Der diskrete Logarithmus auf gewöhnlichen elliptischen Kurven mit einem Endomorphismenring kleiner Klassenzahl

ANNEGRET WENG

Diplomarbeit
am Fachbereich Mathematik
der Johann Wolfgang v. Goethe-Universität
bei Prof. Dr. C.P.Schnorr

Frankfurt, den 27. Mai 1999

LITTERARUM RADICES AMARAS ESSE,
FRUCTUS JUCUNDIORES.

M. Porcius Cato (239-149 v. Chr.)

Herrn Prof. Dr. C. P. Schnorr danke ich sehr herzlich für die Unterstützung bei dieser Arbeit und seine hilfreichen Verbesserungsvorschläge. Meinen Dank richte ich auch an Herrn Dr. S. Paulus, von dem ich wertvolle Anregungen erhielt und der mich an der TU Darmstadt in eine Arbeitsgruppe aufnahm. Ich danke Herrn Prof. Dr. J. Wolfart für lebhafte Diskussionen. Nicht vergessen sind auch J. Merkle und A. Hoffmann, die meine Arbeit Korrektur lasen. Mein besonderer Dank gilt meinen Eltern und meiner Großmutter, die mich immer bei allem unterstützt haben.

Inhaltsverzeichnis

Liste der Algorithmen

Einleitung

Elliptische Kryptosysteme wurden erstmals 1985 von Victor Miller [37] vorgeschlagen und haben seitdem stetig an Bedeutung gewonnen. Sie basieren auf der Schwierigkeit, den diskreten Logarithmus in der Punktegruppe einer elliptischen Kurve über einem endlichen Körper zu berechnen. Im Gegensatz zum Logarithmusproblem in endlichen Körpern ist für das Logarithmusproblem auf beliebigen elliptischen Kurven noch kein subexponentieller Algorithmus bekannt. Dadurch genügen relativ kleine Schlüssellängen zwischen 150 und 200 Bits, um ausreichende Sicherheit zu gewährleisten. Das wirkt sich auf Speicherplatz und Rechenaufwand positiv aus und macht elliptische Kryptosysteme besonders für die Implementierung auf Chipkarten interessant.
Heute betrachtet man für Kryptosysteme, die auf dem diskreten Logarithmus beruhen, fast ausnahmslos gewöhnliche (also nicht supersinguläre) elliptische Kurven, da für supersinguläre Kurven effizientere Angriffe [10, 39] existieren.
Gewöhnliche elliptische Kurven haben einen Endomorphismenring, der zu einer Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ isomorph ist. Interessant sind besonders elliptische Kurven, deren Endomorphismenring zu einer Ordnung $\mathcal{O}$ mit kleiner Klassenzahl $h(\mathcal{O})$ isomorph ist. Zu diesen Kurven zählen die Kurven, die über einem kleinen Körper der Charakteristik zwei definiert sind. Diese wurden von N. Koblitz vorgeschlagen [22] und sind deshalb auch als Koblitz-Kurven bekannt.
Elliptische Kurven mit einem Endomorphismenring mit kleiner Klassenzahl weisen zwei Vorteile gegenüber allgemeinen Kurven auf:

1. Bei Kryptosystemen, die den diskreten Logarithmus verwenden, ist die Kenntnis der Gruppenordnung wichtig. Von ihr hängt ab, ob der diskrete Logarithmus tatsächlich schwierig zu berechnen ist. Obwohl inzwischen auch schnelle Algorithmen zum Punktezählen auf allgemeinen elliptischen Kurven existieren [32], [48], versucht man in der Praxis oft, Kurven zu erzeugen, deren Gruppenordnung besonders einfach zu bestimmen ist. Dazu zählen die Kurven mit kleinem Endomorphismenring.

Für über Primkörpern definierten Kurven können wir zum Beispiel das Konzept der komplexen Multiplikation verwenden [3, 57, 28]. Bei dieser Methode geben wir uns die Gruppenordnung vor und ermitteln eine gewöhnliche elliptische Kurve mit der gewünschten Punktezahl. Damit der Algorithmus aber effizient läuft, müssen Kurven mit komplexer Multiplikation mit einer imaginär quadratischen Ordnung mit *kleiner* Klassenzahl gewählt werden.

2. Der rechenaufwendigste Teil eines Kryptosystems, das auf dem diskreten Logarithmus auf der elliptischen Kurve beruht, ist die Skalarmultiplikation, d.h. die Operation

$$P \to rP.$$

Für Kurven mit kleinem Endomorphismenring gibt es hierfür effizientere Algorithmen. Am schnellsten läßt sich die Skalarmultiplikation auf Kurven, die über einem kleinen Körper der Charakteristik zwei definiert sind, ausführen [40].

Bisher wurden noch keine wirkungsvollen Angriffe auf das diskrete Logarithmusproblem auf gewöhnlichen elliptischen Kurven mit einem Endomorphismenring mit kleiner Klassenzahl entwickelt.

Ausgangspunkt dieser Arbeit ist das diskrete Logarithmusproblem auf elliptischen Kurven mit einem kleinen Endomorphismenring. Dabei möchten wir einige Struktureigenschaften dieser Kurvenklasse aufdecken, näher untersuchen und mit dem diskreten Logarithmus in Verbindung setzen.
Im ersten Kapitel führen wir die grundlegenden Definitionen ein und erklären die Gruppenoperation auf der Punktegruppe einer elliptischen Kurve. Die Gruppenstruktur einer elliptischen Kurve ermöglicht es erst, diese kryptographisch einzusetzen.
Das zweiten Kapitel vermittelt einen Überblick über den diskreten Logarithmus auf der elliptischen Kurve. Wir stellen ein Kryptosystem vor, das auf dem diskreten Logarithmusproblem auf der elliptischen Kurve beruht. Weiter skizzieren wir kurz die bereits bekannten Angriffe auf spezielle Klassen elliptischer Kurven und die sich daraus ergebenden Anforderungen an die Gruppenordnung einer elliptischen Kurve.
Im dritten Abschnitt erklären wir die Zeta-Funktion einer elliptischen Kurve. Wir erläutern, wie wir auf elliptischen Kurven, die über einem kleinen Körper definiert sind, die Ordnung der Punktegruppe eines Erweiterungskörpers effizient ermitteln können. Somit läßt sich für Koblitz-Kurven leicht überprüfen, ob diese eine günstige Gruppenordnung haben.
Im dritten Kapitel diskutieren wir elliptische Kurven, die über einem kleinen Körper $\mathbb{F}_q$ definiert sind. Wir untersuchen eine der Norm in endlichen Körpern ähnliche Abbildung, die die Punktgruppe $E(\mathbb{F}_{q^k})$ auf $E(\mathbb{F}_q)$ abbildet. Wir hoffen, dadurch auch

Informationen für das diskrete Logarithmusproblem auf den Koblitz-Kurven zu gewinnen. Leider sind wir hier erfolglos (siehe Lemma 3.18). Weiter stellen wir fest, daß wir den diskreten Logarithmus r eines zu P konjugierten Punktes $\sigma(P)$ für ein $\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ einfach berechnen können.
Das Thema des vierten Kapitels ist schließlich der Endomorphismenring elliptischer Kurven über endlichen Körpern. Wie bereits erwähnt, entspricht bei gewöhnlichen elliptischen Kurven über einem endlichen Körper der Endomorphismenring einer Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper. Der Endomorphismenring enthält viel Information über die Kurve und ihre Punktegruppen (siehe Abschnitte 4.1 und 4.2). Auch das diskrete Logarithmusproblem läßt sich in der Sprache der Endomorphismen formulieren. Dies führt uns zum verallgemeinerten Logarithmusproblem (siehe Abschnitt 4.4). Davon unabhängig beschreiben wir in Abschnitt 4.5 einen Algorithmus, mit dem wir Kurven mit günstiger Gruppenordnung erzeugen können.
Das Kernstück der Arbeit ist das fünfte Kapitel. D. Kohel hat in seiner Arbeit [24] bereits einen Weg aufgedeckt, den Endomorphismenring einer Kurve über einem endlichen Körper zu bestimmen. Angenommen der Endomorphismenring $\mathcal{O}$ der Kurve sei bekannt, dann stellt sich die Frage, wie wir zu gegebenem $P \in E(\mathbb{F}_q)$ und $\alpha \in \mathcal{O}$ den Bildpunkt $\alpha(P)$ bestimmen. Genauer suchen wir für $\alpha \in \mathcal{O}$ Funktionen $f_1(x,y), f_2(x,y)$, so daß

$$\alpha((x,y)) = (f_1(x,y), f_2(x,y)) \text{ für alle } (x,y) \text{ in } E(\overline{\mathbb{F}_q})$$

ist. Hierfür geben wir einen Algorithmus an, der vor allem für Kurven, deren Endomorphismenring Klassenzahl eins hat, effizient läuft. Wir unterscheiden die beiden Fälle char $\mathbb{F}_q \neq 2,3$ und char $\mathbb{F}_q = 2$.
Unsere Untersuchungen in den Kapiteln 4 und 5 zeigen **nicht**, daß das diskrete Logarithmusproblem auf elliptischen Kurven mit kleiner Klassenzahl einfacher zu lösen ist als auf anderen gewöhnlichen elliptischen Kurven. Wir haben allerdings eine weitere Besonderheit dieser Kurven aufgedeckt: Für eine über $\mathbb{F}_q$ definierte elliptische Kurve E mit kleiner Klassenzahl können wir für beliebiges α in $End(E)$ und einen beliebigen Punkte $P \in E(\overline{\mathbb{F}_q})$ den Bildpunkt $\alpha(P)$ effizient berechnen. Wir können somit auch Instanzen des verallgemeinerten diskreten Logarithmus auf nicht-zyklischen elliptischen Kurven mit einem Endomorphismenring mit kleiner Klassenzahl erzeugen (siehe Abschnitt 5.5). Bei der Implementierung eines Kryptosystems, das auf dem diskreten Logarithmusproblem auf einer elliptischen Kurve mit Endomorphismenring mit kleiner Klassenzahl beruht, sollte man darauf achten, daß der gewählte diskrete Logarithmus nicht zu einem Endomorphismus mit kleiner Norm äquivalent ist (siehe auch Abschnitt 5.6).
Im sechsten Kapitel widmen wir uns einem rein anwendungsorientierten Problem:

den verschiedenen Algorithmen zur schnellen Skalarmultiplikation auf elliptischen Kurven. Diese stellen den wichtigsten und zeitaufwendigsten Bestandteil aller auf dem diskreten Logarithmus beruhenden Kryptosysteme dar. Wir stellen alle bisher veröffentlichten, interessanten Ideen auf diesem Gebiet vor und geben eine Übersicht (siehe Abschnitt 6.5), welche Algorithmen besonders günstig sind. Dabei beschränken wir uns nicht nur auf gewöhnliche elliptische Kurven mit kleinem Endomorphismenring, behandeln diese aber weit ausführlicher. In Abschnitt 6.4 geben wir einen neuen Algorithmus an, der die Skalarmultiplikation auf über Primkörper definierten elliptischen Kurven mit kleinem Endomorphismenring ein wenig beschleunigt. Dieser ist eine Anwendung des in Kapitel fünf entwickelten Algorithmus zur Beschreibung der Koordinatendarstellung von Endomorphismen.
Im Anhang A erläutern wir die Primidealzerlegung in Zahlkörpern. In Anhang B führen wir die wichtigsten Definitionen und Sätze aus der algebraischen Geometrie, die wir für die Kapitel drei und vier benötigen, ein. Im Anhang C sind bekannte j-Invarianten angegeben. Diese sind für die Konstruktion der Endomorphismen in Kapitel vier wichtig. In Anhang D gehen wir kurz auf die Divisionspolynome ein, die es ermöglichen, die Endomorphismen $\alpha \in \mathbb{Z}$ koordinatenmäßig zu beschreiben. In Anhang E werden drei weitere Aussagen über die Normabbildung gemacht, die lediglich von theoretischem Interesse sind.
Einige Teile der Arbeit (etwa Abschnitt 5.2) haben übersichtsartigen Charakter, denn eine ausführliche Darstellung hätte den Umfang bei weitem gesprengt. Aus diesem Grund sind wir auch nicht auf die Konstruktion elliptischer Kurven mit komplexer Multiplikation eingegangen. Abschnitt 4.5 stellt einen einfachen Speziallfall dieses Konstruktionsverfahrens dar. Für Beweise und Details sei auf die angegebene Literatur verwiesen.

Bezeichnungen

Die verwendeten Bezeichnungen orientieren sich an denen für die Begriffe üblichen Symbole und Buchstaben. Wir waren bemüht, Mehrdeutig- und Unstimmigkeiten zu vermeiden. Auf einige Feinheiten möchten wir kurz hinweisen.
Das Symbol $\mathbb{K}$ steht in der ganzen Arbeit für einen beliebigen Körper. Der Buchstabe K bezeichnet in Kapitel vier den imaginär quadratischen Zahlkörper, der als Ring die Ordnung $\mathcal{O}$ enthält. In diesem Kapitel steht L für den Ringklassenkörper von K und M für einen beliebigen Zahlkörper. Im Anhang A steht K für einen beliebigen Zahlkörper und L für eine Körpererweiterung von K.
Auch für den Begriff der Norm ließ sich eine Doppeldeutigkeit nicht vermeiden. In Kapitel drei stehen die Norm und der Buchstabe N für die dort definierte Normabbildung der Punktegruppe einer Körpererweiterung. In den Kapiteln vier und fünf bezeichnet Norm stets die Norm einer imaginär quadratischen Zahl. Dafür verwenden wir wieder abkürzend den Buchstaben N. Nur in Satz E.2 ist hier wieder von der Normabbildung aus Kapitel drei die Rede. Wir bezeichnen sie dort mit dem Symbol $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}$.

Einige weitere Symbole:

$\mathbb{C}[x]$	Polynomring in x mit Koeffizienten in $\mathbb{C}$
$\mathbb{C}(x)$	Körper der rationalen Funktionen in x mit Koeffizienten in $\mathbb{C}$
(p)	Ideal, das von p erzeugt wird
$\mathcal{O} \otimes \mathbb{Q}$	Tensorprodukt von $\mathcal{O}$ mit $\mathbb{Q}$, d.h. der Quotientkörper von $\mathcal{O}$
$\lceil x \rceil$	nächste ganze Zahl, die größer gleich x ist
$\lfloor x \rfloor$	nächste ganze Zahl, die kleiner gleich x ist

Kapitel 1

Grundlagen

1.1 Definition einer elliptischen Kurve

Definition 1.1. *Sei $\mathbb{K}$ ein Körper und $\overline{\mathbb{K}}$ sein algebraischer Abschluß.*
Eine über einem Körper $\mathbb{K}$ definierte ***elliptische Kurve*** *E ist eine Gleichung der Form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{K}, \tag{1.1}$$

mit der Eigenschaft, daß keine Lösung $(x, y) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ existiert, die gleichzeitig die Gleichungen

$$\begin{aligned} y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6, \\ 2y + a_1x + a_3 &= 0 \text{ und} \\ a_1y &= 3x^2 + 2a_2x + a_4 \end{aligned} \tag{1.2}$$

erfüllt.
Die Gleichung (1.1) heißt ***Weierstraß-Gleichung*** *der elliptischen Kurve.*

Die Eigenschaft, daß die Gleichungen 1.2 nicht simultan erfüllt werden können, garantiert, daß die Kurve nicht singulär ist.

Definition 1.2. *Sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Die* ***Menge der $\mathbb{L}$-rationalen Punkte auf*** *E ist die Menge aller Punkte $(x, y) \in \mathbb{L} \times \mathbb{L}$, die der Gleichung 1.1 genügen, vereinigt mit einem unendlich fernen Punkt* ***0****. Sie wird mit $E(\mathbb{L})$ bezeichnet.*

Meist nennen wir die Punktemenge $E(\mathbb{L})$ selbst elliptische Kurve.
Wir interessieren uns hauptsächlich für elliptische Kurven über endlichen Körpern $\mathbb{F}_q$. Hier unterscheidet man zwei Klassen, supersinguläre und gewöhnliche Kurven.

Definition 1.3. *Sei die Anzahl der Punkte auf einer elliptischen Kurve über einem endlichen Körper $\mathbb{F}_q$ der Charakteristik p durch $\#E(\mathbb{F}_q) = q + 1 - t$ gegeben. Eine elliptische Kurve $E(\mathbb{F}_q)$ heißt **supersingulär**, falls $p \mid t^2$. Eine elliptische Kurve $E(\mathbb{F}_q)$ heißt **gewöhnlich**, falls sie nicht supersingulär ist.*

Beide Klassen von Kurven unterscheiden sich durch eine Reihe wichtiger Eigenschaften. Für eine übersichtliche Auflistung siehe Husemöller [17], Seite 258. Auf einen besonderen Unterschied werden wir später zurückkommen, wenn wir die Endomorphismen von elliptische Kurven über endlichen Körpern betrachten.

Definition 1.4. *Seien E_1, E_2 zwei über einem Körper $\mathbb{K}$ definierte elliptische Kurven. Eine **rationale Abbildung** ϕ zwischen E_1 und E_2 ist eine Abbildung $\phi : E_1 \to E_2$, für die rationale Funktionen $f(x,y), g(x,y) \in \overline{\mathbb{K}}(x,y)$ existieren, so daß*

$$\phi((x,y)) = (f(x,y), g(x,y))$$

*für alle (x,y) in $E_1(\overline{\mathbb{K}}) \setminus \{\mathbf{0}\}$ mit $\phi((x,y)) \neq \mathbf{0}$. Falls $f(x,y)$, $g(x,y)$ in $\mathbb{L}(x,y)$ für eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$, dann sagen wir, ϕ ist **über $\mathbb{L}$ definiert**.*
*Eine **Isogenie** zwischen E_1 und E_2 ist eine rationale Abbildung $\phi : E_1 \to E_2$ mit $\phi(\mathbf{0}) = \mathbf{0}$.*
*Eine bijektive Isogenie ist ein **Isomorphismus**, und zwei Kurven, zwischen denen eine bijektive Isogenie existiert, heißen **isomorph**.*

Bei fester Charakteristik des Körpers $\mathbb{K}$ lassen sich einfachere Gleichungen als Gleichung 1.1 angeben, die wir Normalformen nennen. Jede elliptische Kurve ist zu einer Kurve in Normalform über $\mathbb{K}$ isomorph. Allerdings existieren zu einer gegebenen Kurve mehrere isomorphe Kurven in Normalform.
Für char $\mathbb{K} \neq 2, 3$ ist jede elliptische Kurve zu einer Kurve der Form

$$y^2 = x^3 + ax + b \text{ mit } a, b \in \mathbb{K} \text{ und } 4a^3 + 27b^2 \neq 0 \text{ in } \mathbb{K}$$

isomorph.

Für char $\mathbb{K} = 3$ ist die Menge der Isomorphieklassen elliptischer Kurven durch

$$y^2 = x^3 + a_2x^2 + a_6 \text{ mit } \quad a_2, a_6 \in \mathbb{K} \text{ und } a_2a_6 \neq 0,$$

im gewöhnlichen und

$$y^2 = x^3 + a_4x + a_6 \text{ mit } a_4, a_6 \in \mathbb{K} \text{ und } a_4 \neq 0,$$

im supersingulären Fall gegeben.
Für char $\mathbb{K} = 2$ beschreibt

$$y^2 + xy = x^3 + a_2x^2 + a_6 \text{ mit } a_2, a_6 \in \mathbb{K} \text{ und } a_6 \neq 0$$

die Menge der gewöhnlichen und

$$y^2 + a_3y = x^3 + a_4 + a_6 \text{ mit } a_3, a_4, a_6 \in \mathbb{K} \text{ und } a_3 \neq 0$$

die Menge der supersingulären Kurven.
In dieser Arbeit werden wir uns nur mit gewöhnlichen Kurven über Primzahlkörpern $\mathbb{K}$ der Charakteristik ungleich $2, 3$ und Kurven über Körpern der Charakteristik zwei beschäftigen. Diese sind für Anwendungen am interessantesten, da die Arithmetik in Primzahlkörpern und Körpern der Charakteristik zwei besonders effizient ist.
Supersinguläre Kurven behandeln wir in dieser Arbeit nicht, da es gegen die gängigen Kryptoverfahren auf supersingulären Kurven effizientere Angriffe gibt (siehe auch Kapitel zwei und Seite 100).

1.2 Addition auf der elliptischen Kurve

Auf der elliptischen Kurve läßt sich eine Addition erklären. Die Formeln für die Addition ergeben sich aus der geometrischen Anschauung, siehe z.B. Abbildung auf Seite 5 und für eine Erläuterung Silverman [51], Kapitel 2 . Eine Animation der Punktaddition auf der elliptischen Kurve findet sich auf der Certicom-Seite unter *http://www.certicom.ca/ecc/enter/ec51.htm*.
Wir geben die Formeln für gewöhnliche elliptische Kurven über Körpern der Charakteristik $\neq 3$ an.
Für char $\mathbb{K} \neq 2, 3$ ist die Kurve durch $y^2 = x^3 + ax + b$ gegeben. Sei $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ und $P_3 = P_1 + P_2 = (x_3, y_3)$.
Falls $P_1 = \mathbf{0}$, dann ist $P_3 = P_2$, und falls $P_2 = \mathbf{0}$, folgt $P_3 = P_1$.
Wenn $x_2 = x_1$ und $y_2 = -y_1$, dann haben wir $P_3 = \mathbf{0}$.
Für alle anderen Fälle lassen sich folgende Formeln ausrechnen:
Für $P_1 \neq P_2$ ergibt sich

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ \text{und } y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3), \end{aligned}$$

und falls $P_1 = P_2$, dann folgt

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ \text{und } y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{aligned}$$

In char $\mathbb{K} = 2$ ist eine gewöhnliche Kurve durch $y^2 + xy = x^3 + a_2x^2 + a_6$ gegeben.
Wieder folgt aus $P_1 = \mathbf{0}$, daß $P_3 = P_2$, und für $P_2 = \mathbf{0}$, gilt $P_3 = P_1$.
Falls $P_2 = (x_1, x_1 + y_1)$, dann haben wir $P_3 = \mathbf{0}$.
Für die anderen Fälle ergeben sich die folgenden Formeln:

$$\begin{aligned} x_3 &= \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, \\ y_3 &= \frac{y_1 + y_2}{x_1 + x_2}(x_1 + x_3) + x_3 + y_1, \end{aligned}$$

falls $P_1 \neq P_2$, und

$$\begin{aligned} x_3 &= x_1^2 + \frac{a_6}{x_1^2}, \\ y_3 &= x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3, \end{aligned}$$

falls $P_1 = P_2$.
Die Punkte der elliptischen Kurve bilden mit dem angegebenen Additionsgesetz eine abelsche Gruppe. Für einen Beweis der Gruppeneigenschaften, insbesondere der Assoziativität, siehe [62].
Die Gruppenstruktur von elliptischen Kurven über endlichen Körpern ist sehr gut erforscht.

Satz 1.5. *Sei eine elliptische Kurve $E(\mathbb{F}_q)$ gegeben. Dann gilt*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2} \text{ mit } n_2 \mid n_1 \text{ und } n_2 \mid q - 1. \tag{1.3}$$

Beweise für diesen Satz findet man in den Arbeiten von Voloch [59] und Rück [45].

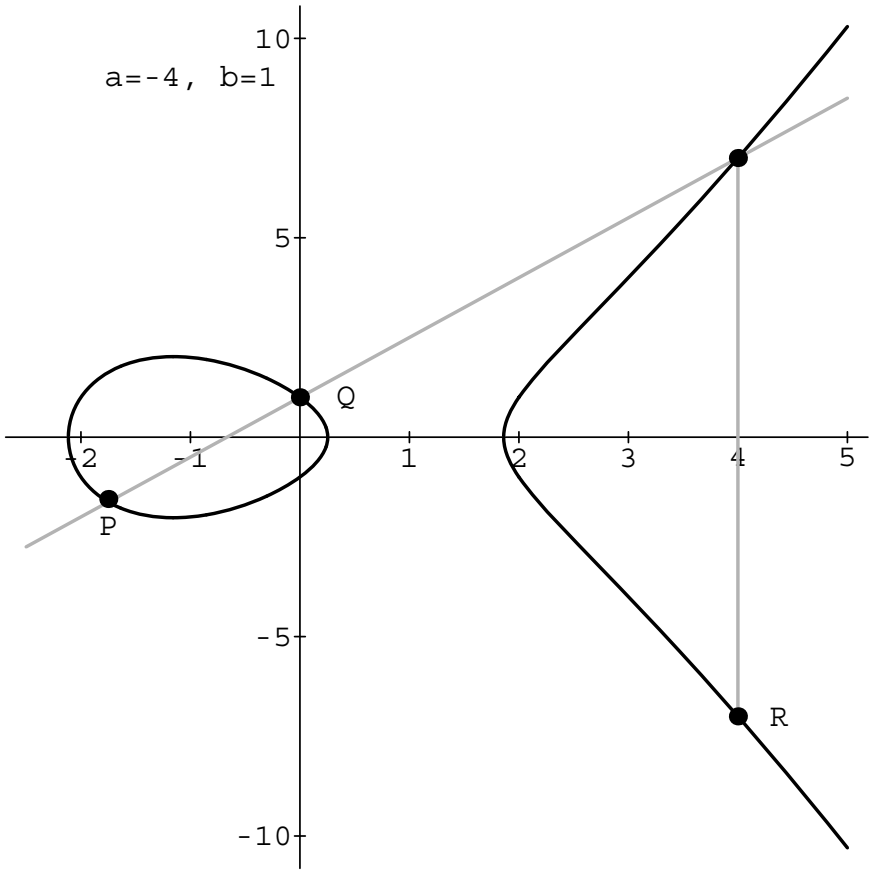

Abbildung 1.1: Illustration der Punktaddition $R = P+Q$ an der elliptischen Kurve $y^2 = x^3+ax+b$ über den reellen Zahlen

Kapitel 2

Der diskrete Logarithmus

In diesem Kapitel stellen wir das Problem des diskreten Logarithmus auf elliptischen Kurven vor. Zur Lösung dieses Problems auf einer beliebigen elliptischen Kurve ist bisher kein subexponentieller Algorithmus bekannt. Auf der Schwierigkeit, den diskreten Logarithmus zu berechnen, basieren die meisten Kryptosysteme auf elliptischen Kurven (siehe z.B. das Kryptosystem auf Seite 8).
Das diskrete Logarithmusproblem ist auch Ausgangspunkt dieser Arbeit. Aus ihm haben wir einige Fragestellungen abgeleitet, die wir in den nächsten Kapiteln behandeln werden. Außerdem werden wir uns damit beschäftigen, wie wir möglichst schnell eine Instanz des diskreten Logarithmusproblems erzeugen können.
Wie wir in Abschnitt 2.2 sehen werden, gibt es bereits eine Reihe von Angriffen gegen spezielle Klassen von Kurven. Durch einen dieser Algorithmen haben sich zum Beispiel Punktegruppen $E(\mathbb{F}_p)$ mit $\#E(\mathbb{F}_p) = p$ als unsicher erwiesen. Durch die Tate-Paarung haben supersinguläre Kurven ihre Attraktiviät verloren. Wirkungsvolle Angriffe, die die Verwendung von gewöhnlichen Kurven mit einem Endomorphismenring mit kleiner Klassenzahl in Frage stellen, gibt es bisher jedoch nicht. Hier gelang es bisher nur, den exponentiellen Pollard-Rho-Angriff um einen konstanten Faktor zu verbessern.
Aus Abschnitt 2.2 lernen wir auch, wie wichtig es ist, die Gruppenordnung der gewählten Punktegruppe der elliptischen Kurve zu kennen, um die Schwierigkeit des diskreten Logarithmusproblems zu gewährleisten. Für Kurven, die über einem kleinen Grundkörper definiert sind, läßt sich diese sehr einfach bestimmen (siehe Abschnitt 2.3).

2.1 Das Problem des diskreten Logarithmus

Unter dem Problem des diskreten Logarithmus auf der elliptischen Kurve versteht man die folgende Fragestellung:

> Gegeben eine über einem endlichen Körper $\mathbb{F}_q$ definierte Kurve und zwei Punkte P, Q aus der Punktegruppe $E(\mathbb{F}_{q^k})$ über einer Körpererweiterung $\mathbb{F}_{q^k}$, finde ein $r \in \mathbb{Z}$, so daß $rP = Q$, falls ein solches r existiert.

Falls $rP = Q$ für $r \in \mathbb{Z}$, dann nennen wir r (in Anlehnung an das Logarithmusproblem in der multiplikativen Gruppe eines endlichen Körpers) den diskreten Logarithmus und schreiben $r = \log_P Q$.
Eine Instanz (E, P, Q) eines diskreten Logarithmusproblems auf einer elliptischen Kurve E läßt sich durch die in Abschnitt 1.2 angegebenen Formeln und mit Hilfe des Repeated-Squaring Algorithmus mit $O(\log m)$ elliptischen Operationen erzeugen, wenn m die Gruppenordnung von $E(\mathbb{F}_{q^k})$ ist. Zu effizienten Algorithmen für die Skalarmultiplikation kommen wir noch in Kapitel 6.
Hingegen scheint es nicht möglich aus P und Q den diskreten Logarithmus r mit $rP = Q$ in subexponentieller, geschweige denn in polynomieller Zeit in $\log m$ zu berechnen. Die bisher bekannten Algorithmen zur Berechnung des diskreten Logarithmus auf der elliptischen Kurve werden kurz im nächsten Abschnitt vorgestellt.
Auf der Schwierigkeit, den diskreten Logarithmus zu berechnen, basieren etliche Public-Key-Kryptosysteme, wie z.B. das Schlüsselaustauschverfahren von Diffie-Hellmann und das System von El-Gamal zur Nachrichtenverschlüsselung. Für die Variante des Signaturalgorithmus DSA für elliptische Kurven (ECDSA) soll ein IEEE-Standard eingeführt werden. Wir geben auf Seite 8 diesen Algorithmus auf einer Kurve über einem Primkörper an.
Wir nehmen an, daß Alice die Signaturerzeugung korrekt ausgeführt hat. Dann berechnet Bob im dritten Schritt

$$u_1 P + u_2 Q = (H(m)w \mod q)P + (rw \mod q)Q = (x_0, y_0).$$

Nun gilt aber $xP = Q$. Also erhält Bob

$$\begin{aligned} & (H(m)w \mod q)P + (rw \mod q)xP \\ = \; & ((H(m)w + rwx) \mod q)P \qquad \textit{da } P \textit{ Ordnung } q \textit{ hat} \\ = \; & (w(H(m) + rx) \mod q)P \\ = \; & kP. \end{aligned}$$

ECDSA:
Parameter (öffentlich): Kurve $E(\mathbb{F}_p)$, Punkt $P \in E(\mathbb{F}_p)$,
privater Schlüssel: eine ganze Zahl x im Intervall $[2 \ldots q-2]$,
öffentlicher Schlüssel: der Punkt Q mit $xP = Q$.

Signaturerzeugung:

1. A(lice) wählt $k \in_R [2..q-2]$.

2. A berechnet $kP = (x_1, y_1)$ und $r = x_1 \mod q$. [1]Falls $r = 0$, dann geht sie zu Schritt 1 zurück, da sonst die Signatur s, die in Schritt 3 berechnet wird, den privaten Schlüssel x nicht enthalten würde.

3. A berechnet $k^{-1} \mod q$ und den Hashwert $H(m)$ der Nachricht m. Dann bildet sie $s = k^{-1}(H(m) + xr) \mod q$.

4. Falls $s = 0$, beginnt sie wieder bei Schritt 1. Sonst sendet A die Nachricht m mit der Signatur (r, s) an B(ob).

Signaturverifikation:

1. B prüft, ob $r, x \in [1..q-1]$.

2. B berechnet $w = s^{-1} \mod q$ und den Hashwert $H(m)$. Dann bildet er $u_1 = H(m)w \mod q$ und $u_2 = rw \mod q$.

3. B ermittelt $u_1P + u_2Q = (x_0, y_0)$.

4. Er akzeptiert genau dann, wenn $x_0 \mod q = r$ ist.

[1] Mit „ mod q“ bezeichnen wir hier und auch später den kleinsten positiven Rest von q modulo m.

Deshalb muß $x_0 = r \mod q$ gelten.
Falls ein beliebiger Benutzer C den diskreten Logarithmus berechnen kann, erhält er aus P und Q den geheimen Schlüssel x und kann damit Signaturen von A fälschen.

2.2 Algorithmen für den diskreten Logarithmus

Es sei E eine über einem endlichen Körper $\mathbb{F}_q$ definierte elliptische Kurve und sei $E(\mathbb{F}_{q^k})$ die möglicherweise nicht zyklische Punktegruppe der Kurve über dem Körper $\mathbb{F}_{q^k}$. Weiter sei n die maximale Ordnung, die ein Punkt P auf der Kurve $E(\mathbb{F}_{q^k})$ haben kann.
Wir möchten in diesem Abschnitt Kriterien erstellen, die die Gruppenordnung einer kryptographisch sicheren elliptischen Kurve erfüllen muß. Dazu betrachten wir die Algorithmen, die es bisher für die Berechnung des diskreten Logarithmus auf der elliptischen Kurve gibt.

Pollards ρ-Methode [43]: Der bisher effizienteste Algorithmus zur Berechnung diskreter Logarithmen in beliebigen Gruppen ist Pollards ρ-Methode. Dieser Algorithmus hat Laufzeit $O(\sqrt{n})$.
Pohlig-Hellmann [16]: Falls n in Primfaktoren $p_i, 1 \leq i \leq k$ zerfällt, können wir das diskrete Logarithmusproblem auf k diskrete Logarithmusprobleme in zyklischen Gruppen der Ordnung p_i zurückführen. Die Laufzeit hängt somit weniger von der Größe der Zahl n als von ihrem größten Primfaktor ab.
Deshalb sollten wir bei der Wahl der Kurve beachten, daß deren Gruppenordnung entweder selbst prim ist oder einen großen Primfaktor $\tilde{p}$ enthält.
Frey-Rück-Reduktion (Tate-Paarung, [10], Weil-Paarung, [39]):
Sei $E(\mathbb{F}_q)_n$ die Gruppe der über $\mathbb{F}_q$ rationalen Punkte auf E, deren Ordnung die Zahl n teilt.
Falls die Gruppe der n-ten Einheitswurzeln μ_n in $\mathbb{F}_q^*$ liegt, also $n \mid q-1$, dann gibt es eine Abbildung Φ_n von Tupeln (P,Q) mit $P \in E(\mathbb{F}_q)_n$ und $Q \in E(\mathbb{F}_q)$ in die Gruppe der n-ten Einheitswurzeln μ_n.
Diese hat folgende Eigenschaften:

1. Sie ist $\mathbb{Z}$-linear in beiden Komponenten, d.h.

$$\begin{aligned} \Phi_n(P+P',Q) &= \Phi_n(P,Q)\Phi_n(P',Q) \text{ und} \\ \Phi_n(P,Q+Q') &= \Phi_n(P,Q)\Phi_n(P,Q'). \end{aligned}$$

2. Zu einer zyklischen Untergruppe von $E(\mathbb{F}_q)$ der Ordnung n existiert ein Punkt

P' in $E(\mathbb{F}_q)$ mit

$$\{\Phi_n(P,P');P\in E(\mathbb{F}_q)_n\}=\mu_n.$$

3. Die Paarung ϕ_n läßt sich in $O(\log q)$ elliptischen Operationen (d.h. Punktadditionen oder -verdopplungen) berechnen. Der Punkt P' aus 2. läßt sich in probabilistisch polynomialer Zeit in $\log q$ finden. Falls die Ordnung der Kurve prim ist, können wir ihn sogar direkt angeben.

Sei nun (E,P,Q) eine Instanz eines diskreten Logarithmusproblems mit $P\in E(\mathbb{F}_q)$, ord $P=n$ und $Q=rP$ für ein noch unbekanntes $r\in\mathbb{Z}_n$. Nun sei P' ein Punkt auf $E(\mathbb{F}_q)$, so daß $\alpha=\Phi_n(P,P')$ eine primitive n-te Einheitswurzel ist. Dieser Punkt existiert nach der zweiten Eigenschaft.
Wir setzen $\beta=\Phi_n(Q,P')$, und wir haben aufgrund der $\mathbb{Z}$-Linearität:

$$\begin{aligned}\beta &= \Phi_n(Q,P')=\Phi_n(rP,P')\\ &= \Phi_n(P,P')^r=\alpha^r.\end{aligned}$$

Somit haben wir das Problem des diskreten Logarithmus auf der elliptische Kurven in ein Problem in dem darunterliegenden Körper reduziert. Da es für das diskrete Logarithmusproblem in $\mathbb{F}_q^*$ subexponentielle Algorithmen gibt, können wir dann den diskreten Logarithmus auf der elliptischen Kurve in subexponentieller Zeit berechnen.
Falls $n\nmid q-1$, aber $n\mid q^k-1$ für kleines k, dann können wir die Punktegruppe $E(\mathbb{F}_{q^k})$ der elliptischen Kurve betrachten. Wir definieren dann die Paarung auf Tupeln (P,Q) mit $P\in E(\mathbb{F}_{q^k})_n$ und $Q\in E(\mathbb{F}_{q^k})$ und reduzieren das diskrete Logarithmusproblem auf $E(\mathbb{F}_q)$ mit der Abbildung Φ_n auf das diskrete Logarithmusproblem in $\mathbb{F}_{q^k}^*$. Beachte, daß wir dann ein diskretes Logarithmusproblem in einer echten Untergruppe von $\mathbb{F}_{q^k}$ lösen müssen.
Damit das diskrete Logarithmusproblem nicht effizient in einen endlichen Körper reduziert werden kann, fordern wir also, daß der größte Primfaktor $\tilde{p}$ der Gruppenordnung keine der Zahlen q^k-1 mit $k\le(\log q)^2$ teilt. Damit sind alle supersingulären Kurven für kryptographische Anwendung uninteressant, da hier $k\le 6$ gilt.
Für eine zufällig gewähltes Paar (p,E) mit p Primzahl und E eine elliptische Kurve über $\mathbb{F}_p$ mit $\#E(\mathbb{F}_p)=l$ schätzen N. Koblitz und R. Balasubramanian [4] die Wahrscheinlichkeit für $l\mid p^k-1$ für ein $k\le(\log p)^2$ ab. Sie erhalten als obere Schranke $\frac{c_3(logM)^9(loglogM)^2}{M}$, mit $M\le p\le 2M$ und einer berechenbaren Konstanten c_3[2]. Für

[2] Die Konstante c_3 ist von allen Parametern unabhängig. Sie ist nicht unerheblich, da in der Praxis mit M nur von beschränkter Größe ist. Leider geben die Autoren in [4] keine obere Schranke für c_3 an. Die Konstante geht unter anderem auf die Arbeit von Lenstra [31] zum Faktorisieren auf elliptischen Kurven zurück und könnte von dort ausgehend ermittelt werden.

Kurven, die nicht über einem Primkörper definiert sind, gibt es noch keine Aussagen über die Wahrscheinlichkeit, eine Kurve zu finden, die gegen die Tate-Paarung sicher ist.

Reine anomale Kurven[3] [46, 54, 49]:
Falls $\#E(\mathbb{F}_p) = p$ gilt, gibt es sogar Algorithmen, die den diskreten Logarithmus in der Punktegruppe $E(\mathbb{F}_p)$ in *linearer* Zeit in $\log p$ berechnen. Diese beruhen darauf, daß man auf elliptischen Kurven, die über den p-adischen Zahlen $\mathbb{Q}_p$ definiert sind, den Logarithmus leicht berechnen kann.
Bei Kurven, für die $\#E(\mathbb{F}_p) = p$ gilt, können wir das Logarithmusproblem nach $\mathbb{Q}_p$ liften. Diese Liftung ist sehr effizient möglich, da es genügt, alle auftretenden Zahlen, insbesondere die Koordinaten der Punkte P und Q, bis zu einer Genauigkeit mod p^2 zu berechnen.
Bei der Wahl einer über einem großen Primkörper $\mathbb{F}_p$ definierten Kurve müssen wir deshalb darauf achten, daß $\#E(\mathbb{F}_p) \neq p$ ist.

Verbesserter Pollard-Rho [63, 12]):
Die Pollard-Rho-Methode kann für Kurven, die über einem Teilkörper definiert sind, durch Ausnutzung des Frobeniusendomorphismus verbessert werden.
Falls E über $\mathbb{F}_q$ definiert ist und wir ein diskretes Logarithmusproblem in der Punktegruppe $E(\mathbb{F}_{q^m})$ betrachten, dann können wir die Laufzeit von Pollards Rho-Algorithmus um einen Faktor $\sqrt{m}$ verbessern. Die gleiche Methode läßt sich auch auf die Kurve mit komplexer Multiplikation mit $\sqrt{-1}$ oder $\frac{1+\sqrt{-3}}{2}$ anwenden. Hier erreichen wir allerdings nur geringfügige Verbesserungen von Faktor 2 und $\sqrt{6}$.
Trotz der Verbesserung läuft der Algorithmus noch exponentiell.

Außerdem sei noch der folgende Artikel von S. Galbraith genannt, der es in einem speziellen Fall erlaubt, das diskrete Logarithmusproblem auf einer Kurve auf das einer anderen Kurve zu transformieren.

Isogene Kurven [11]:
Seien E_1 und E_2 über $\mathbb{F}_p$ definierte elliptische Kurven. Falls $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$, dann gibt es einen Algorithmus zur Konstruktion einer Isogenie zwischen den beiden Kurven. Dieser ermöglicht es, ein diskretes Logarithmusproblem von E_1 nach E_2 zu transformieren. Der Algorithmus hat im allgemeinen aber exponentielle Laufzeit.

Wir fassen die Anforderungen an die Gruppenordnung der elliptischen Kurve zusammen:

1. Die Gruppenordnung soll durch eine große Primzahl p geteilt werden, die die Laufzeit aller Algorithmen für das Logarithmusproblem in beliebigen Grup-

[3] Diese sind nicht mit den anomalen Koblitz-Kurven zu verwechseln.

pen sprengt. Pollards ρ-Methode zusammen mit dem Algorithmus von Pohlig-Hellmann ergeben eine Laufzeit von $\sqrt{p}$ für das diskrete Logarithmusproblem in einer beliebigen Gruppe. Die Primzahl p sollte also mindestens 180 Bits haben.

2. Für die Primzahl p aus 1. sollte $p \nmid q^k - 1$ für alle $k \leq (\log q)^2$ gelten. Insbesondere sollte die Kurve nicht supersingulär sein.

3. Falls wir eine über einem großen Primkörper $\mathbb{F}_p$ definierte Kurve wählen, fordern wir, daß $p \neq \#E(\mathbb{F}_p)$. betreiben.

Um zu überprüfen, ob eine elliptische Kurve den gestellten Anforderungen genügt, müssen wir ihre Gruppenordnung kennen.
Es ist prinzipiell möglich, über einem endlichen Körper $\mathbb{F}_q$ definierte Kurven zufällig zu wählen und dann die Punkte zu zählen, da dafür Algorithmen existierten, die polynomiell in $\log q$ laufen. Der erste Algorithmus zum Punktezählen von Schoof [47] hatte eine Laufzeit in $(\log q)^8$ und war somit völlig unpraktikabel. Mittlerweile gibt es aber neue Ideen und Verbesserungen [48, 32, 29], die den Algorithmus nun für die Praxis interessant machen.
Eine Alternative besteht darin, eine elliptische Kurve mit gewünschter Gruppenordnung zu konstruieren oder spezielle Kurven zu nehmen, bei denen die Punkteanzahl auf der Hand liegt und kein Zählalgorithmus nötig ist. Zu letzteren gehören elliptische Kurven, die bereits über einem Teilkörper definiert sind. Diese werden wir im nächsten Abschnitt etwas genauer untersuchen. Für diese Kurven gibt es auch sehr schnelle Algorithmen zur Skalarmultiplikation rP (siehe Kapitel 6).

Bemerkung 2.1. Für die **Index-Kalkulus-Methode**, die den diskreten Logarithmus in endlichen Körpern in subexponentieller Zeit berechnet, existiert auf elliptischen Kurven bisher noch kein vergleichbarer, subexponentieller Algorithmus. Wenn wir die Idee von endlichen Körpern auf elliptische Kurven übertragen wollen, treten einige Probleme auf [37, 52].
Sei $(E(\mathbb{F}_q), P, Q)$ eine Instanz des diskreten Logarithmusproblems. Wir möchten r mit $rP = Q$ bestimmen.
Wenn wir die Index-Calculus-Methode auf elliptische Kurven übertragen, benötigen wir zunächst ein Äquivalent zu einer Menge kleiner Primzahlen in $\mathbb{Z}$. Dazu müssen wir die über $\mathbb{F}_q$ definierte Kurve zu einer über $\mathbb{Q}$ definierten Kurve E' liften und hier nach einer Menge von Erzeugenden $\{R_s, s \in S\}$ mit kleiner Höhe suchen. Unter einem Punkt mit kleiner Höhe verstehen wir einen Punkt bei dem die Zähler und Nenner der beiden Koordinaten eine festgelegte Schranke nicht überschreiten. Darin liegt bereits das erste Problem. Im Gegensatz zu den ganzen Zahlen $\mathbb{Z}$, die von unendlich vielen Primzahlen erzeugt werden, ist die Punktegruppe $E'(\mathbb{Q})$ nach dem Satz von Mordell-Weil nur endlich erzeugt. Auch wenn vermutet wird, daß elliptische Kurven von beliebig hohem Rang existieren, hat es sich bisher als schwierig

erwiesen, Kurven von hohem Rang zu finden.
Als nächstes müßten die Punkte P und Q nach $E'(\mathbb{Q})$ geliftet werden. Das ist wieder ein Problem.
Dann könnten wir Relation

$$kP = \sum_{s \in S} e_s R_s$$

auf $E(\mathbb{Q})$ suchen, und schließlich benötigen wir noch ein c, so daß $cP + Q$ sich als Linearkombination der R_s darstellen läßt. Die Relationen lassen sich dann nach $E(\mathbb{F}_q)$ reduzieren. Wenn wir genügend Relationen gesammelt haben, erhalten wir die diskreten Logarithmen der R_s bezüglich P und schließlich auch r durch Lösung eines Gleichungssystems.
J.H.Silverman hatte eine neue Idee [53], die die Vorgehensweise umkehrt und deswegen den Namen **Xedni-Kalkulus-Methode** trägt. Er liftet zunächst Punkte über $E(\mathbb{F}_p)$ zu Punkten in $E(\mathbb{Q})$ und sucht dann eine Kurve, die durch diese Punkte geht. Es hat sich aber herausgestellt [19], daß dieser probabilistische Algorithmus fast immer exponentielle Laufzeit in $\log p$ hat.

2.3 Kurven über kleinem Grundkörper

In diesem Abschnitt untersuchen wir über $\mathbb{F}_q$ definierte Kurven, die durch eine Gleichung der Form 1.1 beschrieben sind, bei der wir aber die über $\mathbb{F}_{q^k}$ rationalen Punkte betrachten.
Wir werden sehen, daß wir aus der Kenntnis von $\#E(\mathbb{F}_q)$ die Anzahl $\#E(\mathbb{F}_{q^k})$ leicht berechnen können. Dazu benötigen wir die Zeta-Funktion einer elliptischen Kurve.

Definition 2.2. *Die **Zeta-Funktion** einer über $\mathbb{F}_q$ definierten elliptischen Kurve E, ist die Potenzreihe*

$$Z(E/\mathbb{F}_q; T) = \quad exp\ \left(\sum_{r \geq 1} \#E(\mathbb{F}_{q^r}) \frac{T^r}{r} \right). \tag{2.1}$$

Es gilt der folgende Satz, der in seiner allgemeineren Form für projektive Varietäten als Weilsche Vermutung [61] bekannt ist:

Satz 2.3. *Die Zeta-Funktion einer elliptischen Kurve ist eine Funktion in $\mathbb{Q}(T)$. Sie hat die Form*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - tT + qT^2}{(1-T)(1-qT)}, \tag{2.2}$$

wobei $t = q + 1 - \#E(\mathbb{F}_q)$. *Außerdem hat das Polynom* $1 - tT + qT^2$ *(im Zähler) echt komplexe Nullstellen* $\frac{1}{\alpha}, \frac{1}{\overline{\alpha}}$, *deren Absolutbetrag* $\frac{1}{\sqrt{q}}$ *ist.*

Korollar 2.4. *Sei* $t = q + 1 - \#E(\mathbb{F}_q)$ *und* $1 - tT + qT^2$ *zerfalle in Linearfaktoren* $(1 - \alpha T)(1 - \overline{\alpha}T)$. *Dann gilt*

$$\#E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \overline{\alpha}^k. \tag{2.3}$$

Beweis. Aus Satz 2.3 zusammen mit der Gleichung

$$\ln(1 - cT) = -\sum c^r T^r / r$$

folgt

$$\begin{aligned}
\ln Z(E/\mathbb{F}_q; T) &= \ln\left(\frac{1 - tT + qT^2}{(1 - T)(1 - qT)}\right) \\
&= \ln\left(\frac{(1 - \alpha T)(1 - \overline{\alpha}T)}{(1 - T)(1 - qT)}\right) \\
&= -\sum_{r \geq 1} \alpha^r T^r / r - \sum_{r \geq 1} \overline{\alpha}^r T^r / r + \sum_{r \geq 1} T^r / r + \sum_{r \geq 1} q^r T^r / r \\
&= \sum_{r \geq 1} \left(-\alpha^r - \overline{\alpha}^r + 1 + q^r\right) T^r / r.
\end{aligned}$$

Wenn wir nun wieder exponentieren, ergibt sich

$$Z(E/\mathbb{F}_q; T) = exp(\sum_{r \geq 1} \left(-\alpha^r - \overline{\alpha}^r + 1 + q^r\right) T^r / r).$$

Koeffizientenvergleich mit der Gleichung (2.1) liefert uns nun die Behauptung. □

Zur Illustration betrachten wir noch ein Beispiel:

Beispiel 2.5. Die Kurve E sei durch

$$y^2 + xy = x^3 + 1$$

über $\mathbb{F}_2$ gegeben.
Es gilt $\#E(\mathbb{F}_2) = 4 = 2 + 1 - (-1)$, also $t = -1$. Damit ergibt sich die Gleichung $1 + T + 2T^2$, die die komplexen Nullstellen $\alpha = \frac{-1+\sqrt{-7}}{2}$ und $\overline{\alpha} = \frac{-1+\sqrt{-7}}{2}$ besitzt.
Nach Korollar 2.4 gilt nun $\#E(\mathbb{F}_{2^k}) = 2^k + 1 - \alpha^k - \overline{\alpha}^k$. Wir erhalten zum Beispiel $\#E(\mathbb{F}_{2^{233}}) = 1380349269358112757486951172455405104228376395544900850531234$
$8098965372 = 4 \cdot 345087317339528189371737793113851276057094098886225212632$
087024741343. Die Ordnung der Punktegruppe $E(\mathbb{F}_{2^{233}})$ ist also durch eine Primzahl mit siebzig Dezimalstellen teilbar.

Elliptische Kurven, die über einem Teilkörper definiert sind, haben natürlich einige spezielle Eigenschaften:
• Sie enthalten eine Untergruppe $E(\mathbb{F}_q)$. Wir werden im nächsten Kapitel einen Gruppenhomomorphismus untersuchen, der die Punktegruppe $E(\mathbb{F}_{q^k})$ in die Untergruppe $E(\mathbb{F}_q)$ abbildet.
• Da der Grundkörper der Kurve in der Regel klein ist, ist auch der zugehörige Endomorphismenring eine Ordnung in einem quadratischen Zahlkörper mit kleiner Diskriminante. Das bedeutet, daß es in dem Endomorphismenring von E mehr Elemente mit kleiner Norm gibt und alle Endomorphismen, insbesondere auch die diskreten Logarithmen, über dem Grundkörper definiert sind. Wir werden später noch näher auf diese Begriffe eingehen.
Damit das diskrete Logarithmusproblem dadurch nicht einfacher wird, muß sichergestellt werden, daß diese Eigenschaften die Berechnung des diskreten Logarithmus nicht begünstigen.

Kapitel 3

Die Norm von Punkten in einer Körpererweiterung

In diesem Kapitel beschäftigen wir uns mit den Punktegruppen $E(\mathbb{F}_{q^k})$ elliptischer Kurven, die über einem Körper $\mathbb{F}_q$ definiert sind. Die Punktegruppe $E(\mathbb{F}_{q^k})$ enthält die Menge der über $\mathbb{F}_q$ rationalen Punkte, $E(\mathbb{F}_q)$, als Untergruppe. Wir untersuchen eine Abbildung, die die Punktegruppe $E(\mathbb{F}_{q^k})$ auf die Punktegruppe $E(\mathbb{F}_q)$ abbildet. Diese nennen wir Normabbildung.
Die Normabbildung ist in der Literatur bisher noch nicht untersucht worden und deshalb von theoretischen Interesse. Sie hat viele Eigenschaften, die wir auch von der Spur von Elementen einer endlichen Körpererweiterung kennen.
Wir möchten durch Untersuchung eines Logarithmusproblems auf $E(\mathbb{F}_q)$ Informationen über das diskrete Logarithmusproblem auf $E(\mathbb{F}_{q^k})$ erhalten. Leider bringt diese Methode nicht mehr ein als der Angriff von Pohlig-Hellmann (siehe dazu auch Abschnitt 3.4 und Satz 3.18).
Weiter untersuchen wir eine speziell gewählte Instanz eines diskreten Logarithmusproblems. Wir zeigen, da das Punktepaar $(P, \sigma(P))$ für ein beliebiges σ in $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ ein unsicheres Paar ist, d.h. wir können r mit $\sigma(P) = rP$ polynomial in $\log n$ berechnen, wobei n hier die Größe der von P aufgespannten Untergruppe ist.

3.1 Definition

Im folgenden sei $\mathbb{L}/\mathbb{K}$ eine Galoissche Körpererweitung mit $[\mathbb{L} : \mathbb{K}]$ endlich und sei E eine über $\mathbb{K}$ definierte elliptische Kurve. Wir untersuchen in diesem Abschnitt eine Abbildung der Punktegruppe $E(\mathbb{L})$ nach $E(\mathbb{K})$. In späteren Abschnitten werden wir uns dann auf endliche Körper beschränken.

Lemma 3.1. *Sei $\mathbb{L}/\mathbb{K}$ Galoissch und E über $\mathbb{K}$ definiert. Sei $\sigma \in Gal(\mathbb{L}/\mathbb{K})$ und $(x,y) \in E(\mathbb{L})$. Dann ist auch $(\sigma(x),\sigma(y)) \in E(\mathbb{L})$.*

Beweis. Die elliptische Kurve E sei durch die Weierstraß-Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{K}$$

gegeben.
Es gilt

$$\sigma(y^2 + a_1xy + a_3y) = \sigma(x^3 + a_2x^2 + a_4x + a_6).$$

Da σ in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ haben wir $\sigma(a_i) = a_i$. Weil σ ein Körperautomorphismus ist, also mit der Addition und Multiplikation im Körper verträglich ist, ergibt sich dann

$$\sigma(y)^2 + a_1\sigma(x)\sigma(y) + a_3\sigma(y) = \sigma(x)^3 + a_2\sigma(x)^2 + a_4\sigma(x) + a_6,$$

d.h. $(\sigma(x),\sigma(y)) \in E(\mathbb{L})$. □

Sei E über $\mathbb{K}$ definiert und $P = (x,y) \in E(\mathbb{L})$. Wir bezeichnen den Punkt $(\sigma(x),\sigma(y))$ nun mit $\sigma(P)$.

Lemma 3.2. *Sei E eine über einem Körper K definierte Kurve und $\sigma \in Gal(\mathbb{L}/\mathbb{K})$. Dann gilt*

$$\sigma(P) + \sigma(Q) = \sigma(P+Q). \tag{3.1}$$

Beweis. Sei $P = (x_1,y_1)$, $Q = (x_2,y_2)$ und $P+Q = (x_3,y_3)$. Für den Beweis dieses Lemmas müssen wir zeigen, daß $\sigma(x_1,y_1) + \sigma(x_2,y_2) = \sigma(x_3,y_3)$ ist.
Wir verifizieren dies für den Fall, daß E eine über Charakteristik 2 definierte, gewöhnliche elliptische Kurve in Normalform

$$y^2 + xy = x^3 + a_2x^2 + a6, a_6 \in \mathbb{K} \text{ mit } a_6 \neq 0$$

und $P \neq Q$ ist.
Dann gelten für $P+Q = (x_3,y_3)$ die Formeln (siehe Kapitel 1)

$$\begin{aligned} x_3 &= \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a_2, \\ y_3 &= \frac{y_1+y_2}{x_1+x_2}(x_1+x_3) + x_3 + y_1. \end{aligned}$$

Sei nun $\sigma(P) = (\sigma(x_1),\sigma(y_1))$ und $\sigma(Q) = (\sigma(x_2),\sigma(y_2))$. Dann gilt für $\sigma(P) + \sigma(Q) = (x_3',y_3')$ Dann gelten für $P+Q = (x_3,y_3)$ die Formeln (siehe Kapitel 1)

$$\begin{aligned} x_3' &= \left(\frac{\sigma(y_1)+\sigma(y_2)}{\sigma(x_1)+\sigma(x_2)}\right)^2 + \frac{\sigma(y_1)+\sigma(y_2)}{\sigma(x_1)+\sigma(x_2)} + \sigma(x_1) + \sigma(x_2) + a_2, \\ y_3' &= \frac{\sigma(y_1)+\sigma(y_2)}{\sigma(x_1)+\sigma(x_2)}(\sigma(x_1)+\sigma(x_3)) + \sigma(x_3) + \sigma(y_1). \end{aligned}$$

Da $a_2 = \sigma(a_2)$ und σ ein Körperautomorphismus ist, sehen wir nun, daß $x_3' = \sigma(x_3)$ und $y_3' = \sigma(y_3)$.
Für alle anderen Fälle, falls z.B. Charakterstik $\mathbb{K} \neq 2$ oder die Kurve nicht in Normalform gegeben ist, verläuft der Beweis analog. □

Aus diesem Satz ergeben sich zwei Korollare:

Korollar 3.3. *Sei E eine über $\mathbb{K}$ definierte elliptische Kurve und $(x,y) \in E(\mathbb{L})$. Dann hat der Punkt (x,y) in der Gruppe $E(\mathbb{L})$ die gleiche Ordnung wie der Punkt $(\sigma(x),\sigma(y))$ für alle $\sigma \in Gal(\mathbb{L}/\mathbb{K})$.*

Korollar 3.4. *Sei E eine über $\mathbb{K}$ definierte elliptische Kurve. Falls der Punkt P maximale Ordnung in $E(\mathbb{L})$ hat, dann gilt dies auch für $\sigma(P)$.*

Definition 3.5. *Sei E wie bisher über $\mathbb{K}$ definiert und $\mathbb{L}/\mathbb{K}$ eine Galoissche Körpererweiterung. Die **Norm** ist eine Abbildung von $E(\mathbb{L})$ nach $E(\mathbb{L})$ gegeben durch*

$$N_{\mathbb{L}/\mathbb{K}}(P) = N_{\mathbb{L}/\mathbb{K}}((x,y)) := \sum_{\sigma \in Gal(\mathbb{L}/\mathbb{K})} ((\sigma(x),\sigma(y)) \tag{3.2}$$

für $P \in E(\mathbb{L})$. Die Punkte auf der rechten Seite der Gleichung 3.2 werden nach der Additionsformel auf der elliptischen Kurve summiert.

Wenn klar ist, für welche Körpererweiterung wir die Normabbildung betrachten, dann schreiben wir statt $N_{\mathbb{L}/\mathbb{K}}(P)$ auch einfach $N(P)$.

Satz 3.6. *Für alle P in $E(\mathbb{L})$ gilt*

$$N(P) \in E(\mathbb{K}).$$

Die Normabbildung ist also eine Abbildung von $E(\mathbb{L})$ nach $E(\mathbb{K})$.

Beweis. Wir zeigen $N(P) = \sigma(N(P))$ für alle $\sigma \in Gal(\mathbb{L}/\mathbb{K})$. Da ein Punkte genau dann in $E(\mathbb{K})$ ist, wenn er von allen Automorphismen der Galoisgruppe $Gal(\mathbb{L}/\mathbb{K})$ festgelassen wird, folgt daraus die Behauptung.
Sei $\tilde{\sigma} \in Gal(\mathbb{L}/\mathbb{K})$ beliebig gewählt. Dann gilt unter Benutzung von Lemma 3.2

$$\begin{aligned}
\tilde{\sigma}(N(P)) &= \tilde{\sigma}\left(\sum_{\sigma \in Gal(\mathbb{L}/\mathbb{K})} (\sigma(x),\sigma(y)\right) \\
&= \sum_{\sigma \in Gal(\mathbb{L}/\mathbb{K})} (\tilde{\sigma}\sigma(x),\tilde{\sigma}\sigma(y)) = \sum_{\hat{\sigma} \in Gal(\mathbb{L}/\mathbb{K})} (\hat{\sigma}(x),\hat{\sigma}(y)) \\
&= N(P).
\end{aligned}$$

□

3.2 Eigenschaften der Norm

Im folgenden betrachten wir den für uns interessanten Fall $\mathbb{K} = \mathbb{F}_q$ und $\mathbb{L} = \mathbb{F}_{q^k}$ mit $q = p^n$. Wir werden einige wichtige Eigenschaften, die wir auch von der Normabbildung endlicher Körper kennen, untersuchen.
Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ ist eine zyklische Gruppe der Ordnung k (siehe auch [64], S. 168), die vom Frobeniusautomorphismus

$$\pi_q : x \longmapsto x^q$$

erzeugt wird. Beachte, daß π_q^k auf $\mathbb{F}_{q^k}$ die Identität ist.
Wie wir bisher Elemente der Galoisgruppe auf Punkte der elliptischen Kurve wirken ließen, können wir es auch mit dem Frobeniusendomorphismus machen. Wir erhalten also eine Abbildung $\pi_q : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ gegeben durch

$$\pi_q : (x, y) \longmapsto (x^q, x^q).$$

Diese heißt der **Frobeniusendomorphismus** der Punktegruppe $E(\mathbb{F}_{q^k})$.
Das nächste Lemma gilt auch noch für die allgemeine Situation einer beliebigen Galoisschen Körpererweiterung $\mathbb{L}/\mathbb{K}$ aus Abschnitt 3.1.

Lemma 3.7 (Homomorphismuseigenschaft). *Es gilt*

$$N(P) + N(Q) = N(P + Q)$$

für alle $P, Q \in E(\mathbb{F}_{q^k})$.

Beweis. Seien $P = (x_1, y_1)$, $Q = (x_2, y_2)$ und $P + Q = (x_3, y_3)$. Mit Lemma 3.2 ergibt sich

$$\begin{aligned} N(P) + N(Q) &= \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} (\sigma(x_1), \sigma(y_1)) + \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} (\sigma(x_2), \sigma(y_2)) \\ &= \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} ((\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) \\ &= \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} (\sigma(x_3), \sigma(y_3)) = N(P + Q). \end{aligned}$$

□

Daraus folgt direkt

Korollar 3.8. *Für alle* $P \in E(\mathbb{F}_{q^k})$ *gilt*

$$ord_{E(\mathbb{F}_q)} N(P) \mid ord_{E(\mathbb{F}_{q^k})} P.$$

Der folgende Satz folgt direkt aus der Definition der Normabbildung:

Satz 3.9. *Sei E über $\mathbb{F}_q$ definiert. Dann gilt für alle $P \in E(\mathbb{F}_q)$*

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(P) = k \cdot P. \tag{3.3}$$

Daraus folgt:

Korollar 3.10. *Falls $ggT(\#E(\mathbb{F}_q), k) = 1$, dann läßt sich ein Endomorphismus $f : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ definieren, der auf $E(\mathbb{F}_q)$ die Identität ist, und $E(\mathbb{F}_{q^k})$ auf die Untergruppe $E(\mathbb{F}_q)$ abbildet.*
Dieser Endomorphismus ist durch $l \circ N$ mit $l \in \mathbb{Z}$ und $lk = 1 \mod \#E(\mathbb{F}_q)$, gegeben.

Unter dem Endomorphismus l verstehen wir die Abbildung

$$l : P \to lP.$$

Lemma 3.11 (Transitivität). *Sei E über $\mathbb{F}_q$ definiert und $P \in E(\mathbb{F}_{q^{kl}})$. Dann gilt*

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q}\left(N_{\mathbb{F}_{q^{kl}}/\mathbb{F}_{q^k}}(P)\right) = N_{\mathbb{F}_{q^{kl}}/\mathbb{F}_q}(P). \tag{3.4}$$

Beweis. Der Punkt P sei gegeben durch (x, y). Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ ist die Menge der Automorphismen $\{x \mapsto x^{q^i}, 0 \le i \le k-1\}$, und die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^{kl}}/\mathbb{F}_{q^k})$ ist durch $\{x \mapsto x^{q^{kj}}, 0 \le j \le l-1\}$ gegeben.
Eine Rechnung zeigt

$$\begin{aligned}
N_{\mathbb{F}_{q^k}/\mathbb{F}_q}(N_{\mathbb{F}_{q^{kl}}/\mathbb{F}_{q^k}}(P)) &= \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sigma\Big(\sum_{\hat{\sigma} \in Gal(\mathbb{F}_{q^{kl}}/\mathbb{F}_{q^k})} \hat{\sigma}(P)\Big) \\
&= \sum_{\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sum_{\hat{\sigma} \in Gal(\mathbb{F}_{q^{kl}}/\mathbb{F}_{q^k})} \sigma\hat{\sigma}(P) \\
&= \sum_{i=0}^{k-1} \sum_{j=0}^{l-1} (x^{q^{jk+i}}, y^{q^{jk+i}}) \\
&= \sum_{i=0}^{kl-1} (x^{q^i}, y^{q^i}) = \sum_{\sigma \in Gal(\mathbb{F}_{q^{kl}}/\mathbb{F}_q)} \sigma(P) \\
&= N_{\mathbb{F}_{q^{kl}}/\mathbb{F}_q}(P).
\end{aligned}$$

□

Als nächstes möchten wir die Surjektivität der Normabbildung beweisen. Dazu ist zunächst ein Lemma nötig.

Lemma 3.12. *Folgende Aussagen sind äquivalent:*

1. $P \in KernN$
2. *Es existiert* $Q \in E(\mathbb{F}_{q^k})$ *mit* $P = Q - \pi_q(Q)$, *wobei* π_q *der Frobeniusendomorphismus ist.*

Anders formuliert: Die Sequenz

$$1 \to E(\mathbb{F}_q) \stackrel{i}{\to} E(\mathbb{F}_{q^k}) \stackrel{id-\pi_q}{\to} E(\mathbb{F}_{q^k}) \stackrel{N}{\to} E(\mathbb{F}_q)$$

ist exakt.

Beweis. Eine Richtung ($2 \Rightarrow 1$) ist trivial, da $N(Q) = N(\sigma(Q))$ für alle $\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$.
Für die Richtung ($1 \Rightarrow 2$) betrachte den Endomorphismus

$$f : Q \longmapsto Q - \pi_q(Q)$$

auf $E(\overline{\mathbb{F}}_q)$. Dieser Endomorphismus ist nicht die Nullabbildung und deshalb nach Satz B.5 aus Appendix B surjektiv. Sei nun $P \in KernN$. Es gibt ein $Q \in E(\overline{\mathbb{F}}_q)$ mit $f(Q) = P$, und da $\overline{\mathbb{F}}_{q^k} = \bigcup_{l=1}^{\infty} \mathbb{F}_{q^{kl}}$, gilt $Q \in E(\mathbb{F}_{q^{kt}})$ für ein $t \in \mathbb{N}$.
Es bleibt zu zeigen, daß $t = 1$:

$$\begin{aligned} 0 &= N(P) = P + \pi_q(P) + \cdots + \pi_q(P)^{k-1} \\ &= Q - \pi_q(Q) + \pi_q(Q - \pi_q(Q)) + \cdots + \pi_q^{k-1}(Q - \pi_q(Q)) \\ &= Q - \pi_q(Q) + \pi_q(Q) + \cdots + \pi_q(Q)^k \\ &= Q - \pi_q(Q)^k. \end{aligned}$$

Also gilt $Q \in E(\mathbb{F}_{q^k})$. □

Wir können die Normabbildung $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ zu einer Abbildung $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ auf $E(\overline{\mathbb{F}_q})$ erweitern, indem wir

$$\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(P) = \overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}((x,y)) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i}).$$

für alle $P \in E(\overline{\mathbb{F}_q})$ setzen.
Aus dem Beweis von Lemma 3.12 ergibt sich folgende Aussage für die auf $E(\overline{\mathbb{F}_q})$ erweiterte Normabbildung:

Korollar 3.13. *Falls $P \in Kern\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$, dann ist P über $\mathbb{F}_{q^k}$ rational.*

Satz 3.14 (Surjektivität). *Die Normabbildung $N : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ ist surjektiv, falls sie nicht die Nullabbildung ist.*

Beweis. Betrachte den Endomorphismus $f : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ mit $Q \to Q - \sigma(Q)$ aus dem vorangegangenen Korollar. Wir wissen, daß $Bild\ f = KernN$, und außerdem gilt nach dem Isomorphiesatz für Gruppen

$$\#E(\mathbb{F}_{q^k}) = (\#KernN)(\#BildN) \text{ und}$$
$$\#E(\mathbb{F}_{q^k}) = (\#Bild\ f)(\#Kernf).$$

Daraus ergibt sich $\#BildN = \#Kernf$. Da $BildN \subseteq Kernf = E(\mathbb{F}_q)$, folgt nun $BildN = E(\mathbb{F}_q)$, und das ist die Behauptung. □

Lemma 3.15. *Falls k prim ist, dann gilt*

$$KernN_{\mathbb{F}_{q^k}/\mathbb{F}_q} \equiv 1 \mod k.$$

Beweis. Wir bezeichnen $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ in diesem Beweis schlicht mit N.
Falls $P \in KernN$, dann gilt $\sigma(P) \in KernN$ für alle $\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$.
Somit enthält der Kern von N außer dem neutralen Punkt $\mathbf{0}$ noch l weitere Klassen von jeweils $k = \#Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ zueinander konjugierten Punkten für ein $l \in \mathbb{Z}$.
Es gilt

$$\#KernN = 1 + l \cdot k \equiv 1 \mod k.$$

□

3.3 Bedeutung für den diskreten Logarithmus

3.3.1 Reduktion auf den Kern

Sei $kP = Q$ mit $P, Q \in E(\mathbb{F}_{q^k})$ und E definiert über $\mathbb{F}_q$.
Dann gilt nach Lemma 3.7 $N(Q) = N(kP) = kN(P) = lN(P)$, wobei $l \equiv k \mod \text{ord } N(P)$.

Das diskrete Logarithmusproblem auf der über $E(\mathbb{F}_q)$ definierten elliptischen Kurve läßt sich auf auf zwei Teilprobleme reduzieren:

a) Lösen des diskreten Logarithmus in der kleinen Gruppe $E(\mathbb{F}_q)$.
Dies ist im allgemeinen kein Problem, da $\#E(\mathbb{F}_q)$ klein ist.

b) Lösen des diskreten Logarithmus für Elemente, die im Kern von N liegen.

Algorithmus 1 Reduktion auf den Kern

Input: $P, Q \in E(\mathbb{F}_{q^k})$ mit $Q \in < P >$
Output: $m \in \mathbb{Z}$, so daß $mP = Q$.
1: Berechne $N(P), N(Q)$, ord $N(P)$ und m', so daß $m'N(P) = N(Q)$.
2: Löse das diskrete Logarithmusproblem für $P' = ordN(P)P$ und $Q' = Q - m'P$, d.h. finde l, so daß $l \cdot (ordN(P)) \cdot P = Q - m'P$.
(Beachte, daß P' und $Q' \in KernN$.)
3: Setze $m = m' + l$ ord $N(P)$.

3.3.2 Der Kern der Normabbildung

Wie wir im vorherigen Kapitel gesehen haben, wird die Untergruppe von $E(\mathbb{F}_{q^k})$, die für die Kryptographie interessant ist, im Kern von N liegen. Deshalb untersuchen wir diesen hier gesondert. Wir nehmen dabei an, daß k prim ist. Sonst existiert ein Primteiler k' von k und eine weitere Untergruppe $E(\mathbb{F}_{q^{k'}})$ von $E(\mathbb{F}_{q^k})$.

Der Kern der Normabbildung N ist eine Untergruppe von $E(\mathbb{F}_{q^k})$. Für ein festes P' ist die Menge $\{P, N(P) = P', P' \in E(\mathbb{F}_q)\}$ eine vollständige Nebenklasse von N. Da N surjektiv ist, gilt nach dem Isomorphiesatz für Gruppen $E(\mathbb{F}_{q^k})/KernN \simeq E(\mathbb{F}_q)$. Außerdem haben wir natürlich $\#KernN \mid \#E(\mathbb{F}_{q^k})$.
In dem für kryptographische Anwendung interessanten Fall, $\#E(\mathbb{F}_{q^k}) = aE(\mathbb{F}_q)p^*$ mit a klein, p^* eine große Primzahl, gilt dann $p^* \mid \#KernN$.
Wir zeigen nun, daß das Punktepaar $(P, \sigma(P)), \sigma$ in $Gal(\mathbb{F}_{q^k}, \mathbb{F}_q)$ für ein diskretes Logarithmusproblem vermieden werden sollte. Wir werden dafr zwei Fälle unterscheiden und diese getrennt untersuchen.

Kern von N ist eine zyklische Untergruppe

Falls $KernN$ zyklisch ist, dann existiert ein P mit $KernN =< P >$. Außerdem folgt aus $P \in KernN$, auch $\sigma(P) \in KernN$ d.h. $\sigma(P) \in < P >$ für alle σ in $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$. Von einem konjugierten Punkt $\sigma(P)$ von P läßt sich der diskrete Logarithmus in probabilistisch polynomialer Zeit in k berechnen.

Zunächst nehmen wir an, daß die Ordnung von P prim ist. Dies ist in der Praxis häufig der Fall.

Satz 3.16. *Sei $P \in E(\mathbb{F}_{q^k})$, aber nicht in $E(\mathbb{F}_q)$. Außerdem sei die Ordnung p von P auf E prim und $\sigma(P) \in < P >$ für alle σ in $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$. Es gilt also $mP = \sigma(P)$ für ein m.*
Dann ist m Nullstelle eines Polynoms $f(x) = x^{k-1} + x^{k-2} + \ldots + 1$ modulo der Ordnung von P. Jede Nullstelle von $f \mod ord\ P$ entspricht dem diskreten Logarithmus eines konjugierten Punktes $\sigma(P)$ von P.
Ferner gilt: Falls σ die Gruppe $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ erzeugt und $\sigma(P) \in < P >$, dann gilt bereits $P \in KernN$.

Beweis. Sei $P \in KernN$ und $\sigma(P) \in < P >$ für alle σ in $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$. Sei nun σ ein erzeugendes Element der zyklischen Gruppe $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ und $\sigma(P) = mP$. Dann gilt $\sigma^i(P) = m^iP$ für $1 \leq i \leq k$. Insbesondere haben wir $P = \sigma^k(P) = m^kP$. Somit teilt die Ordnung p von P die Zahl $m^k - 1$, und m ist Nullstelle des Polynoms $x^k - 1$ mod p. Jede der $k-1$ von Eins verschiedenen Nullstellen gibt uns den diskreten Logarithmus eines konjugierten Punktes.
Sei nun $mP = \sigma(P)$. Da $m \neq 1$ und p prim, ist m Nullstelle von $x^{k-1} + x^{k-2} + \cdots + 1$ mod p und somit

$$N(P) = \sum_{\sigma} \sigma(P) = P + mP + m^2P + \ldots + m^{k-1}P = 0.$$

□

Wenn nun k prim ist, dann gilt nach Lemma 3.15, daß

$$p = \#KernN \equiv 1 \mod k.$$

Die Nullstellen des Polynoms $x^k - 1$ bilden eine Untergruppe U, die gerade aus allen Elementen aus $\mathbb{F}_p^*$ besteht, die die Ordnung k haben. Um ein erzeugendes Element von U zu finden, wählen wir zufällig ein Element a aus $\mathbb{F}_p^*$. Falls a erzeugendes Element von $\mathbb{F}_p^*$ ist, dann ist a^l für $l \cdot k = p - 1$ ein erzeugendes Element von U. Die zu P konjugierten Punkte, d.h. die Punkte $\sigma(P)$ für ein $\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$, sind dann durch $a^{li}, 1 \leq i \leq k-1$, gegeben.
Wenn wir a zufällig aus $\mathbb{F}_p^*$ wählen, dann ist a mit Wahrscheinlichkeit $\frac{\varphi(p-1)}{p-1}$ ein erzeugendes Element von $\mathbb{F}_p^*$, wobei φ die Eulersche φ-Funktion ist. Im Durchschnitt müssen wir $\frac{p-1}{\varphi(p-1)}$ Elemente wählen, bis wir das gesuchte $a \in \mathbb{F}_p^*$ gefunden haben. Da $\varphi(n) > c\frac{n}{\log\log n}$ für $n \geq 3$ und eine Konstante $c \in \mathbb{R}$ (siehe Kapitel I, Satz 5.1, [44]), sind dies höchstens $O(\log\log(p-1))$ Runden. In jeder Runde prüfen wir, ob das gewählte Element maximale Ordnung hat. Dafür benötigen wir, falls wir die

Faktorzerlegung von $p-1$ kennen, höchstens $O(\log p)$ Schritte. Schließlich müssen wir noch a^l und die von a^l erzeugte zyklische Gruppe berechnen. Zusammen sind dies polynomial viele Schritte in $\log p$. Da $p \leq \#E(\mathbb{F}_{q^k})$ und $\#E(\mathbb{F}_{q^k}) \approx q^k$ (siehe Abschnitt 2.3), gilt $\log p = O(k)$. Somit können wir den diskreten Logarithmus eines zu P konjugierten Punktes in probabilistisch polynomialer Zeit in k berechnen.

Leicht aufwendiger wird es, wenn der Kern von N zwar zyklisch ist, aber $\#KernN$ nicht prim ist. Sei $\#KernN = p^*n$, wobei n prim oder zusammengesetzt ist, und $\sigma(P) = mP$ mit noch unbekanntem m. Natürlich ist m auch hier wieder Lösung der Gleichung $m^k - 1 \bmod \mathrm{ord}(P)$, aber diese Gleichung kann mehr als k Lösungen haben. Es gilt

$$\sigma(P) = mP = a(nP) + bP \text{ mit } b < n. \tag{3.5}$$

Falls n klein ist, kann man die entsprechende Nebenklasse von $\sigma(P)$ bezüglich nP durch die Weil-Paarung e_{p^*} berechnen. Für Definition und Berechnung dieser Paarung siehe [36], [62].
Diese hat die Eigenschaft, daß

$$e_{p^*}(nP, \sigma(P) - kP) = 1,$$

genau dann, wenn $\sigma(P) - kP$ in dem Erzeugnis von kP liegt (siehe hierzu auch [36], Lemma 5.4, Seite 69). Wir setzen also in $e_{p^*}(nP, \sigma(P) - kP)$ für k die Zahlen in $[0 \ldots n-1]$ ein, bis wir für ein k den Wert eins erhalten. Dies ist dann unsere gesuchte Zahl b in Gleichung (3.5), und es gilt $b \equiv m \mod n$.
Außerdem haben wir $\sigma(nP) = t(nP)$ für ein $t \in \mathbb{F}_{p^*}^*$. Da $ord(nP) = p^*$ und p^* prim, können wir $t \in \mathbb{F}_{p^*}^*$ mit Satz 3.16 ermitteln. Wir haben

$$n\sigma(P) = \sigma(nP) = t(nP) = n(tP) \mod ord(nP).$$

Somit gilt $m \equiv t \mod p^*$. Da wir angenommen haben, daß n relativ klein und p^* eine große Primzahl ist, gilt $ggT(n, p^*) = 1$, und wir erhalten $m \mod np^*$ aus dem Chinesischen Restsatz.

Kern von N ist nicht zyklisch

Wenn der Kern von N eine nicht zyklische Untergruppe ist, so muß er nach Satz 1.5 die Form $\mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}, n_2 \mid n_1$, haben. Dann gilt im allgemeinen nicht $\sigma(P) \in < P >$. Dazu ein Gegenbeispiel:

Beispiel 3.17. Betrachte die Kurve E über $\mathbb{F}_{2^3}$, die durch

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad a_2 = \alpha^3, a_6 = \alpha$$

und α ist ein festes primitives Element in $\mathbb{F}_{2^3}$. Sei nun β ein primitives Element aus $\mathbb{F}_{2^9}$ über $\mathbb{F}_{2^3}$. Dann hat $P = [\beta^{65}, \beta^{53}]$ die konjugierten Punkte $\sigma_1(P) = [\beta^9, \beta^{424}]$ und $\sigma_2(P) = [\beta^{72}, \beta^{326}]$. Es gilt $\sigma_1(P), \sigma_2(P) \notin < P >$, ord P=7 und $KernN \simeq \mathbb{Z}_7 \bowtie \mathbb{Z}_7$.

Angenommen, n_2 sei klein, ord P=n_1 und (P, Q) ein erzeugendes Paar für den Kern von N. Dann gilt

$$\begin{aligned} \sigma(P) &= a_1 P + a_2 Q \text{ und} \\ \sigma(Q) &= b_1 P + b_2 Q. \end{aligned}$$

Da n_2 klein ist, lassen sich b_2 und a_2 durch die Weil-Paarung leicht bestimmen. Auch b_1 läßt sich leicht herausfinden, da $\text{ord}(\sigma(Q)) = ord(Q)$. Damit ist der gesuchte Wert a_1 eine gemeinsame Wurzel zweier Polynome der Ordnung $k-1$.

3.4 Fazit

Die Ausführungen haben gezeigt, daß die kryptographisch interessante Untergruppe immer im Kern der Normabbildung liegt. Dieser ist aber sehr groß und entspricht in den kryptographisch relevanten Fällen oft sogar der zyklischen Untergruppe von großer, primer Ordnung, die die Kurve aufweisen sollte, um gegen den Pohlig-Hellmann-Angriff (siehe Seite 9) gefeit zu sein.
Wenn man die Abbildung $\pi_q^k - 1$, deren Kern $E(\mathbb{F}_{q^k})$ ist, mit dem Polynom $x^k - 1$ identifiziert, dann entspricht unsere Normabbildung $N = \pi_q^{k-1} + \pi_q^{k-2} + \ldots + id$ dem Faktor $x^{k-1} + x^{k-2} + \ldots + 1$. Wir können nun auch ähnlich mit anderen Faktoren $t(x)$ von $x^k - 1$ verfahren, und den diskreten Logarithmus jeweils im Bild von $t(\pi_q)$ berechnen. Daß dies aber nur dann effizient zu einer Lösung des diskreten Logarithmusproblems in $E(\mathbb{F}_q)$ führt, falls wir auch Pohlig-Hellmann-Angriff erfolgreich anwenden können, zeigt der folgende Satz:

Satz 3.18. *Zu jedem Faktor $g(x)$ des Polynoms $x^k - 1$ existiert ein Teiler der Gruppenordnung von $E(\mathbb{F}_{q^k})$, der diesem entspricht.*

Aus diesem Satz ergibt sich, daß $E(\mathbb{F}_{q^k})$ in viele Primfaktoren zerfällt, wenn das Polynom $x^k - 1$ in viele Primfaktoren zerfällt. Die Umkehrung gilt nicht.
Für den Beweis dieses Satzes benötigen wir noch einige theoretische Grundlagen über elliptische Kurven. Deshalb verschieben wir diesen auf das nächste Kapitel. Er folgt auf Seite 32.

Im Abschnitt 3.3.2 haben wir gesehen, daß die Instanzen der Form $(P, \sigma(P))$ für

ein σ der Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$ unsicher sind. Allerdings gibt es für ein festes P höchstens $k-1$ zu P konjugierte Punkte in der von P erzeugten Untergruppe in $\mathrm{E}(\mathbb{F}_{q^k})$. Wenn wir die Instanz (P,Q) also zufällig wählen, ist es sehr unwahrscheinlich, daß Q zu P konjugiert ist.
Auf der anderen Seite muß man in der Praxis damit rechnen, daß ein Angreifer aus P zunächst einige Punkte für Q berechnet. Dafür wird er Punkte wählen, die er einfach aus P erzeugen kann. Dies sind zum Beispiel kleine Vielfache von P, aber eben auch die zu P konjugierten Punkte. Der folgende Satz bezieht sich auf den in der Praxis interessanten Fall $q = 2^n$.

Satz 3.19. *Die Menge aller zu P konjugierten Punkte läßt sich in $2(k-1)\log q$ Quadraturen in $\mathbb{F}_{q^k}$ ermitteln.*

Beweis. Sei $P = P_0 = (x,y)$ und $P_i = (x^{q^i}, y^{q^i})$ für $1 \leq i \leq k-1$. Nun läßt sich $x^{q^{i+1}}$ aus x^{q^i} durch $\log q$ Quadraturen in $\mathbb{F}_{q^k}$ errechnen, und somit benötigen wir $2\log q$ Quadraturen um aus P_i den Punkte P_{i+1} zu bestimmen. Daraus folgt die Behauptung. □

Bei der Implementierung eines Kryptosystems, das auf dem diskreten Logarithmusproblem beruht, stellt sich nach der Wahl eines zufälligen diskreten Logarithmus r nun die Frage, ob man den Fall, daß $Q = rP$ zu P konjugiert ist, abfängt oder das relativ geringe Risiko, daß Q zu P konjugiert sein könnte, auf sich nimmt.

Kapitel 4

Endomorphismen elliptischer Kurven

Der Endomorphismenring einer über einem endlichen Körper definierten Kurve enthält viele Informationen über die elliptische Kurve selbst. So gibt er Aufschluß über die Gruppenordnung (siehe Satz 4.6) und die Gruppenstruktur (siehe Satz 4.14) ihrer Punktegruppen.
Das diskrete Logarithmusproblem kann auch in der Sprache der Endomorphismen formuliert werden. Diese Version nennen wir das verallgemeinerte diskrete Logarithmusproblem:

$$\text{Gegeben } P,\ Q, \text{ finde ein } \alpha \in End(E) \text{ mit } \alpha(P) = Q.$$

Falls $Q = rP$ für ein $r \in \mathbb{Z}$, dann ist $\alpha : P \mapsto rP$ eine Lösung des verallgemeinerten Logarithmusproblems. Doch die Lösung des verallgemeinerten Logarithmusproblems ist nicht eindeutig, denn es gibt unendlich viele Endomorphismen in $End(E)$, die P auf Q abbilden. Damit ergibt sich die natürliche Frage, wann zwei Endomorphismen auf einer Punktegruppe identisch sind. In Abschnitt 4.4 zeigen wir, daß wir aus einer beliebigen Lösung bereits eine Lösung für das diskrete Logarithmusproblem erhalten.
Davon losgelöst betrachten wir genauer die beiden Kurvenklassen, die den Endomorphismenring mit kleinster Diskriminante besitzen (siehe Abschnitt 4.5). Wir geben Algorithmen an, wie wir über Primkörpern definierte Kurven aus diesen Kurvenklassen erzeugen können, die die in Abschnitt 2.2 gestellen Anforderungen an die Gruppenordnung erfüllen.

4.1 Theoretische Grundlagen

Definition 4.1. *Ein* ***Endomorphismus*** ϕ *einer über einem Körper* $\mathbb{K}$ *definierten elliptischen Kurve* E *ist eine rationale Abbildung (siehe Definition 1.4) von* $E(\overline{\mathbb{K}})$ *auf sich selbst, so daß* $\phi(\mathbf{0}) = \mathbf{0}$.

Es läßt sich zeigen, daß jeder Endomorphismus ein Gruppenhomomorphismus ist, d.h. daß

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Für einen Beweis siehe z.B. [51]. Hier ist Achtung geboten, denn die Umkehrung dieser Aussage gilt nicht. Nicht jeder Gruppenendomorphismus einer elliptische Kurve E ist ein Endomorphismus im Sinne der Definition 4.1, da er nicht zwangsläufig rational ist.
Die Endomorphismen einer elliptischen Kurve bilden mit den Verknüpfungen

$$\begin{aligned}(\phi + \psi)(P) &= \phi(P) + \psi(P) \text{ und} \\ (\phi \circ \psi)(P) &= \phi(\psi(P))\end{aligned}$$

einen Ring, den wir mit $End(E)$ bezeichnen.
Der Endomorphismenring $End(E)$ einer elliptischen Kurve E enthält die Menge der Abbildungen

$$P \mapsto rP \text{ für } r \in \mathbb{Z}. \tag{4.1}$$

Dies ist ein zu $\mathbb{Z}$ isomorpher Teilring von $End(E)$. In einigen Fällen ist dies bereits der komplette Endomorphismenring. Das gilt aber nicht immer.

Definition 4.2. *Eine elliptische Kurve hat* ***komplexe Multiplikation****, falls* $End(E)$ *nicht zu* $\mathbb{Z}$ *isomorph ist.*

Wenn eine elliptische Kurve komplexe Multiplikation hat, gibt es also noch andere Endomorphismen als die in Gleichung (4.1) angegebenen. Jede Kurve, die über $\mathbb{F}_q$ definiert ist, hat komplexe Multiplikation, da der
Frobeniusendomorphismus

$$\pi_q : (x, y) \mapsto (x^q, y^q)$$

zu keiner der Abbildung $P \mapsto rP$ für $r \in \mathbb{Z}$ identisch ist, also ein nicht in $\mathbb{Z}$ enthaltener Endomorphismus ist.
Um die Endomorphismenringe beschreiben zu können, benötigen wir eine weitere Definition.

Definition 4.3. *Sei $\mathcal{A}$ eine über $\mathbb{Q}$ endlich erzeugte Algebra. Unter einer* ***Ordnung*** *$\mathcal{O}$ von $\mathcal{A}$ versteht man einen Teilring von $\mathcal{A}$, der ein endlich erzeugtes $\mathbb{Z}$-Modul ist und $\mathcal{O} \otimes \mathbb{Q} = \mathcal{A}$ erfüllt.*

Nun läßt sich zeigen:

Satz 4.4. *Sei E eine gewöhnliche (d.h nicht supersinguläre) elliptische Kurve über $\mathbb{F}_q$. Dann ist der Endomorphismenring $End(E)$ eine Ordnung in einem imaginär quadratischen Zahlkörper.*

Für einen Beweis siehe [50], Kapitel III 9 und V 3.

Bemerkung 4.5.

1. Genauer ist der Endomorphismenring $End(E)$ als Ring isomorph zu einer Ordnung in einem imaginär quadratischen Zahlkörper. Aber wir werden diese im folgenden immer miteinander identifizieren und schreiben $End(E) = \mathcal{O}$.

2. Falls eine elliptische Kurve E über einem algebraisch abgeschlossenen Körper K als Endomorphismenring eine imaginär quadratische Ordnung hat, dann sagen wir, E hat komplexe Multiplikation **mit** $\mathcal{O}$.

3. Die Ordnungen eines imaginär quadratischen Zahlkörpers K lassen sich einfach beschreiben. Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen in K. Dieser ist für $\mathbb{Q}(\sqrt{d})$ mit $d < 0$ gegeben durch

$$\begin{aligned} \mathbb{Z} + (\frac{1+\sqrt{d}}{2})\mathbb{Z} \text{ für } d &\equiv 1 \bmod 4 \text{ und} \\ \mathbb{Z} + \sqrt{d}\mathbb{Z} \text{ für } d &\equiv 2,3 \bmod 4. \end{aligned}$$

   Dann ist für jede natürliche Zahl $f > 1$ der Ring $\mathbb{Z} + f\mathcal{O}_K$ eine Ordnung in K, und dies sind alle möglichen Ordnungen. Die natürliche Zahl f heißt der Führer der Ordnung $\mathcal{O}$ in $\mathcal{O}_K$.

4. Supersinguläre Kurven haben als Endomorphismenring eine maximale Ordnung in einer Quaternionenalgebra. Eine Ordnung ist maximal, wenn sie nicht in einer anderen Ordnung echt enthalten ist. Die maximalen Ordnungen in imaginär quadratischen Zahlkörpern sind gerade die Hauptordnungen. Für gewöhnliche Kurven muß die Ordnung nicht maximal sein. Die Kurve

$$E : y^2 = 4x^3 - 15x - 11 \text{ über } \mathbb{F}_{37},$$

auf die wir später noch ausführlicher eingehen, hat zum Beispiel komplexe Multiplikation mit $\mathbb{Z}[\sqrt{-3}]$. Die Hauptordnung in $\mathbb{Q}(\sqrt{-3})$ ist durch $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ gegeben. Der Endomorphismenring von $E(\overline{\mathbb{F}}_{37})$ ist ein echter Unterring der Hauptordnung.

Zwischen der Punkteanzahl einer elliptischen Kurve und der imaginär quadratischen Zahl, die dem Frobeniusendomorphismus entspricht, besteht ein direkter Zusammenhang. Dieser ermöglicht es insbesondere, bei gegebener Punktezahl $End(E) \otimes \mathbb{Q}$ zu ermitteln.

Satz 4.6. *Sei E eine gewöhnliche Kurve über $\mathbb{F}_q$ mit $EndE(\overline{\mathbb{F}_q}) = \mathcal{O}$ mit einer imaginär quadratischen Ordnung $\mathcal{O}$ und sei α die imaginär quadratische Zahl, die dem Endomorphismus π_q entspricht.*
Setze $t = q + 1 - \#E(\mathbb{F}_q)$. Dann gilt $t = 2Re(\alpha)$ und $\mid t \mid \leq 2\sqrt{q}$. Außerdem erfüllt der Frobeniusendormorphismus in $End(E)$ die quadratische Gleichung

$$x^2 - tx + q = 0. \tag{4.2}$$

Der Endomorphismenring ist dann eine Ordnung in $\mathbb{Q}(\sqrt{t^2 - 4q})$.

Beweis. Wir greifen bei diesem Beweis auf den Begriff der Separabilität eines Endomorphismus und die Eigenschaften separabler Endomorphismen auf Seite 109 zurück.
Der Frobeniusendomorphismus π_q wirkt genau auf den Punkten in $E(\mathbb{F}_q)$ wie die Identität. Daraus ergibt sich $Kern(\pi_q - id) = E(\mathbb{F}_q)$. Die Abbildung $\pi_q - id$ ist separabel, somit gilt $Kern(\pi_q - id) = Grad(\pi_q - id) = Norm(\alpha - 1)$. Nun erhalten wir

$$\begin{aligned} Norm(\alpha - 1) &= (\alpha - 1)(\overline{\alpha} - 1) \\ &= Norm(\alpha) - (\alpha + \overline{\alpha}) + 1 \\ &= Norm(\alpha) - 2Re(\alpha) + 1. \end{aligned}$$

Aus $Norm(\alpha) = Grad(\pi_q) = q$ ergibt sich nun $2Re(\alpha) = t$.
Nun gilt

$$q = Norm(\alpha) = Re(\alpha)^2 + Im(\alpha)^2 \geq Re(\alpha)^2 = 4t^2.$$

Daraus ergibt sich $|t| \leq 2\sqrt{q}$.
Die Abbildung π_q steht für die imaginär quadratische Zahl α. Diese ist Lösung eines Polynoms $p(x)$ zweiten Grades. Das Polynom zerfällt in Linearfaktoren

$$p(x) = (x - \alpha)(x - \overline{\alpha}).$$

Daraus ergibt sich $p(x) = x^2 - tx + q$.
Wenn wir die Gleichung 4.2 nun auflösen, ergibt sich als Diskriminante $t^2 - 4q$, also ist $\mathcal{O}$ eine Ordnung in $\mathbb{Q}(\sqrt{t^2 - 4q})$. □

Die Gleichung 4.2 wird später zu einem effizienteren Algorithmus zur Skalarmultiplikation $r \mapsto rP$ auf elliptischen Kurven, die über kleinem Grundkörper definiert sind, führen (siehe Abschnitt 6.3).
Für Primkörper erhalten wir aus Satz 4.6 eine einfachere Definition für Supersingularität.

Korollar 4.7. *Eine über einem Primkörper $\mathbb{F}_p$ definierte Kurve E ist genau dann supersingulär, falls $\#E(\mathbb{F}_p) = p + 1$.*

Beweis. Nach Definition 1.3 ist $E(\mathbb{F}_p)$ supersingulär, falls

$$p + 1 - \#E(\mathbb{F}_p) = t \equiv 0 \mod p$$

ist. Nun gilt aber nach Satz 4.6, daß $|t| \leq 2\sqrt{p}$. Also folgt $t = 0$ und $\#E(\mathbb{F}_p) = p + 1$. □

Mit den bisher eingeführten Begriffen, Satz 4.4 und Satz 4.6 können wir nun Satz 3.18 aus dem vorherigen Kapitel beweisen.
Zu jedem Faktor $g(x)$ des Polynoms $x^k - 1$ existiert ein Teiler der Gruppenordnung von $E(\mathbb{F}_{q^k})$, der diesem entspricht.

Beweis. Sei $\mathcal{O}_\mathcal{K}$ der Ring der ganzen Zahlen in $\mathbb{Z}[\pi] \otimes \mathbb{Q}$. Es gilt $g(\pi_q) \in \mathcal{O}_\mathcal{K}$ für alle Polyome $g(x)$ in $\mathbb{Z}[x]$. Angenommen $g(x) \mid x^k - 1$ in $\mathbb{Z}[x]$. Dann gilt auch $g(\pi_q) \mid \pi_q^k - 1$ in $\mathcal{O}_K$. Daraus ergibt sich mit Satz 4.6

$$g(\pi_q)g(\overline{\pi_q}) \mid (\pi_q^k - 1)(\overline{\pi_q^k - 1}) = \#E(\mathbb{F}_{q^k}).$$

Nun gilt $g(\pi_q)g(\overline{\pi_q}) \in \mathbb{R}$, da $g(\pi_q)g(\overline{\pi_q}) = \overline{g(\pi_q)g(\overline{\pi_q})}$, und sogar $g(\pi_q)g(\overline{\pi_q}) \in \mathbb{Z}$, da $g(\pi_q) \in \mathcal{O} \cap \mathbb{R}$. □

4.2 Der Ring $End_{\mathbb{F}_q}(E)$

Der Ring $End(E)$ besteht aus allen verschiedenen Endomorphismen über dem algebraischen Abschluß des Körpers $\mathbb{F}_q$ über dem die Kurve definiert ist. Wir interessieren uns nun für Endomorphismen der Punktegruppe $E(\mathbb{F}_q)$. Verschiedene Endomorphismen in $End(E)$ können die gleiche Abbildung auf den über $\mathbb{F}_q$ rationalen Punkten induzieren. Darauf gehen wir in diesem Abschnitt näher ein.
Wir benötigen den Begriff der Separabilität und Aussagen, die mit ihm zusammenhängen. Dafür verweisen wir auf Anhang B.

Satz 4.8. *Sei E eine gewöhnliche elliptische Kurve über $\mathbb{F}_q$ und $\phi \in End_{\overline{\mathbb{F}_q}}(E)$. Dann gilt $\phi(E(\mathbb{F}_{q^k})) \subset E(\mathbb{F}_{q^k})$.*

Beweis. Der Endomorphismenring ist eine Ordnung in einem imaginär quadratischen Zahlkörper, also insbesondere ein kommutativer Ring. Sei π_{q^k} der Frobeniusendomorphismus, ϕ ein beliebiger Endomorphismus und $P \in E(\mathbb{F}_{q^k})$. Dann gilt

$$\pi_{q^k}(\phi(P)) = \phi \circ \pi_q^k(P) = \phi(P).$$

Also läßt der Frobeniusendomorphismus π_{q^k} den Punkt $\phi(P)$ fest. Demnach muß $\phi(P)$ in der Punktegruppe $E(\mathbb{F}_{q^k})$ liegen. □

Nach dem vorhergehenden Satz induziert jeder Endomorphismus $\phi \in End(E)$ einer über $\mathbb{F}_q$ definierten Kurve E einen Endomorphismus $\hat{\phi}_k$ der Gruppen $E(\mathbb{F}_{q^k})$. Wir setzen

$$\begin{aligned} End_{\mathbb{F}_{q^k}}(E) &= End(E(\mathbb{F}_{q^k})) \\ &= \{\phi : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k}) \,\big|\, \exists \tilde{\phi} \in End(E), \tilde{\phi}|_{E(\mathbb{F}_{q^k})} = \phi\}. \end{aligned}$$

Jeder Endomorphismus in $End_{\mathbb{F}_{q^k}}$ ist insbesondere ein Endomorphismus der Gruppe $\mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}$, die zu $E(\mathbb{F}_{q^k})$ isomorph ist. Die Umkehrung gilt jedoch nicht, da Endomorphismen elliptischer Kurven zusätzlich rationale Abbildungen sind. Sie ist genau dann zulässig, wenn $E(\mathbb{F}_{q^k})$ zyklisch ist.
Als nächstes möchten wir untersuchen, wann zwei Endomorphismen in $EndE(\mathbb{F}_q)$ identisch sind.
Seien ϕ und ψ zwei Endomorphismen aus $End(E)$, dann gilt offensichtlich $\phi \equiv \psi$ auf $E(\mathbb{F}_q)$, falls $\phi - \psi \equiv 0$ auf $E(\mathbb{F}_q)$. Deshalb genügt es, wenn wir uns auf die Untersuchung der Abbildungen in $End(E)$ beschränken, die auf $E(\mathbb{F}_q)$ identisch Null sind. Wir kennen bereits einen solchen nicht-trivialen Endomorphismus, nämlich $\pi_q - 1$, wobei π_q der Frobeniusendomorhismus ist. In der Tat sind durch den Frobeniusendomorphismus alle solchen Endomorphismen bestimmt.

Satz 4.9. *Sei E über $\mathbb{F}_q$ definiert. Das Ideal $I = \{\psi \in \mathcal{O} \,|\, \psi(E(\mathbb{F}_q)) = 0\}$ wird von $\pi_q - 1$ erzeugt.*

Beweis. Sei $\psi \in I$, d.h. $\psi \in End(E)$ und $\psi(E(\mathbb{F}_q)) = 0$. Dann gilt $Kern\psi \supset E(\mathbb{F}_q)$, und da $\pi_q - 1$ nach Bemerkung B.3 separabel ist, gilt nach Satz B.4 $\psi = \lambda \circ (\pi_q - 1)$ für ein λ in $End(E)$. Daraus ergibt sich die Behauptung. □

Es folgt

Satz 4.10.

$$End E(\mathbb{F}_{q^k}) \simeq End E/(\pi_{q^k} - 1).$$

Für den Rest des Abschnittes liefern wir nun einen Beweis, daß

$$End E/(\pi_q - 1) \simeq E(\mathbb{F}_q)$$

als Gruppen. Dazu benötigen wir zunächst ein Lemma.

Lemma 4.11. *Sei* $M = \mathbb{Z}^2$ *und* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *in* $Gl_2(\mathbb{Z})$. *Dann ist* AM *eine Untermodul von* M *und*

$$|M/AM| = |\det A|.$$

Beweis. Wir beschreiben M durch seine $\mathbb{Z}$-Basis $[e_1, e_2]$. Dann ist AM durch $[ae_1 + be_2, ce_1 + de_2]$ gegeben. Wir bezeichnen mit A' die Matrix $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Es gilt $AA' = A'A = \det(A)E_2$.
Wir haben

$$\begin{aligned} d(ae_1 + be_2) - b(ce_1 + de_2) &= (ad - bc)e_1 \\ \text{und } -c(ae_1 + be_2) + a(ce_1 + de_2) &= (ad - bc)e_2, \end{aligned}$$

also lassen sich die Erzeugenden von $(\det A)M$ als Linearkombination der Erzeugenden von AM darstellen. Es gilt $(\det A)M \subset AM$.
Wenn wir nun die Faktorgruppe bilden, ergibt sich

$$AM/(\det A)M = AM/(AA')M \simeq M/A'M.$$

Beachte, daß

$$M/(\det A)M \big/ AM/(\det A)M \simeq M/AM \tag{4.3}$$

nach dem zweiten Isomorphiesatz und betrachte die exakte Sequenz

$$0 \to AM/\det(A)M \xrightarrow{i} M/det(A)M \xrightarrow{p} M/AM \to 0. \tag{4.4}$$

Es gilt $|M/(\det A)M| = (detA)^2$. Damit ergibt sich auch, daß M/AM und $AM/(\det A)M$ endlich sind.
Aus den Gleichungen (4.4) und (4.3) folgt nun

$$\begin{aligned} |M/AM| &= |Bild(p)| = |M/(\det A)|/|Kern(p)| = |M/(\det A)|/|Bild(i)| \\ &= (\det A)^2/|AM/(\det A)M| = (\det A)^2/|M/A'M|. \end{aligned}$$

Also gilt $|M/AM||M/A'M| = (\det A)^2$.
Die Abbildung $\theta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erfüllt $\theta A \theta^{-1} = A'$ und induziert einen Isomorphismus $M/AM \to M/A'M$. Daraus schließen wir $|M/AM| = |M/A'M|$ und somit $|M/AM| = |\det A|$. □

Korollar 4.12. *Sei $\mathcal{O} = [1, \tau]$ eine Ordnung in einem imaginär quadratischen Zahlkörper und $\alpha \in \mathcal{O}$. Dann gilt $\mathcal{O}/\alpha\mathcal{O} = N(\alpha)$.*

Beweis. Sei $\alpha = a + b\tau$ und $\alpha\tau = c + d\tau$ mit ganzen Zahlen a, b, c, d. Da $\tau \notin \mathbb{Z}$, haben wir außerdem $ad - bc \neq 0$.
Dann gilt $\alpha\mathcal{O} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\mathcal{O}$. Aus dem vorherigen Lemma folgt dann $|\mathcal{O}/\alpha\mathcal{O}| = |ad - bc|$.
Sei nun f der Führer von $\mathcal{O}$. Wir unterscheiden nun die zwei Fälle, daß τ von der Form $f\sqrt{d}$ oder von der Form $f(\frac{1+\sqrt{d}}{2})$ ist. Dann läßt sich nachrechnen, daß $N(\alpha) = |ad - bc|$. Daraus folgt die Behauptung. □

Satz 4.13. *Sei E eine über $\mathbb{F}_q$ definierte, gewöhnliche elliptische Kurve.*
Es gilt $\#E(\mathbb{F}_q) = |EndE(\mathbb{F}_q)|$.

Beweis. Sei $EndE = \mathcal{O}$ der Endomorphismenring der Kurve E. Nach dem Beweis von Satz 4.6 ist

$$\#E(\mathbb{F}_q) = Norm(\pi_q - 1).$$

Aus Korollar 4.12 ergibt sich die Gleichheit

$$Norm(\pi_q - 1) = |\mathcal{O}/(\pi_q - 1)\mathcal{O}|.$$

Nun ist $\mathcal{O}/(\pi_q - 1)\mathcal{O} \simeq EndE(\mathbb{F}_q)$. □

Korollar 4.14. *Sei E eine elliptische Kurve wie aus dem vorherigen Satz. Dann ist die Punktegruppe $E(\mathbb{F}_q)$ zu $EndE(\mathbb{F}_q)$ als Gruppe isomorph.*

Beweis. Falls $E(\mathbb{F}_q)$ zyklisch ist, dann ist die Aussage sofort klar, da jedes Element aus E($\mathbb{F}_q$) ein Gruppenendomorphismus ist. Die Menge der Gruppenendomorphismen einer zyklischen Gruppe ist zur Gruppe selbst isomorph.
Angenommen $E(\mathbb{F}_q)$ ist nicht zyklisch, d.h. $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}$ mit $n_2 \mid n_1$, und $[1, \tau]$ ist eine $\mathbb{Z}$-Basis für $\mathcal{O}$. Wir behaupten nun, daß dann die Nebenklassen $1 + (\pi_q - 1)\mathcal{O}$ und $\tau + (\pi_q - 1)\mathcal{O}$ der Ring $\mathcal{O}/(\pi_q - 1)\mathcal{O}$ erzeugen.
Es muß ein Element $\alpha \in \mathcal{O}$ existieren, so daß die Nebenklasse $\alpha + (\pi_q - 1)$ keine Zahl in $\mathbb{Z}$ enthält. Denn sonst würde $|EndE(\mathbb{F}_q)| = n_1$ gelten, und dies wäre ein

Widerspruch zu Satz 4.13. Dies bedeute aber bereits, daß $\tau + (\pi_q - 1)$ keine Zahl in $\mathbb{Z}$ enthält.
Somit sind $1 + (\pi_q - 1)$ und $\tau + (\pi_q - 1)$ unabhängige Erzeugende von $\mathcal{O}/(\pi_q - 1)\mathcal{O}$. Aus $\#E(\mathbb{F}_q) = |EndE(\mathbb{F}_q)|$ folgt, daß die Ordnung von τ in $\mathcal{O}/(\pi_q - 1)\mathcal{O}$ gleich n_2 ist. □

4.3 Bestimmung des Endomorphismenringes

Falls wir eine Kurve über einem endlichen Körper $\mathbb{F}_q$ gegeben haben, stellt sich die Frage, wie wir den Endomorphismenring dieser Kurve ermitteln können. Anhand der Ordnung der Punktegruppe $E(\mathbb{F}_q)$ können wir zunächst einmal feststellen, ob die elliptische Kurve supersingulär oder gewöhnlich ist (siehe Definition 1.3). Wenn sie gewöhnlich ist, dann hat sie komplexe Multiplikation mit einer Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper K.
Falls

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

dann ist der Zahlkörper K nach Satz 4.6 durch $\mathbb{Q}(\sqrt{4q - t^2})$ gegeben. Es bleibt die Frage, welchen Führer f die Ordnung $\mathcal{O}$ bezüglich der Hauptordnung $\mathcal{O}_K$ hat. Dies ist ein nicht-triviales Problem, das wir hier nur kurz anschneiden werden.
D. Kohel [24] gibt in seiner Arbeit einen Algorithmus für dieses Problem an. Die Laufzeit hängt exponentiell von der Größe des Index $[\mathcal{O} : \mathbb{Z}[\pi]]$ ab. Wegen des Zerfällungsverhaltens von Zahlen ist dieser aber im allgemeinen klein. Damit ist dieser Algorithmus in vielen Fällen praktikabel.
Wir gehen in diesem Abschnitt nun darauf ein, wann wir den Endomorphismenring bereits aus der Gruppenstruktur einer Punktegruppe ermitteln können.
In Satz 4.14 haben wir gezeigt, daß End $E(\mathbb{F}_q)$ zu $E(\mathbb{F}_q)$ als Gruppe isomorph ist. H.W. Lenstra [30] hat noch mehr bewiesen:

Satz 4.15. *Es gilt*

$$E(\mathbb{F}_q) \simeq End(E)/(\pi_q - 1)$$

als $EndE/(\pi_q - 1)$*-Modul.*

Aus diesem Satz ergibt sich folgende wichtige Aussage:
Es gibt ein $P \in E(\mathbb{F}_q)$ mit

$$\{\alpha(P) : \quad \alpha \in EndE(\mathbb{F}_q)\} = E(\mathbb{F}_q).$$

Wir können den Isomorphismus zwischen $EndE(\mathbb{F}_q)$ und $E(\mathbb{F}_q)$ also durch

$$\alpha \to \alpha(P)$$

beschreiben.
Der Satz 4.15 genügt leider noch nicht, um bei gegebener Gruppenstruktur von $E(\mathbb{F}_q)$ auf $End(E)$ zu schließen.

Dazu ein Gegenbeispiel:

Beispiel 4.16. Sei $y^2 = x^3 + 3x$ über $\mathbb{F}_{89}$ definiert. Die Punktegruppe $E(\mathbb{F}_{89})$ hat Ordnung 106. Der Ring $\mathbb{Z}[\pi_q]$ hat Führer fünf bezüglich der Hauptordnung $\mathbb{Z}[i]$, also $\mathbb{Z}[i] \neq \mathbb{Z}[\pi_q]$.
Aber es gilt

$$\mathbb{Z}[\pi_q]/(\pi_q - 1) \simeq \mathbb{Z}_{89} \simeq \mathbb{Z}[i]/(\pi_q - 1).$$

Wir können trotzdem einige Aussagen gewinnen.

Satz 4.17. *Sei eine über $\mathbb{F}_q$ definierte elliptische Kurve E gegeben, und die Abbildung $\pi_q - 1$ in $End(E) = \mathbb{Z}[\alpha]$ werde durch $a + b\alpha$, $a, b \in \mathbb{Z}$ beschrieben. Dann gilt:*
a) Falls $ggT(a, b) = 1$, dann ist $E(\mathbb{F}_q)$ zyklisch.
b) Wenn $ggT(a, b) > 1$, dann ist $E(\mathbb{F}_q)$ nicht zyklisch oder $\mathcal{O} = ggT(a, b)\mathcal{O}_K$.

Beweis. Die Gruppe $E(\mathbb{F}_q)$ ist nach Satz 4.15 genau dann zyklisch, wenn $End(E)/(\pi_q - 1)$ zyklisch ist. Falls $End(E)/(\pi_q - 1)$ zyklisch ist, dann ist natürlich die Identität ein erzeugendes Element dieser Gruppe, und es gilt

$$\mathbb{Z} + \mathcal{O}(\pi_q - 1) = \mathcal{O}.$$

Wir führen den Beweis nur für den Fall $\alpha = \sqrt{-d}$ für ein $d \in \mathbb{N}$, für $\alpha = \frac{1+\sqrt{-d}}{2}$ läuft er analog.
Sei f der Führer von $\mathcal{O}$, d.h. $\mathcal{O} = \mathbb{Z} + \mathbb{Z}f\alpha$ mit $f \in \mathbb{N}$. Wir haben ein beliebiges Element $a' + b'\alpha$ in $\mathcal{O}$ gegeben und suchen nun $z_1, z_2, z_3 \in \mathbb{Z}$, so daß

$$z_1 + (z_2 + z_3 f\alpha)(a + b\alpha) = a' + b'\alpha. \tag{4.5}$$

Beachte, daß $b = f\tilde{b}$ und $b' = f\tilde{b}'$ für $\tilde{b}, \tilde{b}'$. Die Forderung in Gleichung 4.5 ist äquivalent zu

$$\begin{aligned} z_1 + z_2 a - z_3 f b\alpha^2 &= a' \\ \text{und } (az_3 + \tilde{b}z_2)f &= \tilde{b}'f. \end{aligned}$$

Da $\mathrm{ggT}(a, \tilde{b}) = 1$, können wir z_2, z_3 so wählen, daß $az_3 + \tilde{b}z_2 = \tilde{b}'$. Die Wahl von z_1 ergibt sich danach aus Gleichung 4.6.
b) Sei $\mathrm{ggT}(a, b) = t > 1$. Dann können wir $a + b\alpha = t(\tilde{a} + \tilde{b}\alpha)$ schreiben, und

$$\begin{aligned} \mathbb{Z} + \mathcal{O}(\pi_q - 1) &= \mathbb{Z} + t(\tilde{a} + \tilde{b}\alpha)\mathcal{O} \\ &= \mathbb{Z} + t\mathbb{Z}\alpha. \end{aligned}$$

Somit gilt entweder $\mathbb{Z} + \mathcal{O}(\pi_q - 1) \neq \mathcal{O}$, also $E(\mathbb{F}_q)$ ist nicht zyklisch, oder $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(\pi_q - 1) = \mathcal{O}$, dann gilt $\mathcal{O} = \mathbb{Z} + t\mathbb{Z}\alpha = \mathbb{Z} + t\mathcal{O}_K$. □

Aus diesem Satz können wir nun folgende Information über den Endomorphismenring gewinnen. Falls

$$\pi_q = a + b\alpha$$

mit $\mathrm{ggT}(a, b) = d > 1$ und $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}$ mit $t = \frac{d}{n_2}$, dann gilt $\mathcal{O} = \mathbb{Z} + t\mathcal{O}_K$.

4.4 Ein verallgemeinertes Logarithmusproblem

Unter dem Problem des verallgemeinerten diskreten Logarithmus verstehen wir das folgende:

> Gegeben sei eine über einem Körper $\mathbb{F}_q$ definierte elliptische Kurve und zwei Punkte aus der Punktegruppe $E(\mathbb{F}_{q^k})$. Finde ein $\alpha \in End(E)$ mit $\alpha(P) = Q$, falls ein solches existiert.

Sei (E, P, Q) eine Instanz des verallgemeinerten diskreten Logarithmusproblems. Falls ein Endomorphismus α mit $\alpha(P) = Q$ existiert, dann gibt es sogar unendlich viele weitere Lösungen. Die Menge $\alpha + (\pi_{q^k} - 1)End(E)$ bildet P auf Q ab.
Falls P die Eigenschaft hat, daß

$$\{\alpha(P) : \alpha \in End(E)\} \neq E(\mathbb{F}_{q^k}),$$

dann ist das Verschwindungsideal

$$\{\psi(P) = \mathbf{0} : \phi \in End(E)\}$$

sogar echt größer als das Ideal $(\pi_{q^k} - id)$, und es gibt noch weitere Lösungen.
In den interessanten Fällen, z.B. falls $E(\mathbb{F}_{q^k})$ zyklisch ist und P die Gruppe erzeugt, gilt

$$\{\psi(P) = \mathbf{0} : \psi \in End(E)\} = (\pi_{q^k} - id)End(E).$$

Wir nehmen deshalb für den Rest des Abschnittes an, daß $(\pi_{q^k} - id)$ das Verschwindungsideal von P ist.
Es sei nun (E, P, Q) eine Instanz des diskreten Logarithmusproblems, d.h. $rP = Q$ für ein $r \in \mathbb{Z}$. Wir zeigen, daß bereits eine beliebige Lösung α mit $\alpha(P) = Q$ ausreicht, um r zu bestimmen.

Wir nehmen an, daß der Endomorphismenring der Kurve bekannt ist. Wir beschreiben die Berechnung nun im Fall $\mathcal{O} \subseteq \mathbb{Z}[\sqrt{-d}]$ für ein d. Sie kann aber für Endomorphismenringe $\mathcal{O} \subseteq \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$, $d \equiv 3 \bmod 4$ analog durchgeführt werden.
Sei $\alpha \in End(E)$ mit $\alpha(P) = Q$.
Es gilt

$$\begin{aligned} \alpha + \beta(\pi_{q^k} - 1) &= l \text{ für ein } \beta \in \mathcal{O}, \\ \text{bzw. } \alpha_1 + \alpha_2\sqrt{-d} + (\beta_1 + \beta_2\sqrt{-d})(q_1 + q_2\sqrt{-d}) &= l \\ \text{d.h. wir wissen: } \alpha_1 + \beta_1 q_1 - d\beta_2 q_2 &\in \mathbb{Z} \\ \text{und } \alpha_2 + \beta_2 q_1 + \beta_1 q_2 &= 0. \end{aligned}$$

Aus der unteren Gleichung folgt

$$\beta_2 = -\frac{(q_2\beta_1 + \alpha_2)}{q_1},$$

und insbesondere

$$q_2\beta_1 + \alpha_2 \equiv 0 \bmod q_1. \tag{4.6}$$

Falls q_1, q_2 relativ prim sind, dann läßt sich die Gleichung 4.6 auflösen, und wir finden eine Zahl β_1. Daraus können wir nun auch β_2 berechnen, und wir erhalten $r + n \cdot (ordP)$ für ein $n \in \mathbb{Z}$.
Falls $g = ggT(q_1, q_2) > 1$, dann folgt aus Gleichung 4.6, daß g auch α_2 teilt. Dann lösen wir $\frac{q_2\beta_1+\alpha_2}{g} \equiv 0 \bmod \frac{q_1}{g}$.
Wir weisen daraufhin, daß es diskrete Logarithmen, die zu Endomorphismen kleiner Norm äquivalent sind, selten gibt. Zu jeder imaginär quadratischen Zahl in $\mathcal{O}$ mit kleiner Norm haben wir höchstens einen diskreten Logarithmus, zu dem sie äquivalent ist. Aus $l \equiv \alpha \equiv m \bmod (\pi_{q^k} - 1)$ folgt nämlich trivialerweise $l \equiv m \bmod (\pi_{q^k} - 1)$.

Beispiel 4.18. Angenommen wir haben die elliptische Kurve $E(\mathbb{F}_{5^{167}})$ gegeben, die zu $\pi_q - 1 = (-2 + i)^{167}$ gehört. Weiter wissen wir, daß $rP = Q$ für ein $r \in \mathbb{Z}$ und haben ermittelt, daß $\alpha(P) = Q$ für $\alpha = 1 + i$.
Dann gilt

$$\begin{aligned} (1 + i) + \beta((-2 + i)^{167} - 1) &\in \mathbb{Z} \\ \text{bzw. } (1 + i) + \beta(q_1 + q_2 i) &\in \mathbb{Z} \text{ für ein } \beta \in \mathbb{Z}[i]. \end{aligned}$$

Wir erhalten die beiden Gleichungen

$$\begin{aligned} 1 + \beta_1 q_1 - \beta_2 q_2 &\in \mathbb{Z} \text{ und} \\ 1 + \beta_1 q_2 + \beta_2 q_1 &= 0. \end{aligned}$$

Daraus ergibt sich

$$\beta_2 = -\frac{\beta_1 q_2 + 1}{q_1}.$$

Damit $\beta_2 \in \mathbb{Z}$ ist, verlangen wir

$$\beta_1 q_2 + 1 \equiv 0 \bmod q_1,$$
$$d.h. \quad \beta_1 \equiv \frac{-1}{q_2} \bmod q_1.$$

Es gilt

$$q_1 = 10266965685615852022513633677700318906795700017647190987477$$

und

$$q_2 = 207157514377061820073927226534205392857753942816065406703 71.$$

Somit erhalten wir

$$\beta_1 = 6841792466383518150774958797315498357913350382240097508840,$$
$$\beta_2 = -1380474781566098213763939083758959806499135995063038946733$$

und

$$r = 3562201728899148949782703079576449125776536726607109177257278063254074719657715645419823860457552298871075190304356 24.$$

4.5 Komplexe Multiplikation mit $\mathbb{Z}[i]$ und $\mathbb{Z}[\theta]$

In diesem Abschnitt betrachten wir gewöhnliche, über einem Primkörper $\mathbb{F}_p$ definierte elliptische Kurven mit besonders kleinen Endomorphismenring, $\mathbb{Z}[i]$ oder $\mathbb{Z}[\theta]$ für $\theta^3 = 1$ und $\theta \neq 1$. Die Primzahl p sei im folgenden stets von zwei und drei verschieden.
Wir zeigen, daß wir sehr effizient Kurven mit einer Punktegruppe mit günstiger Gruppenordnung erzeugen können. Unter einer günstigen Gruppenordnung verstehen wir eine Gruppenordnung, die die Bedingungen in Abschnitt 2.2 erfüllt.
Falls eine über $\mathbb{F}_p$ definierte Kurve E_1 von der Gestalt

$$y^2 = x^3 + Bx \text{ mit } B \neq 0 \text{ und } p \equiv 1 \mod 4$$

ist, dann gibt es ein $\hat{i} \in \mathbb{F}_p$ mit $\hat{i}^2 = -1$, und die Abbildung $[i] : (x, y) \mapsto (-x, \hat{i}y)$ ist ein Endomorphismus von E_1. Dieser erfüllt die Gleichung $[i]^2 = [i] \circ [i] = -id$. Somit entspricht der Endomorphismenring $[i]$ der komplexen Zahl i.
Betrachte nun die über $\mathbb{F}_p$ definierte Kurve E_2

$$E_2 : y^2 = x^3 + B \text{ mit } B \neq 0 \text{ und } p \equiv 1 \mod 3.$$

Dann gibt es ein $\hat{\theta} \in \mathbb{F}_p$ mit $\theta^3 = 1$ und $\theta \neq 1$, und die Abbildung $[\theta] : (x, y) \mapsto (\theta x, y)$ ist ein Endomorphismus von E_2. Dieser erfüllt die Gleichung $[\theta]^3 = id$. Er entspricht also der komplexe Zahl $\theta = \frac{-1+\sqrt{-3}}{2}$, die der Gleichung $\theta^3 = 1$ genügt.
Bevor wir auf den Algorithmus zur Konstruktion günstiger Kurven eingehen, machen wir noch einige Aussagen über diese Kurven. Der nächste Satz beschäftigt sich damit, wann diese Kurven gewöhnlich sind.

Satz 4.19. *a) Die Kurve $y^2 = x^3 + Bx, B \neq 0$, über $\mathbb{F}_p$ ist genau dann gewöhnlich, wenn $p \equiv 1 \mod 4$.*
b) Die Kurve $y^2 = x^3 + B, B \neq 0$ über $\mathbb{F}_p$ ist genau dann gewöhnlich, wenn $p \equiv 1 \mod 3$.

Für einen Beweis, siehe [50], Seite 143 f.
Zu gegebener Primzahl p gibt es vier bzw. sechs verschiedene Isomorphieklassen von Kurven mit komplexer Multiplikation mit $\mathbb{Z}[i]$ bzw. $\mathbb{Z}[\theta]$. Repräsentanten lassen sich leicht angeben:

Satz 4.20. *a) Falls p eine feste Primzahl mit $p \equiv 1 \mod 4$ ist, dann sind die Isomorphieklassen von Kurven über $\mathbb{F}_p$ mit komplexer Multiplikation mit $\mathbb{Z}[i]$ durch*

$$E_i : y^2 = 4x^3 - c^{i-1}x \text{ mit } i = 1, \ldots, 4$$

und c nicht vierte Potenz in $\mathbb{F}_p$, gegeben.
b) Falls p eine feste Primzahl mit $p \equiv 1 \mod 3$ ist, dann sind die Isomorphieklssen von Kurven über $\mathbb{F}_p$ mit komplexer Multiplikation mit $\mathbb{Z}[\theta]$ durch

$$E_i : y^2 = 4x^3 - c^{i-1}x \text{ mit } i = 1, \ldots, 6$$

und c nicht sechste Potenz in $\mathbb{F}_p$, gegeben.

Beweis. Wir beweisen nur die Aussage a). Der Beweis für b) verläuft analog.
In $\mathbb{F}_p$ gibt es ein c, das nicht vierte Potenz ist. Dies folgt, da $p \equiv 1 \mod 4$ und damit $x \to x^4$ in $\mathbb{F}_p$ nicht surjektiv ist.
Aus Satz 5.4 erhalten wir nun, daß die angegebenen Kurven nicht untereinander isomorph sind.
Da sie alle die gleiche j-Invariante besitzen, müssen sie also nach Satz 5.7 unterschiedliche Gruppenordnungen haben. Die Gruppenordnung wird nach Satz 4.6

durch den Realteil der imaginär quadratischen Zahl, die dem Frobeniusendomorphismus entspricht, festgelegt. Diese Zahl ist eine imaginär quadratische Zahl mit Norm p in $\mathbb{Z}[i]$. Falls $p = a^2 + b^2$, dann gibt es für den Realteil nur die vier Möglichkeiten $\pm a$ und $\pm b$, die vier unterschiedlichen Gruppenordnungen entsprechen. Demnach sind die angegebenen Kurven ein vollständiges Repräsentantensystem. □

Wir geben nun Algorithmen für die Erzeugung kryptographisch sicherer Kurven über $\mathbb{F}_p$ mit Endomorphismenring $\mathbb{Z}[i]$ oder $\mathbb{Z}[\theta]$ mit Gruppenordnung ungefähr $2M$ an.
Wir erklären den Algorithmus für die Kurven mit Endomorphismenring $\mathbb{Z}[i]$ ausführ-

Algorithmus 2 Algorithmus zur Erzeugung von Kurven mit Endomorphismenring $\mathbb{Z}[i]$

Input: keinen
Output: E über $\mathbb{F}_p$ definiert mit Endomorphismenring $\mathbb{Z}[i]$
und günstiger Gruppenordnung $\#E(\mathbb{F}_p)$

1: Wähle a, b von der Größenordnung $\sqrt{M}$ zufällig.
2: Prüfe, ob $\mathrm{ggT}(a,b) = 1$ und $a - b \equiv 1 \mod 2$. Falls nicht, gehe zurück zu Schritt 1).
3: Teste, ob $a^2 + b^2$ eine Primzahl ist.
Wenn nicht, gehe zurück zu Schritt 1).
Sonst setze $p = a^2 + b^2$.
4: Teste, ob $m_1 = p+1+2a$, $m_2 = p+1-2a$, $m_3 = p+1-2b$ oder $m_4 = p+1+2a$ die Anforderungen erfüllt, die man an die Gruppenordnung einer kryptographisch sicheren elliptischen Kurve stellt (siehe Kapitel 2).
Falls keine dieser Ordnungen m_i alle Bedingungen erfüllt, dann gehe zurück zu Schritt 1).
Sonst setze $M := m_i$ mit m_i geeignet.
5: Teste durch Wahl von zufälligen Punkten auf $E_i(\mathbb{F}_p)$ und Bestimmung deren Ordnung, für welche der vier Kurven E_i aus Satz 4.20 $\#E_i(\mathbb{F}_p) = M$ gilt.

lich und geben dafür den Algorithmus für $\mathbb{Z}[\theta]$ kommentarlos an. Er verläuft nach dem gleichen Prinzip.
Wir wählen nicht zuerst die Primzahl p, sondern a und b, so daß $p = a^2 + b^2$. Dies hat den Vorteil, daß wir dann die Zerlegung von p in $\mathbb{Z}[i]$ bereits kennen. Es gibt dann nämlich genau vier mögliche Zerlegungen von p in $\mathbb{Z}[i]$. Dies sind

$$\begin{gathered}(a+bi)(a-bi)\\(-a+bi)(-a-bi)\\(b+ai)(b-ai)\\\text{und } (-b+ai)(-b-ai).\end{gathered}$$

Somit entspricht der Frobeniusendomorphismus der elliptischen Kurve entweder $(a+bi)$, $(-a+bi)$, $(b+ai)$ oder $(-b+ai)$. Jeder dieser vier Zahlen liefert eine andere Gruppenordnung, die nach Satz 4.6 ermittelt werden kann. Wir erhalten die

folgende Tabelle:

Frobeniusendomorphismus	t aus Satz 4.6	Gruppenordnung m_i
$a+bi$	$2a$	$m_1 = p+1-2a$
$-a+bi$	$-2a$	$m_2 = p+1+2a$
$b+ai$	$2b$	$m_3 = p+1-2b$
$-b+ai$	$-2b$	$m_4 = p+1+2b.$

Im ersten Schritt wählen wir a und b zufällig, so daß a^2+b^2 von der Größenordnung M ist. Wir prüfen dann, ob $\mathrm{ggT}(a,b) = 1$ und $a - b \equiv 1 \mod 2$, denn falls nicht, ist a^2+b^2 auf keinen Fall prim, und wir können unsere Wahl sofort verwerfen. Im dritten Schritt wird schließlich überprüft, ob $p = a^2+b^2$ eine Primzahl ist. Wenn ja, dann werden wir nun die möglichen Punktegruppen $E(\mathbb{F}_p)$ betrachten. Denn nach Satz 4.20 haben die vier Isomorphieklassen von über $\mathbb{F}_p$ definierten Kurven mit Endomorphismenring $\mathbb{Z}[i]$ gerade Punktegruppen mit Gruppenordungen m_1, m_2, m_3 und m_4 (siehe Tabelle). Im vierten Schritt überprüfen wir, ob eine dieser Gruppenordnungen günstig ist. Wenn ja, dann testen wir, welcher der vier Repräsentanten aus Satz 4.20 diese Gruppenordnung hat. Diese Kurve läßt sich dann als Instanz für ein diskretes Logarithmusproblem verwenden.

Algorithmus 3 Algorithmus zur Erzeugung von Kurven mit Endomorphismenring $\mathbb{Z}[\theta]$

Input: keinen

Output: E über $\mathbb{F}_p$ definiert mit Endomorphismenring $\mathbb{Z}[\theta]$ und günstiger Gruppenordnung $\#E(\mathbb{F}_p)$

1: Wähle a, b von der Größenordnung $\sqrt{M}$ zufällig.

2: Teste, ob $\mathrm{ggT}(a,b) = 1$. Falls nicht, gehe zurück zu Schritt 1).

3: Teste, ob $a^2 - ab + b^2$ Primzahl ist.
Wenn nicht, gehe zurück zu Schritt 1).
Sonst setze $p = a^2 - ab + b^2$.

4: Teste, ob $m_1 = p - 2a + b + 1$, $m_2 = p + 2a - b - 1$, $m_3 = p + a + b - 1$, $m_4 = p - a - b + 1$, $m_5 = p - 2b + a + 1$ oder $m_6 = p + 2b - a - 1$ die Anforderungen erfüllt, die man an die Gruppenordnung einer kryptographisch sicheren elliptischen Kurve stellt (siehe Kapitel 2).
Falls keine dieser Ordnungen m_i alle Bedingungen erfüllt, dann gehe zurück zu Schritt 1).
Sonst setze $M := m_i$ für m_i geeignet.

5: Teste durch Wahl von zufälligen Punkten auf $E_i(\mathbb{F}_p)$ und Bestimmung deren Ordnung, für welche der sechs Kurven E_i aus Satz 4.20 $\#E_i(\mathbb{F}_p) = M$ gilt.

Kapitel 5

Koordinatenbeschreibungen von Endomorphismen

Im vierten Kapitel haben wir gesehen, daß es genügt, einen beliebigen Endomorphismus α mit $\alpha(P) = Q$ zu finden, um das diskrete Logarithmusproblem lösen zu können. Vielleicht gibt es gewisse Endomorphismen, bei denen man den Bildpunkt von P sehr einfach bestimmen kann, und so ist es möglicherweise geschickter, erst das verallgemeinerte diskrete Logarithmusproblem anzugehen.
Doch wie läßt sich Multiplikation mit einer imaginär quadratischen Zahl ausdrücken? Angenommen, wir wissen bereits, daß eine Kurve komplexe Multiplikation mit $\sqrt{-2}$ hat. Wie wird dann $\sqrt{-2}P$ beschrieben? Dies ist für sich schon eine interessante Frage, die wir in diesem Kapitel zumindest für Kurven mit einem Endomorphismenring mit kleiner Klassenzahl beantworten. Genauer suchen wir für jede $\alpha \in \mathcal{O}$, wobei $\mathcal{O} \simeq End(E)$, rationale Funktionen $f(x, y)$, $g(x, y)$, so daß

$$\alpha(x, y) = (f(x, y), g(x, y)).$$

Wir skizzieren kurz den gewählten Weg:
Für Kurven über den komplexen Zahlen gibt es bereits eine Idee für die Ermittlung der Koordinatenbeschreibung von Endomorphismen, die M.Stark [58] an einem Beispiel erläutert hat. Wir haben diesen Algorithmus ausgearbeitet und ausführlich erläutert (Abschnitt 5.3).
Falls wir nun eine Kurve über einem Primkörper gegeben haben, liften wir diese zu einer Kurve über $\mathbb{C}$ mit gleichem Endomorphismenring. Wir ermitteln dort die Koordinatenbeschreibung und reduzieren den Endomorphismus anschließend. Dies ist nach zwei Sätzen aus einer Arbeit von Deuring [9] möglich.
Für den Algorithmus zur Koordinatenbeschreibung über den komplexen Zahlen und dessen Erweiterung auf Kurven über endlichen Körpern benötigen wir viele mathe-

matische Grundlagen, die im Abschnitt 5.2 bereitsgestellt werden.
Wir sind auch auf über $\mathbb{F}_{2^n}$ definierten Kurven eingegangen.
Nach diesem Kapitel sind wir also in der Lage, Endomorphismen auf Kurven mit einem Endomorphismenring mit kleiner Klassenzahl koordinatenmäßig zu beschreiben. Dies läßt sich dazu verwenden, auch verallgemeinerte Logarithmenprobleme auf nicht-zyklischen Gruppen zu erklären. Eine weitere Anwendung geben wir in Kapitel 6 an, wenn wir die Skalarmultiplikation auf elliptischen Kurven behandeln (siehe dazu Abschnitt 6.3 und Seite 100).

5.1 Einfache Fälle

In diesem Kapitel wenden wir uns folgender Fragestellung zu:
Sei E eine gewöhnliche elliptische Kurve über $\mathbb{F}_q$ mit bekanntem Endomorphismenring $\mathcal{O}$. Sei α eine imaginär qudaratische Zahl in $\mathcal{O}$, finde rationale Funktionen $f(x,y)$ und $g(x,y)$ in $\mathbb{F}_q(x,y)$, so daß für alle Punkte $(x,y) \in E(\overline{\mathbb{F}}_q)$

$$\alpha((x,y)) \to (f(x,y), g(x,y))$$

gilt.
Für $\alpha \in \mathbb{Z}$ ergeben sich die Funktionen $f(x,y), g(x,y)$ durch wiederholte Anwendung der Additionsformeln auf der elliptischen Kurve (siehe Kapitel 1) oder durch die Divisionspolynome (siehe [27], Kapitel II und Anhang D).

In diesem Abschnitt setzen wir voraus, daß der Endomorphismenring $\mathcal{O}$ der Kurve bekannt ist. Den Endomorphismenring zu berechnen, ist ein nicht triviales Problem. Zwar gilt stets $\mathcal{O} \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{t^2 - 4q})$, aber es bleibt die Frage offen, wie groß der Führer von $\mathcal{O}$ in $\mathcal{O}_K$ ist (siehe auch 4.3).

Zunächst wenden wir uns einigen Spezialfällen zu:

1. Die Kurve E sei isomorph zu

   $$y^2 = x^3 + Bx, B \in \mathbb{F}_q \text{ mit } B \neq 0,$$

   und $q = p^n$ mit $p \equiv 1 \bmod 4$.
   Dann hat E komplexe Multiplikation mit i gegeben durch

   $$[i] : (x,y) \to (-x, \hat{i}y),$$

   wobei $\hat{i}$ eine Wurzel von -1 in $\mathbb{F}_p$ ist.

2. Die Kurve E sei isomorph zu

$$y^2 = x^3 + B \text{ mit } B \in \mathbb{F}_q \text{ und } B \neq 0,$$

und $q = p^n, p \equiv 1 \bmod 3$.

Dann hat E komplexe Multiplikation mit $\frac{1+\sqrt{-3}}{2}$ gegeben durch

$$[\theta] : (x, y) \to (\theta x, y)$$

mit $\theta^3 = 1, \theta \neq 1$.

3. Die Kurve E ist über $\mathbb{F}_q$ definiert und $\mathcal{O} = \mathbb{Z} + \pi_q\mathbb{Z}$. Dann ist $\pi = q_1 + q_2\sqrt{d}$ bzw. $\pi = q_1 + q_2(\frac{1+\sqrt{d}}{2})$ für ganze Zahlen q_1, q_2,und es gibt ein $a \in \mathbb{Z}$ mit $\pi - a = z\sqrt{d}$, bzw. $\pi - a = z\frac{1+\sqrt{d}}{2}$, mit $z \in \mathbb{Z}$. Die imaginär quadratische Zahl, die dem Frobeniusendomorphismus π_q entspricht, läßt sich leicht berechnen, wenn man die Anzahl der Punkte auf $E(\mathbb{F}_q)$ kennt (siehe Satz 4.6).
Der Frobeniusendomorphismus ist durch $(x, y) \to (x^q, y^q)$ gegeben. So können

Algorithmus 4 Algorithmus zur Berechnung des Frobeniusendomorphismus

Input: q und $\#E(\mathbb{F}_q)$

Output: Die imaginär qudaratische Zahl, die π_q entspricht, und die dazu konjugiert komplexe Zahl.

1: Berechne den imaginär quadratischen Zahlkörper K und dessen Hauptordnung $\mathcal{O}_K$. Dabei gilt

$$K = \mathbb{Q}(d) \text{ mit } d = \sqrt{t^2 - 4q}, \text{ wobei } t = q + 1 - \#E(\mathbb{F}_q).$$

2: Finde Lösungen $\pi \in \mathcal{O}_K$ mit $\pi\overline{\pi} = q$ und $\pi + \overline{\pi} = t$. Dabei erhält man genau zwei imaginär quadratische Zahlen, nämlich π_q und $\overline{\pi_q}$.

wir auch in diesem Fall jede imaginär quadratische Zahl aus dem Endomorphismenring durch Koordinaten beschreiben.

4. Falls zwischen zwei Kurven $E, \tilde{E}$ uber $\mathbb{F}_q$ eine Isomorphie $f : E \to \tilde{E}$ uber $\mathbb{F}_q$ im Sinne der Definition 5.1 existiert, dann ist diese durch eine einfache Koordinatentransformation gegeben, die wir leicht berechnen können.
Der Isomorphismus induziert einen Isomorphismus der Endomorphismenringe der beiden Kurven. Falls die koordinatenmäßige Beschreibung von $\alpha \in End(E)$ bekannt ist, dann erhalten wir $\tilde{\alpha} \in End(\tilde{E})$ durch die Gleichung

$$\tilde{\alpha} = f \circ \alpha \circ f^{-1}.$$

Deshalb genügt es, wenn wir uns bei der Untersuchung der Beschreibung von Endomorphismen auf Isomorphieklassen elliptischer Kurven beschränken.

Wenn eine Kurve nicht komplexe Multiplikation mit i oder θ hat oder der Frobeniusendomorphismus bereits die Ordnung erzeugt, muß für die Bestimmung der Koordinatenbeschreibung ihrer Endomorphismen mehr Aufwand getrieben werden. Damit werden wir uns in den nächsten Abschnitten beschäftigen.

5.2 Theoretische Grundlagen

5.2.1 Die j-Invariante

Die j-Invariante ist eine sehr wichtige Größe, die insbesondere auch Information über den Endomorphismenring der Kurve enthält. Außerdem haben isomorphe Kurven die gleiche j-Invariante. In Abschnitt 5.4 werden wir Kurven zu gegebener j-Invariante benötigen.
Wir erinnern noch einmal an die Definition 1.4 aus Kapitel 1.

Definition 5.1. *Zwei Kurven heißen über einem Körper $\mathbb{K}$* ***isomorph****, falls zwischen ihnen eine über $\mathbb{K}$ definierte Isogenie existiert.*

Es gilt der folgende Satz:

Satz 5.2. *Zwei über einem Körper $\mathbb{K}$ definierte elliptische Kurven E_1, E_2 gegeben durch Weierstraß-Gleichungen*

$$\begin{aligned} E_1: \quad y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \text{ und} \\ E_2: \quad y^2 + \tilde{a}_1xy + \tilde{a}_3y &= x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6 \end{aligned}$$

sind isomorph über $\mathbb{K}$, falls $u, r, s, t \in \mathbb{K}$, $u \neq 0$, existieren, so daß die Variablentransformation

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{5.1}$$

die Gleichung für E_1 in die Gleichung für E_2 überführt.

Für einen Beweis siehe J. Silverman [50].

Korollar 5.3. *Zwei über einem Körper $\mathbb{K}$ definierte elliptische Kurven E_1, E_2 gegeben durch Weierstraß-Gleichung wie in Satz 5.2 sind genau dann über $\mathbb{K}$ isomorph, wenn u, r, s, t existieren, die die folgenden Gleichungen erfüllen:*

$$\begin{aligned} u\overline{a}_1 &= a_1 + 2s \\ u^2\overline{a}_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3\overline{a}_3 &= a_3 + ra_1 + 2t \\ u^4\overline{a}_4 &= a_4 + sa_3 + 2ra_2 - (t - rs)a_1 + 3r^2 - 2st \text{ und} \\ u^6\overline{a}_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{5.2}$$

Beweis. Die Gleichungen (5.2) erhalten wir, indem wir die Transformation in (5.1) in die Gleichung für E_1 einsetzen, anschließend beide Seiten der Gleichung durch u^6 dividieren und die Koeffizienten, die wir dann erhalten, mit $\overline{a}_i$ gleichsetzen. □

Falls die beiden Kurven über eine Körper der Charakteristik $\neq 2,3$ in Normalform gegeben sind, läßt sich nun leicht entscheiden, ob sie isomorph sind oder nicht.

Satz 5.4. *Zwei Kurven über einem Körper $\mathbb{K}$ der Charakteristik ungleich zwei und drei gegeben durch die Gleichung*

$$\begin{aligned} E_1 : y^2 &= 4x^3 - g_2 x - g_3 \text{ und} \\ E_2 : y^2 &= 4x^3 - g_2' x - g_3' \end{aligned}$$

sind isomorph über $\mathbb{K}$ genau dann, wenn ein $u \neq 0, u \in \mathbb{K}$ existiert mit

$$\begin{aligned} u^4 g_2' &= g_2 \\ u^6 g_3' &= g_3. \end{aligned}$$

Dann wird die Isomorphie $\phi : E(\mathbb{K}) \to E'(\mathbb{K})$ durch

$$\phi(x,y) \to (\frac{1}{u^2}x, \frac{1}{u^3}y)$$

beschrieben.

Beweis. Wir verwenden Korollar 5.3. Da $a_1 = a_2 = a_3 = \overline{a}_1 = \overline{a_2} = \overline{a_3} = 0$, folgt aus den ersten drei Gleichungen in (5.2), daß $r = s = t = 0$. Dann erhalten wir aus Gleichung vier und fünf, daß E_1 und E_2 genau dann isomorph sind, falls ein u existiert mit $u^4\overline{a}_4 = a_4$ und $u^6\overline{a_6} = a_6$. Das ist die Behauptung. □

Auch für gewöhnliche, über $\mathbb{F}_{2^n}$ definierte elliptische Kurven können wir eine Aussage machen. Die Spur $Spur_{\mathbb{F}_{2^n}/\mathbb{F}_2}$ eines Körperelements $a \in \mathbb{F}_{2^n}$ ist durch $\sum_{i=0}^{n-1} a^{2^i}$ gegeben.

Satz 5.5. *Zwei gewöhnliche Kurven E_1, E_2 in der Form*

$$\begin{aligned} E_1 : \quad y^2 + xy &= x^3 + a_2 x^2 + a_6 \text{ mit } \quad a_i \in \mathbb{F}_{2^n} \text{ und} \\ E_2 : \quad y^2 + xy &= x^3 + \overline{a_2} x^2 + \overline{a_6} \text{ mit } \overline{a}_i \in \mathbb{F}_{2^n} \end{aligned}$$

sind genau dann isomorph, wenn

$$a_6 = \overline{a}_6 \text{ und } Spur_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a_2) = Spur_{\mathbb{F}_2^n/\mathbb{F}_2}(\overline{a}_2).$$

Beweis. Da die Charakteristik des Körpers hier zwei ist, vereinfachen sich zunächst die Gleichungen in (5.2) zu

$$\begin{aligned} u\overline{a}_1 &= a_1 \\ u^2\overline{a}_2 &= a_2 + sa_1 + r + s^2 \\ u^3\overline{a}_3 &= a_3 + ra_1 \\ u^4\overline{a}_4 &= a_4 + sa_3 + (t + rs)a_1 + r^2 \text{ und} \\ u^6\overline{a}_6 &= a_6 + ra_4 + r^2a_2 + r^3 + ta_3 + t^2 + rta_1. \end{aligned}$$

Da $a_1 = \overline{a_1}$ folgt aus der ersten Gleichung $u = 1$. Aus der dritten Gleichung ergibt sich $r = 0$ und aus der vierten $t = 0$. Damit bleiben die Gleichungen zwei und fünf in der Form

$$\begin{aligned} \overline{a}_2 &= a_2 + s + s^2 \text{ und} \\ \overline{a}_6 &= a_6 \end{aligned}$$

übrig. Nach der ersten Gleichung muß also ein $s \in \mathbb{F}_{2^n}$ existieren, so daß $(a_2 + \overline{a_2}) = s + s^2$ ist. Dies ist aber äquivalent zu $Spur(a_2 + \overline{a_2}) = 0$ (siehe z.B. [33], Theorem 2.25, Seite 53). Da dies gleichbedeutend mit $Spur(a_2) = Spur(\overline{a_2})$ ist, ergibt sich die Behauptung. □

Eine wichtige Größe elliptischer Kurven ist die j-Invariante, die sich aus den Koeffizienten der Kurve berechnet.
Für eine elliptische Kurve E über einem Körper der Charakteristik $\neq 2, 3$ beschrieben durch die Gleichung

$$y^2 = 4x^3 + ax + b$$

ist sie durch

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

gegeben, und für gewöhnliche Kurven über Charakteristik 2 der Form

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

erhält man [1]

$$j(E) = 1/a_6.$$

Für eine Beschreibung der j-Invarianten für eine allgemeine elliptische Kurve gegeben durch eine Weierstraß-Gleichung siehe [50].
Die j-Invariante trägt ihren Namen nicht unverdient:

[1] Beachte, daß stets $a_6 \neq 0$.

Satz 5.6. *a) Zwei isomorphe Kurven haben die gleiche j-Invariante.*
b) Zwei Kurven mit gleicher j-Invariante sind isomorph über dem algebraischen Abschluß von $\mathbb{K}$.

Den Beweis dieser Aussagen findet man in [50], Kapitel III, Proposition 1.4. Aus Teil *b*) folgt insbesondere, daß zwei Kurven über $\mathbb{C}$ oder $\overline{\mathbb{F}_q}$ genau dann isomorph sind, falls ihre j-Invarianten übereinstimmen. Für endliche Körper $\mathbb{F}_q$ ist dies aber noch nicht ausreichend. Hier stellen wir noch eine zusätzliche Bedingung.

Satz 5.7. *Seien E und E' zwei gewöhnliche elliptische Kurven über $\mathbb{F}_q$. Dann gilt E und E' sind genau dann isomorph über $\mathbb{F}_{q^k}$, wenn $j(E) = j(E')$ und $|E(\mathbb{F}_{q^k})| = |E(\mathbb{F}_{q^k})|$.*

Für einen Beweis siehe das Buch von D.A. Cox [8].

5.2.2 Komplexe Multiplikation elliptischer Kurven über $\mathbb{C}$

In diesem Abschnitt werden wir sehr komprimiert einige notwendige Definitionen und tiefliegendere Sätze anführen, die für die weitere Arbeit benötigt werden. Eine ausführliche Darstellung der Theorie der komplexen Multiplikation auf elliptischen Kurven findet man in den Büchern von D.A. Cox [8] oder S. Lang [26].
Außerdem benötigen wir noch einige Begriffe über das Zerfällungsverhalten von Primidealen in Körpererweiterungen aus der algebraischen Zahlentheorie. Diese sind in den Anhang A aufgenommen.

Zunächst gehen wir noch etwas genauer auf Ordnungen ein.
Sei $\mathcal{O}$ eine Ordnung in einem imaginär quadratischen Zahlkörper K. Ein **gebrochenes $\mathcal{O}$-Ideal** ist eine Teilmenge von K von der Form $\alpha\mathcal{A}$ mit α aus dem Quotientenkörper K von $\mathcal{O}$ und $\mathcal{A}$ ein $\mathcal{O}$-Ideal. Ein Ideal (gebrochenes Ideal) heißt **echtes $\mathcal{O}$-Ideal** (**echtes gebrochenes $\mathcal{O}$-Ideal**), falls $\mathcal{O} = \{\beta \in K : \beta\mathcal{A} \subset \mathcal{A}\}$. Jedes Hauptideal von $\mathcal{O}$ ist echt.
Sei $I(\mathcal{O})$ die Menge aller echten gebrochenen $\mathcal{O}$-Ideale und $P(\mathcal{O})$ die Menge der Hauptideale in $\mathcal{O}$. Dann ist

$$\mathcal{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

die **Idealklassengruppe der Ordnung** $\mathcal{O}$. Die Ordnung des Idealklassengruppe wird mit $\mathbf{h}(\mathcal{O})$ bezeichnet und heißt die **Klassenzahl von** $\mathcal{O}$. Sie ist stets endlich.
Nun wenden wir uns elliptischen Kurven über den komplexen Zahlen zu.
Über $\mathbb{C}$ gibt es für jede elliptische Kurve E ein Gitter L, so daß

$$\mathbb{C}/L \simeq E(\mathbb{C}). \tag{5.3}$$

Dieser Isomorphismus läßt sich explizit angeben, auf seine Beschreibung gehen wir weiter unten noch ein. Statt elliptische Kurven über den komplexen Zahlen zu betrachten, ist es meist einfacher, die Faktorgruppe $\mathbb{C}/L$ zu untersuchen.
Zwei Gitter heißen **homothetisch**, falls ein $c \in \mathbb{C}$ mit $L' = cL$ existiert. Aus zwei homothetischen Gittern L und L' erhält man isomorphe Kurven.
Falls $E(\mathbb{C})$ komplexe Multiplikation mit einer Ordnung $\mathcal{O}$ hat, so gilt $\alpha L \subset L$ für alle $\mathcal{O}$. Man sagt dann, daß das Gitter L **komplexe Multiplikation mit** $\mathcal{O}$ hat. Deshalb wird der Endomorphismenring $\mathcal{O}$ einer elliptischen Kurve auch mit Multiplikatorenring bezeichnet.
Jedes echt gebrochene $\mathcal{O}$-Ideal entspricht einem Gitter. Falls das Gitter L komplexe Multiplikation mit $\mathcal{O}$ hat, ist L zu dem Gitter L' eines echt gebrochenen $\mathcal{O}$-Ideals homothetisch. Es gilt der folgende Satz:

Satz 5.8. *Zwischen der Idealklassengruppe $C(\mathcal{O})$ und den Homothetieklassen von Gittern mit $\mathcal{O}$ als vollen Multiplikatorenring besteht eine 1:1 Korrespondenz.*

Die für $\mathbb{C}/L$ interessanten Funktionen sind meromorphe doppel-periodische Funktionen. Eine entscheidende Rolle spielt hierbei die Weierstraß'sche $\wp$-Funktion.

Definition 5.9. *Sei L ein Gitter. Dann ist die* ***Weierstraß'sche $\wp$-Funktion*** *durch*

$$\wp(z;L) = \frac{1}{z^2} + \sum_{w \in L - \{0\}} \frac{1}{(z-w)^2} - \frac{1}{w^2} \text{ für } z \in \mathbb{C}$$

gegeben.

Falls klar ist, um welches Gitter L es sich handelt, schreibt man auch $\wp(z)$ statt $\wp(z;L)$.
Es gilt

$$\wp'(z) = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L) \text{ für } z \in \mathbb{C} \setminus L$$

mit von L abhängigen Konstanten $g_2(L), g_3(L)$. Wir erhalten somit eine Parametrisierung der elliptischen Kurve

$$y^2 = 4x^3 - g_2 x - g_3, \text{ mit } \Delta = g_2^3 - 27g_3^2 \neq 0$$

durch $x = \wp(z)$ und $y = \wp'(z)$. Damit gibt es auch zu jedem Gitter eine entsprechende elliptische Kurve über $\mathbb{C}$. Die Weierstraß'sche $\wp$-Funktion liefert auch den Isomorphismus aus Gleichung 5.3. Wir bilden hier $z \in \mathbb{C}/L$ auf $(\wp(z), \wp'(z)) \in E(\mathbb{C})$ ab.
Die j-**Invariante eines Gitters** ist durch

$$j(L) = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}$$

definiert. sie stimmt also mit der j-Invariante der zugehörigen Kurve überein.
Analog definieren wir die j-**Invariante eines echten gebrochenen $\mathcal{O}$-Ideals**. Das gebrochene $\mathcal{O}$-Ideal $\mathcal{A}$ läßt sich durch ein Gitter $L_{\mathcal{A}} = \alpha\mathbb{Z} + \beta\mathbb{Z}$ beschreiben, und wir setzen

$$j(\mathcal{A}) = j(L_{\mathcal{A}}).$$

Zu jeder Ordnung $\mathcal{O}$ gibt es somit $h(\mathcal{O})$ verschiedene j-Invarianten. Es läßt sich zeigen, daß alle j-Invarianten ganze algebraische Zahlen sind. Sei $\mathcal{A}$ ein echtes gebroches $\mathcal{O}$-Ideal und $K = \mathbb{Q}\otimes\mathcal{O}$. Dann heißt $K(j(\mathcal{A}))$ der **Ringklassenkörper der Ordnung** $\mathcal{O}$. Das Minimalpolynom von $K(j(\mathcal{A}))$ über $\mathbb{Q}$ heißt **Klassenpolynom von** $\mathcal{O}$, und es wird durch die Gleichung

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{n}(X - j(\mathcal{A}_i)),$$

gegeben, wobei $\mathcal{A}_i, i = 1, \ldots h(\mathcal{O})$ Idealklassenrepräsentanten von $\mathcal{O}$ sind.
Der Ringklassenkörper $K(j(\mathcal{A}))$ hat zwei wichtige Eigenschaften, auf die wir später noch zurückkommen:

- Er ist der Zerfällungskörper des Klassenpolynoms.
- Er ist eine Galoissche Körpererweiterung von K.
- Alle Primideale von K, die in L verzweigt sind, müssen das Ideal $f\mathcal{O}_K$ teilen (siehe Anhang A für das Zerfällungsverhalten von Primidealen).

5.3 Endomorphismen auf Kurven über $\mathbb{C}$

Wie in der Einleitung zu diesem Kapitel angekündigt, müssen wir zur Bestimmung der Koordinatenbeschreibung auf elliptischen Kurven über endlichen Körpern zunächst die Koordinatenbeschreibung von Endomorphismen auf Kurven über $\mathbb{C}$ behandeln. Dazu geben wir einen Algorithmus an.
Die Idee zu diesem Algorithmus von H.M.Stark, der sie in [58] an dem Beispiel einer Kurve mit komplexer Multiplikation mit $\mathbb{Z}[\sqrt{-2}]$ demonstriert hat.
Wir benötigen zunächst zwei Sätzen (Beweise in D.A. Cox, [8]):

Lemma 5.10. *Sei L ein Gitter, $\wp(z)$ die $\wp$-Funktion von L, $\alpha \in \mathbb{C}-\mathbb{Z}$ und $\alpha(L) \subset L$ (d.h. L habe komplexe Multiplikation mit α). Dann gilt*

$$\wp(\alpha z) = \frac{p(\wp(z))}{q(\wp(z))} \tag{5.4}$$

mit $ggT(p(x), q(x)) = 1$ *und* $Grad\ p(x) = Grad\ q(x) + 1 = [L : \alpha L] = N(\alpha)$.

Lemma 5.11. *Sei* $\alpha \neq 0$ *mit* $\alpha \in End_{\mathbb{C}}(E)$. *Dann existiert ein* $R(x) \in \mathbb{C}(x)$, *so daß für* $(x, y) \in E(\mathbb{C})$

$$\alpha(x, y) = (R(x), \frac{1}{\alpha} R'(x)y) \text{ mit } R'(x) = \frac{d}{dx} R(x)$$

gilt.

Wir werden später sehen, daß dieses Lemma in gewisser Weise auch auf Endomorphismen von gewöhnlichen Kurven über endlichen Körpern zutrifft. Beachte, daß in den Fällen eins und zwei auf Seite 45 die angegebenen Endomorphismen tatächlich diese Form haben. Für den Frobeniusendomorphismus trifft dies jedoch nicht zu.
Für die Berechnung der Koordinatenbeschreibung des Endomorphismus α benötigen wir die Koeffizienten der Reihenentwicklung von $\wp$. Doch diese lassen sich durch eine Rekursionsformel ermitteln (für einen Beweis siehe wieder D.A. Cox [8]).

Lemma 5.12. *Sei* $E(\mathbb{C})$ *durch die Gleichung* $y^2 = 4x^3 - g_2 x - g_3$ *gegeben und* $\wp(z)$ *die Weierstraß'sche* $\wp$*-Funktion zu* L *mit* $\mathbb{C}/L \simeq E(\mathbb{C})$. *Dann lassen sich die Koeffizienten* a_i *der Laurententwicklung*

$$\wp(z) = \frac{1}{z^2} + \sum_{i=1}^{\infty} a_n z^{2n}$$

durch folgende Rekursionsformel ermitteln:

$$\begin{aligned} (2n+3)(n-2)a_n &= 3 \sum_{i=1}^{n-2} a_i a_{n-1-i} \\ mit\ a_1 &= \frac{g_2}{20}, a_2 = \frac{g_3}{28}. \end{aligned}$$

Nun können wir einen Algorithmus zur Berechnung der Koordinatendarstellung von Endomorphismen von elliptischen Kurven über $\mathbb{C}$ angeben.
Sei $E(\mathbb{C})$ eine elliptische Kurve mit $End_{\mathbb{C}}(E) = \mathcal{O}$, die in Normalform

$$y^2 = x^3 - g_2 x - g_3$$

gegeben ist. Sie läßt sich durch die Weierstraßche $\wp$-Funktion parametrisieren, d.h. für alle $(x, y) \in \mathbb{C}$ existiert ein $z \in \mathbb{C}/L$ mit $(\wp(z), \wp'(z)) = (x, y)$.
Die Laurententwicklung der zu E gehörigen Weierstraßschen $\wp$-Funktion erhalten wir aus Lemma 5.12 mit beliebiger Genauigkeit. Nach Lemma 5.10 läßt sich $\wp(\alpha z)$ durch eine rationale Funktion $R(\wp(z))$ in $\wp(z)$ beschreiben. Wenn wir diese berechnet

haben, ergibt sich $\alpha(x, y)$ aus Lemma 5.11.
Der Hauptteil des Algorithmus besteht also darin, die nach Lemma 5.10 existierende rationale Funktion R zu bestimmen, die

$$\wp(\alpha z) = R(\alpha(z)) = \frac{p(\wp(z))}{q(\wp(z))}$$

erfüllt.
Dabei machen wir von der Gleichungkette

$$Grad\ p(x) = Grad\ q(x) + 1 = N(\alpha)$$

Gebrauch. Diese erlaubt es uns, $R(\wp(z))$ in der Form

$$\wp(\alpha(z))) = a\wp(z) + b + \frac{p_1(\wp(z))}{q(\wp(z))}$$

mit $Grad\ p_1 < Grad\ q$ zu schreiben.
Einsetzen von αz für z in die Laurententwicklung von $\wp(z)$ und Vergleich der Koeffizienten von z^{-2} und z^0 liefern uns dann die Werte von a und b.
Wir ermitteln nun die ersten Glieder der inversen Potenzreihe in z zu $(\wp(\alpha(z)) - a\wp(z) - b)$ und fahren anschließend mit der der Gleichung

$$(\wp(\alpha(z)) - a\wp(z) - b))^{-1} = \frac{q(\wp(z))}{p_1(\wp(z))} \tag{5.5}$$

fort.
Es gilt $Grad\ p' + c = Grad\ q$ für ein $c \in \mathbb{N}^+$. Den Wert von c entnehmen wir der Laurententwicklung auf der linken Seite von Gleichung 5.5. Falls z^{-2t} das kleinste Glied mit von Null verschiedenem Koeffizienten ist, dann gilt $c = t$ und wir setzen

$$(\wp(\alpha(z)) - a\wp(z) - b)^{-1} = e_t\wp(z)^t + e_{t-1}\wp(z)^{t-1} + \ldots + e_0 + \frac{p_2(\wp(z))}{p_1(\wp(z))}$$

mit $Grad\ p_2 < Grad\ p_1$.
Nun erhalten wir die $e_i, 0 \leq i \leq t$, wieder durch Koeffizientenvergleich. Falls

$$((\wp(\alpha(z)) - a\wp(z) - b)^{-1} - e_t\wp(z)^t - e_{t-1}\wp(z)^{t-1} - \ldots - e_0) \neq 0,$$

setzen wir die Berechung mit

$$((\wp(\alpha(z)) - a\wp(z) - b))^{-1} - e_t\wp(z)^t - e_{t-1}\wp(z)^{t-1} - \ldots - e_0)^{-1}$$

fort. Sonst sind wir fertig, und wir können unsere kettenbruchartige Gleichung nach $\wp(\alpha(z))$ auflösen.

Dieser Prozeß endet spätestens nach $Norm(\alpha)$ Schritten, da $Grad\ p(x) = Norm(\alpha)$ nach Lemma 5.10, und der Grad des Zählers der rationalen Funktion in jedem Schritt um mindestens eins reduziert wird.
Für den gesamten Algorithmus benötigen wir nur die ersten $2n$ Koeffizienten der Laurententwicklung von $\wp(z)$, wir können die Reihe $\wp$ also durch eine endliche Reihe

$$\frac{1}{z^2} + \sum_{i=1}^{2n-2} c_i z^{2i}$$

ersetzen, wobei c_i der Koeffizient von z^{2i} in der Laurententwicklung der Weierstraßschen $\wp$-Funktion ist. Alle Reihen in dem Algorithmus sind dann endlich, und sie werden mit jedem Schritt kürzer.
Zum besseren Verständnis des Algorithmus, der auf Seite 56 abgedruckt ist, siehe auch das Beispiel in Abschnitt 5.4.4.

Der Algorithmus auf Seite 56 ermittelt in den Schritten 3 bis 14 die rationale Abbildung aus Lemma 5.10, wie wir es zuvor beschrieben haben. Dabei wird eine Art Kettenbruch aufgebaut, der in den Schritten 10 bis 14 aufgelöst wird. In Schritt 15 wird schließlich Lemma 5.11 angewandt, um eine vollständige Beschreibung von α zu erhalten.
Die Schleife von Schritt 4 bis 9 wird höchstens n mal durchlaufen. Auch die Anzahl der Koeffizienten der Laurententwicklung von $\wp(z)$, die bei jedem Schritt bearbeitet werden, hängt von n ab. Somit erhält man eine polynomielle Laufzeit in n.
In der Praxis wird die Laufzeit aber auch entscheidend von der Klassenzahl $h(\mathcal{O})$ abhängen, da mit dieser die Komplexität der Darstellung von α wächst. Denn um Rundungsfehler zu vermeiden, können die auftretenden Wurzeln nicht als komplexe Zahlen sondern als Element des Zahlkörpers behandelt werden.

Sei T eine gerade Potenzreihe in z, dann bezeichne $(T)_i$ den Koeffizienten von z^{2i}. Wir bezeichnen die Norm von α mit n.

Algorithmus 5 Zur Berechnung der Koordinatendarstellung von α auf $\mathbf{E}(\mathbb{C})$

Input: $E(\mathbb{C})$, der Endomorphismenring $\mathcal{O}$ und $\alpha \in \mathcal{O}$

Output: Polynome $f(x,y)$, $g(x,y)$, so daß $\alpha((x,y)) = (f(x,y), g(x,y))$ für alle $(x,y) \in E(\mathbb{C})$

1: Berechne die Koeffizienten a_i, $i = -1, \ldots, 2n-2$ von z^{2i} der Laurententwicklung von $\wp(z)$ für $E(\mathbb{C})$.

2: Setze $a'_i = a_i \alpha^{2i}$, $i = -1, \ldots 2n-2$, d.h. die Zahlen a_i sind die ersten $2n-1$ Koeffizienten der Laurententwicklung von $\wp(\alpha z)$.

2: Setze $c_1 1 := a'_{-1}$, $c_{10} := 0$, $c_{1l} := 0$ für $2 \leq l \leq n$,
$A := \frac{1}{z^2} + \sum_{i=1}^{2n-2} a_i z^{2i}$
und $B := \frac{a'_1}{z^2} + \sum_{i=1}^{2n-2} a'_i z^{2i}$.

3: $D := B - c_{11} A - c_{10}$.

4: **while** $D \neq 0$ **do**

5: Sei l die Länge [2]der Potenzreihe D. Berechne die endliche Potenzreihe E zu D, so daß $E \cdot D$ von der Form $1 + \sum_{i=l}^{\infty} e_i z^i$ ist(Dies entspricht der Inversenbildung, die wir bei der Erklärung des Algorithmus angesprochen haben.).

6: Setze $c_{ij} = (D)_{-j}$ für alle $1 \leq j \leq n$ und $B := D$.

7: Setze $D := B - \sum_{j=0}^{n} c_i j A^j$;

8: $i := i + 1$;

9: **end while**

10: **for** $k = i$ by -1 to 2 do **do**

11: $f(x) := \sum_{j=0}^{n} c_{kj} x^j + f(x)$;

12: $f(x) := \frac{1}{f(x)}$;

13: **end for**

14: $f(x) := c_{11} x + c_{10} + f(x)$.

15: $\alpha := (f(x), \frac{1}{\alpha} f'(x) y)$.

[2]Unter der Länge l einer endlichen Potenzreihe verstehen wir $l = |k_1 - k_2|$, wobei k_1 der kleinste von Null verschiedene Koeffizient und k_2 der größte von Null verschiedene Koeffizient ist.

5.4 Endomorphismen über endlichen Körpern

Wir beschränken uns in diesem Abschnitt auf Kurven mit komplexer Multiplikation mit einer imaginär quadratischen Ordnung $\mathcal{O}$, die von $\mathbb{Z}[\theta]$ und $\mathbb{Z}[i]$ verschieden ist. Alle auftretenden j-Invarianten sind von 0 und 1728 verschieden, da dies genau die j-Invarianten sind, die zu den Ordnungen $\mathbb{Z}[\theta]$ und $\mathbb{Z}[i]$ gehören. Wir haben bereits gesehen, wie sich die beiden Endomorphismen i und θ koordinatenmäßig beschreiben lassen.
Zunächst noch ein Lemma, das wir benötigen:

Lemma 5.13. *Sei E eine Kurve über $\mathbb{F}_p$ mit $End(E) = \mathcal{O}$ mit Einheitengruppe $\mathcal{O}^* = \pm 1$ (d.h. $\mathcal{O} \neq \mathbb{Z}[\theta], \mathbb{Z}[i]$). Dann gibt es über $\mathbb{F}_p$ außer der Isomorphieklasse der Kurve E nur eine weitere Isomorphieklasse von Kurven mit gleicher j-Invariante.*

Beweis. Nach Satz 5.7 sind zwei Kurven über $\mathbb{F}_p$ genau dann isomorph, falls sie die gleiche j-Invariante besitzen und ihre Gruppenordnungen übereinstimmen. Wir zeigen, daß es für gegebenen Endomorphismenring genau zwei mögliche Gruppenordnungen für die Kurve $E(\mathbb{F}_p)$ gibt. Wir wissen aus Korollar 4.14, daß

$$E \simeq \mathcal{O}/(\pi_p - 1),$$

wobei π_p der Frobeniusendomorphismus ist. Nun gilt, daß π_p einer imaginär quadratischen Zahl α mit $Norm(\alpha) = p$ entspricht. Falls α eine imaginär quadratische Zahl mit Norm p ist, dann sind nach Satz A.2 in Anhang A genau α, $\overline{\alpha}$, $-\alpha$ und $-\overline{\alpha}$ die imaginär quadratischen Zahlen in $\mathcal{O}$ mit Norm p. Nun gilt

$$\begin{aligned} \mathcal{O}/(\pi_p - 1) &\simeq \mathcal{O}/(\overline{\pi_p} - 1), \\ \text{aber } \mathcal{O}/(\pi_p - 1) &\not\simeq \mathcal{O}/(-\overline{\pi_p} - 1), \end{aligned}$$

da diese Ringe eine unterschiedliche Anzahl von Elementen haben. Daraus ergibt sich die Behauptung. □

Zwischen Endomorphismen auf elliptischen Kurven über $\mathbb{C}$ mit komplexer Multiplikation mit einer imaginär quadratischen Ordnung $\mathcal{O}$ und elliptischen Kurven über endlichen Körpern $\mathbb{F}_q$ gibt es einen engen Zusammenhang. Diesen werden wir verwenden, um nun auch Endomorphismen auf elliptischen Kurven über endlichen Körpern koordinatenmäßig zu beschreiben.
Dazu müssen wir zunächst auf Reduktion elliptischer Kurven und eine Arbeit von M. Deuring [9] eingehen.

5.4.1 Reduktion elliptischer Kurven

Sei E eine über einem Zahlkörper K definierte elliptische Kurve, die durch eine Normalform

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in K \tag{5.6}$$

gegeben ist.
Es sei u der gemeinsame Nenner von g_2 und g_3. Dann erhalten wir durch die Transformation $x' = u^2x$ und $y' = u^3y$ eine elliptische Kurve in Normalform, die über dem Ring der ganzen Zahlen $\mathcal{O}_K$ definiert ist. Wir nehmen also o.B.d.A. an, daß die Koeffizienten g_2 und g_3 in Gleichung 5.6 in $\mathcal{O}_K$ sind. Somit gibt es zu jeder über einem Zahlkörper K definierten elliptischen Kurve eine Normalform, die über dem Ring der ganzen Zahlen $\mathcal{O}_K$ definiert ist.
Sei nun $\mathfrak{p}$ ein Primideal im Ring der ganzen Zahlen $\mathcal{O}_K$. Dann setzen wir [3]

$$\begin{aligned} [g_2] &= g_2 \mod \mathfrak{p} \\ \text{und } [g_3] &= g_3 \mod \mathfrak{p} \end{aligned}$$

und erhalten eine reduzierte Kurve $\overline{E}$

$$y^2 = 4x^3 - [g_2]x - [g_3]$$

über dem Quotientkörper des Ringes $\mathcal{O}_K/\mathfrak{p}$. Diese Kurve bezeichnen wir auch mit $E \mod \mathfrak{p}$. Falls die Diskriminate

$$\Delta = [g_2]^3 - 27[g_3]^2$$

nicht verschwindet, dann ist $\overline{E}$ (bzw. $E \mod \mathfrak{p}$) wieder eine elliptische Kurve, und wir sagen, daß E **gute Reduktion modulo** $\mathfrak{p}$ hat.
Wenn wir im folgenden von einer über einem Zahlkörper K definierten elliptischen Kurve sprechen, meinen wir stets eine über dem Ring der ganzen Zahlen $\mathcal{O}_K$ definierte elliptische Kurve.

Beispiel 5.14. Wir übertragen diese Reduktion auf einen speziellen Fall. Angenommen p ist eine Primzahl und (p) das von ihr erzeugte Primideal in $\mathbb{Z}$. Weiter sei eine Ordnung $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ in einem imaginär quadratischen Zahlkörper K gegeben, deren Führer nicht von p geteilt wird und in der das Primideal (p) in zwei Ideale $\mathfrak{p}$ und $\overline{\mathfrak{p}}$ zerfällt. Es gilt, $\mathfrak{p}$ teilt nicht das Ideal $f\mathcal{O}_K$.
Betrachten wir nun den Ringklassenkörper L der Ordnung $\mathcal{O}$. Nach den Eigenschaften des Ringklassenkörpers auf Seite 52 ist ein Primideal $\mathfrak{p}$ von $\mathcal{O}$ genau dann in

[3] Mit $g_i \mod \mathfrak{p}$ bezeichnen wir die Restklasse von g_i in $\mathcal{O}_K/\mathfrak{p}$.

L verzweigt, falls das $\mathfrak{p}$ das Ideal $f\mathcal{O}_K$ teilt. Da wir diese Situation ausgeschlossen haben, ist $\mathfrak{p}$ und damit auch (p) in $\mathcal{O}_L$ unverzweigt.
Sei nun $\mathfrak{P}$ ein Ideal in $\mathcal{O}_L$, das (p) enthält.
Dann gilt

$$O_L/\mathfrak{P} \simeq \mathbb{F}_{p^n} \text{ für } n = [\mathcal{O}_L/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}].$$

Sei E eine Kurve über $\mathbb{C}$ mit komplexer Multiplikation mit Endomorphismenring $\mathcal{O}$. Dann ist die j-Invariante j_E über L definiert. Die über L definierte Kurve

$$\tilde{E} : y^2 = 4x^3 - kx - k \text{ mit } k = \frac{27j_E}{j_E - 1728}$$

hat ebenfalls j-Invariante j_E, ist also über $\mathbb{C}$ isomorph zu E. Die Kurve $\tilde{E}$ hat gute Reduktion mod $\mathfrak{P}$, falls $j_E \neq 0, 1728$ ist, und die Kurve $\tilde{E} \mod \mathfrak{p}$ ist eine über $\mathbb{F}_{p^n}$ definierte elliptische Kurve.

Mit dieser Situation beschäftigen sich die Sätze von M. Deuring zur Reduktion elliptischer Kurven [9].

Satz 5.15. *Sei E eine über einem Zahlkörper M definierte elliptische Kurve, und der Endomorphismenring $End(E)$ sei eine Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper. Angenommen p zerfällt in K in Primideale $\mathfrak{p}$ und $\overline{\mathfrak{p}}$ und $\mathfrak{P}$ sei ein Primideal in M, das p enthält, so daß E gute Reduktion mod $\mathfrak{P}$ hat. Sei f der Führer von $\mathcal{O}$ und p teilt nicht f, dann gilt:*
Der Endomorphismenring $End(E \mod \mathfrak{P})$ ist gleich $\mathcal{O}$, und die Reduktion induziert einen Isomorphismus von $End(E)$ nach $End(E \mod \mathfrak{P})$ der durch $\alpha \to \alpha \mod \mathfrak{P}$ für $\alpha \in End(E)$ gegeben ist.

Einen Beweis findet man neben der Arbeit von M. Deuring auch in dem Buch von S.Lang ([26], Kapitel 13, Theorem 12).
Nun wissen wir, daß die elliptische Kurve $(\tilde{E} \mod \mathfrak{P})$, die wir in unserem Beispiel 5.14 erhalten haben, auch komplexe Multiplikation mit $\mathcal{O}$ hat.
Der nächste Satz sagt uns, daß jede elliptische Kurve über einem endlichen Körper auf diese Weise entsteht.

Satz 5.16. *Sei E_0 eine elliptische Kurve über $\mathbb{F}_q$ mit Endomorphismus α_0. Dann gibt es eine elliptische Kurve E definiert über einem Zahlkörper M, einen Endomorphisms α und eine nicht-entartete Reduktion von E bezüglich eines Primideals $\mathfrak{P}$, das (p) enthält, so daß $E \mod \mathfrak{P}$ isomorph zu E_0 ist und $\alpha \mod \mathfrak{P}$ geht unter dem Isomorphismus in α_0 über.*

Daraus ergibt sich das folgende Korollar

Korollar 5.17. *Zu einem endlichen Primkörper $\mathbb{F}_p$ gibt es höchstens $h(\mathcal{O})$ verschiedene j-Invarianten elliptischer Kurven über $\mathbb{F}_p$ mit Endomorphismenring $\mathcal{O}$.*

Beweis. Falls $\overline{E}$ eine über $\mathbb{F}_p$ definierte elliptische Kurve mit Endomorphismenring $\mathcal{O}$ ist, dann gibt es nach Satz 5.16 eine über einem Zahlkörper M definierte elliptische Kurve E mit $E \mod \mathfrak{P} = \overline{E}$ für ein Primideal $\mathfrak{P}$. Es gilt $j_{\overline{E}} = j_E \mod \mathfrak{P}$.
Nun ist j_E Nullstelle des Klassenpolynoms $H_{\mathcal{O}}$ (siehe 52). Also gilt $j_{\overline{E}}$ ist Nullstelle des Polynoms $H_{\mathcal{O}} \mod \mathfrak{P}$. Dieses ist über $\mathbb{Z}$ definiert. Deshalb gilt

$$H_{\mathcal{O}} \mod \mathfrak{P} = H_{\mathcal{O}} \mod (\mathfrak{P} \cap \mathbb{Z}) = H_{\mathcal{O}} \mod p.$$

Das Klassenpolynom hat Grad $h(\mathcal{O})$. Also besitzt es höchstens $h(\mathcal{O})$ verschiedene Nullstellen modulo p. Daraus folgt die Behauptung. □

Wir interessieren uns nun dafür, wie der Zahlkörper M aus Satz 5.16 mit dem Ringklassenkörper L von $\mathcal{O}$ zusammenhängt. Dabei betrachten wir zunächst nur elliptische Kurven über Primkörper $\mathbb{F}_p$.
Sei eine über $\mathbb{F}_p$ definierte Kurve mit Endomorphismenring $\mathcal{O}$ gegeben. Die zugehörige elliptische Kurve E über M aus Satz 5.16 hat komplexe Multiplikation mit $\mathcal{O}$, also ist ihre j-Invariante über dem Rinklassenkörper L definiert. Wie in unserem Beispiel können wir nun die über L definierte Kurve

$$E_1 : y^2 = 4x^3 - kx - k, \text{ mit } k = \frac{27 j_E}{j_E - 1728}$$

betrachten. Diese hat gute Reduktion modulo $\mathfrak{p}$, falls $j \neq 0, 1728 \mod \mathfrak{p}$, was wir zu Beginn des Abschnitts ausgeschlossen haben.
Das gleiche gilt auch für die über L definierte Kurve

$$E_2 : y^2 = 4x^3 - kc^2x - kc^3, \text{ mit } k = \frac{27 j_E}{j_E - 1728}$$

und $c \mod \mathfrak{P}$ ist quadratischer Nichtrest mod p.
Die Kurven $E_1 \mod \mathfrak{P}$ und $E_2 \mod \mathfrak{P}$ sind nach Satz 5.4 nicht isomorph über $\mathbb{F}_p$. Da es aber über $\mathbb{F}_p$ zu gegebener j-Invariante nur zwei Isomorphieklassen von Kurven gibt, muß unsere Ausgangskurve zu $E_1 \mod \mathfrak{P}$ oder $E_2 \mod \mathfrak{P}$ über $\mathbb{F}_p$ isomorph sein.

5.4.2 Endomorphismenringe mit Klassenzahl 1

Lemma 5.18. *Sei $K = \mathbb{Q}(\alpha)$ mit*

$$\alpha = \begin{cases} \sqrt{d} & , \text{falls } d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & , \text{falls } d \equiv 1 \mod 4, \end{cases}$$

ein imaginär quadratischer Zahlkörper und (p) ein Primideal in $\mathbb{Z}$, das im Ring der ganzen Zahlen $\mathcal{O}_K$ in K in zwei Primideale $\mathfrak{p}, \overline{\mathfrak{p}}$ zerfällt. Weiter sei f das Minimalpolynom von α.
Dann hat $f(x)$ eine Lösung x in $\mathbb{Z}/p\mathbb{Z}$. Es gilt $x \equiv \alpha \mod \mathfrak{p}$ oder $x \equiv \overline{\alpha} \mod \mathfrak{p}$.

Beweis. Wir zeigen, daß $f(x)$ genau dann irreduzibel in $\mathbb{Z}/p\mathbb{Z}[x]$ ist, wenn (p) ein Primideal in $\mathcal{O}_K$ ist. Wenn (p) in zwei Primideale zerfällt, muß also $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ reduzibel sein, also insbesondere eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzen, da $Grad\ f = 2$. Das Polynom $f(x)$ ist das Minimalpolynom von K. Es gilt also

$$K \simeq \mathbb{Q}[x]/(f(x)) \text{ und } \mathcal{O}_K/(p) \simeq \mathbb{Z}[x]/(f(x))/p \simeq (\mathbb{Z}/p\mathbb{Z})[x]/(f(x)).$$

Das Polynom $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ ist genau dann irreduzibel, wenn $(\mathbb{Z}/p\mathbb{Z})[x]/f(x) \simeq \mathcal{O}_K/(p)$ ein Körper ist. Dies trifft jedoch genau dann zu, wenn (p) ein Primideal in $\mathcal{O}_K$ ist. □

Wir wenden nun unsere Idee auf einen sehr einfachen Fall an.

Satz 5.19. *Sei E eine gewöhnliche elliptische Kurve über $\mathbb{F}_p$, die durch*

$$y^2 = 4x^3 - a_1 x - a_2, \quad a_i \in \mathbb{F}_p \tag{5.7}$$

beschrieben werde. Wähle feste Repräsentanten $\tilde{a}_i \in \mathbb{Z}$ für die Koeffizienten $a_i \in \mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Ferner gelte nun $E(\mathbb{C})$ gegeben durch $y^2 = 4y^3 - \tilde{a}_1 x - \tilde{a}_2$ habe Endomorphismenring $End_{\mathbb{C}}(E) = \mathcal{O}$ mit $h(\mathcal{O}) = 1$. Dann entsteht E aus $E(\mathbb{C})$ durch Reduktion, es gilt $End_{\overline{\mathbb{F}}_p}(E) = \mathcal{O}$, und für $\alpha \in \mathcal{O}$ läßt sich in polynomieller Zeit in der Norm von α die koordinatenmäßige Beschreibung angeben.

Beweis. Wir nehmen an, daß der Endomorphismus einer imaginär quadratischen Zahl α entspricht, deren Norm nicht durch p teilbar ist. Falls dies nicht der Fall sein sollte, bestimmen wir einfach den Endomorphismus, der $\alpha - n$ entspricht für ein geeignetes $n \in \mathbb{N}$. Zusammen mit den Formeln aus Kapitel 1 für die Multiplikation mit n erhalten wir dann durch Addition die Beschreibung von α.
Sei $K = \mathcal{O} \otimes \mathbb{Q}$. Da $h(\mathcal{O}) = 1$ ist der Ringklassenkörper von $\mathcal{O}$ durch $L = K$ gegeben. Die Primzahl p ist in $\mathcal{O}_L = \mathcal{O}_K$ zerlegt, d.h. $p = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_L$. Weiter gilt $\tilde{a}_i \mod p = a_i$, also insbesondere $\tilde{a}_i \mod \mathfrak{p} = a_i$. Somit hat $E(\mathbb{C})$ gute Reduktion modulo des Primideals $\mathfrak{p}$, und E ist die durch die Reduktion entstehende Kurve. Nach Satz 5.15 gilt dann $End_{\overline{\mathbb{F}}_p}(E) = End_{\mathbb{C}}(E) = \mathcal{O}$.
Sei nun $\alpha \in End_{\mathbb{C}}(E)$ durch $(R(x), \frac{1}{\alpha}R'(x)y)$ gegeben. Dann wird der durch die Reduktion induzierte Endomorphismus $\overline{\alpha}$ durch

$$(R(x) \mod \mathfrak{p}, \frac{1}{\alpha}R'(x)y \mod \mathfrak{p})$$

beschrieben. □

Diese Reduktion sieht in der Praxis wie folgt aus: Ersetze alle $r \in \mathbb{Q}$ durch $r \bmod p$ und $\sqrt{-n}$ bzw. $\frac{1+\sqrt{-n}}{2}$ durch das Element in $\mathbb{F}_p$, daß das Minimalpolynom von $\sqrt{-n}$ bzw. $\frac{1+\sqrt{-n}}{2}$ löst. Dieses gibt es nach Lemma 5.18. Der zeitaufwendigste Teil des Algorithmus ist die Berechnung des Endomorphismus über den komplexen Zahlen.

Etwas schwieriger gestaltet sich die Sache, wenn zwar der Endomorphismenring $\mathcal{O}$ bekannt ist und $h(\mathcal{O}) = 1$ gilt, man aber die geeigneten Repräsentanten $\tilde{a}_i$, für die die Kurve über $\mathbb{C}$ komplexe Multiplikation hat, nicht kennt. Hier müssen wir zunächst eine geeignete Kurve über $\mathbb{C}$ ermitteln.
Wir berechnen die j-Invariante $j(\mathcal{O})$ von $\mathcal{O}$. Da die Klassenzahl 1 ist, ist diese eindeutig. Dann setzen wir (falls $j(\mathcal{O}) \neq 0, 1728$)

$$\begin{aligned} k &= \frac{27j(\mathcal{O})}{j(\mathcal{O}) - 1728} \text{ und} \\ E_1 &: y^2 = 4x^3 - kx - k, \\ E_2 &: y^2 = 4x^3 - kc^2x - kc^3, \\ c \in \mathcal{O}_L - \mathfrak{p}, &\quad c \bmod \mathfrak{p} \text{ kein Quadrat in } \mathbb{F}_p. \end{aligned}$$

Die Kurve E ist entweder zu $E_1 \bmod \mathfrak{p}$ oder $E_2 \bmod \mathfrak{p}$ isomorph.

5.4.3 Endomorphismenringe mit Klassenzahl $h(\mathcal{O}) > 1$

Wieder haben wir $End_{\mathbb{F}_p}(E) = \mathcal{O}$ gegeben. Es gibt $h(\mathcal{O}) < \infty$ viele verschiedene Isomorphieklassen von Kurven über $\mathbb{C}$ mit Endomorphismenring $\mathcal{O}$.

Algorithmus 6 Zur Berechnung von Endomorphismen über $\mathbb{F}_p$

Input: E über $\mathbb{F}_p$ definiert, $End(E) = \mathcal{O}$ und ein $\alpha \in \mathcal{O}$
Output: Polynome $f(x,y)$, $g(x,y)$ in $\mathbb{F}_p[x,y]$, so daß $\alpha((x,y)) = (f(x,y), g(x,y))$ für alle $(x,y) \in E(\overline{\mathbb{F}_p})$

```
for i = 1 to h(O) do
    Berechne j_i; setze k_i = 27j_i/(j_i - 1728).
    if E isomorph zu E_1 : y^2 = 4x^3 - kx - k mod p then
        E' := E_1.
    else if E isomorph zu E_2 = 4x^3 - kx^2 - kx^3 mod p then
        E' := E_2.
    end if
end for
```

Berechne den Endomorphismus α auf E' und reduziere dann mod $\mathfrak{p}$. Eventuell ist noch ein Isomorphismus auszuführen.

Der Algorithmus ist für große Klassenzahlen nicht durchführbar.
Ein Problem besteht in der Berechnung der j_i, was im allgemeinen schwer oder sogar unmöglich ist. Im Appendix sind einige j-Invarianten angegeben.

5.4.4 Ein Beispiel

Wir betrachten die Kurve

$$y^2 = 4x^3 - 15x - 11$$

über dem Körper $\mathbb{F}_{37}$.
Diese Kurve hat komplexe Multiplikation mit $\sqrt{-3}$. Dieselbe Kurve über $\mathbb{C}$ hat j-Invariante 54000, also ebenfalls komplexe Multiplikation mit $\sqrt{-3}$. Zunächst wollen wir den Endomorphismus $\sqrt{-3}$ über den komplexen Zahlen ermitteln. Es gilt $N(\sqrt{-3}) = 3$, d.h. nach Lemma 5.10 gilt

$$\wp(\sqrt{-3}z) = \frac{p(\wp(z))}{q(\wp(z))}$$
$$\text{mit } Grad\ p = Grad\ q + 1 = 3.$$

Durch Division von $q(\wp(z))$ in $p(\wp(z))$ ergibt sich

$$\wp(\sqrt{-3}z) = a\wp(z) + b + \frac{p'(\wp(z))}{q(\wp(z))} \text{ mit } Grad\ p' < Grad\ q = 2 \text{ und } a, b \in \mathbb{C}. \quad (5.8)$$

Aus den Koeffizienten $g_2 = 15$ und $g_3 = 11$ ergibt sich die $\wp$-Funktion der Kurve

$$\wp(z) = \frac{1}{z^2} + \frac{3}{4}z^2 + \frac{11}{28}z^4 + \frac{3}{16}z^6 + \frac{9}{112}z^8 + \frac{683}{20384}z^{10} + \dots$$

und durch Substitution von z durch $\sqrt{-3}z$ erhält man

$$\wp(\sqrt{-3}z) = -\frac{1}{3z^2} - \frac{9}{4}z^2 + \frac{99}{28}z^4 - \frac{81}{16}z^6 + \frac{729}{112}z^8 - \frac{243\dot{6}83}{20384}z^{10} + \dots.$$

Wenn wir nun Gleichung 5.8 betrachten und linke und rechte Seite für $z = 0$ vergleicht, dann ergibt sich $a = -1/3$ und $b = 0$.
Weiter haben wir

$$(\wp(\sqrt{-3}z) - \frac{1}{3}\wp(z)) = -2z^2 + \frac{11}{3}z^4 - 5z^6 + \frac{183}{28}z^8 - 683z^{10} + \cdots,$$

woraus wir durch Koeffizientenvergleich

$$(\wp(\sqrt{-3}z) + \frac{1}{3}\wp(z))^{-1} = -\frac{1}{2}\frac{1}{z^2} - \frac{11}{12} - \frac{31}{72}z^2 - \frac{199}{1512}z^4 - \frac{133}{2592}z^6 + \cdots$$

erhalten. An dieser Entwicklung kann man nun ablesen, daß

$$(\wp(\sqrt{-3}z) + \frac{1}{3}\wp(z))^{-1} = \frac{q(\wp(z))}{p'(\wp(z))}$$

von der Gestalt

$$c\wp(z) + d + \frac{1}{e\wp(z) + f} \text{ mit } c, d, e, f \in \mathbb{C}$$

ist. (Hätte man hingegen für $\frac{q(\wp(z))}{p'(\wp(z))}$ eine Laurententwicklung mit nicht verschwindendem Koeffizienten für z^{-4} erhalten, könnte man daraus schließen, daß $\frac{q(\wp(z))}{p'(\wp(z))}$ sich durch $a\wp^2 + b\wp + c$ darstellen läßt.)
Nun ergibt sich $c = -\frac{1}{2}$ und $d = -\frac{11}{12}$.
Setze $t(z) = (\wp(\sqrt{-3}z) + \frac{1}{3}\wp(z))^{-1}$. Wir berechnen

$$t(z) - c\wp(z) - d = -\frac{1}{18}z^2 - \frac{109}{72}z^4 - \frac{1265}{432}z^6 + \ldots \text{und}$$
$$(t(z) - c\wp(z) - d)^{-1} = -18\frac{1}{z^2} - 21 - \frac{27}{2}z^4 + \cdots = -18\wp(z) - 21.$$

Alles zusammen ergibt nun

$$\begin{aligned}\wp(\sqrt{-3}z) &= -\frac{1}{3}\wp(z) + \frac{1}{-\frac{1}{2}\wp(z) - \frac{11}{12} + \frac{1}{-18\wp(z)-21}} \\ &= -\frac{1}{3}\frac{4x^3 + 12x^2 + 33x + 28}{4x^2 + 12x + 9}.\end{aligned}$$

Die Gleichung $x^2 + 3 = 0$ hat in $\mathbb{F}_{37}$ zwei Lösungen, nämlich 16 und 21. Diese entsprechen bei Reduktion der Kurve mod $\mathfrak{p}$ den imaginär quadratischen Zahlen $\pm\sqrt{-3}$. Damit ergibt sich zusammen mit Lemma 5.11, daß die Abbildungen $\pm\sqrt{-3}$ auf der Kurve $E(\mathbb{F}_{37})$ durch

$$\left(12\frac{4x^3 + 12x^2 + 33x + 28}{4x^2 + 12x + 9}, \frac{1}{\alpha}12\frac{8x^3 + 36x^2 + 6x + 24}{(2x+3)(4x^2 + 12x + 9)}y\right)$$

mit $\alpha = 16, 21$ beschrieben werden.

5.4.5 Der Fall Charakteristik zwei

Bisher sind wir nur auf die Bestimmung von Endomorphismen auf elliptischen Kurven, die über einem Primkörper $\mathbb{F}_p$ definiert sind, eingegangen.

In diesem Abschnitt wenden wir uns Endomorphismen elliptischer Kurven über endlichen Körpern der Charakteristik zwei zu. Die hier beschriebenen Ideen lassen sich auch auf Erweiterungskörper ungerader Charakteristik übertragen.

Sei $\overline{E}_0$ eine über $\mathbb{F}_{2^n}$ definierte elliptische Kurve, deren j-Invariante $j_{\overline{E}_0}$ in $\mathbb{F}_{2^n}$, aber nicht schon in einem Teilkörper $\mathbb{F}_{2^k}$ liegt.
Der Endomorphismenring $\mathrm{End}(\overline{E}_0)$ der Kurve sei eine Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper K, und den Ringklassenkörper der Ordnung $\mathcal{O}$ bezeichnen wir mit L.
Wir betrachten nun die über $\mathbb{F}_{2^n}$ definierte Kurve $\overline{E}$ von der Form

$$y^2 + xy = x^3 + 1/j_{\overline{E}_0}.$$

Diese Kurve hat die gleiche j-Invariante wie $\overline{E}_0$. Sie ist also zu $\overline{E}_0$ über $\overline{\mathbb{F}}_{2^n}$ isomorph und hat insbesondere den gleichen Endomorphismenring wie $\overline{E}_0$.
Nach dem Satz 5.16 existiert eine elliptische Kurve E über einem Zahlkörper M, so daß

$$\overline{E} = E \mod \mathfrak{P}$$

für ein Primideal $\mathfrak{P}$ im Ring der ganzen Zahlen $\mathcal{O}_M$ in M, das das Ideal $(2)\mathcal{O}_M$ enthält. Nun sei j_E die j-Invariante von E. Diese j-Invariante ist über dem Ringklassenkörper L von $\mathcal{O}$ definiert. Der Zahlkörper M ist also eine endliche Körpererweiterung von L.
Die j-Invariante j_E geht bei der Reduktion modulo $\mathfrak{P}$ in $j_{\overline{E}_0}$ über, d.h. es gilt $j_{\overline{E}_0} = j_E \mod \mathfrak{P}$.
Betrachte die über dem Ringklassenkörper L von $\mathcal{O}$ definierte elliptische Kurve

$$\tilde{E} : y^2 + xy = x^3 - \frac{36}{j_E - 1728}x - \frac{1}{j_E - 1728}.$$

Diese Kurve hat die gleiche j-Invariante wie die Kurve E. Nach Satz 5.6 sind E und $\tilde{E}$ isomorph über $\mathbb{C}$.
Wir können die Kurve $\tilde{E}$ auch als elliptische Kurve über M betrachten und dort modulo $\mathfrak{P}$ reduzieren. Da $j_E \mod \mathfrak{P} = j_{\overline{E}_0}$ ergibt sich

$$\tilde{E} \mod \mathfrak{P} \simeq E_1.$$

Nun ist aber E schon über L definiert. Somit bedeutet hier die Reduktion mod $\mathfrak{P}$ einer Reduktion mod $\mathfrak{P}'$ mit einem Primideal $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_L$ in $\mathcal{O}_L$. Da wir bei der Reduktion eine Kurve über $\mathbb{F}_{2^n}$ erhalten, muß $\mathcal{O}_L/\mathfrak{P}'$ zu $\mathbb{F}_{2^n}$ isomorph sein. Dies bedeutet aber, daß das Primideal $\mathfrak{P}'$ Restklassengrad n in $\mathcal{O}_L$ haben muß.

Das Primideal $\mathfrak{P}'$ enthält ein Primideal $\mathfrak{p}$ aus dem Ring der ganzen Zahlen $\mathcal{O}_K$ des imaginär quadratischen Zahlkörpers K. Der Restklassengrad von $\mathfrak{P}'$ in $\mathcal{O}_L$ teilt nach dem Hauptsatz der algebraischen Zahlentheorie (siehe Anhang A) stets den Grad der Körpererweiterung $[L : K]$. Dies ist aber gerade die Klassenzahl $h(\mathcal{O})$ der Ordnung $\mathcal{O}$. Damit haben wir den folgenden Satz

Satz 5.20. *Sei $\overline{E}_0$ eine über $\mathbb{F}_{2^n}$ definierte, gewöhnliche elliptische Kurve, deren j-Invariante echt in $\mathbb{F}_{2^n}$ liegt. Weiter sei $End(E) = \mathcal{O}$ eine Ordnung in einem imaginär quadratischen Zahlkörper. Dann teilt der Erweiterungsgrad n die Klassenzahl $h(\mathcal{O})$ der Ordnung $\mathcal{O}$.*

Damit ergibt sich nun:
Falls (i) $t^2 - 4q$ quadratfrei
oder (ii) $t^2 - 4q = c^2 a$ mit a quadratfrei und $n \mid h(c^2 a)$, aber $n \nmid h(d^2 a)$ für alle $d \mid c$,
dann ist $E(\mathbb{F}_q)$ zyklisch. Insbesondere erzeugt dann der Frobeniusendomorphismus die Hauptordnung.
Mit dem Computer läßt sich nun leicht durchrechnen, daß alle Kurven über $q = \mathbb{F}_{2^n}$ mit $n \leq 7$ Bedingung (i) oder (ii) erfüllen. Sie haben somit Endomorphismenring $\mathbb{Z}[\pi]$.
Die anderen für die Kryptographie interessanten Kurven der Charakteristik zwei sind über dem gleichen Körper definiert, in dem wir auch die Punktegruppe betrachten. Das bedeutet, daß hier n sehr groß ist. Somit ist auch die Klassenzahl des Endomorphismenringes nach Satz 5.20 sehr groß.

Wir geben nun noch einen Algorithmus zur Bestimmung der Endomorphismen in Charakteristik zwei an. Dieser ist weit aufwendiger als der Algorithmus für über Primkörpern definierten Kurven.

Lemma 5.21. *Sei E eine über $\mathbb{F}_{2^n}$ definierte gewöhnliche Kurve mit j-Invariante j_E. Dann ist E über $\mathbb{F}_{2^{2n}}$ zu der Kurve*

$$\tilde{E}: \quad y^2 + xy = x^3 + \frac{1}{j}$$

isomorph.

Beweis. Wir setzen $q = 2^n$. Jede gewöhnliche elliptische Kurve über $\mathbb{F}_q$ läßt sich auf die Form

$$y^2 + xy = x^3 + a_2 x^2 + a_6 \text{ mit } a_2,\, a_6 \in \mathbb{F}_q \text{ und } a_6 \neq 0$$

bringen (siehe Kapitel eins). Die j-Invariante ist durch $\frac{1}{a_6}$ gegeben. Nach Satz 5.5 ist E genau dann zu $\tilde{E}$ über $\mathbb{F}_{q^k}$ isomorph, falls $Spur_{\mathbb{F}_{q^k}/\mathbb{F}_2}(a_2) = 0$. Falls

$Spur_{\mathbb{F}_q/\mathbb{F}_2}(a_2) = 0$, dann ist E bereits über $\mathbb{F}_q$ zu $\tilde{E}$ isomorph. Sonst haben wir $Spur_{\mathbb{F}_q/\mathbb{F}_2}(a_2) = 1$, und wir berechnen

$$\begin{aligned} Spur_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a_2) &= a_2 + a_2^2 + \ldots + a_2^{2n-1} \\ &= a_2 + a_2^2 + \ldots a_2^{n-1} + a_2^n(a_2 + a_2^2 + \ldots a_2^{n-1}) \\ &= Spur_{\mathbb{F}_q/\mathbb{F}_2}(a_2) + a_2^n(Spur_{\mathbb{F}_q/\mathbb{F}_2}(a_2)) \\ &= 2 \cdot Spur_{\mathbb{F}_q/\mathbb{F}_2}(a_2) = 0. \end{aligned}$$

Also ist E über $\mathbb{F}_{q^2} = \mathbb{F}_{2^{2n}}$ zu $\tilde{E}$ isomorph. □

Sei nun eine über $\mathbb{F}_{2^n}$ definierte, gewöhnliche elliptische Kurve $\overline{E}$ mit j-Invariante $j_{\overline{E}}$ gegeben. Dann ist diese über $\mathbb{F}_{2^{2n}}$ zu der Kurve

$$\tilde{\overline{E}} : y^2 + xy = x^3 + \frac{1}{j_{\overline{E}}}$$

isomorph, und wir können den Isomorphismus, der durch eine Koordinatentransformation gegeben ist, bestimmen.
Sei $End(\overline{E})$ eine Ordnung $\mathcal{O}$ in einem imaginär quadratischen Zahlkörper K und L der Ringklassenkörper von $\mathcal{O}$. Zu $\mathcal{O}$ gibt es $h(\mathcal{O})$ verschiedene j-Invariante j_i. Nach Satz 5.16 existiert eine j-Invariante j und ein Primideal $\mathfrak{P}$ in $\mathcal{O}_L$, das das Ideal $(2)\mathcal{O}_L$ enthält, so daß $j \mod \mathfrak{P} = j_{\overline{E}}$. Wenn wir die j-Invariante j und das Primideal $\mathfrak{P}$ gefunden haben, dann setzen wir

$$E : y^2 + xy = x^3 + \frac{1}{j}.$$

Dann gilt $E \mod \mathfrak{P} = \tilde{\overline{E}}$.
Wenn wir nun einen Endomorphismus α koordinatenmäßig beschreiben wollen, suchen wir zunächst die über dem Ringklassenkörper definierte Kurve E. Dann überführen wir diese in die Normalform

$$y^2 = 4x^3 - g_2x - g_3.$$

Dort können wir dann den Endomorphismus nach Algorithmus auf Seite 56 berechnen. Anschließend transformieren wir diesen zu einem Endomorphismus auf der Kurve E. Diesen reduzieren wir $\mod \mathfrak{P}$ zu einem Endomorphismus auf $\tilde{\overline{E}}$.
Für den Algorithmus benötigen wir die $h(\mathcal{O})$ verschiedenen j-Invarianten der Ordnung $\mathcal{O}$ und die Primidealzerlegung des Ideals $(2)\mathcal{O}_L$ im Ring der ganzen Zahlen $\mathcal{O}_L$ des Ringklassenkörpers L.

5.5 Nicht-zyklische Punktegruppen

Bei der herkömmlichen Problemstellung des diskreten Logarithmus ist eine Instanz (E, P, Q) gegeben, bei der E eine über einem endlichen Körper $\mathbb{F}_q$ definierte elliptische Kurve ist, P ein Punkt in der Punktegruppe $E(\mathbb{F}_{q^k})$ für ein $k \geq 1$ ist und Q in der von P erzeugten zyklischen Gruppe liegt. Somit finden nicht-zyklische Anteile der Punktegruppe $E(\mathbb{F}_{q^k})$ keine Verwendung.
Beim verallgemeinerten diskreten Logarithmusproblem können nun alle $\mathbb{F}_q$ rationalen Punkte der Kurve verwendet werden. Wir erinnern noch einmal an die Fragestellung des verallgemeinerten Logarithmusproblems:

> Gegeben sei eine über einem Körper $\mathbb{F}_q$ definierte elliptische Kurve und zwei Punkte aus der Punktegruppe $E(\mathbb{F}_{q^k})$. Finde ein $\alpha \in End(E)$ mit $\alpha(P) = Q$, falls ein solches existiert.

Wir können aber Q nur dann aus α und P bestimmen, wenn wir beschreiben können, wir α auf den Punkten der Kurve operiert. Wie wir in den vorherigen Abschnitten dieses Kapitels gesehen haben, ist dies für alle Kurven mit einem Endomorphismenring mit kleiner Klassenzahl möglich.
Der folgende Satz schätzt den Aufwand, der zum Lösen eines diskreten Logarithmusproblems auf einer nicht-zyklischen Gruppe notwendig ist, nach oben ab. Wir schlagen hier einen möglichen Algorithmus vor, bei dem wir die Weil-Paarung einsetzen. Für die Definition dieser Paarung siehe z.B. [36, 62].

Satz 5.22. *Sei (E, P, Q) eine Instanz des verallgemeinerten diskreten Logarithmusproblems und $E(\mathbb{F}_{q^k}) \simeq \mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}$ mit $n_2 \mid n_1$. Dann läßt sich das Problem in höchstens*

$$n_2 \cdot W(E(\mathbb{F}_{q^k})) + T(n_1)$$

lösen, wobei $W(E(\mathbb{F}_{q^k}))$ der Aufwand für eine Auswertung einer Weil-Paarung auf der elliptischen Kurve $E(\mathbb{F}_{q^k})$ und $T(n_1)$ der Aufwand für das Lösen des diskreten Logarithmusproblems in einer zyklischen Untergruppe von $E(\mathbb{F}_{q^k})$ der Ordnung n_1 ist.

Beweis. Sei $\mathcal{O}$ der Endomorphismenring von $E(\overline{\mathbb{F}_{q^k}})$ und $[1, \gamma]$ eine $\mathbb{Z}$-Basis der Ordnung $\mathcal{O}$. Weiter sei eine Instanz $(E(\mathbb{F}_{q^k}), P, Q)$ des verallgemeinerten diskreten Logarithmusproblems gegeben. Dabei sei $E(\mathbb{F}_{q^k})$ zu $\mathbb{Z}_{n_1} \bowtie \mathbb{Z}_{n_2}, n_2 \mid n_1$, isomorph.
Falls $n_2 = 1$, dann ist $E(\mathbb{F}_{q^k})$ zyklisch, und die Aussage ist trivial.
Nehmen wir also an, daß $n_2 > 1$. Es gilt $Q = \alpha P$ mit $\alpha = a + b\gamma \in End(E)$ für ein $a \in \mathbb{Z}_{n_1}$ und ein $b \in \mathbb{Z}_{n_2}$. Somit ist Q in der gleichen Nebenklasse von $< P >$ in

$E(\mathbb{F}_{q^k})$ wie der Punkt $b\gamma(P)$.
Wir kennen $b \in \mathbb{Z}_{n_2}$ nicht, aber aus den Eigenschaften der Weil-Paarunge_n folgt, daß Q genau dann in der gleichen Nebenklasse wie $k \circ \gamma(P)$ bezüglich $< P >$ ist, wenn $e_n(Q - k\gamma(P), P) = 1$ ist (siehe Lemma 5.4 in [36], S. 68). So können wir b durch höchstens n_2 Auswertungen der Weil-Paarung ermitteln.
Danach setzen wir $Q' := Q - b\gamma(P)$ und bestimmen den diskreten Logarithmus a in $\mathbb{Z}_{n_1}$, so daß $aP = Q'$. □

5.6 Bemerkung zum diskreten Logarithmus

Unsere anfänglichen Hoffnungen bestanden darin, zu gegebenem P und Q einen Endomorphismus zu finden, der P auf Q abbildet. Aus dem Satz von Deuring (Satz 5.15) ergibt sich, daß alle Endomorphismen von über $\mathbb{F}_q$ definierten elliptischen Kurven durch Reduktion von über $\mathbb{C}$ definierten elliptischen Kurven mit komplexer Multiplikation entstehen. Aus den Lemmata 5.10 und 5.11 erhalten wir, daß ein Endomorphismus α, der einer imaginär quadratischen Zahl mit Norm n entspricht, von der Form

$$\alpha(x, y) = (R(x), \frac{1}{\alpha}\frac{d}{dx}R(x)y)$$

mit $R(x) = \frac{p(x)}{q(x)}$ für rationale Funktionen $p(x)$, $q(x)$ und $deg\ p(x) = n$ ist.
Die Beschreibung des Endomorphismus α wird also mit zunehmender Norm immer komplexer. Bei Endomorphismenringen mit *kleiner* Klassenzahl gibt es mehr Endomorphismen mit kleiner Norm, im allgemeinen ist aber anzunehmen, daß kein Endomorphismus mit kleiner Norm existiert, der P auf Q abbildet. Es scheint fraglich, ob sich bei Kurven mit einem Endomorphismenring kleiner Klassenzahl überhaupt mehr Informationen über den diskreten Logarithmus gewinnen läßt. Dann würden die in der Einleitung erwähnten Vorteile für die Verwendung dieser Kurven sprechen.
Wenn wir ein Kryptosystem implementieren, das auf dem diskreten Logarithmusproblem auf einer elliptischen Kurve mit einem Endomorphismenring kleiner Klassenzahl beruht, müssen wir mit Angreifern rechnen, die zunächst alle Endomorphismen mit kleiner Norm ausprobieren, da diese besonders schnell berechnet werden können. Falls wir r zufällig gewählt haben, ist es unwahrscheinlich, daß $rP = \alpha(P)$ für einen Endomorphismus α mit kleiner Norm ist. Es bleibt zu überlegen, ob man dieses relativ geringe Risiko auf sich nimmt oder diesen Fall vorher abfängt.

Kapitel 6

Methoden zur schnellen Skalarmultiplikation

In diesem Kapitel wenden wir uns den Methoden der schnellen Multiplikation auf elliptischen Kurven über $\mathbb{F}_q$ zu.
Bei Signaturverfahren und Verschlüsselungen, die auf dem diskreten Logarithmus beruhen, besteht der kostspieligste Teil in der Berechnung $P \to r \cdot P$. Deshalb ist es von großem Interesse, diese Skalarmultiplikation zu beschleunigen.
Es gibt hier zwei grundsätzliche Möglichkeiten:

1. Man versucht, die einzelne Addition noch effizienter durchzuführen, siehe Abschnitt 6.1.

2. Man wählt ein geeignetes Verfahren, um die r Additionen auszuführen, siehe restliche Abschnitte.
   Hier unterscheiden wir noch zwei Arten von Algorithmen:

   (a) Algorithmen, die zur Berechnung von α^r in endlichen Körpern Verwendung finden und für elliptische Kurven übernommen werden (Abschnitt 2),

   (b) Algorithmen, die speziell für elliptische Kurven verwandt werden (Abschnitte 3 und 4).

Falls nichts anderes angegeben ist, bezeichnet log in diesem Kapitel immer den Logarithmus zur Basis zwei.

6.1 Koordinatensysteme

Wenn wir die Komplexität einer einzelnen Addition bzw. Punktverdoppelung auf der elliptischen Kurve betrachten, so interessiert uns die Anzahl der Multiplikationen und Inversionen im zugrundeliegenden Körper. Additionen und Subtraktionen fallen nicht ins Gewicht und können vernachlässigt werden.
Über schnelle Arithmetik in endlichen Körpern gibt es bereits viel Literatur. Wir werden darauf hier nicht näher eingehen. Es sei hier nur erwähnt, daß die Quadratur einer Zahl in $\mathbb{F}_{2^m}$ einfach auszuführen ist, falls die Elemente bezüglich einer Normalbasis gegeben sind. Dies ist eine Basis der Form $\{\beta, \beta^2, \cdots, \beta^{2^{m-1}}\}$ für ein $\beta \in \mathbb{F}_{2^m}$. Falls α durch einen Vektor $(a_0, \cdots, a_{m-2}, a_{m-1})$ repräsentiert wird, stellt $(a_{m-1}, a_0, \cdots, a_{m-2})$ das Element α^2 dar. Quadrieren bedeutet hier also nur eine zyklische Shift-Operation. Deshalb werden wir gewöhnliche Multiplikationen und Quadraturen unterscheiden.
In diesem Abschnitt gehen wir darauf ein, wie die Inversion in $\mathbb{F}_q$, die für eine elliptische Operation nötig ist, umgangen werden kann. Je nach Art der Implementierung ist diese unter Umständen um ein Vielfaches aufwendiger als eine Multiplikation in $\mathbb{F}_q$.
Ein Wechsel von affinen Koordinaten zu einem der hier angegebenen Koordinatensysteme zahlt sich aus, sobald eine Inversion in $\mathbb{F}_q$ teurer als elf Multiplikationen in $\mathbb{F}_q$ ist.
Seien E_1 durch

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{F}_p \text{ und } \qquad 4a^3 + 27b^2 \neq 0$$

und E_2 durch

$$y^2 + xy = x^3 + a_2x + a_6, \qquad a_i \in \mathbb{F}_{2^m} \text{ und } \qquad a_6 \neq 0$$

gegeben. Nach den Additionsformeln aus Kapitel 1 erhalten wir folgende Tabelle:

	Multiplikationen	Quadraturen	Inversionen
Addition auf E_1	2	1	1
Verdopplung auf E_1	2	2	1
Addition auf E_2	2	1	1
Verdopplung auf E_2	3	1	1

Um die Inversionen in $\mathbb{F}_q$ zu vermeiden, können wir zu projektiven Koordinaten übergehen. Wir setzen $x = X/Z$ und $y = Y/Z$ und erhalten für E_1 die homogene Gleichung

$$Y^2Z = X^2 + aXZ^2 + bZ^3.$$

Nun ergeben sich für die Punktaddition $P + Q$ mit $P = (X_1, Y_1, Z_1)$ und $Q = (X_2, Y_2, Z_2)$ folgende Formeln[1]

$$\begin{aligned} X_3 &= v\alpha \\ Y_3 &= u(v^2 X_1 Z_2 - \alpha) - v^3 Y_1 Z_2 \\ Z_3 &= v^3 Z_1 Z_2 \text{ mit} \\ u &= Y_2 Z_1 - Y_1 Z_2, v = X_2 Z_1 - X_1 Z_2 \text{ und} \\ A &= u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2, \end{aligned}$$

und für die Punktverdopplung

$$\begin{aligned} X_3 &= 2hs \\ Y_3 &= w(4B - h) - 8Y_1^2 s^2 \\ Z_3 &= 8s^3 \text{ mit} \\ w &= aZ_1^2 + 3X_1^2, s = Y_1 Z_1, B = X_1 Y_1 s \text{ und } h = w^2 - 8B. \end{aligned}$$

Für E_2 erhalten wir die Kurve

$$Y^2 Z + XYZ = X^3 + AX^2 Z + a_6 Z^3.$$

Hier ergibt sich für die Addition

$$\begin{aligned} X_3 &= AD \\ Y_3 &= CD + A^2(BX_1 + AY_1) \\ Z_3 &= A^3 Z_1 \text{ mit} \\ A &= (X_2 Z_1 + X_1), B = (Y_2 Z_1 + Y_1), \\ C &= A + B \text{ und } D = A^2(A + a_2 Z_1) + Z_1 BC, \end{aligned}$$

[1] Hier und im folgenden gehen wir nicht auf die Speziallfälle $Q = -P$, $P = 0$ oder $Q = 0$ ein. Es ist jedoch klar, daß diese bei einer Implementierung abgefangen werden müssen.

und für die Punktverdoppelung

$$\begin{aligned} X_3 &= AB \\ Y_3 &= X_1^4 A + B(X_1^2 + Y_1 Z_1 + A) \\ Z_3 &= A^3 \text{ mit} \\ A &= X_1 Z_1 \text{ und } B = a_6 Z_1^4 + X_1^4. \end{aligned}$$

Somit erhalten wir für die projektiven Koordinaten die folgende Tabelle

	Multiplikationen	Quadraturen
Addition auf E_1	12	2
Verdopplung auf E_1	7	5
Addition auf E_2	13	3
Verdopplung auf E_2	7	5

Beweis. Wir zeigen nur die Formel für den Fall $P \neq Q$ und $E = E_1$. Die anderen Formeln lassen sich analog herleiten.
Sei $P := (X_1, Y_1, Z_1)$ und $Q = (X_2, Y_2, Z_2)$ mit $P \neq Q$ und $P, Q \neq \mathbf{0}$. Dann gilt $Z_1, Z_2 \neq 0$, und wir können in projektiven Koordinaten $P = (X_1/Z_1, Y_1/Z_1, 1)$ und $Q = (X_2/Z_2, Y_2/Z_2, 1)$ schreiben. Dann entsprechen P und Q den affinen Punkten $P_a = (X_1/Z_1, Y_1/Z_1)$ und $Q_a = (X_2/Z_2, Y_2/Z_2)$. Nach den affinen Formeln aus Kapitel 1 gilt nun, daß $P_a + Q_a$ durch den Punkt (x_3, y_3) mit

$$\begin{aligned} x_3 &= \left(\frac{Y_2/Z_2 - Y_1/Z_1}{X_2/Z_2 - X_1/Z_1}\right)^2 - X_1/Z_1 - X_2/Z_2 \\ \text{und} & \\ y_3 &= -Y_1/Z_1 + \left(\frac{Y_2/Z_2 - Y_1/Z_1}{X_2/Z_2 - X_1/Z_1}\right)(X_1/Z_1 - X_3) \end{aligned}$$

gegeben ist. Dieser entspricht wiederum dem projektiven Punkt $(x_3, y_3, 1)$. Für x_3 erhalten wir nach einigen Umformungen $\frac{1}{v^2 Z_1 Z_2} A$ und für Y_3 in $\frac{1}{v^3 Z_1 Z_2}(-Y_1 v^3 Z_2 - uA + uX_1 v^2 Z_2)$. Somit ist $(x_3, y_3, 1)$ äquivalent zu $(\lambda x_3, \lambda y_3, \lambda)$ mit $\lambda = \frac{1}{v^3 z_1 z_2}$. Daraus ergibt sich die Behauptung. □

Es gibt noch ein weiteres, weniger gebräuchliches Koordinatensystem, das sich für die Darstellung von Punkten einer elliptischen Kurve eignet. Dieses sind die sogenannten Jacobi-Koordinaten. Hier ist $(x, y, z) \sim (x', y', 1)$, falls $x' = \frac{x}{z^2}$ und $y' = \frac{y}{z^3}$.

Analog zu den projektiven Koordinaten kann man hier für die Addition die folgenden Formeln herleiten:
Die Kurve E_1 geht über in

$$Y^2 = X^3 + aXZ^4 + bZ^6,$$

und für die Addition zweier Punkte $P_1 = (X_1, Y_1, Z_1)$ und $P_2 = (X_2, Y_2, Z_2)$ erhalten wir

$$\begin{aligned}
X_3 &= -H^3 - 2U_1H^2 + r^2 \\
Y_3 &= -S_1H^3 + r(U_1H^2 - X_3) \\
Z_3 &= Z_1Z_2H \text{ mit} \\
U_1 &= X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3, S_2 = Y_2Z_1^3, \\
H &= U_2 - U_1 \text{ und } r = S_2 - S_2.
\end{aligned}$$

Für die Punktverdopplung haben wir folgende Formeln:

$$\begin{aligned}
X_3 &= T \\
Y_3 &= -8Y_1^4 + M(S - T) \\
Z_3 &= 2Y_1Z_1 \text{ mit} \\
S &= 4X_1Y_1^2, M = 3X_1^2 + aZ_1^4 \text{ und } T = -2S + M^2.
\end{aligned}$$

Die Kurve E_2 geht über in

$$Y^2 + XYZ = X^3 + a_2X^2Z^2 + a_6Z^6,$$

und für die Addition auf E_2 gilt:

$$\begin{aligned}
X_3 &= \beta^2 + \gamma\beta + \alpha^3 + a_2\epsilon \\
Y_3 &= \beta(x_1\epsilon + X_3) + \gamma(X_3 + Y_1\epsilon) \\
z_3 &= \gamma \text{ mit} \\
\alpha &= X_1Z_2^2 + X_2Z_1^2, \beta = Y_1Z_2^3 + Y_2Z_1^3, \gamma = \alpha Z_1Z_2, \epsilon = \gamma^2.
\end{aligned}$$

Und für die Verdopplung auf E_2 ergibt sich

$$\begin{aligned}
X_3 &= \beta^2 + a_6\alpha^4 \\
Y_3 &= \gamma(\beta(2\beta + Y_1Z_1) + X_3) \\
Z_3 &= \gamma \text{ mit} \\
\alpha &= Z_1^2, \beta = X_1^2 \text{ und } \gamma = \alpha X_1.
\end{aligned}$$

Somit erhalten wir für die Jacobischen Koordinaten folgende Tabelle:

	Multiplikationen	Quadraturen
Addition auf E_1	12	4
Verdopplung auf E_1	4	6
Addition auf E_2	15	5
Verdopplung auf E_2	4	5

Neben diesen drei Koordinatensystemen kann man noch andere Systeme in Betracht ziehen. Die sogenannten Chudnovsky Jacobischen Koordinaten [6] stellen jeden Punkt als Quintupel $(X_1, Y_1, Z_1, Z_1^2, Z_1^3)$ dar. Dies senkt die Rechenzeit für die Addition, da hierfür ja sonst $Z_1^2, Z_1^3, Z_2^2, Z_2^3$ berechnet werden müssen, aber erhöht die Rechenzeit für die Verdopplung. Das Gegenstück dazu sind die modifizierten Jacobischen Koordinaten [7]. Für Charakteristik $\neq 2$ wird hier jeder Punkt als Quadrupel (X_1, Y_1, Z_1, aZ_1^4) beschrieben. Damit reduziert sich die Rechenzeit der Punktverdopplung auf Kosten der Addition. Dazu gibt es kein entsprechendes System für Charakteristik 2.
In [7] empfehlen die Autoren, die verschiedenen Koordinatensysteme zu vermischen. Die Idee besteht darin, daß unterschiedliche Koordinatensysteme unterschiedliche Operationen besonders schnell ausführen. So sind z.B. die modifizierten Jacobischen Koordinaten für die Punktverdopplung sehr effizient (vier Multiplikationen und vier Quadraturen), leider für die Addition jedoch ineffizient (dreizehn Multiplikationen und sechs Quadraturen).
In [7] ist eine Tabelle für die Anzahl der auszuführenden Operationen $t(C^1 + C^2 = C^3)$ (bzw. $t(2C^1 = C^2)$) bei Addition zweier in den Koordinatensystemen C^1 resp. C^2 gegebenen Punkte mit Ergebnis in C^3 (bzw. Verdopplung eines in C^1 gegebenen Punktes mit Ergebnis in C^2).
Wenn wir etwa eine Fenstermethode (siehe Abschnitt 6.2) verwenden und den Multiplikator r in der Form

$$r = 2^{r_0}(2^{r_1} \ldots (2^{r_v} W[v] + W[v-1]) + \ldots + W[0])$$
$$\text{mit } -2^w + 1 \leq W[i] \leq 2^w - 1 \text{ für alle i}$$

schreiben, dann bietet sich die Verwendung von drei unterschiedlichen Koordinatensystemen C^1, C^2, C^3 an. Das System C^3 werde für die Vorberechnungen, d.h. die Ermittlung aller iP für ungerades i mit $1 \leq i \leq 2^w - 1$, verwendet und C^1 für den größten Teil der Punktverdopplung bis $2^{r_i - 1}P'$. Das Ergebnis von $2(2^{r_i - 1}P')$ schließlich werde in C^2 gegeben, d.h. C^2 ist das Koordinatensystem für das $t(2C^1 = C^2) + t(C^2 + C^3 = C^1)$ minimiert wird. Eine Analyse, welches die bestmögliche Kombination (C^1, C^2, C^3) ist, ergibt für C^1 die modifizierten Jacobischen Koordinaten. Für C^3 wählen wir affine Koordinaten, falls eine Inversion in $\mathbb{F}_p$ billiger als B

Multiplikationen für eine von der Eingabegröße abhängige Schranke B ist, und die Chudnovsky Jacobischen Koordinaten sonst. Für C_2 verwenden wir in jedem Fall am besten die Jacobischen Koordinaten.
Für B geben die Autoren in [7] in Abhängigkeit von $\lfloor \log r \rfloor$ folgende Werte an:

$\lfloor \log r \rfloor$	B
160	30,5
192	33,9
224	37,4

6.2 Herkömmliche Methoden und ihre Anwendung auf elliptische Kurven

6.2.1 Additionsketten

Eine bedeutende Rolle bei der schnellen Multiplikation kommt den Additionsketten zu.

Definition 6.1. *Eine* ***Additionskette*** *für $r \in \mathbb{N}$ ist eine endliche Liste ganzer Zahlen*

$$a_1 = 1, a_2, \cdots, a_l = r,$$

so daß für alle $i > 1$ gilt

$$a_i = a_j + a_k$$

für Indices j und k mit $1 \leq j \leq k < i$.

Eine kurze Additionskette für k ergibt einen schnellen Algorithmus zur Berechnung von kP. Deshalb stellt sich die Frage, wie solche Ketten zu finden sind (siehe z.B. [20]). Die kürzeste Additionskette ist im allgemeinen nicht effizient berechenbar, man wird sich in der Praxis mit einem Kompromiß zufrieden geben.
Für elliptische Kurven läßt sich dieses Konzept noch auf sogenannte Additions- und Subtraktionsketten verallgemeinern [38]. Hier verwenden wir die Tatsache, daß Inversion eines Punktes eine Operation ist, die sich fast kostenlos ausführen läßt. Denn falls die Kurve von der Gestalt $y^2 = x^3 + ax + b$ in char $K \neq 2, 3$ gegeben ist, dann erhält man für $-P = (x, -y)$. Leicht komplizierter verhält es sich für gewöhnliche elliptische Kurven $y^2 + xy = x^3 + a_2x^2 + a_6$ in Charakteristik zwei. Hier gilt $-P = (x, x + y)$.

Definition 6.2. *Eine* ***Additions-Subtraktionskette*** *für $r \in \mathbb{N}$ ist eine endliche Liste ganzer Zahlen*

$$a_1 = 1, a_2, \cdots, a_l = r,$$

so daß für alle $i > 1$ gilt

$$a_i = \pm a_j \pm a_k$$

für Indices j und k mit $1 \leq j \leq k < i$.

Den Vorteil der Additions-Subtraktionskette können wir uns an einem einfachen Beispiel verdeutlichen. Die kürzeste Additionskette von 63 (siehe auch [20]) ist durch

$$1 \quad 2 \quad 3 \quad 6 \quad 12 \quad 15 \quad 30 \quad 60 \quad 63$$

gegeben, die kürzeste Additions-Subtraktionskette hat hingegen ein Glied weniger:

$$1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 32 \quad 64 \quad 63.$$

Es gibt aber auch leider keinen effizienten Weg, die kürzeste Additions-Subtraktionskette zu finden. Deshalb wendet man in der Praxis andere Verfahren an, die aber dem Prinzip der Additionsketten folgen.

6.2.2 Die binäre Methode und NAF

Die binäre Methode (siehe unten) gibt zu jeder natürlichen Zahl genau eine Additionskette vor. Tatsächlich ist diese in einigen Fällen sogar die kürzeste, z.B. für 2^a oder für Zahlen der Form $2^a + 2^b$ [20].
Im nachfolgenden Algorithmus sei $l = \lfloor \log_2 r \rfloor$.

Algorithmus 7 Binärer Algorithmus

Input: $P, r = \sum_{i=0}^{l} c_i 2^i, c_i = 0, 1$
Output: $Q = rP$
  $Q := \mathbf{O}$
  for $d = l$ to 0 by -1 **do**
    if c_d=1 **then**
      $Q := Q + P$
    end if
    Q:=2Q;
  end for

Der Algorithmus macht davon Gebrauch, daß wir $\sum_{i=0}^{l} c_i 2^i$ nach dem Horner-Schema in der Form $(\ldots(2c_l + c_{l-1})2 + c_{l-2})2 + \ldots + c_0$ schreiben können.
Im Mittel sind etwa die Hälfte aller Koeffizienten gleich eins. Die binäre Methode benötigt somit im Durchschnitt $\log r$ Verdopplungen und $1/2 \log r$ Additionen, also zusammen $3/2 \log r$ elliptische Operationen.
Das Prinzip der Additions-Subtraktionsketten erlaubt es uns, die binäre Methode effizient zu verallgemeinern, indem wir als Koeffizienten $c_i = 0, \pm 1$ zulassen [38].
Sei B die Binärdarstellung von r. Dann verwenden wir die Tatsache, daß die Ziffernfolge

$$\underbrace{1 \ldots 1}_{a-mal}, a \geq 2$$

der Folge

$$1 \underbrace{0 \ldots 0}_{a-1-mal} (-1).$$

entspricht. Wir ersetzen jedes Auftreten des Ausschnittes $0\underbrace{1 \ldots 1}_{a-mal}, a \geq 2$ durch die Ziffern $1 \underbrace{0 \ldots 0}_{a-1-mal} (-1)$.
Statt $r = 11100111$ berechnen wir nun $r = 100(-1)0100(-1)$. Hier sind weniger Bits von Null verschieden. Dies bedeutet, daß der Rechenaufwand für rP sinkt.
Wir können auch noch einen zusätzlichen Spezialfall abfangen. Wir substituieren die Ziffernfolge

$$1^a 0 1^b$$

in der Binärdarstellung B von r nicht wie oben durch $10^{a-1}(-1)10^{b-1}(-1)$, sondern geschickter durch

$$10^a(-1)0^{b-1}(-1).$$

Man beachte, daß uns dies die gleiche Zahl liefert, da die Ziffernfolge $(-1)1$ die gleiche ganze Zahl wie $0(-1)$ darstellt. Demnach berechnen wir nun statt $r = 1110111$ die Darstellung $r = 1000(-1)00(-1)$.
Dieser Spezialfall ist durchaus nicht so irrelevant, wie er zunächst erscheint. Auf eine Null folgen immerhin mit Wahrscheinlichkeit $\frac{1}{4}$ mehr als zwei Einser.
Morain und Olivos [38] geben einen Algorithmus an, der diese beiden Transformationen bei seiner Berechnung von $r \to rP$ verwendet. Wir beschäftigen uns nun mit der Definition der NAF (nonadjecent form), die ebenfalls beide Ideen berücksichtigt.

Berechnung mittels NAF

Definition 6.3. *Das **Hamminggewicht** einer x-nären Entwicklung*

$$r = \sum_i c_i x^i$$

ist die Anzahl der von Null verschiedenen Koeffizienten c_i.

Die NAF (nonadjecent form), die wir nun einführen, ist die Reihenentwicklung in Zweierpotenzen mit Koeffizienten $0, \pm 1$ mit dem geringsten Hamminggewicht. Sie ermöglicht es also rP mit sehr wenigen Additionen zu ermitteln.

Definition 6.4. *Die **NAF** für r ist eine Reihenentwicklung*

$$r = \sum_{i=0}^{\infty} c_i 2^i, c_i = 0, \pm 1$$

mit der Eigenschaft, daß keine zwei aufeinanderfolgenden Koeffizienten ungleich Null sind.

Es gilt der folgende Satz:

Satz 6.5. *Die NAF einer natürlichen Zahl r hat folgende Eigenschaften:*

1. *Sie ist eindeutig.*

2. *Sie hat die kleinste Anzahl von 0 verschiedener Koffizienten von allen Reihenentwicklungen der Form*

$$r = \sum_{i=0}^{\infty} c_i 2^i, c_i = 0, \pm 1.$$

3. *Für jedes $r \in \mathbb{N}$ existiert eine NAF.*

4. *Sie ist höchstens ein Bit länger als die binäre Entwicklung von r.*

5. *Die erwartete Anzahl von Null verschiedener Koeffizienten beträgt $l/3$, wobei l die Länge der Entwicklung ist.*

Beweis.

1. Angenommen r habe zwei unterschiedliche NAFs, d.h.

$$r = \sum_{i=0}^{\infty} c_i 2^i = \sum_{i=0}^{\infty} c_i' 2^i, c_i = 0, \pm 1.$$

Sei i die kleinste Zahl mit $c_i \neq c_i'$. O.B.d.A. können wir annehmen, daß $i = 0$ ist. Für $i > 0$ läuft die Argumentation analog. Da r entweder durch 2 teilbar ist oder nicht, folgt $c_0 \neq 0 \neq c_0'$. Wir nehmen $c_0 = 1$ an. Daraus ergibt sich, daß $c_0' = -1$.
Da beide Darstellungen NAFs sind, muß $c_1 = c_1' = 0$ gelten. Bilden wir nun $2r$ durch Addition der beiden Präsentationen, ergibt sich $4 \mid 2r$. Dies steht im Widerspruch zu der Tatsache, daß r ungerade ist.

2. Angenommen r ist durch eine beliebige Reihendarstellung

$$r = \sum_{i=0}^{\infty} c_i 2^i, c_i = 0, \pm 1$$

gegeben. Wir zeigen, daß diese sich in eine NAF transformieren läßt, ohne das Hamminggewicht zu erhöhen. Sie i der minimale Wert, so daß $c_i \neq 0 \neq c_{i+1}$. Dann gibt es die folgenden Fälle
1. $c_i = -1$ und $c_{i+1} = 1$ (analog auch $c_i = 1, c_{i+1} = -1$)
und
2. $c_i = 1$ und $c_{i+1} = 1$ (analog auch $c_i = -1, c_{i+1} = -1$).
Im ersten Fall läßt sich die Bitfolge $1 - 1$ durch 01 ersetzen. Das Hamminggewicht reduziert sich um eins.
Im zweiten Fall läßt sich die Bitfolge 11 durch $10 - 1$ ersetzen. Je nachdem, welchen Wert c_{i+2} hatte, bleibt das Hamminggewicht erhalten oder reduziert sich.

In jedem Fall wird das Hamminggewicht durch diese Operation, deren wiederholte Anwendung schließlich auf die NAF von r führt, nicht erhöht. Daraus folgt, daß die NAF die Darstellung

$$r = \sum_{i=0}^{\infty} c_i 2^i, c_i = 0, \pm 1$$

mit kleinstem Hamminggewicht ist.

3. Zur Existenz der NAF geben wir auf Seite 81 einen Algorithmus an, der diese berechnet. Beim binären Algorithmus wird bei jedem Schritt durch 2 geteilt und der Rest der Division, 0 bzw. 1, gespeichert. Dann führt man diesen Prozeß mit dem Quotienten durch.
   Analog dazu läuft der Algorithmus NAF, doch hier wählt man den Rest entsprechend entweder +1 oder -1, so daß auch der Quotient gerade wird.

Algorithmus 8 Berechnung der NAF

Input: $r \in \mathbb{N}$
Output: S, NAF von r, $< c_l, \cdots c_0 >$

```
k := r
S :=<>;
while k > 0 do
  if k odd then
    u := 2 − (k( mod 4))
  else
    u := 0
  end if
  k := k − u;
  Hänge u an die Liste S an;
  k := k/2;
end while
```

4. Falls r eine Binärdarstellung der Länge l hat, läßt sich diese mit den Transformationen aus dem Beweis der Aussage 2. in eine NAF verwandeln. Dabei wird die Darstellung höchstens um ein Bit länger.

5. Diese stochastische Aussage erfordert einen längeren Beweis. Wir verweisen deswegen auf die Literatur [1].

□

Gegeben die NAF für r

$$r = \sum_{i=0}^{l} c_i 2^i, c_i = 0, \pm 1,$$

läßt sich die Multiplikation rP einfach durchführen.

Algorithmus 9 Berechnung von $r \to rP$ mit NAF

Input: P, NAF von r
Output: $Q = rP$

```
Q := P
for i = l − 1 to 1 by −1 do
  Q := 2Q
  if c_i = 1 then
    Q := Q + P
  else if c_i = −1 then
    Q := Q − P
  end if
end for
```

Nach Satz 6.5 liegt die erwartete Anzahl der von Null verschiedenen Koeffizienten der NAF von r bei 1/3·(Länge der NAF). Die Länge der NAF ist nach Satz 6.5 durch $\lfloor \log r \rfloor + 2$ nach oben beschränkt. Zur Berechnung von $r \to rP$ benötigt man also im Durchschnitt $1/3 \log r$ Additionen und $\log r$ Punktverdopplungen, also insgesamt $4/3 \log r$ elliptische Operationen. Dies bedeutet eine kleine Verbesserung gegenüber dem gewöhnlichen binären Algorithmus.

6.2.3 Die k-näre Methode

Die k-näre Methode ist eine natürliche Verallgemeinerung der binären Methode. Diese Methode wird vor allem für Zweierpotenzen $k = 2^m$ angewandt, denn dann

Algorithmus 10 Die k-näre Methode

Input: P, $r = \sum_{i=0}^{l} c_i k^i$ mit $c_i \in \{0, \cdots k-1\}$.
Output: $Q = rP$
Vorberechnung:
Berechne $2P, 3P, \ldots, (k-1)P$.
$Q := \mathbf{0}$
for $d = l$ to 0 by -1 **do**
a) $Q := kQ$
b) $Q := Q + c_i P$
end for

erfordert die Berechnung von kQ nur Verdopplungen.
Die k-näre Methode für $k = 2^m$ können wir auch auf eine vorher berechnete NAF des Multiplikators r anwenden. Dann ist r in der Form

$$\sum_{i=0}^{l} c_i (2^m)^i$$

gegeben. Die Koeffizienten c_i sind hier Strings in $\{0, \pm 1\}^m$, die die NAF-Eigenschaft erfüllen. In der Vorberechnung müssen wir also nur die Menge $\{cP, c \in \{0, \pm 1\}^m$ mit NAF-Eigenschaft$\}$ berechnen. Es gilt das folgende Lemma, das sich leicht mit Vollständiger Induktion beweisen läßt:

Lemma 6.6. *Sei $C(m)$ die Anzahl aller möglichen NAF's der Länge m und sei $C'(m)$ die Anzahl aller möglichen NAF's der Lange m, bei denen das niedrangigste Bit ungleich Null ist.*
Dann gilt

$$\begin{aligned} C(m) &= \frac{2}{3}(2^m - (-1)^m) \text{ und} \\ C'(m) &= \frac{1}{3}(2^m - (-1)^m). \end{aligned}$$

Damit sind für die Vorberechnung $C(m) = \frac{2}{3}(2^m - (-1)^m)$ Operationen notwendig. Für Schritt a) sind insgesamt $\lfloor \log r \rfloor$ Punktverdopplungen nötig. Für Schritt b) benötigen wir immer eine Addition, falls $c_i \neq 0$. Ein einzelnes Bit einer NAF ist mit Wahrscheinlichkeit $\frac{2}{3}$ gleich Null. Also ist c_i mit Wahrscheinlichkeit $(\frac{2}{3})^m$ gleich Null, und mit Wahrscheinlichkeit $(1 - (\frac{2}{3})^m)$ ist in Schritt b) eine Addition

notwendig. Da die Schleife $\log_{2^m} r$-mal durchlaufen wird, ergeben sich hier insgesamt $(1-(\frac{2}{3})^m)(\frac{\lfloor \log r \rfloor}{m})$ Punktadditionen.
Wir erhalten also eine Gesamtkomplexität von

$$C(m) + \lfloor \log r \rfloor + (1-(\frac{2}{3})^m)(\frac{\lfloor \log r \rfloor}{m})$$

elliptischen Operationen.

Für kleine k, etwa $k = 4, 8, 16$ oder $k \in [3, \ldots, 7]$, können wir für kP eine explizite Formel errechnen [41, 14]. Falls wir zum Beispiel die 4-näre Methode zur Multiplikion wählen (wie in [41] vorgeschlagen), kann die Skalarmultiplikaton mit vier durch die entsprechende Formel statt -wie sonst üblich - durch $2(2P)$ berechnet werden. Die Formel für diese Multiplikation erhält man, indem man das Ergebnis der Verdopplungsformel in sich einsetzt. Der Vorteil besteht darin, daß dann im zugrundeliegenden Körper nur noch eine Inversion ausgeführt werden muß. Die unten abgebildete Tabelle vergleicht die Anzahlen der nötigen Operationen im Grundkörper für die Berechnung von $4P$:

	Inversionen	Multiplikationen	Quadraturen
affin	2	2	4
direkt	1	14	7

Für die projektive Methode ergeben sich hier 14 Multiplikationen und 5 Quadraturen. Es ist also unklar, warum wir statt dieser Methode nicht einfach projektive Koordinaten nehmen und so die Inversion umgehen.
Ähnlich wie bei der Binärdarstellung (Seite 78) läßt sich auch für eine 2^m-äre Darstellung

$$\sum_i c_i (2^m)^i$$

eine Additons-Subtraktionsmethode verwenden, um die Anzahl der von 0 verschiedenen Koeffizienten zu reduzieren. Allerdings erzielen wir hier nicht mehr den gleichen Erfolg. Je größer k ist, desto geringer ist die Wahrscheinlichkeit, daß in der 2^m-nären Darstellung eine Konstellation auftritt, die sich durch eine günstigere Bitfolge mit mehr 0-Einträgen ersetzen läßt.
Für $m = 2$ mag sich dieser programmiertechnische Mehraufwand noch lohnen. Hier ergeben sich die folgenden Substitutionen:
3^a kann durch $10^{a-1} - 1$ ersetzt werden.
$3^a x, x \neq 0$, kann durch $10^a(x-4)$ ersetzt werden.
303^b kann durch $10^a - 30^{b-1} - 1$ ersetzt werden.

6.2.4 Die Fenstermethode

Die k-näre Methode ist ein Spezialfall der Fenstermethode, bei der alle Fenster die Größe k haben und aneinander anschließen. Im allgemeinen liegen jedoch bei der Fenstermethode die Fenster nicht nebeneinander. Nulläufe werden übersprungen. Auch können die einzelnen Fenster von unterschiedlicher Größe sein. Man wird sich allerdings eine obere Grenze setzen.
Am einfachsten machen wir uns das Prinzip an einem Beispiel klar.
Sei $r = 2910371$, und die maximale Fensterbreite $w = 4$. Wir ermitteln zunächst in der Vorberechnung alle ungeraden Zahlen, die kleiner als $2^w = 2^4 = 16$ sind. Die Binärdarstellung von r sei durch

$$1011000110100010100011$$

gegeben.
Dann markieren wir die entsprechenden Fenster:

$$\boxed{1011}000\boxed{1101}000\boxed{101}000\boxed{11}$$

und berechnen $r \to rP$ durch

$$2^{18}(11P) + 2^{11}(13P) + 2^5(5P) + (3P).$$

Die gleiche Idee läßt sich statt auf die binäre Entwicklung auch auf die NAF von r anwenden [56]. Aber die NAF ist hier im Durchschnitt noch nicht optimal. In [25] wird das Prinzip der Additions-Subtraktionsketten der Fenstermethode angepaßt. Hier kommt es auf die erwartete Länge der Nulläufe an. Es scheint also wenig Sinn zu machen, bei einer Zahl der Form $\ldots 00110 \ldots$ die Transformation $11 \to 10 - 1$ anzuwenden. Dies reduziert die Länge des linken Nulllaufs um eins. Der in [25] entwickelte Algorithmus berücksichtigt diese Tatsachen, aber wie wir sehen werden, führt er nicht zur Verbesserung der Laufzeit.
Angenommen wir haben einen Bitstring $B = b_t \ldots b_1$, $b_1 = b_t = 1$, $b_i \in \{0, 1\}$. Dann setze D_i=#(der Einsen unter $b_1 \ldots b_i$) $-$ # (der Nullen unter $b_1 \ldots b_i$). B wird dann und nur dann ersetzt, falls $D_i > 0$ für alle $i > 0$ und $D_t = 3$.
Sei B ein solcher Bitstring und $b_{s_1}, \ldots, b_{s_z} = b_t$ seien die Stellen für die $D_{s_i} \geq 3$, aber $D_{s_{i+1}} < D_{s_i}$ ist. Dann transformieren wir

$$B = b_t \ldots b_{s_{z-1}} \ldots b_{s_1} \ldots b_1$$

in

$$10 \ldots \overline{b_{s_{z-1}+2}}(-1)0\overline{b_{s_z-1}} \ldots \overline{b_{s_1+2}}(-1)0\overline{b_{s_1-1}} \ldots \overline{b_2}(-1),$$

wobei

$$\overline{b_i} = \begin{cases} -1 & \text{falls } b_i = 0 \\ 0 & \text{falls } b_i = 1. \end{cases}$$

Beispiel 6.7. Die Zahl $r = 80658919$ ist durch den Bitstring

$$10011001110110000011110011 1$$

gegeben. Die zugehörige NAF ist

$$1010(-1)01000(-1)0(-1)00001000(-1)0100(-1).$$

Deren Nulläufe haben die Durchschnittslänge $1\frac{8}{9}$.
Der zugehörige String, den wir nach der oben beschriebenen Transformation erhalten, ist

$$101001(-1)000(-1)0(-1)000010000.$$

Hier liegt die Durchschnittslänge bei $2\frac{3}{7}$.

Zur Laufzeitanalyse sei $\lambda = \lfloor \log r \rfloor$, L die durchschnittliche Länge der Darstellung von r nach der Transformation, Z die erwartete Anzahl von Nullen in einem Lauf, und w die Fensterlänge. Dann sind in der Vorberechnung $2^{w-1} - 1$ Punkte zu ermitteln. Die Anzahl der Verdopplungen ist im Wesentlichen L. Hier müssen wir nur die erwartete Länge des höchstwertigsten Fensters abziehen, die bei $w - z$ liegt. Die Anzahl der Fenstersegmente ist durch $L/(w + z)$ gegeben. Es ergibt sich somit eine Gesamtkomplexität R_1 von

$$(L + z - w) + \frac{L}{w + z} + 2^{w-1} - 1.$$

Für L erhalten wir $\lambda + \frac{5}{4}$ und für Z nach Zusammenstellung der möglichen Zustände und Auswertung einer Übergangsmatrix den Wert $\frac{3}{2}$ (für eine Beweis siehe [25]). Für die normale NAF ergibt sich hier $\frac{4}{3}$.
Damit haben wir

$$R_1 = (\lambda + \frac{11}{4} - w) + \frac{\lambda + 5/4}{w + 3/2} + 2^{w-1} - 1.$$

Wir wählen den Parameter w in Abhängigkeit von λ so, daß der Gesamtaufwand R_1 minimiert wird.
Bei näherer Betrachtung stellt sich aber heraus, daß diese Methode gegenüber der Fenstermethode mit NAF keinen Vorteil bringt. Zwar erhält man für die NAF von r

eine durchschnittliche Länge der Nulläufe von $\frac{4}{3}$, aber dafür lassen sich Operationen bei der Vorberechnung einsparen. Hier sind nicht mehr $2^{w-1}-1$ Punkte zu ermitteln, sondern nur alle Punkte in

$\{cP : c \in \{0, \pm 1\}^m, c$ erfüllt die NAF-Eigenschaft und cP ist nicht durch zwei teilbar$\}$.

Die Anzahl der Punkte mit dieser Eigenschaft haben wir in Lemma 6.6 berechnet. Es sind $\frac{1}{3}(2^m - (-1)^m)$ Punkte. Damit ergibt sich für die Gesamtkomplexität

$$R_2 = ((\lambda + \frac{5}{4}) - (w + \frac{4}{3})) + \frac{\lambda + \frac{5}{4}}{w + \frac{4}{3}} + \frac{1}{3}(2^m - (-1)^m).$$

In Abschnitt 6.5 stellen wir R_1 und R_2 einmal für realistische Größen λ gegenüber. Dabei erweist sich die Idee in [25] als unzureichend. Sie ist komplizierter als die Fenstermethode mit NAF und benötigt nicht weniger elliptische Operationen.

6.3 Kurven, die über einem Teilkörper definiert sind

In diesem Abschnitt beschäftigen wir uns mit der Situation aus Kapitel 3. Die elliptische Kurve sei über einem Teilkörper $\mathbb{F}_q$ definiert, und wir betrachten die Punkte aus einer Körpererweiterung $\mathbb{F}_{q^n}$. Dabei gehen wir davon aus, daß der Körper von der Charakteristik zwei ist, da dies der für die Praxis relevante Fall ist. Tatsächlich lassen sich die grundlegenden Resultate aber auf beliebige Charakteristiken übertragen. Es sind dann lediglich einige Feinheiten zu beachten (siehe [55]).
Falls die Kurve bereits über einem Teilkörper $\mathbb{F}_q$ definiert ist, läßt sich die Operation des Frobeniusendomorphismus

$$\pi_q : (x, y) \to (x^q, y^q)$$

ausnutzen. Dieser ist äußerst kostengünstig durchführbar, vor allem wenn die Körperelemente in Charakteristik zwei in Normalbasis gegeben sind (siehe Seite 71).
Für die nachfolgenden Betrachtungen machen wir wiederholt von Satz 4.6 aus Kapitel 4 Gebrauch. Deshalb erinnern wir nochmals an dessen zentrale Aussage:

Sei E eine über $\mathbb{F}_q$ definierte elliptische Kurve mit $t = q + 1 - \#E(\mathbb{F}_q)$. Weiter sei der Endomorphismenring von E durch eine imaginär quadratische Ordnung $\mathcal{O}$ gegeben. Dann entspricht der Frobeniusendomorphismus der imaginär quadratischen Zahl α, die die Gleichung $x^2 - tx - q = 0$ erfüllt.

6.3.1 Die anomalen binären Kurven

Koblitz [22] hat die Verwendung von den sogenannten binären anomalen Kurven vorgeschlagen.
Diese sind die über $\mathbb{F}_2$ definierten Kurven

$$E : y^2 + xy = x^3 + x^2 + 1$$

und der Twist

$$\tilde{E} : y^2 + xy = x^3 + 1.$$

Der Endomorphismenring der Kurven ist isomorph zu $\mathbb{Z}[\alpha]$ mit $\alpha = \frac{1+\sqrt{-7}}{2}$, und der Frobeniusendomorphismus $\pi_2 : (x, y) \to (x^2, y^2)$ entspricht den imaginär quadratischen Zahlen $\alpha = \frac{1+\sqrt{-7}}{2}$ bzw. $\alpha - 1 = \frac{-1+\sqrt{-7}}{2}$.
Er erfüllt somit die Gleichung

$$\begin{aligned} x^2 - x + 2 &= 0 \text{ bzw.} \\ x^2 + x + 2 &= 0. \end{aligned} \tag{6.1}$$

Die beiden Kurven $E, \tilde{E}$ können über einem Erweiterungskörper $\mathbb{F}_{2^n}$ betrachtet werden. Die Ordnung $\#E(\mathbb{F}_{2^n})$ kann leicht mithilfe einer Rekusionsformel (siehe dazu [56]) ermittelt werden.
Die Kurven eröffnen zwei Möglichkeiten der schnellen Multiplikation mit r.
Aus den Gleichungen 6.1 folgen die Identitäten

$$\begin{aligned} 4 &= -\pi_2^3 - \pi_2^2 \\ 8 &= -\pi_2^3 + \pi_2^5 \\ 16 &= \pi_2^4 - \pi_2^8 \text{ auf } E, \text{ bzw.} \\ 4 &= \pi_2^3 - \pi_2^2 \\ 8 &= -\pi_2^5 + \pi_2^3 \\ 16 &= -\pi_2^8 + \pi_2^4 \text{ auf } \tilde{E}. \end{aligned}$$

Dies können wir ausnutzen, um die Operation $P \to 16 \cdot P$ in der Punktegruppe $E(\mathbb{F}_{2^n})$ (bzw. $\tilde{E}(\mathbb{F}_{2^n})$) der Kurve E (bzw. $\tilde{E}$) kostengünstig durchzuführen. Denn statt $P \to 16P$ berechnen wir nun $P \to \pi_2^4(P) - \pi_2^8(P)$ auf E (bzw. $P \to -\pi_2^8(P) + \pi_2^4(P)$ auf $\tilde{E}$). Da der Aufwand für die Anwendung des Frobeniusendomorphismus vernachlässigt werden kann, benötigen wir nun für $16P$ nur noch eine statt vier elliptische Additionen.
Für die beiden anomalen, binären Kurven E und $\tilde{E}$ bietet sich also die 16-näre Methode zur Multiplikation an.

Die andere Möglichkeit besteht darin, den Multiplikator r in eine Reihe bezüglich des Frobeniusendomorphismus π_2 bzw. der ihm zugeordneten imaginär quadratischen Zahl α zu entwickeln:

$$r = \sum_{i=0}^{\infty} c_i \alpha^i, c_i \in \{0, \pm 1\}.$$

Die Koeffizienten dieser Reihenentwicklung ermitteln wir sukzessive von c_0 an aufwärts. Beginnend bei $r = r_1\alpha + c_0$ erhalten wir r_{i+1} aus $r_i = r_{i+1}\alpha + c_i$ für $i = 1, 2, \ldots$ usw. Falls r_i nicht durch α teilbar ist, folgt $c_i = 0$. Wenn r_i jedoch nicht durch α teilbar ist, so sind es $r_i - 1$ und $r_i + 1$, und uns bleiben zwei Vorgehensweisen zur Auswahl: Zum einen können wir c_i stets so wählen, daß $r_i - c_i$ möglichst kleine Norm hat (siehe [35]). Dann ergibt sich eine sehr kurze Entwicklung der Länge höchstens n

$$\sum_{i=0}^{n-1} c_i \alpha^i.$$

Zum anderen können wir die Koeffizienten c_i aber auch stets so wählen, daß $r_i - c_i$ durch α^2, bzw. r_{i+1} durch α teilbar ist. Dies ergibt dann eine Entwicklung mit NAF-Eigenschaft (keine zwei aufeinanderfolgenden Koeffizienten sind von 0 verschieden), die höchstens die Länge $n + 2$ hat. Diese Entwicklung ist aufgrund ihres geringen Hamminggewichtes und der damit verbundenen Einsparung von Additionen der ersten Methode vorzuziehen. Wir werden nun näher die α-näre NAF eingehen, Existenz, Eindeutigkeit, Länge und weitere Eigenschaften beweisen. Dazu betrachten wir nun nur die Kurve E, für $\tilde{E}$ verläuft alles analog.

Satz 6.8. *Jedes Element $r \in \mathbb{Z}[\alpha]$ hat eine eindeutige α-näre NAF. Die Anzahl aller von 0 verschiedener c_i in der α-nären NAF ist die kleinste Anahl von 0 verschiedenen c_i von allen möglichen α-nären Entwicklungen.*

Beweis. Der Beweis verläuft analog zu Satz 6.5.
Sei $r = \sum_{i=0}^{\infty} e_i \alpha^i$ eine beliebige α-näre Entwicklung von r und i die kleinste Zahl, so daß $e_i e_{i+1} \neq 0$. Dann wenden wir eine der folgenden Transformationen an:

$$\begin{aligned} \alpha + 1 &\rightarrow -\alpha^3 - 1 \\ -\alpha - 1 &\rightarrow \alpha^3 + 1 \\ \alpha - 1 &\rightarrow \alpha^2 + 1 \\ -\alpha + 1 &\rightarrow -\alpha^2 - 1. \end{aligned}$$

Dadurch erreichen wir e'_{i+1}. Für den nachfolgenden oder den übernächsten Koeffizienten tritt einer der drei Fälle ein:

1. Er war gleich null und wird durch den Überschlag verändert. Dann bleibt das gesamte Gewicht der Entwicklung nach der Transformation unverändert.

2. Er war ungleich null und addiert sich durch den Überschlag nun zu null auf. Dann haben wir das Gewicht reduziert.

3. Wir erhalten nach der Transformation den Koeffizienten ± 2, der durch die Transformation

$$2 \rightarrow -\tau^3 - \tau$$

eliminiert wird. Auch hier erhöht sich das Gewicht der Entwicklung nicht.

Wiederholte Anwendung der Transformationen überführt somit jede Entwicklung in NAF, ohne deren Hamming-Gewicht zu erhöhen. Die α-näre NAF muß somit die Entwicklung mit kleinstem Hamming-Gewicht sein.
Der Beweis der Eindeutigkeit ist identisch zum Beweis von Satz 6.5. □

Zur Existenz der NAF geben wir einen Algorithmus, der zu gegebenem $\beta \in \mathbb{Z}[\alpha]$, die $\alpha - näre$ NAF ermittelt [56]. Dieser basiert auf einem einfachen Lemma.

Lemma 6.9. *Die Zahl α teilt $\beta = a + b\alpha$ genau dann, wenn a gerade ist.*

Beweis. Falls die Zahl β durch α teilbar ist, dann gilt

$$\beta = \alpha(c + d\alpha) = -2d + (c + d)\alpha \text{ für } c, d \in \mathbb{Z},$$

also ist a gerade.
Wenn a gerade, dann gilt $\alpha \mid a$ (da α zwei teilt) und somit auch $\alpha \mid \beta$. □

Im nachfolgenden Algorithmus wählen wir c_i nun stets so, daß r_{i+1} von der Form $a_{i+1} + \alpha b_{i+1}$ mit geradem a_{i+1} ist.

Algorithmus 11 Berechnung der α-nären NAF

Input: $\beta = a + b\alpha$
Output: S, die α-näre NAF von β

```
x := a, y := b
S :=<>
while x ≠ 0 oder y ≠ 0 do

  if x odd then
    u := 2 − (x − 2y( mod 4))
  else
    u := 0
  end if
  x := x − u
  append u to S
  (x,y):=(y-x/2,-x/2);
end while
```

Um die Länge der Entwicklung zu reduzieren, werden wir aber für Multiplikatoren r mit $r^2 > 2^n$ nicht rP berechnen, sondern γP, wobei $\gamma \in \mathbb{Z}[\alpha]$ die imaginär quadratische Zahl mit der Eigenschaft $\gamma \equiv r \bmod (\pi^n - 1)$ ist und $\mathrm{Norm}(\gamma) < 2^n$.
Die Zahl γ erhält man aus r durch Division mit Rest durch $\pi^n - 1$. Für einen Algorithmus siehe [56].

Satz 6.10. *Die α-näre NAF für ein $r \in \mathbb{Z}[\alpha]$ hat höchstens die Länge $n + 2$.*

Beweis. Wir geben hier keinen vollständigen Beweis, sondern berufen uns auf Lemma 3 in [35].
Für alle $s \in \mathbb{Z}[\alpha]$ mit Norm $N(r) < 2^n, n \in \mathbb{N}$, existiert eine Entwicklung

$$r = \sum_{j=0}^{n-1} c_j \alpha^j \tag{6.2}$$

der Länge n mit $c_j \in \{0, \pm 1\}$.
Zum Beweis dieses Satzes verwenden Meier und Staffelbach die erste Vorgehensweise, die wir auf Seite 89 angesprochen haben. Hier wird c_i immer so gewählt, daß $\mathrm{Norm}(r_i) \geq \mathrm{Norm}(r_{i+1}\alpha)$, also $\mathrm{Norm}(r_{i+1}) \leq \frac{\mathrm{Norm}(r_i)}{2}$ ist. Dadurch erreichen wir für r eine Reihenentwicklung der Länge höchstens $\log(\mathrm{Norm}(r))$, und das war die Behauptung.
Gegeben nun eine Entwicklung von r der Länge n nach Gleichung 6.2 können wir nach Satz 6.8 diese in eine α-näre NAF überführen. Aus dem Beweis des Satzes 6.8 folgt dann, daß diese höchstens zwei Bit länger als die ursprüngliche Entwicklung ist. □

Nach [13] gilt auch für die α-näre Entwicklung, daß die erwartete Anzahl von Null verschiedener Koeffizienten bei $\frac{1}{3}$ liegt. Damit liegt die Gesamtkomplexität der Multiplikation mit r auf anomalen binären Kurven bei etwa $\frac{1}{3}\log r$ elliptischen Operationen.

6.3.2 Kurven über $\mathbb{F}_q$ mit $q > 2$

Die Ideen zur schnellen Multiplikation auf anomalen Kurven sind auf Kurven, die über kleinen Teilkörpern $\mathbb{F}_q, q = 2^m$, definiert sind, übertragen worden [40, 5].
Nun wenden wir uns Frobeniusentwicklungen zu.
Sei α wieder die imaginär quadratische Zahl im Endomorphismenring $\mathcal{O}$, die dem Frobeniusendomorphismus entspricht.

Lemma 6.11. *Sei $r \in \mathbb{Z}[\alpha]$. Dann gibt es ein $s \in \mathbb{Z}$, $-\frac{q}{2} \leq s \leq \frac{q}{2}$ und ein Element $t \in \mathbb{Z}[\alpha]$ mit*

$$r = t \cdot \alpha + s$$

Falls wir s aus dem Intervall $[-\frac{q}{2}+1, \cdots, \frac{q}{2}]$ wählen, sind s und t eindeutig bestimmt.

Wir beweisen Lemma 6.11, da aus dem Beweis hervorgeht, wie wir die Zahlen r und s ermitteln. Diese Konstruktion wird im Algorithmus, den wir später vorstellen, verwendet.

Beweis. Sei $r = r_1 + r_2\alpha$ mit $r_i \in \mathbb{Z}$. Wir suchen ganze Zahlen $t_1, t_2, s \in \mathbb{Z}$ mit

$$r_1 + r_2\alpha = (t_1 + t_2\alpha)\alpha + s. \tag{6.3}$$

Der Frobeniusendomorphimus erfüllt die Identität

$$\pi_q^2 - c\pi_q + q = 0.$$

Deshalb können wir Gleichung (6.3) in

$$(t_1 + t_2\alpha)\alpha + s = (t_1 + t_2 c)\alpha + (s - t_2 q)$$

überführen. Koeffizientenvergleich ergibt $r_1 = -t_2 q + s$ und somit $s \equiv r_1 \bmod q$. Wir wählen $s \in \{-\frac{q}{2}, \cdots, \frac{q}{2}\}$ entsprechend und erhalten dann

$$t_2 = \frac{s - r_1}{q} \text{ und } t_1 = r_2 - ct_2.$$

Die Eindeutigkeit ist klar. □

Durch wiederholte Anwendung von Lemma 6.11 ergibt sich nun die Reihenentwicklung bezüglich des Frobeniusendomorphismus. Deren Länge k folgt aus einer Restgliedabschätzung.
Im folgenden Satz bezeichne $||\cdot||$ die Norm von r im Zahlkörper $\mathbb{Z}[\alpha]$[2].

Satz 6.12. *Sei $r \in Z[\alpha], q \geq 4$. Setze $k = \lceil 2\log_q ||r|| \rceil + 3$. Dann gibt es ganze Zahlen $r_j \in \{-q/2, \cdots q/2\}, 0 \leq j \leq k$, so daß*

$$r = \sum_{j=0}^{k} r_j \alpha^j.$$

Bei spezielleren Angaben von c und q läßt sich das Resultat aus Satz 6.12 noch verbessern. Wir erhalten folgende Tabelle (siehe [40], Corollary 1-3):

q	c	obere Schranke für die Lange $k_{q,c}$ der Frobeniusentwicklung
4	± 1	$\lceil \log_2 \lvert r \rvert \rceil + 1$
4	± 3	$\lceil \log_2 \lvert r \rvert \rceil + 3$
8	± 1	$\lceil \frac{2}{3} \log_2 \lvert r \rvert \rceil + 1$
8	± 3	$\lceil \frac{2}{3} \log_2 \lvert r \rvert \rceil + 1$
8	± 5	$\lceil \frac{2}{3} \log_2 \lvert r \rvert \rceil + 2$
16	bel.	$\lceil \frac{1}{2} \log_2 \lvert r \rvert \rceil + 1$

In dieser Tabelle bezeichnet $|\cdot|$ einfach den Absolutbetrag von r.
Aus diesen theoretischen Erkenntnissen läßt sich nun ein Algorithmus zur schnellen Multiplikation gewinnen. Dieser läuft in drei Schritten ab (siehe Seite 94) .
Sei E über $\mathbb{F}_q$ definiert, und der Frobeniusendomorphismus π_q erfülle auf E die Gleichung $\pi^2 - c\pi + q = 0$.
.

Bemerkung 6.13.

1. In Schritt 1 berechnen wir alle möglichen Koeffizienten in der Reihenentwicklung von r bezüglich α.
   In Schritt 2 wird die Reihenentwicklung

$$r = \sum_{i=0}^{k} r_i \alpha^i$$

[2]Falls $|\cdot|$ der komplexe Absolutbetrag ist, dann gilt $||r|| = |r|^2$.
[3]Hier verstehen wir unter $r_1 = s_1 \bmod q$ die ganze Zahl r_1 mit $r_1 \in \{-q/2+1, \cdots, q/2\}$ mit $r_1 \equiv s_1 \bmod q$.

Algorithmus 12 Skalarmultiplikation mit Frobeniusentwicklung

Input: $r \in \mathbb{N}$ und $P \in E(\mathbb{F}_{q^n})$
Output: $H = rP$
1.Berechne und speichere iP, $1 \leq i \leq q/2$.
2.Setze $s_1 := r$, $s_2 := 0$, $i := 0$.
while ($s_1 > q/2$ oder $s_2 > 1$) **do**
Compute and store $r_1 = s_1 \bmod q^3$
$h := (r_i - s_1)/q$, $i := i + 1$, $s_1 := s_2 - c \cdot h$, $s_2 := h$;
end while
3. $H := s_2 \cdot \pi_q(P) + s_1(P)$
for $j = i - 1$ to 0 by -1 **do**
if $r_j \geq 0$ **then**
$H := \pi_q(H) + r_j P$
else
$H := \pi_q(H) - \mid r_j P \mid$
end if
end for

errechnet und durch Speicherung der Koeffizienten r_i festgehalten. Die Berechnung der r_i verläuft analog zum Beweis von Lemma 6.11.
In Schritt 3 ermitteln wir dann rP durch

$$\begin{aligned} rP &= \sum_{i=0}^{k} r_i \alpha^i(P) \\ &= \alpha(\alpha \cdots (r_k \alpha(P) + r_{k-1})P \cdots) + r_0 P. \end{aligned}$$

2. Falls $s_1 \equiv q/2 \bmod q$ ist, gibt es für die Wahl von r_i zwei Möglichkeiten.
Zum einen können wir r_i so wählen, daß die Norm von $s_1 - r_i$ minimiert wird.
Zum anderen können wir zunächst r_i einfach gleich $q/2$ setzen, aber dann nach Abschluß der Berechnung der Frobeniusentwicklung im 3. Schritt eventuell noch eine Transformation vornehmen, falls sich dadurch die Anzahl der von 0 verschiedenen Koeffizienten reduzieren läßt.
Dazu ein Beispiel:
Es sei ein dreistelliger Ausschnitt einer Frobeniusentwicklung mit $q = 2^3$ und $c = 3$ gegeben:

$$\ldots + 3\pi^{k+2} + (-3)\pi^{k+1} + 4\pi^k + \ldots .$$

Auf E gilt $\pi^2 - 3\pi + q = 0$. Wir können also den Ausschnitt in

$$\ldots + 2\pi^{k+2} - 4\pi^k + \ldots$$

überführen.

Nun kommen wir zur Laufzeitanalyse.
Sei E über $\mathbb{F}_q$ definiert und $k_{q,c}(r)$ die Länge der Frobeniusentwicklung von r.

Satz 6.14. *Sei P ein Punkt in der Punktegruppe $E(\mathbb{F}_{q^n})$. Zur Berechnung von $P \to rP$ benötigt der Algorithmus höchstens*
$q/2 + k_{q,c}(r) - 1$ Inversionen,
$q/2 + 2k_{q,c}(r) - 2$ Multiplikationen und
$(2\log_2 q + 1)k_{q,c}(r) + q/2 - 1$ Quadraturen in $\mathbb{F}_{q^n}$.

Beweis. In Schritt 1 müssen alle Punkte iP, $2 \leq i \leq q/2$, berechnet werden. Dazu benötigen wir $q/2 - 1$ elliptische Additionen. Hinzu kommen höchstens $k_{q,c}(r)$ Additionen in Schritt 3. Das ergibt zusammen

$$q/2 + k_{q,c} - 1$$

elliptische Operationen. Die Anzahl der Auswertungen des Frobeniusendomorphismus ist ebenfalls durch $k_{q,c}(r)$ beschränkt. Der Frobeniusendomorphismus benötigt $2 \cdot \log_2(q)$ Quadraturen in $\mathbb{F}_q$.
Nun gilt (siehe Abschnitt 6.1):
Eine elliptische Operation benötigt höchstens eine Inversion, zwei Quadraturen und zwei Multiplikationen in affiner Darstellung.
Daraus folgt die Behauptung. □

Beispiel 6.15. Für $q = 4$ und $c = 1$ ergibt sich $k_{q,c}(r) \leq \lceil \log_2 \mid r \mid \rceil + 1 < \log_2(r) + 2$. Somit benötigen wir in affiner Darstellung höchstens $\log_2(r) + 3$ Inversionen, $2\log_2(r)+6$ Multiplikationen und $5\log_2(r)+13$ Quadraturen. Berücksichtigen wir, daß im Durchschnitt etwa $1/(q+1) = \frac{1}{5}$ der Koeffizienten der Frobeniusentwicklung gleich Null sind, ergeben sich die Durchschnittswerte von $\frac{4}{5}\log_2(r) + \frac{12}{5}$ Inversionen, $\frac{5}{8}\log_2(r) + \frac{24}{5}$ Multiplikationen und $4\frac{4}{5}(\log_2(r) + 2) + 1$ Quadraturen.
Bei der NAF-Methode sind etwa $\frac{4}{3}\log_2(r)$ elliptische Operationen notwendig. Das ergibt dann etwa $\frac{4}{3}\log_2(r)$ Inversionen, $\frac{8}{3}\log_2(r)$ Multiplikationen und $\frac{8}{3}\log_2(r)$ Quadraturen. Besonders wenn die Quadraturen günstig ausführbar sind, wie etwa im Fall einer Normalbasis, ist die Frobeniusentwicklung eine entscheidende Verbesserung.

In [40] werden außerdem noch die Anzahl der Operationen in $\mathbb{F}_q$ angegeben, falls die Punkte in projektiven Koordinaten dargestellt sind. Daraus läßt sich errechnen, daß sich eine solche Darstellung erst auszahlt, falls eine Inversion in $\mathbb{F}_q$ länger als elf Multiplikationen dauert. In Charakteristik zwei läßt sich aber effizienter invertieren. Schnelle Algorithmen zur Invertierung in Körpern der Charakteristik zwei sind in [14, 18] angeben.

Gegeben die Frobeniusentwicklung einer Zahl r können wir natürlich in Schritt 3 auch eine Fenstermethode anwenden. Wir schreiben

$$rP = \sum_{i=0}^{\lfloor k/w \rfloor} \pi_q^{iw} \sum_{j=0}^{w-1} m_{iw+j} \pi^j(P).$$

In der Vorberechnung müssen wir dann alle möglichen Punkte, die wir als Ergebnisse der inneren Summe erhalten können, berechnen und speichern. Dies sind alle Punkte mit Frobeniusentwicklung der Länge höchstens w repräsentiert durch $(a_0, \ldots a_{w-1}), a_i \in \{-q/2, \ldots q/2\}$ außer $(0, \ldots, 0)$. Allerdings kennen wir mit dem zu $(a_0, \ldots a_{w-1})$ gehörigen Punkt R auch $-R$, der $(-a_0, \ldots -a_{w-1})$ entspricht. Deshalb müssen wir bei der Vorberechnung $((q+1)^w - 1)/2$ Punkte ermitteln. Für die Vorberechnung ergibt sich somit ein Aufwand von $((q+1)^w - 3)/2$ elliptischen Operationen, der eigentliche Algorithmus erfordert noch zusätzliche $\lfloor k/w \rfloor$-1 Operationen, und mit $k < 2\log_q(r)+4$ erhalten wir eine Gesamtkomplexität von höchstens $((q+1)^w - 3)/2 + \frac{2\log_q(r)+4}{w} - 1$ elliptischen Operationen. Außerdem sind höchstens $2\log_q(r) + w + 3$ Auswertungen des Frobeniusendomorphismus nötig.

Die zweite Idee besteht wieder darin, die charakteristische Gleichung des Frobeniusendomorphismus π_q direkt auszunützen, um schnelle Multiplikation mit q zu ermöglichen (siehe [5]).
Sei E über $\mathbb{F}_q$ definiert mit $c = q + 1 - \#E(\mathbb{F}_q)$. Dann gilt

$$q = c\pi_q - \pi_q^2. \tag{6.4}$$

Falls die Spur c klein ist, läßt sich mit Gleichung (6.4) die Multiplikation mit q effizienten durchführen. Wir geben nun je eine Variante der k-nären bzw. der Fenstermethode an, bei denen die Gleichung (6.4) eingebaut ist.
Der folgende Algorithmus ist ohne weiteren Kommentar verständlich. Wir wählen für den Multiplikator r eine q-äre Darstellung $(e_{n-1}e_{n-2}\ldots e_1e_0)$.

Algorithmus 13 Die q-äre Methode

Input: P
Output: $Q = rP$
1: Vorberechungen
   $P_0 := 0$; $P_1 := P$
2: **for** $i = 2$ to $q-1$ **do**
3: $P_i := P_{i-1} + P$ (d.h. $P_i = iP$)
4: **end for**
5: Eigentliche Rechnung
   $Q := P_{e_{n-1}}$
6: **for** $i = n-2$ to 0 **do**
7: $Q := c\pi_q(Q) - \pi_q^2(Q)$ (d.h. $Q := qQ$)
8: $Q := Q + P_{e_i}$
9: **end for**

Zur Laufzeitanalyse sei $R(c)$ die Anzahl der elliptischen Operationen, die für die Multiplikation mit c benötigt werden. Der Schritt 3 kostet $q-2$ Operationen, Schritt 7 $(n-1)(R(c)+1)$ Operationen und Schritt 8 erfordert $n-1$ Operationen. Damit ergibt sich eine Gesamtanzahl von $(n-1)(R(c)+2)+q-2$ Operationen.
Wir geben eine Tabelle der Parameter ($q \leq 2^6$) an, bei denen sich die Laufzeit gegenüber der NAF-Methode verbessert. Hier steht der Parameter l für $\lfloor \log r \rfloor$.

q	$t = \pm 1$	$t = \pm 3$	$t = \pm 5$	$t = \pm 7$
2^2	l	k.V.	-	-
2^3	$2l/3+4$	k.V.	k.V.	-
2^4	$l/2+12$	$l+10$	$5l/4+9$	k.V.
2^5	2l/5+28	$4l/5+26$	$l+25$	$6l/5+24$
2^6	l/3+60	$2l/3+58$	$5l/6+57$	$l+56$

Hier sei l die Bitlänge von r, das Kürzel k.V. steht für keine Verbesserung gegenüber der NAF-Methode.
Wir nehmen wieder an, daß r eine nm-Bit Zahl ist. Dann können wir rP wie folgt

schreiben:

$$\begin{aligned} rP &= \sum_{j=0}^{nm-1} c_j 2^j P \\ &= \sum_{j=0}^{n-1} (\sum_{j=0}^{m-1} c_{mi+j} 2^i) 2^{ri} P \\ &= \sum_{j=0}^{r-1} 2^j (\sum_{j=0}^{n-1} c_{mi+j} 2^{ri} P) \\ &= \sum_{j=0}^{r-1} 2^j (\sum_{j=0}^{n-1} c_{mi+j} P_i), P_i = 2^{mi}, 0 \leq i \leq n-1. \end{aligned}$$

Wir erhalten den folgenden Algorithmus, eine Variante der Fenstermethode:

Algorithmus 14 Fenstermethode mit Frobeniusendomorphismus

Input: P
Output: $Q = rP$

1: Vorberechnungen
   $P_0 := P$;
2: **for** $i = 1$ to $n-1$ **do**
3: $P_i = c\pi_{2^m}(P_{i-1}) - \pi_{2^m}^2(P_{i-1})$
   (d.h. $P_i = 2^m P_{i-1} = 2^{mi} P$);
4: **end for**;
5: Eigentliche Rechnung
   $Q := \mathbf{O}$;
6: **for** $j = m-1$ to 0 by -1 **do**
7: $R := \mathbf{O}$;
8: **for** $i = 0$ to $n-1$ **do**
9: $R := R + c_{mi+j} P_i$;
10: **end for**;
11: $Q := R + 2Q$;
12: **end for**;

Schritt 3 erfordert $R(c) + 1$ Additionen, Schritt 9 erfordert im Durchschnitt etwa $mn/3 + m$ Additionen, da $c_j = 0$ mit Wahrscheinlichkeit $\frac{2}{3}$. Damit ergibt sich eine durchschnittliche Komplexität von

$$mn/3 + m + (R(t) + 1)(n-1)$$

Operationen. Wir geben wieder eine Tabelle der günstigen Parameter ($q \leq 2^{12}$) an. Wieder steht der Paramter l für $\lfloor \log r \rfloor$.

q	$t = \pm 1$	$t = \pm 3$	$t = \pm 5$	$t = \pm 7$
2^3	$l + 2$	k.V.	k.V.	-
2^4	$7l/12 + 3$	$13l/12 + 1$	k.V.	k.V.
2^5	$8l/15 + 4$	$14l/15 + 2$	$17l/15 + 9$	k.V.
2^6	$l/2 + 5$	$5l/6 + 3$	$l + 2$	$7l/6 + 1$
2^7	$10l/21 + 6$	$16l/21 + 4$	$19l/21 + 3$	$22l/21 + 2$
2^8	$l1l/24 + 7$	$17l/24 + 5$	$5l/6 + 4$	$23l/24 + 3$
2^9	$4l/9 + 4$	$2l/3 + 6$	$7l/9 + 5$	$8l/9 + 4$
2^{10}	$l3l/30 + 9$	$19l/30 + 7$	$22l/30 + 6$	$5l/6 + 5$
2^{12}	$5l/12 + 11$	$7l/12 + 9$	$2l/3 + 8$	$3l/4 + 7$

Der zweite Algorithmus läßt sich in einigen Fällen noch entscheidend verbessern, falls man statt der charakteristischen Gleichung von π_q die charakteristisch Gleichung für ein $k > 1$ wählt.

Beispiel 6.16. Sei E über $\mathbb{F}_4$ definiert, und die Spur c des Frobeniusendomorphismus π_4 sei gleich eins. Wir gewinnen hier mit der oben beschriebenen Fenstermethode nichts gegenüber der NAF-Methode.
Betrachte nun den Endomorphismus π_4^6. Dieser erfüllt die Gleichung

$$0 = x^2 + 7x + 4^6,$$

d.h. wir berechnen 2^{12} durch $-\pi_{4^6}^2 - 7\pi_{4^6}(P)$. Dafür benötigen wir gerade fünf Operationen auf E. Falls wir nun den Algorithmus mit $m = 12$ und $c = -7$ anwenden, benötigen wir nur $3l/4 + 7$ Operationen auf E.

6.4 Weitere Ideen

In den letzten beiden Abschnitten haben wir die wesentlichsten Ideen zur schnellen Multiplikation auf elliptischen Kurven vorgestellt. In diesem Abschnitt seien noch ein paar kleinere Verbesserungen aufgeführt.

Koblitz [23] empfiehlt eine spezielle Klasse von Kurven, die besonders schnelle Multiplikation erlaubt. Diese Kurven sind supersingulär, lassen also MOV- bzw. Frey-Rück-Reduktion mit einem kleinen k zu. Er rechtfertigt seine Wahl damit, daß dieses k für die vorgeschlagene Kurvenklasse immerhin gleich sechs ist. Damit soll der Körper, in den das Problem reduziert wird, zu groß sein, um es dort auch zu

lösen.
Die Wahl dieser speziellen supersingulären Kurven ist aus zwei Gründen jedoch mit Vorsicht zu genießen:

1. Die MOV-bzw. Frey-Rück-Reduktion an sich läßt sich jedenfalls bei diesen Kurven durchführen und eröffnet somit prinzipiell die Möglichkeit das Problem auf eine zusätzliche Art und Weise anzugehen, auch wenn diese zur Zeit noch keine effiziente Lösung zu geben scheint. Das Logarithmusproblem in $\mathbb{F}_{q^6}$, das sich durch die Reduktion ergibt, ist möglicherweise sogar einfacher als ein beliebiges Logarithmusproblem in $\mathbb{F}_{q^6}$.

2. Supersinguläre Kurven sind ganz spezielle elliptische Kurven mit einer Reihe von besonderen Eigenschaften [50]. Die MOV-Reduktion hat bereits 1992 eine weitere Beschäftigung mit diesen Kurven für kryptographische Forschung uninteressant gemacht. Deshalb mag es gut möglich sein, daß sich aus den besonderen Eigenschaften noch ein anderer, subexponentieller Algorithmus, der etwas tiefliegender als die Weil- bzw. Tate-Paarung ist, zur Berechnung des diskreten Logarithmus ergibt.

Leicht beschleunigen läßt sich die Anwendung der Additionformeln, falls man spezielle elliptische Kurven auswählt.
Für $a = p - 3$ bzw. $a = -3$ und $E : y^2 + x^3 + b$ kann man bei der Punktverdopplung eine Multiplikation im darunterliegenden Körper einsparen [15]. Denn für $2(X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$ ergibt sich

$$\begin{aligned} X_3 &= (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2 \\ Y_3 &= (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_2) - 8Y_1^4 \text{ und} \\ Z_3 &= 2Y_1Z_1. \end{aligned}$$

Für $a \equiv -3 \bmod p$ erhalten wir

$$3X_1^2 + aZ_1^4 = 3(X_1^2 - Z_1^4) = 3(X_1 + Z_1^2)(X_1 - Z_1^2).$$

Wir können also eine der sonst nötigen drei Multiplikationen einsparen. Ob dies aber die spezielle Wahl der Kurve rechtfertigt, ist fragwürdig.

Falls die Kurve über $\mathbb{F}_p$ definiert ist mit Endomorphismenring $\mathcal{O}$ und die Koordinatenbeschreibung von α bekannt ist, gibt es noch einen kleinen Trick, die Multiplikation zu beschleunigen . Dieser wirkt sich besonders dann aus, wenn die Multiplikation mit α schnell durchführbar ist, d.h. wenn Norm(α) klein ist. Nehmen wir

zum Beispiel

$$E : y^2 = x^3 + Bx \text{ mit } B \neq 0$$

und $\alpha = i$ an.
Wir berechnen $P \to rP$. Falls $\text{Norm}(r) = r^2 < p$, dann ermitteln wir rP nach herkömmlichen Verfahren.
Falls $r^2 \approx p^2$, dann gibt es ein $\gamma \in \mathbb{Z}[i]$ mit $\text{Norm}(\gamma) < p$ und $\gamma \equiv r$ auf E. Dieses Element γ ist von der Form

$$a + bi \text{ mit } a^2 + b^2 = p, \quad 0 < |a|, |b| < \sqrt{p}.$$

Der entscheidende Vorteil besteht darin, daß die Multiplikation mit i gegeben durch

$$(x, y) \to (-x, iy), \quad i \in \mathbb{F}_p \text{ mit } i^2 = -1$$

praktisch kostenlos durchführbar ist.
Um Punktverdopplungen einzusparen, können wir Vorberechnungen anstellen. Wir können zum Beispiel alle Punkte $2^i P$ mit $i < \frac{1}{2} \log_2 p$ berechnen. Verwenden wir dann die binäre Methode mit NAF sind zur Berechnung von $r \to rP$ im Durchschnitt nur etwa $\frac{5}{6} \log p$ elliptische Operationen notwendig.

6.5 Fazit

In diesem Abschnitt diskutieren wir, welche der angeführten Algorithmen praktische Relevanz haben und einem Anwender nahegelegt werden können.

- Die Koordinatensysteme des ersten Abschnitts sind vor allem für Kurven, die über Primkörper $\mathbb{F}_p$ definiert sind, interessant. Für Körper $\mathbb{F}_{2^n}$ sollten am besten affine Koordinaten verwendet werden. In Primkörpern kann die Inversion je nach Implementierung allerdings sehr kostspielig sein, und so mag es günstiger sein, sie durch eine Anzahl von Multiplikationen zu ersetzen. Die Wahl eines speziellen Koordinatensystem ist dann ins Auge zu fassen, falls eine Inversion teurer als 11 Multiplikation ist.
  Die beliebten projektiven Koordinaten sind keinesfalls die günstigste Wahl. Hier spielt der Multiplikationsalgorithmus eine große Rolle. Beim gewöhnlichen NAF-Algorithmus (siehe Abschnitt 6.2.2) benötigt man zur Berechnung von $P \to rP$ etwa $\lfloor \log r \rfloor$ Punktverdopplungen und $\lfloor \frac{1}{3} \log r \rfloor$ elliptische Additionen. Hier sind die modifizierten Jacobischen Koordinaten (siehe Seite 75) empfehlenswert, weil sie schnelle Punktverdopplung ermöglichen.

Die Verwendung gemischter Koordinaten bringt eine zusätzliche Beschleunigung (siehe auch Seite 75). Allerdings wird der Algorithmus dadurch auch komplizierter und erfordert größeren programmiertechnischen Aufwand. Ob sich dieser lohnt, hängt von der gegebenen Situation ab. Gegenüber den modifizierten Jacobischen Koordinaten ist hier noch einmal eine Laufzeitverbesserung von etwa zehn Prozent zu erwarten [7].

- Wir vergleichen die Laufzeiten der wichtigsten Algorithmen des zweiten Abschnitts an einigen Beispielzahlen mit Bitlängen $\lambda = 100, 150, 200, 250$ und 500. Für die Fenstermethode und die 2^k-äre Methode wurde w bzw. k immer optimal gewählt. Wir setzen $c_1(w) = 2(2^w - (-1)^w)/3$ und $c_2(w) = 2^{w-1} - 1$. Fenster I sei die gewöhnliche Fenstermethode mit NAF, Fenster II die Fenstermethode nach [25].

Algorithmus	Operationen (Erwartungswert)	100	150	200	250	500
NAF	$4/3\lambda$	133	200	266	333	666
Fenster I	$(\lambda + \frac{31}{12} - w) + \frac{\lambda+\frac{5}{4}}{w+\frac{4}{3}} + \frac{c_1(w)}{2}$	122	181	240	298	587
Fenster II	$(\lambda + \frac{11}{4} - w) + \frac{\lambda+\frac{5}{4}}{w+\frac{3}{2}} + c_2(w)$	124	183	242	301	589
k-näre M.	$c_1(k) + \lambda + (1 - (2/3)^k)(\frac{\lambda}{k})$	129	190	250	310	608

Nach dieser Tabelle ist die gewöhnliche Fenstermethode mit NAF am günstigsten. Falls wir den programmiertechnischen Aufwand etwas einschränken möchten, erweist sich der k-näre Algorithmus mit NAF als vorteilhaft. Diese Algorithmen sind besonders dann empfehlenswert, falls wir Kryptographie in der Punktegruppe über dem gleichen Körper betreiben, über dem die Kurve definiert ist. Denn falls die Kurve bereits über einem Teilkörper definiert ist, gibt es bessere Algorithmen.

- Für Kurven, die über einem Teilkörper definiert sind, haben wir in Abschnitt 6.3 die Frobeniusentwicklung, die q-näre Methode und die Fenstermethode vorgestellt. Die Multiplikation mit der Frobeniusentwicklung benötigt $q/2+k_{q,c}(r)-1$ elliptische Operationen. Dabei ist $k_{q,c}(r)$ die Länge der Frobeniusentwicklung von r. Für spezielle Werte q und c können obere Schranken für $k_{q,c}$ angegeben werden (siehe Tabelle auf Seite 93). Aus dieser liest man ab, daß sich bei einigen Parametern mit der Frobeniusentwicklung die Laufzeit gegenüber herkömmlichen Methoden um einen Faktor größer als zwei verbessern läßt. Für $q = 16$ erhält man zum Beispiel eine Gesamtanzahl von $7+\frac{1}{2}\lambda$ elliptischen Operationen mit $\lambda = \lfloor \log r \rfloor$. Die q-näre Methode und die Fenstermethode aus Abschnitt

6.3 liefern im allgemeinen keine vergleichbar guten Werte. Somit steigert die Frobeniusentwicklung aus [40] die kryptographische Attraktivität der über einem Teilkörper definierten Kurven, deren Punkteanzahl wir ja auch bequem berechnen können (siehe Kapitel zwei).
Zum Vergleich führen wir hier auch noch die Multiplikationszeit auf anomalen binären Kurven auf. Hier gibt es eine Frobeniusentwicklung mit NAF-Eigenschaft. Dadurch beläuft sich die Multiplikationszeit hier nur auf $1/3(\lambda+2)$ mit $\lambda = \lfloor \log r \rfloor$.

- Für Kurven, die über großen Primkörper $\mathbb{F}_p$ definiert sind, aber einen Endomorphismenring mit kleiner Klassenzahl haben, können wir schließlich durch einen kleinen Trick (siehe Seite 100) den Aufwand der Skalarmultiplikation auf etwa $\lfloor 5/6 \log r \rfloor$ elliptische Operationen reduzieren.

6.6 Vorberechnungen

Falls wir einen festen Punkt wiederholt mit verschiedenen Zahlen multiplizieren wollen, bietet sich eine Beschleunigung durch Vorberechnung einiger Vielfachen von P an. Wir fügen dies als Ergänzung an.
Das einfachste Beispiel ist die Berechnung und Speicherung der Punkte $2^i P$, $i = 1, 2, \ldots$ und anschließender Anwendung der binären Methode. Eine andere Idee besteht darin, den Multiplikator r in der Form

$$r = \sum_{i=0}^{l-1} a_i x_i, \quad 0 \le a_i \le h,$$

darzustellen. Diese Summe können wir auch umstellen:

$$\sum_{i=0}^{l-1} a_i x_i = \sum_{d=0}^{h} \sum_{i \cdot a_i = d} x_i,$$

so daß immer x_i's mit gleichen Koeffizienten zusammengefaßt werden. Wir berechnen dann

$$rP = \sum_{d=1}^{h} d \cdot c_d \text{ mit } c_d = \sum_{i \cdot a_i = d} x_i P. \tag{6.5}$$

Dabei können wir die linke Seite Gleichung 6.5 durch

$$\sum_{d=1}^{h} d \cdot c_d = c_h + (c_h + c_{h-1}) + (c_h + c_{h-1} + \ldots + c_{h-2}) + \ldots (c_h + \ldots c_1)$$

ermitteln. Für die Berechnung der c_d's benötigen wir insgesamt $l-1$ Additionen und für $\sum_{d=1}^{h} c_d^d$ nochmals $h-1$ Additionen, also insgesamt $h+l-2$ Additionen.

Algorithmus 15 Algorithmus I mit Vorberechnung

Input: P
Output: $R = rP$
  $Q := \mathbf{O}$;
  $R := \mathbf{O}$;
  for $d = h$ to 1 by -1 **do**
    for each i with $a_i = d$ **do**
      $Q := Q + x_i P$;
      $R := R + Q$;
    end for
  end for

Eine andere Methode, die auf Vektor-Additionsketten basiert (siehe [13]), wird in [34] vorgestellt. Wir schreiben den Multiplikator r in der Form

$$r = \sum_{i=1}^{h-1} 2^{\frac{n}{h}i} s_i + s_0$$

und erhalten eine Tabelle:

	höchstes Bit von s_i	...	niedrigstes Bit von s_i
s_0	$s_{0,\frac{n}{h}-1}$	...	$s_{0,1}$
s_1	$s_{1,\frac{n}{h}-1}$	...	$s_{1,1}$
...	...	...	...
s_{h-1}	$s_{h-1,\frac{n}{h}-1}$	...	$s_{h-1,1}$

Wir ermitteln rP nun spaltenweise. Dabei fassen wir, um die Berechnung zu beschleunigen, immer b-Bit zu einem Block zusammen. Wir erhalten die Punkte

$$P[\overline{e}] = \sum_{i=0}^{h-1} e_i (2^{ivb} P) \text{ mit } 0 \leq e_i \leq 2^b - 1.$$

Hier steht v für die Anzahl der Spalten, und wir setzen $h = \lceil \frac{n}{vb} \rceil$.
Um mehrere Blöcke gleichzeitig bearbeiten zu können, setzen wir

$$P[j, \overline{e}] = P[e]^{jb}, j = 0, 1, \ldots v-1.$$

All diese Werte werden in der Vorberechnung ermittelt.
Sei $e[i]$ der i-te Spaltenvektor, dann gilt

$$rP = \sum_{k=0}^{b-1} 2^k (\sum_{j=0}^{v-1} P[j, e[k+jb]]).$$

Daraus ergibt sich der Algorithmus.

Algorithmus 16 Algorithmus II mit Vorberechnung

Input: P
Output: $Q = rP$
  $Q := \mathbf{O}$
  for $k = b-1$ to 0 by -1 **do**
    $Q := 2 \cdot Q$;
    for $j = v-1$ to 0 by -1 **do**
      $Q := Q + P[j, e[k+jb]]$;
    end for
  end for

In [40] ist nun ein Algorithmus angegeben, der die oben vorgestellte Methode auf die Frobeniusentwicklung anwendet. Der Multiplikator r sei durch die Reihe

$$rP = \sum_{i=0}^{k-1} m_i \pi_q^i(P)$$

gegeben, die wir in

$$\sum_{i=0}^{k-1} m_i \pi_q^i(P) + \sum_{i=0}^{k-k'} m_{i+k'} \pi_q^i(P') = \sum_{i=0}^{k'-1} \pi_q^i(m_i P + m_{i+k'} P') + \sum_{i=2k'}^{k} \pi_q^i(m_i P)$$

mit $k' = \lfloor \frac{q}{2} \rfloor$ und $P' = \pi_q^{k'}(P)$ umformen können.
Bei der Vorberechnung ermitteln wir alle Punkte $iP + jP'$ mit $i, j \in [-q/2, \ldots, q/2]$. Dafür sind $\frac{(q^2+q)}{2} - 1$ elliptische Operationen notwendig. Bei der eigentlichen Berechnung benötigen wir nochmals $k - k' - 1 \approx k/2$ elliptische Operationen. Das sind nun die Hälfte der Operationen des gewöhnlichen Algorithmus mit Frobeniusentwicklung.

Anhang A

Grundlagen aus der algebraischen Zahlentheorie

Sei K ein Zahlkörper und $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. Falls wir dieses Ideal $\mathfrak{p}$ im Ring der ganzen Zahlen $\mathcal{O}_L$ einer endlichen Erweiterung von L betrachten, dann zerfällt es dort in ein Produkt

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \tag{A.1}$$

aus Primidealen $\mathfrak{P}_i$ in $\mathcal{O}_L$. Alle Primideale $\mathfrak{P}_i$ enthalten das Ideal $\mathfrak{p}$. Es gilt $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{p}_i$ für alle i, und $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ heißt der Trägheitsindex von $\mathfrak{p}$ bezüglich $\mathfrak{P}_i$.
Die Größe e_i heißt Verzweigungindex von $\mathfrak{p}$ bezüglich $\mathfrak{P}_i$. Falls $e_i > 1$ für ein $\mathfrak{P}_i$ in Gleichung A.1, dann heißt $\mathfrak{p}$ in $\mathcal{O}_L$ verzweigt, sonst unverzweigt.
Für eine Galoissche Körpererweiterung L von K stimmen alle Verzweigungsindizes e_i und Trägheitsindizes f_i in Gleichung A.1 überein, und es gilt

$$[L : K] = r \cdot e \cdot f, \tag{A.2}$$

mit r aus Gleichung A.1. Die Gleichung A.2 ist ein Spezialfall des Hauptsatzes der algebraischen Zahlentheorie.

Im Ring der ganzen Zahlen eines imaginär quadratischen Zahlkörpers $\mathcal{O}_K$ gibt es im allgemeinen keine eindeutige Primfaktorzerlegung. So gilt zum Beispiel in $\mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Ideale hingegen zerfallen eindeutig ein Primideale. Dies verwenden wir, um zu zeigen, daß Primzahlen in $\mathbb{Z}$ in $\mathcal{O}_K$ eindeutig in Primelemente zerfallen.

Satz A.1. *Sei K ein imaginär quadratischer Zahlkörper. Eine Primzahl p in $\mathbb{Z}$ hat in $\mathcal{O}_K$ eine eindeutige Primfaktorzerlegung.*

Beweis. Wir gehen davon aus, daß p in $\mathcal{O}_K$ zerfällt. Wenn p prim in $\mathcal{O}_K$ ist, ist diese Aussage nicht interessant, und falls p in $\mathcal{O}_K$ zerlegt ist, dann ist $p = 2$ und $K = \mathbb{Q}(i)$.
Betrachte das von p erzeugte Ideal (p) in $\mathcal{O}_K$. Dies hat eine eindeutige Primidealzerlegung, insbesondere gibt es ein $\mathfrak{p}$ das (p) teilt. Die Norm von $\mathfrak{p}$ muß die $Norm(p) = p^2$ teilen. Somit gilt entweder $Norm(\mathfrak{p}) = p$ oder $Norm(\mathfrak{p}) = p^2$. Falls $Norm(\mathfrak{p}) = p^2$, dann folgt schon $\mathfrak{p} = (p)$. Also gilt $Norm(\mathfrak{p}) = p$ und $p = \mathfrak{p}\overline{\mathfrak{p}}$.
Angenommen, es gebe zwei unterschiedliche Primfaktoren p_1, p_2, so daß p_1 und p_2 die Zahl p teilen. Dann teilt das von (p_1) erzeugt Ideal das Ideal (p). Aus der Eindeutigkeit der Primidealzerlegung folgt, daß $(p_1) = \mathfrak{p}$ oder$(p_1) = \overline{\mathfrak{p}}$. Die gleiche Aussage gilt dann auch für das Ideal (p_2). Somit gilt entweder $(p_1) = (p_2)$ oder $(p_1) = (\overline{p_2})$, also $p_1 = \epsilon p_2$ oder $p_1 = \epsilon\overline{p_2}$ für ein $epsilon \in \mathcal{O}_K^*$. Daraus ergibt sich die Behauptung. □

Korollar A.2. *Für eine Primzahl p die in $\mathcal{O}_K$ zerfällt, gibt es nur $2 \cdot \mathcal{O}_K^*$ verschiedene Zahlen in $\mathcal{O}_K$ mit Norm p, falls p in $\mathcal{O}_K$ zerfällt.*

Beweis. Falls p in $\mathcal{O}_K$ zerfällt, dann gibt es ein α mit $Norm(\alpha) = \alpha \cdot \overline{\alpha} = p$. Aus Satz A.1 folgt dann, daß die Zahlen in $\mathcal{O}_K$ mit Norm p durch $\epsilon \cdot \alpha$ und $\epsilon \cdot \overline{\alpha}$ mit $\epsilon \in \mathcal{O}_K^*$ gegeben sind. □

Anhang B

Grundlagen aus der algebraischen Geometrie

Dieser Anhang ist nicht so allgemein wie der voherige und bezieht sich inhaltlich schon direkt auf elliptische Kurven.
Das Ziel dieses Kapitels besteht darin, eine Aussage darüber zu machen, wann

$$Kern(\phi) = Norm(\alpha)$$

gilt, wenn α die imaginär quadratische Zahl ist, die dem Endomorphismus α entspricht. Wir werden sehen, daß der Frobeniusendomorphismus die Gleichung B nicht erfüllt.
Wir führen den wichtigen Begriff der Separabilität von Endomorphismen ein. Zuvor erinnern wir daran, wann eine Körpererweiterung separabel ist.

Definition B.1. *Eine algebraische Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ heißt **separabel**, wenn jedes $a \in \mathbb{L}$ ein Minimalpolynom über $\mathbb{K}$ hat, das in seinem Zerfällungskörper nur einfache Nullstellen hat.*

Definition B.2. *Ein Endomorphismus ϕ von E induziert einen Endomorphismus des Funktionenkörpers $\overline{\mathbb{F}_q}(E)$, der durch*

$$\phi^* : f \to f \circ \phi$$

*gegeben ist. Der **Grad** von ϕ ist der Grad der endlichen Körpererweiterung*

$$\overline{\mathbb{F}_q}(E)/\phi^*(\overline{\mathbb{F}_q}(E)).$$

*Ein Endomorphismus heißt **separabel**, falls die zugehörige Körpererweiterung separabel ist.*

Mithilfe dieser Definition können wir beweisen, daß der Frobeniusendomorphismus π_q Grad q hat (siehe [50], Kapitel II, Theorem 2.11).
Wir machen noch einige weitere Bemerkungen (siehe auch [50], Kap. III, 4,6,9):

Bemerkung B.3.

1. Sei Grad$(\phi) = m$, dann läßt sich zeigen, daß ein $\hat{\phi}$ existiert, so daß $\phi \circ \hat{\phi} = m$ ([50], Kapitel III, Theorem 6.2). Die Abbildung $\phi \to \hat{\phi}$ ist mit der Ringstruktur des Endomorphismenringes verträglich. Außerdem gilt $\hat{\hat{\phi}} = \phi$. Falls nun α die imaginär quadratische Zahl ist, die ϕ entspricht, dann folgt daraus, daß $\hat{\phi}$ durch die Zahl $\overline{\alpha}$ repräsentiert wird. Daraus ergibt sich $Norm(\alpha)$=Grad(ϕ).

2. Der Endomorphismus ϕ ist genau dann separabel, wenn $\#Kern\phi$ =Gradϕ (siehe [50], Kap. III, Theorem 4.10). Wir sehen nun, daß der Frobeniusendomorphismus π_q kein separabler Endomorphismus ist, da hier Kern $\pi_q = \{\mathbf{0}\}$, aber Grad$\pi_q = q$ gilt.

3. Sei E über $\mathbb{F}_q$ definiert, $\pi_q : E \to E$ der q-te Frobeniusendomorphismus und $m, n \in \mathbb{Z}$. Dann ist die Abbildung

   $$m + n\phi : E \to E$$

   separabel genau dann, wenn die Charakteristik p nicht m teilt. Insbesondere ist $1 - \pi_q$ separabel. ([50], Kap. III, Theorem 5.5)

Von folgendem Satz werden wir auch Gebrauch machen (siehe auch [50], Kapitel III, Theorem 4.11):

Satz B.4. *Seien ϕ und ψ zwei Endomorphismen. Angenommen ϕ ist separabel und Kern $\phi \subset$Kern ψ, dann gibt es einen eindeutigen Endomorphismus $\lambda : E \to E$ mit $\psi = \lambda \circ \phi$.*

Wir benötigen in Kapitel 3 noch einen anderen Satz

Satz B.5. *Eine Isogenie zwischen zwei Kurven ist entweder die Nullabbildung oder surjektiv.*

Für einen Beweis siehe [50], Kap.2, Theorem 2.3.

Anhang C

Einige bekannte j-Invarianten

Es gibt nur 13 Ordnungen mit Klassenzahl 1. Für diese sind die j-Invarianten bekannt.

C.1 Tabelle mit j-Invarianten von Ordnungen mit Klassenzahl 1

Die j-Invarianten der Ordnungen mit Klassenzahl 1 sind alle bekannt.

Diskriminante $-D$ von $K = \mathbb{Q} \otimes \mathcal{O}$	Führer f von $\mathcal{O}$	j-Invariante von E
-3	1	0
	2	$2^4 3^3 5^3$
	3	$-2^{15} 3 \cdot 5^3$
-4	1	$2^6 3^3$
	2	$2^3 3^3 11^3$
-7	1	$2^6 5^3$
-11	1	-2^{15}
-19	1	$-2^{15} 3^3$
-43	1	$-2^{18} 3^3 5^3$
-67	1	$-2^{15} 3^3 5^3 11^3$
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$

C.2 Andere j-Invarianten

Weber [60] gibt eine Tabellen mit Klasseninvarianten weiterer Ordnungen an. Dabei verwendet er die Weberschen Funktionen f und f_1, aus denen aber eine der möglichen $h(\mathcal{O})$ zu einander konjugierten j-Invarianten durch folgende Gleichung gewonnen werden kann:

$$j(\tau) = \gamma_2^3 \text{ und}$$
$$\gamma_2 = \frac{f(\tau)^{24} - 16}{f(\tau)^8} = \frac{f_1(\tau)^{24} + 16}{f_1(\tau)^8}.$$

Dabei entspricht $[\tau, 1]$, $\mathrm{Im}(\tau) > 0$ einem echten gebrochenen $\mathcal{O}$-Ideal.

Anhang D

Divisionspolynome

Die Divisionspolynome ermöglichen es, eine Koordinatendarstellung für Endomorphismen $\alpha: \quad P \mapsto rP$ mit $r \in \mathbb{Z}$ anzugeben.

Definition D.1. *Es sei eine elliptische Kurve E über einem Körper der Charakteristik ungleich zwei und drei in der Form*

$$E : y^2 = x^3 + Ax + B \text{ mit } 4A^3 + 27B^2 \neq 0$$

gegeben. Unter den ***Divisionspolynomen*** $\psi_m \in \mathbb{Z}[A, B, x, y]$ *von E verstehen wir die durch Rekursion definierten Polynome*

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

Die Divisionspolynome ermöglichen es, explizite Formeln für die Abbildung

$$P \to r \cdot P$$

zu berechnen.

Satz D.2. *Sei $E : y^2 = x^3 + Ax + B$ eine elliptische Kurve über einem Körper der Charakteristik ungleich zwei und drei, und sei $P = (x_0, y_0)$ ein Punkt auf E. Dann gilt:*

1. *Der Punkt P hat genau dann die Ordnung m, wenn*
   $\psi_m(P) = \psi_m(A, B, x_0, y_0) = 0$.

2. *Das Polynom* $\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2$ *ist durch* y *teilbar. Setze*

$$\Phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \text{ und } 4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

Dann sind auch Φ_m *und* ω_m *Polynome in den Variablen* A, B, x_0 *und* y_0. *Falls* $mP \neq \mathbf{0}$, *dann ist*

$$mP = \left(\frac{\Phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right) = \left(\frac{\Phi_m(A,B,x_0,y_0)}{\psi_m(A,B,x_0,y_0)^2}, \frac{\omega_m(A,B,x_0,y_0)}{\psi_m(A,B,x_0,y_0)^3}\right).$$

Zum Beweis dieses Satzes siehe S. Lang [27].

Anhang E

Ergänzungen zu Kapitel drei

In diesem Anhang geben wir noch zwei Aussagen über elliptische Kurven über endlichen Körpern an. Diese haben keine weiteren Konsequenzen in dieser Arbeit und sind nur für sich interessant.

Lemma E.1. *Zu jedem Endomorphismus $\phi \in End(E(\mathbb{F}_q))$ existiert die gleiche Anzahl von Fortsetzungen zu einem Endomorphismus in $End(E(\mathbb{F}_{q^k}))$.*

Beweis. Sei ψ und $\phi \in End(E(\mathbb{F}_q))$ und ψ_i, $i = 1, \cdots, m$ seien die verschiedenen Fortsetzungen von ψ. Die Abbildung $\psi - \phi$ ist ebenfalls in $End(E(\mathbb{F}_q))$. Fixiere eine Fortsetzung $\widetilde{\phi - \psi} \in End(E(\mathbb{F}_{q^k}))$ von $\psi - \phi$. Dann sind $\phi_i = \psi_i + \widetilde{\phi - \psi}, i = 1, \cdots, m$ verschiedene Fortsetzungen von ϕ. Damit gibt es mehr als m verschiedene Fortsetzungen von ϕ. Die Gleichheit zeigt man nun, indem man die Rollen von ψ und ϕ vertauscht. □

Satz E.2. *Die Menge der Endomorphismen von $E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$, deren Bild in $E(\mathbb{F}_q)$ liegt, bildet ein Ideal in $EndE(\mathbb{F}_{q^k})$, das von der Normabbildung $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ erzeugt wird.*

Beweis. Die erweiterte Normabbildung (Seite 22) ist durch

$$\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(P) = \overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}((x,y)) = \sum_{i=0}^{k-1}(x^{q^i}, y^{q^i})$$

für alle $P \in E(\overline{\mathbb{F}_q})$ definiert. Zunächst zeigen wir, daß die erweiterte Normabbildung $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ separabel ist, da wir Satz B.4 aus Anhang B anwenden wollen.
Es gilt $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q} = 1 + \pi + \pi^2 + \cdots + \pi^{k-1} = \frac{\pi^k - 1}{\pi - 1}$. Damit ergibt sich

$$Grad(\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}) = Norm(\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}) = \frac{(\pi^k - 1)(\overline{\pi^k - 1})}{(\pi - 1)(\overline{\pi - 1})} = \frac{\#E(\mathbb{F}_{q^k})}{\#E(\mathbb{F}_q)} = |Kern(\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q})|.$$

Nach Bemerkung B.3 in Anhang B ist die erweiterte Normabbilung $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ separabel.
Es läßt sich leicht überprüfen, daß die Menge der Endomorphismen von $E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$, deren Bild in $E(\mathbb{F}_q)$ liegt, ein Ideal in $End_{\mathbb{F}_{q^k}}(E)$ ist. Es bleibt zu zeigen, daß dies von Normabbildung $N_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ erzeugt wird.
Wir betrachten zunächst die Menge der Endomorphismen aus $End_{\overline{\mathbb{F}_q}}(E)$, die die Gruppe $E(\mathbb{F}_{q^k})$ auf die Untergruppe $E(\mathbb{F}_q)$ abbilden. Diese bildet ein Ideal I. Nach Korollar 3.13 besteht der Kern von $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ gerade aus den Punkten $P \in E(\mathbb{F}_{q^k})$, die sich in der Form $R - \sigma(R)$ für ein $R \in E(\mathbb{F}_{q^k})$ schreiben lassen. Sei $\phi \in E$ und $P \in Kern(\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q})$. Dann gilt

$$\phi(P) = \phi(R) - \phi(\sigma(R)) = \phi(R) - \sigma(\phi(R)) = 0,$$

da $R \in E(\mathbb{F}_{q^k})$ und somit $\phi(R) \in E(\mathbb{F}_q)$. Aus Satz B.4 aus Anhang B folgt nun, daß die erweiterte Normabbildung $\overline{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ das Ideal I erzeugt.
Da das Ideal der Endomorphismen ψ in $End_{\mathbb{F}_q^k}$ mit $\psi(E(\mathbb{F}_{q^k})) \subseteq E(\mathbb{F}_q)$ durch Reduktion von I modulo $(\pi_{q^k} - 1)$ entsteht, ergibt sich nun die Behauptung. □

Bemerkung E.3. Für den Leser, der mit hyperelliptischen Kurven vertraut ist, erwähnen wir noch, daß sich die Definition der Normabbildung und ihre Eigenschaften auch auf die Jacobi-Varietät einer hyperelliptischen Kurve übertragen lassen. Zur Definition der Jacobi-Varietät siehe [21].
Sei C eine hyperelliptische Kurve, die über $\mathbb{F}_q$ definiert ist. Dann ist die Jacobi-Varietät $J(\mathbb{F}_q)$ aller über $\mathbb{F}_q$ definierten Divisorklassen eine Untergruppe von $J(\mathbb{F}_{q^k})$. Wir können dann analog eine Abbildung definieren, die $J(\mathbb{F}_{q^k})$ in $J(\mathbb{F}_q)$ abbildet.

Literaturverzeichnis

[1] Arno, S., Wheeler, F.S., *Signed Digit Representations of Minimal Hamming Weight*, IEEE Transactions on Computers, Vol 42, No. 8, 1007-1010, 1993

[2] Atkin, A.O.L., *The number of points on an elliptic curve modulo a prime*, unpublished manuscript, 1991

[3] Atkin, A.O.L., Morain, *Elliptic Curves and Primality Proving*, Mathematics of Computation, Vol. 61, 29-68, 1993

[4] Balasubramanian,R., Koblitz,N., *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone Algorithm*, Journal of Cryptology, 141-145, 1998

[5] Cheon, J.H., Park, S., Park, S., Kim, D., *Two efficient Algorithms for the Arithmetic of Elliptic Curves using Frobenius Map*, Advances of Cryptology, Asiacrypt '98, LNCS 1512, 1998

[6] Chudvnovksy, D.V., Chudnovsky, G.V., *Sequences of numbers generated by addition in formal groups and nex primality and factorization tests*, Advances in Applied Math., 7, 385-434, 1986

[7] Cohen, H., Miyaji, A., Taktoshi, O., *Efficient Elliptic Curve Exponentiation Using Mixed Coordinates*, Advances of Cryptology, Asiacrypt '98, LNCS 1512, 1998

[8] Cox, D.A., *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, 1989

[9] Deuring, M., *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg, 197-272, 1941

[10] Frey, G., Müller, M., Rück, H.-G., *The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems*, preprint 1998

[11] Galbraith, S.D., *On the relationship between the discrete logarithm problems on isogenous elliptic curves*, preprint, erhältlich unter http://www.cs.rhbnc.ac.uk/ stevenga/ecc.html, 1998

[12] Gallant, R., Lambert, R., Vanstone, R., *Improving the Parralized Pollard Lambda Search on Binary Anomalous Curves*, preprint, erhältlich unter http://grouper.ieee.org/groups/1363/contrib.html, 1998

[13] Gordon, D.M., *A Survey of Fast Exponentiation Methods*, Journal of Algorithms 27, 129-146, 1998

[14] Guajardo, J., Paar, C., *Efficient Algorithms for Elliptic Curve Cryptosystems*, Advances of Cryptology, Crypto '97, LNCS 1294, 1997

[15] Hasegawa, T., Nakajima, J., Matsui, M., *A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit Microcomputer*, Asiacrypt '98, LNCS 1512, 1998

[16] Hellmann, R.C., Pohlig,S., *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Trans. Information Theory 24, 106-110, 1978

[17] Husemöller, D., *Elliptic curves*, Springer-Verlag, 1987

[18] Itoh, T, Teechai.O, Tsujii,S.,*A fast algorithm for computing multiplicative inverses in GF(2^t) using normal bases*, J. Society for Electronic Communications, 44, 31-36, 1986

[19] Jacobson, M.J., Koblitz, N., Silverman, J.H., Stein, A., Teske, E., *Analysis of the Xedni Calculus Attack*, preprint, erhältlich unter http://www.cacr.math.uwaterloo.ca, Technical Reports, 1999

[20] Knuth, D.E., *Seminumerical Algorithms*, Vol.2, Addison-Wesley, 1981

[21] Koblitz, N., *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998

[22] Koblitz, N., *CM-Curves with Good Cryptographic Properties*, Advances in Cryptology, Crypto 91, LNCS 576, S. 203-209, 1992

[23] Koblitz, N., *An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm*, Advances in Cryptology, Crypto '98, LNCS 1462, 1998

[24] Kohel, *Endomorphism of elliptic curves over finite fields*, Doktorarbeit, University of California, Berkeley, 1996

[25] Koyama, K., Tsuruoka, Y., *Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method*, Advances in Cryptology, Crypto '92, LNCS 740, 1992

[26] Lang, S., *Elliptic Functions*, 2.Auflage, Springer-Verlag, 1987

[27] Lang, S., *Elliptic Curves, Diophantine Analysis*, Springer-Verlag, 1978

[28] Lay, G.-J., Zimmer, H.G., *Constructing Elliptic Curves with Given Group Order over Large Finite Fields*, Proceedings of Algorithmic Number Theory Symposium I, LNCS 877, 250-263, 1994

[29] Lehmann, R., Maurer, M., Müller, V., Shoup, V., *Counting the Number of Points on Elliptic Curves over Finite Fields of Charakteristik Greater than Three*, Proc. of Algorithmic Number Theory Symposium I, LNCS 877, 60-70, 1994

[30] Lenstra, H.W., *Complex Multiplication Structure of Elliptic Curves*, Journal of Number Theory 56, 227-241, 1996

[31] Lenstra, H.W., *Factoring integers with elliptic curves*, Ann. of Math., 126, 649-673, 1987

[32] Lercier, R., *Algorithmique des courbes ellipiques dans les corps finis*, Doktorarbeit, École polytechnique, erhältlich unter http://ultralix.polytechnique.fr/ lercier/english/pub.html, 1997

[33] Lidl, R., Niederreiter, H., *Finite Fields*, Cambridge University Press, Revised edition, 1994

[34] Lim, C.H., Lee, P.J., *More flexible Exponentiation with Precomputation*, Advances in Cryptology, Crypto '94, LNCS 839, 1994

[35] Meier, W., Staffelbach, O., *Efficient Multiplication on Certain Nonsupersingular Elliptic Curves*, Advances in Cryptology, Crypto '92, LNCS 740, 333-344, 1992

[36] Menezes, A., *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993

[37] Miller, V., *Uses of elliptic curves in cryptography*, Advances in Cryptology, Crypto '85, LNCS 218, 1986

[38] Morain, F., Olivos, J. *Speeding up the computations on elliptic curve using addition-subtraction chains*, Theoretical Informatics and Applications, vol. 24, 531-543, 1990

[39] Menezes, A., Okamoto, T., Vanstone, S., *Reducing eliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory, Nr. 39, 1639-1646, 1993

[40] Müller, V., *Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two*, preprint, 1997, wird 1999 in Journal of Cryptology erscheinen

[41] Müller, V., *Efficient Multiplication on Elliptic Curves*, preprint, erhältlich unter http://www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/reports, 1997

[42] Neukirch,J., *Algebraische Zahlentheorie*, Springer-Verlag, 1992

[43] Pollard, J.M., *Monte Carlo methods for index computation (mod p)*, Mathematics of Computation, 32, 918-924, 1978

[44] Prachar, K., *Primzahlverteilung*, Springer-Verlag, 1957

[45] Rück, H.-G., *A note on elliptic curves over finite fields*, Mathematics of Computation, 301-304, 1987

[46] Satoh,T., Araki,K., *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, preprint

[47] Schoof, R., *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation, 44, 483-494, 1985

[48] Schoof, R., *Counting points on elliptic curves over finite fields*, Journal de Théorie des nombres de Bordeaux 7, 1995

[49] Semaev, I., *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Mathematics of Computation 67, 353-356, 1998

[50] Silverman, J.H., *The Arithmetic of elliptic curves*, Springer-Verlag, 1986

[51] Silverman, J.H., *Rational Points on elliptic curves*, Springer-Verlag, 1992

[52] Silverman, J.H., Suzuki J., *Elliptic Curve Discrete Logarithms and the Index Calculus*, Advances in Cryptology, Asia Crypt '98, LNCS 1512, 110-125, 1998

[53] Silverman, J.H., *The Xedni Calculus and the elliptic curve discrete logarithm problem (preliminary version)*, preprint, erhältlich auf der Homepage von J.H.Silverman, 1998

[54] Smart, N., *The discrete logarithms problem on elliptic curves of trace one*, preprint, wird 1999 in Journal of Cryptology erscheinen

[55] Smart, N.,*Elliptic curve cryptosystems over small fields of odd characteristic*, preprint, 1998

[56] Solinas, J.A., *An Improved Algorithm for Arithmetic on a Family of Elliptic Curves*, Advances in Cryptology, Crypto '97, LNCS 1294, 1997

[57] Spallek, A., *Konstuktion einer elliptischen Kurve über einem endlichen Körper zu gegebener Punktegruppe*, Diplomarbeit, Institut für experimentelle Mathematik, Gesamthochschule Essen, 1992

[58] Stark, H.M., *Class-Numbers of Complex Quadratic Fields*, Modular Functions of one Variable I, LNM 320, 1972

[59] Voloch, J., *A note on elliptic curves over finite fields*, Bull.Soc.math.France, 455-458, 1988

[60] Weber, H., *Lehrbuch der Algebra, Band 3*, Vieweg, 1908

[61] Weil, A. *Number of solutions of equations in finite fields*, Bull. Amer. Math.Sci. 55, 497-508, 1949

[62] Weng, A., *Elliptic Curves*, Studienarbeit an der University of Edinburgh, 1998

[63] Wiener, J.M., Zuccherato, R.J., *Faster Attacks on Elliptic Curve Cryptosystems*, preprint, erhältlich unter http://grouper.ieee.org/groups/1363/contrib.html, 1997

[64] Wolfart, J., *Einführung in die Zahlentheorie und Algebra*, Vieweg, 1996