Bachelorarbeit

Weil-Paarung und Kryptographie

vorgelegt von

Stefan Hackenberg

am

Institut für Mathematik

der

Universität Augsburg

betreut durch

Prof. Dr. Marco Hien

abgegeben am

7. November 2012

Einleitung

Wir müssen ungefähr ins zweite Jahrhundert nach Christus zurück gehen, um die Ursprünge *elliptischer Kurven* festmachen zu können: Nach Alexandrien, zu dem wohl bedeutendsten Algebraiker der Antike: Diophant. Er hat unter anderem kubische Gleichungen untersucht und zu Tage gebracht, dass man, falls zwei Lösungen bekannt sind, eine dritte „produzieren“ kann, indem er eine Gerade durch die beiden bekannten Lösungen legte und herausfand, dass es dann meistens einen dritten Schnittpunkt gibt. Doch erst hunderte von Jahren später entdeckte man, dass sich durch leichte Veränderung an diesem Verfahren eine abelsche Gruppenstruktur offenbart, was wir im Detail in Abschnitt 3.2 besprechen werden (Einen ausführlicheren Artikel über die Geschichte von elliptischen Kurven findet man in [**?**]). Mit einer immer digitaler werdenden Welt haben insbesondere Miller [**?**] und Koblitz [**?**] mitte der 1980er Jahre vorgeschlagen, elliptische Kurven in der Kryptographie einzusetzen, da sie im Allgemeinen sicherer sind als z.B. Verschlüsselungen über endlichen Körpern $\mathbb{F}_q$, in denen Verfahren (Abschnitt 8.2) mit „guter“ Laufzeit, d.h. subexponentiell, existieren. Einen gewissen Höhepunkt hat die Bedeutung elliptischer Kurven in den 90er Jahren erlebt, als sie eine zentrale Rolle im Beweis vom großen Fermatschen Satz (engl. Fermat's last theorem) 1995 durch Andrew Wiles und Richard Taylor spielte. Darauf soll in dieser Arbeit jedoch nicht eingegangen werden.

Diese Arbeit ist gegliedert in zwei große Teile. Zunächst wollen wir uns durch einen eher theoretischen Teil arbeiten und den Begriff *elliptische Kurve* im Sinne der algebraischen Geometrie als *nichstsinguläre projektive Varietät von Geschlecht eins* kennen lernen. Anschließend werden wir – nahezu unabhängig vom ersten Abschnitt – das Konzept der *Divisoren* einführen, welche eine elegante Möglichkeit bieten werden, die oben erwähnte Gruppenstruktur auf elliptischen Kurven zu beweisen (Abschnitt 3.2.1).

Die Kernidee der Arbeit wird in Kapitel 4 vorgestellt, wo wir die *Weil-Paarung* kennen lernen werden, eine Abbildung, welche gewisse Punkte auf elliptischen Kurven auf Einheitswurzeln des Grundkörpers schickt. Diese Paarung wird auch des Pudels Kern des *MOV-Angriffes* (nach **?**) in Kapitel 9 sein, mit dem wir uns zuletzt beschäftigen wollen. Sie lässt sich auf zwei verschiedene Wege konstruieren, welche ich *beide* vorstellen möchte. Wir werden im zweiten Teil zwar nur die Variante von Miller [**?**] brauchen, jedoch findet sich in vielen Büchern die erste wieder. Daher war es meine Intention, an dieser Stelle besonders ausführlich zu sein und auch einen Beweis zu geben, dass beide Varianten miteinander verträglich sind.

Den letzten Abschnitt des ersten Teils (Kapitel 5) möge ein kurzer Überblick über elliptische Kurven über endlichen Körpern bilden, wobei wir insbesondere auf den *Schoof-Algorithmus* eingehen wollen, welcher in polynomialer Zeit in der Lage ist, die Kardinalität der oben erwähnten abelschen Gruppe einer elliptischen Kurve zu berechnen.

Sicherlich könnte man an diesem Punkt – vielleicht mehr als an allen anderen – ansetzen und einen anderen Weg wählen, z.B. genauer auf Schoofs Algorithmus eingehen oder eine bessere Variante besprechen, den sog. *SEA-Algorithmus* (nach Schoof, Elkies und Atkin). Man hätte sich auch genauer mit dem Satz von Hasse (Proposition 5.2) auseinander setzen und das Legendre-Symbol

einführen können. Ich habe in diesem Abschnitt jedoch bewusst auf Ausschweifungen verzichtet. Er soll lediglich dazu dienen, gewissen Aufschluss über die Struktur der additiven Gruppe einer elliptischer Kurve über einem endlichen Körper zu geben und zu erkennen, dass es möglich ist, in polynomialer Zeit die Kardinalität dieser Gruppe zu berechnen.

Den zweiten Teil bilden Anwendungen von elliptischen Kurven in der Kryptographie und die Vorstellung verschiedener Probleme, auf deren „Schwierigkeit“ die Sicherheit der kryptographischen Verfahren liegt. Hier gilt es, das ECDLP (*Elliptic Curve Discrete Logarithm Problem*) und das DLP (*Discrete Logarithm Problem*) zu nennen. Beide beschreiben das Problem, in einer beliebigen Gruppe (oder eben auf einer elliptischen Kurve) den *diskreten Logarithmus* zu berechnen. Daran anknüpfend werden wir einen kleinen Ausflug machen und auf das Vorgehen beim Verschlüsseln und Entschlüsseln einer „Nachricht“ eingehen. Es soll dabei das *ElGamal Public Key Kryptosystem* vorgestellt werden. In dieser Arbeit wird sich eine „Nachricht“ stets auf einen Punkt auf einer elliptischen Kurve beschränken. Man kann beispielsweise in [**?** , Abschnitt 5.6] nachlesen, wie man normalen Text in Punkte auf einer elliptischen Kurve verwandelt.

Dieses Wissen im Hinterkopf behaltend wollen wir in Kapitel 8 einen Algorithmus kennen lernen, welcher das DLP und damit das ECDLP lösen kann: *Pollards ρ-Algorithmus*. Leider haben alle bisher bekannten Algorithmen zur Lösung des ECDLP exponentielle Laufzeit. Der zweite Algorithmus, der in diesem Kapitel vorgestellt werden soll, löst lediglich das DLP über einem endlichen Körper $\mathbb{F}_q$. Er ist jedoch ungleich schneller und hört auf den Namen *Index-Calculus Methode*.

Im letzten Kapitel widmen wir uns dem bereits oben erwähnten MOV-Angriff. Dieser reduziert das ECDLP polynomial auf ein DLP über einem endlichen Körper. In der Regel ist dieser endliche Körper aber viel größer, was das entstehende DLP nicht leichter macht, als das ursprüngliche ECDLP. Für *supersinguläre* elliptische Kurven jedoch fällt das Problem nur nach $\mathbb{F}_{q^2}$, falls wir die elliptische Kurve über $\mathbb{F}_q$ betrachtet haben. Dort kann man dann mit Algorithmen subexponentieller Laufzeit, wie der oben beschriebenen Index-Calculus Methode, das DLP lösen und so eine Lösung in subexponentieller Laufzeit für das ursprüngliche ECDLP erhalten.

Inhaltsverzeichnis

Teil I

Elliptische Kurven – Theoretische Resultate

1 Grundlegendes über affine und projektive Varietäten

Wir treffen in der gesamten Arbeit die folgenden Konventionen:

K sei ein Körper und

$\overline{K}$ ein fest gewählter algebraischer Abschluss von K.

Definieren wir nun anfangs einige Begrifflichkeiten, wobei wir uns an [**?** , Chapter I] orientieren wollen.

1.1 Über affine Varietäten

Definition 1.1 (Affiner Raum)**.** Der n-dimensionale *affine Raum* über K für $n \in \mathbb{N}$ wird definiert durch

$$\mathbb{A}^n \;:=\; \mathbb{A}^n(\overline{K}) \;:=\; \{(x_1, \ldots, x_n) :\; x_i \in \overline{K}\}\,.$$

Seine *K-rationalen* Punkte sind gegeben durch

$$\mathbb{A}^n(K) \;:=\; \{(x_1, \ldots, x_n) :\; x_i \in K\}\,.$$

Definition 1.2 (Affine algebraische Menge, Ideal von V)**.** Eine *affine algebraische Menge* V_I ist eine Menge der Form

$$V_I \;:=\; \{P \in \mathbb{A}^n :\; f(P) = 0 \;\forall f \in I\}\,,$$

wobei $I \subset \overline{K}[X_1, \ldots, X_n]$ ein Ideal ist. Für $\overline{K}[X_1, \ldots, X_n]$ werden wir oft auch nur $\overline{K}[X]$ schreiben.

Jeder affinen algebraischen Menge V ordnen wir das *Ideal von V* zu:

$$I(V) \;:=\; \{f \in \overline{K}[X_1, \ldots, X_n] :\; f(P) = 0 \,\forall P \in V\}\,,$$

Wir nennen V definiert über K, geschrieben V/K, falls $I(V)$ nur durch Polynome aus $K[X_1, \ldots, X_n]$ erzeugt werden kann.

Definition 1.3 (Affine Varietät)**.** Eine affine algebraische Menge V wird als *affine Varietät* bezeichnet, falls $I(V)$ ein Primideal in $\overline{K}[X_1, \ldots, X_n]$ ist.

Definition 1.4 (Affiner Koordinatenring von V, Funktionenkörper von V)**.** Sei V eine affine Varietät. Der *affine Koordinatenring von V* ist definiert durch

$$\overline{K}[V] \;:=\; \overline{K}[X_1,\ldots,X_n]/I(V)\,.$$

Da $I(V)$ Primideal ist, ist $\overline{K}[V]$ ein Integritätsbereich und wir können seinen Quotientenkörper betrachten. Dieser heiße *Funktionenkörper von V*, geschrieben $\overline{K}(V)$.
Analog definieren wir selbiges, falls V über K definiert ist. Also

$$K[V] \;:=\; K[X_1,\ldots,X_n]/I(V/K)$$

und $K(V)$ als Quotientenkörper von $K[V]$.

Definition 1.5 (Dimension von V)**.** Die *Dimension* einer affinen Varietät V, geschrieben $\dim V$, ist der Grad der transzendenten Körpererweiterung $\overline{K}(V)$ über $\overline{K}$.

Definition 1.6 (Lokales Ideal)**.** Sei V eine affine Varietät. Für $P \in V$ definieren wir das *lokale Ideal von P*

$$\mathfrak{m}_P \;:=\; \{f \in \overline{K}[V] :\; f(P) = 0\}\,.$$

Definition 1.7 (Lokaler Ring)**.** Sei V eine affine Varietät und $P \in V$. Der *lokale Ring* von V an P ist gegeben durch die Lokalisierung von $\overline{K}[V]$ an $\mathfrak{m}_P$:

$$\overline{K}[V]_P \;:=\; \left\{F \in \overline{K}(V) :\; F = \tfrac{f}{g} \text{ mit } f,g \in \overline{K}[V],\; g(P) \neq 0\right\}\,.$$

Definition 1.8 (Nichtsingulär/Glatt)**.** Sei V eine affine Varität und $f_1,\ldots,f_m \in \overline{K}[X_1,\ldots,X_n]$ Erzeuger von $I(V)$. Dann heißt V *nichtsingulär* oder *glatt in P*, falls die $m \times n$-Matrix der formalen Ableitungen

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$$

von Rang $n - \dim V$ ist.
Ist V in jedem Punkt nichtsingulär, so nennen wir V *nichtsingulär* oder *glatt*.

1.2 Über projektive Varietäten

Definition 1.9 (Projektiver Raum)**.** Der n-dimensionale *projektive* Raum über K für $n \in \mathbb{N}$ ist definiert durch

$$\mathbb{P}^n \;:=\; \mathbb{P}^n(\overline{K}) \;:=\; \{(x_0,\ldots,x_n) \in \mathbb{A}^{n+1}\}/\sim\,,$$

wobei $\sim$ folgende Äquivalenzrelation beschreibt:

$$(x_0,\ldots,x_n) \sim (x_0',\ldots,x_n') \;\Leftrightarrow\; \exists i \in \{0,\ldots,n\} :\; x_i \neq 0 \;:\wedge\; \exists \lambda \in \overline{K}^* :\; x_i = \lambda x_i' \;\forall i \in \{0,\ldots,n\}\,.$$

Für eine Äquivalenzklasse

$$\{(\lambda x_0,\ldots,\lambda x_n) :\; \lambda \in \overline{K}^*\}$$

schreiben wir $[x_0,\ldots,x_n]$ und bezeichnen die x_is als *homogene Koordinaten*.

Die Menge der *K-rationalen Punkte von $\mathbb{P}^n$* ist definiert durch

$$\mathbb{P}^n(K) \;:=\; \{[x_0,\ldots,x_n] \in \mathbb{P}^n :\; x_i \in K\;\forall i\}\,.$$

Definition 1.10 (Homogenes Polynom)**.** Ein Polynom $f \in \overline{K}[X] := \overline{K}[X_0, \ldots, X_n]$ heißt *homogen von Grad d*, falls gilt

$$f(\lambda X_0, \ldots, \lambda X_n) \;=\; \lambda^d f(X_0, \ldots, X_n) \quad \forall \lambda \in \overline{K}\,.$$

Ein Ideal $I \in \overline{K}[X]$ heißt *homogen*, falls es von homogenen Polynomen erzeugt wird.

Definition 1.11 (Projektive Algebraische Menge, Homogenes Ideal von V, Menge der K-rationalen Punkte)**.** Eine *projektive algebraische Menge* V_I ist eine Menge der Form

$$V_I \;:=\; \{P \in \mathbb{P}^n :\; f(P) = 0 \;\forall f \in I, f \text{ homogen}\}\,,$$

wobei $I \subset \overline{K}[X]$ ein homogenes Ideal ist.

Jeder projektiven algebraischen Menge V ordnen wir das *(homogene) Ideal von V* zu:

$$I(V) \;:=\; \{f \in \overline{K}[X] :\; f \text{ homogen } \wedge\; f(P) = 0 \forall P \in V\}\,,$$

Wir nennen V *definiert über* K, geschrieben V/K, falls $I(V)$ nur von Polynomen aus $K[X]$ erzeugt werden kann.

Ist V definiert über K, so ist die *Menge der K-rationalen Punkte von V* gegeben durch

$$V(K) \;:=\; V \cap \mathbb{P}^n(K)\,.$$

Definition 1.12 (Projektive Varietät)**.** Eine projektive algebraische Menge wird als *projektive Varietät* bezeichnet, falls $I(V)$ ein Primideal in $\overline{K}[X]$ ist.

Da wir gewöhnt sind, mit affinen Koordinaten umzugehen, wollen wir den affinen mit dem projektiven Raum in Verbindungen bringen.

Es ist klar, dass wir für $i \in \{1, \ldots, n\}$ folgende Inklusionen angeben können:

$$\phi_i :\; \mathbb{A}^n \to \mathbb{P}^n, \quad (x_1, \ldots, x_n) \mapsto [x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n]\,.$$

Wir erhalten daraus sogar Bijektionen, falls aus $\mathbb{P}^n$ jeweils eine Hyperebene entfernt wird, also

$$\begin{aligned}\phi_i^{-1} :\; \mathbb{P}^n \setminus \{[x_0, \ldots, x_n] \in \mathbb{P}^n :\; x_i = 0\} &\to \mathbb{A}^n,\\ [x_0, \ldots, x_n] &\mapsto \left(\tfrac{x_0}{x_i}, \ldots, \tfrac{x_{i-1}}{x_i}, \tfrac{x_{i+1}}{x_i}, \ldots, \tfrac{x_n}{x_i}\right)\end{aligned}$$

Dies wollen wir auf Polynome und anschließend auf algebraische Mengen übertragen:

Definition 1.13 (Homogenisierung, Dehomogenisierung)**.** Sei $f \in \overline{K}[X_0, \ldots, X_n]$ ein homogenes Polynom. Die *Dehomogenisierung von f respektive* X_i ist das Polynom $f \in \overline{K}[Y_1, \ldots, Y_n]$ definiert durch

$$f(Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n)\,.$$

Sei umgekehrt $f \in \overline{K}[Y_1, \ldots, Y_n]$ ein Polynom, so bezeichne $f^* \in \overline{K}[X_0, \ldots, X_n]$ die *Homogenisierung von f respektive* X_i, definiert durch

$$f^*(X_0, \ldots, X_n) \;:=\; X_i^d f\left(\tfrac{X_0}{X_i}, \ldots, \tfrac{X_{i-1}}{X_i}, \tfrac{X_{i+1}}{X_i}, \ldots, \tfrac{X_n}{X_i}\right)\,,$$

wobei $d = \deg f$ die kleinste natürliche Zahl ist, sodass f^* ein Polynom wird. Bemerke dabei, dass f^* ein homogenes Polynom ist.

Definition 1.14 (Projektiver Abschluss von V)**.** Sei $V \in \mathbb{A}^n$ eine affine algebraische Menge mit Ideal $I(V)$. Wählen wir ein i fest, so können wir V via ϕ_i als Teilmenge von $\mathbb{P}^n$ auffassen und den *projektiven Abschluss von* V, geschrieben $\overline{V}$, als projektive algebraische Menge definieren, deren homogenes Ideal erzeugt wird von den homogenisierten Polynomen in $I(V)$, also von

$$\{f^*(X) : \ f \in I(V)\}\,.$$

Man kann dann folgende Proposition ([**?** , Proposition I.2.6]) beweisen. Eine Referenz zu einem Beweis findet sich ebenfalls dort.

Proposition 1.15. *(1) Sei V eine affine Varietät. Dann ist $\overline{V}$ eine projektive Varietät und*

$$V \ = \ \overline{V} \cap \mathbb{A}^n\,.$$

(2) Sei V eine projektive Varietät. Dann ist $V \cap \mathbb{A}^n$ eine affine Varietät und es gilt entweder

$$V \cap \mathbb{A}^n \ = \ \emptyset \quad \textit{oder} \quad V \ = \ \overline{V \cap \mathbb{A}^n}\,.$$

(3) Ist eine affine (projektive) Varietät V definiert über K, so ist $\overline{V}$ ($V \cap \mathbb{A}^n$) ebenfalls definiert über K.

Beispiel 1.16. Mit obiger Proposition können wir uns also weitgehend auf affine Koordinaten beschränken. Wählen wir einmal $K = \mathbb{Q}$ und betrachten beispielsweise die projektive Varietät

$$V : \ Y^2 + XY \ = \ X^3 + 13\,. \tag{1.1}$$

In der Tat ist dies keine Varietät in Notation von Definitionen 1.11 und 1.12! Wir meinen damit die Varietät, welche durch das Ideal geben ist, welches von

$$f(\bar{X}, \bar{Y}, \bar{Z}) \ = \ \bar{Z}\bar{Y}^2 + \bar{Z}\bar{X}\bar{Y} - \bar{X}^3 - 13\bar{Z}$$

erzeugt wird. Gleichung (1.1) ist also die Dehomogenisierung respektive $\bar{Z}$ von

$$\bar{Z}\bar{Y}^2 + \bar{Z}\bar{X}\bar{Y} \ = \ \bar{X}^3 + 13\bar{Z}^3\,. \tag{1.2}$$

Welche Punkte haben wir außerhalb der affinen Ebene? Setzen wir in Gleichung (1.2) einmal $\bar{Z} = 0$ ein, so sehen wir, dass $\bar{X} = 0$ und $\bar{Y}$ beliebig folgt. Ergo liegt für $y \neq 0$ gerade $[0, y, 0] = [0, 1, 0] \in V$ (man beachte $[0, 0, 0] \notin \mathbb{P}^2$) und wir folgern, dass

$$V(\mathbb{Q}) \ = \ \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : \ f(x, y, 1) = 0\} \cup \{[0, 1, 0]\}\,.$$

Wir werden alle Punkte, die nicht im affinen Teil liegen, als *Punkte im Unendlichen* bezeichnen.

Definition 1.17 (Dimension von V)**.** Sei V/K eine projektive Varietät und wähle $\mathbb{A}^n \subset \mathbb{P}^n$ so, dass $V \cap \mathbb{A}^n \neq \emptyset$. Die *Dimension von* V ist die Dimension von $V \cap \mathbb{A}^n$ als affine Varietät.

Definition 1.18 (Kurve)**.** Wir nennen eine projektive Varietät der Dimension 1 eine *Kurve*.

Bemerkung 1.19. Wir wollen auch die Begriffe *lokales Ideal*, *lokaler Ring* und *nichtsingulär* (Definitionen 1.6 bis 1.8) auf projektive Varietäten übertragen, indem wir analog zu Definition 1.17 den Schnitt mit $\mathbb{A}^n$ betrachten.

Definition 1.20. Sei V eine projektive Varietät. Für $P \in V$ wähle $\mathbb{A}^n \subset \mathbb{P}^n$, sodass $P \in \mathbb{A}^n \cap V$. Wir definieren das *lokale Ideal von* P als lokales Ideal von $V \cap \mathbb{A}^n$, den *lokalen Ring* als lokalen Ring von $V \cap \mathbb{A}^n$ und V heiße *glatt* in P, falls $V \cap \mathbb{A}^n$ glatt in P ist.

2 Divisoren

Da *Divisoren* in dieser Arbeit eine zentrale Rolle spielen werden, wollen wir besonders auf sie eingehen. In diesem Kapitel werden wir uns an [**?** , Section II.3] orientieren.

2.1 Grundlegendes

Zunächst jedoch ein paar Vorbereitungen, die wir nur zitieren möchten.

Proposition 2.1. *Sei C eine Kurve und $P \in C$ ein glatter Punkt. Dann ist $\overline{K}[C]_P$ ein diskreter Bewertungsring.*

Beweis. [**?** , Proposition II.1.1]. □

Definition 2.2 (Ordnung einer Funktion in einem Punkt)**.** Sei C eine Kurve und $P \in C$ ein glatter Punkt. Eine *Bewertung auf* $\overline{K}[C]_P$ ist gegeben durch

$$\begin{aligned} \mathrm{ord}_P : \ \overline{K}[C]_P \ &\to \ \mathbb{N} \cup \{\infty\}\,, \\ f \ &\mapsto \ \sup\{d \in \mathbb{Z} : \ f \in {\mathfrak{m}_P}^d\}\,. \end{aligned}$$

Wir können ord_P auf $\overline{K}(C)$ erweitern, indem wir

$$\mathrm{ord}_P\left(\tfrac{f}{g}\right) \ := \ \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$$

setzen.
Wir sagen f hat *in P Ordnung n*, falls $n = \mathrm{ord}_P(f)$. Weiter sagen wir, f hat eine *Nullstelle in P*, falls $\mathrm{ord}_P(f) > 0$ und f hat einen *Pol in P*, falls $\mathrm{ord}_P(f) < 0$.

Beispiel 2.3. Geben wir dazu ein Beispiel. Sei durch

$$E : \ F(X,Y) \ := \ Y^2 - (X - e_1)(X - e_2)(X - e_3) \ = \ 0$$

eine Kurve in $\mathbb{P}^2$ mit $e_i \in K$ für $i = 1, 2, 3$ gegeben. Wir sehen, dass $P := (e_1, 0) \in E$.
Betrachten wir nun die Funktion

$$f(X,Y) = X - e_1 \in \overline{K}[E]_P\,.$$

Wir wollen nun die Ordnung von f in P bestimmen. Dazu überlegen wir, dass $\mathfrak{m}_P$ gerade von $X - e_1$ und Y erzeugt wird, also

$$\mathfrak{m}_P \ = \ (X - e_1, Y)/(F)\,.$$

Trivialerweise haben wir also $f \in \mathfrak{m}_P$.
Betrachten wir

$$\mathfrak{m}_P^2 \ = \ ((X - e_1)^2, \ (X - e_1)Y, \ Y^2)/(F)\,,$$

so können wir auf den ersten Blick nicht erkennen, ob $f \in \mathfrak{m}_P^2$. Dazu schreiben wir f um, zu

$$f(X,Y) \;=\; X - e_1 \;=\; \frac{Y^2}{(X-e_2)(X-e_3)} \;=:\; \frac{f_1(X,Y)}{f_2(X,Y)} \in \overline{K}[E]_P\,.$$

Es lässt sich jetzt schon sehen, dass wohl $\mathrm{ord}_P(f) = 2$. Dies wollen wir verifizieren: Wir müssen, da $\mathrm{ord}_P(f) = \mathrm{ord}_P(f_1) - \mathrm{ord}_P(f_2)$, die Ordnungen von f_1 und f_2 bestimmen.
Hier können wir sofort folgern, dass $f_1 = Y^2 \in \mathfrak{m}_P^2$, aber $f_1 \notin \mathfrak{m}_P^3$, da

$$\mathfrak{m}_P^3 \;=\; ((X-e_1)^3,\ (X-e_1)^2 Y,\ (X-e_1)Y^2,\ Y^3)/(F)$$

und sich durch F kein Erzeuger passend umschreiben lässt. Für f_2 scheitern wir bereits bei $\mathfrak{m}_P^1$: Da $f_2(P) \neq 0$, folgt sofort $f_2 \notin \mathfrak{m}_P$. Wir fassen damit zusammen:

$$\mathrm{ord}_P(f) \;=\; \mathrm{ord}_P(f_1) - \mathrm{ord}_P(f_2) \;=\; 2 - 0 \;=\; 2\,.$$

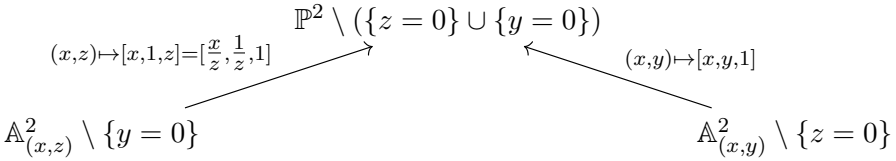
Man sieht sicherlich ein, dass für alle anderen affinen Punkte $P \neq Q \in E$ folgt, dass $\mathrm{ord}_Q(f) = 0$. Doch wie sieht es mit dem Punkt $P_\infty = [0,1,0] \in E$ aus? Betrachten wir einmal die homogenisierte Variante

$$E:\ \bar{Y}^2\bar{Z} - (\bar{X} - e_1\bar{Z})(\bar{X} - e_2\bar{Z})(\bar{X} - e_3\bar{Z}) \;=\; 0$$

und dehomogenisieren respektive $\bar{Y}$, so erhalten wir

$$E_y:\ G(X,Z) \;:=\; Z - (X - e_1Z)(X - e_2Z)(X - e_3Z) \;=\; 0\,,$$

wobei P_∞ nun die Koordinaten $(0,0)$ hat. Das bedeutet, wir arbeiten nun in $\mathbb{A}^2_{(x,z)} \cong \mathbb{P}^2 \setminus \{y=0\}$. Um nun den Koordinatenwechsel richtig zu vollziehen, betrachten wir einmal folgendes Diagramm:



Das bedeutet, ein Punkt $(p_1,p_2) \in E \cap \mathbb{A}^2_{(x,z)}$ mit $p_2 \neq 0$, fällt gerade auf die Koordinaten $(\frac{p_1}{p_2},\frac{1}{p_2}) \in E \cap \mathbb{A}^2_{(x,y)}$, da im Schnitt $\mathbb{P}^2 \setminus (\{z=0\} \cup \{y=0\})$ ja beides auf den selben Punkt $[p_1,1,p_2] = [\frac{p_1}{p_2},\frac{1}{p_2},1]$ fallen muss. Dieser Wechsel überträgt sich analog auf die Funktionenkörper und $f \in \overline{K}(E \cap \mathbb{A}^2_{(x,y)})$ wird zu

$$g(X,Z) \;=\; f(\tfrac{X}{Z},\tfrac{1}{Z}) \;=\; \frac{X - e_1Z}{Z} \quad \in \overline{K}(E \cap \mathbb{A}^2_{(x,z)})\,.$$

Wir können in $\overline{K}[E_y]$ die Funktion g umschreiben zu

$$g(X,Z) \;=\; \frac{1}{(X-e_2Z)(X-e_3Z)} \;=:\; \frac{1}{g_2(X,Z)}\,.$$

Nun müssen wir die Ordnung von $g_2 \in \overline{K}[E_y]_{(0,0)}$ bestimmen. Es ist analog zu oben

$$\mathfrak{m}_{(0,0)} \;=\; (X,Z)/(G)\,,$$

$$\begin{aligned}\mathfrak{m}_{(0,0)}^2 &= (X^2, XZ, Z^2)/(G)\,,\\ \mathfrak{m}_{(0,0)}^3 &= (X^3, X^2Z, XZ^2, Z^3)/(G)\end{aligned}$$

und man sieht nach Ausmultiplizieren sofort, dass g_2 in $\mathfrak{m}_{(0,0)}$ und $\mathfrak{m}_{(0,0)}^2$, aber nicht mehr in $\mathfrak{m}_{(0,0)}^3$ liegt. Schließlich können wir folgern, dass

$$\operatorname{ord}_{P_\infty}(f) \;=\; \operatorname{ord}_{(0,0)}(g) \;=\; -\operatorname{ord}_{(0,0)}(g_2) \;=\; -2\,.$$

Darüber hinaus wollen wir folgendes Resultat zitieren, welches mehr Klarheit über die Anzahl von Null- und Polstellen gibt.

Proposition 2.4. *Sei C eine glatte Kurve und $f \in \overline{K}(C)^*$.*

(1) f hat nur endlich viele Null- und Polstellen.

(2) Hat f keine Polstellen, so ist $f \in \overline{K}^*$.

(3) Hat f keine Nullstellen, so ist $f \in \overline{K}^*$.

Beweis. [**?** , Proposition II.1.2]. □

Definition/Lemma 2.5. Ein *Divisor* auf einer Kurve C ist eine formale Summe

$$D \;:=\; \sum_{P\in C} n_P[P]\,,$$

wobei $n_P \in \mathbb{Z}$ und $n_P \neq 0$ für nur endlich viele P.
Die *Gruppe der Divisoren über C* $\operatorname{Div}(C)$ ist eine freie abelsche Gruppe, die von den Punkten von C erzeugt wird.
Der *Grad eines Divisors D* ist definiert durch

$$\deg(D) \;:=\; \sum_{P\in C} n_P\,.$$

Die Divisoren von Grad 0 bilden eine Untergruppe in $\operatorname{Div}(C)$ und seien zusammengefasst in

$$\operatorname{Div}^0(C) \;:=\; \{D \text{ Divisor } \mid \deg D = 0\}\,.$$

Der *Träger eines Divisors D* ist definiert durch

$$\operatorname{supp}(D) \;:=\; \{P \in C \mid n_P \neq 0\}\,.$$

Ist C eine nichtsinguläre Kurve, so können wir für $f \in \overline{K}(C)^*$ den *Divisor von f* definieren:

$$\operatorname{div}(f) \;:=\; \sum_{P\in C} \operatorname{ord}_P(f)\;[P]\,.$$

Formale Summen dieser Form sind nach Proposition 2.4 (a) Divisoren.
Gibt es für einen gegebenen Divisor D eine Funktion f mit $D = \operatorname{div}(f)$, so heißt dieser *Hauptdivisor*.
Zwei Divisoren D_1, D_2 heißen *linear äquivalent*, geschrieben $D_1 \sim D_2$, falls $D_1 - D_2$ ein Hauptdivisor ist.
Falls D ein Hauptdivisor ist, führen wir noch die verkürzende Notation $D \sim 0$ ein.
Die lineare Äquivalenz definiert eine Äquivalenzrelation und wir können ferner die *Picard-Gruppe von C* als Divisoren von Grad 0 modulo linearer Äquivalenz angeben:

$$\operatorname{Pic}^0(C) \;:=\; \operatorname{Div}^0(C)/\sim\,.$$

Beweis. Alles sehr leicht zu verifizieren. □

Proposition 2.6. *Sei C eine nichtsinguläre Kurve und $f \in \overline{K}(C)^*$. Dann gilt*

$$\operatorname{div}(f) = 0 \quad \Leftrightarrow \quad f \in \overline{K}^*, \text{ d.h. } f \text{ ist konstant.}$$

Beweis. [**?** , Proposition II.3.1] □

Lemma 2.7. *Seien C eine nichtsinguläre Kurve und $f, g \in \overline{K}(C)^*$ mit $\operatorname{div}(f) = \operatorname{div}(g)$. Dann gilt $f = cg$ für $c \in \overline{K}^*$.*

Beweis. Betrachte $\operatorname{div}(\frac{f}{g}) = \operatorname{div}(f) - \operatorname{div}(g) = 0$. Dann ist nach Proposition 2.6 $\frac{f}{g} \in \overline{K}^*$. □

2.2 Der Satz von Riemann-Roch

Sei im Folgenden stets C eine Kurve.

Definition 2.8 (Positiver Divisor)**.** Wir nennen einen Divisor $D = \sum n_P[P]$ über einer Kurve C *positiv*, geschrieben $D \geq 0$, falls $n_P \geq 0$ für alle $P \in C$. Für zwei Divisoren $D_1, D_2 \in \operatorname{Div}(C)$ schreiben wir $D_1 \geq D_2$, falls $D_1 - D_2 \geq 0$.

Definition 2.9. Sei $D \in \operatorname{Div}(C)$. Wir definieren

$$\mathcal{L}(D) \;:=\; \{f \in \overline{K}(C)^* :\; \operatorname{div}(f) \geq -D\} \cup \{0\}\,.$$

Proposition 2.10. *$\mathcal{L}(D)$ ist ein endlich dimensionaler $\overline{K}$-Vektorraum. Seine Dimension sei bezeichnet mit*

$$\ell(D) \;:=\; \dim_{\overline{K}} \mathcal{L}(D)\,.$$

Beweis. [**?** , II.5.19]. □

Lemma 2.11. *Sei $f \in \overline{K}(C)^*$. Dann gilt*

$$\deg \operatorname{div} f \;=\; 0\,.$$

Beweis. [**?** , Remark II.3.7]. □

Proposition 2.12. *Sei $D \in \operatorname{Div}(C)$ mit $\deg D < 0$. Dann gilt*

$$\mathcal{L}(D) \;=\; \{0\} \quad \textit{und} \quad \ell(D) \;=\; 0\,.$$

Beweis. Sei $f \in \mathcal{L}(D)$ mit $f \neq 0$. Dann gilt nach Lemma 2.11

$$\deg \operatorname{div} f \;=\; 0\,.$$

Per definitionem ist aber $\operatorname{div} f \geq -D$, also auch

$$\deg \operatorname{div} f \;\geq\; \deg(-D) \;=\; -\deg D\,,$$

woraus folgt, dass $\deg D \geq 0$. Für $\deg D < 0$ folgt dann die Behauptung und es ist klar, dass $\mathcal{L}(D) = \{0\}$ auch $\ell(D) = 0$ impliziert. □

Satz 2.13 (Riemann-Roch)**.** *Sei C eine glatte Kurve. Dann existieren ein Divisor K auf C und eine natürliche Zahl $g \geq 0$, genannt* das Geschlecht *der Kurve C, sodass für alle $D \in \mathrm{Div}(C)$ gilt*

$$\ell(D) - \ell(K - D) \;=\; \deg D - g + 1\,.$$

Beweis. Z.B. [**?** , IV §1]. □

Bemerkung 2.14. Eigentlich beinhaltet der Satz von Riemann-Roch nicht die Existenz des Divisors K. K ist als *kanonischer Divisor* auf C zu wählen. Was dies ist und dass solche immer existieren, findet man in [**?** , Section II.5].

Korollar 2.15. *Sei Notation gegeben wie im Satz von Riemann-Roch. Dann gilt:*

(1) $\ell(K) = g$.

(2) $\deg K = 2g - 2$.

(3) Falls $\deg D > 2g - 2$*, gilt*

$$\ell(D) = \deg D - g + 1\,.$$

Beweis. (1) Wähle $D = 0$, so ist nach Riemann-Roch

$$\ell(0) - \ell(K) = 0 - g + 1\,.$$

In Proposition 2.4 (2) haben wir gesehen, dass Funktionen, die keine Pole haben, bereits konstant sind. Also ist

$$\mathcal{L}(0) \;=\; \overline{K}^* \cup \{0\} \;=\; \overline{K}\,.$$

Damit folgt $\ell(0) = 1$ und ergo $\ell(K) = g$.

(2) Wähle $D = K$ mit K aus dem Satz von Riemann-Roch. Ferner benutzen wir (1) und können folgern

$$\ell(K) - \ell(K - K) \;=\; \ell(K) - \ell(0) \;=\; g - 1 \;=\; \deg K - g + 1\,.$$

Also $\deg K = 2g - 2$.

(3) Sei D ein Divisor mit $\deg D > 2g - 2$ und K der Divisor wie oben. Nach Definition des Grades ist klar, dass

$$\deg(K - D) \;=\; \deg(K) - \deg(D) \;<\; 0\,,$$

woraus nach Proposition 2.12 $\ell(K - D) = 0$ folgt. Setzen wir das in Riemann-Roch ein, erhalten wir

$$\ell(D) - \ell(K - D) \;=\; \ell(D) \;=\; \deg D - g + 1\,.$$

□

3 Elliptische Kurven

3.1 Elliptische Kurven und Weierstraß-Gleichungen

Wollen wir nun zum eigentlichen Kern dieser Arbeit kommen und (endlich) definieren, was eine elliptische Kurve ist.

Definition 3.1 (Elliptische Kurve)**.** Eine *elliptische Kurve* ist gegeben durch ein Paar (E, O), wobei E eine nichtsinguläre Kurve vom Geschlecht eins und $O \in E$ ist.
Wir schreiben E/K, falls E über K als Kurve definiert und $O \in E(K)$ ist.

Man kann nun zeigen, dass wir uns elliptische Kurven stets auch als Nullstellengebilde bestimmter Gleichungen vorstellen können. Diese Gleichungen heißen Weierstraß-Gleichungen:

Definition 3.2 (Weierstraß-Gleichung)**.** Eine Gleichung der Form

$$Y^2Z + a_1XYZ + a_3YZ^2 \;=\; X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

mit $a_1, \ldots, a_6 \in \overline{K}$ heißt *(kubische) Weierstraß-Gleichung.*
Wir wollen wiederum nur den affinen Teil betrachten, definieren $x = \frac{X}{Z}$ und $y = \frac{Y}{Z}$ und erhalten die *affine Weierstraß-Gleichung*

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6$$

zusammen mit dem Punkt $[0, 1, 0]$ im Unendlichen.

Proposition 3.3. *Sei E/K eine elliptische Kurve mit Basispunkt O.*

(1) Es existieren Funktionen $x, y \in K(E)$, sodass die Abbildung

$$\phi :\; E \to \mathbb{P}^2, \quad \phi = [x, y, 1]\,,$$

einen Isomorphismus von E/K auf eine Kurve gibt, welche durch die Weierstraß-Gleichung

$$C :\; Y^2 + a_1XY + a_3Y \;=\; X^3 + a_2X^2 + a_4X + a_6$$

geben ist. Dabei gilt $a_1, \ldots, a_6 \in K$ und $\phi(O) = [0, 1, 0]$.

(2) Jede glatte kubische Kurve C, die durch eine Weierstass-Gleichung gegeben ist, definiert eine elliptische Kurve über K mit Basispunkt $O = [0, 1, 0]$.

Beweis. [**?** , Proposition III.3.1 (a), (c)]. □

Lemma 3.4. *Zwei Weierstraß-Gleichungen definieren dieselbe elliptische Kurve, falls sie durch einen Koordinatenwechsel der Form*

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t$$

mit $u \in K^*$ und $r, s, t \in K$ auseinander hervorgehen.

Beweis. [**?** , Proposition III.3.1 (b)]. □

Das bedeutet, wir können uns eine elliptische Kurve E/K immer gegeben durch eine Weierstraß-Gleichung vorstellen. Wir sagen auch, E/K ist in Weierstraßscher Normalform gegeben.

Stellen wir gewisse Anforderungen an den Körper, so können wir die Weierstraß-Gleichung noch weiter vereinfachen.

Lemma 3.5. *Sei E/K eine elliptische Kurve.*

(1) Ist $\operatorname{char} K \neq 2$*, so lässt sich E durch eine Weierstraß-Gleichung der Form*

$$E/K: \; y^2 = 4x^3 + b_2x^2 + b_4x + b_6$$

mit $b_2, b_4, b_6 \in K$ beschreiben.

(2) Ist $\operatorname{char} K \neq 2, 3$*, so lässt sich E durch eine Weierstraß-Gleichung der Form*

$$E/K: \; y^2 = x^3 + Ax + B$$

mit $A, B \in K$ beschreiben.

Beweis. Einfache Substitutionen, sodass die Gleichungen äquivalent bleiben (Lemma 3.4). Ausführlich findet man das z.B. in [**?** , Abschnitt III.1]. □

Bemerkung 3.6. Im Allgemeinen beschränken wir uns darauf, elliptische Kurven in Körpern der Charakteristik ungleich 2,3 zu betrachten, was den arithmetischen Aufwand dank obigem Lemma deutlich vereinfacht. Daher wollen wir beispielsweise die *Diskriminante* nur für elliptische Kurven über Körpern mit $\operatorname{char}(K) \neq 2, 3$ definieren.

Definition 3.7. Seien $E/K: \; y^2 = x^3 + Ax + B$ eine elliptische Kurve und $\operatorname{char}(K) \neq 2, 3$. Dann heißt

$$\Delta := -(4A^3 + 27B^2)$$

Diskriminante der elliptischen Kurve.

Bemerkung 3.8. In der Tat ist die Diskriminante der elliptischen Kurve genau die Diskriminante der kubischen Gleichung auf der rechten Seite. Dies ist auch sinnvoll, da wir stets fordern wollen, dass keine Nullstellen höherer Vielfachheit als 1 auftreten. Dies hängt insbesondere mit der Nichtsingularität der elliptischen Kurve zusammen, was nachfolgend postuliert wird und auch für Charakteristik 2 und 3 richtig ist.

Proposition 3.9. *Sei C eine Kurve gegeben durch eine Weierstraß-Gleichung. C ist genau dann nichtsingulär, falls $\Delta \neq 0$.*

Beweis. [**?** , Proposition III.1.4 (a) (i)]. □

Bemerkung 3.10. Wenn wir also von einer elliptischen Kurve sprechen und eine Weierstraß-Gleichung niederschreiben, so gehen wir immer davon aus, dass ihre Diskriminante $\neq 0$ ist.

3.2 Gruppenstruktur

Elliptische Kurven sind besonders interessante Kurven, da man auf ihnen die Struktur einer abelschen Gruppe wiederfindet, was wir im Folgenden sehen werden. Wir beginnen mit einem Resultat aus der algebraischen Geometrie.

Satz 3.11 (Satz von Bézout). *Seien C, D zwei nicht identische Kurven über $\mathbb{P}^2$. C habe Grad c und D Grad d (Gemeint sei der Grad der homogenen Gleichung, die die Kurve definiert). Dann gilt*

$$\sum_{P \in C \cap D} (C, D)_P \;=\; d \cdot e\,,$$

wobei $(C, D)_P$ die Vielfachheit des Schnittes von C mit D im Punkt P meint.

Beweis. [**?** , Corollary I.7.8]. □

Für uns bedeutet das, eine *Gerade* in $\mathbb{P}^2$, also eine Kurve der Form

$$aX + bY + cZ \;=\; 0\,,$$

wobei a, b, c nicht alle gleich 0 sein dürfen, hat mit einer elliptischen Kurve stets 3 Schnittpunkte (mit Vielfachheit gezählt). Das erlaubt uns, aus zwei bekannten Punkten auf einer elliptischen Kurve einen dritten „neuen“ zu generieren. Wir betrachten wieder alles affin. Also sind Geraden die nicht durch O gehen gegeben durch Gleichungen der Form

$$y \;=\; \lambda x + \nu$$

und Geraden durch O sind Gleichungen der Form

$$x - x_0 \;=\; 0\,.$$

Damit können wir die *geometrische Addition auf elliptischen Kurven* formulieren (vgl. [**?** , Composition Law III.2.1]).

Geometrische Addition auf elliptischen Kurven 3.12. Sei E/K eine elliptische Kurve und $P, Q \in E$. Seien L die Gerade durch P und Q (im Falle $P = Q$ die Tangente) und R der dritte Schnittpunkt von L und E. Weiter sei L' die Gerade durch R und O. Dann enthält der Schnitt von L' mit E genau drei Punkte: R, O und einen dritten Punkt, genannt $P + Q$.

Man erhält daraus die nachstehenden Formeln. Sie sind in jedem Lehrbuch über elliptische Kurven zu finden und hier nach [**?** , Group Law Algorithm III.2.3] notiert.

Additionsformeln 3.13. Sei

$$E:\; y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6$$

eine elliptische Kurve.

(1) Sei $P_0 = (x_0, y_0)$. Dann ist

$$-P_0 \;=\; (x_0, -y_0 - a_1x_0 - a_3)\,.$$

Weiter seinen $P_1 + P_2 = P_3$ mit $P_i = (x_i, y_i) \in E$ für $i = 1, 2, 3$.

(2) Ist $x_1 = x_2$ und $y_1 + y_2 + a_1x_2 + a_3 = 0$, so ist $P_1 + P_2 = O$. Andernfalls definiere λ und ν durch

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Dann ist $y = \lambda x + \nu$ die Gerade durch P_1 und P_2 oder die Tangente an E durch $P_1 = P_2$.

(3) Damit ist

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2\,, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3\,. \end{aligned}$$

3.2.1 Beweis der Gruppenstruktur

Man kann nun mit Hilfe der Formeln, die sich aus dieser geometrischen Idee ergeben, zeigen, dass sich in der Tat dadurch eine Gruppenstruktur auf E definieren lässt. Wir wollen aber einen eleganteren Weg wählen und einen Isomorphismus zwischen der Picard-*Gruppe* $\mathrm{Pic}^0(E)$ und den Punkten auf E herstellen. Dabei halten wir uns an [**?** , Abschnitt III.3].

Lemma 3.14. *Sei C eine Kurve von Geschlecht 1 und $P, Q \in C$. Dann gilt*

$$[P] \sim [Q] \quad \Leftrightarrow \quad P = Q\,.$$

Beweis. „⇐“ Klar.

„⇒“ Sei $[P] \sim [Q]$ mit $f \in \overline{K}(C)^*$, sodass

$$\mathrm{div}(f) = [P] - [Q]\,.$$

Dann ist $\mathrm{div}(f) \geq -[Q]$, also $\mathrm{div}(f) \in \mathcal{L}([Q])$. Da $\deg[Q] = 1 > 0$ können wir aus Korollar 2.15 (3)

$$\dim \mathcal{L}([Q]) = \ell([Q]) = \deg([Q]) - g + 1 = 1 - 1 + 1 = 1$$

folgern. Konstante Funktionen, also solche mit Divisor 0, sind in $\mathcal{L}([Q])$ per definitionem enthalten. Dies sind aber auch die einzigen, da konstante und nicht-konstante Funktionen sicherlich linear unabhängig sind. Damit ist f konstant, also $f \in \overline{K}$, $\mathrm{div}(f) = 0$ und ergo $P = Q$. □

Proposition 3.15. *Sei (E, O) eine elliptische Kurve.*

(1) Sei $D \in \mathrm{Div}^0(E)$. Dann existiert ein eindeutiger Punkt $P \in E$, sodass

$$D \sim [P] - [O]\,.$$

Damit ist die Abbildung

$$\sigma : \mathrm{Div}^0(E) \to E, \qquad D \mapsto P$$

wohldefiniert.

(2) σ *ist surjektiv.*

(3) Seien $D_1, D_2 \in \mathrm{Div}^0(E)$*. Dann gilt*

$$\sigma(D_1) \;=\; \sigma(D_2) \quad \Leftrightarrow \quad D_1 \sim D_2\,.$$

Also können wir eine wohldefinierte Bijektion angeben, die wir auch σ *nennen wollen:*

$$\sigma:\; \mathrm{Pic}^0(E) \;\to\; E\,.$$

(4) Die Umkehrabbildung von σ *ist gegeben durch*

$$\kappa:\; E \;\to\; \mathrm{Pic}^0(E), \qquad P \;\mapsto\; (\textit{Äquivalenzklasse von } [P]-[O])\,.$$

(5) Die Addition von Punkten auf E*, welche durch* σ *induziert wird, ist identisch mit der geometrischen Addition von Punkten auf* E *nach 3.12.*

Beweis. (1) Nach Korollar 2.15 (c) haben wir $\dim \mathcal{L}(D+[O]) = 1$. Sei $f \in \mathcal{L}(D+[O])$ ungleich 0, so ist f eine Basis dieses $\overline{K}$-Vektorraums. Weiter haben wir

$$\mathrm{div}(f) \;\geq\; -D-[O] \quad \text{und} \quad \deg \mathrm{div}\, f \;=\; 0\,,$$

woraus wir folgern können, dass es $P \in E$ gibt, sodass

$$\mathrm{div}(f) \;=\; -D-[O]-[P]\,.$$

Also

$$D \sim [P]-[O]\,.$$

Nehmen wir weiter an, wir hätten $P' \in E$ mit $D \sim [P']-[O]$. So können wir aber folgern

$$[P] \;\sim\; D+[O] \;\sim\; [P']\,,$$

woraus mit Lemma 3.14 $P = P'$ erhalten.

(2) Für $P \in E$ wähle $D = [P]-[O]$. Dann ist $\sigma(D) = P$.

(3) Seien $D_1, D_2 \in \mathrm{Div}^0(E)$ und $P_i = \sigma(D_i)$ für $i = 1, 2$. Damit haben wir

$$D_1 - D_2 \;\sim\; [P_1]-[O]-[P_2]+[O] \;=\; [P_1]-[P_2]\,.$$

Ist also $P_1 = \sigma(D_1) = \sigma(D_2) = P_2$, folgt sofort $D_1 \sim D_2$. Ist umgekehrt $D_1 \sim D_2$, folgt $[P_1] \sim [P_2]$ und wieder mit Lemma 3.14 $P_1 = P_2$.

(4) Nichts zu zeigen.

(5) Sei E eine elliptische Kurve gegeben in Weierstraßscher Normalform und $P, Q \in E$. Wir müssen also zeigen, dass

$$\kappa(P+Q) \;=\; \kappa(P)+\kappa(Q)\,,$$

wobei $P+Q$ wie in der geometrischen Addition 3.12 definiert sein möge.
Geben wir uns dazu die beiden Geraden

$$L:\; f(X,Y,Z) \;=\; \alpha X+\beta Y+\gamma Z \;=\; 0$$

und

$$L' : \ f'(X,Z,Z) \ = \ \alpha' X + \beta' Y + \gamma' Z \ = \ 0$$

in $\mathbb{P}^2$ vor. L soll dabei die Gerade durch P und Q sein, deren dritter Schnittpunkt mit E mit R bezeichnet sein soll, und L' diejenige, welche durch R und O geht. Da die Gerade $Z = 0$ die Kurve E in O mit Vielfachheit 3 schneidet, können wir mit Hilfe der geometrischen Addition folgern, dass

$$\begin{aligned} \operatorname{div}(f/Z) \ &= \ [P] + [Q] + [R] - 3[O]\,, \\ \operatorname{div}(f'/Z) \ &= \ [R] + [R+Q] - 2[O]\,. \end{aligned}$$

Also haben wir

$$0 \ \sim \ \operatorname{div}(f/f') \ = \ [P+Q] - [P] - [Q] + [O]\,,$$

was nichts anderes ist, als

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) \ = \ 0\,.$$

□

3.3 Divisoren auf elliptischen Kurven

Definition 3.16. Sei E/K eine elliptische Kurve und $D = \sum_{P \in E} n_P [P]$ ein Divisor auf ihr. Wir definieren

$$\operatorname{sum}(D) \ := \ \sum_{P \in E} n_P P\,.$$

Proposition 3.17. *Sei D ein Divisor auf einer elliptischen Kurve E. Dann gilt:*

$$\exists f \in \overline{K}(E) \text{ mit } \operatorname{div}(f) = D \quad \Leftrightarrow \quad \deg(D) = 0 \text{ und } \operatorname{sum}(D) = 0\,.$$

Beweis. $\deg(D) = 0$ ist nach Lemma 2.11 eine notwendige Bedingung. Ist also $D = \sum n_P [P] \in \operatorname{Div}^0(E)$, so haben wir

$$D \sim 0 \ \Leftrightarrow \ O = \sigma(D) = \sum_{P \in E} n_P P \ \in E\,,$$

was dem Geforderten entspricht. □

Bevor wir einen kleinen Überblick über Rechenregeln für Divisoren auf elliptischen Kurven angeben, brauchen wir ein Resultat über die Multiplikation von Punkten auf elliptischen Kurven mit ganzen Zahlen.

Proposition 3.18. *Sei E eine elliptische Kurve und $m \in \mathbb{Z}$, $m \neq 0$. Dann ist die Abbildung*

$$\begin{aligned} [m] : \ & E \to E \\ & P \mapsto mP \end{aligned}$$

surjektiv, wobei für $m > 0$

$$mP \ = \ \underbrace{P + \cdots + P}_{m\text{-mal}}$$

und für $m < 0$

$$mP \;=\; (-m)(-P) \;=\; \underbrace{(-P) + \cdots + (-P)}_{(-m)\text{-mal}}$$

gemeint ist.

Beweis. Nach [**?** , Proposition 4.2 (a)] ist $[m]$ nicht konstant und nach [**?** , Theorem 2.22] sind nicht konstante Endomorphismen auf elliptischen Kurven surjektiv. □

Bemerkung 3.19 (Rechenregeln für Divisoren auf elliptischen Kurven). Später werden wir einige kleine „Rechenregeln“ für Hauptdivisoren auf elliptischen Kurven brauchen, die hier kurz erläutert werden. Sei also E eine elliptische Kurve und $f, g \in \overline{K}(E)^*$ gegeben. Weiter seien für $m \in \mathbb{Z}$

$$[m] : E \to E,\; P \mapsto mP$$

die Abbildung „multipliziere mit m“ und für $Q \in E$

$$\tau_Q : E \to E,\; P \mapsto P + Q$$

die Abbildung „addiere Q“. Dann gilt:

(1) Sei $\operatorname{div}(f) = n_1[P_1] + \cdots + n_r[P_r]$, $r \in \mathbb{N}$ und wähle für $i = 1, \ldots, r$ jeweils $P_i' \in E$ mit $mP_i' = P_i$. Die Urbilder existieren nach Proposition 3.18. Dann ist

$$\operatorname{div}(f \circ [m]) = n_1\Big(\sum_{S \in \ker[m]} [S + P_1']\Big) + \cdots + n_r\Big(\sum_{S \in \ker[m]} [S + P_r']\Big)$$

Beweis. Sei $i = 1, \ldots, r$, so ist nach Definition des Divisors $\operatorname{ord}_{P_i} f = n_i$. Damit ist $\operatorname{ord}_Q(f \circ [m]) = n_i$ für alle $Q \in [m]^{-1}(P_i)$. Weiter ist

$$[m]^{-1}(P_i) \;=\; \ker[m] + P_i' \,.$$

Die Inklusion $\supset$ ist dabei klar, aber vielleicht sollte man zu $\subset$ ein Wort sagen: Sei also $Q \in [m]^{-1}(P_i)$. Dann ist $Q \in \ker[m] + P_i'$, denn

$$Q = Q - P_i' + P_i'$$

und $Q - P_i' \in \ker[m]$, wegen

$$m(Q - P_i') = mQ - mP_i' = P_i - P_i = O \,.$$

□

(2) Sei $\operatorname{div}(f) = n_1[P_1] + \cdots + n_r[P_r]$, $r \in \mathbb{N}$, dann ist für $Q \in E$

$$\operatorname{div}(f \circ \tau_Q) \;=\; n_1[P_1 - Q] + \cdots + n_r[P_r - Q] \,.$$

Beweis. Es ist $\operatorname{ord}_{P_i}(f) = n_i$ für alle $i = 1, \ldots, r$ und wegen $(f \circ \tau_Q)(X - Q) = f(X)$ haben wir $\operatorname{ord}_{P_i - Q}(f \circ \tau_Q) = n_i$. □

(3) $\operatorname{div}(f \cdot g) = \operatorname{div}(f) + \operatorname{div}(g)$ und $\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g)$. Insbesondere haben wir für $m \in \mathbb{Z}$:

$$\operatorname{div}(f^m) \;=\; m \operatorname{div}(f)$$

Beweis. Klar, da selbiges für ord_P gilt. □

(4) Sei $0 \neq m \in \mathbb{Z}$. Ist $\mathrm{const} = f^m \in \overline{K}(E)$, so gilt $f = \mathrm{const}$.

Beweis. Wir wenden Proposition 2.6 zweimal und Punkt (1) an:

$$0 \;=\; \mathrm{div}(f^m) \;=\; m\,\mathrm{div}(f) \quad \Rightarrow \quad \mathrm{div}(f) \;=\; 0\,.$$

□

4 Die Weil-Paarung

Zunächst müssen wir zwei kleine Definitionen geben, bevor wir das zentrale Ziel dieses Kapitels formulieren können:

Definition 4.1. Die n-Torsionspunkte (oder n-Teilungspunkte) einer elliptischen Kurve E, sind definiert durch

$$E[n] \;:=\; \{P \in E(\overline{K}) :\; nP = O\}\,.$$

Bemerkung 4.2. Die n-Torsionspunkte sind also gerade der Kern der Abbildung $[n]$.

Definition 4.3. Die n-ten Einheitswurzeln von K seien bezeichnet mit μ_n, also

$$\mu_n \;:=\; \{a \in \overline{K} :\; a^n = 1\}\,.$$

Darüber hinaus werden wir ein Resultat über die Struktur der Torsionspunkte brauchen.

Lemma 4.4. *(1) Gilt* $\operatorname{char} K = 0$ *oder* $\operatorname{char} K \neq 0$ *und* $\operatorname{char} K \nmid n$*, so folgt*

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n\,.$$

Insbesondere ist hier $\#E[n] = n^2$*.*

(2) Ist $\operatorname{char} K = p > 0$ *ist entweder*

$$E[p^e] \;=\; \{O\}$$

oder

$$E[p^e] \;=\; \mathbb{Z}_{p^e}$$

für alle $e \in \mathbb{N}^*$*.*

Beweis. [**?** , Corollar III.6.4 (b,c)]. □

Damit möchten wir für $n \in \mathbb{N}^+$, $\mathrm{ggT}(n, \mathrm{char}(K)) = 1$ eine Abbildung $e_n : E[n] \times E[n] \to \mu_n$ konstruieren, die folgende Eigenschaften erfüllt:

Proposition 4.5 (Eigenschaften der Weil-Paarung)**.** *Sei* E/K *eine elliptische Kurve und* $n \in \mathbb{N}^+$ *mit* $\mathrm{ggT}(n, \mathrm{char}(K)) = 1$*. Seien weiter* $P, Q, R \in E[n]$ *beliebig. Dann existiert eine Abbildung* $e_n : E[n] \times E[n] \to \mu_n$ *mit folgenden Eigenschaften:*

I. ***Linear***

$$\begin{aligned} e_n(P+Q, R) \;&=\; e_n(P, R) + e_n(Q, R), \\ e_n(P, Q+R) \;&=\; e_n(P, Q) + e_n(P, R)\,. \end{aligned}$$

II. ***Alternierend*** $\quad e_n(P, P) = 1.$

III. ***Anti-symmetrisch*** $\quad e_n(P, Q) \;=\; e_n(Q, P)^{-1}.$

IV. ***Nicht entartet in beiden Variablen***

$$e_n(P,S) = 1 \ \forall S \in E[n] \quad \Leftrightarrow \quad P = O$$

und

$$e_n(S,P) = 1 \ \forall S \in E[n] \quad \Leftrightarrow \quad P = O\,.$$

V. ***Galois-invariant*** *Für $\sigma \in \mathrm{Gal}(\overline{K}/K)$ gilt*

$$e_n(P,Q)^\sigma \ = \ e_n(P^\sigma, Q^\sigma)\,.$$

Bevor wir anfangen, diese Abbildung zu konstruieren, wollen wir noch eine weitere Eigenschaft zeigen.

Korollar 4.6. *Seien die Voraussetzungen wie oben gegeben. Dann existieren Punkte $S,T \in E[n]$, sodass $e_n(S,T)$ eine primitive n-te Einheitswurzel ist. Insbesondere ist $\mu_n \subset K^*$, falls $E[n] \subset E(K)$.*

Beweis. Aus Proposition 4.5 wissen wir, dass $\{e_n(S,T) : \ S,T \in E[n]\} \subset \mu_n$. Weiter ist klar, dass diese Menge eine Untergruppe von μ_n bildet, sagen wir μ_d. Damit haben wir

$$1 \ = \ e_n(S,T)^d \ = \ e_n(dS,T) \qquad \forall S,T \in E[n]\,.$$

Eigenschaft IV der Weil-Paarung impliziert nun, dass $dS = O$. Da $S \in E[n]$ beliebig war und wir aus Lemma 4.4 die Struktur von $E[n]$ kennen, folgt sofort $d = n$.

Seien schließlich $E[n] \subset E(K)$, $S,T \in E[n]$ und $\sigma \in \mathrm{Gal}(\overline{K}/K)$, so haben wir $S^\sigma = S$ und $T^\sigma = T$. Damit folgt aber nach Eigenschaft V

$$e_n(S,T)^\sigma \ = \ e_n(S^\sigma, T^\sigma) \ = \ e_n(S,T)$$

und damit liegt $e_n(S,T) \in K^*$. Da $S,T \in E[n]$ beliebig waren, folgt die Behauptung. □

4.1 Konstruktion der Weil-Paarung

Um die Weil-Paarung mit ihren Eigenschaften zu konstruieren, geben wir diese Abbildung explizit an, wobei wir uns an [**?** , Kapitel 3.1] orientieren.

Wir wollen Lemma 4.4 nutzen, also wählen wir im Folgenden $n \in \mathbb{N}_{\geq 2}$ fest und teilerfremd zur Charakteristik des Körpers K.

Lemma 4.7. *Sei $T \in E[n]$ und $D := n[T] - n[O]$. Ferner seien $T' \in E[n^2]$ mit $nT' = T$ und*

$$D' := \sum_{R \in E[n]} ([T' + R] - [R])\,,$$

dann existieren Funktionen f und g auf der elliptischen Kurve mit $\mathrm{div}(f) = D$ und $\mathrm{div}(g) = D'$.

Beweis. **Existenz von T'** Nach Proposition 3.18 ist die Multiplikation mit n surjektiv, insbesondere hat T ein Urbild.

Existenz von f Es ist $\deg(D) = n - n = 0$ und $\operatorname{sum}(D) = nT - nO = O - O = O$ nach Wahl von T. Damit existiert nach Proposition 3.17 gesuchtes f.

Existenz von g Um auch g mit Proposition 3.17 zu erlangen, rechnet man zunächst $\deg(D') = \sum_{R \in E[n]}(1-1) = 0$ und

$$\operatorname{sum} D' = \sum_{R \in E[n]} (T' + R - R) = \sum_{R \in E[n]} T' = n^2 T' = O\,,$$

da nach Lemma 4.4 $\#E[n] = n^2$ und $n^2 T' = nT = O$. □

Um später Wohldefiniertheit garantieren zu können, sollte g nicht von der Wahl des Punktes T' abhängen, was nachstehendes Lemma garantiert.

Lemma 4.8. *g wie oben, hängt nicht von der Wahl von T' ab.*

Beweis. Sei $T'' \in E[n^2]$ mit $nT'' = nT' = T$, so unterscheiden sich T'' und T' gerade um ein $S \in E[n]$. □

Analog zu Bemerkung 3.19 (1) haben wir

$$\operatorname{div}(f \circ n) \;=\; n\left(\sum_{R \in E[n]} [T' + R]\right) - n\left(\sum_{R \in E[n]} [R]\right) \;=\; \operatorname{div}(g^n)\,.$$

Damit ist $f \circ n$ nach Lemma 2.7 ein konstantes Vielfaches von g und nach Multiplikation mit geeigneten Konstanten können wir annehmen

$$f \circ n \;=\; g^n\,.$$

Sei nun $S \in E[n]$ und $P \in E(\overline{K})$, so gilt

$$g^n(P+S) = (f \circ n)(P+S) = f(n(P+S)) = f(nP + O) = g^n(P) \tag{4.1}$$

und es folgt, dass

$$\frac{g(P+S)}{g(P)} \;\in\; \mu_n\,.$$

Damit können wir nun die Weil-Paarung definieren:

Definition 4.9 (Weil-Paarung)**.** Seien $T \in E[n]$ und g wie oben definiert, so ist die *Weil-Paarung* eine Abbildung

$$\begin{aligned} e_n : \quad E[n] \times E[n] &\to \mu_n \\ (S,T) &\mapsto \frac{g(P+S)}{g(P)}\,, \end{aligned}$$

wobei $P \in E(\overline{K})$ beliebig ist.

Proposition 4.10. *Die Weil-Paarung ist wohldefiniert.*

Beweis. Da wir P als beliebigen Punkt aus $E(\overline{K})$ gewählt haben, gilt es zu zeigen, dass diese Wahl auch beliebig ist. Betrachte dazu die Translationsabbildung mit S, d.h.

$$\tau_S : E(\overline{K}) \to E(\overline{K}),\ P \mapsto P + S\,.$$

Dann ist

$$(g \circ \tau_S)^n(P) \;=\; g^n(P+S) \;\overset{\text{Gleichung (4.1)}}{=}\; g^n(P)$$

und folglich $\operatorname{div}((g \circ \tau_S)^n) = \operatorname{div}(g^n)$, also $\operatorname{div}(g \circ \tau_S) = \operatorname{div}(g)$. Schlussendlich ist damit

$$\operatorname{div}\left(\frac{g \circ \tau_S}{g}\right) = 0$$

und mit Proposition 2.6 folgt, dass $\frac{g \circ \tau_S}{g}(P)$ konstant als Funktion in P ist. □

4.2 Alternative Definition und Konstruktion der Weil-Paarung

Wie wir aber später sehen werden, ist es vom algorithmischen Standpunkt her sinnvoller, die Weil-Paarung auf anderem Wege zu definieren. Dazu gehen wir wie folgt vor (vergleiche [**?**]):

Definition 4.11. Seien C eine Kurve, $f \in K(C)$ und $D = \sum_{P \in C} n_P[P]$ ein Divisor auf C mit $\operatorname{supp}(D) \cap \operatorname{supp}(\operatorname{div}(f)) = \emptyset$, so können wir definieren:

$$f(D) \;:=\; \prod_{P \in C} f(P)^{n_P}$$

Bemerkung 4.12. Betrachten wir beispielsweise $E : Y^2 = (X - e_1)(X - e_2)(X - e_3)$, $e_i \in K$ und $f = X - e_1$, so wissen wir aus Beispiel 2.3, dass $\operatorname{div}(f) = 2[(e_1, 0)] - 2[O]$. Wählen wir dann $D := [(e_1, 0)] + [(e_2, 0)]$, so ist die Voraussetzung der disjunkten Träger in Definition 4.11 verletzt. Setzen wir den Divisor dennoch in die Funktion ein, sehen wir, warum diese Voraussetzung Sinn macht:

$$f(D) \;=\; f((e_1, 0))^1 \cdot f((e_2, 0))^1 \;=\; 0\,.$$

D.h. für $\operatorname{supp}(D) \cap \operatorname{supp}(\operatorname{div}(f)) \neq \emptyset$ folgte stets $f(D) = 0$ oder $= \infty$.

Definition 4.13 (Weil-Paarung durch Divisoren)**.** Seien $n > 1$, E/K eine elliptische Kurve und D_1, D_2 zwei Divisoren auf ihr mit disjunkten Trägern. Gelte außerdem $nD_i \sim 0$. Dann gibt es nach Proposition 3.17 Funktionen f_i mit $\operatorname{div}(f_i) = nD_i$ für $i = 1, 2$. Definiere die *Weil-Paarung* durch:

$$e_n(D_1, D_2) \;:=\; \frac{f_1(D_2)}{f_2(D_1)}\,.$$

Um die Wohldefiniertheit dieser Konstruktion zu zeigen, benötigen wir noch eine weitere Aussage:

Proposition 4.14 (Weil-Reziprozität)**.** *Sei C eine Kurve und $f, g \in K(C)$ mit $f, g \neq 0$ und $\operatorname{supp}(f) \cap \operatorname{supp}(g) = \emptyset$. Dann gilt:*

$$f(\operatorname{div}(g)) \;=\; g(\operatorname{div}(f))\,.$$

Beweis. [**?** , Excercise 2.11] □

Proposition 4.15. *Die Weil-Paarung aus Definition 4.13 hängt nur von der Divisorklasse von D_1 bzw. D_2 ab.*

Beweis. Wir zeigen nur die Wohldefiniertheit im ersten Argument; im zweiten folgt sie analog. Sei dazu also $D \sim D_1$, d.h. $D - D_1 \sim 0$. Also existiert $f \in \overline{K}(E)^*$ mit $D = D_1 + \operatorname{div}(f)$ und $\operatorname{supp}(\operatorname{div}(f)) \cap D_2 = \emptyset$. Weiter ist $nD = nD_1 + n\operatorname{div}(f) = \operatorname{div}(f_1 \cdot f^n)$ und es folgt:

$$\begin{aligned} e_n(D, D_2) &= \frac{f_1(D_2)f^n(D_2)}{f_2(D_1)f_2(\operatorname{div}(f))} \overset{\boxed{\text{Weil-Reziprozität Proposition 4.14}}}{\underset{\downarrow}{=}} \frac{f_1(D_2)}{f_2(D_1)}\frac{f^n(D_2)}{f(\operatorname{div}(f_2))} \\ &= e_n(D_1, D_2)\,. \end{aligned}$$

Letzte Gleichheit erhalten wir für $D_2 = \sum_{P\in E} n_P[P]$ aus

$$f(\operatorname{div}(f_2)) = f(nD_2) = \prod_{P\in E} f(P)^{nn_P} = f^n(D_2)\,.$$

□

Um nun wieder zurück zu einer Weil-Paarung als Abbildung $E[n] \times E[n] \to \mu_n$ zu kommen, verwenden wir Proposition 3.15 (1), wo wir gezeigt haben, dass für jeden Divisor D ein eindeutiger Punkt $P \in E$ existiert mit $D \sim [P] - [O]$ und können definieren:

Definition 4.16 (Weil-Paarung 2)**.** Sei E/K eine elliptische Kurve und $n > 1$. Seien $P, Q \in E[n]$. Die *Weil-Paarung* ist definiert durch:

$$\tilde{e}_n(P, Q) \;:=\; e_n([P] - [O], [Q] - [O])\,.$$

4.3 Verträglichkeit der Definitionen

Wir haben auf verschiedenen Wegen zwei Definitionen der Weil-Paarung gesehen und möchten diese nun vereinen:

Satz 4.17. *Die Weil-Paarungen e_n aus Definition 4.9 und $\tilde{e}_n$ aus Definition 4.16 sind reziprok gleich, d.h. für alle $S, T \in E[n]$ gilt*

$$e_n(S, T) \;=\; \tilde{e}_n(S, T)^{-1}\,.$$

Beweis. (Vergleiche [**?** , Notes on Exercises (3.16)]) Sei E/K eine elliptische Kurve, $n > 1$ und $P, Q \in E[n]$. Wähle Punkte $P', Q', R \in E$ mit $nP' = P$, $nQ' = Q$, $P' \neq \pm Q'$ und $2R = P' - Q'$. Die Existenz von P', Q' und R bekommen wir wieder mit Proposition 3.18. Weiter definiere Divisoren D_P, D_Q und Funktionen $f_P, f_Q, g_P, g_Q \in \overline{K}(E)$ durch

$$D_P = [P] - [O], \qquad D_Q = [Q + nR] - [nR], \tag{4.2}$$

$$\operatorname{div}(f_P) = nD_P, \qquad \operatorname{div}(f_Q) = nD_Q, \tag{4.3}$$

$$g_P^n = f_P \circ [n], \qquad g_Q^n = f_Q \circ [n]\,. \tag{4.4}$$

Wobei mit $[n]$ die Abbildung $P \mapsto nP$ gemeint ist. Ferner ist die Existenz von f_P und f_Q klar, da $nD_{P,Q} \sim 0$ wegen $P, Q \in E[n]$.

Betrachte nun

$$c_1(X) \;:=\; \frac{g_P(X+Q'+R)g_Q(X)}{g_P(X+R)g_Q(X+P')}$$

und

$$c_2(X) \;:=\; \prod_{i=0}^{n-1} g_Q(X+iQ')\,.$$

Wir behaupten nun $c_{1,2} = \text{const}$, was wir durch Proposition 2.6 beweisen wollen. Betrachten wir zunächst

$$\operatorname{div}(g_P^n) = \operatorname{div}(f_P \circ [n]) = n \sum_{S \in E[n]} ([S+P'] - [S])$$

und

$$\operatorname{div}(g_Q^n) = \operatorname{div}(f_Q \circ [n]) = n \sum_{S \in E[n]} ([S+Q'+R] - [S+R])\,.$$

Also können wir

$$\operatorname{div}(g_P) = \sum_{S \in E[n]} ([S+P'] - [S])$$

und

$$\operatorname{div}(g_Q) = \sum_{S \in E[n]} ([S+Q'+R] - [S+R])$$

folgern. Bezeichnen wir wieder mit $\tau_Q : E(K) \to E(K),\ P \mapsto P+Q$ die Additionsabbildung, so folgt

$$\begin{aligned}
\operatorname{div}(c_1) \;&=\; \operatorname{div}(g_P \circ \tau_{Q'+R}) + \operatorname{div}(g_Q) - \operatorname{div}(g_P \circ \tau_R) - \operatorname{div}(g_Q \circ \tau_{P'}) \\
&=\; \sum_{S \in E[n]} \big([S+P'-Q'-R] - [S-Q'-R] \\
&\qquad\qquad + [S+Q'+R] - [S+R] \\
&\qquad\qquad - [S+P'-R] + [S-R] \\
&\qquad\qquad - [S+Q'+R-P'] + [S+R-P'] \big) \\
&\quad \boxed{Q'+R = P'-R} \\
&\qquad\quad \downarrow \\
&=\; \sum_{S \in E[n]} \big([S+P'-(P'-R)] - [S-(P'-R)] \\
&\qquad\qquad + [S+P'-R] - [S+R] \\
&\qquad\qquad - [S+P'-R] + [S-R] \\
&\qquad\qquad - [S+P'-R-P'] + [S+R-P'] \big) \\
&=\; 0
\end{aligned}$$

und

$$\begin{aligned}
\operatorname{div}(c_2) \;&=\; \sum_{i=0}^{n-1} \operatorname{div}(g_Q \circ \tau_{iQ'}) \;=\; \sum_{i=0}^{n-1} \sum_{S \in E[n]} \big([S+Q'+R-iQ'] - [S+R-iQ']\big) \\
&=\; \sum_{S \in E[n]} \sum_{i=0}^{n-1} \big([S+R-(i-1)Q'] - [S+R-iQ']\big)
\end{aligned}$$

$$
\begin{aligned}
&\boxed{\text{Teleskopsumme}} \\
&\quad\downarrow \\
&= \sum_{S\in E[n]} \left([S+R+Q'] - [S+R+Q'-nQ']\right) \\
&= \sum_{S\in E[n]} [S+R+Q'] - \sum_{S\in E[n]} [S+R+Q'-Q] \\
&\boxed{Q\in E[n]} \\
&\quad\downarrow \\
&= \sum_{S\in E[n]} [S+R+Q'] - \sum_{T:=S-Q\ \in E[n]} [T+R+Q'] \\
&= 0\,.
\end{aligned}
$$

Daraus können wir nun die postulierte Verträglichkeit folgern:

$$
\begin{aligned}
\tilde{e}_n(P,Q) \;&=\; \frac{f_P(D_Q)}{f_Q(D_P)} \;\overset{\boxed{\text{Gleichung (4.2)}}}{\downarrow}\; = \frac{f_P(Q+nR)f_Q(O)}{f_P(nR)f_Q(P)} \\
&\boxed{\text{Gleichung (4.3)}} \qquad\qquad \boxed{\text{Gleichung (4.4)}} \\
&\quad\downarrow \qquad\qquad\qquad\quad \downarrow \\
&= \frac{f_P(nQ'+nR)f_Q(nO)}{f_P(nR)f_Q(nP')} \;=\; \left(\frac{g_P(Q'+R)g_Q(O)}{g_P(R)g_Q(P')}\right)^n \\
&\boxed{c_1=\text{const}} \qquad\qquad\qquad\qquad \boxed{\text{Teleskopprodukt}} \\
&\quad\downarrow \qquad\qquad\qquad\qquad\qquad\quad \downarrow \\
&= \prod_{i=0}^{n-1} \frac{g_P(R+(i+1)Q')g_Q(iQ')}{g_P(R+iQ')g_Q(P'+iQ')} \;=\; \frac{g_P(R+nQ')}{g_P(R)} \prod_{i=0}^{n-1} \frac{g_Q(iQ')}{g_Q(P'+iQ')} \\
&\boxed{c_2=\text{const}} \\
&\quad\downarrow \\
&= \frac{g_P(R+nQ')}{g_P(R)} \;=\; \frac{g_P(R+Q)}{g_P(R)} \;=\; e_n(P,Q)^{-1}\,.
\end{aligned}
$$

□

4.4 Beweis der Eigenschaften der Weil-Paarung

Kommen wir also endlich zum Beweis der Eigenschaften der Weil-Paarung, wobei wir uns jeweils aussuchen können, welche Definition gerade die „einfachere“ ist.

Beweis von Proposition 4.5. I. **Linear** Seien $P \neq Q \neq R \in E[n]$ mit $\operatorname{div}(f_P) = n[P]-n[O]$, $\operatorname{div}(f_Q) = n[Q]-n[O]$, $\operatorname{div}(f_R) = n[R]-n[O]$ für geeignete $f_P, f_Q, f_R \in \overline{K}(E)$. Damit ist $\operatorname{div}(f_P \cdot f_Q) = n([P]+[Q]) - n([O]+[O])$ und wir folgern:

$$
e_n(P+Q,R) = \frac{(f_P\cdot f_Q)([R]-[O])}{f_R([P]+[Q]-2[O])} = \frac{f_P(R)f_Q(R)f_R(O)^2}{f_R(P)f_R(Q)f_P(O)f_Q(O)} = e_n(P,R)e_n(Q,R)\,.
$$

Aufgrund der Symmetrie der Konstruktion zeigt sich die Linearität im zweiten Argument analog (was bei ersterer Definition der Weil-Paarung nicht der Fall ist).

II. **Alternierend** Aus I. haben wir

$$
e_n(S+T,S+T) \;=\; e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T)\,.
$$

Wir müssen also $e_n(T,T) = 1\ \forall T \in E[n]$ zeigen. Dazu betrachten wir die Verschiebung um P, für ein $P \in E$, d.h. die Abbildung $\tau_P : E \to E,\ Q \mapsto Q + P$, erhalten aus Lemma 4.7 Funktionen f mit $\operatorname{div}(f) = n[T] - n[O]$ und g mit $f \circ n = g^n$ und berechnen

$$\operatorname{div}\left(\prod_{i=0}^{n-1} f \circ \tau_{iT}\right) \;=\; n\sum_{i=0}^{n-1}\Big([(1-i)T] - [(-i)T]\Big) \;=\; n[T] - n[(1-n)T] \;\overset{\boxed{T \in E[n]}\ \downarrow}{=}\; 0\,.$$

Nach Proposition 2.6 ist $\prod_{i=0}^{n-1} f \circ \tau_{iT} = \text{const}$. Wir haben

$$\begin{aligned}\left(\prod_{i=0}^{n-1} g \circ \tau_{iT'}\right)^n &= \prod_{i=0}^{n-1} g^n \circ \tau_{iT'} = \prod_{i=0}^{n-1} f \circ n \circ \tau_{iT'} \\ &= \prod_{i=0}^{n-1} f \circ (n \circ \tau_{iT'}) \overset{\boxed{nT' = T}\ \downarrow}{=} \prod_{i=0}^{n-1} f \circ \tau_{iT}\,,\end{aligned}$$

also ist $\left(\prod_{i=0}^{n-1} g \circ \tau_{iT'}\right)^n$ konstant und analog zu Bemerkung 3.19(4) auch $\prod_{i=0}^{n-1} g \circ \tau_{iT'}$. Damit gilt für beliebiges $X \in E$

$$\prod_{i=0}^{n-1} g(X + iT') \;=\; \prod_{i=0}^{n-1} g(X + (i+1)T')\,,$$

wobei wir links alles bis auf den Term für $i = 0$ und rechts bis auf den Term für $i = n-1$ alles kürzen können:

$$g(X) \;=\; g(X + nT') \;=\; g(X + T)\,.$$

Wir haben f und g wie in der Konstruktion der Weil-Paarung gewählt und erhalten letztlich

$$e_n(T,T) \;=\; \frac{g(X+T)}{g(X)} \;=\; 1\,.$$

III. **Anti-symmetrisch** Aus I. und II. können wir folgern:

$$1 = e_n(P+Q, P+Q) = e_n(P,P)e_n(P,Q)e_n(Q,P)e_n(Q,Q) = e_n(P,Q)e_n(Q,P)\,.$$

IV. **Nicht entartet in beiden Variablen** Sei $e_n(S,P) = 1$ für alle $S \in E[n]$. Dann ist $g(X+S) = g(X)$ für g aus der Konstruktion. Aus [**?** , Lemma 3.2.1] können wir dann folgern, dass $g = h \circ [m]$ für geeignetes $h \in \overline{K}(E)$. Damit ist aber für f aus der Konstruktion

$$(h \circ [m])^m \;=\; g^m \;=\; f \circ [m]\,,$$

also $f = h^m$. Wir erinnern uns, dass $\operatorname{div}(f) = m[P] - m[O]$, und haben damit

$$\operatorname{div}(h) \;=\; [P] - [O]\,.$$

Nach Proposition 3.17 muss $\operatorname{sum}([P] - [O]) = O$ gelten, also $P = O$.
Mit Eigenschaft III und dem eben Bewiesenen können wir Selbiges für die erste Variable schnell beweisen: Sei nämlich $e_n(P,S) = 1$ für alle $S \in E[n]$, so gilt

$$1 = e_n(P,S)^{-1} = e_n(S,P) = 1\ \forall S \in E[n]\,,$$

woraus $S = O$ folgt.

V. **Galois invariant** Sei $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Da σ Werte aus K und damit die Koeffizienten von E fest lässt, ist klar, dass für $T \in E(\overline{K})$ auch $T^\sigma \in E(\overline{K})$. Für $T \in E[n]$ ist

$$O = O^\sigma = (nT)^\sigma = (\underbrace{T + \cdots + T}_{n \text{ mal}})^\sigma = \underbrace{T^\sigma + \cdots + T^\sigma}_{n \text{ mal}} = nT^\sigma \,.$$

Also ist auch $T^\sigma \in E[n]$. Damit ist klar, dass f^σ und g^σ (gemeint ist, σ auf die Koeffizienten von f und g angewandt) Funktionen für T^σ und S^σ sind und wir haben

$$e_n(S,T)^\sigma = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = e_n(S^\sigma, T^\sigma)\,.$$

□

5 Elliptische Kurven über $\mathbb{F}_q$

Sei im Folgenden $q = p^m$ mit $p \neq 2, 3$ einer Primzahl.

Wir wollen zunächst ein Resultat über die Struktur der additiven Gruppe einer elliptischen Kurve über $\mathbb{F}_q$ herleiten.

Proposition 5.1. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$. Dann gilt*

$$E(\mathbb{F}_q) \;\cong\; \mathbb{Z}_d \qquad \textit{oder} \qquad E(\mathbb{F}_q) \;\cong\; \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2}$$

mit $d, d_1, d_2 \in \mathbb{N}^*$ und $d_1 \mid d_2$.

Beweis. Aus dem Hauptsatz über endlich präsentierte abelsche Gruppen (z.B. [**?** , Hauptsatz 6.109]) wissen wir, dass

$$E(\mathbb{F}_q) \;\cong\; Z_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n}$$

mit $d_i \in \mathbb{N}^* \; \forall i = 1, \ldots, n$ und $d_i \mid d_{i+1} \; \forall i = 1, \ldots, n-1$. In jeder Gruppe $\mathbb{Z}_{d_i}$ gibt es d_1 Elemente, deren Ordnung d_1 teilt, also haben wir d_1^n Elemente in $E(\mathbb{F}_q)$ deren Ordnung d_1 teilt. Nach Lemma 4.4 wissen wir aber, dass $\#E[d_1] \leq d_1^2$. Also ist erst recht $\#E(\mathbb{F}_q)[d_1] \leq d_1^2$ und damit $n \leq 2$. □

Das liefert uns jedoch noch keinen Aufschluss über die Größe der additiven Gruppe. Wollen wir dazu erst einmal eine kleine Überlegung machen:

Sei also

$$E: \; y^2 \;=\; x^3 + Ax + B$$

eine elliptische Kurve über $\mathbb{F}_q$. Dann lässt sich eine triviale Oberschranke für $\#E(\mathbb{F}_q)$ wie folgt herleiten: Angenommen, die quadratische Gleichung auf der linken Seite obiger Gleichung hat für alle $x \in \mathbb{F}_q$ auf der rechten Seite genau zwei Lösungen, so haben wir

$$\#E(\mathbb{F}_q) \leq 2q + 1\,.$$

Mit mehr Theorie kann man folgende Proposition beweisen:

Proposition 5.2 (Hasse)**.** *Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann gilt*

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

Beweis. [**?** , Theorem V.1.1] . □

5.1 Schoofs Idee

Proposition 5.3. *Sei $q = p^n$ für p prim. Sei $E/\mathbb{F}_q$ eine elliptische Kurve und*

$$\phi_q : \; E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), \qquad (x,y) \mapsto (x^q, y^q), \quad O \mapsto O$$

der Frobenius-Endomorphismus zu q. Dann gilt

(1) ϕ_q ist in der Tat ein Endomorphismus.

(2) $P \in E(\mathbb{F}_q) \quad \Leftrightarrow \quad \phi_q(P) = P$ und $P \in E$.

Beweis. Wir gehen von dem Frobenius-Endomorphismus zu q in $\mathbb{F}_q$ aus, wollen aber keinen Unterschied in der Notation machen, also

$$\phi_q : \; \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q, \qquad x \mapsto x^q \,.$$

Hier wissen wir (z.B. aus [**?** , Theorem C.1 und Proposition C.2]), dass

(1) ϕ_q ein Körperendomorphismus ist und

(2) $x \in \mathbb{F}_q \quad \Leftrightarrow \quad \phi_q(x) = x$.

Kommen wir damit zum eigentlichen Beweis: Sei $E/\mathbb{F}_q$ gegeben durch $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ mit $a_1, \ldots, a_6 \in \mathbb{F}_q$. Nehmen wir $(x,y) \in E$, so ist

$$\begin{aligned} (y^q)^2 + a_1x^qy^q + a_3y^q &= (y^p)^2 + a_1^qx^qy^q + a_3^qy^q \;=\; (y^2 + a_1xy + a_3y)^q \\ &= (x^3 + a_2x^2 + a_4x + a_6)^q \;=\; (x^3)^q + a_2^q(x^2)^q + a_4^qx^q + a_6^q \\ &= (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6^q \,, \end{aligned}$$

also $(x^q, y^q) \in E$. Ganz analog sieht man an den Additionsformeln, dass ϕ_q mit der Addition auf E verträglich ist.

Eigenschaft (2) ist mit Kenntnis der Eigenschaft (2) des Frobenius-Endomorphismus in $\mathbb{F}_q$ ebenfalls klar:

$$\begin{aligned} (x,y) \in E(\mathbb{F}_q) \quad &\Leftrightarrow \quad x,y \in \mathbb{F}_q \;\wedge\; (x,y) \in E \\ &\Leftrightarrow \quad \phi_q(x) = x, \; \phi_q(y) = y \;\wedge\; (x,y) \in E \\ &\Leftrightarrow \quad \phi_q(x,y) = (x,y) \;\wedge\; (x,y) \in E \,. \end{aligned}$$

□

Proposition 5.4. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und*

$$\#E(\mathbb{F}_q) = q + 1 - a_q \,, \qquad \text{mit } |a_q| \le 2\sqrt{q} \,.$$

Des Weiteren sei ϕ_q der Frobenius-Endomorphismus zu q. Dann gilt:

$$\phi_q^2 - a_q\phi_q + [q] \;=\; 0 \qquad \text{in } \mathrm{End}(E) \,.$$

Beweis. [**?** , Theorem 2.3.1 (b)] . □

Nehmen wir nun einen Punkt $P = (x, y) \in E[l] \backslash \{O\}$ für ein $l \in \mathbb{N}$, so haben wir

$$(x^{q^2}, y^{q^2}) - a_q(x^q, y^q) + q(x, y) \;=\; O\,,$$

wobei wir nach Wahl von P den mittleren Term der Summe modulo l reduzieren können. Es gilt also

$$(x^{q^2}, y^{q^2}) - n_l(x^q, y^q) + q(x, y) = O \qquad \begin{array}{l}\text{mit } n_l \equiv a_l \pmod{l} \\ \text{und } 0 \leq n_l < l\,.\end{array} \tag{5.1}$$

Ziel ist es nun, Kongruenzen der Form $a_q \bmod l$ für genügend viele (kleine) Primzahlen l zu finden, um dann mit Hilfe des Chinesischen Restsatzes a_q eindeutig zu bestimmen. Haben wir für eine Menge $S = \{l_1, \ldots, l_r\}$, $r \in \mathbb{N}$, an Primzahlen für alle $l \in S$ einen Wert n_l in Gleichung (5.1) gefunden, so können wir

$$\begin{aligned} n_{l_1} &\equiv a_q \pmod{l_1}, \\ n_{l_2} &\equiv a_q \pmod{l_2}, \\ &\cdots \\ n_{l_r} &\equiv a_q \pmod{l_r} \end{aligned}$$

mit dem Chinesischen Restsatz eindeutig lösen. Die Bedingung für die Eindeutigkeit ergibt aus $|a_q| \leq 2\sqrt{q}$ in Proposition 5.4, d.h. wir brauchen

$$\prod_{l \in S} l \;>\; 4\sqrt{q}\,.$$

Beispiel 5.5. Nehmen wir $q = 173$ und

$$E/\mathbb{F}_{173}: \quad y^2 + xy + 3y \;=\; x^3 + 2x^2 + 4x + 5\,.$$

Man findet heraus, dass

$$P_3 = (36, 51) \;\in E(\mathbb{F}_{173})[3] \quad \text{und} \quad P_{19} = (35, 13) \;\in E(\mathbb{F}_{173})[19]\,.$$

In der Tat ist $3 \cdot 19 = 57 > 52.6 \approx 4\sqrt{q}$. Nun testen wir für alle $i = 0, 1, 2$ ob

$$(36^{173^2}, 51^{173^2}) - i(36^{173}, 51^{173}) + 173(36, 51) \;=\; O$$

und sehen dabei den Erfolg bereits bei $i = 0$.
Analog gehen wir bei P_{19} vor und fassen zusammen:

$$\begin{aligned} 0 &\equiv a_{173} \pmod{3}\,, \\ 3 &\equiv a_{173} \pmod{19}\,. \end{aligned}$$

Wir lösen, erhalten

$$a_q \;\equiv\; 3 \pmod{57}$$

und folgern

$$\#E(\mathbb{F}_q) \;=\; 173 + 1 - 3 \;=\; 171\,.$$

Um die Punkte P_3 und P_{19} zu finden, benutzt man am besten ein Computer-Algebra-System, wie `sage`, indem Primzahl für Primzahl die nicht-trivialen Torsionsgruppen gesucht werden. Der Quelltext findet sich unter Algorithmus A.2.

Die Probleme für eine algorithmische Umsetzung zeigen sich schon deutlich in Beispiel 5.5: Wir haben keine effiziente Möglichkeit kennengelernt, um die l-Torsionsgruppen zu berechnen. Zudem werden diese mit Körpererweiterungen von $\mathbb{F}_q$ immer größer. Doch wie wir dies umgehen und mit allen l-Torsionspunkten „gleichzeitig“ arbeiten können, zeigt uns der folgende Abschnitt.

5.2 Divisions-Polynome

Der Einfachheit halber nehmen wir weiter an, dass $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$.

Definition 5.6 (Divisions-Polynome)**.** Sei $E/\mathbb{F}_q$ eine elliptische Kurve in Weierstraßscher Normalform, gegeben durch

$$y^2 \;=\; x^3 + Ax + B\,.$$

Die *Divisions-Polynome* $\psi_m \in \mathbb{Z}[x, y, A, B]$ für $m \in \mathbb{N}$ sind gegeben durch

$$\begin{aligned}
\psi_0 &= 0\,,\\
\psi_1 &= 1\,,\\
\psi_2 &= 2y\,,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2\,,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)\,,\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ falls } m \geq 2\,,\\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ falls } m \geq 3\,.
\end{aligned}$$

Dass durch letzte Rekursion auch wirklich Polynome entstehen, zeigt nachstehendes Lemma.

Lemma 5.7. *Es gilt*

$$\psi_m \in \begin{cases} \mathbb{Z}[x, y^2, A, B] & \textit{falls } m \textit{ ungerade,}\\ 2y\mathbb{Z}[x, y^2, A, B] & \textit{falls } m \textit{ gerade.}\end{cases}$$

Beweis. Durch Induktion, welche man z.B. in [**?** , Lemma 3.3] findet. □

Definition 5.8. Sei $m \in \mathbb{N}_{\geq 2}$. Definiere

$$\begin{aligned}
\phi_m &= x\,\psi_m^2 - \psi_{m+1}\psi_{m-1}\,,\\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\,.
\end{aligned}$$

Auch hier wollen wir die Wohldefiniertheit zitieren:

Lemma 5.9. *Es gilt*

$$\phi_m \in \mathbb{Z}[x, y^2, A, B]$$

und

$$\omega_m \in \begin{cases} \mathbb{Z}[x, y^2, A, B] & \textit{falls } m \textit{ gerade,}\\ y\mathbb{Z}[x, y^2, A, B] & \textit{falls } m \textit{ ungerade.}\end{cases}$$

Beweis. [**?** , Lemma 3.4]. □

Mit Hilfe dieser Polynome können wir nun eine interessante Aussage formulieren, welche die Teilungs-Polynome mit den Torsionspunkten verbindet.

Satz 5.10. *Sei $n \in \mathbb{N}^*$ und $P = (x, y) \in E$. Dann gilt*

$$nP \;=\; \left(\frac{\phi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right)\,.$$

Beweis. Z.B. in [**?** , Section 9.5]. □

Lemma 5.11. *Sei $n \in \mathbb{N}^*$. Dann haben $\phi_n(x)$ und $\psi_n(x)^2$ als Polynome in x keine gemeinsamen Nullstellen.*

Beweis. Erster Teil des Beweises zu [**?** , Corollary 3.7]. □

Korollar 5.12. *Sei $n \in \mathbb{N}^*$ und $P = (x, y) \in E \setminus \{O\}$. Dann gilt*

$$P \in E[n] \quad \Leftrightarrow \quad \psi_n(x, y) = 0\,.$$

Beweis. Nehmen wir einen Punkt $P = (x, y) \in E[n] \setminus \{O\}$, so folgt per definitionem $nP = O = (\infty, \infty)$. Da nach Lemma 5.11 $\phi_n(x)$ und $\psi_n(x)^2$ teilerfremd sind, folgt $\psi_n(x, y) = 0$.

In der anderen Richtung sei $P = (x, y) \in E \setminus \{O\}$ und $\psi_n(x, y) = 0$. Nach Satz 5.10 und Lemma 5.11 folgt sofort $nP = O$, also $P \in E[n]$. □

Bemerkung 5.13. Um Lemma 4.4 (1) zu beweisen, kann man auch von Satz 5.10 ausgehen, was man beispielsweise so in [**?** , Theorem 3.2 und Section 3.2] findet.

5.3 Schoofs Algorithmus

Mit Hilfe der Divisionspolynome können wir alle Berechnung im Quotientenring

$$R_l \;=\; \mathbb{F}_q[x, y]/(\psi_l(x, y),\; y^2 - x^3 - Ax - B)$$

durchführen und Schoofs Algorithmus formulieren, welcher auch für $\mathrm{char}(\mathbb{F}_q) = 2$ oder 3 funktioniert:

Algorithmus 5.14. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve mit* $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$. *Dann berechnet sich $\#E(\mathbb{F}_q)$ durch* Schoofs-Algorithmus *in $O((\log q)^8)$.*

Schoofs Algorithmus

Output: $\#E(\mathbb{F}_q)$

1 $A := 1$;
2 $l := 3$;
3 **while** $A < \sqrt{q}$ **do**
4 **for** $n = 0$ **to** $l - 1$ **do**
5 **if** $(x^{q^2}, y^{q^2}) + q(x, y) = n(x^q, y^q)$ **then**
6 break;
7 **endfor**;
8 $A := l \cdot A$;
9 $n_l := n$;
10 $l :=$ nächste Primzahl $> l$;
11 **endwhile**;
12 Finde a mit $a \equiv n_l \pmod{l}$ für alle gespeicherten n_l mit Hilfe des Chinesischen Restsatzes;
13 **return** $\#E(\mathbb{F}_q) = q + 1 - a$;

Beweis. Die Korrektheit des Algorithmus haben wir bereits hergeleitet. Einen ausführlichen Beweis zur Laufzeit findet man in [**?** , XI.3.1]. □

Bemerkung 5.15. Wie genau die Berechnung in Schritt `(5)` von Schoofs-Algorithmus im Ring R_l stattfindet, kann man beispielsweise in [**?** , Abschnitt 4.5] nachlesen.

Teil II

Elliptische Kurven – Anwendungen in der Kryptographie

6 Effiziente Berechnung der Weil-Paarung

Die Weil-Paarung, wie sie in den Definitionen 4.9 und 4.16 konstruiert wurde, gibt zunächst keinen expliziten Aufschluss über das Auffinden von Funktionen, deren Divisor einem gegebenen Hauptdivisor entspricht. Für $E[2]$ lässt sich dies ohne große Probleme bewerkstelligen, wie das folgende Beispiel zeigt:

Beispiel 6.1. Sei die elliptische Kurve

$$E: \; y^2 \; = \; (x-e_1)(x-e_2)(x-e_3)$$

gegeben. Wir finden sofort die drei Punkte $P_1 = (e_1, 0)$, $P_2 = (e_2, 0)$ und $P_3 = (e_3, 0)$ auf E.
Man überlegt sich relativ leicht, dass gerade die Punkte P mit $y(P) = 0$ (also deren y-Koordinate verschwindet) genau die Punkte von Ordnung 2 sind. Dazu sei $P \in E$ und es folgt:

$$P \in E[2] \;\Leftrightarrow\; P = -P \;\Leftrightarrow\; y(P) = 0\,,$$

wobei man die letzte Folgerung in den Additionsformeln 3.13 findet.
Damit können wir also festhalten, dass $P_i \in E[2]$ für $i = 1, 2, 3$. Also suchen wir Funktionen f_i, für die $\operatorname{div}(f_i) = 2[P_i] - 2[O]$ gilt. Wie wir bereits in Beispiel 2.3 gesehen haben, erfüllen $f_i(x, y) = x - e_i$ gerade diese Eigenschaft.

Im Allgemeinen ist dies jedoch nicht so einfach, doch der folgende Algorithmus wird uns diesem Ziel einen wesentlichen Schritt näher bringen:

Algorithmus 6.2 (Miller's Algorithmus)**.** *Sei E/K eine elliptische Kurve in Weierstraßscher Normalform*

$$E: \quad y^2 + a_1xy + a_3y \; = \; x^3 + a_2x^2 + a_4x + a_6\,.$$

Für $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(K) \setminus \{O\}$ sei $y = \lambda x + \nu$ die Gerade zwischen P und Q (setze $\lambda = \infty$, falls die Gerade vertikal verläuft). Definiere

$$h_{P,Q} \; = \; \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2 - a_1\lambda + a_2} & \lambda \neq \infty\,, \\ x - x_P & \lambda = \infty\,. \end{cases}$$

Dann ist Miller's Algorithmus gegeben durch:

Miller's Algorithmus

Input: $P \in E(K)$, $(\varepsilon_1, \ldots, \varepsilon_t) \in \{0,1\}^t$ mit $N = \sum_{i=1}^{t} \varepsilon_i 2^i$ und $\varepsilon_t \neq 0$.
Output: $f_P \in K(E)$ mit $\operatorname{div}(f_P) = N[P] - [NP] - (N-1)[O]$.

```
1  T := P;
2  f_P := 1;
3  for  i from t − i to 0 do
4      f_P := f_P^2 · h_{T,T};
5      T := 2T;
6      if ε_i = 1 then
7          f_P := f_P · h_{T,P};
8          T := T + P;
9      endif;
10 endfor;
11 return f_P ;
```

Proposition 6.3. *In Algorithmus 6.2 gilt:*

(1) $\operatorname{div}(h_{P,Q}) = [P] + [Q] - [P+Q] - [O]$.

(2) Am Ende des Algorithmus ist $\operatorname{div}(f_P) = N[P] - [NP] - (N-1)[O]$. *Insbesondere gilt falls* $P \in E[N]$, *dass* $\operatorname{div}(f_P) = N[P] - N[O]$.

Beweis. (1) Sei zunächst $\lambda \neq \infty$. Dann hat die Gerade $y = \lambda x + \nu$ drei Schnittpunkte mit E, nämlich P, Q und $-P-Q$. Damit ist $\nu = y_P - \lambda x_P$ und die Additionsformeln 3.13 lieferen uns

$$x_{P+Q} \;=\; \lambda^2 + a_1\lambda - a_2 - x_P - x_Q\,.$$

Es folgt

$$\begin{aligned}
\operatorname{div}(h_{P+Q}) &= \operatorname{div}(y - y_P - \lambda(x - x_P)) &&- \operatorname{div}(x + x_P + x_Q - \lambda^2 - a_1\lambda + a_2)\\
&= \operatorname{div}(y - \lambda x - \nu) &&- \operatorname{div}(x - x_{P+Q})\\
&= [P] + [Q] + [-P-Q] - 3[O] &&- [P+Q] + [-P-Q] - 2[O]\\
&= [P] + [Q] - [P+Q] - [O]\,.
\end{aligned}$$

Ist $\lambda = \infty$, so ist $Q = -P$ und es folgt $\operatorname{div}(h_{P,Q}) = \operatorname{div}(x - x_P) = [P] + [-P] - 2[O]$, was der geforderte Divisor ist.

(2) Seien mit $T_i^{\text{start}}, f_i^{\text{start}}$ bzw. $T_i^{\text{end}}, f_i^{\text{end}}$ die Werte von T und f_P zu Beginn (Zeile 3) bzw. am Ende (Zeile 10) eines Durchlaufs der i-Schleife bezeichnet. Da $\varepsilon_i \in \{0,1\}$ ergibt sich für T

$$T_i^{\text{end}} \;=\; 2T_i^{\text{start}} + \varepsilon_i P \tag{6.1}$$

und für f_P

$$f_i^{\text{end}} \;=\; (f_i^{\text{start}})^2\; h_{T_i^{\text{start}},T_i^{\text{start}}}\; (h_{2T_i^{\text{start}},P})^{\varepsilon_i}\,. \tag{6.2}$$

Damit folgt für den Divisor von f_i^{end}:

$$\begin{aligned}
&\boxed{\text{Gleichung (6.2)}}\\
&\quad\downarrow\\
\operatorname{div}(f_i^{\text{end}}) &= 2\operatorname{div}(f_i^{\text{start}}) + \operatorname{div}(h_{T_i^{\text{start}},T_i^{\text{start}}}) + \varepsilon_i \operatorname{div}(h_{2T_i^{\text{start}},P})\\
&\quad\boxed{\text{Proposition 6.3}}\\
&\quad\downarrow\\
&= 2\operatorname{div}(f_i^{\text{start}}) + \left(2[T_i^{\text{start}}] - [2T_i^{\text{start}}] - [O]\right)\\
&\quad + \varepsilon_i\,\left([2T_i^{\text{start}}] + [P] - [2T_i^{\text{start}} + P] - [O]\right)
\end{aligned}$$

$$= 2\operatorname{div}(f_i^{\text{start}}) + 2[T_i^{\text{start}}] - [2T_i^{\text{start}} + \varepsilon_i P] + \varepsilon_i[P] - (1+\varepsilon_i)[O] \tag{6.3}$$

Die Schleife läuft von $i = t-1$ bis $i = 0$ und selbstverständlich ist $T_i^{\text{end}} = T_{i-1}^{\text{start}}$ und $f_i^{\text{end}} = f_{i-1}^{\text{start}}$. Damit können wir Gleichung (6.1) und Gleichung (6.3) geeignet umformen zu

$$T_{i-1}^{\text{start}} - 2T_i^{\text{start}} = \varepsilon_i P\,, \tag{6.4}$$

$$\operatorname{div}(f_{i-1}^{\text{start}}) - 2\operatorname{div}(f_i^{\text{start}}) = 2[T_i^{\text{start}}] - [T_{i-1}^{\text{start}}] + \varepsilon_i[P] - (1+\varepsilon_i)[O]\,, \tag{6.5}$$

und erhalten schließlich

$$\begin{aligned}
T_0^{\text{end}} &\overset{\boxed{\text{Gleichung (6.1)}}}{=} \varepsilon_0 P + 2T_0^{\text{start}} = \varepsilon_0 P + 2T_0^{\text{start}} - 2^2 T_1^{\text{start}} + 2^2 T_1^{\text{start}} + \cdots - 2^t T_{t-1}^{\text{start}} + 2^t T_{t-1}^{\text{start}} \\
&= \varepsilon_0 P + \left[\sum_{i=1}^{t-1} 2^i \left(T_{i-1}^{\text{start}} - 2T_i^{\text{start}}\right)\right] + 2^t T_{t-1}^{\text{start}} \overset{\boxed{\text{Gleichung (6.4)}}}{=} \varepsilon_0 P + \left[\sum_{i=1}^{t-1} 2^i\ \varepsilon_i P\right] + 2^t T_{t-1}^{\text{start}} \\
&\overset{\boxed{\varepsilon_t = 1,\ T_{t-1}^{\text{start}} = P}}{=} \sum_{i=0}^{t} 2^i\ \varepsilon_i P \overset{\boxed{\text{Darstellung von } N}}{=} NP\,.
\end{aligned}$$

Ganz analog berechnen wir $\operatorname{div}(f_0^{\text{end}})$ mit derselben Teleskopsumme für $\operatorname{div}(f_{i-1}^{\text{start}})$ und $\operatorname{div}(f_i^{\text{start}})$. Hier gilt jedoch zu beachten, dass der letzte Term $2^t \operatorname{div}(f_{t-1}^{\text{start}})$ verschwindet, da $f_{t-1}^{\text{start}} = 1$.

$$\begin{aligned}
\operatorname{div}(f_0^{\text{end}}) &= 2\operatorname{div}(f_0^{\text{start}}) + 2[T_0^{\text{start}}] - [T_0^{\text{end}}] + \varepsilon_0[P] - (1+\varepsilon_0)[O] \\
&\overset{\boxed{T_0^{\text{end}} = NP}}{=} \left[\sum_{i=1}^{t-1} 2^i\big(\operatorname{div}(f_{i-1}^{\text{start}}) - 2\operatorname{div}(f_i^{\text{start}})\big)\right] + 2[T_0^{\text{start}}] - [T_0^{\text{end}}] + \varepsilon_0[P] - (1+\varepsilon_0)[O] \\
&\overset{\boxed{\text{Gleichung (6.5)}}}{=} \left[\sum_{i=1}^{t-1} 2^i\big(2[T_i^{\text{start}}] - [T_{i-1}^{\text{start}}] + \varepsilon_i[P] - (1+\varepsilon_i)[O]\big)\right] \\
&\quad + 2[T_0^{\text{start}}] - [T_0^{\text{end}}] + \varepsilon_0[P] - (1+\varepsilon_0)[O] \\
&= 2^t[T_{t-1}^{\text{start}}] + \sum_{i=0}^{t-1} 2^i\varepsilon_i[P] - \sum_{i=0}^{t-1} 2^i(1+\varepsilon_i)[O] - [NP] \\
&= N[P] - (N-1)[O] - [NP]
\end{aligned}$$

□

Damit lässt sich nun relativ leicht die Weil-Paarung berechnen:

Proposition 6.4. *Sei E/K eine elliptische Kurve und $P, Q \in E(K)[N]$. Sei $S \in E(K) \setminus (P,Q)$ ((P,Q) bezeichne dabei die von P und Q erzeugte Untergruppe in $E(K)[N]$), so ist*

$$e_N(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}\,.$$

Beweis. Es ist $[Q+S]-[S] \sim [Q]-[O]$, $[P-S]-[-S] \sim [P]-[O]$ und nach Wahl von S ist $\operatorname{supp}([P]-[O]) \cap \operatorname{supp}([Q+S]-[S]) = \emptyset$. Da nach Proposition 4.15 die Weil-Paarung aus Definition 4.16 nur von der Divisorklasse abhängt, können wir einsetzen:

$$e_N(P,Q) \;=\; \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f(P)}{f(O)},$$

wobei $f \in \overline{K}(E)^*$ mit $\operatorname{div}(f) = N[Q+S] - N[S]$. Des Weiteren gilt $\operatorname{div}(f) = \operatorname{div}(f_Q \circ \tau_{-S})$, also ist f ein konstantes Vielfaches von $f_Q \circ \tau_{-S}$, was sich im Bruch gerade wegkürzt:

$$\frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f(P)}{f(O)} \;=\; \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{(f_Q \circ \tau_{-S})(P)}{(f_Q \circ \tau_{-S})(O)} \;=\; \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}.$$

□

Den Fall $P \neq Q$ können wir noch weiter vereinfachen, was wir aber nicht beweisen werden.

Proposition 6.5. *Sei E/K eine elliptische Kurve und $P, Q \in E(K)[N]$ mit $P \neq Q$. Dann ist*

$$e_N(P,Q) \;=\; (-1)^N \frac{f_P(Q)}{f_Q(P)}$$

Beweis. [**?** , Proposition 8] . □

Bemerkung 6.6. Der Beweis von Proposition 6.5 lässt sich für $K = \mathbb{C}$ oder $K = \mathbb{R}$ relativ leicht einsehen. Ausgehend von Proposition 6.4 ist

$$e_N(P,Q) \;=\; \frac{f_Q(-S)}{f_P(S)} \frac{f_P(Q+S)}{f_Q(P-S)}.$$

Betrachten wir für $P \neq Q$ den Grenzwert $S \to O$, so geht der erste Faktor gegen $(-1)^N$ (f_P und f_Q haben nach Konstruktion in O jeweils Pole N-ter Ordnung), der zweite geht gegen $\frac{f_P(Q)}{f_Q(P)}$.

Beispiel 6.7. Sei $E/\mathbb{F}_{67}$ die elliptische Kurve

$$y^2 = x^3 + 5x + 18$$

und $P = (28, 0)$, $Q = (31, 22)$ mit $P, Q \in E(\mathbb{F}_{67})$. Man findet heraus, dass $P, Q \in E(\mathbb{F}_{67})[4]$. Wir benutzen wieder `sage`, wo sich wie folgt die obige Kurve erzeugen und $E(\mathbb{F}_{67})[4]$ ausgeben lässt:

```
p = 67; N = 4;
E = EllipticCurve(GF(p), [5,18]);
E(0).division_points(N)
```

Wählen wir nun einen Punkt $S \in E(\mathbb{F}_{67})$ mit $S \neq P, Q, P-Q, O$, beispielsweise $S = (4, 13) \in E(\mathbb{F}_{67})$. Mit Algorithmus 6.2 berechnen wir

```
P = E(28,0); Q = E(31,22); S = E(4,13);
P._miller_(Q+S, N)
P._miller_(S,N)
Q._miller_(P-S,N)
Q._miller_(-S,N)
```

und erhalten (mit dortiger Notation)

$$f_P(Q+S) = 26,\ f_P(S) = 40,\ f_Q(P-S) = 53,\ f_Q(-S) = 37\,.$$

Also

$$e_N(P,Q) \;=\; \frac{26}{40}\Big/\frac{53}{37} \;=\; 66 \;\in \mathbb{F}_{67}\,.$$

Auch mit Proposition 6.5 erhalten wir selbiges Resultat, da

$$e_N(P,Q) \;=\; (-1)^N \frac{f_P(Q)}{f_Q(P)} \;=\; (-1)^4 \frac{9}{58} \;=\; 66 \;\in \mathbb{F}_{67}\,.$$

Zuletzt können wir in der Tat feststellen, dass $66^4 = 1 \in \mathbb{F}_{67}$.
Selbstverständlich bietet `sage` die Möglichkeit, die Weil-Paarung direkt zu berechnen. Der Algorithmus dort benutzt für $P \neq Q$ genau die Darstellung aus Proposition 6.5.

7 Elliptic Curve Cryptography (ECC)

7.1 Public-Key-Kryptographie

Man kann sich in vielen Quellen (z.B. [**?**], [**?**]) sehr ausführlich über die allgemeinen Grundzüge von Public-Key-Kryptographie informieren, daher möchten wir diese Grundidee nach Diffie und Hellman nur kurz skizzieren:

Gegeben eine Menge M und eine Familie von bijektiven Funktionen $f_K : M \to M$, wobei K ein beliebiger Parameter sei, mit folgenden Eigenschaften:

Eigenschaft 1. Ist K bekannt, so lässt sich $f_K(x)$ $\forall x \in M$ schnell berechnen.

Eigenschaft 2. Ist K bekannt, so lässt sich $f_K(y)^{-1}$ $\forall y \in M$ nur sehr schwer, d.h. mit schlechter Laufzeit, berechnen.

Eigenschaft 3. Es lassen sich Paare (K, K') konstruieren, so dass $f_{K'} = f_K^{-1}$, wobei K' allein aus Kenntnis von K nur sehr schwer zu berechnen ist.

Möchte nun Alice an Bob eine Nachricht, d.h. $x \in M$, sicher schicken, so gehen beide wie folgt vor:

(1) Alice wählt f_{K_B} und $f_{K'_B}$ mit $f_{K'_B} = f_{K_B}^{-1}$.

(2) Bob gibt Alice seinen *public key* f_{K_B} und hält aber seinen *private key* $f_{K'_B}$ geheim.

(3) Alice berechnet $y = f_{K_B}(x)$ und schickt y (über einen möglicherweise unsicheren Kommunikationsweg) an Bob.

(4) Bob berechnet $x = f_{K'_B}(y)$.

Es sollte klar sein, dass für einen beiderseitigen Nachrichtenaustausch Alice analog Funktionen wählen muss.

7.2 ECC

Am Spezialfall der ECC wollen wir nun die am häufigsten verwendeten Realisierungen der Grundidee der Public-Key-Kryptographie vorstellen. Eine kurze aber gute Übersicht findet man in [**?** , Chapter XI], an welcher wir uns im Folgenden auch orientieren werden. Darüber hinaus kann man dies sehr ausführlich in [**?** , Kapitel 2 und 5] oder [**?**] nachlesen.

ElGamal Public Key Kryptosystem 7.1. Auf folgendem Weg kann Alice sicher eine Nachricht an Bob senden:

	Alice	**Bob**
(1)	Alice und Bob einigen sich auf einen endlichen Körper $\mathbb{F}_q$, eine elliptische Kurve $E/\mathbb{F}_q$ und einen Punkt $P \in E(\mathbb{F}_q)$.	
(2)		Bob wählt (zufällig) eine ganze Zahl $b \in \mathbb{Z}^*$ und berechnet $B = bP \in E(\mathbb{F}_q)$.
(3)		Bob veröffentlicht seinen *public key* B. b ist Bobs *private key*.
(4)	Alice wandelt ihre Nachricht in einen Punkt auf $E(\mathbb{F}_q)$ um, d.h. ihr *plaintext* sei $M \in E(\mathbb{F}_q)$. Sie wählt (zufällig) eine ganze Zahl $k \in \mathbb{Z}^*$ und berechnet $A_1 = kP \in E(\mathbb{F}_q)$, $A_2 = M + kB \in E(\mathbb{F}_q)$.	
(5)	Alice sendet Bob den *ciphertext* (A_1, A_2) (über eine nicht zwingend sichere Leitung).	
(6)		Bob berechnet mit Hilfe seines private keys $A_2 - bA_1 \in E(\mathbb{F}_q)$. Dies entspricht Alice' Nachricht M.

Beweis der Korrektheit des ElGamal Public Key Kryptosystems. Es ist

$$A_2 - bA_1 \;=\; M + kB - b(kP) \;=\; M + kbP - bkP \;=\; M\,.$$

□

Will Eve (ein Angreifer) den plaintext M ohne Kenntnis der zufällig gewählten Zahl k berechnen, muss sie das folgende Problem lösen:

Elliptic Curve Diffie-Hellman Problem (ECDHP) 7.2. Sei $E/\mathbb{F}_q$ eine elliptische Kurve und seien $P, aP, bP \in E(\mathbb{F}_q)$ für gewisse (unbekannte) $a, b \in \mathbb{Z}$. Berechne $abP \in E(\mathbb{F}_q)$.

Zum jetzigen Zeitpunkt ist kein Verfahren bekannt, um dieses Problem zu lösen, ohne eine der ganzen Zahlen a oder b (es reicht offensichtlich eine) zu berechnen ([**?** , Remark XI.4.3.4.]). Dieses Problem hat ebenfalls einen eigenen Namen:

Diskretes-Logarithmus-Problem auf elliptischen Kurven (ECDLP) 7.3. Sei E/K eine elliptische Kurve und seien $P, aP \in E(K)$ für eine (unbekannte) ganze Zahl $a \in \mathbb{Z}$. Berechne a.

Oder in seiner allgemeinen Form:

Diskretes-Logarithmus-Problem (DLP) 7.4. Gegeben eine Gruppe G und $x, y \in G$. Berechne $m \in \mathbb{Z}$, sodass $x^m = y$.

Bemerkung 7.5. Nach [**?** , Kapitel 2.3] ist kein Verfahren bekannt, das ECDLP polynomiell auf ECDHP reduziert, d.h. das bei bekannter Lösung von ECDHP auch ECDLP löst.

8 Algorithmen für das (EC)DLP und deren Komplexität

Algorithmus 8.1 (Naiver Algorithmus)**.** *Sei G eine Gruppe der Ordnung N. Dann ist ein* naiver Algorithmus *für das DLP durch „Probieren“ gegeben, d.h. durch das Berechnen von $x, x^2, x^3, \ldots$, solange bis m gefunden wird mit $x^m = y$.*
Die Komplexität der Berechnungen liegt bei $\mathcal{O}(N)$ und der benötigte Speicherplatz bei $\mathcal{O}(1)$.

Bemerkung 8.2. Wir wollen hier nicht näher auf die $\mathcal{O}$-Notation eingehen. Eine kurze Einführung findet sich beispielsweise in [**?** , Kapitel 2.6].

Bemerkung 8.3. Im Folgenden werden wir oft von der Komplexität von *Berechnungen* und *Speicherplatz* sprechen. Eine Berechnung bezieht sich auf eine Gruppenoperation und eine „Einheit“ Speicherplatz bezieht sich auf ein Gruppenelement.

8.1 Pollards ρ-Algorithmus

Es gibt, wie wir im Folgenden sehen werden, bedeutend effizientere Algorithmen als den naiven. Einer davon ist Pollards ρ-Algorithmus [**?**]. Seine Laufzeit liegt nach [**?**] bei $\mathcal{O}(\sqrt{N})$, wobei N die Gruppenordnung bezeichne. Dies ist auch schon die zur Zeit beste bekannte Laufzeit für das DLP in einer allgemeinen Gruppe, insbesondere auch für das ECDLP. Wir wollen diesen Algorithmus lediglich vorstellen, falls die Gruppenordnung prim ist, da dies in kryptographischen Anwendungen in der Regel immer erfüllt ist.

Algorithmus 8.4 (Pollards ρ-Algorithmus)**.** *Sei G eine Gruppe der Ordnung p, p prim.*

Pollards ρ-Algorithmus

Input: $1 \neq x, y \in G$.
Output: $m \in \mathbb{N}$ mit $x^m = y$.

```
1  Teile G in drei disjunkte, etwa gleich große Teilmengen A, B, C;
2  z := 1;
3  w := 1;
4  do
5      if z ∈ A then
6          α := α + 1 mod p;
7          z := xz;
8      else if z ∈ B then
9          α := 2α mod p;
10         β := 2β mod p;
11         z := z^2;
12     else if z ∈ C then
13         β := β + 1 mod p;
```

```
14        z := yz;
15    endif;
16
17    for i from 0 to 1 do
18        if w ∈ A then
19            γ := γ + 1 mod p;
20            w := xw;
21        else if w ∈ B then
22            γ := 2γ mod p;
23            δ := 2δ mod p;
24            w := w^2;
25        else if w ∈ C then
26            δ := δ + 1 mod p;
27            w := yw;
28        endif;
29    endfor;
30 while z ≠ w;
31
32 r := α − γ;
33 s := δ − β;
34 d := ggT(s, p);
35 if d = 1 then
36    m := rs^{-1} mod p;
37    return m;
38 else
39    //Algorithmus hat fehlgeschlagen
40    Teile G erneut in andere A, B, C auf;
41    Gehe zu Zeile 2;
42 endif;
```

Bemerkung 8.5. Der Algorithmus basiert auf folgender Tatsache: Sei S eine endliche Menge mit $\#S = N$ und $f : S \to S$ eine Abbildung. Weiter sei $x_0 \in S$ und wir nehmen an, dass f^i (also die i-fache Hintereinanderausführung von f) für $i \geq 0$ die Elemente von S „gut durchmischt“. Dann erhalten wir für die Folge $(f^i(x_0))_{i\geq 0}$ zunächst verschiedene Werte, die sich nie mehr wiederholen, und ab einer gewissen Iteration eine Schleife bestimmter Länge. Stellt man dies graphisch dar, so erkennt man sofort, wie Pollards Algorithmus zu dem Beinamen ρ gekommen ist.

Bemerkung 8.6. Sei die Notation wie in Algorithmus 8.4. Pollard schlug in [**?**] vor, G in drei disjunkte Mengen A, B, C aufzuteilen und als Misch-Funktion die folgende zu verwenden:

$$f(z) := \begin{cases} xz & z \in A, \\ z^2 & z \in B, \\ yz & z \in C. \end{cases}$$

Wir starten mit $z_0 = 1$ und betrachten die Folge (z_i, w_i), wobei $z_i = f(z_{i-1})$ und $w_i = z_{2i}$. Des Weiteren speichern wir jeweils die Exponten, d.h. $z_i = x^{\alpha_i} y^{\beta_i}$. Diese lassen sich mit folgender Rekursion berechnen:

$$\alpha_{i+1} = \begin{cases} \alpha_i + 1 \mod p & z \in A, \\ 2\alpha_i \mod p & z \in B, \\ \alpha_i & z \in C, \end{cases} \qquad \beta_{i+1} = \begin{cases} \beta_i & z \in A, \\ 2\beta_i \mod p & z \in B, \\ \beta_i + 1 \mod p & z \in C, \end{cases} \tag{8.1}$$

Genauso können wir die Indizes γ_i und δ_i für $w_i = x^{\gamma_i} y^{\delta_i}$ berechnen, indem wir die Formel aus Gleichung (8.1) einmal für w_i benutzen und ein zweites mal für w_{i+1}.

Um wieder zurück zum eigentlichen Thema zu kommen, adaptieren wir Pollards ρ-Algorithmus an einem Beispiel auf eine elliptische Kurve.

Beispiel 8.7. Sei $E/\mathbb{F}_{79}$ gegeben durch:

$$y^2 \;=\; x^3 + x + 3\,.$$

Wir nehmen zwei Punkte $P = (26, 64)$, $Q = (65, 57)$ aus $E(\mathbb{F}_{79})[7]$. Weiter finden wir heraus, dass $\#E(\mathbb{F}_{79})[7] = 7$. Wir erinnern uns kurz daran, dass die Torsionspunkte einer bestimmten Ordnung immer eine Untergruppe der additiven Gruppe der elliptischen Kurve sind und so können wir problemlos Pollards Algorithmus anwenden.
In der Praxis bietet es sich an, die Unterteilung der Gruppe in drei disjunkte Teilmengen durch

$$x(P) \bmod 3 \;\in\; \{0, 1, 2\}$$

für einen Punkt $P \in E(K)[N]$ zu vollziehen. Wie man sich vorstellen kann, lässt sich dies auf eine Unterteilung in beliebig viele disjunkte Teilmengen erweitern, was man beispielsweise in [**?** , Abschnitt 5.2.2] nachlesen kann.
Umformuliert auf die additive Gruppe einer elliptischen Kurve suchen wir also $m \in \mathbb{N}^*$ mit

$$mP \;=\; Q\,.$$

Wir benutzen wieder `sage` mit Algorithmus A.1 und erhalten:

```
Finde Lösung des ECDLP m*x = y für x = (26 : 64 : 1) , y = (65 : 57 : 1)
Iteration  0
z =  (26 : 64 : 1)  with [a,b] =  [1, 0]
w =  (26 : 15 : 1)  with [c,d] =  [1, 1]
Iteration  1
z =  (26 : 15 : 1)  with [a,b] =  [1, 1]
w =  (26 : 64 : 1)  with [c,d] =  [2, 4]
Iteration  2
z =  (13 : 78 : 1)  with [a,b] =  [1, 2]
w =  (13 : 78 : 1)  with [c,d] =  [2, 6]
Kollision gefunden!
ggT(d-b,n) =  1
Lösung gefunden: m =  5
```

In der Tat ist $5P = Q$ und wir haben die Lösung nach $3 = \lceil\sqrt{7}\rceil$ Schritten gefunden.

8.2 Die Index-Calculus Methode

Die Index-Calculus Methode ist zur Zeit die beste bekannte Möglichkeit, um das DLP zu lösen. Wie wir sehen werden, hat die Index-Calculus Methode eine subexponentielle Laufzeit. Ihr Nachteil ist jedoch, dass sie nicht auf beliebige Gruppen adaptierbar ist. Die Grundidee basiert darauf,

dass „ein großer Teil“ aller Gruppenelemente durch Produkte (für eine multiplikativ geschriebene Gruppe) von Elementen einer kleinen Menge geschrieben werden können. In $\mathbb{F}_p^* = \mathbb{Z}_p^*$ für p prim, sind dies gerade diejenigen Elemente, in deren Primfaktorzerlegung nur Primzahlen bis zu einer gewissen Größe vorkommen.

Verständlicherweise lässt sich dies nicht auf alle Gruppen übertragen. In der multiplikativen Gruppe von endlichen Körpern jedoch finden wir derartige Zerlegungen (vgl. Bemerkung 8.14). Wir wollen dies hier aber nur für $\mathbb{F}_p^*$, p prim vorstellen.

Sei $p > 2$ eine Primzahl. Ein wesentlicher Unterschied zwischen einer beliebigen Gruppe und $\mathbb{F}_p^* = \mathbb{Z}_p^*$ ist die Tatsache, dass wir in $\mathbb{F}_p^*$ jede Zahl als Produkt ihrer Primfaktoren schreiben können.

Bevor wir den Algorithmus vorstellen, eine kleine Vokabel:

Definition 8.8 (B-glatt)**.** Eine Zahl $n \in \mathbb{Z}$ heißt *B-glatt*, für $B \in \mathbb{N}$ falls in ihrer Primfaktorzerlegung

$$n = \prod_{i=0}^{l} p_i^{k_i}$$

nur Primfaktoren $\leq B$ vorkommen, also gilt:

$$p_i \leq B \quad \forall i = 0, \ldots, l\,.$$

Algorithmus 8.9 (Die Index-Calculus-Methode)**.** *Seien $p > 2$ eine Primzahl und $g \in \mathbb{F}_p^*$ eine primitive Wurzel modulo p, d.h. ein Erzeuger von $\mathbb{F}_p^*$. Gesucht ist m mit $g^m \equiv h \pmod p$. Wir wollen im Folgenden auch schreiben $m = \log_g(h)$. Darüber hinaus bezeichne $\pi(B)$ die Anzahl der Primzahlen $\leq B$.*

Die Index-Calculus Methode

Input: p, g, h, $p > 2$ prim und g eine primitive Wurzel modulo p.
Output: $m \in \mathbb{N}$ mit $g^m = h$.

```
1  number_of_relations:= 0;
2  GL := leeres Gleichungsystem über Z_{p-1} mit Unbekannten log_g(l) für l ≤ B prim;
3  while number_of_relations ≤ π(B) do
4     Wähle i zufällig aus 1 ≤ i ≤ p − 1;
5     g_i :≡ g^i (mod p);
6     if g_i is B−glatt then
7        Zerlege g_i in Primfaktoren: g_i = ∏_{l≤B} l^{u_l};
8        if i ≡ Σ_{l≤B} u_l log_g(l) (mod p − 1) ist kein Vielfaches anderer Gleichungen in
             GL then
9           GL := GL ∪ i ≡ Σ_{l≤B} u_l log_g(l) (mod p − 1).
10       endif;
11    endif;
12 endwhile;
13
14 Löse GL;
15 //Ab jetzt sind alle log_g(l) für l ≤ B prim bekannt!
16
17 k := 1;
18 while true do
19    if hg^{−k} is B−glatt then
```

```
20          Zerlege hg^{-k} in Primfaktoren: hg^{-k} = ∏_{l≤B} l^{e_l};
21          return k + Σ_{l≤B} e_l log_g(l)
22      endif
23      k := k + 1;
24  endif;
```

Proposition 8.10. *Sei $p > 2$ prim und $g \in \mathbb{F}_p$. Dann berechnet die Index-Calculus Methode in Algorithmus 8.9 korrekt den diskreten Logarithmus $\log_g(h)$ für $h \in \mathbb{F}_p$ mit einer probabilistisch subexponentiellen Laufzeit von $\mathcal{O}(\exp(c\sqrt{(\ln p)(\ln\ln p)}))$, wobei $c > 0$ eine Konstante ist, falls B „sinnvoll“ gewählt wird (vgl. Bemerkung 8.13).*

Beweis. **Zur Laufzeit.** Die Laufzeitanalyse basiert auf dem Auffinden von B-glatten Relationen, was hier wiederum nicht ausführen werden soll – stattdessen soll auf [**?** , Note 3.71] verwiesen sein. Eine Übersicht über verschiedene Varianten und deren Laufzeiten findet man mit weiteren Referenzen in [**?** , § 3.12 Abschnitt „§ 3.6“].

Zur Korrektheit. Die Grundidee der Index-Calculus-Methode besteht darin, $\log_g(l)$ für kleine Primzahlen l zu berechnen. Denn findet man $k \in \mathbb{N}$, sodass hg^{-k} B-glatt ist, also

$$hg^{-k} \equiv \prod_{\substack{l \le B \\ l \text{ prim}}} l^{e_l} \pmod{p},$$

so haben wir

$$\log_g(h) \equiv k + \sum_{\substack{l \le B \\ l \text{ prim}}} e_l \log_g(l) \pmod{p-1}.$$

Wie man sich leicht überlegt, werden – genau wie bei seinem kontinuierlichen Pendant über $\mathbb{R}$ oder $\mathbb{C}$ – aus Produkten im Argument des diskreten Logarithmus Summen von diskreten Logarithmen. Darüber hinaus muss man beachten, dass $\log_g : \mathbb{F}_p^* \to \mathbb{Z}_{p-1}$, da $\operatorname{ord}(g) = p-1$.

Nun gilt es also nur noch $\log_g(l)$ für $l \le B$, l prim zu berechnen. Dazu betreiben wir, wie in Algorithmus 8.9 beschrieben, lineare Algebra und suchen B-glatte g_is der Form

$$g_i \equiv g^i \equiv \prod_{\substack{l \le B \\ l \text{ prim}}} l^{u_{l_i}} \pmod{p}.$$

Dann ist

$$i \equiv \sum_{\substack{l \le B \\ l \text{ prim}}} u_{l_i} \log_g(l) \pmod{p-1}.$$

Haben wir genügend gefunden, d.h. mehr als $\pi(B)$ Stück, können wir das Gleichungssystem über $\mathbb{Z}_{p-1}$, durch elementare Zeilenumformungen lösen. Alternativ können wir mit Hilfe des Chinesischen Restsatzes das Gleichungssystem in (Anzahl der Primfaktoren von $p-1$ ohne Vielfachheit)-viele Gleichungssysteme zerlegen, diese mit dem Gaußschen Eliminationsverfahren auf Stufenform bringen, lösen und die Lösungen kombinieren. [**?** , Remark 3.56] beschreibt dies etwas genauer. □

Bemerkung 8.11. Man nennt die Primzahlen $\{2, 3, \ldots, p_i\}$ mit $p_i \le B$ auch *Faktorbasis* für die Index-Calculus Methode.

Beispiel 8.12. Seien $p = 733$ und $g = 7$. 7 ist in der Tat eine primitive Wurzel modulo 733. Wir wollen $\log_7(20)$ berechnen und wählen dazu zunächst $B = 5$. Wir finden ein paar (wir brauchen mindestens $3 = \pi(5)$) B-glatte Relationen:

$$\begin{aligned} 7^{107} &\equiv 2^1\,3^2\,5^2 && \pmod{733}\,, \\ 7^{322} &\equiv \quad 3^1\,5^2 && \pmod{733}\,, \\ 7^{531} &\equiv \qquad 5^1 && \pmod{733}\,. \end{aligned}$$

Damit bekommen wir ein Gleichungssystem, das wir in Matrixform auf Stufenform bringen:

$$\begin{pmatrix} 1 & 2 & 2 & 107 \\ 0 & 1 & 2 & 322 \\ 0 & 0 & 1 & 531 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 & 107 \\ 0 & 1 & 1 & 523 \\ 0 & 0 & 1 & 531 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 525 \\ 0 & 1 & 0 & 724 \\ 0 & 0 & 1 & 531 \end{pmatrix}.$$

Damit können wir folgern, dass $\log_7(2) = 525$, $\log_7(3) = 724$, $\log_7(5) = 531$.
Wir finden auch

$$20 \cdot 7^{-2} \;\equiv\; 150 \;=\; 2^1\,3^1\,5^2 \pmod{733}$$

und können damit das Ergebnis berechnen:

$$\log_7(20) \;\equiv\; 2 + \Big(1\log_7(2) + 1\log_7(3) + 2\log_7(3)\Big) \;\equiv\; 117 \pmod{732}\,.$$

In der Tat können wir überprüfen, dass $7^{117} \equiv 20 \pmod{733}$.

Bemerkung 8.13. Natürlich hängt das Auffinden der Relation von der Verteilung B-glatter Zahlen im Intervall $[1, p-1]$ ab. Klar ist jedoch: Wählt man B zu klein, finden sich nur wenige; wählt man B zu groß, muss man umso mehr Gleichungen erzeugen. Daher benutzt man heutzutage eher eine Variante, das sog. Zahlkörpersieb, welches eine etwas bessere Laufzeit hat.

Bemerkung 8.14. Wie eingangs erwähnt, kann man dieses Verfahren auf $\mathbb{F}_{p^n}$ für p prim und $n \in \mathbb{N}$ erweitern, indem man

$$\mathbb{F}_{p^n} \;\cong\; \mathbb{F}_p[X]/(f)$$

mit $f \in \mathbb{F}_p[X]$ irreduzibel, $\deg f = n$ benutzt und sich eine Menge aus irreduziblen Polynomen kleinen Grades als Faktorbasis wählt. Verglichen mit Pollards ρ-Algorithmus ist dies ungleich besser, aber nicht erweiterbar auf das ECDLP. Dies lässt das DLP in $\mathbb{F}_{p^n}$ verglichen mit dem ECDLP „leichter“ erscheinen, was auch des Pudels Kern des MOV-Algorithmus im nächsten Kapitel sein wird.

9 Der MOV-Angriff

9.1 Reduktion des ECDLP auf das DLP in einem endlichen Körper

? [**?**] veröffentlichten **?** einen Artikel, wie man mit Hilfe der Weil-Paarung das ECDLP auf ein – möglicherweise einfacheres – DLP in einem endlichen Körper zurückführen kann. Dies möchten wir im Folgenden nachvollziehen, wobei wir uns erneut an [**?** , Abschnitt XI.6] orientieren.

Definition 9.1 (Einbettungsgrad)**.** Sei $\mathbb{F}_q$ ein endlicher Körper und $N \in \mathbb{N}^*$. Der *Einbettungsgrad von N in $\mathbb{F}_q$* ist die kleinste ganze Zahl $d \geq 1$, sodass

$$\mu_N \subset \mathbb{F}_{q^d}^* .$$

Da $\mathbb{F}_{q^d}^*$ eine zyklische Gruppe der Ordnung $q^d - 1$ ist, lässt sich äquivalent fordern, dass d die kleinste ganze Zahl mit

$$q^d \equiv 1 \pmod{N}$$

ist.

Lemma 9.2. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und $N \in \mathbb{N}^*$ mit* $\mathrm{ggT}(q-1, N) = 1$. *Sei weiter d der Einbettungsgrad von N in $\mathbb{F}_q$ und angenommen es gibt einen Punkt in $E(\mathbb{F}_q)$ der Ordnung N. Dann ist*

$$E[N] \subset E(\mathbb{F}_{q^d}) .$$

Beweis. Sei $P \in E(\mathbb{F}_q)$ mit $\operatorname{ord} P = N$ und $\phi_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ der Frobenius-Endomorphismus zu q. Sei weiter $T \in E[N]$, sodass $E[N] = \langle T, P \rangle$. Dann haben wir

$$P^{\phi_q} = P, \qquad T^{\phi_q} = aP + bT ,$$

für geeignete $a, b \in \mathbb{Z}_N$. Mit den Eigenschaften der Weil-Paarung (Proposition 4.5) haben wir

$$e_N(P,T)^q = e_N(P,T)^{\phi_q} = e_N(P^{\phi_q}, T^{\phi_q}) = e_N(P, aP + bT) = e_N(P,P)^a e_N(P,T)^b = e_N(P,T)^b .$$

Da P, T Erzeuger von $E[N]$ sind, ist $e_N(P,T)$ eine primitive N-te Einheitswurzel (vgl. Korollar 4.6), es folgt

$$b \equiv q \mod N$$

und wir können schreiben $T^{\phi_q} = aP + qT$. Betrachten wir nun

$$T^{\phi_q{}^d} = (a(1 + q + q^2 + \cdots + q^{d-1}))P + q^d T.$$

Da $T \in E[N]$ und nach Definition des Einbettungsgrades $q^d \equiv 1 \pmod{N}$, ist $q^d T = T$. Ferner gilt

$$\sum_{i=0}^{d-1} q^i \;\equiv\; 0 \pmod{N},$$

da $\mathrm{ggT}(q-1, N) = 1$ ist, und wir haben schließlich $T^{\phi_{q^d}} = 0P + T = T$, was $T \in E(\mathbb{F}_{q^d})$ zeigt. □

Algorithmus 9.3 (Der MOV-Algorithmus). *Sei $E/\mathbb{F}_q$ eine elliptische Kurve.*

MOV-Algorithmus

Input: $P, Q \in E(\mathbb{F}_q)$ von Ordnung N, N prim, mit $\mathrm{ggT}(q-1, N) = 1$ und d, den Einbettungsgrad von N in $\mathbb{F}_q$.
Output: Ein DLP $\alpha = \beta^m$ in $\mathbb{F}_{q^d}^*$, sodass $Q = \log_\beta(\alpha)\, P$.

1 Finde $T \in E[N] \subset E(\mathbb{F}_{q^d})$, sodass $E[N] = \langle T, P \rangle$;
2 Berechne $\alpha := e_N(Q, T)$;
3 Berechne $\beta := e_N(P, T)$;
4 **return** das DLP $\alpha = \beta^m$ in $\mathbb{F}_{q^d}^*$;

Proposition 9.4. *Der MOV-Algorithmus reduziert das ECDLP für P und Q in probabilistisch polynomialer Zeit auf ein DLP in $\mathbb{F}_{q^d}^*$.*

Beweis. **Zur Korrektheit.** Seien $m \in \mathbb{Z}$ mit $Q = mP$ und $T \in E[N]$, sodass T und P $E[N]$ erzeugen. Dann ist nach Korollar 4.6 $e_N(T, P)$ eine primitive N-te Einheitswurzel, also in $\mathbb{F}_{q^d}$ und es gilt

$$e_N(Q, T) \;=\; e_N(mP, T) \;=\; e_N(P, T)^m .$$

Ist also $m = \log_{e_N(Q,T)}(e_N(P, T))$, so haben wir das ECDLP $Q = mP$ gelöst.

Zur Laufzeit. Die Berechnung der Weil-Paarung in den Schritten 2 und 3 lässt sich mit Millers Algorithmus (Algorithmus 6.2) und Proposition 6.5 in Linearzeit bewältigen. Einzig das Auffinden eines zweiten Erzeugers könnte Schwierigkeiten bereiten. Dazu berechnen wir zunächst $n = \#E(\mathbb{F}_{q^d})$ mit Algorithmus 5.14 in Polynomialzeit. Da

$$E[N] \cong \mathbb{Z}_N \times \mathbb{Z}_N \subset \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong E(\mathbb{F}_{q^d}),$$

Da N in der Regel eine große Primzahl ist, gibt es nur wenige Elemente deren Ordnung N nicht als Primfaktor enthält. Nehmen wir ein $g \in \mathbb{Z}_{n_i}$ mit $N \mid \mathrm{ord}(g)$, so hat $\frac{n_i}{N} g$ gerade Ordnung N. Damit haben wir gute Chancen, dass

$$T = \tfrac{n}{N^2} S$$

Ordnung N hat für beliebiges $S \in E(\mathbb{F}_{q^d})$. In der Tat lässt sich beweisen, dass nach polynomial vielen Versuchen ein Punkt der Ordnung N zu erwarten ist. □

Beispiel 9.5. Sei $q = p = 113$ und

$$E/\mathbb{F}_q : \; y^2 + xy \;=\; x^3 + 18x + 2 .$$

Des Weiteren seien $P = (38, 34)$ und $Q = (67, 38)$ zwei Punkte der Ordnung $N = 11$. Um die Punkte zu finden, habe ich die `sage`-Methode `randPointsOfOrder` (Algorithmus A.4) geschrieben.

Da wir bisher keine Möglichkeit kennen gelernt haben, den Einbettungsgrad effizient zu berechnen, probieren wir $d = 1, 2, \ldots$ bis $113^d \equiv 1 \pmod{11}$ (Algorithmus A.3 zeigt die `sage`-Umsetzung). Wir finden $d = 5$.

Nun können wir die bisherigen Ergebnisse in den MOV-Algorithmus (Algorithmus 9.3) geben, wobei wir – wie im Beweis zu Proposition 9.4 angemerkt – zufällig Punkte aus $E(\mathbb{F}_{113^5})$ wählen, um einen zweiten Erzeuger für $E[N]$ zu finden. Wir berechnen z.B. mit Schoofs Algorithmus (Algorithmus 5.14)

$$n \;=\; \#E(\mathbb{F}_{113^5}) \;=\; 18424131550\,.$$

Sei $\mathbb{F}_{113^5}$ erzeugt von a, so wählen wir

$$S \;=\; (59a^4 + 52a^3 + 98a^2 + 92a + 110, 34a^4 + 86a^3 + 59a^2 + 6a + 74,\,) \;\in E(\mathbb{F}_{113^5})$$

zufällig aus und berechnen

$$T \;=\; \tfrac{18424131550}{121} S \;=\; (59a^4 + 52a^3 + 37a^2 + 64a + 8, 42a^4 + 48a^3 + 65a^2 + 47a + 75)\,.$$

Weiter berechnen wir die Weil-Paarungen

$$\begin{aligned} \alpha \;&=\; e_N(Q, T) \;=\; 112a^4 + 18a^3 + 102a^2 + 9a + 19 \quad &\in \mathbb{F}_{113^5} \\ \beta \;&=\; e_N(P, T) \;=\; 59a^4 + 12a^3 + 54a^2 + 19a + 57 \quad &\in \mathbb{F}_{113^5} \end{aligned}$$

und lösen letztlich das DLP $\alpha = \beta^m$ in $\mathbb{F}_{113^5}^*$, beispielsweise mit Pollards ρ-Algorithmus (Algorithmus 8.4). Dies ergibt

$$m = 7\,.$$

In der Tat können wir verifizieren, dass $7P = Q$. Wiederum wurden alle Berechnungen in `sage` umgesetzt: Algorithmus A.5. Zur Vereinfachung löst diese Methode bereits das DLP in $\mathbb{F}_{q^d}^*$, was im eigentlichen MOV-Algorithmus ja nicht der Fall ist.

Bemerkung 9.6. In der Regel wächst der Einbettungsgrad d proportional zu N, also exponentiell in $\ln q$, d.h. ein DLP in $\mathbb{F}_{q^d}$ lässt sich zwar schneller lösen als ein ECDLP für eine elliptische Kurve über $\mathbb{F}_{q^d}$, doch müssen wir ja das ECDLP „nur“ für eine elliptische Kurve über $\mathbb{F}_q$ lösen! Das bedeutet, dass der MOV-Algorithmus in der Regel das Problem eher schwieriger macht, als leichter (siehe [**?** , Remark XI.6.3] für Referenzen zu einem Beweis des exponentiellen Wachstums).

9.2 Anwendung auf supersinguläre elliptische Kurven

Es gibt jedoch für gewisse elliptische Kurven einen Ausweg, der den MOV-Angriff interessant werden lässt.

Wiederum sei im Folgenden stets $q = p^n$ für eine Primzahl p und eine natürliche Zahl n.

Definition 9.7 (supersingulär)**.** Eine elliptische Kurve $E/\mathbb{F}_q$ heißt *supersingulär*, falls gilt

$$E[p] \;=\; \{O\}\,.$$

Proposition 9.8. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und $\#E(\mathbb{F}_q) = q+1-a_q$ wie in Proposition 5.4. E ist supersingulär nach Definition 9.7 genau dann, wenn*

$$a_q \equiv 0 \pmod{p}.$$

Beweis. [**?** , Proposition 4.31]. □

Proposition 9.9. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und $a_q = q + 1 - \#E(\mathbb{F}_q) = 0$. Sei weiter $N \in \mathbb{N}^*$. Falls ein Punkt $P \in E(\mathbb{F}_q)$ existiert mit* $\operatorname{ord} P = N$*, so gilt*

$$E[N] \subseteq E(\mathbb{F}_{q^2}).$$

Beweis. Wir haben $\#E(\mathbb{F}_q) = q+1$. Die Existenz eines Punktes der Ordnung N impliziert somit $N \mid q+1$, also $-q \equiv 1 \pmod{N}$. Nach Proposition 5.4 gilt für den Frobenius-Endomorphismus ϕ_q zu q

$$\phi_q^2 - a_q\phi_q + q = 0.$$

In unserem Fall vereinfacht sich dies zu $\phi_q^2 = -q$. Sei nun $S \in E[N]$, so gilt

$$\phi_q^2(S) = -qS = S.$$

ϕ_q^2 können wir aber auch als ϕ_{q^2} auffassen und haben dann mit Proposition 5.3 $S \in E(\mathbb{F}_{q^2})$. □

Bemerkung 9.10. Für eine supersinguläre elliptische Kurve mit $a_q \neq 0$ ist der Einbettungsgrad gegebenenfalls größer, aber immernoch akzeptabel. Ausführlich wird dies in [**?**] diskutiert, wo man auch eine Übersicht über alle auftretenden Möglichkeiten findet. Wir beschränken uns hier aber auf die einfache Variante.

Algorithmus 9.11 (Der MOV-Algorithmus für supersinguläre Kurven.)**.** *Sei $E/\mathbb{F}_q$ eine supersinguläre elliptische Kurve mit $q = p^l$, p prim und $l \in \mathbb{N}^*$.*

MOV-Algorithmus-Supersingulär

Input: $P, Q \in E(\mathbb{F}_q)$ von Ordnung N, N prim, mit $\mathrm{ggT}(q-1, N) = 1$
Output: Ein DLP $\alpha = \beta^m$ in $\mathbb{F}_{q^2}^*$, sodass $Q = \log_\beta(\alpha)\, P$.

```
1  while true do
2     Berechne n = #E(F_{q^2});
3     Wähle S zufällig aus E(F_{q^2});
4     T := (n/N^2) S;
5     Berechne α := e_N(Q, T);
6     Berechne β := e_N(P, T);
7     if α ≠ 1 and β ≠ 1 then
8        return das DLP α = β^m in F*_{q^2};
9     endif;
10 endwhile;
```

Satz 9.12. *Algorithmus 9.11 reduziert das ECDLP einer supersingulären elliptischen Kurve über $\mathbb{F}_q$ korrekt in probabilistisch polynomialer Zeit auf ein DLP in $\mathbb{F}_{q^2}^*$.*

Beweis. Nach Proposition 9.9 kennen wir den Einbettungsgrad für gegebene Bedingungen. Alles Weitere wurde schon in Proposition 9.4 gezeigt. □

Beispiel 9.13. Betrachten wir

$$E/\mathbb{F}_{19}: \; y^2 \; = \; x^3 + 9x \,,$$

$N = 5$ und zwei Punkte

$$P = (11, 9), \quad Q = (4, 10) \; \in E(\mathbb{F}_{19})[5] \,.$$

Wir wählen wieder a als Erzeuger von $\mathbb{F}_{19^2}$ und versuchen unser Glück mit

$$T \; = \; \tfrac{400}{25}(10a + 1, 4a + 11) \; = \; (18a + 10, 7a + 16) \,.$$

Mit Millers Algorithmus (Algorithmus 6.2) berechnen wir

$$\begin{aligned} \alpha \; &= \; e_5(Q, T) = 15a + 9 \quad \in \mathbb{F}_{19^2} \,, \\ \beta \; &= \; e_5(P, T) \; = a + 11 \quad\;\; \in \mathbb{F}_{19^2} \,. \end{aligned}$$

Schließlich lösen wir $\log_\alpha(\beta) = 3$ in subexponentieller Laufzeit mit der Index-Calculus Methode aus Abschnitt 8.2 und können in der Tat feststellen, dass $Q = 3P$.

Bemerkung 9.14. Man könnte in Algorithmus 9.11 die Suche nach dem Punkt T vereinfachen. Nach [**?** , Table 1] ist

$$E(\mathbb{F}_{q^2}) \cong \mathbb{Z}_{q+1} \times \mathbb{Z}_{q+1} \,,$$

falls $\#E(\mathbb{F}_q) = q + 1$. So bräuchte man nicht erst die Kardinalität von $E(\mathbb{F}_{q^2})$ berechnen und könnte Zeile 4 umschreiben zu

$$T \; := \; \frac{q+1}{N} S \,.$$

10 Fazit / Ausblicke

Resümieren wir einmal kurz den Inhalt der Arbeit: Wir haben begonnen den Begriff elliptische Kurve auf ein algebraisch untermauertes Fundament zu stellen, wozu wir ein paar Begriffe aus der algebraischen Geometrie brauchten. Anschließend führten wir das Konzept der Divisoren ein, um mit ihrer Hilfe die Verbindung zu schlagen zwischen dem geometrischen Konzept der Addition von Punkten auf elliptischen Kurven und der algebraischen Addition, welche durch die spezielle Darstellungsmöglichkeit von Divisoren auf elliptischen Kurven daherkommt.

Danach haben wir den Kern dieser Arbeit kennen gelernt: Die Weil-Paarung. Die Idee, mit ihrer Hilfe das ECDLP auf ein DLP über einem endlichen Körper zurückzuführen, sollte die weiteren Abschnitte motivieren: Spezielle Eigenschaften elliptischer Kurven über endlichen Körpern, die konkrete Berechnung der Weil-Paarung nach Miller, ein Ausflug in die Elliptic Curve Cryptography und schließlich Algorithmen zum (EC)DLP, wo wir klar gesehen haben, dass die diskrete Logarithmenberechnung in endlichen Körpern weitaus effektiver gestaltet werden kann.

Mit diesem Wissen haben wir abschließend den MOV-Algorithmus besprochen, um eben gerade diesen Vorteil für das ECDLP nutzbar zu machen – was supersinguläre elliptische Kurven unbrauchbar für die Kryptographie macht. Eine Tatsache, die man vor 1993 sicherlich noch nicht berücksichtigt hätte.

Ein Aspekt von Paarungen, den wir hier nicht angesprochen haben, ist die Konstruktion von Kryptosystemen, mit deren Hilfe man zwischen *drei* Parteien Daten sicher austauschen kann. Dies findet man beispielsweise in [**?** , Section 9.6]. Ebenso lassen sich Dokumente mit Hilfe der Weil-Paarung signieren, was z.B. kurz in [**?** , Theorem XI.7.4] beschrieben wird.

Die Weil-Paarung ist jedoch nicht die einzige Paarung, welche interessante Eigenschaften hat. Neben ihr bietet die *Tate-Lichtenbaum-Paarung* (welche über die Weil-Paarung definiert wird) eine Möglichkeit, unter anderen Voraussetzungen – insbesondere kann man auf die Supersingularität verzichten – das ECDLP in ein DLP über einem endlichen Körper zu transferieren. Dies ist unter dem Namen *Frey-Rück-Angriff* bekannt und z.B. in [**?** , Section 5.3.2] beschrieben.

Darüber hinaus gibt es bis heute keine Algorithmen subexponentieller Laufzeit, um das ECDLP im allgemeinen Fall zu lösen, wobei die Forschungen dazu noch nicht aufgegeben wurden (siehe z.B. [**?** , Section 5.5] für einen kurzen Überblick). Dies macht elliptische Kurven in der kryptographischen Anwendung immernoch attraktiv. Beispielsweise dauerte das Lösen eines ECDLPs über $\mathbb{F}_p$ mit p einer 112-bit Primzahl in einem Versuch 2009 etwa 3.5 Monate (siehe [**?**]). In $\mathbb{F}_q^*$ mit $q = 2^{613}$ dagegen löste man 2005 ein DLP in 17 Tagen (siehe [**?**]). Die beiden Berechnungen wurden zwar nicht auf vergleichbaren Systemen durchgeführt, zeigen aber klar, dass es in Zukunft weiter nach effizienteren Algorithmen zur Berechnung von diskreten Logarithmen auf elliptischen Kurven zu suchen gilt.

A Quellcodes

Algorithmus A.1 (Pollards ρ-Algorithmus für Beispiel 8.7)**.**

```
1  def pollard(x,y):
2     print "Finde Lösung des ECDLP m*x = y für x =",x,", y =",y
3     n = x.order();
4     a=0;
5     b=0;
6     z=E[0];
7     c=0;
8     d=0;
9     w=E[0];
10    for i in range(0,50):
11        print "Iteration ",i
12        [a,b] = nextIndices(z,a,b,n);
13        z = f(z,x,y);
14        print "z = ",z," with [a,b] = ",[a,b]
15
16        [c,d] = nextIndices(w,c,d,n);
17        w = f(w,x,y);
18        [c,d] = nextIndices(w,c,d,n);
19        w = f(w,x,y);
20
21        print "w = ",w," with [c,d] = ",[c,d]
22
23        if z == w:
24            print "Kollision gefunden!"
25            ggT = gcd(Integer(d-b),n);
26            print "ggT(d-b,n) = ", ggT
27            if ggT == n:
28                print "ERROR!"
29            else:
30                print "m = ", Mod((a-c)/(d-b),n)
31            break;
32
33 def f(P,x,y):
34     m  = Integer(P[0])%3;
35     if m == 0:
36         return P+x;
37     if m == 1:
38         return 2*P;
39     if m == 2:
40         return P+y;
41 def nextIndices(P,a,b,n):
42     m  = Integer(P[0])%3;
43     if m == 0:
44         return [(a+1)%n,b%n];
```

```
45      if m == 1:
46          return [(2*a)%n,(2*b)%n];
47      if m == 2:
48          return [a%n,(b+1)%n];
```

Algorithmus A.2 (Idee zu Schoofs-Algorithmus für Beispiel 5.5).

```
1  def schoof(E,q):
2      l = 0;
3      A = 1;
4      while A < 4*sqrt(q):
5          l = next_prime(l);
6          lTorsionPoints = E(0).division_points(l);
7          torsionCount = len(lTorsionPoints);
8          if torsionCount == 1: continue;
9          A = A*l;
10         found = false;
11         for j in range(1,torsionCount):
12             if found: break;
13             P = lTorsionPoints[j];
14             for i in range(l-1):
15                 if found: break;
16                 tmp = E(P[0]^(q^2), P[1]^(q^2)) - i*E(P[0]^q, P[1]^q) + q*P;
17                 if tmp == E(0):
18                     print "prime l=",l, " n_l = ",i, " P = ",P;
19                     found = true;
```

Algorithmus A.3 (Algorithmus zum Auffinden von Punkten gegebener Ordnung. Vgl. Beispiel 9.5).

```
1  # finds random points P,Q with order N (N prime) on Ecurve
2  # Q is a multiple of P
3  def randPointsOfOrder(Ecurve, N):
4      gens = Ecurve.gens();
5      P = gens[0];
6      n = P.order()
7      if n >= N: P = int(n/gcd(n,N))*P;
8      else:
9          Q = gens[1];
10         n = Q.order();
11         P = int(n/gcd(n,N))*Q;
12     return P, randint(1,N-1)*P
```

Algorithmus A.4 (Algorithmus zum Auffinden des Einbettungsgrades. Vgl. Beispiel 9.5).

```
1  def embeddingDegree(N,q):
2      for d in range(1,N+1):
3          if Mod(q^d,N) == 1:
4              return d;
5      print "embedding degree not found for N=",N, " , q = ",q
6      raise ValueError;
```

Algorithmus A.5 (MOV-Algorithmus. Vgl. Beispiel 9.5).

```
1  def mov_alg(Ecurve, q, P, Q, N, d, info=False):
2      #trivial cases
3      if Q.is_zero():
4          if info: print "trivial case: Q == O";
5          return 0;
6      if P == Q:
7          if info: print "trivial case: Q == P";
8          return 1;
9      #x(P) = x(Q) iff P = -Q
10     if P[0] == Q[0]:
11         if info: print "trivial case: Q == -P";
12         return N-1;
13     #change Field
14     Ecurve_changed = Ecurve.change_ring(GF(q^d,'a'));
15     n = Ecurve_changed.cardinality();
16     if info: print "Ecurve_changed has cardinality n = ", n
17     while True:
18         #find other point of order N
19         S = Ecurve_changed.random_point();
20         T = int(n/N^2)*S;
21         if info: print "try point T = ", T, ", which is ",n,"/",N^2,"*",S;
22         #compute weil-pairings
23         alpha = Ecurve_changed(Q).weil_pairing(T,N);
24         beta = Ecurve_changed(P).weil_pairing(T,N);
25         if info: print "weil-pairings computed: e_N(Q,T) = ", alpha, " e_N(P,T) =
             ", beta;
26         #compute log in F_(q^d)
27         k = alpha.log(beta);
28         if info: print "alpha.log(beta) = ", k;
29         #check if all is good. If not, T had order less than N, so try again.
30         if Q == k*P: return k;
```