lassen sich durch Integrale

$$\int \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}$$

bestimmen. Das Integral findet auf bestimmten Schleifen in $\mathbb{C}$ statt und der Wert des Integrals hängt auch von der Schleife ab. Diese Integrale heissen aus historischen Gründen **elliptischen Integrale** und sind verantwortlich für den Begriff "elliptisch" in elliptische Kurve.[1]

[1] Elliptische Kurven sind keine Ellipsen!

A. Komplexe Multiplikation

Eines der faszinierendsten Aspekte der Theorie elliptischer Kurven ist die Möglichkeit komplexer Multiplikation. Diese soll nur an einigen Beispielen veranschaulicht werden. Wir beginnen mit einer Weierstrass-Gleichung $E : Y^2 = X^3 + aX + b$ mit a, b in einem beliebigen Körper K. Wie um (2.3) beschrieben, können wir Punkt $P \in E(K)$ mit ganzen Zahlen multiplizieren, z.B. $2 \cdot P = P + P$ und $3 \cdot P = P + P + P$ etc. Dies ist in jeder Gruppe möglich, stellt also keine Besonderheit von elliptischen Kurven dar.

Beispiel A.1. *Wir betrachten die elliptische Kurve die durch $E : Y^2 = X^3 + X$ definiert ist. Der Grundkörper K sei nun $\mathbb{C}$. Sei $(x, y) \in \mathbb{C}^2$ eine Nullstelle von $Y^2 = X^3 + X$. Dann gilt*

$$(\sqrt{-1}y)^2 = -y^2 = -(x^3 + x) = (-x)^3 + (-x).$$

Also ist $(-x, \sqrt{-1}y)$ wieder eine Nullstelle der Weierstrass-Gleichung. Für jeden Punkt $P \in E(\mathbb{C})$ definiert man

$$I(P) = \begin{cases} (-x, \sqrt{-1}y) & : P = (x, y) \\ \mathcal{O} & : P = \mathcal{O}. \end{cases}$$

Damit erhalten wir eine Selbstabbildung $I \colon E(\mathbb{C}) \to E(\mathbb{C})$.
Verkettet man I mit sich selbst, so erhält man

$$I(I(P)) = (x, -y)$$

falls $P \neq \mathcal{O}$. Also ist $I \circ I$ die Inversionsabbildung $- \colon E(\mathbb{C}) \to E(\mathbb{C})$.
In geeigneter Notation gilt $I^2 = I \circ I = -1$.
Man kann nun überprüfen, z.B. von Hand, dass I mit dem Gruppengesetz kompatibel ist. D.h. es gilt

$$I(P + Q) = I(P) + I(Q) \quad \text{für alle} \quad P, Q \in E(\mathbb{C}).$$

Schliesslich kann man für alle $\alpha, \beta \in \mathbb{Z}$ eine weitere Selbstabbildung $\alpha + \beta I$ von $E(\mathbb{C})$ gemäss

$$(\alpha + I\beta)(P) = (\alpha \cdot P) + (\beta \cdot I(P))$$

definieren.
Wie identifizieren die Menge $\{\alpha + I\beta : \alpha, \beta \in \mathbb{Z}\}$ der eben definierten Selbstabbildung mit dem Ring der Gaussschen Zahlen

$$\mathbb{Z}[\sqrt{-1}] = \{\alpha + \sqrt{-1}\beta : \alpha, \beta \in \mathbb{Z}\}.$$

Wir erhalten eine Verknüpfung

$$\mathbb{Z}[\sqrt{-1}] \times E(\mathbb{C}) \to E(\mathbb{C})$$

welche es uns erlaubt, Punkte in $E(\mathbb{C})$ mit Gausssche Zahlen zu multiplizieren. Für festes $\gamma \in \mathbb{Z}[\sqrt{-1}]$ ist der Ausdruck $\gamma \cdot P$ ein komplizierter Bruch von Polynomen in den Koordinaten von P.
Nicht jede elliptische Kurve erlaubt komplexe Multiplikation. In der Tat gibt es (in einem geeigneten Sinn) nur eine elliptische Kurve, die komplexe Multiplikation mit $\mathbb{Z}[\sqrt{-1}]$ wie oben erlaubt.

Übungsaufgabe A.A. *Zeigen Sie, dass der Ring der Gaussschen Zahlen $\mathbb{Z}[\sqrt{-1}]$ unter Addition und Multiplikation in $\mathbb{C}$ abgeschlossen ist.*

Übungsaufgabe A.B. *Überprüfen Sie mit der Definition, dass in der Notation des Beispiels oben $I(P+Q) = I(P) + I(Q)$ für alle $P, Q \in E(\mathbb{C})$ gilt.*

Es gibt auch eine elliptische Kurven, die "komplexe Multiplikation" mit dem Ring der Eisenstein Zahl

$$\left\{\alpha + \beta e^{2\pi\sqrt{-1}/6} : \alpha, \beta \in \mathbb{Z}\right\}$$

hat. Im Allgemeinen taucht jede "quadratische Ordnung", darunter z.B. auch

$$\left\{\alpha + \beta\frac{1+\sqrt{-163}}{2} : \alpha, \beta \in \mathbb{Z}\right\}$$

auf. Die Theorie der "komplexen Multiplikation" von elliptischen Kurven und deren Verallgemeinerung begann im 19ten Jahrhundert und spielt auch noch heute in der Grundlagenforschung eine zentrale Rolle [Slo22].
Komplexe Multiplikation liefert auch eine überzeugende Erklärung, wieso

$$e^{\sqrt{163}\pi} = 262537412640768743,99999999999992500725971\ldots$$

fast die ganze Zahl $640320^3 + 744$ ist.

Literaturverzeichnis

[CFA+06] H. Cohen, G. Frey, R. Avanzi, Chr. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[Sil86] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.

[Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Slo22] L. Sloman. Mathematicians Prove 30-Year-Old André-Oort Conjecture. *Quantamagazine*, 2022. `https://www.quantamagazine.org/mathematicians-prove-30-year-old-andre-oort-conjecture-20220203/`.

[ST15] J.H. Silverman and J.T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

Index