Berechnung elliptischer und hyperelliptischer Kurven für paarungsbasierte Kryptografie

Diplomarbeit
von Patrick Schweitzer

Institut für Mathematik
Technische Universität Berlin

März 2008

Inhaltsverzeichnis

Hiermit versichere ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben.

Berlin, den 9. März 2008

Patrick Schweitzer

Symbolverzeichnis

Kapitel 1

Einleitung

1.1 Geschichtlicher Hintergrund

Elliptische Kurven sind in der Mathematik schon seit Langem bekannt. Ihr Ursprung liegt bei elliptischen Integralen, welche im 19. Jahrhundert untersucht wurden. Auch im 20. Jahrhundert wurde ihnen große Aufmerksamkeit geschenkt. Im Jahre 1949 wurde die berühmte Weil-Vermutung für den Spezialfall von elliptischen Kurven (von Weil selbst) bewiesen. Danach ließ das Interesse an ihnen nach, bis 1985 unabhängig voneinander sowohl Koblitz [Kob87] als auch Miller [Mil86a] erstmals Möglichkeiten vorstellten, elliptische Kurven in der Kryptografie einzusetzen. Der vorgeschlagene Algorithmus wies Ähnlichkeiten mit dem RSA-Algorithmus auf, welcher auf dem diskreten Logarithmusproblem basiert. Im Jahr 1989 wurde dann von Koblitz [Kob89] vorgeschlagen auch hyperelliptische Kurven einzusetzen.

Die ersten Anwendungen von elliptischen Kurven zielten darauf ab, Angriffe auf vorhandene Verschlüsselungsverfahren durchzuführen. Erst im Jahr 1999 wurden von Mitsunari-Sakai-Kasahara und im Jahr 2000 von Sakai-Ohgishi-Kasahara Anwendungen vorgeschlagen, die auch ein Verschlüsseln mittels Paarungen auf elliptischen Kurven ermöglichen. Die ersten Anwendungen nutzten supersingulären elliptischen Kurven. Schnell weiteten sich diese auf elliptischen Kurven und dann auch auf hyperelliptische Kurven aus. Heute, im Jahr 2008, ist die Forschung bezüglich Paarungen auf elliptischen und hyperelliptischen Kurven am blühen, neue Ergebnisse werden fast monatlich veröffentlicht. In 2007 fand eine Konferenz statt, die sich ausschließlich mit dem Thema Paarungen beschäftigte. Ein Trend ist noch nicht abzusehen. So ist noch nicht klar, ob elliptische oder hyperelliptische Kurven vorteilhafter sind. Außerdem wurde erst vor wenigen Monaten eine neue Beschreibung, die Edwards-Koordinaten, für elliptische Kurven entwickelt. Noch ist nicht abzusehen, ob die Weierstraß Koordinaten durch die Edwards-Koordinaten abgelöst werden. Aufgrund der rasanten Entwicklung möchten wir hier als Referenz daher zuerst zwei Internetseiten an-

geben. Die Seite `http://www.isg.rhul.ac.uk/~sdg/ecc.html` gibt einen guten Überblick über die Geschichte der elliptischen Kurven in der Kryptografie, wohingegen sich `http://www.hyperelliptic.org/` den hyperelliptischen Kurven gewidmet hat. Des Weiteren existieren zahlreiche Bücher zu diesem Thema. Als Einstieg ohne mathematische Vorkenntnisse gibt [Kob98] einen groben Überblick. Das wohl umfangreichste Buch über das Thema ist [ACD+06].

Neben dem rein mathematischen Interesse haben elliptische und noch stärker hyperelliptische Kurven auch einen kryptografischen Vorteil: Die verwendete Schlüsselgröße ist gegenüber des RSA-Algorithmus deutlich kleiner. So hat auch die NSA beschlossen die Verschlüsselung mittels des RSA-Algorithmus durch Verschlüsselung mittels Kurven abzulösen, siehe `http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm?MenuID=10.2.7`.

1.2 Rahmen der Arbeit

Auch wenn die Theorie der Paarungen auf elliptischen und hyperelliptischen Kurven weiter fortschreitet und die Algorithmen zu Auswertung der Paarungen immer effizienten werden, bleibt ein Hauptproblem weiter bestehen. In der Theorie der Paarungen werden von Kurven bestimmte Eigenschaften gefordert. Es wir oft davon ausgegangen, dass solche Kurven existieren. Selbst wenn ihre Existenz theoretisch bewiesen werden kann, so wäre die Theorie noch immer nutzlos, wenn sie nicht erzeugt werden können.

Mit der Suche nach Kurven, die für paarungsbasierte Kryptografie geeignet sind, befasst sich diese Arbeit. Zielsetzung war zunächst die Konstruktion von nicht-primen Torsionsgruppenordnungen. Interesse an ihnen entstand auf der Konferenz „EUROCRYPT 2006“ vom 28. Mai bis 1. Juni 2006. Hier wurden zum ersten Mal Anwendungen vorgestellt, deren Kurven mehrere große prime Torsionsgruppen erforderten. Die Zielsetzung wurde im Verlauf der Arbeit erweitert auf die Konstruktion beliebiger hyperelliptischer Kurven. Die elliptischen Kurven wurden unter anderem für eine parallel in Durchführung befindliche Diplomarbeit benötigt. Im Rahmen dieser Arbeit wurde eine Software erstellt, die bei Eingabe beliebiger Anforderungen an die Kurve, unter Nutzung vorhandener und neu entwickelter Algorithmen, eine geeignete Kurve liefert. Vorgeschlagen hierfür war, den Cocks-Pinch- und den Brezing-Weng-Algorithmus zu verwenden und sie für die vorgegebenen Ziele anzupassen. Die Grundlage zur Softwareerstellung bildet das institutseigene Computer Algebra System KASH3.

1.3 Lösungswege und Ergebnisse der Arbeit

Nach Erarbeiten der erforderlichen kryptografischen und algebraischen Grundlagen wurde die Weil-Paarung auf elliptischen Kurven sowie der Cocks-Pinch-Algorithmus in KASH3 implementiert. Der Cocks-Pinch-Algorithmus liefert für

paarungsbasierte Kryptografie geeignete Kurven mit einer großen primen Torsionsgruppe. Dieser Algorithmus wurde dann so weiterentwickelt, dass ein neuer Algorithmus auch Kurven mit zwei großen primen Torsionsgruppen erzeugen kann. Auch der in der Literatur unter Brezing-Weng-Algorithmus bekannte Algorithmus, der Parameter für Scharen von paarungsgeeigneten Kurven liefert, wurde in KASH3 implementiert und ebenfalls so umgeschrieben, dass Scharen von Kurven mit zwei großen Torsionsgruppen erzeugt werden können.

Die Implementierung der Algorithmen für elliptische Kurven führte recht schnell zu einem gewünschten Ergebnis. Die Schwierigkeit lag hier in der Beschleunigung der Algorithmuslaufzeit. Ein weiteres Problem bestand darin aus den durch den Algorithmus gewonnen Parametern, die eigentlichen Kurven zu erzeugen. Für Spezialfälle kann die notwendige Kurvengleichung direkt hingeschrieben werden. In den meisten Fällen jedoch muss zuerst die j-Invariante erzeugt werden. Eine Methode dies zu tun ist im Standard P1363 - Specifications For Public Key Cryptography - der IEEE beschrieben. Dieser ist jedoch missverständlich geschrieben und ein dort angegebenes fehlerhaftes Beispiel erschwerte die Implementierung der Erzeugung der j-Invariante erheblich.

Sowohl der Cocks-Pinch-Algorithmus, als auch dessen Erweiterung liefert eine Vielzahl von Beispielen. Es ist mit dem erstellten Algorithmus also möglich paarungsgeeignete elliptische Kurven zu generieren, die zwei große prime Torsionsgruppen besitzen. Dies ist sowohl für beliebige Einbettungsgrade, als auch für beliebige Fundamentaldiskriminanten problemlos. Der einschränkende Faktor ist letztendlich ausschließlich die Rechenkapazität. Kurven der Ordnung 10^{100} können in durchschnittlich weniger als 5 Minuten gefunden werden. Der Nachteil des Cocks-Pinch-Verfahrens liegt sicherlich im Sicherheitsparameter begründet. Beide Varianten liefern Kurven mit einem Sicherheitsparameter in der Größenordnung von 2, wohingegen 1 als theoretisches Optimum anzustreben ist.

Der Brezing-Weng-Algorithmus setzt hier an, indem durch geschickte Parameterwahl eine Schar von Kurven mit geringerem Sicherheitsparameter erzeugt wird. Die Lösungen des Brezing-Weng-Algorithmus und der erstellten Verallgemeinerung sind in dieser Hinsicht vielversprechend. Versuche aus den Lösungen des Brezing-Weng-Algorithmus und der Verallgemeinerung tatsächliche Kurven mit niedrigem Sicherheitsparameter zu erzeugen, führen zu folgendem Problem: Aus Polynomen mit rationalen Koeffizienten müssen durch Auswertung simultan Primzahlen gewonnen werden. Die durch den Brezing-Weng-Algorithmus erzeugten Polynome lieferten entweder im abgesuchten Bereich keine Lösungen oder nicht simultan Primzahlen, was wiederum den Sicherheitsparameter ungünstigerweise erhöhte. Die Lösungen waren hierdurch schlechter als diejenigen, die der Cocks-Pinch-Algorithmus lieferte. Daher ist für die Erzeugung von einer paarungsgeeigneten elliptischen Kurven der Cocks-Pinch-Algorithmus bzw. dessen Erweiterung, die zwei große prime Torsionsgruppen liefert, zu bevorzugen.

Wir eine Schar von Kurve benötigt, die ungefähr gleichen Sicherheitsparameter besitzen, so sollte der Brezing-Weng-Algorithmus verwendet werden.

Nach einem Vortrag über die Arbeit wurde mit der erweiterten Fragestellung begonnen. Dazu diente ein Anfang des Jahres 2007 von Freeman veröffentlichtes Paper [Fre07b] als Vorlage. Es beschreibt einen Algorithmus zur Generierung hyperelliptischer Kurven von Grad 2 mit ordinärer Jakobischen. Dieser Algorithmus wurde in KASH3 implementiert. Die Aufgabenstellung lautete auch diesen zu verallgemeinern.

Für hyperelliptische Kurven liefert der von Freeman vorgestellte Algorithmus Kurven, deren Sicherheitsparameter größer als 8 ist. Das hyperelliptische Kurven nicht zwingend einen solch großen Sicherheitsparameter besitzen müssen, zeigt ein Beispiel. Es wurde mit dem hier neu entwickelten Algorithmus gewonnenen. Diese Beispielkurve hat jedoch den Nachteil, dass sie eine zu kleine r-Torsionsgruppe ($< 10^6$) besitzt, um auf ihr sichere Kryptografie zu betreiben. Der neue Algorithmus ist durchaus in der Lage Lösungen von relevanter Größenordnung zu finden, benötigt dazu jedoch eine unangemessen große Laufzeit.

Weitere Untersuchungen sind auf dem Gebiet der Erzeugung von hyperelliptischen Kurven notwendig. Hier ist vor allem die Erzeugung von paarungsgeeigneten Kurven höheren Geschlechts, sowie die Erzeugung von Kurven deren Jakobische weder supersingulär noch ordinär ist bedeutsam. Dass dieses Gebiet bei Mathematikern von großem Interesse ist, zeigt auch dessen rasante Entwicklung. Zum einen wurde der im Verlaufe dieser Arbeit neu entwickelte Freeman-Algorithmus aufgegriffen und ist nun Bestandteil dieser Arbeit. Zum anderen wurde zeitgleich zu dieser Arbeit auch von anderen Forschungsgruppen, unter anderem Rubin und Silverberg, eine Verallgemeinerung des Cocks-Pinch-Algorithmus entwickelt.

1.4 Aufbau des Dokumentes

Die vorliegende Arbeit stellt ein zusammenhängendes Werk da, welches mit minimalem Vorwissen die Konstruktion einer paarungsgeeigneten Kurve erklärt, aufbauend auf einem einführenden Algebra-Kurs. Daher wird zunächst in Kapitel 2 eine Einheitliche Notation eingeführt sowie das Konzept von Varietäten und Funktionenkörpern erklärt. Dies wird in Kapitel 3 in Zusammenhang mit elliptischen Kurven gebracht. Das anschließende Kapitel 4 erklärt die Algorithmen, welche eine elliptische Kurve erzeugen. Darauf folgen Kapitel 5, welches die theoretische Einführung bezüglich hyperelliptischer Kurven gibt, und Kapitel 6, das wiederum die Algorithmen beinhaltet. Zu allen vorgestellten Algorithmen befinden sich in Kapitel 7 Beispiele sowie ein kurzer Ausblick. Anhang A beschreibt die benutzen Funktionen welche auf der dort genannten Webseite erhältlich sind.

1.5 Danksagung

Abschließend möchte ich die Gelegenheit nutzen mich bei Prof. Dr. Florian Heß für Themenstellung und die ausgezeichnete Betreuung zu bedanken. Des Weiteren danke ich meinen Korrekturlesern Robert Klinzmann, André Berthe und Vera Reime. Dank gebührt außerdem noch meinen Eltern und insbesondere meinem Bruder Pascal, der mir mit hilfreichen Kommentaren und Korrekturen stets zur Seite stand.

Kapitel 2

Grundlagen

Das Gebiet der elliptischen und hyperelliptischen Kurven und Funktionenkörper ist ein seit langem bekanntes Gebiet der Algebra. Daher gibt es auch eine Vielzahl von Büchern über dieses Thema. Zunächst werden wir Grundlagen der Algebra benötigen, welche wir aus dem Standardwerk Bosch [Bos06] entnommen haben. Daneben werden wir vor allem drei weitere Bücher verwenden. Zum einen ist dies das Handbuch für elliptische und hyperelliptische Kurven in der Kryptografie [ACD+06], welches mit einer in sich abgeschlossenen Einführung auf das Gebiet von Kurven in der Kryptografie beginnt. Den ersten Kapiteln dieses Buches haben wir den roten Faden dieses Kapitels entnommen. Da aber viele Zusammenhänge aus dieser Quelle zu kurz, oder nicht auf die Algorithmen abgestimmt waren, haben wir ausführlichere Erklärungen und Erläuterungen sowohl aus einem Buch von Silverman [Sil86], aus einem Buch von Stichtenoth [Sti93] entnommen oder selbst Erläuterung dazu beigetragen. Hierzu war es notwendig die Notation zu vereinheitlichen. Im Falle von Abweichungen haben wir darauf hingewiesen, sodass alle Bücher durchaus als Nachschlagewerke in Betracht kommen. In diesem Kapitel werden wir im ersten Abschnitt an benötigte Resultate erinnern, die wir als mathematisches Allgemeinwissen ansehen und daran unsere Notation einführen. Danach werden wir uns in 2.2 mit affinen und projektiven Varietäten beschäftigen. In 2.3 werden wir deren Zusammenhang zu Funktionenkörpern erklären, um dann in 2.4 weiter zu Bewertungsringen zu schreiten. Zusammen mit den in 2.5 eingeführten Divisoren, werden Bewertungsringe helfen, Zusammenhänge zwischen Kurven und Funktionenkörpern zu erklären. Dabei zielen speziell die letzten zwei Abschnitte schon darauf ab, hyperelliptische Kurven zu verstehen. Sie sind also die Grundlage der Kapitel 5 und 6.

2.1 Einführung

Zuerst werden wir wichtige grundlegende Definitionen wiederholen, welche zum Teil auch zum Allgemeinwissen gelten. Dennoch existieren zum Teil mehrere

Notationen in der Literatur, daher wollen wir unsere Notation einführen.

Mit K bezeichnen wir einen beliebigen vollkommenen Körper, mit F/K eine Körpererweiterung F über K. Mit $\mathbb{F}_p$, bzw. $\mathbb{F}_q$ bezeichnen wir die endlichen Körper mit $p \in \mathbb{P}$, (d.h. eine Primzahl) bzw. $q = p^n$, $n \in \mathbb{N}$, Elementen.

Definition 2.1.1. (Ganze Zahl, algebraische Zahl) *Sei α eine Nullstelle eines normierten Polynoms über $\mathbb{Z}$. Dann heißt α eine* ganze *oder* algebraische Zahl*, siehe [ACD+06] Definition 2.78.*

Definition 2.1.2. (Ganz abgeschlossenen) *Seien A und B zwei kommutative Ringe (mit 1), wobei $A \subset B$, dann heißt A* ganz abgeschlossen *in B, wenn jedes Element von B das über A ganz ist, auch in A liegt. Mit anderen Worten gibt es keine echte ganze Erweiterung von A, die in B enthalten ist. Ist A ein Integritätsbereich, so heißt A ganz abgeschlossen, wenn A ganz abgeschlossen über seinem Quotientenkörper ist.*

Definition 2.1.3. (Maximalordnung) *Sei K ein Zahlkörper (also ein Körper über $\mathbb{Q}$, was wir mit $K/\mathbb{Q}$ bezeichnen). Dann ist die Menge aller algebraischer Zahlen aus K der Ring der ganzen Zahlen. Dieser wird auch als* Maximalordnung *$\mathcal{O}_K$ (engl.: integer ring of K) bezeichnet, siehe [ACD+06] Definition 2.78.*

Bemerkung 2.1.4. *Sei α eine algebraische Zahl aus K, sodass $\alpha^2 = n$ mit $n \in \mathbb{Z} \setminus \{0, 1\}$ und n quadratfrei ist. Dann ist die Maximalordnung $\mathcal{O}_K$ explizit gegeben durch:*

(a) $\mathcal{O}_K = \mathbb{Z}[\frac{1+\alpha}{2}]$, *falls* $n \equiv 1 \bmod 4$.

(b) $\mathcal{O}_K = \mathbb{Z}[\alpha]$, *falls* $n \equiv 2, 3 \bmod 4$.

Siehe [ACD+06] Beispiel 2.80. Außerdem lässt sich zeigen, dass die Maximalordnung ein Dedekindring ist, oder mit anderen Worten: $\mathcal{O}_K$ ist noethersch, ganz abgeschlossen und jedes von null verschiedene Primideal ist maximal in $\mathcal{O}_K$.

Neben der Maximalordnung existieren natürlich noch weitere Ordnungen. Diese können entweder als Teilmenge der Maximalordnung, welche mit Addition und Multiplikation weiterhin einen Ring bilden, definiert werden, oder wie folgt:

Definition 2.1.5. (Ordnung) *Sei K eine (nicht notwendigerweise kommutative) Algebra, die über $\mathbb{Q}$ endlich erzeugt ist. Eine* Ordnung *R von K ist ein Teilring von K, der als $\mathbb{Z}$-Modul endlich erzeugt ist, welcher außerdem noch $R \otimes \mathbb{Q} = K$ erfüllt, siehe [Sil86] Definition in III.9.*

Starten wir mit einer beliebigen Ordnung von K und suchen eine aufsteigende Kette von Ordnungen, die echt in K enthalten ist, so erhalten wir als stationäres Endglied der Kette gerade die Maximalordnung. Wir werden später kurz zu Ordnungen zurückkehren, siehe Definition 2.4.14. Dieses kleine Beispiel sollte illustrieren, dass gleiche Objekte von unterschiedlichen Standpunkten aus eingeführt werden. Oft ist es unabdingbar, verschiedene Ansichten miteinander zu kombinieren, um zu vernünftigen Resultaten zu gelangen. Im Folgenden werden wir mehrere solcher Standpunkte aufzeigen.

Bevor wir zu komplexeren Strukturen gelangen, verallgemeinern wir aus der Linearen Algebra bekannte Definitionen auf Endomorphismen:

Definition 2.1.6. (Charakteristisches Polynom) *Sei V ein Vektorraum der Dimension n über dem Körper K. Sei $\varphi \in \mathrm{End}_K(V)$ ein Endomorphismus. Weiter sei $M \in K^{n\times n}$ für eine beliebige Basis $v_1, \ldots, v_n$ von V die Darstellungsmatrix bezüglich φ. Es gelte also $(\varphi(v_1), \ldots, \varphi(v_n)) = (v_1, \ldots, v_n)M$. Dann ist $\chi(\varphi)_{V/K} = \det(t \cdot \mathrm{Id}_n - M) \in K[t]$) das* charakteristische Polynom *des Endomorphismus φ. Es ist unabhängig von der gewählten Basis, siehe [Bos06] Kapitel 4.7.*

Definition 2.1.7. (Spur, Norm) *Seien V, K und φ wie eben. Dann besitzt das charakteristische Polynom eine Darstellung der Form $\chi(\varphi)_{V/K} = \sum_{i=0}^{n} a_i t^i$ und die* Spur von φ *ist definiert als:*

$$\mathrm{Tr}_{V/K}(\varphi) = \mathrm{Tr}(M) = a_{n-1}.$$

Des Weiteren definieren wir die Norm *oder auch* Determinante *als*

$$\mathrm{N}_{V/K}(\varphi) = \det(M) = (-1)^n a_0.$$

Siehe [Bos06] Kapitel 4.7.

Bemerkung 2.1.8. *Da jedes Element $a \in F/K$ als Multiplikationsabbildung $a \mapsto ax$ aufgefasst werden kann, induziert a einen Endomorphismus, welchem mit obiger Definition sein charakteristisches Polynom zu geordnet werden kann. Wir erhalten das charakteristische Polynom von a als: $\chi(a)_{V/K}$ und folglich auch die Spur von a als $\mathrm{Tr}_{F/K}(a)$ und die Norm von a als $\mathrm{N}_{F/K}(a)$.*

Für Spur und Norm für Endomorphismen gelten die üblichen Gesetze, siehe [Bos06] Kapitel 4.7 und [ACD+06] Kapitel 2.2.
Die folgenden Strukturen sind weniger geläufig, daher werden wir sie hier erwähnen.

Definition 2.1.9. (Quaternionenalgebra) *Eine* Quaternionenalgebra *ist eine Algebra der Form*

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta,$$

wobei folgende multiplikative Regeln gelten:

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Siehe [Sil86] Kapitel III.9.

Eine weitere fundamentale Eigenschaft für Zahlkörper ist die Signatur. Mittels ihr können wir die Zahlkörper weiter klassifizieren.

Definition 2.1.10. (Rein reelle, rein imaginäre Körpererweiterung) *Sei $K/\mathbb{Q}$ ein Zahlkörper von Grad m. (D.h. $[K/\mathbb{Q}] = m$.) Dann existieren genau m Homomorphismen $\sigma_1, \ldots, \sigma_m$ von K nach $\mathbb{C}$. Ist das Bild eines Homomorphismus σ_i in $\mathbb{R}$ enthalten, so heißt er reeller Homomorphismus, sonst komplexer*

Homomorphismus. Die Signatur (r_1, r_2) *fasst die Anzahl der reellen Homomorphismen* r_1 *und der komplexen Homomorphismen* $2r_2$ *zusammen. Eine Körpererweiterung heißt* rein reell *(engl.: totally real), falls* $r_2 = 0$*, sie heißt* rein imaginär *(engl.: totally complex), falls* $r_1 = 0$.

Bemerkung 2.1.11. *Die Signatur eines Zahlkörpers lässt sich aus den Nullstellen des Minimalpolynoms eines primitiven Elements ablesen. Es besitzt genau* r_1 *reelle und* $2r_2$ *komplexe Nullstellen, siehe [ACD+06] Kapitel 2.2.4.*

Definition 2.1.12. (CM-Körper) *Sei* $K/\mathbb{Q}$ *ein Zahlkörper. Falls ein Zwischenkörper* $K_1/\mathbb{Q}$ *existiert, sodass die Erweiterung* $K_1/\mathbb{Q}$ *rein reell ist und die Erweiterung* K/K_1 *rein imaginär, so heißt* K *ein* CM-Körper.

Definition 2.1.13. (Primitiver CM-Körper) *Besitzt ein CM-Körper keinen echten imaginären Unterkörper, so heißt er* primitiv.

Ein CM-Körper $\mathbb{Q}(\alpha)$ von Grad 2, bezeichnen wir als imaginär-quadratische Körpererweiterung über $\mathbb{Q}$.
Es sei an den chinesischen Restsatz erinnert, welcher ein fundamentaler Bestandteil unserer Algorithmen wird.

Satz 2.1.14. (Chinesischer Restsatz (CRT))
Sei R *ein Ring und seien* $I_1, \ldots, I_n \subset R$ *paarweise teilerfremde Ideale, d.h. es gelte* $I_i + I_j = R$ *für* $i \neq j$ *und* $i, j \in 1, \ldots, n$*. Ist dann* $\pi_i \colon R \to R/I_i$ *jeweils die kanonische Projektion, so ist der Homomorphismus*

$$\varphi \colon R \longrightarrow R/I_1 \times \ldots \times R/I_n, \qquad x \longmapsto (\pi_1(x), \ldots, \pi_n(x))$$

surjektiv und erfüllt $\ker(\varphi) = I_1 \cap \ldots \cap I_n$*. Er induziert also einen Isomorphismus*

$$R/\bigcap_{i=1}^{n} I_i \xrightarrow{\sim} \prod_{i=1}^{n} R/I_i.$$

Dabei bezeichnet $\prod_{i=1}^{n} R/I_i = R/I_1 \times \ldots \times R/I_n$ *das ringtheoretische Produkt der Restklassenringe* R/I_i.

Beweis Siehe [Bos06] Kapitel 2 Satz 12. □

Nach dieser kurzen Wiederholung algebraischer Grundlagen wenden wir uns nun algebraischen Varietäten zu.

2.2 Affine und projektive Varietäten

Die folgenden Definitionen stammen alle aus [Sil86] Kapitel 1.1.

Definition 2.2.1. (Affiner Raum über K) *Sei* K *ein Körper. Der* affine Raum *der Dimension* n *über* K *ist die Menge der Tupel:*

$$\mathbb{A}_K^n := \left\{ P = (x_1, \ldots, x_n) \mid x_i \in \overline{K} \right\}.$$

Wir definieren ihn immer über dem algebraischen Abschluss $\overline{K}$. Stammen die einzelnen Einträge aus einem nicht algebraisch abgeschlossenen Körper $L \subset \overline{K}$, so nennen wir die Menge

$$\mathbb{A}_K^n(L) := \{P = (x_1, \ldots, x_n) \mid x_i \in L\}.$$

die Menge der L-rationalen (affinen) Punkte von $\mathbb{A}_K^n$. Weiter definieren wir:

Definition 2.2.2. (Affine algebraische Menge) *Sei $\overline{K}[X] = \overline{K}[X_1, \ldots, X_n]$ ein Polynomring in n Variablen und $I \subset \overline{K}[X]$ ein Ideal. Dann ist die durch das Ideal definierte Menge*

$$V_I := \{P \in \mathbb{A}_K^n \mid f(P) = 0, \textit{für alle } f \in I\}$$

eine affine algebraische Menge*. Ist andererseits eine affine algebraische Menge V gegeben, so können wir durch*

$$I(V) := \left\{f \in \overline{K}[X] \mid f(P) = 0, \textit{für alle } P \in V\right\}$$

das zugehörige Ideal zurückgewinnen. Das Ideal ist über K definiert, wenn es durch Polynome aus $K[X]$ definiert werden kann. Dies kennzeichnen wir mit $I(V/K)$.

Da $\overline{K}[X]$ ein noetherscher Ring ist, wissen wir, dass alle Ideale endlich erzeugt sind, siehe [Hul00] Kapitel 1.1. Auch hier können wir wieder die Menge der L-rationalen Punkte von V_I definieren und zwar als $V_I(L) = V_I \cap \mathbb{A}_K^n(L)$.

Definition 2.2.3. (Affine Varietät) *Eine affine algebraische Menge V nennen wir eine* affine Varietät*, falls $I(V)$ ein Primideal in $\overline{K}[X]$ ist. Wir sagen die Varietät ist definiert über K, falls $I(V) = I(V/K)\overline{K}[X]$. In diesem Fall reicht es nicht aus lediglich zu überprüfen, ob $I(V/K)$ ein Primideal ist.*

Definition 2.2.4. (Affiner Koordinatenring) *Sei V/K eine über K definierte affine Varietät, dann wird durch*

$$K[V] := K[X]/I(V/K)$$

der affine Koordinatenring *definiert. Der so entstandene Koordinatenring ist stets ein Integritätsbereich.*

Wir wollen nun projektive Varietäten einführen und starten dazu, wie auch bei affinen Varietäten, mit einer Menge von Punkten. Dies ist in [Sil86] Kapitel 1.2 zu finden.

Definition 2.2.5. (Projektiver Raum über K) *Der* projektive Raum $\mathbb{P}_K^n$ über K *mit Dimension n ist definiert durch*

$$\mathbb{P}_K^n := \left\{P = (x_0, \ldots, x_n) \mid (x_0, \ldots, x_n) \in \mathbb{A}_K^{n+1} \backslash (0, \ldots, 0)\right\} / \sim,$$

wobei $\sim$ die Äquivalenzrelation ist, welche durch

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Longleftrightarrow \exists \lambda \in \overline{K}, \textit{sodass für alle } 1 \leq i \leq n : x_i = \lambda \cdot y_i$$

für $(x_0, \ldots, x_n) \neq 0$ *und* $(y_0, \ldots, y_n) \neq 0$ *beschrieben wird. Elemente aus* $\mathbb{P}^n_K$ *heißen* projektive Punkte *und werden mit* $(x_0 : \ldots : x_n) := \{(x_0, \ldots, x_n)\} / \sim = \{(\lambda x_0, \ldots, \lambda x_n)\}$ *mit* $\lambda \in \overline{K}$ *bezeichnet. Dabei heißen die Einträge* $x_0, \ldots, x_n$ homogene Koordinaten.

Auch den projektiven Raum definieren wir immer über dem algebraischen Abschluss $\overline{K}$. Stammen die einzelnen Koordinaten aus einem Erweiterungskörper L mit $K \subset L \subset \overline{K}$, so definieren wir

$$\mathbb{P}^n_K(L) := \left\{(x_0 : \ldots : x_n) \in \mathbb{P}^n_K \mid \exists \lambda \in \overline{K}, \text{sodass für alle } 1 \leq i \leq n : \lambda \cdot x_i \in L\right\}$$

als Menge der L-rationalen projektiven Punkte von $\mathbb{P}^n_K$. Die Definition der L-rationalen affinen Punkte konnte nicht eins-zu-eins übernommen werden, da die projektiven Punkte Äquivalenzklassen sind.

Projektive algebraische Mengen können analog affiner Mengen definiert werden. Um Mengen als offen und abgeschlossen auszeichnen zu können, benötigen wir zusätzlich noch eine Topologie. Die verwendete Topologie ist die Zariski-Topologie und wird wie folgt definiert.

Definition 2.2.6. (Zariski-Topologie) *Sei* $f \in K[X_0, \ldots X_n]$ *ein Polynom, welches homogen von beliebigem Grad ist. (Ein Polynom heißt homogen von Grad* d*, wenn gilt:* $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$*, für alle* $\lambda \in K$*.) Für eine Körpererweiterung* L *über* K *definieren wir den Ausdruck:*

$$D_f(L) := \{P \in \mathbb{P}^n_K(L) \mid f(P) \neq 0\}.$$

Die Mengen $D_f := D_f(\overline{K})$ *sind dann die offenen Mengen der* Zariski-Topologie.

Damit sind auch die abgeschlossenen Mengen eindeutig bestimmt. Charakterisiert werden sie durch von homogenen Polynomen erzeugten Idealen:

Definition 2.2.7. (Projektive algebraische Menge) *Gegeben sei ein Polynomring* $\overline{K}[X] = \overline{K}[X_0, \ldots, X_n]$ *in* $n+1$ *Variablen und* $I \subset \overline{K}[X]$ *ein Ideal. Dann ist die durch das Ideal definierte Menge*

$$V_I := \{P \in \mathbb{P}^n_K \mid f(P) = 0, \textit{für alle } f \in I\}$$

eine projektive algebraische Menge*. Die so erstandenen Mengen sind gerade die in der Zariski-Topologie abgeschlossenen Mengen über* $\overline{K}$*. Ist andererseits eine projektive algebraische Menge* V *gegeben, so können wir durch*

$$I(V) := \left\{f \in \overline{K}[X] \mid f(P) = 0, \textit{für alle } P \in V\right\}$$

das zugehörige Ideal zurückgewinnen.

Auch in diesem Fall können wir die L-rationalen Punkte leicht durch $V_I(L) := V_I \bigcap \mathbb{P}^n_K(L)$. beschreiben. Mit der Kenntnis der Topologie definieren wir weiter:

Definition 2.2.8. (Irreduzible Mengen) *Eine Teilmenge S eines topologischen Raums ist* irreduzibel*, wenn sie sich nicht als Vereinigung zweier echter, abgeschlossener Teilmengen schreiben lässt, d.h. S lässt sich nicht schreiben als $S = S_1 \cup S_2$ mit $S_1, S_2 \subsetneq S$. Außerdem definieren wir die leere Menge als nicht irreduzibel.*

Definition 2.2.9. (Projektive Varietät) *Eine projektive und abgeschlossene Menge V über K nennen wir eine* projektive Varietät *V/K, falls V irreduzibel ist.*

Definition 2.2.10. (Dimension einer Varietät) *Sei V eine projektive (oder affine) Varietät. Dann ist die* Dimension der Varietät *V das Supremum des Indexes aller aufsteigenden Ketten von abgeschlossenen Mengen $S_0 \subsetneq S_1 \subsetneq \ldots \subsetneq S_n$ mit $S_i \subset V$, also $\dim(V) := n$, siehe [ACD+06] Definition 4.17.*

Für den Begriff der Dimension existieren auch andere äquivalente Definitionen. Diese benötigen jedoch den Begriff des Funktionenkörpers, der uns aber erst im nächsten Abschnitt zur Verfügung steht. Nun jedoch können wir den zentralen Begriff der Kurve einführen.

Definition 2.2.11. (Kurve) *Eine Varietät V/K mit Dimension* 1 *heißt* Kurve *und wird mit C/K bezeichnet.*

Aus den vorangegangenen Definitionen wird klar, dass projektive und affine Varietäten eng miteinander verknüpft sind, so haben wir zum Beispiel bei der Definition des projektiven Raums die des affinen Raums ausgenutzt. Wie wir später sehen werden, existiert eine Einbettung des affinen Raums $\mathbb{A}^n_K$ in den projektiven Raum $\mathbb{P}^n_K$. Betrachten wir als Beispiel den affinen Raum der Dimension 1, also $\mathbb{A}^1_K$. Er unterscheidet sich von der projektiven Gerade $\mathbb{P}^1_K$ genau um einen Punkt. Dieser Punkt wird der unendlichferne Punkt genannt und je nach Anwendung mit $\mathcal{O}, P_\infty$ oder ∞ bezeichnet. Auch für die Räume höherer Dimensionen können wir einen solchen Zusammenhang herstellen. Es ist daher nicht verwunderlich, dass manche Autoren bei projektiven, andere bei affinen Räumen beginnen. So existieren auch Lehrbücher, die eine Kurve lediglich als projektive Varietät der Dimension 1 definieren. Wir werden später sehen, dass wir uns oft auf den sogenannten affinen Teil der Kurven beschränken können. Aus dem nächsten Abschnitt wird klar, wie wir eine Kurve aufzufassen haben, wenn wir sie als affine Varietät definieren.

2.3 Funktionenkörper

Aufgrund der Bedeutung des Funktionenkörpers werden wir auch ihn sowohl für affine als auch projektive Varietäten definieren. Beginnen wir mit der Definition für affine Varietäten.

Definition 2.3.1. (Funktionenkörper) *Sei V/K eine affine Varietät V über K. Weiter sei $K[V]$ der affine Koordinatenring, siehe Definition 2.2.4. Dann bezeichnen wir $K(V) := \mathrm{Quot}(K[V])$, den Quotientenkörper von $K[V]$ als* Funktionenkörper von *V/K, siehe [ACD+06] 4.26.*

Möchten wir dagegen den Funktionenkörper für projektive Varietäten erzeugen, ist dies etwas komplizierter. Wir definieren zuerst einen affinen Teil, der die projektive Varietät erzeugt, danach den Koordinatenring und schließlich den Funktionenkörper.

Definition 2.3.2. (Affine Einbettungen) *Die Abbildungen*

$$\begin{aligned} \varphi_i \colon \mathbb{A}_K^n &\longrightarrow U_i := D_{x_i} \subset \mathbb{P}_K^n \\ (x_1, \ldots, x_n) &\longmapsto (x_1 : \ldots : x_i : 1 : x_{i+1} : \ldots : x_n) \end{aligned}$$

nennen wir affine Einbettungen von $\mathbb{A}_K^n$ nach $\mathbb{P}_K^n$.

Der Grund dafür ist, dass $\bigcup_{i=0}^n U_i = \mathbb{P}_K^n$ gilt. Dies liegt daran, dass in der Definition von $\mathbb{P}_K^n$ für jeden Punkt mindestens ein Eintrag immer verschieden von 0 ist; es wird also tatsächlich immer $\mathbb{P}_K^n$ überdeckt. Auch die Umkehrabbildungen

$$\begin{aligned} \varphi_i^{-1} \colon U_i &\longrightarrow \mathbb{A}_K^n \\ (x_0 : \ldots : x_n) &\longmapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}) \end{aligned}$$

sind wohldefiniert. Dies motiviert die folgende Definition.

Definition 2.3.3. (Homogenisierung und Dehomogenisierung) *Sei $f \in K[X_0, \ldots, X_n]$ ein homogenes Polynom von Grad d. Überführen wir $f((x_0 : \ldots : x_n))$ mittels $f((x_0 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n)) = \tilde{f}(x_1, \ldots, x_n)$ nach $K[X_1, \ldots, X_n]$ (Umbenennung der freien Variablen), so nennen wir dies* Dehomogenisierung bezüglich x_i. *Die Umkehrung nennen wir* Homogenisierung bezüglich x_i. *Sie nimmt ein Polynom $g \in K[X_1, \ldots, X_n]$ und überführt es durch*

$$g^*((x_0 : \ldots : x_n)) := x_i^d \cdot g(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$$

mit d minimal, in ein Polynom aus $K[X_0, \ldots, X_n]$, siehe [ACD+06] Kapitel 4.1.1.d.

Diese Bijektionen ermöglichen es eine Beziehung zwischen affinen und projektiven Idealen herzustellen. Sei V eine projektive algebraische Menge welche das zugehörige Ideal $I(V) \subset \overline{K}[X_0, \ldots, X_n]$ besitzt. Dann definiert $V \cap \mathbb{A}_K^n := \varphi_i^{-1}(V \cap U_{x_i})$ unabhängig von i eine affine algebraische Menge, deren Ideal durch $I(V \cap \mathbb{A}_K^n) \subset \overline{K}[X_1, \ldots, X_n]$ gegeben ist. Ist V hingegen eine affine algebraische Menge mit zugehörigem Ideal $I(V)$, so können wir V mittels φ_i in den projektiven Raum $\mathbb{P}_K^n$ abbilden:

$$V \subset \mathbb{A}_K^n \xrightarrow{\varphi_i} \mathbb{P}_K^n.$$

Das homogene Ideal $\overline{I}(V) \subset \mathbb{P}_K^n$ wird generiert durch Homogenisierung: $\overline{I}(V) := \langle \{ f^*(x_0, \ldots, x_n) \mid f \in I(V) \} \rangle$. Dies ermöglicht folgende Definition.

Definition 2.3.4. (Projektiver Abschluss) *Sei V eine affine algebraische Menge mit zugehörigem homogenen Ideal $\overline{I}(V)$. Die dem homogenen Ideal zugehörige Varietät $\overline{V} := V_{\overline{I}(V)}$ wird dann der* projektive Abschluss von V *genannt.*

Folgendes Lemma verdeutlicht die Zusammenhänge:

Lemma 2.3.5. *Sei φ_i eine beliebige affine Einbettung von $\mathbb{A}^n_K$ nach $\mathbb{P}^n_K$. Wir identifizieren $\mathbb{A}^n_K$ mit seinem Bild $\varphi_I(\mathbb{A}^n_K)$. Sei weiter $V \subseteq \mathbb{A}^n_K$ eine affine Varietät, dann ist $\overline{V}$ eine projektive Varietät und es gilt:*

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

Sei $V \subseteq \mathbb{P}^n_K$ eine projektive Varietät, dann ist $V \cap \mathbb{A}^n_K$ eine affine Varietät und es gilt entweder

$$V \cap \mathbb{A}^n_K = \emptyset \text{ oder } V = \overline{V \cap \mathbb{A}^n_K}.$$

Außerdem existiert mindestens ein i, sodass $V \cap \varphi_i(\mathbb{A}^n_K) =: V_{(i)}$ nicht leer ist.

Beweis Siehe [Har97] I.2.3 □

Definition 2.3.6. (Nichtleerer affiner Teil) *Das im vorangegangenen Lemma definierte Varietät $V_{(i)}$ heißt* nichtleerer affiner Teil von V.

Damit können wir nun auch Funktionenkörper für projektive Varietäten definieren.

Definition 2.3.7. (Funktionenkörper) *Sei V/K eine projektive Varietät V über K. Sei $V_{(i)} \subseteq \mathbb{A}^n_K$ ein nichtleerer, affiner Teil von V. Dann wird der* Funktionenkörper von V/K *definiert als:*

$$K(V) := K(V_{(i)}).$$

Bemerkung 2.3.8. *Die Definition des Funktionenkörpers ist unabhängig von dem gewählten nichtleeren, affinen Teil. Lediglich der Koordinatenring $K[V_{(i)}]$ hängt von der gewählten Einbettung ab.*

Nachdem wir Funktionenkörper sowohl für affine als auch projektive Varietäten kennengelernt haben, wenden wir uns nun der Beschreibung von Funktionenkörpern zu.

Definition 2.3.9. (Konstantenkörper) *Sei $K(V)$ ein Funktionenkörper über K. Die maximale algebraische Erweiterung von K in $K(V)$ wird als* Konstantenkörper von $K(V)/K$ *bezeichnet.*

Definition 2.3.10. (Absolut irreduzibel) *Eine projektive (oder affine) Varietät heißt* absolut irreduzibel über K, *falls sie irreduzibel und bezüglich der Zariski-Topologie abgeschlossen ist.*

Lemma 2.3.11. *Eine Varietät V ist genau dann absolut irreduzibel, wenn K der volle Konstantenkörper von $K(V)$ ist.*

Beweis Siehe [Sti93], Korollar III 6.7. □

Neben unserer Definition von Funktionenkörpern existiert in der Literatur auch eine Definition, welche den Begriff von rationalen Funktionen benutzt. Da diese Anschauung für das Verständnis hilfreich ist, werden wir kurz den Zusammenhang zwischen Funktionenkörpern, welche durch Varietäten und deren Ideale definiert sind sowie Funktionenkörpern, die durch rationale Funktionen erzeugt werden, herstellen. Dies werden wir lediglich für affine Varietäten tun, für projektive Varietäten ist dies zu finden in [ACD$^+$06], Kapitel 4.2.2.

Definition 2.3.12. (Morphismus affiner Varietäten) *Ein* Morphismus φ einer affinen Varietät von $\mathbb{A}_K^n$ nach $\mathbb{A}_K^m$ $(n, m \in \mathbb{N})$ *ist gegeben durch ein m-Tupel von Polynomen* $f_i \in K[X_1, \ldots, X_n]$, $1 \leq i \leq m$, *also:*

$$\begin{aligned} \varphi \colon \mathbb{A}_K^n &\longrightarrow \mathbb{A}_K^m \\ P = (a_1, \ldots, a_n) &\longmapsto (f_1(P), \ldots, f_m(P)) \end{aligned}$$

Ein Morphismus einer affinen Varietät $V \subset \mathbb{A}_K^n$ nach $W \subset \mathbb{A}_K^m$ *ist gegeben durch Einschränkung des Definitionsbereichs auf* V *und folglich des Bildbereichs auf* W.

Wir definieren rationale Abbildungen erst nach $\mathbb{A}_K^1$ und erweitern dies dann auf beliebige affine Varietäten.

Definition 2.3.13. (Rationale Abbildung von V nach $\mathbb{A}_K^1$) *Seien* $\psi : U_1 \to \mathbb{A}_K^1$ *und* $\varphi : U_2 \to \mathbb{A}_K^1$ *zwei Elemente aus einem Polynomring für deren Definitionsbereiche zusätzlich gilt, dass* $U := U_1 \cap \{P \in U_2 \mid f(P) \neq 0\}$ *eine nichtleere, offene Teilmenge einer affinen Varietät* V. *Dann definiert* r_U *gegeben durch*

$$\begin{aligned} r_U \colon U &\longrightarrow \mathbb{A}_K^1 \\ P &\longmapsto (\frac{\psi}{\varphi})(P) \text{ mit } \psi, \varphi \in K[X_1, \ldots, X_n] \end{aligned}$$

eine rationale Abbildung von V (mit Definitionsbereich U) nach $\mathbb{A}_K^1$, *siehe [ACD$^+$06] Definition 4.40.*

Definition 2.3.14. (Rationale Funktionen) *Seien* U *und* $\tilde{U}$ *zwei nichtleere, offene Teilmengen einer affinen Varietät* V. *Zwei rationale Abbildungen von* V *nach* $\mathbb{A}_K^1$ *heißen äquivalent, falls für alle* $P \in U \cap \tilde{U}$ *gilt:* $r_U(P) = r_{\tilde{U}}(P)$. *Die Äquivalenzklassen dieser Funktionen heißen* rationale Funktionen.

Nun definieren wir eine allgemeine rationale Abbildung:

Definition 2.3.15. (Rationale Abbildung) *Seien* $V \subset \mathbb{A}_K^n$ *und* $W \subset \mathbb{A}_K^m$ *zwei beliebige Varietäten. Eine* rationale Abbildung von V nach W *ist ein m-Tupel von rationalen Funktionen* $(r_1, \ldots, r_m)$, *mit* $r_i \in K(V)$ *für* $i \in \{1, \ldots, m\}$, *wobei jedes* r_i *einen Repräsentanten* $R_i \in r_i$ *besitzt, der auf einer nichtleeren, offenen Teilmenge* $U \subset V$ *definiert ist und es gilt:* $R(U) := (R_1(U), \ldots, R_m(U)) \subset W$.

Definition 2.3.16. (Birationale Abbildung) *Seien $V \subset \mathbb{A}_K^n, W \subset \mathbb{A}_K^m$ zwei affine Varietäten. Sei R eine rationale Abbildung von V nach W. Dann heißt R* birational, *wenn eine rationale Abbildung $\tilde{R} : W \to V$ existiert mit $R \circ \tilde{R} = \mathrm{Id}_W$ und $\tilde{R} \circ R = \mathrm{Id}_V$. In diesem Fall heißen V und W birational äquivalent und es gilt, dass $K(V)$ und $K(W)$ isomorph sind, siehe [Sti93] Anhang B.5.*

Definition 2.3.17. (Regulär im Punkt P) *Eine rationale Abbildung $f = (f_1, \ldots, f_m)$ von $V \subset \mathbb{A}_K^n$ nach $W \subset \mathbb{A}_K^m$ heißt* regulär im Punkt $P \in V$, *wenn es einen Repräsentanten $\frac{g_i}{h_i} \in f_i$ gibt, sodass h_i in einer offenen Umgebung U von P ungleich 0 ist. Dabei sind g_i und $h_i \in K[X]$ für alle $i \in \{1, \ldots, m\}$, siehe [ACD+06] Definition 4.49.*

Definition 2.3.18. (Reguläre Funktion) *Eine Funktion f ist* regulär, *wenn sie in allen Punkten regulär ist. Mit anderen Worten ist f regulär, wenn f lokal als Tupel von Quotienten von Polynomen dargestellt werden kann. In diesem Fall sagen wir, dass f in allen Punkten P definiert ist und den Funktionswert $f(P) = \frac{g(P)}{h(P)}$ besitzt.*

Bemerkung 2.3.19. *Aus Definition 2.3.18 ergibt sich, dass ein Morphismus eine reguläre Funktion ist.*

Der folgende Satz klärt den Zusammenhang zwischen Funktionenkörpern und rationalen Funktionen:

Satz 2.3.20. (Funktionenkörper und rationale Funktionen)
Die Menge der rationalen Funktionen einer absolut irreduziblen, affinen Varietät V ist isomorph zu dem Funktionenkörper $K(V)$. Die Addition (und Multiplikation) der rationalen Abbildung entspricht der Addition (und Multiplikation) im Funktionenkörper.

Mit dieser Äquivalenz erklärt sich folgende, bei [Sti93] zu findende, Definition, welche mit Satz 2.3.20 trivialerweise äquivalent zu unserer ist.

Definition 2.3.21. (Funktionenkörper (Stichtenoth)) *Ein (algebraischer)* Funktionenkörper F/K *(in einer Variablen) ist eine endliche algebraische Erweiterung von $K(x)$ für ein Element $x \in F$, dass über K transzendent ist.*

Ein Funktionenkörper wird dabei oft als einfache algebraische Erweiterung über dem rationalen Funktionenkörper $K(x)$ dargestellt. D.h.:

$$F = F(x, y) = \mathrm{Quot}(K(x)[T]/(\varphi(T))$$

mit $\varphi(y) = 0, \varphi(T) \in F(x)[T]$. Die genaue Konstruktion des Isomorphismus findet sich in [Sti93] Anhang B.

Dieser Isomorphismus erlaubt uns also die Theorie der algebraischen Funktionenkörper mit Transzendenzgrad 1 zu nutzen. Im folgenden Abschnitt werden wir auch auf die von Stichtenoth [Sti93] eingeführte Definitionen zurückgreifen. Diese benötigen wir, um den Zusammenhang zwischen Abelschen Varietäten höherer Dimensionen und hyperelliptischen Kurven zu erklären. Dieser Sachverhalt gilt - wie wir sehen werden - auch für elliptische Kurven, ist für deren Verständnis aber nicht zwingend notwendig.

2.4 Bewertungsringe

Ist also die Dimension der Varietät größer als 1, so benötigen wir neue Methoden. Wir werden zunächst die Begriffe Gruppe und Varietät miteinander verknüpfen. Wir definieren hierzu:

Definition 2.4.1. (Absolut irreduzible algebraische Gruppe) *Eine* absolut irreduzible, algebraische Gruppe $\mathcal{G}$ über einem Körper K *ist eine (affine oder projektive,) absolut irreduzible Varietät über* K*, zusammen mit zwei Morphismen* m *und* i *sowie einem ausgezeichneten Element* 0*. Formal ist die Gruppe gegeben durch eine Addition (seltener auch Multiplikation):*

$$m\colon \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G},$$

ein Inverses:

$$i\colon \mathcal{G} \longrightarrow \mathcal{G}$$

und ein neutrales Element (d.h. ein K*-rationaler Punkt)*

$$0 \in \mathcal{G}(K).$$

Diese Verknüpfungen müssen die Gruppengesetze erfüllen. Das bedeutet, sie genügen der Assoziativität:

$$m \circ (\mathrm{Id}_{\mathcal{G}} \times m) = m \circ (m \times \mathrm{Id}_{\mathcal{G}}).$$

Sie erfüllen die Eigenschaft des neutralen Elements:

$$m|_{\{0\}\times\mathcal{G}} = p_2,$$

wobei p_2 *die Projektion von* $\mathcal{G} \times \mathcal{G}$ *auf das zweite Argument ist. Und schließlich gilt die Eigenschaft des inversen Elements:*

$$m \circ (i \times \mathrm{Id}_{\mathcal{G}}) \circ \delta_{\mathcal{G}} = c_0,$$

wobei $\delta_{\mathcal{G}}$ *die Diagonalmatrix von* $\mathcal{G}$ *nach* $\mathcal{G} \times \mathcal{G}$ *und* c_0 *die Abbildung, die* $\mathcal{G}$ *auf* 0 *abbildet, ist.*

Es ist eine überraschende Tatsache, dass falls $\mathcal{G}$ eine projektive Varietät ist, m zwingend kommutativ ist. Für affine Varietäten müssten wir dies zusätzlich voraussetzen. Aus diesem Grund werden wir uns in den weiteren Betrachtungen auf projektive Varietäten einschränken und die additive Gruppenschreibweise verwenden, d.h. $m(P,Q) = P \oplus Q, m(P,P) = 2P, i(P) = -P$ für $P, Q \in \mathcal{G}[\overline{K}]$.

Definition 2.4.2. (Abelsche Varietät) *Eine projektive algebraische Gruppe heißt* Abelsche Varietät *und wird im Folgenden mit* $\mathcal{A} := \mathcal{G}$ *bezeichnet.*

Definition 2.4.3. (Einfache Abelsche Varietät) *Eine Abelsche Varietät heißt* einfach*, wenn sie keine echte Unter-Varietät enthält.*

Neben Kenntnissen über Abelsche Varietäten benötigen wir noch das Konzept von Divisoren. Sie werden benötigt, um hyperelliptische Kurven mit einer Gruppenstruktur zu versehen, was wir in 5 tun werden. Auch elliptischen Kurven besitzen eine Gruppenstruktur, sie wird aber leichter durch das Chord-Tangent-Law beschrieben. Daher sind die nächsten zwei Abschnitte nicht zwingend notwendig für das Verständnis von Kapitel 3 und 4.

Diesmal werden wir die Herangehensweise von Stichtenoth nutzen und danach erst die eingeführten Konzepte auf Varietäten übertragen.

Definition 2.4.4. (Bewertungsring (nach Stichtenoth)) *Ein* Bewertungsring *eines Funktionenkörpers F/K ist ein Ring $\mathcal{O} \subseteq F$ mit den folgenden Eigenschaften:*

(a) $K \subsetneq \mathcal{O} \subsetneq F$.

(b) $\forall z \in F, z \in \mathcal{O}$ *oder* $z^{-1} \in \mathcal{O}$.

Daraus folgt, dass Bewertungsringe lokal sind, also ein eindeutiges maximales Ideal $\mathcal{M} = \mathcal{O} \backslash \mathcal{O}^*$ besitzen, wobei $\mathcal{O}^*$ die Einheitengruppe von $\mathcal{O}$ ist. Des Weiteren gilt, dass das maximale Ideal $\mathcal{M}$ ein Hauptideal ist.

Bemerkung 2.4.5. *Die Menge der rationalen Funktionen die regulär in P sind, bilden einen Ring $\mathcal{O}_P$. Auch dieser Ring ist lokal. Er besitzt das eindeutig bestimmte maximale Ideal:*

$$\mathcal{M}_P = \{f \in \mathcal{O} \mid f(P) = 0\}.$$

Wir definieren weiter:

Definition 2.4.6. (Stelle (eines Funktionenkörpers), uniformisierendes Element) *Ein maximales Ideal $\mathcal{M}$ des Funktionenkörpers F/K nennen wir* Stelle*. Jedes Element $t \in \mathcal{M}$, für das $\mathcal{M} = t\mathcal{O}$ gilt, nennen wir* uniformisierendes Element*, lokaler Parameter oder auch Primelement. Außerdem gilt, falls $\mathcal{O}$ ein Bewertungsring von F/K ist und $\mathcal{M}$ das dazugehörige maximale Ideal, dann ist $\mathcal{O}$ schon eindeutig durch $\mathcal{M}$ bestimmt und wird daher oft als Bewertungsring der Stelle $\mathcal{M}$ mit $\mathcal{O}_{\mathcal{M}} := \mathcal{O}$ bezeichnet, siehe [Sti93] Definition I.1.8.*

Damit haben wir gesehen, dass jeder Punkt P ein eindeutig bestimmtes maximales Ideal $\mathcal{M}_P$ besitzt, welches wiederum einen eindeutig bestimmten Bewertungsring $\mathcal{O}_{\mathcal{M}_P} =: \mathcal{O}_P$ besitzt. Wir können also jedem Punkt eindeutig eine Stelle (bzw. einen Bewertungsring) zuordnen.

Leider existiert im Allgemeinen zwischen Punkten und Stellen keine Bijektion. Dies kann aber durch eine Äquivalenzrelation auf Punkten behoben werden. Wir erinnern an die Definition von ganz abgeschlossen, siehe Definition 2.1.2 und definieren:

Definition 2.4.7. (Singuläre und nichtsinguläre Punkte) *Sei P ein Punkt einer projektiven Kurve C. Dann heißt P* nichtsingulär *wenn $\mathcal{O}_P$ ganz abgeschlossen in $K(C)$ ist. Sonst heißt P* singulär*.*

Definition 2.4.8. (Nichtsinguläre Kurve) *Eine Kurve heißt* nichtsingulär *oder* glatt*, wenn jeder Punkt von $C(\overline{K})$ nichtsingulär ist, andernfalls heißt sie singulär, siehe [ACD+06] Definition 4.93.*

Bemerkung 2.4.9. *Da wir mit nichtsingulären Kurven arbeiten werden, interessieren wir uns für Möglichkeiten Singularitäten zu eliminieren. Wir sprechen dabei auch von Desingularisierung oder Aufblasen. Zur Eliminierung der Singularitäten wird dazu ein birationales Äquivalent zur ursprünglichen Kurve gesucht. Hironaka [Hir64] bewies 1964, dass dies für Kurven über Körpern der Charakteristik* 0 *stets möglich ist. Für den allgemeinen Fall (Dimension größer als* 4*) ist dies bis heute ein offenes Problem, siehe auch [Hul00] Kapitel III.2 und [ACD+06] Kapitel 4.2.*

Definition 2.4.10. (Diskrete Bewertung (eines Punktes)) *Sei C eine nichtsinguläre Kurve und $P \in C$. Eine* Bewertung von P *ist gegeben durch:*

$$\begin{aligned} v_P \colon \mathcal{O}_P &\longrightarrow \mathbb{N} \cup \{\infty\} \\ f &\longmapsto v_P(f) = \max\left\{i \in \mathbb{N} \mid f \in (\mathcal{M}_P)^i\right\} \text{ bzw. } v_P(0) = \infty \end{aligned}$$

Die (diskrete) Bewertung wird auf $K(C)$ fortgesetzt, durch $v_P(g/h) = v_P(g) - v_P(h)$, sodass dann die verallgemeinerte Bewertung nach $\mathbb{Z} \cup \{\infty\}$ abbildet, siehe [Sil86] II.2.

Bemerkung 2.4.11. *Sei t ein uniformisierendes Element von P, dann existiert zu jedem Element $z \in K(C)^*$ (d.h. $K(C) \setminus \{0\}$) eine eindeutige Darstellung der Form $z = t^n u$, wobei $u \in \mathcal{O}_P^*$. Die Bewertung v_P kann dann auch definiert werden durch $v_P(z) = n$ und $v_P(0) = \infty$, siehe [Sti93] Theorem I.1.6.*

Definition 2.4.12. (Äquivalente Bewertung) *Zwei Bewertungen v_1 und v_2 eines Funktionenkörpers heißen* äquivalent *falls eine positive Zahl $c > 0$ existiert, für die gilt: $v_1 = c \cdot v_2$, siehe [ACD+06] Kapitel 4.4.1.*

Diese Definition ermöglicht uns das Bilden von Äquivalenzklassen von Bewertungen. Diese Äquivalenzklassen stehen, wie wir gleich sehen werden, in Beziehung mit einem schon bekannten Konstrukt.

Definition 2.4.13. (Stelle (einer Kurve)) *Sei v eine Bewertung von $K(C)$, die trivial auf K ist. (D.h.: $v(a) = 0$ für alle $a \in K$.) Dann heißt die Äquivalenzklasse von v eine* Stelle von $K(C)$ *und wird mit $\mathfrak{p}$ bezeichnet. Die Menge der Stellen von $K(C)/K$ wird mit $\mathbb{P}_{K(C)/K}$ bezeichnet, siehe [ACD+06] Definition 4.97.*

Bemerkung 2.4.14. *Jede Stelle $\mathfrak{p}$ besitzt einen Vertreter deren Wertegruppe $\mathbb{Z}$ ist. Dieser Vertreter heißt* normalisierte Bewertung von $\mathfrak{p}$ *und wird mit $v_\mathfrak{p}$ bezeichnet. Die oben angegebene Bewertung ist die normalisierte Bewertung, siehe [ACD+06] Definition 4.95, und wird auch als Ordnung bezeichnet. In Stichtenoth [Sti93] werden Stellen als $P := \mathfrak{p}$ bezeichnet, die normalisierte Bewertung mit* $\mathrm{ord}_P := v_\mathfrak{p}$.

Von nun an bezeichnen wir mit $v_\mathfrak{p}$ stets die normalisierte Bewertung. Die vorangegangene Bemerkung ermöglicht jetzt auch formal den Zusammenhang zwischen der Definition der Stelle eines Funktionenkörpers und der einer Kurve, welcher für nichtsinguläre Kurven gerade eine Bijektion ist.

Satz 2.4.15. (Verbindung projektiver Kurven und $K(C)$)
Sei C eine glatte, projektive Kurve (Varietät) über einem algebraisch abgeschlossenen Körper K. Dann entsprechen die Stellen des Funktionenkörpers $K(C)$ bijektiv den Äquivalenzklassen der Bewertungen der Punkte von C. ([ACD+06] Lemma 4.98, [Sti93] Anhang B, [Hes06] Kapitel 3)

Konkret bedeutet dies, jede Bewertung von $K(C)$ entspricht einem lokalen Ring, der wie folgt definiert ist:

$$\mathcal{O}_v := \{f \in K(C) \mid v(f) \geq 0\}.$$

Dieser lokale Ring besitzt das maximale Ideal $\mathfrak{m}_v$. Betrachten wir andererseits die Kurve C. Diese ist glatt, somit existiert ein maximales Ideal $M_v \subset K[C_{(i)}]$. Hierbei können M_v und $C_{(i)}$ so gewählt werden, dass zum einen $M_v = \mathfrak{m}_v$ und zum anderen $K[C_{(i)}] \subset \mathcal{O}_v$. Des Weiteren existieren auf der Kurve Punkte $P_1, \ldots, P_d$, deren zugehörige Ordnungen gerade $\mathcal{O}_v = \mathcal{O}_{P_i}$ für alle $i \in 1, \ldots, d$ erfüllen. Für diese Punkte gibt es ein $\sigma \in \mathrm{Aut}_K(\overline{K})$, sodass $\sigma^k(P_j) = P_i$ für alle $1 \leq i, j \leq d$. Wir sagen auch, dass die Punkte einen Galois-Orbit unter $\mathrm{Aut}_K(\overline{K})$ bilden.

Weiter sei angemerkt, dass, falls die Kurve über dem algebraischen Abschluss definiert ist, die Gruppe der $\overline{K}$-Automorphismen trivial ist und es gilt, dass der Galois-Orbit eines Punktes lediglich sich selbst enthält.

Definition 2.4.16. (Gradbewertung) *Sei $\mathfrak{p} = \mathcal{M}$ eine Stelle und $\mathcal{O}$ der dazugehörige Bewertungsring. Weiter seien P_i die Punkte für die $\mathcal{O}_{P_i} = \mathcal{O}$ gilt. Dann ist $F_\mathfrak{p} := (F_{P_i}) := \mathcal{O}/\mathcal{M}$ der Restklassenkörper von $\mathfrak{p}$ bzw. P_i. Diese Definition ist offensichtlich unabhängig von P_i. Die* Gradbewertung einer Stelle $\deg(\mathfrak{p})$ *bzw. von Punkten* $\deg(P_i)$ *ist dann gegeben durch*

$$\deg(\mathfrak{p}) = [F_\mathfrak{p} : K]$$

Zusammenfassend erhalten wir also den folgenden Satz:

Satz 2.4.17. (Zusammenhang Stellen)
Sei C/K eine glatte, projektive, absolut irreduzible Kurve und F/K der dazugehörige Funktionenkörper. Sei φ der Isomorphismus, welcher $F \cong K(C)$ beschreibt und die Elemente aus K unverändert lässt. Dann wird durch φ ebenfalls eine eins-zu-eins Beziehung der Stellen von F/K und der Äquivalenzklassen der Bewertungen der Punkte von C induziert.

Beweis Dieser Satz ergibt sich aus den obigen Definitionen, siehe auch [Sil86] Bemerkung 2.5 oder ausführlicher [Har97] Proposition I.6.9. □

Definition 2.4.18. (Nullstelle, Pol) *Sei $\mathfrak{p}$ eine Stelle und $v_\mathfrak{p}$ seine normalisierte Bewertung. Für $z \in F/K$ als Element aus dem Funktionenkörper sagen wir z besitzt in $P \in \mathfrak{p}$ eine* Nullstelle *(oder $\mathfrak{p}$ ist Nullstelle von f), falls $v_\mathfrak{p}(z) > 0$. Genauso sagen wir z besitzt einen* Pol *in $\mathfrak{p}$ (bzw. $\mathfrak{p}$ ist Pol von f), falls $v_\mathfrak{p}(z) < 0$.*

Bemerkung 2.4.19. *Reguläre Funktionen f sind dadurch charakterisiert, dass $v_{\mathfrak{p}}(f) \geq 0$. Und wir definieren $f(\mathfrak{p}) = f(P)$ für $P \in \mathfrak{p}$. Besitzt f einen Pol in $\mathfrak{p}$, so ist $f(P) = \infty$ für $P \in \mathfrak{p}$.*

Da wir nun sowohl eine Anschauung für das Konzept von Stellen in Funktionenkörpern haben, als auch wissen wie wir Stellen von Kurven aufzufassen haben, können wir von Funktionenkörpern bekannte Konzepte auf Kurven übertragen und umgekehrt. Wir können zum Beispiel die Ordnung einer rationalen Funktion f in $P \in C$ als $v_P(f)$ definieren. Aber auch alle anderen Konzepte wie zum Beispiel die Gradbewertung, oder die noch einzuführenden Divisoren haben eine jeweilige Entsprechung. Um dies noch einmal deutlich zu illustrieren, definieren wir sowohl gebrochene Ideale als auch Idealklassen und ihre Entsprechungen.

Definition 2.4.20. (Gebrochenes Ideal) *Sei C eine glatte affine Kurve, $K(C)$ der zugehörige Funktionenkörper und $R = K[C]$ der Koordinatenring, siehe Definition 2.2.4. Da R ein Dedekindring ist, ist jedes seiner Ideale eindeutig als Produkt von maximalen Idealen darstellbar. Die Menge $B \subset K(C)$ ist ein* gebrochenes R-Ideal*, falls eine Funktion $f \in K(C)^*$ existiert, sodass fB ein Ideal von R ist. Für ein maximales Ideal $M \subset R$ sei v_M die normalisierte Bewertung von M. Dann gilt:*

$$B = \prod_{M \text{ maximal in } R} M^{v_M(B)},$$

und B ist Teilmenge von $\mathcal{O}$ genau dann, wenn für alle maximalen Ideale M von R gilt: $v_M(B) \geq 0$.

Außerdem definieren wir die Idealklassengruppe.

Definition 2.4.21. (Idealklassengruppe) *Zwei Ideale B_1 und B_2 heißen genau dann äquivalent, wenn ein $f \in K(C)$ existiert, mit $v_M(B_1) = v_M(B_2) + v_M(\langle f \rangle)$. Hierbei ist $\langle f \rangle$ das von f erzeugte Ideal. Die Gruppe von R-Idealen heißt* Idealklassengruppe *und wird mit $\mathcal{C}\ell(R)$ bezeichnet. Ihre Mächtigkeit heißt Klassenzahl und wird mit h_D bezeichnet. Wir verstehen unter der Idealklassengruppe eines Körpers die Idealklassengruppe der Maximalordnung $\mathcal{O}$. Die Klassenzahl $|\mathcal{C}\ell(\mathcal{O})|$ kann interpretiert werden als Maß, wie weit $\mathcal{O}$ von einem Hauptidealring entfernt ist und berechnet sich als Anzahl der Ideale modulo Hauptidealen.*

2.5 Divisoren

Um die Entsprechung der Idealklassen zu charakterisieren, führen wir schließlich noch das Konzept von Divisoren ein. Gleichzeitig, oder besser gerade deswegen sind Divisoren der Grundbaustein, der uns dabei helfen wird, für hyperelliptische Kurven eine Gruppenstruktur zu erzeugen.

Definition 2.5.1. (Divisorgruppe) *Sei C/K eine Kurve und F/K ein Funktionenkörper, wobei gelten soll, dass $F \cong K(C)$ und K exakter Konstantenkörper ist. Dann erzeugen die Stellen von F/K eine freie Abelsche Gruppe $\mathcal{D}_C$*

bezüglich F, die Divisorgruppe von F/K. *Wenn der Funktionenkörper und die Kurve klar aus dem Kontext ergeben, wird oft nur $\mathcal{D}$ geschrieben. Ein Element D aus $\mathcal{D}$ heißt* Divisor *und hat die Form:*

$$D = \sum_{\mathfrak{p}_i \in \mathbb{P}_F/K} n_i \mathfrak{p}_i \text{ mit } n_i \in \mathbb{Z} \text{ und } n_i = 0 \text{ für fast alle } i$$

Die n-fache Addition eines Divisors D mit sich selbst bezeichnen wir mit $[n]D$, also $[2]D = D + D$. Die n-fache Punkt- oder Stellenaddition bezeichnen wir dagegen mit nP, also für einen Punkt P ist $P + P = 2P$.

Haben wir die Kurve C über dem algebraischen Abschluss $\overline{K}$ definiert, so entsprechen die Punkte der Kurve eins zu eins ihren Stellen, daher können wir sie auch als formale Summe von Punkten auffassen.

$$D = \sum_{P_i \in C/\overline{K}} n_i P_i \text{ mit } n_i \in \mathbb{Z} \text{ und } n_i = 0 \text{ für fast alle } i$$

Ist C jedoch nicht über $\overline{K}$ definiert, so erhalten wir die zusätzliche Bedingung, dass alle Punkte einer Stelle gleiche Koeffizienten besitzen müssen. D.h. falls $\sigma^k(P_i) = P_j$ für ein $\sigma \in \mathrm{Aut}_K(\overline{K})$ so muss $n_i = n_j$ gelten. Dies ist gleichbedeutend mit folgender Bedingung:

Definition 2.5.2. (L-rationale Divisoren) *Sei C/K eine Kurve, $D \in \mathcal{D}$ ein Divisor ihrer Divisorgruppe sowie L ein Zwischenkörper $K \subseteq L \subseteq \overline{K}$. Die Menge*

$$\mathcal{D}_L = \left\{ D \in \mathcal{D} \mid \sigma(D) = D, \text{für alle } \sigma \in \mathrm{Aut}_L(\overline{K}) \right\}$$

heißt Menge der L-rationalen Divisoren. *Ihre Elemente sind L-rationale Divisoren oder werden als Divisoren, die über L definiert sind, bezeichnet.*

Bemerkung 2.5.3. *Um zu überprüfen, ob D tatsächlich L-rational ist, also dass $\sigma(D) = D = \sum_{P_i \in C}$, genügt es nicht zu überprüfen, ob alle $P_i \in L^2$.*

Nun wollen wir weiter den Grad eines Divisors definieren.

Definition 2.5.4. (Grad eines Divisors) *Sei D ein Divisor einer Kurve C, dann ist der* Grad eines Divisors *definiert durch:*

$$deg(D) = \sum_i n_i \cdot \deg(\mathfrak{p}_i)$$

Ist C gegeben über dem algebraischen Abschluss $\overline{K}$, so vereinfacht sich die Definition, da $\deg(\mathfrak{p}_i) = 1$ und so lediglich alle $n_i \neq 0$ summiert werden. In diesem Fall ist die Summation über Stellen und die Summation über Punkte wieder gleichbedeutend.

Definition 2.5.5. (Primdivisor, effektiver Divisor) *Sei C eine Kurve und F/K ein Funktionenkörper, sodass $F \cong K(C)$. Weiter sei*

$$D = \sum_{\mathfrak{p}_i \in \mathbb{P}_F/K} n_i \mathfrak{p}_i \in \mathcal{D}$$

ein Divisor, dann heißt D Primdivisor *falls gilt $D = \mathfrak{p}$ für ein $\mathfrak{p} \in \mathcal{D}$. Weiter heißt D* effektiv *(oder positiv) falls $n_i \geq 0$ für alle i. Wir schreiben dafür $D \geq 0$.*

Definition 2.5.6. (Träger (Support) eines Divisors) *Sei $D = \sum_{\mathfrak{p}_i \in \mathbb{P}_F/K}$ ein Divisor. Der* Träger *oder auch* Support $\mathrm{Tr}(D)$ *von D ist die Menge aller Stellen für die $n_i \neq 0$. Es gilt also:*

$$D = \sum_{\mathfrak{p}_i \in \mathrm{Tr}(D)} n_i \mathfrak{p}_i.$$

Definition 2.5.7. (Divisor einer Funktion, Hauptdivisor) *Sei C/K eine Kurve und $f \in K(C)^*$ (d.h. $f \in K(C)$ und $f \neq 0$), dann ist der* Divisor einer Funktion *definiert durch:*

$$\begin{aligned}(\cdot)\colon K(C) &\longrightarrow \mathcal{D} \\ f &\longmapsto (f) = \sum_{\mathfrak{p}_i \in \mathbb{P}_{K(C)/K}} v_{\mathfrak{p}_i}(f)(\mathfrak{p}_i)\end{aligned}$$

Auch die Notation $\mathrm{div}(f) := (f)$ *ist üblich. Divisoren, für die eine erzeugende Funktion $f \in K(C)^*$ existiert, heißen* Hauptdivisoren.

Bemerkung 2.5.8. *Die Menge der L-rationalen Hauptdivisoren wird analog zur Menge der L-rationalen Divisoren, siehe Definition 2.5.2 definiert.*

Satz 2.5.9. (Grad eines Hauptdivisors)
Sei C eine glatte Kurve und $f \in \overline{K}(C)^*$. Dann gilt, dass der Divisor eines Elementes aus dem Grundkörper immer gleich 0 ist und Hauptdivisoren stets Grad 0 haben. Formal schreiben wir:

(a) $(f) = 0 \Leftrightarrow f \in \overline{K}^*$.

(b) $\deg((f)) = 0$.

Beweis Siehe [Sil86] Proposition II.3.1. □

Wir können Hauptdivisoren addieren, indem wir die zugehörigen Funktionen multiplizieren, also $(f) + (g) = (f \cdot g)$ für $f, g \neq 0$. Auch die anderen Gruppengesetze lassen sich leicht nachprüfen. So erhalten wir:

Definition 2.5.10. (Hauptdivisorengruppe) *Die Menge der Hauptdivisoren bildet eine (Abelsche) Gruppe. Sie wird als* Hauptdivisorengruppe Princ *bezeichnet.*

Definition 2.5.11. (Nulldivisor, Poldivisor) *Sei C eine glatte Kurve und $f \in K(C)^*$. Sei $\mathfrak{Zer}$ die Menge aller Nullstellen und $\mathfrak{Pol}$ die Menge aller Polstellen von f. Dann heißt*

$$(f)_0 := \sum_{\mathfrak{p}_i \in \mathfrak{Zer}} v_{\mathfrak{p}_i}(f)\mathfrak{p}_i$$

der Nulldivisor von f. *Dabei gilt, dass $v_{\mathfrak{p}_i}(f) > 0$. Analog definieren wir*

$$(f)_\infty := \sum_{\mathfrak{p}_i \in \mathfrak{Pol}} (-v_{\mathfrak{p}_i}(f))\mathfrak{p}_i$$

den Poldivisor von f *mit $-v_{\mathfrak{p}_i}(f) > 0$. Mit anderen Worten gibt es eine Zerlegung von f in zwei effektive Divisoren:*

$$(f) = (f)_0 - (f)_\infty.$$

Der Support von (f) zerlegt sich dabei in die Menge aller Pol- und die Menge aller Nullstellen. Für nicht konstante Funktionen gilt außerdem $\deg((f)_0) = \deg((f)_\infty) = [K(C) : K(f)]$, *siehe [ACD+06] Proposition 4.104 und [Sti93] Proposition I.4.11.*

Abschließend können wir nun die Picard-Gruppe definieren. Sie besitzt die nötige Abelsche Gruppenstruktur, um auch auf hyperelliptischen Kurven Kryptografie zu betreiben.

Definition 2.5.12. (Picard-Gruppe) *Sei $\mathcal{D}$ die Gruppe aller Divisoren einer Kurve C und $\mathcal{D}^0$ die Untergruppe aller Divisoren von Grad* 0. *Sei weiter* Princ, *die Gruppe der Hauptdivisoren. Da sowohl, $\mathcal{D}, \mathcal{D}^0$ als auch* Princ *Abelsch sind und außerdem gilt* $\text{Princ} \subset \mathcal{D}^0 \subset \mathcal{D}$, *definieren wir*

$$\text{Pic}_C := \mathcal{D}^0 / \text{Princ}$$

als Divisorklassengruppe von Grad 0 *oder auch* Picard-Gruppe. *Die Elemente hieraus werden auch Divisorklassen genannt. Zwei Divisoren D und D' heißen äquivalent, falls sie sich nur um einen Hauptdivisor unterscheiden:*

$$D \sim D' \Leftrightarrow D - D' = (f) \text{ mit } f \in K(C)$$

Definition 2.5.13. (Picard-Gruppe der L-rationalen Divisorklassen) *Sei C/K eine Kurve und* Pic *ihre Picard-Gruppe. Für L mit $K \subseteq L \subseteq \overline{K}$ definieren wir* $\text{Princ}(L)$ *und $\mathcal{D}^0(L)$ in der offensichtlichen Weise. Wir können zeigen, dass* $\text{Princ}(L)/\mathcal{D}^0(L) \cong \text{Pic}(L)$ *gilt und dass* $\text{Pic}(L)$ *eine Untergruppe von* Pic *ist. Sie wird als* Picard-Gruppe der L-rationalen Divisorklassen *bezeichnet.*

Stellen wir nun abschließend den Zusammenhang der in diesem Kapitel erarbeiteten Begriffe dar.

Bemerkung 2.5.14.

$$1 \to \overline{K}^* \to \overline{K}(C) \to \mathcal{D}^0(C) \to \mathrm{Pic}(C) \to 0$$

bildet eine exakte Sequenz, siehe [Sil86] Bemerkung 3.4. Sie bildet das Analogon zu der fundamentalen exakten Sequenz der algebraischen Zahlentheorie. Für einen Zahlkörper K gilt:

$$1 \to \text{ Einheiten von } K \to K^* \to \text{ gebrochene Ideale von } K \to \mathcal{C}\ell(K) \to 1$$

Dabei existiert ein Homomorphismus zwischen den entsprechenden Elementen der ersten und der zweiten Sequenz. Zwischen $\mathrm{Pic}(C)$ *und* $\mathcal{C}\ell(K)$ *ist dieser Homomorphismus surjektiv. Im optimalen Fall ist dieser Homomorphismus auch injektiv, stellt also einen Isomorphismus dar. Wir verzichten hier auf Details, siehe [ACD+06] Proposition 4.140, möchten aber festhalten, dass für elliptische und hyperelliptische Kurven, die in Kapitel 3 und 5 einführt werden, dies immer ein Isomorphismus ist.*

Dieser Zusammenhang zwischen der Varietäten, Divisoren und der Idealtheorie in Dedekindringen, welchen wir in Kürze dargestellt haben, ermöglicht also stets zwei grundlegend verschiedene Betrachtungsweisen. Einerseits kann mittels der Idealklassengruppen die Arithmetik (zum Beispiel in KASH3) durchgeführt werden, andererseits liefern die Divisorklassengruppen (oder im elliptischen Fall die Punkte) den geometrischen Hintergrund sowie den strukturellen Gruppenhintergrund.

Kapitel 3

Elliptische Kurven

In Kapitel 2 haben wir in Definition 2.2.11 den Begriff einer Kurve als affine bzw. projektive Varietät der Dimension 1 definiert. Ferner haben wir die Begriffe nichtsinguläre, absolut irreduzible sowie projektive Kurve kennengelernt. Dieses Kapitel beginnen wir damit, das Geschlecht einer Kurve einzuführen, damit wir elliptische und hyperelliptische Kurven definieren können. Weiter werden wir dann Eigenschaften, die speziell für elliptische Kurven gelten, entwickeln. Die meisten Eigenschaften lassen sich zwar auf hyperelliptische Kurven übertragen, jedoch sind diese oft komplizierter oder lassen sich nur durch eine deutlich komplexere Notation beschreiben, sodass sich eine geringfügige Redundanz in Kapitel 5 nicht vermeiden lässt. Nach der Abgrenzung der elliptischen Kurven werden wir in Abschnitt 3.2 den Zusammenhang zwischen elliptischen Funktionenkörpern und elliptischen Kurven herstellen. Danach werden wir in 3.3 erklären, was wir unter einem Morphismus von elliptischen Kurven verstehen. In 3.4 werden wir die Diskriminante eines CM-Körpers erklären, um dann in 3.5, aufbauend auf den beiden Abschnitten zuvor, sowohl Endomorphismenringe zu erklären als auch den Zusammenhang zu CM-Körpern zu verdeutlichen. In 3.6 werden wir weitere Eigenschaften von elliptischen Kurven herstellen, die wir in 3.7 und 3.8 verwenden, um die elliptischen Kurven in einen kryptologischen Kontext zu interpretieren.

3.1 Geschlecht einer Kurve

In diesem Abschnitt definieren wir das Geschlecht einer Kurve. Mithilfe des Geschlechts können wir elliptische und hyperelliptische Kurven voneinander unterscheiden. Dazu benötigen wir zunächst den Satz von Riemann-Roch. Der Satz ist ein zentrales Ergebnis der algebraischen Geometrie. Deswegen ist es nicht verwunderlich, dass in der Literatur verschiedene Herleitungen existieren, siehe [Sil86] Kapitel II.5, [Sti93] Kapitel I.5 sowie [ACD$^+$06] Kapitel 4.4.2. Wir werden hier weitestgehend [ACD$^+$06] folgen.

Ausgehend vom Begriff des effektiven Divisors, siehe Definition 2.5.5, definieren wir eine Halbordnung auf der Gruppe der Divisoren. Analog zur Schreibweise $D \geq 0$ schreiben wir für zwei beliebige Divisoren $D_1 \geq D_2$, falls $D_1 - D_2$ effektiv ist. Damit definieren wir:

Definition 3.1.1. (Riemann-Roch-Raum) *Sei $K(C)$ der Funktionenkörper einer Kurve C und $D \in \mathcal{D}$ ein Divisor ihrer Divisorgruppe. Dann bezeichnet der Vektorraum*

$$\mathcal{L}(D) := \{ f \in K(C)^* \,|(f) \geq -D \} \cup \{0\}$$

den Riemann-Roch-Raum von D. *Weiter definieren wir die Dimension des Riemann-Roch-Raums als*

$$\ell(D) := \dim_K \mathcal{L}(D).$$

Der folgende Satz von Riemann-Roch gibt nun Auskunft über den Zusammenhang zwischen der Dimension $\ell(D)$ des Riemann-Roch-Raums von D und dem Grad $\deg(D)$ des Divisors D.

Satz 3.1.2. (Riemann-Roch)
Sei C eine absolut irreduzible, glatte Kurve mit Funktionenkörper $K(C)$. Dann existiert eine natürliche Zahl $g \geq 0$, sodass für jeden Divisor $D \in \mathcal{D}$ gilt:

$$\ell(D) \geq \deg(D) - g + 1$$

Für alle D mit $\deg(D) > 2g - 2$ gilt sogar Gleichheit.

Beweis Siehe [Sil86] Theorem 5.4 oder [Sti93] Proposition I.5.15. □

Bemerkung 3.1.3. *Der Satz von Riemann-Roch kann auch mittels Differentialen und daraus resultierenden kanonischen Divisoren angegeben werden, auch bei den oben angegebenen Quellen zu finden. Dies hat den Vorteil, dass auch für Divisoren beliebigen Grades eine Gleichheitsbedingung existiert. Da wir diese im Folgenden aber nicht benötigen, verzichten wir darauf.*

Der Satz von Riemann-Roch impliziert das Geschlecht einer Kurve:

Definition 3.1.4. (Geschlecht einer Kurve) *Gelten Voraussetzungen von Satz 3.1.2, dann heißt die eindeutig bestimmte Zahl g Geschlecht von $K(C)$, bzw. das geometrische Geschlecht von C. Ist C zusätzlich projektiv und nichtsingulär, so nennen wir g das* Geschlecht der Kurve C, *siehe [ACD+06] Theorem 4.106 oder [Sil86] Theorem 5.4.*

Dies ermöglicht es uns eine elliptische Kurve zu definieren:

Definition 3.1.5. (Elliptische Kurve) *Eine* elliptische Kurve E/K *ist eine nichtsinguläre, absolut irreduzible, projektive Kurve über K, welche Geschlecht* 1 *und mindestens einen K-rationalen Punkt besitzt, siehe [ACD+06] Definition 4.111. Ist das Geschlecht größer als* 1, *so bezeichnen wir sie als hyperelliptische Kurve, siehe hierzu Definition 5.1.1.*

3.2 Elliptische Funktionenkörper und Kurven

Mit der Kenntnis des Begriffs *elliptische Kurve*, wollen wir zu Funktionenkörpern zurückkehren. Hier bietet [Sil86] Kapitel III eine sehr ausführliche Darstellung. Dieser Abschnitt soll erklären, weshalb unter einer elliptischen Kurve vielfach lediglich eine Gleichung der Form $y^2 = x^3 + ax + b$ verstanden wird. Sie stellt zwar nicht mehr die allgemeinste Form einer elliptischen Kurvengleichung dar, ist jedoch ausreichend für spätere Betrachtungen. Um diese Form zu erhalten, werden wir die Einschränkung vornehmen, dass wir elliptische Kurven nur über Körpern betrachten, deren Charakteristik verschieden von 2 und 3 ist.

Definition 3.2.1. (Elliptischer Funktionenkörper) *Sei K ein voller Konstantenkörper des algebraischen Funktionenkörpers F/K. Dann heißt F* elliptischer Funktionenkörper*, falls gilt:*

(a) Das Geschlecht von F/K ist gleich 1.

(b) Es existiert ein Divisor $D \in \mathcal{D}_F$ mit $\deg(D) = 1$.

Bedingung (b) ist immer erfüllt, falls K algebraisch abgeschlossen oder K ein endlicher Körper ist, siehe [Sti93] Definition VI.1.1.

Nun können wir die definierende Gleichung einer elliptischen Kurve herleiten.

Satz 3.2.2. (Die Gleichung einer elliptischen Kurve)
Sei C/K eine elliptische Kurve und $K(C) \cong F$ der dazugehörige elliptische Funktionenkörper. Dann existieren Funktionen $x, y \in F$, sodass $F = K(x, y)$, wobei x und y folgende Beziehung erfüllen:

$$C\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ mit } a_i \in K. \tag{3.1}$$

Dies ist die Gleichung einer absolut irreduziblen affinen Kurve in der Ebene in Weierstraß-Normalform.

Zunächst einige Bemerkungen.

Bemerkung 3.2.3. *(a) Die Indizes in Gleichung (3.1) sind historisch bedingt. Es gilt, dass x eine Polstelle der Ordnung* 2 *und y eine Polstelle der Ordnung* 3 *besitzt. Der jeweilige Index gibt an, wie viel die Ordnung des Summanden von* 6*, der maximalen Ordnung, abweicht.*

(b) Ist C gegeben durch eine Weierstraß-Normalform, werden wir von nun an E statt C schreiben. Dies soll kennzeichnen, dass es sich um eine elliptische Kurve in Weierstraß-Normalform handelt.

Beweis Der Beweis folgt [Sti93] Proposition VI.1.2, ist aber abgewandelt und deutlich ausführlicher. Zunächst bemerken wir, dass $g = 1$ gilt. Damit folgt in Satz 3.1.2 Gleichheit für Divisoren, deren Grad größer als 0 ist. Außerdem existiert nach Definition der elliptischen Kurve ein K-rationaler Punkt P. Da

der unendlichferne Punkt P_∞ stets K-rational ist, können wir auch diesen betrachten. Ist C über dem algebraischen Abschluss definiert, so ist P gleichzeitig der geforderte Divisor von Grad 1 aus der Definition des elliptischen Funktionenkörpers. Anderenfalls muss er zuerst konstruiert werden, siehe 2.5. Sei also P ein beliebiger K-rationaler Punkt. Für diesen gilt dann nach dem Satz von Riemann-Roch mit $g = 1$ sogar der Gleichheitsfall $\ell(P) = 1$. Es gilt sogar $\ell(i \cdot P) = i$. Folglich haben wir:

$$\mathcal{L}(0) \subseteq \mathcal{L}(P) \subset \mathcal{L}(2 \cdot P) \subset \ldots \subset \mathcal{L}(i \cdot P) \subset \mathcal{L}((i+1) \cdot P) \subset \ldots,$$

wobei die Inklusionen für $i > 0$ aufgrund der steigenden Dimensionen strikt sind. Nun suchen wir für die Riemann-Roch-Räume eine Basis. Die Menge $\mathcal{L}(0) = \{f \in K(C)^* \mid (f) \geq 0\} \cup \{0\}$ besteht also aus allen Funktionen, die nach Definition 2.5.11 keine Polstellen und demnach, aufgrund der Gradgleicheit von Pol- und Nulldivisor, auch keine Nullstellen besitzen. Die Funktionen ohne Polstellen und ohne Nullstellen sind aber gerade die konstanten Funktionen. Somit ergibt sich $\mathcal{L}(0) = K = \{\langle 1 \rangle\}$. Weiter haben wir $\ell(P) = 1$ und $\dim_K(K) = 1$, also $\mathcal{L}(P) = K$. Da $\ell(2 \cdot P) = 2$ können wir ein Element $x \in \mathcal{L}(2P) \backslash K$ wählen. Somit ist eine Basis von $\mathcal{L}(2P)$ gegeben durch $\{1, x\}$. Aufgrund der Definition des Riemann-Roch-Raumes hat dieses Element einen Poldivisor $(x)_\infty = [2](P)_\infty$. Analog wählen wir für $\mathcal{L}(3P)$ ein Element $y \in \mathcal{L}(3P) \backslash \mathcal{L}(2P)$ mit Poldivisor $(y)_\infty = [3](P)_\infty$, die Basis nun gegeben durch $\{1, x, y\}$. Nun besagt Definition 2.5.11, dass für $f \in F$ gilt: $\deg((f)_\infty) = [F : K(f)]$, also hier speziell $[F : K(x)] = 2$ und $[F : K(y)] = 3$. Da K Unterkörper von F ist, kann dann nur gelten $[F : K(x, y)] = 1$ bzw. $F = K(x, y)$. D.h. wir haben nun zwei Elemente x und y gefunden, die den Funktionenkörper erzeugen, vergleiche auch Satz 2.3.20. Bleibt noch zu zeigen, dass diese die vorgeschriebene Gleichung (3.1) erfüllen.

Dazu betrachten wir x^2, welches über K linear unabhängig zu $\{1, x, y\}$ ist. Dies können wir sehen, indem wir zum Beispiel die Grade der Poldivisoren betrachten. Da nun Hauptdivisoren eine Gruppenstruktur aufweisen, gilt $(x^2) = [2](x)$, also $x^2 \in \mathcal{L}(4P)$, was aber bedeutet, dass $\left\{1, x, y, x^2\right\}$ eine Basis für $\mathcal{L}(4P)$ ist. Betrachten wir wiederum die Poldivisoren, erhalten wir mit dem gleichen Argument die Basis von $\mathcal{L}(5P)$ als $\left\{1, x, y, x^2, xy\right\}$. Weiter gilt für $(y^2)_\infty = (x^3)_\infty = [6](P)_\infty$, somit erhalten wir, dass $\left\{1, x, y, x^2, xy, x^3, y^2\right\}$ ein Erzeugendensystem von $\mathcal{L}(6P)$ ist. Da $\ell(6P) = 6$ folgt aber, dass diese Funktionen linear abhängig sind.

Nun müssen wir lediglich noch zeigen, dass die Koeffizienten vor x^3 und y^2 nicht verschwinden und gleichzeitig zu 1 normiert werden können. Würde der Koeffizient von y^2 verschwinden, könnten wir y als rationale Funktion in x ausdrücken. Dies steht aber im Widerspruch zu $[F : K(x, y)] = 1$ und $[F : K(x)] = 2$. Würde der Koeffizient vor x^3 verschwinden, wären beide Seiten der Gleichung quadratisch. Durch quadratische Ergänzung der Terme in x und y erhalten wir eine Gleichung der Form: $(y - \alpha)^2 = (x - \beta)^2 + \gamma$ mit $\alpha, \beta, \gamma \in K$.

Dies bedeutet $[K(x) : K] = [K(y) : K] = 2$ und steht im Widerspruch zu $3 = [F : K(y)] \neq [F : K(x)] = 2$.

Gegeben ist nun also eine Gleichung der Form:

$$by^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6 \text{ mit } a_i, b \in K \text{ und } ba_0 \neq 0$$

Ersetzen wir y durch ba_0^2y und x durch ba_0x, teilen anschließend durch $b^3a_0^4 \neq 0$ und benennen die Variablen um, so erhalten wir mit normiertem x^3 und y^2, die Weierstraß-Normalform, Gleichung (3.1). □

Satz 3.2.4. (Elliptische Kurven und Projektive Koordinaten)

(a) Homogenisieren der Gleichung (3.1), liefert eine Gleichung einer projektiven Kurve in der Ebene, den projektiven Abschluss $\overline{E}$:

$$\overline{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \text{ mit } a_i \in K, \tag{3.2}$$

Dabei gilt $\overline{E} \backslash E = P_\infty$: Die projektive Gleichung beschreibt zusätzlich genau einen weiteren Punkt, den unendlichfernen Punkt $P_\infty = \mathcal{O}$. Dehomogenisierung der projektiven Gleichung liefert wieder eine affine Gleichung. Auch dann gilt, dass sie sich lediglich um einen Punkt unterscheiden.

(b) Ebenfalls gilt: Ist eine affine oder projektive Gleichung (3.1) oder (3.2) gegeben, so ist sie genau dann definierende Gleichung einer nichtsingulären, absolut irreduziblen Kurve, wenn sie keine mehrfachen Nullstellen besitzt.

Beweis Teil *(a)* ergibt sich aus den Vorbetrachtungen zu [ACD$^+$06] Theorem 4.112, für *(b)* verweisen wir auf [Sil86] Proposition III.3.1(c). □

Wir können auch *(a)* und *(b)* gemeinsam auffassen und verstehen dann darunter, dass ein Isomorphismus φ von E nach $\mathbb{P}^2_K$ existiert, welcher die Punkte der Kurve auf ihre Restklassen überführt. Mit $P = (x, y)$ gilt $\varphi(P) = (x : y : 1)$ und $\varphi(P_\infty) = (0 : 1 : 0)$. Daher genügt es sich auf die affine Beschreibung der Kurve zu beschränken. Dabei werden x und y die Weierstraß-Koordinatenfunktionen von C genannt, siehe hierzu auch [Sil86] Proposition III.3.1.

Satz 3.2.5. (Kurze Weierstraß-Normalform einer elliptischen Kurve) *Sei E/K eine elliptische Kurve und* $\mathrm{char}(K)$ *teilerfremd zu* 6*, also verschieden von* 2 *und* 3*. Dann existiert für E eine kurze Weierstraß-Normalform:*

$$E\colon\ y^2 = x^3 + ax + b \text{ mit } a, b \in K. \tag{3.3}$$

Beweis Ausgehend von Gleichung (3.1) führen wir zwei lineare Koordinatentransformationen durch. Zuerst ersetzen wir y durch $\tilde{y} - 1/2(a_1x + a_3/2)$. Dann erhalten wir:

$$\tilde{y}^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

mit $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$ und $b_6 = a_3^2 + 4a_6$. Führen wir nun eine weitere Transformation durch und ersetzen dabei x durch $\tilde{x} - b_2/12$, so erhalten wir die kurze Weierstraß-Normalform:

$$\tilde{y}^2 = \tilde{x}^3 + a\tilde{x} + b$$

mit $a = (b_2^2 - 24b_4)/48$ und $b = (-b_2^3 + 36b_2b_4 - 216b_6)/864$, siehe auch [ACD+06] Kapitel 4.4.2.a. □

Bemerkung 3.2.6. *(a) Auch für elliptische Kurven definieren wir für L mit $K \subseteq L \subseteq \overline{K}$ die Menge der L-rationalen Punkte. Die sind gegeben durch:*

$$E(L) = \left\{P \in L^2 \mid P \text{ ist Lösung der definierenden Gleichung } E\right\} \cup \{P_\infty\}.$$

(b) Zur Unterscheidung geben wir noch einmal an: Die Kurve ist definiert über K, wenn die Varietät über K definiert ist. Dies bedeutet, dass die Koeffizienten ihrer definierenden Gleichung (3.3) oder (3.1) aus K stammen. Falls $K \subset L \subset \overline{K}$, so ist jede über K definierte Kurve auch über L definiert. Die Menge der rationalen Punkte ist dabei nicht abhängig von dem Körper, über dem die Kurve definiert ist.

(c) Nicht alle Gleichungen der Form (3.3) erzeugen eine glatte Kurve. Die Kurve ist nicht glatt, falls das Polynom in x (d.h. $x^3 + ax + b$) eine mehrfache Nullstelle besitzt. Dies kann auch mittels der Diskriminante Δ_E ausgedrückt werden. Bis auf Vorzeichen ist sie gleich dem Produkt aller Nullstellen des Polynoms in x. Sie ist daher definiert als:

$$\Delta_E = -16(4a^3 + 27b^2). \tag{3.4}$$

Weiter gilt, dass $\Delta_E \neq 0$, ist äquivalent dazu, dass die Kurve glatt ist.

3.3 Morphismen von elliptischen Kurven

Für elliptische Kurven über Körpern, deren Charakteristik verschieden von 2 und 3 ist, steht uns nun eine einheitliche Normalform zur Verfügung. Wir benötigen aber noch ein Kriterium, welches besagt, wann zwei Kurven algebraisch gleich, also isomorph, sind. Mittels der Normalformen können wir diese Fragen nun beantworten. Zunächst erinnern wir uns an Definition 2.3.12: Ein Morphismus zwischen zwei glatten Kurven ist eine reguläre, rationale Abbildung.

Definition 3.3.1. (Induzierte Abbildung, Grad einer Abbildung) *Sei φ ein Morphismus zwischen zwei glatten Kurven C_1/K und C_2/K. Dieser Morphismus* induziert eine Abbildung *zwischen den beiden Funktionenkörper $K(C_2)$ nach $K(C_1)$ wie folgt:*

$$\varphi^* : K(C_2) \longrightarrow K(C_1)$$
$$\varphi^* f := f \circ \varphi$$

Die Abbildung besitzt dann den Grad: $\deg(\varphi^*) := [K(C_1) : \varphi^* K(C_2)]$.

Bemerkung 3.3.2. *(a) Ein Morphismus zwischen zwei glatten Kurven ist stets entweder konstant oder surjektiv.*

(b) Der Grad des Morphismus ist immer endlich.

(c) Ein Morphismus ist separabel (inseparabel), falls die induzierte Körpererweiterung separabel (inseparabel) ist.

Für einen Beweis, siehe [Har97] II.6.8.

Existiert ein Morphismus zwischen zwei elliptischen Kurven und fixiert dieser zusätzlich noch die unendlichfernen Punkte, so definieren wir:

Definition 3.3.3. (Isogenie) *Seien E_1 und E_2 zwei elliptische Kurven und φ ein Morphismus zwischen E_1 und E_2, für den zusätzlich $\varphi(P_{\infty,1}) = P_{\infty,2}$ gilt, so heißt φ* Isogenie *von E_1 nach E_2. Zwei Kurven heißen isogen, falls die Isogenie nicht trivial ist, also $\varphi(E_1) \neq P_{\infty,2}$.*

Bemerkung 3.3.4. *Betrachten wir lediglich einen affinen Teil von $\tilde{E}_1$ und $\tilde{E}_2$ (zum Beispiel die Weierstraß-Normalform (3.1)), so genügt es zur Definition von isogen vorauszusetzen, dass zwischen E_1 und E_2 eine birationale Abbildung existiert. Diese wird dann so fortgesetzt, dass $\varphi(P_{\infty,1}) = P_{\infty,2}$ gilt. Die Abbildung φ ist dann natürlich ein Morphismus.*

Etwas strenger fordern wir für die nächste Definition:

Definition 3.3.5. (Isomorphismus) *Seien E_1/K und E_2/K zwei elliptische Kurven. Falls zwei Morphismen $\varphi : E_1 \to E_2$ und $\psi : E_2 \to E_1$ existieren, sodass $\psi \circ \varphi = \mathrm{Id}_{E_1}$ und $\varphi \circ \psi = \mathrm{Id}_{E_2}$, so sind φ und ψ* Isomorphismen. *Die zugehörigen Funktionenkörper sind isomorph, siehe [ACD+06] Definition 4.62.*

Bemerkung 3.3.6. *(a) Da für Isomorphien zwingend folgt, dass $\varphi(P_{\infty,1}) = P_{\infty,2}$ gilt, ist jeder Isomorphismus zwischen zwei Kurven eine Isogenie.*

(b) Die Umkehrung gilt jedoch nicht: Sind zwei Kurven isogen, so sind sie nicht zwingend isomorph. Hierzu existieren nicht triviale Beispiele, siehe [ACD+06] Beispiel 13.25.

(c) Ein Teil der Literatur schließt bei der Definition von isogen den trivialen Morphismus nicht aus.

(d) Aus der Definition des Grades einer Abbildung ist klar: Jede Abbildung von Grad 1 ist ein Isomorphismus zweier Kurven, siehe [Sil86] Korollar 2.4.1.

Satz 3.3.7. (Gruppengesetz auf der elliptischen Kurve)
Sei E eine elliptische Kurve gegeben in Weierstraß-Normalform, seien $P, Q \in E$ und L die Gerade, welche die Punkte P und Q miteinander verbindet. (Bzw. falls $P = Q$, sei L die Tangente an E.) Sei R der dritte Schnittpunkt von L mit E. Dieser existiert nach einem Satz von Bézout [Har97] Satz I.7.8 immer, da E als Gleichung dritten Grades gegeben ist. Der Schnittpunkt ist nicht zwingend

von P oder Q verschieden. Weiter sei L' die Gerade durch R und P_∞. Dann definieren wir $P \oplus Q$ (auch $P + Q$) als den dritten Schnittpunkt der Gerade L' mit E. Die so definierte Operation führt zu einer Abelschen Gruppenstruktur auf E und nennt sich Chord-Tangent-Law.

Beweis Siehe [Sil86] Proposition III.2.2, auch [Hus04] Theorem 3.1.2. □

Bemerkung 3.3.8. *(a) Der unendlichferne Punkt P_∞ der elliptischen Kurve erfüllt die Eigenschaften des neutralen Elements einer Gruppe und wird daher auch als neutrales Element $\mathcal{O}$ bezeichnet.*

(b) Diese Gruppenstruktur existiert für hyperelliptische Kurven nicht. Wir werden uns dort mit Divisoren und Divisorklassen behelfen, siehe 5.2. Aus dem dort gewonnenen Verständnis wird sofort klar, dass die elliptische Kurve eine Gruppenstruktur besitzt.

(c) Für das Chord-Tangent-Law existieren explizite, geschlossene Formeln, siehe [Sil86] Kapitel III.2.

(d) Für die Gruppe der L-rationalen Punkte mit $K \subset L \subset \overline{K}$ wird sofort klar, dass $E(L)$ eine Untergruppe von E ist.

(e) Da wir nun wissen, dass elliptische Kurven auch eine Abelsche Gruppenstruktur besitzen, bilden auch die Abbildungen zwischen ihnen eine Gruppe, siehe [Sil86] Satz III.4.8. Darauf werden wir in 3.5 zurück kommen.

(f) Sprechen wir von isogenen oder isomorphen Kurven, so ist damit auch stets gemeint, dass die Gruppenstrukturen der Kurven übertragen werden, also leicht zu beschreiben sind, siehe [Sil86] Kapitel III.4 und [ACD+06] Kapitel 13.1.6.

Bevor wir uns weiter mit Isogenien zwischen elliptischen Kurven beschäftigen, wenden wir uns zunächst den Isomorphismen elliptischer Kurven zu.

Satz 3.3.9. (Charakterisierung von Isomorphismen elliptischer Kurven)
Seien E_1/K und E_2/K zwei elliptische Kurven gegeben in kurzer Weierstraß-Normalform ($y_1^2 = x_1^3 + a_1x_1 + b_1$) bzw. ($y_2^2 = x_2^3 + a_2x_2 + b_2$) mit $a_1, a_2, b_1, b_2 \in K$ und $\mathrm{char}(K)$ *ist verschieden von* 2 *und* 3. *Dann unterscheiden wir drei Fälle:*

(a) Falls $a_1 = 0$ ist:

$$E_1 \cong E_2 \Leftrightarrow a_2 = 0 \text{ und } (b_2/b_1) \text{ ist eine sechste Potenz in } K^*.$$

(b) Falls $b_1 = 0$ ist:

$$E_1 \cong E_2 \Leftrightarrow b_2 = 0 \text{ und } (a_2/a_1) \text{ ist eine vierte Potenz in } K^*.$$

(c) Falls $a_1 b_1 \neq 0$ ist:

$$E_1 \cong E_2 \Leftrightarrow a_2 b_2 \neq 0 \text{ und es gibt ein } v \in K^* \text{ mit } a_2 = v^2 a_1 \text{ und } b_2 = v^3 b_1.$$

Beweis Dadurch, dass isomorphe Transformationen invertierbar sein müssen, ergibt sich für die zugelassenen Transformationen lediglich $x_2 = u^{-2} x_1$ und $y_2 = u^{-3} y_1$. Substituieren wir in E_2 und zwar $y_2^2 = x_2^3 + u^4 a x_2 + u^6 b$. Daraus geben sich direkt die oben angegebenen Bedingungen, siehe [ACD+06] Proposition 4.113 sowie Kapitel 13.1.5. □

Um festzustellen, ob zwei Kurven isomorph sind, ziehen wir den Körper heran, über dem die elliptischen Kurven definiert sind. Sind zwei elliptische Kurven zum Beispiel über $\overline{K}$ definiert und gilt $a_1 = a_2 = 0$, so sind sie (über $\overline{K}$) stets isomorph, da alle sechsten Wurzeln in $\overline{K}$ liegen. Besitzen zwei elliptische Kurven jedoch Koeffizienten aus K, sind sie über K nicht isomorph, falls $\sqrt[6]{b_2/b_1} \notin K$. Dies motiviert folgende Definition:

Definition 3.3.10. (Twist einer Kurve) *Seien E_1/K und E_2/K zwei elliptische Kurven. Außerdem gelte $K \subset L \subset \overline{K}$. Falls $E_1(L) \ncong E_2(L)$, aber $E_1(\overline{K}) \cong E_2(\overline{K})$, so heißt E_2* Twist *von E_1.*

Bemerkung 3.3.11. *(a) Ist E_2 Twist von E_1, so ist E_1 stets auch Twist von E_2.*

(b) Sprechen wir von echten Twists einer Kurve, so ist die Kurve selbst nicht eingeschlossen, sprechen wir von allen Twists einer Kurve, so sind damit auch die zur ursprünglichen Kurve isomorphen gemeint, obwohl sie nach Definition 3.3.10 kein Twist von ihr sind.

Satz 3.3.12. (Twists der Kurve)
Sei K ein Körper mit Charakteristik verschieden von 2 und 3 sowie E eine elliptische Kurve, gegeben durch die kurze Weierstraß-Normalform:

$$E\colon y^2 = x^3 + a \cdot x + b.$$

Dann sind alle Twists gegeben durch:

$$\tilde{E}_i\colon y^2 = x^3 + \tilde{a}_i \cdot x + \tilde{b}_i,$$

und es tritt einer der drei folgenden Fälle auf:

Twists von Grad 2: *Falls $ab \neq 0$, sind die Twists gegeben durch $\tilde{a}_i = a$ und $\tilde{b}_i = b/c^i$ mit $\mathrm{ord}(c) = 2$, $i \in \{1, 2\}$.*

Twists von Grad 4: *Falls $b = 0$, sind die Twists gegeben durch $\tilde{a}_i = a/c^i$ mit $\mathrm{ord}(c) = 4$, $i \in \{1 \ldots 4\}$.*

Twists von Grad 6: *Falls $a = 0$, sind die Twists gegeben durch $\tilde{b}_i = b/c^i$ mit $\mathrm{ord}(c) = 6$, $i \in \{1 \ldots 6\}$.*

Der Grad eines Twists zeigt an, wie viele über K nicht isomorphe Kurven $E(K)/K$ maximal existieren.

Beweis Siehe [Sil86] Proposition 5.4 und [ACD$^+$06] Korollar 4.114. □

Eine elliptische Kurve E/K mit $\mathrm{char}(K)$ verschieden von 2 und 3 besitzt also maximal sechs Twists. Mit der folgenden Invariante lassen sich die Kurven bis auf Twists leicht charakterisieren:

Definition 3.3.13. (j-Invariante) *Sei E/K eine glatte, elliptische Kurve in kurzer Weierstraß-Normalform (3.3). Dann ist die j-*Invariante *j_E (oder auch absolute Invariante) definiert durch:*

$$j_E := \begin{cases} 0 & \Leftrightarrow a = 0 \\ 12^3 & \Leftrightarrow b = 0 \\ 12^3 \cdot (-4a^3/(-16a^3 + 27b^2)) & \Leftrightarrow ab \neq 0 \end{cases}$$

Dabei halten wir fest, dass alle Twists einer Kurve dieselbe j-Invariante haben. Es gilt sogar darüber hinaus, dass wir mittels der j-Invariante die definierende Gleichung zurückgewinnen können. Sei j_E eine j-Invariante. Eine Kurve mit dieser j-Invariante erhalten wir durch:

$$E_{j_E}: \quad \begin{cases} y^2 = x^3 + b & \text{, falls } j_E = 0 \\ y^2 = x^3 + ax & \text{, falls } j_E = 12^3 \\ y^2 = x^3 - \frac{27 j_E}{4(j-12^3)} x + \frac{27 j_E}{4(j-12^3)} & \text{, sonst} \end{cases}$$

Hierbei sind $a, b \in K$ so zu wählen, dass die Kurve nichtsingulär ist, vergleiche hierzu die Diskriminante der elliptischen Kurve, siehe Definition 3.4. Berechnen wir zu einer gegebenen Kurve deren j-Invariante und erzeugen daraus dann wieder eine Kurve, so liegen beide Kurven stets in derselben $\overline{K}$-Isomorphieklasse, oder mit anderen Worten sie stimmen bis auf K-Isomorphie und Twist überein. Wir fassen zusammen:

Bemerkung 3.3.14. *Die j-Invariante charakterisiert die Kurve E/K bis auf Twists und Isomorphie über K.*

3.4 Diskriminanten und CM-Körper

Um uns weiter mit Isogenien zu beschäftigen, benötigen wir Kenntnisse über Diskriminanten. Dazu holen wir etwas weiter aus und definieren die Polynomialdiskriminante eines Polynoms als Quadrat der paarweisen Differenzen der Nullstellen. Dies haben wir in Definition 3.4 für eine elliptische Kurve in kurzer Weierstraß-Normalform bereits getan, siehe auch [Coh93] Proposition 3.3.5.

Definition 3.4.1. (Diskriminante eines Polynoms) *Sei $f \in \overline{K}[x]$ ein Polynom von Grad m mit $f = a(x - \alpha_1) \cdots (x - \alpha_m)$. Sei $\hat{f}$ die Ableitung des*

Polynoms und $\mathrm{Res}(f, \hat{f}) = a^{m-1}\hat{f}(\alpha_1)\cdots\hat{f}(\alpha_m)$ *die Resultante von* f *und* $\hat{f}$. *Dann ist die* Diskriminante von f *definiert als:*

$$d(f) = \frac{(-1)^{m(m-1)/2}\,\mathrm{Res}(f, \hat{f})}{a}.$$

Siehe [Coh93] Definition 3.3.2 und 3.3.3.

Wir definieren weiter die Diskriminante einer Menge:

Definition 3.4.2. (Diskriminante einer Menge) *Sei* K *ein Zahlkörper von Grad* $2g$, $M = \{\alpha_j \in K \mid 1 \leq j \leq 2g\}$ *eine Menge von* $2g$ *Elementen aus* K *und* σ_i *mit* $1 \leq i \leq 2g$ *die* $2g$*-Einbettungen von* K *nach* $\mathbb{C}$. *Dann gilt:*

$$d(M) = \det(\sigma_i(\alpha_j))^2 = \det(Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j))$$

Diese so definierte Zahl $d(M) = d(\alpha_1, \ldots, \alpha_{2g})$ *heißt dann die* Diskriminante (von $\alpha_1, \ldots, \alpha_{2g}$, bzw. M).

Diese Definition lässt sich auch auf Zahlkörper erweitern:

Definition 3.4.3. (Diskriminante eines Zahlkörpers) *Sei* $\mathcal{A}$ *eine* $\mathbb{Z}$*-Basis der Maximalordnung eins Zahlkörpers* K. *Dann ist die* Diskriminante von K *definiert als* $d(K) := d(\mathcal{A})$. *Sie ist unabhängig von der Wahl der Basis.*

Die drei Diskriminantenbegriffe stehen in folgendem Zusammenhang:

Satz 3.4.4. (Diskriminantenzusammenhänge)
Sei $f(t)$ *ein normiertes, irreduzibles Polynom in* $\mathbb{Z}[t]$ *von Grad* $2g$. *Sei* α *eine Nullstelle von* f, *also* $f(\alpha) = 0$. *Weiter sei* $K = \mathbb{Q}(\sqrt{\alpha})$. *Dann gilt*

(a) Die Diskriminante des Minimalpolynoms ist gleich der Diskriminante der Potenzen der Nullstelle, also $d(1, \alpha, \alpha^2, \ldots, \alpha^{2g-1}) = d(f)$.

(b) Sei $h_K = [Z_K : Z[\alpha]]$ *der Index der Gleichungsordnung* $Z[\alpha]$ *in der Maximalordnung* Z_K. *Dann ist der Zusammenhang zwischen der Diskriminante des Minimalpolynoms und der Diskriminante des Zahlkörpers gegeben durch* $d(K) := d(f) \cdot h_K^2$.

Beweis Der Beweis ergibt sich aus den obigen Definitionen, siehe auch [Coh93] Proposition 4.4.4. □

Für den Fall $g = 1$ ergibt sich ein quadratisches Minimalpolynom: $f(t) = t^2 + at + b \in \mathbb{Z}[t]$. Da es in K zerfällt, können nur zwei Fälle auftreten: Es besitzt zwei reelle oder zwei konjugiert komplexe Nullstellen.

Fall 1: Betrachten wir die Faktorisierung in zwei reelle Nullstellen: $f(t) = (t-c)(t-d)$ mit $c, d \in \mathbb{R}$. Die Diskriminante berechnet sich als Quadrat der Differenz der Nullstellen, also $d(f) = (c-d)^2$. Da c und d reell sind, ist die Diskriminante stets positiv und somit auch die Körper-Diskriminante, welche sich ja nur um ein reelles Quadrat von der Polynomialdiskriminante unterscheidet.

Fall 2: Betrachten wir nun die Faktorisierung für zwei komplex konjugierte Nullstellen: $f(t) = (t - c + id)(t - c - id)$ mit $c, d \in \mathbb{R}$. In diesem Fall berechnet sich die Polynomialdiskriminante zu: $d(f) = ((c - id) - (c + id))^2 = (-2id)^2 = -4d^2$. Hierbei ist die Diskriminante also stets negativ, somit auch die Körper-Diskriminante.

Wie aus der Algebra bekannt, lassen sich quadratische Körpererweiterungen über $\mathbb{Q}$ immer durch eine rationale Quadratwurzel $\sqrt{T}, T \in \mathbb{Q}$ erzeugen. Außerdem erzeugen zwei Parameter den gleichen quadratischen Erweiterungskörper, falls sie sich nur um ein Element aus $\mathbb{Q}$ unterscheiden, also $a\sqrt{T} = \sqrt{a^2 T}$ mit $a, T \in \mathbb{Q}$. Somit brauchen wir ausschließlich Körper zu betrachten, die durch die Wurzel einer quadratfreien Zahl, oder mit anderen Worten, die durch das Minimalpolynom $f(t) = t^2 - T = \left(t - \sqrt{T}\right)\left(t + \sqrt{T}\right)$ mit T quadratfrei, erzeugt werden. Für dieses Minimalpolynom berechnet sich die Polynomialdiskriminante leicht:

$$d(f) = \left(\sqrt{T} - (-\sqrt{T})\right)^2 = \left(2\sqrt{T}\right)^2 = 4T$$

Ist $T \equiv 0 \bmod 4$, so ist T nicht quadratfrei. Es sind also noch 3 Fälle zu betrachten:

(a) $T \equiv 1 \bmod 4 \Longrightarrow \mathbb{Z}[\sqrt{T}]$ ist noch nicht die Maximalordnung, ein Aufstieg (von 4) ist noch von Nöten daher ist $4d(K) = d(f) \Leftrightarrow d(K) = T$.

(b) $T \equiv 2 \bmod 4 \Longrightarrow \mathbb{Z}[\sqrt{T}]$ ist schon die Maximalordnung, also $d(K) = d(f) = 4T$.

(c) $T \equiv 3 \bmod 4 \Longrightarrow \mathbb{Z}[\sqrt{T}]$ ist schon die Maximalordnung, also $d(K) = d(f) = 4T$.

Dies folgt direkt aus [Coh93] Proposition 5.1.1. Damit haben wir $d(K)$ für jede quadratische Körpererweiterung eindeutig bestimmt und wir definieren:

Definition 3.4.5. (Fundamentaldiskriminante) *Sei $d(K) \neq 1$ die Diskriminante eines quadratischen Zahlkörpers mit $K \cong \mathbb{Q}(\sqrt{T})$ und $T \in \mathbb{Z}$ quadratfrei. Dann heißt $D := d(K)$* Fundamentaldiskriminante *des Zahlkörpers $\mathbb{Q}(\sqrt{T})$. Sie ist eindeutig bestimmt.*

Diese Herleitung verdeutlicht auch die Definition von [Coh93] Definition 5.1.2, der eine Fundamentaldiskriminante dadurch definiert, dass sie eine ganze Zahl $D = d(K)$, $D \neq 1$ ist, für die entweder *(a)*: $D \equiv 1 \bmod 4$ oder *(b)* und *(c)* $D \equiv 8, 12 \bmod 16$ gilt. Wir werden in Zusammenhang mit der CM-Gleichung (3.6) noch einmal auf die Fundamentaldiskriminante stoßen. Zunächst halten wir fest: Die Fundamentaldiskriminante ist eine ganze Zahl, die bestimmten Kongruenz-Bedingungen genügt.

Betrachten wir wieder einen quadratischen CM-Körper. Er ist eine imaginärquadratische Erweiterung $\mathbb{Q}(\sqrt{T})$ über $\mathbb{Q}$, also ist T negativ. Somit ist auch $d(K)$, die Fundamentaldiskriminante des quadratischen CM-Körpers, negativ. Wir weisen darauf hin, dass in der Literatur auch $-D$ als Fundamentaldiskriminante definiert wird, siehe [ACD+06] Kapitel 18.

3.5 Endomorphismenringe und CM-Körper

Betrachten wir nun wieder Isogenien von elliptischen Kurven. Diese werden wir in Zusammenhang mit den bereits erläuterten CM-Körpern bringen. Zunächst erinnern wir an Satz 3.3.7, welcher besagt, dass Isogenien einen Homomorphismus auf der Gruppenstruktur der elliptischen Kurve induzieren.

Definition 3.5.1. (Endomorphismenring) *Seien E_1/K und E_2/K zwei elliptische Kurven, dann ist* $\mathrm{Hom}_K(E_1, E_2)$ *die Menge der Isogenien von E_1 nach E_2. Seien weiter $\varphi, \psi \in \mathrm{Hom}_K(E_1, E_2)$. Die Isogenien besitzen auf natürliche Weise eine Addition $(\varphi + \psi)(P) := \varphi(P) + \psi(P)$ für $\psi, \varphi \in \mathrm{Hom}(E_1, E_2)$ und $P \in E_1$.*
Ist sogar $E_1 = E_2 = E$, so existiert auf $\mathrm{Hom}_K(E, E)$ *neben der Addition auch eine Multiplikation. Für $\varphi, \psi \in \mathrm{Hom}(E, E)$ und $P \in E$ gilt: $(\varphi \odot \psi)(P) := \psi(\varphi(P))$.*
Die Menge der Isogenien von E nach E zusammen mit der eben beschriebenen Addition und Multiplikation bildet also ein Ring, den Endomorphismenring *von E, welcher mit* $\mathrm{End}(E)$ *bezeichnet wird. Sind die elliptischen Kurven über K definiert, so ist es manchmal nötig sich auf Isogenien, welche über K definiert sind, zu beschränken. Dafür schreiben wir* $\mathrm{End}_K(E)$*. Siehe [Sil86] Kapitel III.4. Im Allgemeinen ist der Endomorphismenring nicht kommutativ.*

Dies ermöglicht uns den Begriff der komplexen Multiplikation einzuführen.

Definition 3.5.2. (Komplexe Multiplikation) *Eine elliptische Kurve hat* komplexe Multiplikation*, wenn ihr Endomorphismenring* $\mathrm{End}(E)$ *ungleich $\mathbb{Z}$ ist. In diesem Fall nennen wir sie elliptische Kurven mit komplexer Multiplikation oder CM-Kurve, siehe [ACD+06] Definition 13.26.*

Dieser Ausdruck stammt von der ursprünglichen Anschauungsweise der elliptischen Kurven. Sie haben ihren Ursprung in der Untersuchung elliptischer Integrale, welche mittels doppeltperiodischen Funktionen berechnet werden. Diese doppelte Periodizität kann mit Hilfe eines Gitters ausgedrückt werden. Besitzt eine Funktion über $\mathbb{C}$ auf allen Gitterpunkten den gleichen Wert, so erhalten wir eine doppeltperiodische Funktion.

Es existiert ein Satz [ACD+06] Proposition 5.42, der besagt, dass zwei elliptische Kurven E_1 und E_2 über $\mathbb{C}$ mit zugehörigen Gittern Λ_1 und Λ_2, genau dann isogen sind, falls ein $\alpha \in \mathbb{C}^*$ existiert, sodass $\alpha\Lambda_1 \subset \Lambda_2$. Auf diese Weise kann jede Isogenie durch eine Zahl α beschrieben werden. Als Beschreibung des Endomorphismenrings ergibt sich: $\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_E \subset \Lambda_E\}$, wobei Λ_E

das zu $E/\mathbb{C}$ gehörige Gitter ist. Die Multiplikation mit $\alpha = 1$ liegt trivialerweise im Endomorphismenring, damit auch Vielfache von 1 und damit auch ganz $\mathbb{Z}$. Weiter lässt sich zeigen, dass α entweder aus $\mathbb{Z}$ oder aus $\mathbb{C}\backslash\mathbb{R}$ ist. Daher erklärt sich der historische Ausdruck: Existiert also ein komplexes α im Endomorphismenring der Kurve, so besitzt die Kurve komplexe Multiplikation, siehe auch [Coh93] Kapitel 7.2.3.

Auch CM-Körper, die wir bereits im einleitenden Kapitel 2.1 definiert haben, können wir nun mit dem Begriff der komplexen Multiplikation verknüpfen. Der folgende Satz stellt die Zusammenhänge der letzten beiden Kapitel klar:

Satz 3.5.3. (Endomorphismenring einer elliptischen Kurve)
Der Endomorphismenring einer elliptischen Kurve ist entweder $\mathbb{Z}$, *eine Ordnung in einem imaginär-quadratischen Zahlkörper (CM-Körper von Grad 2) oder einer Quaternionenalgebra. Weiter gilt:*

(a) Ist die Kurve über einem Körper K *mit* $\mathrm{char}(K) = 0$ *definiert, so ist der Endomorphismenring niemals eine Ordnung in einer Quaternionenalgebra; ist er größer als* $\mathbb{Z}$ *besitzt er komplexe Multiplikation.*

(b) Ist die Kurve über einem endlichen Körper definiert, so ist der Endomorphismenring niemals $\mathbb{Z}$.

Beweis Siehe [Sil86] Korollar II.9.4. Bzw. VI.6.1 für *(a)* und V.3.1 für *(b)*. □

Mit *(b)* lassen sich elliptische Kurven über endlichen Körpern also in zwei Fälle unterscheiden. Auch wenn wir diese später deutlich einfacher beschreiben können, benötigen wir die Unterscheidung bereits jetzt.

Definition 3.5.4. (Supersingulär, ordinär) *Sei E eine elliptische Kurve über einem endlichen Körper. Eine Kurve heißt* supersingulär*, falls ihr Endomorphismenring eine Ordnung in einer Quaternionenalgebra ist. Sie heißt* ordinär *oder gewöhnlich, falls ihr Endomorphismenring eine Ordnung in einem imaginär-quadratischen Zahlkörper ist, siehe [Sil86] Theorem V.3.1.*

Neben dieser Definition existieren weitere äquivalente Definitionen für supersinguläre Kurven, siehe [Sil86] Theorem V.3.1. Eine davon werden wir in 3.6 kennenlernen.

Ordinäre elliptische Kurven mit komplexer Multiplikation besitzen also einen Endomorphismenring, der eine Ordnung in einem CM-Körper ist. Umgekehrt gilt aber auch, dass jedem imaginär-quadratischen Zahlkörper (mindestens) eine elliptische Kurve mit komplexer Multiplikation zugeordnet werden kann. Das ist der Grund, weshalb imaginär-quadratische Zahlkörper auch CM-Körper heißen und die Fundamentaldiskriminante des CM-Körpers auch der elliptischen Kurve zugeordnet wird.

3.6 Weitere Eigenschaften von elliptischen Kurven

Wir werden nun weitere Eigenschaften elliptischer Kurven kennenlernen, um einsehen zu können, ob sie auch kryptografisch geeignet sind oder nicht. Dafür definieren wir zunächst:

Definition 3.6.1. (Torsionsgruppe) *Sei E eine elliptische Kurve und $r \in \mathbb{N}$. Dann ist die r-*Torsionsgruppe *- eine Untergruppe von E - definiert als:*

$$E[r] := \{P \in E \mid rP = \mathcal{O}\}.$$

Dies ist lediglich eine andere Bezeichnung für $\mathrm{Ker}(r)$.

Weiter definieren wir die Torsionsgruppe der L-rationalen Punkte:

Definition 3.6.2. (Torsionsgruppe der L-rationalen Punkte) *Sei E/K eine elliptische Kurve über K. Sei L eine Körpererweiterung von K mit $K \subset L \subset \overline{K}$ und sei $r \in \mathbb{N}$. Dann heißt*

$$E(L)[r] := \{P \in E(L) \mid rP = \mathcal{O}\}$$

*die r-*Torsionsgruppe der L-rationalen Punkte *von E.*

Satz 3.6.3. (Anzahl der Punkte der Torsionsgruppe)
Sei E/K eine elliptische Kurve und $r \in \mathbb{N}\setminus\{0\}$. Für $\mathrm{char}\, K = 0$ *oder r teilerfremd zu* $\mathrm{char}\, K$ *gilt:*

$$E[r] \cong (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z}),$$

anderenfalls, also falls $\mathrm{char}(K) = r$, *so gilt für alle $e \in \{1, 2, 3, \ldots\}$:*

(a) $E[r^e] = \{\mathcal{O}\}$ *oder*

(b) $E[r^e] = \mathbb{Z}/r^e\mathbb{Z}$.

Hierbei ist (a) gleichbedeutend damit, dass die Kurve supersingulär ist.

Beweis Siehe [Sil86] Kapitel III.6 und Kapitel V.3. □

Zu beachten ist, dass Torsionsgruppen L-rationaler Punkte jeweils Untergruppen der Torsionsgruppen sind. Somit gibt der Satz eine obere Schranke für die Ordnungen der jeweiligen Gruppe an.

3.6.1 Reduktion von elliptischen Kurven

Bislang haben wir elliptische Kurven stets über einem beliebigen Körper K betrachtet. Davon werden wir nun abweichen und elliptische Kurven speziell über endlichen Körpern betrachten. Hierzu gibt es verschiedene Möglichkeiten, wie wir solche Kurven konstruieren können: entweder direkt über endlichen Körpern oder über den komplexen Zahlen $\mathbb{C}$, die anschließend modulo einer Primzahl

bzw. eines Primideals reduziert werden. Diesen Prozess nennen wir Reduktion $\bmod p$. Detaillierte Darstellungen hierzu bei [Hus04] Kapitel 5, [Sil86] Kapitel VII sowie eine kurze Zusammenfassung in [ACD+06] Auszüge von Kapitel 5.1. Uns genügt hier eine kurze Darstellung:

Definition 3.6.4. (Minimale Normalform) *Sei E/K gegeben in Weierstraß-Normalform aus Gleichung (3.1) mit* $\mathrm{char}(K) = 0$. *Sei v eine diskrete Bewertung von K. Dann ist E in* minimaler Normalform*, falls alle a_i aus dem Bewertungsring $\mathcal{O}_v$ sind und die Bewertung der Diskriminante $v(\Delta_E)$ minimal unter allen zu E isomorphen Kurven ist, siehe [Sil86] Kapitel II.1.*

Betrachten wir nun die Reduktion $\bmod p$, (wir bezeichnen sie mit $\tilde{}$), welche die Elemente des Körpers K in ihre Restklassen K/pK abbildet. Ist eine nichtsinguläre elliptische Kurve $E/\mathbb{C}$ in minimaler Normalform gegeben, so erzeugen wir die reduzierte Kurve, in dem wir die Koeffizienten modulo p berechnen. Die reduzierte Kurve $\tilde{E}$ kann jedoch sowohl singulär als auch nichtsingulär sein. Ist sie nichtsingulär, so sprechen wir von guter Reduktion $\bmod p$.

Ein zentraler Satz klärt den Übergang von Körpern mit Charakteristik 0 zu endlichen Körpern:

Satz 3.6.5. (Reduktion $\bmod p$)
Sei E/K eine elliptische Kurve mit $\mathrm{char}(K) = 0$, *gegeben in minimaler Normalform und Δ_E die Diskriminante der elliptischen Kurve. So hat E genau dann gute Reduktion in p, falls $\Delta_E \bmod p \neq 0$. In diesem Fall ist auch $E/(\tilde{K}/pK)$ eine elliptische Kurve. Ferner gilt, dass die Reduktion ein Gruppenmorphismus $E/K \to \tilde{E}/(K/pK)$ ist.*

Beweis Siehe [Sil86] Proposition VII.5.1. und [Hus04] Bemerkung 5.3.2 Proposition 5.3.4. □

Bemerkung 3.6.6. *(a) Ist E über $\mathbb{Q}$ definiert, so ist die reduzierte Kurve über $\mathbb{F}_p$ definiert.*

(b) Offensichtlich verträgt sich das Bilden von Invarianten wie der j-Invariante, siehe Definition 3.3.13, mit der Reduktion modulo p.

(c) Die Reduktionstheorie wird auch mit Primidealen formuliert.

(d) Auch für das Hilbertsche Klassenpolynom, welches wir in 4.2.1 verwenden, gilt diese Aussage. Es hat genau dann einfache Nullstellen modulo p, falls p nicht die Fundamentaldiskriminante des Körpers teilt, siehe [ACD+06] Kapitel 5.1.5.b.

3.6.2 Elliptische Kurven über endlichen Körpern

Da es keine offensichtliche Weise gibt, wie Computer mit unendlichen elliptischen Kurven umgehen sollen, benutzen wir in der Kryptografie fast ausschließlich endliche Strukturen. Zwar hat der algebraische Abschluss eines endlichen

Körpers immer noch unendlich viele Elemente, schränken wir uns aber weiter auf Torsionsgruppen endlicher Körper ein, so wissen wir bereits, dass diese endlich sind. Daher werden wir jetzt weitere Eigenschaften von elliptischen Kurven über endlichen Körpern untersuchen. Im Folgenden werden also alle elliptischen Kurven stets über endlichen Körpern definiert sein.

Dabei spielt es keine Rolle, ob der jeweilige Körper $\mathbb{F}_q$ oder $\mathbb{F}_p$ ist. Oft wird in der Kryptografie auf $\mathbb{F}_{2^m}$ bzw. $\mathbb{F}_{3^m}$ oder auf Primkörper zurückgegriffen. Für $\mathbb{F}_{2^m}$ und $\mathbb{F}_{3^m}$ existieren günstige Hardware-Implementierungen. Primkörper großer Charakteristik haben dagegen den offensichtlichen Vorteil, dass sie eine große Charakteristik besitzen. Auch wenn bislang keine Angriffe bekannt sind, welche die Charakteristik sinnvoll ausnutzen ist es durchaus denkbar, dass solche existieren. Deswegen haben Primkörper großer Charakteristik gegenüber echten Primpotenzkörpern einen potentiellen Sicherheitsvorteil. Des Weiteren sind sie leichter zu finden, da in der Regel in einem gegebenen Intervall mehr Primzahlen als echte Primzahlpotenzen liegen.

Zunächst halten wir fest, die Anzahl der $\mathbb{F}_q$-rationalen Punkte von Kurven über $\mathbb{F}_q$ ist endlich:

Definition 3.6.7. (Ordnung einer Kurve) *Sei $E/\mathbb{F}_q$ eine Kurve über einem endlichen Körper $\mathbb{F}_q$. Die* Ordnung von $E/\mathbb{F}_q$ *ist die Anzahl der $\mathbb{F}_q$-rationalen Punkte von E, die wir im Folgenden mit R bezeichnen wollen.*

$$R := |E(\mathbb{F}_q)|$$

Aufgrund der Gruppenstruktur der elliptischen Kurven ergibt sich, dass, falls R endlich ist, die Anzahl der Punkte der r-Torsionsgruppe über $\mathbb{F}_q$ die Ordnung R teilt, also:

$$E(\mathbb{F}_q)[r] \mid E(\mathbb{F}_q).$$

Für elliptische Kurven können wir weitere Aussagen über ihre Größenordnungen treffen:

Satz 3.6.8. (Hasse-Schranke)
Sei $E/\mathbb{F}_q$ eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$. Dann gilt:

$$|R - q - 1| \leq 2\sqrt{q}$$

Diese Schranke wird Hasse-Schranke (oder auch Hasse-Weil-Schranke) genannt. Das dazugehörige Intervall $[-2\sqrt{q}+q+1; 2\sqrt{q}+q+1]$ heißt Hasse-Weil-Intervall.

Beweis Siehe [Sil86] Theorem V.1.1. oder [ACD+06] Beispiele 5.83. □

Bemerkung 3.6.9. *Die Hasse-Weil-Schranke liefert uns ein Intervall, in welchem wir die Anzahl der Punkte der Kurve suchen müssen. Sie garantiert allerdings nicht, dass im Hasse-Weil-Intervall eine Primzahl enthalten ist. Später*

werden wir uns auf prime Torsionsgruppen zurückziehen. Daher wäre es für unsere Zwecke von Vorteil, wenn bereits die Anzahl der Elemente der Kurve prim wäre und damit ein r existiert, sodass die gesamte Kurve bereits in der r-Torsionsgruppe enthalten ist. Obwohl das Hasse-Weil-Intervall mit einer Spanne von $4\sqrt{q}$ recht groß ist, existiert bis heute kein Beweis, dass darin stets eine Primzahl enthalten ist.

Betrachten wir nun einen für endliche Körper $\mathbb{F}_q$ speziellen Endomorphismus, der durch potenzieren der Elemente mit q gegeben ist:

Definition 3.6.10. (Frobenius-Endomorphismus) *Sei $E/\mathbb{F}_q$ eine elliptische Kurve über einem endlichen Körper mit Charakteristik p, also* $\mathrm{char}(\mathbb{F}_q) = p$ *und $q = p^d$. Wir definieren eine Abbildung:*

$$\begin{aligned} \phi_q \colon E &\longrightarrow E^q \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

Wir nennen ϕ_q den relativen Frobenius-Endomorphismus. *Im Gegensatz hierzu heißt die Abbildung ϕ_p, welche die Elemente komponentenweise in die p-te Potenz erhebt,* absoluter Frobenius-Endomorphismus. *Für den Fall $K = \mathbb{F}_p$ fallen diese beiden Definitionen selbstverständlich zusammen, siehe [Sil86] Kapitel II.2.*

Bemerkung 3.6.11. *(a) Elemente aus $\mathbb{F}_q$ werden von ϕ_q fixiert, mit anderen Worten $\{P \in E \mid \phi_q(P) = P\} = E(\mathbb{F}_q)$, siehe [Hus04] Definition 13.1.1.*

(b) Im Sprachgebrauch werden beide Morphismen auch nur als Frobenius bezeichnet, wenn aus dem Kontext klar wird, welcher gemeint ist.

(c) Obwohl ϕ_q bijektiv ist, ist der Frobenius-Endomorphismus kein Isomorphismus, siehe [Sil86] Aufgabe I.1.8.

Für diesen speziellen Endomorphismus werden wir nun das charakteristische Polynom, siehe Definition 2.1.6, bestimmen.

Definition 3.6.12. (Charakteristisches Polynom des Frobenius) *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und ϕ_q der relative Frobenius-Endomorphismus. Wir bezeichnen das* charakteristisches Polynom des Frobenius *als*

$$\chi(\phi_q)_E(T)$$

Für eine elliptische Kurve E/K besitzt es folgende Struktur: $\chi(\phi_q)_E(T) = T^2 + \mathrm{Tr}(\phi_q)T + q^2$. Dabei wird die Spur $\mathrm{Tr}(\phi_q)$ mit dem Parameter t abgekürzt.

Bemerkung 3.6.13. *Auch dies kann genutzt werden, um zwischen supersingulären und ordinären Kurven zu unterschieden. Ist $t = 0$ so ist die Kurve supersingulär, sonst ordinär, siehe Definition 3.5.4 .*

Das charakteristische Polynom ist Bestandteil des folgenden Satzes:

Satz 3.6.14. (Hasse-Weil-Vermutung)
Sei $E/\mathbb{F}_q$ eine elliptische Kurve über einem endlichen Körper, ϕ_q der relative Frobenius-Endomorphismus und $\chi(\phi_q)_E(T)$ das charakteristische Polynom. Seien α und β die (komplexen) Nullstellen des Polynoms. Dann haben α und β aufgefasst als komplexe Zahlen den Absolutbetrag $\sqrt{q}$ und weiter gilt:

$$|E(\mathbb{F}_{q^n})| = q^n + \alpha^n - \beta^n + 1.$$

Insbesondere gilt, dass α und β komplex konjugiert sind, ja sogar dass $\alpha + \beta = t = \mathrm{Tr}(\phi_q) \in \mathbb{Z}$. Aufgrund des oben etablierten Zusammenhangs entspricht daher die Auswertung des Frobenius an der Stelle $T = 1$ der Anzahl der $\mathbb{F}_q$-rationalen Punkte der Kurve. Es gilt also:

$$R = q + t - 1 \tag{3.5}$$

Beweis Siehe [ACD+06] Beispiel 5.73 und 5.83 sowie [Sil86] Kapitel V.2. □

Bemerkung 3.6.15. *Obwohl die Hasse-Weil-Vermutung auch in allgemeinerer Form schon längst bewiesen ist, hat sich der Begriff Vermutung (engl.: Weil-conjectures) durchgesetzt.*

Mithilfe des charakteristischen Polynoms des Frobenius können wir die Fundamentaldiskriminante für nichtsinguläre Kurven auch wie folgt berechnen:

Satz 3.6.16. (CM-Gleichung)
Sei $E/\mathbb{F}_q$ eine elliptische Kurve über einem endlichen Körper und sei t die Spur des charakteristischen Polynoms des relativen Frobenius ϕ_q. Dann ist die Fundamentaldiskriminante D der quadratfreie Teil der negativen natürlichen Zahl $4q - t^2$. Das bedeutet also:

$$4q = t^2 - D \cdot y^2 \tag{3.6}$$

mit $D < 0$ und D quadratfrei. In der Literatur wir diese Gleichung als CM-Gleichung *für elliptische Kurven bezeichnet [FST06], [BN05], [Tes07] u.a.*

Beweis Die Diskriminante des charakteristischen Polynoms des relativen Frobenius $\chi(\phi_q)_E(T) = T^2 + tT + q$ berechnet sich als $D(\chi) = t^2 - 4q$. Dabei unterscheiden sich $D(T)$ und D maximal um ein Quadrat. Dieses spielt aber bei der Erzeugung von quadratischen Zahlkörpererweiterungen keine Rolle, da die Wurzel eines Quadrates bereits im Grundkörper $\mathbb{Q}$ enthalten ist. Umstellen zu $D(\chi) = t^2 - 4q$ und herauslösen des Quadrats liefert die Aussage, siehe auch [Sil86] Theorem V.3.1. □

Bemerkung 3.6.17. *Die CM-Gleichung verdeutlicht, warum $D \equiv 0, 1 \bmod 4$. Es ist bekannt, dass Quadrate immer kongruent 0 oder 1 modulo 4 sind. Es folgt $t^2 - 4q \equiv 0, 1 \bmod 4$. Somit gilt $(D \bmod 4 \cdot y^2 \bmod 4) \bmod 4 \equiv 0, 1$ und wir sehen leicht, dass $D \equiv 0, 1 \bmod 4$. Für $D \equiv 0 \bmod 4$ gibt es modulo 16 gerade vier*

Möglichkeiten. Im Fall $D(T) \equiv 0, 1 \bmod 16$ bedeutet dies, dass $D(T)$ ein Quadrat in y^2 werden kann, daher bleiben für $D \equiv 0 \bmod 4$ die beiden Möglichkeiten $D \equiv 8, 12 \bmod 16$. Dies erklärt die Äquivalenz der Definition nach [Coh93] und der Definition 3.4.5.
Für supersinguläre Kurven kann diese Definition nicht angewendet werden, da der Endomorphismenring einer supersingulären Kurve eine Ordnung in einer Quaternionenalgebra ist.

Definition 3.6.18. (Einbettungsgrad) *Sei E/K eine elliptische Kurve mit einer nicht trivialen r-Torsionsgruppe. Der* Einbettungsgrad k *von E bezüglich r ist definiert als der Grad der kleinsten Körpererweiterung L/K, für welche die Menge der r-ten Einheitswurzeln μ_r in L enthalten ist, siehe [FST06] Definition 2.1.*

Der Einbettungsgrad hängt also von der Kurve und r ab. Später werden wir sehen, dass E und r implizit durch eine Paarung, siehe Definition 3.7.1, gegeben sind. Wir sprechen daher oft einfach vom Einbettungsgrad der Paarung.

Über einem endlichen Körper gibt es eine Reihe von äquivalenten Definitionen des Einbettungsgrades.

Lemma 3.6.19. *Sei $E/\mathbb{F}_q$ eine Kurve über einem endlichen Körper und r ein Teiler der Anzahl der $\mathbb{F}_q$-rationalen Punkte R, also $r \mid R = |E(\mathbb{F}_q)|$. Dann sind folgende Aussagen äquivalent:*

(a) E hat Einbettungsgrad k bezüglich r.

(b) k ist die kleinste natürliche Zahl, sodass $r \mid q^k - 1$.

(c) k ist die multiplikative Ordnung von $q \bmod r$.

Siehe [FST06] Bemerkung 2.2.
Mit der zusätzlichen Voraussetzung, dass $r \nmid k, r$ prim und t die Spur des Frobenius-Endomorphismus ist, gelten weitere Äquivalenzen:

(d) $\Phi_k(q) \equiv 0 \bmod r$.

(e) $\Phi_k(t-1) \equiv 0 \bmod r$.

wobei Φ_k das k-te Kreisteilungspolynom ist. Siehe [FST06] Proposition 2.4. Im Gegensatz zu (b), muss in (d) und (e) für $1 \leq i < k$ nicht überprüft werden, ob $\Phi_i(q) \not\equiv 0 \bmod r$ bzw. $\Phi_i(t-1) \not\equiv 0 \bmod r$.

Bemerkung 3.6.20. *In [Hit06] untersucht Laura Hitt den Einbettungsgrad weitergehend und schlägt eine andere Definition vor. Anstatt vom Körper $\mathbb{F}_q$, über dem die Kurve definiert ist, auszugehen, bettet sie die Kurve in eine Erweiterung von $\mathbb{F}_p$ ein. Sie wählt die Potenz dabei so, dass $\mu_r \subset \mathbb{F}_p^{k_{\text{Hitt}}}$. Dadurch ergeben sich andere Werte für k_{Hitt}. Für $q \in \mathbb{P}$ ergibt sich jedoch kein Unterschied.*

Satz 3.6.21. (Existenz einer speziellen elliptischen Kurve)
Gegeben seien $q, R, k \in \mathbb{N}$, $r \in \mathbb{P}$, D *negative Fundamentaldiskriminante und* $t, y \in \mathbb{Z} \setminus \{0\}$, *welche folgenden fünf Bedingungen genügen:*

(a) q *ist Primzahlpotenz. Ist* q *prim, wird* q *mit* p *bezeichnet.*

(b) $r \mid R$.

(c) Die Variablen erfüllen die CM-Gleichung $4q = t^2 - D \cdot y^2$; *Gleichung (3.6).*

(d) Die Variablen erfüllen die Ordnungs-Gleichung $R = q + t - 1$; *Gleichung (3.5).*

(e) k *ist die kleinste natürliche Zahl, sodass* $r \mid q^k - 1$; *siehe Lemma 3.6.19.*

Dann und nur dann existiert eine elliptische Kurve $E/\mathbb{F}_q$ *mit Einbettungsgrad* k, *Fundamentaldiskriminante* D, *der Spur* $t \neq 0$ *und einer Torsionsgruppe* $E(\mathbb{F}_q)[r]$, *die* r *Elemente enthält.*

Beweis Der Beweis ergibt sich aus den bisher eingeführten Definitionen. Der Satz ist keine allgemeine Aussage darüber, wann eine elliptische Kurve existiert, sondern lediglich wann eine Kurve mit speziellen Eigenschaften existiert. Obwohl die folgenden Algorithmen auch auf supersinguläre Kurven anwendbar sind, wollen wir uns nicht mit ihnen beschäftigen und schließen sie mittels $t \neq 0$ einfach aus. Somit ergibt sich der Beweis leicht, da *(a)*, *(c)* und *(e)* äquivalente Definitionen zur Existenz eines Körpers, der Spur t und der Fundamentaldiskriminante D respektive des Einbettungsgrades k sind. Schließlich garantieren *(b)* und *(d)* dass es eine prime Untergruppe der Kurve gibt, welche Ordnung r besitzt. Hier folgt die Äquivalenz direkt aus der (bewiesenen) Weil-Vermutung 3.6.14. Zum Beweis siehe auch [FST06] Seite 7-8. □

Bemerkung 3.6.22. *Wir werden* r *so wählen, dass die Kurve die richtige kryptografische Größenordnung besitzt. Zusätzlich ist es wünschenswert, dass* $\frac{r}{R}$ *möglichst nahe an* 1 *liegt. Ist* R *prim, dann ist sogar* $r = R$, *was sich später als Vorteil herausstellen wird, siehe Definition 3.8.2.*

3.7 Paarungen

Wir haben nun einige Eigenschaften von elliptischen Kurven kennengelernt. Im Verlaufe der Arbeit wurde bereits angedeutet, dass wir mittels elliptischer Kurven ver- und entschlüsseln wollen. Daher werden wir nun kurz einen Einblick geben, wie elliptische Kurven in der Kryptografie eingesetzt werden. Bekannt ist das auch unter dem Akronym ECC (engl.: Elliptic Curve Cryptography). Eine leichte und sehr gut zu lesende Einführung bietet Koblitz [Kob98] in Kapitel VI. Außerdem sehr hilfreich zum Verständnis von Paarungen ist Kapitel X in [BSS05]. Für Verschlüsselungen, die nicht auf Paarungen basieren, siehe `http://www.certicom.com/index.php?action=ecc_tutorial,home`.

Paarungen wurden erstmals dazu verwendet das diskrete Logarithmus Problem (DLP) auf einem endlichen Körper anzugreifen. Heute werden elliptische Kurven auf verschiedene Arten verwendet. Zum einen kann mittels Paarungen die Verschlüsselung direkt auf der elliptischen Kurve generiert werden, Paarungen können aber auch dazu verwendet werden, Punkte der elliptischen Kurve in den endlichen Körper zu übersetzen. Sowohl das Diffie-Hellman-, das Massey-Omura- als auch das ElGamal-Verschlüsselungsverfahren kann auf elliptische Kurven angewendet werden.

Wir geben zunächst eine Verschlüsselungsmethode an, die nicht auf Paarungen basiert. Wir möchten einen Text verschlüsseln und einigen uns vorab auf eine elliptische Kurve $E/\mathbb{F}_q$, einen Basispunkt $B \in E$ und auf eine Methode der Chiffrierung (d.h. lesbarer Text wird reversibel in Zeichen / Elemente der elliptischen Kurve abgebildet). Jeder Nutzer des Kryptosystems besitzt einen geheimen Schlüssel. Für Agate sei dieser einmal $a \in \mathbb{F}_q$. Außerdem besitze jeder Nutzer einen öffentlichen Schlüssel, der sich als $[a]B$ berechnet. Möchte Boris nun den chiffrierten Text $P \in E$ an Agate übermitteln, so generiert er sich eine beliebige Zahl k, berechnet dann $[k]B$ und $P + [k]([a]B)$ und überträgt $([k]B, P + [k][a]B)$. Agate kann dann mittels ihres geheimen Schlüssels a durch die Operation $P + [k]([a]B) - [a]([k]B) = P$ die Nachricht decodieren. Die Sicherheit des Verfahrens beruht dann drauf, dass aus der Kenntnis von B und $[a]B$ der geheime Schlüssel $[a]$ bzw. a und dementsprechend die Nachricht P nicht ohne Lösen des DLPs rekonstruiert werden kann.

Wir geben nun ein auf elliptischen Kurven basierendes Verfahren an, welches eindeutige Identifizierung ermöglicht. Es werde vorab ein geheimer Schlüssel s, der zum Beispiel von einer vertrauenswürdigen Quelle (Trust Authority) ausgegeben wird, eine elliptische Kurve und eine bilineare Funktion e (eine Paarung) bestimmt. Nun seien A und B zwei private Schlüssel von Agate und Boris; $[s]A$ und $[s]B$ seien die zugehörigen öffentlichen Schlüssel. Möchten nun Agate und Boris miteinander kommunizieren, so berechnet Agate mittels des öffentlichen Schlüssels von Boris das Element $e(A, [s]B)$ und Boris berechnet mittels Agates öffentlichem Schlüssel das Element $e([s]A, B)$. Die Bilinearität der Paarung garantiert, dass $e(A, [s]B) = e(A, B)^s = e(A, [s]B)$. Dieser Wert ist eindeutig und kann allein aus der Kenntnis von $e, [s]A$ und $[s]B$, also ohne Kenntnis von s, nicht rekonstruiert werden. Daher ist für Agate und Boris $e(A, B)^s$ ein gemeinsamer, geheimer Schlüssel.

Im Wesentlichen verläuft dies analog zu einer Verschlüsselung mittels RSA. Ein Vorteil der elliptischen Kurven und Paarungen liegt darin, dass mehrere geheime Schlüssel $s_1, s_2, ...$ von verschiedenen Trust Authorities verwendet werden können. Wir berechnen zum Beispiel $e([s_1][s_2]A, B) = e(A, [s_1][s_2]B)$. Ohne die Komplexität des Verfahrens zu erhöhen, ist es uns möglich, auch Sicherheit gegenüber einer Trust Authority zu erhalten. Ausführlicher siehe [BSS05].

Das DLP kann also mittels Paarungen auf elliptischen Kurven realisiert werden. Deshalb wollen wir nun zunächst formal den Begriff der Paarung einführen. Dann werden wir sehen, dass wir diese zwar auf allen elliptischen Kurven definieren können, sie auf ihnen aber nicht immer effizient berechnen können. Auf manchen Kurven laufen Algorithmen dank verschiedener Tricks (siehe unter anderem [ELM03], [RS07]) schneller. Außerdem sind Berechnungen auf Untergruppen von Kurven langsamer, wenn die Berechnung auf der gesamten Kurve, anstatt der Untergruppe, geschieht. Dies motiviert den Begriff der paarungsgeeigneten Kurve.

Definition 3.7.1. (Paarung) *Eine nicht entartete, bilineare Funktion über zwei elliptischen Kurven in die multiplikative Gruppe eines endlichen Körpers nennen wir* Paarung. *Sie wird in der Regel mit e bezeichnet. Formal bedeutet dies:*

$$e : G_1 \times G_2 \longrightarrow G_T.$$

Mit $G_1 = E_1(\mathbb{F}_{q^k}), G_2 = E_2(\mathbb{F}_{q^k})$ *und* $G_T = \mathbb{F}_{q^k}$.

Im Folgenden werden wir kurz aufzeigen, warum in der Literatur Paarungen durchaus auf Untergruppen von G_1 und G_2 definiert werden, siehe unter anderem [BSS05] und [BN05].

In der Anwendung werden Paarungen in der Regel auf zwei gleichen elliptischen Kurven definiert, also $E_1 = E_2 = E$. Außerdem wählen wir G_1 als r-Torsionsgruppe. Dies hat den Vorteil, dass wir auch über dem algebraischen Abschluss mit endlichen Gruppen arbeiten. Da die volle r-Torsionsgruppe Ordnung r^2 hat, siehe Satz 5.4.9, wird folglich jede r-Torsionsgruppe L-rationaler Punkte $E(L)[r]$ als Untergruppe von $E[r]$ maximal r^2 Elemente beinhalten. Weiter schränken wir G_2 auf Restklassen ein. Dazu wählen wir $G_2 = E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$, siehe [BSS05] Kapitel IX.3. Die Paarung bildet also ab von:

$$e\colon E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow G_T.$$

Falls $E(\mathbb{F}_{q^k})$ keine Punkte der Ordnung r^2 besitzt, so sind $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ und $E(\mathbb{F}_{q^k})[r]$ isomorph und wir erhalten einen neuen, dem ursprünglichen recht ähnlichen Definitionsbereich:

$$e\colon E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \longrightarrow G_T.$$

Da wir G_2 aber im Wesentlichen auf Restklassen eingeschränkt haben, ist die Paarung lediglich bis auf r-te Potenzen definiert, daher bilden wir nach $G_T = \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$, was isomorph zu $\mu_r = \mathbb{F}^*_{q^k}[r] \subset \overline{\mathbb{F}}_q$ ist, ab. Dieser Schritt ist auch bekannt unter *final exponentiation*.

$$e\colon E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \longrightarrow \mu_r \subset \mathbb{F}_{q^k}.$$

Dabei liegt μ_r als Erweiterung über $\mathbb{F}_q$ in genau einem Körper minimal. Es gilt dann: $\mu_r \not\subset \mathbb{F}_{q^{k-1}}$ aber $\mu_r \subset \mathbb{F}_{q^k}$. Hierbei ist k gerade der Einbettungsgrad,

siehe Definition 3.6.18, für den sowohl gilt, dass die volle Torsionsgruppe $E[r] \subset E(\mathbb{F}_q)$ als auch $\mu_r \subset \mathbb{F}_{q^k}$ gilt. Wir erinnern uns nun an die Definition des Einbettungsgrades. Dabei war k abhängig von E und r. Eine Paarung, welche auf einer r-Torsionsgruppe definiert ist, legt beide Parameter fest, sodass wir auch von dem Einbettungsgrad der Paarung sprechen.

Nachdem wir Paarungen auf ihren idealen Definitionsbereich eingeschränkt haben, geben wir die expliziten Beispiele auf ihrem in der Literatur vorrangig anzutreffenden Definitionsbereich an.

Definition 3.7.2. (Weil Paarung) *Sei E/K eine elliptische Kurve und r eine Primzahl mit* $\mathrm{ggT}(r, \mathrm{char}(K)) = 1$. *Die* Weil Paarung *ist dann die nicht entartete, bilineare Funktion mit:*

$$e_r \colon E[r] \times E[r] \longrightarrow \mu_r.$$

Seien weiter $P, Q \in E[r]$, D und D' Divisoren von Grad 0 mit disjunktem Träger, welche die folgenden Äquivalenzen erfüllen: $D \sim (P) - (\mathcal{O})$ und $D' \sim (Q) - (\mathcal{O})$. Außerdem seien f und g Funktionen aus $K(E)$, sodass für deren Divisoren gilt: $(f) = [r]D$ und $(g) = [r]D'$. Dann berechnet sich der Wert der Weil Paarung durch:

$$e_r(P, Q) = \frac{f(D')}{g(D)}.$$

Siehe [BSS05] Kapitel IX.6.

Die Weil Paarung ist zwar die älteste Paarung, hat aber den großen Nachteil, dass ihre Einschränkung auf Unterräume möglicherweise degeneriert und damit nicht nützlich ist. Für weitere Eigenschaften und Anwendungen der Weil Paarung siehe [BSS05] Kapitel IX.6 oder [Sil86] Kapitel III.8.

Bevor wir zu einer weiteren, von der Weil Paarung abgeleiteten Paarung kommen, benötigen wir folgende Notation.

Definition 3.7.3. (Notation einer Funktion mit gegebenem Punkt) *Für jede natürliche Zahl s und für jeden $P \in C$ sei $f_{s,P}$ eine Funktion deren Divisor gegeben ist durch:*

$$(f_{s,P}) = [s](P) - (sP) - (s-1)\mathcal{O}.$$

Definition 3.7.4. (Tate Paarung, reduzierte Tate Paarung) *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und r eine (große) Primzahl für die gilt: $r|R$. Sei k der Einbettungsgrad bezüglich r und $E[r] \subset E(\mathbb{F}_{q^k})$. Weiter seien $P \in E(\mathbb{F}_q)[r]$ und $Q \in E(\mathbb{F}_{q^k})$. Sei D ein Divisor mit $D \sim (Q \oplus R) + (R)$ für einen beliebigen Punkt $R \in E(\mathbb{F}_{q^k})$. Dann ist die* Tate Paarung $\langle \cdot, \cdot \rangle_r$ *wohldefiniert durch:*

$$\begin{aligned} \langle \cdot, \cdot \rangle_r \colon E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \\ (P, Q) &\longmapsto \langle P, Q \rangle_r = f_{r,P}(D) \end{aligned}$$

Dies liefert jedoch nur den Wert einer Restklasse von $(\mathbb{F}_{q^k}^*)^r$. *Da bei kryptografischen Anwendungen ein eindeutiger Wert in* $\mathbb{F}_{q^k}^*$ *benötigt wird, definieren wir die* reduzierte Tate Paarung *durch abschließende „final exponentiation“ mit* $(q^k-1)/r$*:*

$$e(P,Q) := \langle P,Q\rangle_r^{(q^k-1)/r} = f_{r,P}(D)^{(q^k-1)/r}$$

Auch für die Tate Paarung existieren weitere Modifikationen, die entwickelt wurden, um die Paarungsberechnungen zu beschleunigen. Die Ate Paarung ist eine Kombination aus der Tate Paarung und der hier nicht erwähnten Eta Paarung.

Definition 3.7.5. (Ate Paarung) *Sei* E *eine elliptische Kurve über* $\mathbb{F}_q$, r *eine große Primzahl mit* $r|R$. *Weiter seien* t *die Spur des relativen Frobenius-Endomorphismus* ϕ_q *und* $T := t-1$, $P \in G_1 := E[r] \cap \mathrm{Ker}(\phi_q - [1])$ *sowie* $Q \in G_2 := E[r] \cap \mathrm{Ker}(\phi_q - [q])$. *Dann definiert*

$$f_{T,Q}(P)$$

eine bilineare Paarung auf $G_2 \times G_1$, *die wir* Ate Paarung *nennen.*

Der Hauptunterschied zu den vorher benutzen Paarungen ist, dass die Ate Paarung zusätzlich auf die Eigenräume des Frobenius-Endomorphismus eingeschränkt ist. In [HSV06] ist die Ate Paarung ausführlich beschrieben und ein Zusammenhang zur Tate Paarung hergestellt. Es existieren auch weitere, speziellere Paarungen wie die Twisted Ate Paarung, siehe wiederum [HSV06], oder eine optimierte Version der Ate Paarung [MKHO07]. Die ausführliche Behandlung von Paarungen würde den Rahmen dieser Diplomarbeit sprengen. Wir verweisen hierzu auf die Diplomarbeit von Anika Frischwasser [Fri08], welche sich mit der Weiterentwicklung von Paarungen auf hyperelliptischen Kurven beschäftigt.

3.8 Elliptischen Kurven in der Kryptografie

Unser Verständnis von Paarungen nutzen wir jetzt dazu, zusätzliche Forderungen an die Eigenschaften der elliptischen Kurven zu stellen, sodass die Kurven und somit die möglichen Paarungen auf ihnen aus kryptografischer Sicht interessanter werden.

3.8.1 Anforderungen an elliptische Kurven

Definition 3.8.1. (Paarungsgeeignet) *Sei* E *eine elliptische Kurve über einem endlichen Körper* $\mathbb{F}_q$. E *heißt* paarungsgeeignet *(engl.: pairing friendly), wenn folgende zwei Bedingungen gelten:*

(a) Es gibt eine Primzahl $r \geq \sqrt{q}$, *die* $|E(\mathbb{F}_q)|$ *teilt.*

(b) Der Einbettungsgrad von E *bezogen auf* r *ist kleiner als* $\frac{\log_2(r)}{8}$.

Bedingung *(a)* garantiert, dass die Kurven nicht zu viel unnütze Information enthalten und dass die r-Torsionsgruppe nicht trivial, also verschieden von $\mathcal{O}$, ist. Bedingung *(b)* sichert, dass die Paarungen relativ schnell zu berechnen sind, aber der endliche Körper auch vor Angriffen geschützt ist, siehe auch 3.8.2. Der Wert $\frac{\log_2(r)}{8}$ stammt aus [FST06] Definition 2.3 und ist willkürlich gewählt. Bedeutsam ist lediglich, dass der Einbettungsgrad klein im Verhältnis zur verwendeten Torsionsgruppenordnung r ist.

Definition 3.8.2. (Sicherheitsparameter ρ) *Die Qualität (Sicherheit) der Kurve messen wir dann anhand des* Sicherheitsparameters ρ *mit* $\rho := \frac{\log q}{\log r}$.

Dabei gibt ρ an, um welchen Faktor der Grundkörper größer ist als die benutzte Torsionsgruppe, also wie viel Information des Körpers nicht verwendet wird. Vorzugsweise sollte der Wert nahe bei 1 liegen. Dies ist aber nicht immer möglich. Weiter besteht zur Größe der multiplikativen Gruppe folgender Zusammenhang:

$$\frac{log(q^k)}{log(r)} = \rho \cdot k \tag{3.7}$$

Dies motiviert also die Suche nach paarungsgeeigneten ordinären elliptischen Kurven. Unser Ziel wird es also sein, Algorithmen zur Erzeugung von elliptischen Kurven anzugeben, sodass ρ möglichst klein und k klein aber variabel ist. Der nächste Abschnitt 3.8.2 versucht diesen Zusammenhang weiter zu erläutern, siehe auch [FST06] Kapitel 1. Dank des Satzes 3.6.21 über spezielle elliptische Kurven, haben wir ein Mittel zur Hand, welches etliche Kurven liefert. Nun müssen wir aus ihnen die Kurven herausfiltern, die paarungsgeeignet sind.

3.8.2 Sicherheitsaspekte elliptischer Kurven

Abschließend werden wir uns noch kurz mit Sicherheitsaspekten der Kryptografie beschäftigen. Da uns Paarungen eine Möglichkeit geben zwischen elliptischen Kurven und endlichen Körpern zu wechseln, müssen Angriffe auf beiden Strukturen in Betracht gezogen werden, siehe auch [ACD$^+$06] Kapitel 22.

Der schnellste bekannte Angriff auf elliptische Kurven ist der parallelisierte Pollard-rho-Algorithmus mit einer Laufzeit von $\mathcal{O}(\sqrt{p})$ (was für $p \in \mathbb{P}$ auch $\mathcal{O}(\sqrt{r})$ ist. Das diskrete Logarithmusproblem in der multiplikativen Gruppe endlicher Körper wird am schnellsten durch den Index-Calculus-Angriff gelöst, der eine subexponentielle Laufzeit von ungefähr $\mathcal{O}(e^{c(k \log q)^{1/3}})$ oder genauer $\mathcal{O}(e^{(\log\log q^k \log q^k)^{1/2}})$ hat. Nun sind diese beiden Angriffe mittels Paarungen ineinander überführbar. Möchten wir die gleiche Sicherheit sowohl auf der Kurve als auch im endlichen Körper erreichen, so können wir dies nach Gleichung (3.7) durch Steuerung des Sicherheitsparameters ρ oder des Einbettungsgrades k tun. Wird dabei ρ erhöht, so verlangsamen sich die Arithmetik auf der elliptischen Kurve und die Paarungsauswertung. Konstruktionsbedingt ist ρ allerdings stets größer als 1. In [FST06] Tabelle 8.2 sind die bislang kleinsten bekannten Werte für ρ in Abhängigkeit von D und k gegeben. Da sich ein kleines ρ positiv auf die

Symmetrisch	RSA und Diffie-Hellman entspricht q^k	Elliptische Kurve entspricht r	Ungefähres k bei $\rho = 1$
80	1024	160	7
112	2048	224	10
128	3072	256	12
192	7680	384	20
256	15360	512	30

Tabelle 3.1: Schlüsselgrößen für Verschlüsselungen im Vergleich in bit

Arithmetik der elliptischen Kurve auswirkt, wollen wir für ρ den theoretischen Wert von 1 wählen. Da wir ρ möglichst klein halten möchten, ist also nur k variabel. Es ist so zu wählen, dass die Laufzeiten der beiden Angriffe in etwa gleiche Größenordnung haben. Gleichsetzen der beiden Laufzeiten und Auflösen nach k ergibt in erster Näherung einen Wert von $k \approx \frac{(\log q)^2}{8c^3}$. Dieser hängt jedoch noch sehr stark von dem Parameter c ab. Es lässt sich zwar keine absolute, aber eine relative Aussage treffen. Falls wir q quadrieren, also die Sicherheit von zum Beispiel 128 bit auf 256 bit erhöhen, sollte sich der Einbettungsgrad vervierfachen. D.h. der Einbettungsgrad wächst quadratisch mit der Bit-Zahl. Dies ist natürlich nur eine erste Näherung, sie verdeutlicht aber die Notwendigkeit eines variablen Einbettungsgrades.

Über die eigentliche Laufzeit der Angriffe und daher auch über die benötigten Schlüsselgrößen herrschen in der Literatur jedoch sehr unterschiedliche Meinungen. Die Webseite `http://www.keylength.com/` bietet verschiedene Vergleichsmöglichkeiten zur Sicherheit der Schlüsselgrößen. Tabelle 3.1 stellt eine exemplarische Zusammenstellung dar.
Berechnen wir aus diesen Werten den Faktor, der bei einer Verdopplung der Bit-Zahl entsteht, so wächst der Einbettungsgrad langsamer als quadratisch. Das ist natürlich damit zu erklären, dass wir lediglich eine approximative Formel verwendet haben. Für eine detaillierte Auswertung müssten wir den parallelisierten Pollard-rho-Algorithmus und die Index-Calculus-Methode genauer betrachten.

Diese Analyse liefert aber immerhin den Grund, warum wir uns nicht mit supersingulären elliptischen Kurven beschäftigen wollen. Diese weisen zwar eine sehr einfache Struktur auf, und wir können auf ihnen auch schnell berechenbare Paarungen konstruieren, dennoch haben sie zwei große Nachteile. Zum einen ist ihre Spur immer gleich 0. Dies bedeutet zwar zunächst, dass sich der Sicherheitsparameter zu $\rho = \log p / \log (p + 1)$ berechnet. Ein solcher kommt aber nicht in Frage, da $p + 1$ für $p \in \mathbb{P}, p > 2$ keine Primzahl ist. Somit wird jede Torsionsgruppe nie die volle Kurve ausschöpfen. Zum anderen ist der Einbettungsgrad von supersingulären Kurven beschränkt. Vielmehr gilt:

Satz 3.8.3. (Einbettungsgrad supersingulärer Kurven)
Supersinguläre elliptische Kurven haben einen Einbettungsgrad von $k \leq 6$.

Beweis Siehe [MOV93]. □

Hieraus folgt zwar sofort, dass alle supersingulären Kurven die zweite Bedingung der Definition für Paarungseignung erfüllen. Da aber mit steigender Größe von q auch die notwendige Größe des Einbettungsgrades steigt, sind supersinguläre Kurven schon ab einer Schlüsselgröße von $r = 160$ bit nicht mehr geeignet. Dies ist der Grund, warum supersinguläre Kurven im Allgemeinen als unsicher angesehen werden, auch wenn sie den derzeitigen Sicherheitskriterien (80 bit Verschlüsselung) noch genügen würden.

Verglichen mit dem RSA-Algorithmus gibt es neben der Schlüsselgröße noch einen weiteren Vorteil von elliptischen Kurven. Die Operationen Verschlüsseln und Entschlüsseln lassen sich deutlich schneller berechnen. Der Geschwindigkeitsvorteil liegt bei einer 80 bit Verschlüsselung bei einem Faktor von 3, bei einer 256 bit Verschlüsselung bereits bei einem Faktor von 64 und steigt weiter.

Ein dritter Vorteil der elliptischen Kurven liegt auch darin, dass zu jeder Primzahl und somit zu jedem Primkörper verschiedene Kurven konstruiert werden können. In dem Bereich in dem die Verschlüsselung eine vertretbare Geschwindigkeit besitzt, existieren also deutlich mehr Kurven als Primzahlen.

Kapitel 4

Algorithmen für elliptische Kurven

Nachdem wir im letzten Kapitel die wichtigsten Eigenschaften von elliptischen Kurven kennengelernt haben, werden wir nun dieses Wissen dazu nutzen, paarungsgeeignete Kurven zu generieren. Dazu geben wir in 4.1 einen Überblick über unsere Herangehensweise. In 4.2 werden wir uns mit der CM-Methode beschäftigen. In den folgenden Kapiteln 4.3 bis 4.6 werden wir die Cocks-Pinch-Methode, eine Verallgemeinerung, die Brezing-Weng-Methode und wiederum eine Verallgemeinerung davon erschließen. Anschließend werden wir uns in 4.7 mit der Frage befassen, wie wir überprüfen können, ob gegebene Kurven tatsächlich den erwarteten Anforderungen genügen.

4.1 Struktur der Algorithmen

In diesem Abschnitt beschreiben wir die Struktur der gängigsten Algorithmen zur Erzeugung von elliptischen Kurven. Der Vollständigkeit halber werden wir kurz erwähnen, dass es neben unserer Herangehensweise viele weitere Möglichkeiten gibt, elliptische Kurven zu erzeugen. Da deren Einsatz in der Kryptografie schon lange bekannt ist, gibt es einige Zusammenfassungen. Ein einführendes Buch ist [Kob98]. Eine Zusammenfassung über weitere gängige Möglichkeiten Kurven zu generieren, ist in [FST06] gegeben. Dazu zählen unter anderem die Barreto Naehrig Kurven [BN05], so wie die MNT-Kurven [MNT01].
Unsere vorgestellten Algorithmen folgen alle einer Grundstruktur, siehe auch [FST06] Kapitel 2, die wir hier aber etwas anders aufbrechen werden.

Bemerkung 4.1.1. *Die hier vorgestellten Methoden zur Generierung paarungsgeeigneter, elliptischer Kurven folgen im Wesentlichen einer Struktur:*

(1) Lege den Einbettungsgrad k, die Fundamentaldiskriminante D sowie die Größenordnung von r fest.

(2) Berechne drei ganze Zahlen q, r und t, welche bestimmten Bedingungen genügen, die im Weiteren erläutert werden. Dabei ist wie üblich, q die Anzahl der Elemente des endlichen Körpers, r der Torsionsgruppenparameter und t die Spur der relativen Frobenius.

(3) Erzeuge mittels der eng gefassten CM-Methode die gesuchte Gleichung der elliptischen Kurve.

Zunächst einige Erläuterungen. In Schritt *(1)* legen wir die gewünschte Sicherheit der Kurve fest. Die Parameter r und k sind so zu wählen, dass sie zueinanderpassen, siehe 3.8. Die Fundamentaldiskriminante D kann beliebig gewählt werden. Dann führen wir Schritt *(2)* aus und berechnen für festes k und D die Parameter q, r und t. Auch q bestimmt in gewisser Weise noch die Sicherheit der Kurve. Mittels der gefundenen Werte erzeugen wir in Schritt *(3)* die Gleichung der elliptischen Kurve.
In der Literatur tritt die CM-Methode als Schritt *(2)* und Schritt *(3)* zusammen auf. Hierbei werden solange Parameter getestet, bis der Algorithmus eine Lösung liefert. Da wir verschiedene Methoden zur Parametererzeugung kennenlernen werden, bezeichnen wir Schritt *(3)* als eng gefasste CM-Methode, mit deren Hilfe wir aus gegebenen Parametern die elliptische Kurve erzeugen. Dadurch wird die eng gefasste CM-Methode zu einem deterministischen Prozess, der immer eine Lösung liefert.

Mit diesen Vorbetrachtungen bleiben nur noch zwei Fragen offen. Erstens: Wie wird q, r und t gefunden? Dafür gibt es bereits einige Methoden, zwei davon werden wir im Folgenden erläutern und verallgemeinern, siehe [FST06]. Zweitens: Wie funktioniert die CM-Methode und welche Voraussetzungen besitzt sie? Siehe hierzu [ACD$^+$06] oder [AM93]. Beginnen werden wir im nächsten Abschnitt mit der zweiten Frage.

4.2 CM-Methode

Die CM-Methode wurde erstmals von Atkin und Morain in [AM93] entwickelt. Seitdem ist sie weiterentwickelt worden und kann daher verkürzt wiedergegeben werden. Betrachten wir zunächst den relativen Frobenius ϕ_q einer elliptischen Kurve $E/\mathbb{F}_q$. Sein charakteristisches Polynom ist gegeben durch $\chi(\phi_q)_E(T) = T^2 + tT + q$. Nach der Weil-Vermutung, Gleichung (3.5), wissen wir, dass beide Nullstellen den Absolutbetrag $\sqrt{q}$ haben. Die einzigen reellen Zahlen mit Absolutbetrag $\sqrt{q}$ sind aber $\sqrt{q}$ und $-\sqrt{q}$. Ist $t \neq 0$, was wir voraussetzen, um supersinguläre Kurven auszuschließen, sind beide Nullstellen stets komplex konjugiert. Nach Definition 3.4.1 ist die Polynomialdiskriminante folglich $d(\chi) = t^2 - 4q$. Die Fundamentaldiskriminante D ist bis auf einen eventuellen Faktor von 4 quadratfrei, siehe Definition 3.4.5. Um sie aus der Polynomialdiskriminante zu erhalten, müssen wir aus $d(\chi)$ den quadratfreien Anteil q_f abspalten. Jetzt treffen wir eine Fallunterscheidung: Falls $q_f \equiv 1 \bmod 4$, so

ist $D = q_f$, sonst ist $D = 4q_f$. Diese Fallunterscheidung wird auch bei genauer Untersuchung des Algorithmus wieder auftreten. Wir erhalten eine explizite Form der CM-Gleichung:

$$t^2 - 4q = Dy^2 = \begin{cases} q_f y^2 & \text{falls } q_f \equiv 1 \bmod 4 \quad (\Leftrightarrow D \equiv 1 \bmod 4) \\ 4q_f y^2 & \text{sonst} \qquad\qquad\quad (\Leftrightarrow D \equiv 8, 12 \bmod 16) \end{cases}$$

Die CM-Gleichung ist auch das Kernstück der CM-Methode. Diese werden wir nun angeben, bevor wir die einzelnen Schritte genauer untersuchen. Es sei angemerkt, dass die CM-Methode auch für Primpotenzkörper adaptiert werden kann, wir werden hier aber darauf verzichten.

Algorithmus 1 CM-Methode

Eingabe: $D < -5, D \in \mathbb{Z}$ (Fundamentaldiskriminante), $k > 1, k \in \mathbb{N}$ (Einbettungsgrad), Größenordnung von p bzw. r.

Ausgabe: Elliptische Kurve $E/\mathbb{F}_p$ mit Einbettungsgrad k bezüglich r und einem Endomorphismenring $\mathrm{End}(E)$ isomorph zu einer Ordnung in $\mathbb{Q}(\sqrt{D})$.

1: **repeat**
2: Wähle ein $p \in \mathbb{P}$.
3: Finde für p Lösungen (t, y) der CM-Gleichung

$$t^2 - D \cdot y^2 = 4p.$$

4: **until** Es existiert eine Lösung der CM-Gleichung, welche $r \mid (p - t + 1)$ erfüllt sowie den Einbettungsgrad k besitzt.
5: Berechne das Hilbertsche Klassenpolynom H_D zur Fundamentaldiskriminante D, siehe nächster Abschnitt.
6: Berechne eine Nullstelle j des Hilbertschen Klassenpolynoms $\bmod p$. Dies ist dann die j-Invariante.
7: Erzeuge aus der j-Invarianten die elliptische Kurve mittels der Formel:

$$E\colon y^2 = x^3 + a \cdot x + b \text{ mit } a = -\frac{27j}{4(j - 12^3)} \text{ und } b = \frac{27j}{4(j - 12^3)}. \quad (4.1)$$

8: Überprüfe die Ordnung der Kurve. Ist die Ordnung gleich $p + 1 - t$, so ist E die gesuchte Kurve. Anderenfalls ist der quadratische Twist von E die gesuchte Kurve.

Zunächst einige Bemerkungen.

Bemerkung 4.2.1. *(a) Falls $D = -3$ oder $D = -4$ wäre, so würden wir auf die Schritte 5-7 verzichten. Für diese beiden Fundamentaldiskriminanten kennen wir bereits die j-Invarianten ($j = 0$. bzw. $j = 12^3$.) Für $D = -3$ ist die Kurve durch $a = 0$ in der kurzen Weierstraß-Normalform dann bis*

auf sechs Twists gegeben. Für $D = -4$ ist sie wiederum durch $b = 0$ bis auf vier Twists gegeben. Zu beachten ist, dass $D = -4$ fälschlicherweise oft als $D = -1$ angegeben wird. Dabei erzeugen $D = -4$ und $D = -1$ zwar die gleichen Körpererweiterungen, aber nur $D = -4$ ist eine Fundamentaldiskriminante.

(b) Der als Lösung der CM-Gleichung berechnete Parameter $t \neq 0$ ist die Spur des Frobenius, siehe Definition 3.6.12. Dieser soll verschieden von null sein, damit die Kurve nicht supersingulär ist.

(c) Die Hilbertschen Klassenpolynome zerfallen modulo p in Linearfaktoren. Für p und D teilerfremd ist jede dieser Nullstellen des Klassenpolynoms einfach, siehe Satz 3.6.5, und eine zulässige j-Invariante. Da sie im nicht reduzierten Fall alle dieselbe Körperweiterung, den Hilbertschen Klassenkörper erzeugen, siehe Satz 4.2.3, werden sie das auch modulo p tun.

(d) Der Algorithmus funktioniert für beliebige $D < -2$. Aufgrund von Beschränkungen der Computerrechenleistung wird gefordert, dass D eine gewisse Grenze nicht unterschreiten darf, momentan sinnvoll ($D > -10^{10}$) siehe [FST06] Kapitel 2, da sonst die Klassenpolynome nicht mehr in angemessener Zeit berechnet werden können.

(e) Anstatt den Algorithmus mit Hilbertschen Klassenpolynomen zu implementieren, wird die j-Invariante aus Weberpolynomen zurückgewonnen. Diese können besser tabellarisch gespeichert werden, da sie deutlich kleinere Koeffizienten besitzen. Somit ist in Schritt 5 nur eine Abfrage und keine aktive Berechnung erforderlich.

(f) Wählen wir als Input-Parameter p, r, t, D, k, die bereits eine elliptische Kurve erzeugen, so beschreiben die Schritte 5-8, wie wir daraus die Kurve erzeugen. Wir bezeichnen daher die Schritte 5-8 als eng gefasste CM-Methode.

Grob gesprochen besteht die CM-Methode aus zwei Teilen. Zum einen dem Lösen der CM-Gleichung, zum anderen der Erzeugung der Kurve mittels der Hilbertschen Klassenpolynome (bzw. der Weberpolynome). In [AM93] Kapitel 7 ist beschrieben, wie aus tabellierten Weberpolynomen die Hilbertschen Klassenpolynome erzeugt werden. Wir werden aus Gründen der Vollständigkeit die Erzeugung der Hilbertschen Klassenpolynom ansprechen. Danach erklären wir, wie wir überprüfen welcher Twist der Kurve der gesuchte ist, bevor wir uns dem Lösen der CM-Gleichung zuwenden.

4.2.1 Hilbertsche Klassenpolynome

Die Theorie der Klassenpolynome ist in [ACD$^+$06] Kapitel 5.1.5 beschrieben und dort in Kapitel 18.1. zusammengefasst. Außerdem ist sie im Anhang C von [Sil86] zu finden. Wir werden hier kurz die Konstruktion andeuten.

Definition 4.2.2. (Reduzierte, binäre quadratische Form) *Eine quadratische Form $ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ heißt* reduzierte, binäre quadratische Form*, wenn sie folgende Bedingungen erfüllt:*

(a) $|b| \leq a \leq c$.

(b) $b \geq 0$ *falls* $a = |b|$ *oder* $a = c$.

(c) $\mathrm{ggT}(a, b, c) = 1$.

Siehe [ACD+06] Definition 18.2.

Quadratischen Formen, welche durch Elemente aus $\mathrm{SL}_2(\mathbb{Z})$ ineinander überführt werden können, heißen äquivalent. Wir können zeigen, dass jede Äquivalenzklasse - bezüglich Transformation von binären quadratischen Formen - genau eine reduzierte, binäre quadratische Form besitzt. Diese reduzierten Formen definieren wiederum ein eindeutiges Ideal $I_\tau = \mathbb{Z} + \tau\mathbb{Z}$, mit

$$\tau = \frac{b + \sqrt{b^2 - 4ac}}{2a}.$$

Der bekannte Ausdruck unter der Wurzel ist die Polynomialdiskriminante $D = b^2 - 4ac$. Aus *(a)* folgt, dass sie stets negativ ist. Es kann gezeigt werden, dass die Anzahl der verschiedenen reduzierten, binären quadratischen Formen mit gleichem D endlich ist. Sie entspricht der Mächtigkeit der Idealklassengruppe von $K = \mathbb{Q}(\sqrt{D})$, siehe Definition 2.4.21, also der Klassenzahl h_D. Zu jedem $I_{\tau_i}, i \in \{1, 2, \ldots, h_D\}$, definieren wir:

$$j(I_{\tau_i}) = \frac{\left(1 + 240 \sum_{n=1}^{\infty} \sigma(n) q^n\right)^3}{q \prod_{n=0}^{\infty} (1 - q^n)^{24}}$$

mit $q = e^{2\pi i \tau_i}$ und $\sigma(n) = \sum_{t|n} t^3$.
Über die $j(I_{\tau_i})$ lässt sich nun eine Reihe von Aussagen treffen:

Satz 4.2.3. (Weber, Fueter)
Sei $K/\mathbb{Q}$ ein quadratischer CM-Körper, $\mathcal{O}_K \subset K$ dessen Maximalordnung und $\mathcal{C}\ell(\mathcal{O}_K)$ die zugehörige Idealklassengruppe. Dann gilt:

(a) $j(I_{\tau_i})$ *ist ganz über* $\mathbb{Q}$.

(b) Seien $I_{\tau_1}, \ldots, I_{\tau_{h_D}}$ ein Erzeugendensystem von $\mathcal{C}\ell(\mathcal{O}_K)$. Die zugehörigen j-Invarianten $j(I_{\tau_1}), \ldots, j(I_{\tau_{h_D}})$ sind dann invariant unter den Galois-Automorphismen $\mathrm{Aut}(K(j(I_{\tau_i}))/K)$. Sie erzeugen also alle den Körper $K(j(I_{\tau_i}))$, den wir als Hilbertschen Klassenkörper bezeichnen. Er ist die maximale unverzweigte Abelsche Erweiterung von K.

Beweis Siehe [Lan87] Theorem 5.4 und Theorem 10.1. □

Dann berechnet sich das Hilbertsche Klassenpolynom aus den $j(I_{\tau_i})$:

Definition 4.2.4. (Hilbertsches Klassenpolynom) *Seien die $j(I_{\tau_i})$ definiert wie oben. Dann ist das* Hilbertsche Klassenpolynom *definiert als:*

$$H_D(x) = \prod_{i=1}^{h_D} \big(x - j(I_{\tau_i})\big).$$

Es besitzt Koeffizienten aus $\mathbb{Z}$. Siehe [ACD+06] Korollar 5.48.

Alle Berechnungen werden über $\mathbb{C}$ durchgeführt, da wir wissen, dass $H_D(x) \in \mathbb{Z}[x]$, muss nur eine bestimmte Genauigkeit eingehalten werden. Da die Reduktion modulo p ein Gruppenhomomorphismus ist, siehe 3.6.1, folgt nun für p mit guter Reduktion, teilerfremd zu D, dass das modulo p reduzierte Hilbertsche Klassenpolynom das Klassenpolynom von $E/\mathbb{F}_p$ ist. Die Nullstellen des reduzierten Polynoms sind also j-Invarianten der reduzierten Kurve. Durch Einsetzen in Gleichung 4.1, können wir eine Kurve mit passender j-Invariante erzeugen.

4.2.2 Ordnungen von Twists

Die CM-Methode bestimmt also die elliptische Kurve anhand ihrer j-Invarianten. Diese kennzeichnet die Kurve aber nur bis auf $\overline{K}$-Isomorphie und Twists eindeutig, siehe Bemerkung 3.3.14. Um herauszufinden, welcher Twist der Kurve gesucht ist, müssen wir die Ordnungen der Twists herausfinden. Sie muss gleich $p - t + 1$ sein. Dazu nutzen wir die Gruppenstruktur der Kurve aus. Aus der Gruppentheorie wissen wir, dass jedes Element einer Gruppe, potenziert (bzw. multipliziert) mit der Gruppenordnung das neutrale Element ergibt. Für ein beliebiges Element $P \neq \mathcal{O}$ berechnen wir RP. Ist dies nicht $\mathcal{O}$, so wissen wir, dass die Gruppenordnung nicht R teilt und somit nicht die gesuchte Kurve ist. Falls $RP = \mathcal{O}$, so haben wir einen möglichen Kandidaten gefunden. Leider können auch hier verschiedene Fälle auftreten: Erstens, die Gruppenordnung ist richtig gewählt. Zweitens, die Gruppenordnung ist ein Teiler von R, drittens, der Exponent der Kurve ist nicht gleich der Gruppenordnung oder viertens, wir haben ein Element nicht maximaler Ordnung gewählt, sodass die wirkliche Ordnung der Gruppe ein Vielfaches des fälschlicherweise angenommenen R ist.

Falls R jedoch prim ist, so existiert Fall 2 nicht. Auch Fall 3 und 4 können wir ausschließen. Durch die Hasse-Weil-Schranke kennen wir den Bereich, in dem die Gruppenordnung liegen muss. Damit zwei Ordnungen echt Teiler voneinander sind, müsste das Doppelte der unteren Schranke kleiner sein als die obere Schranke, also $2 \cdot (p + 1 - 2\sqrt{2}) \leq (p + 1 + 2\sqrt{2})$. Umformen liefert als Bedingung: $(1 - \sqrt{p})^2 \leq 0$, welche nie erfüllt ist. Somit schließen wir aus, dass die Gruppenordnung echt größer als R ist.
Ist R nicht prim, so können wir durch einen solch leichten Test keine Aussage treffen. Wir erläutern die Fälle 2 und 3 an Beispielen.

Beispiel 1: Sei $p = 17$, somit ergeben sich nach der Hasse-Weil-Ungleichung die Schranken 10 und 26. Weiter sei $t = 3$, sodass E_1/K mit $R_1 = 21$ und E_2/K mit $R_2 = 15$ existieren. Nehmen wir an, R_1 sei die gesuchte Kurve. Alle K-rationalen Punkte von E_1 werden durch 21-fache Addition auf $\mathcal{O}$ abgebildet, allerdings existieren auf E_2 zum Beispiel Elemente der Ordnung 3. Diese werden durch 21-fache Addition auch auf $\mathcal{O}$ abgebildet.

Beispiel 2: Sei $p = 19$. Es ergeben sich Schranken 12 und 28. Für $t = 4$ ergeben sich Gruppenordnungen von $R_1 = 16$ bzw. $R_2 = 24$. Für die Kurve $E_1 \colon y^2 = x^3 + 5x + 1$ werden aber alle Elemente schon durch 8-fache Addition auf $\mathcal{O}$ abgebildet. Überprüfen wir daher Elemente von E_1 und E_2 mittels 24-facher Addition, so werden alle Punkte beider Kurven auf $\mathcal{O}$ abgebildet.

Um in diesen beiden Fällen herauszufinden, welches die richtige Kurve ist, gibt es aber noch andere Methoden. Das Problem in Beispiel 1 können wir angreifen, indem wir mehrere Punkte überprüfen, um die Wahrscheinlichkeit zu erhöhen, die richtige Kurve zu finden. Das Problem in Beispiel 2 könnten wir dadurch lösen, dass wir einfach alle Punkte der Kurve zählen, d.h. für alle Punkte aus $(\mathbb{F}_{19})^2$ testen, ob sie die definierende Gleichung erfüllen. Natürlich löst jeder deterministische Algorithmus, der die Kurvenordnung bestimmt, das Problem.

Diese deterministischen Algorithmen besitzen aber in unseren Fällen sehr große Laufzeiten. Da die Fälle 2 und 3 sehr selten auftreten, begnügen wir uns damit, Fall 4 auszuschließen, indem wir fünf Punkte wählen und ihre R-fache Addition überprüfen. Da wir für Primzahltests auch randomisierte Algorithmen benutzen, verschlechtert die abermalige Randomisierung den Algorithmus nicht.

4.2.3 Lösung der CM-Gleichung

Nach dieser genaueren Betrachtung der Schritte 5-8, wollen wir uns nun dem ersten Teil des Algorithmus zuwenden. Zunächst werden wir erläutern, welche Rolle die oben angesprochene Fallunterscheidung spielt. Betrachten wir zunächst den Fall $D \equiv 0 \bmod 4$. Konkret bedeutet dies:

$$t^2 - Dy^2 = t^2 - 4q_f y^2 = 4p.$$

Wir sehen, dass t gerade ist, daher können wir das Problem vereinfachen zu:

$$(t/2)^2 - q_f y^2 = p.$$

Dies ist eine Verallgemeinerung eines historischen Problems von Fermat: Wann kann eine ungerade Primzahl durch die Summe zweier Quadrate beschrieben werden? Der Algorithmus von Cornacchia, siehe [ACD+06] Algorithmus 18.4 oder [Coh93] Algorithmus 1.5.2, löst genau diese Problemstellung.
Für den Fall $D \equiv 1 \bmod 4$ ergibt sich:

$$t^2 - Dy^2 = t^2 - q_f y^2 = 4p.$$

Hierbei ist apriori nicht klar, ob t (oder äquivalent dazu y) ungerade ist. Also lässt sich der zweite Fall nicht auf den ersten zurückführen. Sehr ausführlich ist dies in [Coh93] Kapitel 1.5 beschrieben. Daher werden wir hier einen modifizierten Algorithmus angeben, der den zweiten Fall löst und trivialerweise auch den ersten Fall mit einschließt.

Der Algorithmus berechnet eine Wurzel von $D \bmod p$, also muss D ein Quadrat $\bmod p$ sein, was durch das Legendresymbol ausgedrückt wird: $\left(\frac{D}{p}\right) = 1$. Angemerkt sei noch, dass die Gleichung weder eine eindeutige, noch überhaupt eine Lösung besitzen muss.

Algorithmus 2 Modifizierter Cornacchia Algorithmus

Eingabe: $D < -3, D \in \mathbb{Z}$ und $p > 2, p \in \mathbb{P}$ mit $\left(\frac{D}{p}\right) = 1$ und $-D < 4p$.

Ausgabe: $(t, y) \in \mathbb{Z}^2$ mit $(t/2)^2 - q_f y^2 = p \Leftrightarrow t^2 - Dy^2 = 4p$ oder „Keine Lösung“.

1: Berechne eine Wurzel β von $D \bmod p$, also $\beta^2 \equiv D \bmod p$. Wähle β so, dass $0 \leq \beta < p$.
2: **if** $\beta \not\equiv D \bmod 2$ **then**
3: $\quad \beta := p - \beta$.
4: **end if**
5: Setze $u := 2p, v := \beta$ und $w := \lfloor 2\sqrt{p} \rfloor$.
6: **while** $v > w$ **do**
7: $\quad r := u \bmod v$.
8: $\quad u := v$.
9: $\quad v := r$.
10: **end while**
11: **if** $D \nmid 4p - v^2$ oder $(4p - v^2)/D$ ist kein Quadrat **then**
12: $\quad$ **return** Keine Lösung.
13: **else**
14: $\quad$ **return** $(t, y) = (v, \sqrt{(4p - v^2)/-D})$.
15: **end if**

Siehe [Coh93] Algorithmus 1.5.3. Die gefundenen Parameter verwenden wir dann weiter in Zeile 5 der CM-Methode.

4.3 Cocks-Pinch-Algorithmus

Die CM-Methode findet also eine Kurve mit vorgegebener Fundamentaldiskriminante D und vorgegebenem Einbettungsgrad k, indem Schritte 1-4 als Schleife durchlaufen werden. Auch wenn wir mittels des Algorithmus von Cornacchia mit Sicherheit sagen können, ob die CM-Gleichung eine Lösung besitzt oder nicht,

bedeutet dass nicht, dass sich die Laufzeit der Schleife abschätzen lässt oder aber zumindest „kurz“ ist. Dies liegt daran, dass in Schritt 4 weitere Bedingungen an die Kurve gestellt werden. Die Anforderungen an den Einbettungsgrad führen dazu, dass eine zufällige Kurve fast nie paarungsgeeignet ist.

Dies ist genau der Ansatzpunkt des Cocks-Pinch-Algorithmus, siehe [CP01] nicht publiziert, daher [FST06] Theorem 4.1. Bevor wir geeignete Kurvenparameter suchen, schränken wir uns auf Kurven von gewünschtem Einbettungsgrad ein, siehe hierzu [FST06] in Kapitel 4 oder vergleiche aktuelle Vorträge von Freeman, Scott oder Teske. Wir wollen zunächst wieder den Algorithmus angeben, danach einige Bemerkungen machen, bis wir schließlich erklären, warum der Algorithmus auch tatsächlich eine Lösung liefert.

Algorithmus 3 Cocks-Pinch-Algorithmus

Eingabe: $D < 0, D \in \mathbb{Z}, k \geq 1, k \in \mathbb{N}$ sowie r_0, welches die Größenordnung der r-Torsionsgruppe angibt.

Ausgabe: Parameter $p, r \in \mathbb{P}$ und $t \in \mathbb{Z}$, sodass die CM-Gleichung (3.6) erfüllt ist. Außerdem wird garantiert, dass für einen Twist der mit diesen Parametern erzeugten Kurve gilt: Er hat Einbettungsgrad k und seine Ordnung R wird von r geteilt.

1: **repeat**
2: Wähle $r > 5, r \in \mathbb{P}$ sodass $k|(r-1)$ und $\left(\frac{D}{r}\right) = 1$.
3: Berechne $\sqrt{D}$ in $\mathbb{Z}/r\mathbb{Z}$.
4: Bestimme alle k-ten primitiven Einheitswurzeln $\zeta_{k,i}$ in der Einheitengruppe von $(\mathbb{Z}/r\mathbb{Z})^*$. Davon existieren $\varphi(k)$ viele.
5: Berechne $t_i \equiv (\zeta_{k,i} + 1) \bmod r$.
6: Berechne $y_i \equiv \frac{\zeta_{k,i}-1}{\sqrt{D}} \bmod r$.
7: Wähle für t_i und y_i die natürlichen Vertreter aus $]0, r]$.
8: Berechne $p_i = \frac{1}{4}(t_i^2 - Dy_i^2) \in \mathbb{Z}$. .
9: **until** p_i ist eine Primzahl. (Setze für dieses i dann $p := p_i, t := t_i$.)
10: **return** p, t und r.

Bemerkung 4.3.1. *(a) Die Parameter (p, t, r, D, k) können als Input für die eng gefasste CM-Methode verwendet werden.*

(b) Es kann vorkommen, dass p_i für mehrere i prim ist und so mehrere Lösungen geliefert werden. In diesem Fall spielt es keine Rolle, welches der i wir betrachten. In der Analyse des Algorithmus werden wir den Index i weglassen und wollen damit andeuten, dass die jeweiligen Parameter t, y, ζ zu einer Lösung p_i gehören.

(c) Beachte, dass $r \in \mathbb{P}$ gewählt wird. Dabei ist nur sichergestellt, dass $r|R = p + 1 - t$. Wir werden zeigen, dass wir für $\rho = \frac{\log p}{\log r}$ ungefähr 2 erwarten können, siehe 4.5.

(d) Aufgrund der Bedingung $\left(\frac{D}{r}\right) = 1$ ist die Existenz der Wurzel $\sqrt{D} \in \mathbb{Z}/r\mathbb{Z}$ garantiert. Gibt es mehrere, so sind diese beliebig mit den k-ten Einheitswurzeln kombinierbar, um in Zeile 6 die y_i zu berechnen. Dies sollte auch getan werden, da sonst viele mögliche Lösungen wegfallen. Dies wurde aus Gründen der Übersichtlichkeit ausgelassen.

Wir werden nun kurz erläutern, warum der Algorithmus eine elliptische Kurve mit den gewünschten Parametern findet, indem wir die fünf notwendigen Bedingungen von Satz 3.6.21 nachprüfen. Aus Zeile 8 des Algorithmus folgt, dass die CM-Gleichung (3.6) erfüllt ist. Das so gewählte p wird nur akzeptiert, falls es prim ist. Außerdem haben wir r prim gewählt. Womit drei notwendige Bedingungen schon erfüllt sind. Betrachten wir Zeile 6 des Algorithmus so folgt durch quadrieren:

$$Dy^2 \equiv (t-2)^2 \bmod r \tag{4.2}$$

Andererseits gilt:

$$\begin{aligned} 4R = 4(p+1-t) &\overset{8}{=} 4\left(\frac{(t^2 - Dy^2)}{4} + 1 - t\right) = \\ &= t^2 - Dy^2 + 4 - 4t = -Dy^2 + (t-2)^2 \overset{4.2}{\equiv} 0 \bmod r. \end{aligned} \tag{4.3}$$

Wobei das erste Gleichheitszeichen aus der Definition folgt, das zweite sich aus Zeile 8 ergibt, das dritte und vierte Umformungen darstellen und das fünfte durch Gleichung (4.2) gegeben ist. Wir folgern also: r teilt $4R$. Da nun r aber größer als 5 und prim ist, folgt $r|R : r$ teilt die Anzahl der Punkte der Kurve. Betrachten wir schließlich noch Zeile 5 des Algorithmus so gilt:

$$t \equiv \zeta_k + 1 \bmod r \Leftrightarrow t - 1 \equiv \zeta_k \bmod r.$$

Nun ist ζ_k eine der k-ten primitiven Einheitswurzeln modulo r also Nullstelle des k-ten Kreisteilungspolynoms. Dies, zusammen mit der Voraussetzung $r \nmid k$, ist nach Lemma 3.6.19 äquivalent damit, dass der Einbettungsgrad gleich k ist. Somit sind die fünf Bedingungen erfüllt, sodass die Parameter (p, t, r, D, k) nach Satz 3.6.21 eine elliptische Kurve mit den gewünschten Eigenschaften darstellen.

Dieser Algorithmus ist seit 2001 bekannt und bereits mehrfach in Software implementiert. Da die nächsten, verfeinerten Algorithmen sehr stark auf diesem Algorithmus aufbauen, werden wir hier zwei Beispiele angeben, die mittels eigenem KASH3-Code erlangt worden sind. Da sie nur der Anschauung dienen, haben die Parameter p, t und r keine kryptografisch relevante Größenordnung. Wir wählen ein r_0, welches die Größenordnung von r aufweisen soll und starten damit den Algorithmus.

Beispiel 1: Für `CocksPinch(-3,5,100)`, also $D = -3, k = 5, r_0 = 100$ ergibt sich folgende Lösung: $p = 153151, t = 49, r = 541$. Aus der CM-Gleichung lässt sich also y^2 zurückgewinnen. Es gilt:

$$4p = 4 \cdot 153151 = 49^2 - (-3) \cdot 451^2 = t^2 - (-D) \cdot y^2.$$

Da wir $D = -3$ gewählt haben, wissen wir, dass $a = 0$ ist, somit erhalten wir folgende sechs Twists der elliptischen Kurve über $\mathbb{F}_{153151}$:

$$\begin{array}{lcll} E_1 \colon y^2 & = & x^3 + 93726 & (R = 153804 = 2^2 \cdot 3 \cdot 7 \cdot 1831) \\ E_2 \colon y^2 & = & x^3 + 93723 & (R = 153853 = 7 \cdot 31 \cdot 709) \\ E_3 \colon y^2 & = & x^3 + 153148 & (R = 153201 = 3 \cdot 223 \cdot 229) \\ E_4 \colon y^2 & = & x^3 + 59425 & (R = 152500 = 2^2 \cdot 5^4 \cdot 61) \\ E_5 \colon y^2 & = & x^3 + 59428 & (R = 152451 = 3^2 \cdot 13 \cdot 1303) \\ E_6 \colon y^2 & = & x^3 + 3 & (R = 153103 = 283 \cdot 541) \end{array}$$

Nun wissen wir zusätzlich, dass die Ordnung der gesuchten Kurve $r = 541$ teilt, somit wissen wir, sogar ohne Methoden aus 4.2.2, dass E_6 die gesuchte Kurve ist. Wir stellen fest, dass r die Ordnung teilt, keineswegs aber in der Größenordnung von R liegt. Dies lässt sich auch anhand des Sicherheitsparameters ρ erkennen. Die Kurve besitzt ein Sicherheitsparameter ρ von $\frac{\log(153151)}{\log(541)} = 1,90$. Dies ist ein Anzeichen dafür, dass die r-Torsionsgruppe nicht auf der gesamten Kurve definiert ist.

Beispiel 2: Für `CocksPinch(-4,17,100)` ergibt sich folgende Lösung: $p = 1429, t = 60, r = 137$. Analog zum Beispiel 1 lässt sich y^2 zurückgewinnen. Es gilt:

$$4p = 4 \cdot 1429 = 60^2 - (-4)23^2.$$

Da $D = -4$ erhalten wir vier Twists der elliptischen Kurve über $\mathbb{F}_{1429}$

$$\begin{array}{lcll} E_1 \colon y^2 & = & x^3 + 998x & (R = 1370 = 2 \cdot 5 \cdot 137) \\ E_2 \colon y^2 & = & x^3 + 1426x & (R = 1476 = 2^2 \cdot 3^2 \cdot 41) \\ E_3 \colon y^2 & = & x^3 + 431x & (R = 1490 = 2 \cdot 5 \cdot 149) \\ E_4 \colon y^2 & = & x^3 + 3x & (R = 1384 = 2^3 \cdot 173) \end{array}$$

Wiederum anhand der Ordnungen der Kurven erkennen wir, dass E_1 der einzige Twist ist, für den $r|R$ gilt. Er ist also die gesuchte Kurve. Sie besitzt ein ρ von $\frac{\log(1429)}{\log(137)} = 1,48$. Dies ist schon deutlich besser, da es näher am optimalen Wert von 1 ist. Leider kann im Vorhinein keine Aussage über den ρ-Wert getroffen werden. Er kann erst berechnet werden, wenn der Cocks-Pinch-Algorithmus eine Lösung gefunden hat.

4.4 Eine Verallgemeinerung des Cocks-Pinch--Algorithmus

Der Cocks-Pinch-Algorithmus löst also die Aufgabe, eine elliptische Kurve für gegebene Fundamentaldiskriminante und gegebenen Einbettungsgrad zu erzeugen. Dabei liefert er Kurven, deren ρ in der Größenordnung von 2 liegt. Dies

bedeutet jedoch lediglich, dass R einen großen Primteiler besitzt. Anhand der Beispiele des vorherigen Abschnittes erkennen wir, dass die restlichen Faktoren rein zufällig sind. Neuere kryptografische Anwendungen benötigen Kurven, deren Ordnung aus mindestens zwei großen Primteilern mit ungefähr gleicher Ordnung besteht. Dies wird zwar im Cocks-Pinch-Algorithmus nicht explizit ausgeschlossen, siehe Beispiel 1 Kurve E_6, dennoch sind die Kurven, in denen ein solcher Fall auftritt, ab einer gewissen Größe von p sehr selten. Zu Beginn dieser Arbeit gab es keinerlei Implementierungen auf diesem Gebiet. Im Verlaufe der Arbeit wurde von Freeman und Teske, siehe u.a. [Fre07a], die naheliegende Anwendung des chinesischen Restsatzes vorgeschlagen. Dieser wurde in der vorliegenden Arbeit unabhängig davon implementiert. Die große Schwierigkeit bestand nicht in der Anwendung des chinesischen Restsatzes, sondern darin die Geschwindigkeit eines lauffähigen Algorithmus zu optimieren, sodass kryptografisch relevante Kurvenordnungen erzielt werden konnten. Wir werden zunächst den Cocks-Pinch-Algorithmus mittels des chinesischen Restsatzes erweitern, kurz erläutern, warum dies funktioniert und dann einige Aspekte zur Laufzeitverkürzung erläutern. Alle weiteren Beispiele sind aufgrund ihrer Größe in Kapitel 7 ausgelagert.

Algorithmus 4 Cocks-Pinch-Produkt-Algorithmus

Eingabe: $D < 0, D \in \mathbb{Z}, k \geq 1, k \in \mathbb{N}$, sowie r_0, welches die Größenordnungen der r_1- und r_2-Torsionsgruppen angibt.

Ausgabe: Parameter $p, r_1, r_2 \in \mathbb{P}$ und $t \in \mathbb{Z}$, sodass die CM-Gleichung (3.6) erfüllt ist. Außerdem wird sichergestellt, dass für einen Twist der mit diesen Parametern erzeugten Kurve gilt: Er hat Einbettungsgrad k und seine Ordnung wird vermutlich von $r_1 r_2$ geteilt.

1: **repeat**
2: Wähle r_1, r_2 so, dass $k \,|\, (r_1 - 1) \cdot (r_2 - 1)$ und $\left(\frac{D}{r_1}\right) = \left(\frac{D}{r_2}\right) = 1$.
3: Berechne $\sqrt{D}$ in $\mathbb{Z}/(r_1 r_2)\mathbb{Z}$.
4: Erzeuge k-te Wurzeln $\zeta_{k,i}$ im Restklassenring $\mathbb{Z}/(r_1 r_2)\mathbb{Z}$. (Das bedeutet $\zeta_{k,i}^k \equiv 1 \bmod (r_1 r_2)$.)
5: Berechne $t_i \equiv (\zeta_{k,i} + 1) \bmod (r_1 r_2)$.
6: Berechne $y_i \equiv \frac{\zeta_{k,i} - 1}{\sqrt{D}} \bmod (r_1 r_2)$.
7: Wähle für t_i und y_i die natürlichen Vertreter aus $]0, r_1 r_2]$.
8: Berechne $p_i = \frac{1}{4}(t_i^2 - D y_i^2) \in \mathbb{Z}$. .
9: **until** p_i ist eine Primzahl. (Setze für dieses i dann $p := p_i, t := t_i$.)
10: **return** p, t, r_1 und r_2.

Bemerkung 4.4.1. *(a) Es sollte klar sein, dass sich der Algorithmus nun ganz leicht auf Kurven ausweiten lässt, deren Ordnung von beliebig vielen „großen“ Primzahlen geteilt wird.*

(b) Wir sehen, dass die Grundstruktur des Algorithmus nicht verändert wurde.

Anstatt in Restklassenkörpern rechnen wir in Restklassenringen. Probleme treten dadurch bei der Berechnung von $\sqrt{D}$ und $\zeta_{k,i} \in \mathbb{Z}/(r_1 r_2)\mathbb{Z}$ auf. Diese Probleme sind nicht algebraischer, sondern algorithmischer Natur, wir werden sie weiter unten beleuchten.

(c) Auch hier genügt es, dass eine der $\sqrt{D}$ und $\zeta_{k,i}$ Kombinationen ein primes p_i erzeugt.

(d) Anstatt in jeder Schleife r_1 und r_2 neu zu wählen, genügt es r_1 einmal geschickt zu wählen und ausschließlich r_2 in jeder Schleife zu verändern, siehe unten.

Ein formaler Beweis für die Korrektheit dieses Algorithmus existiert nicht, es ist aber auch kein anderer Algorithmus bekannt, der mit Sicherheit eine Kurve mit zwei großen Torsionsgruppen vorgegebener Größe liefert. Versuchen wir den Beweis des Cocks-Pinch-Algorithmus analog anzuwenden, so stellen wir fest, dass in der Gleichungskette (4.3) die letzte mit (4.2) bezeichnete Gleichheit, aufgrund der nicht vorhandenen Nullteilerfreiheit nicht gegeben ist. Ein formaler Beweis ist also nicht möglich. Wir begnügen uns also damit, dass wir fast immer eine Kurve mit den gewünschten Eigenschaften erhalten.

Einige Anmerkungen zur Implementierung: Zunächst halten wir fest, dass die in Zeile 2 des Cocks-Pinch-Produkt-Algorithmus gegebenen Bedingungen garantieren, dass beide Objekte auch wirklich im Restklassenring $\mathbb{Z}/(r_1 r_2)\mathbb{Z}$ existieren. Quadrieren bzw. potenzieren wir alle Elemente aus $\mathbb{Z}/(r_1 r_2)\mathbb{Z}$ mit k, so können wir leicht mittels Trial and Error feststellen, ob ein Element $\sqrt{D}$ bzw. eine k-te Wurzel ist. Dies ist bei Zahlen in der Größenordnung von 100 bit jedoch nicht praktikabel.

In KASH3 sind für Restklassenringe einige Funktionen enthalten. Die Berechnung einer Quadratwurzel kann direkt erfolgen, die Berechnung einer k-ten Einheitswurzel ist nicht möglich. Daher wurde letzteres implementiert. Der erste Ansatz war zwei $(r_1 - 1)$-te bzw. $(r_2 - 1)$-te primitive Einheitswurzeln der jeweiligen Restklassenkörper zu erzeugen und mittels des chinesischen Restsatzes in den Restklassenring zu überführen. Das so erzeugte Element hat Ordnung $(r_1 - 1)(r_2 - 1)$, somit hat die $((r_1 - 1)(r_2 - 1)/k)$-te Potenz gerade Ordnung k. Da wir in KASH3 in Restklassenkörpern k-te Einheitswurzeln erzeugen können, hat sich herausgestellt, dass es günstig ist, eine k-te Einheitswurzel in $\mathbb{Z}/r_1\mathbb{Z}$ zu erzeugen. Wenden wir dann den chinesischen Restsatz auf diese und $1 \in \mathbb{Z}/r_2\mathbb{Z}$ an, erhalten wir ein Element der Ordnung k in $\mathbb{Z}/(r_1 r_2)\mathbb{Z}$, die gesuchte k-te Wurzel. Im Fall $p \notin \mathbb{P}$ fordern wir also, strenger als $k \mid (r_1 - 1)(r_2 - 1)$, dass $k \mid (r_1 - 1)$. Auf dieser Grundlage bauen wir unseren Algorithmus wie folgt auf:

Schritt 1: Wir suchen eine beliebige Zahl r_1, sodass $k|(r_1 - 1)$. Ist dies der Fall überprüfen wir, ob r_1 eine Primzahl ist, falls nicht, erhöhen wir r_1 in Schritten von k bis $nk + r_1$ eine Primzahl ist. Hierbei führen wir zu Gunsten einer kürzeren Laufzeit nur randomisierte Primzahltests durch.

Schritt 2: Wir überprüfen mittels `LegendreSymbol(D,r)`, ob D eine Wurzel $\bmod r_1$ besitzt. Falls nicht, gehen wir zurück zu Schritt 1.
Schritt 3: Wir überprüfen, ob das k-te Kreisteilungspolynom in $\mathbb{Q}[x]/r(x)$ reduzibel ist und ausreichend schnell berechnet werden kann. Falls möglich berechnen wir eine primitive k-te Einheitswurzel und bezeichnen sie mit `RU`.
Schritt 4: Nun suchen wir randomisiert ein primes r_2, wobei lediglich $\sqrt{D} \bmod r_2$ existieren muss.
Schritt 5: Wir erzeugen mittels des chinesischen Restsatzes, also des Befehls

```
ChineseRemainderTheorem([Coerce(Z,RU),Coerce(Z,1)],[r1,r2]));
```

eine k-te Wurzel im Restklassenring $\mathbb{Z}/r_1r_2\mathbb{Z}$. Außerdem gilt, dass für alle $i \leq k, i$ und k teilerfremd, `RU`^{i} auch eine k-te Wurzel ist, somit erhalten wir eine Teilmenge der Einheitswurzeln.
Schritt 6: Wir erzeugen mittels des in KASH3 implementierten Befehls

```
SquareRoot(Coerce(ResidueClassRing(r1r2),D))
```

eine Wurzel aus D im Restklassenring.
Schritt 7: Wir führen mit den so gewonnen Wurzeln den restlichen Teil des Algorithmus aus.
Dies hat nun zwei große Vorteile: Zum einen kann die Überprüfung, ob r_1 und r_2 prim sind, randomisiert durchgeführt werden, zum anderen muss lediglich jeweils ein neues primes r_2 gesucht werden, welches nur die Bedingung erfüllen muss, dass Wurzel D ein Quadrat $\bmod r_2$ ist. Als Nachteil müssen wir anmerken, dass wir so nicht alle möglichen Lösungen durchprobieren, im Fall von $k \notin \mathbb{P}$ sogar sehr viele Lösungen auslassen. Damit r_1 und r_2 nicht zu stark voneinander abweichen, können wir einen Kompromiss eingehen, indem wir, bevor wir wieder ein neues r_1 wählen, mehrere r_2 ausprobieren. Auch hier befinden sich die Beispiele in Kapitel 7.

4.5 Brezing-Weng-Algorithmus

Der Algorithmus von Cocks und Pinch liefert zwar stets eine Lösung, er hat jedoch auch Nachteile. Aufgrund seines zufälligen Generierungsprozesses ist auch der ρ-Wert der Kurve zufällig. Aus Zeile 8 des Cocks-Pinch-Algorithmus bzw. aus Zeile 8 des erweiterten Algorithmus wird klar, dass y_i und t_i zufällig verteilt im Intervall $]0, r]$ bzw. $]0, r_1r_2]$ liegen. Der Erwartungswert eines zufällig gewählten y_i und t_i beträgt gerade $r/2$ bzw. $r_1r_2/2$. So erhalten wir unter dieser Voraussetzung das schon mehrfach angedeutete Resultat:

$$\mathbb{E}[\rho] = \mathbb{E}\big[\frac{\log(p)}{\log(r)}\big] \leq \frac{\log(1/4\mathbb{E}[(t^2 - Dy^2)])}{\log(r)} = \frac{\log(1/4(1/4r^2 - 1/4Dr^2))}{\log(r)} =$$
$$= \frac{\log(1/16(1-D)r^2)}{\log(r)} = \frac{\log(1/16(1-D)) + 2\log(r)}{\log(r)} \approx 2 \qquad (4.4)$$

Bei diesen Gleichungsumformungen haben wir die Linearität des Erwartungswertes, dass $\log(r)$ konstant, die Jensen'schen Ungleichung (für konkave Funktionen), die obigen Vorbetrachtungen zum Erwartungswert sowie eine Approximation für $-D \ll r$, mit der ein Term der Summe vernachlässigt werden kann, verwendet. Wir erhalten dann ein ungefähres Resultat für ρ. Es hat sich gezeigt, dass der ρ-Wert der meisten mittels des Cocks-Pinch-Algorithmus erzeugten Kurven nahe bei 2 liegt. Der Brezing-Weng-Algorithmus versucht dieses Dilemma ein Stück weit zu lösen. Der Algorithmus ist so konzipiert, dass er Polynome $p(x)$, $r(x)$ und $t(x)$ sucht, welche Familien von gewünschten Parametern darstellen. Für die Kurven aus den Familien gilt, dass sie annähernd den gleichen ρ-Wert besitzen. Haben wir Parameter gefunden, die einen guten ρ-Wert liefern, so erhalten wir gleich eine ganze Kurvenschar mit diesem Sicherheitsparameter.

Algorithmus 5 Brezing-Weng-Algorithmus

Eingabe: $D < 0, D \in \mathbb{Z}, k \geq 1, k \in \mathbb{N}$ sowie $r(x) \in \mathbb{Z}[x]$, welchen den CM-Körper K erzeugt.

Ausgabe: Polynome $p(x), t(x)$ und $r(x)$, die für alle $x \in \mathbb{Z}$ die CM-Gleichung (3.6) erfüllen. Außerdem wird garantiert, dass für einen Twist der mit diesen Parametern erzeugten Kurve gilt: Er hat Einbettungsgrad k und ihre Ordnung $R(x)$ wird von $r(x)$ geteilt.

1: **repeat**
2: **repeat**
3: Wähle ein normiertes, irreduzibles $r(x)$ aus $\mathbb{Z}[x]$.
4: Generiere den Körper $K := \mathbb{Q}[x]/(r(x))$.
5: **until** $\sqrt{D} \in K$ und eine k-te primitive Einheitswurzel liegt in K.
6: Bestimme nun Repräsentanten $k_{1,i}(x)$ für $\sqrt{D}$ und $k_{2,i}(x)$ für die k-te primitive Einheitswurzel. (D.h. $(k_{1,i}(x))^2 \equiv D \bmod r(x)$ und $(k_{2,i})^k \equiv 1 \bmod r$).
7: Berechne dann (analog zum Cocks-Pinch-Algorithmus) $t_i(x) \equiv 1 + k_{2,i}(x) \bmod r(x)$ und $y_i(x) \equiv \frac{k_{2,i}(x)-1}{k_{1,i}} \bmod r(x)$.
8: Wähle für $t_i(x)$ und $y_i(x)$ die reduzierten Repräsentanten der jeweiligen Restklassen.
9: Berechne: $p_i(x) = \frac{1}{4}\big(t_i(x))^2 - D \cdot (y_i(x))^2\big) \in \mathbb{Q}[x]$.
10: **until** Eines der $p_i(x)$ ist irreduzibel. (Setze für dieses i dann $p(x) := p_i(x), t(x) := t_i(x)$.)
11: **return** $p(x), t(x)$ und $r(x)$.

Bemerkung 4.5.1. *(a) Der Brezing-Weng-Algorithmus ist also der Cocks-Pinch-Algorithmus für Polynome. Anstatt wie im Cocks-Pinch Fall einzelne Kurven als Lösungen zu finden, findet der Algorithmus eine Schar von Kurven. Die einzelnen Kurven entstehen durch Evaluierung der Polynome für $x \in \mathbb{Z}$ und anschließende Überprüfung, ob das Ergebnis eine Primzahl ist.*

(b) Auch der Beweis verläuft analog zum Beweis des Cocks-Pinch-Algorithmus. Irreduzibilität ist eine notwendige Bedingung, dass r(x) und p(x) Primzahlen darstellen.

(c) Um eine Kurve generieren zu können, suchen wir nun x, sodass $p(x)$ und $r(x)$ Primzahlen sind und $R(x) = p(x) + 1 - t(x)$ möglichst einen großen Faktor und sonst nur kleine Faktoren besitzt.

Im Algorithmus teilen wir die Behandlung einer Wurzel modulo $r(x)$ in zwei Schritte auf. Zunächst wird die Existenz sichergestellt, danach erfolgt die eigentliche Berechnung. Um die Existenz sicherzustellen, überprüfen wir ob das zu $\sqrt{D}$ zugehörige Polynom $f(x) = x^2 - D$, und das k-te Kreisteilungspolynom $\Phi_k(x)$ in K vollständig zerfallen. Falls nicht, wird ein neues $r(x)$ gewählt und somit ein neuer Körper K erzeugt. Ist das $r(x)$ fest gewählt, so erfolgt der eigentliche Berechnungsschritt. Auch hier gilt, dass mehrere Möglichkeiten für $k_{1,i}$ und $k_{2,i}$ existieren, die beliebig kombiniert werden können. Es bleiben noch zwei Fragen offen:. Wie wird $r(x)$ gewählt und wie werden $k_{1,i}$ und $k_{2,i}$ berechnet?

Die irreduziblen Polynome sollten möglichst kleine Koeffizienten haben. Dazu eignen sich die Kreisteilungspolynome. Wegen des Einbettungsgrades muss die Ordnung der Kreisteilungspolynome ein Vielfaches von k sein. Natürlich sind auch andere Polynome für $r(x)$ vorstellbar. Wir werden dies bei der Verallgemeinerung des Brezing-Weng-Algorithmus 4.6 genauer untersuchen. Die algorithmische Berechnung der $k_{1,i}$ erfolgt über ein Element der multiplikativen Gruppe des Körpers mit maximaler Ordnung. Dazu werden einige in KASH3 implementierte Befehle kombiniert: Zuerst erzeugt `TUG:=TorsionUnitGroup(K);` die Einheitengruppe der Maximalordnung des Körpers. Danach erzeugt der Befehl `PrimEle:=TUG.1;` ein Element der multiplikativen Gruppe mit maximaler Ordnung. Anschließend erzeugt der Befehl `phi:=TUG.ext1;` eine Abbildung der multiplikativen Gruppe in den Körper und die Auswertung `phi(PrimEle);` liefert das Bild im Körper. Dieses Element potenzieren wir mit $(|U| - 1)/2$ und multiplizieren es abschließend mit der Wurzel aus D innerhalb des Körpers, wobei U die Anzahl der Elemente der Einheitengruppe ist. In Code:

```
k_{1,i}:=Element(K,Wurz_D*phi(Coerce(Z,(U-1)/2*(i-1))*PrimEle));
```

Die Berechnung der $k_{2,i}$ erfolgt durch potenzieren des Elements maximaler Ordnung mit $(|U| - 1)/k$.
Zur Betrachtung der Güte der Kurven berechnen wir den ρ-Wert über die Beziehung:

$$\rho = \frac{\log p(x)}{\log r(x)} \approx \frac{\deg p(x)}{\deg r(x)}.$$

Achten wir also bei der Wahl von p auf einen niedrigen Grad, d.h., dass sich bei der Berechnung mittels der CM-Gleichung die Koeffizienten der höchsten Faktoren eliminieren, so erhalten wir eine Kurvenschar, deren einzelne Kurven annähernd den gleichen, günstigen ρ-Wert haben. Beispiele finden sich in [Tes07]. Sie wurden mittels unseres Algorithmus nachgeprüft. Weitere Beispiele sind in Kapitel 7 zu finden.

4.6 Verallgemeinerung des Brezing-Weng-Algorithmus

Da der Algorithmus von Brezing und Weng sehr stark auf dem Algorithmus von Cocks und Pinch aufbaut, liegt die Frage nahe, ob es auch mittels des Brezing-Weng-Algorithmus möglich ist Kurven zu generieren, deren Gruppenordnung wie bei der Cocks-Pinch Verallgemeinerung aus mehreren großen Primteilern besteht. Aus Restklassenkörpern werden wieder Restklassenringe. Fast ohne Modifikation kann auch die Verallgemeinerung des Cocks-Pinch-Algorithmus übernommen werden.

Algorithmus 6 Brezing-Weng-Verallgemeinerung

Eingabe: $D < 0, D \in \mathbb{Z}$ und $k \geq 1, k \in \mathbb{N}$.

Ausgabe: Polynome $p(x), t(x), r_1(x)$ und $r_2(x)$, die für alle $x \in \mathbb{Z}$ die CM-Gleichung (3.6) erfüllen. Außerdem wird garantiert, dass für einen Twist der mit diesen Parametern erzeugten Kurve gilt: Er hat Einbettungsgrad k und ihre Ordnung $R(x)$ wird von $r_1(x)r_2(x)$ geteilt.

1: **repeat**
2: **repeat**
3: Wähle zwei normierte, irreduzible $r_1(x)$ und $r_2(x)$ aus $\mathbb{Z}[x]$.
4: Generiere die Körper $K_1 = \mathbb{Q}[x]/(r_1(x))$ und $K_2 = \mathbb{Q}[x]/(r_2(x))$.
5: **until** Eine Wurzel aus D sowie eine k-te primitive Einheitswurzel liegt jeweils in K_1 und K_2.
6: Bestimme für beide Körper die Repräsentanten $k_{K_1,1,i}(x)$ und $k_{K_2,1,i}(x)$ für $\sqrt{D}$ sowie $k_{K_1,2,i}(x)$ und $k_{K_2,2,i}(x)$ für die k-te primitive Einheitswurzel. (Analog zu Schritt 6 im Brezing-Weng-Algorithmus.)
7: Überführe sie mittels des chinesischen Restsatzes in den Restklassenring $\mathbb{Q}[x]/(r_1(x)r_2(x))$. Das erzeugt $k_{1,i}(x)$ als Repräsentanten von $\sqrt{D} \bmod r_1(x)r_2(x)$ und $k_{2,i}(x)$ als Repräsentanten k-ter Einheitswurzeln $\bmod r_1(x)r_2(x)$.
8: Berechne dann (analog zum Cocks-Pinch-Algorithmus) $t_i(x) \equiv 1 + k_{2,i}(x) \bmod r_1(x)r_2(x)$ und $y_i(x) \equiv \frac{k_{2,i}(x)-1}{k_{1,i}} \bmod r_1(x)r_2(x)$.
9: Wähle für $t_i(x)$ und $y_i(x)$ die reduzierten Repräsentanten der jeweiligen Restklassen.
10: Berechne: $p_i(x) = \frac{1}{4}\big(t_i(x))^2 - D \cdot (y_i(x))^2\big) \in \mathbb{Q}[x]$.
11: **until** Eines der $p_i(x)$ ist irreduzibel. (Setze für dieses i dann $p(x) := p_i(x), t(x) := t_i(x)$.)
12: **return** $p(x), t(x), r_1(x)$ und $r_2(x)$.

Bemerkung 4.6.1. *(a) Die Verallgemeinerung des Brezing-Weng-Algorithmus folgt der Verallgemeinerung des Cocks-Pinch-Algorithmus. Wir versuchen irreduzible Polynome r_1 und r_2 zu finden, die Primteiler der Ord-*

nung darstellen und gleichzeitig zwei Körper erzeugen, die sowohl $\sqrt{D}$ als auch k-te Einheitswurzeln enthalten.

(b) Die zwei irreduziblen Polynome bilden einen Ring, der nicht nullteilerfrei ist. Daher kann auch hier wieder nur geschlussfolgert werden, dass die Ordnung der Kurve mit großer Wahrscheinlichkeit von den Primzahlen geteilt wird, welche von den irreduziblen Polynomen $r_1(x)$ und $r_2(x)$ erzeugt werden.

(c) Um eine Kurve zu generieren, suchen wir nun x, sodass $p(x), r_1(x)$ und $r_2(x)$ Primzahlen sind, $r_1(x) \neq r_2(x)$ und die Ordnung $R(x) = p(x) + 1 - t(x)$ möglichst zwei große und sonst nur kleine Faktoren besitzt.

Auch diese Verallgemeinerung folgt der Intuition und erzeugt mittels des chinesischen Restsatzes die relevanten Ausdrücke für Wurzel D und k-te Einheitswurzeln.

Algorithmisch ist die Verallgemeinerung nicht so leicht umzusetzen wie im Cocks-Pinch Fall. Zunächst wählen wir r_1 und erzeugen einen Körper K_1, der den zwei Wurzel-Bedingungen genügt. Ein guter Kandidat ist stets ein Kreisteilungspolynom. (Das k-te, das $2k$-te, das $3k$-te, ...) Dann wählen wir ein beliebiges Element des Körpers K_1 und erzeugen dessen Minimalpolynom. Falls der Grad dieses Polynoms mit dem von r_1 übereinstimmt, haben wir r_2 schon gefunden. Sonst nehmen wir ein weiteres zufälliges Element, bis der Grad stimmt. Die Wahl von r_2 ist jedoch sehr wichtig. Aufgrund nachfolgender Berechnungen ist es auch wünschenswert, dass die Koeffizienten des Polynoms möglichst kleine absolute Werte besitzen. Genauer gesagt, da die Koeffizienten stets rationale Zahlen sind, sollen die Zähler- und Nennerkoeffizienten kleine Absolutbeträge besitzen, so wie das bei Kreisteilungspolynomen oft der Fall ist. Dies ermöglicht dann das Finden einer Stelle, an der die Polynome $p(x), r_1(x)$ und $r_2(x)$ ganzzahlig sind. Um zu überschlagen, wie wahrscheinlich es ist, dass diese Lösungen auch noch Primzahlen sind, führen wir eine kurze Betrachtung durch. Eine Reihe von selbst durchgeführten Tests lässt vermuten, dass ca. jede 1000. Stelle für $r_1(x), r_2(x)$ und $p(x)$ gleichzeitig ganz ist. Dass $p(x)$ dann eine Primzahl ist, entspricht der Wahrscheinlichkeit, dass diese beliebige Zahl dieser Größenordnung eine Primzahl ist: $\frac{1}{\log(p(x))} \approx 1/$ (Anzahl der Stellen von) x. Da wir aber weiter fordern, dass auch noch $r_1(x)$ und $r_2(x)$ Primzahlen sein müssen, ergibt sich in erster Abschätzung eine Erfolgswahrscheinlichkeit von:

$$\frac{1}{1000 \cdot \log(p(x)) \cdot \log(r_1(x)) \cdot \log(r_2(x))}.$$

Die Aussichten auf Erfolg sind nicht gerade vielversprechend.

Ebenso wie in der Verallgemeinerung des Cocks-Pinch-Algorithmus treten im Restklassenring Nullteiler auf. Es ist also nicht gesagt, dass alle durch die irreduziblen Polynome dargestellten Faktoren von $r_1(x)$ und $r_2(x)$ auch wirklich

die Ordnung der Kurve teilen. Da die Faktoren von $r_1(x)$ und $r_2(x)$ groß sind, ist die Wahrscheinlichkeit hierfür jedoch relativ groß.

In dieser Erweiterung des Algorithmus ist die Wahl der $r_2(x)$ besonders wichtig. Es ist nicht leicht vorauszusagen, welche Polynome überhaupt Lösungen liefern. Einige Beispiele hierzu sind im Kapitel 7 angegeben. Die Suche dieser Beispiele ist recht zeitaufwendig.

4.7 Testen elliptischer Kurven

Haben wir aus den gegebenen Parametern nun eine Kurve generiert, (ob nach der Cocks-Pinch-Methode oder der Brezing-Weng-Methode,) oder ist uns auf andere Art und Weise eine Kurve gegeben, so ist das Testen, ob diese die gewünschten Anforderungen erfüllt, recht einfach. Hierfür rechnen wir alle fünf Bedingungen aus Satz 3.6.21 konkret durch Einsetzen der errechneten Parameter in die Gleichungen nach. Ob p und r Primzahlen sind und ob r die Ordnung der Kurve $p - t + 1$ teilt, ist leicht bestimmt und die CM-Gleichung überprüfen wir ebenso leicht. Um zu überprüfen, ob der Einbettungsgrad stimmt, testen wir $\Phi_j(q) \bmod r$. Das Gelingen des Tests hängt also ab von der Überprüfung der Ordnung der Kurve. Dazu nutzen wir wieder das Verfahren aus 4.2.2, um festzustellen, welcher Twist der Kurve der richtige ist. Zusammengefasst: Wir generieren einen zufälligen Punkt auf der Kurve, multiplizieren diesen mit der vermuteten Ordnung und überprüfen, ob wir das neutrale Element erhalten. Durch mehrfache Wahl zufälliger Punkte können wir die Irrtumswahrscheinlichkeit reduzieren. Absolute Garantie werden wir aber nie erhalten, dafür müssten wir das Verfahren wechseln. Da die bislang bekannten Verfahren aber rechenintensiv sind, werden wir das randomisierte Verfahren verwenden.

Kapitel 5

Hyperelliptische Kurven

Wir haben uns in den letzten Kapiteln ausführlich mit elliptischen Kurven und deren Erzeugung befasst. Dieses Gebiet ist seit Längerem wieder in den Fokus der Mathematiker und Kryptologen gelangt. Deutlich weniger erforscht, aber mittlerweile ebenfalls von Interesse, sind die hyperelliptischen Kurven und hyperelliptischen Funktionenkörper. Auf elliptischen Kurven existiert das Gruppengesetz (Chord-Tangent-Law). Dieses kann jedoch nicht auf hyperelliptische Kurven verallgemeinert werden. Um hyperelliptische Kurven kryptologisch nutzbar zu machen, werden wir uns die Struktur der Picard-Gruppe zunutze machen. Dazu werden wir in 5.1 zunächst eine Einführung zu hyperelliptischen Kurven geben. Dann werden wir in 5.2 sehen, dass jede Kurve mit einer Einbettung in ihre Picard-Gruppe eine unterliegende Gruppenstruktur besitzt. Es stellt sich heraus, dass die elliptische Kurve isomorph zu ihrer, aus der algebraischen Geometrie bekannten, Jakobischen Varietät (und somit auch ihrer Picard-Gruppe) ist, dass wir also bereits schon mit Divisorklassen rechnen. Also werden wir die wichtigsten Begriffe, Isogenie, Frobenius-Endomorphismus und charakteristisches Polynom auch für hyperelliptische Kurven erklären. In 5.3 werden wir Jakobische Varietäten als Spezialfälle Abelscher Varietäten charakterisieren. Im wichtigen Kapitel 5.4 werden wir weitere Unterschiede zwischen elliptischen und hyperelliptischen Kurven und damit verbundene komplexere Notationen kennenlernen. Dazu werden wir die in 2.5 eingeführten Divisoren weiterentwickeln. Hierfür nehmen wir an manchen Stellen eine gewisse Redundanz in Kauf, da wir so den elliptischen Fall eigenständig und mit einfacher Notation betrachten konnten. In 5.5 werden wir die wichtigsten Paarungen auf hyperelliptische Kurven erweitern, um in 5.6 ein Untersuchen der Sicherheit der Kurven zu ermöglichen. Abschließend werden wir in 5.7 Vor- und Nachteile paarungsgeeigneter hyperelliptischer Kurven herausstellen.

5.1 Die Gleichung einer hyperelliptischen Kurve

Beginnen wir zunächst mit einer formalen Definition einer hyperelliptischen Kurve. Sie wurde im elliptischen Fall bereits angedeutet. Dazu möchten wir an den Satz von Riemann-Roch 3.1.2 erinnern. Wir definieren formal:

Definition 5.1.1. (Hyperelliptische Kurve) *Eine* hyperelliptische Kurve *C ist eine nichtsinguläre, absolut irreduzible, projektive Kurve über K von Geschlecht größer 1, wenn sie mindestens einen K-rationalen Punkt besitzt.*

Analog zum elliptischen Fall können wir über die Dimension der Riemann-Roch-Räume eine definierende Gleichung des affinen Teils einer hyperelliptischen Kurven herleiten. Dazu benötigen wir wieder den Zusammenhang zu Funktionenkörpern. Nach [Sti93] Definition I.1.1 ist ein algebraischer Funktionenkörper in einer Variablen stets eine algebraische Erweiterung über einer transzendenten Erweiterung. Analog zum elliptischen Fall, siehe Definition 3.2.1, definiert er einen hyperelliptischen Funktionenkörper:

Definition 5.1.2. (Hyperelliptischer Funktionenkörper) *Ein* hyperelliptischer Funktionenkörper *F/K ist ein algebraischer Funktionenkörper von Geschlecht größer gleich 2, der einen rationalen Funktionenkörper $K(x)$, mit $x \in F$ und $[F : K(x)] = 2$ als Teilkörper besitzt, siehe [Sti93] Definition VI.2.1.*

Bemerkung 5.1.3. *Manche Bücher beziehen auch elliptische Funktionenkörper in die Definition mit ein. Wir werden dies nicht tun. Hyperelliptische Funktionenkörper unterscheiden sich von elliptischen dadurch, dass der Teilkörper $K(x)$ eindeutig bestimmt ist. Im elliptischen Fall gibt es unendlich viele Teilkörper L, für die gilt $[F : L] = 2$, siehe [ACD$^+$06] Kapitel 4.4.2.b.*

Zur Herleitung der definierenden Gleichung folgen wir [ACD$^+$06] 4.4.2.b. Sei $K(C)$ ein hyperelliptischer Funktionenkörper. Laut Definition gibt es ein $x \in K(C)\backslash K$, für welches $2 = [K(C) : K(x)] = \deg((x)_0)$ gilt. Sei nun $D := (x)_0$. Dann ist D ein Divisor von Grad 2 und $\{1, x\}$ eine Basis des Riemann-Roch-Raums $\mathcal{L}(D)$. Folglich gilt auch $\ell(D) = 2$. Nach Definition der Riemann-Roch-Räume folgt weiter, dass für $1 \leq j \leq g$ gilt: $\ell([j]D) \geq 2j$. Außerdem liegen die Elemente $\left\{1, x, \ldots, x^j\right\}$ in $\mathcal{L}([j]D)$ und sind linear unabhängig. Für $([g+1])D$ gilt nach Linearität der Gradbewertung: $\deg([g+1]D) = 2(g+1) > 2g-2$. Daher folgt nach Riemann-Roch 3.1.2 Gleichheit, also:

$$\ell([g+1]D) = \deg([g+1]D) - g + 1 = g + 3$$

Folglich muss neben den $g+2$ Elementen eine weitere Funktion y in $\mathcal{L}([g+1]D)$ liegen, für die gilt $y \notin K[x]$.

Wiederum nach Riemann-Roch gilt, dass der Raum $\mathcal{L}([2(g+1)]D)$ die Dimension $\ell([2(g+1)]D) = 2(2(g+1)) - g + 1 = 3g + 5$ besitzt. Die folgende Menge enthält Funktionen, die auf jeden Fall in diesem Raum enthalten sind:

$$\mathcal{M} := \left\{1, x, x^2, x^3, \ldots, x^{2(g+1)}, y, xy, \ldots, x^{(g+1)}y, y^2\right\}$$

Das sind $1 + 2(g + 1) + 1 + (g + 1) + 1 = 3g + 6$ Funktionen. (Diese Kardinalitäten wurden in [ACD$^+$06] falsch berechnet.) Nun haben wir einen Vektorraum $\mathcal{L}([g + 1]D)$ von Dimension $3g + 5$ und $3g + 6$ verschiedene Funktionen dieses Vektorraums. Darum ist $\mathcal{M}$ linear abhängig. Nun zeigen wir noch, dass der Koeffizient vor y^2 nicht 0 ist und zu 1 normiert werden kann. Hier benutzen wir denselben Widerspruch wie im elliptischen Fall. Würde der Koeffizient von y^2 verschwinden, wäre y eine rationale Funktion von x. Dies steht aber im Widerspruch zu $[F : K(x, y)] = 1$ und $[F : K(x)] = 2$. Schließlich multiplizieren wir die Gleichung mit dem Inversen des Koeffizienten vor y^2 und normieren so die Gleichung.

Satz 5.1.4. (Gleichung einer hyperelliptischen Kurve)
Sei C/K eine hyperelliptische Kurve und $K(C) \cong F$ der dazugehörige hyperelliptische Funktionenkörper. Dann existieren Funktionen $x, y \in F$, sodass $F = K(x, y)$, wobei x und y folgende Beziehung erfüllen:

$$y^2 + h(x)y = f(x).$$

Dabei sind $h, f \in K[x]$ mit $\deg(h) \leq g + 1, \deg(f) \leq 2g + 2$. Diese Gleichung heißt affine Weierstraß-Normalform einer hyperelliptischen Kurve.

Beweis Die Erörterungen vor dem Satz liefern den Beweis. □

Bemerkung 5.1.5. *(a) Da die hyperelliptische Kurve nichtsingulär ist, verschwinden die partiellen Ableitungen (nach x und y) nicht gleichzeitig.*

(b) Ist die Charakteristik ungleich 2, können wir wie im elliptischen Fall, siehe Satz 3.2.5, den Term $h(x)y$ durch Substitution eliminieren. Die Gleichung der Kurve ergibt sich dann durch

$$C\colon y^2 = f(x), \text{mit } f \in K[x] \text{ und } \deg(f) \leq 2g + 2.$$

Siehe Bemerkungen nach [ACD$^+$06] Theorem 4.122.

(c) Nichtsinguläre Kurven zeichnen sich in der in (b) angegebenen Form dadurch aus, dass $f(x)$ keine doppelten Nullstellen besitzt. Setzen wir weiter voraus, dass die projektive Kurve genau einen K-rationalen Punkt in $\mathcal{O}_\infty$ besitzt, so hat f stets Grad $2g + 1$ und der unendliche ferne Punkt $\mathcal{O}$ entsteht eindeutig durch Homogenisierung. In diesem Fall besitzt er den Verzweigungsindex 2, siehe nächste Definition.

Wir definieren abschließend den in obiger Bemerkung erwähnten Verzweigungsindex:

Definition 5.1.6. (Verzweigungsindex) *Seien C_1 und C_2 zwei glatte Kurven und φ eine nicht konstante Abbildung zwischen C_1 und C_2. Weiter sei $P \in C_1$. Der* Verzweigungsindex e_φ *von φ in P ist definiert als*

$$e_\varphi(P) := v_\mathfrak{p}(\varphi^* t_{\varphi(P)}),$$

wobei $t_{\varphi(P)} \in K(C_2)$ ein uniformisierendes Element ist. In den Anwendungen ist C_1 meist $\mathbb{P}^1$, sodass alle Überlegungen im rationalen Funktionenkörper durchgeführt werden können, siehe [Sil86] Kapitel II.2.

Mit dieser Definition können wir das Geschlecht einer Kurve ermitteln, wenn wir das Geschlecht einer anderen Kurve kennen und eine rationale Abbildung zwischen den Kurven gefunden haben. Dies besagt folgende Formel von Hurwitz:

Satz 5.1.7. (Hurwitz)
Sei $\varphi : C_1/K \to C_2/K$ eine nicht konstante Abbildung zwischen zwei Kurven. Dann gilt

$$2g_1 - 2 \geq (\deg(\varphi))(2g_2 - 2) + \sum_{P \in C_1} (e_\varphi(P) - 1),$$

wobei g_i das Geschlecht von C_i für $i \in \{1, 2\}$. Weiter gilt Gleichheit genau dann, wenn $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = p > 0$ und für alle $P \in C_1$ die Charakteristik p nicht $e_\varphi(P)$ teilt.

Beweis Siehe [Sil86] Theorem II.5.9 auch [ACD$^+$06] Theorem 4.110. □

5.2 Frobenius-Morphismus

Neben der Verallgemeinerung der Kurvengleichung auf hyperelliptische Kurven haben wir zusätzlich das Problem, dass hyperelliptische Kurven keine Gruppe bilden. Aus diesem Grund haben wir in 2.5 Divisoren, Divisorklassen und die Picard-Gruppe eingeführt. Nun wäre es vorteilhaft, genauso wie bei elliptischen Kurven das Gruppengesetz, auch die Picard-Gruppe mittels rationaler Funktionen beschreiben zu können. Dazu beleuchten wir zunächst Morphismen und rationale Abbildungen. Rationale Abbildungen haben wir bereits in Definition 2.3.15 definiert, Morphismen in Definition 2.3.12. Für Morphismen auf Abelschen Varietäten hilft uns eine folgende Tatsache:

Satz 5.2.1. (Morphismus und Homomorphismen Abelscher Varietäten)
Seien $\mathcal{A}$ und $\mathcal{B}$ zwei Abelsche Varietäten und φ ein Morphismus von $\mathcal{A}$ nach $\mathcal{B}$. Dann ist φ genau dann ein Homomorphismus, wenn $\varphi(\mathcal{O}_\mathcal{A}) = \mathcal{O}_\mathcal{B}$.

Beweis Siehe [ACD$^+$06] Kapitel 4.3.3. □

Weiter gilt nach [ACD$^+$06] Proposition 4.60, dass wir Abelsche Varietäten als Abelsche Gruppen auffassen können. Wir erinnern uns an die Definition von Isogenien und erweitern sie auf Abelsche Varietäten.

Definition 5.2.2. (Isogenie zwischen Abelschen Varietäten) *Seien $\mathcal{A}$ und $\mathcal{B}$ zwei Abelsche Varietäten über K. Weiter sei $\varphi \in \mathrm{Hom}(\mathcal{A}, \mathcal{B})$. Dann heißt φ eine* Isogenie*, wenn das Bild von φ gleich $\mathcal{B}$ und der Kern von φ endlich ist.*

In diesem Fall sind $\mathcal{A}$ und $\mathcal{B}$ isogen. Isogene Abelsche Varietäten bilden eine Isogenieklasse, siehe [ACD$^+$06] Definition 4.62.

Homomorphismen sind genau dann Isogenien, wenn die Dimensionen der Abelschen Varietäten gleich sind und der Kern der Abbildung zwischen den Abelschen Varietäten eine maximale, absolut irreduzible Untervarietät der Dimension 0 besitzt. Der Zusammenhang ist komplizierter als der im elliptischen Fall, siehe Definition 3.3.3. Daher benötigen wir die Definition der einfachen Abelschen Varietäten, siehe Definition 2.4.3. Ein Homomorphismus zwischen einfachen Abelschen Varietäten ist nämlich entweder konstant, oder besitzt einen endlichen Kern, siehe [ACD$^+$06] Definition 4.69. Daher ist jeder nicht konstante Morphismus zwischen einfachen Abelschen Varietäten eine Isogenie, was auch schon im elliptischen Fall galt.
Wir können nun also Isogenieklassen Abelscher Varietäten bestimmen. Wir adaptieren die Definition von Isomorphieklasse auf Abelsche Varietäten.

Definition 5.2.3. (Isomorphismen Abelscher Varietäten) *Seien $\mathcal{A}$ und $\mathcal{B}$ zwei Abelsche Varietäten. Falls zwei Homomorphismen $\varphi : \mathcal{A} \to \mathcal{B}$ und $\psi : \mathcal{B} \to \mathcal{A}$ existieren, sodass $\psi \circ \varphi = \mathrm{Id}_{\mathcal{A}}$ und $\varphi \circ \psi = \mathrm{Id}_{\mathcal{B}}$, so sind φ und ψ* Isomorphismen*.*

Somit haben wir auch den Begriff der Isomorphieklasse definiert. Für den Spezialfall $\mathcal{A} = \mathcal{B}$ können wir auch den Endomorphismenring definieren:

Definition 5.2.4. (Endomorphismenring Abelscher Varietäten) *Sei $\mathcal{A}$ eine Abelsche Varietät und φ eine Isogenie von $\mathcal{A}$ nach $\mathcal{A}$. Dann erzeugt die in Definition 3.5.1 definierte Addition und Multiplikation den* Endomorphismenring $\mathrm{End}(\mathcal{A})$*, siehe [ACD$^+$06] Definition 4.67.*

Bevor wir nun weiter den Endomorphismenring von Abelschen Varietäten untersuchen, werden wir ein zentrales Resultat der algebraischen Geometrie angeben. Es erschließt den Zusammenhang zwischen Abelschen Varietäten und hyperelliptischen Kurven.

Definition 5.2.5. (Jakobische Varietät) *Sei C/K eine hyperelliptische Kurve und* Pic *ihre Picard-Gruppe. Für L mit $K \subseteq L \subseteq \overline{K}$ sei* $\mathrm{Pic}(L)$ *die Untergruppe der L-rationalen Divisorklassen. Die* Jakobische *oder auch* Jakobische Varietät *ist diejenige algebraische Varietät J_C, welche C enthält und für die für alle L gilt:*

$$\mathrm{Pic}(L) \cong J_C(L).$$

Siehe [Sti93] V.1.2, [ACD$^+$06] Kapitel 4.4.4 und [Sil86] Kapitel X.3.

Bemerkung 5.2.6. *(a) Sei E/K eine elliptische Kurve und $\overline{D} \in \mathcal{D}_E$ eine Divisorklasse von Grad* 0*. Dann ist $D \in \overline{D}$ ein K-rationaler Divisor und nach dem Satz von Riemann-Roch hat $\mathcal{L}(D + P_\infty)$ die Dimension* 1*. Also existiert darin ein effektiver Divisor von Grad* 1*. Dieser ist ein Primdivisor, kann also eindeutig einem Punkt P der projektiven Kurve zugeordnet*

werden. Umgekehrt kann dieser Punkt aber auch mittels $P - P_\infty \in \overline{D}$ eindeutig der Divisorklasse zugeordnet werden. Wir können nachprüfen, dass diese Abbildung einen Isomorphismus zwischen den Punkten der Kurve $E(K)$ und ihrer Jakobischen $J_E(K)$ darstellt. Somit sind elliptische Kurven und ihre Jakobische und damit auch ihre Picard-Gruppe isomorph, siehe [ACD+06] Kapitel 4.4.5.

(b) Obwohl die Elemente der Jakobischen Divisorklassen entsprechen, werden sie auch als Punkte bezeichnet. Dies verdeutlicht, dass die Theorie der elliptischen Kurven vor und losgelöst von der Theorie der hyperelliptischen Kurven entstanden ist.

(c) Betrachten wir unser gewonnenes Resultat andersherum, stellen wir fest, dass Picard-Gruppen bestimmte Varietäten und somit mittels rationaler Funktionen beschreibbar sind. Den Beweis, dass zu jeder Kurve auch wirklich eine Jakobische existiert, bleiben wir schuldig.

Wir werden uns im nächsten Abschnitt mit der Frage beschäftigen, welche Abelsche Varietäten auch gleichzeitig Jakobische sind, dafür betrachten wir nun weiter den Zusammenhang zum Endomorphismenring einer Abelschen Varietät. Wie auch schon im elliptischen Fall wollen wir ein spezielles Element für den Endomorphismenring einer Abelschen Varietät über einem endlichen Körper $\mathbb{F}_q$ auszeichnen.

Definition 5.2.7. (Frobenius-Morphismus) *Sei also V eine projektive Varietät über $\mathbb{F}_q$ mit Ideal I. Weiter sei ϕ_q die Abbildung, welche die Elemente komponentenweise in die q-te Potenz erhebt. Wenden wir ϕ_q auf $I \subset V$ an, ϕ_q wird hierbei auf die Koeffizienten der rationalen Funktionen angewendet, so erhalten wir eine Varietät $\phi_q(V)$ und ein dazugehöriges Ideal $\phi_q(I)$. Der dazugehörige Morphismus von V nach $\phi_q(V)$ heißt* Frobenius-Morphismus *bezüglich $\mathbb{F}_q$, siehe [ACD+06] Kapitel 5.2.1.*

Bemerkung 5.2.8. *Im Allgemeinen ist V nicht isomorph zu $\phi_q(V)$, dies ist jedoch immer der Fall, wenn $d|k$ mit $q = p^d$, siehe [ACD+06] Proposition 5.67.*

Fassen wir die letzten Ergebnisse zusammen: Es ist möglich die Picard-Gruppe zusätzlich durch rationale Funktionen zu beschreiben oder umgekehrt, bestimmten Varietäten der Jakobischen die Gruppenstruktur der Picard-Gruppe zuzuordnen. Der Frobenius-Morphismus, der sowohl auf den Punkten einer hyperelliptischen Kurve als auch auf den rationalen Funktionen operiert, bildet Hauptdivisoren auf Hauptdivisoren ab und erhält den Grad eines Divisors. Dieser so auf Pic fortgesetzte Frobenius kann mit dem Frobenius-Morphismus der Abelschen Varietät identifiziert werden. Er ist also auf Pic bzw. der Jakobischen ein Homomorphismus, oder genauer ein Endomorphismus. Dies halten wir fest:

Satz 5.2.9. (Frobenius-Endomorphismus auf der Jakobischen)
Der Frobenius-Morphismus einer Abelschen Varietät induziert einen Endomorphismus auf Pic, *folglich ist der Frobenius-Morphismus auch auf der Jakobischen ein Endomorphismus. Er kann identifiziert werden mit dem Frobenius-Endomorphismus, der durch lineare Erweiterung des Frobenius auf der Kurve,*

entsteht. Wir bezeichnen den Frobenius-Endomorphismus unabhängig von der unterliegenden Struktur (Kurve, Picard-Gruppe oder Jakobische) mit ϕ_q.

Beweis Siehe [ACD+06] Satz 5.68. □

Bemerkung 5.2.10. *Die von ϕ_q fixierten Elemente sind die $\mathbb{F}_q$-rationalen Punkte der Jakobischen. Es gilt also $J_C(\mathbb{F}_q) = \mathrm{Pic}(\mathbb{F}_q)$ und die Anzahl berechnet sich über $|\mathrm{Pic}(\mathbb{F}_q)| = \deg(\mathrm{Id}_{J_C} - \phi_q) = \chi(\phi_q)_C(1)$.*

Über die Theorie der ℓ-adischen Darstellungen können wir auch dem verallgemeinerten Frobenius-Endomorphismus auf der Jakobischen bzw. der Picard-Gruppe sein charakteristisches Polynom zuordnen. Dies werden wir im Folgenden nur kurz andeuten.

5.2.1 Tate-Moduln

Die ℓ-adische Darstellung ist sehr eng mit dem Begriff des Tate-Moduls verknüpft. Wir werden hier lediglich die notwendige Definition einführen, damit wir das charakteristische Polynom auf Abelschen Varietäten definieren können. Wir bemerken zunächst, dass für die Torsionspunkte einer Abelschen Varietät gilt:

$$[\ell]\mathcal{A}[\ell^{k+1}] = \mathcal{A}[\ell^k],$$

für $\mathcal{A}/K$ mit $\mathrm{char}(K)$ teilerfremd zu $\ell \in \mathbb{P}$. Dies liegt der Definition des ℓ-adischen Tate-Moduls von $\mathcal{A}$ zugrunde.

Definition 5.2.11. (ℓ-adischer Tate-Modul) *Sei $\mathcal{A}/K$ eine Abelsche Varietät mit* $\mathrm{char}(K)$ *teilerfremd zu $\ell \in \mathbb{P}$. Der* ℓ-adische Tate-Modul *ist dann der projektive Limes:*

$$T_\ell(\mathcal{A}) := \lim_{\infty \leftarrow k} \mathcal{A}[\ell^k].$$

Siehe [ACD+06] Definition 4.79.

Zu jedem Endomorphismus $\varphi \in \mathrm{End}_K(\mathcal{A})$ können wir nun das charakteristische Polynom $\chi(T_\ell(\varphi))(T) := \det(T - T_\ell(\varphi))$ zuordnen, wobei $T_\ell(\varphi)$ das φ entsprechende Element aus $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(\mathcal{A}))$ ist. Diese Definition ist unabhängig von ℓ, daher wird das charakteristische Polynom von $\varphi \in \mathrm{End}(\mathcal{A})$ als

$$\chi(\varphi)_(\mathcal{A})(T) := \chi(T_\ell(\varphi))(T)$$

für beliebiges ℓ teilerfremd zu $\mathrm{char}(K)$ definiert.

5.2.2 Charakteristisches Polynom des Frobenius auf der Jakobischen

Die allgemeine Definition des letzten Abschnitts legt uns folgende spezielle Definition nahe:

Definition 5.2.12. (Charakteristisches Polynom des Frobenius auf C und J_C) *Wir bezeichnen das über dem Tate-Modul und der ℓ-adischen Darstellung gewonnene* charakteristische Polynom des Frobenius auf der Kurve C und der Jakobischen J_C *mit $\chi(\phi_q)_C(T)$. Es ist eindeutig auf C, da jeder Kurve eindeutig ihre Jakobische J_C zugeordnet werden kann. Neben dem Begriff der charakteristischen Polynome des Frobenius sind diese Polynome auch bekannt als q-Weil-Polynome.*

Bemerkung 5.2.13. *(a) Analog zum elliptischen Fall definieren wir die Spur des Frobenius als negative Summe der Eigenwerte, dem zweithöchsten Koeffizienten des Polynoms.*

(b) Es lässt sich zeigen, dass zwei Abelsche Varietäten über $\mathbb{F}_q$ genau dann isogen sind, wenn sie das gleiche charakteristische Polynom besitzen.

Definition 5.2.14. (Eigenwerte des Frobenius, q-Weil-Zahlen) *Es seien $\lambda_1, \ldots, \lambda_{2g}$ die Nullstellen des Frobenius auf der Jakobischen $\chi(\phi_q)_C(T)$. Sie werden auch als* Eigenwerte des Frobenius der Kurve C bzw. der Jakobischen J_C *bezeichnet. Im Zusammenhang mit der Bezeichnung q-Weil-Polynom, werden die Nullstellen auch als* q-Weil-Zahlen *bezeichnet, siehe [GO85],[Odo91] und [Oor03].*

Die Weil-Vermutung, ein bedeutendes Resultat der Mathematik des 20. Jahrhunderts, werden wir nun noch in allgemeinerer Form angeben. Sie betrifft die Eigenwerte des relativen Frobenius und wurde in allgemeinster Form von Deligne [Del74] bewiesen. Bereits in Satz 3.6.14 haben wir eine elliptische Version der Weil-Vermutung bewiesen. Die folgende Version für Abelsche Varietäten über endlichen Körpern wurde von Weil selbst bewiesen.

Satz 5.2.15. (Weil-Vermutung)
Sei C eine projektive, absolut irreduzible, nichtsinguläre Kurve über $\mathbb{F}_q$ von Geschlecht $g > 0$. Weiter seien λ_i mit $1 \leq i \leq 2g$ die Eigenwerte des charakteristischen Polynoms des Frobenius-Endomorphismus auf C. Dann gilt

(a) Jeder Eigenwert ist eine algebraische Zahl, der in einer Erweiterung von Grad kleiner gleich $2g$ enthalten ist.

(b) Die verschiedenen Eigenwerte können so angeordnet werden, dass gilt:

$$\lambda_i \cdot \lambda_{i+g} = q.$$

(c) Fassen wir die Eigenwerte λ_i für $1 \leq i \leq 2g$ als komplexe Zahlen auf, so ist ihr Absolutbetrag gerade gleich Wurzel aus q, also $|\lambda_i| = \sqrt{q}$.

Beweis Siehe [Sti93] Kapitel V.2 oder [Mum74] Theorem 21.4. □

Im elliptischen Fall war das charakteristische Polynom des Frobenius Ausgangspunkt für die CM-Gleichung. Im hyperelliptischen Fall besitzt das Polynom einen größeren Grad. Dennoch besitzt es aufbauend auf dem letzten Satz eine Struktur. Für eine kurze Zusammenfassung siehe [ACD$^+$06] Theorem 5.76 und Korollar 5.82.

Satz 5.2.16. (Struktur des Frobenius)
Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve mit Geschlecht g über einem endlichen Körper. Dann ist das charakteristische Polynom des Frobenius von C (bzw. J_C) gegeben durch:

$$\chi(\phi_q)_C(T) = T^{2g} + a_1 T^{2g-1} + \ldots + a_g T^g + a_{g-1} q T^{g-1} + \ldots + a_1 q^{g-1} T + q^g$$

Dabei gilt $a_i \in \mathbb{Z}$ für $1 \leq i \leq g$.

Beweis Siehe [Mil86b] Theorem 19.1 sowie [Sti93] Kapitel V.1. □

Satz 5.2.17. (Punkte zählen)
Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve mit Geschlecht g über einem endlichen Körper $\mathbb{F}_q$. Weiter sei die Faktorisierung des charakteristischen Polynoms des Frobenius über $\mathbb{C}$ gegeben durch $\chi(\phi_q)_C(T) = \prod_{i=1}^{2g}(T - \lambda_i)$ mit $\lambda_i \in \mathbb{C}$. Dann gilt für jede natürliche Zahl $k \in \mathbb{N}$:

(a)

$$N_k = \prod_{i=1}^{2g}(1 - \lambda_i^k),$$

wobei N_k die Anzahl der $\mathbb{F}_{q^k}$-rationalen Divisorklassen in Pic *ist.*

(b)

$$M_k = q^k + 1 - \sum_{i=1}^{2g}(\lambda_i^k),$$

wobei M_k die Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte von C ist.

(c)

$$\left|M_k - (q^k + 1)\right| \leq g\lfloor 2q^{k/2} \rfloor,$$

als sogenannte Serre-Schranke. Sie ist eine stärkere Version der Hasse-Weil-Schranke $|M_1 - (q+1)| \leq 2\sqrt{q}$ des elliptischen Falls.

Außerdem existiert eine rekursive Beziehung zwischen den Punkten auf der Kurve, sodass es ausreicht, die ersten g Zahlen M_k mit $1 \leq k \leq g$ zu kennen, um das charakteristische Polynom des Frobenius zu konstruieren. Sie ist gegeben durch:

$$k a_k = (M_k - (q^k + 1))a_0 + (M_{k-1} - (q^{k-1} + 1))a_1 + \ldots + (M_1 - (q+1))a_{k-1}$$

Die a_k bezeichnen dabei die Koeffizienten des charakteristischen Polynoms aus Satz 5.2.16

Beweis [ACD$^+$06] Theorem 14.17. Für Beweise siehe [Sti93] Kapitel V.1, oder auch [Mum74] Kapitel 21. □

5.3 Hyperelliptische Kurven und Abelsche Varietäten

In Kapitel 3 und 4 haben wir uns mit elliptischen Kurven beschäftigt. Da sie isomorph zu ihrer Jakobischen sind, besitzen sie schon eine Gruppenstruktur. Es war daher auch nicht nötig, sie als Jakobische und somit als spezielle Abelsche Varietät zu betrachten. Nun werden wir zumindest teilweise eine Antwort darauf geben, welche zusätzlichen Eigenschaften eine Abelsche Varietät besitzen muss, damit sie eine Jakobische ist und somit einer hyperelliptischen Kurve zugeordnet werden kann.

Eine Jakobische ist immer eine prinzipiell polarisierte Abelsche Varietät, siehe [ACD$^+$06] Proposition 5.24. Dies alleine ist jedoch nicht hinreichend. Ein Resultat von Mumford besagt, dass jede Isogenieklasse über einem algebraisch abgeschlossenen Grundkörper eine prinzipiell polarisierte Abelsche Varietät enthält ([Mum74] Korollar 23.4). Leider ist es keinesfalls so, dass wir allgemein sagen können, wann prinzipiell polarisierte Varietäten auch Jakobische darstellen. Für Abelsche Varietäten über $\mathbb{C}$ mit Dimension 2 oder 3 zeigt Weil [Wei57], dass jede prinzipiell polarisierte Abelsche Varietät $\mathcal{A}$ eine Jakobische J_C einer Kurve C ist. Weiter existiert ein Satz von Torelli, der besagt, dass die Isomorphieklasse von $\mathcal{A}$ zusammen mit ihrer Polarisierung eindeutig durch die Isomorphieklasse von C bestimmt ist. Für höher-dimensionale Fälle ist dies ein seit 1888 ungelöstes Problem, das Schottky Problem. Dies alles ist wenig hilfreich, wenn wir Abelsche Varietäten über endlichen Körpern betrachten. Wir beschränken uns auf den Fall $g = 2$. Abelsche Varietäten der Dimension 2 heißen Abelsche Flächen. Howe charakterisiert in [How95] diesen Fall und gibt folgende Antwort:

Satz 5.3.1. (Abelsche Flächen und Jakobische)
Gegeben seien der endliche Körper $\mathbb{F}_q$ sowie $a, b \in \mathbb{N}$. Weiter sei $h \in \mathbb{Z}[x]$ das charakteristische Polynom des Frobenius-Endomorphismus mit folgender Form:

$$h(x) = x^4 + sx^3 + tx^2 + sqx + q^2.$$

Dann erzeugt dieses Polynom eine Isogenieklasse einer zweidimensionalen ordinären Varietät über $\mathbb{F}_q$. (Den Begriff ordinär werden wir in Definition 5.4.14 einführen.)

(a) Diese enthält genau dann keine prinzipiell polarisierte Varietät, wenn $q = s^2 - t$, t eine negative Zahl ist, und alle Primteiler von q gerade 1 modulo 3 sind.

(b) Andernfalls enthält die Isogenieklasse sogar eine Jakobische, somit also auch eine polarisierte Varietät.

Beweis Für *(a)* siehe [How95] Kapitel 12, für *(b)* [How95] Theorem 13.3. □

Für ordinäre Abelsche Varietäten $\mathcal{A}$ über endlichen Körpern gilt sogar ein allgemeineres Resultat. Das charakteristische Polynom des Frobenius von $\mathcal{A}$ liefert eine Bijektion zwischen Isogenieklassen ordinärer Abelscher Varietäten und ordinären q-Weil-Polynomen, also Jakobischen. Details werden wir hier nicht anführen und verweisen auf [Tat68] und [How95]. Falls die Abelsche Varietät sogar einfach ist, können wir noch konkreter werden:

Satz 5.3.2. (Honda und Tate)
Sei h ein charakteristisches Polynom des Frobenius-Endomorphismus einer einfachen Abelschen Varietät. Dann ist die Abbildung

$$A \longmapsto \pi \text{ mit } h(\pi) = 0$$

eine Bijektion von $\mathbb{F}_q$-Isogenieklassen von einfachen Abelschen Varietäten und Konjugationsklassen von q-Weil-Zahlen π.

Beweis Siehe [Tat68]. □

Wir haben somit einen Zusammenhang zwischen ordinären q-Weil-Polynomen von Grad 4 und Isogenieklassen zweidimensionaler ordinärer Varietäten über $\mathbb{F}_q$ hergestellt. Ist die Varietät einfach, so existiert zwischen den Nullstellen der q-Weil-Polynome und den $\mathbb{F}_q$-Isogenieklassen der Jakobischen sogar eine Bijektion.

5.4 Unterschiede zu dem elliptischen Fall

Um im elliptischen Fall Kryptografie zu betreiben, benötigten wir weitere Konzepte, siehe 3.6. Dazu zählten Torsionsgruppen, die Fundamentaldiskriminante (bzw. die Klassenzahl), die j-Invariante und die CM-Gleichung. Diese Konzepte haben alle eine Entsprechung im hyperelliptischen Fall. Torsionsgruppen werden für Divisoren definiert, die Klassenzahl existiert auch für hyperelliptische Funktionenkörper, an die Stelle der j-Invarianten treten Igusa-Invarianten und die CM-Gleichung wird ersetzt durch drei Gleichungen. Wir werden im Folgenden auf die Unterschiede genauer eingehen.

5.4.1 Divisoren II

Auf elliptischen Kurven wurde durch eine spezielle Punktaddition eine Gruppenstruktur induziert. Dies funktioniert bei hyperelliptischen Kurven nicht. Daher nutzen wir das in 2.5 eingeführte Konzept von Divisoren. Anstatt Paarungen auf der Punktegruppe zu definieren, werden wir sie auf der Divisorgruppe definieren. In Definition 2.5.2 haben wir bereits rationale Divisoren eingeführt. Mit den neuen Begriffen der letzten Kapitel können wir sie nun auf eine weitere Art charakterisieren.

Wir erinnern uns an die Definition der L-rationalen Divisoren, siehe Definition 2.5.2. Für endliche Körper spezifizieren wir:

Lemma 5.4.1. *Sei ϕ_q der Frobenius-Endomorphismus auf $C/\mathbb{F}_q$ und J_C. Sei $D \in \mathcal{D}$ mit der Darstellung $D = \sum_{P \in C(\overline{F}_q)} v_P(P)$. Dann wenden wir den Frobenius-Endomorphismus punktweise auf die Divisoren an:*

$$\phi_q(D) = \sum_{P \in C(\overline{F}_q)} v_P(\phi_q(P)).$$

Des Weiteren ist D genau dann $\mathbb{F}_{q^k}$-rational, falls gilt $\phi_{q^k}(D) = D$, siehe [ACD+ 06] Proposition 5.68.

Nun sind wir aber an den Divisorklassen interessiert, die auf der Jakobischen liegen, das bedeutet alle Divisorklassen $\overline{D}$ mit Grad 0. Sie sind Elemente der Jakobischen. Der Divisor D ist ein Repräsentant der Divisorklasse $\overline{D}$, es gilt also: $D \in \overline{D} \in J_C$. Um eine Divisorklasse eindeutig kennzeichnen zu können, führen wir reduzierte Divisoren ein:

Definition 5.4.2. (Reduzierter Divisor) *Sei $\overline{D} \in J_C$ gegeben, dann heißt ein Divisor der Form*

$$\sum_{i=1}^{m} (P_i) - m(P_\infty), \qquad m \leq g$$

mit $P_i = (x_i, y_i) \in C(\overline{\mathbb{F}}_q), P_i \neq P_\infty$ und $P_i \neq \iota(P_j)$ für $i \neq j$ reduzierter Divisor*. Hierbei ist ι die hyperelliptische Involution, welche einen Punkt auf die zweite Lösung der definierenden Gleichung abbildet. Ist eine Kurve in affiner Weierstraß-Normalform gegeben, so bildet ι den Punkt $P = (x, y)$ auf $(x, -y)$ ab. Der reduzierte Divisor ist eindeutig, siehe [Kob98] Anhang Theorem 6.1, daher kennzeichnet er auch eindeutig eine Divisorklasse. Er wird mit $\rho(\overline{D})$ bezeichnet, siehe auch [GHO+ 07].*

Es ergibt sich ein Zusammenhang zu den in Definition 2.5.5 eingeführten Divisor:

Bemerkung 5.4.3. *Sei $\overline{D}$ eine Divisorklasse, und $\rho(\overline{D})$ der reduzierte Divisor. Dann besitzt $\rho(\overline{D})$ einen effektiven Teil $\epsilon(\overline{D})$ und es gilt:*

$$\rho(\overline{D}) := \epsilon(\overline{D}) - \deg(\epsilon(\overline{D}))(P_\infty).$$

Weiter führen wir die n-fache Divisorklassenaddition ein:

Definition 5.4.4. (Divisorklassenaddition) *Gegeben sei eine Divisorklasse $\overline{D} \in J_C$. Mit $[n]$ bezeichnen wir die n-*fache Divisorklassenaddition*, weiter bezeichnen wir mit $\oplus_n D := \rho([n]\overline{D})$ die Reduktion der n-fachen Divisorklasse. (In [GHV07] wird das mit $[n]$ bezeichnet, aber dieses Symbol benutzen wir bereits, um die n-fache Divisorklassenaddition zu bezeichnen.)*

Analog zum elliptischen Fall, siehe Definition 3.7.3, führen wir ein:

Definition 5.4.5. (Funktion mit Divisor) *Mit $f_{n,D} \in K(C)$ bezeichnen wir eine Funktion, welche folgenden Divisor besitzt:*

$$(f_{n,D}) = ([n]D - \oplus_n D)$$

Siehe [GHO+07].

5.4.2 Die Torsionsgruppe

Wiederum analog zum elliptischen Fall führen wir die Torsionsgruppe auf der Jakobischen ein.

Definition 5.4.6. (Torsionsgruppe einer Abelschen Varietät) *Sei $\mathcal{A}$ eine Abelsche Varietät über $\mathbb{F}_q$. Sei $[r]$ die r-fache Divisorklassenaddition. Mit*

$$\mathcal{A}[r] := \mathrm{Ker}([r])$$

*bezeichnen wir die r-*Torsionsgruppe der Abelschen Varietät $\mathcal{A}$, *(also im Speziellen die r-Torsionsgruppe auf einer Jakobischen.) Ihre Elemente werden weiterhin als r-Torsionspunkte bezeichnet. Auch hier bezeichnen wir mit $\mathcal{A}(\mathbb{F}_q)[r]$ die $\mathbb{F}_q$-rationalen r-Torsionspunkte.*

Über dem algebraischen Abschluss gilt dann:

Satz 5.4.7. (Isomorphie der Torsionsgruppe)
Sei $[r]$ die r-fache Addition auf einer Abelschen Varietät $\mathcal{A}/K$. Dann ist $[r] : \mathcal{A} \to \mathcal{A}$ eine Isogenie. Sie ist genau dann separabel (d.h. ihre induzierte Körpererweiterung ist separabel), falls r und $\mathrm{char}(K)$ teilerfremd sind. In diesem Fall gilt:

$$\mathcal{A}[r] \cong (\mathbb{Z}/r\mathbb{Z})^{2\cdot \dim \mathcal{A}}$$

Für eine Jakobische J_C ist die Dimension $\dim \mathcal{A}$ gerade gleich dem Geschlecht g der hyperelliptischen Kurve C.
Falls $r = p^s$ mit $p = \mathrm{char}(K)$ gilt:

$$\mathcal{A}[p^s] \cong (\mathbb{Z}/p^s\mathbb{Z})^t$$

für ein t mit $0 \leq t \leq \dim(\mathcal{A})$ unabhängig von $s \in \mathbb{N}$.

Beweis Siehe [Mum74] Theorem in Kapitel 6 auf Seite 64. □

Den Parameter t werden wir im nächsten Abschnitt genauer untersuchen. Um nicht zu weit ausholen zu müssen, werden wir zunächst mit der Untersuchung der Torsionsgruppen fortfahren. Betrachten wir die Torsionsgruppe nicht über dem algebraischen Abschluss, sondern über einem endlichen Zwischenkörper, so gilt:

Satz 5.4.8. (Struktursatz zur hyperelliptischen Torsionsgruppe)
Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve von Geschlecht $g \geq 2$. Falls $(\mathbb{Z}/r\mathbb{Z})^t \subseteq J_C(\mathbb{F}_q)[r]$ für ein $t > g$, folgt $r|(q-1)$.

Beweis Beweis wie in [ACD+06] 5.77 □

Satz 5.4.9. (Torsionsgruppen über endlichen Körpern)
Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve von Geschlecht $g \geq 2$. Für die Struktur der $\mathbb{F}_q$-rationalen Divisoren der Jakobischen gilt dann

$$J_C(\mathbb{F}_q)[r] \cong \mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z} \times \ldots \times \mathbb{Z}/r_{2g}\mathbb{Z},$$

wobei $r_i | r_{i+1}$ für $1 \leq i \leq 2g$ und für $1 \leq j \leq g$ gilt $r_j | q-1$.

Beweis Beweis Satz 5.4.7 zusammen mit Satz 5.4.9. □

Diesen Struktursatz haben wir im elliptischen Fall auch gesehen. Hier wurde die Torsionsgruppe aber immer so groß gewählt, dass für $\mathrm{char}(K) = p$ teilerfremd zu n galt $E(\mathbb{F}_{p^k})[r] = (\mathbb{Z}/r\mathbb{Z})^2$. Diese Beziehung war äquivalent zur Definition des Einbettungsgrades für ordinäre Kurven.

Da die Struktur von hyperelliptischen Kurven deutlich komplexer ist, müssen wir für diese zwei verschiedene Einbettungsgrade definieren, siehe [Fre07b].

Definition 5.4.10. (Einbettungsgrad) *Sei $\mathcal{A}$ eine Abelsche Varietät über K. Sei weiter $r \in \mathbb{N}$ teilerfremd zu* $\mathrm{char}(K)$. *Dann hat $\mathcal{A}$ den (gewöhnlichen)* Einbettungsgrad *k bezüglich r, falls*

(a) $\mathcal{A}$ einen K-rationalen Punkt mit Ordnung r hat und

(b) k die kleinste natürliche Zahl ist, sodass die r-ten Einheitswurzeln μ_r in einer Grad k Erweiterung von K liegen.

Eine nichtsinguläre Kurve C hat Einbettungsgrad k, falls ihre Jakobische J_C einen Einbettungsgrad von k bezüglich r hat, siehe [Fre07b] Definition 2.1.

Definition 5.4.11. (Voller Einbettungsgrad) *Sei $\mathcal{A}$ eine Abelsche Varietät über K. Weiter sei $r \in \mathbb{N}$ teilerfremd zu* $\mathrm{char}(K)$. *Dann hat $\mathcal{A}$* vollen Einbettungsgrad *k bezüglich r, falls*

(a) $\mathcal{A}$ einen K-rationalen Punkt mit Ordnung r hat und

(b) k die kleinste natürliche Zahl ist, sodass alle r-Torsionspunkte in einer Grad k Erweiterung von K liegen.

Eine nichtsinguläre Kurve C hat vollen Einbettungsgrad k, falls ihre Jakobische J_C einen vollen Einbettungsgrad von k bezüglich r hat, siehe Satz 5.4.9 und [Fre07b] Definition 2.4.

Bemerkung 5.4.12. *Wir verzichten darauf zu zeigen, dass der volle Einbettungsgrad ein Vielfaches des Einbettungsgrades ist, siehe [Mil86b] und [Fre07b] Bemerkung 2.5.*

5.4.3 p-Rang

Wir wenden uns wieder dem Parameter t aus Satz 5.4.7 zu und definieren:

Definition 5.4.13. (p-Rang) *Sei C/K eine hyperelliptische Kurve, wobei $\mathrm{char}(K) = p$ gelte. Weiter sei $[n]$ die n-fache Addition auf der Jakobischen J_C. Es existiert ein t mit $0 \leq t \leq g$, sodass für alle $s \in \mathbb{N}$ gilt:*

$$J_C[p^s] \cong (\mathbb{Z}/p^s\mathbb{Z})^t.$$

Den Parameter t bezeichnen wir als p-Rang *der Kurve.*

Definition 5.4.14. (ordinäre Jakobische) *Eine Abelsche Varietät bzw. Jakobische heißt* ordinär*, falls sie einen p-Rang von g hat, siehe [ACD+06] Definition 4.74.*

Bemerkung 5.4.15. *Auch für elliptische Kurven, die isomorph zu ihrer Jakobischen sind, können wir den p-Rang definieren. Es folgt, dass eine elliptische Kurve ordinär ist, falls sie einen p-Rang von 1 hat. Hat die Kurve den p-Rang 0, so ist sie supersingulär, siehe Definition 3.5.4. Auch die Supersingulärität verallgemeinern wir: Eine Jakobische heißt supersingulär, wenn sie isogen zu einem Produkt supersingulärer elliptischer Kurven ist. (Analog verläuft die allgemeinere Definition für Varietäten.) Für supersinguläre Jakobische gilt also, dass sie p-Rang 0 haben. Die Umkehrung dagegen ist falsch.*

Der p-Rang ist also eine Eigenschaft, die sich im hyperelliptischen Fall als deutlich komplizierter darstellt. Es treten Kurven auf, deren p-Rang weder voll (also gleich g) noch gleich 0 ist. In den meisten Anwendungen werden derzeit Kurven und Varietäten betrachtet, die vollen p-Rang besitzen, also ordinär sind.

5.4.4 Die CM-Gleichungen im hyperelliptischen Fall

Wenden wir uns nun noch einmal dem Frobenius-Endomorphismus auf der hyperelliptischen Kurve zu. Für den Fall des Geschlechts 2 ist er gegeben durch:

$$h(x) = x^4 + sx^3 + tx^2 + sqx + q^2 \tag{5.1}$$

Aus der Anzahl der Punkte der hyperelliptischen Kurve über $\mathbb{F}_q$ und $\mathbb{F}_{q^2}$, d.h. M_1 und M_2 lassen sich die Parameter s und t nach Satz 5.2.17 zurückgewinnen. Es gilt (wir setzen dort $a_1 = s$ und $a_2 = t$):

$$s = M_1 - q - 1 \qquad\qquad t = (M_2 - q^2 - 1 + s^2)/2 \tag{5.2}$$

Umgekehrt sehen wir aber auch, dass sich aus den Koeffizienten des Frobenius (auch ohne Faktorisierung) die Anzahl der Punkte der Kurve berechnen lässt.

Maisner und Nart berechnen in [MN02] obere Schranken für s und t. Abgesehen davon sind keine genaueren Kriterien bekannt, die beschreiben, wie s und t gewählt werden müssen, damit eine Kurve mit gewünschten Eigenschaften dazu existiert.
Werten wir ein beliebiges $h(x)$ an der Stelle 1 aus, so erhalten wir: $h(1) = |J_C(\mathbb{F}_q)|$. Dies ergibt sich sofort aus Satz 5.2.16. Für Kurven von Geschlecht 2 ergibt sich somit die Ordnungs-Gleichung:

$$\begin{aligned} |J_C(\mathbb{F}_q)| &= 1 + s + t + sq + q^2 \\ &= q^2 + s(q+1) + t + 1 \end{aligned} \tag{5.3}$$

5.4.5 CM-Körper

Um hyperelliptische Kurven zu erzeugen, brauchen wir einen geeigneten CM-Körper, in dem der Endomorphismenring eine Ordnung ist. An den CM-Körper werden in der Literatur daher zwei weitere Forderungen gestellt, siehe [ACD$^+$06] Kapitel 5.1.6.d und [Fre07b]. Zum einen wird gefordert, dass der total-reelle Unterkörper Klassenzahl 1 besitzt. Dies erleichtert die Berechnung der Isomorphieklassen der prinzipiell polarisierten Abelschen Varietäten. Zum anderen wird gefordert, dass der CM-Körper primitiv ist, siehe Definition 2.1.13, er also keinen imaginären Unterkörper enthält. Im elliptischen Fall ist der CM-Körper stets eine Erweiterung über $\mathbb{Q}$ von Grad 2. Der total-reelle Unterkörper ist $\mathbb{Q}$ selbst, außerdem besitzt der CM-Körper natürlich keinen imaginären Unterkörper. Diese beiden Eigenschaften sind also im elliptischen Fall stets erfüllt. Obwohl wir einen anderen Weg wählen werden, werden wir der Vollständigkeit halber erwähnen, dass Eisenträger und Lauter in [EL04] mit Lemma 6 eine Charakterisierung der Jakobischen vornehmen, deren Endomorphismenring gleich der Maximalordnung des CM-Körpers ist. Leider ist dies lediglich eine Existenzaussage, die keine Konstruktion der Kurve ermöglicht.

5.4.6 Igusa-Invarianten

Für gegebenen imaginär-quadratischen CM-Körper haben wir mittels der j-Invarianten die Gleichung der elliptischen Kurve erzeugt. Das Äquivalent der j-Invarianten sind die Igusa-Invarianten im hyperelliptischen Fall. Ihre Theorie ist deutlich komplexer. Angeregt wurde sie von Igusa [Igu60] und weiterentwickelt von Mestre [Mes91]. Wir werden hier nicht weiter auf sie eingehen. Eine kurze Zusammenfassung kann in [ACD$^+$06] Kapitel 5.1.6 gefunden werden. Für den Fall $g = 2$ bestimmen drei Igusa-Invarianten j_1, j_2 und j_3 die Isomorphieklasse der prinzipiell polarisierten Abelschen Varietät $\mathcal{A}/\mathbb{C}$ von Dimension 2. Mithilfe der Igusa-Invarianten können wir eine hyperelliptische Kurve, falls diese existiert, angeben, deren Jakobische $\mathcal{A}$ ist. Explizite Formeln dazu finden sich in [Wen03] und [ACD$^+$06] Lemma 5.53 sowie Theorem 5.54. Anstatt die Igusa-Invarianten zu berechnen, werden wir nur die CM-Körper aus [Wam99]

verwenden. Für sie wurden bereits in [Wam99] auch hyperelliptische Kurvengleichungen (bis auf Twists) berechnet. Diese Kurven sind alle über $\mathbb{Q}$ definiert, ihre CM-Körper besitzen die Klassenzahl 1 oder 2.

5.4.7 Quadratischer Twist von Kurven mit Geschlecht 2

Die Igusa-Invarianten und somit auch die Gleichungen in [Wam99] bestimmen die hyperelliptischen Kurven nur bis auf Twists. Daher müssen wir uns auch im hyperelliptischen Fall mit Twists beschäftigen. Wie auch im elliptischen Fall existieren Kurven C/K, die über $\overline{K}$ isomorph sind, nicht jedoch über allen Zwischenkörpern von K und $\overline{K}$. Für eine Beschreibung quadratischer Twists schränken wir uns abermals auf den Fall $g = 2$ ein.

Definition 5.4.16. (Quadratischer Twist einer hyperelliptischen Kurve) *Sei K ein Körper mit* $\mathrm{char}(K) \neq 2$. *Sei $\lambda \in (K \backslash K^2)$. Sei weiter C/K gegeben durch die Gleichung $y^2 = f(x)$. Die durch*

$$y^2 = \lambda f(x)$$

erzeugten Kurven heißen quadratische Twists *von C/K. Wie im elliptischen Fall bezeichnen wir mit echten Twists alle Kurven, die nicht K-isomorph zur Ausgangskurve sind. Sprechen wir von allen Twists einer Kurve, so sind damit auch die zur ursprünglichen Kurve isomorphen gemeint, siehe [MN02] Kapitel 3.2.*

Bemerkung 5.4.17. *Sei $M_k(C) = \left|C(\mathbb{F}_{q^k})\right|$ die Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte von C und $\tilde{C}$ ein echter quadratischer Twist von C. Dann gilt:*

$$M_1(C) + M_1(\tilde{C}) = 2q + 2, \text{ und } M_2(C) = M_2(\tilde{C}).$$

Wir sehen anhand der definierenden quadratischen Gleichung in y, dass für gegebenes $x \in \mathbb{F}_q$ jeweils genau zwei y existieren, welche die Gleichung lösen, und beide Punkte entweder in der Kurve oder ihrem Twist liegen. Auf beiden Kurven zusammen existieren also $2q$ affine Punkte plus die zwei unendlichfernen Punkte $\mathcal{O}$. Der zweite Teil folgt aus der gegebenen Isomorphie über der quadratischen Erweiterung. Beide Gleichungen zusammen sind dann nach Gleichung (5.2) äquivalent zu $s + \tilde{s} = 0$ und $t = \tilde{t}$, was die Berechnung des Frobenius eines echten Twists löst, siehe [MN02] Kapitel 3.2.

5.4.8 Reduktion hyperelliptischer Kurven

Auch die Reduktion hyperelliptischer Kurven ist deutlich komplizierter als im elliptischen Fall. Die Polynome, welche die Igusa-Invarianten erzeugen, sind rationale Polynome, besitzen also nicht notwendigerweise Koeffizienten aus $\mathbb{Z}$. Eine eventuelle Reduktion modulo p ist daher so zu wählen, dass p und die Nenner teilerfremd sind. Im Gegensatz dazu kann die Reduktion auf das charakteristische Polynom des Frobenius wie im elliptischen Fall, angewendet werden, siehe Satz 3.6.5.

Wir gehen noch einen Schritt weiter und berechnen die Reduktion auf der Torsionsgruppe der Jakobischen. Das charakteristische Polynom berechnet sich dann wie folgt:

Satz 5.4.18. (Restriktion des charakteristischen Polynoms auf J_C $[r]$) *Seien $p, r \in \mathbb{N}$ teilerfremd. Dann ist die Restriktion des charakteristischen Polynoms auf $J_C[r]$ gegeben durch:*

$$\chi(\phi_q)_C(T) \bmod r$$

Beweis Siehe [ACD+06] Lemma 5.71. □

5.5 Paarungen auf hyperelliptischen Kurven

Anstatt mit Punkten wie im elliptischen Fall, werden wir im hyperelliptischen Fall mit Divisoren bzw. Divisorklassen rechnen. Diese werden in der Literatur dennoch oft als Punkte bezeichnet, siehe zum Beispiel [ACD+06] Kapitel 4.4.4. Dazu nutzen wir die in 5.4.1 eingeführten effektiven und reduzierten Divisoren. Sie können auch in der sogenannten Mumford-Darstellung, in Form von Polynomen, angegeben werden. Auch darauf werden wir nicht eingehen, siehe [Kob98] Anhang, Kapitel 5 und 6. Da wir nun nicht mehr mit Punkten der Kurve rechnen, sondern mit Divisorklassen auf der Jakobischen, muss die Definition von Paarungen angepasst werden. Dies stellt kein theoretisches Problem dar, lediglich ein praktisches: Die Geschwindigkeit wird im Vergleich zum elliptischen Fall deutlich reduziert. Mit den im letzten Kapitel eingeführten Notationen können wir nun hyperelliptische Paarungen definieren:

Definition 5.5.1. (Weil Paarung auf hyperelliptischen Kurven) *Seien $C/\mathbb{F}_q$ eine hyperelliptische Kurve, J_C die dazugehörige Jakobische, $r \in \mathbb{N}$ und* $\mathrm{ggT}(r, q) = 1$. *Die* Weil Paarung auf J_C *ist eine nicht entartete, bilineare Funktion mit:*

$$W_r \colon J_C(\overline{\mathbb{F}}_q)[r] \times J_C(\overline{\mathbb{F}}_q)[r] \longrightarrow \mu_r.$$

Sie bildet immer nach μ_r ab, siehe [GHV07] Kapitel 4.1.

Definition 5.5.2. (Tate-Lichtenbaum Paarung auf hyperelliptischen Kurven) *Seien $C/\mathbb{F}_q$ eine hyperelliptische Kurve, $r \in \mathbb{N}$ und* $\mathrm{ggT}(r, q) = 1$. *Die* Tate-Lichtenbaum Paarung *auf hyperelliptischen Kurven ist definiert durch:*

$$\langle \cdot, \cdot \rangle_r \colon J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

Siehe [GHO+07] Kapitel 2.2.

Nutzen wir unsere in Definition 5.4.5 eingeführte Bezeichnung, so können wir der $\mathbb{F}_{q^k}$-rationalen Divisorklasse $\overline{D}_1$ der Ordnung r mittels $D_1 \in \overline{D}_1$ eine Funktion f_{r,D_1} zuordnen. Da aber $\overline{D}_1$ eine Divisorklasse der Ordnung r ist, gilt:

$$(f_{r,D_1}) = rD_1 - \oplus_r D_1 = rD_1$$

Wählen wir für eine zweite Divisorklasse einen Repräsentanten D_2 so, dass der Schnitt der Träger von D_1 und D_2 disjunkt wäre, erhalten wir eine explizite Formel für die Berechnung der Paarung:

$$\langle \overline{D}_1, \overline{D}_2 + r \operatorname{Pic}_C(\mathbb{F}_{q^k})\rangle_r = f_{r,D_1}(D_2) = \prod_P f_{r,D_1}(P)^{v_P(D_2)}$$

Hierbei ist zu beachten, dass D_1 und D_2 nicht gleichzeitig die reduzierten Divisoren ihrer Klassen sein können, da sonst der Schnitt der beiden Träger nicht disjunkt ist. Durch geschickte Normalisierung jedoch kann die Paarung durch $f_{r,\rho(\overline{D}_1)}(\epsilon(\overline{D}_2))$ berechnet werden.

Auch im hyperelliptischen Fall werden wir weitere Vereinfachungen vornehmen. Zum einen werden wir auch hier wieder annehmen, dass $J_C(\mathbb{F}_{q^k})$ kein Element der Ordnung r^2 enthält. Dann können wir mittels der Abbildung $\overline{D}_2 \mapsto \overline{D}_2 + r \operatorname{Pic}_C(\mathbb{F}_{q^k})$ die beiden Gruppen $J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k})$ und $J_C(\mathbb{F}_{q^k})[r]$ identifizieren. Zum anderen werden wir eine „final exponentiation“ mit $(q^k-1)/r$ durchführen, sodass die Abbildung stets nach μ_r abbildet. Dies definieren wir als reduzierte Tate-Lichtenbaum Paarung.

Definition 5.5.3. (Reduzierte Tate-Lichtenbaum Paarung) *Seien C/K eine hyperelliptische Kurve, $r \in \mathbb{N}$ und $\operatorname{ggT}(r,q) = 1$. Dann heißt die nicht entartete, bilineare Funktion*

$$T\colon J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})[r] \longrightarrow \mu_r$$
$$T(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2\rangle_r^{(q^k-1)/r} \in \mu_r \subset \mathbb{F}_{q^k}^*$$

reduzierte Tate-Lichtenbaum Paarung.

Auch die reduzierte Tate-Lichtenbaum Paarung kann weiter modifiziert werden, um den Miller-Algorithmus zur Paarungsauswertung weiter zu beschleunigen. Anstatt die Paarung auf $J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})[r]$ zu definieren, wird sie analog zum elliptischen Fall definiert:

$$G_2 := J_C(\mathbb{F}_{q^k})[r] \cap \operatorname{Ker}(\phi_q - [q])$$
$$G_1 := J_C(\mathbb{F}_{q^k})[r] \cap \operatorname{Ker}(\phi_q - [1]).$$

Hierbei sind q und 1 Eigenwerte von ϕ_q, die Indizes der Gruppen G_2 und G_1 sind historisch bedingt. Durch die Einschränkung auf die Eigenräume des Frobenius können wir auch die Ate Paarung auf hyperelliptische Kurven verallgemeinern:

Definition 5.5.4. (Ate Paarung auf hyperelliptischen Kurven) *Seien G_2 und G_1 wie oben definiert. Dann heißt die nicht entartete, bilineare Funktion, welche durch*

$$A\colon G_2 \times G_1 \longrightarrow \mu_r$$

definiert wird, *Ate Paarung auf hyperelliptischen Kurven.*

Bemerkung 5.5.5. *Die Ate Paarung hängt mit der reduzierten Tate-Lichtenbaum Paarung wie folgt zusammen:*

$$T(\overline{D}_1, \overline{D}_2) = A(\overline{D}_1, \overline{D}_2)^{kq^{k-1}}$$

Im Allgemeinen können die Repräsentanten nicht frei gewählt werden. Jedoch können wir auch hier unter bestimmten Umständen garantieren, dass wir zur Paarungsauswertung den effektiven und reduzierten Divisor wählen dürfen, siehe [GHO$^+$07].

Der obige Abschnitt fasst die Artikel [GHV07] und [GHO$^+$07] kurz zusammen. Dort befinden sich auch Beweise der Zusammenhänge.

5.6 Hyperelliptische Kurven in der Kryptografie

5.6.1 Anforderungen an hyperelliptische Kurven

Wie im elliptischen Fall sind nicht alle hyperelliptischen Kurven für kryptografische Zwecke geeignet. Wir definieren also:

Definition 5.6.1. (Paarungsgeeignete hyperelliptische Kurve) *Eine hyperelliptische Kurve ist* paarungsgeeignet*, wenn sie folgende Eigenschaften besitzt:*

(a) Die Anzahl der Punkte der Jakobischen der Kurve besitzt einen großen Primteiler r.

(b) Bezüglich r besitzt die Jakobische einen kleinen Einbettungsgrad k. In [GHV07] Kapitel 5 wird zum Beispiel $2 \leq k \leq 30g$ vorgeschlagen.

Auch hyperelliptischer Kurven können supersingulär sein. Für Geschlecht 2 besitzen diese nach [RS02] stets einen Einbettungsgrad kleiner gleich 12 und gelten aus den gleichen Gründen wie supersinguläre elliptische Kurven als unsicher, siehe 3.8.2. Den Sicherheitsparameter des elliptischen Falls verallgemeinern wir wie folgt auf hyperelliptische Kurven:

Definition 5.6.2. (Sicherheitsparameter ρ) *Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve von Geschlecht g. Weiter besitze die Anzahl der Punkte der Jakobischen einen großen Primteiler r. Die Sicherheit der Kurve wird dann anhand des* Sicherheitsparameters $\rho = \frac{g \log q}{\log r}$ *gemessen.*

Wir sehen, dass für Geschlecht $g = 1$ die beiden Definitionen übereinstimmen. Für Geschlecht 2 wird deutlich, da r nach Gleichung (5.3) die Größenordnung von q^2 besitzt, dass auch hier bestenfalls gilt: $\rho \approx \frac{2 \log q}{\log q^2} = 1$.

5.6.2 Sicherheitsaspekte hyperelliptischer Kurven

Die Sicherheitsaspekte für hyperelliptische Kurven sind denen elliptischer Kurven sehr ähnlich. Angriffe erfolgen zum einen direkt auf der hyperelliptischen Kurve bzw. der Jakobischen, oder aber auf dem endlichen Körper. Die möglichen Angriffe auf endliche Körper sind identisch zum elliptischen Fall, siehe 3.8.2. Auch auf hyperelliptischen Kurven bzw. deren Jakobischen existiert (zumindest für kleines Geschlecht) der Index-Calculus-Angriff. (Für Details siehe [FR94], [Thé03] und [Nag07].)
Da elliptische Kurven isomorph zu ihrer Jakobischen sind, sind alle Angriffe, die auf die Jakobische abzielen, auch auf elliptische Kurven anwendbar. Angriffe auf der hyperelliptischen Kurve selbst sind bis jetzt noch nicht bekannt. Um also die Sicherheit einer hyperelliptischen Kurve mit der einer elliptischen zu vergleichen, vergleichen wir die Angriffe auf den Jakobischen. Im hyperelliptischen Fall von Geschlecht 2 hat die Jakobische, nach Gleichung (5.3), eine Ordnung, die etwa q^2 entspricht. Allgemein ist die Ordnung der Jakobischen q^g, weshalb hyperelliptische Kurven von Geschlecht g mit vergleichbarem Sicherheitsparameter einen um die g-te Wurzel kürzeren Schlüssel besitzen. Im nächsten Abschnitt werden wir abschließend elliptische und hyperelliptische Kurven miteinander vergleichen.

5.7 Vergleich elliptischer und hyperelliptischer Kurven

Wie wir im letzten Abschnitt gesehen haben, sind alle Angriffe, die auf der Jakobischen einer hyperelliptischen Kurve basieren, auch auf der Jakobischen einer elliptischen Kurve (also auf ihr selbst) durchführbar. Es hat zunächst den Anschein, dass hyperelliptische Kurven sicherer sind als elliptische Kurven. Hyperelliptische Kurven haben außerdem den Vorteil der kleineren Schlüsselgrößen. Ihre Berechnungen finden somit in einem kleineren Körper statt.

Deutlich ausführlicher kamen auch Bernstein in [Ber06] und Lange in [Lan06] zu diesem Ergebnis. Dass trotzdem noch großer Forschungsbedarf gegeben ist, liegt daran, dass für den elliptischen Fall deutlich schnellere Algorithmen zur Paarungsauswertung existieren. Da hauptsächlich Multiplikationen für eine hohe Laufzeit verantwortlich sind, wird versucht, die Anzahl der Multiplikationen zu reduzieren. Weitere Details sind in den oben genannten Vorträgen zu finden. Neben einer Beschleunigung der Schritte des Algorithmus, siehe zum Beispiel [ELM03], [BKLS02] und [DL03], ist es oft notwendig besondere Bedingungen an die Kurven zu stellen. Hierfür seien nur zwei Beispiele genannt. In [BGhS07] wird ein Ansatz von [DL03] auf supersinguläre Abelsche Varietäten verallgemeinert. Dieser Algorithmus besitzt aber eine Einschränkung auf supersinguläre Kurven, weswegen er für kryptografische Zwecke uninteressant wird. Ein anderes Beispiel ist von Barreto und Naehrig in [BN05] gegeben. Sie konstruieren elliptische Kurven mit Einbettungsgrad 12, auf denen ein sehr schneller Algorithmus zur Paa-

rungsauswertung existiert. Einen guten Überblick über den derzeitigen Stand der Dinge liefert `http://www.ecrypt.eu.org/ebats/`. Die zwischenzeitlich verallgemeinerten Edwards-Koordinaten, die momentan nur für elliptische Kurven existieren, weisen eine deutliche Beschleunigung der Paarungsauswertung auf, siehe [Lan07]. Daher trügt der Anschein und es ist noch nicht abzusehen, welche Kurven sich in der Kryptografie durchsetzen werden.

Kapitel 6

Algorithmus für hyperelliptische Kurven

Im letzten Kapitel haben wir Methoden zur Behandlung von hyperelliptischen Kurven und deren Jakobischen kennengelernt. Dabei ließen sich die meisten Konzepte des elliptischen Falls auf die Jakobische übertragen (zum Beispiel Divisoren, Igusa-Invarianten, Torsionsgruppen, ...). Durch die Restriktion auf volle p-Ränge, also auf ordinäre Kurven, haben wir auch hier einen, dem elliptischen entsprechenden, Fall zurückgewonnen. Zwei Probleme jedoch lassen sich nicht ohne Weiteres zurückführen. Zum einen ist das die Auswahl und Erzeugung der CM-Körper aus einem Polynom vierten Grades. Zum anderen ist dies das damit verbundene Problem, dass die CM-Gleichung sich nicht mehr so leicht ausdrücken lässt. Dennoch werden wir den Cocks-Pinch-Algorithmus verallgemeinern. Zeitgleich zur ersten Phase dieser Arbeit wurde ein möglicher Ansatz von Freeman [Fre07b] entwickelt. Dieser neue Ansatz wurde nach seinem Erscheinen in dieser Arbeit mit in Betracht gezogen. Wir werden ihn in 6.1 vorstellen. Wie auch Freeman, werden wir ihn in 2 Teile, Algorithmus 7 und 8, zerlegen. Der erste generiert die nötigen Kurvenparameter, der zweite erzeugt dann aus den Parametern mit großer Wahrscheinlichkeit eine passende hyperelliptische Kurve. Dann werden wir in 6.2 den Algorithmus erweitern, indem wir ihn mit dem Brezing-Weng-Algorithmus kombinieren. Im letzten Abschnitt dieses Kapitels 6.3 beschreiben wir kurz, wie wir überprüfen können, ob die hyperelliptische Kurve bzw. deren Jakobische die gewünschten Eigenschaften erfüllt.

6.1 Freemans Algorithmus für hyperelliptische Kurven

Anfang des Jahres 2007 hat Freeman einen Algorithmus vorgestellt, mit dem es möglich ist für eine vorgegebene Torsionsgruppenordnung r eine dazu passende

ordinäre hyperelliptische Kurve zu erzeugen. Für supersinguläre Kurven war bereits vorher ein Algorithmus bekannt, siehe [BN05]. Wir werden zunächst in 6.1.1 noch einmal CM-Körper und die CM-Gleichung betrachten, bevor wir in 6.1.2 den ersten Teil des Algorithmus, welcher die Kurvenparameter liefert, beschreiben. Danach folgt in 6.1.3 der zweite Teil des Algorithmus, welcher aus den zuvor gefundenen Parametern eine hyperelliptische Kurve erzeugt.

6.1.1 Primitive quartische CM-Körper

Wie auch im elliptischen Fall benötigen wir zum Erzeugen einer hyperelliptischen Kurve einen CM-Körper. Da wir hyperelliptische Kurven von Grad 2 erzeugen möchten, betrachten wir einen CM-Körper von Grad 4. Dieser ist eine rein-reelle Erweiterung von Grad 2 über $\mathbb{Q}$ gefolgt von einer rein-imaginären Erweiterung von Grad 2. Wir wissen, dass das charakteristische Polynom des Frobenius-Endomorphismus auf der Jakobischen ein Grad 4 Minimalpolynom ist, welches einen solchen CM-Körper erzeugt. Nach Definition 5.2.12 besitzt es die Struktur von Gleichung (5.1):

$$h(x) = x^4 + sx^3 + tx^2 + sqx + q^2$$

mit $q, s, t \in \mathbb{Z}$. Für die Nullstellen eines Polynoms vierten Grades existiert eine geschlossene Lösungsformel für seine Nullstellen. Sie sind gegeben durch:

$$\pi_{1,2} := \frac{-s}{4} + \frac{1}{2}\sqrt{\frac{s^2}{4} - t + 2q} \pm \frac{1}{2}\sqrt{\left(\frac{s^2}{2} - t - 2q\right) - s\sqrt{\frac{s^2}{4} - t + 2q}}$$

$$\pi_{3,4} := \frac{-s}{4} - \frac{1}{2}\sqrt{\frac{s^2}{4} - t + 2q} \pm \frac{1}{2}\sqrt{\left(\frac{s^2}{2} - t - 2q\right) + s\sqrt{\frac{s^2}{4} - t + 2q}}$$

Nun definieren wir:

$$\begin{aligned} \delta &:= \frac{s^2}{4} - t + 2q \\ \alpha &:= -\left(\frac{s^2}{2} - t - 2q\right) \\ \gamma_\pm &:= -\alpha \pm s\sqrt{\delta} \end{aligned}$$

Damit $\gamma_\pm$ einen CM-Körper $\mathbb{Q}(\sqrt{\gamma_\pm})$ erzeugt, fordern wir:

$$\delta > 0 \text{ und } -\alpha \pm s\sqrt{\delta} < 0.$$

Damit die zweite Ungleichung erfüllt ist, muss gelten, dass $\alpha > 0$. Das doppelte Vorzeichen von $\gamma_\pm$ ist so zu verstehen, dass $\sqrt{-\alpha - s\sqrt{\delta}}$ und $\sqrt{-\alpha + s\sqrt{\delta}}$ denselben Körper erzeugen. Da also die Wahl des Vorzeichens von s keine Rolle spielt, definieren wir $\beta := |s|$. Wir fassen zusammen: Für $\alpha, \beta, \delta > 0$ erzeugt $\eta := \sqrt{-\alpha + \beta\sqrt{\delta}}$ einen CM-Körper von Grad 4.

Der CM-Körper $\mathbb{Q}(\eta)$ ist genau dann primitiv, wenn $\alpha^2 - \beta^2\delta$ kein Quadrat in $\mathbb{Q}$ ist, siehe [KW89] Seite 135. Dies ist nach Einsetzen von s, t und q gleichbedeutend damit, dass $(t + 2q)^2 - 4s^2q$ kein Quadrat ist. Wäre $q = s^2 - t$, so vereinfacht sich der Term zu t^2. Dies ist aber mit Sicherheit ein Quadrat in $\mathbb{Q}$, da $t \in \mathbb{Q}$. Wir schließen daraus, dass für primitive CM-Körper niemals $q = s^2 - t$ gelten darf. Der Fall *(b)* aus Satz 5.3.1 tritt somit niemals ein. Das aber wiederum bedeutet, dass $h(x)$ ein erzeugendes Polynom einer ordinären Jakobischen ist. Wir erhalten folgenden spezialisierten Satz:

Satz 6.1.1. (Erzeugung eines bestimmten CM-Körpers von Grad 4) *Sei $h(x)$ ein Polynom der Form von Gleichung (5.1), welches für oben definierte Variablen $\alpha, \beta, \delta > 0$ erfüllt. Weiter gelte $\mathrm{ggT}(t, q) = 1$. Sei $\eta := \sqrt{-\alpha + \beta\sqrt{\delta}}$ und $\mathbb{Q}(\eta)$ primitiv. Dann existiert eine Kurve $C/\mathbb{F}_q$ von Geschlecht 2, deren Jakobische J_C das charakteristische Polynom des Frobenius-Endomorphismus $h(x)$ besitzt. Des Weiteren ist der Endomorphismenring der Jakobischen gerade die Maximalordnung, d.h.* $\mathrm{End}(J_C) \cong \mathcal{O}_{\mathbb{Q}(\eta)}$.

Beweis Satz 5.3.1 zusammen mit den Bemerkungen oberhalb des Satzes und der Tatsache, dass $\mathrm{ggT}(t, q) = 1$ eine ordinäre Abelsche Varietät erzeugt. Alternativ siehe [Fre07b] Proposition 3.4. □

Bemerkung 6.1.2. *In Satz 5.3.2 haben wir einen solchen Zusammenhang bereits für einfache Abelsche Varietäten kennengelernt. Da es aber schwierig ist diesen zu verwenden, werden wir die Charakterisierung primitiver CM-Körper nutzen.*

Für ein vorgegebenes Polynom vierten Grades $h(x)$ haben wir die Nullstellen berechnet und eine minimale Körpererweiterung erzeugt, welche die Nullstellen $\pi_{1,\ldots,4}$ enthält: $\mathbb{Q}[x]/(h(x)) = \mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{-\alpha + \beta\sqrt{\delta}})$. Dabei haben wir η so gewählt, dass $\mathbb{Q}(\eta)$ primitiv ist. Anstatt K aus den Nullstellen von $h(x)$ zu erzeugen, genügt es uns einen isomorphen Körper zu erzeugen. Primitive quartische CM-Körper lassen sich aber immer in der Form $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ für a, b und $d \in \mathbb{N}$ darstellen. Sie sind genau dann primitiv, wenn $a^2 - b^2d$ kein Quadrat in $\mathbb{Q}$ ist. Dies wird uns für den späteren Algorithmus zusätzliche Freiheitsgrade eröffnen. Dabei hilft uns folgender Satz von Freeman:

Satz 6.1.3. (Erzeugung isomorpher CM-Körper von Grad 4) *Sei $\mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ ein primitiver, quartischer CM-Körper und seien $u, v, w \in \mathbb{Z}$. Setzen wir*

$$\begin{aligned} \alpha &= w^2(au^2 + adv^2 + 2bduv) \\ \beta &= bu^2 + bdv^2 + 2auv \\ \delta &= dw^4, \end{aligned}$$

dann gilt $\mathbb{Q}(\sqrt{-\alpha + \beta\sqrt{\delta}}) \cong \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$.

Beweis Siehe [Fre07b] Proposition 4.1. □

Möchten wir zu einem Polynom $h(x)$, welches die Bedingungen aus Satz 6.1.1 erfüllt, einen isomorphen CM-Körper erzeugen, so erhalten wir folgende Gleichungen:

$$\frac{s^2}{2} - t - 2q = -w^2(au^2 + adv^2 + 2bduv) \tag{6.1}$$

$$s = bu^2 + bdv^2 + 2auv \tag{6.2}$$

$$\frac{s^2}{4} - t + 2q = dw^4 \tag{6.3}$$

Durch Umstellen der Gleichungen (6.1), (6.2) und (6.3) erhalten wir Ausdrücke für q und t.

$$t = \frac{1}{2}w^2(au^2 + adv^2 + 2bduv) - \frac{1}{2}dw^4 + \frac{3}{8}(bu^2 + bdv^2 + 2auv)^2 \tag{6.4}$$

$$q = \frac{1}{4}w^2(au^2 + adv^2 + 2bduv) + \frac{1}{4}dw^4 + \frac{1}{16}(bu^2 + bdv^2 + 2auv)^2 \tag{6.5}$$

Die Gleichungen (6.2), (6.4) und (6.5) beschreiben also einen primitiven, quartischen CM-Körper, der isomorph zu dem Körper ist, welcher durch Adjunktion der Nullstellen $\pi_{1,\ldots,4}$ entsteht. Im elliptischen Fall war dies deutlich einfacher, da hier $h(x) = x^2+T$ und somit das Polynom lediglich zwei komplex konjugierte Nullstellen besitzt. Der quadratfreie Anteil von T erzeugt den CM-Körper und alle isomorphen Körper unterscheiden sich dabei nur um Quadrate von T. In Analogie nennen wir die Gleichungen (6.2), (6.4) und (6.5) die hyperelliptischen CM-Gleichungen.

Wir wenden uns nun Satz 3.6.21, dem Satz über die Existenz von speziellen elliptischen Kurven zu, um auch seine weiteren vier Voraussetzungen auf hyperelliptische Kurven zu verallgemeinern. Die Anzahl der Punkte auf der Kurve war gegeben durch die Auswertung des charakteristischen Polynoms des Frobenius an der Stelle 1, siehe Gleichung (5.3). Dies soll ein Vielfaches der betrachteten Torsionsgruppenordnung r sein. Damit wir eine möglichst kryptografisch günstige r-Torsionsgruppe darauf erhalten, fordern wir für ein möglichst großes, primes r :

$$q^2 + 1 - s(q + 1) + t \equiv 0 \pmod{r}. \tag{6.6}$$

Auch diese Ordnungsgleichung ist komplizierter als ihr Pendant im elliptischen Fall, da hier q quadratisch in die Gleichung eingeht. Bei den restlichen drei Bedingungen des Satzes haben wir Glück. Den Torsionsgruppenparameter r haben wir gerade als großen Teiler der Mächtigkeit der Jakobischen festgelegt

und auch die Bedingung, dass q eine Primzahlpotenz ist, bleibt erhalten. Für $q = p \in \mathbb{P}$ haben wir gesehen, dass sich auch die Definition des Einbettungsgrades nicht verändert. Wir erhalten somit folgende Bedingung:

$$\Phi_k(q) \equiv 0 \pmod{r} \tag{6.7}$$

Wir fassen unsere Ergebnisse zusammen und erhalten eine Existenzaussage für spezielle hyperelliptische Kurven:

Satz 6.1.4. (Existenz einer speziellen hyperelliptischen Kurve)
Seien $q, r \in \mathbb{P}$, $k \in \mathbb{N}, a, b, d \in \mathbb{Q}$ so, dass sie einen primitiven, quartischen CM-Körper erzeugen. Des Weiteren seien s, t, u, v und w Lösungen der Gleichungen (6.2) und (6.4) bis (6.7). Dann ist $h(x) = x^4 + sx^3 + tx^2 + sqx + q^2$ das charakteristische Polynom einer hyperelliptischen Kurve mit Einbettungsgrad k bezüglich r. Die Anzahl der Punkte der Jakobischen berechnet sich nach Gleichung (6.6). Ihr Endomorphismenring ist isomorph zur Maximalordnung.

Beweis Auch dieser Satz ist keine Existenzaussage für beliebige hyperelliptische Kurven, sondern lediglich eine Aussage darüber, wann eine hyperelliptische Kurve mit gewissen Eigenschaften existiert. Die Voraussetzungen des Satzes sind äquivalente Umformungen der Anforderungen an die Eigenschaften der Kurve bzw. ihrer Jakobischen. □

6.1.2 Hyperelliptische Kurven: Parametergenerierung

Freeman hat in [Fre07b] die Konstruktion hyperelliptischer Kurven in zwei Schritten durchgeführt. Zunächst beschreiben wir die Erzeugung von q, s und t. Wir stellen Freemans Algorithmus 4.2 für den Fall des gewöhnlichen Einbettungsgrades vor.

Algorithmus 7 Hyperelliptische Kurvenparameter nach Freeman

Eingabe: $a, b, d \in \mathbb{Q}, k, r \in \mathbb{N}$ und $I \subset \mathbb{Z}$. Hierbei muss $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ ein primitiver quartischer CM-Körper sein und $r \in \mathbb{P}$ mit $r \equiv 1 \bmod k$ gelten.

Ausgabe: Eine Primzahl q und $s, t \in \mathbb{Z}$, sodass $h(x) = x^4 + sx^3 + tx^2 + sqx + q^2$ potenziell das charakteristische Polynom des Frobenius einer hyperelliptischen Kurve von Geschlecht 2 über $\mathbb{F}_q$ mit Einbettungsgrad k bezüglich r ist, und die Jakobische der Kurve einen zu $\mathcal{O}_K$ isomorphen Endomorphismenring besitzt. Oder die Ausgabe keine Lösung gefunden.

1: Setze $v_0 := 0$.
2: **repeat**
3: Suche simultane Lösung $(u_0, w_0, q_0, s_0, t_0)$ des Gleichungssystems bestehend aus den Gleichungen (6.2) und (6.4) bis (6.7) für festes v_0.
4: **if** Keine Lösung gefunden **then**
5: Setze $v_0 := v_0 + 1$.
6: **else**
7: Gehe zu Zeile 11.
8: **end if**
9: **until** $v \equiv 0 \bmod r$.
10: **return** Keine Lösung gefunden.
11: Reduziere $u_0, w_0 \bmod r$ in das Intervall $[0, r[$.
12: **repeat**
13: Wähle ein noch nicht gewähltes $(i_1, i_2, i_3) \in I^3$.
14: Berechne die Werte $u := u_0 + ri_1$, $v := v_0 + ri_2$, $w := w_0 + ri_3$.
15: Berechne die Werte von s, t und q mittels der Gleichungen (6.2), (6.4) und (6.5).
16: **until** $(s, t \in \mathbb{Z}, q \in \mathbb{P}$ und $q \nmid t)$ oder alle $(i_1, i_2, i_3) \in I^3$ erfolglos durchprobiert.
17: **if** Alle $(i_1, i_2, i_3) \in I^3$ erfolglos durchprobiert **then**
18: **return** Keine Lösung gefunden.
19: **else**
20: **return** (q, s, t).
21: **end if**

Bemerkung 6.1.5. *(a) Das Lösen des Gleichungssystems reduziert sich hier sehr leicht auf die beiden Gleichungen (6.6) und (6.7), da die Gleichungen für s, t und q in diese einfach eingesetzt werden können.*

(b) Die Kunst liegt nun darin dieses nichtlineare Gleichungssystem für kryptografisch relevante Größenordnungen zu lösen.

(c) Freeman stellt fest, dass nur bei ungeradem Eingabeparameter b Lösungen gefunden worden sind. Dies stellt kein Problem dar, da alle Faktoren von

b auch quadratisch unter die Wurzel zu d gezogen werden können, ohne den Körper K zu verändern.

(d) Aufgrund der Gleichung für q und der zufälligen Verteilung der Parameter im Intervall von 0 *bis r erwartet Freeman Lösungen, bei denen* $q \approx r^4$ *ist, was* $\rho \approx 8$ *entspricht. Im Gegensatz dazu geben wir in 7.5 ein mit dem neuen Algorithmus 9 gefundenes Beispiel an, dass einen* ρ*-Wert von* 2.1745 *hat.*

(e) Die Schwierigkeit des Algorithmus liegt im Lösen des Gleichungssystems. Die zweite Schleife des Algorithmus dient lediglich dazu zu überprüfen, ob für gefundene Lösungen (u_0, v_0, w_0) *auch ein primes q existiert. Haben wir bereits eine Lösung gefunden, ist dies leicht.*

6.1.3 Hyperelliptische Kurven: Kurvenerzeugung

Die aus Algorithmus 7 erhaltenen Parameter (q, s, t) setzen wir nun im folgenden Algorithmus 8 ein, um mit ihm mit hoher Wahrscheinlichkeit eine Kurve der richtigen Ordnung von Geschlecht 2 zu erhalten. Da es sehr rechenintensiv ist, die Ordnung einer hyperelliptischen Kurve bzw. die Ordnung der Jakobischen exakt zu bestimmen, wird auf einen randomisierten Test zurückgegriffen. Dieser berechnet die Ordnung jedoch manchmal falsch, weshalb nicht mit Sicherheit garantiert werden kann, dass der Algorithmus die richtige Kurve liefert. Wie auch schon im elliptischen Fall erzeugen die Parameter die Kurven nur bis auf Twists. Ein Negativ-Test ist schnell möglich, d.h., falls die vorgegebene Ordnung nicht die der Jakobischen ist, können wir dies schnell feststellen; einen Positiv-Test führen wir jedoch nur randomisiert durch, siehe auch 6.3. Vorausgesetzt der Algorithmus liefert eine richtige Lösung, können wir einen Positiv-Test umgehen, indem wir alle anderen Kurven mittels eines Negativ-Tests ausschließen, aber auch dies ist mit hohem Rechenaufwand verbunden.

Algorithmus 8 Erzeugung der hyperelliptischen Kurve aus Parametern

Eingabe: Eine Primzahl q und ein Polynom $h(x)$, welche die Eigenschaften der Ausgabe von Algorithmus 7 besitzt.

Ausgabe: Mit hoher Wahrscheinlichkeit eine hyperelliptische Kurve, deren Jakobische J_C das charakteristische Polynom $h(x)$ besitzt und deren Endomorphismenring gleich $\mathcal{O}_K$ ist, mit $K = \mathbb{Q}[x]/(h(x))$. Oder die Ausgabe keine Lösung gefunden.

1: Berechne $K := \mathbb{Q}[x]/(h(x))$.
2: Berechne die Igusa-Klassenpolynome $H_i(x)$ für K und $i \in \{1, 2, 3\}$.
3: Bestimme für $i \in \{1, 2, 3\}$ alle Wurzeln des i-ten Klassenpolynoms in $\mathbb{F}_q$ und bezeichne die jeweilige Menge mit S_i. (D.h. für alle $s \in S_i$ gilt $H_i(s) \equiv 0 \bmod q$.)
4: Setze $n_1 := h(1)$ und $n_2 := h(-1)$.
5: **repeat**
6: Wähle ein noch nicht gewähltes Tupel $(j_1, j_2, j_3) \in S_1 \times S_2 \times S_3$.
7: Benutze Mestres Algorithmus [Mes91], um die Kurve $C/\mathbb{F}_q$ mit absoluten Igusa-Invarianten j_1, j_2 und j_3 zu errechnen.
8: Wähle einen Repräsentanten einer Restklasse $D \in \overline{D} \in J_C(\mathbb{F}_q)$.
9: **if** ($[n_1]D$ ist ein Hauptideal) **then**
10: **return** Kurve C.
11: **end if**
12: **if** ($[n_2]D$ ist ein Hauptideal) **then**
13: **return** Quadratischen Twist der Kurve C.
14: **end if**
15: **if** ($K \cong \mathbb{Q}(\zeta_5)$) **then**
16: Überprüfe für alle quintischen Twists von C, ob $[n_1]D$ ein Hauptideal ist.
17: **return** Passende Kurve bei Gleichheit.
18: **end if**
19: **until** Alle Tupel (j_1, j_2, j_3) probiert.
20: **return** Keine Lösung gefunden.

Bemerkung 6.1.6. *(a) Da nicht für alle $h(x)$ die Igusa-Klassenpolynome in angemessener Zeit berechenbar sind, werden oft die Parameter a, b, d zur Berechnung von K vorgegeben, sodass ein isomorpher Körper berechnet werden kann, für den die Igusa-Klassenpolynome bereits bekannt sind.*

(b) Die Berechnung der Igusa-Invarianten und der Igusa-Klassenpolynome kann unter anderem in [Wen03], [EL04] oder [Ber06] gefunden werden.

(c) Zur Überprüfung der Ordnung, siehe 6.3.

6.2 Brezing-Weng Verallgemeinerung

Nun werden wir den eben beschriebenen Algorithmus von Freeman als Grundlage nehmen und ihn mit dem Brezing-Weng-Algorithmus für elliptische Kurven verknüpfen. Statt als Ausgabeparameter q, s, t und $r \in \mathbb{Z}$ möchten wir also Polynome erhalten. Diese werten wir wie im Brezing-Weng-Algorithmus, an einer Stelle $x \in N$ aus und erhalten so die Parameter mittels welcher wir die hyperelliptische Kurve erzeugen können. Im Gegensatz zum Algorithmus von Freeman werden wir r nicht vorgeben, sondern lediglich überprüfen, ob mit dem im Algorithmus gewonnenen r die Erzeugung einer paarungsgeeigneten Kurve möglich ist. Auch den Einbettungsgrad werden wir nicht vorgeben, sondern nur eine obere Schranke, welche wir intern auf 50 gesetzt haben. Unter Berücksichtigung von Definition 5.6.1 ist dies zunächst willkürlich. Bei diesem Wert benötigte KASH3 für einen Schleifendurchlauf ca. eine Sekunde.

Ein solches Vorgehen hat den Vorteil, dass uns dann eine ganze Schar von Kurven zur Verfügung steht. Durch geschickte Parameterwahl soll ein günstigeres ρ als im Algorithmus 7 erzielt werden. Wünschenswert ist, dass die Polynome kleine Grade und betragsmäßig kleine Koeffizienten besitzen, also berechenbar bleiben und erst durch Auswertung große Kurven entstehen. Die Gleichungen (6.2) und (6.4) bis (6.7) sind auch für Polynome gültig. Analog zu Freeman werden wir nicht alle möglichen Lösungen suchen, sondern uns auf einen Bereich einschränken, in dem wir Lösungen suchen. Diesen Bereich grenzen wir ein, indem wir den Grad und den Absolutbetrag der Polynome $u(x), v(x)$ und $w(x) \in \mathbb{Z}[x]$ vorgeben. Des Weiteren wählen wir einen oder mehrere CM-Körper, deren erzeugende Parameter a, b und d wir aus [Wam99] übernommen haben. Im Einzelnen sind diese in Tabelle 6.1 zu finden.

	1	2	3	4	5	6	7	8	9	10	11	12	13
a	$\frac{5}{2}$	2	13	5	65	29	85	37	10	65	13	53	61
b	$\frac{1}{2}$	1	2	1	26	2	34	6	5	10	3	2	6
d	5	2	13	5	5	29	5	37	2	13	13	53	61

Tabelle 6.1: Parameter (a, b, d) zur Erzeugung verschiedener CM-Körper

Die Koeffizienten der ersten Spalte erzeugen einen zu $\mathbb{Q}(\zeta_5)$, die restlichen einen zu $\mathbb{Q}(\sqrt{-a+b\sqrt{d}})$ isomorphen Körper. Sie sind codiert durch die Werte 1 bis 13.

Ebenso wie im Algorithmus 7 erhalten wir aus den fünf oben genannten Gleichungen ein nichtlineares Gleichungssystem modulo r, bestehend aus lediglich zwei Gleichungen, indem wir die drei Gleichungen (6.2), (6.4) und (6.5) in Gleichungen (6.6) und (6.7) einsetzen. Um das Gleichungssystem für Werte

$u(x), v(x), w(x) \in \mathbb{Z}[x]$ zu lösen, berechnen wir den größten gemeinsamen Teiler der linken Seiten beider Gleichungen. Wir unterscheiden hierbei folgende Fälle: Erstens u, v und w sind ganze Zahlen und zweitens eines der $u(x), v(x)$ und $w(x)$ ist ein Polynom.
Der erste Fall entspricht einer abgewandelten Version des Algorithmus 7. Im Unterschied zu Freeman, siehe [Fre07b] Algorithmus 4.2, haben wir kein r vorgegeben, was den Algorithmus langsamer aber flexibler macht. Ein Eingabeparameter ist also ρ_0, eine Größenordnung für den Sicherheitsparameter $\rho = \frac{2 \log q}{\log r}$, aus dem sich eine Größenordnung für r berechnen lässt. Da wir fordern, dass r prim sein soll, müssen wir für $r(x)$ ein irreduzibles Polynom wählen. Ist der größte gemeinsame Teiler nicht irreduzibel, so können wir für $r(x)$ nicht den größten gemeinsamen Teiler wählen, sondern müssen einen irreduziblen Faktor des größten gemeinsamen Teilers wählen. Auch hier können wir ρ berechnen $\rho \approx \frac{2 \deg q(x)}{\deg r(x)}$. Er wird im Algorithmus nicht abgefragt, da wir zuerst daran interessiert sind, überhaupt Lösungen zu finden. Er kann daher dazu missbraucht werden, Freeman-Lösungen auszuschließen, indem wir mit $\rho = 0$ die theoretische untere Schranke von ρ unterschreiten. Es ist zu beachten, dass r letztendlich prim sein muss. Ist also der größte gemeinsame Teiler ein reduzibles Polynom, so ist für $r(x)$ lediglich ein irreduzibler Faktor als $r(x)$ zu wählen.

Algorithmus 9 Neuer Algorithmus

Eingabe: Ein Intervall $I \subset [1, \ldots, 14]$, das die zu überprüfenden CM-Körper codiert, sechs natürliche Zahlen $\mathrm{Grad}_u, \mathrm{Grad}_v, \mathrm{Grad}_w, \mathrm{Koef}_u, \mathrm{Koef}_v, \mathrm{Koef}_w$, die bestimmen, in welchem Bereich gesucht werden soll sowie den maximalen Sicherheitsparameter ρ_0.

Ausgabe: Zwei irreduzible Polynome $q(x), r(x) \in \mathbb{Q}[x]$ sowie zwei weitere Polynome $s(x), t(x) \in \mathbb{Q}[x]$, sodass für $x \in \mathbb{Z}$ ganzzahlige Lösungen q, s, t und r existieren, für die $h(x)$ potenziell das charakteristische Polynom des Frobenius einer hyperelliptischen Kurve von Geschlecht 2 über $\mathbb{F}_q$ mit Einbettungsgrad k bezüglich r ist. Oder die Ausgabe keine Lösung gefunden.

1: Setze Parameter a, b, d je nach CM-Körper, siehe Tabelle 6.1.
2: **repeat**
3: Erzeuge Polynome bzw. Integer $u(x), v(x)$ und $w(x)$ aus $\mathbb{Z}[x]$, deren Grad und absolute Koeffizienten kleiner sind als die vorgegebenen.
4: Erzeuge durch Einsetzen der Polynome $u(x), v(x)$ und $w(x)$ in Gleichungen (6.2), (6.4) und (6.5) die Polynome $q(x), s(x)$ und $t(x)$.
5: **if** $\mathrm{Grad}_u = \mathrm{Grad}_v = \mathrm{Grad}_w = 0$ **then** $\{\backslash *$ *Freeman-Fall* $* \backslash\}$
6: **if** $q, s, t \in \mathbb{Z}$ **then**
7: Berechne nach Gleichung (6.6) die Anzahl der Punkte der Jakobischen R, und nach Gleichung (6.7) die k-ten Kreisteilungspolynome $\Phi_k(q)$ für die Einbettungsgrade $1 < k \leq J$.
8: Berechne die größten gemeinsamen Teiler R_k von R und Φ_k für alle k. Ist für ein k der ρ-Wert des größten Primfaktors r_k eines R_k kleiner als ρ_0, so überprüfe, ob durch Abänderung von $u, v, w \bmod r_k$ ein $\tilde{q} \equiv q \bmod r_k$ mit $\tilde{q} \in \mathbb{P}$ existiert, siehe Bemerkung 6.2.1.
9: **if** $\tilde{q} \in \mathbb{P}$ **then**
10: **return** $(\tilde{q}, s, t, r_k, k)$
11: **end if**
12: **end if**
13: **else** $\{\backslash *$ *neuer Fall* $* \backslash\}$
14: Berechne nach Gleichung (6.6) das Polynom $R(x)$, welches die Punktezahl der Jakobischen angibt und nach Gleichung (6.7) die k-ten Kreisteilungspolynome $\Phi_k(q(x))$ für die Einbettungsgrade $1 < k \leq J$. (Hier $J = 50$.)
15: Berechne die größten gemeinsamen Teiler $R_k(x)$ der Polynome $R(x)$ und $\Phi_k(x)$.
16: **if** $\deg(R_k(x)) > 0$ **then**
17: Setze $r_k(x)$ als größten irreduziblen Faktor von $R_k(x)$.
18: **return** $(q(x), s(x), t(x), r_k(x), k)$.
19: **end if**
20: **end if**
21: **until** Alle Polynome überprüft, die die Eingabeparameter erfüllen.
22: **return** Keine Lösung gefunden.

Bemerkung 6.2.1. *(a) Suchen wir für den Output $q(x), s(x), t(x), r_k(x)$ und k für $x \in \mathbb{Z}$ Lösungen in $\mathbb{P}$ bzw. $\mathbb{Z}$, so können wir dann mit Algorithmus 8 randomisiert eine hyperelliptische Kurve mit den gewünschten Eigenschaften generieren.*

(b) Ist $\mathrm{Grad}_u = \mathrm{Grad}_v = \mathrm{Grad}_w = 0$, liefert der Algorithmus dieselben Lösungen wie Algorithmus 7. Diesen wollen wir als den Freeman-Fall bezeichnen.

(c) Das Abändern von Lösungen $\bmod r$, siehe Bemerkung 6.1.5 bzw. Algorithmus 7 Zeilen 12 bis 16, ist nur im Freeman-Fall sinnvoll. Im anderen Fall wird $q(x)$ erst auf Teilerfreiheit überprüft, nachdem ein x festgelegt wurde, um so ein primes q zu erhalten. Änderungen $\bmod r$ würden dazu führen, dass q nicht mehr prim ist.

Ein Beweis für die Korrektheit des Algorithmus ergibt sich aus den Bemerkungen, die wir für Algorithmus 7 gemacht haben.

Im Gegensatz zu Freeman, der ein r vorgibt, haben wir den Algorithmus so geschrieben, dass er überprüft, ob zwei Polynome einen gemeinsamen Teiler besitzen. Haben wir eine Lösung gefunden, so setzen wir $r(x)$ als einen irreduziblen Teil dieser Lösung und können dann durch Einsetzen von x analysieren, ob eine ganzzahlige Lösung existiert. Da für uns bei Torsionsgruppen nur prime Ordnungen von Nutzen sind, müssen wir gegebenenfalls auch hiervon einen Teiler wählen.

Die freie Wahl von $r(x)$ hat - wie immer - Vor- und Nachteile. Zum einen müssen wir deutlich mehr Berechnungen durchführen, zum anderen haben wir uns aber nicht im Vorhinein auf ein $r(x)$ festgelegt, sodass wir (speziell im Polynomfall) alle Lösungen finden. Im Polynomfall ist eine vorherige Beschränkung auf $r(x)$ jedoch nicht geeignet, da eine Kurve mit gesuchten Parametern noch von der Wahl von x abhängt.

Die Berechnung von Gleichungen (6.6) und (6.7) könnte auch auf eine andere Art durchgeführt werden. Nach einsetzen von $q(x), s(x)$ und $t(x)$ könnte Gleichung (6.6) daraufhin überprüft werden, ob das resultierende Polynom irreduzibel ist. Ist dies der Fall, so verschwindet die linke Seite der Gleichung ausschließlich, wenn diese mit $r(x)$ übereinstimmt. In diesem Fall überprüfen wir dann für jedes Kreisteilungspolynom bis zu einem bestimmten Grad J, ob es von $r(x)$ geteilt wird. Ist es reduzibel, so müssen wir für jeden Teiler überprüfen, ob dieser nicht die Kreisteilungspolynome teilt. Das ist ohne Weiteres möglich. Da aber möglichst große r-Torsionsgruppen gesucht sind, sind diese Lösungen nicht wünschenswert.

6.3 Testen der hyperelliptischen Kurven

Auch im hyperelliptischen Fall sollten wir die Möglichkeit haben die gewonnenen Kurven auf alle fünf Bedingungen des Satzes 6.1.4 zu testen, also festzustellen, ob es sich um gesuchte Kurven handelt. Auch hier lässt sich direkt nachrechnen, ob q, s, t, r und k korrekt zueinander in Beziehung stehen, q und r Primzahlen sind sowie die Kurve einen niedrigen Einbettungsgrad k besitzt. Schwieriger ist es die Ordnung der Jakobischen zu bestimmen, was im Folgenden beschrieben wird.

Zur gegebenen hyperelliptischen Kurve konstruieren wir zunächst den Funktionenkörper. Dann wählen wir einen beliebigen Divisor von Grad 0, indem wir zum Beispiel zwei Punkte der Kurve voneinander subtrahieren. Wir multiplizieren diesen mit der vermuteten Ordnung der Jakobischen (d.h. Addition mit sich selbst). Ist das Ergebnis kein Hauptdivisor, so wissen wir, dass wir eine falsche Kurve bzw. falschen Twist bestimmt haben, der Negativ-Test ist also erfolgreich.
Wie auch im elliptischen Fall ist der Positiv-Test weniger aussagekräftig. Es treten die gleichen gruppentheoretischen Probleme auf wie in 4.2.2. Auch im Fall hyperelliptischer Kurven rechnen wir mit randomisierten Primzahltests. Daher werden wir uns auch im hyperelliptischen Fall mit einer stochastischen Absicherung durch Wahl von fünf Divisoren von Grad 0 und deren Überprüfung begnügen.

Kapitel 7

Beispiele und Laufzeitbetrachtungen

In diesem letzten Kapitel werden wir die Ergebnisse der Algorithmen betrachten. Dabei werden in allen Abschnitten die verwendeten KASH3 Befehle erläutert, mit denen die Kurven erzeugt wurden. Die ersten vier Abschnitte 7.1 bis 7.4 behandeln dabei die elliptischen Kurven. Die Beispiele werden in derselben Reihenfolge wie die Algorithmen vorgestellt. Zuerst werden Beispiele für den Cocks-Pinch-Algorithmus erzeugt, danach für den Cocks-Pinch-Produkt-Algorithmus, dann für den Brezing-Weng-Algorithmus und den Brezing-Weng-Produkt-Algorithmus. Schließlich befassen sich 7.5 und 7.6 mit hyperelliptischen Kurven. Auch hier wird zuerst der Freeman-Algorithmus und danach der verallgemeinerte Algorithmus untersucht. Abschließend wird eine kurze Zusammenfassung gegeben.

7.1 Cocks-Pinch Beispiele

Dieser Abschnitt beschreibt die Suche nach elliptischen Kurven mittels des Cocks-Pinch-Algorithmus. Die Eingabeparameter des Algorithmus sind die Fundamentaldiskriminante D, der Einbettungsgrad k sowie ein Startparameter r_0, welcher vorgibt, wie groß die Torsionsgruppe der Kurve mindestens sein soll. In der Literatur wird fälschlicherweise -1 als Fundamentaldiskriminante benutzt. Diese Zahl ist keine Fundamentaldiskriminante, sie erzeugt aber dieselbe Körpererweiterung wie $D = -4$. Des Weiteren wird oft $D = -3$ gewählt, siehe u.a. [ACD$^+$06] Bemerkung 18.6 und [MKHO07] Kapitel 4. Diese beiden Körpererweiterungen haben den Vorteil, dass für die zu erzeugenden Kurven die j-Invariante und somit ein Twist der Kurve schon bekannt sind. Für alle anderen Fälle wurde für diese Arbeit ein Algorithmus implementiert, der mittels Weberpolynomen eine Nullstelle des Hilbertschen Klassenpolynoms, also eine j-Invariante erzeugt. Daher werden wir auch Beispiele für andere Fundamentaldiskriminanten erzeugen, die in der Literatur nicht sehr häufig zu finden sind.

Die Größenordnung von derzeit eingesetzten r-Torsionsgruppen beträgt 160 bis 512 bit, was ungefähr folgenden Zehnerpotenzen entspricht: $160\,\text{bit} = 2^{160} \approx 10^{48}, 256\,\text{bit} = 2^{256} \approx 10^{77}, 512\,\text{bit} = 10^{144}$. Unser dritter Parameter ist der Einbettungsgrad. Dieser wird sinnvollerweise so gewählt, dass die Kurve gegenüber Angriffen balanciert ist, siehe Tabelle 3.1. In unseren Beispielen werden wir bewusst auch andere Einbettungsgrade wählen, um zu verdeutlichen, dass der Algorithmus nicht auf bestimmte Startparameter beschränkt ist. Zunächst wird ein Beispiel berechnet, das aufgrund der Wahl der Fundamentaldiskriminante leicht zu überprüfen ist. Das zweite Beispiel wurde unter dem Gesichtspunkt ausgewählt, dass es keinem Spezialfall zugeordnet werden kann. Die Fundamentaldiskriminante ist weder -3 noch -4, der Einbettungsgrad ist keine Primzahl und der Startparameter der Torsionsgruppenordnung ist in der Größenordnung von 512 bit . Diese ersten zwei Kurven der Beispiele 1 und 2 wurden mit Hilfe des Cocks-Pinch-Algorithmus berechnet.

Die Berechnungen wurden sowohl mit der KASH3 Version für Windows vom 19. November 2005 als auch mit der Linux Version vom 31. Januar 2006 durchgeführt. Die Beispiele sind so aufgebaut, dass sie mittels KASH3 Schritt für Schritt nachvollzogen werden können. Die zu diesem Zweck entwickelten Funktionen sind auch in Anhang A beschrieben.

Beispiel 1: Starten wir den Algorithmus 3 mit `CocksPinch(D,k,r0)`, und wählen dabei folgende Parameter $D = -3, k = 4, r_0 = 10^{50}$, so erhalten wir folgendes Ergebnis:

$$\begin{aligned} r =& 10^{50} + 6633 \\ p =& 191811319333298580507941703025814109190981171889978689674555673\backslash \\ & 6821634247669583799450886339158085821 \\ t =& 584486317797883707165160525613008245085278519058 97 \end{aligned}$$

Daraus berechnen wir dann die Ordnung der gesuchten Kurve:

$$\begin{aligned} R =& p - t + 1 = 191811319333298580507941703025814109190981171889972 84\backslash \\ & 4811377694845091773161702249862637781130617992 5 \\ =& 3^3 \cdot 5^2 \cdot 3853 \cdot 737516007087497305641363451378201148469133 9 \cdot \\ & (10^{50} + 6633). \end{aligned}$$

Wir sehen also, dass $r \mid R$ gilt. Des Weiteren können wir nachprüfen, dass auch die CM-Gleichung erfüllt ist: $4 \cdot p = t^2 - (-3) \cdot y^2$ für

$$y = 37666121897547209242637797483445916836279055548416$$

Aufgrund der Tatsache, dass wir $D = -3$ gewählt haben, sind alle Twists der Kurve gegeben durch

$$E\colon y^2 = x^3 + a_6,$$

wobei $a_6 \in \mathbb{F}_q$ so zu wählen ist, dass die Kurve keine mehrfachen Nullstellen hat. Wir überprüfen dies anhand der Diskriminante Δ_E, siehe Definition 3.4. Die Wahrscheinlichkeit einen Parameter zu wählen, für den wir eine singuläre Kurve erhalten ist sehr gering. Wir wählen zum Beispiel $a_6 = 4$. Dann können wir in KASH3 die Kurve mittels des Befehls `EllipticCurve(p,[0,a_6])`, oder, da die j-Invariante gleich 0 ist, auch mittels des implementierten Befehls

```
EllipticCurveFromJInvariantWithZero(Coerce(GF(p),0))
```

erzeugen.
Danach berechnen wir mittels `Twists` alle Twists der Kurve, wobei es in diesem Fall fünf weitere Kurven gibt. Zusammen mit der ursprünglichen erhalten wir die Kurven:

$$E_1\colon y^2 = x^3 + 980590701062974416798029902473096013214428522944810202 \setminus 126379564070435081887875219529865327414883567$$

$$E_2\colon y^2 = x^3 + 306317384400826912916443502637308025632617888701472729 \setminus 91889304364758216760189376923350939913662368 8$$

$$E_3\colon y^2 = x^3 + 470107237475828063963947593650166293265174613008788057 \setminus 53943576981254333796902226471356344217837992$$

$$E_4\colon y^2 = x^3 + 142897221331841164418363061512606122202930731096564863 \setminus 87060300741426795741705809961662437407000192 11$$

$$E_5\colon y^2 = x^3 + 160768835667053878106001533755994992521003531003845397 \setminus 93306079477725325761216577993181648450961092 27$$

$$E_6\colon y^2 = x^3 + 341875571408764611609539158360851537685430302373056212 \setminus 93794355313510023570945359719590425118511632 9$$

Wir überprüfen mittels des Befehls `IsSize(Kurve,R)`, welcher Twist die richtige Ordnung besitzt. Lediglich einer der Twist wird das Ergebnis `TRUE` haben. Es genügt also fünf falsche Ordnungen herauszufiltern. (Zur Erinnerung: Die Negativ-Tests sind deterministisch.) In unserem Fall ist Kurve E_6 die gesuchte. Sie besitzt einen Sicherheitsparameter von $\rho = 1,9867$.

Wir sehen also, dass zur Erzeugung einer paarungsgeeigneten Kurve mehrere Schritte hintereinander ausgeführt werden müssen. Zur Vereinfachung wurde daher die Routine `CP_Kurve(D,k,r0)` implementiert. Sie führt neben verschiedenen Fallunterscheidungen die oben beschriebenen Schritte hintereinander aus, liefert also bei Eingabe der obigen Parameter D, k und r_0 sofort die gesuchte Kurve E_6. Ist lediglich eine paarungsgeeignete Kurve mit vorgegebener Fundamentaldiskriminante und vorgegebenem Einbettungsgrad gesucht, so ist liefert der Befehl diese Kurve.

Beispiel 2: Betrachten wir nun ein Beispiel mit nicht speziellen Parametern, zum Beispiel mit den Parametern $D = -51, k = 12, r_0 = 10^{150}$. Hierbei ergibt sich die Kurvengleichung nicht sofort aus Kenntnis der Fundamentaldiskriminante. Zuerst berechnen wir wiederum die gesuchten Kurvenparameter mittels `CocksPinch(D,k,r)`. Danach führen wir den eigens implementierten Befehl `Weber_to_Hilbert(D,p)` aus, siehe auch hier Anhang A. Er liest aus einer Tabelle die Koeffizienten der Weberpolynome, um daraus eine j-Invariante modulo p zu erzeugen. Dann generieren wir wieder die Kurve mittels des Befehls `EllipticCurveFromJInvariantWithZero(j)`. Die Überprüfung der Twists verläuft analog zu Beispiel 1. Wir erhalten folgendes Ergebnis:

$$
\begin{aligned}
r =& 10^{150} + 77877 \\
p =& 10371647068261165414312294297338400070771490686869851605208451 \backslash \\
& 64206062575879432017064374440622258368529569427374173831793241 \backslash \\
& 83101029695661735535756911767157625807860103829176558073434876828 \backslash \\
& 33026399442149552463908337488678098859646455272379031233873291 \backslash \\
& 48114125941653167406513093316679519108942769 \\
t =& 84226510288897052861827354911234054478116629659833309776134707 \backslash \\
& 83966501846140354226441145069737275563975249559044309087333292419 \backslash \\
& 72261897365565550638 1
\end{aligned}
$$

Außerdem berechnen wir die Ordnung der Kurve zu:

$$
\begin{aligned}
R =& p - t + 1 = 10371647068261165414312294297338400070771490686869851 \backslash \\
& 60520845146642060625758794320170643744406222583685295694273741738 \backslash \\
& 31793241831010296956617355357569117587349747789703985429938225 \backslash \\
& 83114713802213634334588185748504375535221762527192922288312339 \backslash \\
& 61496597727829561853549856229407358889609048978255238770523
\end{aligned}
$$

Für obiges p liefert der Befehl `Weber_to_Hilbert(-51,p)` die j-Invariante:

$$
\begin{aligned}
j =& 66170270741738504597960072211874591769705014450221534572955157990 \backslash \\
& 80931960113260240616983634426774675864476570143140605859471900 \backslash \\
& 24901442379473670902140049642740457957276872452223406530974028265 \backslash \\
& 37617925574124376357440856610897719661667285313120529971148024270 \backslash \\
& 52412430608767422789173150516101185981959974 7
\end{aligned}
$$

Aus der j-Invariante können wir die Parameter der Kurvengleichung $a_4 = \frac{-27j}{4(j-12^3)}$ und $a_6 = \frac{-27j}{4(j-12^3)}$ berechnen. Die Kurvengleichung lautet:

$$E\colon y^2 = x^3 + a_4 x + a_6$$

mit den Parametern

$$\begin{aligned}
a_4 =& 91871649153812900011923394161502748540196037766360207264810753 0 \backslash \\
& 99206974642496996183077470859687078217266653235100889079577771 8 \backslash \\
& 89021365960588023311501824516516358809277060872433033622000037 7 \backslash \\
& 02331465273091570613177220166320350238830366795996952237890039 9 \backslash \\
& 47302374558321979947316598585464238514999512969 49 \\
a_6 =& 11844821528798754131199548811881252167518869102338308787273761 5 \backslash \\
& 64999087933382435833986903580935180151262916192273284752215469 9 \backslash \\
& 41988930996029332046067293155059899269323977419332547112348730 5 \backslash \\
& 77998798721329924911461863208566430749766097756726838074448692 9 \backslash \\
& 70745739567619673220089914507852441004109429799 54
\end{aligned}$$

Diese Kurve besitzt einen einzigen quadratischen Twist. Wir können ihn nach Satz 3.3.12 durch ein v, welches kein quadratischer Rest modulo p (Legendresymbol) ist, bestimmen. Hier ist zum Beispiel $v = 3$ möglich. Somit hat die getwistete Kurve die Parameter:

$$\begin{aligned}
\tilde{a}_4 &= 9a_4 \\
\tilde{a}_6 &= 27a_6
\end{aligned}$$

Mit Hilfe des eigens implementierten Befehls `IsSize(Elk,R)` finden wir heraus, dass wir die ursprüngliche Kurve suchen. Der Sicherheitsparameter berechnet sich zu $\rho = 2,00677$. Wie auch schon in Beispiel 1, ist auch dieser vom günstigen Wert 1 weit entfernt. Offensichtlich ist ρ sogar größer als 2. Dies mag auf den ersten Blick verblüffen, da in 4.4 das Ergebnis kleiner gleich 2 ist, wir schlussfolgern also, dass für betragsmäßig großes D die Approximation zu falschen Ergebnissen führt.

7.2 Cocks-Pinch-Produkt Beispiele

Nun werden wir den Cocks-Pinch-Produkt-Algorithmus mit den gleichen Parametern wie den Cocks-Pinch-Algorithmus ausführen. Dies ermöglicht einen besseren Größenvergleich mit den bereits gefundenen Kurvenordnungen. Aufgrund eines Sicherheitsparameters in der Größenordnung von 2, erwarten wir eine Vervierfachung der Gruppenordnung gegenüber den Kurven aus Beispielen 1 und 2.

Beispiel 3: Starten wir die entwickelte Funktion `CocksPinchProduct(D,k,r)` mit den Parametern aus Beispiel 1, $D = -3, k = 4, r_0 = 10^{50}$, so finden wir

folgende Lösung:

$$
\begin{aligned}
r_1 =& 10^{50} + 1521 \\
r_2 =& 10^{50} + 3021 \\
p =& 29400588179618356813927893202409881404779565924040566 4840245363 \backslash \\
& 2583736656289825933064347857072087078324947094469707610282116 81 \backslash \\
& 3728683029398945407771942465118528086607856628666207619 88139408 \backslash \\
& 22740569863 \\
t =& 63006837606837606837606837606666666666666666666695284365641025641 \backslash \\
& 0256410256409740000000000000002895127
\end{aligned}
$$

Wiederum berechnet sich die Ordnung zu:

$$
\begin{aligned}
R =& p - t + 1 = 29400588179618356813927893202409881404779565924040566 \backslash \\
& 4840245363258373665628982593306434785707208707769487871840133 15 \backslash \\
& 4190604843766201636273227874107665809947750244558221560302523 36 \backslash \\
& 188813940822737674737
\end{aligned}
$$

Nun überprüfen wir, ob die Ordnung der Kurve tatsächlich r_1 und r_2 als Teiler besitzt. Dies ist notwendig, da wir im Algorithmus 4 über Ringen, die nicht nullteilerfrei sind, gearbeitet haben. Wir stellen also fest, dass $r_1 r_2$ tatsächlich R teilt. Da wir $D = -3$ gewählt haben, kennen wir bereits die Kurvengleichung aus Beispiel 1. Leider ist die Implementierung der elliptischen Kurven solcher Größenordnungen sehr langsam (Abbruch nach 24 Stunden). Wir verzichten daher darauf den genauen Twist zu berechnen. Auch den Sicherheitsparameter berechnen wir nicht. Da wir die Torsionsgruppe bewusst so gewählt haben, dass sie zwei große Primteiler besitzt, ist er ohne Aussagekraft.

Beispiel 4: Auch hier verläuft die Berechnung analog zu den vorherigen Beispielen. Wir benutzen die Parameter $D = -51, k = 12, r_0 = 10^{150}$, die wir aus Beispiel 2 kennen. Zu erkennen ist, dass der eigens implementiere Algorithmus auch für diese Größenordnungen problemlos die Kurvenparameter erzeugen kann. Die Größenordnung des endlichen Körpers hat sich in der Tat vervierfacht. Es ergeben sich folgende Werte:

$$
\begin{aligned}
r_1 =& 10^{150} + 95841 \\
r_2 =& 10^{150} + 104001 \\
p =& 1129472927774133685174567982676462801864466474421197754366711738269056243074693131923012540663046459803784166634844443321787054533382333483435933107834442793676101304496259560364487106905086987559989280044794690884856064543985282883899392682025486161192542831040192221744010586488352607624153742949747802383665218822908643479014231249091159541732609713124323898192844464912869559202982399179215574676688607787869394449178019696190786850740038635314999676102723088945872277221601177643239770493426681047794099217593889055931494008594495316959120904238357527397166393308789564508498964096031816593444618 \\
t =& 7426069009673238153993040227367371822655518267351631360961844289767696843545263653469540473631988509343090554939972207458889691846562838661635014135986030750264412534301766864340369279965553228923183171392767980130239425550965224485678798200436960190760804312049547931986841734381783648702301937613 0
\end{aligned}
$$

Weiter berechnen wir die j-Invariante mit Hilfe des hierfür neu entworfenen Befehls `Weber_to_Hilbert(-51,p)` zu:

$$
\begin{aligned}
j =& 8157177812365390485906131911583840789685183464566194450055105869701177735906668044216307733520957912581672359042915257618883171082208074874502342790688317035328766777760672654900298949653221164570555180929518644194373228699258522762140358278737748709006294314903710351915890051678149019750638359589356824174553612908567753831581639539232669335674244233405579837971978864610051665990787523359994993925648694527796339049234058653131696791149236685321622525185888949885402876649140792111300845350358599577697059845103950261277193505444034855531300134267426308255564409873885548935734596168353921617713850 \\
\end{aligned}
$$

Daraus lassen sich dann wie in Beispiel 2 die Parameter der kurzen Weierstraß-Normalform errechnen. Wir verzichten wieder auf die genaue Bestimmung des Twists.

Da die Laufzeitabhängigkeit von D und k sehr stark vom Startparameter r_0 abhängt, haben wir für verschiedene Werte von D und k stochastische Untersuchungen durchgeführt. Dazu haben wir den Algorithmus mit gleichem D und

		$k=5$	$k=8$	$k=20$	$k=37$	$k=101$
160 bit	CPP , $D=-3$	28 sec	18, 5 sec	12 sec	6 sec	2, 5 sec
256 bit	CPP , $D=-3$	122 sec	132 sec	67 sec	24 sec	6, 5 sec
256 bit	CPP , $D=-8$	165 sec	155 sec	124 sec	32 sec	12 sec
256 bit	CPP , $D=-20$	322 sec	270 sec	211 sec	31 sec	20 sec
256 bit	CPP , $D=-51$	223 sec	183 sec	152 sec	25 sec	14 sec
512 bit	CPP , $D=-3$	11332 sec	8924 sec	6256 sec	698 sec	179 sec
512 bit	CPP , $D=-51$	11703 sec	7202 sec	4778 sec	1808 sec	432 sec

Tabelle 7.1: Laufzeitvergleich für verschiedene Einbettungsgrade, Fundamentaldiskriminanten und Schlüsselgrößen

k für verschiedene Werte von r_0 gestartet. Es wurden lediglich die Kurvenparameter r, p und t berechnet. Um einen Mittelwert über die Laufzeiten bilden zu können, wurde die Startgröße r_0 schrittweise um ein Tausendstel erhöht. So erfolgten zum Beispiel elf Programmaufrufe zur Mittelwertbildung der Parameter $D = -3, k = 5$ und $r_0 = 160\,\text{bit}$. Hierfür wurden D und k konstant gehalten, wohingegen r_0 die Werte $(-3, 5, 10^{48}), (-3, 5, 10^{48} + 10^{45}), (-3, 5, 10^{48} + 2 \cdot 10^{45}), \ldots, (-3, 5, 10^{48} + 10 \cdot 10^{45})$ annahm.
Aus Tabelle 7.1 sehen wir zunächst, dass mit steigender Schlüssellänge die Laufzeit zunimmt. Die Laufzeit erhöht sich bei einer Verdopplung der Sicherheit (quadrieren von r_0) nicht einheitlich. Von 256 auf 512 bit liegt der Faktor zwischen 28 und 92. Eine Erhöhung der Laufzeit ist bei Erhöhung der Schlüsselgröße zu erwarten. Die Berechnung einer Wurzel modulo p, also auch die Berechnung der nächst größeren Primzahl, beansprucht bei größeren Zahlen mehr Laufzeit. Unerwartet ist die Abhängigkeit der Laufzeit von der Fundamentaldiskriminante. Bei gleicher Schlüsselgröße und Einbettungsgrad sollte sie nicht so stark variieren, da sie weder die Laufzeit der Suche nach einer Primzahl noch die nach einer Wurzel beeinflusst. Vermutlich liegen die starken Abweichungen in hoher Varianz begründet. Das Phänomen scheint sich im Fall der 512 bit Schlüssel umzudrehen. Mit statistischen Methoden könnte festgestellt werden, wie viele Wiederholungen notwendig sind, um die Varianz ausreichend zu reduzieren.

Eine weitere Erkenntnis ist, dass sich die Laufzeit mit wachsendem Einbettungsgrad verringert. Das spricht dafür, dass der Einbettungsgrad einer beliebigen Kurve nicht gleichverteilt ist, sondern weniger Kurven mit niedrigem

Einbettungsgrad existieren. Dies wiederum bedeutet natürlich, dass es schwierig ist, Kurven mit kleinem Einbettungsgrad zu finden.

Konkrete Aussagen lassen sich ohne extensive Tests nicht treffen. Diese würden den Rahmen der Arbeit sprengen. Zum einen besitzt die Laufzeit eine große Varianz, die durch das Auffinden geeigneter Primzahlen bedingt ist. Zum anderen hängt die absolute Laufzeit mit der genauen Implementierung des Algorithmus zusammen. Die Berechnungen wurden alle auf einem $2,4\,\text{GHz}$ AMD-Opteron Cluster mit $1\,\text{GByte}$ Hauptspeicher des Max-Planck-Instituts für Informatik in Saarbrücken durchgeführt. Auf diesem ist sichergestellt, dass die Laufzeiten deterministisch sind. Gleiche Programmausführung führt also immer zu gleichen Laufzeiten. Der Algorithmus liefert auch Kurven größerer Mächtigkeit. So benötigte er beispielsweise 4370 Sekunden für $r_0 = 768\,\text{bit}$, mit $D = -3$ und $k = 101$ und 3455 Sekunden für $r_0 = 1024\,\text{bit}$, mit $D = -3$ und $k = 101$.

7.3 Brezing-Weng Beispiele

Es existieren bereits Kurven, die mit dem Brezing-Weng-Algorithmus berechnet wurden, siehe [Tes07]. Wir geben zunächst eine bisher unbekannte an, bevor wir uns dann mit der Produktvariante auseinandersetzen.

Beispiel 5: Gestartet wird der Brezing-Weng-Algorithmus durch den Aufruf von `BrezingWeng(D,k,r)`. Wie auch im Cocks-Pinch-Algorithmus steht D wieder für die Fundamentaldiskriminante und k für den Einbettungsgrad. Im Gegensatz zum Parameter r_0 des Cocks-Pinch-Algorithmus ist r ein Polynom. Es existieren verschiedene Möglichkeiten $r(x)$ zu erzeugen. Wählen wir ein zufälliges $r(x)$, so erzeugt dies fast nie einen passenden CM-Körper. Daher wurden folgende, zusätzliche Funktionen für diese Arbeit erstellt. Der Befehl `Poly_Dk(D,k)` erzeugt ein Minimalpolynom des Körpers, der durch die beiden Polynome $\Phi_k(x)$ und $x^2 - D$ erzeugt wurde. KASH3 erzeugt dieses Minimalpolynom deterministisch. Wählen wir jedoch ein anderes Element des Körpers, so bestehen gute Chancen, dass auch sein Minimalpolynom denselben Körper erzeugt. Dies ist genau dann der Fall, wenn das neue Minimalpolynom denselben Grad besitzt wie das ursprüngliche Minimalpolynom. Ein solch randomisiertes Minimalpolynom erzeugen wir mit `Zufallspoly_Dk(D,k)`. Schließlich ist ein Aufruf von `CyclotomicPolynomial(CheckCyclo(D,k))` möglich, um eine geeignete Körpererweiterung zu erzeugen. Diese Funktion berechnet das $(n \cdot k)$-te Kreisteilungspolynom kleinsten Grades, welches auch Wurzel aus D enthält. Die Berechnung des Befehls `CheckCyclo` dauert für Kreisteilungspolynome, die einen Grad größer 80 besitzen, unverhältnismäßig lange. Um dies zum umgehen, kann das $(D \cdot k)$-te Kreisteilungspolynom verwendet werden. Es erzeugt immer eine passende Körpererweiterung, die eventuell jedoch nicht minimal ist. Außerdem muss im Algorithmus die Einheitengruppe der Maximalordnung bestimmt werden, welches der rechenintensivste Schritt des Algorithmus ist.

Starten wir den Algorithmus mit den Parametern $D = -3$, $k = 7$ und $r =$ `CyclotomicPolynomial(CheckCyclo(-3,7))`, so erhalten wir

$$\begin{aligned} p(x) =& \frac{1}{3}x^{22} + \frac{1}{3}x^{18} + \frac{1}{3}x^{15} + \frac{1}{3}x^{14} - \frac{2}{3}x^{11} + \frac{1}{3}x^8 + \frac{1}{3}x^7 - \frac{2}{3}x^4 + \frac{1}{3} \\ t(x) =& -x^{11} - x^4 + 1 \\ r(x) =& x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1 \end{aligned}$$

Hierbei ist $r(x) = \Phi_{21}(x)$. Weiter überprüfen wir leicht, dass $r(x)|R(x) = p(x) - t(x) + 1$ gilt.
Um nun eine Kurve zu generieren, müssen wir ein x finden, für welches $p(x)$ und $r(x)$ prim sind bzw. $p(x)$ prim ist und $r(x)$ einen möglichst großen Primfaktor besitzt. Wir nutzen die erstellte Funktion `IsPolyPrime2(Pol1,Pol2,Schranke)`. Sie liefert ein x, für das beide Polynome Primzahlen sind. In unserem Beispiel ergibt sich ein x von 1979 und somit Werte von:

$$\begin{aligned} p(1979) =& 1108373714617236149727464501768276911876731770587712906470122419997462361 \\ t(1979) =& -18234914707372479691668887147099862590 \\ r(1979) =& 3606866129583640330015081813453865533321 \\ R(1979) =& 11083737146172361497274645017682769137002232413249608756370111347074486217 \end{aligned}$$

Auch hier überprüfen wir leicht, dass gilt: $4 \cdot p(1979) = (t(1979))^2 - (-3) \cdot y^2$ mit $y = 607830490245828578535587888856994739$. Indem wir den in KASH3 vorhandenen Befehl `EllipticCurve` mittels des Parameters $p(1979)$ ausführen, können wir wie in den vorangegangenen Beispielen eine Kurve und ihre Twists erzeugen:

$$\begin{aligned} E_1 &: y^2 = x^3 + 26493998342339389102601049472132634142452798595083009020403828511881065 \\ E_2 &: y^2 = x^3 + 489171418850157488092857285945619126298135162432921099723529842007874485 \\ E_3 &: y^2 = x^3 + 8919027928587256429384990234680897375960491933393584958207209365308340 6 \\ E_4 &: y^2 = x^3 + 7445876384358249158334319649821896898462660833654950069999213080695400 19 \\ E_5 &: y^2 = x^3 + 8324464355149707335770784726049724789871773442804252995777271564474118 \\ E_6 &: y^2 = x^3 + 4423034780018171894683132865391304123701851150790814949170384104511505 48 \end{aligned}$$

Mittels `IsSize` lässt sich herausfinden, dass E_3 der gesuchte Twist ist. Berechnen wir ρ, so ergibt sich $\rho \approx 1.82128$. Zwei weitere Beispiele finden sich in Teske [Tes07]. Dort ist auch erwähnt, dass für $D = -1$ (also eigentlich -4) und $D = -3$ am häufigsten Beispiele gefunden werden. Es gibt also einige Unterschiede zwischen dem Cocks-Pinch- und dem Brezing-Weng-Algorithmus. Letzterer liefert für große Fundamentaldiskriminanten seltener Lösungen, für kleine jedoch gleich eine Schar von Lösungen. Ein weiterer Unterschied hängt lediglich mit der Implementierung zusammen. Der Algorithmus ist so gebaut, dass keine Schleife durchlaufen wird, die ein $r(x)$ selbstständig sucht, sondern dass er mit „keine Lösung gefunden“ terminiert. Dies wurde so implementiert, da nicht klar ist, welches weitere $r(x)$ getestet werden soll.

Beispiel 6: Starten wir den Algorithmus 5 mit dem von Teske in [Tes07] erwähnten Parametern ($D = -1, k = 5, r = \Phi_{20}$) mittels des Befehls

```
BrezingWeng(-1,5,CyclotomicPolynomial(20))
```

verifizieren wir unseren Algorithmus; Er liefert die dort angegebene Kurvenschar. Starten wir ihn mit den anderen Parametern ($D = -3, k = 5, r = \Phi_{30}$), so erhalten wir folgende, dort nicht angegebene Kurvenschar:

$$\begin{aligned} p(x) =& \frac{1}{3}(x^{14} + x^{12} + x^{10} + x^9 - 2x^7 + x^5 + x^4 - 2x^2 + 1) \\ t(x) =& -x^7 - x^2 + 1 \\ r(x) =& x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \end{aligned}$$

Durch `IsPolyPrime(p)` finden wir eine erste Lösung $x = 22$, mit der $p(x)$ eine Primzahl wird. Es ergeben sich folgende Werte: $p(22) = 2078234679422516707$, $t(22) = -2494358371$ und $r(22) = 52386445651 = 61 \cdot 858794191$. Dabei gilt:

$$4 \cdot 2078234679422516707 = (-2494358371)^2 - (-3) \cdot 834888223^2$$

Wir berechnen die sechs Twists der Kurve und finden heraus, dass der Twist

$$E_5 : y^2 = x^3 + 940306857130849360$$

die Ordnung $R = p - 1 + t = 3 \cdot 13^4 \cdot 61 \cdot 463 \cdot 858794191$ hat. Wie wir sehen, tauchen beide Faktoren von r in R auf.

Weitere geeignete Startparameter sind $(D, k, r) = (-4, 6, \Phi_{12}), (-19, 5, \Phi_{95})$ und $(-23, 6, \Phi_{138})$. Dabei werden die Polynome jedoch deutlich komplizierter. Für die erste Kurvenschar finden wir mit $x = 36$ einen Wert, der für $p(x)$ und $r(x)$ gleichzeitig eine Primzahl liefert. Dies ist in den beiden weiteren Beispielen bis zu $x = 10000$ nicht gelungen. Für $x = 993$ respektive $x = 8$ ist zumindest $p(x)$ eine Primzahl, sodass tatsächlich eine Kurve konstruiert werden kann. Auch wenn für noch größere Werte von x beide Polynome tatsächlich Primzahlen liefern, sind diese irgendwann zu groß, um daraus geeignete Kurven zu

konstruieren. Für ein Polynom von Grad 100, kommen wir sehr schnell in diesen ungünstigen Bereich. So ist beispielsweise $10000^{100} \approx 10^{400} \approx 2^{1333}$ eine Größenordnung, die für p gerade noch vertretbar ist. Finden wir für $x \leq 10000$ keinen geeigneten Wert, sodass die Auswertung von $p(x)$ und $r(x)$ gleichzeitig prim ist, so müssten wir einen primen Teiler von $r(x)$ wählen. Dies hätte zur Folge, dass die maximale, prime r-Torsionsgruppe kleiner und damit gleichzeitig auch ρ größer als vermutet ist. Wir erhalten also keine Kurvenscharen mehr, die ähnliches, günstiges ρ besitzen. Dies ist sicherlich ein Nachteil der Brezing-Weng-Methode, welcher in der Literatur so nicht angesprochen wird. Der Algorithmus an sich liefert zwar Lösungen, diese sind aber weitestgehend unbrauchbar bzw. nicht besser als die Lösungen des Cocks-Pinch-Algorithmus.

7.4 Brezing-Weng-Produkt Beispiele

Der Übergang von Brezing-Weng-Algorithmus zum Brezing-Weng-Produkt-Algorithmus verläuft analog zum Übergang vom Cocks-Pinch-Algorithmus zum Cocks-Pinch-Produkt-Algorithmus mittels des chinesischen Restsatzes. Der Brezing-Weng-Produkt-Algorithmus wird demnach wieder benutzt, um Torsionsgruppen zu erzeugen, deren Ordnung 2 große Primteiler besitzt. Ein Problem tritt bei der Koeffizientenwahl von $r_1(x)$ und $r_2(x)$ auf. Die beiden Polynome müssen verschieden voneinander sein und beide einen Körper erzeugen, der sowohl eine k-te Einheitswurzel also auch eine Wurzel aus D enthält. Wie wir in 7.3 erwähnt haben, können wir dies durch ein Minimalpolynom eines beliebigen Elementes, das den Körper erzeugt, erreichen. Je größer dabei die Beträge der Zähler und der Nenner der Koeffizienten sind, desto eher erwarten wir, dass das resultierende Polynom $p(x)$ auch sehr große Zähler und Nenner besitzt. Dies erschwert die Aufgabe eine Zahl x zu finden, für die die Auswertung des Polynoms in $\mathbb{P}$ liegt. Daher geben wir in diesem Algorithmus standardmäßig als Polynom $r_1(x)$ das kleinste Kreisteilungspolynom vor, welches die notwendigen Bedingungen erfüllt. Darüber hinaus sucht der Algorithmus randomisiert ein Polynom $r_2(x)$ mit möglichst kleinen Absolutkoeffizienten (im Sinne von oben). Daher kommt es vor, dass der Algorithmus, der mittels `BrezingWengProduct(D,k)` (D = Fundamentaldiskriminante, k = Einbettungsgrad) aufgerufen wird, nicht immer dieselbe Lösung liefert.

Der Algorithmus ist so aufgebaut, dass er nicht nur irreduzible Polynome $p(x)$ sucht, sondern auch gleichzeitig überprüft, ob bis zu einer gewissen Schranke von x (hier $x \leq 2000$) die Auswertung des Polynoms eine Primzahl ist. Ohne diese Überprüfung liefert der Algorithmus eine Vielzahl von rationalen Polynomen. Diese eignen sich aber nicht dazu elliptische Kurven zu erzeugen.

Eine Schwierigkeit liegt bei dem Algorithmus darin, dass der benötigte Grad der Körpererweiterung, also der Grad von $r_1(x)$ und $r_2(x)$, für große k und D sehr schnell wächst und dadurch die Maximalordnung der Körpererweiterung in KASH3 nicht mehr bestimmt werden kann. KASH3 gibt als Fehlermeldung

einen MPQS-Fehler aus und der ganze Algorithmus bricht ab. Trotzdem sind für kleine D und k (also $|Dk| < 500$) Beispiele gefunden worden, zum Beispiel das folgende:

Beispiel 7: Starten wir den Algorithmus `BrezingWengProduct(D,k)` mit $D = -3$ und $k = 5$, so erhalten wir eine brauchbare Lösung:

$$\begin{aligned}
p(x) =& \frac{1}{12}\cdot x^{30} - \frac{1}{6}\cdot x^{29} + \frac{1}{6}\cdot x^{28} + \frac{1}{12}\cdot x^{27} - \frac{1}{12}\cdot x^{26} + \frac{1}{6}\cdot x^{24} - \frac{1}{4}\cdot x^{23} \\
& - \frac{1}{12}\cdot x^{20} - \frac{1}{6}\cdot x^{19} + \frac{7}{12}\cdot x^{18} + \frac{1}{12}\cdot x^{17} - \frac{1}{12}\cdot x^{16} - \frac{1}{2}\cdot x^{15} \\
& + \frac{1}{4}\cdot x^{14} - \frac{1}{4}\cdot x^{13} - \frac{1}{12}\cdot x^{12} - \frac{1}{12}\cdot x^{10} - \frac{1}{6}\cdot x^{9} + \frac{1}{6}\cdot x^{8} + \frac{1}{12}\cdot x^{7} \\
& - \frac{1}{6}\cdot x^{6} + \frac{1}{4}\cdot x^{4} + \frac{1}{4}\cdot x^{3} + \frac{1}{4} \\
t(x) =& -\frac{1}{2}\cdot x^{15} + \frac{1}{2}\cdot x^{14} - \frac{1}{2}\cdot x^{12} - \frac{1}{2}\cdot x^{6} + \frac{1}{2}\cdot x^{4} + \frac{1}{2}\cdot x^{3} + 1 \\
r_1(x) =& x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\
r_2(x) =& x^8 + x^7 - x^5 - x^4 - x^3 + x + 1
\end{aligned}$$

Auch hier stellen wir fest, dass $r_1(x)\cdot r_2(x) \mid R(x)$. Nun müssen wir ein x finden, für welches wir akzeptable Kurven erzeugen können. Die Wahrscheinlichkeit, dass wir ein x finden für das $p(x), r_1(x)$ und $r_2(x)$ gleichzeitig Primzahlen liefern, wurde in 4.6 abgeschätzt. Da sie sehr gering ist, erwarten wir nicht ein geeignetes x zu finden. Um zu überprüfen, ob trotzdem ein solches x existiert, benutzen wir die eigens implementierte Funktion `IsPolyPrime3(r1,r2,p,10^4)`. Bis zu $x = 10000$ existiert keine solche Lösung, daher reicht es für uns aus, dass $p(x)$ und $r_1(x)$ Primzahlen sind und $r_2(x)$ einen großen Primteiler besitzt. Für $x = 3501$ erhalten wir:

$$\begin{aligned}
p(3501) =& 176333155585316748278204939719932071428031282647684502940475611 \setminus \\
& 409561604398072327959563682200387917791179098917 \\
t(3501) =& -72732346558093047915334160754093840648212395401770999 \\
r_1(3501) =& 225638300365543536381715140 01 \\
r_2(3501) =& 225767236526658594463675140 01 \\
=& 1685581 \cdot 13394030694855874292821
\end{aligned}$$

Insgesamt ergibt sich:

$$\begin{aligned}
R =& 176333155585316748278204939719932071428031282647684502940475611 \setminus \\
& 969744598766212031777604103613018658086991 7 \\
=& 223 \cdot 1685581^2 \cdot 687534447671192179 \cdot 13394030694855874292821^2 \cdot \\
& 225638300365543536381715140 01
\end{aligned}$$

Hiermit können wir durch `EllipticCurve(p(3501),[0,a])` mit $a \in \mathbb{F}_p$ eine Kurve und anschließend mit `Twists` ihre Twists erzeugen. Wir erhalten:

$E_1 : y^2 = x^3 + 160716963338877879815923634712234840292138704659046392 \setminus$
$98807998925676046343768507212396051984786324118793 20$

$E_2 : y^2 = x^3 + 570377257011479646015116816346635482093500871575787609 \setminus$
$13477728195998954163830829738706092060213936583176 1$

$E_3 : y^2 = x^3 + 138193952973407733015131570350713835573220008842144079 \setminus$
$38558884054965172654040251650834859951514361228977 14$

$E_4 : y^2 = x^3 + 570377257011479646015116816346635482093500871575787609 \setminus$
$13477728195998954163830829738706092060213936583175 8$

$E_5 : y^2 = x^3 + 153810145219846601477412875358411066709112586830782182 \setminus$
$06474980745333107033551340075260811845905948901173 11$

$E_6 : y^2 = x^3 + 176333155585316748278204939719932071428031282647684495 \setminus$
$66724095616043980723279595636822003879177911790989 14$

Überprüfung mittels `IsSize(E_i,R)` liefert, dass E_1 die gesuchte Kurve ist. Dieses Beispiel zeigt die Funktionsfähigkeit des Algorithmus. Auch für andere Parameter (D und k) haben wir Lösungen gefunden. Diese Polynome besaßen aber sehr große Nenner sowie Zähler, sodass die Auswertung ihrer Stellen nicht in $\mathbb{N}$ lag. Zusätzlich traten für ein großes Produkt von Dk, auch Polynome $r_1(x)$ und $r_2(x)$ mit sehr großem Grad auf. Für Polynome ab Grad 500 dauert die Arithmetik unverhältnismäßig lange.

7.5 Hyperelliptische Kurven Beispiele

Wenden wir uns dem hyperelliptischen Fall zu. Hier haben wir den von Freeman in [Fre07b] eingeführten Algorithmus mit der Brezing-Weng-Methode kombiniert. Im Spezialfall mit $\text{Grad}_u = \text{Grad}_v = \text{Grad}_w = 0$, also dem Freeman-Fall, konnten die Lösungen, die in [Fre07b] beschrieben sind, erzielt werden. Bevor wir ein Beispiel des Freeman-Falls angeben, werden wir die grundlegende Funktionsweise des Algorithmus erläutern.

Zu Beginn müssen wir die Parameter der Kurve generieren und starten Algorithmus 9 mittels des Befehls `BWH(CMField,Grad,Koef,rho)`, wobei `CMField` ein Vektor mit zwei Komponenten ist, die angeben, welche CM-Körper untersucht werden sollen. (Auch hier sind die erstellten Funktionen im Anhang A zu finden.) Zur Verfügung stehen 13 verschiedene Möglichkeiten. Sie sind durch das Intervall von 1 bis 14 anzusprechen, d.h. $[4, 7]$ untersucht die CM-Körper aus Spalten 4,5 und 6. Weiter ist `Grad` ein Vektor mit drei Komponenten aus $\mathbb{N}$ und `Koef` ein Vektor mit sechs Komponenten aus $\mathbb{Z}$. Sie bestimmen die Erzeugung der Polynome $u(x), v(x)$ und $w(x)$. Die Variable `Grad`

gibt den Grad der Polynome $u(x), v(x)$ und $w(x)$ an, `Koef` gibt sowohl den minimal als auch den maximal auftretenden Koeffizienten an. So untersucht `Grad`$= [3, 3, 3]$, `Koef`$= [0, 3, 0, 3, 0, 3]$ zum Beispiel alle Polynome von Grad maximal 3, deren Koeffizienten zwischen -3 und 3 liegen. Der letzte Eingabeparameter ist der Sicherheitsparameter $\rho \in \mathbb{R}$. Ihn können wir nutzen, um im Freeman-Fall Kurven zu eliminieren, die nicht paarungsgeeignet sind. Mit $\rho = 0$ schließen wir alle ganzzahligen Lösungen aus und lassen nur echte Polynome zu. Als Lösung des Algorithmus erhalten wir $r(x)$ und die Polynome $q(x), s(x)$ und $t(x)$, mittels welcher wir die definierende Gleichung der Kurve zurückgewinnen können, siehe Gleichung (5.1). Letzteres muss die Ordnung der Jakobischen $|J(C)(x)| = (q(x)^2 + 1 - s(x)) \cdot (q(x) + 1) + t(x))$ teilen. Falls wir uns im Freeman-Fall befinden, sind die Polynome aus $\mathbb{Z}$, im anderen Fall müssen wir wie im Brezing-Weng-Algorithmus eine Zahl x ermitteln, für welche $q(x)$ eine Primzahl ist. Dazu verwenden wir die erstellte Funktion `IsPolyPrime(q)`. Danach berechnen wir mit dem erhaltenen x die Zahlen $s(x), t(x), r(x), J(C)(x) \in \mathbb{Z}$.

Da der gewählte CM-Körper aus [Wam99] stammt und für diese Körper dort direkt definierende Gleichungen angegeben sind, brauchen wir keine Igusa-Invarianten zu bestimmten, sondern können die Gleichung einfach übernehmen. Mittels der CM-Körper überprüfen wir, ob die Jakobische der hyperelliptischen Kurve tatsächlich die gewünschte Ordnung besitzt. Dazu erzeugen wir einen beliebigen Divisor von Grad 0, indem wir zum Beispiel zwei Stellen von Grad 1 voneinander abziehen. Danach multiplizieren wir diesen Divisor mit $|J(C)(x)| \in \mathbb{Z}$ und überprüfen, ob das Ergebnis ein Hauptdivisor ist. Genau wie im elliptischen Fall müssen wir noch die quadratischen Twists der Kurve überprüfen - lediglich für den Körper $\mathbb{Q}(\zeta_5)$ existieren fünf Twists. Liefert ein Test keinen Hauptdivisor, so verwerfen wir die Kurve. Ist er ein Hauptdivisor, können wir jedoch, wie bereits in 6.3 erläutert, nicht sicher schließen, dass die Kurve die richtige Ordnung hat.

Zur Illustration führen wir ein Beispiel aus dem Freeman-Fall vor.

Beispiel 8: Wir starten den Algorithmus mit `BWH(CMField,Grad,Koef,rho)` wobei wir `CMField`$= [2, 3]$, `Grad`$= [0, 0, 0]$, `Koef`$= [0, 100, 0, 100, 0, 100]$ und $\rho = 2,5$ wählen. Dies liefert folgende Werte:

$s = 796$	$t = 262374$	$q = 53281$
$a = 2$	$b = 1$	$d = 2$
$r = 22247$	$\rho = 2.1745$	

Da s, t und q keine Polynome sind, muss `IsPolyPrime(q)` nicht angewendet werden. Die Ordnung der Jakobischen ergibt sich zu:

$$|J(C)(\mathbb{F}_{53281})| = (q^2 + 1 - s * (q + 1) + t) = 2796714864 = 2^4 \cdot 3^4 \cdot 97 \cdot 22247;$$

Anhand [Wam99] Tabelle 1, erhalten wir die Kurvengleichung:

$$C_1 \colon y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$$

Dazu konstruieren wir einen Funktionenkörper und wählen einen Divisor von Grad 0 aus, der kein Hauptdivisor ist. Diesen multiplizieren wir mit der Ordnung der Jakobischen. Da das Resultat kein Hauptdivisor ist, berechnen wir den quadratischen Twist. Hierfür wählen wir eine natürliche Zahl l, die einen nicht quadratischen Rest modulo q, also $\left(\frac{l}{q}\right) = -1$, besitzt. Wir multiplizieren alle x-Monome mit diesem l und erhalten die getwistete Kurve. Auch ihre Ordnung überprüfen wir. In KASH3 wurde dies für diese Arbeite implementiert durch die Funktion `Check_BWH(q,s,t,r,CMField)`. In unserem Fall ist der Twist der Kurve die gesuchte Lösung:

$$C_2 \colon y^2 = 11x^5 - 33x^4 - 22x^3 + 66x^2 + 33x + 11$$

Die Kurve ist zwar zu klein, um für die Kryptografie geeignet zu sein, besitzt aber ein ρ, das wesentlich kleiner ist als 8. Die von Freeman gefundenen Kurven besaßen alle ein ρ, welches stets größer als 8 war. Aufgrund dieser Tatsache ist davon auszugehen, dass auch hyperelliptische Kurven kryptografisch relevanter Größenordnung mit kleineren Sicherheitsparametern existieren.

Für Lösungen, die nicht dem Freeman-Fall entsprechen, müssen wir zuerst ein x finden, für das $q(x)$ prim ist. Danach können wir analog dem eben beschriebenen Fall vorgehen, um die richtige Kurve zu ermitteln. Dies wird im nächsten Abschnitt verdeutlicht.

7.6 Hyperelliptische Kurven und Brezing-Weng

Für die Suche nach hyperelliptischen Kurvenscharen, wurden alle 13 in [Wam99] vorgestellten CM-Körper überprüft. Hierbei wurden (a, b, d) so normiert wurde, dass b ungerade war. Dazu wurde der Algorithmus 9 in KASH3 mit der für diese Arbeit erstellten Routine `BWH([1,14],[2,2,2],[0,2,0,2,0,2],0)` gestartet. Es wurden insgesamt ca. 500.000 Berechnungen in jedem CM-Körper durchgeführt. Eine Berechnung bedeutet hier das berechnen des größten gemeinsamen Teiles eines nach 6.7 erzeugten Polynoms mit allen Kreisteilungspolynomen $\Phi_k(q(x))$ bis zu Grad 50. Die Berechnung alle 50 Teiler zusammen kann auf einem Standard-PC in ca. einer Sekunde ausgeführt werden, so dass die Laufzeit $500.000 \cdot 13\,\text{sec} \approx 70$ entspricht. Um dies zu ermöglichen, wurde das Programm parallelisiert, um es auf einem $2,4\,\text{GHz}$ AMD-Opteron Cluster mit $1\,\text{GByte}$ Hauptspeicher auf 30 Nodes gleichzeitig laufen zu lassen. Die gewonnene Geschwindigkeitsverbesserung lag dabei in der Größenordnung von $50 - 100$. Die Berechnungen dauerten ca. 24 Stunden auf 30 parallel arbeitenden Clustern.

Um den Algorithmus zu beschleunigen, wurden redundante Aufrufe eliminiert, so liefern (u, v, w) und $(u, v, -w)$ aufgrund des ausschließlich quadratischen Auftretens von w dieselben Lösungen. Ebenso liefern (u, v, w) und $(-u, -v, w)$ sowie $(u, -v, w)$ und $(-u, v, w)$, siehe Gleichungen (6.1) bis (6.3), dieselben Ergebnisse. Daher wurden alle Kombinationen für (u, v, w) mit negativen Leitkoeffizienten der Polynome w und v ausgeschlossen. Es ist also nur notwendig, Lösungen zu überprüfen, bei denen die Polynome v und w einen positiven Leitkoeffizienten besitzen. So reduzierten sich die oben angegebenen Berechnungen von $13 \cdot 5^9$ um ein viertel auf $13 \cdot 500.000$.

Aufgrund der angewendeten Brute-Force-Methode, konnte auch nur ein kleiner Teil der CM-Körper überprüft werden. Zwar liefern die Parameter (a, b, d) und $(a, b/2^l, 4^l d)$ isomorphe CM-Körper, für den Algorithmus bedeuteten sie aber unterschiedliche Lösungen. Daher haben wir uns auf solche Parameterkombinationen beschränkt, deren b ungerade war.

Leider wurden trotz intensiver Suche keine Beispiele gefunden. Die lange Laufzeit des Algorithmus ist darin begründet, dass für Polynome ein größter gemeinsamer Teiler gesucht werden muss. Dies ist für Polynome höheren Grades nur geringfügig zu beschleunigen. Dem wurde versucht durch größere Rechenleistung entgegenzuwirken. Eine notwendige Ausweitung der Suchparameter war aus zeitlichen Gründen leider nicht mehr möglich.

7.7 Zusammenfassung und Ausblick

Alle vier Algorithmen für elliptische Kurven funktionieren wie gewünscht. Die Cocks-Pinch-Algorithmen liefern r-Torsionsgruppen mit ein oder zwei großen Primteilern gleicher Größenordnung. Dies ist ohne Schwierigkeiten auf eine größere Anzahl von Torsionsgruppen erweiterbar. Auch die Brezing-Weng-Algorithmen liefern das Versprochene, und zwar Polynome, die paarungsgeeignete Kurvenscharen darstellen. Dennoch sind sie dem Cocks-Pinch-Algorithmus nicht vorzuziehen. Für Werte der Eingabeparameter D und k ab einer Größenordnung von 500 benötigen beide Brezing-Weng-Algorithmen mehr als 24 Stunden, um Lösungen zu finden. Ein weiterer Nachteil ist, dass wir aus den gewonnenen Kurvenscharen durch Auswertung der Polynome Parameter aus $\mathbb{Z}$ erzeugen müssen, welche wir dann erst nutzen können, um Kurven zu konstruieren. Irreduzible Polynome, deren Auswertung zwei teilerfremde ganze Zahlen liefert, stellen Primzahlen dar, dies sagt aber nichts über die Größenordnung dieser Primzahlen aus. Je größer der Grad der Polynome, desto unwahrscheinlicher ist es, dass ihre Auswertung für $x \in \mathbb{N}$ Lösungen für eine vorgegebene kryptografische Größenordnung liefert.

Sollte der Algorithmus für hyperelliptische Kurven von Geschlecht 2 Polynomlösungen finden, so sind diese zuerst noch auszuwerten, also Lösungen aus $\mathbb{Z}$ zu finden. Dabei werden für Polynome großen Grades dieselben Probleme wie

bei den Polynomlösungen im Brezing-Weng-Algorithmus auftreten. Daher sollen eventuelle Lösungen dahingehend eingeschränkt werden, dass die Polynome $q(x)$ einen Grad kleiner als 100 besitzen. Obwohl wir nach extensiver Suche keine Lösungen gefunden haben, halten wir es für angebracht sich nicht im Voraus auf ein bestimmtes $r(x)$ einzuschränken, für das wir Lösungen suchen. Um den Algorithmus weiter zu beschleunigen, könnte es vorteilhaft sein, sich auf einen Einbettungsgrad festzulegen, und somit die Struktur des Kreisteilungspolynoms Φ_k besser ausnutzen zu können.

Auch die Ausweitung der Erzeugung von gewöhnlichen Kurven von Geschlecht 3 wäre ein mögliches Forschungsgebiet. Dies birgt natürlich als Komplikation, dass die benötigten CM-Körper Grad 6 Erweiterungen sind, die von von Polynome von Grad 6 erzeugt werden, für Polynome von Grad 6 aber keine geschlossene Lösungsformel existiert.

Anhang A

Dokumentation der verwendeten KASH3 - Funktionen

Die folgenden Funktionen sind Zusätze für das Programm KASH3, welches von der Webseite `http://www.math.tu-berlin.de/~kant/kash.html` herunter geladen werden können.

Zusätzlich wurden für diese Arbeit einige KASH3-Funktionen verwendet, die von Anita Krahmann erstellt wurden. Zusammen mit den für diese Arbeit erstellten Algorithmen sind sie unter: `http://www.patrick-schweitzer.de` zu erhalten. Abschließend folgt eine Auflistung der wichtigsten im Rahmen dieser Arbeit erstellten Funktionen samt Input und Output Parameter:

- `BrezingWeng(D,k,r0)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad, r_0 = Polynom, welches den CM-Körper generiert, indem sowohl $\sqrt{D}$ als auch die k-te Einheitswurzel liegen.

Ausgabe: Polynome $r(x), p(x)$ und $t(x)$, welche die Torsionsgruppenordnung, die Anzahl der Elemente der endlichen Körper als auch die Spur der Frobenius-Endomorphismen darstellen.

$r(x)$ kann sowohl mit `CyclotomicPolynomial`, mit `Poly_Dk` als auch mit `Zufallspoly_Dk` erzeugt werden. Danach muss mit `IsPolySize` oder auch `IsPolySize2` ein x gesucht werden, für das $p(x)$ und bestenfalls auch $r(x)$ prim sind, damit daraus dann die Kurve mittels `Weber_to_Hilbert` und `EllipticCurveFromJInvariatnWithZero` erzeugt werden kann.

- `BrezingWengProduct(D,k)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad.

Ausgabe: Polynome $r_1(x), r_2(x), p(x)$ und $t(x)$, welche die Torsionsgruppenordnung, die Anzahl der Elemente der endlichen Körper als auch die Spur der Frobenius-Endomorphismen darstellen.

Hier wurde auf die Eingabe der Parameter $r_1(x)$ und $r_2(x)$ verzichtet, da diese sehr selten die notwendigen Anforderungen erfüllen. Der Algorithmus wählt $r_1(x)$ als das passende Kreisteilungspolynom niedrigsten Grades und sucht dann ein zweites Polynom mit möglichst kleinen Absolutkoeffizienten.

- `BWH(CMField,Grad,Koef,rho)`

Eingabe: `CMField`= welcher CM-Körper überprüft werden soll, `Grad`= Grad der Parameter u, v und w im Algorithmus, `Koef` = Bestimmt u, v und w des Algorithmus näher, ρ = maximaler Sicherheitsparameter.

Ausgabe: Liste mit Einträgen: p = Anzahl der Elemente über dem die hyperelliptische Kurve definiert ist, Parameter s und Parameter t des Frobenius, Parameter a, Parameter b und Parameter d des CM-Körpers, Torsionsgruppenordnung r, Sicherheitsparameter ρ.

`Grad = [0,0,0]` erzeugt ausschließlich den Freeman-Fall.

- `Check_BWH(p,s,t,r,i)`

Eingabe: p = Anzahl der Elemente über dem die hyperelliptische Kurve definiert ist, (s, t) = Als Parameter des Frobenius-Endomorphismus, r = Torsionsgruppenordnung, i = gibt den gewählten CM-Körper an.

Ausgabe: Boolesche Variable, die besagt, ob hyperelliptische Kurve wirklich eine Ordnung hat, welche von der Torsionsgruppenordnung geteilt wird. Falls ja, wird zusätzlich die Gleichung der hyperelliptischen Kurve ausgegeben.

- `CocksPinch(D,k,r0)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad, r_0 = Startparameter für Torsionsgruppenordnung.

Ausgabe: r = Torsionsgruppenordnung, p = Anzahl der Elemente des endlichen Körpers über dem die Kurve definiert ist, t = Spur des Frobenius.

Die Erzeugung der Kurve erfolgt dann mittels `Weber_to_Hilbert` und `EllipticCurvefromJInvariant`.

- `CocksPinchProduct(D,k,r0)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad, r_0 = Startparameter für Torsionsgruppenordnung.

Ausgabe: r_1 = Teiler der Ordnung der Kurve, r_2 = Teiler der Ordnung der Kurve, p = Anzahl der Elemente des endlichen Körpers über dem die Kurve definiert ist, t = Spur des Frobenius.

Die Erzeugung der Kurve erfolgt dann mittels `Weber_to_Hilbert` und `EllipticCurvefromJInvariant`.

- `CP_Kurve(D,k,r0)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad, r_0 = Startparameter für Torsionsgruppenordnung.

Ausgabe: Korrekte elliptische Kurve, deren größte prime Torsionsgruppe die Größenordnung von r_0 besitzt.

- `EllipticCurve(p, [a,b])`

Eingabe: p = Anzahl der Elemente des endlichen Körpers über dem die Kurve definiert ist, `[a,b]`= Koeffizienten a_4 und a_6 in der kurzen Weierstraß-Normalform.

Ausgabe: Elliptische Kurve über $\mathbb{F}_p$.

- `EllipticCurveFromJInvariantWithZero(j)`

Eingabe: j = j-Invariante als Element aus dem Körper $\mathbb{F}_p$.

Ausgabe: Elliptische Kurve über $\mathbb{F}_p$.

- `IsPolyPrime(p,i)`

Eingabe: p = Polynom über $\mathbb{C}$, i = natürliche Zahl.

Ausgabe: Boolesche Variable sowie x. Entweder `[FALSE,0]`, falls $p(x)$ für alle $x \leq i$ nicht prim, sonst `[TRUE,x]` mit $p(x) \in \mathbb{P}$.

- `IsPolyPrime2(p1,p2,i)`

Eingabe: p_1, p_2 = Polynome über $\mathbb{C}$, i = natürliche Zahl.

Ausgabe: Boolesche Variable sowie x. Entweder `[FALSE,0]`, falls $p_1(x)$ und $p_2(x)$ für alle $x \leq i$ nicht gleichzeitig prim, sonst `[TRUE,x]` mit $p_1(x)$ und $p_2(x) \in \mathbb{P}$.

- `IsPolyPrime3(p1,p2,p3,i)`

Eingabe: p_1, p_2, p_3 = Polynome über $\mathbb{C}$, i = natürliche Zahl.

Ausgabe: Boolesche Variable sowie x. Entweder `[FALSE,0]`, falls $p_1(x), p_2(x)$ und $p_3(x)$ für alle $x \leq i$ nicht gleichzeitig prim, sonst `[TRUE,x]` mit $p_1(x), p_2(x)$ und $p_3(x) \in \mathbb{P}$.

- `IsSize(Elk,Order)`

Eingabe: `Elk`= elliptische Kurve in Kurzer Weierstraß-Normalform. Vermutete Ordnung der Kurve.

Ausgabe: Boolesche Variable, ob Vermutung wahr oder falsch.

- `Poly_Dk(D,k)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad.

Ausgabe: Minimalpolynom des Zahlkörpers, welcher durch die Adjunktion der Nullstellen von $x^2 - D$ und der k-ten Einheitswurzeln entstanden ist.

Wird in der Eingabe von `BrezingWeng` verwendet.

- `Twists(Elk)`

Eingabe: `Elk`= elliptische Kurve in Kurzer Weierstraß-Normalform.

Ausgabe: Alle Twists der Kurve.

Hinweis: Die erste Kurve der Liste ist nicht unbedingt die eingegebene Kurve.

- `Weber_to_Hilbert(D,p)`

Eingabe: D = negative Fundamentaldiskriminante, p = Anzahl der Elemente des endlichen Körpers über dem die Kurve definiert ist.

Ausgabe: j-Invariante über $\mathbb{F}_p$.

Hinweis: Die Datei KP.txt muss in demselben Verzeichnis wie die Code-Datei liegen. Außerdem ist diese Funktion besonders anfällig in Bezug auf falsche Parametereingaben.

- `Zufallspoly_Dk(D,k)`

Eingabe: D = negative Fundamentaldiskriminante, k = Einbettungsgrad.

Ausgabe: Minimalpolynom eines Zahlkörpers, der zu dem Zahlkörper isomorph ist, der durch die Adjunktion der Nullstellen von $x^2 - D$ und der k-ten Einheitswurzeln entstanden ist. Die Koeffizienten des Minimalpolynoms werden so gewählt, dass die Summe der Absolutbeträge von Zähler und Nenner möglichst minimal ist. Die Schleife wird 200 Mal durchlaufen und dann das Polynom mit den kleinsten Werten ausgesucht.

Wird in der Eingabe von `BrezingWeng` verwendet.

Stichwortverzeichnis

Algorithmustabelle

Literaturverzeichnis

[ACD+06] Roberto M. Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC, 2006.

[AM93] Arthur O.L. Atkin and François Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), no. 203, 29–68.

[Ber06] Daniel J. Bernstein, *Elliptic vs. hyperelliptic, part 1*, talk at ECC 2006, Toronto, Canada, 20 September 2006, 2006, `http://cr.yp.to/talks/2006.09.20/slides.pdf`.

[BGhS07] Paulo S. Barreto, Steven D. Galbraith, Colm Ó hÉigeartaigh, and Michael Scott, *Efficient pairing computation on supersingular Abelian varieties*, Designs, Codes and Cryptography **42** (2007), no. 3, 239–271.

[BKLS02] Paulo S.L.M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott, *Efficient algorithms for pairing-based cryptosystems*, Cryptology ePrint Archive, Report 2002/008, 2002, `http://eprint.iacr.org/`.

[BN05] Paulo S.L.M. Barreto and Michael Naehrig, *Pairing-friendly elliptic curves of prime order*, Cryptology ePrint Archive, Report 2005/133, 2005, `http://eprint.iacr.org/`.

[Bos06] Siegfried Bosch, *Algebra*, sixth ed., Berlin: Springer, 2006.

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart (eds.), *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series 317. Cambridge: Cambridge University Press, 2005.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138. Berlin: Springer, 1993.

[CP01] Clifford Cocks and Richard G.E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript, 2001.

[Del74] Pierre Deligne, *La conjecture de Weil I*, Institut des Hautes Études Scientifiques Publications Mathématiques **43** (1974), 273–307.

[DL03] Iwan Duursma and Hyang-Sook Lee, *Tate-pairing implementations for tripartite key agreement*, Cryptology ePrint Archive, Report 2003/053, 2003, `http://eprint.iacr.org/`.

[EL04] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, ArXiv Mathematics e-prints: math/0405305, 2004, `http://arxiv.org/abs/math/0405305`.

[ELM03] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery, *Improved Weil and Tate pairings for elliptic and hyperelliptic curves*, ArXiv Mathematics e-prints: math/0311391, 2003, `http://arxiv.org/abs/math/0311391`.

[FR94] Gerhard Frey and Hans-Georg Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation **62** (1994), no. 206, 865–874.

[Fre07a] David Freeman, *Constructing pairing-friendly elliptic curves for cryptography*, Unpublished Talk, 2007, `http://math.berkeley.edu/~dfreeman/papers/kias2.pdf`.

[Fre07b] ———, *Constructing pairing-friendly genus 2 curves over prime fields with ordinary jacobians*, Cryptology ePrint Archive, Report 2007/057, 2007, `http://eprint.iacr.org/`.

[Fri08] Anika Frischwasser, *Diplomarbeit*, To appear, Lehrstuhl für Algebra und Zahlentheorie, TU Berlin, 2008.

[FST06] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive, Report 2006/372, 2006, `http://eprint.iacr.org/`.

[GHO+07] Robert Granger, Florian Hess, Roger Oyono, Nicolas Thériault, and Frederik Vercauteren, *Ate Pairing on Hyperelliptic Curves*, Advances in Cryptology - EUROCRYPT 2007, LNCS 4515, Springer, May 2007, pp. 430–447.

[GHV07] Steven D. Galbraith, Florian Hess, and Frederik Vercauteren, *Hyperelliptic pairings*, To Appear in Pairings 2007, 2007.

[GO85] A. Greaves and Robert Winston Keith Odoni, *Weil numbers and CM-fields*, Journal für die reine und angewandte Mathematik **391** (1985), no. 7, 198–212.

[Har97] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, 56. New York, NY: Springer, April 1997.

[Hes06] Florian Hess, *Dedekindringe in Funktionenkörpern*, Vorlesungsskript SS2006, 2006, `http://www.math.tu-berlin.de/~hess/algcurves/dedekind.pdf`.

[Hir64] Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero: I*, The Annals of Mathematics **79** (1964), no. 2, 109–203.

[Hit06] Laura Hitt, *On the minimal embedding field*, Cryptology ePrint Archive, Report 2006/415, 2006, `http://eprint.iacr.org/`.

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Transactions of the American Mathematical Society **347** (1995), no. 7, 2361–2401.

[HSV06] Florian Hess, Nigel P. Smart, and Frederick Vercauteren, *The Eta Pairing revisited*, Cryptology ePrint Archive, Report 2006/110, 2006, `http://eprint.iacr.org/`.

[Hul00] Klaus Hulek, *Elementare Algebraische Geometrie*, Vieweg, 2000.

[Hus04] Dale Husemöller, *Elliptic curves. With appendices by Otto Forster, Ruth Lawrence, and Stefan Theisen*, second ed., Graduate Texts in Mathematics, 111. New York, NY: Springer, 2004.

[Igu60] Jun-Ichi Igusa, *Arithmetic variety of moduli for genus two*, The Annals of Mathematics **72** (1960), no. 3, 612–649.

[Kob87] Neal Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203–209.

[Kob89] ———, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), no. 3, 139–150.

[Kob98] ———, *Algebraic aspects of cryptography. With an appendix on Hyperelliptic curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato*, Algorithms and Computation in Mathematics. Vol. 3. Berlin: Springer, 1998.

[KW89] Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, The American Mathematical Monthly **96** (1989), no. 2, 133–137.

[Lan87] Serge Lang, *Elliptic functions*, Graduate Texts in Mathematics, 112. New York, NY: Springer, 1987.

[Lan06] Tanja Lange, *Elliptic vs. hyperelliptic, part 2*, talk at ECC 2006, Toronto, Canada, 20 September 2006, 2006, `http://www.hyperelliptic.org/tanja/vortraege/ECC_06.ps`.

[Lan07] ———, *Elliptic vs. hyperelliptic, part 3 - elliptic strikes back*, talk at Eurocrypt 07 Rump Session, Barcelona, Spain, 22 May 2007, 2007, `http://www.hyperelliptic.org/tanja/vortraege/EC_vs_HEC_III.ps`.

[Mes91] Jean-François Mestre, *Construction des courbes de genre 2 à partir de leurs modules*, Progress in Mathematics **94** (1991), 313–334.

[Mil86a] Victor S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology, Crypto 85, LNCS 218, vol. 218, Berlin: Springer, August 1986, pp. 417–426.

[Mil86b] James S. Milne, *Abelian varieties*, Proceedings of Conference on Arithmetic Geometry, Storrs, August 1984 (Gary Cornell and Joseph H. Silvermann, eds.), New York,NY: Springer, 1986, pp. 103–150.

[MKHO07] Seiichi Matsuda, Naoki Kanayama, Florian Hess, and Eiji Okamoto, *Optimised versions of the ate and twisted ate pairings*, Cryptology ePrint Archive, Report 2007/013, 2007, `http://eprint.iacr.org/`.

[MN02] Daniel Maisner and Enric Nart, *Abelian surfaces over finite fields as Jacobians. With an appendix by Everett W. Howe*, Experimental Mathematics **11** (2002), no. 3, 321–337, `http://www.expmath.org/expmath/volumes/11/11.html`.

[MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, In IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **84a** (2001), no. 5, 1234 – 1243, `citeseer.ist.psu.edu/miyaji01new.html`.

[MOV93] Alfred Menezes, Tatsuaki Okamoto, and Scott A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), no. 5, 1639–1646.

[Mum74] David Mumford, *Abelian Varieties*, second ed., Oxford University Press, 1974.

[Nag07] Koh-ichi Nagao, *Index calculus attack for jacobian of hyperelliptic curves of small genus using two large primes*, Japan Journal of Industrial and Applied Mathematics **24** (2007), no. 3, 289–305.

[Odo91] Robert W. K. Odoni, *Weil numbers and CM fields, II*, Journal of Number Theory **38** (1991), 366–377.

[Oor03] Frans Oort, *Abelian varieties over finite fields*, 2003, `http://www.cirm.univ-mrs.fr/videos/2005/exposes/07/Oort.pdf`.

[RS02] Karl Rubin and Alice Silverberg, *Supersingular abelian varieties in cryptology*, CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, Springer, 2002, pp. 336–353.

[RS07] ———, *Using abelian varieties to improve pairing-based cryptography*, 2007, `http://www.math.uci.edu/asilverb/bibliography/`.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106. New York, NY: Springer, 1986.

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Berlin: Springer, 1993.

[Tat68] John Tate, *Classes d'isogénie des variétés Abéliennes sur un corps fini (d'après Taira Honda)*, Séminaire Bourbaki **352** (1968), 95–110.

[Tes07] Edlyn E. Teske, *Pairing-friendly elliptic curves for cryptography*, talk at AMS Sectional Meeting, Hoboken, NJ, 15 April 2007, Unpublished slides, 2007.

[Thé03] Nicolas Thériault, *Index Calculus Attack for Hyperelliptic Curves of Small Genus*, Advances in Cryptology - ASIACRYPT 2003, LNCS 2894, Berlin: Springer, 2003, pp. 75–92.

[Wam99] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Mathematics of Computation **68** (1999), no. 225, 307–320.

[Wei57] André Weil, *Zum Beweis des Torellischen Satzes*, Nachrichten der Akademie der Wissenschaften in Göttingen **2** (1957), 33–53.

[Wen03] Annegret Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Mathematics of Computation **72** (2003), no. 241, 435–458.