# Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei

Dissertation
zur Erlangung des Grades
des Doktors der Naturwissenschaften
der Technischen Fakultät
der Universität des Saarlandes
von

**Volker Müller**

Saarbrücken
1995

| | |
|---|---|
| Tag des Kolloquiums: | 18. Mai 1995 |
| Dekan: | Prof. Dr. H. Bley |
| Berichterstatter: | Prof. Dr. J. Buchmann |
| | Prof. Dr. K. Mehlhorn |

An dieser Stelle möchte ich Herrn Professor Buchmann herzlich dafür danken, daß ich an seinem Lehrstuhl diese Arbeit erstellen durfte. Er nahm sich stets die Zeit, meine Arbeit durch Ratschläge, Diskussionen und Verbesserungsvorschläge zu unterstützen. Insbesondere ermöglichte er mir auch einen Besuch bei Herrn Professor Oliver Atkin an der University of Illinois at Chicago.

Herr Professor Atkin hat mir sehr bei dem Verstehen der Theorie des Algorithmus geholfen. Außerdem hatten wir sehr fruchtbare Diskussionen um praktische Probleme, die bei der Implementierung des Algorithmus auftreten. Ich danke ihm herzlich für sein Engagement und seine Hilfe.

Herrn Professor Mehlhorn bin ich für sein Interesse an meiner Arbeit sehr dankbar.

Besonders herzlich danke ich meinen Kollegen Frank Lehmann, Markus Maurer und Victor Shoup. Mit Frank Lehmann und Markus Maurer hatte ich während der Implementierung des Algorithmus viele anregende Diskussionen. Viele praktischen Probleme konnten mit ihrer Hilfe gelöst werden. So ist ein sehr effizientes Programm zur Lösung des vorgegebenen Problems für große endliche Primkörper entstanden. Victor Shoup stellte uns dabei ein sehr effizientes Programmpaket zur Arithmetik und Faktorisierung von Polynomen zur Verfügung und gab sehr viele Hinweise zur Implementierung.

Besonders dankbar bin ich auch meinen Eltern, meinem Bruder und meinem Freundeskreis. Meine Eltern und mein Bruder haben mich während meines Studiums stets tatkräftig unterstützt. Meine lieben Freundinnen und Freunde Franz-Dieter Berger, Ingrid Biehl, Thomas Denny, Bernd Meyer, Ralf Roth, Erik Schank, Christoph Thiel und Jörg Zayer hatten stets Zeit für Diskussionen und motivierende Gespräche.

Letztendlich möchte ich mich auch sehr herzlich bei Christine Abel bedanken, die mir durch die stete Bereitschaft zu Diskussionen, durch viele konstruktive Vorschläge und nicht zuletzt durch ihr sorgfältiges Korrekturlesen sehr geholfen hat.

# Inhaltsverzeichnis

# Tabellenverzeichnis

# Kapitel 1

# Einführung

## 1.1 Einleitung

Gegenstand der vorliegenden Arbeit ist die Beschreibung eines Algorithmus zur Bestimmung der Punktanzahl einer elliptischen Kurve über einem endlichen Körper der Charakteristik größer als drei.

Die Gruppe der Punkte einer elliptischen Kurve über einem Körper $K$ ist die Menge aller Lösungen einer Gleichung der Form $y^2 = x^3 + ax + b$ über dem Körper $K$. Dabei sind beide Kurvenkoeffizienten $a$ und $b$ ebenfalls Elemente aus $K$. (Wir werden diese Begriffe in einem folgenden Kapitel noch genauer definieren.)

Das Problem der Bestimmung der Ordnung dieser Punktgruppe für endliche Körper hat in den letzten Jahren nicht nur für Zahlentheoretiker, sondern auch für Kryptographen große Bedeutung erlangt. In der Literatur wurden die Punktgruppen elliptischer Kurven über endlichen Körpern mehrmals zur Konstruktion von Public Key Kryptosystemen vorgeschlagen (siehe u.a. [Ko86] und [Mi86]). Die Sicherheit solcher Kryptosysteme basiert auf der Schwierigkeit des sogenannten diskreten Logarithmusproblems in der Punktgruppe einer elliptischen Kurve. Zur Lösung dieses Problems sind zur Zeit nur für spezielle elliptische Kurven (sogenannte supersinguläre Kurven) Algorithmen mit subexponentieller Laufzeit bekannt [Me93, Abschnitt 5]. Der beste Algorithmus zur Bestimmung diskreter Logarithmen für eine beliebige elliptische Kurve über einem endlichen Körper ist der Algorithmus von Pohlig und Hellman [PoHe78], dessen Komplexität proportional zu der Quadratwurzel des größten Primfaktors der Gruppenordnung der zugrundeliegenden elliptischen Kurve ist. Damit ist es eine notwendige Voraussetzung für die Sicherheit eines Public Key Kryptosystems basierend auf elliptischen Kurven, daß die Ordnung der Punktgruppe der Kurve mindestens einen „großen“ Primfaktor besitzt. Um diese Voraussetzung testen zu können, muß man in der Lage sein, diese Gruppenordnung zu berechnen.

Ein Algorithmus zur Bestimmung der Gruppenordnung einer elliptischen Kurve über einem endlichen Körper ist der Babystep-Giantstep Algorithmus von Shanks. Dies ist ein Algorithmus, der für jede endliche abelsche Gruppe benutzt werden kann, um die Gruppenordnung zu bestimmen (für den Fall elliptischer Kurven siehe z.B. [Mü91]). Die Laufzeit dieses Algorithmus ist proportional zu der vierten Wurzel aus der Anzahl der Elemente im zugrundeliegenden endlichen Körper, so daß dieser Algorithmus in der Praxis nur für „kleine“ Körper (mit Elementanzahl bis zu $\approx 10^{25}$) angewandt werden kann. René Schoof hat 1985 in [Sc85] einen weiteren Algorithmus vorgestellt, der das Problem in Polynomzeit löst. Im Gegensatz zu diesem theoretischen Resultat ist der Algorithmus in der Praxis wegen enormer Laufzeiten nur bedingt einsetzbar. Im Rahmen meiner Diplomarbeit [Mü91] wurde eine Kombination der Algorithmen von Schoof und Shanks entwickelt und implementiert, mit der es möglich ist, Gruppenordnungen über Primkörpern mit bis zu $10^{42}$ Elementen in einigen Tagen zu bestimmen. Oliver Atkin entwickelte 1988 einen neuen Algorithmus für Primkörper, mit dem die Gruppenordnung einer Kurve über einem Primkörper mit 65-stelliger Charakteristik berechnet werden konnte [At88]. Durch Kombination der Ideen von Schoof und Atkin konnten Oliver Atkin und ich 1992 die Ordnung einer elliptischen Kurve über einem Primkörper mit ungefähr $10^{75}$ Elementen ausrechnen. Noam Elkies [El] hatte in der Zwischenzeit eine weitere Verbesserung theoretisch beschrieben. Diese Verbesserung wurde von Oliver Atkin in einen praktischen Algorithmus für große Primkörper umgeformt [At92]. In der vorliegenden Arbeit werden die beiden letztgenannten Algorithmen theoretisch genau untersucht und beschrieben. Dabei werden die bisher nur für Primkörper bekannten Algorithmen auf beliebige endliche Körper „genügend großer“ Charakteristik verallgemeinert. Weiterhin wird die Korrektheit all dieser Algorithmen bewiesen. In der Praxis haben sich diese Algorithmen als sehr effizient erwiesen, denn mit Hilfe einer in Saarbrücken erfolgten Implementierung ([Le94], [Ma94]) konnte die Gruppenordnung einer elliptischen Kurve über einem Primkörper mit 375-stelliger Charakteristik berechnet werden (siehe dazu [LMMS94]). Unser bisheriger Rekord (Weltrekord bis 26. Januar 1995) ist die Bestimmung der Gruppenordnung einer elliptischen Kurve über einem Primkörper mit 425-stelliger Charakteristik, der ebenfalls mit Hilfe unserer Implementierung erfolgte (siehe Abschnitt 10.4).

## 1.2 Gliederung der Arbeit

Im weiteren Verlauf dieses Kapitels werden einige Bezeichnungen vereinbart, die in den folgenden Kapiteln nicht mehr explizit eingeführt werden.

Kapitel 2 beschäftigt sich ausführlich mit den Grundlagen elliptischer Kurven. Zuerst werden die in diesem Zusammenhang wichtigen Begriffe eingeführt. Anschließend werden einige einfache Tatsachen bewiesen, die im weiteren Verlauf der Arbeit häufiger benutzt werden.

In Kapitel 3 geben wir an, wie wir Information über die gesuchte Gruppenordnung gewinnen können, wenn wir den Zerfällungstyp eines speziellen Polynoms kennen. Die Bestimmung dieses Zerfällungstyps wird anschließend auf das Verhalten spezieller Untergruppen der Punktgruppe sowie auf die Untersuchung sogenannter $j$-Invarianten geeigneter elliptischer Kurven reduziert.

In Kapitel 4 beschreiben wir die theoretischen Grundlagen sogenannter „modularer“ Polynome. Mit Hilfe dieser Polynome können wir die in Kapitel 3 beschriebene

Untersuchung der speziellen $j$-Invarianten durchführen. Modulare Polynome untersuchen wir zuerst für den Körper der komplexen Zahlen und führen danach den Fall der endlichen Körper auf den komplexen Fall zurück. Anschließend untersuchen wir spezielle Eigenschaften dieser Polynome, insbesondere auch die Galoisgruppe dieser Polynome. Im letzten Abschnitt von Kapitel 4 beschreiben wir die theoretischen Grundlagen sogenannter „äquivalenter“ Polynome. Äquivalente Polynome können in unserer Anwendung an Stelle von modularen Polynomen verwendet werden und sind in der Praxis viel leichter zu berechnen als diese.

In Kapitel 5 beschreiben wir Algorithmen zur Bestimmung solcher äquivalenter Polynome. Dabei stellen wir zwei verschiedene Typen vor. In beiden Fällen geben wir zuerst einige Eigenschaften dieser Polynome an und beschreiben dann, wie wir diese Eigenschaften benutzen können, um die Polynome zu berechnen. Im abschließenden Abschnitt dieses Kapitels beschreiben wir eine Implementierung dieser Algorithmen und geben einige praktische Erfahrungen und Laufzeiten an.

In den Kapiteln 6 und 7 beschreiben wir eine Variante des Algorithmus von Elkies für endliche Körper. Dazu leiten wir den Algorithmus zuerst für den Körper der komplexen Zahlen her und zeigen dann, wie sich dieser Algorithmus auf endliche Körper überträgt. Kapitel 6 behandelt dabei den Fall des komplexen Körpers und gibt den theoretischen Hintergrund an. Im folgenden Kapitel 7 werden diese Formeln dann auf endliche Körper übertragen und es wird gezeigt, wie wir damit Information über die Gruppenordnung einer elliptischen Kurve über einem endlichen Körper gewinnen können. Außerdem beschreiben wir unsere Implementierung dieses Algorithmus für endliche Primkörper sowie Laufzeitresultate, die wir mit dieser Implementierung erzielt haben.

In Kapitel 8 wird eine Erweiterung des Algorithmus von Schoof beschrieben. Dabei werden Ideen aus den vorhergehenden Kapiteln benutzt, um einen Algorithmus zur Bestimmung der Gruppenordnung modulo kleiner Primzahlpotenzen herzuleiten.

In Kapitel 9 wird untersucht, wie wir für elliptische Kurven mit speziellen Eigenschaften die Gruppenordnungen bestimmen können. Für solche elliptische Kurven sind die in den vorherigen Kapiteln beschriebenen Algorithmen nicht anwendbar.

In Kapitel 10 beschreiben wir einen auf der Babystep-Giantstep Idee basierenden Algorithmus, mit dem wir aus einer Menge von vielen Möglichkeiten die gesuchte Gruppenordnung effizient bestimmen können. Anschließend fassen wir alle bisher beschriebenen Teilalgorithmen zusammen und erhalten so einen „Gesamtalgorithmus“, der das vorgegebene Problem löst. Zum Abschluß des Kapitels beschreiben wir einige praktische Aspekte unserer Implementierung und geben praktische Laufzeiten an. Insbesondere beschreiben wir die Berechnungen der vier größten bisher von uns bestimmten Gruppenordnungen.

Im letzten Kapitel der Arbeit beschreiben wir einen Algorithmus, der für eine gegebene „wahrscheinliche“ Gruppenordnung beweist, daß diese korrekt ist. Dieser Korrektheitsbeweis ist notwendig, denn theoretisch können wir nicht beweisen, daß der vorgestellte Algorithmus immer genau die Gruppenordnung bestimmt. In der Praxis ist allerdings noch kein Beispiel aufgetreten, in dem dies nicht der Fall war.

## 1.3 Bezeichnungen

Wir verwenden folgende Symbole zur Bezeichnung von Zahlbereichen:

| | |
|---|---|
| $\mathbb{N}$ | Menge der natürlichen Zahlen (ohne Null), |
| $\mathbb{Z}$ | Menge der ganzen Zahlen, |
| $\mathbb{Q}$ | Menge der rationalen Zahlen, |
| $\mathbb{R}$ | Menge der reellen Zahlen, |
| $\mathbb{C}$ | Menge der komplexen Zahlen, |
| $\mathbb{F}_q$ | endlicher Körper mit $q = p^d$ Elementen, |
| $\overline{\mathbb{F}}_q$ | algebraischer Abschluß des Körpers $\mathbb{F}_q$. |

Weiterhin vereinbaren wir die folgenden Bezeichnungen, die während der ganzen Arbeit beibehalten werden:

| | |
|---|---|
| $p$ | Charakteristik des Körpers $\mathbb{F}_q$, $p > 3$, |
| $q$ | Elementanzahl des zugrundeliegenden Körpers $\mathbb{F}_q$, |
| $l$ | ungerade Primzahl ungleich $p$, |
| $\mathbb{F}_l$ | endlicher Körper mit $l$ Elementen ($\cong \mathbb{Z}/l\mathbb{Z}$), |
| $\#G$ | Anzahl der Elemente der Menge $G$, |
| $\Im(z)$ | Imaginärteil der komplexen Zahl $z$. |

Wir werden die folgenden Gruppen benötigen. Da wir allerdings nicht genauer auf Eigenschaften dieser Gruppen eingehen werden, geben wir hier nur ihre Definition an (Eigenschaften und eine genaue Untersuchung dieser Gruppen findet man beispielsweise in [Hu67, Seite 177ff]):

$$\mathrm{PSL}_2(\mathbb{F}_l) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_l^{2\times 2};\ ad - bc = 1 \right\} \Big/ \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

$$\mathrm{PGL}_2(\mathbb{F}_l) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_l^{2\times 2};\ ad - bc \neq 0 \right\} \Big/ \left\{ \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix};\ e \in \mathbb{F}_l^* \right\},$$

| | |
|---|---|
| $S_n$ | Gruppe der Permutationen auf $n$ Elementen, |
| $A_n$ | Gruppe der alternierenden Permutationen in $S_n$. |

In der ganzen Arbeit markieren wir das Ende von Beweisen durch das Zeichen $\blacksquare$. Diese Regel wird nur unterbrochen, wenn innerhalb eines Beweises ein Hilfslemma formuliert wird. Beweise für solche Hilfslemmata werden mit dem Zeichen $\square$ beendet.

Zur Darstellung von Algorithmen verwenden wir eine modifizierte Form der von Nassi und Shneiderman [NaSh73] eingeführten Struktogramme (Nassi-Shneiderman-Diagramme). In diesen Diagrammen wird der Ablauf der Algorithmen durch die Aneinanderreihung und Verschachtelung einzelner sogenannter Strukturblöcke dargestellt. Da diese Struktogramme selbsterklärend sind, verzichten wir hier auf eine weitere Beschreibung.

# Kapitel 2

# Grundlegende Definitionen und Eigenschaften

In diesem Kapitel werden wir die grundlegenden mathematischen Begriffe einführen, die wir bei der Beschreibung des in dieser Arbeit vorgestellten Algorithmus benötigen werden. Im ersten Abschnitt werden wir den Begriff einer elliptischen Kurve definieren. Anschließend werden Abbildungen zwischen solchen Kurven eingeführt, bevor wir uns mit einer speziellen Abbildung genauer beschäftigen. Diese spezielle Abbildung besitzt eine fundamentale Bedeutung für das Problem der Bestimmung der Ordnung einer elliptischen Kurve, denn fast alle bekannten Algorithmen zur Lösung dieses Problems benutzen Eigenschaften dieser Abbildung. Einige Eigenschaften dieser Abbildung werden deshalb in den abschließenden Abschnitten dieses Kapitels vorgestellt.

In der ganzen Arbeit machen wir die Voraussetzung, daß $\mathbb{F}_q$ der endliche Körper mit $q = p^d$ Elementen und Charakteristik $p > 3$ ist.

## 2.1 Elliptische Kurven über endlichen Körpern

Zuerst definieren wir den grundlegenden Begriff der ganzen Arbeit, eine elliptische Kurve.

**Definition 2.1** *Sei $K$ ein Körper mit Charakteristik ungleich zwei und drei. Unter einer* **elliptischen Kurve $E$ über dem Körper $K$** *verstehen wir ein Paar $(a, b) \in K^2$ mit der Eigenschaft $4\,a^3 + 27\,b^2 \neq 0$.*

*Für einen Erweiterungskörper $\mathcal{K}$ von $K$ definieren wir die Menge aller* **$\mathcal{K}$-rationalen Punkte** *von $E$ als*

$$E(\mathcal{K}) \quad = \quad \{\, (x, y) \in \mathcal{K}^2 \; ; \; y^2 = x^3 + a\,x + b \,\} \quad \cup \quad \{\, \mathcal{O} \,\}, \tag{2.1}$$

*wobei $\mathcal{O}$ ein „idealisierter“ Punkt ist.*

Wir schreiben im folgenden für eine über dem Körper $K$ definierte elliptische Kurve $E$ auch kürzer $E/K$. Auf der Menge der $\mathcal{K}$-rationalen Punkte einer elliptischen Kurve $E = (a, b)$ können wir auf die folgende Weise eine Verknüpfung definieren, die als Addition bezeichnet wird:

- Für jeden Punkt $P \in E(\mathcal{K})$ gilt $P + \mathcal{O} = \mathcal{O} + P = P$.
- Zu einem Punkt $\mathcal{O} \neq P = (x, y) \in E(\mathcal{K})$ definieren wir als negativen Punkt
$$-P := (x, -y) \quad \in E(\mathcal{K}).$$
- Für Punkte $P_1$ und $P_2$ mit $P_1 = -P_2$ wird die Summe als $P_1 + P_2 := \mathcal{O}$ definiert.
- Für Punkte $P_1 = (x_1, y_1) \neq \mathcal{O}$ und $P_2 = (x_2, y_2) \neq \mathcal{O}$ mit $P_1 \neq -P_2$ wird die Summe gegeben als $P_1 + P_2 = (x_3, y_3)$, wobei
$$\begin{aligned} x_3 &= -x_1 - x_2 + \lambda^2 \\ y_3 &= -y_1 + \lambda \cdot (x_1 - x_3) \end{aligned}$$
mit
$$\begin{aligned} \lambda &= \frac{y_1 - y_2}{x_1 - x_2} \quad \text{falls } P_1 \neq P_2. \\ \lambda &= \frac{3x_1^2 + a}{2y_1} \quad \text{falls } P_1 = P_2. \end{aligned}$$

Dann erhalten wir den folgenden Satz (siehe [Si85, Prop. 2.2, Seite 55]):

**Satz 2.2** *Sei $E$ eine elliptische Kurve über $K$ und $\mathcal{K}$ ein Erweiterungskörper von $K$. Dann bildet die Menge der $\mathcal{K}$-rationalen Punkte von $E$ mit dieser Verknüpfung eine additive abelsche Gruppe mit Nullelement $\mathcal{O}$.*

**Bemerkung 2.3** Betrachten wir elliptische Kurven über dem Körper der reellen Zahlen, so besitzt die Addition zweier Punkte eine geometrische Bedeutung. Diese Bedeutung wird in der folgenden Abbildung 2.1 verdeutlicht. Dort betrachten wir die elliptische Kurve $E = (-10, 10)$ sowie die Punkte $P = (-3, \sqrt{13}), Q = (1, -1)$ und $H \approx (-2.209736791, -4.615989934)$.

Das Thema dieser Arbeit besteht darin, für einen beliebigen endlichen Körper $\mathbb{F}_q$ der Charakteristik $p > 3$ und eine beliebige elliptische Kurve über diesem Körper die Ordnung der Punktgruppe $E(\mathbb{F}_q)$, d.h. die Anzahl der $\mathbb{F}_q$-rationalen Punkte, zu berechnen. Diese Anzahl ist sicherlich endlich, denn offensichtlich gibt es maximal $q^2$ viele Paare in $\mathbb{F}_q^2$, da $\mathbb{F}_q$ nur $q$ Elemente besitzt. In [Si85, Th. 1.1, Seite 131] finden wir das folgende Resultat über die Größenordnung der Gruppenordnung.

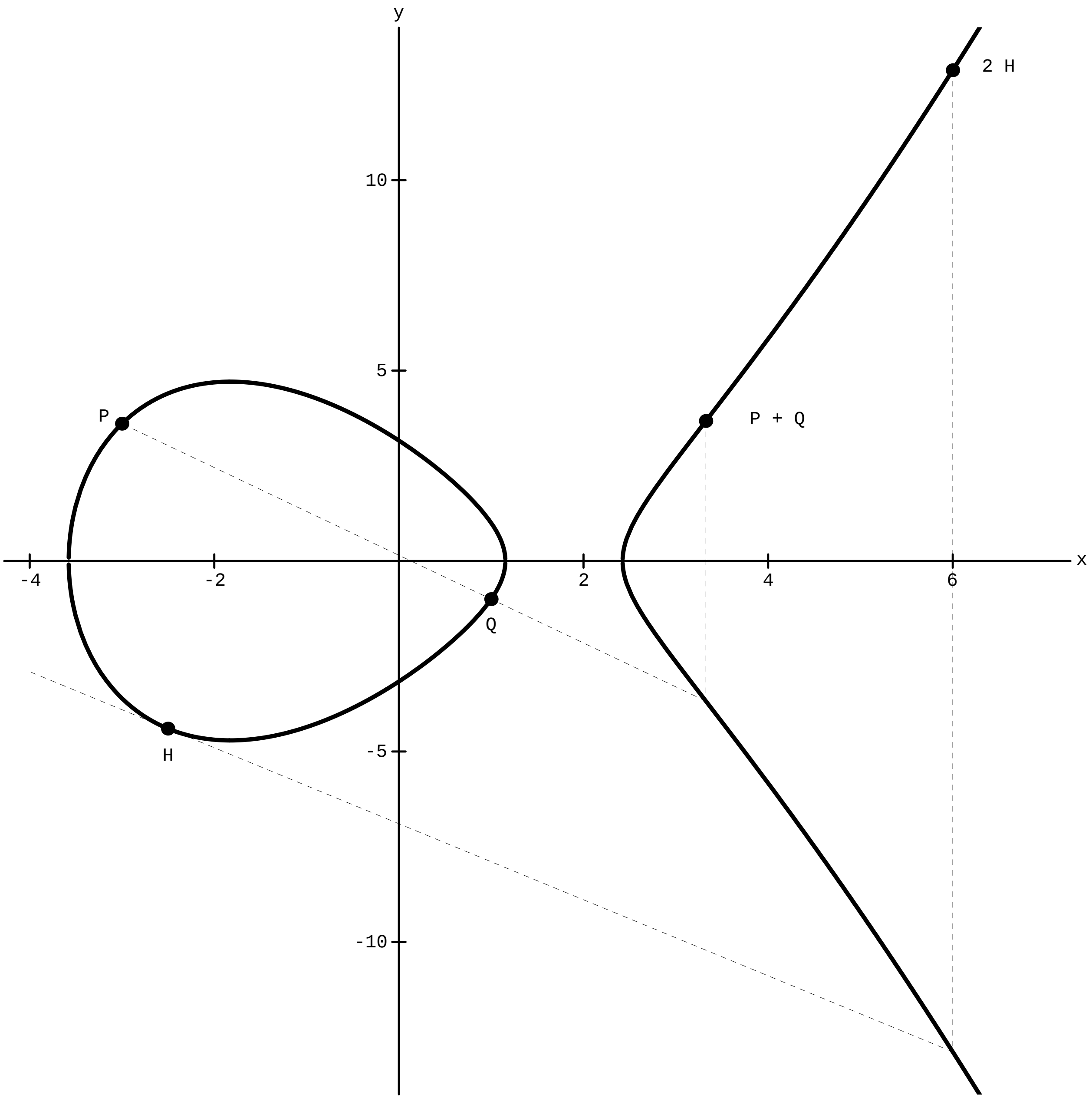


Abbildung 2.1: Elliptische Kurve über $\mathbb{R}$, Punktaddition

**Satz 2.4 (Satz von Hasse)**
*Sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Dann gilt für die Ordnung der Punktgruppe der $\mathbb{F}_q$-rationalen Punkte*

$$\left| \#E(\mathbb{F}_q) - q - 1 \right| \quad \leq \quad 2\sqrt{q},$$

*d.h.*

$$q + 1 - 2\sqrt{q} \quad \leq \quad \#E(\mathbb{F}_q) \quad \leq \quad q + 1 + 2\sqrt{q}. \tag{2.2}$$

Aus diesem Satz folgt, daß die Anzahl der $\mathbb{F}_q$-rationalen Punkte einer über dem endlichen Körper $\mathbb{F}_q$ definierten elliptischen Kurve $E$ ungefähr gleich der Anzahl der Elemente des Körpers $\mathbb{F}_q$ ist. Ist die Anzahl der Elemente in dem zugrundeliegenden Körper $\mathbb{F}_q$ „klein", so kann man mit einfachen Zählalgorithmen die Ordnung der Punktgruppe $E(\mathbb{F}_q)$ bestimmen [Mü91]. Wir stellen in dieser Arbeit einen Algorithmus zur Lösung dieses Problems vor, der auch für „große" endliche Körper hinreichend großer Charakteristik in der Praxis anwendbar ist. Um die Theorie dieses Algorithmus zu verstehen, beschreiben wir im folgenden Abschnitt einige Grundlagen über Abbildungen zwischen Punktgruppen elliptischer Kurven.

## 2.2 Rationale Funktionen und Isogenien

In diesem Abschnitt beschreiben wir Abbildungen zwischen Punktgruppen elliptischer Kurven. Diese Abbildungen stehen in enger Beziehung zu rationalen Funktionen. Zuerst geben wir deshalb die Definition von rationalen Funktionen auf einer elliptischen Kurve $E$ an, bevor wir spezielle Abbildungen definieren. Sei im weiteren in diesem Abschnitt $E = (a, b)$ eine elliptische Kurve über dem Körper $\mathbb{F}_q$.

**Definition 2.5** *Ein* **Polynom auf** $E$ *ist ein Element aus dem Ring*

$$\overline{\mathbb{F}}_q[X,Y] \Big/ (Y^2 - X^3 - a\,X - b).$$

*Der Ring aller Polynome auf $E$ wird mit $\overline{\mathbb{F}}_q[E]$ bezeichnet. Falls ein Polynom auf $E$ sogar aus dem Ring $K[X,Y] \Big/ (Y^2 - X^3 - a\,X - b)$ für einen Erweiterungskörper $K$ von $\mathbb{F}_q$ ist, so sagen wir, daß das Polynom auf $E$ über $K$ definiert ist.*

**Definition 2.6** *Der* **Körper der rationalen Funktionen auf** $E$ *ist der Quotientenkörper von $\overline{\mathbb{F}}_q[E]$; wir bezeichnen ihn mit $\overline{\mathbb{F}}_q(E)$. Eine rationale Funktion auf $E$ ist über einem Erweiterungskörper $K$ von $\mathbb{F}_q$ definiert, falls Vertreter $f/g$ mit $f, g \in K[E]$ existieren.*

Für solche rationalen Funktionen können wir wie üblich den Begriff einer Nullstelle oder eines Pols definieren. Weiterhin können wir rationale Funktionen auf $E$ an Punkten $P$ von $E$ auf die offensichtliche Art und Weise auswerten, wenn $P$ kein Pol der rationalen Funktion ist. Ist $P$ ein Pol einer rationalen Funktion $r$ auf $E$, so setzen wir $r(P) = \infty$. Dann können wir den Begriff der Isogenie zwischen zwei elliptischen Kurven definieren.

**Definition 2.7** *Seien $E = (a, b)$ und $E' = (a', b')$ elliptische Kurven. Eine* **nichtkonstante Isogenie** *von $E$ nach $E'$ ist ein Paar $(r, s)$ von rationalen Funktionen auf $E$ mit den Eigenschaften $s^2 = r^3 + a'\, r + b'$ und $(r(\mathcal{O}), s(\mathcal{O})) = \mathcal{O}'$. Wir sagen, daß die Isogenie über dem Körper $\mathbb{F}_q$ definiert ist, falls sowohl $r$ als auch $s$ rationale Funktionen auf $E$ über $\mathbb{F}_q$ sind. Zwei elliptische Kurven heißen* **isogen**, *falls es eine nichtkonstante Isogenie zwischen ihnen gibt.*

**Bemerkung 2.8** Zusätzlich zu nichtkonstanten Isogenien gibt es noch die Abbildung, die alle Punkte von $E$ auf den Nullpunkt von $E'$ abbildet. Diese Abbildung wird als konstante Isogenie (oder Nullisogenie) bezeichnet. Im folgenden wird bei Benutzung von Isogenien immer angenommen, daß sie nicht die Nullisogenie sind.

Wir wissen schon, daß die Menge aller Punkte auf einer elliptischen Kurve eine Gruppe bildet. Isogenien sind dann genau Homomorphismen der Punktgruppe und umgekehrt, wie in [ChRo90, Th. 2.2, Seite 8] gezeigt wird.

In den folgenden Abschnitten werden wir häufig zu einer gegebenen Isogenie eine „Umkehrung", die sogenannte duale Isogenie, verwenden. Diese führen wir im folgenden Satz aus [Si85, Th. 6.1, Seite 84] ein.

**Satz 2.9** *Sei $\psi : E \longrightarrow E'$ eine nichtkonstante Isogenie zwischen den elliptischen Kurven $E$ und $E'$. Dann existiert eine zu $\psi$* **duale Isogenie** $\hat{\psi} : E' \longrightarrow E$ *und eine eindeutig bestimmte positive Zahl $m \in \mathbb{N}$ mit*

$$\hat{\psi} \circ \psi \quad = \quad m.$$

**Bemerkung 2.10** Wir können eine ganze Zahl $m$ auch als eine Isogenie von $E$ nach $E$ interpretieren, die jeden Punkt $P \in E(\overline{\mathbb{F}}_q)$ auf den Punkt $m \cdot P$ abbildet. Sprechen wir also von einer Isogenie $m$, so ist dies in dieser Weise zu interpretieren.

Zu einer gegebenen Isogenie $\psi$ bezeichnet man eine Zahl $m$ wie aus Satz 2.9 auch als **Grad** der Isogenie $\psi$. Der Grad einer Isogenie besitzt eine algebraische Bedeutung, auf die wir aber nicht eingehen werden, weil wir sie nicht benutzen. Für nähere Informationen beachte man [Si85].

Wie in der Gruppentheorie üblich, nennt man eine Isogenie von $E$ auf sich selbst auch einen **Endomorphismus**. Alle über dem algebraischen Abschluß $\overline{\mathbb{F}}_q$ definierten Endomorphismen einer elliptischen Kurve $E$ bilden einen Ring, den wir im folgenden mit $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ bezeichnen. In dem folgenden Abschnitt werden wir uns genauer mit einem speziellen Endomorphismus beschäftigen, der in der gesamten Arbeit eine gewichtige Bedeutung besitzt.

## 2.3 Der Frobenius-Endomorphismus

Ein spezieller Endomorphismus der Punktgruppe einer elliptischen Kurve besitzt eine besonders große Bedeutung bei der Bestimmung der Gruppenordnung dieser Punktgruppe. Diesen Endomorphismus werden wir zuerst vorstellen. Danach werden wir Eigenschaften dieses Endomorphismus beschreiben, die wir in den folgenden Kapiteln verwenden werden.

**Definition 2.11** *Sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Dann ist der* **Frobenius-Endomorphismus zu** $E$ *die folgende Abbildung:*

$$\begin{array}{rrcl} \Phi_E: & E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ & (x,y) & \longmapsto & (x^q, y^q). \end{array}$$

**Bemerkung 2.12** Wir können leicht zeigen, daß diese Abbildung wirklich ein Endomorphismus ist. Die Homomorphie-Eigenschaft wird dabei dadurch deutlich, daß die elliptische Kurve $E$ und damit die Addition in $E(\overline{\mathbb{F}}_q)$ über dem Körper $\mathbb{F}_q$ definiert sind und Elemente aus $\mathbb{F}_q$ die Gleichung $X^q = X$ erfüllen.

Der Frobenius-Endomorphismus besitzt eine enge Beziehung zur Gruppenordnung von $E(\mathbb{F}_q)$, die wir im folgenden Satz angeben.

**Satz 2.13** *Sei $E$ eine elliptische Kurve über $\mathbb{F}_q$ und sei $\#E(\mathbb{F}_q) = q + 1 - c$. Dann erfüllt der Frobenius-Endomorphismus im Endomorphismenring $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ von $E$ die Gleichung*

$$\Phi_E^2 - c\,\Phi_E + q \quad = \quad 0. \tag{2.3}$$

**Beweis:** [ChRo88, Th. 12.16, Seite 71] ■

**Bemerkung 2.14** Die Zahl $c$ aus Satz 2.13 nennen wir auch die **Spur des Frobenius-Endomorphismus**. Kennen wir zu gegebener elliptischer Kurve $E/\mathbb{F}_q$ die Spur $c$ des zugehörigen Frobenius-Endomorphismus, so kennen wir offensichtlich auch die Ordnung der Gruppe der $\mathbb{F}_q$-rationalen Punkte von $E$.

Der Frobenius-Endomorphismus gibt uns weiterhin die Möglichkeit, für eine gegebene elliptische Kurve $E/\mathbb{F}_q$ aus der Ordnung der Punktgruppe $E(\mathbb{F}_q)$ die Ordnung der Punktgruppen $E(\mathbb{F}_{q^j})$ für Erweiterungskörper $\mathbb{F}_{q^j}$ von $\mathbb{F}_q$ zu bestimmen. Diese Ordnungen können wir mit Hilfe der folgenden rekursiven Formel berechnen.

**Satz 2.15** *Sei $E$ eine elliptische Kurve über $\mathbb{F}_q$ und sei die Ordnung der Punktgruppe von $E$ über dem Erweiterungskörper $\mathbb{F}_{q^j}$ für $j \geq 1$ gegeben als*

$$\#E(\mathbb{F}_{q^j}) \quad = \quad q^j + 1 - c_j.$$

*Setzen wir $c_0 = 2$, so gilt für $j \geq 1$ die Rekursionsformel*

$$c_{j+1} \quad = \quad c_1 \cdot c_j - q \cdot c_{j-1}.$$

**Beweis:** Sei $\Phi_E$ der Frobenius-Endomorphismus für $E/\mathbb{F}_q$. Fassen wir $E$ als über $\mathbb{F}_{q^j}$ definiert auf, so wird der zugehörige Frobenius-Endomorphismus für den Erweiterungskörper $E(\mathbb{F}_{q^j})$ gegeben als $\Phi_E^j$. Aus [Si85, Th. 6.2 (b), Seite 86] folgt, daß der zu $\Phi_E^j$ duale Endomorphismus $\hat{\Phi}_E^j$ ist, wobei $\hat{\Phi}_E$ der duale Endomorphismus zu $\Phi_E$ ist. Nun beachten wir, daß $c_{j+1} = \Phi_E^{j+1} + \hat{\Phi}_E^{j+1}$ ist (dies folgt aus dem Beweis zu [ChRo88, Th. 12.16, Seite 71]) und erhalten dann für $j \geq 1$

$$\begin{aligned} c_{j+1} &= \Phi_E^{j+1} + \hat{\Phi}_E^{j+1} \\ &= (\Phi_E + \hat{\Phi}_E) \circ (\Phi_E^j + \hat{\Phi}_E^j) - (\Phi_E \circ \hat{\Phi}_E^j + \Phi_E^j \circ \hat{\Phi}_E) \\ &= c_1 \cdot c_j - (\Phi_E \circ \hat{\Phi}_E) \circ (\Phi_E^{j-1} + \hat{\Phi}_E^{j-1}) \\ &= c_1 \cdot c_j - q \cdot c_{j-1}. \end{aligned}$$

Bei dieser Umformung wird noch benutzt, daß der Grad des Frobenius-Endomorphismus $q$ ist. ■

Also können wir für eine elliptische Kurve $E$ über dem Körper $\mathbb{F}_q$ die Ordnungen der Punktgruppen $E(\mathbb{F}_{q^j})$ leicht berechnen, wenn wir die Ordnung von $E(\mathbb{F}_q)$ und damit $c_1$ kennen. Im folgenden werden wir daher nur noch dieses Problem untersuchen.

Der Frobenius-Endomorphismus besitzt noch eine weitere wichtige Eigenschaft. Oft ist es von Interesse, den minimalen Erweiterungskörper von $\mathbb{F}_q$ zu finden, über dem eine Isogenie definiert ist. Ein Kriterium, um diesen Erweiterungsgrad zu bestimmen, liefert das folgende Lemma.

**Lemma 2.16** *Seien $E, E'$ zwei elliptische Kurven über dem Körper $\mathbb{F}_q$ und seien $\Phi_E, \Phi_{E'}$ die zugehörigen Frobenius-Endomorphismen. Dann gilt für jede Isogenie $\psi$ von $E$ nach $E'$*

$$\psi \text{ über } \mathbb{F}_{q^d} \text{ definiert} \quad \Longleftrightarrow \quad \psi \circ \Phi_E^d = \Phi_{E'}^d \circ \psi.$$

**Beweis:** Jede Isogenie ist nach Definition ein Paar rationaler Funktionen auf $E$. Sei zuerst $\psi(X,Y) = (u(X,Y), v(X,Y))$ über $\mathbb{F}_{q^d}$ definiert, d.h. die beiden rationalen Funktionen $u$ und $v$ auf $E$ sind über $\mathbb{F}_{q^d}$ definiert. Dann gilt

$$\begin{aligned} \psi \circ \Phi_E^d(X,Y) &= \psi(X^{q^d}, Y^{q^d}) \\ &= (u(X^{q^d}, Y^{q^d}), v(X^{q^d}, Y^{q^d})) \\ &= (u(X,Y)^{q^d}, v(X,Y)^{q^d}) \\ &= \Phi_{E'}^d \circ \psi(X,Y). \end{aligned}$$

Dabei wurde benutzt, daß für jede rationale Funktion $f(X,Y) \in \overline{\mathbb{F}}_q(X,Y)$ genau dann $f(X,Y) \in \mathbb{F}_{q^d}(X,Y)$ ist, wenn

$$f(X,Y)^{q^d} = f(X^{q^d}, Y^{q^d})$$

gilt. Da $E$ über dem Grundkörper $\mathbb{F}_q$ definiert ist, gilt diese Eigenschaft sicherlich auch für rationale Funktionen auf $E$. Die umgekehrte Richtung der Behauptung folgt direkt aus dem gleichen Grund. ■

## 2.4 Supersinguläre elliptische Kurven

Wir haben in Abschnitt 2.2 schon den Endomorphismenring $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ für eine gegebene elliptische Kurve $E/\mathbb{F}_q$ definiert. In diesem Abschnitt werden wir diesen Ring genauer untersuchen und damit eine Einteilung elliptischer Kurven in verschiedene Klassen erhalten. Wir geben zuerst die Struktur dieses Rings an.

**Satz 2.17** *Der Endomorphismenring einer elliptischen Kurve über einem endlichen Körper $\mathbb{F}_q$ ist entweder eine Ordnung eines imaginärquadratischen Zahlkörpers oder eine Ordnung einer Quaternionenalgebra.*

**Beweis:** [Si85, Cor. 9.4, Seite 102] ■

Je nach Art des Endomorphismenrings unterscheidet man dann die beiden folgenden Klassen von elliptischen Kurven.

**Definition 2.18** *Eine elliptische Kurve $E$ heißt* **supersingulär**, *falls $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ eine Ordnung in einer Quaternionenalgebra ist. Ansonsten heißt die elliptische Kurve* **ordinär**.

Supersinguläre Kurven werden später bei der Beschreibung unseres Algorithmus eine besondere Rolle spielen. Insbesondere benötigen wir einen Test, um eine gegebene elliptische Kurve auf Supersingularität überprüfen zu können. Um später die Korrektheit eines solchen Tests begründen zu können, stellen wir die folgende Eigenschaften von supersingulären Kurven vor.

**Proposition 2.19** *Sei $E$ eine elliptische Kurve über dem Körper $\mathbb{F}_q$ der Charakteristik $p > 3$ und sei $\#E(\mathbb{F}_q) = q + 1 - c$. Dann gilt*

$$E \text{ supersingulär} \qquad \Longleftrightarrow \qquad c \equiv 0 \bmod p.$$

**Beweis:** Wir gehen analog zum Beweis von Satz 4.1(a) in [Si85, Seite 140] vor. Sei $\Phi_E$ der Frobenius-Endomorphismus zu $E$. Nach Satz 3.1(a)(ii) in [Si85, Seite137] gilt dann, daß $E$ genau dann supersingulär ist, wenn der zu $\Phi_E$ duale Endomorphismus $\hat{\Phi}_E$ inseparabel ist (die Bedeutung des Begriffs „inseparabel" kann man an derselben Stelle nachlesen). Falls die Gruppenordnung von $E(\mathbb{F}_q)$ gleich $q+1-c$ ist, so erfüllt der Frobenius-Endomorphismus die Gleichung

$$\Phi_E^2 - c\,\Phi_E + q \quad = \quad 0,$$

und damit wird der zu $\Phi_E$ duale Endomorphismus gegeben als

$$\hat{\Phi}_E \quad = \quad c - \Phi_E.$$

Die Separabilitätseigenschaften von Endomorphismen dieser Gestalt sind aber bekannt: ein Endomorphismus $m + n\,\Phi_E$ ist genau dann inseparabel, wenn die Charakteristik $p$ des endlichen Körpers $\mathbb{F}_q$ $m$ teilt (vgl. [Si85, Cor. 5.5, Seite 83]). Damit ist in unserem Fall $\hat{\Phi}_E$ genau dann inseparabel und damit $E$ supersingulär, wenn $c \equiv 0 \bmod p$ ist. ■

Wir werden im nächsten Kapitel noch ein Resultat über die Gestalt der Endomorphismenringe zweier isogener elliptischer Kurven benötigen. Dazu geben wir das folgende Lemma an.

**Lemma 2.20** *Seien $E, E'$ elliptische Kurven über dem Körper $\mathbb{F}_q$ und sei $E$ ordinär. Sei weiterhin $\psi$ eine Isogenie von $E$ nach $E'$ mit der Eigenschaft, daß die Ordnung des Kerns von $\psi$ und $q$ teilerfremd sind. Dann ist $E'$ ebenfalls ordinär.*

**Beweis:** Sei $p$ die Charakteristik des Körpers $\mathbb{F}_q$. Nach Satz 3.1 aus [Si85, Seite 137] gibt es genau dann einen Punkt $P$ der Ordnung $p$ in $E(\overline{\mathbb{F}}_q)$, wenn $E$ ordinär ist. Dieser Punkt kann wegen $\mathrm{ggT}(\#\ker\psi, q) = 1$ kein Element des Kerns der Isogenie $\psi$ sein. Wäre $P$ ein Element des Kerns, so wäre die von ihm erzeugte Gruppe eine Untergruppe des Kernes von $\psi$ der Ordnung $p$. Also würde $p$ die Ordnung des Kernes von $\psi$ teilen und obiger größter gemeinsamer Teiler wäre nicht eins. Da $p$ eine Primzahl ist, ist damit $\psi(P)$ ein Punkt der Ordnung $p$ in $E'(\overline{\mathbb{F}}_q)$, d.h. $E'$ ist ebenfalls ordinär. ■

## 2.5 Isomorphe elliptische Kurven

In dem abschließenden Abschnitt dieses Kapitels werden wir uns noch mit einem weiteren wichtigen Thema in der Theorie der elliptischen Kurven beschäftigen, mit Isomorphismen der Punktgruppe. Insbesondere werden wir uns mit über dem Grundkörper definierten Isomorphismen befassen.

**Satz 2.21** *Sei $E = (a, b)$ eine elliptische Kurve über $\mathbb{F}_q$ und sei $u \in \overline{\mathbb{F}}_q^*$. Dann ist die Punktgruppe $E'(\overline{\mathbb{F}}_q)$ der elliptischen Kurve $E' = (u^4\, a, u^6\, b)$ isomorph zur Punktgruppe $E(\overline{\mathbb{F}}_q)$. Die Isomorphie wird gegeben durch die Abbildung*

$$\begin{array}{ccc} E(\overline{\mathbb{F}}_q) & \longrightarrow & E'(\overline{\mathbb{F}}_q) \\ (x, y) & \longmapsto & (u^2\, x, u^3\, y). \end{array}$$

**Beweis:** [Si85, Prop. 1.4, Seite 50] ■

Ein Kriterium, wie man feststellen kann, ob zwei gegebene elliptische Kurven isomorph sind, läßt sich leicht beschreiben. Dazu benötigen wir die folgende Definition.

**Definition 2.22** *Sei $E = (a, b)$ eine elliptische Kurve. Dann definieren wir die* **j-Invariante** *zu $E$ als*

$$j(E) \quad = \quad 1728\, \frac{4\, a^3}{4\, a^3 + 27\, b^2}.$$

Diese $j$-Invariante ist eine Invariante der Isomorphieklasse, d.h. der Klasse aller elliptischer Kurven, die über dem algebraischen Abschluß $\overline{\mathbb{F}}_q$ isomorph sind. Dies wird in folgenden Satz gezeigt [Si85, Prop. 1.4 (b), Seite 50]:

**Satz 2.23** *Zwei elliptische Kurven $E$ und $E'$ sind genau dann über $\overline{\mathbb{F}}_q$ isomorph, wenn sie die gleiche $j$-Invariante besitzen.*

Wir werden nun noch spezielle Isomorphismen untersuchen, die „schöne“ Eigenschaften haben, was die Ordnung der beiden Punktgruppen angeht. Dies wird in einem späteren Kapitel dazu benutzt werden, einen Algorithmus zum Beweis der Korrektheit einer berechneten „wahrscheinlichen“ Gruppenordnung vorzustellen.

**Lemma 2.24** *Sei $E = (a, b)$ eine elliptische Kurve über dem Körper $\mathbb{F}_q$ und sei $\#E(\mathbb{F}_q) = q + 1 - c$. Sei weiterhin $d$ kein Quadrat in $\mathbb{F}_q^*$. Dann gilt für die Ordnung der Punktgruppe der zu $E$ isomorphen elliptischen Kurve $E' = (d^2\, a, d^3\, b)$*

$$\#E'(\mathbb{F}_q) \quad = \quad q + 1 + c.$$

**Beweis:** Die Isomorphie der elliptischen Kurven $E$ und $E'$ folgt direkt aus Satz 2.21, wenn wir $u \in \overline{\mathbb{F}}_q^*$ als eine Quadratwurzel aus $d$ wählen. Nun zum Beweis der Behauptung über die Ordnungen der beiden Punktgruppen. Sei für $x \in \mathbb{F}_q$

$$\chi(x) \quad = \quad \begin{cases} 1 & x \text{ Quadrat in } \mathbb{F}_q^*, \\ 0 & x = 0, \\ -1 & x \text{ kein Quadrat in } \mathbb{F}_q^*. \end{cases}$$

Dann erkennt man durch Abzählen leicht, daß für die Gruppenordnung $\#E(\mathbb{F}_q)$ die Formel

$$\#E(\mathbb{F}_q) \quad = \quad 1 + \sum_{x \in \mathbb{F}_q} \Big(\chi(x^3 + a\,x + b) + 1\Big) \quad = \quad q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + a\,x + b)$$

gilt. Dazu betrachten wir einfach den Wert jedes Summanden und erkennen direkt, daß dieser Wert gerade die Anzahl der Punkte aus $E(\mathbb{F}_q)$ mit $x$-Koordinate $x$ angibt. Ein Element $x \in \mathbb{F}_q^*$ ist genau dann ein Quadrat, wenn $x^{(q-1)/2} = 1$ ist. Damit ist $\chi$ sogar multiplikativ, d.h. es gilt $\chi(x \cdot y) = \chi(x) \cdot \chi(y)$. Da mit $d$ auch $d^3$ ein Nichtquadrat ist und damit $\chi(d^3) = -1$ gilt, erhalten wir für die Gruppenordnung der isomorphen Kurve $E'$

$$\begin{aligned} \#E'(\mathbb{F}_q) \quad &= \quad q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + a\,d^2\,x + b\,d^3) \\ &= \quad q + 1 + \sum_{d \cdot x \in \mathbb{F}_q} \chi(d^3\,x^3 + a\,d^3\,x + b\,d^3) \\ &= \quad q + 1 + \sum_{x \in \mathbb{F}_q} \chi(d^3) \cdot \chi(x^3 + a\,x + b) \\ &= \quad q + 1 - \sum_{x \in \mathbb{F}_q} \chi(x^3 + a\,x + b), \end{aligned}$$

und damit ist die Spur des Frobenius-Endomorphismus zu $E'$ genau die negative Spur des Frobenius-Endomorphismus zu $E$. Dabei wurde bei den Umformungen benutzt, daß für ein Element $d \in \mathbb{F}_q^*$ die Menge $\{d \cdot x;\ x \in \mathbb{F}_q\} = \mathbb{F}_q$ ist. ■

Damit haben wir alle notwendigen Grundlagen und Definitionen aus der Theorie der elliptischen Kurven angegeben. Im folgenden Kapitel werden wir zeigen, wie wir Information über die Gruppenordnung einer elliptischen Kurve über einem endlichen Körper bestimmen können. Dabei werden die in diesem Kapitel angegebenen Grundlagen benutzt werden.

# Kapitel 3

# Informationen über die Spur des Frobenius-Endomorphismus

Wir haben im vorherigen Kapitel schon gesehen, daß der Frobenius-Endomorphismus zu einer elliptischen Kurve eine enge Beziehung zu dem Problem der Bestimmung der Ordnung der Punktgruppe dieser Kurve besitzt. In diesem Kapitel werden wir ein Verfahren beschreiben, wie wir Information über die Spur des Frobenius-Endomorphismus gewinnen können. Dies liefert dann mit Hilfe von Satz 2.13 auch Information über die Gruppenordnung der zugrundeliegenden elliptischen Kurve. Insbesondere sind wir dabei an der Bestimmung möglicher Werte für die Spur des Frobenius-Endomorphismus modulo kleiner ungerader Primzahlen $l$ interessiert.

Sei dazu während des gesamten Kapitels $l$ eine ungerade, von der Charakteristik $p$ des Körpers $\mathbb{F}_q$ verschiedene Primzahl.

## 3.1 Die Spur von $\Phi_E$ modulo $l$

In diesem Abschnitt werden wir herleiten, wie wir eine Liste von möglichen Werten für die Spur $c$ des Frobenius-Endomorphismus modulo $l$ erhalten, wenn wir den Zerfällungstyp des Polynoms $X^2 - c\,X + q$ modulo $l$ kennen. Damit erhalten wir eine Reduktion auf ein neues Problem, mit dem wir uns in den weiteren Abschnitten genauer beschäftigen werden.

Der Frobenius-Endomorphismus $\Phi_E$ erfüllt die in Satz 2.13 angegebene Gleichung

$$\Phi_E^2 - c\,\Phi_E + q \quad = \quad 0$$

im Endomorphismenring $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$. Um Aussagen über die Spur $c$ modulo $l$ machen zu können, betrachten wir diese Gleichung für eine Untergruppe von $E(\overline{\mathbb{F}}_q)$. Diese Untergruppe ist die Gruppe aller Punkte in $E(\overline{\mathbb{F}}_q)$ mit Exponent $l$, d.h. die Gruppe

$$E[l] \quad = \quad \Big\{ P \in E(\overline{\mathbb{F}}_q);\; l \cdot P = \mathcal{O} \Big\}.$$

Diese Gruppe wird als $l$-**Torsionsgruppe** bezeichnet. Wir kennen einige Eigenschaften dieser Untergruppe, insbesondere ist die Struktur dieser Gruppe bekannt:

**Satz 3.1** *Ist $l$ teilerfremd zu $q$, so gilt $E[l] \cong \mathbb{F}_l \times \mathbb{F}_l$.*

**Beweis:** [Si85, Cor. 6.4.b, Seite 89] ∎

Wir betrachten im folgenden die Einschränkung des Frobenius-Endomorphismus $\Phi_E$ zu $E$ auf die $l$-Torsionsgruppe $E[l]$; aus Gründen der Überschaubarkeit nennen wir diesen Endomorphismus weiterhin $\Phi_E$. Als Einschränkung des „normalen Frobenius-Endomorphismus" erfüllt $\Phi_E$ sicherlich ebenfalls die Gleichung aus Satz 2.13. Da die Einschränkung nur für Punkte der Ordnung $l$ definiert ist, können wir die beiden „Zahlen" $c$ und $q$ modulo $l$ reduzieren, denn für Punkte $Q \in E[l]$ gilt $k \cdot Q = k' \cdot Q$ genau dann, wenn $k \equiv k' \bmod l$ ist. Damit erfüllt die Einschränkung sogar die Gleichung

$$\Phi_E^2 - \overline{c}\,\Phi_E + \overline{q} \quad = \quad 0, \tag{3.1}$$

wobei $\overline{c}$, $\overline{q}$ die kleinsten positiven Reste von $c$ bzw. $q$ modulo $l$ sind. Nach Satz 3.1 können wir $E[l]$ als 2-dimensionalen $\mathbb{F}_l$-Modul auffassen. Dann ist das Polynom

$$f(X) \quad = \quad X^2 - \overline{c}\,X + \overline{q} \quad \in \mathbb{F}_l[X]$$

ein Vielfaches des Minimalpolynoms von $\Phi_E$. Nach [Si85, Prop. 2.3, Seite 134] ist $f(X)$ sogar das charakteristische Polynom von $\Phi_E$. Betrachten wir dann das Minimalpolynom von $\Phi_E$, so gibt es zwei mögliche Fälle:

1. das Minimalpolynom von $\Phi_E$ besitzt Grad 1,
2. das Minimalpolynom von $\Phi_E$ besitzt Grad 2 und ist damit gleich dem charakteristischen Polynom $f(X)$.

Untersuchen wir im folgenden, welche Auswirkungen diese beiden Fälle auf mögliche Werte für $\overline{c}$ haben. Falls das Minimalpolynom Grad eins besitzt, muß das charakteristische Polynom $f(X)$ als

$$f(X) \quad = \quad (X - \alpha)^2$$

zerfallen. Diese Gleichung liefert direkt mögliche Werte für $\overline{c} \bmod l$: durch Koeffizientenvergleich erhalten wir die Gleichungen

$$\begin{aligned} \overline{c} \quad &\equiv \quad 2 \cdot \alpha \mod l, \\ \overline{q} \quad &\equiv \quad \alpha^2 \mod l. \end{aligned}$$

Daraus folgt durch einfaches Umrechnen, daß

$$\overline{c} \equiv \pm 2 \cdot \sqrt{\overline{q}} \mod l$$

gilt, wobei $\sqrt{\overline{q}}$ eine Quadratwurzel modulo $l$ von $\overline{q}$ ist. Damit können wir in Fall 1 genau 2 mögliche Werte für $\overline{c}$ bestimmen.

Behandeln wir nun den zweiten Fall, daß das Minimalpolynom gleich dem charakteristischen Polynom ist. Wir nehmen an, daß $\alpha$, $\beta$ die beiden Nullstellen des Polynoms $f(X)$ in seinem Zerfällungskörper sind, d.h. es gilt

$$f(X) \quad = \quad (X-\alpha)\cdot(X-\beta).$$

Dabei sind wegen des Grades von $f(X)$ entweder beide Nullstellen Elemente des Grundkörpers $\mathbb{F}_l$ oder aber Elemente des quadratischen Erweiterungskörpers $\mathbb{F}_{l^2}$. Wir gehen nun wie im ersten Fall vor und führen einen Koeffizientenvergleich durch. Dann erhalten wir die Gleichungen (in dem jeweiligen Körper $\mathbb{F}_l$ bzw. $\mathbb{F}_{l^2}$)

$$\begin{aligned} \alpha+\beta &= \overline{c}, \\ \alpha\cdot\beta &= \overline{q}. \end{aligned}$$

Aus diesen zwei Gleichungen erhalten wir

$$\overline{c} \quad = \quad \alpha + \overline{q}\cdot\alpha^{-1}.$$

Offensichtlich reicht dies nicht aus, um $\overline{c}$ eindeutig zu bestimmen. Nehmen wir daher an, wir wüßten die Ordnung $d$ des Elements $\alpha\cdot\beta^{-1}$ in $\mathbb{F}_l$ bzw. $\mathbb{F}_{l^2}$. Dann ist $\alpha\cdot\beta^{-1} = \zeta_d$, wobei $\zeta_d$ ein Element der Ordnung $d$ im jeweiligen Körper ist. Damit erhalten wir die neue Gleichung

$$\alpha^2 \quad = \quad \overline{q}\cdot\zeta_d.$$

Kombinieren wir beide Gleichungen, so erhalten wir eine Gleichung für $\overline{c}$ als

$$\overline{c} \quad = \quad (\zeta_d+1)\cdot\sqrt{\overline{q}\cdot\zeta_d^{-1}}.$$

Leider kennen wir das Element $\zeta_d$ nicht. Bestimmen wir aber alle Elemente der Ordnung $d$ in dem jeweiligen Körper und verwenden wir alle diese Elemente in dieser Gleichung, so erhalten wir mögliche Werte für $\overline{c}$. Insbesondere ist der korrekte Wert von $\overline{c}$ in der Menge aller solcher Lösungen enthalten. Wir haben also Information über $\overline{c}$ bestimmt. Da es genau $\varphi(d)$ viele Elemente der Ordnung $d$ in dem jeweiligen Körper gibt und da inverse Elemente dieselben Möglichkeiten für $\overline{c}$ liefern, erhalten wir insgesamt genau $\varphi(d)$ viele Möglichkeiten für $\overline{c}$. Dabei sei $\varphi$ die Eulersche $\varphi$-Funktion. Wir schätzen diese Anzahl in dem folgenden Lemma ab.

**Lemma 3.2** *Falls $f(X)$ über $\mathbb{F}_l$ zerfällt, so erhalten wir mit dieser Vorgehensweise maximal $\frac{l-1}{2}-1$ viele mögliche Werte für $\overline{c}$; ist $f(X)$ irreduzibel über $\mathbb{F}_l$, so ist die Anzahl der möglichen Werte maximal $\frac{l+1}{2}-1$.*

**Beweis:** Zuerst zu dem Fall, daß $f(X)$ über dem Körper $\mathbb{F}_l$ zerfällt. Dann ist $\alpha\cdot\beta^{-1}$ ein Element von $\mathbb{F}_l^*$. Damit muß die Ordnung $d$ dieses Elements ein Teiler von $l-1$ sein. Da $l$ ungerade ist, tritt die maximale Anzahl von Möglichkeiten genau dann auf, wenn $(l-1)/2$ eine Primzahl und $d$ gleich $l-1$ ist. Berechnen wir $\varphi(d)$ für diesen Fall, so erhalten wir den ersten Teil des Lemmas.

Sei $f(X)$ nun irreduzibel über $\mathbb{F}_l$ und $\alpha$, $\beta$ die beiden Nullstellen über $\mathbb{F}_{l^2}$. Da $\beta$ die zu $\alpha$ konjugierte Nullstelle ist, gilt $\beta = \alpha^l$. Damit ist

$$\alpha \cdot \beta^{-1} \quad = \quad \alpha^{1-l}.$$

Die Ordnung dieses Elements muß die Gruppenordnung von $\mathbb{F}_{l^2}^*$, also $l^2 - 1$ teilen. Genauer muß die Ordnung $d$ des Elements $\alpha \cdot \beta^{-1}$ sogar $l + 1$ teilen, denn aus

$$\left(\alpha \cdot \beta^{-1}\right)^d \quad = \quad \left(\alpha^{1-l}\right)^d \quad = \quad 1$$

folgt $(1 - l)d$ teilt $l^2 - 1$ bzw. $d$ teilt $l + 1$. Die obere Schranke für die Anzahl der Möglichkeiten ergibt sich dann wie im ersten Fall. ■

Damit können wir Informationen über die Spur des Frobenius-Endomorphismus bestimmen, wenn wir wissen, wie das Polynom $f(X)$ zerfällt. Leider kennen wir dieses Polynom $f(X)$ allerdings nicht. Im folgenden Abschnitt werden wir daher untersuchen, wie wir den Zerfällungstyp dieses Polynoms auf die Untersuchung bestimmter Untergruppen der $l$-Torsionsgruppe reduzieren können.

## 3.2 Das Verhalten von $l$-Gruppen unter $\Phi_E$

Zur Lösung des gerade gestellten Problems betrachten wir das Verhalten bestimmter Untergruppen der $l$-Torsionsgruppe bei Anwendung des eingeschränkten Frobenius-Endomorphismus. Diese Untergruppen werden wir im folgenden $l$-Gruppen nennen (obwohl dieser Begriff in der Algebra eine etwas andere Bedeutung besitzt). Für uns ist eine **$l$-Gruppe** eine Untergruppe von $E(\overline{\mathbb{F}}_q)$ der exakten Ordnung $l$. Offensichtlich ist jede $l$-Gruppe sogar eine Untergruppe der $l$-Torsionsgruppe $E[l]$.

Wir haben im vorherigen Abschnitt verschiedene Fälle unterschieden, wie das Polynom $f(X) = X^2 - \overline{c}X + \overline{q}$ zerfallen kann. Für diese Fälle untersuchen wir nun, welche Auswirkungen dies auf das Verhalten von $l$-Gruppen unter dem Frobenius-Endomorphismus hat. Wir sagen, daß eine $l$-Gruppe $C$ **invariant** unter einem Endomorphismus $\kappa$ ist, wenn $\kappa(C) \subseteq C$ ist. Ist $\kappa$ nicht der Nullendomorphismus, so gilt wegen der Primalität von $l$ sogar $\kappa(C) = C$.

Nehmen wir zuerst an, daß das charakteristische Polynom $f(X)$ von $\Phi_E$ als $f(X) \equiv (X - \alpha)^2 \bmod l$ zerfällt. Dann ist $\alpha$ als Nullstelle des charakteristischen Polynoms ein Eigenwert von $\Phi_E$. Es können nun zwei mögliche Unterfälle auftreten, wenn wir den Eigenraum betrachten:

1.1 Die Dimension des Eigenraums ist zwei, d.h. der Eigenraum ist $E[l]$. Dann sind alle Elemente in $E[l]$ Eigenvektoren und daher sind alle $l$-Gruppen von $E[l]$ invariant unter $\Phi_E$.

Wir haben in Abschnitt 3.1 gesehen, daß wir damit wissen, daß $c \equiv \pm 2\sqrt{q} \bmod l$ ist. Wie wir in dem folgenden Lemma zeigen, können wir in diesem speziellen Fall sogar zwei mögliche Werte für $c$ modulo $l^2$ bestimmen.

**Lemma 3.3** *Sei $0 \leq \alpha < l$ gegeben, so daß für alle $l$-Torsionspunkte $Q$ gilt $\Phi_E(Q) = \alpha \cdot Q$. Dann gilt sogar $c \equiv \alpha + q\,\alpha^{-1} \bmod l^2$.*

**Beweis:** Sei $P$ ein beliebiger $l^2$-Torsionspunkt. Dann ist $l \cdot P$ ein $l$-Torsionspunkt und damit gilt $\Phi_E(l \cdot P) = \alpha \cdot l \cdot P$, wobei $\alpha$ wie im Lemma gegeben wird. Somit ist $l \cdot (\Phi_E(P) - \alpha \cdot P) = \mathcal{O}$ und wir erhalten $\Phi_E(P) = \alpha \cdot P + T$, wobei $T$ ein $l$-Torsionspunkt ist. Hieraus folgt

$$\begin{aligned}
\mathcal{O} &= \Phi_E^2(P) - c\,\Phi_E(P) + q \cdot P \\
&= \alpha^2 \cdot P + 2\,\alpha \cdot T - c\,(\alpha \cdot P + T) + q \cdot P \\
&= (\alpha^2 - c\,\alpha + q) \cdot P.
\end{aligned}$$

Dabei beachte man, daß $2\alpha \equiv c \bmod l$ ist und daß sich daher die beiden Summanden $2\alpha \cdot T$ und $c \cdot T$ auslöschen. Damit folgt

$$c \equiv \alpha + q \cdot \alpha^{-1} \mod l^2.$$ ■

Damit erhalten wir in diesem Fall zwei mögliche Werte für $c \bmod l^2$, denn – wie wir schon gesehen haben – gibt es nur zwei Möglichkeiten für $\alpha$, nämlich die beiden Quadratwurzeln modulo $l$ aus $q$.

1.2 Die Dimension des Eigenraums ist eins. Sei $P_1$ ein Erzeuger des Eigenraums und $P_2$ ein beliebiger $l$-Torsionspunkt, der nicht in dem Eigenraum liegt. Dann existiert $r \in \mathbb{F}_l^*$ mit

$$\Phi_E(P_1) = \alpha \cdot P_1 \quad \text{und} \quad \Phi_E(P_2) = r \cdot P_1 + \alpha \cdot P_2,$$

denn das charakteristische Polynom von $\Phi_E$ besitzt die doppelte Nullstelle $\alpha$ und daher müssen die beiden Diagonalelemente der zugehörigen Abbildungsmatrix $\alpha$ sein. Um die minimale Potenz des Frobenius-Endomorphismus zu bestimmen, unter der die von $P_2$ erzeugte $l$-Gruppe invariant ist, formulieren wir das folgende Lemma.

**Lemma 3.4** *Für $i \in \mathbb{N}$ gilt in dieser Situation $\Phi_E^i(P_2) = i \cdot \alpha^{i-1} \cdot r \cdot P_1 + \alpha^i \cdot P_2$.*

**Beweis:** Der Beweis geschieht durch Induktion. Der Fall $i = 1$ ist offensichtlich, sei die Behauptung daher für alle $i \leq k$ bewiesen. Dann gilt

$$\begin{aligned}
\Phi_E^{k+1}(P_2) &= \Phi_E(\,\Phi_E^k(P_2)\,) \\
&= \Phi_E(k \cdot \alpha^{k-1} \cdot r \cdot P_1 + \alpha^k \cdot P_2) \\
&= k \cdot \alpha^{k-1} \cdot r \cdot \Phi_E(P_1) + \alpha^k \cdot \Phi_E(P_2) \\
&= k \cdot \alpha^k \cdot r \cdot P_1 + \alpha^k \cdot (r \cdot P_1 + \alpha \cdot P_2) \\
&= (k+1) \cdot \alpha^k \cdot r \cdot P_1 + \alpha^{k+1} \cdot P_2.
\end{aligned}$$ ■

Bestimmen wir damit die minimale Zahl $i > 0$, für die $\Phi_E^i(P_2) \in \langle P_2 \rangle$ ist, so erhalten wir aus $i \cdot \alpha^{i-1} \cdot r \equiv 0 \bmod l$ direkt $i = l$. Also ist die minimale Potenz von $\Phi_E$, unter der die $l$-Gruppe $\langle P_2 \rangle$ invariant ist, $l$. Leicht zeigt man, daß dies auch für alle anderen von $\langle P_1 \rangle$ verschiedenen $l$-Gruppen gilt. Damit gibt es genau eine unter $\Phi_E$ invariante $l$-Gruppe und die minimale Potenz von $\Phi_E$, unter der alle von $\langle P_1 \rangle$ verschiedenen $l$-Gruppen invariant sind, ist $l$.

Anschließend untersuchen wir den Fall 2 aus Abschnitt 3.1, daß das Minimalpolynom von $\Phi_E$ gleich dem charakteristischen Polynom $f(X)$ ist. Seien wiederum $\alpha \neq \beta$ die Nullstellen von $f(X)$ in seinem Zerfällungskörper, also $f(X) = (X - \alpha) \cdot (X - \beta)$. Wir unterscheiden zwei Fälle:

2.1 Seien $\alpha, \beta \in \mathbb{F}_l$. Dann bilden die beiden zugehörigen Eigenvektoren $P_1$ und $P_2$ eine Basis des $\mathbb{F}_l$-Moduls $E[l]$ (die Eigenwerte $\alpha$ und $\beta$ sind verschieden) und es gilt

$$\Phi_E(P_1) \quad = \quad \alpha \cdot P_1 \qquad \text{und} \qquad \Phi_E(P_2) \quad = \quad \beta \cdot P_2.$$

Damit gibt es mindestens zwei unter $\Phi_E$ invariante $l$-Gruppen, nämlich die von $P_1$ bzw. $P_2$ erzeugten $l$-Gruppen. Sei nun $Q$ der Erzeuger einer beliebigen weiteren $l$-Gruppe, und sei etwa $Q = x_1 \cdot P_1 + x_2 \cdot P_2$ mit $x_1 \cdot x_2 \not\equiv 0 \bmod l$. Dann gilt für $i \geq 1$

$$\begin{aligned} \Phi_E^i(Q) &= \Phi_E^i(x_1 \cdot P_1 + x_2 \cdot P_2) \\ &= x_1 \cdot \Phi_E^i(P_1) + x_2 \cdot \Phi_E^i(P_2) \\ &= x_1 \cdot \alpha^i \cdot P_1 + x_2 \cdot \beta^i \cdot P_2. \end{aligned}$$

Ist $i$ gleich der Ordnung $d$ von $\alpha \cdot \beta^{-1}$ in $\mathbb{F}_l^*$, so gilt $\alpha^d = \beta^d$ und damit insbesondere

$$\Phi_E^d(Q) \quad = \quad \alpha^d \cdot (x_1 \cdot P_1 + x_2 \cdot P_2) \quad = \quad \alpha^d \cdot Q.$$

Also ist die von $Q$ erzeugte $l$-Gruppe invariant unter $\Phi_E^d$, wobei $d$ die Ordnung von $\alpha \cdot \beta^{-1}$ ist. Weiterhin erkennen wir durch die folgende Beobachtung, daß für keine Zahl $0 < i < d$ die von $Q$ erzeugte $l$-Gruppe invariant unter $\Phi_E^i$ ist. Wäre dies der Fall, so gäbe es eine Zahl $0 < k < l$ mit

$$k \cdot x_1 \cdot P_1 + k \cdot x_2 \cdot P_2 \;=\; k \cdot Q \;=\; \Phi_E^i(Q) \;=\; \alpha^i \cdot x_1 \cdot P_1 + \beta^i \cdot x_2 \cdot P_2.$$

Damit erhalten wir $\alpha^i \equiv k \bmod l$ und $\beta^i \equiv k \bmod l$, was offensichtlich ein Widerspruch dazu ist, daß $d$ die Ordnung von $\alpha \cdot \beta^{-1}$ ist. Also sind in diesem Fall genau zwei $l$-Gruppen invariant unter $\Phi_E$ und die minimale Potenz von $\Phi_E$, unter der alle anderen $l$-Gruppen invariant sind, ist genau die Ordnung von $\alpha \cdot \beta^{-1}$ in der multiplikativen Gruppe $\mathbb{F}_l^*$.

2.2 Sei $f(X)$ irreduzibel in $\mathbb{F}_l$ und seien $\alpha$ und $\beta = \alpha^l$ die beiden Nullstellen in $\mathbb{F}_{l^2}$. In diesem Fall kann keine $l$-Gruppe invariant unter $\Phi_E$ sein, denn sonst gäbe es einen Eigenwert in $\mathbb{F}_l$, und $f(X)$ müßte eine Nullstelle in $\mathbb{F}_l$ besitzen.

Den reduzierten Frobenius-Endomorphismus fassen wir nun als Endomorphismus von $\mathbb{F}_l \times \mathbb{F}_l$ auf. Wir betten $\mathbb{F}_l \times \mathbb{F}_l$ wie üblich in die Gruppe $\mathbb{F}_{l^2} \times \mathbb{F}_{l^2}$ ein. Durch Bestimmung der Abbildungsmatrix von $\Phi_E$ angewandt auf die Basis $\{(1,0),(0,1)\}$ von $\mathbb{F}_l \times \mathbb{F}_l$ können wir $\Phi_E$ auf $\mathbb{F}_{l^2} \times \mathbb{F}_{l^2}$ fortsetzen. Da die beiden Eigenwerte dieser Abbildung Elemente von $\mathbb{F}_{l^2}$ sind, gibt es zwei Eigenvektoren in $\mathbb{F}_{l^2} \times \mathbb{F}_{l^2}$, etwa $\underline{v}_1, \underline{v}_2$, die eine Basis von $\mathbb{F}_{l^2} \times \mathbb{F}_{l^2}$ bilden. Sei dann $\underline{v}$ ein Erzeuger einer beliebigen $l$-Gruppe und sei

$$\underline{v} \quad = \quad x_1 \cdot \underline{v}_1 + x_2 \cdot \underline{v}_2 \qquad \text{mit} \quad x_1, x_2 \in \mathbb{F}_{l^2}.$$

Wenden wir nun Potenzen des fortgesetzten Endomorphismus $\Phi_E$ auf $\underline{v}$ an, so erhalten wir

$$\begin{aligned} \Phi_E^i(\underline{v}) &= x_1 \cdot \Phi_E^i(\underline{v}_1) + x_2 \cdot \Phi_E^i(\underline{v}_2) \\ &= x_1 \cdot \alpha^i \cdot \underline{v}_1 + x_2 \cdot \beta^i \cdot \underline{v}_2. \end{aligned}$$

Nehmen wir wieder an, daß $d$ der minimale Exponent ist, so daß $\Phi_E^d(\underline{v}) = k \cdot \underline{v}$ mit einem Element $k \in \mathbb{F}_{l^2}^*$ ist, so ergibt sich ein System von zwei Bedingungen. Lösen wir dies, so muß $d$ die minimale Zahl mit

$$\alpha^d \quad = \quad \beta^d$$

in $\mathbb{F}_{l^2}^*$ sein, d.h. $d$ ist die Ordnung von $\alpha \cdot \beta^{-1}$ in $\mathbb{F}_{l^2}^*$. Weiterhin gilt wegen $\beta = \alpha^l$ ($\beta$ ist die zu $\alpha$ konjugierte Nullstelle) für das Element $k$

$$k \quad = \quad \beta^d \quad = \quad \alpha^{ld} \quad = \quad k^l,$$

d.h. es gilt sogar $k \in \mathbb{F}_l^*$. Damit ist die minimale Potenz von $\Phi_E$, unter der die von $Q$ erzeugte $l$-Gruppe invariant ist, genau gleich der Ordnung von $\alpha \cdot \beta^{-1}$ in $\mathbb{F}_{l^2}^*$. Da wir $Q$ nicht genauer spezifiziert hatten, gilt dies für alle $l$-Gruppen. Aus $\beta = \alpha^l$ können wir noch eine Bedingung an $d$ herleiten. Es gilt

$$(\alpha \cdot \beta^{-1})^d \quad = \quad \alpha^{(1-l)\cdot d} \quad = \quad 1$$

und $(1-l) \cdot d$ muß damit ein Teiler der Gruppenordnung $\#\mathbb{F}_{l^2}^* = l^2 - 1 = (l-1)\cdot(l+1)$ sein. Also ist $d$ ein Teiler von $l+1$.

Damit sind wir in der Lage, eine genaue Klassifizierung der möglichen Wirkungen des Frobenius-Endomorphismus auf $l$-Gruppen vorzunehmen. Mit den im vorherigen Abschnitt 3.1 vorgestellten Ergebnissen liefert der folgende Satz direkt auch Information über $c \bmod l$.

**Satz 3.5** *Sei $E$ eine elliptische Kurve über $\mathbb{F}_q$ und $l \in \mathbb{P}_{>2}, l \neq p$. Sei $\Phi_E$ die Einschränkung des Frobenius-Endomorphismus auf die $l$-Torsionsgruppe $E[l]$. Dann gilt für das charakteristische Polynom $f(X)$ von $\Phi_E$*

1. *$f(X) = (X-\alpha)^2 \iff$ entweder alle $l$-Gruppen sind invariant unter $\Phi_E$ oder genau eine $l$-Gruppe ist invariant unter $\Phi_E$ und die minimale Potenz von $\Phi_E$, unter der alle anderen $l$-Gruppen invariant sind, ist $l$.*

2.1 $f(X) = (X - \alpha) \cdot (X - \beta)$ *mit* $\alpha, \beta \in \mathbb{F}_l$, $\operatorname{ord}(\alpha \cdot \beta^{-1}) = d > 1 \iff$ *genau zwei* $l$*-Gruppen sind invariant unter* $\Phi_E$*; die minimale Potenz von* $\Phi_E$*, unter der alle anderen* $l$*-Gruppen invariant sind, ist* $d$*.*

2.2 $f(X) = (X - \alpha) \cdot (X - \alpha^l)$ *mit* $\alpha \in \mathbb{F}_{l^2} - \mathbb{F}_l$, $\operatorname{ord}(\alpha^{1-l}) = d \iff$ *die minimale Potenz von* $\Phi_E$*, unter der alle* $l$*-Gruppen invariant sind, ist* $d$*; keine* $l$*-Gruppe ist unter einer kleineren Potenz von* $\Phi_E$ *invariant.*

**Beweis:** Die Behauptung, wie aus dem Zerfällungstyp von $f(X)$ das Verhalten von $\Phi_E$ auf den $l$-Gruppen folgt, haben wir gerade gezeigt. Um die andere Richtung der Behauptung zu zeigen, beachte man nur, daß alle auftretenden Möglichkeiten für Wirkungen von $\Phi_E$ auf $l$-Gruppen eindeutig einem bestimmten Zerfällungstyp zugeordnet werden können. Man beachte etwa nur, wieviele unter $\Phi_E$ invariante $l$-Gruppen es jeweils gibt. ■

Damit hat sich das Problem der Bestimmung des Zerfällungstyps des charakteristischen Polynoms des eingeschränkten Frobenius-Endomorphismus $\Phi_E$ darauf reduziert, festzustellen, wie sich die $l$-Gruppen unter Potenzen des Frobenius-Endomorphismus $\Phi_E$ verhalten. Wir werden im nächsten Abschnitt eine Verbindung zwischen diesen Fragen und Isogenien bestimmter elliptischer Kurven herstellen.

## 3.3 $l$-Gruppen und Isogenien

Wir müssen nun das Verhalten aller $l$-Gruppen von $E(\overline{\mathbb{F}}_q)$ bei Anwendung von Potenzen des Frobenius-Endomorphismus untersuchen. Dieses Problem ist allerdings immer noch sehr „unhandlich“, so daß wir eine weitere Reduktion durchführen werden. Dazu vergleichen wir das Verhalten der $l$-Gruppen mit den $j$-Invarianten bestimmter zu $E$ isogener Kurven. Bevor wir allerdings darauf näher eingehen, bestimmen wir in dem folgenden Lemma die Anzahl der $l$-Gruppen.

**Lemma 3.6** *Sind* $l$ *und* $q$ *teilerfremd, so gibt es in* $E(\overline{\mathbb{F}}_q)$ *genau* $l + 1$ *verschiedene* $l$*-Gruppen.*

**Beweis:** Wir haben schon gesehen, daß jede $l$-Gruppe eine Untergruppe der $l$-Torsiongruppe ist. Sei also $\{P_1, P_2\}$ eine Basis von $E[l]$. Dann werden alle $l$-Gruppen gegeben als

$$\begin{aligned} C_i &= \{m \cdot (P_1 + i \cdot P_2)\,;\ m = 0, \ldots, l-1\} \qquad \text{für} \quad i = 0, \ldots, l-1, \\ C_l &= \{m \cdot P_2;\ m = 0, \ldots, l-1\}. \end{aligned}$$

Offensichtlich ist jede Menge $C_i$ eine $l$-Gruppe. Leicht erkennen wir außerdem, daß sich im Schnitt zweier $l$-Gruppen nur das Element $\mathcal{O}$ befindet. Damit müssen dies alle $l$-Gruppen sein, denn die Ordnung der Vereinigung aller dieser $C_i$ ist $l^2$ und damit gleich der Ordnung der $l$-Torsionsgruppe $E[l]$ (vgl. Satz 3.1). ■

Wir wollen nun untersuchen, wie die Verbindung zwischen Isogenien und solchen $l$-Gruppen aussieht. Als Basis dazu dient die folgende Proposition aus [Si85, Prop. 4.12, Seite 78].

**Proposition 3.7** *Sei $E$ eine elliptische Kurve und $C$ eine endliche Untergruppe von $E$. Dann gibt es eine (bis auf Isomorphie) eindeutig bestimmte elliptische Kurve $E/C$ und eine Isogenie $\psi : E \to E/C$ mit $Kern(\psi) = C$.*

Aus [Ve71] und [El] erhalten wir sogar die genaue Gestalt der elliptischen Kurve $E/C$ und der Isogenie $\psi$. Sei etwa $\psi(P) = (x'(P), y'(P))$ und $E/C$ gegeben durch $(a', b')$. Dann gilt mit den Koordinatenfunktionen $x(P)$, $y(P)$ von $E = (a, b)$

$$\begin{aligned}
x'(P) &= x(P) + \sum_{\substack{Q \in C \\ Q \neq \mathcal{O}}} [\, x(P+Q) - x(Q)\,], \\
y'(P) &= y(P) + \sum_{\substack{Q \in C \\ Q \neq \mathcal{O}}} [\, y(P+Q) - y(Q)\,], \\
a' &= a - 5 \cdot \sum_{\substack{Q \in C \\ Q \neq \mathcal{O}}} \Big[\, 3 \cdot x^2(Q) + a \,\Big], \\
b' &= b - 7 \cdot \sum_{\substack{Q \in C \\ Q \neq \mathcal{O}}} \Big[\, 5 \cdot x^3(Q) + 3 \cdot a \cdot x(Q) + 2 \cdot b \,\Big].
\end{aligned}$$

Zu einer gegebenen Untergruppe $C$ von $E(\overline{\mathbb{F}}_q)$ ist damit die elliptische Kurve $E/C$ bis auf Isomorphie über dem algebraischen Abschluß eindeutig definiert. Analog definieren wir $j/C$ als die $j$-Invariante dieser elliptischen Kurve $E/C$. Wir wollen nun untersuchen, wie das Verhalten von zyklischen Untergruppen $C$ unter Potenzen des Frobenius-Endomorphismus und die $j$-Invarianten der zugehörigen Kurven $E/C$ zusammenhängen. Dazu beachten wir den folgenden Satz.

**Satz 3.8** *Sei $E$ eine elliptische Kurve über $\mathbb{F}_q$ und $C$ eine zyklische Untergruppe von $E(\overline{\mathbb{F}}_q)$. Dann gilt*

$$\min\{\, i \in \mathbb{N};\ \Phi_E^i(C) \subseteq C\} \quad \geq \quad \min\{\, i \in \mathbb{N};\ j/C \in \mathbb{F}_{q^i}\}.$$

**Beweis:** Sei also $C = \langle H \rangle$ eine zyklische Untergruppe von $E(\overline{\mathbb{F}}_q)$ und $d$ die minimale Potenz von $\Phi_E$, so daß $\Phi_E^d(C) \subseteq C$ gilt. Wir müssen zeigen, daß dann $j/C \in \mathbb{F}_{q^d}$ gilt.

Überprüfen wir dazu für die im Anschluß an Proposition 3.7 angegebene elliptische Kurve $E/C = (a', b')$, ob sie über dem Körper $\mathbb{F}_{q^d}$ definiert ist. Wir zeigen dies für $a'$, der Beweis für $b' \in \mathbb{F}_{q^d}$ läuft analog. Sei dazu $\Phi$ der Frobenius-Automorphismus für den endlichen Körper $\mathbb{F}_q$, d.h. der Endomorphismus von $\mathbb{F}_q$, der jedes Element $x$ auf $x^q$ abbildet. Dann gilt aufgrund der Formel für $a'$

$$\Phi^d(a') \quad = \quad \Phi^d\Big(a - 5 \cdot \sum_{\substack{Q \in C \\ Q \neq \mathcal{O}}} [\, 3 \cdot x^2(Q) + a \,]\Big)$$

$$\begin{aligned}
&= \Phi^d(a) - 5 \cdot \sum_{\substack{Q\in C\\ Q\neq\mathcal{O}}} [\, 3\cdot\Phi^d(x^2(Q)) + \Phi^d(a)\,] \\
&= a - 5\cdot \sum_{\substack{Q\in C\\ Q\neq\mathcal{O}}} [\, 3\cdot x^2(\Phi_E^d(Q)) + a\,] \\
&= a - 5\cdot \sum_{\substack{Q'\in C\\ Q'\neq\mathcal{O}}} [\, 3\cdot x^2(Q') + a\,] \\
&= a'.
\end{aligned}$$

Dabei beachte man, daß $\Phi^d(x^2(Q)) = x^2(\Phi_E^d(Q))$ gilt, was man direkt aus der Definition der Abbildungen $\Phi$ und $\Phi_E$ erkennt. Weiterhin wurde benutzt, daß die elliptische Kurve $E$ und damit $a$ und $b$ über dem Körper $\mathbb{F}_q$ definiert sind.

Damit ist die elliptische Kurve $E/C = (a', b')$ über $\mathbb{F}_{q^d}$ definiert und somit gilt insbesondere $j/C \in \mathbb{F}_{q^d}$. ■

Die umgekehrte Ungleichung in diesem Satz gilt im allgemeinen nicht. Wir werden aber im folgenden Satz 3.10 zeigen, daß die Umkehrung für eine spezielle Klasse von elliptischen Kurven doch gilt. Bevor wir dies beweisen können, müssen wir in folgendem Satz die nötigen Voraussetzungen schaffen.

**Satz 3.9** *Seien $E, E'$ nicht supersinguläre elliptische Kurven über dem endlichen Körper $\mathbb{F}_q$, die über einem Erweiterungskörper $\mathbb{F}_{q^d}$ isogen sind. Weiterhin gebe es keine über $\mathbb{F}_q$ definierte Isogenie von $E$ zu einer elliptischen Kurve mit $j$-Invariante gleich 0 oder 1728. Dann gibt es eine zu $E'$ isomorphe elliptische Kurve $E''/\mathbb{F}_q$, so daß $E$ sogar über $\mathbb{F}_q$ isogen zu $E''$ ist.*

**Beweis:** Zum Beweis dieses Satzes benutzen wir das folgende Kriterium von Tate [Ta66, Th. 1, (c1),(c2)]:

Für jeden Erweiterungskörper $\mathbb{F}_{q^d}$ sind zwei über $\mathbb{F}_q$ definierte elliptische Kurven $E, E'$ genau dann $\mathbb{F}_{q^d}$-isogen, wenn die charakteristischen Polynome von $\Phi_E^d$ und $\Phi_{E'}^d$ gleich sind.

Da $E$ und $E'$ nicht supersingulär sind, bilden die jeweiligen Endomorphismenringe $R$ bzw. $R'$ eine Ordnung in einem imaginärquadratischen Zahlkörper. Seien die charakteristischen Polynome der beiden Frobenius-Endomorphismen gegeben als

$$f_E(X) \;=\; (X-\pi_1)\cdot(X-\overline{\pi}_1) \qquad \text{und} \qquad f_{E'}(X) \;=\; (X-\pi_2)\cdot(X-\overline{\pi}_2),$$

wobei $\pi_1 \in R$ und $\pi_2 \in R'$ gilt. Dabei können wir ohne Einschränkung annehmen, daß $\Phi_E$ (bzw. $\Phi_{E'}$) der algebraischen Zahl $\pi_1$ (bzw. $\pi_2$) entspricht. Wegen der Ordinarität von $E$ ist offensichtlich $\mathbb{Q}(\pi_1) = \mathbb{Q}(\pi_1^d)$, denn $\pi_1$ erfüllt das ganzzahlige Polynom $f_E(X)$ vom Grad 2. Aus der Voraussetzung des Satzes wissen wir, daß $E$ und $E'$ über $\mathbb{F}_{q^d}$ isogen sind und daß damit die charakteristischen Polynome von $\Phi_E^d$ und $\Phi_{E'}^d$ gleich sind. Diese werden gegeben als

$$g_E(X) \;=\; (X-\pi_1^d)\cdot(X-\overline{\pi}_1^d) \;=\; (X-\pi_2^d)\cdot(X-\overline{\pi}_2^d) \;=\; g_{E'}(X).$$

Damit können wir ohne Einschränkung annehmen, daß $\pi_1^d = \pi_2^d$ ist. Somit gilt

$$\mathbb{Q}(\pi_1) \quad = \quad \mathbb{Q}(\pi_1^d) \quad = \quad \mathbb{Q}(\pi_2^d) \quad = \quad \mathbb{Q}(\pi_2).$$

Weiterhin folgt $\pi_1 = \pi_2 \cdot \omega$, wobei $\omega$ eine $d$-te Einheitswurzel in der Maximalordnung von $\mathbb{Q}(\pi_1)$ ist. Dann gibt es aber nur wenige Möglichkeiten für $\omega$ (vgl. [Wei63, Prop. 6.3.1, Seite 238]):

**1.** $\omega = 1$**:** In diesem Fall ist alles klar, denn aus $\pi_1 = \pi_2$ folgt, daß die charakteristischen Polynome $f_E(X)$ und $f_{E'}(X)$ gleich sind und damit ist $E'$ selbst $\mathbb{F}_q$-isogen zu $E$.

**2.** $\omega = -1$**:** Dann ist $\pi_1 = -\pi_2$ und damit gilt $\pi_1 + \overline{\pi}_1 = -(\pi_2 + \overline{\pi}_2)$. Wir wissen aber mit Lemma 2.24, daß es eine zu $E'$ isogene Kurve $E''$ über $\mathbb{F}_q$ gibt, deren Spur des Frobenius-Endomorphismus gerade die negative Spur des Frobenius-Endomorphismus zu $E'$ ist. Damit aber sind $E''$ und $E$ $\mathbb{F}_q$-isogen.

**3.** $\omega \in \{\pm i\}$ **und** $\mathbb{Q}(\pi_1) = \mathbb{Q}(i)$**:**

**4.** $\omega \in \{\pm\zeta, \pm\zeta^2\}$ **mit** $\zeta^2 + \zeta + 1 = 0$ **und** $\mathbb{Q}(\pi_1) = \mathbb{Q}(\sqrt{-3})$**:**

Behandeln wir die beiden verbleibenden Fälle 3. und 4. zusammen. Deuring hat in [De41] gezeigt, daß es eine elliptische Kurve $\tilde{E}/\mathbb{F}_q$ gibt, deren Endomorphismenring isomorph zu dem Ganzheitsring $\mathcal{O}$ des entsprechenden imaginärquadratischen Zahlkörpers $\mathbb{Q}(i)$ bzw. $\mathbb{Q}(\sqrt{-3})$ ist und deren Frobenius-Endomorphismus auf $\pi_1$ abgebildet wird. Die Automorphismengruppe von $\tilde{E}$ ist größer als $\{\pm 1\}$, denn jedes Element der Norm 1 in $\mathcal{O}$ besitzt als Urbild einen Automorphismus. Daher muß $j(\tilde{E}) \in \{0, 1728\}$ gelten [Si85, Th. 10.1, Seite 103]. Außerdem sind die charakteristischen Polynome der Frobenius-Endomorphismen zu $\tilde{E}$ und $E$ gleich (für beide elliptischen Kurven wird der Frobenius-Endomorphismus auf $\pi_1$ abgebildet). Damit ist $E$ $\mathbb{F}_q$-isogen zu $\tilde{E}$, also zu einer Kurve mit $j$-Invariante 1728 bzw. 0. Dies ist aber ein Widerspruch zu unserer Voraussetzung, und somit können beide Fälle 3. und 4. nicht auftreten. ∎

Mit Hilfe dieses Satzes können wir nun endlich das angestrebte Resultat dieses Abschnitts formulieren.

**Satz 3.10** *Sei $E$ eine nicht supersinguläre elliptische Kurve über $\mathbb{F}_q$, die nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist und $C$ eine zyklische Untergruppe von $E(\overline{\mathbb{F}}_q)$, deren Ordnung teilerfremd zu $q$ ist. Dann gilt*

$$\min\{\, i \in \mathbb{N};\ j/C \in \mathbb{F}_{q^i}\} \quad \geq \quad \min\{\, i \in \mathbb{N};\ \Phi_E^i(C) \subseteq C\}.$$

**Beweis:** Sei $j/C \in \mathbb{F}_{q^d}$ und $d$ minimal mit dieser Eigenschaft. Dann können wir mit Proposition 1.4 (c) aus [Si85, Seite 50] annehmen, daß $E/C$ schon über $\mathbb{F}_{q^d}$ definiert ist (ansonsten wenden wir einen Isomorphismus an). Weiterhin können wir mit Lemma 2.20 und dem vorherigen Satz 3.9 annehmen, daß es eine über $\mathbb{F}_{q^d}$

definierte Isogenie von $E/C$ nach $E$ gibt. Sei $\psi : E \to E/C$ „die Isogenie" mit Kern $C$ aus Proposition 3.7 und $\lambda : E/C \to E$ diese über $\mathbb{F}_{q^d}$ definierte Isogenie. Zum Beweis des Satzes genügt es zu zeigen, daß $\psi$ über $\mathbb{F}_{q^d}$ definiert ist. Dann gilt nämlich mit Lemma 2.16, daß

$$\Phi^d_{E/C} \circ \psi \quad = \quad \psi \circ \Phi^d_E$$

ist. Damit gilt für einen beliebigen Punkt $Q \in C$

$$\psi \circ \Phi^d_E(Q) \quad = \quad \Phi^d_{E/C} \circ \psi(Q) \quad = \quad \Phi^d_{E/C}(\mathcal{O}) \quad = \quad \mathcal{O}$$

und $\Phi^d_E(Q)$ muß ein Element des Kernes von $\psi$ sein, d.h. es gilt $\Phi^d_E(C) \subseteq C$.

Zum Beweis dieser Aussage betrachten wir die folgende Abbildung:

$$\begin{array}{rcl} \Lambda :\ \mathrm{Hom}_{\overline{\mathbb{F}}_q}(E, E/C) & \longrightarrow & \mathrm{End}_{\overline{\mathbb{F}}_q}(E) \\ \omega & \longmapsto & \lambda \circ \omega. \end{array}$$

Diese Abbildung ist sicherlich wohldefiniert, es gilt sogar das folgende Lemma.

**Lemma 3.11** *Die Abbildung $\Lambda$ ist injektiv.*

**Beweis (Lemma):** Sei der Grad der (nichtkonstanten) Isogenie $\lambda$ gleich $s$. Dann gibt es wegen Satz 2.9 eine zu $\lambda$ duale Isogenie $\hat{\lambda} : E \to E/C$ mit $\hat{\lambda} \circ \lambda = s$. Nehmen wir nun an, die beiden Elemente $\kappa_1, \kappa_2 \in \mathrm{Hom}_{\overline{\mathbb{F}}_q}(E, E/C)$ hätten dasselbe Bild unter der Abbildung $\Lambda$. Dann gilt offensichtlich auch

$$\hat{\lambda} \circ (\lambda \circ \kappa_1) \quad = \quad \hat{\lambda} \circ (\lambda \circ \kappa_2).$$

Damit erhalten wir aber

$$\kappa_1 \circ s \quad = \quad s \circ \kappa_1 \quad = \quad s \circ \kappa_2 \quad = \quad \kappa_2 \circ s.$$

Als Endomorphismus ist die Abbildung $s$ surjektiv (siehe [ChRo88, Prop. 10.10, Seite 52]) und damit muß $\kappa_1 = \kappa_2$ gelten, d.h. $\Lambda$ ist injektiv. □

Betrachten wir nun das Bild der Elemente $\psi \circ \Phi^d_E$ und $\Phi^d_{E/C} \circ \psi$ aus $\mathrm{Hom}_{\overline{\mathbb{F}}_q}(E, E/C)$ unter der Abbildung $\Lambda$. Es gilt dann nach Definition von $\Lambda$

$$\Lambda(\psi \circ \Phi^d_E) \ = \ \lambda \circ \psi \circ \Phi^d_E \qquad \text{und} \qquad \Lambda(\Phi^d_{E/C} \circ \psi) \ = \ \lambda \circ \Phi^d_{E/C} \circ \psi.$$

Da die Isogenie $\lambda$ über $\mathbb{F}_{q^d}$ definiert ist, gilt mit Lemma 2.16 $\Phi^d_E \circ \lambda = \lambda \circ \Phi^d_{E/C}$. Also erhalten wir

$$\Phi^d_E \circ \lambda \circ \psi \quad = \quad \lambda \circ \Phi^d_{E/C} \circ \psi.$$

Da $E$ nicht supersingulär ist, ist der Endomorphismenring von $E$ isomorph zu einer Ordnung in einem imaginärquadratischen Zahlkörper, also insbesondere abelsch. Damit gilt mit $(\lambda \circ \psi) \in \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$

$$\Phi^d_E \circ (\lambda \circ \psi) \quad = \quad (\lambda \circ \psi) \circ \Phi^d_E$$

und damit

$$\Lambda(\psi \circ \Phi_E^d) \;=\; (\lambda \circ \psi) \circ \Phi_E^d \;=\; \Phi_E^d \circ (\lambda \circ \psi) \;=\; \lambda \circ \Phi_{E/C}^d \circ \psi \;=\; \Lambda(\Phi_{E/C}^d \circ \psi).$$

Wegen der Injektivität von $\Lambda$ folgt daraus die Gleichheit von $\psi \circ \Phi_E^d$ und $\Phi_{E/C}^d \circ \psi$. Damit aber ist nach Lemma 2.16 $\psi$ über $\mathbb{F}_{q^d}$ definiert, und der Beweis des Satzes ist beendet. ■

Durch Kombination der Ergebnisse der Sätze 3.8 und 3.10 erhalten wir das Hauptresultat dieses Abschnitts, das wir in folgendem Korollar formulieren.

**Korollar 3.12** *Ist $E$ eine nicht supersinguläre elliptische Kurve über $\mathbb{F}_q$, die nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist, so gilt für jede zyklische Untergruppe $C$ von $E(\overline{\mathbb{F}}_q)$, deren Ordnung teilerfremd zu $q$ ist,*

$$\min\{\, i \in \mathbb{N};\ j/C \in \mathbb{F}_{q^i}\} \quad = \quad \min\{\, i \in \mathbb{N};\ \Phi_E^i(C) \subseteq C\}.$$

**Bemerkung 3.13** Wir sollten beachten, daß dieses Korollar auch für Gruppen $C$ der Ordnung 2 gilt (dazu beachte man einfach, daß wir in den Sätzen 3.8, 3.9 und 3.10 nie verwendet haben, daß die Ordnung der Untergruppe $C$ ungerade sein soll). Weiterhin ist die Voraussetzung, daß $E$ nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist, für die Korrektheit des Korollars absolut erforderlich.

Betrachten wir zum Beispiel die elliptische Kurve

$$E:\ y^2 \quad = \quad x^3 - b$$

mit $j(E) = 0$, wobei $b \in \mathbb{F}_q^*$ keine 3-te Potenz in dem zugrundeliegenden endlichen Körper $\mathbb{F}_q$ ist. Weiterhin nehmen wir $q \equiv 1 \bmod 3$ an, so daß $E$ nicht supersingulär ist (vgl. [Si85, Bsp. 4.4, Seite 143]). In $E(\mathbb{F}_q)$ gibt es keinen Punkt der Ordnung 2, denn die $x$-Koordinate eines solchen Punktes wäre eine Nullstelle von $X^3 - b$. Seien die drei 2-Gruppen gegeben als $C_1, C_2$ und $C_3$. Dann können wir ohne Einschränkung annehmen, daß

$$\Phi_E(C_1) \quad = \quad C_2, \qquad \Phi_E(C_2) \quad = \quad C_3 \qquad \text{und} \qquad \Phi_E(C_3) \quad = \quad C_1$$

gilt, denn der Frobenius-Endomorphismus bildet nie Punkte ungleich $\mathcal{O}$ auf den Nullpunkt ab und $\Phi_E(C_i) = C_i$ würde bedeuten, daß es einen Zweitorsionspunkt in der Punktgruppe $E(\mathbb{F}_q)$ gibt. Seien $\psi_i$ die Isogenien von $E$ nach $E/C_i$ für $i = 1, 2, 3$. Dann betrachten wir für $(i, j) \in \{(1, 2), (2, 3), (3, 1)\}$ die folgende Abbildung

$$\begin{array}{rcl} E/C_i(\overline{\mathbb{F}}_q) & \longrightarrow & E/C_j(\overline{\mathbb{F}}_q) \\ \psi_i(Q) & \longmapsto & \psi_j(\Phi_E(Q)), \end{array}$$

wobei $Q$ ein Punkt in $E(\overline{\mathbb{F}}_q)$ ist. Die Isogenien $\psi_i$ sind surjektiv, deswegen können wir die Urbilder obiger Abbildung in dieser Form schreiben. Man zeigt dann durch

Nachrechnen, daß dies ein Isomorphismus zwischen $E/C_i(\overline{\mathbb{F}}_q)$ und $E/C_j(\overline{\mathbb{F}}_q)$ ist (und damit insbesondere wohldefiniert ist). Also gilt

$$j/C_1 \quad = \quad j/C_2 \quad = \quad j/C_3.$$

Wir werden im folgenden Kapitel zeigen, daß das Polynom

$$g(X) \quad = \quad (X - j/C_1) \cdot (X - j/C_2) \cdot (X - j/C_3)$$

über $\mathbb{F}_q$ definiert ist. Damit erkennen wir durch Koeffizientenvergleich, daß $j/C_i \in \mathbb{F}_q, i = 1, 2, 3$ ist und wir haben ein Beispiel konstruiert, in dem die Aussage aus Satz 3.10 nicht gilt. Alle $j$-Invarianten $j/C_i$ befinden sich im Grundkörper $\mathbb{F}_q$ (Erweiterungsgrad 1); die minimale Potenz von $\Phi_E$, unter der eine beliebige 2-Gruppe invariant ist, ist aber drei. Allerdings ist in diesem Fall auch die Voraussetzung des Satzes 3.10 nicht erfüllt, denn die $j$-Invariante von $E$ ist selbst schon Null, womit $E$ insbesondere auch $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 ist.

Weiterhin sollte man beachten, daß die Bedingung, daß $E$ nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist, nicht bedeutet, daß die $j$-Invariante von $E$ schon 0 oder 1728 ist. Als Beispiel wähle man $\mathbb{F}_q = \mathbb{Z}/43\mathbb{Z}$. Dann gilt für die beiden elliptischen Kurven $E = (2, 2)$ und $E' = (0, 1)$, daß ihre Punktgruppen über $\mathbb{F}_q$ beide 36 Elemente enthalten und daß es damit eine $\mathbb{F}_q$-Isogenie zwischen beiden Kurven gibt, jedoch ist $j(E) = 35$ sicherlich ungleich 0 oder 1728.

Im folgenden nehmen wir deswegen an, daß $E$ eine nicht supersinguläre elliptische Kurve ist, die auch nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist. Einen Algorithmus zur Überprüfung dieser Bedingungen werden wir in Kapitel 9 angeben. Insbesondere werden wir für diese „ungünstigen“ Fälle zeigen, wie wir direkt die Gruppenordnung $\#E(\mathbb{F}_q)$ berechnen können. Die Ergebnisse dieses Kapitels zusammenfassend, ergibt sich dann folgende Tabelle 3.1 (siehe Seite 34).

Wir suchen nun eine Möglichkeit, mit Hilfe eines (sogenannten modularen) Polynoms festzustellen, in welchem Erweiterungskörper von $\mathbb{F}_q$ sich die $j$-Invarianten $j/C$ für die $l$-Gruppen $C$ befinden. Diese Information liefert mit Hilfe von Korollar 3.12 dann genau die Information über das Verhalten der $l$-Gruppen unter Potenzen des Frobenius-Endomorphismus, woraus wieder Information über die Spur des Frobenius-Endomorphismus modulo $l$ gewonnen werden kann. In dem folgenden Kapitel behandeln wir zunächst die theoretischen Grundlagen und Eigenschaften modularer Polynome. Anschließend beschreiben wir eine Methode, andere „geeignete“ Polynome (sogenannte äquivalente Polynome) zu bestimmen. Die praktische Berechnung solcher Polynome werden wir in Kapitel 5 genau abhandeln.

Tabelle 3.1: Verhalten von $l$-Gruppen und Möglichkeiten für $c \bmod l$

| Verhalten von $l$-Gruppen | Möglichkeiten für $c \bmod l$ |
|---|---|
| alle $l$-Gruppen invariant unter $\Phi_E$ | $c \equiv \alpha + q\,\alpha^{-1} \bmod l^2$, wobei $\alpha^2 \equiv q \bmod l$, $0 < \alpha < l$. |
| eine $l$-Gruppe invariant unter $\Phi_E$, alle anderen invariant unter $\Phi_E^l$ | $c \equiv 2\alpha \bmod l$, wobei $\alpha^2 \equiv q \bmod l$. |
| zwei $l$-Gruppen invariant unter $\Phi_E$, alle anderen unter $\Phi_E^d$ ($d$ minimal) | $c \equiv (\zeta_d + 1)\sqrt{q\,\zeta_d^{-1}} \bmod l$, wobei $\zeta_d \in \mathbb{F}_l$ mit $\operatorname{ord}(\zeta_d) = d$. |
| alle $l$-Gruppen invariant unter $\Phi_E^d$ ($d$ minimal) | $c = (\zeta_d + 1)\sqrt{q\,\zeta_d^{-1}}$, wobei $\zeta_d \in \mathbb{F}_{l^2}$ mit $\operatorname{ord}(\zeta_d) = d$. |

# Kapitel 4

# Modulare und äquivalente Polynome

Wir haben im letzten Kapitel gesehen, daß wir das Zerlegungsverhalten des charakteristischen Polynoms des eingeschränkten Frobenius-Endomorphismus $\Phi_E$ einer elliptischen Kurve $E/\mathbb{F}_q$ zurückführen können auf die Bestimmung von minimalen Körpererweiterungen von $\mathbb{F}_q$, in denen sich spezielle $j$-Invarianten befinden. Die Bestimmung dieses Erweiterungsgrades kann mit Hilfe von sogenannten modularen Polynomen geschehen. In diesem Kapitel werden wir diese Polynome einführen und einige Eigenschaften dieser Polynome beschreiben. Anschließend werden wir die Grundlagen für sogenannte äquivalente Polynome angeben, die in dem Algorithmus anstelle der modularen Polynome verwendet werden können. Im folgenden Kapitel werden wir dann die Berechnung solcher äquivalenter Polynome beschreiben.

## 4.1 Elliptische Kurven über $\mathbb{C}$

Wir werden uns in diesem Abschnitt zuerst mit elliptischen Kurven über dem Körper der komplexen Zahlen beschäftigen. Für diesen Körper werden wir modulare Polynome herleiten. Im Anschluß daran werden wir eine Vorgehensweise angeben, wie wir damit geeignete Polynome für endliche Körper bestimmen können.

Elliptische Kurven über den komplexen Zahlen stehen in einer engen Beziehung zu zweidimensionalen Gittern in $\mathbb{C}$. Wir definieren nun zuerst den Begriff Gitter, bevor wir diesen Zusammenhang erläutern.

**Definition 4.1** *Ein zweidimensionales* **Gitter** *$L$ in $\mathbb{C}$ ist eine Teilmenge*

$$L \quad = \quad \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

*von $\mathbb{C}$ mit $\omega_1, \omega_2 \in \mathbb{C}^*$, $\Im\left(\frac{\omega_2}{\omega_1}\right) > 0$.*

Dann besteht der folgende Zusammenhang zwischen solchen Gittern und elliptischen Kurven über den komplexen Zahlen.

**Satz 4.2** *Sei $L$ ein zweidimensionales Gitter in $\mathbb{C}$. Dann gibt es eine elliptische Kurve $E/\mathbb{C}$, so daß ein Isomorphismus zwischen $\mathbb{C}/L$ und der Punktgruppe $E(\mathbb{C})$ existiert.*

**Beweis:** Zum Beweis kombiniere man [Si85, Prop. 3.6 (b), Seite 158] mit den Isomorphieformeln aus [Si85, Seite 46ff]. ■

Wir können damit viele Probleme für elliptische Kurven über den komplexen Zahlen auf entsprechende Probleme in der Menge aller zweidimensionalen Gitter in $\mathbb{C}$ überführen. Daher macht es Sinn, sich mit der Frage zu beschäftigen, wie sich Isomorphien von elliptischen Kurven über $\mathbb{C}$ auf Gitter auswirken. Dies ist ebenfalls wohlbekannt, es gilt nämlich die folgende Proposition aus [Si85, Cor. 4.1.1, Seite 161].

**Proposition 4.3** *Seien $E_1$ und $E_2$ elliptische Kurven über $\mathbb{C}$ und $L_1$ bzw. $L_2$ Gitter, so daß $E_i(\mathbb{C}) \cong \mathbb{C}/L_i$ $(i = 1, 2)$. Genau dann ist $E_1$ isomorph zu $E_2$, wenn es eine komplexe Zahl $\alpha \in \mathbb{C}^*$ mit $L_1 = \alpha \cdot L_2$ gibt. Solche Gitter heißen* **äquivalent**.

Aufgrund dieser Proposition können wir uns im folgenden auf Gitter der Gestalt

$$L = \mathbb{Z} + \mathbb{Z}\tau$$

mit $\Im(\tau) > 0$ beschränken. Zu jedem Gitter können wir eine komplexe Zahl $j(L)$ definieren, die sogenannte $j$-**Invariante** des Gitters $L$ (vgl. [La87, Seite 39ff]). Ähnlich zu elliptischen Kurven über endlichen Körpern ist die $j$-Invariante eine Invariante der Isomorphieklassen von elliptischen Kurven über $\mathbb{C}$:

**Satz 4.4** *Zwei Gitter $L_1$ und $L_2$ sind genau dann äquivalent und damit die zugehörigen elliptischen Kurven isomorph, wenn $j(L_1) = j(L_2)$ gilt.*

Da zu jedem Gitter ein äquivalentes Gitter der Gestalt $\mathbb{Z} + \mathbb{Z}\tau$ existiert, können wir diese $j$-Invariante auch als Funktion $j(\tau)$ für komplexe Zahlen $\tau$ mit positivem Imaginärteil auffassen. Bevor wir für elliptische Kurven über den komplexen Zahlen ein modulares Polynom herleiten, benötigen wir einige spezielle Eigenschaften dieser Funktion $j(\tau)$, die wir im folgenden Abschnitt angeben.

## 4.2 Modulfunktionen

Wir haben im vorherigen Abschnitt zu einem Gitter $L = \mathbb{Z} + \mathbb{Z}\tau$ die zugehörige $j$-Invariante $j(\tau)$ eingeführt. In diesem Abschnitt wollen wir Eigenschaften dieser Funktion untersuchen. Dazu definieren wir zuerst einige notwendige Begriffe:

**Definition 4.5** *Die (homogene)* **Modulgruppe** *wird gegeben als die Menge*

$$\Gamma \quad = \quad \left\{ M \in \mathbb{Z}^{2\times 2}\,;\ \det(M) = 1 \right\}.$$

*Eine Matrix* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *induziert eine* **gebrochen rationale Transformation***:*

$$\begin{array}{rcl} \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} \\ \tau & \longmapsto & M(\tau) \quad := \quad \dfrac{a\tau + b}{c\tau + d}. \end{array}$$

*Wir schreiben die Matrix* $M$ *auch kürzer als* $M = (a, b; c, d)$.

**Bemerkung 4.6** Dabei sollen die „üblichen“ Rechenregeln für das Rechnen mit $\infty$ gelten, d.h. $\tau = \infty$ wird abgebildet auf $\lim_{\tau\to\infty} \frac{a\tau+b}{c\tau+d}$.

Die in Definition 4.5 angegebene Abbildung $\tau \mapsto M(\tau)$ läßt sich auch auf beliebige Matrizen $M' \in \mathbb{Z}^{2\times 2}$ mit Determinante ungleich Null verallgemeinern. Wir sagen dann, daß wir auf $\tau$ die **Transformation** $M'$ anwenden. Ist $M \in \Gamma$, so sprechen wir auch von **unimodularen Transformationen**.

Weiterhin beachten wir, daß für zwei Transformationen $M_1$, $M_2$ die folgende Rechenregel gilt: es ist $M_1(M_2(\tau)) = (M_1 \cdot M_2)(\tau)$. Diese Regel beweist man durch einfaches Nachrechnen.

Sei im folgenden $\mathcal{H}$ die obere Halbebene von $\mathbb{C}$, d.h. die Menge aller komplexen Zahlen mit positivem Imaginärteil und $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Wir untersuchen nun das Verhalten komplex-wertiger Funktionen bei Anwendung unimodularer Transformationen.

**Definition 4.7** *Eine Funktion* $f : \mathcal{H}^* \longrightarrow \mathbb{C} \cup \{\infty\}$ *heißt* **Modulfunktion***, wenn sie die folgenden Bedingungen erfüllt:*

1. *$f$ ist meromorph auf $\mathcal{H}$.*
2. *Für alle $M \in \Gamma$ und für alle $\tau \in \mathcal{H}^*$ gilt $f(M(\tau)) = f(\tau)$.*
3. *Es existieren Zahlen $a > 0$, $k_0 \in \mathbb{Z}$ und eine Folge $(b_k)_{k=k_0}^{\infty}$ komplexer Zahlen, so daß für alle $\tau$ mit $\Im(\tau) > a$ gilt*

$$f(\tau) \quad = \quad \sum_{k=k_0}^{\infty} b_k \cdot \exp(2\pi i \tau)^k.$$

Für die $j$-Invariante $j(\tau)$ gilt dann der folgende wichtige Satz [Sc74, Th. 8, Seite 36]:

**Satz 4.8** *Die Menge aller Modulfunktionen bildet einen Körper* $K_\Gamma$ *und es gilt*

$$K_\Gamma \quad = \quad \mathbb{C}\Big(j(\tau)\Big).$$

Diese Bedeutung der $j$-Invariante $j(\tau)$ wird in den folgenden Abschnitten eine wichtige Rolle spielen, wenn wir Eigenschaften der sogenannten modularen Polynome untersuchen. Diese Polynome werden im folgenden Abschnitt eingeführt.

## 4.3 Modulare Polynome

Wir werden in diesem Abschnitt Polynome für den Körper der komplexen Zahlen und für endliche Körper vorstellen, mit deren Hilfe wir die in der Einleitung dieses Kapitels gestellte Aufgabe lösen können. Wir beginnen dabei mit dem Körper der komplexen Zahlen als Grundkörper und leiten daraus diese Polynome über endlichen Körpern ab.

Sei im folgenden $L = \mathbb{Z} + \mathbb{Z}\,\tau$ ein gegebenes Gitter, $E$ eine elliptische Kurve über den komplexen Zahlen, so daß $E(\mathbb{C}) \cong \mathbb{C}/L$ ist und $l$ eine ungerade Primzahl. Wir betrachten dann die $j$-Invariante $j(\tau) = j(E)$ als komplexwertige Funktion und wenden auf sie die folgenden Transformationen an:

$$\alpha_n = \begin{pmatrix} 1 & n \\ 0 & l \end{pmatrix} \quad \text{für} \quad 0 \leq n \leq l-1, \tag{4.1}$$

$$\alpha_l = \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}. \tag{4.2}$$

Damit können wir das folgende Polynom definieren.

**Definition 4.9** *Für eine ungerade Primzahl $l$ definieren wir mit den Transformationen $\alpha_n$, $(0 \leq n \leq l)$ aus (4.1), (4.2) das* **$l$-te modulare Polynom über $\mathbb{C}$** *als*

$$\Phi_l\Big(X\Big) = \prod_{n=0}^{l} \Big(X - j(\alpha_n(\tau))\Big).$$

Diese Polynome sind in der Literatur genau untersucht worden. Eine wichtige Eigenschaft des $l$-ten modularen Polynoms $\Phi_l(X)$ ist, daß $\Phi_l(X)$ über dem Ring $\mathbb{Z}[j(\tau)]$ definiert ist [La87, Th. 3, Seite 55]. Genauer folgt aus [Sc74, Lemma 2, Seite 143], daß es ganze Zahlen $a_{r,k} \in \mathbb{Z}$ gibt, so daß für das Polynom

$$\tilde{\Phi}_l(X, Y) = \sum_{r=0}^{l+1} \sum_{k=0}^{l+1} a_{r,k} \cdot X^r \cdot Y^k$$

die Gleichung

$$\Phi_l\Big(X\Big) = \tilde{\Phi}_l\Big(X, j(\tau)\Big)$$

gilt. Damit können wir im folgenden das $l$-te modulare Polynom als Polynom einer Variablen mit Koeffizienten aus dem Ring $\mathbb{Z}[j(\tau)]$ oder als Polynom in zwei Variablen mit Koeffizienten aus $\mathbb{Z}$ auffassen. Wir werden im weiteren die jeweils günstigste der beiden Darstellungen verwenden und mit $\Phi_l$ bezeichnen.

Das $l$-te modulare Polynom besitzt für elliptische Kurven über den komplexen Zahlen die gewünschte Beziehung zu Isogenien. Dies wird aus folgendem Satz deutlich [La87, Th. 5, Seite 59]:

**Satz 4.10** *Seien $E, E'$ zwei elliptische Kurven über $\mathbb{C}$ und $l \in \mathbb{P}_{>2}$. Genau dann existiert eine Isogenie von $E$ nach $E'$ mit zyklischem Kern der Ordnung $l$, wenn $j(E')$ eine Nullstelle von $\Phi_l\Big(X, j(E)\Big)$ ist.*

Damit ist das im vorherigen Kapitel gestellte Problem, Information über die $j$-Invarianten von zu einer gegebenen elliptischen Kurve $E$ $l$-isogenen Kurven zu finden, für den Fall des komplexen Grundkörpers gelöst. Das modulare Polynom $\Phi_l(X, j(E))$ besitzt als Nullstellen die $j$-Invarianten von Kurven $E/C$ für $l$-Gruppen $C$. Wir interessieren uns nun für ein modulares Polynom im Falle der endlichen Körper. Um die Berechnung solcher Polynome zu beschreiben, benötigen wir noch eine zweite Möglichkeit, die $j$-Invarianten der zu $E$ $l$-isogenen Kurven zu bestimmen. Diese Invarianten kann man nach [Ve71] bzw. [El] sogar explizit ausrechnen, wie wir im Anschluß an Proposition 3.7 schon beschrieben hatten. Dort erhielten wir folgendes Resultat:

Sei $E = (a, b)$ eine elliptische Kurve über einem Körper $K$ der Charakteristik ungleich 2,3, und sei $C$ eine Untergruppe von $E(K)$. Dann wird die Kurve $E/C = (a', b')$ gegeben durch die Gleichungen

$$a' = a - 5 \cdot \sum_{\substack{P \in C \\ P \neq \mathcal{O}}} \Big[3\,x^2(P) + a\Big], \tag{4.3}$$

$$b' = b - 7 \cdot \sum_{\substack{P \in C \\ P \neq \mathcal{O}}} \Big[5\,x^3(P) + 3\,a\,x(P) + 2\,b\Big]. \tag{4.4}$$

Zusätzlich zu diesen Formeln werden wir im folgenden noch sogenannte Divisionspolynome benutzen, die wir nun definieren.

**Definition 4.11** *Für eine elliptische Kurve $E = (a, b)$ über einem Körper $K$ der Charakteristik ungleich 2,3 und $n \geq -1$ definieren wir das $n$-te* **Divisionspolynom** *$\psi_n \in K[X, Y]$ zu $E$ durch folgende Formeln:*

- $\psi_{-1}(X, Y) = -1$,
- $\psi_0(X, Y) = 0$,
- $\psi_1(X, Y) = 1$,
- $\psi_2(X, Y) = 2\,Y$,
- $\psi_3(X, Y) = 3\,X^4 + 6\,a \cdot X^2 + 12\,b \cdot X - a^2$,
- $\psi_4(X, Y) = 4\,Y \cdot (X^6 + 5\,a \cdot X^4 + 20\,b \cdot X^3 - 5\,a^2 \cdot X^2 - 4\,a\,b \cdot X - 8\,b^2 - a^3)$,
- $\psi_{2n}(X, Y) = \frac{\psi_n(X,Y)}{2\,Y} \cdot \Big(\psi_{n+2}(X, Y) \cdot \psi_{n-1}^2(X, Y) - \psi_{n-2}(X, Y) \cdot \psi_{n+1}^2(X, Y)\Big)$ *für $n \geq 3$,*
- $\psi_{2n+1}(X, Y) = \psi_{n+2}(X, Y) \cdot \psi_n^3(X, Y) - \psi_{n+1}^3(X, Y) \cdot \psi_{n-1}(X, Y)$ *für $n \geq 2$.*

Die in dieser Definition angegebene Eigenschaft $\psi_n \in K[X,Y]$ läßt sich sehr leicht mit Induktion zeigen. Im folgenden werden wir diese Polynome als Polynome auf $E$ betrachten. Dann kann man ebenfalls durch Induktion zeigen, daß für ungerade Zahlen $n$ in $\psi_n(X,Y) \in K[E]$ keine $Y$-Terme auftreten. Eine andere Beschreibung dieser Polynome wird durch folgende Gleichung aus [ChRo88, Seite 42] gegeben. Es gilt

$$\psi_n^2(X,Y) \quad = \quad n^2 \prod_{P \in E[n]-\{\mathcal{O}\}} \Big(X - x(P)\Big).$$

Damit werden alle Nullstellen des $n$-ten Divisionspolynoms genau durch die verschiedenen $x$-Koordinaten von nichttrivialen $n$-Torsionspunkten gegeben. Durch Gradbetrachtungen kann man leicht zeigen, daß das $n$-te Divisionspolynom ein Polynom minimalen Grades mit dieser Eigenschaft ist (vgl. [ChRo88, Seite 42]). Zusätzlich werden wir in den folgenden Kapiteln noch häufig die im nächsten Satz beschriebene Eigenschaft solcher Polynome benötigen (vgl. [Sc85]).

**Satz 4.12** *Sei $n \in \mathbb{N}$ und $P = (x,y) \in E(K)$ ein Punkt der elliptischen Kurve $E$ über einem Körper $K$ der Charakteristik ungleich 2,3 mit $n \cdot P \neq \mathcal{O}$. Dann gilt*

$$n \cdot P = \left( x - \frac{\psi_{n-1} \cdot \psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2} \cdot \psi_{n-1}^2 - \psi_{n-2} \cdot \psi_{n+1}^2}{4\, y \cdot \psi_n^3} \right).$$

*Dabei fasse man $\psi_k$ immer als $\psi_k(x,y)$ auf.*

Somit können wir Vielfache eines Punktes mit Hilfe der Divisionspolynome berechnen. Diese Eigenschaften werden wir nun benutzen, um im folgenden Satz die Berechnung von modularen Polynomen über endlichen Körpern der Charakteristik größer drei zu beschreiben. Dabei bezeichnen wir im folgenden Satz mit $\overline{E}$ eine elliptische Kurve über einem Körper der Charakteristik $p$ und mit $E$ eine elliptische Kurve über einem beliebigen Körper (analog für alle anderen Symbole).

**Satz 4.13** *Sei $\mathbb{F}_q$ ein Körper der Charakteristik $p > 3$, $\overline{E}$ eine elliptische Kurve über $\mathbb{F}_q$ und $l \in \mathbb{P}_{>2}$ teilerfremd zu $q$. Sei $\overline{\Phi}_l(X,Y) \equiv \Phi_l(X,Y) \bmod p$, wobei $\Phi_l(X,Y)$ das $l$-te modulare Polynom über $\mathbb{C}$ ist. Sind die elliptischen Kurven $\overline{E}/C_i$ für die $l$-Gruppen $C_i$, $1 \leq i \leq l+1$, von $\overline{E}(\overline{\mathbb{F}}_q)$ nicht isomorph, so werden die Nullstellen von $\overline{\Phi}_l(X, \overline{j}(\overline{E})) \in \mathbb{F}_q[X]$ gegeben durch die $j$-Invarianten $\overline{j}/C_i$, $1 \leq i \leq l+1$.*

**Beweis:** Sei $E = (a,b)$ eine elliptische Kurve über einem beliebigen Körper $K$ der Charakteristik ungleich $2,3$. Wir werden zuerst zeigen, daß wir eine rationale Funktion $j(A,B,X) \in \mathbb{Z}(A,B,X)$ finden können, so daß wir für eine $l$-Gruppe $C$ von $E(\overline{K})$ die $j$-Invariante $j/C$ erhalten, indem wir $j(A,B,X)$ an der Stelle $(a,b,x_1)$ auswerten. Dabei sei $x_1$ die $x$-Koordinate eines beliebigen nichttrivialen Punktes in $C$.

Sicherlich können wir die $j$-Invariante einer elliptischen Kurve als rationale Funktion über $\mathbb{Z}$ in den Unbestimmten $A$ und $B$ auffassen. Mit Hilfe der Divisionspolynome (vgl. Satz 4.12) können wir die $x$-Koordinate jedes Vielfachen eines „formalen“ Punktes $(X, Y)$ als rationale Funktion über $\mathbb{Z}(A, B, X)$ bestimmen. Insbesondere können wir so $(l-1)$ viele solche rationale Funktionen aus $\mathbb{Z}(A, B, X)$ finden, die die $x$-Koordinaten der Punkte $j \cdot (X, Y)$ für $j = 1, \ldots, l-1$ „darstellen“. Damit folgt aus (4.3) und (4.4), daß auch die $j$-Invariante $j/C$ formal als rationale Funktion über $\mathbb{Z}(A, B, X)$ aufgefaßt werden kann. Werten wir diese Funktion an der Stelle $(a, b, x_1)$ aus, so erhalten wir den Wert von $j/C$. Im folgenden bezeichnen wir die rationale Funktion für $j/C$ mit $j(A, B, X)$.

Sei nun $K = \mathbb{C}$. Dann betrachten wir mit dem $l$-ten modularen Polynom über $\mathbb{C}$ die folgende rationale Funktion

$$\Phi_l\Big(j(A, B, X), j(A, B)\Big) \quad = \quad \sum_{r=0}^{l+1} \sum_{k=0}^{l+1} a_{r,k} \cdot j(A, B, X)^r \cdot j(A, B)^k$$

aus $\mathbb{Z}(A, B, X)$. Wir multiplizieren diese Funktion mit dem Hauptnenner und erhalten so ein Polynom $H(X) \in \mathbb{Z}[A, B, X]$. Werten wir dieses Polynom an den Koordinaten $(a, b)$ einer elliptischen Kurve $E$ aus, so sind die $x$-Koordinaten der nichttrivialen $l$-Torsionspunkte wegen Satz 4.10 Nullstellen des dann entstehenden Polynoms aus $\mathbb{Z}[a, b, X]$. Das $l$-te Divisionspolynom $\psi_l(X)$ ist nach Definition ein Polynom minimalen Grades in $\mathbb{Z}[a, b, X]$, das als Nullstellen alle $x$-Koordinaten von $l$-Torsionspunkten von $E(\mathbb{C})$ besitzt. Damit muß $\psi_l(X)$ ein Teiler von $H(X)$ sein, etwa

$$G(X) \quad = \quad \frac{H(X)}{\psi_l(X)}.$$

Man beachte, daß diese Gleichung für alle elliptischen Kurven über $\mathbb{C}$ und damit für alle komplexen Zahlen $a$ und $b$ mit $4a^3 + 27b^2 \neq 0$ gilt. Da der führende Koeffizient von $\psi_l(X)$ $l$ ist, können wir die Gleichung

$$G(X) \cdot \psi_l(X) \quad = \quad H(X)$$

sogar als Polynomgleichung über dem Ring $\mathbb{Z}[A, B, \frac{1}{l}]$ auffassen.

Wir betrachten nun die kanonische Reduktionsabbildung $\overline{\phantom{x}} : \mathbb{Z}[A, B, \frac{1}{l}] \to \mathbb{F}_p[A, B]$. Man beachte, daß dabei $l$ modulo $p$ invertierbar ist, da $p$ und $l$ teilerfremd sind. Sei $\overline{E} = (\overline{a}, \overline{b})$ eine elliptische Kurve über $\mathbb{F}_q$, so daß nach Voraussetzung die Kurven $\overline{E}/C$ für die $l$-Gruppen $C$ von $\overline{E}(\overline{\mathbb{F}}_q)$ nicht isomorph sind. Dann können wir für alle $x$-Koordinaten $\overline{x}$ von echten $l$-Torsionspunkten von $\overline{E}(\overline{\mathbb{F}}_q)$ die mit obiger Abbildung reduzierten rationalen Funktionen $\overline{j}(A, B, X) \in \mathbb{F}_p(A, B, X)$ an der Stelle $(\overline{a}, \overline{b}, \overline{x})$ auswerten, denn die $j$-Invarianten $j/C$ für $l$-Gruppen $C$ von $\overline{E}(\overline{\mathbb{F}}_q)$ existieren. Insbesondere ist $(\overline{a}, \overline{b}, \overline{x})$ keine Polstelle von $\overline{j}(A, B, X)$. Wir wenden dann obige Abbildung auf $\Phi_l(j(A, B, X), j(A, B))$ an und werten $(A, B)$ an $(\overline{a}, \overline{b})$ aus. Die reduzierte rationale Funktion $\overline{\Phi}_l(\overline{j}(\overline{a}, \overline{b}, X), \overline{j}(\overline{a}, \overline{b}))$ besitzt als Nullstellen zumindest die $x$-Koordinaten von $l$-Torsionspunkten in $\overline{E}(\overline{\mathbb{F}}_q)$. Dazu beachte man, daß die reduzierte rationale Funktion $\overline{\Phi}_l$ an der Stelle $X = x_1$ keinen Pol hat, da alle $j$-Invarianten $\overline{j}/C$ nach Voraussetzung existieren. Dann können wir direkt die obige Konstruktion übernehmen, wobei wir benutzen, daß die Reduktionsabbildung das $l$-te Divisionspolynom für $E$ in das $l$-te Divisionspolynom für $\overline{E}$ abbildet. Werten wir für alle diese Nullstellen (die $x$-Koordinaten von nichttrivialen $l$-Torsionspunkten) die Funktion $\overline{j}(\overline{a}, \overline{b}, X)$ aus, so erhalten wir die $l+1$ verschiedenen $j$-Invarianten $\overline{j}/C_i$ für die $l$-Gruppen $C_i$, $1 \leq i \leq l+1$, von $\overline{E}(\overline{\mathbb{F}}_q)$. Damit besitzt das Polynom $\overline{\Phi}_l(X, \overline{j}(\overline{E}))$ zumindestens die Nullstellen $\overline{j}/C_i$ für $1 \leq i \leq l+1$. Aus Gradgründen sind dies sogar alle Nullstellen (nach Voraussetzung sind alle $j$-Invarianten $\overline{j}/C_i$ verschieden) und der Satz ist bewiesen. ■

Damit müssen wir noch zeigen, wann die Voraussetzungen dieses Satzes 4.13 erfüllt sind. Aus dem folgenden Lemma folgt, daß dies immer dann der Fall ist, wenn die Voraussetzungen aus Korollar 3.12 zutreffen. Diese Voraussetzungen werden im Algorithmus überprüft werden.

**Lemma 4.14** *Sei $E$ eine ordinäre elliptische Kurve über $\mathbb{F}_q$ mit $j$-Invariante ungleich 0 oder 1728 und $l$ teilerfremd zu $q$. Dann sind alle elliptischen Kurven $E/C_i$ für die $l$-Gruppen $C_i$, $1 \leq i \leq l+1$ von $E(\overline{\mathbb{F}}_q)$ nicht isomorph.*

**Beweis:** Nehmen wir an, die Voraussetzungen des Lemmas wären erfüllt, aber es gäbe zwei verschiedene $l$-Gruppen $C_r$ und $C_s$, so daß die elliptischen Kurven $E/C_r$ und $E/C_s$ isomorph sind. Seien $\psi_r$ und $\psi_s$ die Isogenien mit Kern $C_r, C_s$ und $\kappa$ der Isomorphismus zwischen $E/C_r$ und $E/C_s$, so daß die Situation folgendermaßen ist:

$$\begin{array}{lcl} \psi_r : E & \longrightarrow & E/C_r \\ & & \downarrow \kappa \\ \psi_s : E & \longrightarrow & E/C_s. \end{array}$$

Sei $\hat{\psi}_s$ die zu $\psi_s$ duale Isogenie. Dann sind die beiden Abbildungen $\hat{\psi}_s \circ \psi_s$ und $\hat{\psi}_s \circ (\kappa \circ \psi_r)$ Elemente des Endomorphismenrings $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ von $E$. Weiterhin ist der Grad beider Endomorphismen genau $l^2$ [Si85, Th. 6.2, Seite 86]. Damit können sich diese beiden Endomorphismen nur durch einen Endomorphismus vom Grad 1, also einen Automorphismus, unterscheiden. Weil nach Voraussetzung die $j$-Invariante von $E$ ungleich 0 oder 1728 ist und die Automorphismengruppe von $E$ daher trivial ist [Si85, Th. 10.1, Seite 103], kann dieser Automorphismus nur $\pm$id sein. Also gilt

$$\hat{\psi}_s \circ \kappa \circ \psi_r \quad = \quad \pm\hat{\psi}_s \circ \psi_s \quad = \quad \pm l.$$

Wenden wir auf beiden Seiten $\psi_s$ an, so erhalten wir folgende Gleichheit von Isogenien von $E$ nach $E/C_s$

$$\psi_s \circ \hat{\psi}_s \circ \kappa \circ \psi_r \quad = \quad l \circ \kappa \circ \psi_r \quad = \quad \kappa \circ \psi_r \circ l \quad = \quad \psi_s \circ \pm l.$$

Sei nun $P \in E(\overline{\mathbb{F}}_q)$ ein Punkt, für den $l \cdot P \in C_r - \{\mathcal{O}\}$ gilt (beachte, daß so ein Punkt existiert). Dann gilt wegen $C_r \neq C_s$

$$\kappa \circ \psi_r\,(l \cdot P) \quad = \quad \mathcal{O} \qquad \text{und} \qquad \psi_s\,(\pm l \cdot P) \quad \neq \quad \mathcal{O}.$$

Dies ist ein Widerspruch, so daß die Annahme falsch und damit das Lemma bewiesen ist. ■

In den folgenden Abschnitten werden wir uns genauer mit Eigenschaften modularer Polynome beschäftigen. Dazu betrachten wir zuerst wieder den komplexen Grundkörper und transformieren diese Ergebnisse dann für den Fall eines endlichen Körpers.

## 4.4 Die Galoisgruppe modularer Polynome über den komplexen Zahlen

In diesem Abschnitt wollen wir für eine ungerade Primzahl $l$ die Galoisgruppe des $l$-ten modularen Polynoms für die komplexen Zahlen über bestimmten transzendenten Erweiterungen der rationalen Zahlen untersuchen. Daraus werden wir im folgenden Abschnitt Eigenschaften des $l$-ten modularen Polynoms über einem endlichen Körper bestimmen. Um die Galoisgruppe von $\Phi_l(X)$ zu bestimmen, beachten wir, daß das modulare Polynom ein Spezialfall einer viel allgemeineren Gleichung ist.

**Definition 4.15** *Sei $f(\tau)$ eine nichtkonstante Modulfunktion und sei $M_l$ die Menge aller Matrizen aus $\mathbb{Z}^{2\times 2}$ mit Determinante $l$. Dann heißt*

$$Q_{l,f(\tau)}\Big(X\Big) \quad = \quad \prod_{\alpha_i} \Big(X - f(\alpha_i(\tau))\Big) \in K_\Gamma[X]$$

*die* **Transformationsgleichung der Ordnung** $l$ **zu** $f(\tau)$. *Dabei sei $\{\alpha_i\}$ ein Vertretersystem der Menge $M_l \Big/ \Gamma$.*

Damit wird deutlich, daß das $l$-te modulare Polynom genau die Transformationsgleichung der Ordnung $l$ für die Modulfunktion $j(\tau)$ ist. Dazu beachte man nur, daß mit [La87, Seite 52] die Matrizen $\alpha_i$ aus (4.1),(4.2) für eine Primzahl $l$ ein Vertretersystem für $M_l \,/\, \Gamma$ bilden. Wir geben im folgenden Satz eine Eigenschaft solcher Transformationsgleichungen an, die wir im weiteren noch benötigen werden.

**Satz 4.16** *Sei $Q_{l,f(\tau)}(X)$ wie in Definition 4.15 eine Transformationsgleichung der Ordnung $l$ für eine Modulfunktion $f(\tau)$. Dann ist $Q_{l,f(\tau)}(X)$ irreduzibel in $K_\Gamma[X]$, also insbesondere besitzt $Q_{l,f(\tau)}(X)$ keine doppelte Nullstellen.*

**Beweis:** [Sc74, Th. 14, Seite 141]. ■

Bereits Weber hat sich genauer mit der Galoisgruppe solcher Gleichungen über speziellen Erweiterungen der rationalen Zahlen beschäftigt. Dabei hat er das folgende Resultat erhalten [We08, Seite 287-289]:

**Satz 4.17** *Die Galoisgruppe einer Transformationsgleichung der Ordnung $l \in \mathbb{P}_{>2}$ über dem Körper $\mathbb{Q}(j(\tau))$ ist $\mathrm{PGL}_2(\mathbb{F}_l)$. Ist der Grundkörper jedoch*

$$\mathbb{Q}\left(j(\tau), \sqrt{(-1)^{(l-1)/2}\cdot l}\right),$$

*so ist die Galoisgruppe $\mathrm{PSL}_2(\mathbb{F}_l)$.*

In der Galoistheorie stellt man Galoisgruppen auch häufig als Untergruppen von Permutationsgruppen dar. Wir wollen im folgenden Satz die Untergruppe von $S_{l+1}$ charakterisieren, die wir in den gerade vorgestellten Fällen erhalten.

**Satz 4.18** *Sei $l \in \mathbb{P}_{>2}$. Dann gilt:*

1. $\mathrm{PSL}_2(\mathbb{F}_l)$ *ist isomorph zu einer Untergruppe von* $A_{l+1}$.
2. *In der zu* $\mathrm{PGL}_2(\mathbb{F}_l)$ *isomorphen Untergruppe von* $S_{l+1}$ *gibt es ungerade Permutationen.*

**Beweis:** Um den ersten Teil des Satzes zu beweisen, benutzen wir folgende spezielle Eigenschaften der alternierenden Gruppe und der Gruppe $\mathrm{PSL}_2(\mathbb{F}_l)$:

1. Es gilt nach [Hu67, Satz 6.14, Seite183] $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.
2. Für $l > 3$ ist $\mathrm{PSL}_2(\mathbb{F}_l)$ einfach, d.h. sie besitzt nur triviale Normalteiler [Hu67, Satz 6.13, Seite 182].
3. Für $l > 1$ ist $A_l$ ein Normalteiler von $S_l$.
4. Sei $G$ eine Gruppe und $N$, $U$ Untergruppen von $G$. Zusätzlich sei $N$ Normalteiler von $G$. Dann ist $N \cap U$ Normalteiler von $U$ (2. Isomorphiesatz, vgl. [Hu67, Satz 3.12, Seite 17]).

Sei $\mathrm{PSL}_2(\mathbb{F}_l)$ isomorph zu der Untergruppe $H$ von $S_{l+1}$. Wir wenden nun den zweiten Isomorphiesatz an mit $U = H, N = A_{l+1}$ und $G = S_{l+1}$. Dann liefert der Satz, daß $H \cap A_{l+1}$ ein Normalteiler von $H$ ist. Nach der zweiten Bemerkung und wegen o.E. $l > 3$ ist $H \cong \mathrm{PSL}_2(\mathbb{F}_l)$ einfach und daher gibt es nur zwei Möglichkeiten:

(a) $A_{l+1} \cap H = H$, d.h. $H$ ist schon Untergruppe von $A_{l+1}$,

(b) $A_{l+1} \cap H = \{id_{l+1}\}$, wobei $id_{l+1}$ die identische Permutation ist.

Können wir den Fall (b) ausschließen, so ist der erste Teil des Satzes bewiesen. Nehmen wir an, Fall (b) liege vor, d.h. in $H$ gibt es keine gerade Transformation außer der Identität. Dann beachte man

- Angenommen, $H$ enthält eine ungerade Permutation $\pi$, die nicht zu sich selbst invers ist. Damit ist sicherlich auch die gerade, nicht identische Permutation $\pi \circ \pi \in H$, ein Widerspruch zu (b).
- Angenommen, $H$ enthält eine ungerade Permutation, die zu sich selbst invers ist. Enthält $H$ eine andere solche Permutation, so muß es eine ungerade Permutation geben, die nicht zu sich selbst invers ist (nimmt man an, dies gäbe es nicht, so existiert ein nichttrivialer Normalteiler von $H$). Damit ergibt sich entweder ein Widerspruch zu (b) oder es gilt $|H| \leq 2$.

Da $H$ isomorph ist zu $\mathrm{PSL}_2(\mathbb{F}_l)$, besitzen beide Gruppen dieselbe Ordnung. Nun gilt aber mit [Hu67, Hilfssatz 6.2, Seite 178]

$$|\,\mathrm{PSL}_2(\mathbb{F}_l)\,| \quad = \quad \frac{l\cdot(l^2-1)}{2} \quad > \quad 2.$$

Damit kann (b) nicht zutreffen und $H$ muß eine Untergruppe von $A_{l+1}$ sein, d.h. die erste Behauptung ist bewiesen.

Zum Beweis der zweiten Behauptung wenden wir ein vollkommen anderes Vorgehen an. Diesmal untersuchen wir das Verhalten der Nullstellen bei einer speziellen Transformation der Galoisgruppe. Sei $Q_{l,f(\tau)}(X)$ die Transformationsgleichung für eine Modulfunktion $f(\tau)$ und sei die Galoisgruppe von $Q_{l,f(\tau)}(X)$ $\mathrm{PGL}_2(\mathbb{F}_l)$. Betrachten wir nun die spezielle Transformation

$$M \quad = \quad \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$$

aus $\mathrm{PGL}_2(\mathbb{F}_l)$, wobei $m$ ein Erzeuger von $\mathbb{F}_l^*$ ist. Diese Transformation bildet $\tau$ ab auf $\tau' = M(\tau) = m\cdot\tau$. Damit erhalten wir die transformierten Nullstellen von $Q_{l,f(\tau)}(X)$ als (seien dabei $\alpha_i$ die Transformationen aus (4.1), (4.2))

$$\begin{aligned} f(M(\alpha_0(\tau))) &= f(\alpha_0(\tau')), \\ f(M(\alpha_l(\tau))) &= f(\alpha_l(\tau')), \\ f(M(\alpha_i(\tau))) &= f(\alpha_{i\cdot m}(\tau')) \quad \text{für } i = 1,\ldots,l-1. \end{aligned}$$

Da $f(\tau)$ eine Modulfunktion ist, gilt $f(\tau) = f(\tau+1)$. Damit können wir den Index $i$ der Transformationen $\alpha_i$ sicherlich modulo $l$ reduzieren, d.h. wir erhalten

$$f(\alpha_{i\cdot m}(\tau')) \quad = \quad f(\alpha_{i\cdot m \bmod l}(\tau')).$$

Da $m \neq 1$ ist, werden genau zwei Nullstellen der Transformationsgleichung festgehalten. Um zu zeigen, daß die Anwendung dieser Transformation einer ungeraden Permutation der Nullstellen entspricht, betrachten wir einen solchen Zyklus, wie die Nullstellen transformiert werden:

$$f(\alpha_i(\tau)) \to f(\alpha_{i\cdot m \bmod l}(\tau)) \to \ldots \to f(\alpha_{i\cdot m^k \bmod l}(\tau)) \;=\; f(\alpha_i(\tau)).$$

Damit ist die Länge dieses Zykus genau $k$, wobei $k = l-1$ die Ordnung von $m$ in $\mathbb{F}_l^*$ ist. Damit ist $k$ insbesondere gerade. Ein Zyklus der Länge $k$ kann in ein Produkt von $k-1$ Transpositionen zerlegt werden (vgl. Lemma 4.25). Also entspricht diese Transformation einem Produkt von $l-2$ Transpositionen und ist damit ungerade. ∎

Mit Hilfe dieser Resultate werden wir in den folgenden beiden Abschnitten die Galoisgruppe von modularen Polynomen über endlichen Körpern untersuchen.

## 4.5 Die Galoisgruppe modularer Polynome über endlichen Körpern

Wir wollen in diesem Abschnitt die Beziehung zwischen der Galoisgruppe modularer Polynome über den komplexen Zahlen und endlichen Körpern untersuchen. Da das modulare Polynom für einen Körper der Charakteristik $p$ nach Satz 4.13 aus dem modularen Polynom über den komplexen Zahlen durch Reduktion der Koeffizienten modulo $p$ berechnet werden kann, betrachten wir in dem folgenden Satz dieses Problem allgemein.

**Satz 4.19** *Seien $l, p \in \mathbb{P}_{>2}$, $l \neq p$, $R$ ein Integritätsbereich, so daß $\mathbb{Z}[j(\tau)] \subseteq R$, und $\mathcal{Q}$ der Quotientenkörper von $R$. Seien weiterhin $J \in \mathbb{F}_{p^d}^*$ und ein Homomorphismus*

$$\overline{\phantom{x}} : \quad R \quad \longrightarrow \quad \mathbb{F}_{p^d}$$

*gegeben, der $x \in \mathbb{Z}$ auf $\overline{x} \equiv x \bmod p$ und $j(\tau)$ auf $J$ abbildet. Seien ein Polynom $f(X) \in R[X]$ sowie das Bild $\overline{f}(X) \in \mathbb{F}_{p^d}[X]$ unter dieser Abbildung ohne mehrfache Nullstellen.*

*Dann ist bei passender Anordnung der Nullstellen die Galoisgruppe von $\overline{f}(X)$ über $\mathbb{F}_{p^d}$ eine Untergruppe der Galoisgruppe von $f(X)$ über $\mathcal{Q}$.*

**Beweis:** Wir übertragen einen Beweis aus [Wa71, Seite 202] auf die hier speziell gegebene Situation. Seien $\beta_1, \ldots, \beta_n$ die Nullstellen des Polynoms $f(X)$ in dem Zerfällungskörper von $f(X)$. Dann bilden wir mit Hilfe der Unbekannten $u_1, \ldots, u_n$ den Ausdruck

$$\theta \quad = \quad u_1\beta_1 + \ldots + u_n\beta_n.$$

Wenden wir auf $(u_1, \ldots, u_n)$ alle Permutationen $s \in S_n$ an, so können wir das Polynom

$$F(z,u) \quad = \quad \prod_{s \in S_n} \Big(z - s(\theta)\Big)$$

bestimmen. Dieses Polynom ist eine symmetrische Funktion der Nullstellen $\beta_1, \ldots, \beta_n$ und damit über $R[z,u]$ definiert. Wir zerlegen dieses Polynom nun über $\mathcal{Q}[z,u]$ in irreduzible Faktoren:

$$F(z,u) \quad = \quad F_1(z,u) \cdot \ldots \cdot F_r(z,u).$$

Die Permutationen aus $S_n$, die einen Faktor (z.B. $F_1(z,u)$) in sich selbst überführen, bilden gerade die Galoisgruppe des Polynoms $f(X)$ über $\mathcal{Q}$ (vgl. [Wa71, Seite 202]). Die Zerlegung von $F(z,u)$ in irreduzible Faktoren über $\mathcal{Q}$ kann ganzrational in $R[z,u]$ geschehen, wenn wir $F(z,u)$ mit einer Einheit aus $\mathcal{Q}[z,u]$ multiplizieren. Diese Einheit können wir gerade als Produkt aller auftretenden Nenner in der Zerlegung wählen. Dabei ändert sich die Galoisgruppe nicht. Nun können wir den angegebenen Homomorphismus auf diese Faktorisierung von $F(z,u)$ anwenden. Damit wird $F_1(z,u)$ auf ein Polynom $\overline{F_1}(z,u) \in \mathbb{F}_{p^d}[z,u]$ abgebildet. Die Galoisgruppe von $\overline{f}(X)$ über $\mathbb{F}_{p^d}$ entspricht dann genau der Menge aller Permutationen, die die über

$\mathbb{F}_{p^d}[z,u]$ irreduziblen Faktoren von $\overline{F_1}(z,u)$ wieder in sich selbst abbilden, d.h. insbesondere wird auch $F_1(z,u)$ durch eine solche Permutation wieder in sich selbst abgebildet. Damit aber ist eine solche Permutation auch ein Element der Galoisgruppe von $f(X)$ über $\mathcal{Q}$. ∎

Wir werden bei der Beschreibung des Algorithmus Polynome verwenden, die denselben Zerfällungskörper wie das $l$-te modulare Polynom über den komplexen Zahlen besitzen, die aber „einfacher" zu berechnen sind als dieses Polynom. Wir formulieren daher zuerst ein Lemma, das wir später bei der Begründung der Korrektheit dieser Vorgehensweise benutzen müssen.

**Lemma 4.20** *Seien die Bezeichnungen und Voraussetzungen wie in Satz 4.19. Weiterhin besitze ein Polynom $g(X) \in R[X]$ denselben Zerfällungskörper wie $f(X)$. Dann sind die Galoisgruppen von $\overline{f}(X)$ und $\overline{g}(X)$ über $\mathbb{F}_{p^d}$ gleich und $\overline{g}(X)$ besitzt ebenfalls keine doppelte Nullstellen.*

**Beweis:** Seien $\{\beta_1,\ldots,\beta_n\}$, $\{\beta'_1,\ldots,\beta'_n\}$ die Nullstellen von $f(X)$ bzw. $g(X)$. Da $g(X)$ und $f(X)$ denselben Zerfällungskörper besitzen, gibt es insbesondere einen Isomorphismus zwischen $\mathcal{Q}(\beta_1,\ldots,\beta_n)$ und $\mathcal{Q}(\beta'_1,\ldots,\beta'_n)$, der $\mathcal{Q}$ festläßt. Dann können wir die komplette Konstruktion aus dem Beweis zu Satz 4.19 mit Hilfe dieses Isomorphismus übertragen. ∎

In dem folgenden Lemma werden wir eine Beziehung zwischen der Faktorisierung eines Polynoms über einem endlichen Körper und der Galoisgruppe dieses Polynoms herstellen.

**Lemma 4.21** *Angenommen, das Polynom $\overline{f}(X) \in \mathbb{F}_{p^d}[X]$ zerfällt über $\mathbb{F}_{p^d}$ als*

$$\overline{f}(X) \quad = \quad \overline{f_1}(X)\cdot\ldots\cdot\overline{f_k}(X)$$

*und sei dabei $d_i = \deg(\overline{f_i}(X))$ für $1 \le i \le k$. Dann wird nach passender Anordnung der Nullstellen von $\overline{f}(X)$ die Galoisgruppe von $\overline{f}(X)$ über $\mathbb{F}_{p^d}$ erzeugt von der Permutation*

$$(1\ldots d_1)\circ((d_1+1)\ldots(d_1+d_2))\circ\ldots\circ((d_1+\ldots+d_{k-1}+1)\ldots(d_1+\ldots+d_k)).$$

**Beweis:** Die Galoisgruppe von $\overline{f}(X)$ über $\mathbb{F}_{p^d}$ ist zyklisch, da $\mathbb{F}_{p^d}$ endlich ist (vgl. [Wa71, Seite 203ff]). Sei

$$s \quad = \quad (1\ldots j_1)\circ((j_1+1)\ldots j_2)\circ\ldots$$

die die Galoisgruppe von $\overline{f}(X)$ über $\mathbb{F}_{p^d}$ erzeugende Permutation. Die Transitivitätsgebiete der Galoisgruppe (d.h. die Teilmengen der Nullstellen, die durch die Galoisgruppe in sich abgebildet werden) entsprechen genau den über $\mathbb{F}_{p^d}$ irreduziblen Faktoren $\overline{f_i}(X)$ von $\overline{f}(X)$. Damit besitzt $\overline{f}(X)$ einen irreduziblen Faktor vom Grad $j_1$, einen weiteren vom Grad $j_2 - j_1$ und so weiter. Nach entsprechender Anordnung der Nullstellen von $\overline{f}(X)$ folgt die Behauptung des Lemmas. ∎

Wir sprechen im folgenden auch von dem **Zerfällungstyp** des Polynoms $\overline{f}(X)$ über $\mathbb{F}_{p^d}$. Darunter verstehen wir die „Länge“ der einzelnen Zyklen in einer die Galoisgruppe erzeugenden Permutation (nach Größe geordnet). Zerfällt $\overline{f}(X)$ also wie in Lemma 4.21, so besitzt dieses Polynom den Zerfällungstyp $(d_1\, d_2\, \ldots\, d_{k-1}\, d_k)$, d.h. wir erhalten den Zerfällungstyp als die Grade der über $\mathbb{F}_{p^d}$ irreduziblen Faktoren von $\overline{f}(X)$. Beachte, daß wir aus der Kenntnis des Zerfällungstyps eines Polynoms $\overline{f}(X)$ Information über eine die Galoisgruppe erzeugende Permutation erhalten.

**Korollar 4.22** *Seien die Voraussetzungen wie in Lemma 4.20. Dann besitzen $\overline{f}(X)$ und $\overline{g}(X)$ über $\mathbb{F}_{p^d}$ denselben Zerfällungstyp.*

Wir beachten, daß die Bestimmung des Zerfällungstyps von $\overline{\Phi}_l(X, j(E))$ ausreicht, um die in Kapitel 3 gestellte Aufgabe, Information über die $j$-Invarianten $j/C$ für $l$-Gruppen $C$ zu bestimmen, zu lösen. Dazu bemerke man, daß $j/C \in \mathbb{F}_{q^d}$ genau dann gilt, wenn $j/C$ Nullstelle eines irreduziblen Polynoms vom Grad $d$ ist. Wie wir in Kapitel 3 gezeigt haben, muß der Zerfällungstyps von $\overline{\Phi}_l(X, j(E))$ damit eine der folgenden Formen besitzen:

- $(1 \ldots 1)$,
- $(1\, l)$,
- $(1\, 1\, d \ldots d)$, $d > 1$,
- $(d \ldots d)$, $d > 1$.

Somit bildet das gerade formulierte Korollar 4.22 die Grundlage dafür, daß wir an Stelle des reduzierten $l$-ten modularen Polynoms auch sogenannte „äquivalente“ Polynome verwenden können, wenn diese denselben Zerfällungstyp wie $\overline{\Phi}_l(X, j(E))$ besitzen. Bevor wir die theoretischen Grundlagen für solche Polynome angeben, beschäftigen wir uns im folgenden Abschnitt mit möglichen Werten für $d$ in den beiden letzten erwähnten Möglichkeiten für Zerfällungstypen.

## 4.6 Einschränkung möglicher Zerfällungstypen

Wir haben in den bisherigen Abschnitten keine Aussage über die Gestalt der Galoisgruppe des $l$-ten modularen Polynoms über den komplexen Zahlen benutzt. Diese Galoisgruppe ist aber mit Hilfe von Satz 4.17 bekannt. Wir werden in diesem Abschnitt beschreiben, welche zusätzlichen Informationen über mögliche Zerfällungstypen des reduzierten $l$-ten modularen Polynoms wir durch die Kenntnis dieser Galoisgruppe erhalten und wie wir dies im Algorithmus benutzen können.

Bevor wir den wichtigen Satz dieses Abschnitts beweisen, der im Algorithmus später eine Rolle spielen wird, benötigen wir noch ein Lemma.

**Lemma 4.23** *Seien $l, p \in \mathbb{P}_{>2}$ teilerfremd. Genau dann ist $(-1)^{(l-1)/2} \cdot l$ ein Quadrat modulo $p$, wenn $p$ ein Quadrat modulo $l$ ist.*

**Beweis:** Der Beweis folgt direkt aus dem quadratischen Reziprozitätsgesetz für das Legendre-Symbol. ■

Schließlich können wir den Hauptsatz dieses Abschnitts formulieren und beweisen. Anschließend werden wir die praktischen Auswirkungen dieses Satzes für einen Algorithmus angeben.

**Satz 4.24** *Sei $E$ eine ordinäre elliptische Kurve mit $j$-Invariante ungleich 0 und 1728 und $p$ ungleich $l$. Genau dann ist eine die Galoisgruppe von $\overline{\Phi}_l(X, j(E))$ über $\mathbb{F}_{p^d}$ erzeugende Permutation gerade, wenn $p$ ein Quadrat modulo $l$ ist.*

**Beweis:** Wir definieren zu dem $l$-ten modularen Polynom $\Phi_l(X, j(\tau))$ wie in [Hu74, Def. 4.4, Seite 270] den Wert

$$\Delta \quad = \quad \prod_{1 \le i < j \le n} \Big(\beta_i - \beta_j\Big),$$

wobei $\beta_1, \ldots, \beta_n$ die Nullstellen von $\Phi_l(X, j(\tau))$ in dem Zerfällungskörper sind. Beachte, daß die Diskriminante von $\Phi_l(X, j(\tau))$ durch $\Delta^2$ gegeben wird. Nach [Hu74, Prop. 4.5, Seite 271] entspricht für ein Polynom $f(X) \in K[X]$ ein Element $\sigma$ der Galoisgruppe von $f(X)$ über $K$ genau dann einer geraden Permutation, wenn $\sigma(\Delta) = \Delta$ gilt. Aus Satz 4.18 und der Definition der Galoisgruppe eines Polynoms folgt dann

$$\Delta \in \mathbb{Q}\left(j(\tau), \sqrt{(-1)^{(l-1)/2} \cdot l}\right) \qquad \text{und} \qquad \Delta \notin \mathbb{Q}\Big(j(\tau)\Big).$$

Da das modulare Polynom $\Phi_l(X, j(\tau))$ über dem Ring $\mathbb{Z}[j(\tau), \sqrt{(-1)^{(l-1)/2} \cdot l}]$ definiert ist, folgt aus [Co93, Lemma 3.3.4, Seite 118] sogar

$$\Delta \in \mathbb{Z}\left[j(\tau), \sqrt{(-1)^{(l-1)/2} \cdot l}\right] \qquad \text{und} \qquad \Delta^2 \in \mathbb{Z}\Big[j(\tau)\Big].$$

Sei nun $\zeta \in \overline{\mathbb{F}}_p$ gegeben, so daß $\zeta^2 \equiv (-1)^{(l-1)/2} \cdot l \bmod p$ ist. Analog zu Satz 4.19 können wir eine Reduktionsabbildung von $\mathbb{Z}[j(\tau), \sqrt{(-1)^{(l-1)/2} \cdot l}]$ nach $\mathbb{F}_{p^d}(\zeta)$ konstruieren, die $\Delta$ in $\overline{\Delta} \in \mathbb{F}_{p^d}(\zeta)$ abbildet (beachte, daß alle Voraussetzungen dieses Satzes erfüllt sind). Dann gilt nach Konstruktion

$$\overline{\Delta} \quad = \quad \prod_{1 \le i < j \le n} \Big(\overline{\beta}_i - \overline{\beta}_j\Big)$$

mit den Nullstellen $\overline{\beta}_1, \ldots, \overline{\beta}_n$ von $\overline{\Phi}_l(X, j(E))$ (im zugehörigen Zerfällungskörper). Mit [Hu74, Cor. 4.6, Seite 271] erhalten wir nun das folgende Kriterium, daß die Galoisgruppe von $\overline{\Phi}_l(X, j(E))$ über $\mathbb{F}_{p^d}$ genau dann eine Untergruppe der alternierenden Gruppe ist, wenn $\overline{\Delta} \in \mathbb{F}_{p^d}$ gilt.

Falls $p$ ein Quadrat modulo $l$ ist, so folgt mit Lemma 4.23 $\mathbb{F}_{p^d}(\zeta) = \mathbb{F}_{p^d}$ und damit ist die Galoisgruppe von $\overline{\Phi}_l(X, j(E))$ über $\mathbb{F}_{p^d}$ eine Untergruppe der alternierenden Gruppe.

Sei nun $p$ kein Quadrat modulo $l$ und damit $\mathbb{F}_{p^d}(\zeta)$ eine quadratische Erweiterung von $\mathbb{F}_{p^d}$. Da das reduzierte $l$-te modulare Polynom $\overline{\Phi}_l(X, j(E))$ keine doppelten Nullstellen besitzt (vgl. Lemma 4.14), gilt offensichtlich $\overline{\Delta} \neq 0$. Damit folgt aus $\Delta^2 \in \mathbb{Z}[j(\tau)]$, daß

$$\overline{\Delta} \in \mathbb{F}_{p^d}(\zeta) \qquad \text{und} \qquad \overline{\Delta} \notin \mathbb{F}_{p^d}.$$

Damit enthält die Galoisgruppe von $\overline{\Phi}_l(X, j(E))$ eine ungerade Permutation; insbesondere ist damit eine die Galoisgruppe erzeugende Permutation ungerade. ■

Damit haben wir ein einfach zu entscheidendes Kriterium angegeben, wie wir bestimmte Zerfällungstypen des reduzierten $l$-ten modularen Polynoms $\overline{\Phi}_l(X, j(E))$ über $\mathbb{F}_{p^d}$ ausschließen können. Nach Korollar 4.22 überträgt sich dieses Kriterium natürlich auch direkt auf die sogenannten „äquivalenten“ Polynome. Bevor wir praktische Auswirkungen dieses Satzes beschreiben, benötigen wir noch folgendes Lemma.

**Lemma 4.25** *Ein Zykel der Länge $d > 1$ kann in ein Produkt von $d - 1$ Transpositionen zerlegt werden.*

**Beweis:** Sei der Zykel der Länge $d$ gegeben als $(i_1 i_2 \dots i_d)$. Dann finden wir im Beweis zu [Hu74, Cor. 6.5, Seite 48] die Formel

$$(i_1 i_2 \dots i_d) \quad = \quad (i_1 i_d)(i_1 i_{d-1}) \dots (i_1 i_2),$$

woraus durch einfaches Abzählen die Behauptung des Lemmas folgt. ■

Wir haben in Kapitel 3 gesehen, daß die $j$-Invarianten $j/C$ für alle $l$-Gruppen $C$ von $E(\overline{\mathbb{F}}_q)$ und damit die Nullstellen des Polynoms $\overline{\Phi}_l(X, j(E))$ nur in bestimmten Körpern liegen können. Damit gibt es wegen Korollar 3.12 und Tabelle 3.1 nur bestimmte mögliche Zerfällungstypen für das reduzierte $l$-te modulare Polynom, nämlich

- $(1 \dots 1)$,
- $(1\, l)$,
- $(1\, 1\, d \dots d)$ mit $d > 1$,
- $(d \dots d)$ mit $d > 1$.

Wir interessieren uns im folgenden nur für die beiden speziellen Zerfällungstypen $(1\, 1\, d \dots d)$ und $(d \dots d)$ und wollen weitere Einschränkungen für mögliche Werte von $d$ bestimmen. Dazu beachten wir, daß ein Zykel der Länge 1 sicherlich in ein Produkt zweier Transpositionen zerlegt werden kann (z.B. $(i) = (i1)(1i)$).

Nehmen wir an, das $l$-te modulare Polynom $\overline{\Phi}_l(X, j(E))$ zerfalle als $(1\, 1\, d \dots d)$. Dann muß $d$ ein Teiler von $l - 1$ sein. Weiterhin kann nach Lemma 4.25 die dem Zerfällungstyp $(11d \dots d)$ entsprechende Permutation in ein Produkt von

$$2 + 2 + (d - 1) \cdot \frac{l - 1}{d}$$

Transpositionen zerlegt werden. Damit erhalten wir aus Satz 4.24

- Falls $p$ ein Quadrat modulo $l$ ist, so ist $(d-1)\cdot\frac{l-1}{d}$ gerade.
- Falls $p$ kein Quadrat modulo $l$ ist, so ist $(d-1)\cdot\frac{l-1}{d}$ ungerade.

Ist der Zerfällungstyp des reduzierten $l$-ten modularen Polynoms $(d\ldots d)$, so ist die Anzahl der Transpositionen, in die wir die entsprechende Permutation zerlegen können, $(d-1)\cdot\frac{l+1}{d}$ und wir erhalten in diesem Fall

- Falls $p$ ein Quadrat modulo $l$ ist, so ist $(d-1)\cdot\frac{l+1}{d}$ gerade.
- Falls $p$ kein Quadrat modulo $l$ ist, so ist $(d-1)\cdot\frac{l+1}{d}$ ungerade.

Wir haben damit beschrieben, wie wir mit dem modularen Polynom die im vorherigen Kapitel gewünschte Information über spezielle $j$-Invarianten berechnen können. Die Berechnung dieser modularen Polynome stellt sich in der Praxis aber als sehr zeitaufwendig heraus. Wir verwenden in der Praxis daher andere, besser zu berechnende sogenannte „äquivalente“ Polynome. Dies sind über $\mathbb{Z}[j(\tau)]$ definierte Polynome, die den gleichen Zerfällungskörper wie das $l$-te modulare Polynom besitzen. Damit besitzt nach Korollar 4.22 die Reduktion solcher äquivalenter Polynome denselben Zerfällungstyp wie das $l$-te reduzierte modulare Polynom. Die Berechnung äquivalenter Polynome werden wir im folgenden Kapitel beschreiben; die theoretischen Grundlagen zur Bestimmung dieser Polynome geben wir im nächsten Abschnitt an.

## 4.7 Äquivalente Polynome

Untersuchen wir zuerst, warum die Berechnung der modularen Polynome in der Praxis lange dauert. Für das $l$-te modulare Polynom $\Phi_l(X,Y)$ über den komplexen Zahlen gilt mit Satz 16 aus [Sc74, Seite 144], daß es als

$$\Phi_l\Big(X,Y\Big) \quad = \quad \sum_{r=0}^{l+1}\left(\sum_{s=0}^{l+1} b_{r,s}\cdot Y^s\right)\cdot X^r$$

mit Koeffizienten $b_{r,s}\in\mathbb{Z}$ dargestellt werden kann. Damit ist der Grad der Koeffizientenpolynome (in $Y$) genau $l+1$. Dies führt dazu, daß wir bei Anwendung der im nächsten Kapitel beschriebenen Methoden zur Berechnung dieses Polynoms Fourierreihenentwicklungen mit sehr großer Genauigkeit ausrechnen müssen, was natürlich zeitaufwendig ist. Wir werden im folgenden die theoretischen Grundlagen vorstellen, wie wir ein Polynom finden können, das alle Voraussetzungen aus Lemma 4.20 und Korollar 4.22 erfüllt und das daher an Stelle des modularen Polynoms verwendet werden kann. Bei solchen sogenannten „äquivalenten“ Polynomen wird der Grad der Koeffizientenpolynome maximal $(l-1)/2$ sein.

Wir haben in Satz 4.8 schon den Körper $K_\Gamma$ aller Modulfunktionen eingeführt. Da das modulare Polynom über diesem Körper definiert ist, ist

$$K_\Gamma[X]\Big/\Phi_l(X,j(\tau)) \tag{4.5}$$

ein endlicher Erweiterungskörper von $K_\Gamma$. Wir wollen zuerst untersuchen, wie wir diesen Erweiterungskörper genauer spezifizieren können. Dazu benötigen wir folgende Definition (vgl. [Sc74, Seite 104 ff]).

**Definition 4.26** *Sei $\Gamma_1$ eine Untergruppe mit endlichem Index in $\Gamma$ und $-I \in \Gamma_1$. Eine auf $\mathcal{H}^*$ definierte Funktion $f(\tau)$ heißt* **Modulfunktion für** $\Gamma_1$*, wenn gilt*

1. *$f$ ist meromorph auf $\mathcal{H}$,*
2. *für alle $S \in \Gamma_1$ und alle $\tau \in \mathcal{H}^*$ gilt $f(S(\tau)) = f(\tau)$,*
3. *es existieren Zahlen $k_0 \in \mathbb{Z}$, $\kappa \in \mathbb{N}$, $a > 0$, eine Folge $(b_k)_{k=k_0}^{\infty}$ komplexer Zahlen und eine Matrix $A \in \Gamma$, so daß für alle $\tau$ mit $\Im(A(\tau)) > a$ gilt*

$$f(\tau) \quad = \quad \sum_{k=k_0}^{\infty} b_k \cdot \exp\left(\frac{2\pi i}{\kappa} \cdot A(\tau)\right)^k .$$

Man kann leicht zeigen, daß die Menge aller solcher Funktionen einen Körper bildet; diesen Körper bezeichnen wir mit $K_{\Gamma_1}$. Wir betrachten nun die folgende spezielle Untergruppe von $\Gamma$.

**Definition 4.27** *Wir definieren die folgende Untergruppe von $\Gamma$*

$$\Gamma_0(l) \quad = \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma;\ c \equiv 0 \bmod l \right\}.$$

Man beachte, daß die Untergruppe $\Gamma_0(l)$ alle Voraussetzungen an $\Gamma_1$ aus Definition 4.26 erfüllt (der Index von $\Gamma_0(l)$ in $\Gamma$ ist nach [Sc74, Seite 99] $l+1$).

Eine wichtige Rolle wird im folgenden die **Invarianzgruppe** von Funktionen spielen. Die Invarianzgruppe einer Funktion ist die Menge aller Transformationen aus $\Gamma$, unter denen die Funktion invariant ist. Wir untersuchen nun die Invarianzgruppe der speziellen Funktion $j(l\tau)$.

**Lemma 4.28** *Sei $f(\tau)$ eine Modulfunktion. Dann ist die Invarianzgruppe der Funktion $f(l\tau)$ genau $\Gamma_0(l)$.*

**Beweis:** Als Modulfunktion ist $f(\tau)$ invariant unter Transformationen aus $\Gamma$. Dann folgt aus Lemma 1 aus [AtLe70], daß mit

$$\alpha_l \quad = \quad \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$$

die Invarianzgruppe der Funktion $f(\alpha_l(\tau)) = f(l\tau)$ gegeben wird als $\alpha_l^{-1} \cdot \Gamma \cdot \alpha_l \cap \Gamma$. Sei also eine beliebige Transformation $A \in \Gamma$ gegeben. Offensichtlich gilt dann

$$\alpha_l^{-1} \cdot A \cdot \alpha_l \quad = \quad \begin{pmatrix} 1/l & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} a & b/l \\ c\,l & d \end{pmatrix}. \tag{4.6}$$

Ist also $\alpha_l^{-1} \cdot A \cdot \alpha_l \in \Gamma$, so ist ist diese Matrix insbesondere sogar in $\Gamma_0(l)$. Damit ist die Invarianzgruppe der Funktion $f(l\tau)$ eine Untergruppe von $\Gamma_0(l)$. Weiterhin können wir zu einer gegebenen Matrix $A' \in \Gamma_0(l)$ leicht eine Matrix $A \in \Gamma$ ausrechnen, so daß $\alpha_l^{-1} \cdot A \cdot \alpha_l = A'$ ist (vgl. (4.6)). Damit gilt $\alpha_l^{-1} \cdot \Gamma \cdot \alpha_l \cap \Gamma = \Gamma_0(l)$ und das Lemma ist bewiesen. ■

Dann können wir den Erweiterungskörper aus (4.5) mit Hilfe des folgenden Satzes genauer spezifizieren (siehe [Sc74, Th. 5, Seite 129]).

**Satz 4.29** *Ist $f(\tau)$ eine Funktion mit Invarianzgruppe $I_f$ und besitzt $I_f$ endlichen Index in $\Gamma$, so gilt*

$$K_{I_f} \quad = \quad K_\Gamma(f(\tau)).$$

Mit Hilfe dieses Satzes erhalten wir folgendes Korollar.

**Korollar 4.30** *Es ist*

$$K_\Gamma[X]\Big/\Phi_l(X, j(\tau)) \quad \cong \quad K_{\Gamma_0(l)} \quad = \quad K_\Gamma(j(l\tau)).$$

**Beweis:** Wir benutzen, daß $j(l\tau)$ eine Nullstelle des $l$-ten modularen Polynoms ist und daß die Invarianzgruppe von $j(l\tau)$ nach Lemma 4.28 genau $\Gamma_0(l)$ ist. Da der Index von $\Gamma_0(l)$ in $\Gamma$ endlich ist, können wir dann Satz 4.29 anwenden. ■

Die Idee zur Bestimmung eines zum $l$-ten modularen Polynoms äquivalenten Polynoms ist nun, daß wir eine andere geeignete Funktion mit Invarianzgruppe $\Gamma_0(l)$ verwenden und das Minimalpolynom dieser Funktion berechnen. Dieses Minimalpolynom erzeugt dann ebenfalls den Körper $K_{\Gamma_0(l)}$ und ist ein Kandidat für ein äquivalentes Polynom. Wir werden im folgenden zeigen, daß diese Vorgehensweise wirklich erfolgreich ist. Dazu formulieren wir die folgenden Sätze.

**Satz 4.31** *Sei $f(\tau)$ eine Funktion mit Invarianzgruppe $\Gamma_0(l)$ und seien die folgenden Transformationen gegeben:*

$$S_n \quad = \quad \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix} \quad \textit{für} \quad 0 \le n < l \qquad \textit{und} \qquad S_l \quad = \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

*Dann ist das Polynom*

$$G_l(X) \quad = \quad \prod_{n=0}^{l} \Big(X - f(S_n(\tau))\Big) \quad \in K_\Gamma[X]$$

*irreduzibel.*

**Beweis:** Zuerst beachten wir, daß der Index von $\Gamma_0(l)$ in $\Gamma$ endlich ist und daß damit aus Satz 4.29

$$K_{\Gamma_0(l)} = K_\Gamma(f(\tau))$$

folgt. Wenn wir zeigen können, daß für die angegebenen Matrizen $S_n$ gilt

$$\Gamma = \bigcup_{n=0}^{l} \Gamma_0(l) \cdot S_n,$$

so folgt die Behauptung des Satzes aus [Sc74, Satz 1, Seite 128]. Dazu müssen wir zeigen, daß jede Matrix $A \in \Gamma$ dargestellt werden kann als $B \cdot S_\nu$ für ein $0 \leq \nu \leq l$ und eine Matrix $B \in \Gamma_0(l)$. Sei dazu $A = (a', b'; c', d') \in \Gamma$. Ohne Einschränkung können wir annehmen, daß $A \notin \Gamma_0(l)$ gilt und daß damit $c' \not\equiv 0 \bmod l$ ist. Wir müssen nun eine Matrix $B \in \Gamma_0(l)$ und ein $0 \leq \nu < l$ bestimmen, so daß $A = B \cdot S_\nu$ gilt. Betrachte dazu den Ansatz

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{=:B\in\Gamma_0(l)} \cdot \begin{pmatrix} 0 & -1 \\ 1 & \nu \end{pmatrix}.$$

Durch äquivalente Umformungen erhalten wir daraus

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & \nu \end{pmatrix}^{-1} = \begin{pmatrix} a'\nu - b' & a' \\ c'\nu - d' & c' \end{pmatrix}.$$

Da $c \equiv 0 \bmod l$ sein soll ($B \in \Gamma_0(l)$), erhalten wir die folgende Gleichung zur Bestimmung von $\nu$:

$$c' \cdot \nu \equiv d' \bmod l.$$

Daraus können wir wegen $c' \not\equiv 0 \bmod l$ den Wert von $\nu$ bestimmen. Dann lassen sich die anderen Einträge der Matrix $B$ leicht aus den Gleichungen

$$c = c'\nu - d', \quad a = a'\nu - b', \quad b = a', \quad d = c'$$

bestimmen. Durch Nachrechnen erhalten wir $\det(B) = 1$ und damit $B \in \Gamma_0(l)$ und der Satz ist bewiesen. ■

Wir werden im folgenden Kapitel zeigen, daß für speziell gewählte Funktionen $f(\tau)$ dieses Polynom $G_l(X)$ über dem Ring $\mathbb{Z}[j(\tau)]$ definiert ist. Dann können wir auf dieses Polynom die Reduktionsabbildung aus Satz 4.19 anwenden. Da das $l$-te modulare Polynom über den komplexen Zahlen und über endlichen Körpern keine doppelte Nullstellen besitzt (Satz 4.16, Lemma 4.14), können wir aus Korollar 4.22 folgern, daß die Reduktion des Polynoms $G_l(X)$ denselben Zerfällungstyp besitzt wie das reduzierte $l$-te modulare Polynom, wenn wir gezeigt haben, daß $G_l(X)$ denselben Zerfällungskörper besitzt wie $\Phi_l(X)$. Dies wird im folgenden Satz untersucht.

**Satz 4.32** *Der Zerfällungskörper des Polynoms $G_l(X) \in K_\Gamma[X]$ aus Satz 4.31 ist $K_{\Gamma^*(l)}$, wobei*

$$\Gamma^*(l) = \left\{ S \in \Gamma;\ S \equiv \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \bmod l \right\}.$$

**Beweis:** Der Beweis des Satzes orientiert sich stark an der in [Sc74, Seite 148] beschriebenen Bestimmung des Zerfällungskörpers von $\Phi_l(X)$. Wir untersuchen die Invarianzgruppen der Nullstellen $f(S_n(\tau))$ des Polynoms $G_l(X)$. Dazu benutzen wir folgende Aussage aus dem Buch von Schoeneberg (siehe [Sc74, Th. 2, Seite 128]):

Falls $K_{\Gamma_0(l)} = K_\Gamma(f(\tau))$ ist, so gilt $K_{S^{-1}\cdot\Gamma_0(l)\cdot S} = K_\Gamma(f(S(\tau)))$.

Damit muß die Invarianzgruppe von $f(S_n(\tau)))$ für festes $n$ gerade $S_n^{-1}\cdot\Gamma_0(l)\cdot S_n$ sein. Nach Satz 4.29 gilt nämlich für diese Invarianzgruppe $I$ von $f(S_n(\tau))$

$$K_I \quad = \quad K_\Gamma(f(S_n(\tau))) \quad = \quad K_{S_n^{-1}\cdot\Gamma_0(l)\cdot S_n}$$

und damit folgt $I = S_n^{-1}\cdot\Gamma_0(l)\cdot S_n$ (benutze dazu, daß beide Gruppen denselben Index in $\Gamma$ besitzen [Sc74, Th. 14, Seite 123]). Diese Invarianzgruppe läßt sich auch noch auf andere Weise schreiben. Wir benutzen dazu die Notation wie in [Sc74, Seite 132 ff] und definieren für eine Matrix $\alpha$ der Determinante $l$

$$\Gamma_\alpha \quad = \quad \{A \in \Gamma;\ \alpha\cdot A\cdot\alpha^{-1} \in \Gamma\}.$$

Dann gilt mit der Matrix $\alpha_l = (l, 0;\, 0, 1)$

$$\Gamma_{\alpha_l} \quad = \quad \Gamma_0(l).$$

Nun verwenden wir die Formel $\Gamma_{S\cdot\alpha\cdot S_1} = S_1^{-1}\cdot\Gamma_\alpha\cdot S_1$ für alle $S, S_1 \in \Gamma$ [Sc74, Seite 132] und erhalten so

$$\begin{aligned} I &= S_n^{-1}\cdot\Gamma_0(l)\cdot S_n \\ &= S_n^{-1}\cdot\Gamma_{\alpha_l}\cdot S_n \\ &= \Gamma_{\alpha_l\cdot S_n} \\ &= \Gamma_{T\cdot\alpha_l\cdot S_n}, \end{aligned}$$

wobei $T = (0, 1;\, -1, 0)$ ist. Durch Ausrechnen erhalten wir $\alpha_n = T\cdot\alpha_l\cdot S_n$ mit $\alpha_n$ wie in (4.1),(4.2) (Seite 38). Damit ist die Invarianzgruppe der Funktion $f(S_n(\tau))$ genau $\Gamma_{\alpha_n}$. Nun können wir die Herleitung des Zerfällungskörpers des $l$-ten modularen Polynoms aus [Sc74, Seite 146] direkt übertragen und erhalten so den Zerfällungskörper von $G_l(X)$ als $K_{\Gamma^*(l)}$. ■

Somit läßt sich leicht das folgende Korollar formulieren:

**Korollar 4.33** *Ist das Polynom $G_l(X)$ über $\mathbb{Z}[j(\tau)]$ definiert, so besitzt das Bild unter der Reduktionsabbildung aus Satz 4.19 denselben Zerfällungstyp wie das reduzierte $l$-te modulare Polynom.*

**Beweis:** Man beachte, daß der Zerfällungskörper des $l$-ten modularen Polynoms ebenfalls $K_{\Gamma^*(l)}$ ist [Sc74, Th. 18, Seite 148] und wende dann Korollar 4.22 an. ■

Damit haben wir in der Theorie beschrieben, wie wir äquivalente Polynome erhalten, die wir an Stelle der modularen Polynome verwenden können und die uns dieselbe Information liefern. In dem folgenden Kapitel werden wir auf die praktische Berechnung solcher Polynome eingehen. Durch geeignete Wahl von Funktionen $f(\tau)$ mit Invarianzgruppe $\Gamma_0(l)$ können wir dabei sicherstellen, daß das zugehörige äquivalente Polynom Koeffizienten aus $\mathbb{Z}[j(\tau)]$ besitzt. Analog zu modularen Polynomen können diese äquivalenten Polynome aber auch als Polynome in zwei Variablen über dem Ring $\mathbb{Z}$ aufgefaßt werden. Im folgenden Kapitel werden wir geeignete Funktionen $f(\tau)$ vorstellen und verschiedene Algorithmen angeben, um daraus die Polynome $G_l(X, Y)$ als Polynom in zwei Unbestimmten zu bestimmen.

# Kapitel 5

# Berechnung äquivalenter Polynome

Wir haben im letzten Kapitel die theoretischen Grundlagen zur Berechnung sogenannter äquivalenter Polynome angegeben. Diese Polynome besitzen in unserem Fall denselben Zerfällungstyp wie das modulare Polynom und können daher anstelle der modularen Polynomen verwendet werden, um Informationen über die Gruppenordnung einer elliptischen Kurve modulo ungerader Primzahlen $l$ zu berechnen. In diesem Kapitel werden wir beschreiben, wie wir diese äquivalenten Polynome berechnen können. Dabei werden alle Berechnungen über den ganzen Zahlen durchgeführt werden. In den ersten beiden Abschnitten geben wir einen allgemein für jede ungerade Primzahl $l$ gültigen Algorithmus an. Anschließend untersuchen wir Verfahren, die nur für spezielle Werte von $l$ korrekt sind, bevor wir im letzten Abschnitt praktische Aspekte diskutieren.

## 5.1 Eine Modulfunktion für $\Gamma_0(l)$

Nach Satz 4.31 können wir ein zum modularen Polynom äquivalentes Polynom mit Hilfe einer Funktion $f(\tau)$ mit Invarianzgruppe $\Gamma_0(l)$ bestimmen. In diesem Abschnitt geben wir eine solche Funktion an, für die das zugehörige äquivalente Polynom (als Polynom in zwei Unbestimmten) über den ganzen Zahlen definiert ist und zeigen einige Eigenschaften dieser Funktion. Diese Eigenschaften werden wir im folgenden Abschnitt zur Herleitung eines Algorithmus zur Bestimmung des zugehörigen äquivalenten Polynoms verwenden. Eine Grundlage zur Bestimmung einer Funktion mit Invarianzgruppe $\Gamma_0(l)$ liefert die sogenannte Dedekindsche $\eta$-Funktion (zur Konvergenz des unendlichen Produkts vgl. [Ap90, Seite 47 ff.]).

**Definition 5.1** *Die* **Dedekindsche $\eta$-Funktion** *wird gegeben als*

$$\eta(\tau) \quad = \quad q_\tau^{1/24} \cdot \prod_{n=1}^{\infty} \left(1 - q_\tau^n\right),$$

*wobei* $q_\tau = \exp(2\pi i \tau)$ *ist.*

Bei der Berechnung eines äquivalenten Polynoms, wie wir sie im folgenden Abschnitt vorstellen, werden wir Rechnungen mit Fourierreihenentwicklung in der Variablen $q_\tau$ von geeigneten Funktionen benutzen. Die Fourierreihenentwicklung für die Dedekindsche $\eta$-Funktion läßt sich mit Hilfe einer einfachen Formel berechnen, wie schon in [We08, Seite 112] gezeigt wurde.

**Satz 5.2** *Die Dedekindsche $\eta$-Funktion besitzt die Fourierreihenentwicklung*

$$\eta(\tau) \quad = \quad q_\tau^{1/24} \cdot \left(1 + \sum_{n=1}^{\infty} (-1)^n \cdot \left(q_\tau^{n(3n-1)/2} + q_\tau^{n(3n+1)/2}\right)\right).$$

Im folgenden werden wir sehr häufig das Verhalten dieser Funktion bei Anwendung unimodularer Transformationen benötigen. Dieses Verhalten wurde wiederum von Weber genau untersucht [We08, Seite 113, 126 (15), 130]; wir geben hier das Ergebnis an.

**Satz 5.3** *Für ganze Zahlen $a, b, c, d \in \mathbb{Z}$ mit $ad - bc = 1$ gilt*

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) \quad = \quad \epsilon \cdot \sqrt{c\tau + d} \cdot \eta(\tau),$$

*wobei $\epsilon$ eine 24-te komplexe Einheitswurzel ist. Genauer ergeben sich für $\epsilon$ die Formeln (dabei sei $(-)$ das Jacobi-Symbol)*

$$d \text{ ungerade, positiv:} \quad \epsilon \quad = \quad \left(\frac{c}{d}\right) \cdot i^{(d-1)/2} \cdot \exp\left(\frac{\pi i}{12}\left[d(b-c) - (d^2-1)ac\right]\right).$$

$$c \text{ ungerade, positiv:} \quad \epsilon \quad = \quad \left(\frac{d}{c}\right) \cdot i^{(1-c)/2} \cdot \exp\left(\frac{\pi i}{12}\left[c(a+d) - (c^2-1)bd - 3\right]\right).$$

*Damit gilt insbesondere*

$$\eta\left(\frac{-1}{\tau}\right) \quad = \quad \sqrt{-i\tau} \cdot \eta(\tau).$$

Man beachte, daß die beiden Fälle zur Bestimmung der Einheitswurzel $\epsilon$ alle Möglichkeiten erfassen, denn wir können immer ohne Einschränkung annehmen, daß die Zahlen $d$ bzw. $c$ positiv sind. Mit Hilfe dieser Dedekindschen $\eta$-Funktion wollen wir nun eine Funktion mit Invarianzgruppe $\Gamma_0(l)$ bestimmen. Dazu setzen wir

$$f(\tau) \quad = \quad \left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s}, \tag{5.1}$$

wobei $s \in \mathbb{N}$ minimal gewählt ist, so daß $v = \frac{s\cdot(l-1)}{12}$ eine positive ganze Zahl ist. In den folgenden beiden Lemmata werden wir zeigen, daß diese Funktion dann die gewünschten Eigenschaften besitzt.

**Lemma 5.4** *Die in (5.1) definierte Funktion $f(\tau)$ ist eine Funktion mit Invarianzgruppe $\Gamma_0(l)$.*

**Beweis:** Im ersten Teil des Beweises zeigen wir, daß für eine beliebige unimodulare Transformation $V = (a, b; cl, d) \in \Gamma_0(l)$ die Funktion $f(\tau)$ invariant unter der Transformation $V$ ist. Durch Einsetzen und Ausrechnen mit Hilfe der Formeln aus Satz 5.3 erhalten wir

$$\begin{aligned} f(V(\tau)) &= \left(\frac{\eta(V(\tau))}{\eta(l\cdot V(\tau))}\right)^{2s} \\ &= \left(\frac{\eta\left(\frac{a\tau+b}{cl\tau+d}\right)}{\eta\left(\frac{l\cdot(a\tau+b)}{cl\tau+d}\right)}\right)^{2s} \\ &= \left(\frac{\epsilon_1\cdot\sqrt{(cl)\tau+d}\cdot\eta(\tau)}{\epsilon_2\cdot\sqrt{c(l\tau)+d}\cdot\eta(l\tau)}\right)^{2s} \\ &= f(\tau). \end{aligned}$$

Dabei haben wir die Formeln aus Satz 5.3 benutzt, um $(\epsilon_1/\epsilon_2)^{2s}$ zu berechnen. Nehmen wir etwa an, daß $d$ ungerade und positiv ist. Dann erhalten wir

$$\begin{aligned} \left(\frac{\epsilon_1}{\epsilon_2}\right)^{2s} &= \left(\frac{\left(\frac{cl}{d}\right)\cdot i^{(d-1)/2}\cdot\exp(\pi i/12\cdot[d(b-cl)-(d^2-1)acl])}{\left(\frac{c}{d}\right)\cdot i^{(d-1)/2}\cdot\exp(\pi i/12\cdot[d(bl-c)-(d^2-1)ac])}\right)^{2s} \\ &= \left(\left(\frac{l}{d}\right)\cdot\exp\left(\pi i/12\cdot(1-l)\cdot[d\,(b+c)+(d^2-1)\,ac]\right)\right)^{2s} \\ &= \exp\left(\frac{2s(1-l)}{24}\cdot 2\pi i\cdot[d\,(b+c)+(d^2-1)ac]\right) \\ &= 1. \end{aligned}$$

Dabei beachte man für die letzte Umformung, daß $s(l-1)$ ein Vielfaches von 12 ist und daß das Argument der Exponentialfunktion damit ein Vielfaches von $2\pi i$ ist. Den zweiten möglichen Fall „$c$ ungerade, positiv" kann man vollkommen analog berechnen.

Im folgenden Lemma 5.5 werden wir die Gleichung

$$f\left(-\frac{1}{l\tau}\right) = \frac{l^s}{f(\tau)}$$

zeigen. Damit besitzen die beiden Funktionen $f(\tau)$ und $f\left(\frac{-1}{l\tau}\right)$ dieselbe Invarianzgruppe. Aus dem Beweis zu Lemma 1 aus [AtLe70] folgt für die Invarianzgruppe von $f\left(\frac{-1}{l\tau}\right)$

$$I_{f\left(\frac{-1}{l\tau}\right)} = \begin{pmatrix} 0 & 1/l \\ -1 & 0 \end{pmatrix} I_{f(\tau)} \begin{pmatrix} 0 & -1 \\ l & 0 \end{pmatrix} \cap \Gamma.$$

Rechnen wir die rechte Seite dieser Gleichung aus und beachten die Gleichheit der beiden Invarianzgruppen, so folgt direkt, daß die Invarianzgruppe von $f(\tau)$ genau $\Gamma_0(l)$ ist. ∎

Damit haben wir eine Funktion mit Invarianzgruppe $\Gamma_0(l)$ gefunden. Wir werden im folgenden Lemma einige Eigenschaften der Funktion $f(\tau)$ angeben, die wir bei der Beschreibung der Ideen des Algorithmus zur Bestimmung des zugehörigen Polynoms verwenden werden.

**Lemma 5.5** *Für die in (5.1) definierte Funktion $f(\tau)$ gilt*

- *Die Fourierreihenentwicklung von $f(\tau)$ hat die Gestalt*

$$f(\tau) \quad = \quad \sum_{n=-v}^{\infty} a_n \cdot q_\tau^n,$$

*wobei $a_n \in \mathbb{Z}$ und $a_{-v} = 1$ gilt.*

- *Es gilt $f\left(-\frac{1}{l\tau}\right) = \frac{l^s}{f(\tau)}$.*

**Beweis:** Die erste Behauptung folgt offensichtlich aus der Definition der Funktion $f(\tau)$ und der Fourierentwicklung der $\eta$-Funktion (vgl. Satz 5.2). Dabei sollte man noch beachten, daß bei Division zweier Fourierreihenentwicklungen mit ganzen Koeffizienten, wobei der Divisor zusätzlich noch „niedrigsten" Koeffizienten eins besitzt, die Ergebnisreihe wiederum ganze Koeffizienten besitzt. Die zweite Behauptung des Lemmas erhalten wir durch folgende kleine Rechnung

$$\begin{aligned}
f\left(-\frac{1}{l\tau}\right) &= \left(\frac{\eta(-1/(l\tau))}{\eta(-1/\tau)}\right)^{2s} \\
&= \left(\frac{\sqrt{-i\,l\tau}\cdot\eta(l\tau)}{\sqrt{-i\,\tau}\cdot\eta(\tau)}\right)^{2s} && \text{(vgl. Satz 5.3)} \\
&= l^s\cdot\left(\frac{\eta(l\tau)}{\eta(\tau)}\right)^{2s} \\
&= \frac{l^s}{f(\tau)}.
\end{aligned}$$

■

Im folgenden Abschnitt werden wir neben der Funktion $f(\tau)$ aus (5.1) auch noch die Funktion

$$g(\tau) \quad = \quad \frac{l^s}{f(\tau)} \tag{5.2}$$

benutzen. Offensichtlich ist $g(\tau)$ ebenfalls eine Funktion mit Invarianzgruppe $\Gamma_0(l)$. Weiterhin folgt aus Lemma 5.5 direkt die Gleichung

$$g\left(\frac{-1}{l\tau}\right) \quad = \quad f(\tau).$$

Da der minimale Koeffizient der Fourierreihenentwicklung von $f(\tau)$ eins ist, sind auch alle Koeffizienten der Fourierreihenentwicklung von $g(\tau)$ ganze Zahlen.

Im folgenden wollen wir ein äquivalentes Polynom $G_l(X)$ wie in Satz 4.31 beschrieben mit Hilfe dieser Funktion $g(\tau)$ bestimmen. Die Berechnung dieses Polynoms wird durch Rechnungen mit Fourierreihenentwicklungen der beiden Funktionen $f(\tau)$ und $j(\tau)$ geschehen. Dabei können wir diese (unendlich langen) Entwicklungen natürlich nur mit endlicher Genauigkeit berechnen. Wir sagen im folgenden, daß wir die Fourierreihenentwicklung einer Funktion $f(\tau)$ **mit Genauigkeit** $m \in \mathbb{N}$ **kennen**, falls wir die „ersten“ $m$ Koeffizienten der Fourierreihenentwicklung von $f(\tau)$ kennen, d.h. wird die Fourierreihenentwicklung von $f(\tau)$ wie in Lemma 5.5 gegeben, so kennen wir die Koeffizienten $a_{-v}, \ldots, a_{-v+m-1}$.

Um im folgenden Abschnitt mit der Fourierreihenentwicklung von $j(\tau)$ rechnen zu können, müssen wir diese Entwicklung bestimmen. Wiederum kann dies mit Hilfe der Fourierreihenentwicklung der $\eta$-Funktion geschehen. Analog zu [We08, Seite 114] definieren wir dazu die 2. Webersche Funktion als

$$f_2(\tau) \quad = \quad \sqrt{2} \cdot \frac{\eta(2\tau)}{\eta(\tau)}.$$

Dann erhalten wir damit die Fourierentwicklung von $j(\tau)$ mit Hilfe des folgenden Satzes aus [We08, Seite 179].

**Satz 5.6** *Es gilt*

$$j(\tau) \quad = \quad \frac{\left(f_2^{24}(\tau) + 16\right)^3}{f_2^{24}(\tau)}.$$

Damit können wir sowohl die Fourierreihenentwicklung der Funktion $f(\tau)$ als auch $j(\tau)$ berechnen. Diese Entwicklungen werden wir im folgenden Abschnitt in einem Algorithmus verwenden, um ein zu der Funktion $g(\tau)$ aus (5.2) „gehörendes“ äquivalentes Polynom $G_l(X)$ zu berechnen.

## 5.2 Berechnung eines äquivalenten Polynoms zu $g(\tau)$

Seien im folgenden die Funktionen $f(\tau)$ aus (5.1) und $g(\tau)$ aus (5.2) mit Invarianzgruppe $\Gamma_0(l)$ gegeben. Dann können wir wie in Satz 4.31 beschrieben mit Hilfe von $g(\tau)$ ein Polynom $G_l(X) \in K_\Gamma[X]$ bestimmen, das den Körper $K_{\Gamma_0(l)}$ erzeugt. Wir werden in diesem Abschnitt ein Verfahren angeben, wie wir dieses Polynom $G_l(X)$ berechnen können. Es existieren Koeffizienten $a_{r,k}$ und eine Zahl $\kappa \in \mathbb{N}$, so daß

$$G_l(X) \quad = \quad \sum_{r=0}^{l+1} \left( \sum_{k=0}^{\kappa} a_{r,k} \cdot j(\tau)^k \right) \cdot X^r.$$

Aus der folgenden Gleichung (5.4) folgt direkt, daß alle Koeffizienten ganze Zahlen sind, denn die Fourierreihenentwicklung von $j(l\tau)^k \cdot f(\tau)^r$ beginnt für jedes Paar $(r,k)$ mit dem Koeffizienten eins und besitzt nur ganze Koeffizienten. Den Wert von $\kappa$ werden wir in dem folgenden Lemma 5.7 herleiten; er hängt nur von der verwendeten Funktion $g(\tau)$ ab. Da $g(\tau)$ eine Nullstelle von $G_l(X)$ ist, gilt folgende Gleichung

$$\sum_{r=0}^{l+1} \sum_{k=0}^{\kappa} a_{r,k} \cdot j(\tau)^k \cdot g(\tau)^r \quad = \quad 0. \tag{5.3}$$

Auf diese Gleichung wenden wir die Transformation $(0,-1;\, l,0)$ an. Wegen den Gleichungen $g(-1/l\tau) = f(\tau)$ und $j(-1/l\tau) = j(l\tau)$ ($j(\tau)$ ist eine Modulfunktion) erhalten wir mit denselben Koeffizienten $a_{r,k}$ wie in (5.3) die folgende neue Beziehung

$$\sum_{r=0}^{l+1}\sum_{k=0}^{\kappa} a_{r,k}\cdot j(l\tau)^k\cdot f(\tau)^r \quad = \quad 0. \tag{5.4}$$

Wir betrachten die Wirkung der folgenden Transformationen auf Gleichung (5.4):

$$V_n \quad = \quad \begin{pmatrix} l & n \\ 0 & l \end{pmatrix} \quad \text{für } 0 \le n \le l-1 \qquad \text{und} \qquad V_l \quad = \quad \begin{pmatrix} 0 & -1 \\ l^2 & 0 \end{pmatrix}. \tag{5.5}$$

Wenn wir das Verhalten der Funktionen $f(\tau)$ und $j(l\tau)$ unter diesen Transformationen bestimmen, so erhalten wir für $0 \le n \le l-1$

$$\begin{aligned} j\Big(l\cdot V_n(\tau)\Big) \quad &= \quad j\left(l\cdot\frac{l\tau+n}{l}\right) \quad = \quad j\Big(l\tau+n\Big) \quad = \quad j\Big(l\tau\Big), \\ f\Big(V_n(\tau)\Big) \quad &= \quad f\left(\frac{l\tau+n}{l}\right) \quad = \quad f\left(\tau+\frac{n}{l}\right) \end{aligned}$$

und

$$\begin{aligned} j\Big(l\cdot V_l(\tau)\Big) \quad &= \quad j\left(l\cdot\left(-\frac{1}{l^2\tau}\right)\right) \quad = \quad j\left(-\frac{1}{l\tau}\right) \quad = \quad j\Big(l\tau\Big), \\ f\Big(V_l(\tau)\Big) \quad &= \quad f\left(-\frac{1}{l^2\tau}\right) \quad = \quad \frac{l^s}{f(l\tau)}. \end{aligned}$$

Definieren wir für $0 \le r \le l+1$ die Funktionen

$$s_r(\tau) \quad = \quad \sum_{k=0}^{\kappa} a_{l+1-r,k}\cdot j(l\tau)^k, \tag{5.6}$$

so sind alle $s_r(\tau)$, $0 \le r \le l+1$, offensichtlich invariant unter allen Transformationen $V_n$, $0 \le n \le l$. Betrachten wir also das Polynom

$$h(X) \quad = \quad \sum_{r=0}^{l+1} s_r(\tau)\cdot X^{l+1-r}, \tag{5.7}$$

so werden alle Nullstellen dieses Polynom nach obigen Bemerkungen durch die Funktionen $f(V_n(\tau))$ für $0 \le n \le l$ gegeben. Offensichtlich können wir aber bei Kenntnis des Polynoms $h(X)$ durch Koeffizientenvergleich in (5.6) leicht die gewünschten Koeffizienten $a_{r,k}$ berechnen. Bevor wir diese Beobachtung ausnutzen, um einen Algorithmus zur Bestimmung der Polynomkoeffizienten $a_{r,k}$ anzugeben, untersuchen wir in folgendem Lemma den Wert von $\kappa$.

**Lemma 5.7** *In (5.3) und (5.4) gilt $\kappa = v$.*

**Beweis:** Wir kennen die Nullstellen des Polynoms $h(X)$ aus (5.7) und mit (5.6) die Darstellung der Koeffizienten von $h(X)$ als Polynom in $j(l\tau)$. Damit fängt die Fourierentwicklung von $s_r(\tau)$ mit einem Term mit $q_\tau$-Exponenten $-\kappa\, l$ an. Diese Koeffienten werden aber andererseits als elementarsymmetrische Funktionen der Nullstellen gegeben. Die $q_\tau$-Entwicklungen der Nullstellen $f(V_n(\tau))$ für $0 \leq n \leq l$ besitzen die folgenden minimalen $q_\tau$-Exponenten (beachte, daß die zugehörigen Koeffizienten ungleich null, aber nicht eins sind):

- $-v$ für $0 \leq n < l$ ,
- $l\, v$ für $n = l$ .

Untersuchen wir mit dieser Beobachtung die Fourierreihenentwicklungen der elementarsymmetrischen Funktionen der Nullstellen, so erkennen wir leicht, daß die Fourierentwicklung des Koeffizient $s_l(\tau)$ von $X^1$ in $h(X)$ mit dem „kleinsten" $q_\tau$-Exponenten beginnt. Dieser Exponent ist aber genau $-l\, v$, so daß $\kappa = v$ gewählt werden kann. ■

Ein Verfahren zur Bestimmung eines normierten Polynoms mit gegebenen Nullstellen liefert der Satz von Newton [Wa71, Seite 99 ff]. Nach Definition ist das Polynom $G_l(X)$ und damit auch $h(X)$ normiert. Also ist der Satz von Newton anwendbar, um $h(X)$ auszurechnen. Sei dazu $h(X)$ wie beschrieben gegeben als

$$h(X) \quad = \quad X^{l+1} + s_1(\tau) \cdot X^l + \ldots + s_{l+1}(\tau) \cdot X^0.$$

Zur Bestimmung der Koeffizienten $s_r(\tau)$ mit Hilfe des Satzes von Newton benötigen wir die $r$-ten Potenzsummen der Nullstellen, d.h. für $0 \leq r \leq l+1$ die Werte

$$c_r(\tau) \quad = \quad \sum_{n=0}^{l-1} f\left(\tau + \frac{n}{l}\right)^r + \left(\frac{l^s}{f(l\tau)}\right)^r .$$

Setzen wir $s_0(\tau) = 1$, so können wir dann die Werte von $s_r(\tau)$ für $1 \leq r \leq l+1$ sukzessive mit Hilfe der Formel

$$s_r(\tau) \quad = \quad \frac{(-1)^r}{r} \cdot \sum_{m=1}^{r} (-1)^{m-1} \cdot c_m(\tau) \cdot s_{r-m}(\tau) \tag{5.8}$$

berechnen. Dabei sollte man beachten, daß die Division durch $r$ nicht zur Bildung von rationalen Koeffizienten führen kann.

Also benötigen wir nun noch eine Methode, um für unsere spezielle Funktion $f(\tau)$ schnell Fourierreihenentwicklungen der Potenzsummen $c_r(\tau)$ zu berechnen. Dazu teilen wir diese Potenzsumme in zwei Teile auf. Sei

$$c_r(\tau) \quad = \quad \underbrace{\sum_{n=0}^{l-1} f\left(\tau + \frac{n}{l}\right)^r}_{=c_{r,1}(\tau)} + \underbrace{\left(\frac{l^s}{f(l\tau)}\right)^r}_{=c_{r,2}(\tau)} .$$

Dann läßt sich die Bestimmung der Entwicklung von $c_{r,2}(\tau)$ leicht durchführen. Dazu benutzen wir nur die dünn besetzte Reihenentwicklung für $f(l\tau)$. Zur Berechnung von $c_{r,1}(\tau)$ nehmen wir an, daß wir die Fourierreihenentwicklung der Funktion $f(\tau)^r$ als

$$f(\tau)^r \quad = \quad q_\tau^{-vr} \cdot \left[\sum_{\nu=0}^{\infty} a_\nu \cdot q_\tau^\nu\right]$$

kennen. Dann erhalten wir daraus

$$\begin{aligned}
f\left(\tau + \frac{n}{l}\right)^r \quad &= \quad \exp\Big(-2\pi i\,(\tau + n/l)vr\Big) \cdot \left[\sum_{\nu=0}^{\infty} a_\nu \cdot \exp\Big(2\pi i\,(\tau + n/l)\,\nu\Big)\right] \\
&= \quad q_\tau^{-vr} \cdot \exp\left(\frac{-2\pi i\,n\,vr}{l}\right) \cdot \left[\sum_{\nu=0}^{\infty} a_\nu \cdot q_\tau^\nu \cdot \exp\left(\frac{2\pi i\,n\,\nu}{l}\right)\right] \\
&= \quad q_\tau^{-vr} \cdot \left[\sum_{\nu=0}^{\infty} a_\nu \cdot q_\tau^\nu \cdot \exp\left(\frac{2\pi i\,n\,(\nu - vr)}{l}\right)\right].
\end{aligned}$$

Damit erhalten wir für $c_{r,1}(\tau)$ die folgende Gleichung

$$\begin{aligned}
c_{r,1}(\tau) \quad &= \quad \sum_{n=0}^{l-1} f\left(\tau + \frac{n}{l}\right)^r \\
&= \quad \sum_{n=0}^{l-1} q_\tau^{-vr} \cdot \left[\sum_{\nu=0}^{\infty} a_\nu \cdot q_\tau^\nu \cdot \exp\left(\frac{2\pi i\,n\,(\nu - vr)}{l}\right)\right] \\
&= \quad q_\tau^{-vr} \cdot \sum_{\nu=0}^{\infty} a_\nu \cdot q_\tau^\nu \cdot \underbrace{\sum_{n=0}^{l-1} \exp\left(\frac{2\pi i\,n(\nu - vr)}{l}\right)}_{=l_\nu}.
\end{aligned} \tag{5.9}$$

Rechnen wir den Wert von $l_\nu$ aus, so müssen wir zwei mögliche Fälle unterscheiden:

$\nu - vr \equiv 0 \bmod l$: Sei etwa $(\nu - vr)/l = d$. Dann erhalten wir

$$l_\nu \quad = \quad \sum_{n=0}^{l-1} \exp(2\pi i\,n\,d) \quad = \quad \sum_{n=0}^{l-1} 1 \quad = \quad l.$$

$\nu - vr \not\equiv 0 \bmod l$: Wir beachten, daß für alle $0 \leq n \leq l-1$ die komplexe Zahl $\exp\left(2\pi i \frac{n\,(\nu - vr)}{l}\right)$ eine $l$-te Einheitswurzel in $\mathbb{C}$, d.h. eine Nullstelle der Gleichung $X^l - 1 = 0$ in $\mathbb{C}$, ist. Es sind dies sogar alle Lösungen, denn man erkennt leicht, daß alle diese Zahlen verschieden sind. Wiederum durch Anwendung der Newtonschen Regel erhalten wir dann, daß die Summe aller Nullstellen von $X^l - 1$ der Koeffizient von $X^{l-1}$, also Null ist. Damit gilt in diesem Fall

$$l_\nu \quad = \quad 0.$$

Damit können wir mit Hilfe von (5.9) auch die Fourierreihenentwicklung von $c_{r,1}(\tau)$ mit vorgegebener Genauigkeit berechnen, wenn wir die Fourierreihenentwicklung von

$f(\tau)^r$ mit genügend großer Genauigkeit kennen. Man beachte, daß es ein Vorteil des hier beschriebenen Verfahrens ist, daß überwiegend Operationen auf dünn besetzten Fourierreihenentwicklungen angewandt werden. Die Bestimmung der Potenzen $f(\tau)^r$ sind die einzigen Operationen mit dicht besetzten Fourierreihenentwicklungen. Die daraus berechnete Fourierreihe $c_{r,1}(\tau)$ ist nach Konstruktion dünn besetzt und damit ist sogar $c_r(\tau)$ dünn besetzt. Es ist leicht ersichtlich, daß sich diese Eigenschaft dann auf alle anderen benutzten Fourierreihen fortpflanzt.

Untersuchen wir nun noch, welche Genauigkeit wir verwenden müssen, um die Koeffizienten von $G_l(X)$ eindeutig bestimmen zu können. Dazu beachte man, daß die Genauigkeit der Summe oder des Produktes zweier Fourierreihenentwicklungen genau das Minimum der beiden Genauigkeiten der Summanden ist. Betrachten wir daher einen beliebigen Koeffizienten $s_r(\tau)$ aus (5.6). Offensichtlich können wir die Polynomkoeffizienten $a_{r,k}$ eindeutig bestimmen, wenn wir alle Koeffizienten von nicht-positiven $q_\tau$-Potenzen in den Fourierreihenentwicklungen $j(l\tau)^k$ für $0 \leq k \leq v$ kennen (beachte: Lemma 5.7 liefert $\kappa = v$). Damit müssen wir $j(l\tau)^v$ mit Genauigkeit $l\,v$ kennen. Verwenden wir diese Genauigkeit auch für alle anderen Fourierreihenentwicklungen, so folgt aus obigen Bemerkungen über die Änderung der Genauigkeit bei Operationen, daß wir für alle auftretenden Fourierreihenentwicklungen immer alle Koeffizienten von nicht-negativen $q_\tau$-Potenzen genau kennen. Daher wählen wir als Genauigkeit, mit der wir alle Fourierreihenentwicklungen berechnen, genau $l\,v$. Damit erhalten wir den folgenden Algorithmus zur Berechnung des äquivalenten Polynoms $G_l(X,Y)$ für die gegebene Funktion $g(\tau)$:

**Algorithmus 5.8** [Bestimmung von $G_l(X,Y)$ für Funktion $g(\tau)$]

**Eingabe:** Fourierreihenentwicklungen für $f(\tau)$ und $j(l\tau)$ mit Genauigkeit $l\,v$.
**Ausgabe:** Polynomkoeffizienten $a_{r,k}$ für $0 \leq r \leq l+1,\ 0 \leq k \leq v$.

| | | |
|---|---|---|
| Setze $a_{l+1,k} \leftarrow 0$ für $1 \leq k \leq v$ und $a_{l+1,0} \leftarrow 1$. | | (1) |
| Setze $s_0(\tau) \leftarrow 1,\ h_1(\tau) \leftarrow 1,\ h_2(\tau) \leftarrow 1$. | | (2) |
| FOR $r = 1, \ldots, l+1$ | | (3) |
| | Berechne $h_1(\tau) \leftarrow h_1(\tau) \cdot f(\tau)$. /* $h_1(\tau) = f(\tau)^r$ */ | (4) |
| | Berechne $c_{r,1}(\tau)$ mit Formel (5.9) aus $h_1(\tau)$. | (5) |
| | Berechne $h_2(\tau) \leftarrow h_2(\tau) \cdot \left(\frac{l^s}{f(l\tau)}\right)$. /* $h_2(\tau) = c_{r,2}(\tau)$ */ | (6) |
| | Setze $c_r(\tau) \leftarrow c_{r,1}(\tau) + h_2(\tau)$. | (7) |
| | Berechne $s_r(\tau)$ mit Formel (5.8). | (8) |
| | Bestimme $a_{l+1-r,k}$ für $0 \leq k \leq v$ mit Formel (5.6). | (9) |

Bei der Implementierung dieses Algorithmus kann man den folgenden Trick ausnutzen: aus der Definition der Koeffizienten $s_r(\tau)$ aus (5.6) folgt, daß wir zur Bestimmung der Polynomkoeffizienten $a_{r,k}$ nur die Koeffizienten aller nicht-positiven $q_\tau$-Potenzen in der Reihenentwicklung von $s_r(\tau)$ benötigen. Aus (5.8) folgt direkt, daß wir dann die Fourierreihenentwicklungen der Potenzsummen $c_r(\tau)$ bis zum Koeffizienten von $q_\tau^{lv}$ einschließlich exakt kennen müssen. Der minimale $q_\tau$-Koeffizient der Funktion $c_{r,2}(\tau)$ ist aber nur für $r = 0$ und $r = 1$ kleiner als diese Schranke; für alle anderen Werte von $r$ ist der minimale $q_\tau$-Exponent echt größer als $lv$. Daher können wir uns die Berechnung der Funktionen $c_{r,2}(\tau)$ für $r > 1$ sparen. In obigem Algorithmus kann daher die Berechnung von $h_2(\tau)$ in den Schritten (2), (6) und (7) für $r > 1$ unterbleiben.

## 5.3 Funktionen invariant unter Transformationen aus $\Gamma_0^*(l)$

Wir haben in Abschnitt 5.1 eine Funktion vorgestellt, mit der wir für jede ungerade Primzahl $l$ ein zum modularen Polynom äquivalentes Polynom berechnen können. Der Grad dieser Polynome in der zweiten Variable $Y$ war nach Lemma 5.7 $v = \frac{s\,(l-1)}{12}$, wobei $s$ die kleinste natürliche Zahl ist, so daß $v \in \mathbb{N}$ gilt. Dieser Grad $v$ ist für Primzahlen $l \equiv -1 \bmod 12$ aber $(l-1)/2$. Wir werden deshalb in diesem Abschnitt beschreiben, wie wir für eine feste ungerade Primzahl $l > 3$ „bessere“ Funktionen bestimmen können. Der Nachteil bei der Benutzung solcher Funktionen ist der, daß für jede ungerade Primzahl $l > 3$ diese Funktion explizit berechnet werden muß, d.h. wir haben keine für jedes $l$ gültige Formel für solche Funktionen.

Wir definieren die folgende Menge von Transformationen

$$\Gamma_0^*(l) \quad = \quad \Gamma_0(l) \ \bigcup \ \begin{pmatrix} 0 & -1 \\ l & 0 \end{pmatrix} \cdot \Gamma_0(l).$$

Wir wollen nun mit Hilfe der Dedekindschen $\eta$-Funktion Funktionen bestimmen, die unter allen Transformationen aus $\Gamma_0^*(l)$ invariant sind. Die Invarianzgruppe einer solchen Funktion ist ebenfalls $\Gamma_0(l)$ (die Invarianzgruppe besteht nach Definition nur aus unimodularen Transformationen, unter denen eine Funktion invariant ist). Damit können wir aus Satz 4.31 wiederum folgern, daß ein mit Hilfe einer solchen Funktion berechnetes äquivalentes Polynom an Stelle des $l$-ten modularen Polynoms verwendet werden kann.

Sei ab sofort $l > 3$ und $a(\tau)$ die spezielle Funktion

$$a(\tau) \quad = \quad \eta(\tau) \cdot \eta(l\tau). \tag{5.10}$$

Sei im folgenden $s$ die kleinste positive Zahl, so daß 24 ein Teiler von $s \cdot (l+1)$ ist. Wir werden mit Hilfe von $a(\tau)$ eine unter allen Transformationen aus $\Gamma_0^*(l)$ invariante Funktion $A(\tau)$ bestimmen. Ein wichtiger Hinweis auf die dazu nötige Vorgehensweise liefert folgendes Lemma aus [AtLe70, Lemma 16].

**Lemma 5.9** *Angenommen $A(\tau)$ ist eine formale Potenzreihe mit ganzen positiven Potenzen von $q_\tau$ und $A(s\tau)$ ist invariant unter Transformationen aus $\Gamma_0(ls)$. Dann ist $A(\tau)$ invariant unter allen Transformationen aus $\Gamma_0(l)$.*

Wir untersuchen daher nun, wie sich die Funktion $a(s\tau)$ aus (5.10) bei Anwendungen von Transformationen aus $\Gamma_0(ls)$ verhält.

**Lemma 5.10** *Für eine Transformation $V = (a, b; cls, d) \in \Gamma_0(ls)$ gilt*

$$a\Big(V(s\tau)\Big) \quad = \quad \epsilon(a,b,c,d)\cdot(cls\,\tau + d)\cdot a\Big(s\tau\Big),$$

*wobei $\epsilon = \epsilon(a,b,c,d)$ gegeben wird durch*

$$\epsilon = \begin{cases} \left(\frac{l}{d}\right)\cdot i^{d-1}\cdot\exp\left(\frac{-\pi i}{12}c\,(l+1)\cdot\Big[d + a\,(d^2-1)\Big]\right), & \textit{falls } d \textit{ ungerade, positiv.} \\ \left(\frac{d}{l}\right)\cdot i^{-c(l+1)/2}\cdot\exp\left(\frac{\pi i}{12}c\,(l+1)\Big[a+d\Big]\right), & \textit{falls } c \textit{ ungerade, positiv.} \end{cases}$$

**Beweis:** Für die Transformation $V$ wie im Lemma gegeben benutzen wir die Formeln aus Satz 5.3 und erhalten so

$$\begin{aligned} a\Big(V(s\tau)\Big) &= \eta\Big(s\cdot V(\tau)\Big)\cdot\eta\Big(ls\cdot V(\tau)\Big) \\ &= \eta\left(\frac{as\,\tau + bs}{cls\,\tau + d}\right)\cdot\eta\left(\frac{als\,\tau + bls}{cls\,\tau + d}\right) \\ &= \epsilon(a,b,c,d)\cdot(cls\,\tau + d)\cdot\eta(s\tau)\cdot\eta(ls\,\tau) \\ &= \epsilon(a,b,c,d)\cdot(cls\,\tau + d)\cdot a(s\tau). \end{aligned}$$

Den Wert von $\epsilon(a,b,c,d)$ berechnen wir dabei ebenfalls mit den Formeln aus Satz 5.3. Ist $d$ ungerade und ohne Einschränkung positiv, so erhalten wir

$$\begin{aligned} \epsilon &= \left(\frac{c\,l}{d}\right)\cdot\left(\frac{c}{d}\right)\cdot i^{d-1}\cdot\exp\left(\frac{\pi i}{12}(l+1)\cdot\Big[bds - cd - ac\,(d^2-1)\Big]\right) \\ &= \left(\frac{l}{d}\right)\cdot i^{d-1}\cdot\exp\left(\frac{-\pi i}{12}c\,(l+1)\cdot\Big[d + a\,(d^2-1)\Big]\right). \end{aligned}$$

Dabei wurde bei der Umformung ausgenutzt, daß 24 ein Teiler von $s\,(l+1)$ ist und daß daher $\exp(\frac{\pi i}{12}\,s\,(l+1)) = 1$ gilt. Die Bestimmung von $\epsilon$ für den Fall, daß $c$ ungerade und positiv ist, erfolgt auf dieselbe Weise. ■

Wir werden in der folgenden Definition einen Operator vorstellen, mit dessen Hilfe es möglich ist, eine gegebene komplexwertige Funktion „leicht" zu verändern. Diesen Operator werden wir dann anschließend auf die hier verwendete Funktion $a(s\tau)$ anwenden.

**Definition 5.11** *Seien eine Primzahl $r$ und die Transformationen*

$$H_j \quad = \quad \begin{pmatrix} 1 & j \\ 0 & r \end{pmatrix} \quad 0 \le j < r \qquad \textit{und} \qquad H_r \quad = \quad \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

*gegeben. Dann definieren wir für eine Funktion $f(\tau)$ den $r$-ten* **Hecke-Operator** *auf $f(\tau)$ als*

$$T_r\Big(f(\tau)\Big) \quad = \quad \frac{1}{r}\cdot\sum_{k=0}^{r-1} f\Big(H_k(\tau)\Big) \;+\; f\Big(H_r(\tau)\Big).$$

Wir wenden spezielle Hecke-Operatoren auf die Funktion $a(\tau)$ aus (5.10) an. Auf diese Weise werden wir Funktionen $A(\tau)$ erhalten, so daß $A(s\tau)$ invariant unter Transformationen aus $\Gamma_0(ls)$ ist. Eine Funktion aus dieser Menge, bei der alle Exponenten in der $q_\tau$-Entwicklung ganze Zahlen sind, ist nach Lemma 5.9 eine Funktion, die sogar unter allen Transformationen aus $\Gamma_0(l)$ invariant ist. Wir beschreiben in dem folgenden Satz die Menge der Hecke-Operatoren, die wir verwenden können.

**Satz 5.12** *Sei $a(\tau)$ wie in (5.10) gegeben. Sei weiterhin $r$ eine ungerade Primzahl ungleich $l$, so daß $r$ ein Quadrat modulo $l$ und $s$ ein Teiler von $r-1$ ist. Wir definieren die Funktion $A(\tau)$ als*

$$A(\tau) = \frac{T_r(a(\tau))}{a(\tau)}. \tag{5.11}$$

*Dann ist die Funktion $A(s\tau)$ invariant unter allen Transformationen aus $\Gamma_0(ls)$.*

**Beweis:** Der Beweis dieses Satzes wird mit Hilfe einer Reihe von Lemmata geschehen. Seien während des ganzen Beweises die Voraussetzungen des Satzes erfüllt; sei eine Transformation $V \in \Gamma_0(sl)$ wie in Lemma 5.10 und die Transformationen $H_j$ aus Definition 5.11 gegeben. Dann formulieren wir zuerst folgendes Lemma.

**Lemma 5.13** *Es gibt eine Permutation $\pi \in S_{r+1}$, so daß es für alle $0 \leq k \leq r$ eine Matrix $V_k' \in \Gamma_0(ls)$ gibt mit*

$$H_k \cdot V = V_k' \cdot H_{\pi(k)}.$$

**Beweis (Lemma):** Die Existenzaussage des Lemmas wird in [Ap90, Th. 6.9, Seite 124] bewiesen. Die Behauptung $V' \in \Gamma_0(sl)$ folgt direkt aus der Konstruktion der Matrix $V'$ in dem zugehörigen Beweis. Die Tatsache, daß auf der rechten Seite obiger Gleichung alle Matrizen $H_k$ auftreten, folgt durch Berechnen aller zugehörigen Matrizen. □

Damit können wir die folgende Umrechnung für den „Zähler“ der Funktion $A(s\tau)$ durchführen, wenn wir eine Transformation $V \in \Gamma_0(ls)$ darauf anwenden:

$$\begin{aligned}
T_r\Big(a(sV(\tau))\Big) &= \frac{1}{r} \cdot \sum_{k=0}^{r-1} a\Big(s\,H_k(V(\tau))\Big) + a\Big(s\,H_r(V(\tau))\Big) \\
&= \frac{1}{r} \cdot \sum_{k=0}^{r-1} a\Big(s\,(H_k \cdot V)(\tau)\Big) + a\Big(s\,(H_r \cdot V)(\tau)\Big) \\
&= \frac{1}{r} \cdot \sum_{k=0}^{r-1} a\Big(s\,(V_k' \cdot H_{\pi(k)})(\tau)\Big) + a\Big(s\,(V_r' \cdot H_{\pi(r)})(\tau)\Big) \\
&= \frac{1}{r} \cdot \sum_{k=0}^{r-1} a\Big(s\,V_k'(H_{\pi(k)}(\tau))\Big) + a\Big(s\,V_r'(H_{\pi(r)}(\tau))\Big).
\end{aligned}$$

Da die Funktion $a(\tau)$ mit Hilfe der $\eta$-Funktion definiert ist, folgt aus Satz 5.3, daß bei Anwendung von Transformationen $V_k'$ auf $\tau_k = H_{\pi(k)}(\tau)$ 24-te Einheitswurzeln $\epsilon$ entstehen. Andererseits entstehen solche Einheitswurzeln auch bei der Anwendung von $V$ auf $\tau$ in $a(s\tau)$. Wir untersuchen im folgenden Lemma, wie diese Einheitswurzeln zusammenhängen.

**Lemma 5.14** *Seien $\epsilon_i, i = 1, 2$, die Einheitswurzeln, die wir bei Anwendung der Transformation $V_k'$ auf $\tau_k$ bzw. $V$ auf $\tau$ erhalten. Dann gilt $\frac{\epsilon_1}{\epsilon_2} = 1$.*

**Beweis (Lemma):** Zum Beweis des Lemmas müssen wir zu gegebenem $V$ alle möglichen Matrizen $V_k'$ ausrechnen und zu diesen Transformationen die zugehörigen Einheitswurzeln berechnen. Wir rechnen dies hier an einem Beispiel vor; alle anderen Fälle kann man analog berechnen. Sei etwa $k = r$ und $V$ wie üblich gegeben. Dann erhalten wir $V_r'$ als die Matrix

$$V_r' = \begin{cases} \begin{pmatrix} a & br \\ cls/r & d \end{pmatrix}, & \text{falls } c \equiv 0 \bmod r, \\ \begin{pmatrix} a\,r & b - f\,a \\ cls & (d - clsf)/r \end{pmatrix}, & \text{falls } c \not\equiv 0 \bmod r. \end{cases}$$

Dabei sei im zweiten Fall $f$ so gewählt, daß $d - clsf$ durch $r$ teilbar ist. Nun müssen wir alle möglichen Fälle, die wir in Satz 5.3 angegeben haben, untersuchen. Nehmen wir etwa an, $d$ wäre ungerade und ohne Einschränkung positiv. Dann können wir $\frac{\epsilon_1}{\epsilon_2}$ im Fall $c \equiv 0 \bmod r$ mit Hilfe der Formeln aus Satz 5.3 und Lemma 5.10 ausrechnen und erhalten so

$$\begin{aligned} \frac{\epsilon_1}{\epsilon_2} &= \frac{\left(\frac{l}{d}\right) \cdot i^{d-1} \cdot \exp\left(\frac{-\pi i}{12}(l+1) \cdot \left[\frac{cd}{r} + (d^2-1) \cdot \frac{ac}{r}\right]\right)}{\left(\frac{l}{d}\right) \cdot i^{d-1} \cdot \exp\left(\frac{-\pi i}{12}(l+1) \cdot \left[cd + (d^2-1)ac\right]\right)} \\ &= \exp\left(\frac{\pi i}{12}(l+1) \cdot (r-1) \cdot \frac{cd + (d^2-1)\,ac}{r}\right) \\ &= 1. \end{aligned}$$

Dabei wird benutzt, daß $r$ ein Teiler von $c$ ist, daß $s$ $r-1$ teilt und damit 24 ein Teiler von $(l+1)(r-1)$ ist. Der zweite mögliche Fall für $V_r'$ geht vollkommen analog, wenn $(d - clsf)/r$ ungerade ist. Untersuchen wir daher die Möglichkeit, daß dieser Wert gerade ist. Dann muß $cls$ ungerade sein, denn sonst wäre die Determinante von $V_r'$ gerade. Damit können wir die zweite Möglichkeit für den Multiplikator in Lemma 5.10 anwenden und erhalten so (setze dabei $d' = (d - clsf)/r$)

$$\begin{aligned} \frac{\epsilon_1}{\epsilon_2} &= \frac{\left(\frac{d'}{l}\right) \cdot i^{-c(l+1)/2} \cdot \exp\left(\frac{\pi i}{12}c\,(l+1)\,(ar+d')\right)}{\left(\frac{d}{l}\right) \cdot i^{-c(l+1)/2} \cdot \exp\left(\frac{\pi i}{12}c(l+1)(a+d)\right)} \\ &= \left(\frac{r}{l}\right) \cdot \exp\left(\frac{\pi i}{12}c(l+1)(d'-d)\right) \\ &= 1. \end{aligned}$$

Dabei wird ausgenutzt, daß 24 ein Teiler von $(l+1)(1-r)$ und $s\,(l+1)$ ist. Zusätzlich setzt man noch die Definition von $d'$ ein. Alle anderen Fälle für Matrizen $V_k'$ kann man analog untersuchen. In allen Fällen erhält man dann $\frac{\epsilon_1}{\epsilon_2} = 1$. □

Damit haben wir gezeigt, daß bei Anwendung einer Transformation $V \in \Gamma_0(sl)$ auf die Funktion $A(s\tau)$ immer nur der Multiplikator eins entsteht. Um zu zeigen, daß $A(s\tau)$ invariant unter diesen Transformationen ist, müssen wir noch untersuchen, wie sich der Zähler von $A(\tau)$ unter solchen Transformationen verhält.

**Lemma 5.15** *Sei $\epsilon_2$ der Multiplikator, den wir bei Anwendung einer Transformation $V$ wie oben auf $a(\tau)$ erhalten. Dann gilt*

$$\frac{1}{\epsilon_2} \cdot T_r\Big(a(s\,V(\tau))\Big) \quad = \quad (cls\tau + d) \cdot T_r\Big(a(s\tau)\Big).$$

**Beweis (Lemma):** Die Aussage über den Multiplikator haben wir schon im letzten Lemma bewiesen. Die zweite Behauptung des Lemmas wird in [Ap90, Th. 6.10, Seite 125] bewiesen. Der dort angegebene Beweis kann direkt auf unsere Situation übertragen werden. □

Setzen wir alle diese Lemmata zusammen, so erhalten wir die Aussage des Satzes, denn wir berechnen

$$\begin{aligned} A\Big(s\,V(\tau)\Big) \quad &= \quad \frac{T_r\Big(a(s\,V(\tau))\Big)}{a(s\,V(\tau))} \\ &= \quad \frac{T_r\Big(a(s\,V(\tau))\Big)}{\epsilon_2 \cdot (cls\tau + d) \cdot a(s\tau)} \\ &= \quad \frac{T_r\Big(a(s\tau)\Big)}{a(s\tau)} \\ &= \quad A(s\tau). \end{aligned}$$ ■

Wir werden im folgenden zeigen, daß eine solche Funktion $A(\tau)$ auch invariant unter der Transformation $(0,-1;l,0)$ ist. Auf die gleiche Weise wie in Lemma 5.4 können wir dann zeigen, daß $A(\tau)$ nicht invariant unter einer unimodularen Transformation, die kein Element von $\Gamma_0(l)$ ist, sein kann. Aus dem Satz 5.24 (siehe Seite 74) wird folgen, daß alle solche Funktionen $A(\tau)$ eine Fourierreihenentwicklung mit „ganzen" $q_\tau$-Exponenten besitzen. Damit haben wir eine Methode gefunden, um Funktionen zu bestimmen, die invariant unter Transformationen aus $\Gamma_0(l)$ sind. Aus Lemma 5.9 folgt dann direkt das folgende Korollar:

**Korollar 5.16** *Die Funktion $A(\tau)$ wie in Satz 5.12 ist invariant unter allen Transformationen aus $\Gamma_0(l)$.*

Damit haben wir durch verschiedene Wahl des Parameters $r$ aus Satz 5.12 die Möglichkeit, verschiedene geeignete Funktionen $A(\tau)$ zu berechnen. Die Fourierreihenentwicklungen dieser Funktionen besitzen unter Umständen auch verschiedene minimale Anfangspotenzen von $q_\tau$.

Untersuchen wir noch das Verhalten solcher Funktionen unter einer weiteren schon betrachteten Transformation, nämlich $\tau \to \frac{-1}{l\tau}$. Dabei sollen alle Voraussetzungen an $r$, die wir in Satz 5.12 gemacht haben, weiterhin erfüllt sein.

**Satz 5.17** *Falls $l > 3$ ein Quadrat modulo $r$ ist, so ist die in Satz 5.12 definierte Funktion $A(\tau)$ invariant unter der Transformation* $(0,-1;l,0)$.

**Beweis:** Der Beweis geschieht wiederum mit Hilfe verschiedener Lemmata.

**Lemma 5.18** *Für alle ganzen Zahlen $x, y, z, w$ mit $l^2xw - lzy = l$ gibt es eine Matrix $V \in \Gamma_0(l)$, so daß gilt*

$$\begin{pmatrix} 0 & -1 \\ l & 0 \end{pmatrix} \quad = \quad V \cdot \begin{pmatrix} lx & y \\ lz & lw \end{pmatrix}.$$

**Beweis (Lemma):** Durch Vergleich der Determinanten der Matrizen $(0,-1;l,0)$ und $(lx, y; lz, lw)$ erkennen wir direkt, daß eine solche Matrix $V$ Determinante 1 haben muß. Setzen wir nun $V$ allgemein an als $(a, b; c, d)$ und betrachten wir für beliebige Zahlen $lx$, $y$, $lz$ und $lw$ folgende Gleichung:

$$V^{-1} \cdot \begin{pmatrix} 0 & -1 \\ l & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} lx & y \\ lz & lw \end{pmatrix}.$$

Hieraus erhalten wir durch Berechnung der „linken" Seite eine Menge von Gleichungen und daraus die Einträge von $V$ als $a = z$, $b = -x$, $c = lw$ und $d = -y$. Damit gilt $V \in \Gamma_0(l)$ und dieses Lemma ist bewiesen. □

**Lemma 5.19** *Sei $r$ eine ungerade Primzahl. Für jede Primzahl $l > 3$, die ein Quadrat modulo $r$ ist, gibt es eine Matrix $W_l = (lx, y; lz, lw)$ wie in Lemma 5.18, so daß $x = w$, $z = 2\,rs$ und $y \equiv 0 \bmod r$ gilt.*

**Beweis (Lemma):** Zum Beweis dieses Lemmas benutzen wir, daß unter den gegebenen Voraussetzungen die Zahlen $l$ und $2\,r^2s$ teilerfremd sind. Damit gibt es ganze Zahlen $x_1$ und $x_2$, so daß gilt

$$x_1 \cdot (2\,r^2s) \; + \; x_2 \cdot l \quad = \quad 1.$$

Da $l$ ein Quadrat modulo $r$ und verschieden von $r$ ist, folgt aus Hensels Lemma, daß $l$ sogar ein Quadrat modulo $r^2$ ist (beachte auch $r > 2$). Betrachten wir alle Möglichkeiten für $l \bmod 24$ und die zugehörigen Werte $s$, so wird direkt deutlich, daß immer $l \equiv 1 \bmod s$ gilt und daß damit $l$ auch immer ein Quadrat modulo $s$ ist. Insgesamt ist $l$ also sogar ein Quadrat modulo $2r^2s$. Damit ist auch $x_2$ ein Quadrat modulo $2r^2s$ und es gibt Zahlen $y_1, y_2 \in \mathbb{Z}$ mit $x_2 = y_1^2 + y_2 \cdot (2r^2s)$. Setzen wir dies in obige Gleichung ein, so erhalten wir

$$y_1^2 \cdot l + 2\,r^2 s \cdot (x_1 + l\,y_2) \quad = \quad 1 \qquad \text{bzw.} \qquad y_1^2 \cdot l^2 + 2\,lr^2 s \cdot (x_1 + l\,y_2) \quad = \quad l.$$

Wählen wir die Einträge der Matrix $W_l$ dann als $x = w = y_1$, $z = 2rs$ und $y = -r(x_1 + ly_2)$, so sind offensichtlich alle Bedingungen erfüllt. □

Sei im folgenden die Matrix $W_l$ wie in Lemma 5.19 gegeben. Mit Lemma 5.18 gibt es eine Matrix $V \in \Gamma_0(l)$, so daß

$$\begin{pmatrix} 0 & -1 \\ l & 0 \end{pmatrix} \quad = \quad V \cdot W_l$$

gilt. Da $A(\tau)$ invariant unter Transformationen aus $\Gamma_0(l)$ ist, können wir das Verhalten der Funktion $A(\tau)$ unter $\tau \to \frac{-1}{l\tau}$ durch Untersuchung des Verhaltens bei Anwendung der Transformation $W_l$ bestimmen, denn es gilt

$$A\left(\frac{-1}{l\tau}\right) \quad = \quad A\Big(V(W_l(\tau))\Big) \quad = \quad A\Big(W_l(\tau)\Big).$$

Dies untersuchen wir mit Hilfe der folgenden Lemmata, in denen wir alle in $A(\tau)$ vorkommenden „Teilfunktionen“ unter dieser Transformation $W_l$ betrachten.

**Lemma 5.20** *Für die Funktion $a(\tau) = \eta(\tau)\,\eta(l\tau)$ gilt*

$$a\Big(W_l(\tau)\Big) \quad = \quad \left(\frac{z}{l}\right) \cdot i^{(l+1)\cdot w/2-1} \cdot \exp\Big(\pi i\,(l+1)\,w\,y/12\Big) \cdot \sqrt{l} \cdot (z\tau + w) \cdot a(\tau).$$

**Beweis (Lemma):** Der Beweis erfolgt durch Nachrechnen mit Hilfe der Formeln aus Satz 5.3 (Seite 58). Dabei beachte man, daß bei der angegebenen Wahl von $W_l$ $z$ gerade und kongruent zu 0 mod $s$ ist. Damit liefern alle Terme mit $z\,(l+1)$ in dem Argument der Exponentialfunktion Vielfache von $2\pi i$ und fallen damit weg. □

**Lemma 5.21** *Für $a(\tau) = \eta(\tau)\,\eta(l\tau)$ und die Transformation $H_r$ aus Definition 5.11 gilt*

$$\frac{a(H_r(W_l(\tau)))}{a(W_l(\tau))} \quad = \quad \frac{a(H_r(\tau))}{a(\tau)}.$$

**Beweis (Lemma):** Durch Ausrechnen erhalten wir die Gleichung

$$H_r \cdot W_l \quad = \quad \underbrace{\begin{pmatrix} lx & ry \\ lz/r & lw \end{pmatrix}}_{=:W_l'} \cdot H_r,$$

wobei $W_l'$ eine über $\mathbb{Z}$ definierte Matrix der Determinante $l$ ist. Damit müssen wir für den Zähler der gegebenen Funktion das Verhalten unter der Transformation $W_l'$ untersuchen, denn es gilt

$$a\Big(H_r(W_l(\tau))\Big) \;=\; a\Big((H_r \cdot W_l)(\tau)\Big) \;=\; a\Big((W_l' \cdot H_r)(\tau)\Big) \;=\; a\Big(W_l'(H_r(\tau))\Big).$$

Rechnen wir dies wiederum mit den Formeln aus Satz 5.3 aus, so erhalten wir

$$a\Big(W_l'(H_r(\tau))\Big) \quad = \quad \epsilon_z \cdot \sqrt{l} \cdot (z\tau + w) \cdot a\Big(H_r(\tau)\Big),$$

wobei wir für die Einheitswurzel $\epsilon_z$ erhalten

$$\epsilon_z \quad = \quad \left(\frac{z/r}{l}\right) \cdot i^{(l+1)\cdot w/2-1} \cdot \exp\Big(\pi i\,(l+1)\,w\,r\,y/12\Big).$$

Aus Lemma 5.20 kennen wir das Verhalten der Funktion $a(\tau)$ unter der Transformation $W_l$. Setzen wir beide Ergebnisse zusammen, so erhalten wir das Resultat des Lemmas. Dabei heben sich die Einheitswurzeln aus Zähler und Nenner genau weg, denn $r$ ist ein Quadrat modulo $l$ und $s$ ein Teiler von $r-1$, so daß das Argument der Exponentialfunktion ein Vielfaches von $2\pi i$ ist. □

**Lemma 5.22** *Für alle Transformationen $H_k$ mit $0 \leq k < r$ aus Definition 5.11 gilt*

$$\frac{a(H_k(W_l(\tau)))}{a(W_l(\tau))} \quad = \quad \frac{a(H_k(\tau))}{a(\tau)}.$$

**Beweis (Lemma):** Wir zeigen die Behauptung für beliebiges, aber festes $k$ aus der vorgegebenen Menge. Ähnlich zum Beweis zu Lemma 5.20 untersuchen wir zuerst das Verhalten des Zählers. Dazu benutzen wir die Gleichung (Beweis wiederum durch Nachrechnen)

$$\begin{pmatrix} 1 & k \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} lx & y \\ lz & lw \end{pmatrix} \quad = \quad \underbrace{\begin{pmatrix} l(x+kz) & (y-k^2lz)/r \\ rlz & l(w-kz) \end{pmatrix}}_{=W_l''} \cdot \begin{pmatrix} 1 & k \\ 0 & r \end{pmatrix}.$$

Wegen der Bedingungen an die Koeffizienten der Matrix $W_l$ folgt direkt, daß $W_l''$ eine Matrix mit ganzzahligen Einträgen ist (beachte $y \equiv z \equiv 0 \bmod r$). Analog zum Beweis des vorherigen Lemmas 5.21 erhalten wir $a(H_k(W_l(\tau))) = a(W_l''(H_k(\tau)))$ und müssen daher untersuchen, wie sich die Funktion $a(\tau)$ unter der Transformation $W_l''$ verhält, was wiederum mit den Formeln aus Satz 5.3 geschieht. Der interessante Teil dabei ist die Bestimmung der Konstanten $\epsilon_z$; alles andere läuft analog zum vorherigen Beweis ab. Rechnen wir diese Konstante aus, so erhalten wir:

$$\epsilon_z \quad = \quad \left(\frac{z}{l}\right) \cdot i^{(l+1)\cdot w/2-1} \cdot \exp\Big(\pi i(l+1)w\,(y/r)\,/12\Big).$$

Dabei benutzen wir wiederum die spezielle Wahl der Transformation $W_l$, insbesondere die Eigenschaften $y \equiv 0 \bmod r$ und $z \equiv 0 \bmod rs$. Durch Zusammensetzen dieses Ergebnisses mit Lemma 5.20 erhalten wir das Resultat dieses Lemmas. □

Durch Zusammensetzen all dieser Lemmata erhalten wir das Resultat des Satzes auf die folgende Art und Weise:

$$A\Big(W_l(\tau)\Big) \quad = \quad \frac{T_r\Big(a(W_l(\tau))\Big)}{a(W_l(\tau))}$$

$$\begin{aligned}
&= \frac{1}{r}\cdot\sum_{k=0}^{r-1}\frac{a(H_k(W_l(\tau)))}{a(W_l(\tau))} + \frac{a(H_r(W_l(\tau)))}{a(W_l(\tau))} \\
&= \frac{1}{r}\cdot\sum_{k=0}^{r-1}\frac{a(H_k(\tau))}{a(\tau)} + \frac{a(H_r(\tau))}{a(\tau)} \qquad \text{(vgl. Lemma 5.21 und 5.22)} \\
&= A(\tau).
\end{aligned}$$

■

Damit haben wir eine Methode gefunden, wie wir eine Funktion bestimmen können, die invariant unter allen Transformationen aus $\Gamma_0^*(l)$ ist. Durch Zusammensetzen von Korollar 5.16 und Satz 5.17 erhalten wir dann den folgenden Satz:

**Satz 5.23** *Sei $l$ eine Primzahl größer drei, $s \in \mathbb{N}$ minimal, so daß $s \cdot (l+1) \equiv 0 \bmod 24$ und $r$ eine ungerade Primzahl, die folgende Bedingungen erfüllt:*

- *$s$ teilt $r-1$,*
- *$r$ ist ein Quadrat modulo $l$,*
- *$l$ ist ein Quadrat modulo $r$.*

*Dann ist die Funktion*

$$A(\tau) = \frac{T_r\Big(\eta(\tau)\cdot\eta(l\tau)\Big)}{\eta(\tau)\cdot\eta(l\tau)}$$

*invariant unter allen Transformationen aus $\Gamma_0^*(l)$. Die Invarianzgruppe dieser Funktion ist $\Gamma_0(l)$.*

Um diesen Satz benutzen zu können, müssen wir eine Formel angeben, wie wir bei gegebener Fourierreihenentwicklung der angegebenen Funktion $a(\tau)$ die Fourierreihenentwicklung der Funktion $T_r(a(\tau))$ für eine Zahl $r$ bestimmen können. Dann können wir die Funktion $A(\tau)$ (genauer: die Fourierreihenentwicklung dieser Funktion mit gewisser Genauigkeit) leicht bestimmen, denn mit Satz 5.2 ist es möglich, die Fourierreihenentwicklung der Funktion $\eta(\tau)\cdot\eta(l\tau)$ auszurechnen. Eine solche Formel geben wir in folgendem Satz an.

**Satz 5.24** *Sei eine Funktion $a(\tau)$ durch die folgende Fourierreihenentwicklung gegeben (mit o.E. $\mathrm{ggT}(z,s)=1$)*

$$a(\tau) = \exp\left(2\pi i\tau\frac{z}{s}\right)\cdot\sum_{j=0}^{\infty}a_j\exp\Big(2\pi i\tau\Big)^j.$$

*Dann können wir für eine Primzahl $r$, die die Voraussetzungen aus Satz 5.23 erfüllt, die Fourierreihenentwicklung der Funktion $T_r(a(\tau))$ mit Hilfe der Formel (5.12) bestimmen.*

**Beweis:** Zum Beweis des Satzes betrachten wir

$$T_r\Big(a(s\tau)\Big) \quad = \quad \frac{1}{r}\cdot\sum_{k=0}^{r-1} a\left(\frac{s\tau+ks}{r}\right) \; + \; a\Big(rs\tau\Big).$$

Können wir die Entwicklung von $T_r(a(s\tau))$ als Fourierreihe in $q_\tau$ bestimmen, so erhalten wir daraus die Fourierreihenentwicklung für $T_r(a(\tau))$, indem wir $s\tau$ durch $\tau$ ersetzen. Wird $a(\tau)$ durch die Fourierreihenentwicklung aus dem Satz gegeben, so gilt offensichtlich

$$a(s\tau) \quad = \quad \sum_{j=0}^{\infty} a_j \, \exp\Big(2\pi i\tau\,(js+z)\Big).$$

Die Fourierreihenentwicklung von $a(rs\tau)$ ist hieraus direkt ersichtlich; wenden wir uns daher den „ersten $r$“ Summanden in der Definition des Hecke-Operators zu. Durch Ausrechnen erhalten wir dafür

$$\begin{aligned}
\frac{1}{r}\cdot\sum_{k=0}^{r-1} a\left(\frac{s\tau+ks}{r}\right) \quad &= \quad \frac{1}{r}\cdot\sum_{k=0}^{r-1}\Bigg[\exp\left(2\pi i\frac{(s\tau+ks)z}{rs}\right) \\
&\qquad\qquad \cdot\sum_{j=0}^{\infty} a_j\,\exp\left(2\pi i\,\frac{j(s\tau+ks)}{r}\right)\Bigg] \\
&= \quad \frac{1}{r}\cdot\sum_{j=0}^{\infty} a_j \sum_{k=0}^{r-1}\exp\left(2\pi i\,\frac{s\tau+ks}{rs}\,(js+z)\right) \\
&= \quad \frac{1}{r}\cdot\sum_{j=0}^{\infty}\left[a_j\,\exp\left(2\pi i\tau\,\frac{(js+z)}{r}\right)\cdot\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{k(js+z)}{r}\right)\right] \\
&= \quad \frac{l}{r}\cdot\sum_{\substack{j=0\\ js+z\equiv 0 \bmod r}}^{\infty} a_j\,\exp\left(2\pi i\tau\frac{(js+z)}{r}\right).
\end{aligned}$$

Dabei können wir die letzte Umformung ähnlich zur Herleitung der Funktion $c_{r,1}(\tau)$ auf Seite 63 begründen. Die Exponentialfunktion $\exp(2\pi ik(js+z)/r)$ ist genau für Zahlen $j$ mit $js+z\equiv 0 \bmod r$ eins; ansonsten können wir die Summe dieser $r$-ten Einheitswurzeln ausrechnen und erhalten dafür den Wert null. Damit ergibt sich insgesamt

$$T_r\Big(a(s\tau)\Big) \;=\; \sum_{\substack{j=0\\ js+z\equiv 0 \bmod r}}^{\infty} \frac{l\cdot a_j}{r}\,\exp\left(2\pi i\tau\frac{(js+z)}{r}\right) \;+\; \sum_{j=0}^{\infty} a_j\,\exp\Big(2\pi i\tau(js+z)r\Big).$$

In dieser Gleichung wollen wir $s\tau$ durch $\tau$ ersetzen. Dazu beachten wir, daß $(js+z)/r \equiv (js+z)r \equiv z \bmod s$ gilt (beachte die Bedingung an $r$ aus Satz 5.23).

Damit erhalten wir die Fourierreihenentwicklung von $T_r(a(\tau))$ als

$$T_r\Big(a(\tau)\Big) = \exp\left(2\pi i\tau\frac{z}{s}\right)\cdot\left[\sum_{\substack{j=0\\ js+z\equiv 0 \bmod r}}^{\infty}\frac{l\cdot a_j}{r}\exp\left(2\pi i\tau\frac{(js+z)/r-z}{s}\right)+\sum_{j=0}^{\infty}a_j\exp\left(2\pi i\tau\Big(jr+\frac{(r-1)z}{s}\Big)\right)\right]. \qquad (5.12)$$

■

Damit haben wir alle Voraussetzungen geschaffen, um für Primzahlen $l > 3$, für die die Voraussetzungen aus Satz 5.23 erfüllbar sind, Funktionen zu berechnen, die invariant unter allen Transformationen aus $\Gamma_0^*(l)$ sind und die Invarianzgruppe $\Gamma_0(l)$ besitzen. Wir bestimmen eine geeignete Primzahl $r$, wenden die gerade angegebene Formel an und bestimmen so die Fourierreihenentwicklung für $A(\tau)$. Die Fourierreihenentwicklung dieser Funktion ist eventuell noch nicht über den ganzen Zahlen definiert, doch folgt aus Satz 5.24, daß nach Multiplikation mit dem Skalar $r$ die Fourierentwicklung der Funktion $A(\tau)$ sicher ganze Koeffizienten besitzt.

Weiterhin sollte man beachten, daß wir solche Funktionen $A(\tau)$ auch noch anders bestimmen können. Gibt es zwei verschiedene geeignete Zahlen $r_1$ und $r_2$, so daß die Fourierreihenentwicklungen für $T_{r_1}(a(\tau))$ und $T_{r_2}(a(\tau))$ mit derselben Potenz von $q_\tau$ beginnen, so können wir $A(\tau)$ auch als

$$A(\tau) = \frac{T_{r_1}(a(\tau)) - T_{r_2}(a(\tau))}{a(\tau)}$$

wählen. Man kann aus den angegebenen Beweisen dann leicht erkennen, daß diese Funktion ebenfalls invariant unter Transformationen aus $\Gamma_0^*(l)$ ist.

Im folgenden Abschnitt werden wir uns nun damit beschäftigen, für eine solche Funktion das zugehörige äquivalente Polynom zu bestimmen.

## 5.4 Berechnung eines äquivalenten Polynoms zu $A(\tau)$

In diesem Abschnitt beschreiben wir, wie wir bei Kenntnis einer unter Transformationen aus $\Gamma_0^*(l)$ invarianten Funktion $A(\tau)$ wie im letzten Abschnitt beschrieben ein zum modularen Polynom äquivalentes Polynom $G_l(X) = G_l(X, j(\tau))$ bestimmen können. Dabei nehmen wir an, daß $A(\tau)$ die folgende Fourierentwicklung

$$A(\tau) = \sum_{n=-v}^{\infty} b_n \cdot q_\tau^n$$

mit ganzen Koeffizienten $b_n \in \mathbb{Z}$ besitzt (dabei ist nicht notwendig $b_{-v} = 1$). Wir wollen nun Polynomkoeffizienten $a_{r,k}$ bestimmen, so daß gilt

$$G_l\Big(A(\tau), j(\tau)\Big) = \sum_{r=0}^{l+1}\sum_{k=0}^{\kappa} a_{r,k}\cdot j(\tau)^k\cdot A(\tau)^r = 0. \qquad (5.13)$$

Den Wert von $\kappa$ werden wir im folgenden Lemma 5.25 bestimmen. Aus den im folgenden Abschnitt 5.5 hergeleiteten Ideen und dem dort angegebenen Algorithmus 5.28 folgt direkt, daß die Polynomkoeffizienten $a_{r,k}$ ganze Zahlen sind, wenn die Fourierreihenentwicklung von $A(\tau)$ nur ganze Koeffizienten besitzt. Auf die Gleichung (5.13) wenden wir nun die Transformation $(0,-1;l,0)$ an. Wegen der Invarianz der Funktion $A(\tau)$ unter dieser Transformation und wegen der Gleichung $j(-1/(l\tau)) = j(l\tau)$ erhalten wir dann

$$\sum_{r=0}^{l+1}\sum_{k=0}^{\kappa} a_{r,k}\cdot j(l\tau)^k\cdot A(\tau)^r \quad = \quad 0. \tag{5.14}$$

Diese beiden Gleichungen werden wir im folgenden verwenden, um die Koeffizienten $a_{r,k}$ zu bestimmen. Zuerst geben wir allerdings in dem folgenden Lemma den Wert von $\kappa$ an.

**Lemma 5.25** *In (5.13) und (5.14) ist $\kappa = 2v$.*

**Beweis:** Wir simulieren den Beweis zu Lemma 5.7. Wir wenden auf Gleichung (5.14) die Transformationen $V_n$ für $0 \le n \le l$ wie in (5.5) auf Seite 62 an. Dort haben wir gesehen, daß die Funktion $j(l\tau)$ invariant unter allen diesen Transformationen ist. Betrachten wir, wie die Funktion $A(\tau)$ transformiert wird, so erhalten wir für $0 \le n < l$

$$A\Big(V_n(\tau)\Big) \quad = \quad A\left(\frac{l\,\tau+n}{l}\right) \quad = \quad A\left(\tau+\frac{n}{l}\right)$$

und für $n = l$

$$A\Big(V_l(\tau)\Big) \quad = \quad A\left(\frac{-1}{l^2\tau}\right) \quad = \quad A\Big(l\tau\Big).$$

Damit kennen wir alle Nullstellen des Polynoms

$$h(X) \quad = \quad \sum_{r=0}^{l+1}\left(\sum_{k=0}^{\kappa} a_{r,k}\cdot j(l\tau)^k\right)\cdot X^r;$$

es sind dies gerade die Funktionen $A(V_n(\tau))$ für $0 \le n \le l$. Die $q_\tau$-Entwicklungen der Koeffizienten von $h(X)$ erhalten wir mit Hilfe des Satzes von Newton, angewandt auf die Fourierreihenentwicklungen der Nullstellen. Daher untersuchen wir den minimalen Exponenten von $q_\tau$ in diesen Fourierreihenentwicklungen und erhalten dann

- $-v$ für $0 \le n < l$,
- $-lv$ für $n = l$.

Untersuchen wir mit dieser Beobachtung die Fourierentwicklungen der elementarsymmetrischen Funktionen der Nullstellen, so erkennen wir leicht, daß die Fourierentwicklung des Koeffizienten von $X^0$ in $h(X)$ mit minimalem $q_\tau$-Exponenten (unter allen Koeffizienten) beginnt. Diesen „Startexponenten“ können wir leicht ausrechnen als

$$-lv - \sum_{n=0}^{l-1} v \quad = \quad -2\,lv.$$

Damit folgt aus der Definition von $h(X)$, daß $\kappa = 2v$ gewählt werden kann. ∎

Wir geben nun einen Algorithmus zur Bestimmung des äquivalenten Polynoms $G_l(X,Y)$ für eine solche Funktion $A(\tau)$ an. Prinzipiell können wir dabei vorgehen wie bei der Berechnung des Polynoms zugehörig zur Funktion $g(\tau)$ aus (5.2). Dies hat aber den Nachteil, daß die Fourierreihenentwicklung für $A(l\tau)^k$ mit minimalem Exponent $-klv$ beginnt. Damit ist die maximale Genauigkeit, die wir verwenden müssen, um alle Polynomkoeffizienten genau berechnen zu können, mindestens $l^2v$. Dies führt in der Praxis zu enormen Laufzeiten, die überwiegend bei der Bestimmung der Potenzsummen der Nullstellen des Polynoms $G_l(X, j(l\tau))$ entstehen. Um diese Laufzeiten zu reduzieren, wenden wir den folgenden Trick an, der dazu führt, daß mit kleinerer Genauigkeit gerechnet werden kann.

Wir schreiben das Polynom $G_l(X)$ in der folgenden Art und Weise:

$$G_l(X) = \underbrace{\prod_{n=0}^{l-1}\left(X - A\left(\tau + \frac{n}{l}\right)\right)}_{=:H(X)} \cdot \Big(X - A(l\tau)\Big).$$

Dann können wir die Koeffizienten des Polynoms $H(X)$ als Fourierreihenentwicklungen in $q_\tau$ mit Hilfe des Satzes von Newton ausrechnen. Daraus können wir durch eine Multiplikation die Fourierreihenentwicklungen der Koeffizienten des Polynoms $G_l(X)$ bestimmen. Der Vorteil dieses Verfahrens ist es, daß wir – wie auf Seite 64 beschrieben – die Potenzsummen der Nullstellen von $H(X)$ bestimmen können, wenn wir die Fourierreihenentwicklung für $A(\tau)^k$ kennen. Der dabei auftretende minimale $q_\tau$-Exponent ist $-lv$. Zur Bestimmung der Polynomkoeffizienten $a_{r,k}$ wie in (5.13) reicht es aus, die Fourierreihenentwicklungen der Koeffizienten von $G_l(X)$ bis zum Koeffizienten von $q_\tau^0$ exakt zu kennen. Da der minimale Koeffizient von $A(l\tau)$ genau $-lv$ ist, folgt direkt, daß wir die Fourierreihenentwicklung der Potenzen von $A(\tau)$ nur mit Genauigkeit $2lv$ kennen müssen. Diese Genauigkeit ist deutlich geringer als die Genauigkeit, die wir bei dem Analogon zu dem in Abschnitt 5.2 vorgestellten Algorithmus benötigen würden. Ein weiterer Vorteil dieses Verfahrens ist es, daß die benutzten Fourierreihenentwicklungen überwiegend dünn besetzt sind. Insbesondere sind auch die Koeffizienten von $H(X)$ dünn besetzte Fourierreihenentwicklungen. Damit kann die Multiplikation von $H(X)$ mit dem Polynom $X - A(l\tau)$ durch Multiplikationen dünner Reihenentwicklungen geschehen. Anschließend berechnen wir aus den Koeffizienten von $G_l(X)$, dargestellt als Fourierreihenentwicklungen, durch einen Koeffizientenvergleich mit Potenzen von $j(l\tau)$ die gesuchten Polynomkoeffizienten $a_{r,k}$. Damit ergibt sich der folgende Algorithmus:

**Algorithmus 5.26** [Bestimmung von $G_l(X,Y)$ für $A(\tau)$]

**Eingabe:** Fourierreihenentwicklungen für $A(\tau), j(l\tau)$ mit Genauigkeit $2\,lv$.
**Ausgabe:** Koeffizienten $a_{r,k}$ aus (5.13).

| | |
|---|---|
| Setze $a_{r,k} \leftarrow 0$ für $0 \le k \le l+1,\ 0 \le k \le 2v$ und $a_{l+1,0} \leftarrow 1$. | (1) |
| Setze $s'_0(\tau) \leftarrow 1$ und $h(\tau) \leftarrow 1$. | (2) |
| FOR $r = 1, \ldots, l$ | (3) |
|     Berechne $h(\tau) \leftarrow h(\tau) \cdot A(\tau)$. /* $h(\tau) = A(\tau)^r$ */ | (4) |
|     Berechne $c_r(\tau)$ mit (5.9) aus $h(\tau)$. /* $r$-te Potenzsumme der Nullst. von $H(X)$ */ | (5) |
|     Berechne $s'_r(\tau)$ mit Formel (5.8). /* Koeff. von $X^{l-r}$ in $H(X)$*/ | (6) |
|     Setze $s_r(\tau) \leftarrow s'_r(\tau) - s'_{r-1}(\tau) \cdot A(l\tau)$. /* Koeffizient von $X^{l+1-r}$ in $G_l(X)$ */ | (7) |
|     Bestimme $a_{l+1-r,k}$ für $0 \le k \le 2v$ aus $s_r(\tau)$ durch Koeffizientenvergleich mit Potenzen von $j(l\tau)$. | (8) |
| Setze $s_{l+1}(\tau) \leftarrow\ - s'_l(\tau) \cdot A(l\tau)$. | (9) |
| Bestimme $a_{0,k}$ für $0 \le k \le 2v$ aus $s_{l+1}(\tau)$ durch Koeffizientenvergleich mit Potenzen von $j(l\tau)$. | (10) |

## 5.5 Bestimmung äquivalenter Polynome modulo $p$

Wir haben in den Abschnitten 5.2 und 5.4 beschrieben, wie wir sowohl für die unter Transformationen aus $\Gamma_0(l)$ invariante Funktion $g(\tau)$ (vgl. (5.2)) als auch für die unter Transformationen aus $\Gamma_0^*(l)$ invariante Funktion $A(\tau)$ (vgl. Satz 5.12) ein zugehöriges äquivalentes Polynom $G_l(X,Y)$ aus $\mathbb{Z}[X,Y]$ bestimmen können. In beiden Algorithmen 5.8 und 5.26 wird das äquivalente Polynom über den ganzen Zahlen bestimmt. Wie wir in Kapitel 4 gezeigt haben, benötigen wir die Koeffizienten der äquivalenten Polynome jedoch nur modulo der Charakteristik $p$. In diesem Abschnitt beschreiben wir auf den vorherigen Abschnitten aufbauende Verfahren zur Lösung dieser Aufgabe; im folgenden Abschnitt werden wir unsere praktische Implementierung beschreiben und einige Laufzeiten angeben.

Offensichtlich müssen wir zur Bestimmung von $G_l(X,Y) \bmod p$ die Fourierreihenentwicklungen aller benutzten Funktionen ebenfalls nur modulo $p$ kennen. Leicht erkennen wir, daß wir die Basisoperationen von Fourierreihenentwicklungen mit ganzen Koeffizienten direkt modulo $p$ übertragen können, wenn wir sicherstellen, daß bei der Division der „minimale“ Koeffizient des Divisors invertierbar modulo $p$ ist.

Betrachten wir alle Divisionen, die zur Berechnung der Funktionen $f(\tau)$ bzw. $A(\tau)$ notwendig sind, so ist leicht ersichtlich, daß alle Divisoren den minimalen Koeffizienten Eins besitzen und damit die Voraussetzungen erfüllen. Damit können wir alle verwendeten Fourierreihenentwicklungen in den Algorithmen 5.8 bzw. 5.26 direkt modulo $p$ berechnen.

Untersuchen wir, wo es noch Probleme bei der Reduktion aller Schritte der Algorithmen 5.8 bzw. 5.26 modulo $p$ geben könnte, so erkennen wir leicht, daß der Satz von Newton zu einer Schwierigkeit führt. Wie aus Formel (5.8) ersichtlich, muß dabei durch $r$ geteilt werden, wobei $r$ aus der Menge $\{1, \ldots, l+1\}$ gewählt wird. Dies ist natürlich für $p \leq l$ nicht immer möglich. Für Moduln $p > l$ kann es hingegen keine Schwierigkeiten geben; wir können zur Berechnung von $G_l(X,Y) \bmod p$ alle Schritte in den Algorithmen 5.8 bzw. 5.26 modulo $p$ durchführen.

Daher betrachten wir im folgenden die Situation $p < l$. Wir geben im folgenden zwei Algorithmen an, mit denen wir für die Funktion $g(\tau)$ aus (5.2) bzw. für die Funktion $A(\tau)$ aus Abschnitt 5.3 das zugehörige äquivalente Polynom $G_l(X,Y) \bmod p$ berechnen können, falls $p < l$ ist. Wir können nach obigen Bemerkungen davon ausgehen, daß wir in beiden Fällen Fourierreihenentwicklungen modulo $p$ mit einer gewissen Genauigkeit für alle verwendeten Funktionen kennen. Bei beiden Algorithmen werden wir durch einen geschickten simultanen Koeffizientenvergleich die Polynomkoeffizienten bestimmen.

Betrachten wir zuerst die Situation für die Funktion $g(\tau)$ aus (5.2). Da das Polynom $G_l(X,Y)$ normiert sein soll, gilt als erstes $a_{l+1,k} = 0$ für $1 \leq k \leq v$ und $a_{l+1,0} = 1$. Wir wollen die Koeffizienten $a_{r,k}$ des Polynoms $G_l(X,Y)$ durch einen Koeffizientenvergleich bestimmen. Dazu subtrahieren wir in (5.4) alle Reihenentwicklungen, die mit schon bekannten Koeffizienten $a_{r,k}$ multipliziert werden. Dann versuchen wir damit, einen weiteren (bisher unbekannten) Polynomkoeffizienten zu bestimmen, indem wir Startexponenten und Startkoeffizienten auf beiden Seiten vergleichen. Um zu zeigen, daß wir so alle Polynomkoeffizienten eindeutig bestimmen können, untersuchen wir in (5.4), wie groß der Startexponent der Fourierreihenentwicklung für $j(l\tau)^k \cdot f(\tau)^r$ ist, die mit dem Koeffizienten $a_{r,k}$ multipliziert wird. Dabei erhalten wir $-rv-kl$. Untersuchen wir nun, wann für zwei Paare $(r_1,k_1)$ und $(r_2,k_2)$ die Fourierreihenentwicklungen $j(l\tau)^{k_j} \cdot f(\tau)^{r_j}$ für $j = 1,2$ mit demselbem $q_\tau$-Exponenten anfangen. Dazu betrachten wir den Exponenten modulo $l$ und erhalten so als notwendige Bedingung

$$r_1 \equiv r_2 \bmod l.$$

Durch Testen der wenigen verbleibenden Möglichkeiten erhalten wir folgende beiden Konfliktpaare

$$\Big\{(l+1,0),(1,v)\Big\} \qquad \text{und} \qquad \Big\{(l,0),(0,v)\Big\}.$$

Da wir den Koeffizienten $a_{l+1,0} = 1$ kennen, ergibt sich hieraus direkt $a_{1,v} = -1$ (beachte dazu, daß die Fourierreihenentwicklungen $j(l\tau)^k \cdot f(\tau)^r$ den minimalen Koeffizienten eins haben). Zur Bestimmung der Polynomkoeffizienten $a_{l,0}$ bzw. $a_{0,v}$ untersuchen wir analog den Startexponenten von $j(\tau)^k \cdot g(\tau)^r$ in (5.3). Dabei erhalten wir $rv-k$. Damit tritt der Startexponent $-v$ der Fourierreihe, die in (5.3) mit

$a_{0,v}$ multipliziert wird, nur einmal als Startexponent einer Fourierreihe $j(\tau)^k \cdot g(\tau)^r$ auf und ist außerdem minimal. Also ist $a_{0,v} = 0$ und damit können wir auch $a_{l,0}$ exakt bestimmen. Mit dieser kleinen Beobachtung folgt direkt, daß wir mit Hilfe eines Koeffizientenvergleichs in (5.4) alle Polynomkoffizienten eindeutig bestimmen können.

Zur Bestimmung der benötigten Präzision für die verwendeten Fourierreihenentwicklungen beachten wir wieder, daß wir in allen Reihenentwicklungen alle Koeffizienten von nicht-positiven $q_\tau$-Potenzen exakt kennen müssen. Daraus folgt direkt, daß wir auch in diesem Algorithmus mit Präzision $lv$ rechnen können, ohne daß dabei ein Fehler durch zu kleine Präzision auftritt.

Damit erhalten wir den folgenden Algorithmus zur Bestimmung des äquivalenten Polynoms $G_l(X,Y)$ modulo einer Primzahl $p < l$, in dem wir die beiden Hilfsfunktionen $min_{exp}$ und $min_{coeff}$ benutzen. Diese beiden Funktionen liefern den minimalen $q_\tau$-Exponenten bzw. den zugehörigen Koeffizienten einer Fourierreihenentwicklung:

**Algorithmus 5.27** [Bestimmung von $G_l(X,Y)$ modulo $p < l$ für $g(\tau)$ aus (5.2)]

**Eingabe:** Fourierreihenentwicklungen für $f(\tau)$ und $j(l\tau)$ modulo $p$ mit Genauigkeit $lv$.

**Ausgabe:** Koeffizienten $a_{r,k}$ mod $p$ des zugehörigen Polynoms $G_l(X,Y)$ für $0 \leq r \leq l+1,\ 0 \leq k \leq v$.

| | | | |
|---|---|---|---|
| Setze $a_{r,k} \leftarrow 0$ für $0 \leq r \leq l+1,\ 0 \leq k \leq v$. | | | (1) |
| Setze $a_{l+1,0} \leftarrow 1,\ a_{1,v} \leftarrow -1$ und $h(\tau) \leftarrow j(l\tau)^v \cdot f(\tau) - f(\tau)^{l+1}$. | | | (2) |
| WHILE $min_{exp}(h(\tau)) \leq 0$ | | | (3) |
| | IF $min_{exp}(h(\tau)) = l\,v$ | | (4) |
| | THEN | Setze $a_{l,0} \leftarrow min_{coeff}(h(\tau))$. | (5) |
| | | Setze $h(\tau) \leftarrow h(\tau) - a_{l,0} \cdot f(\tau)^l$. | (6) |
| | ELSE | Berechne Zahlen $0 \leq r \leq l, 0 \leq k \leq v$ mit $-(r\,v + k\,l) = min_{exp}(h(\tau))$. | (7) |
| | | Setze $a_{r,k} \leftarrow min_{coeff}(h(\tau))$. | (8) |
| | | Setze $h(\tau) \leftarrow h(\tau) - a_{r,k} \cdot j(l\tau)^k \cdot f(\tau)^r$. | (9) |

Man sollte beachten, daß $v$ immer kleiner als $\frac{l}{2}$ und damit invertierbar modulo $l$ ist und daß man in Schritt (7) damit ein Paar $(r,k)$ leicht durch Division mit Rest von $min_{exp}(h(\tau))$ und $l$ bestimmen kann.

Wenden wir uns nun der Berechnung des äquivalenten Polynoms $G_l(X,Y)$ modulo einer Primzahl $p < l$ für eine Funktion $A(\tau)$ wie in Abschnitt 5.3 zu. Wiederum wollen wir die Polynomkoeffizienten durch einen simultanen Koeffizientenvergleich bestimmen. In diesem Fall müssen wir dazu die beiden schon in Abschnitt 5.4 angegebenen Formeln

$$\sum_{r=0}^{l+1}\sum_{k=0}^{2v} a_{r,k}\cdot j(\tau)^k\cdot A(\tau)^r \quad = \quad 0 \tag{5.15}$$

und

$$\sum_{r=0}^{l+1}\sum_{k=0}^{2v} a_{r,k}\cdot j(l\tau)^k\cdot A(\tau)^r \quad = \quad 0 \tag{5.16}$$

verwenden. Wegen der Normierung gilt zuerst wiederum $a_{l+1,0}=1$ und $a_{l+1,k}=0$ für $1\le k\le 2v$. Untersuchen wir für beide Gleichungen (5.15) und (5.16), wie der minimale $q_\tau$-Exponent der Fourierreihenentwicklung ist, die mit dem Koeffizienten $a_{r,k}$ multipliziert wird, so erhalten wir

- in (5.15) $-rv-k$,
- in (5.16) $-rv-kl$.

Wir suchen nun für diese beiden Gleichungen den minimalen Exponenten, für den es zwei verschiedene Paare $(r,k)$ und $(r',k')$ gibt, so daß $a_{r,k}$ bzw. $a_{r',k'}$ mit Fourierreihenentwicklungen mit diesem Startexponenten multipliziert werden. Sicherlich müssen Polynomkoeffizienten $a_{r,k}$, die mit einer Fourierreihe multipliziert werden, die einen Anfangsexponenten kleiner als den so bestimmten Exponenten haben, gleich Null sein. Aus (5.15) erhalten wir so notwendigerweise $a_{l,k}=0$ für $v<k\le 2v$ und

$$min_{coeff}\left(A(\tau)^{l+1}\right)+a_{l,v}\cdot min_{coeff}\left(A(\tau)^{l}\right)+a_{l-1,2v}\cdot min_{coeff}\left(A(\tau)^{l-1}\right) \;=\; 0.$$

Dabei beachte man, daß der Startkoeffizient der Fourierreihenentwicklung für $j(\tau)$ eins ist. Weiterhin können in (5.16) nur dann zwei verschiedene Paare $(r,k)$ und $(r',k')$ existieren, die mit einer Fourierreihenentwicklung mit derselben Anfangspotenz multipliziert werden, wenn $r\equiv r' \bmod l$ gilt. Damit bleiben als mögliche solche Werte für $r$ nur noch $r=l+1$ und $r=l$. Aus $a_{l+1,k}=0$ für $1\le k\le 2v$ und $a_{l,k}=0$ für $v<k\le 2v$ erhalten wir dann den minimalen Startexponenten in (5.16), den zwei verschiedene Fourierreihenentwicklungen besitzen, als $-2vl$ (kritisches Paar $(l,v)$ und $(0,2v)$). Da der Startexponent der Fourierreihenentwicklung zu $a_{l-1,2v}$ in (5.16) kleiner als dieser kritische Exponent ist, folgt $a_{l-1,2v}=0$ und damit aus obiger Gleichung

$$a_{l,v} \quad = \quad \frac{-min_{coeff}\left(A(\tau)^{l+1}\right)}{min_{coeff}\left(A(\tau)^{l}\right)} \quad = \quad -min_{coeff}\left(A(\tau)\right).$$

Betrachten wir damit wieder die Gleichung (5.16), so erhalten wir

$$a_{l,v}\cdot min_{coeff}\left(A(\tau)^{l}\right)+a_{0,2v}=0 \qquad \text{und so} \qquad a_{0,2v}=min_{coeff}\left(A(\tau)^{l+1}\right).$$

Wir haben schon gesehen, daß es nur für $r\in\{0,l\}$ zwei verschiedene Paare geben kann, so daß $a_{r,k}$ in (5.16) nicht eindeutig bestimmt wird. Ansonsten können wir $a_{r,k}$

immer eindeutig bestimmen, wenn wir uns die bisher schon berechneten Fourierreihen, multipliziert mit den entsprechenden $a_{r,k}$, in einer Hilfsvariable (in dem unteren Algorithmus $h_2(\tau)$) merken. Parallel merken wir uns in einer Hilfsvariable $h_1(\tau)$, wie die analog berechneten Teilergebnisse in (5.15) sind. Für die Konfliktpaare $a_{l,k}$ und $a_{0,k+v}$ für $0 \leq k < v$ benutzen wir dann diese Hilfsfunktion $h_1(\tau)$. Damit erhalten wir $a_{l,k}$, denn dieser Koeffizient wird in (5.15) mit einer Fourierreihenentwicklung mit im Vergleich zu $a_{0,k+v}$ kleineren Exponenten multipliziert. Dabei treten keine Zweideutigkeiten auf, denn man sollte beachten, daß wir die Koeffizienten $a_{l-1,k+v}$ schon vorher berechnet haben, wie man bei Untersuchung der entsprechenden Grade erkennen kann.

Zur Bestimmung der benötigten Präzision gelten dieselben Bemerkungen wie in Algorithmus 5.27. Damit erhalten wir in diesem Fall die untere Schranke $2lv$ für die Präzision. Somit ergibt sich der folgende Algorithmus:

**Algorithmus 5.28** [Bestimmung $G_l(X,Y)$ modulo $p < l$ für $A(\tau)$]

**Eingabe:** Fourierreihenentwicklungen für $A(\tau), j(\tau), j(l\tau) \bmod p$ mit Genauigkeit $2lv$.

**Ausgabe:** Koeffizienten $a_{r,k} \bmod p$ für zugehöriges Polynom $G_l(X,Y)$ für $0 \leq r \leq l+1$, $0 \leq k \leq 2v$.

| | | | |
|---|---|---|---|
| Setze $a_{r,k} \leftarrow 0$ für alle $0 \leq r \leq l+1,\ 0 \leq k \leq 2v$. | | | (1) |
| Setze $a_{l+1,0} \leftarrow 1,\ a_{l,v} \leftarrow -\, min_{coeff}(A(\tau))$ und $a_{0,2v} \leftarrow min_{coeff}(A(\tau)^{l+1})$. | | | (2) |
| Setze $h_1(\tau) \leftarrow -\, a_{l,v}\, j(\tau)^v \cdot A(\tau)^l - a_{0,2v}\, j(\tau)^{2v} - A(\tau)^{l+1}$. | | | (3) |
| Setze $h_2(\tau) \leftarrow -\, a_{l,v}\, j(l\tau)^v \cdot A(\tau)^l - a_{0,2v}\, j(l\tau)^{2v} - A(\tau)^{l+1}$. | | | (4) |
| WHILE $min_{exp}(h_2(\tau)) \leq 0$ | | | (5) |
| | Bestimme $(r,k) \in \{0,\ldots,l\} \times \{0,\ldots,2v\}$ mit $-rv - kl = min_{exp}(h_2(\tau))$. | | (6) |
| | IF $r = 0$ oder $r = l$ | | (7) |
| | THEN | Setze $s \leftarrow k \bmod v$. | (8) |
| | | Setze $a_{l,s} \leftarrow min_{coeff}(h_1(\tau))/min_{coeff}(A(\tau))^l$. | (9) |
| | | Setze $a_{0,s+v} \leftarrow min_{coeff}(h_2(\tau)) - a_{l,s}$. | (10) |
| | | Setze $h_1(\tau) \leftarrow h_1(\tau) - a_{l,s} \cdot j(\tau)^s \cdot A(\tau)^l - a_{0,s+v} \cdot j(\tau)^{s+v}$. | (11) |
| | | Setze $h_2(\tau) \leftarrow h_2(\tau) - a_{l,s} \cdot j(l\tau)^s \cdot A(\tau)^l - a_{0,s+v} \cdot j(l\tau)^{s+v}$. | (12) |
| | ELSE | Setze $a_{r,k} \leftarrow min_{coeff}(h_2(\tau))/min_{coeff}(A(\tau)^r)$. | (13) |
| | | Setze $h_1(\tau) \leftarrow h_1(\tau) - a_{r,k} \cdot j(\tau)^k \cdot A(\tau)^r$. | (14) |
| | | Setze $h_2(\tau) \leftarrow h_2(\tau) - a_{r,k} \cdot j(l\tau)^k \cdot A(\tau)^r$. | (15) |

Bei der Implementierung dieses Algorithmus kann man noch einige praktische Verbesserungen einbauen. Es ist aus der Formulierung des Algorithmus offensichtlich, daß wir die Fourierreihe $h_1(\tau)$, mit deren Hilfe wir alle schon berechneten Teilfourierreihen in (5.15) aufsammeln, nicht mehr benötigen, wenn wir alle Koeffizienten $a_{l,k}$ berechnet haben. Daher kann man sich die Berechnung von $h_1(\tau)$ in diesem Fall sparen.

## 5.6 Beschreibung unserer Implementierung

In dem letzten Abschnitt dieses Kapitels werden wir eine Implementierung der beschriebenen Algorithmen vorstellen. Diese Implementierung wird ausführlich in [Le94] erläutert. Alle in diesem Abschnitt angegebenen Laufzeiten wurden auf Rechnern vom Typ SPARC ELC (ca. 20 MiPS) mit 16 MegaByte Hauptspeicher berechnet.

Wir berechnen äquivalente Polynome über den ganzen Zahlen einmal in einer Vorberechnung und speichern sie dann auf Platte. Wir haben so für alle Primzahlen $l \leq 850$ ein äquivalentes Polynom berechnet und gespeichert; der benötigte Speicherplatzbedarf dafür ist ungefähr 140 MegaByte. Führt man die Berechnungen über $\mathbb{Z}$ durch (wie in den Abschnitten 5.2 und 5.4 angegeben), so sind sehr zeitaufwendige Rechnungen mit sehr großen Zahlen notwendig. So besitzt zum Beispiel $G_{829}(X, Y)$ Koeffizienten mit ungefähr 640 Dezimalstellen. Wir wenden daher zur Berechnung der Polynome die folgende Strategie an:

1. bestimme $G_l(X, Y)$ modulo verschiedener Primzahlen $p_i > l$, $i = 1, \ldots, w$,
2. kombiniere die in Schritt 1 erhaltenen Teilergebnisse mit Hilfe des Chinesischen Restsatzes.

Dabei werden die Primzahlen $p_i$ so gewählt, daß sie in einem Computerwort (d.h. 32 Bit) gespeichert werden können und daß es modulo $p_i$ möglich ist, die schnelle Fouriertransformation (FFT) als Multiplikationsmethode für Fourierreihenentwicklungen zu benutzen. Genauer wählen wir die Primzahlen $p_i$ aus technischen Gründen kleiner als $2^{26}$ (dies wird bei der vorhandenen FFT-Implementierung vorausgesetzt). Damit können viele Rechnungen mit in der Praxis sehr viel schnellerer einfacher Präzision durchgeführt werden. Der Vorteil der FFT-Methode gegenüber der „Standardmethode“ zur Multiplikation wird durch die folgende Tabelle 5.1 deutlich.

Die Anzahl $w$ der benötigten Primzahlen $p_i$ wird nicht genau vorgegeben; wir kombinieren nach jeder Teilberechnung das Ergebnis modulo $p_i$ aus Schritt 1 mit dem bisher schon bekannten Gesamtergebnis. Ändert sich das Gesamtergebnis dabei, so bestimmen wir eine neue geeignete 26-Bit Primzahl $p_i$ und fahren fort; ansonsten nehmen wir an, daß wir das gesuchte äquivalente Polynom über $\mathbb{Z}$ berechnet haben. Die „Korrektheit“ dieses Polynoms wird anschließend durch einige Berechnungen von Gruppenordnungen von elliptischen Kurven, für die wir die Ordnung bereits kennen, überprüft. Tritt dabei kein Fehler auf, so sind wir „sicher“, daß das Polynom korrekt ist und speichern es ab. Dieses Verfahren hat in der Praxis bisher

Tabelle 5.1: Vergleich Standardmultiplikationsalgorithmus $\leftrightarrow$ FFT-Methode:
es wird die Zeit für eine Multiplikation einer Fourierreihenentwicklung der angegebenen Präzision modulo einer 26-Bit Primzahl angegeben.

| Präzision | Standard | FFT | FFT / Std. |
|---|---|---|---|
| 1000 | 1.5 sec | 0.3 sec | 20.00 % |
| 2000 | 6.5 sec | 0.7 sec | 10.78 % |
| 4000 | 26.4 sec | 1.5 sec | 5.68 % |
| 8000 | 1 min 45.0 sec | 3.2 sec | 0.03 % |
| 16000 | 7 min 10.0 sec | 6.8 sec | 0.01 % |

noch zu keinem Fehler geführt, beschleunigt den Algorithmus aber wesentlich, denn theoretische Schranken für die Anzahl der benötigten Primzahlen sind sehr schlecht.

Einige Tricks beschleunigen die Berechnungen in den Algorithmen 5.8 bzw. 5.26 noch zusätzlich. Wir geben diese Tricks hier für Algorithmus 5.8 an; für Algorithmus 5.26 verwenden wir analoge Techniken.

1. Es ist sehr sinnvoll, die Eigenschaft der dünnen Besetzung von Reihenentwicklungen auszunutzen. Dazu haben wir zwei verschiedene Computerarithmetiken für Fourierreihenentwicklungen implementiert (dicht besetzt, dünn besetzt) und benutzen jeweils die optimale Version.

2. Zur Bestimmung der Reihen $c_r(\tau)$ im Satz von Newton (vgl. (5.8)) benötigen wir die Potenzen $f(\tau)^r$ für $1 \leq r \leq l+1$. Alle diese Potenzen können sukzessive mit Hilfe jeweils einer Multiplikation berechnet werden. Da allerdings die Quadrierung von Fourierreihenentwicklungen billiger ist als die Multiplikation, berechnen wir alle diese Potenzen mit Hilfe von Quadrierungen. Dabei wird die Berechnungsreihenfolge etwas verändert, so daß wir die Ergebnisse speichern müssen, um sie im Satz von Newton anwenden zu können. Genauer berechnen wir die Potenzen in der folgenden Reihenfolge:

$$\begin{aligned} f(\tau) \;&\rightarrow\; f(\tau)^2 \rightarrow f(\tau)^4 \rightarrow \ldots \rightarrow f(\tau)^{2^x} \\ &\rightarrow\; f(\tau)^3 = \frac{1}{2}\left(\left(f(\tau)^2 + f(\tau)\right)^2 - f(\tau)^4 - f(\tau)^2\right) \rightarrow f(\tau)^6 \rightarrow \ldots \\ &\;\vdots \end{aligned}$$

   Man beachte, daß wir bei der Berechnung von $f(\tau)^3$ die Reihenentwicklungen für $f(\tau)^2$ und $f(\tau)^4$ schon kennen. Dieser Trick führt zu einer deutlichen Laufzeitreduktion, wie Tabelle 5.2 zeigt.

Tabelle 5.2: Tabellenberechnung mit sukzessiver Multiplikation $\leftrightarrow$ Quadrierungen

| $l$ | sukzessiv | Quadr. Trick | Quadr. / sukz. |
|---|---|---|---|
| 53 | 16,7 sec | 11,5 sec | 68,8 % |
| 101 | 146,17 sec | 99,5 sec | 68,1 % |
| 151 | 221,0 sec | 151,6 sec | 68,6 % |
| 211 | 680,3 sec | 462,7 sec | 68,0 % |
| 283 | 1887,7 sec | 1287,9 sec | 68,2 % |

3. Bei der Berechnung der elementarsymmetrischen Funktionen in (5.8) werden viele Multiplikationen von Reihenentwicklungen benötigt. Deshalb bestimmen wir nach Berechnung einer Reihe $s_r(\tau)$ deren Darstellung durch Potenzen von $j(l\tau)^k$ (vgl. (5.6)). Berechnen wir dann $c_m(\tau) \cdot j(l\tau)^k$, so speichern wir diese Reihenentwicklung; sie kann im Laufe des Algorithmus mehrmals verwendet werden. Dieser Trick reduziert die Anzahl der Multiplikationen in (5.8) von $\frac{1}{2}(l^2 + l)$ auf $lv$.

Folgende Tabelle 5.3 zeigt die Aufteilung der Laufzeit auf die zwei wichtigen Phasen in Algorithmus 5.8. Wir geben gleichzeitig die Anzahl der 26-Bit Primzahlen an, die wir zur Berechnung der äquivalenten Polynome über $\mathbb{Z}$ benötigt haben.

Tabelle 5.3: Laufzeitaufteilung in Algorithmus 5.8

| $l$ | $f(\tau)$-Potenzen | Koeff.vergleich | Anzahl 26-Bit Pz. |
|---|---|---|---|
| 53 | 11,5 sec | 1,5 sec | 16 |
| 101 | 99,5 sec | 15,3 sec | 32 |
| 151 | 151,6 sec | 33,3 sec | 35 |
| 211 | 462,7 sec | 115,0 sec | 52 |
| 283 | 1287,9 sec | 356,8 sec | 72 |

Das Problem bei der Berechnung äquivalenter Polynome mit Hilfe der Funktion $f(\tau)$ aus (5.1) ist die schnell wachsende Genauigkeit, die für in der Berechnung benutzte Fourierreihenentwicklungen benötigt wird. Die Genauigkeit beträgt für $l = 307$ schon 15 657; für $l = 503$ schon 126 253 und für $l = 719$ sogar 258 121. Im Vergleich dazu beträgt die Genauigkeit, die wir bei Berechnung des äquivalenten Polynoms für

Tabelle 5.4: Vergleich Algorithmus 5.28 $\leftrightarrow$ Algorithmus 5.26

In Algorithmus 5.28 wird ein simultaner Koeffizientenvergleich benutzt; Algorithmus 5.26 verwendet ein auf dem Satz von Newton basierendes Verfahren. Wir geben jeweils die Laufzeit zur Bestimmung der äquivalenten Polynome modulo einer 26-Bit Primzahl an.

| $l$ | simultaner Koeff.Vergleich | Newton-Methode |
|---|---|---|
| 307 | 53 min | 16 min |
| 401 | 1 h 44 min | 25 min |
| 503 | 3 h 31 min | 58 min |
| 599 | 7 h 50 min | 1 h 26 min |
| 719 | 17 h 00 min | 3 h 49 min |

eine Funktion $A(\tau)$ wie in Abschnitt 5.3 benötigen, für $l = 307$ nur 6 140, für $l = 503$ dann 10 060 und für $l = 719$ nur 21 570. Betrachten wir daher noch Laufzeiten zur Berechnung dieser äquivalenten Polynome. Wir haben in den vorherigen Abschnitten zwei Algorithmen zur Berechnung solcher äquivalenter Polynome beschrieben: Algorithmus 5.26 (basierend auf der „Newton-Methode“) und Algorithmus 5.28 („simultaner Koeffizientenvergleich“). Beide Algorithmen wurden implementiert. In der Tabelle 5.4 werden Laufzeiten beider Algorithmen zur Bestimmung äquivalenter Polynome modulo einer 26-Bit Primzahl angegeben.

Die in Tabelle 5.4 angegebenen Laufzeiten sind Laufzeiten zur Berechnung äquivalenter Polynome modulo einer 26-Bit Primzahl. Zur Berechnung der Polynome über den ganzen Zahlen sind für große Werte von $l$ allerdings „viele“ solche 26-Bit Primzahlen nötig, beispielsweise war für $l = 829$ die Anzahl der benutzten 26-Bit Primzahlen 86. Daraus wird schon deutlich, daß trotz aller Tricks bei der Berechnung äquivalenter Polynome für Primzahlen $l \geq 500$ enorme Laufzeiten entstehen. Daher verteilen wir die Berechnung über ein Netz von Workstations, indem wir äquivalente Polynome modulo verschiedener 26-Bit Primzahlen verteilt auf verschiedenen Rechnern berechnen. Damit war es in ungefähr 28 Stunden Real-Zeit möglich, $G_{829}(X, Y)$ über $\mathbb{Z}$ zu berechnen. Die dabei benötigte Gesamtlaufzeit betrug 827 Stunden bzw. 689 MiPS Tage. Hieraus wird klar, daß die am Anfang dieses Abschnitts vorgestellte Strategie der Speicherung einmal berechneter äquivalenter Polynome sinnvoll ist.

Damit haben wir zwei Möglichkeiten vorgestellt, äquivalente Polynome zu berechnen. Mit Hilfe dieser Polynome können wir wie beschrieben Information über die Gruppenordnung einer elliptischen Kurve über einem endlichen Körper bestimmen. Dabei erhalten wir in der Regel allerdings immer mehrere Werte für die Gruppenordnung modulo einer ungeraden Primzahl $l$. In den folgenden beiden Kapiteln stellen wir einen Algorithmus vor, mit dem es manchmal möglich ist, die Gruppenordnung einer elliptischen Kurve sogar exakt modulo einer ungeraden Primzahl $l$ zu bestimmen.

# Kapitel 6

# Der Algorithmus von Elkies über den komplexen Zahlen

Mit den bisher beschriebenen Ideen können wir für eine elliptische Kurve über einem endlichen Körper der Charakteristik größer drei Information über die Gruppenordnung modulo kleiner ungerader Primzahlen $l$ bestimmen. Dabei erhalten wir im allgemeinen allerdings nicht den exakten Wert der Gruppenordnung modulo $l$. Schoof hat in [Sc85] beschrieben, wie man die Spur exakt modulo $l$ bestimmen kann. Allerdings ist dieser Algorithmus in der Praxis nicht gut anwendbar, denn es wird dabei mit Polynomen von ungefähr quadratischem Grad (in $l$) gerechnet. Elkies zeigt in [El], wie man „manchmal" die Gruppenordnung modulo $l$ auch mit Hilfe von Polynomrechnungen von Polynomen mit Grad $(l-1)/2$ bestimmen kann. In diesem Kapitel werden wir eine Variante dieser Idee von Atkin beschreiben. Dabei werden zuerst alle Formeln für elliptische Kurven über den komplexen Zahlen hergeleitet. Im folgenden Kapitel werden wir diese Formeln benutzen, um dasselbe Problem für elliptische Kurven über endlichen Körpern genügend großer Charakteristik zu lösen.

## 6.1 Gitter und elliptische Kurven

Sei im folgenden $L$ ein zweidimensionales Gitter in $\mathbb{C}$. Bei den Betrachtungen dieses Kapitels werden wir häufig die folgenden beiden Funktionen zu Gittern benutzen.

**Definition 6.1** *Die* **Weierstrass-$\wp$-Funktion** *und die* **Weierstrass-$\zeta$-Funktion** *zu einem Gitter $L$ sind definiert als*

$$\begin{aligned} \wp(z, L) &= \frac{1}{z^2} + \sum_{w \in L - \{0\}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right), \\ \zeta(z, L) &= \sum_{w \in L - \{0\}} \left( \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right). \end{aligned}$$

Wir werden häufig die abkürzende Schreibweise $\wp(z)$ anstelle von $\wp(z, L)$ verwenden, wenn das zugehörige Gitter klar ist.

Wir haben in Kapitel 4 schon gesehen, daß es einen Isomorphismus zwischen $\mathbb{C}/L$ und elliptischen Kurven über den komplexen Zahlen gibt. Sei also $E$ eine elliptische Kurve über $\mathbb{C}$, so daß für das Gitter $L$ die Gruppe $\mathbb{C}/L$ isomorph zu $E(\mathbb{C})$ ist. Dann können wir mit Hilfe der Koeffizienten der elliptischen Kurve $E$ eine Fourierreihenentwicklung für die Funktionen $\wp(z, L)$ und $\zeta(z, L)$ bestimmen (siehe [ChCoRo, Seite 8] und [La87, Seite 240]).

**Lemma 6.2** *Sei $E = (a, b)$ eine elliptische Kurve über $\mathbb{C}$ und $L$ ein Gitter, so daß $E(\mathbb{C}) \cong \mathbb{C}/L$ gilt. Dann besitzen die Weierstrass-$\wp$- und $\zeta$-Funktion zu $L$ die folgenden Fourierentwicklungen*

$$\begin{aligned} \wp(z, L) &= \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k \cdot z^{2k}, \\ \zeta(z, L) &= \frac{1}{z} - \sum_{k=1}^{\infty} c_k \cdot \frac{z^{2k+1}}{2k+1}, \end{aligned}$$

*wobei für die Koeffizienten $c_k$ gilt*

$$c_1 = -\frac{a}{5}, \quad c_2 = -\frac{b}{7}, \quad c_k = \frac{3}{(k-2)(2k+3)} \cdot \sum_{h=1}^{k-2} c_h \cdot c_{k-1-h} \quad \textit{für } k \geq 3.$$

Weiterhin werden wir in den folgenden Abschnitten sogenannte Eisenstein-Reihen benutzen, um einen Algorithmus zur Bestimmung eines Teilers eines Divisionspolynoms herzuleiten. Diese Reihen sind folgendermaßen definiert.

**Definition 6.3** *Sei $\tau \in \mathcal{H}$ gegeben. Dann definieren wir die folgenden* **(normalisierten) Eisenstein-Reihen**

$$\begin{aligned} E_2(\tau) &= 1 - 24 \cdot \sum_{n=1}^{\infty} \sigma_1(n) \cdot q_\tau^n, \\ E_4(\tau) &= 1 + 240 \cdot \sum_{n=1}^{\infty} \sigma_3(n) \cdot q_\tau^n, \\ E_6(\tau) &= 1 - 504 \cdot \sum_{n=1}^{\infty} \sigma_5(n) \cdot q_\tau^n, \end{aligned}$$

*wobei $\sigma_k(n) = \sum_{d|n} d^k$ ist.*

Wie sich zeigt, besitzen auch diese Funktionen eine enge Beziehung zu komplexen elliptischen Kurven und damit auch zu Gittern. Das folgenden Lemma gibt eine Beziehung zwischen Koeffizienten komplexer elliptischer Kurven und diesen normalisierten Eisenstein-Reihen an (vgl. [Ap90, Seite 11 ff]).

**Lemma 6.4** *Sei* $\lambda = \frac{\sqrt{3}}{\pi}$ *und* $E = (a, b)$ *eine elliptische Kurve über* $\mathbb{C}$*, so daß* $E(\mathbb{C}) \cong \mathbb{C}/L$ *für ein Gitter* $L = \mathbb{Z}\,\lambda + \mathbb{Z}\,\lambda\,\tau$*. Dann gilt* $a = -3\,E_4(\tau)$ *und* $b = -2\,E_6(\tau)$*.*

Sei im folgenden $\lambda = \frac{\sqrt{3}}{\pi}$ fest und sei ein Gitter $L = \mathbb{Z}\,\lambda + \mathbb{Z}\,\lambda\,\tau$ vorgegeben. Kennen wir für die durch dieses Gitter vorgegebene Zahl $\tau$ den Wert von $E_4(\tau)$ und $E_6(\tau)$, so kennen wir mit Hilfe des gerade angegebenen Lemmas auch die Kurvenkoeffizienten einer komplexen elliptischen Kurve $E$ mit $E(\mathbb{C}) \cong \mathbb{C}/L$ und damit mit Lemma 6.2 alle Koeffizienten $c_k$ der Fourierentwicklung der zugehörigen $\wp$-Funktion $\wp(z, L)$. Andererseits gibt es zu vorgegebener Kurve $E$ auch ein Gitter in dieser Gestalt und wir kennen dann die Werte von $E_4(\tau)$ und $E_6(\tau)$ für die durch dieses Gitter bestimmte komplexe Zahl $\tau$.

Wir werden im folgenden Abschnitt bei der Herleitung der gesuchten Formeln noch einen weiteren Wert $P_1(L)$ zu dem Gitter $L$ benötigen:

$$P_1(L) \quad := \quad \sum_{n=1}^{(l-1)/2} \wp\left(\frac{n\,\lambda}{l}, L\right). \tag{6.1}$$

Wie wir im folgenden Abschnitt sehen werden, handelt es sich bei diesem Wert um die Summe der $x$-Koordinaten speziell gewählter $l$-Torsionspunkte von $E(\mathbb{C})$. In Lemma 6.5 stellen wir auch für diesen Wert eine Beziehung zu normalisierten Eisenstein-Reihen her.

**Lemma 6.5** *Sei das Gitter* $L = \mathbb{Z}\,\lambda + \mathbb{Z}\,\lambda\,\tau$ *vorgegeben. Dann gilt*

$$P_1(L) \quad = \quad -\frac{l}{2}\Big(E_2(\tau) - l \cdot E_2(l\tau)\Big).$$

**Beweis:** Aus [El, Seite 33] erhalten wir die folgende Fourierentwicklung für $P_1(L)$

$$P_1(L) \quad = \quad \frac{l(l-1)}{2} + 12\,l \sum_{n=1}^{\infty} \sigma_1'(n)\,q_\tau^n,$$

wobei $\sigma_1'(n)$ die Summe aller zu $l$ teilerfremden Teiler von $n$ ist. Wir versuchen, die dabei auftretende unendliche Summe anders darzustellen. Dazu beachten wir die folgende „Aufteilung“ von $\sigma_1(n)$ für festes $n \in \mathbb{N}$:

$$\sigma_1(n) \quad = \quad \sum_{\substack{d|n \\ \mathrm{ggT}(d,l)=1}} d \; + \sum_{\substack{d|n \\ \mathrm{ggT}(d,l)>1}} d \quad = \quad \sigma_1'(n) + \sum_{\substack{d|n \\ \mathrm{ggT}(d,l)>1}} d.$$

Durch Einsetzen dieser Gleichung erhalten wir

$$\begin{aligned}
\sum_{n=1}^{\infty} \sigma_1'(n)\,q_\tau^n \quad &= \quad \sum_{n=1}^{\infty} \left(\sigma_1(n)\,q_\tau^n \; - \sum_{\substack{d|n \\ \mathrm{ggT}(d,l)>1}} d\,q_\tau^n\right) \\
&= \quad \sum_{n=1}^{\infty} \sigma_1(n)\,q_\tau^n - \sum_{n=1}^{\infty} \left(l \cdot \sum_{d|n} d\,q_\tau^{n\,l}\right) \\
&= \quad \sum_{n=1}^{\infty} \sigma_1(n)\,q_\tau^n - l \cdot \sum_{n=1}^{\infty} \sigma_1(n) \cdot q_{l\tau}^n.
\end{aligned}$$

Aus Definition 6.3 folgt

$$\sum_{n=1}^{\infty} \sigma_1(n)\, q_\tau^n \quad = \quad \frac{1 - E_2(\tau)}{24}.$$

Setzen wir dies in die gerade berechnete Formel ein und fassen dann zusammen, so erhalten wir das Ergebnis des Lemmas. ■

Wir benötigen noch einige weitere Beziehungen zwischen normalisierten Eisenstein-Reihen und anderen komplexwertigen Funktionen, die eine Beziehung zu elliptischen Kurven haben. Wir geben alle benutzten Formeln hier an; man findet sie zum Beispiel in [Si85] und bei Ramanujan (siehe [Ra16] oder [Se71, Th. 4 (ii), Seite 78]):

$$\Delta(\tau) \quad = \quad \frac{E_4^3(\tau) - E_6^2(\tau)}{1728} \tag{6.2}$$

$$j(\tau) \quad = \quad \frac{E_4^3(\tau)}{\Delta(\tau)} \tag{6.3}$$

$$j(\tau) - 1728 \quad = \quad \frac{E_6^2(\tau)}{\Delta(\tau)} \tag{6.4}$$

$$E_2(\tau) \quad = \quad \frac{\Delta'(\tau)}{\Delta(\tau)} \tag{6.5}$$

$$\frac{3E_4'(\tau)}{E_4(\tau)} \quad = \quad E_2(\tau) - \frac{E_6(\tau)}{E_4(\tau)} \tag{6.6}$$

$$\frac{2E_6'(\tau)}{E_6(\tau)} \quad = \quad E_2(\tau) - \frac{E_4^2(\tau)}{E_6(\tau)} \tag{6.7}$$

$$12 \cdot E_2'(\tau) \quad = \quad E_2^2(\tau) - E_4(\tau) \tag{6.8}$$

$$j'(\tau) \quad = \quad \frac{-E_4^2(\tau) \cdot E_6(\tau)}{\Delta(\tau)} \tag{6.9}$$

$$\frac{j'(\tau)}{j(\tau)} \quad = \quad -\frac{E_6(\tau)}{E_4(\tau)} \tag{6.10}$$

## 6.2 Bestimmung eines Teilers des $l$-ten Divisionspolynoms für komplexe elliptische Kurven

Im Algorithmus von Schoof wird die Gruppenordnung modulo $l$ durch Polynomrechnungen modulo des $l$-ten Divisionspolynoms (siehe Definition 4.11 (Seite 39)) berechnet. Die Idee von Elkies war es, diese Rechnungen durch Rechnungen modulo eines Teilers des $l$-ten Divisionspolynoms zu ersetzen. In diesem Abschnitt werden wir angeben, wie man für elliptische Kurven über den komplexen Zahlen solche Teiler bestimmen kann.

Seien ein Gitter $L = \mathbb{Z}\,\lambda + \mathbb{Z}\,\lambda\,\tau$ und eine komplexe elliptische Kurve $E$ mit $E \cong \mathbb{C}/L$ vorgegeben. Wir wollen ein Polynom $f_C(X)$ vom Grad $d := (l-1)/2$ bestimmen, welches ein Teiler des $l$-ten Divisionspolynoms ist (d.h. dessen Nullstellen $x$-Koordinaten von $l$-Torsionspunkten sind). Dazu beachten wir, daß nach [Si85, Prop. 5.4, Seite 163] die zur $l$-Torsionsgruppe isomorphe Gruppe in $\mathbb{C}/L$ die Gruppe

$$\frac{1}{l}\,L\Big/L$$

ist. Das Polynom $f_C(X)$ soll als Nullstellen genau die verschiedenen $x$-Koordinaten von Punkten der $l$-Gruppe $\left\{r\,\frac{\lambda}{l};\ -d \le r \le d,\ r \ne 0\right\}$ (des Gitters) haben, d.h. wir erhalten

$$f_C(X) \quad := \quad \prod_{r=1}^{d} \left( X - \wp\left(\frac{r\,\lambda}{l}, L\right) \right).$$

Dabei beachte man, daß die zu einer Zahl $z \in \mathbb{C}/L$ korrespondierende $x$-Koordinate genau $\wp(z, L)$ ist [Si85, Kapitel 6] und daß $\wp(z, L) = \wp(-z, L)$ gilt (aus der Definition direkt ersichtlich). Offensichtlich ist dieses Polynom $f_C(X)$ dann ein Teiler des $l$-ten Divisionspolynoms zu $E$.

Zur Herleitung eines Algorithmus zur Bestimmung dieses Polynoms $f_C(X)$ definieren wir das folgende, im Vergleich zu dem Startgitter $L$ etwas veränderte Gitter

$$\tilde{L} \quad = \quad \mathbb{Z}\,\frac{\lambda}{l} + \mathbb{Z}\,\lambda\,\tau.$$

Wir vergleichen die Weierstrass-$\zeta$-Funktion zu $\tilde{L}$ mit der $\zeta$-Funktion zu dem Startgitter $L$. Dann liefert Formel (XXI-3) aus [TaMo72, Seite 224]

$$\zeta(z, \tilde{L}) \;=\; \zeta(z, L) + \sum_{\substack{r=-d \\ r \ne 0}}^{d} \zeta\left(z + \frac{2r\lambda}{l}, L\right) + 2\,z\,P_1(L), \tag{6.11}$$

wobei

$$2\,P_1(L) \quad = \quad \sum_{n=1}^{l-1} \wp\left(\frac{2\,n\,\lambda}{l}, L\right)$$

ist. Da für eine Primzahl $l$ die Zahlen $-d, \ldots, -1, 1, \ldots, d$ ein komplettes Restsystem aller modulo $l$ invertierbarer Zahlen bilden und da die $\wp$-Funktion eine elliptische

Funktion ist (d.h. es gilt für $a \in L$ $\wp(z+a,L) = \wp(z,L)$), können wir diese Summe auch als

$$2\,P_1(L) \quad = \sum_{n=-d, n\neq 0}^{d} \wp\left(\frac{n\,\lambda}{l}, L\right)$$

schreiben. Nun nutzen wir $\wp(z,L) = \wp(-z,L)$ aus und erhalten so wie in (6.1) schon angegeben

$$P_1(L) \quad = \quad \sum_{n=1}^{d} \wp\left(\frac{n\,\lambda}{l}, L\right).$$

In [La87, Seite 240] finden wir die Gleichung $\zeta(z+\lambda, L) = \zeta(z,L) + \eta(\lambda)$ für eine Konstante $\eta(\lambda)$, für die zusätzlich gilt $\eta(-\lambda) = -\eta(\lambda)$. Damit können wir in (6.11) in der Summe $\zeta\left(z + \frac{2r\lambda}{l}, L\right)$ ersetzen durch $\zeta\left(z + \frac{r\lambda}{l}, L\right)$. Um (6.11) noch weiter zu vereinfachen, benötigen wir eine weitere Eigenschaft der $\zeta$-Funktion, das sogenannte **Additionsgesetz** für die $\zeta$-Funktion [TaMo72, Bd. III, Seite 42, 396]:

$$\zeta(z \pm a, L) \quad = \quad \zeta(z,L) \pm \zeta(a,L) + \frac{\wp'(z,L) \mp \wp'(a,L)}{2\left(\wp(z,L) - \wp(a,L)\right)}.$$

Addieren wir also $\zeta(z+a,L)$ und $\zeta(z-a,L)$, so erhalten wir mit Hilfe des Additionsgesetzes

$$\zeta(z+a,L) \;+\; \zeta(z-a,L) \quad = \quad 2\,\zeta(z,L) \;+\; \frac{\wp'(z,L)}{\wp(z,L) - \wp(a,L)}.$$

Setzen wir diese Gleichung in (6.11) ein und formen dann um, so erhalten wir

$$\begin{aligned}
\zeta(z,\tilde{L}) \quad &= \quad \zeta(z,L) \;+\; \sum_{r=1}^{d} \left(\zeta\left(z + \frac{r\,\lambda}{l}, L\right) + \zeta\left(z - \frac{r\,\lambda}{l}, L\right)\right) \;+\; 2\,z\,P_1(L) \\
&= \quad \zeta(z,L) \;+\; \sum_{r=1}^{d} \left(2\,\zeta(z,L) + \frac{\wp'(z,L)}{\wp(z,L) - \wp\left(\frac{r\lambda}{l}, L\right)}\right) \;+\; 2\,z\,P_1(L) \\
&= \quad (2d+1)\,\zeta(z,L) \;+\; \sum_{r=1}^{d} \frac{\wp'(z,L)}{\wp(z,L) - \wp\left(\frac{r\lambda}{l}, L\right)} \;+\; 2\,z\,P_1(L).
\end{aligned}$$

In diese letzte Gleichung wollen wir nun die aus Lemma 6.2 bekannten Fourierreihenentwicklungen der $\zeta$-Funktion einsetzen. Seien dazu $c_k$ und $\tilde{c}_k$, $k = 1, \ldots, \infty$ die Koeffizienten der Fourierentwicklung von $\zeta(z,L)$ bzw. $\zeta(z,\tilde{L})$. Dann erhalten wir durch Einsetzen

$$\sum_{r=1}^{d} \frac{\wp'(z,L)}{\wp(z,L) - \wp\left(\frac{r\lambda}{l}, L\right)} \quad = \quad \frac{1-l}{z} - \sum_{k=1}^{\infty} (\tilde{c}_k - l\,c_k) \cdot \frac{z^{2k+1}}{2k+1} - 2\,z\,P_1(L). \qquad (6.12)$$

Aus dieser Gleichung wollen wir nun auf einfache Art und Weise das gewünschte Polynom $f_C(X)$ bestimmen. Seien die Koeffizienten dieses Polynoms folgendermaßen vorgegeben:

$$f_C(X) \quad = \quad X^d + a_{d-1} \cdot X^{d-1} + \ldots + a_0 \quad = \quad \prod_{r=1}^{d} \left( X - \wp\left( \frac{r\,\lambda}{l}, L \right) \right).$$

Damit wird die Bedeutung von (6.12) schon deutlicher. Integrieren wir (6.12) und exponentieren wir die dann entstehende Gleichung, so wird der Term auf der linken Seite der Gleichung (6.12)

$$\prod_{r=1}^{d} \left( \wp(z, L) - \wp\left( \frac{r\,\lambda}{l}, L \right) \right), \qquad \text{d.h. genau} \qquad f_C\big(\wp(z, L)\big).$$

Damit erhalten wir so mit einer geeigneten Konstanten $D$ die Gleichung

$$f_C\big(\wp(z, L)\big) \quad = \quad D \cdot z^{1-l} \cdot \exp\left( \sum_{k=1}^{\infty} (l\,c_k - \tilde{c}_k) \cdot \frac{z^{2k+2}}{(2k+1)(2k+2)} - P_1(L)\,z^2 \right). \tag{6.13}$$

Dann ist die Idee zur Bestimmung der Polynomkoeffizienten $a_{d-1}, \ldots, a_0$ folgendermaßen: wir entwickeln die linke und rechte Seite dieser Gleichung (6.13) als Reihe in $z$ und bestimmen dann durch einen Koeffizientenvergleich der „minimalen“ $z$-Potenz beider Seiten die Polynomkoeffizienten. Zur Bestimmung der Reihenentwicklung der rechte Seite von (6.13) benutzen wir die bekannte Fourierentwicklung der Exponentialfunktion. Dann erhalten wir

$$D \cdot z^{1-l} \cdot \exp\left( \sum_{k=1}^{\infty} (l\,c_k - \tilde{c}_k) \cdot \frac{z^{2k+2}}{(2k+1)(2k+2)} - P_1(L)\,z^2 \right) \quad = \quad D \cdot z^{1-l} \cdot \sum_{r=0}^{\infty} \frac{\left( \sum_{k=1}^{\infty} (l\,c_k - \tilde{c}_k) \cdot \frac{z^{2k+2}}{(2k+1)(2k+2)} - P_1(L)\,z^2 \right)^r}{r!}. \tag{6.14}$$

Betrachten wir in (6.13) auf beiden Seiten den Term mit der minimalen Potenz von $z$, so können wir leicht $D$ bestimmen; wir erhalten so $D = 1$. Damit können wir für die rechte Seite von (6.13) eine Fourierentwicklung der Form

$$z^{1-l} \cdot \sum_{r=0}^{\infty} d_r \cdot z^{2r}$$

berechnen, wenn wir die Werte $c_k, \tilde{c}_k$ und $P_1(L)$ kennen. Die Berechnung der Koeffizienten $c_k$ ist nach Lemma 6.2 leicht möglich; mit Hilfe desselben Lemmas können wir auch die Werte $\tilde{c}_k$ bestimmen, wenn wir die Kurvenkoeffizienten der elliptischen Kurve $E/C$ für die hier speziell gewählte $l$-Gruppe $C$ kennen. Durch Koeffizientenvergleich in Gleichung (6.13) können wir dann alle Koeffizienten des Polynoms $f_C(X)$ berechnen.

In den folgenden beiden Abschnitten werden wir beschreiben, wie wir für die beiden in Kapitel 5 vorgestellten äquivalenten Polynome die jetzt noch gesuchten Werte (d.h. $P_1(L)$ und die Koeffizienten der elliptischen Kurve $E/C$ für die speziell vorgegebene $l$-Gruppe $C$) bestimmen können.

## 6.3 Bestimmung von $E/C$ und $P_1(L)$ mit Hilfe des äquivalenten Polynoms aus Abschnitt 5.2

Wir werden in diesem Abschnitt zeigen, wie wir mit Hilfe einer Nullstelle des in Abschnitt 5.2 vorgestellten äquivalenten Polynoms $G_l(X, j(\tau))$ die im letzten Abschnitt gesuchten Werte $E/C$ und $P_1(L)$ bestimmen können.

### 6.3.1 Benutzung eines zu $\tilde{L}$ äquivalenten Gitters

Wir haben im vorherigen Abschnitt beschrieben, wie wir bei Kenntnis der Kurvenkoeffizienten einer elliptischen Kurve $\tilde{E}$, die isomorph zu $\mathbb{C}/\tilde{L}$ mit $\tilde{L} = \mathbb{Z}\,\frac{\lambda}{l} + \mathbb{Z}\,\lambda\,\tau$ ist, und des Wertes $P_1(L)$ über den komplexen Zahlen einen Teiler des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$ bestimmen können. Zur Herleitung von Formeln zur Bestimmung dieser Werte benutzen wir aus technischen Gründen das folgende zu $\tilde{L}$ äquivalente Gitter

$$\hat{L} \quad = \quad \mathbb{Z}\,\lambda + \mathbb{Z}\,\lambda\,l\,\tau.$$

Wir werden nun zuerst zeigen, wie wir aus den Koeffizienten einer elliptischen Kurve $\hat{E}$, für die $\hat{E} \cong \mathbb{C}/\hat{L}$ gilt, die Koeffizienten der elliptischen Kurve $\tilde{E}$ bestimmen können. Aus diesen Kurvenkoordinaten können wir dann mit Lemma 6.2 die Koeffizienten der Fourierreihenentwicklung von $\zeta(z, \tilde{L})$ bestimmen.

**Lemma 6.6** *Angenommen, die Gitter $\tilde{L}$ und $\hat{L}$ besitzen die gerade angegebene Gestalt und $\tilde{E} = (\tilde{a}, \tilde{b})$ und $\hat{E} = (\hat{a}, \hat{b})$ sind die zugehörigen elliptischen Kurven. Dann gilt*

$$\tilde{a} \;=\; l^4 \cdot \hat{a} \qquad \text{und} \qquad \tilde{b} \;=\; l^6 \cdot \hat{b}.$$

**Beweis:** Der Beweis folgt durch einfache Umrechnungen (vgl. [Ap90, Th. 1.18, Seite 20ff]). ■

Mit Hilfe der Lemmata 6.4 und 6.2 können wir damit die Koeffizienten $\tilde{a}$ und $\tilde{b}$ und so die Fourierreihenentwicklung der Funktion $\wp(z, \tilde{L})$ bestimmen, wenn wir den Wert der Eisenstein-Reihen $E_4(l\tau)$ und $E_6(l\tau)$ kennen. Beachte, daß $\tau$ bei Vorgabe einer elliptischen Kurve $E$ eine durch das zugehörige Gitter $L$ eindeutig bestimmte komplexe Zahl ist. Weiterhin werden wir eine Methode angeben, wie wir den Wert der Funktion

$$E_2^*(\tau) \quad := \quad E_2(\tau) - l \cdot E_2(l\tau) \tag{6.15}$$

bestimmen können. Dann liefert Lemma 6.5 auch den Wert von $P_1(L)$ und wir können die im vorherigen Abschnitt beschriebene Vorgehensweise anwenden, um über den komplexen Zahlen einen Teiler des $l$-ten Divisionspolynoms zu bestimmen.

### 6.3.2 Einige Hilfsmittel

Wir nehmen in diesem Abschnitt an, daß wir das zum $l$-ten modularen Polynom äquivalente Polynom $G_l(X,Y)$ mit Hilfe der Funktion

$$g(\tau) = \frac{l^s}{f(\tau)} \qquad \text{mit} \qquad f(\tau) = \left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s}$$

berechnet haben (vgl. die Abschnitte 5.1, 5.2). Dabei war $s$ die kleinste natürliche Zahl, so daß 12 ein Teiler von $s\cdot(l-1)$ ist. Wir leiten nun Beziehungen zwischen diesen beiden Funktionen und normalisierten Eisenstein-Reihen her, mit denen wir bei Kenntnis des Wertes von $g(\tau)$ die Werte von $E_4(l\tau)$, $E_6(l\tau)$ und $E_2^*(\tau)$ bestimmen können. Bei der Herleitung dieser Beziehungen werden wir öfter die Ableitung einer Funktion nach der Variablen $\tau$ benötigen; dabei kennzeichnen wir die Ableitung wie üblich mit einem $'$ (d.h. $f'(\tau)$ ist die Ableitung der Funktion $f(\tau)$ nach der Variablen $\tau$).

**Lemma 6.7** *Es gilt*

$$E_2^*(\tau) = \frac{12\, f'(\tau)}{s\cdot f(\tau)} = \frac{-12\, g'(\tau)}{s\cdot g(\tau)}.$$

**Beweis:** Zuerst beachte man, daß aus der Definition der Funktion $g(\tau)$ folgt

$$\frac{g'(\tau)}{g(\tau)} = \frac{-l^s\cdot f'(\tau)\cdot f(\tau)}{l^s\cdot f^2(\tau)} = \frac{-f'(\tau)}{f(\tau)}.$$

Damit müssen wir nur noch den ersten Teil der Behauptung zeigen. Leiten wir dazu die Funktion $f(\tau)$ ab, so erhalten wir

$$f'(\tau) = 2s\cdot\left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s-1}\cdot\frac{\eta'(\tau)\eta(l\tau)-l\cdot\eta(\tau)\eta'(l\tau)}{\eta^2(l\tau)}.$$

Beachten wir nun, daß

$$\Delta(\tau) = (2\pi)^{12}\,\eta^{24}(\tau) \qquad \text{und damit} \qquad \Delta'(\tau) = 24\,(2\pi)^{12}\,\eta^{23}(\tau)\cdot\eta'(\tau)$$

gilt [Ap90, Th. 3.3, Seite 51], so folgt aus Gleichung (6.5)

$$E_2(\tau) = 24\cdot\frac{\eta'(\tau)}{\eta(\tau)} \qquad \text{und analog} \qquad E_2(l\tau) = 24\cdot\frac{\eta'(l\tau)}{\eta(l\tau)}.$$

Zum Beweis des Lemmas müssen wir nun zeigen, daß

$$f'(\tau) = \frac{s}{12}\,f(\tau)\cdot\Big(E_2(\tau)-l\cdot E_2(l\tau)\Big)$$

gilt. Wir rechnen dazu die rechte Seite dieser Behauptung aus:

$$\begin{aligned}\frac{s}{12}\,f(\tau)\cdot\Big(E_2(\tau)-l\cdot E_2(l\tau)\Big) &= 2s\cdot\left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s}\cdot\left(\frac{\eta'(\tau)}{\eta(\tau)}-l\cdot\frac{\eta'(l\tau)}{\eta(l\tau)}\right)\\ &= 2s\cdot\left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s-1}\cdot\left(\frac{\eta'(\tau)\eta(l\tau)-l\cdot\eta'(l\tau)\eta(\tau)}{\eta^2(l\tau)}\right).\end{aligned}$$

Durch Vergleich dieser Gleichung mit der berechneten Ableitung der Funktion $f(\tau)$ folgt die Behauptung des Lemmas. ∎

Aus der speziellen Gestalt der Funktion $g(\tau)$ ergibt sich noch eine weitere schöne Eigenschaft. Wir können bei Kenntnis des Wertes von $g(\tau)$ nämlich sogar den Wert von $\Delta(l\tau)$ leicht ausrechnen, wie das folgende Lemma angibt.

**Lemma 6.8** *Es gilt*

$$\Delta(l\tau) = \frac{\Delta(\tau)}{f(\tau)^{12/s}}.$$

**Beweis:** Wiederum benutzen wir die Gleichungen $\Delta(l\tau) = (2\pi)^{12}\,\eta^{24}(l\tau)$ und $\Delta(\tau) = (2\pi)^{12}\,\eta^{24}(\tau)$ und rechnen mit Hilfe der Definition der Funktion $f(\tau)$ die rechte Seite der Behauptung aus. Dann erhalten wir

$$\begin{aligned} \frac{\Delta(\tau)}{f(\tau)^{12/s}} &= (2\pi)^{12}\left(\left(\frac{\eta(l\tau)}{\eta(\tau)}\right)^{2s}\right)^{12/s}\cdot\eta^{24}(\tau) \\ &= (2\pi)^{12}\,\eta(l\tau)^{24} \\ &= \Delta(l\tau). \end{aligned}$$ ■

**Bemerkung 6.9** Wir sollten beachten, daß $\frac{12}{s}$ immer eine ganze Zahl ist. Wir hatten nämlich $s$ als die kleinste positive Zahl gewählt, so daß 12 ein Teiler von $s\cdot(l-1)$ ist. Offensichtlich gilt dann $1 \le s \le 12$. Da $l$ immer eine ungerade Primzahl ist, folgt sogar $1 \le s \le 6$. Damit wäre der einzige kritische Fall $s = 5$. Dann gilt $5\,(l-1) \equiv 0 \bmod 12$ und, da 5 invertierbar ist modulo 12, sogar

$$l-1 \equiv 0 \bmod 12.$$

Damit kann die Wahl $s = 5$ nicht vorkommen.

Nun kennen wir alle benötigten Informationen, um die Vorgehensweise zur Berechnung von $E_4(l\tau)$, $E_6(l\tau)$ und $E_2^*(\tau)$ anzugeben. Wir nehmen an, daß wir die Werte

$$E_4(\tau),\quad E_6(\tau),\quad j(\tau),\quad \Delta(\tau),\quad g(\tau),\quad f(\tau),\quad \Delta(l\tau)\quad \text{und}\quad j'(\tau)$$

kennen. Dabei erhalten wir $g(\tau)$ als eine Nullstelle des Polynoms $G_l(X, j(\tau))$; alle anderen Werte können wir direkt mit Hilfe der obigen Formeln (6.3), (6.2), (6.9) und Lemma 6.8 berechnen. In den folgenden Abschnitten leiten wir Beziehungen zwischen diesen Funktionen her, mit denen wir die gesuchten Werte bestimmen können.

### 6.3.3 Berechnung von $E_2^*(\tau)$

Sei im folgenden $G_l(X,Y) \in \mathbb{Z}[X,Y]$ das zu $g(\tau)$ „gehörende" äquivalente Polynom, für das gilt

$$G_l\Big(g(\tau), j(\tau)\Big) = 0.$$

Leiten wir diese Gleichung nach $\tau$ ab, so erhalten wir durch Anwendung der Kettenregel

$$g'(\tau)\cdot\left(\frac{d}{dX}G_l(X,Y)\right)(g(\tau),j(\tau))+j'(\tau)\cdot\left(\frac{d}{dY}G_l(X,Y)\right)(g(\tau),j(\tau)) \;=\; 0. \quad (6.16)$$

Hierbei ist $\frac{d}{dX}G_l(X,Y)$ die partielle Ableitung von $G_l(X,Y)$ nach der ersten Variablen $X$ und $\frac{d}{dY}G_l(X,Y)$ die partielle Ableitung von $G_l(X,Y)$ nach der zweiten Variablen $Y$. Um diese Gleichung dazu zu benutzen, den Wert von $E_2^*(\tau)$ zu berechnen, definieren wir zuerst folgende Funktionen

$$DF(\tau) \;:=\; g(\tau)\cdot\left(\frac{d}{dX}G_l(X,Y)\right)(g(\tau),j(\tau))$$

und

$$DJ(\tau) \;:=\; j(\tau)\cdot\left(\frac{d}{dY}G_l(X,Y)\right)(g(\tau),j(\tau)).$$

Mit Hilfe dieser Funktionen können wir eine Formel für $E_2^*(\tau)$ herleiten als

$$E_2^*(\tau) \;=\; \frac{-12\,E_6(\tau)\cdot DJ(\tau)}{s\cdot E_4(\tau)\cdot DF(\tau)}. \quad (6.17)$$

Zum Beweis der Korrektheit dieser Gleichung formen wir die Formel aus Lemma 6.7 mit Hilfe von (6.16) und (6.10) um:

$$\begin{aligned} E_2^*(\tau) &= \frac{-12\,g'(\tau)}{s\cdot g(\tau)} \\ &= \frac{12\,j'(\tau)\cdot g(\tau)\cdot DJ(\tau)}{s\cdot j(\tau)\cdot g(\tau)\cdot DF(\tau)} \\ &= \frac{-12\,E_6(\tau)\cdot DJ(\tau)}{s\cdot E_4(\tau)\cdot DF(\tau)}. \end{aligned}$$

### 6.3.4 Berechnung von $E_4(l\tau)$

Wir können damit im weiteren davon ausgehen, daß wir den Wert von $E_2^*(\tau)$ berechnet haben. In diesem Abschnitt leiten wir Beziehungen her, um zusätzlich den Wert $E_4(l\tau)$ berechnen zu können. Dazu setzen wir

$$E_0(\tau) \;:=\; \frac{E_6(\tau)}{E_4(\tau)\cdot E_2^*(\tau)}. \quad (6.18)$$

Wiederum beachte man, daß wir den Wert von $E_0(\tau)$ berechnen können. Um eine erste Gleichung herzuleiten, die wir anschließend zur Bestimmung von $E_4(l\tau)$ benutzen werden, leiten wir diese Funktion nach $\tau$ ab, dividieren durch $E_0(\tau)$ und erhalten so

$$\frac{E_0'(\tau)}{E_0(\tau)} = \frac{E_2^*(\tau)\cdot E_4(\tau)\cdot E_6'(\tau) - E_6(\tau)\cdot\left[E_2^*(\tau)\cdot E_4'(\tau) + E_2^{*\prime}(\tau)\cdot E_4(\tau)\right]}{E_2^*(\tau)\cdot E_4(\tau)\cdot E_6(\tau)}. \quad (6.19)$$

Hierin können wir $E_4'(\tau)$ und $E_6'(\tau)$ mit Hilfe von Formel (6.6) bzw. (6.7) ersetzen. Die Ableitung von $E_2^*(\tau)$ können wir leicht aus der Definition von $E_2^*(\tau)$ ausrechnen, wir erhalten sie als

$$E_2^{*\prime}(\tau) \quad = \quad E_2'(\tau) - l^2 \cdot E_2'(l\tau).$$

Diese Identitäten setzen wir in Gleichung (6.19) ein. Nach Multiplizieren mit dem Nenner erhalten wir dann die neue Gleichung

$$\begin{aligned} \frac{E_0'(\tau)}{E_0(\tau)} \cdot E_2^*(\tau) \cdot E_4(\tau) \cdot E_6(\tau) \quad &= \quad 2^{-1} \cdot E_2^*(\tau) \cdot E_4(\tau) \cdot \Big[E_2(\tau) \cdot E_6(\tau) - E_4^2(\tau)\Big] \\ &\quad -3^{-1} \cdot E_2^*(\tau) \cdot E_6(\tau) \cdot \Big[E_2(\tau) \cdot E_4(\tau) - E_6(\tau)\Big] \\ &\quad -E_4(\tau) \cdot E_6(\tau) \cdot \Big[E_2'(\tau) - l^2 \cdot E_2'(l\tau)\Big]. \end{aligned}$$

In dieser Gleichung können wir mit Hilfe von Formel (6.8) die beiden Werte $E_2'(\tau)$ bzw. $E_2'(l\tau)$ ersetzen und anschließend durch $E_4(\tau) \cdot E_6(\tau)$ teilen. Dann erhalten wir

$$\begin{aligned} \frac{E_0'(\tau)}{E_0(\tau)} \cdot E_2^*(\tau) \quad &= \quad 2^{-1}\, E_2^*(\tau) \cdot \left[E_2(\tau) - \frac{E_4^2(\tau)}{E_6(\tau)}\right] - 3^{-1}\, E_2^*(\tau) \cdot \left[E_2(\tau) - \frac{E_6(\tau)}{E_4(\tau)}\right] \\ &\quad -12^{-1} \Big[E_2^2(\tau) - E_4(\tau)\Big] + 12^{-1}\, l^2 \cdot \Big[E_2^2(l\tau) - E_4(l\tau)\Big]. \end{aligned}$$

Damit haben wir einen Ausdruck erhalten, der $E_4(l\tau)$ enthält. Formen wir diesen Ausdruck um, so erhalten wir folgende Gleichung zur Berechnung von $E_4(l\tau)$

$$\begin{aligned} l^2\, E_4(l\tau) \quad &= \quad E_4(\tau) - E_2^*(\tau) \cdot \left[12\, \frac{E_0'(\tau)}{E_0(\tau)} + 6\, \frac{E_4^2(\tau)}{E_6(\tau)} - 4\, \frac{E_6(\tau)}{E_4(\tau)}\right] \\ &\quad +2\, E_2^*(\tau) \cdot E_2(\tau) - E_2^2(\tau) + l^2\, E_2^2(l\tau). \end{aligned}$$

Nun ersetzen wir in der zweiten Zeile dieser Gleichung $E_2^*(\tau)$ durch seine Definition; dies ergibt dann

$$\begin{aligned} 2\, E_2^*(\tau) \cdot E_2(\tau) - E_2^2(\tau) + l^2\, E_2^2(l\tau) \quad &= \quad 2\, \Big(E_2(\tau) - l \cdot E_2(l\tau)\Big) \cdot E_2(\tau) \\ &\quad -E_2^2(\tau) + l^2\, E_2^2(l\tau) \\ &= \quad E_2^2(\tau) - 2\, l\, E_2(\tau) \cdot E_2(l\tau) + l^2\, E_2^2(l\tau) \\ &= \quad E_2^{*2}(\tau). \end{aligned}$$

Durch Einsetzen erhalten wir dann eine erste „brauchbare“ Gleichung zur Berechnung des Wertes von $E_4(l\tau)$ als

$$l^2\, E_4(l\tau) \;=\; E_4(\tau) - E_2^*(\tau) \cdot \left[12\, \frac{E_0'(\tau)}{E_0(\tau)} + 6\, \frac{E_4^2(\tau)}{E_6(\tau)} - 4\, \frac{E_6(\tau)}{E_4(\tau)}\right] + E_2^{*2}(\tau). \tag{6.20}$$

In dieser Gleichung kennen wir alle Werte (oder können sie leicht berechnen) bis auf $E_0'(\tau)$. Wir benötigen daher noch eine zweite Gleichung, mit deren Hilfe wir

$E_0'(\tau)$ bestimmen können. Um eine solche Gleichung herzuleiten, schreiben wir die Gleichung für $E_2^*(\tau)$ aus (6.17) etwas anders als

$$DF(\tau) \;+\; \frac{12}{s} \underbrace{\frac{E_6(\tau)}{E_4(\tau)\cdot E_2^*(\tau)}}_{=E_0(\tau)} \cdot DJ(\tau) \quad = \quad 0. \tag{6.21}$$

Wir erhalten damit den Wert von $E_0'(\tau)$, wenn wir diese Gleichung ableiten. Dazu benötigen wir allerdings die Ableitungen von $DF(\tau)$ und $DJ(\tau)$, die wir aus ihrer Definition berechnen können als

$$\begin{aligned} DF'(\tau) \quad &= \quad g'(\tau)\cdot\left(\frac{d}{dX}G_l(X,Y)\right)(g(\tau),j(\tau)) \\ &\quad +g(\tau)\cdot\left[g'(\tau)\cdot\left(\frac{d}{dX^2}G_l(X,Y)\right)(g(\tau),j(\tau))\right. \\ &\qquad \left. +j'(\tau)\cdot\left(\frac{d}{dXY}G_l(X,Y)\right)(g(\tau),j(\tau))\right]. \end{aligned}$$

Analog berechnen wir die Ableitung $DJ'(\tau)$ aus der Definition von $DJ(\tau)$ als

$$\begin{aligned} DJ'(\tau) \quad &= \quad j'(\tau)\cdot\left(\frac{d}{dY}G_l(X,Y)\right)(g(\tau),j(\tau)) \\ &\quad +j(\tau)\cdot\left[j'(\tau)\cdot\left(\frac{d}{dY^2}G_l(X,Y)\right)(g(\tau),j(\tau))\right. \\ &\qquad \left. +g'(\tau)\cdot\left(\frac{d}{dYX}G_l(X,Y)\right)(g(\tau),j(\tau))\right]. \end{aligned}$$

Wiederum sollte man beachten, daß wir diese beiden Werte ausrechnen können. Wir kennen nämlich $j'(\tau)$ mit Hilfe von Formel (6.10) und können $g'(\tau)$ mit Lemma 6.7 aus $E_2^*(\tau)$ berechnen. Zusätzlich müssen wir das Polynom $G_l(X,Y)$ nur noch zweimal partiell ableiten, was auch einfach berechenbar ist. Als Ableitung von (6.21) erhalten wir dann

$$DF'(\tau) + \frac{12}{s}\cdot\left[E_0'(\tau)\cdot DJ(\tau) + E_0(\tau)\cdot DJ'(\tau)\right] \quad = \quad 0.$$

Damit können wir durch Einsetzen aus dieser Gleichung den Wert von $E_0'(\tau)$ berechnen. Diesen Wert $E_0'(\tau)$ setzen wir dann in (6.20) ein und bestimmen damit den Wert von $E_4(l\tau)$.

### 6.3.5 Berechnung von $E_6(l\tau)$

Leider können wir nicht dieselbe Formel benutzen, um auch $E_6(l\tau)$ zu berechnen. Wir können jedoch mit den nun zur Verfügung stehenden Informationen

$$j(l\tau) \quad = \quad \frac{E_4^3(l\tau)}{\Delta(l\tau)}$$

ausrechnen (Formel (6.3)). Dann verwenden wir eine weitere in Kapitel 5 bewiesene Eigenschaft des äqivalenten Polynoms. Wir haben dort in (5.4) gezeigt, daß sogar

$$G_l\Big(f(\tau), j(l\tau)\Big) \quad = \quad 0$$

gilt. Leiten wir diese Gleichung nach $\tau$ ab, so erhalten wir

$$f'(\tau)\cdot\left(\frac{d}{dX}G_l(X,Y)\right)(f(\tau), j(l\tau)) + l\, j'(l\tau)\cdot\left(\frac{d}{dY}G_l(X,Y)\right)(f(\tau), j(l\tau)) \;=\; 0.$$

Hieraus können wir nach einer Umformung den Wert von $j'(l\tau)$ berechnen, da wir mit $g(\tau)$ auch $f(\tau)$ kennen und damit den Wert $f'(\tau)$ aus $E_2^*(\tau)$ berechnen können. Dann wenden wir (6.10) an und erhalten daraus

$$E_6(l\tau) \quad = \quad -\frac{E_4(l\tau)\cdot j'(l\tau)}{j(l\tau)}.$$

Damit haben wir für das in Abschnitt 5.2 eingeführte äquivalente Polynom gezeigt, wie wir bei Kenntnis von $E_4(\tau)$ und $E_6(\tau)$ die Werte von $E_4(l\tau)$, $E_6(l\tau)$ und $E_2^*(\tau)$ bestimmen können. Daraus können wir mit Hilfe der Lemmata 6.4 und 6.6 die Koeffizienten der Kurve $\tilde{E}$ und den Wert von $P_1(L)$ bestimmen. Die Kenntnis dieser Werte wurde in Abschnitt 6.2 vorausgesetzt, als wir eine Methode zur Bestimmung eines Teilers des $l$-ten Divisionspolynoms angegeben haben. Im folgenden Abschnitt werden wir dasselbe Problem für das in den Abschnitten 5.3 und 5.4 eingeführte äquivalente Polynom $G_l(X)$ (basierend auf einer Funktion $A(\tau)$, invariant unter Transformationen aus $\Gamma_0^*(l)$) lösen.

## 6.4 Bestimmung von $E/C$ und $P_1(L)$ mit Hilfe des äquivalenten Polynoms aus Abschnitt 5.4

Sei in diesem Abschnitt das äquivalente Polynom $G_l(X,Y)$ mit Hilfe einer Funktion $A(\tau)$, die invariant unter Transformationen aus $\Gamma_0^*(l)$ ist, berechnet (wie in Abschnitt 5.4 beschrieben). Diese Funktion hat keinen direkten Zusammenhang zur Dedekindschen $\eta$-Funktion mehr, so daß wir eine etwas andere Vorgehensweise zur Bestimmung der Werte von $E_2^*(\tau)$, $E_4(l\tau)$ und $E_6(l\tau)$ verwenden müssen. Wir gehen wieder davon aus, daß wir $E_4(\tau)$ und $E_6(\tau)$ kennen. Außerdem kennen wir den Wert von $A(\tau)$ als Nullstelle von $G_l(X, j(\tau))$. Wir leiten im folgenden wiederum Beziehungen zwischen den verwendeten Funktionen her, um so die gesuchten Werte zu bestimmen.

### 6.4.1 Berechnung von $E_4(l\tau)$ und $E_6(l\tau)$

Wie wir auf Seite 76 in (5.13) und (5.14) gezeigt haben, gelten für ein mit Hilfe einer solchen Funktion $A(\tau)$ berechnetes äquivalentes Polynom $G_l(X,Y) \in \mathbb{Z}[X,Y]$ die beiden Gleichungen

$$G_l\Big(A(\tau), j(\tau)\Big) = 0 \quad \text{und} \quad G_l\Big(A(\tau), j(l\tau)\Big) = 0. \tag{6.22}$$

Wir werden im folgenden Beziehungen zwischen den Funktionen $E_4(\tau)$, $E_6(\tau)$, $j(\tau)$ und $j(l\tau)$ herleiten. Mit Hilfe dieser Beziehungen können wir dann unter Kenntnis der Werte dieser Funktionen für das aktuelle Gitter die gewünschten Funktionswerte $E_2^*(\tau)$, $E_4(l\tau)$ und $E_6(l\tau)$ ausrechnen. Diese Vorgehensweise hat den Nachteil, daß wir für gegebene Eingabekurve zwar die Werte $E_4(\tau)$ und $E_6(\tau)$ und damit $j(\tau)$ kennen, nicht aber den Wert von $j(l\tau)$. Da wir $A(\tau)$ kennen, können wir das folgende Polynom

$$H(Y) := \frac{G_l\Big(A(\tau), Y\Big)}{Y - j(\tau)}$$

betrachten. Der Wert von $j(l\tau)$ ist dann eine Nullstelle dieses Polynoms. Wir können dann für alle Nullstellen von $H(Y)$, also alle „vermeintlichen" Werte von $j(l\tau)$, mit Hilfe der folgenden Formeln „vermeintliche" Werte $E_2^*(\tau)$, $E_4(l\tau)$ und $E_6(l\tau)$ bestimmen. Mit diesen Werten können wir mit den in Abschnitt 6.2 beschriebenen Ideen ein Polynom von Grad $(l-1)/2$ bestimmen. Dann können wir testen, ob wir so wirklich einen Teiler des $l$-ten Divisionspolynoms bestimmt haben, indem wir das $l$-te Divisionspolynom modulo des „vermeintlichen" Teilers berechnen. Damit finden wir mit Sicherheit einen solchen Teiler, da $j(l\tau)$ nach Konstruktion eine Nullstelle von $H(Y)$ ist.

Zur Herleitung von Beziehungen zwischen allen verwendeten Funktionen definieren wir wieder die folgenden Hilfswerte

$$DF_1(\tau) := \left(\frac{d}{dX} G_l(X,Y)\right)(A(\tau), j(\tau))$$

und

$$DJ_1(\tau) := \left(\frac{d}{dY} G_l(X,Y)\right)(A(\tau), j(\tau)).$$

Nun gehen wir ähnlich vor wie in Abschnitt 6.3 und leiten die Gleichungen aus (6.22) ab. Dann erhalten wir

$$A'(\tau) \cdot DF_1(\tau) + j'(\tau) \cdot DJ_1(\tau) = 0. \tag{6.23}$$

Da wir $j'(\tau)$ mit Hilfe von Formel (6.9) berechnen können, können wir durch Umformung von Gleichung (6.23) mit folgender Formel den Wert von $A'(\tau)$ berechnen:

$$A'(\tau) = \frac{-j'(\tau) \cdot DJ_1(\tau)}{DF_1(\tau)}.$$

Anschließend leiten wir die Gleichung $G_l(A(\tau), j(l\tau)) = 0$ ab und erhalten so

$$A'(\tau) \cdot DF_2(\tau) + l \cdot j'(l\tau) \cdot DJ_2(\tau) = 0, \tag{6.24}$$

wobei $DF_2(\tau)$ bzw. $DJ_2(\tau)$ der Wert der partiellen Ableitung von $G_l(X,Y)$ nach $X$ bzw. $Y$, ausgewertet an der Stelle $(A(\tau), j(l\tau))$, ist. Damit können wir den Wert von $j'(l\tau)$ ausrechnen:

$$j'(l\tau) \quad = \quad \frac{-A'(\tau) \cdot DF_2(\tau)}{l \cdot DJ_2(\tau)}.$$

Hiermit haben wir die Berechnung von $E_4(l\tau)$ und $E_6(l\tau)$ schon fast erledigt. Aus der Formel (6.10) und den Formeln (6.3) und (6.4) wissen wir

$$\frac{j'(l\tau)}{j(l\tau)} \quad = \quad -\frac{E_6(l\tau)}{E_4(l\tau)} \qquad \text{und} \qquad \frac{j(l\tau)}{j(l\tau)-1728} \quad = \quad \frac{E_4^3(l\tau)}{E_6^2(l\tau)}.$$

Damit ergibt sich die folgende Formel zur Berechnung von $E_4(l\tau)$

$$E_4(l\tau) \quad = \quad \frac{j(l\tau)}{j(l\tau)-1728} \cdot \left(\frac{j'(l\tau)}{j(l\tau)}\right)^2 \quad = \quad \frac{j'^2(l\tau)}{(j(l\tau)-1728) \cdot j(l\tau)}.$$

Danach können wir durch Einsetzen des gerade berechneten Wertes von $E_4(l\tau)$ auch leicht den Wert von $E_6(l\tau)$ berechnen. Damit verbleibt also nur noch die Berechnung von $E_2^*(\tau)$.

### 6.4.2 Berechnung von $E_2^*(\tau)$

Zur Herleitung einer Formel zur Bestimmung von $E_2^*(\tau)$ leiten wir die beiden Gleichungen aus (6.22) zweimal ab. Dazu definieren wir für $(x_1, y_1) = (A(\tau), j(\tau))$ und $(x_2, y_2) = (A(\tau), j(l\tau))$ folgende weitere Hilfswerte $(i = 1, 2)$

$$\begin{aligned}
DFF_i(\tau) \quad &:= \quad \left(\frac{d}{dX^2} G_l(X,Y)\right)(x_i, y_i), \\
DJJ_i(\tau) \quad &:= \quad \left(\frac{d}{dY^2} G_l(X,Y)\right)(x_i, y_i), \\
DFJ_i(\tau) \quad &:= \quad \left(\frac{d}{dX\,dY} G_l(X,Y)\right)(x_i, y_i) \quad = \quad \left(\frac{d}{dY\,dX} G_l(X,Y)\right)(x_i, y_i).
\end{aligned}$$

Dann erhalten wir die beiden neuen Gleichungen

$$\begin{aligned}
&A''(\tau) \cdot DF_1(\tau) \;+\; j''(\tau) \cdot DJ_1(\tau) \;+\; A'(\tau) \cdot [A'(\tau) \cdot DFF_1(\tau) \;+\; j'(\tau) \cdot DFJ_1(\tau)] \\
&\qquad + j'(\tau) \cdot [A'(\tau) \cdot DFJ_1(\tau) \;+\; j'(\tau) \cdot DJJ_1(\tau)] \quad = \quad 0,
\end{aligned} \tag{6.25}$$

$$\begin{aligned}
&A''(\tau) \cdot DF_2(\tau) \;+\; l^2 \cdot j''(l\tau) \cdot DJ_2(\tau) \\
&\qquad + A'(\tau) \cdot [A'(\tau) \cdot DFF_2(\tau) \;+\; l \cdot j'(l\tau) \cdot DFJ_2(\tau)] \\
&\qquad + l \cdot j'(l\tau) \cdot [A'(\tau) \cdot DFJ_2(\tau) \;+\; l \cdot j'(l\tau) \cdot DJJ_2(\tau)] \quad = \quad 0.
\end{aligned} \tag{6.26}$$

Diese beiden Gleichungen (6.25) und (6.26) enthalten die zweiten Ableitungen der Funktionen $A(\tau)$, $j(\tau)$ und $j(l\tau)$. Um den Wert von $E_2^*(\tau)$ berechnen zu können, benötigen wir daher eine Beziehung zwischen $j''(\tau)$ und $E_2(\tau)$. Diese können wir herleiten, indem wir Gleichung (6.9) ableiten und anschließend die Formeln (6.5), (6.6) und (6.7) benutzen. Dann erhalten wir

$$\begin{aligned} j''(\tau) &= \frac{\Delta'(\tau)\cdot E_4^2(\tau)\cdot E_6(\tau) - \Delta(\tau)\cdot\Big(2\,E_4(\tau)\cdot E_4'(\tau)\cdot E_6(\tau) + E_4^2(\tau)\cdot E_6'(\tau)\Big)}{\Delta^2(\tau)} \\ &= \frac{1}{\Delta(\tau)}\Bigg(E_2(\tau)\cdot E_4^2(\tau)\cdot E_6(\tau) - \frac{2}{3}\,E_4(\tau)\cdot E_6(\tau)\cdot\Big(E_2(\tau)\cdot E_4(\tau) - E_6(\tau)\Big) \\ &\qquad -\frac{1}{2}\,E_4^2(\tau)\cdot\Big(E_2(\tau)\cdot E_6(\tau) - E_4^2(\tau)\Big)\Bigg) \\ &= \frac{-E_2(\tau)\cdot E_4^2(\tau)\cdot E_6(\tau)}{6\,\Delta(\tau)} + \frac{\frac{2}{3}\,E_4(\tau)\cdot E_6^2(\tau) + \frac{1}{2}\,E_4^4(\tau)}{\Delta(\tau)} \\ &= \frac{E_2(\tau)\cdot j'(\tau)}{6} + \frac{2\,E_4(\tau)\cdot E_6^2(\tau)}{3\,\Delta(\tau)} + \frac{j(\tau)\cdot E_4(\tau)}{2}. \end{aligned} \tag{6.27}$$

Mit einer analogen Rechnung erhalten wir die folgende Gleichung für $j''(l\tau)$

$$j''(l\tau) = \frac{E_2(l\tau)\cdot j'(l\tau)}{6} + \frac{2\,E_4(l\tau)\cdot E_6^2(l\tau)}{3\,\Delta(l\tau)} + \frac{j(l\tau)\cdot E_4(l\tau)}{2}. \tag{6.28}$$

Damit können wir durch einfache Rechnungen den Wert von $E_2^*(\tau)$ bestimmen, wenn wir den Wert von

$$\frac{j''(\tau)}{j'(\tau)} - l\,\frac{j''(l\tau)}{j'(l\tau)} \tag{6.29}$$

kennen. Dividieren wir nämlich Gleichung (6.27) durch $j'(\tau)$, so erhalten wir

$$\frac{j''(\tau)}{j'(\tau)} = \frac{E_2(\tau)}{6} + \frac{2\,E_4(\tau)\cdot E_6^2(\tau)}{3\,\Delta(\tau)\cdot j'(\tau)} + \frac{j(\tau)\cdot E_4(\tau)}{2\,j'(\tau)}.$$

Analog erhalten wir aus (6.28)

$$\frac{j''(l\tau)}{j'(l\tau)} = \frac{E_2(l\tau)}{6} + \frac{2\,E_4(l\tau)\cdot E_6^2(l\tau)}{3\,\Delta(l\tau)\cdot j'(l\tau)} + \frac{j(l\tau)\cdot E_4(l\tau)}{2\,j'(l\tau)}.$$

Damit gilt

$$\begin{aligned} &\frac{j''(\tau)}{j'(\tau)} - l\,\frac{j''(l\tau)}{j'(l\tau)} = \\ &\frac{1}{6}\underbrace{\Big(E_2(\tau) - l\cdot E_2(l\tau)\Big)}_{=E_2^*(\tau)} + \frac{2\,E_4(\tau)\cdot E_6^2(\tau)}{3\,\Delta(\tau)\cdot j'(\tau)} + \frac{j(\tau)\cdot E_4(\tau)}{2\,j'(\tau)} \\ &- l\cdot\left[\frac{2\,E_4(l\tau)\cdot E_6^2(l\tau)}{3\,\Delta(l\tau)\cdot j'(l\tau)} + \frac{j(l\tau)\cdot E_4(l\tau)}{2\,j'(l\tau)}\right]. \end{aligned}$$

Durch eine einfache Umformung erhalten wir hieraus den Wert von $E_2^*(\tau)$. Damit verbleibt die Bestimmung des Wertes aus (6.29). Alle anderen Funktionswerte, die in dieser Gleichung vorkommen, sind zu diesem Zeitpunkt bekannt. Aus (6.23) erhalten wir nach einer einfachen Umformung die Gleichung

$$DJ_1(\tau) \quad = \quad \frac{-A'(\tau)}{j'(\tau)} \cdot DF_1(\tau).$$

Setzen wir diese Gleichung in (6.25) ein, so können wir durch Zusammenfassen und Ausrechnen offensichtlich den Wert von

$$W_1(\tau) \quad := \quad \frac{A''(\tau)}{A'(\tau)} - \frac{j''(\tau)}{j'(\tau)}$$

berechnen. Auf dieselbe Art können wir aus (6.24) die Gleichung

$$DJ_2(\tau) \quad = \quad \frac{-A'(\tau)}{l \cdot j'(l\tau)} \cdot DF_2(\tau)$$

folgern. Durch Einsetzen in (6.26) und Zusammenfassen erhalten wir daraus den Wert von

$$W_2 \quad = \quad \frac{A''(\tau)}{A'(\tau)} - l\,\frac{j''(l\tau)}{j'(l\tau)}.$$

Durch einfache Kombination dieser beiden Resultate erhalten wir den gesuchten Wert aus (6.29) als

$$W_2 - W_1 \quad = \quad \frac{j''(\tau)}{j'(\tau)} - l\,\frac{j''(l\tau)}{j'(l\tau)}.$$

Somit sind wir in der Lage, auch den Wert von $E_2^*(\tau)$ zu berechnen. Damit haben wir auch für diese Art von äquivalentem Polynom gezeigt, wie wir die Werte von $E_4(l\tau), E_6(l\tau)$ und $E_2^*(\tau)$ bestimmen können.

Damit haben wir beschrieben, wie wir für den Körper der komplexen Zahlen Teiler des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$ bestimmen können. Im folgenden Kapitel werden wir untersuchen, ob wir diese Formeln auf endliche Körper übertragen können. Für endliche Körper „genügend großer“ Charakteristik werden wir so einen Algorithmus erhalten, um die Spur des Frobenius-Endomorphismus modulo einer ungeraden Primzahl $l$ exakt zu berechnen.

# Kapitel 7

# Der Algorithmus von Elkies für endliche Körper

Der schon im vorherigen Kapitel erwähnte Algorithmus von Schoof [Sc85] bestimmt für Primzahlen $l$ die Gruppenordnung einer elliptischen Kurve modulo $l$. Wegen der dabei auftretenden großen Polynomgrade von $\approx (l^2-1)/2$ ist dieser Algorithmus in der Praxis nur schlecht einsetzbar. Wir haben im letzten Kapitel beschrieben, wie wir für den Körper der komplexen Zahlen Polynome vom Grad $(l-1)/2$ berechnen können, die Teiler des $l$-ten Divisionspolynoms sind. In diesem Kapitel werden wir zuerst beschreiben, unter welchen Voraussetzungen solche Polynome für endliche Körper existieren. Danach werden wir angeben, wann wir die im vorherigen Kapitel angegebenen Formeln auf endliche Körper übertragen können. Im abschließenden Kapitel beschreiben wir einen Algorithmus, wie wir mit Hilfe eines solchen Polynoms die Spur des Frobenius-Endomorphismus modulo $l$ exakt berechnen können. Außerdem beschreiben wir einige Aspekte unserer Implementierung und geben praktische Laufzeiten an.

## 7.1 Existenz eines Teilers des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$

Sei im folgenden $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$ der Charakteristik $p$. Das $l$-te Divisionspolynom zu $E$ kann nach den in Kapitel 4 gemachten Bemerkungen auch auf folgende Art und Weise geschrieben werden:

$$\psi_l(X) \quad = \quad l \prod_{\pm P \in E[l]-\{\mathcal{O}\}} \Big(X - x(P)\Big) \quad \in \ \mathbb{F}_q[X].$$

Sei $C$ eine beliebige $l$-Gruppe von $E(\overline{\mathbb{F}}_q)$. Wir betrachten dann in Analogie zum vorherigen Kapitel das folgende „zu $C$ gehörende“ Polynom

$$f_C(X) \quad = \quad \prod_{\pm P \in C-\{\mathcal{O}\}} \Big(X - x(P)\Big). \tag{7.1}$$

Dieses Polynom ist nach Definition sicherlich ein Teiler des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$. Wir untersuchen nun, wann dieses Polynom $f_C(X)$ über $\mathbb{F}_q$ definiert ist.

Ist die $l$-Gruppe $C$ invariant unter $\Phi_E$, so wird $f_C(X)$ bei Anwendung des Frobenius-Automorphismus für den endlichen Körper $\mathbb{F}_q$ in sich selbst überführt, denn alle Nullstellen von $f_C(X)$ sind $x$-Koordinaten von Punkten aus $C$ und diese werden unter $\Phi_E$ in Punkte aus $C$ abgebildet. Damit ist in diesem Fall das Polynom $f_C(X)$ über $\mathbb{F}_q$ definiert.

Nehmen wir an, $C$ ist nicht unter $\Phi_E$ invariant. Falls dann $f_C(X)$ über $\mathbb{F}_q$ definiert wäre, so würde der Frobenius-Automorphismus für $\mathbb{F}_q$ die Nullstellen von $f_C(X)$ aufeinander abbilden. Insbesondere würde damit die $x$-Koordinate eines beliebigen Punktes aus $C$ auf die $x$-Koordinate eines anderen Punktes aus $C$ abgebildet werden. Da es zu fester $x$-Koordinate nur zwei mögliche $y$-Koordinaten gibt und beide zugehörigen Punkte Elemente der $l$-Gruppe $C$ sind, wäre dann die $l$-Gruppe $C$ invariant unter $\Phi_E$; ein Widerspruch zu unserer Voraussetzung.

Damit gibt es genau dann ein solches über $\mathbb{F}_q$ definiertes Polynom $f_C(X)$, wenn die zugehörige $l$-Gruppe $C$ invariant unter $\Phi_E$ ist. Die Existenz einer solchen $l$-Gruppe können wir mit Hilfe der äquivalenten Polynome leicht überprüfen. Nach Korollar 3.12 und Satz 4.13 gibt es eine solche $l$-Gruppe genau dann, wenn das zugehörige äquivalente Polynom für $E$ mindestens eine Nullstelle in $\mathbb{F}_q$ besitzt.

## 7.2 Übertragung der Formeln für komplexe Zahlen auf endliche Körper

Wir haben im letzten Kapitel 6 Formeln hergeleitet, wie wir für elliptische Kurven über den komplexen Zahlen einen Teiler des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$ bestimmen können. In diesem Abschnitt werden wir zeigen, wie wir diese Formeln auf endliche Körper $\mathbb{F}_q$ hinreichend großer Charakteristik $p$ übertragen können, um einen solchen Teiler über $\mathbb{F}_q$ zu bestimmen. Dabei sollen exakt dieselben Formeln wie in Kapitel 6 verwendet werden; nun aber als Formeln über dem Körper $\mathbb{F}_q$ angesehen werden.

Wir nehmen im folgenden an, daß die schon in Korollar 3.12 (Seite 32) gestellten Voraussetzungen an $E$ erfüllt sind, d.h. $E$ ist nicht supersingulär und es existiert keine über $\mathbb{F}_q$ definierte Isogenie von $E$ zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728. Dies wird im Gesamtalgorithmus, den wir in Kapitel 10 vorstellen werden, im ersten Schritt überprüft werden. Desweiteren setzen wir voraus, daß wir eine Nullstelle des reduzierten äquivalenten Polynoms $\overline{G_l}(X, j(E))$ in $\mathbb{F}_q$ kennen (beachte die Existenz einer solchen Nullstelle). Sei $C$ die zu dieser Nullstelle „gehörende" unter $\Phi_E$ invariante $l$-Gruppe. Zuerst untersuchen wir das Problem der Bestimmung der Koeffizienten von $E/C$ und des zweithöchsten Koeffizienten $P_1$ des Polynoms $f_C(X)$ (vgl. Abschnitt 6.2).

**Satz 7.1** *Sei $E$ eine ordinäre elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$ mit Charakteristik $p > l$, die nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist. Sei $\overline{g} \in \mathbb{F}_q$ eine Nullstelle von $\overline{G_l}(X, j(E)) \in \mathbb{F}_q[X]$ für das äquivalente Polynom $G_l(X,Y)$ aus Abschnitt 5.2. Dann können wir durch Übertragung der Formeln aus Abschnitt 6.3 maximal zwei Möglichkeiten für das Tripel $(E/C, P_1)$ bestimmen, wobei $C$ eine unter $\Phi_E$ invariante $l$-Gruppe von $E(\overline{\mathbb{F}}_q)$ ist.*

**Beweis:** Wir fassen alle in Abschnitt 6.3 angegebenen Formeln als rationale Formeln über den ganzen Zahlen in den Variablen $a$, $b$ und $g = g(\tau)$ auf. Anschließend untersuchen wir alle diese Formeln unter Anwendung der kanonischen Reduktionsabbildung $^{-} : \mathbb{Z}(a,b,g) \to \mathbb{F}_p(a,b,g)$. Im folgenden bezeichnen wir die reduzierte Formeln als $\Delta$ (für $\Delta(\tau)$) und $\Delta^{(l)}$ (für $\Delta(l\tau)$) etc. .

Wir müssen zuerst zeigen, daß kein Fehler auftritt, wenn wir die reduzierten Formeln an der Stelle $(\overline{a}, \overline{b}, \overline{g})$ auswerten. Dabei sei $E = (\overline{a}, \overline{b}) \in \mathbb{F}_q^2$ die vorgegebene elliptische Kurve. Dazu beachten wir die folgenden Eigenschaften:

1. $E$ ist nach Voraussetzung nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728, d.h. insbesondere ist damit $j(E)$ ungleich 0 und 1728 und somit $\overline{a} \cdot \overline{b} \neq 0$. Daraus erhalten wir direkt die Eigenschaft $E_4 \cdot E_6 \neq 0$. Aus der Voraussetzung und Lemma 4.20 folgt weiterhin $\overline{g} \neq 0$.

2. Anhand der Formeln von Seite 92 erkennen wir dann, daß auch $j' \cdot \Delta \cdot \Delta^{(l)} \neq 0$ ist.

3. Wegen Lemma 4.14 besitzt das $l$-te modulare Polynom und somit auch das äquivalente Polynom keine doppelte Nullstelle, so daß die partielle Ableitung nach X, ausgewertet an der Stelle $(\overline{g}, j(E))$ (d.h. $DF$), ungleich Null ist. Dazu beachten wir noch, daß das äquivalente Polynom den Grad $l+1$ in $X$ hat und außerdem normiert ist, so daß der höchste Koeffizient der partiellen Ableitung nach $X$ sicherlich nicht Null modulo $p$ ist.

Damit erkennt man leicht, daß sich alle Rechnungen aus Abschnitt 6.3 direkt übertragen lassen, wenn der Wert von $DJ \neq 0$ ist. Bei allen Rechnungen kann dann kein Fehler durch Division durch Null auftreten. Somit wird genau ein Tripel $(E/C, P_1)$ bestimmt.

Ist $DJ = 0$, so erhalten wir aus (6.17) direkt $E_2^* = 0$. Nun wenden wir Formel (6.20) an und erhalten so $E_4^{(l)} = l^{-2} \cdot E_4$. Da wir mit $\Delta$ und der Nullstelle $\overline{g}$ mit Hilfe von Lemma 6.8 den Wert $\Delta^{(l)}$ berechnen können, reicht dies aus, um mit Formel (6.2) das Quadrat von $E_6^{(l)}$ zu bestimmen. Damit haben wir genau zwei mögliche Werte für $E_6^{(l)}$. Insgesamt ergeben sich also in diesem Fall maximal zwei mögliche Tripel $(E/C, P_1)$.

Um zu zeigen, daß die mit Hilfe der reduzierten Formeln berechneten Werte dieselbe Bedeutung besitzen wie im Fall des komplexen Körpers, benutzen wir dieselbe Technik wie im Beweis von Satz 4.13. Im Falle des komplexen Körpers können wir die Kurve $E/C$ und damit auch die $j$-Invariante $j/C$ als rationale Funktion über

$\mathbb{Z}(a,b,g)$ auffassen. Diese rationale Funktion reduzieren wir mit obiger Reduktionsabbildung. Beachten wir, daß $j/C$ eine Nullstelle des $l$-ten modularen Polynoms über $\mathbb{C}$ ist, so ergibt sich hieraus, daß die reduzierten rationalen Funktionen eine Nullstelle des reduzierten $l$-ten modularen Polynoms liefern, d.h. wir erhalten mit Hilfe der reduzierten Formeln ebenfalls eine $j$-Invariante $j/C$. Damit liefern die reduzierten Formeln im Falle des endlichen Körpers die Koeffizienten einer elliptischen Kurve $E/C$ für eine unter $\Phi_E$ invariante $l$-Gruppe $C$ (beachte, daß die Nullstelle $\overline{g} \in \mathbb{F}_q$ liegt). Auch $P_1$ besitzt für komplexe und endliche Körper dieselbe Bedeutung. In beiden Fällen ist $P_1$ genau der zweithöchste Koeffizient des Polynoms $f_C(X)$. Der zweithöchste Koeffizient von $f_C(X)$ ist genau die Summe aller verschiedenen $x$-Koordinaten der nichttrivialen Punkte der $l$-Gruppe $C$. Fassen wir diese wieder als rationale Funktion auf und reduzieren wir dann diese Funktion, so folgt die Aussage, daß $P_1$ in beiden Fällen dieselbe Bedeutung besitzt. ■

**Bemerkung 7.2** Wir sollten beachten, daß der Fall $DJ = 0$ in der Praxis auftreten kann. Als Beispiel wählen wir $p = 65537$ und die elliptische Kurve $E = (1, 33965)$ über $\mathbb{F}_p$. Diese Kurve besitzt Gruppenordnung $\#E(\mathbb{F}_p) = 65592$ (d.h. $c = -54$); die Voraussetzungen an die Kurve sind damit erfüllt. Für $l = 19$ besitzt das zugehörige äquivalente Polynom den Zerfällungstyp $(1\,1\,9\,9)$; es gibt also zwei unter $\Phi_E$ invariante $l$-Gruppen. Die zugehörigen Nullstellen des äquivalenten Polynoms sind $g_1 = 24273$ und $g_2 = 1616$. Wählen wir die Nullstelle $g_1$, so ergibt sich der Wert $DJ = 0$. Dann erhalten wir zwei Möglichkeiten für $(E/C, P_1)$. Wählen wir dagegen als Nullstelle $g_2$, so ist $DJ = 6974$ und die Berechnung verläuft ohne Probleme. Insgesamt erhalten wir dann den korrekten Wert $c \equiv 3 \bmod 19$.

Bemerkung 7.2 legt schon eine alternative Strategie zum Umgang mit dem Fall $DJ = 0$ dar. Tritt dieser Fall auf, so können wir zuerst eine weitere Nullstelle des äquivalenten Polynoms $\overline{G_l}(X, j(E))$ in $\mathbb{F}_q$ benutzen (falls eine solche existiert) und testen, ob wir damit $(E/C, P_1)$ eindeutig bestimmen können.

Damit können wir den folgenden Algorithmus angeben, der die Formeln aus Abschnitt 6.3 auf endliche Körper überträgt. Die Ausgabe dieses Algorithmus ist in der Form wie in Abschnitt 6.2 verlangt. Den dort vorgestellten Algorithmus zur Bestimmung eines Teilers des $l$-ten Divisionspolynoms übertragen wir in Algorithmus 7.8; dort werden wir die Ausgabe des nun vorzustellenden Algorithmus als Eingabe verwenden.

**Algorithmus 7.3** [Bestimmung von $\tilde{a}, \tilde{b}$ analog zu Abschnitt 6.3]

**Eingabe:** elliptische Kurve $E = (a, b) \in \mathbb{F}_q^2$, Nullstelle $g \in \mathbb{F}_q$ von $\overline{G}_l(X, j(E))$, $s \in \mathbb{N}$ (vgl. Abschnitte 5.1, 5.2).
**Ausgabe:** Menge möglicher Werte für $(E/C, P_1) = (\tilde{a}, \tilde{b}, P_1)$.

| | | |
|---|---|---|
| Berechne $E_4 \leftarrow -3^{-1} \cdot a$, $E_6 \leftarrow -2^{-1} \cdot b$, $\Delta \leftarrow 1728^{-1} \cdot (E_4^3 - E_6^2)$ und $\Delta^{(l)} \leftarrow l^{-12} \cdot \Delta \cdot g^{12/s}$. | | (1) |
| Berechne $DF$ und $DJ$ (analog zu Seite 99). | | (2) |
| IF $DJ = 0$ /* Spezialfall */ | | (3) |
| THEN | Setze $E_4^{(l)} \leftarrow l^{-2} \cdot E_4$ und $\tilde{a} \leftarrow -3 \cdot l^4 \cdot E_4^{(l)}$. | (4) |
| | Berechne $j^{(l)} \leftarrow \left(E_4^{(l)}\right)^3 \cdot \left(\Delta^{(l)}\right)^{-1}$. | (5) |
| | RETURN $\left\{\left(\tilde{a},\ \pm 2 \cdot l^6 \cdot \sqrt{(j^{(l)} - 1728) \cdot \Delta^{(l)}},\ 0\right)\right\}$. | (6) |
| ELSE | Berechne $E_2^* \leftarrow -(12/s) \cdot E_6 \cdot DJ \cdot (E_4 \cdot DF)^{-1}$. | (7) |
| | Berechne $E_0 \leftarrow E_6 \cdot (E_4 \cdot E_2^*)^{-1}$. | (8) |
| | Berechne $g' \leftarrow -(s/12) \cdot E_2^* \cdot g$ und $j' \leftarrow -E_4^2 \cdot E_6 \cdot \Delta^{-1}$. | (9) |
| | Berechne $DF'$ und $DJ'$ (analog zu Seite 101). | (10) |
| | Berechne $E_0' \leftarrow ((-s/12) \cdot DF' - E_0 \cdot DJ') \cdot DJ^{-1}$. | (11) |
| | Berechne $E_4^{(l)} \leftarrow l^{-2} \cdot \Big(E_4 - E_2^* \cdot [12\, E_0' \cdot E_0^{-1} + 6\, E_4^2 \cdot E_6^{-1} - 4\, E_6 \cdot E_4^{-1}] + (E_2^*)^2\Big)$. | (12) |
| | Berechne $j^{(l)} \leftarrow \left(E_4^{(l)}\right)^3 \cdot \left(\Delta^{(l)}\right)^{-1}$. | (13) |
| | Berechne $f \leftarrow l^s \cdot g^{-1}$ und $f' \leftarrow (s/12) \cdot E_2^* \cdot f$. | (14) |
| | Berechne $DF_2 \leftarrow \left(\frac{d}{dX} G_l(X, Y)\right)\left(f, j^{(l)}\right)$ und $DJ_2 \leftarrow \left(\frac{d}{dY} G_l(X, Y)\right)\left(f, j^{(l)}\right)$. | (15) |
| | Berechne $j^{(l)\prime} \leftarrow -l^{-1} \cdot f' \cdot DF_2 \cdot DJ_2^{-1}$. | (16) |
| | Berechne $E_6^{(l)} \leftarrow -E_4^{(l)} \cdot j^{(l)\prime} \cdot \left(j^{(l)}\right)^{-1}$. | (17) |
| | Setze $\tilde{a} \leftarrow -3 \cdot l^4 \cdot E_4^{(l)}$, $\tilde{b} \leftarrow -2 \cdot l^6 \cdot E_6^{(l)}$ und $P_1 \leftarrow -l \cdot 2^{-1} \cdot E_2^*$. | (18) |
| | RETURN $\left\{(\tilde{a},\ \tilde{b},\ P_1)\right\}$. | (19) |

Man beachte, daß es sich bei der Quadratwurzel in Schritt (6) natürlich um eine Wurzel in $\mathbb{F}_q$ handelt. Eine ähnliche Aussage wie in Satz 7.1 können wir auch für das äquivalente Polynom zu der in Abschnitt 5.3 eingeführten Funktion $A(\tau)$ formulieren. Dazu untersuchen wir die über den komplexen Zahlen gefundenen Formeln aus Abschnitt 6.4. Wir verwenden dabei dieselbe Bezeichnungsweise wie im Beweis zum vorherigen Satz.

**Satz 7.4** *Sei $E$ eine ordinäre elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$ mit Charakteristik $p > l$, die nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist. Sei $\overline{A} \in \mathbb{F}_q$ eine Nullstelle von $G_l(X, j(E)) \in \mathbb{F}_q[X]$ für das äquivalente Polynom $G_l(X,Y)$ aus Abschnitt 5.4. Ist $DJ_1 \neq 0$, so erhalten wir durch Übertragung der Formeln aus Abschnitt 6.4 eine Menge von Möglichkeiten für $(E/C, P_1)$. Ein Element dieser Menge besteht tatsächlich aus den Koeffizienten einer Kurve $E/C$ für eine unter $\Phi_E$ invarianten $l$-Gruppe $C$ und der Summe $P_1$ aller verschiedenen $x$-Koordinaten von nichttrivialen Punkten aus $C$.*

**Beweis:** Wir gehen ähnlich vor wie im Beweis zu Satz 7.1; insbesondere verwenden wir dieselbe Bezeichnungsweise wie in diesem Beweis. Wir untersuchen dann, ob wir die reduzierten Formeln immer ohne Fehler an der Stelle $(\overline{a}, \overline{b}, \overline{A})$ auswerten können (sei dazu $E = (\overline{a}, \overline{b})$):

1. Nach Voraussetzung gilt, daß die Koeffizienten $\overline{a}$ und $\overline{b}$ der Kurve $E$ beide ungleich Null sind. Damit sind auch $E_4$ und $E_6$ nicht Null.

2. Da die elliptische Kurve $E$ nicht $\mathbb{F}_q$-isogen zu einer Kurve mit $j$-Invariante 0 oder 1728 ist, besitzt das äquivalente Polynom $\overline{G}_l(X, j(E))$ wegen Lemma 4.14 keine doppelte Nullstelle. Damit ist $DF_1 \neq 0$ und $DF_2 \neq 0$. Nach Voraussetzung ist außerdem auch $DJ_1$ ungleich Null.

Damit können wir aus (6.24) folgern, daß $A'$, $j^{(l)\prime}$ und $DJ_2$ nicht Null sind. Also sind $E_4^{(l)}$ und $E_6^{(l)}$ berechenbar und es kann bei dieser Berechnung kein Fehler auftreten. Dabei beachte man, daß die Möglichkeiten $j^{(l)} = 0$ oder $j^{(l)} = 1728$ nach Voraussetzung nicht auftreten können (und damit natürlich auch nicht bei der „zufälligen Wahl" von $j^{(l)}$ berücksichtigt werden). Wegen $A' \neq 0$ sind auch die Formeln (6.25) und (6.26) anwendbar, um die Werte $W_1$ und $W_2$ auszurechnen. Dabei kann bei der Berechnung von $E_2^*$ ebenfalls kein Fehler auftreten, denn alle Werte im Nenner sind ungleich Null, wie man leicht sieht.

Die Tatsache, daß die mit Hilfe der reduzierten Formeln berechneten Werte dieselbe Bedeutung besitzen wie im komplexen Fall (falls wir den Wert $j^{(l)}$ als $j$-Invariante einer elliptischen Kurve $E/C$ für eine $l$-Gruppe $C$ von $E$ korrekt gewählt haben), kann mit derselben Technik wie im Beweis zu Satz 7.1 gezeigt werden (betrachte wieder rationale Funktionen). Die letzte Aussage des Satzes folgt direkt aus der angewandten Vorgehensweise. ■

**Bemerkung 7.5** Auch in diesem Fall ist die Voraussetzung, daß $DJ_1 \neq 0$ sein muß, notwendig. Als Beispiel betrachte man diesmal die elliptische Kurve $E = (1, 22476)$ über dem Primkörper $\mathbb{F}_{65537}$. Diese Kurve besitzt Gruppenordnung 65294 und erfüllt die Voraussetzungen an die elliptische Kurve. Der Zerfällungstyp des 53-ten äquivalenten Polynoms ist $(1\,53)$, die Nullstelle in $\mathbb{F}_{65537}$ ist $A = 6627$. Für diesen Wert von $A$ besitzt das äquivalente Polynom $\overline{G}_{53}(A, Y) \in \mathbb{F}_{65537}[Y]$ die doppelte Nullstelle $j(E) = 41621$, so daß für diese Kurve $DJ_1 = 0$ gilt. Damit scheitert in diesem Fall die Berechnung.

Somit können wir auch für diese äquivalente Polynome die Formeln aus Abschnitt 6.4 übertragen, wenn $DJ_1 \neq 0$ ist. Im Gegensatz zu Algorithmus 7.3 erhalten wir in diesem Fall eine Liste von Möglichkeiten für $\tilde{a}, \tilde{b}$ und $P_1$ (wie in Abschnitt 6.4 schon erwähnt). Alle diese möglichen Werte werden als Eingabe von Algorithmus 7.8 verwendet werden. Dort wird mit Hilfe dieser Werte ein Polynom vom Grad $(l-1)/2$ bestimmt und dann überprüft, ob dies ein Teiler des $l$-ten Divisionspolynoms ist. Wir erhalten dann den folgenden Algorithmus:

**Algorithmus 7.6** [Bestimmung von $\tilde{a}, \tilde{b}$ analog zu Abschnitt 6.4]

**Eingabe:** elliptische Kurve $E = (a, b) \in \mathbb{F}_q^2$, Nullstelle $A \in \mathbb{F}_q$ des reduzierten äquivalenten Polynoms $\overline{G}_l(X, j(E))$ (wie in Abschnitt 5.4).

**Ausgabe:** Menge von Möglichkeiten für $(E/C, P_1) = (\tilde{a}, \tilde{b}, P_1)$.

| | |
|---|---|
| Bestimme alle Nullstellen $j_1, \dots j_k \in \mathbb{F}_q$ von $\overline{G}_l(A, Y)/(Y - j(E)) \in \mathbb{F}_q[Y]$. | (1) |
| Setze $E_4 \leftarrow -3^{-1} \cdot a$, $E_6 \leftarrow -2^{-1} \cdot b$, $\Delta \leftarrow 1728^{-1} \cdot (E_4^3 - E_6^2)$ und $j' \leftarrow -E_4^2 \cdot E_6 \cdot \Delta^{-1}$. | (2) |
| Bestimme $DF_1$, $DJ_1$ und $A'$ (vgl. Seite 103). | (3) |
| Bestimme $DFF_1, DJJ_1, DFJ_1$ (vgl. Seite 104). | (4) |
| Setze $L \leftarrow \emptyset$. | (5) |
| FOR $s = 1, \dots, k$ | (6) |
| IF $j_s = 0$ oder $j_s = 1728$ | (7) |
| THEN Fahre mit FOR-Schleife fort. | (8) |
| Setze $j^{(l)} \leftarrow j_s$. /* alle Rechnungen nun mit Nullstelle $j_s$ */ | (9) |
| Bestimme $DF_2$, $DJ_2$ und $j^{(l)'}$ (analog zu (6.24)). | (10) |
| Bestimme $E_4^{(l)} \leftarrow \left(j^{(l)'}\right)^2 \cdot \left((j^{(l)} - 1728) \cdot j^{(l)}\right)^{-1}$ und $E_6^{(l)} \leftarrow -j^{(l)'} \cdot E_4^{(l)} \cdot \left(j^{(l)}\right)^{-1}$. | (11) |
| Berechne $DFF_2, DJJ_2, DFJ_2$ (vgl. Seite 104). | (12) |
| Bestimme $W_1$ und $W_2$ mit Formel (6.25) und (6.26). | (13) |
| Bestimme $E_2^* \leftarrow 6 \cdot (W_2 - W_1) - 4\, E_4 \cdot E_6^2 \cdot (\Delta \cdot j')^{-1} - 3\, j \cdot E_4 \cdot j'^{-1} + l \cdot \left[4\, E_4^{(l)} \cdot \left(E_6^{(l)}\right)^2 \cdot \left(\Delta^{(l)}\right)^{-1} \cdot \left(j^{(l)'}\right)^{-1} + 3\, j^{(l)} \cdot E_4^{(l)} \cdot \left(j^{(l)'}\right)^{-1}\right]$. | (14) |
| Setze $L \leftarrow L \bigcup \left\{\left(-3 \cdot l^4 \cdot E_4^{(l)}, -2 \cdot l^6 \cdot E_6^{(l)}, -l \cdot 2^{-1} \cdot E_2^*\right)\right\}$. | (15) |
| RETURN $L$. | (16) |

Mit Hilfe der letzten beiden Sätze haben wir Algorithmen beschrieben, um mögliche Werte $\tilde{a}, \tilde{b}$ und $P_1$ analog zu den Abschnitten 6.3 und 6.4 zu bestimmen. Nun beschreiben wir, wie wir daraus wirklich ein Polynom $f_C(X) \in \mathbb{F}_q[X]$ vom Grad $(l-1)/2$ bestimmen können, das ein Teiler des $l$-ten Divisionspolynoms ist. In Abschnitt 6.2 haben wir beschrieben, wie wir ein solches Polynom über den komplexen Zahlen bestimmen können. In dem folgenden Satz werden wir auch diese Formeln auf den Fall endlicher Körper übertragen.

**Satz 7.7** *Angenommen, wir kennen für eine elliptische Kurve $E/\mathbb{F}_q$ die Werte $(E/C,\ P_1) \in \mathbb{F}_q^3$, wobei $C$ eine unter $\Phi_E$ invariante $l$-Gruppe von $E(\overline{\mathbb{F}}_q)$ und $P_1$ die Summe aller verschiedenen $x$-Koordinaten von nichttrivialen Punkten aus $C$ ist. Ist die Charakteristik $p$ von $\mathbb{F}_q$ größer als $l$, so können die Formeln aus Abschnitt 6.2 modulo $p$ reduziert werden. Insbesondere ist es mit Hilfe dieser Formeln möglich, einen Teiler $f_C(X) \in \mathbb{F}_q[X]$ des $l$-ten Divisionspolynoms vom Grad $(l-1)/2$ zu bestimmen.*

**Beweis:** Zuerst beachte man, daß wir zur Bestimmung der Koeffizienten des Polynoms $f_C(X)$ wie in Abschnitt 6.2 beschrieben die unendlichen Summen nur mit endlicher Präzision berechnen müssen. Betrachten wir die linke Seite $f_C(\wp(z, L))$ von Gleichung (6.13), so wird ersichtlich, daß wir die Polynomkoeffizienten $a_{d-1}, \ldots, a_0$ von $f_C(X)$ bestimmen können, wenn wir alle auftretenden Fourierreihenentwicklungen bis zum Koeffizienten von $z^0$ einschließlich exakt kennen. Damit müssen wir in den Summen aus (6.14) nur die Summenglieder für $1 \leq k \leq (l-3)/2$ und $0 \leq r \leq (l-1)/2$ berechnen. Offensichtlich können wir dann die Koeffizienten des Polynoms $f_C(X)$ ähnlich zum Beweis von Satz 4.13 als rationale Funktionen mit den Variablen $a, b, \tilde{a}, \tilde{b}$ und $P_1$ auffassen. Dabei beachte man, daß sich mit Lemma 6.2 auch die Koeffizienten $c_k$ bzw. $\tilde{c}_k$ als rationale Funktion in $a, b$ bzw. $\tilde{a}, \tilde{b}$ schreiben lassen. Weiterhin beachte man, daß diese rationalen Funktionen die spezielle Gestalt besitzen, daß nur ganze Zahlen im Nenner sind. Wir untersuchen nun die dabei auftretenden Nenner. Offensichtlich gilt für die Nenner, die durch die Entwicklung der Exponentialfunktion in (6.14) auftreten, daß diese als Potenzprodukte von Primzahlen kleiner als $(l-1)/2$ geschrieben werden können (beachte die Grenze für $r$). Genauso erkennt man, daß auch die auftretenden Nenner $(2k+1)(2k+2)$ für die vorgegebenen Werte von $k$ nur Primteiler kleiner $l-1$ besitzt. Durch Induktion über den Index kann man schließlich auch leicht zeigen, daß in der Darstellung des Koeffizienten $c_k$ als rationale Funktion im Nenner ein Primzahlpotenzprodukt aus Primzahlen $\leq (2k+3)$ auftritt, welches für die vorgegebenen Möglichkeiten für $k$ nur Primzahlen $\leq l$ enthält. Damit erhalten wir insgesamt, daß die beschriebenen rationalen Funktionen nur Nenner besitzen, die ein Potenzprodukt von Primzahlen $\leq l$ sind. Man beachte, daß damit die Nenner insbesondere auch modulo $p$ invertierbar sind, denn $p$ war größer als $l$ vorausgesetzt. Damit kann bei der Reduktion des in Abschnitt 6.2 beschriebenen Koeffizientenvergleichs modulo $p$ und Auswertung der dann entstehenden Formeln an den durch die Eingabe $E$ bzw. $(E/C, P_1)$ vorgegebenen Stellen kein Fehler auftreten.

Da über den komplexen Zahlen $f_C(X)$ ein Teiler des $l$-ten Divisionspolynoms $\psi_l(X)$ ist, erhalten wir

$$\psi_l(X) \quad = \quad f_C(X) \cdot h(X).$$

Diese Gleichung gilt im Ring der rationalen Funktionen mit den Variablen $a$, $b$, $\tilde{a}$, $\tilde{b}$, $P_1$. Nach obigen Ausführungen können wir diese Gleichung modulo der Charakteristik $p$ des endlichen Körpers $\mathbb{F}_q$ reduzieren. Dabei bilden wir das $l$-te Divisionspolynom über $\mathbb{C}$ in das $l$-te Divisionspolynom über $\mathbb{F}_p[a, b]$ und $f_C(X)$ in ein Polynom über $\mathbb{F}_p[a, b, \tilde{a}, \tilde{b}, P_1]$ ab, das ein Teiler des $l$-ten Divisionspolynoms ist. Werten wir dieses Polynom an den vorgegebenen Stellen aus, so erhalten wir einen Teiler des $l$-ten Divisionspolynoms, womit die Behauptung des Satzes gezeigt ist. ■

Damit haben wir gezeigt, daß wir die in Kapitel 6 gefundenen Formeln auf endliche Körper übertragen können, wenn die Charakteristik des endlichen Körpers größer als $l$ ist. Dies ist in der Praxis sehr häufig der Fall; insbesondere dann, wenn man die Gruppenordnung elliptischer Kurven über großen Primkörpern bestimmen möchte. Wir erhalten dann den folgenden Algorithmus, bei dem wir voraussetzen, daß er als Eingabe genau die Ausgabe der Algorithmen 7.3 bzw. 7.6 erhält.

**Algorithmus 7.8** [ Bestimmung von $f_C(X)$]

**Eingabe:** elliptische Kurve $E = (a, b)$, Menge von Tripeln $(\tilde{a}, \tilde{b}, P_1)$ (vgl. Ausgabe von Algorithmus 7.3 bzw. 7.6).

**Ausgabe:** Polynom $f_C(X) = X^d + a_{d-1} \cdot X^{d-1} + \ldots + a_1 \cdot X + a_0 \in \mathbb{F}_q[X]$ (Teiler des $l$-ten Divisionspolynoms).

| | |
|---|---|
| Setze $d \leftarrow (l-1)/2$ und $a_d \leftarrow 1$. | (1) |
| FOR $k = 1, \ldots, (l-3)/2$ | (2) |
| Berechne $c_k$ aus $a, b$ mit Lemma 6.2. | (3) |
| Setze $wp_1(z) \leftarrow 1/z^2 + \sum_{k=1}^{(l-3)/2} c_k \cdot z^{2k}$. /* $\wp(z)$ mit Präz. $l-3$ */ | (4) |
| FOR $\nu = 2, \ldots, d$ | (5) |
| Berechne $wp_\nu(z) \leftarrow wp_{\nu-1}(z) \cdot wp_1(z)$ /* $\wp(z)^\nu$ mit Präz. $l-3$ */ | (6) |
| FOR Jedes Tripel $(\tilde{a}, \tilde{b}, P_1)$ aus der Eingabe | (7) |
| FOR $k = 1, \ldots, (l-3)/2$ | (8) |
| Berechne $\tilde{c}_k$ aus $\tilde{a}, \tilde{b}$ mit Lemma 6.2. | (9) |
| Setze $h(z) \leftarrow z^{1-l} \cdot \sum_{r=0}^{(l-1)/2} (r!)^{-1} \cdot \left(\sum_{k=1}^{(l-3)/2} (l \cdot c_k - \tilde{c}_k) \cdot ((2k+1)(2k+2))^{-1} z^{2k+2} - P_1 \cdot z^2\right)^r$. | (10) |
| FOR $\nu = d-1, \ldots, 0$ | (11) |
| Setze $h(z) \leftarrow h(z) - a_{\nu+1} \cdot wp_{\nu+1}(z)$. | (12) |
| Bestimme $a_\nu \leftarrow \min_{coeff}(h(z))$. | (13) |
| Setze $f_C(X) \leftarrow X^d + a_{d-1} \cdot X^{d-1} + \ldots + a_1 \cdot X + a_0$. | (14) |
| IF $\psi_l(X, Y) \equiv 0 \bmod f_C(X)$ /* als Funktion in $\mathbb{F}_q[E]$ */ | (15) |
| THEN RETURN $f_C(X)$. | (16) |

Damit haben wir in diesem Abschnitt gezeigt, wie wir für den Fall, daß die Charakteristik $p$ des Körpers $\mathbb{F}_q$ größer als die Primzahl $l$ ist, ein Polynom $f_C(X) \in \mathbb{F}_q[X]$ vom Grade $(l-1)/2$ bestimmen können, das das $l$-te Divisionspolynom teilt. Im folgenden Abschnitt werden wir einen Algorithmus beschreiben, wie wir unter Benutzung von $f_C(X)$ die Spur des Frobenius-Endomorphismus einer elliptischen Kurve über dem endlichen Körper $\mathbb{F}_q$ modulo der Primzahl $l$ exakt bestimmen können.

## 7.3 Die Berechnung von $c \bmod l$

Wir haben in dem vorherigen Abschnitt beschrieben, wie wir ein Polynom $f_C(X) \in \mathbb{F}_q[X]$ bestimmen können, dessen Nullstellen alle verschiedenen $x$-Koordinaten von

Punkten (ungleich $\mathcal{O}$) einer unter $\Phi_E$ invarianten $l$-Gruppe $C$ sind. Damit existiert eine Zahl $1 \leq \alpha < l$, so daß für alle Punkte $P \in C$ gilt

$$\Phi_E(P) \quad = \quad \alpha \cdot P.$$

In diesem Abschnitt werden wir einen Algorithmus angeben, mit dem wir diese Zahl $\alpha$ bestimmen können. Damit kennen wir auch die Spur $c$ des Frobenius-Endomorphismus modulo $l$, denn wie wir in Kapitel 3 beschrieben haben, ist das Polynom $X - \alpha \in \mathbb{F}_l[X]$ ein Teiler (über $\mathbb{F}_l$) des charakteristischen Polynoms $X^2 - \overline{c}\,X + \overline{q} \in \mathbb{F}_l[X]$ des auf $E[l]$ eingeschränkten Frobenius-Endomorphismus $\Phi_E$. Durch Koeffizientenvergleich erhalten wir dann direkt den Wert von $c \bmod l$ als

$$c \quad \equiv \quad \alpha + \overline{q} \cdot \alpha^{-1} \bmod l.$$

Zur Berechnung der Zahl $\alpha$ benutzen wir eine zum Algorithmus von Schoof [Sc85] analoge Idee. Wir transformieren die Gleichung $\Phi_E(P) = \alpha \cdot P$ im Endomorphismenring von $C$ in Polynomgleichungen. Dabei können wir den maximal auftretenden Polynomgrad durch $(l-1)/2$ beschränken, wie wir sehen werden. Für diese Transformation benutzen wir die Divisionspolynome, die wir in Definition 4.11 (Seite 39) schon eingeführt haben. Wir betrachten dabei Divisionspolynome immer als Polynome auf $E$ (reduzieren also alle $Y^2$-Terme mit Hilfe der rechten Seite $X^3 + aX + b$ der Kurvengleichung). Durch Induktion kann man dann leicht zeigen, daß für ungerades $n$ das „reduzierte" $n$-te Divisionspolynom in $\mathbb{F}_q[X]$ und für gerades $n$ in $Y \cdot \mathbb{F}_q[X]$ liegt.

Die Divisionspolynome besitzen wegen Satz 4.12 (Seite 40) die Eigenschaft, daß wir mit ihrer Hilfe die speziellen Endomorphismen $\alpha \in \mathbb{Z}$ in Polynomgleichungen transformieren können. Es gilt für $n \in \mathbb{N}$ und einen Punkt $P = (x, y) \in E(\overline{\mathbb{F}}_q)$ mit $n \cdot P \neq \mathcal{O}$ (interpretiere dabei $\psi_k$ als $\psi_k(x, y)$)

$$n \cdot P = \left( x - \frac{\psi_{n-1} \cdot \psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2} \cdot \psi_{n-1}^2 - \psi_{n-2} \cdot \psi_{n+1}^2}{4\, y \cdot \psi_n^3} \right).$$

Die Idee des nun vorzustellenden Algorithmus ist dann folgendermaßen: wir setzen einen Punkt $P \in C$ aus der unter $\Phi_E$ invarianten $l$-Gruppe $C$ allgemein an als $(X, Y)$. Dann können wir mit Hilfe von Satz 4.12 alle Vielfache $\alpha \cdot P$ als rationale Funktion in $X, Y$ schreiben. Da wir auch $\Phi_E(X, Y)$ als Polynom ausdrücken können (trivialerweise nach Definition von $\Phi_E$), läßt sich die Gleichung $\Phi_E(P) = \alpha \cdot P$ durch Vergleich zweier Polynome (nach Multiplikation mit dem Hauptnenner) überprüfen. Da wir die Gleichung $\Phi_E(P) = \alpha \cdot P$ nur für Punkte $P$ aus der speziellen $l$-Gruppe $C$ untersuchen und da die $x$-Koordinaten solcher Punkte Nullstellen von $f_C(X)$ sind, können wir alle Polynomgleichungen modulo $f_C(X)$ reduzieren, so daß alle auftretenden Polynome maximal Grad $(l-1)/2$ besitzen. Damit wird der Algorithmus in der Praxis gut anwendbar, wie wir im folgenden Abschnitt sehen werden.

Wir leiten jetzt den sich aus dieser Idee ergebenden Algorithmus her. Zuerst bestimmen wir für einen allgemeinen Punkt $P = (X, Y) \in C$ die Polynomgleichung für $\Phi_E(P)$ als

$$\begin{aligned}\Big(X^q \bmod f_C(X),\, Y^q \bmod f_C(X)\Big) \quad &= \\ &\Big(X^q \bmod f_C(X),\, Y \cdot (X^3+aX+b)^{(q-1)/2} \bmod f_C(X)\Big).\end{aligned}$$

Offensichtlich ist der Wert von $\alpha$ nur modulo $l$ bestimmt. Da wir für einen beliebigen Punkt $(X, Y)$ den negativen Punkt leicht als $(X, -Y)$ erhalten, wählen wir als Restsystem modulo $l$ die absolut kleinsten Reste. Dann bestimmen wir iterativ für alle $\alpha = \pm 1, \pm 2, \ldots, \pm(l-1)/2$ mit Hilfe der Formeln aus Satz 4.12 die Punkte $\alpha \cdot (X, Y)$ und testen, ob nach Multiplikation mit dem Nenner Gleichheit modulo $f_C(X)$ besteht. Ist dies sowohl für die $x$- als auch für die $y$-Koordinate der Fall, so haben wir $\alpha$ und damit $c \bmod l$ gefunden. Damit erhalten wir den folgenden Algorithmus:

**Algorithmus 7.9** [Berechnung von $c \bmod l$]

**Eingabe:** elliptische Kurve $E = (a, b) \in \mathbb{F}_q^2$, $f_C(X) \in \mathbb{F}_q[X]$ wie beschrieben.
**Ausgabe:** $c \bmod l$.

| | |
|---|---|
| FOR $n = -1$ TO $(l+3)/2$ | (1) |
|     Berechne $\psi_n(X, Y) \bmod f_C(X)$ mit Formeln aus Definition 4.11. | (2) |
| Berechne $l_x(X) \leftarrow X^q \bmod f_C(X)$. | (3) |
| Berechne $l_y(X, Y) \leftarrow Y \cdot (X^3+aX+b)^{(q-1)/2} \bmod f_C(X)$ . | (4) |
| FOR $\alpha = 1$ TO $(l-1)/2$ | (5) |
|     $r_x(X, Y) \leftarrow X \cdot \psi_\alpha^2(X, Y) - \psi_{\alpha-1}(X, Y) \cdot \psi_{\alpha+1}(X, Y) \bmod f_C(X)$. | (6) |
|     IF $l_x(X) \cdot \psi_\alpha^2(X, Y) \equiv r_x(X, Y) \bmod f_C(X)$ /*$x$-Koord. gleich*/ | (7) |
|     THEN $r_y(X, Y) \leftarrow \psi_{\alpha+2}(X, Y) \cdot \psi_{\alpha-1}^2(X, Y) - \psi_{\alpha-2}(X, Y) \cdot \psi_{\alpha+1}^2(X, Y) \bmod f_C(X)$. | (8) |
|         IF $4Y \cdot l_y(X, Y) \cdot \psi_\alpha^3(X, Y) \equiv r_y(X, Y) \bmod f_C(X)$ /* $\Phi_E = +\alpha$ */ | (9) |
|         THEN RETURN $c \equiv \alpha + q \cdot \alpha^{-1} \bmod l$. | (10) |
|         IF $4Y \cdot l_y(X, Y) \cdot \psi_\alpha^3(X, Y) \equiv -r_y(X, Y) \bmod f_C(X)$ /* $\Phi_E = -\alpha$ */ | (11) |
|         THEN RETURN $c \equiv -\alpha - q \cdot \alpha^{-1} \bmod l$. | (12) |

Man beachte, daß in den Schritten (6) bis (11) dieses Algorithmus alle verwendeten Polynome als Polynome auf $E$ aufgefaßt werden. Innerhalb des Algorithmus werden die Polynome $l_x(X)$ bzw. $l_y(X, Y)$ dazu benutzt, die Polynome $X^q \bmod f_C(X)$ bzw. $Y^q \bmod f_C(X)$ zwischenzuspeichern. Der Gleichheitstest für die $x$-Koordinate findet dann in Schritt (7) statt; in (9) testen wir bei erfolgreichem $x$-Test den Fall $+\alpha$, in (11) den Fall $-\alpha$.

Wir haben bisher immer Wert darauf gelegt, daß wir $c$ nur modulo ungerader Primzahlen berechnen. Es ist jedoch auch auf elementare Art und Weise möglich, $\#E(\mathbb{F}_q) \bmod 2$ zu berechnen [Mü91].

## 7.4 Beschreibung unserer Implementierung

In diesem Abschnitt beschreiben wir praktische Erfahrungen, die mit einer Implementierung des Algorithmus für endliche Primkörper $\mathbb{F}_p$ erzielt wurden. Eine genaue Beschreibung dieser Implementierung findet man in [Ma94]. Alle in diesem Abschnitt angegebenen Laufzeiten wurden auf einem SPARC ELC Rechner mit 16 MegaByte Hauptspeicher berechnet.

Bei der Bestimmung des Polynoms $f_C(X)$ finden Berechnungen mit den dicht besetzten Fourierreihenentwicklungen für $\wp^i(z, L)$, $1 \leq i \leq l+1$ statt (vgl. Algorithmus 7.8). Dabei benutzen wir analog zu Abschnitt 5.6 eine Fourierreihenarithmetik, die zur Multiplikation eine Variante von FFT benutzt. Dabei führen wir eine Multiplikation zweier Reihenentwicklungen modulo $p$ folgendermaßen durch: wir fassen beide Multiplikanten als Reihenentwicklungen über $\mathbb{Z}$ auf, reduzieren diese modulo einer 26-Bit Primzahl $p_i$ und multiplizieren diese reduzierten Entwicklungen mit FFT (dabei werden die Primzahlen $p_i$ natürlich speziell gewählt, so daß die Benutzung von FFT modulo $p_i$ möglich ist). Haben wir das Ergebnis für „genügend viele" 26-Bit Primzahlen $p_i$ berechnet, so kombinieren wir die Resultate mit Hilfe des Chinesischen Restsatzes und reduzieren die Koeffizienten des Gesamtergebnisses modulo der Charakteristik $p$ des Körpers $\mathbb{F}_p$. Man beachte, daß in diesem Fall die Anzahl der benötigten 26-Bit Primzahlen vorher berechnet werden kann. Stellt man beispielsweise die Restklassen modulo $p$ durch absolut kleinste Vertreter dar, so erhält man eine obere Schranke für die Koeffizienten im Ergebnis (über $\mathbb{Z}$, nicht modulo $p$ reduziert) als $(p-1)^2 \cdot$ (obere Schranke für Präzision der Reihenentwicklungen).

Bei der Berechnung der Potenzen $\wp(z, L)^i$ benutzen wir wiederum den Quadrierungstrick, den wir schon in Abschnitt 5.6 beschrieben haben. Allerdings können wir aus Speicherplatzgründen nicht alle Potenzen von $\wp(z, L)$ im Speicher halten. Daher berechnen (und speichern) wir nur die Potenzen $\wp(z, L)^i$ für $1 \leq i \leq \lfloor\sqrt{l+1}\rfloor$ und $\wp(z, L)^{\lceil\sqrt{l+1}\rceil \cdot j}$ für $1 \leq j \leq \lceil\sqrt{l+1}\rceil$. Aus diesen Reihenentwicklungen können wir dann jede gesuchte Potenz von $\wp(z, L)$ mit einer Multiplikation ausrechnen.

Betrachten wir zuerst in Tabelle 7.1, wie lange die Berechnung der Kurve $E/C$ und des Wertes $P_1$ mit den Algorithmen 7.3 bzw. 7.6 dauert. Anschließend beschreiben wir in Tabelle 7.2, wie sich bei der Berechnung des gesuchten Polynoms $f_C(X)$ mit Algorithmus 7.8 die Laufzeit auf die einzelnen Phasen aufteilt.

Wenden wir uns nun Algorithmus 7.9, d.h. der Bestimmung des Eigenwertes $\alpha$, zu. In der Praxis reicht es häufig aus, in der Gleichung $\Phi_E(P) = \alpha \cdot P$ nicht beide Koordinaten zu testen, sondern sich auf die $y$-Koordinate zu beschränken. Dies hat

Tabelle 7.1: Bestimmung von $(E/C, P_1)$ mit Algorithmus 7.3 bzw. 7.6.
Angegeben werden die Anzahl der Dezimalstellen der Charakteristik $p$, der Wert von $l$, der Typ des äquivalenten Polynoms (1 für Polynom aus Abschnitt 5.2, 2 für Polynom aus Abschnitt 5.4) und die Laufzeit zur jeweiligen Berechnung von $(E/C, P_1)$.

| dd($p$) | l | Typ | Laufzeit | | | |
|---|---|---|---|---|---|---|
| 100 | 53 | 1 | | | 2 | sec |
| | 97 | 1 | | | 2 | sec |
| | 157 | 1 | | | 6 | sec |
| | 199 | 1 | | | 25 | sec |
| 200 | 103 | 2 | | | 44 | sec |
| | 193 | 1 | | | 22 | sec |
| | 307 | 2 | 8 | min | 9 | sec |
| | 401 | 2 | 8 | min | 52 | sec |
| 300 | 101 | 1 | | | 33 | sec |
| | 317 | 2 | 32 | min | 53 | sec |
| | 421 | 2 | 42 | min | 6 | sec |
| | 523 | 2 | 50 | min | 15 | sec |
| 375 | 103 | 2 | 3 | min | 28 | sec |
| | 223 | 1 | 3 | min | 19 | sec |
| | 503 | 2 | 38 | min | 31 | sec |
| | 839 | 2 | 1 | h | 16 | min |

den Vorteil, daß man die Berechnung von $l_x(X) \equiv X^q \bmod f_C(X)$ sparen kann (beachte, daß die zeitaufwendigsten Schritte in Algorithmus 7.9 die Potenzierungen in den Schritten (3), (4) sind, vgl. dazu Tabelle 7.3). Da die $x$-Koordinaten von $P$ und $-P$ gleich sind, reicht es offensichtlich nicht aus, nur $x$-Koordinaten zu testen.

Finden wir bei den Tests der $y$-Koordinaten in Schritt (9) bzw. (11) nur für einen Wert $\alpha \in \{\pm 1, \ldots, \pm(l-1)/2\}$ Gleichheit, so ist die Spur $c$ modulo $l$ eindeutig bestimmt. Dies bedeutet aber, daß alle Möglichkeiten für $\alpha$ getestet werden müßten. In der Praxis ist allerdings der erste gefundene Wert von $\alpha$, der Gleichheit ergibt, „immer" der gesuchte Eigenwert. Deshalb nehmen wir in unserer Implementierung schon bei dem ersten gefundenen Wert für $\alpha$ mit Gleichheit an, daß wir den Eigenwert und damit $c \bmod l$ gefunden haben. War dieser Wert falsch (was in der Praxis bei uns noch nie vorgekommen ist), so wird bei der Bestimmung der Gruppenordnung mit dem in Kapitel 10 angegebenen Verfahren keine Lösung gefunden und damit festgestellt, daß wir durch diese „Cutting Corners" Methode einen Fehler produziert haben.

Die in Algorithmus 7.9 angegebene Methode, alle Möglichkeiten für $\alpha$ zu testen, führt unter Umständen zu vielen „unnötigen" Tests. Haben wir die erste Phase des

Tabelle 7.2: Aufteilung der Laufzeit in Algorithmus 7.8.

Angegeben werden die Anzahl der Dezimalstellen der Charakteristik $p$, der Wert von $l$, Bestimmung der rechten Seite (Schritte (8) - (10) in Algorithmus 7.8), Bestimmung der $\wp$-Potenzen wie beschrieben und der Koeffizientenvergleich (dabei wird zusätzlich die aktuell benötigte $\wp(z, L)$-Potenz aus der Tabelleninformation berechnet). Man beachte, daß manchmal die Berechnung für kleine Werte $l$ länger dauert als für größere Werte von $l$. Dies wird verursacht, wenn in Algorithmus 7.8 mehrere Eingaben getestet werden müssen, bis das Polynom $f_C(X)$ korrekt berechnet ist (vgl. Schritt (15)).

| dd($p$) | $l$ | rechte Seite | $\wp$-Potenzen | Koeff.vgl. |
|---|---|---|---|---|
| 100 | 53 | 6 sec | 1 sec | 4 sec |
| | 97 | 22 sec | 4 sec | 16 sec |
| | 157 | 1 min 11 sec | 12 sec | 55 sec |
| | 199 | 1 min 38 sec | 15 sec | 1 min 22 sec |
| 200 | 103 | 2 min 32 sec | 21 sec | 1 min 14 sec |
| | 193 | 3 min 33 sec | 33 sec | 2 min 50 sec |
| | 307 | 13 min 16 sec | 1 min 28 sec | 9 min 30 sec |
| | 401 | 19 min 6 sec | 1 min 54 sec | 14 min 17 sec |
| 300 | 101 | 1 min 35 sec | 20 sec | 1 min 12 sec |
| | 317 | 1 h 11 min | 7 min 46 sec | 51 min 11 sec |
| | 421 | 34 min 59 sec | 3 min 25 sec | 26 min 33 sec |
| | 523 | 1 h 8 min | 6 min 23 sec | 53 min 59 sec |
| 375 | 103 | 5 min 42 sec | 46 sec | 2 min 53 sec |
| | 223 | 10 min 2 sec | 1 min 29 sec | 8 min 5 sec |
| | 503 | 1 h 28 min | 8 min 5 sec | 1 h 9 min |
| | 839 | 3 h 5 min | 13 min 17 sec | 2 h 32 min |

Algorithmus durchlaufen, so kennen wir einige mögliche Werte für $c \bmod l$ und damit auch einige mögliche Werte für $\alpha$. Daher benutzen wir in unserer Implementierung die folgenden zwei Strategien, um den Wert von $\alpha$ wirklich zu finden (vgl. [Ma94]):

1. Erhalten wir nach der Bestimmung des Zerfällungstyps des $l$-ten äquivalenten Polynoms „viele" Möglichkeiten für $c \bmod l$ und damit für $\alpha$, so verwenden wir die in Algorithmus 7.9 angegebene Strategie und testen mit Hilfe der Divisionspolynome sukzessive alle Möglichkeiten für $\alpha$. Diese Methode besitzt gegenüber der im folgenden beschriebenen Methode einen Laufzeitvorteil, allerdings auch den Nachteil eines größeren Speicherplatzbedarfs. Zur effizienten Benutzung der Divisionspolynome müssen diese alle vorberechnet und gespeichert werden. Der dabei benötigte Hauptspeicherbedarf beträgt für $l \approx 800$ und $p \approx 10^{480}$ ungefähr 48 MegaByte, was auf vielen Rechnern nicht zur Verfügung steht.

2. Erhalten wir in der ersten Phase „wenige" Möglichkeiten für $\alpha$ (oder wird der Speicherplatzbedarf bei der ersten Methode zu groß), so speichern wir uns verschiedene Punkte $i \cdot (X, Y)$ als rationale Funktion aus $\mathbb{F}_p(E)$ und versuchen dann, mit Hilfe möglichst weniger Punktadditionen die möglichen Werte für $\alpha$ zu testen. Dazu beachte man, daß man Punktadditionen als rationale Funktionen ausdrücken kann (vgl. Satz 4.12). Mit dieser Strategie sinkt der Speicherplatzbedarf für obige Werte von $l$ und $p$ auf 6.4 MegaByte, allerdings steigt die Laufzeit.

In der folgenden Tabelle 7.3 vergleichen wir für einige Beispiele Laufzeiten für beide Strategien. Dabei wird deutlich, daß für große Werte von $l$ das Finden des Eigenwertes $\alpha$ sehr aufwendig wird. Daher stellt sich die Frage, ob es nicht eine bessere Strategie zum Finden des Eigenwertes gibt. Dabei sind folgende neue Strategien, die in unserer Implementierung noch nicht verwendet werden (aber zur Probe schon implementiert wurden), denkbar:

3. Man kann versuchen, mit Hilfe von $X^q \bmod f_C(X)$ einen Teiler von $f_C(X)$ zu finden und dann alle Rechnungen modulo dieses Teilers durchführen (beachte das folgende Kapitel 8 zur Existenz eines solchen Teilers).

4. Man kann mit Hilfe einer Babystep-Giantstep Strategie alle Möglichkeiten für $\alpha$ testen. Dabei muß man allerdings die rationalen Funktionen für $\alpha \cdot (X, Y)$ in Polynome modulo $f_C(X)$ umwandeln, indem man die Nenner modulo $f_C(X)$ invertiert.

5. Man kann mit Hilfe einer Babystep-Giantstep Strategie und Betrachtung der $x$-Koordinaten einen Kandidaten für $\pm\alpha$ bestimmen. Danach versucht man, einen Faktor des Polynoms $f_C(X)$ zu finden (vgl. Kapitel 8) und dann modulo dieses Faktors den korrekten Wert von $\alpha$ zu bestimmen. Diese letzte Variante erscheint sehr aussichtsreich für die Praxis zu sein, ist aber noch nicht ausreichend in der Praxis untersucht. Erste Experimente deuten an, daß ab etwa $l \geq 500$ diese Variante zu einer Verbesserung führen könnte.

Damit haben wir beschrieben, wie wir die Ideen von Elkies auf endliche Körper übertragen können, wenn die Charakteristik des endlichen Körpers hinreichend groß ist. Außerdem haben wir praktische Erfahrungen angegeben, die wir mit unserer Implementierung gesammelt haben. In dem folgenden Kapitel werden wir aufbauend auf diesen Ideen beschreiben, wie wir für kleine Primzahlen $l$ die Spur des Frobenius-Endomorphismus einer elliptischen Kurve über einem endlichen Körper sogar modulo Primzahlpotenzen $l^i$ bestimmen können.

Tabelle 7.3: Laufzeiten der Algorithmen zum Finden des Eigenwertes $\alpha$.
Angegeben sind die Anzahl der Dezimalstellen von $p$, der Wert von $l$, Zeiten zum Finden des Eigenwertes mit Hilfe von Divisionspolynomen (siehe 1.) und rationalen Funktionen (siehe 2.) und die Zeit, die benötigt wird zur Berechnung von $Y^p$ mod $f_C(X)$.

| dd($p$) | $l$ | Divisionspolynome | | | | rat. Funktionen | | | | $Y^p$ mod $f_C(X)$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 100 | 53 | | | 3 | sec | | | 9 | sec | 1 | min | 28 | sec |
| | 97 | | | | | 2 | min | 34 | sec | 2 | min | 9 | sec |
| | 157 | 2 | min | 40 | sec | 4 | min | 42 | sec | 4 | min | 11 | sec |
| | 199 | 6 | min | 9 | sec | 9 | min | 44 | sec | 4 | min | 35 | sec |
| 200 | 103 | | | 29 | sec | 1 | min | 8 | sec | 11 | min | 36 | sec |
| | 193 | 14 | min | 16 | sec | 18 | min | 42 | sec | 23 | min | 21 | sec |
| | 307 | 45 | min | 59 | sec | 1 | h | 2 | min | 42 | min | 58 | sec |
| | 401 | 57 | min | 25 | sec | 46 | min | 41 | sec | 49 | min | 42 | sec |
| 300 | 101 | 1 | min | 48 | sec | 3 | min | 16 | sec | | | 33 | min |
| | 317 | 1 | h | 16 | min | 1 | h | 53 | min | 1 | h | 55 | min |
| | 421 | | | 20 | min | | | 35 | min | 2 | h | 21 | min |
| | 523 | 2 | h | 31 | min | 3 | h | 36 | min | 3 | h | 37 | min |
| 375 | 103 | | | 9 | min | | | 14 | min | | | 55 | min |
| | 223 | | | 8 | min | | | 17 | min | 2 | h | 1 | min |
| | 503 | 5 | h | 26 | min | 7 | h | 39 | min | 4 | h | 34 | min |
| | 839 | 19 | h | 59 | min | 23 | h | 19 | min | 8 | h | 10 | min |

# Kapitel 8

# Benutzung von Primzahlpotenzen

In diesem Kapitel beschreiben wir eine Erweiterung des bisher vorgestellten Algorithmus, mit der wir die Gruppenordnung einer elliptischen Kurve über einem endlichen Körper der Charakteristik größer drei modulo Potenzen „kleiner“ ungerader Primzahlen bestimmen können. Dabei werden ähnlich wie bei den bisher vorgestellten Algorithmen Polynomrechnungen modulo eines Teilers von Divisionspolynomen durchgeführt. Wir beschreiben im ersten Abschnitt die Bestimmung eines solchen Teilers und gehen anschließend darauf ein, wie wir damit den Wert der Spur des Frobenius-Endomorphismus der elliptischen Kurve modulo der verwendeten Primzahlpotenz bestimmen können.

## 8.1 Bestimmung von Teilern von Divisionspolynomen

In diesem Abschnitt beschreiben wir eine Methode, wie wir einen Teiler eines geeigneten Divisionspolynoms bestimmen können. Wir unterscheiden dabei die zwei folgenden Fälle.

### 8.1.1 Der Elkies-Fall

Im sogenannten Elkies-Fall machen wir die folgende Annahme: wir kennen für eine ungerade Primzahlpotenz $l^i$ eine Zahl $0 < \alpha < l^i$ und eine Menge von $l^i$-Torsionspunkten $\{P_1, \ldots, P_k\}$, so daß für alle $1 \leq j \leq k$ gilt

$$\Phi_E(P_j) \quad = \quad \alpha \cdot P_j.$$

Weiterhin nehmen wir an, daß wir ein Polynom $f(X) \in \mathbb{F}_q[X]$ kennen, dessen Nullstellen die verschiedenen $x$-Koordinaten aller Punkte $P_j$, $1 \leq j \leq k$, sind (beachte: damit teilt $f(X)$ das $l^i$-te Divisionspolynom). Wir beachten, daß wir für eine Primzahl $l < p$ diese Voraussetzungen erfüllen können, indem wir $\alpha$ als einen Eigenwert von $\Phi_E$ und $f(X)$ als das Polynom $f_C(X)$ für die unter $\Phi_E$ invariante zugehörige $l$-Gruppe $C$ (siehe Abschnitt 7.1) wählen. Für Primzahlpotenzen werden diese Voraussetzungen aus der iterativen Vorgehensweise folgen.

Sei $d$ im folgenden die Ordnung von $\alpha$ in $(\mathbb{Z}/l^i\mathbb{Z})^*$. Aus $\mathrm{ggT}(l,q) = 1$ folgt dabei direkt, daß $\alpha$ teilerfremd zu $l^i$ ist. Dann gilt für alle $1 \leq j \leq k$

$$\Phi_E^d(P_j) \quad = \quad \alpha^d \cdot P_j \quad = \quad P_j.$$

Übertragen wir diese Gleichung wie üblich in Polynomgleichungen, so erhalten wir aus der Gleichung für die $x$-Koordinaten

$$X^{q^d} \quad \equiv \quad X \bmod f(X).$$

Da es modulo Primzahlpotenzen nur zwei Quadratwurzeln aus Eins gibt, folgt für gerade Ordnung $d$ sogar

$$\Phi_E^{d/2}(P_j) \quad = \quad -P_j \qquad \text{bzw.} \qquad X^{q^{d/2}} \quad \equiv \quad X \bmod f(X).$$

Setzen wir also

$$d' \quad = \quad \begin{cases} d/2, & \text{falls } d \text{ gerade,} \\ d, & \text{falls } d \text{ ungerade,} \end{cases} \tag{8.1}$$

so folgt

$$X^{q^{d'}} - X \quad \equiv \quad 0 \bmod f(X).$$

Damit zerfällt $f(X)$ über dem Körper $\mathbb{F}_q$ in Polynome vom Grad $d'$. Sei im folgenden $g(X)$ ein Teiler von $f(X)$ vom Grad $d'$. Dabei beachte man, daß nach Voraussetzung $g(X)$ dann sogar ein Teiler des $l^i$-ten Divisionspolynoms ist. Wir wollen mit Hilfe von $g(X)$ einen Teiler des $l^{i+1}$-ten Divisionspolynoms bestimmen. Die Grundlage dazu bildet das folgende Lemma.

**Lemma 8.1** *Sei $g(X) = \sum_{i=0}^{d'} a_i \cdot X^i \in \mathbb{F}_q[X]$ ein Teiler des $l^i$-ten Divisionspolynoms und sei $h(X) = X \cdot \psi_l^2(X,Y) - \psi_{l-1}(X,Y) \cdot \psi_{l+1}(X,Y) \in \mathbb{F}_q[E]$, wobei $\psi_j(X,Y)$ das $j$-te Divisionspolynom ist. Dann ist das Polynom*

$$\tilde{g}(X) \;=\; g\left(\frac{h(X)}{\psi_l^2(X,Y)}\right) \cdot \psi_l^{2d'}(X,Y) \;=\; \sum_{i=0}^{d'} a_i \cdot h(X)^i \cdot \psi_l^{2(d'-i)}(X,Y) \;\in\; \mathbb{F}_q[E]$$

*ein Teiler des $l^{i+1}$-ten Divisionspolynom vom Grad $d' \cdot l^2$.*

**Beweis:** Zuerst beachte man, daß wir alle benutzten Polynome als Polynome auf $E$ auffassen und daß daher $h(X)$ und $\tilde{g}(X)$ wirklich nur von einer Variablen $X$ abhängen. Durch eine Division mit Rest folgt dann direkt, daß die Polynome $\tilde{g}(X)$ und $\psi_l(X,Y)$ als Funktionen auf $E$ teilerfremd sind (beachte dabei die Teilerfremdheit verschiedener Divisionspolynome).

Damit besitzt das Polynom $\tilde{g}(X)$ dieselben Nullstellen wie die rationale Funktion

$$g\left(\frac{h(X)}{\psi_l^2(X,Y)}\right),$$

die wir aus $\tilde{g}(X)$ durch Division durch $\psi_l^{2d'}(X,Y)$ erhalten. Also gilt für jede Nullstelle $\tilde{x}$ von $\tilde{g}(X)$, daß $h(\tilde{x})/\psi_l^2(\tilde{x})$ eine Nullstelle von $g(X)$ und damit die $x$-Koordinate eines $l^i$-Torsionspunktes ist. Nach Satz 4.12 wird für einen beliebigen Punkt $(X,Y)$ die $x$-Koordinate des Punktes $l \cdot (X,Y)$ gegeben durch $h(X)/\psi_l^2(X,Y)$, so daß damit $\tilde{x}$ die $x$-Koordinate eines Punktes $\tilde{P}$ ist, für den $l \cdot \tilde{P}$ ein $l^i$-Torsionspunkt ist. Damit ist $\tilde{P}$ selber ein $l^{i+1}$-Torsionspunkt und alle Nullstellen von $\tilde{g}(X)$ sind $x$-Koordinaten von $l^{i+1}$-Torsionspunkten. Also ist $\tilde{g}(X)$ insbesondere ein Teiler des $l^{i+1}$-ten Divisionspolynoms.

Die Aussage über den Grad des Polynoms $\tilde{g}(X)$ erhalten wir, indem wir in einer einfachen Gradrechnung den maximal auftretenden Polynomgrad in der Summe ausrechnen. ■

Damit haben wir beschrieben, wie wir ein Polynom berechnen können, dessen Nullstellen $x$-Koordinaten von $l^{i+1}$-Torsionspunkten sind. Durch Induktion über $i$ kann man leicht zeigen, daß die Nullstellen von $\tilde{g}(X)$ $x$-Koordinaten von „echten“ $l^{i+1}$-Torsionspunkten sind (d.h. die entsprechenden Punkte sind keine $l^i$-Torsionspunkte), falls alle Nullstellen von $g(X)$ $x$-Koordinaten „echter“ $l^i$-Torsionspunkte waren. Wir werden im folgenden Lemma die theoretische Voraussetzung dafür angeben, wie wir mit Hilfe dieser Polynome die Spur des Frobenius-Endomorphismus modulo Primzahlpotenzen berechnen können.

**Lemma 8.2** *Seien die beiden Eigenwerte des charakteristischen Polynoms des Frobenius-Endomorphismus für die Primzahl $l$ verschieden. Dann gilt in obiger Situation für alle Punkte $Q$, deren $x$-Koordinate eine Nullstelle von $\tilde{g}(X)$ ist, die Gleichung $\Phi_E(Q) = \tilde{\alpha} \cdot Q$, wobei $\tilde{\alpha} \equiv \alpha \bmod l^i$ und $0 \leq \tilde{\alpha} < l^{i+1}$ ist.*

**Beweis:** Sei $Q$ ein Punkt, der die Voraussetzungen des Lemmas erfüllt. Aus dem Beweis zu Lemma 8.1 folgt, daß die $x$-Koordinate von $P = l \cdot Q$ eine Nullstelle von $g(X)$ ist und daß damit $\Phi_E(P) = \alpha \cdot P$ gilt. Nehmen wir an, es wäre $\tilde{\alpha} = \alpha' + r \cdot l^i$. Dann gilt

$$\alpha \cdot l \cdot Q \quad = \quad \alpha \cdot P \quad = \quad \Phi_E(P) \quad = \quad \Phi_E(l \cdot Q) \quad = \quad \alpha' \cdot l \cdot Q.$$

Da $Q$ ein $l^{i+1}$-Torsionspunkt ist, folgt hieraus $\alpha \equiv \alpha' \bmod l^i$.

Nehmen wir nun an, es gäbe zwei verschiedene Punkte $Q_1$ und $Q_2$, die die Voraussetzungen des Lemmas erfüllen und für die $\Phi_E(Q_j) = (\alpha + r_j \cdot l^i) \cdot Q_j$ mit $r_1 \not\equiv r_2 \bmod l$ gilt. Dann besitzt das charakteristische Polynom $X^2 - c\,X + q$ des Frobenius-Endomorphismus modulo $l^{i+1}$ die beiden Nullstellen $\alpha + r_j\, l^i$. Modulo $l$ sind beide Nullstellen aber gleich, so daß dies im Widerspruch zu der Voraussetzung steht, daß die beiden Nullstellen modulo $l$ verschieden sein sollen. Die Größenbeschränkung für $\tilde{\alpha}$ folgt direkt, da nach Lemma 8.1 alle „geeigneten“ Punkte $Q$ $l^{i+1}$-Torsionspunkte sind. ■

Wir werden bei der Beschreibung eines Algorithmus zur Bestimmung von $c \bmod l^{i+1}$ im Elkies-Fall genauer darauf eingehen, welche Auswirkungen die Voraussetzung hat, daß beide Eigenwerte modulo $l$ verschieden sind. Im folgenden Unterabschnitt beschreiben wir zuerst die Bestimmung eines geeigneten Polynoms $\tilde{g}(X)$ für den Fall, daß der Frobenius-Endomorphismus keine unter $\Phi_E$ invariante $l$-Gruppe besitzt.

### 8.1.2 Der Atkin-Fall

Wir nehmen in diesem Unterabschnitt an, daß es keine $l$-Gruppe gibt, die invariant unter dem Frobenius-Endomorphismus $\Phi_E$ ist. Wir haben in Kapitel 3 bewiesen, daß das $l$-te modulare Polynom in diesem Fall in irreduzible Faktoren vom Grad $d$ zerfällt. Dabei ist $d$ die kleinste positive Zahl, so daß eine beliebige $l$-Gruppe invariant unter $\Phi_E^d$ ist. Damit gibt es für jede $l$-Gruppe $C$ eine Zahl $1 \leq k < l$, so daß für jeden Punkt $P \in C$ gilt $\Phi_E^d(P) = k \cdot P$. Offensichtlich folgt hieraus

$$\Phi_E^{d \cdot \mathrm{ord}(k)}(P) \quad = \quad P.$$

Sei $f(X)$ analog zum Elkies-Fall ein Polynom, dessen Nullstellen durch verschiedene $x$-Koordinaten von $l^i$-Torsionspunkten gegeben werden, die invariant unter $\Phi_E^{\hat{d}}$ sind. Für den Fall $i = 1$ (d.h. für eine ungerade Primzahl $l$) können wir nach obigen Bemerkungen $f(X) = \psi_l(X, Y) \in \mathbb{F}_q[E]$ und $\hat{d} = d \cdot \mathrm{ord}(k)$ wählen. Leider kennen wir $k$ und damit die Ordnung von $k$ nicht; es ist aber leicht möglich, alle Möglichkeiten für $\mathrm{ord}(k)$ durchzuprobieren. Bestimmen wir dann $d'$ aus $\hat{d}$ analog zu (8.1), so erhalten wir durch Übertragung der Gleichung von Punkten in eine Polynomgleichung bei Betrachtung der $x$-Koordinate

$$X^{q^{d'}} \quad \equiv \quad X \mod f(X).$$

Damit existiert auch in diesem Fall ein Teiler $g(X)$ von $f(X)$ vom Grad $d'$. Analog zu Lemma 8.1 können wir damit ein Polynom $\tilde{g}(X)$ bestimmen, das dann ein Teiler des $l^{i+1}$-ten Divisionspolynoms ist. Mit Hilfe dieses Polynoms und dem im folgenden Abschnitt vorgestellten Algorithmus können wir dann $c \bmod l^{i+1}$ bestimmen.

Um dieses Verfahren iterieren zu können, müssen wir zeigen, daß auch das Polynom $\tilde{g}(X)$ wieder zerfällt. Dazu formulieren wir das folgende Lemma.

**Lemma 8.3** *Sei $P$ ein unter $\Phi_E^{\hat{d}}$ invarianter $l^i$-Torsionspunkt, $\hat{d} > 0$ minimal mit dieser Eigenschaft und $Q$ ein Punkt, so daß $l \cdot Q = P$ ist. Dann ist die kleinste Potenz des Frobenius-Endomorphismus, unter der $Q$ invariant ist, entweder $\hat{d}$ oder $\hat{d} \cdot l$.*

**Beweis:** Offensichtlich gilt

$$l \cdot \Phi_E^{\hat{d}}(Q) \quad = \quad \Phi_E^{\hat{d}}(P) \quad = \quad P \quad = \quad l \cdot Q.$$

Damit ist $\Phi_E^{\hat{d}}(Q) = Q + T_l$, wobei $T_l$ ein $l$-Torsionspunkt ist. Ist $T_l = \mathcal{O}$, so ist $Q$ invariant unter $\Phi_E^{\hat{d}}$; ansonsten zeigt man leicht durch Induktion, daß $\Phi_E^{j \cdot \hat{d}}(Q) = Q + j \cdot T_l$ gilt. Hiermit folgt die Behauptung des Lemmas. ∎

Mit Hilfe dieses Lemmas und den gerade vorgestellten Ideen folgt dann, daß das Polynom $\tilde{g}(X)$ selbst wieder mindestens einen Teiler vom Grad $d'$ oder $d' \cdot l$ besitzt.

Finden wir einen solchen Teiler, so können wir das Verfahren iterieren, um Teiler "größerer" Divisionspolynome zu bestimmen.

Damit haben wir für beide mögliche Fälle ein Verfahren beschrieben, wie wir geeignete Teiler von Divisionspolynomen bestimmen können. Im folgenden Abschnitt werden wir beschreiben, wie wir unter Kenntnis eines solchen Teilers $\tilde{g}(X)$ den Wert der Gruppenordnung modulo $l^{i+1}$ bestimmen können.

## 8.2 Bestimmung der Spur modulo $l^{i+1}$

Wir werden in diesem Abschnitt beschreiben, wie wir die Spur $c$ des Frobenius-Endomorphismus modulo $l^{i+1}$ bestimmen können. Dabei setzen wir voraus, daß wir Polynome $g(X)$ und $\tilde{g}(X)$ sowie Zahlen $\alpha \bmod l^i$ bzw. $c \bmod l^i$ wie im letzten Abschnitt beschrieben kennen. Analog zu Abschnitt 8.1 unterscheiden wir wieder zwei Fälle.

### 8.2.1 Der Elkies-Fall

Wir machen in diesem Abschnitt dieselben Voraussetzungen wie in Abschnitt 8.1.1, insbesondere kennen wir also den Wert von $\alpha$. Wir haben dort in Lemma 8.2 schon gezeigt, daß für Punkte $P$, deren $x$-Koordinate eine Nullstelle von $\tilde{g}(X)$ ist, die Gleichung $\Phi_E(P) = \tilde{\alpha}\cdot P$ gilt, wobei $\tilde{\alpha} \equiv \alpha \bmod l^i$ ist. Wählen wir $0 \leq \tilde{\alpha} < l^{i+1}$, so ist $\tilde{\alpha}$ eindeutig bestimmt, wenn die beiden Eigenwerte des Frobenius-Endomorphismus modulo der Primzahl $l$ verschieden sind. Ist dies nicht der Fall, so kann es maximal zwei verschiedene Werte für $\tilde{\alpha}$ geben.

Zur Bestimmung eines Wertes für $\tilde{\alpha}$ setzen wir $\tilde{\alpha}$ an als $\tilde{\alpha} = \alpha + k \cdot l^i$ mit einer unbekannten Zahl $0 \leq k < l$. Dann transformieren wir wie gewohnt die Gleichung $\Phi_E(P) = \tilde{\alpha} \cdot P = (\alpha + k \cdot l^i) \cdot P$ in Polynomgleichungen modulo $\tilde{g}(X)$. Damit müssen wir testen, für welche Zahl $0 \leq k < l$

$$(x^q, y^q) \quad = \quad (\alpha + k \cdot l^i) \cdot (x, y)$$

für Punkte $(x, y)$ mit $\tilde{g}(x) = 0$ erfüllt ist. Sind die beiden Eigenwerte modulo $l$ verschieden, so gibt es für alle solche Punkte nur eine Zahl $k$ und daher können wir testen, ob die Kongruenz

$$(X^q, Y^q) \quad \equiv \quad (\alpha + k \cdot l^i) \cdot (X, Y) \mod \tilde{g}(X) \tag{8.2}$$

gilt. Im anderen Fall kann es sein, daß diese Kongruenz modulo eines Teilers von $\tilde{g}(X)$, aber nicht modulo $\tilde{g}(X)$ gilt. Dies stellen wir fest, indem wir beide Seiten modulo $\tilde{g}(X)$ berechnen und dann den ggT von $\tilde{g}(X)$ und der Differenz beider Seiten dieser Gleichung bestimmen. Besitzt dieser ggT einen Grad größer Null, so haben wir einen möglichen Wert für $\tilde{\alpha}$ gefunden. Durch Umformung der Gleichung

$$X^2 - cX + q \quad \equiv \quad (X - \tilde{\alpha}) \cdot (X - \tilde{\beta}) \mod l^{i+1}$$

für das charakteristische Polynom des Frobenius-Endomorphismus können wir mit $\tilde{\alpha}$ auch den Wert von $c \bmod l^{i+1}$ als $c \equiv \tilde{\alpha} + q \cdot \tilde{\alpha}^{-1} \bmod l^{i+1}$ berechnen.

Bei der Implementierung des Algorithmus können wir uns darauf beschränken, die $x$-Koordinaten der Polynomgleichung (8.2) zu überprüfen. Da $\alpha$ nicht von $l$ geteilt wird ($\mathrm{ggT}(l, q) = 1$) und $l$ ungerade vorausgesetzt wird, gilt für verschiedene Zahlen $0 \leq j_1, j_2 < l$ immer

$$\alpha + j_1 \cdot l^i \quad \not\equiv \quad \pm(\alpha + j_2 \cdot l^i) \bmod l^{i+1}.$$

Deshalb können wir nur mit Hilfe eines Tests der $x$-Koordinaten den Wert $\tilde{\alpha}$ eindeutig bestimmen. Damit erhalten wir den folgenden Algorithmus, um unter den gegebenen Voraussetzungen die Spur des Frobenius-Endomorphismus modulo $l^{i+1}$ exakt zu berechnen:

**Algorithmus 8.4** [Bestimmung von $c \bmod l^{i+1}$ im Elkies-Fall]

**Eingabe:** Polynom $f(X)$ und $\alpha \bmod l^i$ wie beschrieben.
**Ausgabe:** $c \bmod l^{i+1}$.

| | | | |
|---|---|---|---|
| Bestimme $d \leftarrow \mathrm{ord}(\alpha) \bmod l^i$ und daraus $d'$ wie in (8.1). | | | (1) |
| Bestimme einen Faktor $g(X)$ von $f(X)$ vom Grad $d'$. | | | (2) |
| Bestimme $\tilde{g}(X)$ wie in Lemma 8.1. | | | (3) |
| Berechne $xq(X) \equiv X^q \bmod \tilde{g}(X)$. | | | (4) |
| FOR $k = 0, \ldots, l-1$ | | | (5) |
| | Setze $\tilde{\alpha} \leftarrow \alpha + k \cdot l^i$. | | (6) |
| | Setze $z(X) \leftarrow X \cdot \psi_{\tilde{\alpha}}(X,Y) - \psi_{\tilde{\alpha}-1}(X,Y) \cdot \psi_{\tilde{\alpha}+1}(X,Y) \bmod \tilde{g}(X)$. | | (7) |
| | Setze $h(X) \leftarrow \mathrm{ggT}\left(xq(X) \cdot \psi_{\tilde{\alpha}}^2(X,Y) - z(X)\ ,\ \tilde{g}(X)\right)$. | | (8) |
| | IF $\deg(h(X)) > 0$ | | (9) |
| | THEN | RETURN $c \equiv \tilde{\alpha} + q \cdot \tilde{\alpha}^{-1} \bmod l^{i+1}$. | (10) |

Man beachte, daß man sich zur Iterierung dieses Verfahrens den gefundenen Wert $\tilde{\alpha} \bmod l^{i+1}$ und das Polynom $h(X)$ merken muß. Diese Werte dienen bei der folgenden Iteration als neue Eingabe. In der Praxis ist dieses Verfahren nur selten iterierbar, denn der Wert von $d'$ und damit der Grad des Polynoms $\tilde{g}(X)$ wächst im allgemeinen schnell an. Dennoch ist es häufig möglich, zumindest für kleine Primzahlen bis 19 die Spur modulo des Quadrats der verwendeten Primzahl auszurechnen. Couveignes und Morain haben in [CoMo94] allerdings ein Verfahren vorgestellt, wie man die Spur $c$ modulo Potenzen von Primzahlen auch mit Hilfe von Polynomen noch kleineren Grades bestimmen kann. Dabei hängt der Grad der verwendeten Polynome aber ebenfalls von der Ordnung des Eigenwertes $\alpha$ ab, so daß für diese Variante ähnliche Probleme wie bei dem hier beschriebenen Algorithmus auftreten.

### 8.2.2 Der Atkin-Fall

In diesem Fall gehen wir analog zum Schoof-Algorithmus vor. Wir nehmen wiederum an, daß wir ein Polynom $f(X)$ und den Wert von $c \bmod l^i$ kennen. Dann berechnen wir daraus $\tilde{g}(X)$ wie in Lemma 8.1 beschrieben. Für alle $l^{i+1}$-Torsionspunkte gilt im Endomorphismenring die folgende Gleichung (setze dabei $q' \equiv q \bmod l^{i+1}$):

$$\Phi_E^2 + q' \quad = \quad c \cdot \Phi_E. \tag{8.3}$$

Da wir $0 \leq c' < l^i$ mit $c' \equiv c \bmod l^i$ schon kennen, müssen wir die Menge $\{c' + k \cdot l^i;\ k = 0, \ldots, l-1\}$ von möglichen Werten für $c$ modulo $l^{i+1}$ testen. Dazu überprüfen wir diese Gleichung nur für $l^{i+1}$-Torsionspunkte, deren $x$-Koordinate Nullstelle von $\tilde{g}(X)$ ist. Da diese Punkte nach Konstruktion von $\tilde{g}(X)$ alle „echte" $l^{i+1}$-Torsionspunkte (d.h. keine $l^i$-Torsionspunkte) sind, können wir damit $c \bmod l^{i+1}$ eindeutig bestimmen. Wie üblich formen wir für diesen Test die Gleichung (8.3) in Polynomgleichungen modulo $\tilde{g}(X)$ um. Die sich dann ergebenden Gleichungen haben wir ausführlich in [Mü91] ausgerechnet und geben sie daher hier nur an. Dabei sei $\psi_j$ das $j$-te Divisionspolynom (zur Abkürzung lassen wir im folgenden das Argument $(X, Y)$ weg) als Polynom auf $E$ betrachtet und $q'$ der kleinste positive Rest von $q \bmod l^{i+1}$. Analog zu Abschnitt 8.2.1 können wir uns auch in diesem Fall auf das Überprüfen der $x$-Koordinaten beschränken, falls $c \not\equiv 0 \bmod l^i$ ist. Wollen wir für eine Zahl $0 \leq t < l^{i+1}$ mit $t \not\equiv 0 \bmod l^i$ testen, ob $c \equiv t \bmod l^{i+1}$ gilt, so müssen wir die folgende Gleichung überprüfen:

$$\begin{aligned}\Big(\Big(\psi_{q'-1} \cdot \psi_{q'+1} - \psi_{q'}^2 \cdot (X^{q^2} + X^q + X)\Big) \cdot \beta^2 \,+\, \alpha\Big) \cdot \psi_t^{2q} \\ +\quad \psi_{t-1}^q \cdot \psi_{t+1}^q \cdot \beta^2 \cdot \psi_{q'}^2 \quad \equiv \quad 0 \mod \tilde{g}(X).\end{aligned}$$

Dabei seien $\alpha$ und $\beta$ folgendermaßen gewählt:

$$\begin{aligned}\alpha &\equiv \psi_{q'}^2 \left(\psi_{q'+2} \cdot \psi_{q'-1}^2 - \psi_{q'-2} \cdot \psi_{q'+1}^2 - 4\,(X^3 + aX + b)^{(q^2+1)/2} \cdot \psi_{q'}^3\right) \bmod \tilde{g}(X), \\ \beta &\equiv 4Y \cdot \psi_{q'} \cdot \left(\left(X - X^{q^2}\right) \cdot \psi_{q'}^2 - \psi_{q'-1} \cdot \psi_{q'+1}\right) \mod \tilde{g}(X).\end{aligned} \tag{8.4}$$

Ist $c \equiv 0 \bmod l^i$, so müssen wir auch die $y$-Koordinate der Gleichung im Endomorphismenring überprüfen. Beachte, daß wir dabei den Fall $c \equiv 0 \bmod l^{i+1}$ mit einer speziellen Formel testen müssen. Dies können wir tun, indem wir überprüfen, ob

$$\left(X^{q^2} - X\right) \cdot \psi_{q'}^2 + \psi_{q'-1} \cdot \psi_{q'+1} \quad \equiv \quad 0 \mod \tilde{g}(X)$$

gilt. Für alle anderen Zahlen $0 \leq t < l^{i+1}$, die von $l^i$ geteilt werden, müssen wir zusätzlich zu obigem Test der $x$-Koordinaten auch noch die folgende Formel für die $y$-Koordinate überprüfen:

$$\begin{aligned}4Y \cdot (X^3 + aX + b)^{(q-1)/2} \cdot \psi_t^{3q} \Big(((2X^{q^2} + X) \cdot \psi_{q'}^2 - \psi_{q'-1} \cdot \psi_{q'+1}) \cdot \alpha \cdot \beta^2 - \\ Y \cdot (X^3 + aX + b)^{(q^2-1)/2} \cdot \beta^3 \cdot \psi_{q'}^2 - \alpha^3 \cdot \psi_{q'}^2\Big) \;- \\ \beta^3 \cdot \psi_{q'}^2 \cdot \left(\psi_{t+2} \cdot \psi_{t-1}^2 - \psi_{t-2} \cdot \psi_{t+1}^2\right)^q \quad \equiv \quad 0 \mod \tilde{g}(X).\end{aligned} \tag{8.5}$$

Bei der Implementierung dieser Formel sollte man beachten, daß wir ein Polynom $h(X) \in \mathbb{F}_q[X]$ leicht mit Hilfe der folgenden Formel zur $q$-ten Potenz erheben können:

$$h(X)^q \quad \equiv \quad h\left(X^q\right) \bmod \tilde{g}(X).$$

Außerdem kann man verschiedene Teile dieser Formel vorberechnen, so daß diese nicht mehr für alle Werte $t$ neu berechnet werden müssen (siehe [Mü91]). Damit erhalten wir den folgenden Algorithmus:

**Algorithmus 8.5** [Bestimmung von $c \bmod l^{i+1}$ im Atkin-Fall]

**Eingabe:** elliptische Kurve $E = (a, b)$, Polynom $f(X)$, $\hat{d}$ und kleinsten pos. Rest $c' \equiv c \bmod l^i$ wie beschrieben.

**Ausgabe:** $c \bmod l^{i+1}$.

| | | | | | |
|---|---|---|---|---|---|
| Bestimme $d'$ aus $\hat{d}$ mit (8.1). | | | | | (1) |
| Bestimme einen Faktor $g(X)$ von $f(X)$ vom Grad $d'$. | | | | | (2) |
| Bestimme $\tilde{g}(X)$ mit Lemma 8.1. | | | | | (3) |
| Berechne $xq(X) \equiv X^q \bmod \tilde{g}(X)$ und $xq2(X) \equiv X^{q^2} \bmod \tilde{g}(X)$. | | | | | (4) |
| Berechne $\alpha$ und $\beta$ wie in (8.4). | | | | | (5) |
| Berechne $kl \leftarrow ((\psi_{q'-1} \cdot \psi_{q'+1} - \psi_{q'}^2 \cdot (xq2(X) + xq(X) + X)) \cdot \beta^2 + \alpha) \bmod \tilde{g}(X)$. | | | | | (6) |
| IF $c' = 0$ und $(xq2(X) - X) \cdot \psi_{q'}^2 + \psi_{q'-1} \cdot \psi_{q'+1} \equiv 0 \bmod \tilde{g}(X)$ | | | | | (7) |
| THEN | RETURN $c \equiv 0 \bmod l^{i+1}$. | | | | (8) |
| FOR $k = 0, \ldots, l-1$ | | | | | (9) |
| | Setze $t \leftarrow c' + k \cdot l^i$. | | | | (10) |
| | IF $kl \cdot \psi_t^{2q} + \psi_{t-1}^q \cdot \psi_{t+1}^q \cdot \beta^2 \cdot \psi_{q'}^2 \equiv 0 \bmod \tilde{g}(X)$ /*$x$-Test erfüllt*/ | | | | (11) |
| | THEN | IF $c' \neq 0$ /* $c \not\equiv 0 \bmod l^i$ */ | | | (12) |
| | | THEN | RETURN $c \equiv t \bmod l^{i+1}$. | | (13) |
| | | ELSE | /* Teste $y$-Koordinate */. | | (14) |
| | | | IF Formel (8.5) erfüllt | | (15) |
| | | | THEN | RETURN $c \equiv k \cdot l^i \bmod l^{i+1}$. | (16) |

Auch in diesem Fall kann das Verfahren iteriert werden, wenn man zusätzlich zu $c \bmod l^{i+1}$ auch noch das Polynom $\tilde{g}(X)$ zurückgibt. Dann liefert Lemma 8.3, daß das Polynom $\tilde{g}(X)$ entweder einen Teiler vom Grad $d'$ oder $d' \cdot l$ besitzt. Zur praktischen Anwendung dieses Algorithmus gelten dieselben Bemerkungen wie bei der Bestimmung der Spur modulo Primzahlpotenzen im Elkies-Fall.

# Kapitel 9

# Untersuchung der Spezialfälle

Wir haben bei der Beschreibung der Theorie in Kapitel 3 zwei Voraussetzungen an die elliptische Kurve $E/\mathbb{F}_q$ gestellt, die erfüllt sein müssen, um mit Hilfe von modularen (bzw. äquivalenten) Polynomen Information über die Gruppenordnung $\#E(\mathbb{F}_q)$ bestimmen zu können. Insbesondere mußten wir in Korollar 3.12 voraussetzen, daß $E$ nicht supersingulär und nicht $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist. Wir werden in diesem Kapitel Algorithmen beschreiben, mit denen wir diese Voraussetzungen testen können. Sind die Voraussetzungen aus Korollar 3.12 nicht erfüllt, so wird bei diesem Test ein „wahrscheinlicher" Kandidat für die Ordnung der Gruppe $E(\mathbb{F}_q)$ bestimmt. In dem ersten Abschnitt werden wir uns besonders um die Supersingularität kümmern; anschließend wird die zweite Bedingung, die Existenz spezieller Isogenien, untersucht werden.

## 9.1 Test auf Supersingularität

Wir wollen für eine gegebene elliptische Kurve $E/\mathbb{F}_q$ überprüfen, ob $E$ supersingulär oder ordinär ist und dabei wollen wir, falls $E$ supersingulär ist, direkt die „wahrscheinliche Gruppenordnung" von $E(\mathbb{F}_q)$ bestimmen. Dabei bedeutet „wahrscheinliche Gruppenordnung", daß für „mehrere" zufällig gewählte Punkte aus der Punktgruppe $E(\mathbb{F}_q)$ diese wahrscheinliche Gruppenordnung ein Vielfaches der jeweiligen Punktordnung ist. In der Praxis ist eine solche Zahl „immer" die gesuchte Gruppenordnung. Wir werden in Kapitel 11 einen Algorithmus vorstellen, mit dem wir die Korrektheit einer solchen wahrscheinlichen Gruppenordnung beweisen oder widerlegen können. Der vorzustellende Test auf Supersingularität basiert auf dem Satz von Waterhouse [Wa69, Th. 4.1, Seite 536]:

**Satz 9.1 (Satz von Waterhouse)**
*Sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_{p^d}$. Dann gilt für die Gruppenordnung $\#E(\mathbb{F}_{p^d}) = p^d + 1 - c$ mit $|c| \leq 2\sqrt{p^d}$, wobei $c$ eine der folgenden Bedingungen erfüllt:*

1. $\mathrm{ggT}(c, p) = 1$,

2. *$c = \pm 2\sqrt{p^d}$, falls $d$ gerade,*

3. *$c = \pm\sqrt{p^d}$, falls $d$ gerade und $p \equiv 2 \bmod 3$,*

4. *$c = \pm p^{(d+1)/2}$, falls $d$ ungerade und $p = 2, 3$,*

5. *$c = 0$, falls $d$ ungerade oder $d$ gerade und $p \equiv 3 \bmod 4$.*

In diesem Satz finden wir eine Liste von möglichen Ordnungen von Punktgruppen elliptischer Kurven über dem endlichen Körper $\mathbb{F}_{p^d}$. Diese Liste können wir für supersinguläre Kurven stark einschränken, denn wir wissen aus Proposition 2.19, daß eine elliptische Kurve $E$ genau dann supersingulär ist, wenn $c \equiv 0 \bmod p$ gilt (dabei sei $c$ die Spur des Frobenius-Endomorphismus wie in Satz 9.1). Damit gilt für supersinguläre elliptische Kurven $\mathrm{ggT}(c, p) = p$ und Fall 1 in Satz 9.1 kann nicht auftreten. Weiterhin beschäftigen wir uns in dieser Arbeit nur mit Körpern der Charakteristik größer drei und somit kann auch Fall 4 nicht auftreten. Damit verbleiben nur fünf Möglichkeiten (die Fälle 2, 3 und 5) für die Gruppenordnung von $E(\mathbb{F}_q)$, falls $E$ supersingulär sein sollte. Diese überprüfen wir, indem wir für einen zufälligen Punkt $Q \in E(\mathbb{F}_q)$ und den sich aus Satz 9.1 ergebenden Kandidaten $m$ für die Gruppenordnung das Vielfache $m \cdot Q$ berechnen. Ist $m$ die Gruppenordnung von $E(\mathbb{F}_q)$, so muß nach dem Satz von Lagrange $m \cdot Q = \mathcal{O}$ gelten. Ist also $m \cdot Q \neq \mathcal{O}$, so wissen wir mit Sicherheit, daß $m$ nicht die Gruppenordnung von $E(\mathbb{F}_q)$ sein kann. Haben wir alle sich aus dem Satz von Waterhouse ergebenden möglichen Werte so mit negativem Resultat überprüft, so kann $E$ nicht supersingulär sein. Finden wir allerdings einen Wert $m$ mit $m \cdot Q = \mathcal{O}$, so haben wir ein Vielfaches der Ordnung von $Q$ in dem Lösungsintervall und damit einen Kandidaten für die Gruppenordnung gefunden. Diesen Kandidaten überprüfen wir dann mit Hilfe weiterer zufällig gewählter Punkte. Durch Kombination dieser beiden Ideen erhalten wir den auf der folgenden Seite angegebenen Algorithmus 9.2 zum Test auf Supersingularität.

In Schritt (1) dieses Algorithmus wird die zufällige Wahl eines Punktes aus $E(\mathbb{F}_q)$ benötigt. Dies kann leicht mit Hilfe des folgenden probabilistischen Algorithmus geschehen: wir wählen ein Element $x \in \mathbb{F}_q$ zufällig und testen, ob $x^3 + ax + b$ ein Quadrat in $\mathbb{F}_q$ ist. Bei positivem Test bestimmen wir eine Quadratwurzel $y \in \mathbb{F}_q$ aus $x^3 + ax + b$. Dann ist $(x, y)$ ein zufälliger Punkt der Punktgruppe $E(\mathbb{F}_q)$. Der Quadrattest kann mit Hilfe des im Beweis zu Lemma 2.24 angegebenen Kriteriums geschehen; zum Wurzelziehen kann man einen probabilistischen Algorithmus von Shanks (siehe [Mü91]) verwenden.

**Algorithmus 9.2** [Test auf Supersingularität]

**Eingabe:** elliptische Kurve $E$ über Körper $\mathbb{F}_{p^d}$.
**Ausgabe:** „$E$ ordinär" oder „wahrscheinliche Ordnung" von $E(\mathbb{F}_{p^d})$.

| | | | | |
|---|---|---|---|---|
| Wähle zufällig Punkt $Q \in E(\mathbb{F}_{p^d})$. | | | | (1) |
| IF $d$ ungerade oder ($d$ gerade und $p \equiv 3 \bmod 4$) | | | | (2) |
| THEN | Setze $m \leftarrow p^d + 1$. | | | (3) |
| | IF $m \cdot Q = \mathcal{O}$ | | | (4) |
| | THEN | Überprüfe $m$ durch weitere zufällige Punkte, ggf. RETURN „wahrsch. Ordnung" $p^d + 1$. | | (5) |
| IF $d$ gerade | | | | (6) |
| THEN | FORALL $c \in \{\pm p^{d/2}, \pm 2p^{d/2}\}$ | | | (7) |
| | | Setze $m \leftarrow p^d + 1 - c$. | | (8) |
| | | IF $m \cdot Q = \mathcal{O}$ | | (9) |
| | | THEN | Überprüfe $m$ durch weitere zufällige Punkte, ggf. RETURN „wahrsch. Ordnung " $m$. | (10) |
| RETURN „$E$ ordinär" . | | | | (11) |

Damit wissen wir, wie wir für eine gegebene elliptische Kurve $E/\mathbb{F}_q$ überprüfen können, ob $E$ supersingulär ist und für supersinguläre elliptische Kurven können wir direkt einen wahrscheinlichen Kandidaten für die Gruppenordnung $\#E(\mathbb{F}_q)$ berechnen. In dem folgenden Abschnitt beschäftigen wir uns nun mit dem Test der zweiten Voraussetzung aus Korollar 3.12.

## 9.2 Isogenie zu Kurven der $j$-Invariante 0 oder 1728

In diesem Abschnitt wollen wir einen Algorithmus entwickeln, der überprüft, ob eine ordinäre, über $\mathbb{F}_q$ definierte elliptische Kurve $E$ $\mathbb{F}_q$-isogen zu einer elliptischen Kurve mit $j$-Invariante 0 oder 1728 ist. Existiert eine solche Isogenie, so wollen wir wiederum einen „wahrscheinlichen" Kandidaten für die Gruppenordnung $\#E(\mathbb{F}_q)$ bestimmen.

Angenommen, $E$ ist $\mathbb{F}_q$-isogen zu einer elliptischen Kurve $E'$ mit $j(E') \in \{0, 1728\}$. Dann muß auch die elliptische Kurve $E'$ über $\mathbb{F}_q$ definiert sein. Damit wissen wir aus dem schon im Beweis zu Satz 3.10 benutzten Kriterium von Tate (Seite 30), daß eine solche $\mathbb{F}_q$-Isogenie zwischen $E$ und $E'$ genau dann existiert, wenn die Ordnungen der Punktgruppen der beiden Kurven über $\mathbb{F}_q$ gleich sind. Damit können wir den Existenz-Test für eine solche Isogenie auf die Überprüfung „weniger" Gruppenordnungen reduzieren. Dabei handelt es sich um alle Gruppenordnungen, die Punktgruppen von elliptischen Kurven mit $j$-Invariante 0 oder 1728 besitzen können. Alle diese möglichen Gruppenordnungen $m$ überprüfen wir wie in Algorithmus 9.2, indem wir für einen zufälligen Punkt $Q \in E(\mathbb{F}_q)$ testen, ob $m \cdot Q = \mathcal{O}$ ist. Ist dies nicht der Fall, so kann $m$ nicht die Gruppenordnung sein; ansonsten ist $m$ ein „wahrscheinlicher" Kandidat für die Gruppenordnung und wir überprüfen dies mit Hilfe mehrerer zufälliger Punkte bzw. versuchen, dies mit Algorithmus 11.2 zu beweisen.

Damit verbleibt noch das Problem, wie wir alle möglichen Ordnungen von Punktgruppen von elliptischen Kurven mit $j$-Invariante 0 oder 1728 bestimmen können. Beide Möglichkeiten für die $j$-Invariante werden wir in den folgenden Abschnitten untersuchen.

### 9.2.1 $j$-Invariante 0

Wir zeigen zuerst, wie wir alle Ordnungen von Punktgruppen von elliptischen Kurven $E'$ mit $j$-Invariante 0 bestimmen können. Der Endomorphismenring der ordinären elliptischen Kurven mit $j$-Invariante 0 ist $\mathbb{Z}[\omega]$, wobei $\omega^2 + \omega + 1 = 0$ ist, d.h. der Ganzheitsring von $\mathbb{Q}(\sqrt{-3})$. Dies folgt aus der Tatsache, daß solche Kurven nach [Si85, Th10.1, Seite 103] genau 6 Automorphismen besitzen und daß $\mathbb{Z}[\omega]$ die einzige Maximalordnung eines imaginärquadratischen Zahlkörpers mit sechs Einheiten ist. Genauer können wir sogar die folgende Fallunterscheidung treffen:

1. Falls $p \equiv 2 \bmod 3$, dann ist die elliptische Kurve $E' : y^2 = x^3 + 1$ mit $j$-Invariante 0 supersingulär (vgl. [Si85, Bsp. 4.4, Seite 143]). Damit sind alle elliptischen Kurven mit $j$-Invariante 0 supersingulär, denn isomorphe Kurven besitzen denselbem Endomorphismenring. Demnach wurde die Gruppenordnung von $E$ schon im Test auf Supersingularität überprüft und wir müssen diesen Fall nicht weiter untersuchen.

2. Sei nun $p \equiv 1 \bmod 3$ und $E'$ eine elliptische Kurve mit $j$-Invariante 0. Dann wird der Frobenius-Endomorphismus $\Phi_{E'}$ für $E'$ über $\mathbb{F}_q$ auf ein Element $\pi$ in $\mathbb{Z}[\omega] \cong \mathrm{End}_{\overline{\mathbb{F}}_q}(E')$ mit Norm $q$ abgebildet. Weiterhin gilt für die Gruppenordnung
$$\#E'(\mathbb{F}_q) \quad = \quad 1 - (\pi + \overline{\pi}) + q.$$
Kennen wir also alle Elemente der Norm $q$ in $\mathbb{Z}[\omega]$, so können wir alle möglichen Gruppenordnungen von elliptischen Kurven über $\mathbb{F}_q$ mit $j$-Invariante 0 berechnen.

   Angenommen, wir kennen ein Element $\pi$ der Norm $q$ in $\mathbb{Z}[\omega]$. Alle anderen Elemente von $\mathbb{Z}[\omega]$ mit Norm $q$ können sich von $\pi$ nur um ein Element mit Norm 1 (d.h. eine Einheit) unterscheiden. Damit kennen wir mit einem Element der Norm $q$ sogar alle Elemente von $\mathbb{Z}[\omega]$ mit Norm $q$ und somit alle möglichen Ordnungen von Punktgruppen von elliptischen Kurven mit $j$-Invariante 0, denn die Einheitengruppe von $\mathbb{Z}[\omega]$ ist wohlbekannt als
$$\mathbb{Z}[\omega]^* \quad = \quad \{\pm 1, \pm\omega, \pm\omega^2\}.$$

Wir betrachten nun zuerst mögliche Gruppenordnungen für elliptische Kurven mit $j$-Invariante 1728, bevor wir einen Algorithmus zur Bestimmung eines Elements der Norm $q$ angeben.

### 9.2.2 $j$-Invariante 1728

Die Bestimmung der Ordnungen der Punktgruppen über $\mathbb{F}_q$ von elliptischen Kurven der $j$-Invariante 1728 läuft vollkommen analog. Deshalb geben wir nur kurz den Ablauf an:

1. Falls $p \equiv 3 \bmod 4$, so ist die elliptische Kurve $E' : y^2 = x^3 + x$ mit $j$-Invariante 1728 supersingulär [Si85, Bsp. 4.5, Seite 144]. Damit sind in diesem Fall alle elliptischen Kurven mit $j$-Invariante 1728 supersingulär, so daß mögliche Gruppenordnungen schon in Algorithmus 9.2 überprüft wurden.

2. Sei $p \equiv 1 \bmod 4$. Die Endomorphismenringe von ordinären elliptischen Kurven mit $j$-Invariante 1728 sind isomorph zu dem Ganzheitsring $\mathbb{Z}[i]$ von $\mathbb{Q}(i)$ (vgl. [Si85, Th. 10.1, Seite 103]). Aus einem Element $\pi$ der Norm $q$ in $\mathbb{Z}[i]$ erhalten wir wiederum alle Elemente der Norm $q$ in $\mathbb{Z}[i]$, indem wir $\pi$ mit allen Einheiten aus $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ multiplizieren. Damit kennen wir auch alle möglichen Ordnungen von $E'(\mathbb{F}_q)$ für elliptische Kurven $E'$ mit $j$-Invariante 1728.

Im nächsten Abschnitt beschreiben wir einen Algorithmus für das noch ausstehende Problem der Bestimmung eines Elementes der Norm $q$ in den Maximalordnungen $\mathbb{Z}[i]$ bzw. $\mathbb{Z}[\omega]$. Danach können wir dann den Algorithmus formulieren, mit dem wir alle möglichen Ordnungen von elliptischen Kurven mit $j$-Invariante 0 oder 1728 überprüfen und so die zweite Voraussetzung in Korollar 3.12 sicherstellen können.

### 9.2.3 Bestimmung von Elementen der Norm $q$

Wir beschreiben in diesem Abschnitt einen Algorithmus, wie wir in dem Ganzheitsring $\mathcal{O}_K$ des algebraischen Zahlkörpers $\mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(i)$ bzw. $\mathbb{Q}(\sqrt{-3})$ ein Element der Norm $q = p^d$ bestimmen können. Dieser Algorithmus wird ausführlich in [BuMü92, Seite 18ff] beschrieben; wir geben hier daher nur die zum Verständnis notwendigen Grundlagen der algebraischen Zahlentheorie an. Dabei können wir ohne Einschränkung voraussetzen, daß $d$ ungerade ist, denn ansonsten ist $p^{d/2}$ ein gewünschtes Element.

Sei also $D \in \{-4, -3\}$, $K = \mathbb{Q}(\sqrt{D})$ und $\mathcal{O}_K$ die Maximalordnung von $K$. Ein **invertierbares Ideal** $\mathcal{A}$ von $\mathcal{O}_K$ ist eine Teilmenge von $K$ der Form

$$\mathcal{A} = \alpha \cdot \left( \mathbb{Z}\, a + \mathbb{Z}\, \frac{b + \sqrt{D}}{2} \right) \tag{9.1}$$

mit $\alpha \in K^*$, $a, b \in \mathbb{Z}$, $a > 0$, $c = \frac{b^2 - D}{4a} \in \mathbb{Z}$ und $\mathrm{ggT}(a, b, c) = 1$. Man sollte beachten, daß die Maximalordnung $\mathcal{O}_K$ von $K$ ebenfalls ein invertierbares Ideal ist, nämlich

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\, \frac{D + \sqrt{D}}{2}.$$

Dann definieren wir auf folgende Weise eine Äquivalenzrelation auf der Menge der invertierbaren Ideale von $K$:

$$\mathcal{A} \sim \mathcal{B} \quad \Longleftrightarrow \quad \mathcal{A} = \gamma \cdot \mathcal{B} \quad \text{mit } \gamma \in K^*.$$

Damit wird die Menge aller invertierbaren Ideale von $K$ in verschiedene Äquivalenzklassen eingeteilt. Wir werden die Äquivalenzklasse des Ideals $\mathcal{A}$ aus (9.1) durch das Tripel $(a, b, c)$ darstellen. Ein weiterer wichtiger Begriff ist der eines **reduzierten Ideals**. Ein Ideal $(a, b, c)$ heißt reduziert, wenn gilt

$$|b| \leq a \leq c \qquad \text{und} \qquad b \geq 0 \quad \text{falls } |b| = a \text{ oder } a = c.$$

Man kann zeigen, daß es in jeder Äquivalenzklasse genau ein reduziertes Ideal gibt, so daß wir das reduzierte Ideal einer Äquivalenzklasse als Vertreter dieser Äquivalenzklasse auffassen können. Folgender Algorithmus berechnet zu einem gegebenen Ideal $(a', b', c')$ ein Element $\gamma \in K^*$, so daß $\gamma \cdot (a', b', c')$ reduziert ist.

**Algorithmus 9.3** [Reduktion eines Ideals]

**Eingabe:** Ideal $\mathcal{A} = (a', b', c')$, Körper $K$.
**Ausgabe:** $\gamma \in K^*$ und reduziertes Ideal $(a, b, c) = \gamma \cdot \mathcal{A}$ .

| | | | |
|---|---|---|---|
| Setze $\gamma \leftarrow 1$, $(a, b, c) \leftarrow (a', b', c')$. | | | (1) |
| | Reduziere $b$ modulo $2a$, so daß $\lvert b\rvert < a$ und passe $c$ entsprechend an. | | (2) |
| BREAKIF $\lvert b\rvert \leq a \leq c$. | | | (3) |
| | Setze $\gamma \leftarrow \gamma \cdot \frac{2c}{b+\sqrt{D}}$ und $(a, b, c) \leftarrow (c, -b, a)$. | | (4) |
| IF $b < 0$ und entweder $a = -b$ oder $a = c$ | | | (5) |
| THEN | IF $a = c$ | | (6) |
| | THEN | Setze $\gamma \leftarrow \gamma \cdot \frac{2a}{b+\sqrt{D}}$. | (7) |
| | Setze $(a, b, c) \leftarrow (a, -b, c)$. | | (8) |

Wir zeigen nun zuerst, daß es genau dann ein Element in $\mathcal{O}_K$ mit Norm $p^d$ gibt, wenn es auch ein Element in $\mathcal{O}_K$ mit Norm $p$ gibt. Sei zuerst $\pi \in \mathcal{O}_K$ ein Element mit Norm $p$. Offensichtlich ist dann $\pi^d$ ein Element mit Norm $p^d$. Nehmen wir daher nun an, daß in der Maximalordnung ein Element mit Norm $p^d$ existiert. Für ein beliebiges Element $\pi = x + y\,\frac{D+\sqrt{D}}{2} \in \mathcal{O}_K$ können wir folgende Formel für die Norm dieses Elementes bestimmen:

$$N(\pi) \quad = \quad \left(x + \frac{y \cdot D}{2}\right)^2 - \left(\frac{y}{2}\right)^2 \cdot D. \tag{9.2}$$

Gibt es also ein Element der Norm $p^d$, so muß $D$ ein Quadrat modulo $4p^d$ und – da $d$ ungerade ist – auch modulo $p$ sein. Wir geben nun einen Algorithmus an, wie wir dann ein Element mit Norm $p$ bestimmen können.

Dazu definieren wir die **Norm eines Ideals** $\mathcal{A} = \alpha \cdot \left( \mathbb{Z}\, a + \mathbb{Z}\, \frac{b+\sqrt{D}}{2} \right)$ als

$$N(\mathcal{A}) \quad = \quad |N(\alpha)| \cdot a.$$

Finden wir damit ein Hauptideal (also ein Ideal der Form $\beta \cdot \mathcal{O}_K$) der Norm $p$ und gilt dabei $\beta \in \mathcal{O}_K$, so ist $\beta$ ein Element in $\mathcal{O}_K$ mit Norm $p$ (für $D < 0$ ist wegen (9.2) die Norm von Elementen der Maximalordnung immer nichtnegativ). Sei nun das Ideal

$$\mathcal{P} \quad = \quad \mathbb{Z}\, p + \mathbb{Z}\, \frac{b+\sqrt{D}}{2}$$

gegeben, wobei $b \in \mathbb{Z}$ so gewählt ist, daß $4p$ ein Teiler von $b^2 - D$ ist (dies ist nach obiger Bemerkung möglich). Dann ist $\mathcal{P}$ ein Ideal der Norm $p$. Wir berechnen nun mit Algorithmus 9.3 zu den beiden Idealen $\mathcal{P}$ und $\mathcal{O}_K$ das zugehörige reduzierte Ideal. Dabei beachte man, daß wegen [Wei63, Prop. 6.4.2, Seite 243] beide Körper $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{-3})$ Klassenzahl eins besitzen und daß beide reduzierten Ideale gleich sind. Mit Algorithmus 9.3 erhalten wir auch Elemente $\gamma_{\mathcal{P}} \in K^*$ und $\gamma_{\mathcal{O}_K} \in K^*$, so daß gilt

$$\gamma_{\mathcal{P}} \cdot \mathcal{P} \quad = \quad \gamma_{\mathcal{O}_K} \cdot \mathcal{O}_K.$$

Hieraus folgt aber

$$\mathcal{P} \quad = \quad \gamma_{\mathcal{O}_K} \cdot \gamma_{\mathcal{P}}^{-1} \cdot \mathcal{O}_K$$

und $\pi = \gamma_{\mathcal{O}_K} \cdot \gamma_{\mathcal{P}}^{-1}$ ist ein Element des Körpers mit Norm $p$. Damit müssen wir nur noch überprüfen, ob $\pi$ sogar ein Element der Maximalordnung ist. Wegen der Primalität von $p$ kann es weiterhin nur zwei Ideale mit Norm $p$ geben, so daß dieser Algorithmus genau dann ein Element der Maximalordnung mit Norm $p$ berechnet, wenn ein solches Element existiert. Zusammenfassend erhalten wir den folgenden Algorithmus:

**Algorithmus 9.4** [Element mit Norm $q$]

**Eingabe:** Zahlkörper $\mathbb{Q}(\sqrt{D})$ mit $D \in \{-3, -4\}$, $q = p^d$.
**Ausgabe:** $\pi \in \mathcal{O}_K$ mit $N(\pi) = p^d$ oder „Element mit Norm $q$ existiert nicht“ .

| | | | |
|---|---|---|---|
| IF $d$ gerade | | | (1) |
| THEN | RETURN $p^{d/2}$. | | (2) |
| IF $\left(\frac{D}{p}\right) \neq 1$ | | | (3) |
| THEN | RETURN „Element mit Norm $q$ existiert nicht“ . | | (4) |
| ELSE | Bestimme $b \in \mathbb{Z}$ mit $b^2 \equiv D \bmod 4p$. | | (5) |
| | Setze $\mathcal{P} \leftarrow \left(p, b, \frac{b^2-D}{4p}\right)$. | | (6) |
| | Berechne $\gamma_{\mathcal{P}}$ mit $\gamma_{\mathcal{P}} \cdot \mathcal{P}$ reduziert. (Algorithmus 9.3) | | (7) |
| | Setze $\mathcal{O}_K \leftarrow \left(1, D, \frac{D^2-D}{4}\right)$. | | (8) |
| | Berechne $\gamma_{\mathcal{O}_K}$ mit $\gamma_{\mathcal{O}_K} \cdot \mathcal{O}_K$ reduziert. (Algorithmus 9.3) | | (9) |
| | Setze $\pi \leftarrow \gamma_{\mathcal{O}_K} \cdot \gamma_{\mathcal{P}}^{-1}$. | | (10) |
| | IF $\pi^d \in \mathcal{O}_K$ | | (11) |
| | THEN | RETURN $\pi^d$. | (12) |
| | ELSE | RETURN „Element mit Norm $q$ existiert nicht“ . | (13) |

Wir haben noch nicht beschrieben, wie wir eine geeignete Zahl $b$ in Schritt (5) finden. Dazu bestimmen wir mit Hilfe des RESSOL-Algorithmus eine Quadratwurzel modulo $p$ aus $D$. Da $D$ nach Voraussetzung entweder kongruent null oder eins modulo 4 ist, können wir daraus leicht eine Lösung modulo $4p$ bestimmen. Diese Teilalgorithmen verwenden wir in dem folgenden Abschnitt, um einen Algorithmus zum Test der zweiten Voraussetzung zu formulieren.

### 9.2.4 Ein Algorithmus zum Test der zweiten Voraussetzung

Damit haben wir alle Voraussetzungen geschaffen, um den folgenden Algorithmus zu formulieren, mit dessen Hilfe wir die zweite Voraussetzung aus Korollar 3.12 überprüfen können. Der Algorithmus ergibt sich direkt aus den in den beiden vorherigen

Abschnitten vorgestellten Ideen.

**Algorithmus 9.5** [Gruppenordnungen für Kurven mit $j$-Invariante 0, 1728]

**Eingabe:** nicht supersinguläre elliptische Kurve $E/\mathbb{F}_q$, $q = p^d$.
**Ausgabe:** „nicht $\mathbb{F}_q$-isogen zu Kurve $E'$ mit $j(E') \in \{0, 1728\}$" oder „wahrscheinliche Ordnung" von $E(\mathbb{F}_q)$.

<table>
<tr><td colspan="5">Wähle zufällig $Q \in E(\mathbb{F}_q)$.</td><td>(1)</td></tr>
<tr><td colspan="5">IF $p \equiv 1 \bmod 4$</td><td>(2)</td></tr>
<tr><td rowspan="6">THEN</td><td colspan="4">Wende Algorithmus 9.4 mit Eingabe $(D = -4,\ q)$ an.</td><td>(3)</td></tr>
<tr><td colspan="4">IF Algorithmus 9.4 liefert Element $\pi$ mit Norm $q$</td><td>(4)</td></tr>
<tr><td rowspan="4">THEN</td><td colspan="3">FORALL $x \in \{\pm\pi, \pm i \cdot \pi\}$</td><td>(5)</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Setze $m \leftarrow q + 1 - (x + \overline{x})$.</td><td>(6)</td></tr>
<tr><td colspan="2">IF $m \cdot Q = \mathcal{O}$</td><td>(7)</td></tr>
<tr><td>THEN</td><td>Überprüfe $m$ durch „mehrere" zufällige Punkte, ggf. RETURN „wahrsch. Ordnung" $m$.</td><td>(8)</td></tr>
<tr><td colspan="5">IF $p \equiv 1 \bmod 3$</td><td>(9)</td></tr>
<tr><td rowspan="6">THEN</td><td colspan="4">Wende Algorithmus 9.4 mit Eingabe $(D = -3,\ q)$ an.</td><td>(10)</td></tr>
<tr><td colspan="4">IF Algorithmus 9.4 liefert Element $\tau$ mit Norm $q$</td><td>(11)</td></tr>
<tr><td rowspan="4">THEN</td><td colspan="3">FORALL $y \in \{\pm\tau, \pm\omega \cdot \tau, \pm\omega^2 \cdot \tau\}$</td><td>(12)</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Setze $n \leftarrow q + 1 - (y + \overline{y})$.</td><td>(13)</td></tr>
<tr><td colspan="2">IF $n \cdot Q = \mathcal{O}$</td><td>(14)</td></tr>
<tr><td>THEN</td><td>Überprüfe $n$ durch „mehrere" zufällige Punkte, ggf. RETURN „wahrsch. Ordnung" $n$.</td><td>(15)</td></tr>
<tr><td colspan="5">RETURN „nicht $\mathbb{F}_q$-isogen zu Kurve $E'$ mit $j(E') \in \{0, 1728\}$" .</td><td>(16)</td></tr>
</table>

Damit haben wir alle in Kapitel 3 gestellten Voraussetzungen behandelt. Wir können daher im folgenden davon ausgehen, daß diese Voraussetzungen erfüllt sind. Die in diesem Kapitel vorgestellten Teilalgorithmen werden bei der Beschreibung des Gesamtalgorithmus 10.5 in Kapitel 10 in einem ersten Schritt verwendet werden, um die in Kapitel 3 gemachten Voraussetzungen sicherzustellen.

# Kapitel 10

# Der komplette Algorithmus

In diesem Kapitel beschreiben wir einen Algorithmus zur Bestimmung der Punktanzahl einer elliptischen Kurve über einem endlichen Körper der Charakteristik größer drei. Dabei verwenden wir die in den vorhergehenden Kapiteln entwickelten Teilalgorithmen als Unterprogramme. Mit diesen Algorithmen können wir in einer ersten Phase des Algorithmus Information über die Gruppenordnung bestimmen, nämlich mögliche Werte für die Gruppenordnung modulo „kleiner" Primzahlen oder Primzahlpotenzen. Im ersten Abschnitt setzen wir die bisher schon angegebenen Teilalgorithmen zusammen und erhalten so die erste Phase des Algorithmus. Im zweiten Abschnitt dieses Kapitels geben wir einen Algorithmus an, mit dem wir aus dieser Information einen sehr wahrscheinlichen Kandidaten für die Gruppenordnung berechnen können. Bei diesem Algorithmus wird es sich um eine Variante des schon in [Mü91] vorgestellten Babystep-Giantstep Algorithmus handeln. Anschließend kombinieren wir alle vorgestellten Teilalgorithmen und erhalten so eine Beschreibung des gesamten Algorithmus zur Lösung des vorgegebenen Problems. Im letzten Abschnitt dieses Kapitels geben wir einige Hinweise zur Implementierung des Algorithmus sowie praktische Beispiele mit Laufzeitergebnissen an.

## 10.1 Die erste Phase

Im ersten Abschnitt kombinieren wir die in den vorherigen Kapiteln vorgestellten Ideen und Teilalgorithmen. Wir stellen so einen Algorithmus vor, mit dem wir für eine ungerade, von der Charakteristik $p$ des Körpers $\mathbb{F}_q$ verschiedene Primzahl $l$ Information über die Gruppenordnung $\#E(\mathbb{F}_q) \bmod l$ berechnen können. Dabei unterscheiden wir die Fälle, daß die Primzahl $l$ größer oder kleiner als die Charakteristik $p$ des Körpers $\mathbb{F}_q$ ist.

Die Grundstruktur des Algorithmus ist folgendermaßen: zuerst wird ein zum $l$-ten modularen Polynom äquivalentes Polynom $G_l(X,Y) \in \mathbb{F}_p[X,Y]$ (wie in Kapitel 5 beschrieben) bestimmt. An der Anzahl der Nullstellen des Polynoms $G_l(X, j(E)) \in \mathbb{F}_q[X]$ über $\mathbb{F}_q$ können wir mit Hilfe von Satz 4.13 und Korollar 3.12 feststellen, ob es eine unter dem Frobenius-Endomorphismus invariante $l$-Gruppe gibt. Ist dies nicht der Fall, so bestimmen wir den Zerfällungstyp von $G_l(X, j(E))$ und erhalten so eine Menge von möglichen Werten für $c \bmod l$ (beachte dazu Tabelle 3.1). Gibt es hingegen eine unter $\Phi_E$ invariante $l$-Gruppe, so können wir – falls $p > l$ ist – ein Polynom $f_C(X)$ vom Grad $(l-1)/2$ (wie in Kapitel 6 beschrieben) berechnen und damit den Wert von $c \bmod l$ exakt bestimmen.

Wir verwenden im folgenden bei der Angabe des Algorithmus immer nur zum modularen Polynom äquivalente Polynome, wie wir sie in den Abschnitten 5.1 und 5.2 beschrieben haben. In Klammern geben wir die entsprechenden Algorithmen bei Verwendung der äquivalenten Polynome aus den Abschnitten 5.3 bzw. 5.4 an. Zur besseren Übersichtlichkeit verwenden wir innerhalb des Algorithmus einen Subalgorithmus, in dem wir alle Fälle behandeln, in denen wir nur partielle Information über $c \bmod l$ erhalten. Diesen Subalgorithmus werden wir direkt anschließend beschreiben.

**Algorithmus 10.1** [Information über $c \bmod l$]

**Eingabe:** ordinäre elliptische Kurve $E/\mathbb{F}_q$, nicht $\mathbb{F}_q$-isogen zu ellipt. Kurve mit $j$-Invariante 0 oder 1728, ungerade Primzahl $l \neq p$.

**Ausgabe:** Menge von Möglichkeiten für $c \bmod l$.

| | | |
|---|---|---|
| IF $l > p$ | | (1) |
| THEN | Bestimme äquivalentes Polynom $G_l(X,Y) \in \mathbb{F}_p[X,Y]$ mit Algorithmus 5.8 (Algorithmus 5.26). | (2) |
| ELSE | Bestimme äquivalentes Polynom $G_l(X,Y) \in \mathbb{F}_p[X,Y]$ mit Algorithmus 5.27 (Algorithmus 5.28). | (3) |
| Berechne $j(E)$ und setze $\tilde{G}_l(X) \leftarrow G_l(X, j(E))$. | | (4) |
| Berechne $d_1 \leftarrow \deg\left(\mathrm{ggT}(X^q - X, \tilde{G}_l(X))\right)$. /* Anzahl Nullst. in $\mathbb{F}_q$*/ | | (5) |
| IF $d_1 \geq 1$ und $p > l$ | | (6) |
| THEN | Bestimme eine Nullstelle von $\tilde{G}_l(X)$. | (7) |
| | Bestimme mögliche Werte für $(\tilde{a}, \tilde{b}, P_1)$ mit Algorithmus 7.3 (Algorithmus 7.6). | (8) |
| | Bestimme Polynom $f_C(X) \in \mathbb{F}_q[X]$ mit Algorithmus 7.8. | (9) |
| | Bestimme $c \bmod l$ mit Algorithmus 7.9. | (10) |
| | RETURN $\{c \bmod l\}$. | (11) |
| ELSE | Setze $\tilde{G}_l(X) \leftarrow \tilde{G}_l(X) \,/\, \mathrm{ggT}(X^q - X, \tilde{G}_l(X))$. | (12) |
| | RETURN Ausgabe von Algorithmus 10.2. | (13) |

Anschließend beschreiben wir den Teilalgorithmus, den wir zur Bestimmung partieller Information anwenden werden. Dabei müssen wir die in Tabelle 3.1 angegebenen verschiedenen Fälle unterscheiden, weswegen der Algorithmus etwas unübersichtlich erscheint. Außerdem können wir wie in Abschnitt 4.6 beschrieben durch die Untersuchung des Legendre-Symbols $\left(\frac{p}{l}\right)$ einige mögliche Zerfällungstypen des äquivalenten Polynoms ausschließen.

**Algorithmus 10.2** [Partielle Information]

**Eingabe:** $d_1$ und $\tilde{G}_l(X)$ wie in Algorithmus 10.1.
**Ausgabe:** Menge von Möglichkeiten für $c \bmod l$.

| | | | | | |
|---|---|---|---|---|---|
| IF $d_1 = 1$ /* Zerf. typ $(1l)$ */ | | | | | (1) |
| THEN | RETURN $\{\pm 2\sqrt{q} \bmod l\}$. | | | | (2) |
| IF $d_1 = l+1$ /* Zerf. typ $(1\ldots1)$ */ | | | | | (3) |
| THEN | Setze $\alpha \leftarrow \sqrt{q} \bmod l$. | | | | (4) |
| | RETURN $\{\pm(\alpha + q \cdot \alpha^{-1}) \bmod l^2\}$. | | | | (5) |
| Setze $d_{rest} \leftarrow \deg(\tilde{G}_l(X))$. | | | | | (6) |
| IF $\left(\frac{p}{l}\right) = 1$ | | | | | (7) |
| THEN | FORALL $d$ mit $d \mid d_{rest}$ und $(d-1) \cdot \frac{d_{rest}}{d}$ gerade, in aufsteigender Reihenfolge | | | | (8) |
| | | Berechne $d_2 \leftarrow \deg\left(\mathrm{ggT}(X^{q^d} - X, \tilde{G}_l(X)\right)$. | | | (9) |
| | | IF $d_2 > 0$ und $d_1 = 2$ /* Zerf. typ $(11d\ldots d)$ */ | | | (10) |
| | | THEN | RETURN $\left\{(\zeta_d + 1) \cdot \sqrt{q\,\zeta_d^{-1}};\ \zeta_d \in \mathbb{F}_l,\ \mathrm{ord}(\zeta_d) = d\right\}$. | | (11) |
| | | IF $d_2 > 0$ und $d_1 = 0$ /* Zerf. typ $(d\ldots d)$ */ | | | (12) |
| | | THEN | RETURN $\left\{(\zeta_d + 1) \cdot \sqrt{q\,\zeta_d^{-1}};\ \zeta_d \in \mathbb{F}_{l^2},\ \mathrm{ord}(\zeta_d) = d\right\}$. | | (13) |
| ELSE | FORALL $d$ mit $d \mid d_{rest}$ und $(d-1) \cdot \frac{d_{rest}}{d}$ ungerade, in aufsteigender Reihenfolge | | | | (14) |
| | | Berechne $d_2 \leftarrow \deg\left(\mathrm{ggT}(X^{q^d} - X, \tilde{G}_l(X)\right)$. | | | (15) |
| | | IF $d_2 > 0$ und $d_1 = 2$ /* Zerf. typ $(11d\ldots d)$ */ | | | (16) |
| | | THEN | RETURN $\left\{(\zeta_d + 1) \cdot \sqrt{q\,\zeta_d^{-1}};\ \zeta_d \in \mathbb{F}_l,\ \mathrm{ord}(\zeta_d) = d\right\}$. | | (17) |
| | | IF $d_2 > 0$ und $d_1 = 0$ /* Zerf. typ $(d\ldots d)$ */ | | | (18) |
| | | THEN | RETURN $\left\{(\zeta_d + 1) \cdot \sqrt{q\,\zeta_d^{-1}};\ \zeta_d \in \mathbb{F}_{l^2},\ \mathrm{ord}(\zeta_d) = d\right\}$. | | (19) |

Bei der Beschreibung des Algorithmus fasse man alle Quadratwurzeln natürlich als

Quadratwurzeln modulo $l$ auf. Diese Quadratwurzeln kann man entweder mit dem schon erwähnten probabilistischen Algorithmus von Shanks (vgl. [Mü91]) oder durch Ausprobieren bestimmen (beachte, daß $l$ im allgemeinen klein ist).

Damit haben wir Teilalgorithmen beschrieben, wie wir Information über die Spur $c$ des Frobenius-Endomorphismus einer elliptischen Kurve modulo Primzahlen $l$ bestimmen können. Im folgenden Abschnitt beschäftigen wir uns damit, wie wir unter Kenntnis von „genügend" Information daraus die Ordnung der Punktgruppe bestimmen können.

## 10.2 Kombination der berechneten Information

Sei $E$ eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$, für die wir mögliche Werte für die Spur $c$ des Frobenius-Endomorphismus $\Phi_E$ modulo Primzahlen bzw. Primzahlpotenzen $l_i$ für $i = 0, \ldots, k$ kennen. Dabei nehmen wir weiterhin an, daß das Produkt aller Moduln $l_i$ größer als die Größe des Hasse-Intervalls ist, d.h.

$$\prod_{i=0}^{k} l_i \quad > \quad 4\sqrt{q}.$$

Wir werden in diesem Abschnitt einen Algorithmus vorstellen, wie wir aus diesen Informationen einen Kandidaten für die Gruppenordnung von $E(\mathbb{F}_q)$ bestimmen können. In der Praxis ist dieser Kandidat „immer" die gesuchte Gruppenordnung.

Sei $m_3$ das Produkt aller Moduln $l_i$, für die wir $c \bmod l_i$ exakt kennen. Mit Hilfe des Chinesischen Restsatzes können wir eine Zahl $c_3 \in \{0, \ldots, m_3 - 1\}$ bestimmen, so daß $c \equiv c_3 \bmod m_3$ gilt. Alle weiteren Moduln $l_i$ werden auf zwei Mengen $L_1, L_2$ aufgeteilt. Aus der Liste der möglichen Werte für $c$ modulo der Elemente in $L_1$ bestimmen wir mit dem Chinesischen Restsatz die Menge $C_1$ aller möglichen Werte für $c$ modulo dem Produkt $m_1$ aller Primzahlen (bzw. Primzahlpotenzen) in $L_1$. Auf analoge Weise berechnen wir aus der Menge $L_2$ eine Zahl $m_2$ und eine Menge $C_2$ von möglichen Werten für $c \bmod m_2$. Dabei werden $L_1$ und $L_2$ so gewählt, daß die Mengen $C_1$ und $C_2$ ungefähr gleich viele Elemente enthalten, insbesondere soll keine der Mengen $C_i, i = 1, 2$ leer sein (d.h. $m_i > 1$ für $i = 1, 2$). Dann gilt

- $c \equiv c_1 \bmod m_1$, wobei $c_1 \in C_1$,
- $c \equiv c_2 \bmod m_2$, wobei $c_2 \in C_2$,
- $c \equiv c_3 \bmod m_3$.

Man beachte, daß wir die Mengen $C_1$ und $C_2$ berechnen können, aber die Werte von $c_1$ und $c_2$ nicht kennen. Die Elemente der Mengen $C_i, i = 1, 2$ sind modulo $m_i$ eindeutig bestimmt, so daß wir davon ausgehen können, daß alle Mengenelemente verschieden modulo $m_i$ sind. Dann existieren ganze Zahlen $r_i \in \mathbb{Z}$, $i = 1, 2$, so daß sich die Spur $c$ des Frobenius-Endomorphismus $\Phi_E$ in der folgenden Art und Weise schreiben läßt:

$$c \quad = \quad c_3 + m_3 \cdot (m_1 \, r_2 + m_2 \, r_1). \tag{10.1}$$

Die Existenz einer solchen Darstellung folgt direkt aus dem Chinesischen Restsatz. Andererseits folgt wegen des Restverhaltens der Spur $c$ für die Zahlen $r_i$

$$r_1 \equiv (c_1 - c_3)\,(m_2\, m_3)^{-1} \bmod m_1 \qquad \text{und} \qquad r_2 \equiv (c_2 - c_3)\,(m_1\, m_3)^{-1} \bmod m_2.$$

Leider kennen wir die Zahlen $c_1$ und $c_2$ nicht, aber wir kennen jeweils eine Menge von Möglichkeiten (nämlich $C_i$, $i = 1, 2$), in denen sich $c_1$ bzw. $c_2$ befindet. Damit können wir mit Hilfe dieser Formel für alle Elemente $c_{i,s} \in C_i$, $i = 1, 2$ korrespondierende Zahlen $r_{i,s}$ bestimmen und dann alle Kombinationsmöglichkeiten durchtesten, bis wir die korrekten Zahlen $r_1$, $r_2$ aus (10.1) gefunden haben. Wir bestimmen also für $1 \le s \le \#C_1$ bzw. $1 \le s \le \#C_2$ Zahlen

$$r_{1,s} \equiv (c_{1,s} - c_3)\,(m_2\, m_3)^{-1} \bmod m_1 \quad \text{und} \quad r_{2,s} \equiv (c_{2,s} - c_3)\,(m_1\, m_3)^{-1} \bmod m_2. \tag{10.2}$$

Das Testen aller Möglichkeiten in (10.1) führen wir dann geschickt mit einer Baby-step-Giantstep Strategie durch. Dazu müssen wir festlegen, welches Vertretersystem wir für die Restklassen $c_3$, $c_{1,s}$ und $c_{2,s}$ wählen. Nehmen wir dazu an, daß wir für $c_3$ den kleinsten positiven Rest und für die Restklassen $r_{1,s}$ die absolut kleinsten Reste gewählt haben; es gilt also für alle $1 \le s \le \#C_1$

$$0 \;\le\; c_3 \;<\; m_3 \qquad \text{und} \qquad \left\lfloor \frac{-m_1}{2} \right\rfloor \;<\; r_{1,s} \;\le\; \left\lfloor \frac{m_1}{2} \right\rfloor.$$

Dann erhalten wir die folgende Größenabschätzung für die Zahl $r_2$ aus (10.1).

**Lemma 10.3** *In dieser Situation gilt* $|r_2| \le m_2$.

**Beweis:** Wir formen Gleichung (10.1) um und erhalten so

$$r_2 \quad = \quad \frac{\frac{c-c_3}{m_3} - m_2\, r_1}{m_1} \quad = \quad \frac{1}{m_1\, m_3}\,(c - c_3 - m_2\, m_3\, r_1)\,.$$

Wegen der Bedingung an das Produkt aller verwendeten Moduln gilt $|c| \le 2\sqrt{q} < (m_1\, m_2\, m_3)/2$. Unter Verwendung der Abschätzung für $c_{1,s}$ und $c_3$ erhalten wir daraus

$$|r_2| \quad < \quad \frac{m_2}{2} + \frac{1}{m_1} + \frac{m_2}{2}.$$

Hieraus folgt die Behauptung des Lemmas, denn $r_2$ muß eine ganze Zahl sein. ■

Die Idee zur Bestimmung der Zahlen $c_1$ und $c_2$ ist nun folgendermaßen: für einen zufälligen Punkt $P \in E(\mathbb{F}_q)$ gilt wegen des Satzes von Lagrange (beachte $\#E(\mathbb{F}_q) = q + 1 - c$)

$$(q+1)\cdot P \quad = \quad c \cdot P \quad = \quad \Big(c_3 + m_3 \cdot (m_1\, r_2 + m_2\, r_1)\Big)\cdot P.$$

Durch Umformung dieser Gleichung erhalten wir

$$(q + 1 - c_3)\cdot P - r_1\, m_2\, m_3 \cdot P \quad = \quad r_2\, m_1\, m_3 \cdot P.$$

Damit berechnen wir mit Formel (10.2) alle Zahlen $r_{1,s}$ für $1 \leq s \leq \#C_1$ als absolut kleinsten Vertreter modulo $m_1$ und berechnen dann damit alle Punkte

$$(q + 1 - c_3) \cdot P - r_{1,s}\, m_2\, m_3 \cdot P.$$

Diese Punkte speichern wir zusammen mit dem entsprechenden Zahlen $r_{1,s}$ in einer Tabelle ab. Diesen ersten Teil des Algorithmus nennen wir die Babystep-Phase. Anschließend berechnen wir mit (10.2) alle Restklassen $r_{2,s}$ für $1 \leq s \leq \#C_2$. Dabei wählen wir als vollständiges Restsystem modulo $m_2$ die Menge $\{-m_2, \ldots, -1\}$ und stellen alle Restklassen $r_{2,s}$ in diesem Restsystem dar. Für alle diese „Zahlen" $r_{2,s}$ berechnen wir dann die Punkte

$$r_{2,s}\, m_1\, m_3 \cdot P \qquad \text{und} \qquad (r_{2,s} + m_2)\, m_1\, m_3 \cdot P \;=\; r_{2,s}\, m_1\, m_3 \cdot P + m_1\, m_2\, m_3 \cdot P$$

(bzw. zusätzlich noch $m_1\, m_2\, m_3 \cdot P$ für $r_{2,s} = -m_2$) und testen, ob einer dieser beiden (drei) Punkte in der in der Babystep-Phase berechneten Tabelle vorkommt. Nach obigem Lemma 10.3 reicht es aus, nur diese beiden (bzw. drei) Zahlen aus der Restklasse $r_{2,s}$ zu testen. Finden wir einen Punkt, der schon in der in der Babystep-Phase berechneten Tabelle vorkommt, so kennen wir Zahlen $r'_1$ und $r'_2$, für die gilt

$$(q + 1 - c_3 - r'_1\, m_2\, m_3) \cdot P \quad = \quad r'_2\, m_1\, m_3 \cdot P$$

(beachte, daß in der Babystep-Tabelle die entsprechende Zahl $r_{1,s}$ mit abgespeichert wird). Damit kennen wir ein Vielfaches der Ordnung des Punktes $P$ in dem durch den Satz von Hasse vorgegebenen Intervall. Wie in [Mü91] schon gezeigt, ist es für einen zufälligen Punkt im allgemeinen sehr wahrscheinlich, daß die Ordnung dieses Punktes größer als $4\sqrt{q}$ ist. In diesem Fall muß das berechnete Vielfache der Punkteordnung genau die gesuchte Gruppenordnung von $E(\mathbb{F}_q)$ sein. Probabilistisch können wir dies durch Wahl „einiger" weiterer zufälliger Punkte überprüfen. Scheitert einer dieser Tests, so wissen wir, daß die berechnete Zahl nicht die Gruppenordnung ist, und wir können versuchen, durch Faktorisierung der Zahl die Ordnung von $P$ und so einen Teiler der Gruppenordnung $\#E(\mathbb{F}_q)$ zu bestimmen. Ansonsten kennen wir einen „wahrscheinlichen" Kandidaten für die Gruppenordnung. Wir werden in Kapitel 11 einen Algorithmus angeben, mit dem wir die Korrektheit einer solchen „wahrscheinlichen" Gruppenordnung beweisen können. In der Praxis war es bei unserer Implementierung allerdings immer der Fall, daß eine solche „wahrscheinliche" Gruppenordnung auch die exakte Gruppenordnung von $E(\mathbb{F}_q)$ war.

Wir schreiben diese Ideen nun in Form eines Algorithmus auf. Alle in dieser Beschreibung verwendeten Symbole sollen dieselbe Bedeutung wie bei dieser Beschreibung der Idee besitzen, insbesondere soll das Produkt $m_1\, m_2\, m_3$ größer als $4\sqrt{q}$ sein. In dem Algorithmus wird wie schon in früheren Algorithmen ein zufälliger Punkt gewählt. Dies kann mit folgendem schon in [Mü91] beschriebenen Algorithmus geschehen: wähle $x \in \mathbb{F}_q$ zufällig und teste, ob $x^3 + ax + b$ ein Quadrat in $\mathbb{F}_q$ ist. In diesem Fall bestimmen wir eine Quadratwurzel $y$ aus diesem Wert und erhalten einen zufälligen Punkt $P \in E(\mathbb{F}_q)$ als $(x, y)$; ansonsten wählen wir ein anderes zufälliges Element $x \in \mathbb{F}_q$ und wiederholen das Verfahren. Das Testen auf ein Quadrat kann mit dem in Lemma 2.24 (Seite 18) angegebenen Kriterium erfolgen, zur Bestimmung einer Quadratwurzel können wir den Ressol-Algorithmus von Shanks (siehe [Mü91]) verwenden.

**Algorithmus 10.4** [Kombination der partiellen Informationen]

**Eingabe:** elliptische Kurve $E/\mathbb{F}_q$, Mengen $C_i$ möglicher Werte für $c \bmod m_i$, $(i = 1, 2)$ wie beschrieben, $c_3 \in \{0, \ldots, m_3 - 1\}$ mit $c \equiv c_3 \bmod m_3$.

**Ausgabe:** „wahrscheinliche" Gruppenordnung $\#E(\mathbb{F}_q)$.

| | | | |
|---|---|---|---|
| Wähle zufällig $P \in E(\mathbb{F}_q)$. | | | (1) |
| Setze $Q_0 \leftarrow (q + 1 - c_3) \cdot P$, $Q_1 \leftarrow (m_2\, m_3) \cdot P$, $Q_2 \leftarrow (m_1\, m_3) \cdot P$, $Q_3 \leftarrow (m_1\, m_2\, m_3) \cdot P$, $h \leftarrow 0$. | | | (2) |
| FORALL $x \in C_1$ | | | (3) |
| | Setze $r_1' \equiv (x - c_3)\,(m_2\, m_3)^{-1} \bmod m_1$ mit $\lfloor \frac{-m_1}{2} \rfloor < r_1' \le \lfloor \frac{m_1}{2} \rfloor$. | | (4) |
| | Berechne $H \leftarrow Q_0 - r_1' \cdot Q_1$ und speichere $(H, r_1')$ in einer Tabelle. | | (5) |
| FORALL $y \in C_2$ | | | (6) |
| | Setze $r_2' \equiv (y - c_3)\,(m_1\, m_3)^{-1} \bmod m_2$ mit $-m_2 \le r_2' < 0$. | | (7) |
| | IF $r_2' = -m_2$ und $(Q_3, r')$ existiert in Tabelle | | (8) |
| | THEN | Setze $h \leftarrow q + 1 - c_3 - r'\, m_2\, m_3 + m_1\, m_2\, m_3$. | (9) |
| | Berechne Punkte $H_1 \leftarrow r_2' \cdot Q_2$ und $H_2 \leftarrow r_2' \cdot Q_2 + Q_3$. | | (10) |
| | IF Eintrag $(H_1, r')$ existiert in Tabelle | | (11) |
| | THEN | Setze $h \leftarrow q + 1 - c_3 - r'\, m_2\, m_3 - r_2'\, m_1\, m_3$. | (12) |
| | IF Eintrag $(H_2, r')$ existiert in Tabelle | | (13) |
| | THEN | Setze $h \leftarrow q + 1 - c_3 - r'\, m_2\, m_3 - (r_2' + m_2)\, m_1\, m_3$. | (14) |
| | IF $h \cdot P' = \mathcal{O}$ für „mehrere" zufällige Punkte $P' \in E(\mathbb{F}_q)$ | | (15) |
| | THEN | RETURN „wahrsch. Gruppenordnung" $h$. | (16) |
| | ELSE | Faktorisiere $h$. | (17) |
| | | Bestimme Ordnung von $P$ durch Ausprobieren aller Teiler. | (18) |
| | | Verändere $c_3, m_3$ entsprechend und beginne wieder in (1). | (19) |

Offensichtlich muß der Algorithmus bei korrekter Eingabe terminieren, denn alle Kombinationen der sich aus den Mengen $C_1$ und $C_2$ ergebenden Werte werden durchprobiert, so daß mit Sicherheit auch die beiden „korrekten" Zahlen $r_1$ und $r_2$ getestet werden. Für diese Zahlen terminiert der Algorithmus dann in Schritt (14). Für die Laufzeit des Algorithmus ist die Größe der beiden Mengen $C_1$ und $C_2$ bestimmend, denn schlimmstenfalls müssen wir ungefähr $\#C_1 + 2\,\#C_2$ viele Punktadditionen durchführen. In der Praxis sollte man daher – falls es der zur Verfügung stehende Hauptspeicher zuläßt – beide Mengen ungefähr gleich groß wählen. Wir werden zum Abschluß dieses Kapitels einige praktische Ergebnisse unserer Implementierung dieses Algorithmus angeben.

## 10.3 Der Gesamtalgorithmus

Kombinieren wir alle diese Teilalgorithmen, so erhalten wir den folgenden Gesamtalgorithmus, der das in dieser Arbeit behandelte Problem der Bestimmung der Gruppenordnung einer elliptischen Kurve über einem endlichen Körper der Charakteristik größer drei löst:

**Algorithmus 10.5** [Gesamtalgorithmus]

**Eingabe:** elliptische Kurve $E = (a, b)$ über $\mathbb{F}_q$.
**Ausgabe:** „wahrscheinliche" Gruppenordnung $\#E(\mathbb{F}_q)$.

| | | |
|---|---|---|
| IF $E$ supersingulär (Test mit Algorithmus 9.2) | | (1) |
| THEN | RETURN „wahrscheinliche" Gruppenordnung (Ausgabe von Algorithmus 9.2). | (2) |
| IF $E$ $\mathbb{F}_q$-isogen zu Kurve mit $j$-Inv. 0, 1728 (Algorithmus 9.5) | | (3) |
| THEN | RETURN „wahrscheinliche" Ordnung (Ausgabe von Algorithmus 9.5). | (4) |
| Initialisiere Menge $C$ aller bisherigen Möglichkeiten und Produkt $m$ aller Moduln. | | (5) |
| Setze $l \leftarrow 3$. | | (6) |
| | Berechne Information über $c \bmod l$ mit Algorithmus 10.1. | (7) |
| | Bestimme neue Menge $C$ (Chinesischer Restsatz). | (8) |
| | Setze $m \leftarrow m \cdot l$, $l \leftarrow$ nächste Primzahl. | (9) |
| UNTIL $m \geq 4\sqrt{q}$. | | (10) |
| Berechne Mengen $C_1$, $C_2$ und $m_1$, $m_2$, $m_3$ (vgl. Abschnitt 10.2). | | (11) |
| Wende Babystep-Giantstep Algorithmus 10.4 an. | | (12) |
| RETURN „wahrscheinliche" Gruppenordnung als Ausgabe von Algorithmus 10.4. | | (13) |

Wir haben uns bei dieser Beschreibung auf die Bestimmung von Information über die Gruppenordnung modulo Primzahlen beschränkt. Wie wir in Kapitel 8 gezeigt haben, können wir unter Umständen auch Information über die Gruppenordnung modulo Potenzen von Primzahlen bestimmen. Dies ist in der Praxis allerdings nur selten der Fall, da die in den Algorithmen 8.4 bzw. 8.5 verwendeten Polynome in der Regel einen Grad besitzen, der für praktische Berechnungen zu groß ist. Dennoch kann man Algorithmus 10.5 leicht modifizieren, so daß auch Potenzen von Primzahlen benutzt werden können.

## 10.4 Implementierung und praktische Erfolge

In diesem Abschnitt werden wir die Beschreibung unserer Implementierung für Primkörper aus den Abschnitten 5.6 und 7.4 fortsetzen. Außerdem werden wir einige mit dieser Implementierung berechnete Gruppenordnungen angeben, darunter auch den zur Zeit bestehenden „Weltrekord", die Ordnung einer elliptischen Kurve über einem Primkörper mit 425-stelliger Charakteristik. Eine ausführliche Beschreibung der Implementierung mit vielen weiteren praktischen Beispielen findet man in [Le94] und [Ma94].

Da in den beschriebenen Algorithmen überwiegend Operationen mit Polynomen über $\mathbb{F}_p$ stattfinden, ist es sehr wichtig, eine sehr effiziente Polynomarithmetik zu verwenden. Die von uns benutzte Arithmetik verwendet zur Multiplikation von Polynomen eine Variante der FFT-Methode (analog zu der Beschreibung der Arithmetik für Fourierreihenentwicklungen aus Abschnitt 7.4). Dies hat sich bei unseren Rechnungen als absolut notwendig erwiesen (betrachte etwa nur die enormen Laufzeiten zur Berechnung von $Y^p \bmod f_C(X)$ aus Tabelle 7.3). Eine genaue Beschreibung dieser Arithmetik findet man in [Sh95]. Dort findet man auch bessere Algorithmen zur Bestimmung des Zerfällungstyps eines Polynoms, die wir in Algorithmus 10.2 (Bestimmung partieller Information mit Hilfe der Idee von Atkin) verwenden.

Für große Primzahlen $l$ (z.B. $l \geq 500$) haben wir mit unserer praktischen Implementierung festgestellt, daß es nicht sinnvoll ist, den exakten Zerfällungstyp des $l$-ten äquivalenten Polynoms zu bestimmen. Wir berechnen nur noch die Anzahl der Nullstellen des äquivalenten Polynoms in $\mathbb{F}_p$, so daß wir wissen, ob eine unter $\Phi_E$ invariante $l$-Gruppe existiert oder nicht. Existiert eine solche Gruppe, so können wir mit Hilfe des in Kapitel 7 geschilderten Verfahrens die Spur modulo $l$ exakt ausrechnen. Dabei wirkt sich die Laufzeitzunahme durch die größere Anzahl von Möglichkeiten für den gesuchten Eigenwert nicht so stark aus wie die Bestimmung des exakten Zerfällungstyps des $l$-ten äquivalenten Polynoms. Existiert andererseits keine unter $\Phi_E$ invariante $l$-Gruppe und ist der Zerfällungstyps des $l$-ten äquivalenten Polynoms $(d\,d \dots d)$, so erhalten wir mit Tabelle 3.1 $\varphi(d)$ viele Möglichkeiten für $c \bmod l$. Für große Werte von $l$ ist diese Anzahl oft auch „sehr groß", so daß wir nur wenig neue Information erhalten. In der Praxis ist es daher sinnvoller, eine neue Primzahl $l'$ zu testen und zu hoffen, daß eine unter $\Phi_E$ invariante $l'$-Gruppe existiert.

Heuristisch kann man annehmen, daß etwa für jede zweite Primzahl $l$ eine unter $\Phi_E$ invariante $l$-Gruppe in $E(\overline{\mathbb{F}}_p)$ existiert. Damit können wir für ungefähr jede zweite Primzahl $l$ die Gruppenordnung modulo $l$ exakt berechnen. Nach unseren praktischen Erfahrungen stimmt diese Annahme mit der Praxis überein. Dies gewinnt an Bedeutung, denn die Abbruchbedingung aus Algorithmus 10.5 (Schritt (11)) muß in der Praxis geändert werden. Bricht man die Repeat-until Schleife in Schritt (11) schon dann ab, wenn das Produkt der verwendeten Moduln größer als $4\sqrt{q}$ ist, so ist in der Regel die Anzahl der zu testenden Möglichkeiten für die Gruppenordnung sehr groß. Daher berechnen wir für weitere, noch nicht benutzte ungerade Primzahlen $l$ Information über die Gruppenordnung modulo $l$ und verändern die Mengen $C_i$ (vgl. Algorithmus 10.4) so, daß sie möglichst klein sind, das Produkt aller verwendeten Moduln aber größer als $4\sqrt{p}$ bleibt (siehe [Ma94]).

In der Tabelle 10.1 (Seite 154) geben wir einige Laufzeiten für verschieden große Charakteristiken $p$ an. Außerdem beschreiben wir die Aufteilung der Laufzeiten auf die zwei wichtigen Teilbereiche des Algorithmus, die (unter Umständen nicht exakte) Bestimmung des Zerfällungstyps und die exakte Bestimmung der Spur modulo $l$.

Auch bei der Implementierung des Babystep-Giantstep Algorithmus 10.4 konnten einige praktische Verbesserungen erreicht werden. So kann man die Berechnung der verschiedenen Punkte in der Babystep- und der Giantstep-Phase mit Hilfe verschiedener Tabellen zusätzlich beschleunigen. Außerdem kann man durch „parallele“ Punktaddition eine Beschleunigung erreichen (siehe dazu [LMMS94]). Das Problem des Suchens in der in der Babystep-Phase berechneten Tabelle lösen wir, indem wir die Tabelle nach ihrer Berechnung mit Quicksort sortieren, so daß wir mit binärer Suche in der Giantstep-Phase suchen können. Eine weitere Verbesserung ergibt sich, wenn man die in der Tabelle berechneten Punkte nicht komplett abspeichert, sondern nur z.B. ein Computerwort abspeichert. Diese auf Hashing basierende Vorgehensweise führt zu deutlich kleineren Tabellen (den benötigten Hauptspeicherbedarf betreffend). Alle diese Ideen sind in [Ma94] genauer beschrieben. Allerdings haben diese Verbesserungen für große Charakteristiken keinen signifikanten Einfluß auf die Gesamtlaufzeit, wie wir im folgenden sehen werden.

Mit dieser Implementierung wurde der bis Ende Januar 1995 bestehende Weltrekord erzielt. Dabei handelt es sich um die Berechnung der Gruppenordnung der elliptischen Kurve

$$E: \quad y^2 \quad = \quad x^3 \; + \; 9051969\,x \; + \; 11081969$$

über dem Primkörper mit Charakteristik $p = 10^{424} + 627$. Dies ist der kleinste Primkörper mit 425-stelliger Charakteristik. Dabei berechneten wir die Gruppenordnung als $\#E(\mathbb{F}_p) = p + 1 - c$ mit

```
c = 107935028397184038159792711696870382619667\
    606645999557317560435430849755297081480014\
    447687610763674476782845355141662551498888\
    463561969473570069537180769483342760068825\
    516954031495253277258593340528327820362332\
    32712243.
```

Diese Gruppenordnung konnte mit dem im folgenden Kapitel vorzustellenden Algorithmus 11.2 leicht als korrekt bewiesen werden, denn die Gruppenordnung kann schnell als

$$\#E(\mathbb{F}_p) \quad = \quad 2^2 \cdot 3 \cdot 47^2 \cdot 61 \cdot 352201 \cdot \mathrm{p}391$$

faktorisiert werden. Zur Berechnung dieser Gruppenordnung war eine Gesamtlaufzeit von 3064 Stunden notwendig. Aus diesen enormen Rechenzeiten wird deutlich, daß die Gruppenordnung elliptischer Kurven über solch großen Körpern nur mit Hilfe einer verteilten Implementierung über ein Netz von Workstations berechnet werden kann, wenn man akzeptable Real-Zeiten erwartet. Dazu werden verschiedene Primzahlen $l$ auf einem Netz von Workstations verteilt und dort parallel berechnet (näheres dazu siehe in [Ma94] und [LMMS94]).

Im folgenden geben wir noch einige Details zu den vier größten von uns bisher berechneten Gruppenordnungen an. Dabei haben wir die Ordnung einer elliptischen Kurve über dem kleinsten Primkörper mit 303, 375, 400 bzw. 425 Dezimalstellen berechnet. Wir erhielten bei diesen Berechnungen die folgenden Daten (seien dabei Elkies-Primzahlen solche Primzahlen $l$, für die wir $c \bmod l$ exakt berechnen können). Man sollte beachten, daß sich durch Verbesserungen im Programm die Laufzeiten für 375-stellige und 400-stellige Charakteristik nicht sehr unterscheiden.

### 303-stellige Charakteristik

- $p = 10^{302} + 399, \quad E = (90569, 110869)$
- $\#E(\mathbb{F}_p) = p + 1 - c$ mit

```
c = - 78392099853395259982053426361920012256271613133 12\
      286929789466358953200631518568753474568393017477 6\
      418367482492942926744221012337083132760923224411 5\
      6548.
```

- 127 verschiedene Primzahlen $l \leq 787$ benutzt, davon 55 Elkies-Primzahlen (43.3%)
- Überprüfung von $7 \cdot 10^6$ Möglichkeiten mit Algorithmus 10.4: 40 min
- Laufzeit zur Berechnung der Zerfällungstypen: 911 Stunden (759 MiPS Tage)
- Laufzeit zur Berechnung der Spuren: 421 Stunden (351 MiPS Tage)
- Gesamtlaufzeit: 1332 Stunden (1110 MiPS Tage)

### 375-stellige Charakteristik

- $p = 10^{374} + 169, \quad E = (9051969, 11081969)$
- $\#E(\mathbb{F}_p) = p + 1 - c$ mit

```
c = 66515880622942259450404201980659722700703805586159\
    21954875689416574608874172702047221235742840908900\
    76694286008710131839030508234600082299764940462429\
    851774412934970116342270618994978236 8.
```

- 137 verschiedene Primzahlen $l \leq 839$ benutzt, davon 70 Elkies-Primzahlen (51.1%)
- Laufzeit des Babystep-Giantstep Algorithmus 10.4: 2 min
- Laufzeit zur Berechnung der Zerfällungstypen: 1295 Stunden (1080 MiPS Tage)
- Laufzeit zur Berechnung der Spuren: 821 Stunden (685 MiPS Tage)
- Gesamtlaufzeit: 2117 Stunden (1765 MiPS Tage)

### 400-stellige Charakteristik

- $p = 10^{399} + 1311, \quad E = (9051969, 11081969)$
- $\#E(\mathbb{F}_p) = p + 1 - c$ mit

```
c = - 40835957523285587377674593201589690170481310488848 87\
      95533926324933484042275237008114584300872538067364 24\
      22273739536871443693098022752247528667430763450670 96\
      836306378117534386782887221902410653579680 15.
```

- 145 verschiedene Primzahlen $l \leq 857$ benutzt, davon 73 Elkies-Primzahlen (50.3%)
- Überprüfung von 15360 Möglichkeiten mit Algorithmus 10.4: 30 min
- Laufzeit zur Berechnung der Zerfällungstypen: 1339 Stunden (1116 MiPS Tage)
- Laufzeit zur Berechnung der Spuren: 893 Stunden (744 MiPS Tage)
- Gesamtlaufzeit: 2232 Stunden (1860 MiPS Tage)

### 425-stellige Charakteristik

- $p = 10^{424} + 627, \quad E = (9051969, 11081969)$
- $\#E(\mathbb{F}_p) = p + 1 - c$ mit

```
c = 10793502839718403815979271169687038261967606645999557311\
    75604354308497552970814801444768761076367447678284535511\
    41662551498884635619694735700695371807694833427600682551\
    169540314952532772585933405283278203623232712243.
```

- 151 verschiedene Primzahlen $l \leq 983$ benutzt, davon 77 Elkies-Primzahlen (51.0%)
- Überprüfung von $5 \cdot 10^6$ Möglichkeiten mit Algorithmus 10.4: 30 min
- Laufzeit zur Berechnung der Zerfällungstypen: 1736 Stunden (1447 MiPS Tage)
- Laufzeit zur Berechnung der Spuren: 1326 Stunden (1105 MiPS Tage)
- Gesamtlaufzeit: 3062 Stunden (2552 MiPS Tage)

Dieses letzte Beispiel verdeutlicht die Notwendigkeit und Nützlichkeit einer verteilten Implementierung des Algorithmus. Die Berechnung konnte auf einem Netz von 50 Workstations SPARC ELC in ungefähr einer Woche Real-Zeit berechnet werden.

Damit haben wir unsere Implementierung von Algorithmus 10.5 beschrieben. Die angegebene Laufzeiten machen deutlich, daß dieser Algorithmus auch in der Praxis sehr gut anwendbar ist. Im folgenden Kapitel werden wir zum Abschluß dieser Arbeit einen Algorithmus beschreiben, mit dem wir die Korrektheit einer vorgegebenen „wahrscheinlichen“ Gruppenordnung beweisen können.

Tabelle 10.1: Laufzeiten von Algorithmus 10.5

Angegeben wird die Anzahl der Dezimalstellen der Charakteristik $p$ ($p$ ist dabei die kleinste Primzahl mit dieser Dezimalstellenanzahl), die Gesamtlaufzeit zur Bestimmung der Gruppenordnung $\#E(\mathbb{F}_p)$ für die elliptische Kurve $E = (9051969, 11081969)$ sowie der Laufzeitanteil, der zur (partiellen) Bestimmung des Zerfällungstyps der äquivalenten Polynome bzw. zur Bestimmung der Spur modulo $l$ (vgl. Kapitel 7) benötigt wird. Die Zeiten wurden auf einem Rechner mit SPARC ELC-Prozessor berechnet. Beachte, daß die Bestimmung des Zerfällungstyps immer ungefähr 60 % der Gesamtlaufzeit benötigt.

| dd($p$) | Gesamtlaufzeit | | | | Zerfällungstyp | | | | Spurberechnung | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | | | 2 | sec | | | 2 | sec | | $<$ | 1 | sec |
| 20 | | | 21 | sec | | | 13 | sec | | | 8 | sec |
| 30 | 1 | min | 33 | sec | | | 53 | sec | | | 40 | sec |
| 40 | 4 | min | 24 | sec | 3 | min | 24 | sec | 1 | min | 0 | sec |
| 50 | 20 | min | 43 | sec | 14 | min | 27 | sec | 6 | min | 16 | sec |
| 60 | 33 | min | 51 | sec | 21 | min | 30 | sec | 12 | min | 21 | sec |
| 70 | 53 | min | 43 | sec | 31 | min | 45 | sec | 21 | min | 37 | sec |
| 80 | 1 | h | 41 | min | 1 | h | 2 | min | 38 | min | 14 | sec |
| 90 | 2 | h | 36 | min | 1 | h | 45 | min | 50 | min | 48 | sec |
| 100 | 6 | h | 38 | min | 4 | h | 13 | min | 2 | h | 19 | min |
| 110 | 6 | h | 14 | min | 4 | h | 17 | min | 1 | h | 55 | min |
| 120 | 11 | h | 4 | min | 6 | h | 42 | min | 4 | h | 21 | min |
| 130 | 12 | h | 59 | min | 8 | h | 20 | min | 4 | h | 38 | min |
| 140 | 27 | h | 46 | min | 19 | h | 35 | min | 8 | h | 8 | min |
| 150 | 29 | h | 10 | min | 17 | h | 51 | min | 11 | h | 17 | min |
| 175 | 80 | h | 31 | min | 54 | h | 13 | min | 26 | h | 15 | min |
| 200 | 147 | h | 48 | min | 88 | h | 16 | min | 59 | h | 27 | min |
| 225 | 190 | h | 42 | min | 123 | h | 1 | min | 67 | h | 36 | min |
| 250 | 328 | h | 2 | min | 200 | h | 30 | min | 127 | h | 24 | min |
| 275 | 469 | h | 36 | min | 252 | h | 2 | min | 217 | h | 23 | min |

# Kapitel 11

# Verifikation der Gruppenordnung

Der Algorithmus, den wir in dem vorigen Kapitel vorgestellt haben, berechnet einen „wahrscheinlichen“ Kandidaten für die Ordnung der Punktgruppe $E(\mathbb{F}_q)$ für eine gegebene elliptische Kurve $E$ über dem endlichen Körper $\mathbb{F}_q$. In der Praxis war es „immer“ so, daß dieser „wahrscheinliche“ Kandidat auch der korrekte Wert der Gruppenordnung war. Oft möchte man aber auch einen Beweis dafür haben, daß diese vermeintliche Ordnung wirklich die korrekte Gruppenordnung ist. In diesem Kapitel stellen wir einen Algorithmus vor, der einen solchen Beweis liefert. Der erste Abschnitt beschäftigt sich mit der Beschreibung der dem Algorithmus zugrundeliegenden Idee. Anschließend formulieren wir den Algorithmus und beweisen die Terminierung des Algorithmus.

## 11.1 Beschreibung der Idee

Sei $E_1$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$, für die wir den „wahrscheinlichen“ Wert $e_1 = q + 1 - c$ für die Gruppenordnung $\#E_1(\mathbb{F}_q)$ kennen. Dabei bedeutet „wahrscheinlich“, daß wir für mehrere zufällige Punkte $P \in E_1(\mathbb{F}_q)$ überprüft haben, daß $e_1 \cdot P = \mathcal{O}$ gilt. Wir wollen nun beweisen, daß diese Zahl $e_1$ wirklich die korrekte Gruppenordnung von $E_1(\mathbb{F}_q)$ ist. Dabei können wir voraussetzen, daß $e_1$ in dem durch den Satz von Hasse (Satz 2.4) vorgegebenen Lösungsintervall liegt.

Zuerst nutzen wir aus, daß wir — unter der Annahme, daß $\#E_1(\mathbb{F}_q) = e_1$ korrekt ist — mit Hilfe von Lemma 2.24 eine elliptische Kurve $E_2/\mathbb{F}_q$ kennen, die die Ordnung $\#E_2(\mathbb{F}_q) = q+1+c = e_2$ besitzt. Wir bestimmen dann eine Teilfaktorisierung dieser beiden Zahlen $e_1$ und $e_2$. Nehmen wir etwa an, wir kennen alle Teiler von $e_1$ und $e_2$ kleiner als eine vorgegebene Schranke $B$, etwa

$$e_1 \quad = \quad f_1 \cdot u_1 \qquad \text{und} \qquad e_2 \quad = \quad f_2 \cdot u_2,$$

wobei $f_i$ $(i = 1, 2)$ komplett faktorisierte Potenzprodukte von Primzahlen kleiner als $B$ und $u_i$ $(i = 1, 2)$ der verbleibende Rest (d.h. Potenzprodukte von Primzahlen größer als $B$ oder Eins) sind. Diese Teilfaktorisierungen können wir beispielsweise durch Probedivision berechnen.

Wir bestimmen dann zu beiden elliptischen Kurven $E_1$ und $E_2$ jeweils eine Untergruppe der Ordnung $f_i' \cdot u_i'$ $(i = 1, 2)$, wobei $f_i'$ ein (bekannter) Teiler von $f_i$ und $u_i'$ ein (unbekannter) Teiler von $u_i$ ist. Zur Bestimmung solcher Untergruppen wählen wir zufällig Punkte $P_1 \in E_1(\mathbb{F}_q)$ und $P_2 \in E_2(\mathbb{F}_q)$ und betrachten die von diesen Punkten erzeugte Untergruppe. Dabei sollten wir zuerst natürlich überprüfen, ob $(q+1-c) \cdot P_1 = \mathcal{O}$ bzw. $(q+1+c) \cdot P_2 = \mathcal{O}$ (auf den jeweiligen Kurven) erfüllt ist. Ist dies nicht der Fall, dann haben wir sicherlich bewiesen, daß unsere Eingabe $e_1$ nicht die korrekte Gruppenordnung war. Folgendes Lemma liefert ein einfaches Kriterium zur Bestimmung der Ordnung der so erzeugten Untergruppen.

**Lemma 11.1** *Sei $P \in E(\mathbb{F}_q)$ ein beliebiger Punkt der elliptischen Kurve $E$ und sei für ein Vielfaches der Ordnung von $P$ eine Faktorisierung $f \cdot u$ bekannt, wobei $f$ ein Potenzprodukt von bekannten Primzahlen kleiner als eine Schranke $B$ und $u$ der verbleibende Rest ist. Sei die Ordnung des Punktes $P$ gegeben als* $\mathrm{ord}(P) = f' \cdot u'$, *wobei $f'$ ein Teiler von $f$ und $u'$ ein Teiler von $u$ ist. Dann gilt für die Ordnung des Punktes $Q = u \cdot P$*

$$\mathrm{ord}(Q) \quad = \quad f'.$$

**Beweis:** Sei etwa $u = u' \cdot u''$ und $f = f' \cdot f''$. Offensichtlich gilt dann

$$f' \cdot Q \;=\; f' \cdot u \cdot P \;=\; f' \cdot u' \cdot u'' \cdot P \;=\; u'' \cdot (f' \cdot u' \cdot P) \;=\; \mathcal{O}$$

und damit ist die Ordnung von $Q$ ein Teiler von $f'$.

Nehmen wir an, daß $\mathrm{ord}(Q) = \tilde{f}$ ein echter Teiler von $f'$ ist. Dann betrachten wir den Punkt $H = \tilde{f} \cdot u' \cdot P$. Die Ordnung von $H$ muß ein Teiler von $u''$ sein, denn nach unserer Annahme gilt

$$u'' \cdot H \;=\; u'' \cdot (\tilde{f} \cdot u' \cdot P) \;=\; \tilde{f} \cdot u \cdot P \;=\; \tilde{f} \cdot Q \;=\; \mathcal{O}.$$

Da $H$ nicht der Nullpunkt ist (beachte die Ordnung von $P$), muß $u'' > 1$ sein. Falls $u = 1$ war, haben wir damit einen Widerspruch erreicht. Nehmen wir daher an, $u$ ist echt größer als Eins. Dann gilt

$$\left(\frac{f'}{\tilde{f}}\right) \cdot H \;=\; \left(\frac{f'}{\tilde{f}}\right) \cdot \tilde{f} \cdot u' \cdot P \;=\; f' \cdot u' \cdot P \;=\; \mathcal{O}.$$

Dies ist aber ein Widerspruch, denn alle Primteiler von $(f'/\tilde{f}) > 1$ sind kleiner und alle Primteiler von $u'' > 1$ größer als $B$; beide Zahlen sind jedoch Vielfache der Ordnung von $H$. Damit kann die Ordnung von $Q$ kein echter Teiler von $f'$ sein und das Lemma ist bewiesen. ∎

Sei die Ordnung der beiden Punkte nun $\mathrm{ord}(P_i) = f_i' \cdot u_i'$, wobei $f_i', u_i'$ die üblichen Bedingungen erfüllen sollen. Da wir die komplette Faktorisierung der Zahlen $f_i$ kennen, können wir mit Hilfe dieses Lemmas die Zahl $f_i'$ berechnen. Dazu bestimmen wir die Ordnung der Punkte $u_i \cdot P_i$, $(i = 1, 2)$, indem wir durch Ausprobieren den kleinsten Teiler $f_i'$ von $f_i$ mit $f_i' \cdot u_i \cdot P_i = \mathcal{O}$ bestimmen. Genauso einfach können wir überprüfen, ob die unbekannten Werte $u_i'$ größer als Eins sind. Diese sind nämlich genau dann größer als Eins, wenn $f_i' \cdot P_i \neq \mathcal{O}$ ist.

Sei die korrekte Gruppenordnung von $E_1$ gegeben als $\#E_1(\mathbb{F}_q) = q + 1 - C$ und damit die korrekte Ordnung des Twists $\#E_2(\mathbb{F}_q) = q+1+C$. Dann ist die Ordnung $\mathrm{ord}(P_i) = f_i' \cdot u_i'$ von $P_i$ sicherlich ein Teiler von $|C - c|$. Wir beachten, daß dies für beide elliptische Kurven $E_1$ und $E_2$ gilt. Damit wissen wir, daß sogar

$$\mathrm{kgV}(f_1' \cdot u_1', f_2' \cdot u_2') \quad = \quad \mathrm{kgV}(f_1', f_2') \cdot \mathrm{kgV}(u_1', u_2') \tag{11.1}$$

ein Teiler von $|C - c|$ ist. Falls $u_1'$ und $u_2'$ teilerfremd sind, ist sogar

$$\mathrm{kgV}(f_1', f_2') \cdot u_1' \cdot u_2'$$

ein Teiler von $|C - c|$. Die Teilerfremdheit von $u_1'$ und $u_2'$ läßt sich durch folgende Überlegungen häufig feststellen. Wir wissen, daß die Zahlen $u_i'$ Teiler von $e_i$ sind und nur Primfaktoren größer als $B$ besitzen. Insbesondere ist $u_i'$ damit ein Teiler von $e_i/f_i$. Damit ist der größte gemeinsame Teiler der beiden Zahlen $u_1'$ und $u_2'$ ein Teiler von

$$d \quad = \quad \mathrm{ggT}\left(\frac{e_1}{f_1}, \frac{e_2}{f_2}\right).$$

Insbesondere folgt aus $d = 1$ die Teilerfremdheit von $u_1'$ und $u_2'$. Ist $d > 1$, so können wir den größten gemeinsamen Teiler von $u_1'$ und $u_2'$ nach oben durch $d$ abschätzen. Damit gilt für $u_i' > 1$, $(i = 1, 2)$ in jedem Fall

$$\mathrm{kgV}(u_1', u_2') \quad = \quad \frac{u_1' \cdot u_2'}{\mathrm{ggT}(u_1', u_2')} \quad \geq \quad \frac{B^2}{d}.$$

Schätzen wir damit das kleinste gemeinsame Vielfache aus (11.1) ab, so erhalten wir

$$\mathrm{kgV}(f_1' \cdot u_1', f_2' \cdot u_2') \geq \begin{cases} \mathrm{kgV}(f_1', f_2') \cdot \frac{B^2}{d} & \text{falls } u_1', u_2' > 1. \\ \mathrm{kgV}(f_1', f_2') \cdot B & \text{falls } u_i' = 1 \text{ für genau ein } i \in \{1, 2\}. \\ \mathrm{kgV}(f_1', f_2') & \text{falls } u_1' = u_2' = 1. \end{cases}$$

Schätzen wir die Differenz $|C - c|$ nach oben ab, so erhalten wir aus dem Satz von Hasse

$$|C - c| \quad \leq \quad 4\sqrt{q}.$$

Ist also die untere Abschätzung für $\mathrm{kgV}(f_1' \cdot u_1', f_2' \cdot u_2')$ echt größer als $4\sqrt{q}$, so muß $|C - c|$ gleich Null sein, d.h. unsere Eingabe muß die korrekte Gruppenordnung sein. Ansonsten können wir neue Punkte $P_i$ wählen oder den Parameter $B$ vergrößern und damit $e_1$ und $e_2$ weiter faktorisieren.

Im folgenden Abschnitt werden wir diese Ideen in Form eines Algorithmus aufschreiben. Die Korrektheit des Algorithmus folgt dann direkt aus den bis jetzt beschriebenen Tatsachen, wenn wir zeigen können, daß der Algorithmus mit Sicherheit terminiert. Diese Frage werden wir in Abschnitt 11.3 untersuchen.

## 11.2 Beschreibung eines Algorithmus zur Verifikation

Mit den im vorigen Abschnitt beschriebenen Ideen formulieren wir den folgenden Algorithmus, der die Korrektheit einer „wahrscheinlichen" Gruppenordnung einer elliptischen Kurve beweist.

**Algorithmus 11.2** [Korrektheit einer „wahrscheinlichen" Ordnung]

**Eingabe:** elliptische Kurve $E_1 = (a, b) \in \mathbb{F}_q^2$, „wahrscheinliche" Ordnung $e_1 = q + 1 - c$ von $E_1(\mathbb{F}_q)$ im Lösungsintervall.

**Ausgabe:** „$e_1$ korrekte Gruppenordnung" oder „$e_1$ nicht korrekte Gruppenordnung" .

| | |
|---|---|
| Wähle $d \leftarrow$ Nichtquadrat in $\mathbb{F}_q^*$. | (1) |
| Setze $E_2 \leftarrow (d^2 \cdot a, d^3 \cdot b)$ und $e_2 \leftarrow q + 1 + c$. | (2) |
| Wähle Faktorisierungsschranke $B$. | (3) |
| Berechne Teilfaktorisierung $e_i = f_i \cdot u_i$ mit $f_i = \prod_{l \leq B, l \in \mathbb{P}} l^{\nu_{i,l}}$ und $u_i = e_i / f_i \qquad (i = 1, 2)$. | (4) |
| Wähle zufällig Punkte $P_1 \in E_1(\mathbb{F}_q)$ und $P_2 \in E_2(\mathbb{F}_q)$. | (5) |
| IF $e_1 \cdot P_1 \neq \mathcal{O}$ oder $e_2 \cdot P_2 \neq \mathcal{O}$ | (6) |
| THEN RETURN „$e_1$ nicht korrekte Gruppenordnung" . | (7) |
| Bestimme $f_i' = \operatorname{ord}(u_i \cdot P_i)$, $(i = 1, 2)$ durch Ausprobieren aller Teiler von $f_i$. | (8) |
| IF $\operatorname{kgV}(f_1', f_2') > 4\sqrt{q}$ | (9) |
| THEN RETURN „$e_1$ korrekte Gruppenordnung" . | (10) |
| IF $f_i' \cdot P_i \neq \mathcal{O}$ für genau ein $i \in \{1, 2\}$ und $\operatorname{kgV}(f_1', f_2') \cdot B > 4\sqrt{q}$ | (11) |
| THEN RETURN „$e_1$ korrekte Gruppenordnung" . | (12) |
| Berechne $d \leftarrow \operatorname{ggT}(e_1/f_1, e_2/f_2)$. | (13) |
| IF $f_i' \cdot P_i \neq \mathcal{O}$ für $i = 1, 2$ und $\operatorname{kgV}(f_1', f_2') \cdot \frac{B^2}{d} > 4\sqrt{q}$ | (14) |
| THEN RETURN „$e_1$ korrekte Gruppenordnung" . | (15) |
| UNTIL Vorbestimmte Anzahl von Versuchen negativ. | (16) |
| Vergrößere $B$. | (17) |
| UNTIL FOREVER | (18) |

In der Praxis liefert dieser Algorithmus in der Regel schon mit den ersten zufällig gewählten Punkten einen Beweis der Korrektheit der vermeintlichen Gruppenordnung, wenn wir eine der beiden Gruppenordnungen komplett faktorisieren können.

Den laufzeitmäßig dominierenden Teil stellt dabei die Berechnung der Teilfaktorisierungen in Schritt (4) dar. Für sehr große Körper ist es allerdings häufig nicht mehr möglich, eine der beiden vermeintlichen Ordnungen $e_i$ ganz zu faktorisieren bzw. die dazu benötigten Schranken $B$ sind sehr groß, so daß es nicht mehr möglich ist, geeignete Teilfaktorisierungen zu bestimmen. Wir haben in Abschnitt 7.4 schon darauf hingewiesen, daß wir in der Praxis bei der Berechnung von $c \bmod l$ für Elkies Primzahlen $l$ stoppen, wenn wir den ersten „möglichen" Eigenwert gefunden haben. Wir können nun obiges Beweisverfahren noch etwas verbessern, wenn wir gleichzeitig die Korrektheit dieser Spur $c \bmod l$ beweisen. Dann ist offensichtlich $|C - c| \equiv 0 \bmod l$ (sowohl die wahrscheinliche Spur $c$ als auch die richtige Spur $C$ besitzen modulo $l$ den gleichen Rest) und damit können wir das kleinste gemeinsame Vielfache aus (11.1) mit $l$ multiplizieren. Führen wir dies für „genügend" viele Elkies-Primzahlen durch, so wird es auch so möglich, die Gruppenordnung zu beweisen.

Der Beweis der Korrektheit der Spur modulo $l$ geschieht auf dieselbe Weise wie in Abschnitt 7.3 beschrieben. Zuerst müssen wir testen, ob das berechnete Polynom $f_C(X)$ wirklich ein Teiler des $l$-ten Divisionspolynoms ist, d.h. wir berechnen das $l$-te Divisionspolynom modulo $f_C(X)$. Anschließend testen wir für **alle** möglichen Werte $\alpha$, ob $\Phi_E(X,Y) \equiv \alpha \cdot (X,Y) \bmod f_C(X)$ ist (vgl. Abschnitt 7.3). Erhalten wir dabei nur für einen Wert von $\alpha$ eine Übereinstimmung, so haben wir die Korrektheit der Spur des Frobenius-Endomorphismus modulo $l$ bewiesen.

Wir werden im folgenden Abschnitt zeigen, daß der Algorithmus auch theoretisch terminieren muß, wenn wir den letzten Schritt, d.h. den Korrektheitsbeweis für $c \bmod l$ nicht durchführen.

## 11.3 Terminierung des Algorithmus

In diesem Abschnitt untersuchen wir die Frage, ob obiger Algorithmus 11.2 immer mit der richtigen Ausgabe terminiert. Die Terminierung hängt sicherlich davon ab, ob die Wahl der zufälligen Punkte in Schritt (5) „gute" Punkte geliefert hat. Wir werden noch angeben, welche Punkte „gute" Punkte sind.

In der Hauptschleife von Algorithmus 11.2 wird die Faktorisierungsschranke $B$ immer weiter vergrößert. Deshalb erhalten wir nach endlich vielen Iterationen die komplette Faktorisierung von $e_1$ und $e_2$. Dann können wir die exakte Ordnung der beiden gewählten Punkte auf den jeweiligen Kurven berechnen. Die Ordnung von Punkten hängt eng mit dem Isomorphietyp der zugrundeliegenden elliptischen Kurve zusammen. Der folgende Satz von Rück [Rü87] beschreibt diesen Typ.

**Satz 11.3 (Satz von Rück)**
*Falls die Ordnung $N_q$ der $\mathbb{F}_q$-rationalen Punkte $E(\mathbb{F}_q)$ die Primfaktorzerlegung*

$$N_q = \prod_{l \in \mathbb{P}} l^{\nu_l}$$

*besitzt, so besitzt die Gruppe $E(\mathbb{F}_q)$ den Isomorphietyp*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/p^{\nu_p}\mathbb{Z} \oplus \bigoplus_{l \neq p} (\mathbb{Z}/l^{\alpha_l}\mathbb{Z} \oplus \mathbb{Z}/l^{\nu_l - \alpha_l}\mathbb{Z}),$$

*wobei*

1. $\alpha_l = \nu_l/2$, *falls* $N_q = q + 1 \pm 2\sqrt{q}$,
2. $0 \le \alpha_l \le \min\{\, \max_{j\ge 0}\{l^j \,|\, (q-1)\},\ \lfloor \nu_l/2 \rfloor\,\}$, *sonst.*

Seien nun die elliptischen Kurven $E_i$, $(i = 1, 2)$ gegeben wie in Abschnitt 11.1 und sei ihr Typ

$$E_i(\mathbb{F}_q) \quad \cong \quad \mathbb{Z}/m_i\mathbb{Z} \,\oplus\, \mathbb{Z}/n_i\mathbb{Z}, \qquad (i = 1, 2)$$

wobei $n_i$ ein Teiler von $q-1$ und von $m_i$ ist. Dann terminiert Algorithmus 11.2 mit Sicherheit mit der korrekten Antwort, wenn mindestens einer der beiden Werte $m_i$ größer als $4\sqrt{q}$ ist. In diesem Fall existieren auf einer der beiden Kurven Punkte der Ordnung größer $4\sqrt{q}$ und damit ist bei Wahl eines solchen Punktes $\mathrm{kgV}(f_1' \cdot u_1', f_2' \cdot u_2') > 4\sqrt{q}$.

Nehmen wir daher nun an, beide Zahlen $m_i$ wären kleiner als $4\sqrt{q}$. Dann folgt aus $n_i \le m_i$ und $\#E_i(\mathbb{F}_q) \ge (\sqrt{q} - 1)^2$, daß immer

$$m_i \quad \ge \quad \sqrt{q} - 1 \qquad (i = 1, 2)$$

gelten muß. Da $n_i\,(i = 1, 2)$ ein Teiler von $q - 1$ ist, gilt mit $\#E_1(\mathbb{F}_q) = q + 1 - C$ und $\#E_2(\mathbb{F}_q) = q + 1 + C$, daß $n_1$ auch $C - 2$ und $n_2$ auch $C + 2$ teilen muß. Durch Kombination beider Aussagen erhalten wir $\mathrm{ggT}(n_1, n_2) \le 4$. Angenommen, wir wählen dann auf beiden Kurven einen Punkt der Ordnung $n_i$. Dann gilt

$$\mathrm{kgV}(n_1, n_2) \;=\; \frac{n_1 \cdot n_2}{\mathrm{ggT}(n_1, n_2)} \;\ge\; \frac{(q + 1 - C) \cdot (q + 1 + C)}{4\, m_1\, m_2} \;\ge\; \frac{(q+1)^2 - 16\,q}{64\,q}.$$

Für $q \ge 65564$ ist diese untere Abschätzung für $\mathrm{kgV}(n_1, n_2)$ echt größer als $4\sqrt{q}$ und damit terminiert der Algorithmus für solche $q$ mit Sicherheit.

Damit haben wir gezeigt, daß unter der Voraussetzung, daß die Eingabe $e_1$ die korrekte Ordnung der Gruppe $E_1(\mathbb{F}_q)$ ist, der Algorithmus mit der exakten Antwort terminiert. Leicht kann man sich auch überlegen, daß bei Eingabe eines falschen Wertes $e_1$ (d.h. falls $e_1$ nicht die korrekte Gruppenordnung $\#E_1(\mathbb{F}_q)$ ist) und Wahl eines „guten" Punktes der Test in Schritt (6) zur Ausgabe „$e_1$ nicht korrekt" führt: offensichtlich führt Schritt (6) zu dieser Ausgabe, wenn die Ordnung eines der gewählten Punkte $P_i$ größer als $4\sqrt{q}$ ist. Nehmen wir also an, daß beide Zahlen $m_i < 4\sqrt{q}$, $i = 1, 2$ sind und daß damit

$$n_i \quad = \quad \frac{q + 1 \mp C}{m_i} \quad \ge \quad \frac{(\sqrt{q} - 1)^2}{4\sqrt{q}}$$

gilt. Weiterhin nehmen wir an, daß wir zwei Punkte mit Ordnung $n_i$, $i = 1, 2$ gewählt haben. War der Test des Punktes $P_1$ in Schritt (6) von Algorithmus 11.2 erfolgreich, so gibt es eine ganze Zahl $r$ mit

$$e_1 \quad = \quad q + 1 - C + r \cdot n_1 \qquad \text{und damit} \qquad |C - c| \quad = \quad |r| \cdot n_1.$$

Aus der oberen Schranke für $|C - c|$ folgt durch Ausrechnen leicht $1 \leq |r| \leq 53$. Nach Konstruktion gilt dann $e_2 = q + 1 + C - r \cdot n_1$. Nehmen wir an, der Test in Schritt (6) wäre auch für den Punkt $P_2$ erfolgreich, so muß $n_2$ ein Teiler von $r \cdot n_1$ sein. Aus $\mathrm{ggT}(n_1, n_2) \leq 4$ erhalten wir hieraus für $q \geq 45794$ einen Widerspruch zur oberen Abschätzung für $r$.

Damit haben wir gezeigt, daß der Algorithmus 11.2 zur Verifikation einer „wahrscheinlichen" Gruppenordnung sicherlich für $q \geq 65564$ mit der korrekten Antwort terminiert. Alle Gruppenordnungen von elliptischen Kurven über kleineren Körpern kann man mit einem einfachen, auf der Formel aus dem Beweis zu Lemma 2.24 basierenden Zählalgorithmus direkt beweisen.

Somit haben wir alle Ziele dieser Arbeit erreicht. Wir haben in den Kapiteln 2 bis 9 Grundlagen und Teilalgorithmen zur Lösung des gegebenen Problems der Bestimmung der Gruppenordnung einer elliptischen Kurve über einem endlichen Körper der Charakteristik größer drei vorgestellt. Diese Teilalgorithmen haben wir in Kapitel 10 zu dem Gesamtalgorithmus 10.5 zusammengefaßt. Dies ist der fundamentale Algorithmus, der unser gegebenes Problem löst. In diesem letzten Kapitel haben wir schließlich noch einen Algorithmus zur Verifikation einer gegebenen Gruppenordnung hergeleitet.

Aus den geschilderten praktischen Beispielen wird deutlich, daß dieser Algorithmus für große Primkörper sehr gut anwendbar ist. Eine noch offene interessante Frage ist es, das praktische Verhalten des Algorithmus für endliche Körper, die keine Primkörper sind, zu untersuchen. Von praktischem Interesse ist weiterhin die Übertragung des Algorithmus auf endliche Körper kleiner Charakteristik, insbesondere auf Körper der Charakteristik 2. Dabei sind die in den Kapiteln 3 und 4 beschriebenen Resultate sehr leicht zu übertragen. Couveignes hat einen ersten Algorithmus beschrieben, wie man auch die in den Kapiteln 6 und 7 geschilderten Algorithmen in Körpern der Charakteristik 2 anwenden kann. Das praktische Verhalten dieses Algorithmus ist allerdings noch nicht intensiv erforscht worden. Dennoch sieht es so aus, daß schon in wenigen Jahren das Problem der Bestimmung der Gruppenordnung einer elliptischen Kurve über einem beliebigen endlichen Körper in der Praxis zufriedenstellend gelöst sein wird.

# Literaturverzeichnis


[Ap90] T. Apostol: *Modular Functions and Dirichlet Series in Number Theory,* Springer-Verlag, 1990

[At88] A.O.L. Atkin: *The number of points on an elliptic curve modulo a prime,* Manuskript, veröffentlicht über das Number Theory Net, 1988

[At92] A.O.L. Atkin: *The number of points on an elliptic curve modulo a prime (ii),* Manuskript, veröffentlicht über das Number Theory Net, 1992

[AtLe70] A.O.L. Atkin, J. Lehner: *Hecke Operators on* $\Gamma_0(m)$, Math. Ann. 185, 1970, Seite 134 - 160

[BuMü92] J. Buchmann, V. Müller: *Primality Testing,* Informatik Fachbericht 2/92, Universität des Saarlandes, Saarbrücken, 1992

[ChRo88] L. Charlap, D. Robbins: *An Elementary Introduction to Elliptic Curves*, CRD Expository Report No. 31, 1988

[ChRo90] L. Charlap, D. Robbins: *An Elementary Introduction to Elliptic Curves II*, CRD Expository Report No. 34, 1990

[ChCoRo] L. Charlap, R. Coley, D. Robbins: *Enumeration of Rational Points on Elliptic Curves over Finite Fields,* Preprint

[Co93] H. Cohen: *A Course in Computational Algebraic Number Theory,* Springer-Verlag, 1993

[CoMo94] J. M. Couveignes, F. Morain: *Schoof's algorithm and isogeny cycles,* Proceedings of ANTS I 1994, Lecture Notes in Computer Science 877, Seite 43 - 58

[De41] M. Deuring: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg 14, 1941, Seite 197 - 272

[El] N. Elkies: *Explicit Isogenies,* Preprint

[Hu74] T. W. Hungerford: *Algebra,* Springer-Verlag, 1974

[Hu67] B. Huppert: *Endliche Gruppen I,* Springer-Verlag, 1967

[Ko86] N. Koblitz: *Elliptic curve cryptosystems*, Math. Comp. 48, 1987, Seite 203 - 209

[La87] S. Lang: *Elliptic functions*, Springer-Verlag, 1987

[LMMS94] F. Lehmann, M. Maurer, V. Müller, V. Shoup: *Counting the Number of Points on Elliptic Curves over Finite Fields of Characteristic Greater than Three,* Proceedings of ANTS I 1994, Lecture Notes in Computer Science 877, Seite 60 - 70

[Le94] F. Lehmann: *Implementierung von Algorithmen zur Berechnung modularer Polynome und deren Anwendung im Algorithmus von Atkin*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1994

[Ma94] M. Maurer: *Eine Implementierung des Algorithmus von Atkin zur Berechnung der Punktanzahl elliptischer Kurven über endlichen Primkörpern*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1994

[Me93] A. Menezes: *Elliptic Curve Public Key Cryptosystems*, Kluver Academic Publishers, 1993

[Mi86] V. Miller: *Uses of elliptic curves in cryptography*, Advances in Cryptology: Proceedings of Crypto '85, Lecture Notes in Computer Science 218, 1986, Springer-Verlag, Seite 417-426

[Mü91] V. Müller: *Die Berechnung der Punktanzahl elliptischer Kurven über endlichen Körpern,* Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1991

[NaSh73] I. Nassi, B. Shneiderman: *Flowchart techniques for structured programming,* SIGPLAN Notices 8, No. 8, 1973, Seite 12 - 26

[PoHe78] S. C. Pohlig, M. E. Hellman: *An Improved Algorithm for Computing Logarithms in GF*$(p)$ *and Its Cryptographic Significance*, IEEE Transactions on Information Theory 24, 1978, Seite 106 - 111

[Ra16] S. Ramanujan: *On certain arithmetical functions*, Trans. Cambridge phil. Society 22, 1916, (Collected papers, no. 18, Seite 136 - 162)

[Rü87] H. G. Rück: *A Note on Elliptic Curves over Finite Fields,* Math. Comp. 49, 1987, Seite 301 - 304

[Sc74] B. Schoeneberg: *Elliptic Modular Functions,* Springer-Verlag, 1974

[Sc85] R. Schoof: *Elliptic Curves over Finite Fields and the Computation of Square Roots mod* $p$, Math. Comp. 44, 1985, Seite 483 - 494

[Se71] J. P. Serre: *Congruences et formes modulaires*, Seminair Bourbaki Nr. 416, 1971/72 (Collected Works III, Seite 74ff.)

[Sh95] V. Shoup: *Practical computations with large polynomials over finite fields*, in Vorbereitung

[Si85] J. Silverman: *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1985

[TaMo72] J. Tannery, J. Molk: *Fonctions Elliptiques*, Chelsea Publishing Company, 2nd edition, 1972

[Ta66] J. Tate: *Endomorphisms of Abelian Varieties over finite Fields*, Inventiones Math. 10, 1966, Seite 134 - 144

[Ve71] J. Vélu: *Isogénies entre courbes elliptiques*, Comptes Rendus A 273-7, 1971, Seite 238 - 241

[Wa71] B. L. van der Waerden: *Algebra*, Springer-Verlag, 1971

[Wa69] W. Waterhouse: *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) 2, 1969, Seite 521 - 560

[We08] H. Weber: *Lehrbuch der Algebra,* Band 3, Chelsea Publishing Company, New York, 1908

[Wei63] E. Weiss: *Algebraic Number Theory,* McGraw-Hill Bode Company Inc., 1963

# Stichwortverzeichnis