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 31. August 2022 um 17:48

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 Ungenaugigkeiten an meine Email-Adresse auf der Titelseite.

0.1 Notation

Wir verwenden die folgenden Konventionen.

- Die Menge der natürlichen Zahlen ist $\mathbb{N} = \{1, 2, 3, \dots\}$.
- 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 rechwinkligen 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 die Zahl $a'b'/2 = \lambda^2 ab/2 = \lambda^2 n$ kongruent, falls sie ganz ist.*

(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 Fermat bewiesen.

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

Beweis. TODO □

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 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.
In der Definition von kongruente Zahl kommen

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

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

Beweis. Teil (i) ist eine direkt Rechnung. Es gilt
$$y^2 = \frac{4n^4}{(c-a)^2} = \frac{a^4b^4}{4(c-a)^2}$$
und
$$x^3 - n^2x = n^3\frac{b^3}{(c-a)^3} - n^3\frac{b}{c-a} = n^3\frac{b}{c-a}\left(\frac{b^2}{(c-a)^2} - 1\right) = n^3b\frac{b^2-(c-a)^2}{(c-a)^3} = \frac{a^3b^4}{8}\frac{b^2-(c-a)^2}{(c-a)^3}.$$
Es gilt
$$y^2 - (x^3 - n^2x) = \frac{a^3b^4}{8(c-a)^3}\left(2a(c-a) - b^2 + (c-a)^2\right) = \frac{a^3b^4}{8(c-a)^3}(c^2 - a^2 - b^2) = 0,$$
was für (i) zu zeigen.
Für den Beweis von (ii) setzen wir
$$a = \left|\frac{n^2 - x^2}{y}\right|, \quad b = \left|\frac{2nx}{y}\right|, \quad \text{und} \quad c = \left|\frac{n^2 + x^2}{y}\right|.$$
Eine direkt Rechnung zeigt $a^2 + b^2 = c^2$. Weiterhin gilt
$$\frac{ab}{2} = \frac{|(n^2 - x^2)(2nx)|}{2y^2} = \frac{2n|n^2x - x^3|}{2y^2} = \frac{n|-y^2|}{y^2} = n.$$
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 Lösungsmenge der kubischen Gleichung

$$Y^2 = X^3 - n^2 X \tag{1.1}$$

definiert 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. 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.
Die Gleichung (1.1) ist ein Spezialfall der Weierstrass-Gleichung, welche im Allgemeinen eine elliptische Kurve definiert.
Den Satz von Fermat, Satz 1.5, lässt sich wie folgt umformulieren.

Satz 1.9 (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 ein 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 Krytographie 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 die arithmetischen 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 (1.1) 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) mit $\Delta_{E_n} = -2^4 3^3 n^4$.

(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 $2 = 0$.*

[1] Diese Beizeichnung ist nicht standard.

Das ist unbefriedigend, da für Anwendung in der Kryptographe endliche Körper der Charakteristik 2 wichtig sind. 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 $F(x, y) \neq 0$. 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

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

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

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, 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 Tangent 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 "Glattheitsbedigung" verstehen lässt.

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

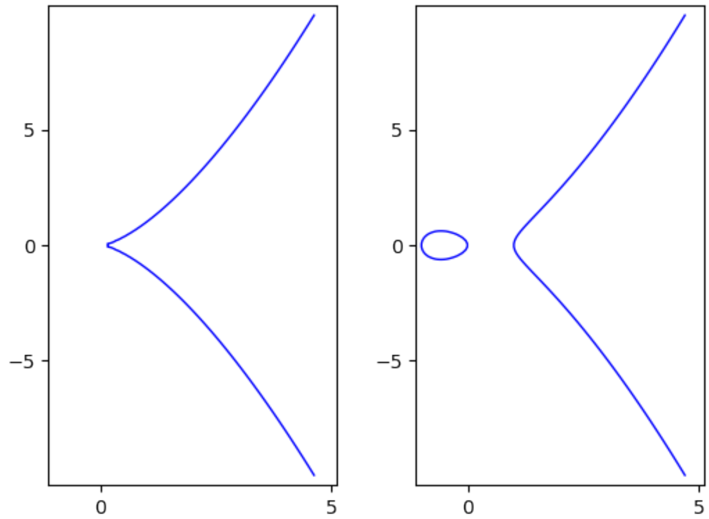
$$\frac{\frac{\partial F}{\partial X}}{-\frac{\partial F}{\partial Y}}(x,y) = \frac{3x^2+a}{2y}$$

***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 veraschaulichen. 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 1.9, dass*

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

aus vier Elementen besteht.

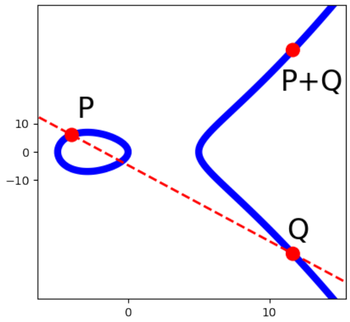
Wir werden zeigen, dass wir $E(K)$ mit der Struktur einer abelschen Gruppe verstehen können. Dazu müssen wir eine Verknüpfung $+\colon E(K) \times E(K) \to E(K)$, eine Inversionsabbildung $-\colon E(K) \to E(K)$, sowie ein neutrales Element in $E(K)$ produzieren.

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

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

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



definieren. Es ist üblich, die Verknüpfung mit "+" zu bezeichnen. Später werden wir feststellen, dass die so konstruierte Gruppe eine abelsche Gruppe ist.
Seien P und Q Elemente von $E(K)$. Es folgt eine Aufspaltung in verschiendene Fälle. Wir werden bereits in der Konstruktion überprüfen, dass die Verküpfung $+$ 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.

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 hat die Gesalt

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

mit $q = y_1 - mx_1$. 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 defineren wir das Polynom

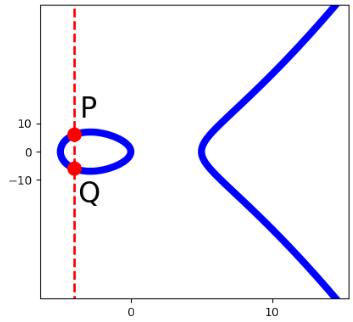
$$A = (mX + q)^2 - (X^3 + aX + b) = -X^3 + m^2 X + (\text{Terme von Grad} \leq 1 \text{ in } X) \in K[X].$$

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 $A = -(X - x_1)(X - x_2)(X - x_3)$, 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.

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



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

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

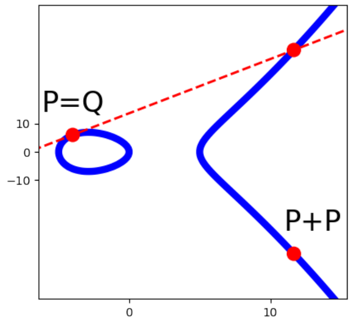
und daher $y_1 = -y_2$ da $P \neq Q$. Nun stehen wir vor einem Dilemma, die Gerade G hat keine weiteren Schnittpunkte mit $E(K)$ in der Ebene K^2. Jetzt kommt uns der Punkt $\mathcal{O}$ zur Hilfe.
In Unterfall 1b definieren wir

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

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 $E(\mathbb{R}) \setminus \{Q, \mathcal{O}\}$, 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 and $E(\mathbb{R}) \setminus \{\mathcal{O}\}$ durch den Punkte P. Vgl. Abbildung 2.4.
Für einen allgemeinen Körper können wir zwar nicht mit solchen Grenzbegriffen argumentieren, aber wir haben einen Ersatz für die Tangente in Bemerkung 2.5 und Definition 2.6 gefunden.

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



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 nur 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

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

Trivialierweise 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

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

Trivialierweise 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 mah 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 gilt $P = (x, y)$. Wegen $y^2 = x^3 + ax + b$ ist auch $(x, -y)$ eine Lösung der Weierstrass-Gleichung. Wir definieren

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

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

Die Abbildung $+\colon E(K) \times E(K) \to E(K)$ ist wohldefiniert. Weiterhin überprüfen wir mit der Hilfe von den Unterfällen 1b, 2b und Fall 3 der Konstruktion, dass

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

für alle $P \in E(K)$.
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 Ansätz 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. ingesamt 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 E 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 Gruppengesetzt der Picard-Gruppe in Verbindung setzt.

Bemerkung 2.11. *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 Teilnmenge von $E(K')$. Da die Verknüpfung algebraisch ist, ist $E(K)$ eine Untergruppe von $E(K')$.

2.4 Die Projektive Ebene

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

Definition 2.12. *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 2.13. *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 $(x, y, z) \in K^3 \setminus \{0\}$. Zwei Tripel $(x, y, z), (x', y', z') \in K^3 \setminus \{0\}$ definieren die gleiche Gerade genau dann, wenn $(x, y, z) = (\lambda x', \lambda y', \lambda z')$ für ein $\lambda \in K \setminus \{0\}$. In diesem Fall schreiben wir $(x, y, z) \sim (x', y', z')$. Dabei definiert $\sim$ eine Äquivalenzrelation auf $K^3 \setminus \{0\}$.
Die K-Punkte projektive Ebene sind die Äquivalenzklassen dieser Äquivalenzrelation, d.h.

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

Wir bezeichnen Punkte in $\mathbb{P}^2(K)$ mit $[x : y : z]$, wobei $(x, y, z) \in K^3 \setminus \{0\}$. 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. <u>nicht</u> durch den Punkt $[x : y : z]$ bestimmt.*
Die Abbildung

$$K^2 \ni (x, y) \to [x : y : 1] \tag{2.3}$$

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.

$$F^{\mathrm{hom}} = F(X/Z, Y/Z)Z^3 = Y^2Z - X^3 - aXZ^2 - bZ^3. \tag{2.4}$$

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

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

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 $F^{\mathrm{hom}}(x, y, z) = 0$.

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

Ist eine dieser Aussagen erfüllt, so schreiben wir $F^{\mathrm{hom}}(P) = 0$.
betrachten wir die "Nullstellenmenge"

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

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 $F^{\mathrm{hom}}(P) = 0$ heisst nun $F(x, y) = 0$ und damit ist $(x, y) \in E(K) \smallsetminus \{\mathcal{O}\}$.
Fall 2. Es gilt $z = 0$. Die Bedingung $F^{\mathrm{hom}}([x : y : 0]) = 0$ impliziert $x = 0$ wegen (2.4). 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 $(x, y) \in E(K) \smallsetminus \{\mathcal{O}\}$, so liegt $[x : y : 1]$ in $E^{\mathrm{hom}}(K)$.
Vermöge der Abbildung (2.3) haben wir die natürliche Bijektion

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

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 drei Punkte $P = Q, [0 : 1 : 0]$ auf einer projektiven Gerade in $\mathbb{P}^2(K)$, welche E "mit Vielfachheit 2" schneidet.

Lemma 2.14. *Sei $E : Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung mit $a, b \in K$. Sei $P = (x, y) \in E(K) \smallsetminus \{0\}$. 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 2.15. *Sei $n \in \mathbb{N}$ und $E_n : Y^2 = X^3 - n^2X$. Dann ist n genau dann eine kongruente Zahl, wenn $E_n(\mathbb{Q}) \supsetneq \{(0, 0), (\pm n, 0), \mathcal{O}\}$.*

Beweis. Das Korollar folgt aus Lemma 1.8. □

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

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

Beispiel 2.16. *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 1.9, dass $E_1(\mathbb{Q}) = H = \{(0,0), (\pm 1, 0), \mathcal{O}\}$.

Beispiel 2.17. *Sei E durch $Y^2 = X^3 - 5^2X$ definiert und $P = (-4, 6) \in E(\mathbb{Q})$. Wir berechnen*

$$\begin{aligned} 2P = P + P &= \left(\frac{1681}{144}, \frac{62279}{1728}\right), \\ 3P = P + P + P &= \left(\frac{-2439844}{5094049}, \frac{-39601568754}{11497268593}\right), \\ 4P = P + P + P + P &= \left(\frac{11183412793921}{2234116132416}, -\frac{17910765342322245919}{3339324446657665536}\right). \end{aligned}$$

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

Lemma 2.18. *Sei $n \neq 0$ in $\mathbb{Q}$ und $E : Y^2 = X^3 - n^2X$. Sei $P \in E(\mathbb{Q})$, dann hat P nicht Ordnung 4.*

Beweis. Sei $P = (x, y) \in E(\mathbb{Q})$. Wir dürfen annehmen, dass P nicht Ordnung 2 hat. Also gilt $y \neq 0$ wegen Lemma 2.14. Es gilt $2P = (*, y')$ mit $y' \in \mathbb{Q}$.
Mit Unterfall 2a berechnen wir

$$\begin{aligned} 2P = P + P &= \left(*, \frac{-27x^6 + 27n^2x^4 + 36y^2x^3 - 9n^4x^2 - 12n^2y^2x + (-8y^4 + n^6)}{8y^3}\right) \\ &= \left(*, \frac{x^6 - 5n^2x^4 - 5n^4x^2 + n^6}{8y^3}\right) \end{aligned}$$

dabei verwendeten wir $y^2 = x^3 - n^2x$. 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 $\mathbb{Q}$. 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 2.14. □

Satz 2.19 (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 $x, y \in \mathbb{Z}$.*

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 $a, b \in \mathbb{Z}$.
Ein tiefes Resultat von Barry Mazur legt die Gruppe G bis auf ein paar wenige Möglichkeiten fest.

Satz 2.21 (Mazur (1978))**.** *In der Notation von Mordells Satz ist G zu einer der folgenden Gruppen isomorph:*

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

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

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 2.14 ein $(x, y) \in E_n(\mathbb{Q})$ mit $y \neq 0$. Wegen Korollar 2.15 ist n eine kongruente Zahl.
Sei umgekehrt n eine kongruente Zahl. Wegen Korollar 2.15 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. Lemma 2.16. Die Untergruppe H ist ebenfalls eine Untergruppe von G wie in Mazurs Satz. Folglich ist $G = H$ oder G ist zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ isomorph. Im zweiten Fall hätte $E_n(\mathbb{Q})$ ein Element der Ordnung 4, aber dies ist durch Lemma 2.18 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. $\square$

Man kann diesen letzten Satz auch ohne den tiefen Satz von Mazur beweisen.
Hier ist der aktuelle Weltrekord bzgl. dem Rang.

Satz 2.24 (Elkies (2006))**.** *Es gibt eine Weierstrass-Gleichung mit rationalen Koeffizienten und Rang* ≥ 28.[2]

Frage 2.25. *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 Mathcett Wood, welche nahelegt, dass der Rang gegen oben beschränkt ist.

[2]Eine lange Weierstrass-Gleichung für das entsprechende Beispiel ist $Y^2 + XY + Y = X^3 - X^2 - 20067762415575526585033208209338542750930230312178956502X + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$.

3 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 detailierten Zugang zu diesen Überlegungen ist in Kapitel VI von Silvermans Buch [Sil86] zu finden.

Definition 3.1. *Ein* ***Gitter in*** $\mathbb{C}$*, ist eine Teilmenge*

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

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 3.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 $\Omega \subseteq \mathbb{C}$ 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 des Gitters Ω. Kurzhand Notation ist $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Die Basis ist <u>nicht</u> eindeutig durch das Gitter festgelegt.

Beispiel 3.2. *Das Gitter mit Basis* $(1, e^{2\pi\sqrt{-1}/6})$ *ist in Abbildung 3.1 darsgestellt.*

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

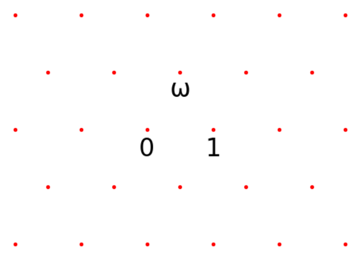
$$\wp_\Omega(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{3.1}$$

Bemerkung 3.3. *Die Reihe (3.1) konvergiert absolut für alle* $z \in \mathbb{C} \setminus \Omega$*. 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 3.1: Das Gitter $\mathbb{Z} + \omega\mathbb{Z}$ 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 meromorphic Funktion mit einer doppelten Polstelle an jedem Punkt auf Ω. Man nennt $\wp_\Omega$ die **Weierstrass-$\wp$ Funktion**.

Lemma 3.4. *Sei $\Omega \subseteq \mathbb{C}$ eine Gitter und $\wp_\Omega$ die Funktion oben. Für alle $z \in \mathbb{C} \setminus \Omega$ erfüllt die Ableitung*

$$\wp'_\Omega(z) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}. \tag{3.2}$$

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 (3.1), 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 (3.2) invariant unter Translation von z um ein Gitterpunkt ist. 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 (3.1) davon überzeugen, dass $\wp_\omega(z) = \wp_\omega(-z)$ gilt, d.h. $\wp_\omega$ ist eine gerade Funktion. Es folgt $c(\omega) = 0$. $\square$

Bemerkung 3.5. *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 $g_2, g_3 \in \mathbb{C}$, so dass

$$g_2^3 - 27g_3^2 \neq 0 \tag{3.3}$$

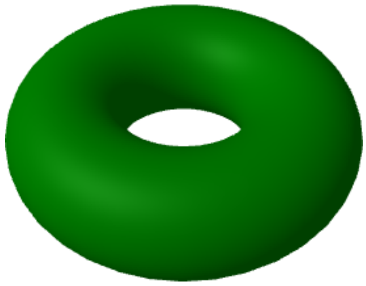
und

$$\wp_\Omega'^{\,2} = 4\wp_\Omega^3 - g_2\wp_\Omega - g_3. \tag{3.4}$$

Bis auf den Faktor 4 liegen die Werte des Paars $(\wp_\Omega, \wp'_\Omega)$ auf einer elliptischen Kurve. Die Bedingung (3.3) entspricht dabei der Bedingung (2.2).
Der Faktor 4 ist harmlos, wir können die gesamten Überlegungen aus Kapitel 2 auf die **modifizierte Weierstrass-Gleichung**

$$Y^2 = 4X^3 - g_2X - g_3 \quad \text{wobei} \quad g_2^3 - 27g_3^2 \neq 0 \tag{3.5}$$

Abbildung 3.2: Ein Torus



anwenden und ein Gruppengesetzt 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 Gruppenhomomorphism, 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 2.4 die Struktur eines topologischen Raums. Aus topologischer Sicht sind $\mathbb{C}/\Omega$ und $E(\mathbb{C})$ ununterscheidbar.

Bemerkung 3.6. *Aus topologischer Sicht ist $\mathbb{C}/\Omega$ nichts anderes als ein Torus, vgl. Abbildung 3.2. 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 für die Topologie "unsichtbar", aber nicht für die komplexe Geometrie.*

Eine modifizierte Weierstrass-Gleichung (3.5) legt ein Gitter $\Omega \subseteq \mathbb{C}$ fest, für welches (3.4) gilt. Die "Perioden" in Ω lassen sich durch Integrale

$$\int \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

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!

4 Anwendungen

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

- Der Diffie-Hellman Schlüsselaustausch mit elliptischen Kurven
- Lenstras (statistisches) Faktorisierungsverfahrung 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.

4.1 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 also ungestört, d.h. verschlüssel miteinander kommunizieren. Bei 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 rationalen Punkt $P \in E(\mathbb{F}_p) \smallsetminus \{\mathcal{O}\}$. Die Sicherheit wird gewährleistet, wenn p "gross" ist und wenn die Ordnung of P als Element der abelschen Gruppe auch eine grosse Primzahl. [1] Die gesamte Information (p, E, P) ist an dieser

[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.

Stelle rein öffentlich. A und B müssen davon ausgehen, dass dritte Zugriff auf diese Information haben.

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

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

Diese Berechnung lässt sich wie folgt effizient gesalten. Ist die Entwicklung von a zur Basis 2 durch $\sum_i a_i 2^i$ mit $a_i \in \{0, 1\}$, 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.

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 anhin wurde noch keine Information zwischen A und B ausgetausch (bis auf die Wahl von (p, E, P).) In Schritt 4 schickt A den Punkt $a \cdot P$ and B und B schickt $b \cdot P$ an A. Der Informationsaustausch geschieht auf dem öffentlichen und unsicheren Kanal.

Schritt 5. Zu diesem Zeitpunkt besitzt A die Information a und $b \cdot P$. 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

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

Das gemeinsame Geheimnis ist der Punkt $(ab) \cdot P$. Diese 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 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 $(\log p)^C$ Rechenschritt für eine Konstante C.
Im Jahr 1994 hat Peter Shor einen "Quantum-Algorithmus" entwickelt, welcher den Diffie-Hellman Schlüsselaustausch unsicher macht, sobald man einen hinreichend mächtigen Quantumcomputer bauen kann. Kurzum, die zukunftige Bedeutung des Diffie-Hellman Schlüsselaustausches ist offen.

4.2 Lenstras Verfahren

Literaturverzeichnis

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

01d5cdef9233c1080ef09ea6b81fba598a0ff11b