Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation

Dissertation
zur Erlangung des Grades
eines Doktors der Naturwissenschaften

dem Fachbereich 6 (Mathematik und Informatik)
der Universität GH Essen
vorgelegt von

Annegret Weng
aus Hanau

Essen, den 28. Mai 2001

Ich habe diese Arbeit selbständig verfasst und dabei keine anderen als die angegebenen Hilfsmittel benutzt.

Annegret Weng
Essen, Mai 2001

„ ... Dewegen brüten wir immerzu über neuen Beweisen. Ein ewiges Grübeln und Bohren und Tüfteln ist das. Doch wenn uns dann endlich ein Licht aufgeht - [...] -, na, dann freuen wir uns natürlich wie die Schneekönige. Dann sind wir glücklich. “

Aus dem *Zahlenteufel*
von Hans Magnus Enzensberger

Danksagungen

Mein besonderer Dank gebührt meinem Doktorvater, Herrn Prof. Dr. Dr. h.c. Frey. Seine Unterstützung, sein Rat und seine zahlreichen Vorschläge waren für mich entscheidend und von unschätzbarem Wert. Für meine Fragen hatte er immer ein offenes Ohr. Ich konnte in seiner Arbeitsgruppe unter optimalen Bedingungen arbeiten: mit einem interessanten Thema, guter Betreuung und einer angenehmen Arbeitsatmosphäre.
Beim Center for Applied Cryptography an der University of Waterloo bedanke ich mich für die Gastfreundschaft während meines dreimonatigen Forschungsaufenthaltes von Mai bis August 2000. Die dort entstandenen Kontakte sowie das Interesse an meiner Arbeit gaben mir weitere Anstöße für meine Forschung.
Nicht vergessen seien auch (in alphabetischer Reihenfolge) Dr. Galbraith, Prof. Okazaki, Prof. Menezes, Dipl. math. Müller, Prof. Rück und Prof. Stein für fruchtbare Anregungen und Korrekturvorschläge.
Weiter möchte ich besonders auch Kim Nguyen danken, der in diesen zwei Jahren mit mir das Zimmer teilte. Wir führten in dieser Zeit viele mathematische Diskussionen.
Ohne die finanzielle Unterstützung durch den Forschungsverbund „NRW Datensicherheit“ und das Graduiertenkolleg „Mathematische und ingenieurwissenschaftliche Methoden der Datenverarbeitung“ wäre diese Promotion nicht möglich gewesen.
Mein Dank richtet sich auch an meine Eltern und meiner Oma, die mich mein ganzes Leben lang unterstützt haben und denen diese Dissertation gewidmet ist. Mein letzter Dank gilt Andreas für seine unendliche Geduld mit mir.

Inhaltsverzeichnis

Kapitel 0

Einleitung

Motivation

Um den deterministischen Primzahltest von Goldwasser-Kilian praktikabel zu machen, schlug Atkin [1] 1986 ein Konstruktionsverfahren für elliptische Kurven über endlichen Primkörpern vor. Der Algorithmus (unter dem Namen „CM-Methode“ bekannt) basiert auf der Theorie der komplexen Multiplikation auf elliptischen Kurven. Er findet zu einer gegebenen imaginär quadratischen Ordnung $\mathcal{O}$ und einer Primzahl p eine über $\mathbb{F}_p$ definierte elliptische Kurve E, deren Endomorphismenring zu $\mathcal{O}$ isomorph ist. Die Gruppenordnung $\#E(\mathbb{F}_p)$ hängt dann nur von p und $\mathcal{O}$ ab und läßt sich einfach und schnell berechnen.
Die Komplexität der CM-Methode wird dabei von der Klassenzahl $h(\mathcal{O})$ und der Diskriminante der Ordnung $\mathcal{O}$ bestimmt. Atkin und Morain [2] erweiterten die Idee im folgenden zu einem sehr effizienten Algorithmus. Nach heutigem Stand lassen sich Kurven mit Klassenzahl um 200 in einigen Sekunden erzeugen. Der rechenaufwendigste Teil, die Bestimmung des Klassenpolynoms, kann vorberechnet und in einer Datei abgespeichert werden.
Eine weitere Anwendung neben Primzahltests besteht in der Erzeugung kryptographisch geeigneter Kurven [55]. Um die Sicherheit von Kryptosystemen, die auf dem diskreten Logarithmus basieren, zu gewährleisten, müssen wir wissen, daß die Ordnung der zugrundeliegenden Gruppe einen großen Primfaktor enthält [40]. Deshalb müssen wir die Gruppenordnung ermitteln.
Die Bestimmung der Anzahl $\mathbb{F}_p$-rationaler Punkte einer elliptischen Kurve ist ein nichttriviales Problem. Mittlerweile gibt es einen effizienten Algorithmus von Schoof, Atkin, Elkies u.a. zur Berechnung der Punktanzahl einer elliptischen Kurve (für einen Übersichtsartikel siehe z.B. [45]). Trotzdem ist die CM-Methode noch attraktiv, da sie den Vorteil hat, daß wir bei geeigneter Wahl von $\mathcal{O}$ und p stets eine Kurve mit kryptographisch guter Gruppenordnung konstruieren. Bei Punktezählalgorithmen sind in der Regel einige Kurven abzuzählen, bevor wir eine Gruppe von fast primer Ordnung erhalten.
Nicht-supersinguläre Kurven mit einem Endomorphismenring kleiner Klassenzahl sind nach heutigem Stand genauso sicher wie zufällig gewählte Kurven. Es ist kein Algorithmus bekannt, der die besonderen Eigenschaften ausnutzt, um das diskrete Logarithmusproblem auf diesen Kurven schneller zu lösen (siehe auch [63]).

Koblitz [24] schlug 1989 die Verwendung von Jacobi-Varietäten hyperelliptischer Kurven in der Kryptographie vor. Mit der Erweiterung auf höhere Geschlechter steht eine größere Auswahl von Kurven zu Verfügung. Weiter kann der zugrundeliegende Körper $\mathbb{F}_q$ kleiner gewählt werden, da die Jacobi-Varietät einer Kurve vom Geschlecht g etwa q^g $\mathbb{F}_q$-rationale Punkte hat.
Für sorgfältig gewählte Kurven von kleinem Geschlecht ($1 \leq g \leq 3$) sind bis heute keine Algorithmen bekannt, deren Laufzeit die der generischen Algorithmen schlägt. Die besten bekannten generischen Algorithmen (etwa Baby-Step-Giant-Step oder Pollard-Cangeroo) haben eine Laufzeit von $O(\sqrt{l})$ wobei l der größte Primfaktor der Gruppenordnung ist. Aus der heute möglichen Rechenleistung ergibt sich damit, daß der größte Primfaktor mindestens 2^{160} Bits lang sein sollte.
Die Bestimmung der Gruppenordnung hyperelliptischer Kurven ist noch schwerer als im elliptischen Fall. Bisher ist kein Algorithmus bekannt, der die Ordnung einer zufällig gewählten, kryptographisch geeigneten Kurve über einem Definitionskörper mit großer Charakteristik ermittelt. Gaudry und Harley [15] haben Teile des SEA-Algorithmus auf hyperelliptische Kurven übertragen und erreichten damit Gruppenordnungen um 2^{126}. Teske und Stein [57] halten der Rekord für $g = 3$. Sie ermittelten Gruppenordnungen um 2^{93}. Da man in beiden Fällen noch weit von der praktisch relevanten Größe entfernt ist, ist es sehr interessant, nach Alternativen Ausschau zu halten.

Spallek [56] verallgemeinerte die CM-Methode für Geschlecht zwei. Sie konstruierte in ihrer Arbeit einige Beispiele, bei denen der CM-Körper Klassenzahl eins hat. Wang und Weber [60], [61] schlugen vor, die Berechnung der Gröbner-Basen durch den Algorithmus von Mestre zu ersetzen. Van Wamelen [59] konstruierte eine wahrscheinlich vollständige Liste aller über $\mathbb{Q}$ definierten hyperelliptischen Kurven vom Geschlecht zwei, die komplexe Multiplikation haben. Weber [61] verallgemeinerte den Algorithmus von Mestre auf höhere Geschlechter. Dieser ermöglicht es, von einer Kurve über $\mathbb{C}$ mit nicht-trivialen, über einem Zahlkörper M definierten Mestre-Invarianten die Reduktion mod $\mathfrak{p}|p$ zu berechnen. Alle bisher konstruierten Kurven vom Geschlecht zwei hatten über $\mathbb{Q}$ definierte Invarianten. Es existierte keine Implementierung des Algorithmus im Falle $g = 2$. Niemand hatte eine Verallgemeinerung der CM-Methode auf Geschlechter $g \geq 3$ betrachtet.

Inhalt der Arbeit

Diese Arbeit beschäftigt sich mit den beiden Fällen $g = 2$ und 3.
Wir haben nach den Vorarbeiten von Spallek, Weber und Wang eine komplette Implementierung der CM-Methode für Geschlecht zwei geschrieben. Damit ist es nun möglich, die wichtigen Fragen nach Praktikabilität, Komplexität, Laufzeit und Grenzen des Verfahrens zu klären.
Die CM-Methode für $g = 2$ stellt ein effizientes Konstruktionsverfahren dar. Sie erlaubt es in wenigen Minuten, die Parameter einer nach heutigem Stand kryptographisch sicheren Kurve zu erzeugen. Selbst die einzige zuvor bekannte Kurve über $\mathbb{F}_p$, bei der man leicht

die Gruppenordnung ermitteln konnte, nämlich die Koblitzkurve [25]

$$y^2 = x^5 - 1 \text{ über } \mathbb{F}_p \text{ mit } p \equiv 1 \mod 5,$$

gehört zu dieser Klasse. Sie hat offensichtlich komplexe Multiplikation mit $\mathbb{Q}(\zeta_5)$.
Die Laufzeit hängt wesentlich von der Berechnung des Klassenpolynoms ab. Die Komplexität der Klassenpolynome wird von der Klassenzahl und der Diskriminante des CM-Körpers bestimmt. Die möglichen Klassenpolynome lassen sich allerdings im voraus ermitteln.
Wir können das Klassenpolynom von CM-Körpern abhängig von der Diskriminante bis zu Klassenzahl 10 berechnen. Es ist somit möglich, Kurven über endlichen Primkörpern anzugeben, deren Lift nach $\mathbb{C}$ Invarianten vom Grad 20 über $\mathbb{Q}$ hat.

Durch Untersuchung der CM-Körper nach theoretischen Gesichtspunkten können wir den Algorithmus noch weiter vereinfachen. Wir zeigen, daß die Klassenpolynome für Geschlecht zwei modulo p eine Nullstelle haben, falls p eine relative Normgleichung bezüglich K/K_0 erfüllt.
Das Verfahren läßt sich auch auf die Konstruktion von hyperelliptischen Kurven über Erweiterungkörpern der Form $\mathbb{F}_{p^n}$ mit $n > 1$ anwenden. Wir geben ein Rezept an, wie wir größtmöglichen Erweiterungsgrad erreichen können. Damit konstruieren wir eine kryptographisch gute Kurve über einem Körper $\mathbb{F}_{p^{10}}$ mit komplexer Multiplikation mit der Hauptordnung eines CM-Körper mit Klassenzahl 5.

Als nächstes wenden wir uns dem Fall $g = 3$ zu. Wir geben an, wie sich die Periodenmatrix und ein vollständigen Repräsentantensystems prinzipal polarisierter Abelscher Varietäten in diesem Fall beschreiben lassen. Dabei ist es nötig, sich auf CM-Körper zu beschränken, deren reeller Teilkörper Klassenzahl eins und einen monogenen Ganzheitsring hat. Hier sind auch Teilaussagen für $g = 4$ möglich.
Aufgrund der Vorarbeiten von Weber und basierend auf Mumford [36] und Poor [42] können wir abhängig von den Thetanullwerten explizite Formeln für das Rosenhain-Modell einer hyperelliptischen Kurve vom Geschlecht drei angeben.
Die CM-Methode in der von uns betrachteten Form ist ausschließlich für hyperelliptische Kurven geeignet. Das Repräsentantensystem prinzipal polarisierter Abelscher Varietäten mit komplexer Multiplikation mit $\mathcal{O}_K$ der Dimension drei enthält aber fast nie eine hyperelliptische Kurve. Genauer hat der Modulraum der hyperelliptischen Kurven vom Geschlecht drei im Modulraum aller prinzipal polarisierten Abelschen Varietäten der Dimension drei die Kodimension eins.
Mit unserem Algorithmus können wir testen, ob es zu einem zufällig gewählten CM-Körper K (dessen reeller Teilkörper Klassenzahl eins und einen monogenen Ganzheitsring hat) vom Grad sechs eine hyperelliptische Kurve gibt, deren Jacobische komplexe Multiplikation mit $\mathcal{O}_K$ hat. So gibt es zum Beispiel keinen CM-Körper K mit $h_K = 1$ und $[L : \mathbb{Q}] = 24$ (L der Galoissche Abschluß von K) mit dieser Eigenschaft (Abschnitt 4.3).

Prinzipal polarisierte Abelsche Varietäten der Dimension drei mit einem Automorphis-

mus der Ordnung vier sind immer hyperelliptische Kurven (siehe Satz 4.4.2). Wir haben uns deshalb auf spezielle CM-Körper konzentriert, die insbesondere die vierten Einheitswurzeln enthalten. Leider schließt die Existenz von weiteren Automorphismen neben der hyperelliptischen Involution die Anwendung von Mestres Algorithmus aus, da in diesem Fall Mestres Invarianten verschwinden. Wir mußten deshalb den Weg à la Spallek einschlagen und versuchen, über die Invarianten mit Hilfe von Gröbner-Basen eine geeignete Kurve zu finden.
Zusätzlich können wir annehmen, daß ein Twist der Kurve über $\mathbb{F}_p$ einer speziellen Normalform genügt. Damit läßt sich der Buchberger-Algorithmus effizient einsetzen. Wir geben einige so konstruierte, kryptographisch geeignete Kurven vom Geschlecht 3 an. Diese Kurven haben eine kleinere Automorphismengruppe als die einzige Kurve über $\mathbb{F}_p$ vom Geschlecht drei, deren Gruppenordnung man bisher bestimmen konnte, nämlich die Koblitz-Kurve mit komplexer Multiplikation mit $\mathbb{Q}(\zeta_7)$. Wir haben ingesamt neun verschiedene CM-Körper berücksichtigen können.
Weiter geben wir zwei über $\mathbb{Q}$ definierte hyperelliptische Kurven mit komplexer Multiplikation mit einem CM-Körper $\neq \mathbb{Q}(\zeta_7)$ an.

Mit unseren Programmen haben wir Statistiken für Kurven vom Geschlecht eins und zwei erstellt. Wir untersuchen, wie oft eine fast prime Gruppenordnung im CM-Fall auftritt.
Wir erweitern die Arbeit von Koblitz [24] für elliptische Kurven, indem wir für die imaginär quadratischen Körper beliebige Diskriminante und beliebige Klassenzahl zulassen.
Außerdem verallgemeinern wir seine Idee auf Kurven vom Geschlecht zwei. Dabei widmen wir uns der Verteilung von Eigenwerten in abelschen Untergruppen der allgemeinen symplektischen Gruppe.

Die Arbeit ist wie folgt aufgebaut: In Kapitel 1 erklären wir die Idee der CM-Methode und führen dabei die wichtigsten Begriffe ein. In Kapitel 2 beschreiben wir den Algorithmus und unsere Implementierung im Fall $g = 2$. Wir diskutieren unsere Ergebnisse. Das dritte Kapitel beschäftigt sich mit theoretischen Ergänzugen für Geschlecht zwei und Kurven über Nicht-Primkörpern. Im Kapitel 4 leiten wir die Theorie für $g = 3$ her, beschreiben die auftretenden Probleme und geben Beispiele an. Kapitel 5 ist den Statistiken und ihrer Interpretation gewidmet.

Kapitel 1

Einführung

1.1 Definitionen und Grundlagen

In dieser Arbeit betrachten wir hyperelliptische Kurven, die über einem (nicht unbedingt algebraisch abgeschlossenen) Körper κ der Charakteristik **ungleich zwei** definiert sind. Wir nehmen an, daß die Kurve durch eine Gleichung der Form

$$C: \quad y^2 = f(x), \quad \deg f(x) = 2g+1 \text{ oder } 2g+2,$$

gegeben ist. Das Polynom $f(x)$ hat in $\overline{\kappa}$ nur einfache Nullstellen, so daß die Kurve in $\mathbb{P}_2$ außerhalb von ∞ nicht singulär ist.
Die Jacobi-Varietät einer über κ definierten hyperelliptischen Kurve C ist eine Abelsche Varietät, deren Gruppe λ-rationaler Punkte für alle Körpererweiterungen $\lambda|\kappa$ funktoriell isomorph zur Divisorklassengruppe vom Grad 0 über λ ist. Insbesondere bilden für $\kappa = \mathbb{F}_q$ die über κ definierten Divisorklassen vom Grad 0 eine endliche abelsche Gruppe.

1.1.1 Prinzipal polarisierte Abelsche Varietäten

Wir betrachten zunächst den Fall $\kappa = \mathbb{C}$.
Eine **Riemannform** auf einem Gitter $\Lambda \subset \mathbb{C}^g$ ist eine reellwertige Bilinearform $E(x,y)$ auf $\mathbb{C}^g$ mit den folgenden Eigenschaften:

1. $E(x,y) \in \mathbb{Z}$ für $x, y \in \Lambda$,
2. $E(x,y) = -E(y,x)$ und
3. $E(ix,y)$ ist eine positiv definite symmetrische Form.

Jede über $\mathbb{C}$ definierte Abelsche Varietät ist zu $\mathbb{C}^g/\Lambda$ für ein Gitter Λ isomorph. Damit $\mathbb{C}^g/\Lambda$ eine Abelsche Varietät ist, muß zusätzlich auf Λ eine Riemannform existieren. Die Abelsche Varietät $(A,E) = (\mathbb{C}^g/\Lambda, E)$ nennen wir dann **polarisierte Abelsche Varietät**.

Abbildung 1.1: Homologiegruppe auf der Riemannschen Fläche, $g = 3$

Die Abelsche Varietät heißt **prinzipal polarisiert**, falls für Λ eine Basis $\{\alpha_1, \dots, \alpha_{2g}\}$ existiert, so daß

$$E_{ij} = (E(\alpha_i, \alpha_j))_{1 \le i,j \le 2n} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Das Gitter können wir dann in der Form $w_1\mathbb{Z}^g + w_2\mathbb{Z}^g$ mit

$$w_i = \left(\alpha_{1+(i-1)g}, \dots, \alpha_{g+(i-1)g}\right)$$

angeben. Die Matrix $\Omega = w_2^{-1}w_1$ liegt dann in der **Siegelschen oberen Halbebene**, d.h. sie ist symmetrisch und besitzt einen positiv definiten Imaginärteil. Das Gitter ist in diesem Fall zu $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ äquivalent. Die Matrix Ω nennen wir die **Periodenmatrix** der Abelschen Varietät.
Für den Begriff der prinzipalen Polarisierung gibt es auch eine äquivalente, algebraische Definition für beliebigen Definitionskörper κ (siehe z.B. [33], S.126).
Jacobi-Varietäten von Kurven lassen sich prinzipal polarisieren (für κ beliebig siehe [34]). Eine über $\mathbb{C}$ definierte Kurve C vom Geschlecht g ist eine kompakte Riemannsche Fläche mit g Henkeln. Die Homologiegruppe $H_1(C, \mathbb{Z})$ hat Rang $2g$. Wir wählen eine Basis $a_1, \dots, a_g, b_1, \dots, b_g$ auf C, so daß sich jeweils nur die Kurven a_i und b_i in einem Punkte schneiden (siehe Abbildung 1.1.1).
Es sei nun $w_1, \dots, w_g$ eine Basis des Vektorraums der holomorphen Differentiale $\Omega_1(C)$ auf C. Dann wird von den Vektoren

$$\left\{\gamma_{a_i} = \left(\int_{a_i} w_1, \dots, \int_{a_i} w_g\right), i = 1, \dots, g\right\} \cup \left\{\gamma_{b_i} = \left(\int_{b_i} w_1, \dots, \int_{b_i} w_g\right), i = 1, \dots, g\right\}$$

ein Gitter $\mathrm{Per}(w_1, \dots, w_g)$ aufgespannt. Dies heißt das **Periodengitter** der Kurve C. Unter der **Jacobi-Varietät** von C versteht man

$$Jac(C) = \mathbb{C}^g/\mathrm{Per}(w_1, \dots, w_g).$$

Die Inzidenzpaarung (für die Definition siehe z.B. [52]) induziert eine Riemannsche Form auf der Basis $\{\gamma_c\}$:

$$\begin{aligned} &E(\gamma_{a_i}, \gamma_{a_j}) = 0, \quad E(\gamma_{b_i}, \gamma_{b_j}) = 0, \\ &E(\gamma_{a_i}, \gamma_{b_j}) = E(\gamma_{b_i}, \gamma_{a_j}) = 0 \text{ für } i \neq j \text{ und} \\ &E(\gamma_{a_i}, \gamma_{b_i}) = -E(\gamma_{b_i}, \gamma_{a_i}) = 1. \end{aligned}$$

Ein **Isomorphismus zwischen zwei prinzipal polarisierten Abelschen Varietäten** (J_1, E_1) und (J_2, E_2) ist ein Isomorphismus zwischen den Varietäten J_1 und J_2, der die prinzipalen Polarisierungen E_1 und E_2 ineinander überführt. Ein Isomorphismus von Kurven induziert (bis auf Translation) einen Isomorphismus ihrer prinzipal polarisierten Jacobischen Varietäten. Nach Torelli ([33], S.202) gilt auch die Rückrichtung.

Satz 1.1.1 (Torelli). *Es seien C_1 und C_2 zwei über einem algebraisch abgeschlossenen Körper κ definierte Kurven, die in ihre Jacobische durch die Abbildungen $f_1 : C \to J_1$ und $f_2 : C_2 \to J_2$ mit Aufpunkten $P_1 \in C_1$ bzw. $P_2 \in C_2$ eingebettet sind. Weiter sei*

$$\alpha : (J_1, E_1) \to (J_2, E_2)$$

ein Isomorphismus zwischen den prinzipal polarisierten Jacobischen Varietäten von C_1 und C_2 definiert über κ. Dann ergibt die Einschränkung von α auf C_1 einen Isomorphismus β zwischen C_1 und C_2, so daß $f_2 \circ \beta = \pm\alpha \circ f_1 + c$ für einen Punkt $c \in J_2(\kappa)$. Insbesondere sind die Kurven C_1 und C_2 isomorph.
Sei das Geschlecht von $C \geq 2$. Falls C hyperelliptisch ist, kann das Vorzeichen beliebig gewählt werden, aber dann sind α und c eindeutig festgelegt. Falls C nicht hyperelliptisch ist, dann sind die Abbildung β, das Vorzeichen $\pm$ und c durch α und die Punkte P_1 und P_2 eindeutig bestimmt.

Aus dieser ausführlichen Version des Torellischen Satzes läßt sich das folgende Korollar ableiten:

Korollar 1.1.2. *Sei C eine hyperelliptische Kurve und (J, E) ihre prinzipal polarisierte Jacobische. Dann gilt*

1. *$Aut(C) = Aut((J, E))$, falls C hyperelliptisch, und*
2. *$Aut(C) = Aut((J, E))/\{\pm 1\}$, falls C nicht hyperelliptisch ist.*

Beweis. Hier wenden wir Torelli mit $C = C_1 = C_2$ und $J = J_1 = J_2$ an. Weiter sei α ein Automorphismus der prinzipal polarisierten Jacobischen J von C. Falls C hyperelliptisch ist, haben wir die Wahl des Vorzeichens, und wir legen fest, daß es stets positiv sein soll. Dann ist $\phi : \alpha \to \beta$ ein Isomorphismus von $Aut((J, E))$ nach $Aut(C)$.
Falls C nicht hyperelliptisch, dann ist $\phi : \alpha \to \beta$ ein surjektiver Homomorphismus von $Aut((J, E))$ nach C mit Kern $\{\pm 1\}$. Sei nämlich $\alpha \in Aut((J, E))$. Dann bestimmt α nach Satz 1.1.1 ein Vorzeichen (etwa $+$), einen Automorphismus β und einen Punkt $c \in J(\kappa)$. Der Automorphismus $-\alpha$ hingegen führt auf das Vorzeichen $-$, den gleichen Automorphismus β und $c \in J(\kappa)$. □

1.1.2 Komplexe Multiplikation

CM-Körper und CM-Typen

Ein algebraischer Zahlkörper K mit $[K:\mathbb{Q}] = 2g$ heißt **CM-Körper**, falls K eine total imaginär quadratische Erweiterung eines total reellen Zahlkörpers K_0 ist. Unter einem total reellen Zahlkörper K_0 versteht man einen Zahlkörper, für den alle Einbettungen σ von K_0 nach $\mathbb{C}$ reell sind.
Sei K ein CM-Körper vom Grad $2g$ über $\mathbb{Q}$ und $\varphi_i, 1 \leq i \leq g$ seien n verschiedene Einbettungen von K nach $\mathbb{C}$. Ein Tupel $(K, \{\varphi_1, \varphi_2, \cdots, \varphi_g\})$ heißt **CM-Typ**, falls alle Einbettungen echt unterschiedlich und keine zwei Einbettungen φ_i komplex konjugiert zueinander sind. Wir schreiben abkürzend $(K, \Phi) := (K, \{\varphi_1, \varphi_2, \cdots, \varphi_g\})$.
Sei (K, Φ) ein CM-Typ und L der kleinste über $\mathbb{Q}$ Galoissche Körper, der K enthält. Sei $G = Gal(L/\mathbb{Q})$, $H = Gal(L/K)$ und $H_0 = Gal(L/K_0)$. Wir definieren die Mengen

$$\begin{aligned} S &:= \{\sigma \in G : \sigma|_K = \varphi_i, i = \{1, \cdots, g\}\}, \\ S^* &:= \{\gamma^{-1} \in G : \gamma \in S\} \\ H^* &:= \{\gamma \in G : \gamma S^* = S^*\} \text{ und} \\ H' &:= \{\gamma \in G : \gamma S = S\}. \end{aligned}$$

Der CM-Typ (K, Φ) heißt **primitiv**, falls H und H' gleich sind.
Sei nun $K^* = Fix(H^*)$ und $\{\psi_i\}$ die Menge aller Einbettungen von K^* nach $\mathbb{C}$, so daß

$$\gamma\,|_{K^*} = \psi_j$$

für ein $\gamma \in S^*$. Dann gilt

$$K^* = \mathbb{Q}(\sum_{i=1}^{n} \varphi_i(\xi), \xi \in K)$$

und (K^*, ψ_j) ist auch ein CM-Typ. Er heißt der zu $(K, \{\varphi_i\})$ **duale CM-Typ** und K^* ist der **Reflexivkörper**.

Sei A eine einfache Abelsche Varietät über $\mathbb{C}$ und $\mathrm{End}_0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$. Weiter nehmen wir an, daß $e : K \to \mathrm{End}_0(A)$ ein Isomorphismus ist, und die Abbildung $S_\Phi = \Phi_1 \circ e$ mit $\Phi_1 : \mathrm{End}_0(A) \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}^g) \simeq M_g(\mathbb{C})$ nach geeigneter Basiswahl durch

$$S_\Phi(\alpha) = \begin{pmatrix} \varphi_1(\alpha) & & \\ & \ddots & \\ & & \varphi_g(\alpha) \end{pmatrix}$$

beschrieben wird. Dann heißt A eine **Abelsche Varietät vom CM-Typ** $(K, \Phi) = (K, \{\varphi_1, \cdots, \varphi_g\})$. Zu jeder Abelscher Varietät A mit $\mathrm{End}_0(A) \simeq K$ existiert ein solcher CM-Typ.
Es läßt sich auch definieren, was es bedeutet, wenn eine nicht-einfache Abelsche Varietät vom CM-Typ (K, Φ) ist (siehe [30]). Wir interessieren uns aber nur für einfache Abelsche Varietäten, und es gilt der folgende Satz ([50], Abschnitt 8.2).

Satz 1.1.3. *Eine Abelsche Varietät vom CM-Typ (K, Φ) ist genau dann einfach, wenn ihr CM-Typ primitiv ist.*

Somit sind zu einem gegeben CM-Typ entweder alle Abelschen Varietäten einfach oder nicht einfach. Bei unserer Konstruktion werden wir uns auf primitive CM-Typen beschränken.
Sei $\mathfrak{A}$ ein Ideal im Ring der ganzen Zahlen $\mathcal{O}_K$ und (K, Φ) ein CM-Typ. Dann hat das Gitter

$$\Phi(\mathfrak{A}) := \left\{ (\varphi_1(\alpha), \dots, \varphi_g(\alpha))^t, \alpha \in \mathfrak{A} \right\}$$

in $\mathbb{C}^g$ komplexe Multiplikation mit $\mathcal{O}_K$. Genauer läßt die Transformation

$$S_\Phi(\gamma) = \begin{pmatrix} \varphi_1(\gamma) & & \\ & \ddots & \\ & & \varphi_g(\gamma) \end{pmatrix}, \gamma \in \mathcal{O}_K$$

das Gitter invariant (siehe [50]). Man kann zeigen, daß der komplexe Torus $\mathbb{C}^g/\Phi(\mathfrak{A})$ in diesem Fall eine Abelsche Varietät beschreibt (siehe [30], Abschnitt 1.4). Diese Abelsche Varietät, die vom CM-Typ (K, Φ) ist, bezeichnen wir mit $A(\mathfrak{A})$. Umgekehrt läßt sich jede Abelsche Varietät vom CM-Typ (K, Φ) auf diese Weise beschreiben ([30], Satz 4.1).

Polarisierungen

Sei $\mathfrak{A}$ ein Ideal in K und $A(\mathfrak{A}) = \mathbb{C}^g/\Phi(\mathfrak{A})$ die oben definierte Abelsche Varietät vom CM-Typ (K, Φ) mit $\mathrm{End}(A) = \mathcal{O}_K$. Dann gibt es ein Element $\xi \in K$ mit $K = K_0(\xi)$, ξ total imaginär und $-\xi^2$ total positiv in K_0 (d.h. $-\xi^2$ ist für alle Einbettungen von K_0 nach $\mathbb{C}$ positiv). Weiter gilt $\mathrm{Im}(\varphi_i(\xi)) > 0$ für $i = 1, \cdots, g$. Für das Element ξ ist mit

$$E_\xi(x, y) = r \cdot \sum_{i=1}^{g} \varphi_i(\xi)(\overline{x_i} y_i - x_i \overline{y_i})$$

für geeignetes $r \in \mathbb{Z}$ eine Riemannform E_ξ auf $\mathbb{C}^g/\Phi(\mathfrak{a})$ gegeben (siehe [56]).
Jede Riemannform, die die Bedingung

$$E(x, S_\Phi(\alpha)y) = E(S_\Phi(\overline{\alpha})x, y) \tag{1.1}$$

erfüllt, kann durch ein geeignetes Element $\xi \in K$ definiert werden. Falls $\mathbb{C}^g/\Phi(\mathfrak{a})$ eine einfache Abelsche Varietät ist, dann ist nach Lang ([30], S. 21, Theorem 4.5. (iii)) jede von Null verschiedene Riemannform nicht-degeneriert und erfüllt Bedingung (1.1).
Eine prinzipale Polarisierung definiert ξ allerdings nur, wenn

$$\xi \delta \overline{\mathfrak{A}} \mathfrak{A} = \mathcal{O}_K$$

für $\delta = \delta_{K/\mathbb{Q}}$ die Differente von K bezüglich $\mathbb{Q}$.
Für den Fall $\mathfrak{A} = \mathcal{O}_K$ ergibt sich damit der folgende Satz ([56], Proposition 3.15):

Satz 1.1.4. *Eine prinzipale Polarisierung auf $A(\mathcal{O}_K)$ vom CM-Typ $(K, \{\varphi_i\})$ existiert genau dann, wenn es ein γ in K gibt, so daß $\delta_{K/\mathbb{Q}} = (\gamma)$ und Im $\varphi_i(\gamma) < 0$ für alle i gilt. Wir können dann $\xi = \gamma^{-1}$ setzen.*

Sei K ein CM-Körper, dessen reeller Teilkörper K_0 Klassenzahl eins hat, dann hat $\mathcal{O}_K$ eine Ganzheitsbasis über $\mathcal{O}_{K_0}$, und die Differente $\delta_{K/\mathbb{Q}}$ ist ein Hauptideal (γ). Wir können die φ_i so wählen, daß Im $\varphi_i(\gamma) < 0$ für alle φ_i. Somit existiert zu K ein CM-Typ, für den es eine prinzipale Polarisierung auf $A(\mathcal{O}_K)$ gibt. Nach Satz 1.1.4 können wir $\xi = \gamma^{-1}$ setzen.

Repräsentantensysteme prinzipal polarisierter Abelscher Varietäten

Wir möchten ein Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit $\mathcal{O}_K$ und CM-Typ (K, Φ) angeben.
Seien A_1, A_2 zwei Abelsche Varietäten über $\mathbb{C}$ vom gleichen CM-Typ (K, Φ). Wir schreiben $A_1 \simeq \mathbb{C}^g/\Phi(\mathfrak{A}_1)$ und $A_2 \simeq \mathbb{C}^g/\Phi(\mathfrak{A}_2)$. Dann lassen sie sich durch ein Element γ in $\mathfrak{A}_1^{-1}\mathfrak{A}_2$ ineinander überführen, und die Elemente in $\mathfrak{A}_1^{-1}\mathfrak{A}_2$ sind genau die Homomorphismen von A_1 nach A_2. Wir nennen diesen Homomorphismus dann eine $\gamma\mathfrak{A}_\mathbf{1}^{-\mathbf{1}}\mathfrak{A}_\mathbf{2}$**-Multiplikation** von A_1 nach A_2, und A_2 ist eine $\gamma\mathfrak{A}_\mathbf{1}^{-\mathbf{1}}\mathfrak{A}_\mathbf{2}$**-Transformation** von A_1.
Es gelten die drei folgenden Sätze, die es uns erlauben werden, ein Repräsentantensystem anzugeben [56]:

- Es sei U^+ die Gruppe der total positiven Einheiten in K_0, U_1 die Untergruppe von U^+ mit Elementen der Form $\epsilon\overline{\epsilon}$ für ein $\epsilon \in K$ und $\{\epsilon_1 = 1, \epsilon_2, \ldots, \epsilon_d\}$ Repräsentanten für U/U_1. Falls $(A(\mathfrak{A}), \xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K, Φ) ist, dann ist $\{(A(\mathfrak{A}), \epsilon_i\xi) : i = 1, \ldots, d\}$ ein Repräsentantensystem aller Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten zu der Abelschen Varietät $A(\mathfrak{A})$.

- Zwei prinzipal polarisierte Abelsche Varietäten $(A(\mathfrak{A}_1), \xi_1)$ und $(A(\mathfrak{A}_2), \xi_2)$ vom gleichen CM-Typ (K, Φ) sind genau dann isomorph, wenn es ein Element $\gamma \in K$ gibt, so daß $\gamma\mathfrak{A}_1 = \mathfrak{A}_2$ und $\xi_1 = \gamma\overline{\gamma}\xi_2$.

- Sei $(A(\mathfrak{A}), \xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K, Φ). Ist A' eine $\mathfrak{A}'$-Transformation von A, so gibt es genau dann eine prinzipale Polarisierung ξ' auf A', wenn $\mathfrak{A}'$ total positive relative Norm bezüglich K/K_0 hat.

Wir nehmen nun an, daß es eine prinzipal polarisierte Abelsche Varietät $A(\mathcal{O}_K)$ vom CM-Typ (K, Φ) gibt. Dann liefert jedes Ideal mit total positiver relativer Norm eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K, Φ). Da zwei äquivalente Ideale isomorphe prinzipal polarisierte Abelsche Varietäten definieren, genügt es, die Elemente aus der Klassengruppe mit total positiver Norm zu betrachten. Diese Elemente der Klassengruppe bilden eine Untergruppe, die wir mit c'_K bezeichnen.
Nun können wir für den CM-Typ (K, Φ) ein vollständiges Repräsentantensystem angeben [56]:

Satz 1.1.5. *Sei (K, Φ) ein CM-Typ, für den eine prinzipal polarisierte Abelsche Varietät der Form $A(\mathcal{O}_K)$ existiert. Es seinen $\epsilon_1, \cdots, \epsilon_d$ Repräsentanten für U/U_1, $\mathfrak{A}_1, \cdots, \mathfrak{A}_{h'}$ ein Repräsentantensystem von c'_K mit $\mathfrak{A}_i\overline{\mathfrak{A}_i} = (\alpha_i)$ für α_i total positiv. Dann gibt es $h' \cdot d$ zueinander isomorphe prinzipal polarisierte Abelsche Varietäten mit komplexer Multiplikation mit $\mathcal{O}_K$ von diesem Typ. Sei $K_\Phi = \bigcup_{l=1}^{d} K_\Phi^l$ mit*

$$K_\Phi^l = \{(A(\mathfrak{A}_i), \epsilon_l\xi) : i = 1, \cdots, h', \xi = (\alpha_i\gamma)^{-1}\}.$$

Dann ist K_Φ das Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten vom CM-Typ (K, Φ).

Falls für einen CM-Typ (K, Φ) keine prinzipal polarisierte Abelsche Varietät $A(\mathcal{O}_K)$ existiert, müssen wir untersuchen, ob es eine prinzipal polarisierte Abelsche Varietät $A(\mathfrak{A})$ für ein $A \notin c'_K$ gibt. Falls ja, erhalten wir auf analoge Weise ein vollständiges Repräsentantensystem.

1.1.3 Endomorphismenringe über endlichen Körpern

In diesem Abschnitt erklären wir, warum kryptographisch geeignete Jacobi-Varietäten über $\mathbb{F}_q$ mit $q = p^n$ stets komplexe Multiplikation mit einem CM-Körper haben.
Wie allgemein bekannt unterscheiden wir bei elliptischen Kurven über endlichen Körpern zwei Klassen von Endomorphismenringen, Ordnungen in Quaternionenalgebren und Ordnungen in imaginär quadratischen Zahlkörpern. Dabei nennen wir die Kurven mit Quaternionenalgebren supersinguläre Kurven. Wegen der Frey-Rück-Reduktion (siehe [13] oder [12]) sind diese kryptographisch uninteressant. Alle kryptographisch interessanten elliptischen Kurven haben also komplexe Multiplikation mit der Ordnung in einem imaginär quadratischen Zahlkörper, d.h. einem CM-Körper vom Grad zwei über $\mathbb{Q}$.
Sei nun C eine hyperelliptische Kurve über einem endlichen Körper $\mathbb{F}_q$. Dann induziert die Abbildung

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

auf der Kurve einen Endomorphismus π (den **Frobenius-Endomorphismus**) auf der Jacobischen J_C.
Es sei $T_l(J_C)$ der Tate-Modul von J_C bezüglich $l \neq p$ und $V_l(J_C) = \mathbb{Q}_l \otimes T_l(J_C)$. Der Frobenius-Endomorphismus induziert eine Abbildung auf dem Vektorraum $V_l(J_C)$. Diese Darstellung besitzt ein charakteristisches Polynom

$$P(T) = \prod_{i=1}^{2g}(T - \pi_i)$$

vom Grad $2g$. Die Gruppenordnung von $J_C(\mathbb{F}_q)$ ist durch den Wert $P(1)$ gegeben. Das charakteristische Polynom beschreibt außerdem die Isogenieklassen der Jacobischen, denn es gilt der folgende Satz:

Satz 1.1.6 (Tate). *Die Abelsche Varietät A ist genau dann zu einer Abelschen Untervarietät von B isogen, falls $P_A \mid P_B$. Insbesondere sind A und B genau dann isogen, wenn $P_A = P_B$.*

Falls die Jacobi-Varietät nicht einfach ist, dann zerfällt das charakteristische Polynom in Faktoren, die zu den einzelnen Abelschen Untervarietäten gehören. Die Gruppenordnung ist dann natürlich nicht prim und wird im allgemeinen auch nicht annähernd prim sein. Wir betrachten deshalb nur einfache Abelsche Varietäten. Genauer fordern wir sogar, daß das charakteristische Polynom irreduzibel ist, da jeder echte Teiler zu einem Primteiler der Gruppenordnung führt. Wir schließen damit auch den Fall aus, daß das charakteristische Polynom Primpotenz eines einzigen Faktors ist, was bei einfachen Abelschen Varietäten mit nicht-kommutativen Endomorphismenringen auftreten kann.
Wir setzen nun $End_0(A) = \mathbb{Q} \otimes End_{\mathbb{F}_q}(A)$. Da A einfach ist, ist jeder Endomorphismus von A eine Isogenie. Das Inverse eines Elements in $End_0(A)$ läßt sich also mit Hilfe der dualen Isogenie beschreiben. Somit ist $End_0(A)$ ein Schiefkörper. Der Frobenius kommutiert mit jedem Endomorphismus, und es gilt sogar: $\mathbb{Q}(\pi)$ ist das gesamte Zentrum von $End_0(A)$ (siehe [58], S. 140). Das Zentrum eines Schiefkörpers ist ein Körper.
Wenn das charakteristische Polynom irreduzibel ist, folgt $End_0(A) = \mathbb{Q}(\pi)$. Somit ist $End_0(A)$ ein Körper.
Nach dem Satz von Weil gilt $|\pi| = q^{1/2}$ für alle Einbettungen von $\mathbb{Q}(\pi)$ nach $\mathbb{C}$. Eine algebraische Zahl w, für die alle Einbettungen den Absolutbetrag $\sqrt{q}$ haben, heißt **Weil-Zahl für** q.
Da das charakteristische Polynom irreduzibel ist und $\pi = \pm\sqrt{q}$ nur im supersingulären Fall für elliptische Kurven auftritt, muß π in allen Einbettungen echt komplex sein. Es gilt, $q = \pi\overline{\pi}$ und $\beta = \pi + \overline{\pi}$ ist total reell. Damit ist $\mathbb{Q}(\pi)$ eine imaginär quadratische Erweiterung eines total reellen Zahlkörpers $\mathbb{Q}(\beta)$ definiert durch die Gleichung

$$\pi^2 - \beta\pi + q = 0.$$

Nach Definition ist $\mathbb{Q}(\pi)$ ein CM-Körper. Jede kryptographisch interessante Kurve über $\mathbb{F}_q$ hat also komplexe Multiplikation mit einer Ordnung in einem CM-Körper.

1.1.4 Grundlagen aus der Klassenkörpertheorie

Sei K ein Zahlkörper, P_K die Menge alle Primstellen in K, $S \subset P_K$ eine Teilmenge, dann definieren wir die **Dirichletsche Dichte** von S durch

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum\limits_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

falls der Grenzwert existiert.
Die Dirichletsche Dichte tritt an die Stelle einer Wahrscheinlichkeitsverteilung. Sie hat die gewünschten Eigenschaften (siehe [8], S. 169). Wir schreiben $S \dot{\subseteq} T$, falls $S \subseteq T$ bis auf eine Menge der Dichte 0.

Sei nun L/K Galoissch (nicht unbedingt abelsch) und $\mathfrak{p}$ eine Primstelle in K, die in L unverzweigt ist, dann können wir das Artinsymbol $((L|K), \mathfrak{P})$ für $\mathfrak{P}$ über $\mathfrak{p}$ definieren. Alle Artinsymbole $((L|K), \mathfrak{P})$ für ein $\mathfrak{p}$ sind zueinander konjugiert. Wir können deshalb ein nur von $\mathfrak{p}$ abhängiges Symbol einführen:

$$((L|K), \mathfrak{p}) =< \sigma >,$$

wobei $< \sigma >$ die Konjugationsklasse von σ in $\mathrm{Gal}(L|K)$ ist.
Die Dirichlet-Dichte von Primzahlklassen kann mit ihrem Artinsymbol in Verbindung gebracht werden [37]:

Satz 1.1.7 (Cebotarevs Dichtesatz). *Sei $L|K$ eine Galoissche Erweiterung, $< \sigma >$ die Konjugationsklasse von σ in $Gal(L|K)$ und*

$$S = \{\mathfrak{p} \in P_K : \mathfrak{p} \text{ unverzweigt in } L, ((L|K), \mathfrak{p}) =< \sigma >\}.$$

Dann gilt

$$\delta(S) = \frac{| < \sigma > |}{|Gal(L|K)|} = \frac{| < \sigma > |}{|L : K|}.$$

Der Satz von Cebotarev ist ungeheuer mächtig. Unter anderem können wir aus ihm das folgende Korollar ableiten (siehe [37], S. 135):

Korollar 1.1.8. *Seien L, M Zahlkörper und $L|\mathbb{Q}$ Galoissch. Es bezeichne $P(L, \mathbb{Q})$ die Menge aller Primideale, die in L total zerlegt sind. Dann gilt*

$$P(L|\mathbb{Q}) \dot{\supseteq} P(M|\mathbb{Q}) \Leftrightarrow L \subseteq M.$$

Weiter benötigen wir den Zerlegungssatz aus der Klassenkörpertheorie [37]. Wir bezeichnen mit I_K die Menge der gebrochenen Ideale in K. Die Hauptideale seien durch H_K gegeben. Dann ist der Hilbertsche Klassenkörper von K der Körper, der zur Idealgruppe der Hauptideale korrespondiert. Jede andere unverzweigte, abelsche Erweiterung korrespondiert zu einer Idealgruppe, die die Hauptideale enthält.

Satz 1.1.9. *Sei M/K eine unverzweigte, abelsche Erweiterung vom Grad n, $\mathfrak{p}$ ein Primideal. Weiter sei H die zu M/K gehörige Idealgruppe. Falls f die Ordnung von $\mathfrak{p}$ mod H in der Idealklassengruppe I_K/H ist, dann zerfällt $\mathfrak{p}$ in M in ein Produkt*

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_r$$

von $r = \frac{n}{f}$ verschiedenen Primidealen $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ vom Grad f über p.

1.1.5 Der Modulkörper

Es sei (A, E) eine prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K, \{\varphi_i\})$ mit Endomorphismenring $\mathcal{O}_K$ und dualem CM-Typ (K^*, ψ_j). Der **Modulkörper** k_0 von (A, E) ist der eindeutige Körper mit folgender Eigenschaft:
Eine Automorphismus σ von $\mathbb{C}$ ist genau dann die Identität auf k_0, wenn ein Isomorphismus

$$\lambda : (A, E) \to (A^\sigma, E^\sigma) = (A, E)^\sigma$$

existiert.
Der Hauptsatz der CM-Theorie ([50], Main Theorem 1, S. 112) beschreibt die abelsche Körpererweiterung $k_0^* = k_0 K^*$ klassentheoretisch.

Satz 1.1.10 (Hauptsatz der CM-Theorie). *Betrachte die Idealgruppe H_0 der gebrochenen Ideale $\mathcal{A}^*$ in K^*, für die es ein Element μ in K gibt, so daß*

$$\prod_j \psi_j(\mathcal{A}^*) = (\mu) \text{ und } N(\mathcal{A}^*) = \mu\overline{\mu}.$$

Die Gruppe H_0 enthält die Hauptideale. Der zugehörige unverzweigte Klassenkörper über K^* ist der Körper k_0^*.

Bemerkung 1.1.11. Dieser Satz zeigt insbesondere, daß der Körper $k_0^* = k_0 K^*$ nur vom gegebenen CM-Typ, jedoch nicht von der Abelschen Varietät selbst, abhängt.

1.1.6 Charakterisierung hyperelliptischer Periodenmatrizen

Thetanullwerte

Sei $\Omega \in \mathbb{H}_g$ die Periodenmatrix zu einer prinzipalen Polarisierung eines Gitters $\mathbb{C}^g/\Lambda$ und $z \in \mathbb{C}^g$ ein Spaltenvektor. Dann können wir die **Riemannsche Thetafunktion** definieren:

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} exp(\pi i(n^t \Omega n + 2n^t z)).$$

Diese Funktion ist $\mathbb{C}$-wertig, holomorph und symmetrisch, d.h. es gilt $\theta(z, \Omega) = \theta(-z, \Omega)$. Für festes $\Omega \in \mathbb{H}_g$ erhalten wir eine Funktion von $\mathbb{C}^g$ nach $\mathbb{C}$, und wir können dann den **Riemannschen Thetadivisor** definieren:

$$\Theta^{(\Omega)} := \{z \mod \Lambda : \theta(z, \Omega) = 0\}.$$

Zwei Periodenmatrizen Ω, Ω' definieren isomorphe prinzipal polarisierte Abelsche Varietäten, falls sie in der gleichen Bahn unter der Operation

$$\Omega \mapsto \frac{A\Omega + B}{C\Omega + D}$$

der **symplektischen Gruppe**

$$Sp(g,\mathbb{Z}) = \left\{ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Gl(2g,\mathbb{Z}) : M^t J M = J \text{ mit } J = \begin{pmatrix} O & I_g \\ -I_g & 0 \end{pmatrix} \right\}$$

auf $\mathbb{H}_g$ liegen.
Wenn wir eine zu Ω äquivalente Matrix Ω' in $\mathbb{H}_g$ betrachten, dann muß deren Thetafunktion nicht notwendigerweise den gleichen Thetadivisor haben. Jedoch wird er auch symmetrisch sein und eine prinzipale Polarisierung induzieren. Es läßt sich zeigen, daß dann $\Theta^{(\Omega')}$ zu einem um a verschobenen Divisor $\Theta_a^{(\Omega)}$ mit $a \in \Omega(\frac{1}{2}\mathbb{Z}^g) + \frac{1}{2}\mathbb{Z}^g$ identisch ist (siehe [35], 3.10).
Dies motiviert die Betrachtung der **Thetacharakteristiken**

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (z,\Omega) = \sum_{n \in \mathbb{Z}^g} exp\left(\pi i (n + \frac{1}{2}\delta)^t \Omega (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (z + \frac{1}{2}\epsilon) \right)$$

mit Spaltenvektoren $\delta, \epsilon \in (\mathbb{Z}/2\mathbb{Z})^g$. Falls wir $\theta \left[\begin{smallmatrix} \delta \\ \epsilon \end{smallmatrix}\right] (0,\Omega)$ für festes δ, ϵ betrachten, erhalten wir eine Funktion auf $\mathbb{H}_g$. Diese Funktionen heißen **Thetanullwerte**. Falls $\delta^t \epsilon \equiv 0 \mod 2$ nennen wir den Thetanullwert **gerade**, sonst **ungerade**. Wegen

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (-z,\Omega) = (-1)^{\delta^t \epsilon} \theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (z,\Omega)$$

verschwinden die ungeraden Thetanullwerte identisch. Nach Igusa ([20], S.189) bestimmen die geraden Thetanullwerte die Äquivalenzklasse einer prinzipal polarisierten Abelschen Varietät eindeutig.
Es gibt $2^{g-1}(2^g + 1)$ gerade und $2^{g-1}(2^g - 1)$ ungerade Thetanullwerte.

Hyperelliptische Periodenmatrizen

Wir interessieren uns nun für die Frage, wann eine einfache prinzipal polarisierte Abelsche Varietät A gegeben durch eine Periodenmatrix Ω Jacobi-Varietät einer hyperelliptischen Kurve ist. Wir nennen die Periodenmatrix dann **hyperelliptische Periodenmatrix**.
Für $g = 2$ ist die Antwort einfach: Jede einfache prinzipal polarisierte Abelsche Varietät ist Jacobi-Varietät einer hyperelliptischen Kurve. Für $g \geq 3$ ist dies nicht mehr richtig.
Wir skizzieren zunächst, wie eine hyperelliptische Kurven ihre Thetanullwerte bestimmt. Die hyperelliptische Kurve über $\mathbb{C}$ sei durch folgendes Modell gegeben:

$$C : y^2 = \prod_{i=1}^{2g+1} (x - a_i).$$

Dann steht $B = \{a_1, \ldots, a_{2g+1}, \infty\}$ für die Menge der Verzweigungspunkte $(a_i, 0)$ von C über $\mathbb{P}^1$. Es sei L die Divisorenklasse in $Pic(C)$, die alle Divisoren der Form $P + \imath P$ mit $P \in C$ enthält, wobei $\imath$ die hyperelliptische Involution bezeichne.

Definition 1.1.12. *Für $T \subseteq B$, $\#T \equiv 0 \mod 2$ sei $e_T \in Pic^0[2](C)$ definiert durch*

$$e_T = \sum_{i \in T} a_i - \frac{\#T}{2} L,$$

wobei a_i für $P_i = (a_i, 0)$ steht.

Das Zeichen $\circ$ stelle folgende Verknüpfung zweier Mengen A, B dar: $A \circ B = A \cup B \setminus A \cap B$. Sei

$$T_0(2) = \{\text{Teilmengen } T \text{ von } B, \#T \equiv 0 \mod 2\} \mod \sim,$$

wobei $C \sim \tilde{C}$, falls $\tilde{C}$ das Komplement von C ist. Diese Menge können wir mit der Menge $\{T \subseteq B \setminus \infty : \#T \equiv 0 \mod 2\}$ identifizieren. Die Menge $T_0(2)$ bildet mit der Verknüpfung $\circ$ eine Gruppe, wie man sich leicht überzeugen kann.
Nach ([36], 3.32) ist die Gruppe $(T_0(2), \circ)$ isomorph zu $\mathrm{Pic}^0[2]$.
Sei nun $\hat{C}$ die universelle Überlagerung von C und $\pi : \hat{C} \to C$ die Projektion. Wir wählen den Basispunkt $a_\infty = \infty$ auf der hyperelliptischen Kurve und $\hat{a}_\infty$ auf $\hat{C}$, so daß $\pi(\hat{a}_\infty) = a_\infty$. Sei $\varphi : Pic^0(C) \to \mathbb{C}^g / Per$ mit $Per = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ die Abel-Jacobi-Abbildung. Es gibt eine Abbildung $\hat{\varphi} : \hat{C} \to \mathbb{C}^g$, so daß $\hat{\varphi}(z) \mod Per = \varphi(\pi(z) - a_\infty)$ ist.
Da der Divisor $P_i - P_\infty$ mit $P_i = (a_i, 0)$ und $P_\infty = a_\infty$ in $\mathrm{Pic}^0[2]$ liegt, folgt $\varphi(\hat{a}_i) \in \frac{1}{2} Per$. Für alle $i \in B$ setzen wir nun $\eta_{a_i} \in (\mathbb{Z}/2\mathbb{Z})^{2g}$, so daß $\varphi(\hat{a}_i) = \frac{1}{2}(I\Omega)\eta_{a_i}$. Diese Definition können wir für alle Teilmengen $T \subseteq B$ fortsetzen, so daß $\varphi(\sum_T \hat{a}_i) = (I\Omega)\eta_T$.
Wir benötigen eine weitere Definition:

Definition 1.1.13. *Ein **azygetisches Fundamentalsystem** $\{\eta_i\}$ ist eine Menge aus $2g+1$ verschiedenen Spaltenvektoren $\eta_i \in (\mathbb{Z}/2\mathbb{Z})^{2g} - \{0\}, i = 1, \ldots, 2g+1$, so daß für alle $\eta_i = \begin{bmatrix} \delta_i \\ \epsilon_i \end{bmatrix}$ und $\eta_j = \begin{bmatrix} \delta_j \\ \epsilon_j \end{bmatrix}$ mit $i \neq j$*

$$\eta_i^t \eta_j \equiv 1 \mod 2$$

gilt.

Bemerkung 1.1.14.

1. Falls $B = \{a_1, \ldots, a_{2g+1}, \infty\}$ die Menge der Verzweigungspunkte ist, dann bildet η_{a_i} ein azygetisches Fundamentalsystem ([42], S.825).
2. Die Menge der Isomorphismen von $T_0(2)$ nach $(\mathbb{Z}/2\mathbb{Z})^{2g}$ stehen in 1:1 Beziehung zu den verschiedenen azygetischen Fundamentalsystemen von $(\mathbb{Z}/2\mathbb{Z})^{2g}$ ([42], Lemma 1.4.13).

Sei nun U die Menge der Verzweigungspunkte mit ungeradem Index, also

$$U = \{1, 3, \ldots, 2g+1\}.$$

Falls wir die η_i wie oben durch eine hyperelliptische Kurve erhalten haben, dann gilt für T mit $\#T \equiv 0 \mod 2$ (siehe [36], Satz 6.7)

$$\theta(\eta_T)[0, \Omega] = 0 \Leftrightarrow \#(T \circ U) \neq g + 1.$$

Daraus erhalten wir bereits ein notwendiges Kriterium: Für eine hyperelliptische Periodenmatrix verschwinden genau s Thetanullwerte, wobei

$$s = \#\{T \subseteq B : \#T \equiv 0 \mod 2, \#(T \circ U) \neq g+1\}.$$

Für $g = 2$ veschwinden somit nur die ungeraden Thetanullwerte. Für $g = 3$ verschwindet genau ein gerader Thetanullwert.
Sei Ω eine beliebige Periodenmatrix und ρ ein beliebiger Isomorphismus mit

$$\rho : T_0(2) \simeq (\mathbb{Z}/2\mathbb{Z})^{2g}.$$

Falls

$$\theta(\rho_T)[0,\Omega] = 0 \Leftrightarrow \#(T \circ U) \neq g+1,$$

dann ist Ω die Periodenmatrix einer Jacobischen einer hyperelliptischen Kurve ([36], Satz 9.1).
Damit erhalten wir den folgenden Satz:

Satz 1.1.15. *Sei Ω eine beliebige Periodenmatrix. Dann sind folgende Aussagen äquivalent:*

1. *Ω ist hyperelliptisch.*
2. *Es existiert ein azygetisches Fundamentalsystem $\{\eta_1, \ldots, \eta_{2g+1}\}$, so daß die Thetanullwerte $\theta[\eta_T](\Omega) = \theta[\eta_T](0,\Omega)$ für $T \equiv 0 \mod 2$ mit $\infty \notin T$ genau dann in Ω verschwinden, wenn $\#(T \circ U) \neq g+1$, wobei $\eta_T = \sum_{i \in T} \eta_i$ und $U = \{\eta_1, \eta_3, \ldots, \eta_{2g+1}\}$.*

Um diese Bedingungen zu überprüfen, helfen uns zwei Tatsachen:

- Mumford hat ein azygetisches Fundamentalsystem $\eta_i = \binom{\delta_i^t}{\epsilon_i^t}$ konstruiert:

  $$\eta_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \eta_3 = \frac{1}{2}\begin{pmatrix} 0 & 1 \ldots & 0 \\ 1 & 0 \ldots & 0 \end{pmatrix}, \ldots, \eta_{2g+1} = \frac{1}{2}\begin{pmatrix} 0 & 0 \ldots & 0 \\ 1 & 1 \ldots & 1 \end{pmatrix},$$
  $$\eta_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{pmatrix}, \eta_4 = \frac{1}{2}\begin{pmatrix} 0 & 1 \ldots & 0 \\ 1 & 1 \ldots & 0 \end{pmatrix}, \ldots, \eta_{2g} = \frac{1}{2}\begin{pmatrix} 0 & 0 \ldots & 1 \\ 1 & 1 \ldots & 1 \end{pmatrix}.$$

  Dieses hat bereits die schöne Eigenschaft, daß die ungeraden Thetacharakteristiken in der Menge $\{\theta[\eta_S] : \#S \equiv 0 \mod 2, \#(S \circ U) \neq g+1\}$ enthalten sind.

- Die Gruppe $Sp(g, \mathbb{F}_2)$ operiert transivitiv auf der Menge der azygetischen Fundamentalsysteme. Die Operation γv für einen Vektor v aus $(\mathbb{Z}/2\mathbb{Z})^{2g}$ und $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(g, \mathbb{F}_2)$ ist durch

  $$\begin{pmatrix} D & C \\ B & A \end{pmatrix} v + \begin{pmatrix} diag(CD^t) \\ diag(AB^t) \end{pmatrix}$$

  gegeben, wobei $diag(CD^t) \in (\mathbb{Z}/2\mathbb{Z})^g$ den Vektor mit den Diagonalelementen von CD^t bezeichnet.

Rosenhain-Modell

Wenn wir für eine hyperelliptische Kurve ein passendes Fundamentalsystem $\{\eta_1, \ldots, \eta_{2g+1}\}$ gefunden haben, können wir daraus das **Rosenhain-Modell** über $\mathbb{C}$ berechnen. Dieses beschreibt die Kurve durch eine Gleichung der Form

$$y^2 = x(x-1)(x-\lambda_3)\ldots(x-\lambda_{2g+1}).$$

Dazu zerlegen wir für $i = 3, \ldots, 2g+1$ die Menge $\mathcal{B} = \{1, 2, 3, \ldots, 2g+1, \infty\}$ in drei disjunkte Teile $\{1, 2, i, \infty\}$, $\mathcal{B}_0^i$, $\mathcal{B}_1^i$ mit $\#\mathcal{B}_0^i = \#\mathcal{B}_1^i = g-1$ und setzen

$$\begin{array}{ll} S_1^{(i)} = \{1,2\} \cup \mathcal{B}_0^i & S_2^{(i)} = \{1,2\} \cup \mathcal{B}_1^i \\ S_3^{(i)} = \{1,i\} \cup \mathcal{B}_0^i & S_4^{(i)} = \{1,i\} \cup \mathcal{B}_1^i \\ S_5^{(i)} = \{2,i\} \cup \mathcal{B}_0^i & S_6^{(i)} = \{2,i\} \cup \mathcal{B}_1^i. \end{array}$$

Nun gilt der folgende Satz ([61], Seite 13):

Satz 1.1.16. *Sei $U_j^i = U \circ S_j^{(i)}$. Der Wert λ_{i-2} aus dem Rosenhain-Modell ist gleich*

$$\frac{(\theta[U_1^i](\Omega)\theta[U_2^i](\Omega))^4 + (\theta[U_3^i](\Omega)\theta[U_4^i](\Omega))^4 - (\theta[U_5^i](\Omega)\theta[U_6^i](\Omega))^4}{2(\theta[U_1^i](\Omega)\theta[U_2^i](\Omega))^4}.$$

1.1.7 Invarianten hyperelliptischer Kurven

Ein Teil unseres Algorithmus besteht darin, aus den Invarianten der Kurve eine Kurvengleichung zu bestimmen. Wir geben hier die dafür nötigen Definitionen an und erklären Mestres Algorithmus.

Definitionen

Es sei $f(x,z) = a_m x^m + a_{m-1}x^{m-1}z + \ldots + a_0 z^m$ eine homogene, binäre Form vom Grad m mit Koeffizienten a_i in einem algebraisch abgeschlossenen Körper $\overline{\kappa}$. Für ein Element

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

aus $Gl_2(\kappa)$ erklären wir die folgende Operation

$$\begin{aligned} x &\to ax' + bz' \text{ und} \\ z &\to cx' + dz'. \end{aligned}$$

Wir erhalten dann aus $f(x,z)$ eine projektiv äquivalente binäre Form $f(x',z') = f'(x,z)$. Eine **Kovariante** von f ist ein Polynom R in den Koeffizienten a_i und den Variablen x, z von f, so daß für eine beliebige Transformation M in $Gl_2(\overline{k})$ und ein festes $s \in \mathbb{N}$ gilt

$$R(a_0, \ldots, a_m, x, z) = det(M)^s R'(a_0', \ldots, a_m', x', z').$$

Der **Grad** der Kovariante ist der Grad des Polynoms R in x und z. Die **Ordnung** gibt den Grad in den Koffizienten a_i an. Die Zahl s heißt das **Gewicht** der Kovariante.
Eine **Invariante** ist eine Kovariante vom Grad 0. Der Quotient zweier Invarianten gleichen Gewichts führt uns auf eine **absolute Invariante**. Falls zwei Formen projektiv äquivalent sind, stimmen ihre absoluten Invarianten überein. Da wir Kurven bis auf die Isomorphieklasse festlegen möchten, interessieren wir uns vor allem für die komplementäre Frage: Wieviele und welche absoluten Invariante müssen wir bestimmen, um festzustellen, ob zwei binäre Formen projektiv äquivalent sind oder nicht?
Ein wichtiges Hilfsmittel zur Erzeugung von Kovarianten ist die Überschiebung. Mit dieser Operation lassen sich aus der binären Form $f(x, z)$, die selbst eine Kovariante vom Grad m und der Ordnung eins ist, weitere Kovarianten erzeugen.
Die **k-te Überschiebung** zweier binärer Formen g und h vom Grad n und m sei

$$(gh)_k = \frac{(m-k)!(n-k)!}{m!n!}\left(\frac{\partial g}{\partial x}\frac{\partial h}{\partial z} - \frac{\partial g}{\partial z}\frac{\partial h}{\partial x}\right)^k.$$

Falls g und h zwei Kovarianten vom Grad e_1 und e_2 und der Ordnung i_1 und i_2 sind, dann ist die k-te Überschiebung eine Kovariante vom Grad $e_1 + e_2$ und von der Ordnung $i_1 + i_2 - 2k$.
Alle Kovarianten lassen sich durch Überschiebung aus der binären Form $f(x, z)$ gewinnen [6].

Mestres Algorithmus

Da Mestres Algorithmus [32] für unser Verfahren von fundamentaler Bedeutung ist, erklären wir hier kurz das Grundprinzip. Wir verwenden dabei häufiger die oben eingeführte Operation, die Überschiebung binärer Formen.
Es seien q_1, q_2 und q_3 drei binäre quadratische Formen. Durch Anwendung der ersten Überschiebung ergeben sich drei weitere quadratischen Formen

$$q_1^* = (q_2q_3)_1, q_2^* = (q_3q_1)_1 \text{ und } q_3^* = (q_1q_2)_1.$$

Diese genügen der Gleichung

$$\sum_{i,j} A_{ij}q_i^*q_j^* = 0 \tag{1.2}$$

mit $A_{ij} = (q_iq_j)_2$, $1 \le i, j \le 3$.
Die Determinante der Quadrik (1.2) ist

$$R = -(q_1q_2)_1(q_2q_3)_1(q_3q_1)_1.$$

Es sei nun f eine homogene binäre Form vom Grad $2n$. Wir können dann verifizieren ([32],[6], Kapitel 58), daß

$$R^n f = \sum H_{i_1\dots i_n} q_{i1}^* \dots q_{in}^*,$$

wobei

$$H_{i_1\dots i_n} = ((\dots((f, q^*_{i_1})_2, q^*_{i_2})_2, \dots), q^*_{i_n})_2 \text{ mit } \{i_1 \dots i_n\} \in \{1, 2, 3\}.$$

Wir nehmen an, daß $R \neq 0$. Dann beschreibt die Gleichung 1.2 eine reguläre Quadrik Q. Diese läßt sich parametrisieren, d.h. es existiert ein Isomorphismus

$$\varphi : \mathbb{P}_1 \to V(Q), \quad (x, z) \to (a^*_1, a^*_2, a^*_3) = a^*,$$

wobei $Q(a^*) = 0$.
Sei nun (x, z) eine Nullstelle von f in $\mathbb{P}_1$. Dann liegt der Punkt $\varphi((x, z))$ auf der Kurve

$$\sum H_{i_1\dots i_n} q^*_{i1} \dots q^*_{in} = 0.$$

Somit können wir die Nullstellen von f bzw. die Weierstraßpunkte von C mit $H \cap Q$ identifizieren.
Diese Methode erlaubt es nun, zu einer gegebenen binären Form f eine projektiv äquivalente Form f' zu bestimmen, deren Koeffizienten in einer quadratischen Erweiterung des Körpers liegen, über dem die absoluten Invarianten definiert sind.
Falls die quadratischen Formen q_i Kovarianten von f sind, dann sind die A_{ij} und $H_{i_1\dots i_n}$ Invarianten von f.
Nun gilt der folgende Satz (siehe [32]):

Satz 1.1.17. *Sei*

$$C : y^2 = f(x)$$

eine hyperelliptische Kurve und sei κ der Körper, in dem die absoluten Invarianten der homogenisierten Form $f(x, z)$ liegen. Die Kurve C ist genau dann über κ definiert, falls die Quadrik Q einen κ-rationalen Punkte besitzt.

In diesem Fall läßt sich die Quadrik nämlich über κ parametrisieren (siehe [5], Kapitel 1). Wenn wir die Parametrisierung

$$(a^*_1, a^*_2, a^*_3) = (f_1(t), f_2(t), f_3(t))$$

in die Kurve H einsetzen, erhalten wir das Polynom f'.

Bemerkung 1.1.18. Die Quadrik Q hat spätestens nach einer quadratischen Erweiterung einen κ-rationalen Punkt.
Für einen endlichen Körper $\kappa = \mathbb{F}_q, q \neq 2^n$ und eine Quadrik $Q = (a_{ij})$ mit $p \nmid \det(a_{ij})$ gilt, daß Q stets einen $\mathbb{F}_q$-rationalen Punkt hat (siehe [5], Kapitel 3, Aufgabe 1-3). Somit läßt sich hier die Kurve immer über dem Körper definieren, in dem auch die Invarianten liegen.

Die absoluten Invarianten einer hyperelliptischen Kurve C sind nach Torelli auch absolute Invarianten ihrer prinzipal polarisierten Jacobischen Varietät (J_C, E_C). Nach Definition liegen die absoluten Invarianten im Modulkörper von (J_C, E_C).

Sei C eine hyperelliptische Kurve vom Geschlecht zwei, deren Jacobische (J_C, E_C) vom CM-Typ (K, Φ) ist. Alle prinzipal polarisierten Abelschen Varietäten zum CM-Typ (K, Φ) sind ebenfalls Jacobische hyperelliptischer Kurven. Somit sind die absoluten Invarianten erklärt. Aus Bemerkung 1.1.11 folgt nun das nächste Korollar.

Korollar 1.1.19. *Die absoluten Invarianten der hyperelliptischen Kurven, deren Jacobische prinzipal polarisierten Abelschen Varietäten zum CM-Typ* (K, Φ) *sind, liegen alle in* $k_0^* = k_0 K^*$.

Beweis. Sei k_0 der Modulkörper einer Abelschen Varietät vom CM-Typ (K, Φ). Da der Körper $k_0 K^*$ nur vom CM-Typ abhängt, sind auch die Modulkörper aller anderen prinzipal polarisierten Abelschen Varietäten von diesem Typ in k_0^* enthalten. □

Sei $\{(A_i, E_i)\}$ ein Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten des CM-Typs (K, Φ) mit komplexer Multiplikation mit $\mathcal{O}_K$ und j eine absolute Invariante. Die Koeffizienten des Klassenpolynoms

$$H_\Phi^{(j)}(X) = \prod_{A_i} (X - j^{A_i})$$

zu einem festen CM-Typ Φ liegen in K_0^*, d.h. im reellen Teilkörper des Reflexivkörper K^*. Das Produkt der Klassenpolynome aller möglichen CM-Typen zu einem CM-Körper K, ist ein Polynom mit Koeffizienten in $\mathbb{Q}$ (siehe [56], Satz 5.8.).

Bemerkung 1.1.20. Sei J_C die Jacobische einer hyperelliptischen Kurve vom Geschlecht zwei mit komplexer Multiplikation, deren j-Invarianten im Modulkörper k_0^* liegen, und sei $\mathfrak{p}$ ein Primideal vom Grad 1 in k_0^*. Dann können wir J_C über einer quadratischen Erweiterung M/k_0^* definieren, für die ein Primideal $\mathfrak{P} \in \mathcal{O}_M$ vom Grad 1 über $\mathfrak{p}$ existiert. Dies sieht man durch leichte Modifikation des Beweises in [5], Kapitel 3, Aufgabe 1-3.

1.2 Die Grundidee der CM-Methode

Wir beschränken uns hier auf hyperelliptische Kurven, die über einem endlichen Primkörper definiert sind. Wie wir später sehen werden, ist es mit unserem Verfahren aber auch möglich, Kurven über $\mathbb{F}_q = \mathbb{F}_{p^n}$ für kleines n zu konstruieren.
Unsere Konstruktion beschränkt sich auf CM-Körper K, deren größter reeller Teilkörper K_0 Klassenzahl eins und einen monogenen Ganzheitsring (d.h. $\mathcal{O}_{K_0} = \mathbb{Z}[w]$ für ein w) hat.

Der Algorithmus zerfällt in zwei Teile.
Der erste Teil besteht aus Vorberechnungen. Dafür nehmen wir an, daß wir bereits eine Kurve über $\mathbb{F}_p$ gegeben haben, deren Jacobische J_C komplexe Multiplikation mit einer uns bekannten maximalen Ordnung $\mathcal{O}_K$ hat.
Die Isogenie

$$(x, y) \to (x^p, y^p)$$

auf der Kurve induziert einen Endomorphismus π auf der Jacobischen J_C. Der Frobenius-Endomorphismus entspricht einem Element w in $\mathcal{O}_K$.
Es gilt

$$p = w\overline{w} \text{ and}$$
$$\#J_C(\mathbb{F}_p) = \prod_{i=1}^{2g}(1 - \xi w_i) \text{ für eine Einheitswurzel } \xi \in K,$$

wobei $w_1 = w$ und w_i, $i > 1$ die anderen Wurzeln des charakteristischen Polynoms von w sind. Wir nehmen nun an, daß K keinen zyklotomischen Körper enthält. Sei p eine Primzahl, die eine relative Normgleichung erfüllt, d.h.

$$p = w\overline{w}.$$

Dann gilt für alle $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ auch

$$p = w^{\varphi}\overline{w}^{\varphi}.$$

Wenn wir zusätzlich noch die Vorzeichenwahl berücksichtigen, sind dies bereits alle möglichen Lösungen der Normgleichung. Somit gibt es höchstens $2g$ Möglichkeiten für die Gruppenordnung. Die tatsächliche Anzahl hängt vom Zerfällungsverhalten der Primzahl p in der absoluten Körpererweiterung $K/\mathbb{Q}$ ab. Unterschiedliche Lösungen der relativen Normgleichungen können zu identischen Gruppenordnungen führen.
Damit ist klar, wie wir die Gruppenordnung von $J_C(\mathbb{F}_p)$ bestimmen. Wir müssen hierzu nur eine relative Normgleichung bezüglich K/K_0 lösen. Mit einem zufällig gewählten $\mathbb{F}_p$-rationalen Divisor D aus $J_C(\mathbb{F}_p)$ testen wir, welche der möglichen Gruppenordnungen die richtige ist.

Der zweite Teil beschäftigt sich mit der Konstruktion einer hyperelliptischen Kurve über $\mathbb{F}_p$, deren Jacobische komplexe Multiplikation mit einer vorgegebenen Maximalordnung $\mathcal{O}_K$ hat. Er ist der Hauptteil des Algorithmus und meist am zeitaufwendigsten. Allerdings muß dieser Teil nur ein einziges Mal durchlaufen werden, denn wir führen ihn nur aus, falls sich in den Vorberechnungen zeigte, daß die Primzahl p zusammen mit der Ordnung $\mathcal{O}_K$ zu einer kryptographisch geeigneten Gruppenordnung führt.
Wir nehmen also an, daß wir einen CM-Körper K mit $[K : \mathbb{Q}] = 2g$ und eine Primzahl p, die bezüglich K/K_0 eine relative Normgleichung erfüllt, gegeben haben. Außerdem haben wir eine Menge von höchstens $g \cdot d$ Gruppenordnungen, wobei d die Anzahl der Einheitswurzeln ist.
Im Erfolgsfall liefert der Algorithmus eine hyperelliptische Kurve C über $\mathbb{F}_p$, deren Jacobische $J_C(\mathbb{F}_p)$ eine der möglichen Gruppenordnungen hat. Andernfalls erhalten wir die Information, daß keine Kurve gefunden wurde. Wir beschreiben nun die einzelnen Schritte. Die grobe Idee besteht darin, eine Kurve über einem Zahlkörper zu konstruieren und dann bezüglich eines über p liegenden Primideals zu reduzieren.

1. Berechne eine vollständige Menge aller Periodenmatrizen $\{\Omega_i\}$ der einfachen prinzipal polarisierten Abelschen Varietäten über $\mathbb{C}$, die komplexe Multiplikation mit $\mathcal{O}_K$ haben. Jede Periodenmatrix liegt in der Siegelschen oberen Halbebene und beschreibt damit ein Gitter Λ (siehe 1.1.1). Die zugehörige Abelsche Varietät wird durch $\mathbb{C}^g/\Lambda$ beschrieben.

2. Berechne (bis zu einer gegebenen Genauigkeit) alle geraden Thetanullwerte

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega_i, 0) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i (n + \frac{1}{2}\delta)^t \Omega_i (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon)).$$

   mit $\delta^t \epsilon \equiv 0 \mod 2$ für $\delta, \epsilon \in \{0,1\}^g$.
   Dieser Schritt wird für alle Ω_i durchgeführt.

3. Entscheide anhand der Thetanullwerte, ob Ω_i die Periodenmatrix der Jacobischen einer hyperelliptischen Kurve ist oder nicht. Falls keine Periodenmatrix Ω_i hyperelliptisch ist, dann gebe aus, daß zu dem gegebenen CM-Körper und seiner Maximalordnung keine hyperelliptischen Kurven existieren. Sonst fahre mit dem reduzierten Repräsentantensystem, bestehend aus den hyperelliptischen Ω_i, fort.

4. Berechne das Rosenhain-Modell

$$y^2 = x(x-1) \prod_{i=1}^{2g-1} (x - \lambda_i)$$

   einer Kurve über $\mathbb{C}$ deren Jacobische zu Ω_i gehört. Dieses kann aus den Thetanullwerten berechnet werden [62].

5. Nun gibt es mehrere Möglichkeiten:

1. Möglichkeit	**2. Möglichkeit**	**Kombination**
Berechne die erzeugenden absoluten Invarianten $j_1, \ldots, j_{2g-1}$.	Berechne Mestres Invarianten[32].	Berechne $j_1, \ldots, j_{2g-1}$
Reduziere $j_1, \ldots, j_{2g-1} \mod p$.	Reduziere sie mod p.	Reduziere sie mod p. Drücke Mestres Invarianten durch die j_i aus.
Finde eine Kurve mit den entsprechenden j-Invarianten mittels Gröbner-Basen.	Wende Mestres Algorithmus an.	Wende Mestres Algorithmus an.

Die absoluten Invarianten der Kurven in unserem Repräsentantensystem liegen in einem Zahlkörper und sind zueinander konjugiert. Wenn wir ein vollständiges Repräsentantensystem haben, können wir das Minimalpolynom über $\mathbb{Q}$ bestimmen. Reduktion mod p bedeutet dann Reduktion der Koeffizienten des Minimalpolynoms. Die j-Invarianten über $\mathbb{F}_p$ sind die Nullstellen des reduzierten Minimalpolynoms.

Da wir nur an Kurven interessiert sind, die fast prime Gruppenordnung haben, werden wir in der Regel versuchen, die Anzahl der möglichen Gruppenordnungen einzuschränken. Einige Primzahlen lassen weniger mögliche Gruppenordnungen zu als andere. Für $g = 2$ und einen nicht Galoisschen CM-Körper K sind etwa Primzahlen, die in K nicht total zerfallen, besonders günstig. Hier gibt es nur zwei mögliche Ordnungen. Wenn wir in Schritt 5 eine Kurve C gefunden haben, hat entweder die Jacobi-Varietät der Kurve C oder des Twistes $\tilde{C}$ die gewünschte Ordnung (siehe S. 37).

1.3 Verallgemeinerungen

Es stellt sich die Frage, ob man das CM-Verfahren auch für andere Klassen von Kurven anwenden kann. Für Geschlecht $g \geq 3$ enthält das zu Anfang erzeugte Repräsentantensystem auch Jacobische nicht-hyperelliptischer Kurven. Wir stoßen dabei auf eine Reihe von Problemen, bei vielen Punkten bewegen wir uns auf theoretisch unerforschtem Boden:

- Wir können entscheiden, wann eine Periodenmatrix zur Jacobischen einer hyperelliptischen Kurve gehört. Wir haben aber kein Kriterium, wann eine prinzipal polarisierte Abelsche Varietät Jacobische einer nicht-hyperelliptischen Kurve ist. Dies ist ab $g = 4$ ein Problem, da es dann auch prinzipal polarisierte Abelsche Varietäten gibt, die nicht Jacobische von Kurven sind.

- Es gibt keine Formeln, die es uns erlauben aus den Thetanullwerten ein Modell einer nicht-hyperelliptischen Kurve abzuleiten. Insbesondere wissen wir nicht, wie wir aus den Thetanullwerten die Invarianten einer nicht-hyperelliptischen Kurve berechnen können.

- Es sei $\mathfrak{I}$ der Ring der Invarianten einer hyperelliptischen Kurve. Die Invarianten $j_1, \ldots, j_{2g+1}$ einer hyperelliptischen Kurven vom Geschlecht g liegen in $\mathrm{Spec}(\mathfrak{I}(\Delta^{-1}))$, wobei Δ die Diskriminante der Kurve ist [17]. Für $g = 3$ sind zum Beispiel die erzeugenden absoluten Invarianten des Modulraums bekannt ([48]), aber leider nicht von der Form I/Δ für eine Invariante I . Für Computerberechnungen würden wir aber gerne eine geeignete Form wie etwa bei hyperelliptischen Kurven haben, um den Nenner kontrollieren zu können.

- Angenommen, wir hätten nun die Invarianten gegeben und wollten daraus eine Kurve konstruieren. Mestres Algorithmus basiert auf der gut untersuchten Invariantentheorie binärer Formen. Für nicht-hyperelliptische Kurven kennen wir keinen ähnlichen Algorithmus.

Ansätze mit Gröbner-Basen sind hier noch schwieriger, da für die Gleichung einer nicht-hyperelliptischen Kurve mehr Koeffizienten berechnet werden müssen.

Es ist nicht klar, wie man diese Punkte umgehen kann. Ein Algorithmus hingegen, der ohne all diese Schritte auskommt, hat kaum mehr etwas mit der uns bekannten CM-Methode zu tun.

Kapitel 2

Die CM-Methode für Geschlecht zwei

In diesem Kapitel beschreiben wir die CM-Methode für $g = 2$. Wir erklären zunächst alle notwendigen Einzelschritte (die Berechnung der Periodenmatrizen, die Berechnung der Thetanullwerte, die Formeln für Igusas und Mestres Invarianten, Mestres Algorithmus über $\mathbb{F}_p$ und Lösungen relativer Normgleichungen). Dann beschreiben wir in Abschnitt 2.6 den gesamten Algorithmus.
Im Abschnitt 2.7 untersuchen wir die Laufzeit des Algorithmus. Hier findet sich eine Tabelle aller CM-Körper, deren Klassenpolynom wir berechnet haben. Dann geben wir zwei kryptographisch relevante Beispiele (siehe 2.8) an und betrachten einige günstige Primzahlen für den Definitionskörper (siehe 2.9).

2.1 Berechnung der Periodenmatrix

Hier beziehen wir uns auf Spallek, die die Periodenmatrizen und das Repräsentantensystem im Fall $g = 2$ explizit berechnet hat [56].
Jacobische Varietäten hyperelliptischer Kurven vom Geschlecht zwei sind genau die prinzipal polarisierten Abelschen Varietäten der Dimension zwei [35].
Sei $K_0 = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$, ein reell quadratischer Zahlkörper mit Klassenzahl eins. Angenommen $\alpha = a + b\sqrt{d}$ ist quadratfrei und total positiv (d.h. $a \pm b\sqrt{d} > 0$), dann ist $K = \mathbb{Q}(i\sqrt{\alpha})$ ein CM-Körper vom Grad vier über $\mathbb{Q}$. Ein CM-Typ (K, Φ) ist genau dann nicht primitiv, falls K Galoissch mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist.
Sei ϵ_0 eine Fundamentaleinheit von K_0. Wir bezeichnen die Gruppe aller Einheiten mit positiver Norm mit U^+. Die Gruppe U^+ hat eine Untergruppe U_1, die aus den Normeinheiten bezüglich K/K_0 besteht. Falls die Fundamentaleinheit in K_0 negative Norm hat, folgt sofort $U^+ = U_1$.
Da K_0 Klassenzahl eins hat, kann der Ganzheitsring von K in der Form

$$\mathcal{O}_{K_0} + \gamma\mathcal{O}_{K_0}$$

mit $\gamma \in \mathcal{O}_K$ beschrieben werden. Weiter hat jedes Ideal $\mathfrak{A}_j$ in K eine relative Basis

$$\alpha_j \mathcal{O}_{K_0} + \beta_j \mathcal{O}_{K_0}, \quad \alpha_j, \beta_j \in \mathcal{O}_K.$$

Jedes Ideal $\mathfrak{A}_j$ ist zu einem Ideal der Form

$$\mathcal{O}_{K_0} + \tau_j \mathcal{O}_{K_0}, \quad \tau_j = \frac{\alpha_j}{\beta_j} \in \mathcal{O}_K$$

mit Im $\tau_j > 0$ äquivalent. Falls $\epsilon_0 \notin U^+$, wählen wir τ_j so, daß $N_{K,K_0}(\tau_j)$ positiv ist.
Die reelle Konjugation in K_0 besitzt zwei Fortsetzungen nach K. Wir setzen

$$\hat{\sigma}(i\sqrt{\alpha}^+) = i\sqrt{\sigma(\alpha)}^+ \text{ und } \rho\hat{\sigma}(i\sqrt{\alpha}^+) = -i\sqrt{\sigma(\alpha)}^+$$

wobei $\sqrt{a}^+$ die positive Quadratwurzel von $a \in \mathbb{R}$ bezeichnet.
Spallek ([56], Satz 4.7. und 4.8.) zeigte den folgenden Satz:

Satz 2.1.1. *Sei K ein CM-Körper wie oben mit K entweder nicht galoissch über $\mathbb{Q}$ oder mit Galoisgruppe isomorph zu $\mathbb{Z}/4\mathbb{Z}$.*
Weiter sei $K_0 = \mathbb{Z} + \mathbb{Z}w$ der reelle Teilkörper, σ die reelle Konjugation und $\varphi = \rho\hat{\sigma}$.

1. *Ein Repräsentantensystem aller Isomorphieklassen einfacher prinzipal polarisierter Abelscher Varietäten, die komplexe Multiplikation mit $\mathcal{O}_K$ haben, ist gegeben durch*

$$\mathcal{K} = \mathcal{K}_{1,\varphi} \cup \mathcal{K}_{1,\overline{\varphi}} \text{ mit}$$

$$\mathcal{K}_{1,\varphi} = \begin{cases} \{(\tau_j, \tau_j^{\varphi}), (\epsilon_0\tau_j, \epsilon_0\tau_j^{\varphi}) : N_{K,K_0}(\tau_j) \text{ total pos.}\}, & \epsilon_0 \in U_1 \\ \{(\tau_j, \tau_j^{\varphi}) : N_{K,K_0}(\tau_j) \text{ total pos.}\}, & \epsilon_0 \in U^+ - U_1 \\ \{(\tau_j, \tau_j^{\varphi}) : N_{K,K_0}(\tau_j) \text{ total pos.}\}, & \text{sonst.} \end{cases}$$

$$\mathcal{K}_{1,\overline{\varphi}} = \begin{cases} \{\}, & \text{falls } K \text{ Galoissch} \\ \{(\tau_j, \tau_j^{\overline{\varphi}}), (\epsilon_0\tau_j, (\epsilon_0\tau_j)^{\overline{\varphi}}) : N_{K,K_0}(\tau_j) \text{ nicht total pos.}\}, & \epsilon_0 \in U_1 \\ \{(\tau_j, \tau_j^{\overline{\varphi}}) : N_{K,K_0}(\tau_j) \text{ nicht total pos.}\}, & \epsilon_0 \in U^+ - U_1 \\ \{(\epsilon_0\tau_j, \epsilon_0\tau_j^{\varphi}) : N_{K,K_0}(\tau_j) \text{ total pos.}\}, & \text{sonst.} \end{cases}$$

2. *Eine prinzipal polarisierte Abelsche Varietät vom Typ $(K, \{1, \psi\})$ von der Form (s_j, s_j^{ψ}) hat die Periodenmatrix*

$$\Omega_{s_j, s_j^{\psi}} = \frac{1}{w - w^{\sigma}} \begin{pmatrix} w^2 s_j - (w^{\psi})^2 s_j^{\psi} & w s_j - w^{\psi} s_j^{\psi} \\ w s_j - w^{\psi} s_j^{\psi} & s_j - s_j^{\psi} \end{pmatrix}$$

Wie wir in Abschnitt 3.1.1 zeigen, können wir den Fall $\epsilon_0 \in U_1$ ausschließen.

2.2 Berechnung der Thetanullwerte

Nachdem wir die Periodenmatrix Ω erhalten haben, möchten wir die Invarianten der Kurve berechnen, deren Jacobische durch Ω gegeben ist. Dafür verwenden wir die Thetanullwerte

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega, 0) = \sum_{n \in \mathbb{Z}^2} \exp(\pi i (n + \frac{1}{2}\delta)^t \Omega (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon)). \tag{2.1}$$

mit $\delta, \epsilon \in \{0,1\}^2$. Wie bereits erwähnt, verschwinden die ungeraden Thetanullwerte (siehe 1.1.6). Deshalb konzentrieren wir uns auf die geraden Thetanullwerte

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega, 0) \text{ mit } \delta^t \epsilon \equiv 0 \mod 2.$$

Wir erhalten für $g = 2$ genau zehn gerade Thetanullwerte

$$\theta_1 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{0}{0} \end{bmatrix}, \theta_2 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{1}{0} \end{bmatrix}, \theta_3 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{0}{1} \end{bmatrix}, \theta_4 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{1}{1} \end{bmatrix}, \theta_5 := \theta \begin{bmatrix} \binom{1}{0} \\ \binom{0}{0} \end{bmatrix},$$
$$\theta_6 := \theta \begin{bmatrix} \binom{1}{0} \\ \binom{0}{1} \end{bmatrix}, \theta_7 := \theta \begin{bmatrix} \binom{0}{1} \\ \binom{0}{0} \end{bmatrix}, \theta_8 := \theta \begin{bmatrix} \binom{0}{1} \\ \binom{1}{0} \end{bmatrix}, \theta_9 := \theta \begin{bmatrix} \binom{1}{1} \\ \binom{0}{0} \end{bmatrix}, \theta_{10} := \theta \begin{bmatrix} \binom{1}{1} \\ \binom{1}{1} \end{bmatrix}.$$

Wir beschäftigen uns nun mit der Berechnung der Thetanullwerte zu einer gegebenen Genauigkeit. Da wir uns auch für die CM-Methode in höheren Dimensionen interessieren und auch für $g > 2$ die Thetanullwerte berechnen müssen, werden wir für den Rest dieses Abschnitts das Geschlecht g offen lassen.

2.2.1 Der Algorithmus

Der Algorithmus ist eine Verallgemeinerung von Algorithmus (3.15) in [41].
Gegeben eine symmetrische Matrix $A \in Gl(g, \mathbb{R})$ und ein fester Vektor $\epsilon \in (\mathbb{R}^+)^g$, bestimme die Menge aller Vektoren $x \in \mathbb{Z}^k$ mit

$$(x + \epsilon)^t A (x + \epsilon) \leq C \tag{2.2}$$

für eine feste, gegebene Konstante C.
Man bestimme zunächst eine obere Dreiecksmatrix $(q_{ij}) \in Gl(g, \mathbb{R})$ mit folgender Eigenschaft:

$$x^t A x = \sum_{i=1}^{g} q_{ii} (x_i + \sum_{j=i+1}^{g} q_{ij} x_j)^2$$

für alle $x \in \mathbb{R}^g$ (siehe [41]).
Falls $x \in \mathbb{Z}^g$ die Bedingung (2.2) erfüllt, dann gilt für alle i mit $g \geq i \geq 1$

$$q_{ii} \left((x_i + \epsilon_i) + \sum_{j=i+1}^{g} q_{ij} (x_j + \epsilon_j) \right)^2 \leq C - \sum_{\nu=i+1}^{g} q_{\nu\nu} \left(x_\nu + \epsilon_\nu) + \sum_{j=\nu+1}^{g} q_{\nu j} (x_j + \epsilon_j) \right)^2 =: T_i$$

Also bestimmen wir für jedes $x_g \in \mathbb{Z}$ mit

$$|x_g| \leq (c/q_{gg})^{\frac{1}{2}} - \epsilon_g, \text{ falls } x_g \text{ positiv, und}$$
$$|x_g| \leq (c/q_{gg})^{\frac{1}{2}} + \epsilon_g, \text{ falls } x_g \text{ negativ,}$$

alle Möglichkeiten für x_{g-1}. So bestimmen wir suzkessive x_i für $i = g-1, \ldots, 1$. Für festes $x_{i+1}, \ldots, x_g \in \mathbb{Z}$ mit

$$\sum_{\nu=i+1}^{g} q_{\nu\nu}(x_\nu + \epsilon_\nu) + \sum_{j=\nu+1}^{g} (q_{\nu j}(x_j + \epsilon_j))^2 \leq T_{i+1}$$

erhalten wir alle Möglichkeiten für x_i durch die Ungleichung

$$-(T_i/q_{ii})^{\frac{1}{2}} - U_i - \epsilon_i \leq x_i \leq (T_i/q_{ii})^{\frac{1}{2}} - U_i - \epsilon_i$$
$$\text{mit } U_i := \sum_{j=i+1}^{g} q_{ij}x_j \text{ für } g-1 \geq i \geq 1.$$

Damit ergibt sich der folgende Algorithmus:

Algorithmus zur Lösung von $Q(\mathbf{x}+\epsilon) \leq C$

Input: Matrix (q_{ij}), Konstante C, Vektor $\epsilon \in (\mathbb{R}^+)^g$.
Output: $\mathbf{x} \in \mathbb{Z}^g$, $\mathbf{x} \neq 0$ mit $Q(\mathbf{x}+\epsilon) \leq C$

(Initialisierung) Vektoren für T_i, U_i, x_i und $OS(x_i)$
$i := k; T_i := C; U_i := 0;$
while $i \leq g$ **do**
  bool_value:=TRUE;
  $Z := (T_i/q_{ii})^{\frac{1}{2}};$
  $OS(x_i) := \lfloor Z - U_i - \epsilon_i \rfloor;$
  $x_i := \lceil -Z - U_i - \epsilon_i \rceil - 1;$
  while bool_value=TRUE AND $i \leq$groesse **do**
    $x_i := x_i + 1;$
    if $(x_i \leq OS(x_i))$ **then**
      if i=1 **then**
        Ausgabe x;
      else
        $i := i - 1;$
        $U_i := \sum_{j=i+1}^{g} q_{ij}(x_j + \epsilon_j);$
        $T_i := T_{i-1} - q_{i+1,i+1}(x_{i+1} + \epsilon_{i+1} + U_{i+1});$
        bool_value:=FALSE;
      end if
    else

$i := i + 1;$
end if
end while
end while

Bemerkung 2.2.1. Der Algorithmus läuft auch für beliebiges $\epsilon \in \mathbb{R}^g$ korrekt, aber dies ist für unsere Zwecke (Berechnung der Thetanullwerte) uninteressant.

2.2.2 Berechnung der Schranke C für die Thetanullwerte

Wir wollen die Thetanullwerte mit einer Genauigkeit von s Nachkommastellen berechnen. Dazu müssen wir ein C bestimmen, so daß

$$\left| \sum_{\substack{n\in\mathbb{Z}^g \\ (n+\frac{1}{2}\delta)^t \mathrm{Im}\ \Omega(n+\frac{1}{2}\delta)>C}} \exp(\pi i((n+\frac{1}{2}\delta)^t\Omega(n+\frac{1}{2}\delta)+2(n+\frac{1}{2}\delta)^t(\frac{1}{2}\epsilon))) \right| \leq 10^{-s}$$

ist. Um $\theta\left[\begin{smallmatrix}\delta\\ \epsilon\end{smallmatrix}\right](\Omega,0)$ mit Fehlergenauigkeit kleiner gleich 10^{-s} zu bestimmen, müssen wir dann nur alle Vektoren $n \in \mathbb{Z}^g$ mit $(n+\frac{1}{2}\delta)^t \mathrm{Im}\ (n+\frac{1}{2}\delta) \leq C$ mit dem Algorithmus in Abschnitt 2.2.1 aufzählen.
Es gilt

$$\begin{aligned}
&\left| \sum_{\substack{n\in\mathbb{Z}^g \\ (n+\frac{1}{2}\delta)^t \mathrm{Im}\ \Omega(n+\frac{1}{2}\delta)>C}} \exp(\pi i((n+\frac{1}{2}\delta)^t\Omega(n+\frac{1}{2}\delta)+2(n+\frac{1}{2}\delta)^t(z+\frac{1}{2}\epsilon))) \right| \\
&\leq \sum_{\substack{n\in\mathbb{Z}^g \\ (n+\frac{1}{2}\delta)^t \mathrm{Im}\ \Omega(n+\frac{1}{2}\delta)>C}} |\exp(-\pi(n+\frac{1}{2}\delta)^t \mathrm{Im}\ \Omega(n+\frac{1}{2}\delta))| \\
&\leq \sum_{m=C}^{\infty} \mu(m)\exp(-\pi m),
\end{aligned}$$

wobei

$$\mu(m) = \#\{n \in \mathbb{Z}^g : m < (n+\frac{1}{2}\delta)^t \mathrm{Im}\ \Omega(n+\frac{1}{2}\delta) \leq m+1\}.$$

Um die Größenordnung festzulegen, bedienen wir uns der Volumenheuristik:

$$\mu(m) \simeq \frac{\mathrm{Vol}\ (K_g(m))}{(\min\Omega)^g}$$

mit $K_g(m) = \{z \in \mathbb{C}^g : m \leq \|z\| \leq m+1\}$ und $\min\Omega = \min_{g\in\mathbb{Z}^g}\{g^t(\mathrm{Im}\ \Omega)g\}$. Die Größe $\min\Omega$ bezeichnet also das erste sukzessive Minimum der positiv definiten Matrix $\mathrm{Im}\ \Omega$.

Wir können das Volumen von $K_g(m)$ über das Volumen der g-dimensionalen Kugel berechnen und erhalten folgende grobe Abschätzungen für $m \geq 5$:

$$\text{Vol}\,(K_g(m)) \leq \begin{cases} 7m & \text{für } g = 2 \\ 17m^2 & \text{für } g = 3 \\ 30m^3 & \text{für } g = 4. \end{cases}$$

Wir widmen uns nun getrennt den Fällen $g = 2$ und 3.

Der Fall $g = 2$

Hier haben wir

$$\sum_{m=C}^{\infty} \mu(m) \exp(-\pi m) \simeq \frac{1}{(\min \Omega)^2} \sum_{m=C}^{\infty} \frac{7m}{\exp(\pi m)}$$
$$= \frac{7}{(\min \Omega)^2} \sum_{m=C}^{\infty} m x^{-m} \quad \text{mit } x = \exp(\pi).$$

Wir können die Summe $\sum_{m=C}^{\infty} m x^{-m}$ mit $x = \exp(\pi)$ durch das Integral $|\int_{C-1}^{\infty} m x^{-m}|$ abschätzen, da die Funktion $f(x) = x \exp(-\pi x)$ für $x \geq 1$ monoton fallend ist.
Wir erhalten so mit $x = \exp(\pi)$:

$$\frac{7}{(\min \Omega)^2} \sum_{m=C}^{\infty} m x^{-m} = \frac{7}{(\min \Omega)^2} \int_{m=C-1}^{\infty} m x^{-m} dm$$
$$= \frac{7}{(\min \Omega)^2} \left((C-1) \frac{\exp(-\pi(C-1))}{\pi} + \frac{1}{\pi^2} \exp(-\pi(C-1) \right)$$
$$< \frac{7}{(\min \Omega)^2} \left(\frac{C}{\pi} \exp(-\pi(C-1)) \right) < \frac{2,3}{(\min \Omega)^2} \exp(-\frac{3}{4}\pi C),$$

falls $C \exp(-\pi(C-1)) < \exp(-\frac{3\pi}{4} C)$, also $C \geq 7$.
Falls $C \geq 75$ können wir die Summe sogar durch $\frac{2,3}{\min \Omega} \exp(-\frac{29}{30}\pi C)$ abschätzen.
Damit der Fehler kleiner als 10^{-s} ist, muß nun

$$\frac{2,3}{(\min \Omega)^2} \exp(-\frac{3}{4}\pi C) < 10^{-s}$$

sein. Daraus erhalten wir eine grobe Abschätzung für C:

$$C > (s + 0,35 - 2 \log_{10}(\min \Omega)).$$

Diese läßt sich für $C \geq 75$ noch zu

$$C > \frac{3}{4}(s + 0,35 - 2 \log_{10}(\min \Omega))$$

verbessern. Es ist plausibel, daß eine Formel für C immer vom ersten sukzessiven Minimum $\min \Omega$ abhängen sollte.

Der Fall $g = 3$

Das Integral $\int_{m=C-1}^{\infty} m^2 x^{-m} dm$ können wir für $C \geq 10$ durch $\frac{1}{\pi^2}\exp(-\frac{3}{4}\pi C)$ abschätzen. Wir erhalten so

$$C > (s + 0,75 - 3\log_{10}(\min\Omega))$$

und für $C \geq 122$ mit der gleichen Überlegung wie oben

$$C > \frac{3}{4}(s + 0,75 - 3\log_{10}(\min\Omega)).$$

2.3 Igusas und Mestres Invarianten

Da wir in der Literatur oft fehlerhafte Angaben gefunden haben, führen wir hier Igusas und Mestres Invarianten nochmals ein.
Durch die zehn geraden Thetanullwerte können wir die drei j-Invarianten der zu Ω gehörigen hyperelliptischen Kurve berechnen. Zunächst definieren wir die Werte h_4, h_{10}, h_{12} und h_{16}, die von Modulformen vom Gewicht 4, 10, 12 und 16 kommen:

$$h_4 := \sum_{i=1}^{10} \theta_i^8, \quad h_{10} := \prod_{i=1}^{10} \theta_i^2,$$
$$\begin{aligned} h_{12} :=\ & (\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10})^4 + (\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3)^4 + (\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 + (\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7)^4 \\ & + (\theta_1\theta_5\theta_2\theta_{10}\theta_3\theta_7)^4 + (\theta_1\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4 + (\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_4)^4 + (\theta_1\theta_5\theta_9\theta_8\theta_3\theta_4)^4 \\ & + (\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4 + (\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + (\theta_1\theta_2\theta_9\theta_6\theta_7\theta_4)^4 + (\theta_1\theta_5\theta_6\theta_8\theta_7\theta_4)^4 \\ & + (\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4 + (\theta_5\theta_2\theta_9\theta_3\theta_7\theta_4)^4 + (\theta_1\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4, \end{aligned}$$

$$h_{16} := \theta_8^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_8\theta_{10})^4 + \theta_5^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_8\theta_3)^4 + \theta_{10}^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_3)^4 + \theta_3^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_3)^4$$
$$+ \theta_1^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 + \theta_2^4(\theta_5\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 + \theta_1^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7)^4 + \theta_9^4(\theta_5\theta_2\theta_9\theta_6\theta_8\theta_3\theta_7)^4$$
$$+ \theta_9^4(\theta_1\theta_5\theta_2\theta_9\theta_{10}\theta_3\theta_7)^4 + \theta_6^4(\theta_1\theta_5\theta_2\theta_6\theta_{10}\theta_3\theta_7)^4 + \theta_5^4(\theta_1\theta_5\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_2^4(\theta_1\theta_2\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4$$
$$+ \theta_6^4(\theta_1\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_8^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_{10}^4(\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_3^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4$$
$$+ \theta_7^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_7)^4 + \theta_7^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3\theta_7)^4 + \theta_9^4(\theta_1\theta_5\theta_2\theta_9\theta_8\theta_{10}\theta_4)^4 + \theta_6^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_4)^4$$
$$+ \theta_2^4(\theta_1\theta_5\theta_2\theta_9\theta_8\theta_3\theta_4)^4 + \theta_6^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_3\theta_4)^4 + \theta_1^4(\theta_1\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4 + \theta_2^4(\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4$$
$$+ \theta_1^4(\theta_1\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_5^4(\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_9^4(\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_8^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4$$
$$+ \theta_{10}^4(\theta_1\theta_5\theta_9\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_3^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_5^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_7\theta_4)^4 + \theta_2^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_7\theta_4)^4$$
$$+ \theta_9^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_7\theta_4)^4 + \theta_8^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_7\theta_4)^4 + \theta_1^4(\theta_1\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_5^4(\theta_5\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4$$
$$+ \theta_6^4(\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_{10}^4(\theta_1\theta_2\theta_9\theta_6\theta_{10}\theta_7\theta_4)^4 + \theta_{10}^4(\theta_1\theta_5\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_1^4(\theta_1\theta_5\theta_2\theta_9\theta_3\theta_7\theta_4)^4$$
$$+ \theta_6^4(\theta_5\theta_2\theta_9\theta_6\theta_3\theta_7\theta_4)^4 + \theta_8^4(\theta_5\theta_2\theta_9\theta_8\theta_3\theta_7\theta_4)^4 + \theta_5^4(\theta_1\theta_5\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_2^4(\theta_1\theta_2\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4$$
$$+ \theta_9^4(\theta_1\theta_9\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_8^4(\theta_1\theta_6\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_{10}^4(\theta_5\theta_2\theta_9\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_3^4(\theta_1\theta_2\theta_9\theta_6\theta_3\theta_7\theta_4)^4$$
$$+ \theta_3^4(\theta_1\theta_5\theta_6\theta_8\theta_3\theta_7\theta_4)^4 + \theta_3^4(\theta_2\theta_9\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_7^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_7^4(\theta_1\theta_5\theta_9\theta_8\theta_3\theta_7\theta_4)^4$$
$$+ \theta_7^4(\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_7^4(\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_4^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_4)^4 + \theta_4^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3\theta_4)^4$$
$$+ \theta_4^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_4^4(\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7\theta_4)^4 + \theta_4^4(\theta_1\theta_5\theta_2\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_4^4(\theta_1\theta_9\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4.$$

Wir erhalten die Invarianten I_2, I_4, I_6, I_{10}:

$$I_2 := \frac{h_{12}}{h_{10}}, \quad I_4 := h_4, \quad I_6 := \frac{h_{16}}{h_{10}} \text{ und } I_{10} := h_{10}.$$

Von diesen Invarianten lassen sich die absoluten Invarianten j_1', j_2' und j_3' ableiten. Sie sind rationale Erzeugende des Körpers der absoluten Invarianten. Zwei prinzipal polarisierte Abelsche Varietäten (mit $I_2 \neq 0$) sind genau dann isomorph, wenn sie die gleichen j'-Invarianten haben. Nach Igusa [21] definieren wir

$$j_1' := \frac{I_2^5}{I_{10}}, \quad j_2' := \frac{I_4 I_2^3}{I_{10}} \text{ und } j_3' := \frac{I_6 I_2^2}{I_{10}}.$$

Wir können nun die absoluten Invarianten für Mestres Algorithmus durch j_1', j_2', j_3' ausdrücken. Wir folgen Mestres Notation und setzen

$$j_1 = \frac{A^5}{D}, j_2 = \frac{A^3 B}{D} \text{ und } j_3 = \frac{A^2 C}{D},$$

wobei A, B, C, D Mestres Invarianten vom Grad 2, 4, 6 und 10 sind (siehe [32]). Die Invarianten A, B, C, D sind nicht mit den Igusa Invarianten I_2, I_4, I_6, I_{10} identisch. Die absoluten Invarianten j_1, j_2, j_3 sind auch rationale Erzeugende von $\mathbb{Q}(j_1', j_2', j_3')$.
Wir erhalten folgende Transformationsformeln

$$j_1 = -\frac{j_1'}{120^5}, \quad j_2 = \frac{720 j_1}{6750} - \frac{j_2'}{120^3 \cdot 6750} \text{ und}$$
$$j_3 = \frac{j_3'}{120^2 \cdot 2025100} + \frac{1080 j_2}{2025} - \frac{16 j_1}{375}.$$

Da $\alpha = \frac{D}{I_{10}}$ eine absolute Invariante ist, können wir sie auch durch j_i ausdrücken:

$$\alpha = -\frac{1}{4556250}\left(\frac{1}{j_1} + 62208\right) + \frac{16j_2}{75j_1} + \frac{16j_3}{45j_1} - 2\frac{j_2^2}{3j_1^2} - \frac{4j_2j_3}{3j_1^2}.$$

Wir normalisieren Mestres Invarianten Q_{ij} und $H_{l_1,\dots,l_3}$, damit sie zu absoluten Invarianten werden.

$$\begin{gathered}
Q'_{11} = \tfrac{Q_{11}}{A^3} = \tfrac{(2j_3+\frac{1}{3}j_2)}{j_1},\\
Q'_{12} = \tfrac{Q_{12}}{A^4} = \tfrac{2}{3}\tfrac{j_2^2+j_1j_3}{j_1^2},\\
Q'_{13} = Q'_{22} = \tfrac{Q_{13}}{A^5} = \alpha,\\
Q'_{23} = \tfrac{Q_{23}}{A^6} = \tfrac{1}{j_1^2}(\tfrac{j_2^3}{3j_1} + \tfrac{4j_2j_3}{9} + \tfrac{2j_3^2}{3}),\\
Q'_{33} = \tfrac{Q_{33}}{A^7} = \tfrac{1}{j_1^2}(\tfrac{j_1j_2\alpha}{2} + \tfrac{2j_2^2j_3}{9j_1} + \tfrac{2j_3^2}{9}),\\
H'_{111} = \tfrac{H_{111}}{A^5} = \tfrac{2}{9}\tfrac{j_1^2j_3-6j_1j_2j_3+9j_1^2}{j_1^2},\\
H'_{112} = \tfrac{H_{112}}{A^6} = \tfrac{1}{9}\tfrac{2j_2^3+4j_1j_2j_3+12j_1j_3^2+3j_1^2}{j_1^3},\\
H'_{113} = H'_{122} = \tfrac{H_{113}}{A^7} = \tfrac{1}{9}\tfrac{j_2^3+4/3j_1j_2j_3+4j_2^2j_3+6j_1j_3^2+3j_1j_2}{j_1^3},\\
H'_{123} = \tfrac{H_{123}}{A^6} = \tfrac{1}{18j_1^3}2\tfrac{j_2^4}{j_1} + 4j_2^2j_3 + \tfrac{4j_1j_3^2}{3} + 4j_2j_3^2 + 3j_1j_2 + 12j_1j_3,\\
H'_{133} = \tfrac{H_{133}}{A^7} = \tfrac{1}{18j_1^3}(\tfrac{j_2^4}{j_1} + \tfrac{4j_2^2j_3}{3} + \tfrac{16j_2^3j_3}{3j_1} + \tfrac{26j_2j_3^2}{3} + 8j_3^3 + 3j_2^2 + 2j_1j_3),\\
H'_{222} = \tfrac{H_{222}}{A^6} = \tfrac{1}{9j_1^3}(3\tfrac{j_2^4}{j_1} + 6j_2^2j_3 + \tfrac{8}{3}j_1j_3^2 + 2j_2j_3^2 - 3j_1j_3),\\
H'_{223} = \tfrac{H_{223}}{A^7} = \tfrac{1}{18j_1^3}(-\tfrac{2j_2^3j_3}{3j_1} - \tfrac{4j_2j_3^2}{3} - 4j_3^3 + 9j_2^2 + 8j_1j_3),\\
H'_{233} = \tfrac{H_{233}}{A^8} = \tfrac{1}{18j_1^3}(\tfrac{j_2^5}{j_1^2} + 2\tfrac{j_2^3j_3}{j_1} + \tfrac{8}{9}j_2j_3^2 + \tfrac{2j_2^2j_3^2}{3j_1} - j_2j_3 + 9j_1),\\
H'_{333} = \tfrac{H_{333}}{A^9} = \tfrac{1}{36j_1^3}(-2\tfrac{j_2^4j_3}{j_1^2} - 4\tfrac{j_2^2j_3^2}{j_1} - \tfrac{16}{9}j_3^3 - \tfrac{4j_2j_3^3}{j_1} + 9\tfrac{j_2^3}{j_1} + 12j_2j_3 + 20j_3^2).
\end{gathered}$$

Ab nun schreiben wir Q_{ij} und H_{ijk} anstatt Q'_{ij} und H'_{ijk}.

2.4 Mestres Algorithmus über endlichen Körpern

Wir haben Mestres Algorithmus in Abschnitt 1.1.7 beschrieben und erläutern hier noch kurz die Vorgehensweise für $\kappa = \mathbb{F}_q$.

Angenommen wir haben die drei j-Invarianten $\tilde{j}_1, \tilde{j}_2, \tilde{j}_3 \in \mathbb{F}_q$. Wir berechnen Mestres Invarianten

$$\begin{aligned} &Q_{11}, Q_{12}, Q_{13} = Q_{22}, Q_{23}, Q_{33} \quad \text{und} \\ &H_{111}, H_{112}, H_{113}, H_{123}, H_{133}, H_{222}, H_{223}, H_{233}, H_{333}, \end{aligned}$$

die die Koeffizienten einer Quadrik Q, bzw. einer Kubik H

$$Q: \quad \sum_{1 \le i \le j \le 3} Q_{ij} x_i x_j \text{ und} \quad H: \sum_{1 \le i \le j \le k \le 3} H_{ijk} x_i x_j x_k$$

sind. Wir würden die Quadrik nun gerne durch Polynome

$$(f_1(t), f_2(t), f_3(t))$$

parametrisieren. Dazu transformieren wir sie auf eine Normalform

$$Q': \quad Q'_{11} x_1^2 + Q'_{22} x_2^2 + Q'_{33} x_3^2. \tag{2.3}$$

Hier können wir leicht eine Lösung und schließlich eine Parametrisierung finden. Aus einer Parametrisierung von Q' erhalten wir die Parametrisierung von Q.
Wir setzen die Lösung in die Kubik ein

$$\sum_{i \le j \le k} H_{ijk} f_i(t) f_j(t) f_k(t) =: f(t)$$

und erhalten so ein Modell $y^2 = f(t)$ der hyperelliptischen Kurve über $\mathbb{F}_q$.
Das Polynom $f(t)$ hat Grad sechs. Cantors Algorithmus ist leichter zu implementieren als die Arithmetik in der Infrastruktur. Deshalb würden wir eine Darstellung vom Grad fünf bevorzugen. Die hyperelliptische Kurve

$$C_f : y^2 = f(t), \quad \deg f = 6$$

hat genau dann ein Modell der Form

$$C_g : y^2 = g(t), \quad \deg g = 5,$$

wenn C_f einen $\mathbb{F}_q$-rationalen Weierstraß-Punkt besitzt. Dies bedeutet einfach, daß $f(t)$ in $\mathbb{F}_q$ eine Nullstelle besitzt. Durch eine projektive Transformation können wir diesen in den unendlich fernen Punkt schieben. Wir erhalten dann ein Polynom vom Grad fünf.
Es gibt $q^6 - q^5$ Polynome vom Grad 6 mit nicht-verschwindender Diskriminante. Davon

haben $\frac{1}{144}(-24q - 3q^3 + 10q^2 + 91q^6 + 43q^4 - 117q^5)$ eine $\mathbb{F}_q$-rationale Nullstelle. Der Quotient

$$\frac{-24q - 3q^3 + 10q^2 + 91q^6 + 43q^4 - 117q^5}{144(q^6 - q^5)}.$$

gibt uns einen Näherungswert für den Anteil der Kurven, die ein Modell mit einem Polynom vom Grad 5 erlauben.
Der vollständige Algorithmus sieht nun wie folgt aus:

Berechnung der Kurve aus ihren j-Invarianten

Input: $j_1, j_2, j_3 \in \mathbb{F}_q$
Output: Eine hyperelliptische Kurve der Form $y^2 = f(t)$ mit $f(t) \in \mathbb{F}_q[t]$, $\deg(f) = 5$ oder 6.

1: Berechne Mestres Invarianten Q_{ij}, H_{ijk} aus den j-Invarianten $j_i, i = 1, \ldots, 3$.
2: Parametrisiere die Quadrik (Q_{ij}) durch $(f_1(t), f_2(t), f_3(t))$.
3: Erhalte $f(t) := \sum_{i \le j \le k} H_{ijk} f_i(t) f_j(t) f_k(t) \in \mathbb{F}_p[t]$.
4: Transformiere f in ein Polynom vom Grad fünf, falls dies möglich ist.
5: Gebe $y^2 = f(t)$ aus.

2.5 Relative Normgleichungen

In diesem Abschnitt geben wir eine elementare Methode an, um für einen gegebenen CM-Körper eine geeignete Primzahl p mit der Eigenschaft

$$w\overline{w} = p \tag{2.4}$$

für ein $w \in \mathcal{O}_K$ zu finden. Die Gleichung (2.4) ist eine relative Normgleichung bezüglich der relativen Körpererweiterung K/K_0. Die ganze Zahl w nennen wir eine **Weil-Zahl** bezüglich p. Wir können also auch zufällig Primzahlen wählen und die relative Normgleichung mit der Pari-Bibliothek lösen, indem wir die Funktion

$$< bnfisintnorm >$$

auf p^2 anwenden. Die Primzahlen, die wir auf diese Weise finden, werden von ganz allgemeiner Form sein. Allerdings benötigt diese Funktion tiefliegende Bausteine aus der algorithmischen Zahlentheorie, z.B. Klassengruppen. Es ist aber durchaus denkbar, daß wir, nachdem alle möglichen Klassenpolynome berechnet und abgespeichert wurden, mit einer kleineren Bibliothek (etwa NTL) auskommen möchten. Dann wünschen wir uns einen elementaren Algorithmus, um eine Primzahl der Form (2.4) zu finden.

Angenommen, die Weil-Zahl w ist ein Element in der Ordnung $\mathcal{O} = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$ mit

$$\eta = i\sqrt{a + b\sqrt{d}}$$

bzw.

$$\eta = i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})}.$$

Beachte, daß die Ordnung $\mathcal{O}$ nicht die maximale Ordnung in K sein muß.

Es sei D die Diskriminante des reellen Teilkörpers K_0.
Wir betrachten zunächst den Fall $D \equiv 0 \mod 4$.
Setze $p = w\overline{w}$ und

$$w = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})i\sqrt{a + b\sqrt{d}}.$$

Wir erhalten zwei Gleichungen für c_1, c_2, c_3 und c_4:

$$\begin{aligned} c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3c_4bd &= p \text{ und} \\ 2c_1c_2 + 2c_3c_4a + c_3^2 b + c_4^2 bd &= 0. \end{aligned}$$

Daraus leiten wir den folgenden Algorithmus ab:

Weilzahlen für $D \equiv 0 \mod 4$

Input: CM-Körper $K = \mathbb{Q}(i\sqrt{a + b\sqrt{d}})$.
Output: Eine Primzahl p, die eine relative Normgleichung erfüllt und die zwei zugehörigen Gruppenordnungen.

1: Wähle zufällig c_3, c_4[1], $(c_3, c_4) = 1$.
2: **if** $c_3^2 b - c_4^2 db \not\equiv 0 \mod 2$ **then**
3: Beginne noch einmal.
4: **end if**
5: Setze $2n := -2c_3c_4a - c_3^2 b - c_4^2 bd$.
6: Setze $c_1 := q$ mit $q \mid n$.
7: $c_2 := n/q$;
8: $p := c_1^2 + c_2^2 d + c_3^2 a + c_4^2 da + 2c_3c_4bd$;
9: **if** p ist nicht prim **then**
10: Beginne noch einmal.
11: **end if**
12: Setze die beiden möglichen Gruppenordnungen auf $(p+1)^2 \pm 4(p+1)c_1 + 4(c_1^2 - c_2^2 d)$.

Der Algorithmus für $D \equiv 1 \mod 4$ basiert auf der gleichen Idee.

Weilzahlen für $D \equiv 1 \mod 4$

Input: CM-Körper $K = \mathbb{Q}\left(i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})}\right)$.

[1]Falls c_3, c_4 ungefähr 12 Dezimalstellen haben, dann wird p ungefähr 25 Dezimalstellen haben.

Output: Eine Primzahl p, die eine relative Normgleichung erfüllt, und die zwei zugehörigen Gruppenordnungen.

1: Wähle c_3, c_4 zufällig, $(c_3, c_4) = 1$.
2: $n := 2c_3c_4a - c_4^2a + c_3^2b - 2c_3c_4b + (\frac{d+3}{4})bc_4^2$;
3: **if** $n \mod 4 \equiv 2$ **then**
4: Beginne noch einmal.
5: **end if**
6: **if** n gerade **then**
7: c_2 :=gerade Teiler von n;
8: **else**
9: c_2 :=ungerade Teiler von n;
10: **end if**
11: $c_1 := \frac{1}{2}(-\frac{n}{c_2} + c_2)$;
12: $p := c_1^2 + c_2^2(\frac{d-1}{4}) + c_3^2a + c_4^2a(\frac{d-1}{4}) + 2c_3c_4b(\frac{d-1}{4}) - bc_4^2(\frac{d-1}{4})$;
13: **if** p ist nicht prim **then**
14: Beginne noch einmal.
15: **end if**
16: Setze die zwei möglichen Gruppenordnungen auf $(p+1)^2 \pm (p+1)(4c_1 - 2c_2) + 4(c_1^2 - c_1c_2 + c_2^2(\frac{1-d}{4}))$.

Der Algorithmus findet nur eine mögliche Lösung w für die Normgleichung $p = w\overline{w}$. Da das Vorzeichen von w nicht festgelegt ist, ergeben sich zwei mögliche Gruppenordnungen. Wenn K nicht Galoissch ist und p in K total zerfällt, kann es zwei verschiedene Lösungen für die Normgleichung und vier verschiedene Möglichkeiten für die Gruppenordnung (siehe 3.1.8) geben. Unser Algorithmus findet aber nur eine Lösung.
Diese elementare Methode ist nicht immer schneller als die Anwendung der Pari-Funktion $< bnfisintnorm >$. In Schritt 6 sollte man die Zahl n nicht vollständig faktorisieren, sondern nur teilweise bis zu einer vorgegebenen Schranke. So erreicht man effiziente Laufzeiten.
Die Tabelle gibt die Zeit (in Sekunden) an, die wir benötigten, um in ausgewählten CM-Körpern 1000 Primzahlen zu finden, die einer relativen Normgleichung genügen. Für das Programm, das zufällig Primzahlen wählt und prüft, ob diese eine relative Normgleichung bezüglich K/K_0 erfüllen, ist es wesentlich, wie hoch die Dichte von Primzahlen mit dieser Eigenschaft ist. Dies spielt für unseren elementaren Ansatz keine Rolle und schlägt sich dort deshalb auch nicht in der Laufzeit nieder.

Laufzeit, um 1000 Primzahlen zu finden, die eine relative Normgleichung bezgl. K/K_0 erfüllen		
CM-Körper	Elementares Programm	<bnfisintnorm>
$\mathbb{Q}(i\sqrt{2+\sqrt{2}})$	247	296
$\mathbb{Q}(i\sqrt{3+\sqrt{2}})$	256	371
$\mathbb{Q}(i\sqrt{4+\sqrt{2}})$	252	394
$\mathbb{Q}(i\sqrt{29+6\sqrt{23}})$	302	403
$\mathbb{Q}(i\sqrt{3+\frac{-1+\sqrt{5}}{2}})$	243	328
$\mathbb{Q}(i\sqrt{4+\frac{-1+\sqrt{5}}{2}})$	241	424
$\mathbb{Q}(i\sqrt{5+\frac{-1+\sqrt{5}}{2}})$	240	429
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{5}}{2}})$	235	208
$\mathbb{Q}(i\sqrt{55+4\frac{-1+\sqrt{53}}{2}})$	285	378
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{73}}{2}})$	263	424
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{89}}{2}})$	268	197
$\mathbb{Q}(i\sqrt{7+\frac{-1+\sqrt{101}}{2}})$	257	303
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{113}}{2}})$	266	435
$\mathbb{Q}(i\sqrt{7+\frac{-1+\sqrt{113}}{2}})$	257	353
$\mathbb{Q}(i\sqrt{9+\frac{-1+\sqrt{141}}{2}})$	292	356
$\mathbb{Q}(i\sqrt{9+\frac{-1+\sqrt{269}}{2}})$	288	186

2.6 Der vollständige Algorithmus

Bevor wir mit der Konstruktion einer hyperelliptischen Kurve starten, müssen wir einen CM-Körper fixieren und eine geeignete Primzahl finden.

Vorberechnung für die Gruppenordnung

1: Wähle einen CM-Körper $K = \mathbb{Q}\left(i\sqrt{a+b\sqrt{d}}\right)$.
2: Suche eine Primzahl p, für die es ein $w \in K$ gibt, so daß

$$w\overline{w} = p.$$

3: Berechne die zwei (bzw. vier) möglichen Gruppenordnungen n_1, n_2 (bzw. n_3, n_4) abhängig von p und $\mathcal{O}_K$.
4: **if** n_1 und n_2 haben keinen großen Primfaktor **then**
5: Gehe zurück zu 2.
6: **else**

7: Gebe K, p, n_1, n_2 (n_3 und n_4) aus.
8: **end if**

Der nächste Schritt ist der eigentliche Konstruktionsalgorithmus. Wir nehmen an, daß wir einen CM-Körper K und eine passende Primzahl p gefunden haben. Nun müssen wir eine hyperelliptische Kurve über $\mathbb{F}_p$ konstruieren, die komplexe Multiplikation mit $\mathcal{O}_K$ hat.

Konstruktion hyperelliptischer Kurven

Input: CM-Körper K mit $h_{K_0} = 1$, eine Primzahl p und die zwei (bzw. vier) möglichen Gruppenordnungen n_1 und n_2 (bzw. n_3, n_4).

Output: Eine hyperelliptische Kurve der Form $y^2 = f(t)$ mit $f(t) \in \mathbb{F}_p[t]$, $\deg(f) = 5$ oder 6.

1: Bestimme ein vollständiges Repräsentantensystem von Periodenmatrizen Ω_i aller Isomorphieklassen einfacher prinzipal polarisierter Abelscher Varietäten, die komplexe Multiplikation mit $\mathcal{O}_K$ haben (siehe Abschnitt 2.1) . Sei s die Anzahl der Isomorphieklassen.
2: Berechne für jede Periodenmatrix die zehn geraden Thetanullwerte

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega_i, 0) = \sum_{n \in \mathbb{Z}^g} exp(\pi i (n + \frac{1}{2}\delta)^t \Omega_i (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon))$$

mit hinreichender Genauigkeit. Siehe Abschnitt 2.2.
3: Berechne $3s$ erzeugende j-Invarianten

$$j_1^{(i)}, j_2^{(i)} \text{ und } j_3^{(i)}, i = 1, \ldots, s.$$

4: Berechne die Klassenpolynome

$$H_1(X) = \prod_{i=1}^{s} (X - j_1^{(i)}), H_2(X) = \prod_{i=1}^{s} (X - j_2^{(i)}) \text{ und } H_3(X) = \prod_{i=1}^{s} (X - j_3^{(i)}).$$

Es gilt $H_i \in \mathbb{Q}[x]$.
5: Finde den Nenner (siehe Bemerkung 2.6.1) und berechne die Polynome $H_i'(X) \in \mathbb{Z}[X]$.
6: **for** alle Tripel (a_1, a_2, a_3), a_i Nullstelle von $H_i'(X) \mod p$ **do**
7: Setze

$$j_1 := a_1; \quad j_2 := a_2; \quad j_3 := a_3.$$

8: Berechne Mestres Invarianten (siehe Abschnitt 2.3).
9: Wende Mestres Algorithmus an, um eine Kurve

$$C : y^2 = f(t), f(t) \in \mathbb{F}_p[t], \quad \deg f(t) = 6,$$

zu erhalten.
10: **if** $\#J(C) = n_1$ oder n_2 **then**
11: Gebe C aus.

12: **end if**
13: **end for**

Bemerkung 2.6.1. 1. Der Algorithmus beschränkt sich auf CM-Körper, deren reeller Teilkörper Klassenzahl eins hat. Dies stellt sicher, daß die Ideale in $\mathcal{O}_K$ eine relative Basis bezüglich $\mathcal{O}_{K_0}$ besitzen. Dadurch können wir die Periodenmatrizen berechnen (siehe Satz 2.1.1).

2. Vor der Ausführung des zweiten Schrittes ist es günstig, die Periodenmatrizen Ω_i durch geeignete Transformation in $Sp(4,\mathbb{Z})$ so zu modifizieren, daß das sukzessive Minimum maximal wird. Dies beschleunigt die Berechnung der Thetanullwerte.

3. Für den 5. Schritt des Algorithmus wenden wir den Kettenbruchalgorithmus auf die Koeffizienten der Polynome $H_i(X)$ an. Wir berechnen das kleinste gemeinsame Vielfache $n_K^{(i)}$ der Nenner aller Koeffizienten. Durch Multiplikation mit $n_K^{(i)}$ erhalten wir aus $H_i(X)$ ein ganzzahliges Polynom.

4. Für die Berechnung von Klassenpolynomen von sehr hoher Klassenzahl können wir noch einen Trick anwenden. Dieser wurde z.B. für Klassenzahl 10 eingesetzt. Wir durchlaufen zunächst das Programm mit niedriger Präzision, z.B. nur 20 Nachkommmastellen. Auf diese Weise erfahren wir, welche Invarianten zueinander komplex konjugiert sind. Einige Nullstellen können wir paaren. Von diesen Paaren müssen wir beim anschließenden Durchlauf nur immer eine Invariante berechnen.

5. Um den Algorithmus zu beschleunigen, können wir die Existenz des Twists verwenden.

   Definition 2.6.2. *Sei $C : y^2 = f(x)$ eine über $\mathbb{F}_p$ definierte hyperelliptische Kurve und $k \in \mathbb{N}$ ein quadratischer Nichtrest modulo p. Dann heißt*

   $$\tilde{C} : y^2 = kf(x)$$

   *der **Twist** von C.*

   Die Gruppenordnung der Jacobischen der getwisteten Kurve läßt sich leicht aus der Gruppenordnung von $J(C)$ bestimmen.

   Satz 2.6.3. *Es sei*

   $$P(T) = 1 + a_1T + \ldots + a_{g-1}T^{g-1} + a_gT^g + qa_{g-1}T^{g+1} + \ldots + q^gT^{2g}$$

   das charakteristische Polynom des Frobenius der Kurve C. Dann gilt für den Twist

   $$\begin{aligned}\tilde{P}(T) =& 1 - a_1T + \ldots + (-1)^{g-1}a_{g-1}T^{g-1} + (-1)^g a_gT^g \\ &+ (-1)^{g+1}qa_{g-1}T^{g+1} + \ldots + q^gT^{2g}.\end{aligned}$$

   Beweis. Wir skizzieren kurz den Beweis:

(a) Es gilt

$$\begin{aligned} 2p+2 &= \#C(\mathbb{F}_{p^r}) + \#C(\mathbb{F}_{p^r}) && \text{für } r \text{ ungerade und} \\ \#C(\mathbb{F}_{p^r}) &= \#C(\mathbb{F}_{p^r}) && \text{für } r \text{ gerade.} \end{aligned}$$

(b) Verwende Koeffizientenvergleich in der Gleichung

$$\frac{P'(T)}{P(T)} = \sum_{r\geq 0}(M_{r+1} - 1 - q^{r+1})T^r$$

(siehe [26], S.147) und zeige durch Vollständige Induktion nach k

$$a_k = \tilde{a}_k \text{ für } k \text{ gerade und } a_{2k} = (-1)\tilde{a}_{2k} \text{ für } k \text{ ungerade.}$$

□

Falls nun nicht $P(1)$, sondern $P(-1)$ auf eine gute Gruppenordnung überführt, können wir leicht die zugehörige Kurve bestimmen. Die Transformation

$$x' = \frac{1}{k}x \text{ und } y' = \frac{1}{k^3}y$$

führt die Kurvengleichung $y^2 = kf(x)$ in eine projektiv äquivalente Gleichung $y^2 = g(x)$ mit normiertem Polynom g.

6. Im Gegensatz zum Fall $g = 1$ zerfallen die Klassenpolynome nicht immer in Linearfaktoren. Die Bedingung, daß p eine relative Normgleichung erfüllt, ist dazu nicht ausreichend (mehr in Abschnitt 3.2). Es gibt aber immer eine Nullstelle.

Beispiel 2.6.4. Betrachte den CM-Körper $\mathbb{Q}(i\sqrt{3+\sqrt{2}})$ und die Primzahl

$$p = 907978164842524484436193557995633106029.$$

Jedes der Klassenpolynome $H_1(X)$, $H_2(X)$ und $H_3(X)$ zerfällt in zwei Linearfaktoren und einen Faktor vom Grad zwei.
Die zwei Linearfaktoren geben uns

$$j_1 \in \{382761742543636490072599637158920059149, 236850294046638331292356742738514228943\}$$

$$j_2 \in \{360928830608881747691513692268006353606, 429143299291851306561265935953995843647\}$$

$$j_3 \in \{198845775319911753423103719821254472626, 468243090297888903170273113515934956773\}.$$

Mit dem irreduziblen Faktor können wir auch Kurven über $\mathbb{F}_{p^2}$ konstruieren (siehe Abschnitt 3.2).

2.7 Komplexität des Algorithmus

2.7.1 Analyse

Der Algorithmus besteht im wesentlichen aus zwei Teilen,

1. der Berechnung des Klassenpolynoms und

2. Mestres Algorithmus.

Die Berechnung der Thetanullwerte dominiert die Laufzeit des ersten Teiles. Im Abschnitt 2.2 haben wir gesehen, daß der Aufwand für die Berechnung der Thetanullwerte vom ersten sukzessiven Minimum der Periodenmatrix abhängt. Eine genaue Analyse ist darum schwierig.
Da wir nicht mit beliebig hoher Präzision arbeiten können, ist die Anzahl der CM-Körper beschränkt. Im Prinzip können wir deshalb die möglichen Klassenpolynome alle im voraus berechnen.
Weiter unten geben wir eine Tabelle der CM-Körper an, von denen wir das Klassenpolynom berechnet haben. Diese gibt Aufschluß darüber, wie Diskriminante, Klassenzahl und Komplexität des Klassenpolynoms zusammenhängen.
Der zweite Teil ist die Anwendung von Mestres Algorithmus. Hier müssen wir zuerst das Klassenpolynom faktorisieren. Zur Polynomfaktorisierung gibt es einen effizienten probabilistischen Algorithmus [14], der für ein Polynom vom Grad n

$$O(n^{2+\epsilon} + n \log p)$$

Operationen in $\mathbb{F}_p$ benötigt. In unserer Situtation ist der Grad des Polynoms klein und beschränkt. Somit können wir die Anzahl der Operationen durch $O(\log p)$ abschätzen.
Wir müssen Mestres Algorithmus s^3-mal anwenden, wobei s der Grad des Klassenpolynoms ist. In den meisten Fällen gilt $s = 2h_K$.
Insbesondere müssen wir s^3 Skalarmultiplikationen auf der Jacobi-Varietät hyperelliptischer Kurven ausführen. Jede Skalarmultiplikation benötigt

$$O(g^2 \log p) = O(\log p)$$

Operationen in $\mathbb{F}_p$ (siehe zum Beispiel [39] für die Komplexität einer Addition in der Jacobischen).
Als Gesamtlaufzeit (ohne Berechnung des Klassenpolynoms) erhalten wir

$$O((2h_K)^3 \log p)$$

Operationen in $\mathbb{F}_p$.

2.7.2 Liste berechneter CM-Körper

Die ersten drei Spalten beschreiben den CM-Körper K. Es gilt

$$K = \begin{cases} \mathbb{Q}\left(i\sqrt{a+b\sqrt{d}}\right), & d = \frac{D}{4}, \quad \text{falls } D \equiv 0 \mod 4. \\ \mathbb{Q}\left(i\sqrt{a+b\frac{-1+\sqrt{d}}{2}}\right), & d = D, \quad \text{falls } D \equiv 1 \mod 4. \end{cases}$$

Die vierte Spalte gibt uns die Klassenzahl von K, die fünfte die Anzahl der Polarisierungen. Beachte, daß $h_k \cdot (\#\text{Pol})$ der Grad des Klassenpolynoms ist.
Das normierte Klassenpolynom hat im allgemeinen rationale Koeffizienten. Die sechste Spalte gibt die Anzahl der Dezimalstellen des Nenners an. Ein Stern markiert, daß wir damit noch nicht den Nenner des gesamten Polynoms gefunden haben. Die Genauigkeit, die für die korrekte Berechnung notwendig ist, ist in der siebten Spalte in Nachkommastellen angeführt. In der achten Spalte findet sich dann die Zeit in Sekunden.
Wir konnten das Klassenpolynom eines CM-Körpers mit Klassenzahl 10 bestimmen.

Komplexität der Klassenpolynome

D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)	D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)
5	3	1	1	1	1	20	1	5	4	1	2	2	11	100	6
5	5	1	2	2	24	100	3	5	6	1	2	2	44	200	12
5	7	1	1	2	1	20	1	5	11	1	1	2	12	20	1
5	6	2	2	1	24	50	1	5	8	1	4	2	66	300	141
5	8	2	2	2	68	300	21	5	10	3	1	2	4	20	1
5	18	7	1	2	23	50	1	5	16	7	4	2	132	600	625
5	19	4	1	2	31	100	1	5	23	5	1	2	52	200	6
5	91	52	2	1	50	200	12	5	119	68	2	1	76	300	52
5	35	8	5	2	97	400	315	5	18	6	4	1	110	400	52
5	43	8	8	2	125	500	2381	5	27	8	3	2	49	200	25
5	27	−8	5	2	97	500	510	8	2	1	1	1	1	20	1
8	3	1	2	2	19	50	1	8	4	1	2	2	29	100	2
8	5	1	2	2	56	150	10	8	6	1	4	2	62	300	111
8	6	3	2	1	22	100	1	8	5	2	1	2	2	100	1
8	7	2	2	2	19	100	3	8	9	2	1	2	4	20	1
8	11	4	1	2	9	50	1	8	13	4	2	2	90	200	28
8	13	6	3	2	11	100	7	8	19	4	2	2	38	200	17
8	15	4	5	2	17	300	193	8	10	2	2	1	56	150	6
8	19	8	1	2	53	100	1	8	17	2	1	2	42	150	2
8	23	8	7	2	80	600	1246	12	6	1	4	2	76	500	678

D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)	D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)
12	9	4	2	2	1	20	1	12	11	4	4	2	5	100	15
12	5	2	2	2	4	50	1	12	17	8	2	2	4	100	5
12	23	8	10	2	81	600	3096	13	3	1	2	2	1	20	1
13	5	1	1	2	2	20	1	13	6	2	2	2	23	150	6
13	8	3	1	1	1	20	1	13	11	4	1	2	9	50	1
13	7	1	4	2	84	400	421	13	16	6	2	1	106	200	4
13	75	20	2	1	28	100	2	13	25	9	1	2	35	150	3
13	16	3	1	2	33	150	2	17	23	8	7	2	55	500	1778
17	9	1	4	1	24	200	83	17	147	56	2	1	64	400	60
17	6	1	4	2	97	400	155	17	3	1	1	2	1	20	1
17	11	4	1	2	4	20	1	17	4	1	1	2	1	20	1
17	43	16	1	2	32	150	3	17	27	8	1	2	51	200	5
21	15	4	2	2	29	200	26	21	22	7	2	2	43	200	21
21	7	1	2	2	14	100	6	21	5	1	4	2	68	600	1105
24	3	1	2	2	13	100	14	24	4	1	2	2	49	200	8
24	9	2	4	2	21	150	23	24	31	12	4	2	40	200	151
24	17	6	6	2	19	400	1973	28	3	1	2	2	11	100	6
28	43	16	2	2	56	100	5	28	7	2	4	2	46	150	53
29	7	2	4	2	34	500	3950	29	5	1	1	2	4	20	1
29	17	5	1	1	9	20	1	29	4	1	2	2	35	200	25
29	9	1	2	2	14	200	44	29	15	4	1	2	41	150	3
29	24	7	4	2	27	150	34	29	12	3	2	2	18	200	25
29	31	4	2	1	9	50	1	33	7	2	2	2	1	50	40
33	95	28	4	2	62	400	38	33	15	4	2	2	24	100	6
37	15	4	2	2	17	100	10	37	7	1	2	2	2	50	1
37	19	5	3	2	26	100	31	37	26	7	3	2	33	300	366
37	4	1	2	2	32	150	19	37	43	12	1	1	16	100	1
41	4	1	2	2	11	100	14	41	5	1	2	2	19	50	1
41	6	1	1	2	1	20	1	41	9	2	2	2	65	300	46
41	10	2	4	2	8	200	238	44	4	1	2	2	62	200	26
44	7	2	2	2	7	100	9	44	67	20	4	2	111	400	302
53	7	1	1	2	33	100	1	53	5	1	4	2	80	400	1497
53	55	4	1	1	33	150	1	56	4	1	2	2	27	200	22
56	53	14	2	2	33	300	526	57	5	1	4	2	26	150	34
57	9	2	2	2	6	100	48	61	5	1	1	2	1	20	1
61	9	2	2	2	30	200	1193	69	5	1	4	2	21	200	504
61	67	12	1	1	38	150	10	69	6	1	4	2	161	600	4308
73	6	1	4	2	13	200	667	73	5	1	1	2	11	50	1
73	115	24	1	2	57	200	7	76	9	2	2	2	38	300	93

D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)	D	a	b	h_K	# Pol.	Nenner Dezst.	Präz.	Zeit (in s.)
76	5	1	2	2	74	200	29	76	279	64	4	2	8	200	880
88	5	1	2	2	66	300	85	88	85	18	2	2	59	300	855
89	6	1	1	2	1	20	1	89	11	2	4	2	25	400	777
92	5	1	2	2	55	400	392	92	29	6	4	2	26	400	4728
92	77	16	2	2	176	200	33	93	6	1	4	2	84	400	1265
97	8	1	3	2	11	150	30	97	9	1	2	2	1	100	10
101	7	1	3	2	4	100	26	109	9	1	1	2	14	20	1
113	7	1	2	2	90	400	109	113	6	1	4	2	9	400	92
124	39	7	4	2	59	400	1521	124	23	4	2	2	29	150	14
129	13	2	4	2	88	400	2221	137	7	1	2	2	64*	400	238
137	51	8	1	2	16	100	3	137	10	1	4	2	58	400	2498
141	9	1	2	2	45	400	155	149	7	1	1	2	13	100	2
152	13	2	2	2	16	100	9	157	13	1	1	2	83	150	5
181	22	3	1	2	45	200	9	233	10	1	1	2	57	100	3
269	9	1	1	2	22	100	2	281	9	1	1	2	42	200	77
389	114	11	1	2	108	200	1170								

2.7.3 Bemerkung zur Implementierung

Die zwei Teile des Algorithmus unterscheiden sich nicht nur in der Laufzeit, sondern auch bezüglich ihres programmiertechnischen Aufwandes.
Für den ersten Teil war eine Bibliothek notwendig, die Berechnungen in relativen Zahlkörpern unterstützt. Am besten geeignet ist hierfür die C-Bibliothek PARI (siehe S. 129).
Der zweite Teil benötigt eine effiziente Polynomarithmetik. Wir setzen hier die C++-Bibliothek NTL ein (siehe S. 129) .

2.8 Kryptographisch interessante Beispiele

Komplexe Multiplikation mit $\mathbb{Q}\left(i\sqrt{8+\frac{-1+\sqrt{5}}{2}}\right)$

Wir möchten eine hyperelliptische Kurve konstruieren, deren Jacobische komplexe Multiplikation mit dem Ganzheitsring in

$$K = \mathbb{Q}\left(i\sqrt{8+\frac{-1+\sqrt{5}}{2}}\right)$$

hat. Der Körper K ist nicht Galoissch und hat Klassenzahl vier. Die Fundamentaleinheit des reellen Teilkörpers $K_0 = \mathbb{Q}(\sqrt{5})$ hat negative Norm.

Wir können die Elemente der Klassengruppe bezüglich einer relativen Ganzheitsbasis angeben:

$$\begin{aligned}
\mathfrak{A}_1 &= \mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0} \\
\mathfrak{A}_2 &= (-3 + (\frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0} \\
\mathfrak{A}_3 &= (-2 + (1 + \frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0} \text{ und} \\
\mathfrak{A}_4 &= (-6 + (3 + \frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}
\end{aligned}$$

wobei

$$\eta = i\sqrt{8 + \frac{-1+\sqrt{5}}{2}}.$$

Insgesamt erhalten wir ein Repräsentantensystem aus acht prinzipal polarisierten Abelschen Varietäten der Dimension zwei. Für jede Periodenmatrix berechnen wir die Thetanullwerte und dann die Invarianten j_i. Wir führen die Berechnung mit einer Präzision von 300 Nachkommastellen durch.
Wir erhalten die drei Klassenpolynome $H_1(X), H_2(X), H_3(X)$. Die Nenner sind

$$3^5 \cdot 11^6 \cdot 13^{12}, \quad 3^3 \cdot 11^4 \cdot 13^8 \text{ und } 3^4 \cdot 11^4 \cdot 13^8, .$$

Durch Multiplikation ergeben sich die Klassenpolynome in $\mathbb{Z}[x]$

$\mathbf{H_1(X)}$=$3^{28}11^{24}13^{24}X^8$−$337503445451902141890313841427503119291691678716239465747186472518245011767752796\cdot10^5X^7$

+$913970718385211922821077796612510713970233753255052240399206313861971793823482737238703784 71\cdot10^{10}X^6$

−$173796770018336099403614014114897494491017108925040622184394270731565993050278850809541737819159069551\cdot10^{15}X^5$

−$636514261697568411352799211528014635645769750535201922294097825682372233120611279222215451128801358660519625\cdot10^{17}X^4$

+$709767264851464107772124436666352559884708792365905571742011750346017840114895083865705453192604661802921171875\cdot10^{23}X^3$

−$128610964893075668569027439853058949582898682627273670857332535338577429493259002136347383502929576751128585972265625\cdot10^{26}X^2$

+$487362350954437149675166144249601071551205254853411463251882317393997705828298501918049460313264884617765413513730468 75\cdot10^{31}X$

$-2^{32}5^{45}641^5124304229010474495^8731^5$,

$\mathbf{H_2(X)}$=$3^{12}11^{14}13^{16}X^8$−$277790965367266538189506746019219718902923960451074000 00X^7$

+$346720036970164864520633999647836053021001931772327731602397 5\cdot10^8X^6$

−$323935892173647531870709212399984173294274072173523094304605750150875\cdot10^{12}X^5$

−$209372188379501941132201276457668070320842985529512926296239981565946640625\cdot10^{13}X^4$

+$603288625340422507388887591081772665967647934740738205039824762464032519531 25\cdot10^{18}X^3$−

$234016705253685894380561947610280137543191874931402823057202858579513193969726562 5\cdot10^{20}X^2$+

$105347345309814515146862103901160150349725383070903879520477458135413894500732421875\cdot10^{24}X$

$-2^{24}5^{45}89^2\cdot641^3\cdot12430422901047449^3\cdot8731^3$,

$$\mathbf{H_3(X)}=3^{16}11^{14}13^{16}X^8-729492083009078214954469563082495216331370162398131704000X^7$$
$$+2352471624843596058274058277393819726824986070464844750544518496000000X^6$$
$$-7121830568414949628694688180365328479288275719603482688282644866543674240000000000X^5$$
$$-252677862820318487407709039586809534365329624302249538149360732758909401670 4\cdot 10^{12}X^4$$
$$+1494153308776771208249857176806582155698622602142017799597946070247520432730496\cdot 10^{16}X^3$$
$$-1587611669743429174278413580828877937905552079125060838258075470368068607354246 4\cdot 10^{21}X^2$$
$$+2316402019180109507410465138578907343598456459680153059405857961935515260542217216\cdot 10^{24}X$$
$$-2301278160950684272567382868757734769467183124209058525832554501879148986013579916 8\cdot 10^{27}.$$

Eine passende Primzahl ist durch $p = 1298992167307454227473799805 09$ gegeben. Sie führt zusammen mit K zu den zwei möglichen Gruppenordnungen

$$16873806507261171556624961017693968657279916616235023963476 \text{ und}$$
$$16873806507261171553245686803138166610780248276948805535516.$$

Dabei gilt für die erste Gruppenordnung

$$n = 16873806507261171556624961017693968657279916616235023963476 = 4 \cdot q_{prim},$$

für eine Primzahl q_{prim}.
Nun wenden wir Mestres Algorithmus an und finden die folgende Kurve C über $\mathbb{F}_p$, deren Jacobische genau n Elemente hat:

$$C : y^2 = t^5 + 1108540658589940613910785602 11t^4 + 526902799779485659284759835 53t^3$$
$$+ 8101666852884083160211758594 3t^2 + 4384235302179874940177332733 3t$$
$$+ 8455475808734236491840081997 5.$$

Komplexe Multiplikation mit $\mathbb{Q}\left(i\sqrt{3+\sqrt{7}}\right)$

Wir betrachten den CM-Körper

$$\mathbb{Q}\left(i\sqrt{3+\sqrt{7}}\right)$$

mit Klassenzahl zwei und zwei Polarisierungen.
Die Klassenpolynome $H_1(X)$, $H_2(X)$ und $H_3(X)$ sind

$$\mathbf{H_1(X)}=X^4-2130771672X^3+198502979432505408X^2+67287241032943472939335 68X-530217930917049930071565926 4,$$
$$\mathbf{H_2(X)}=4X^4-236549430X^3+1322300792925225X^2-10889814068091756720 00X-630204755989268223360000 \text{ und}$$
$$\mathbf{H_3(X)}=64X^4-1045893528X^3+1368605510700597X^2+252176436760922772192X+1073447428265129562 8544.$$

Hier liegt der für Geschlecht 2 seltene Fall vor, daß die Invarianten der vier Kurven ganze algebraische Zahlen sind.

Eine geeignete Primzahl ist $p = 58094331481464218131068859646359 3$. Sie führt zu den Gruppenordnungen

$$n_1 = 337495135027824453733283789094149750817279621391373902756574895952 \text{ und}$$
$$n_2 = 337495135027824453733281165453395182011292833807497899521740278848.$$

Die Zahl n_1 ist bis auf den Schmutzfaktor 16 eine Primzahl. Die zugehörige Kurve ist

$$\begin{aligned} C : y^2 = {} & t^5 + 474727596586211034284401845850785t^4 \\ & + 31474823459647441873958033995764 8t^3 \\ & + 31474076653298434619192952799340 9t^2 \\ & + 57439798836119065894404356378001 8t \\ & + 54622869385947037941877059359468 7. \end{aligned}$$

2.9 Mersenne-Zahlen

Mersenne- bzw. verallgemeinerte Mersennezahlen eignen sich besonders gut zur Implementierung, da bei ihnen Modulo-Operationen kostengünstig ausgeführt werden können. Betrachte zum Beispiel eine Primzahl der Form $p = 2^n - 1$. Das Ergebnis zweier Zahlen $a, b \in \{0, \ldots, p-1\}$ ist im allgemeinen größer als p, also von der Form

$$c = c_1 + c_2 p \text{ mit } c_i \in \{0, \ldots, p-1\}.$$

Wir erhalten

$$\begin{aligned} c &= c_1 + c_2(2^n - 1) \\ &= c_1 - c_2 + c_2 2^n. \end{aligned}$$

Damit kann die Modulo-Operation durch eine einfache Subtraktion realisiert werden. Mehr dazu findet man in [22] oder [54].

Verallgemeinerte Mersenne-Zahlen, die zu kryptographisch geeigneten Gruppenordnungen führen

D	a	b	prim	Schmutzfaktor k, Gruppenordnung $= k \cdot q, q$ prim
5	6	2	$2^{89}-1$	580
			$2^{130}-5$	4
5	16	7	$2^{150}-3$	64
5	18	7	$2^{192}-2^{64}-1$	1
			$2^{224}-2^{96}+1$	1
5	11	1	$2^{96}-2^{32}+1$	151
			$2^{116}-3$	59
			$2^{113}-3$	11
8	5	2	$2^{89}-1$	188
8	6	3	$2^{96}-2^{32}+1$	32
8	13	6	$2^{116}-3$	4
13	5	1	$2^{192}-2^{64}-1$	816
13	6	2	$2^{150}-3$	16
13	11	4	$2^{116}-3$	13
13	75	20	$2^{127}-1$	859
17	3	1	$2^{107}-1$	64
21	15	4	$2^{118}-3$	1,67
24	3	1	$2^{174}-3$	800
28	7	2	$2^{127}-1$	300
29	15	4	$2^{107}-1$	647
37	19	5	$2^{107}-1$	747
37	26	7	$2^{96}-2^{32}+1$	511
41	6	1	$2^{174}-3$	100
44	4	1	$2^{94}-3$	16
			$2^{174}-3$	280
44	7	2	$2^{94}-3$	14
53	7	1	$2^{192}-2^{64}-1$	1
61	67	12	$2^{94}-3$	25
89	6	1	$2^{127}-1$	136
129	13	2	$2^{96}-2^{32}+1$	20
149	7	1	$2^{192}-2^{64}-1$	7
269	9	1	$2^{94}-3$	16

Kapitel 3

Erweiterungen für Geschlecht zwei

Dieses Kapitel beschäftigt sich wie das vorhergehende mit dem Fall Geschlecht $g = 2$.
Wir untersuchen primitive CM-Körper vom Grad vier etwas genauer. Wir zeigen, daß sich einige Fälle aus Satz 2.1.1 ausschließen lassen. Damit vereinfacht sich die Berechnung des Repräsentantensystems der Isomorphieklassen aller prinzipal polarisierten Abelschen Varietäten.
Weiter betrachten wir das Zerfällungsverhalten des Klassenpolynoms und erweitern die Konstruktionsmethode auf Körper $\mathbb{F}_q$ mit $q = p^n$. Wir erläutern diese Idee und führen ein Beispiel an.
Wir beschränken uns auf $K \neq \mathbb{Q}(\xi_5)$, d.h. $\nu_K = \{\pm 1\}$ (siehe Abschnitt 4.4.1). Im ganzen Kapitel setzen wir voraus, daß die Klassenzahl h_{K_0} des reell-quadratischen Zahlkörpers gleich 1 ist.
Für die Einheitengruppe und ihre Untergruppen verwenden wir die Bezeichnungen aus Abschnitt 2.1.

3.1 Primitive CM-Körper vom Grad vier

3.1.1 Reflexivkörper und die Einheitengruppe

Reflexivkörper

Falls K Galoissch mit zyklischer Galoisgruppe ist, dann ist der zu $(K, \{1, \varphi\})$ duale CM-Typ durch $(K, \{1, \rho\varphi\})$ gegeben, wobei ρ die komplexe Konjugation bezeichne. In diesem Fall gilt also $K = K^*$.
Wenn K nicht Galoissch ist, dann bezeichnen wir den Galoisabschluß von K mit L. Dessen Galoisgruppe ist isomorph zur Diedergruppe mit acht Elementen. Sei $K = K_0(\xi)$ mit $\xi = i\sqrt{a + b\sqrt{d}}$ mit rationalen Zahlen a, b und $a + b\sqrt{d}$ total positiv. Dann können wir wie im Abschnitt 2.1 die reelle Konjugation durch $\xi^\varphi = i\sqrt{a - b\sqrt{d}}$ auf K fortsetzen. Es gilt dann $L = \mathbb{Q}(\xi, \xi^\varphi)$. Es ergibt sich

$$Gal(L, \mathbb{Q}) =< \sigma, \varphi | \sigma^4 = \varphi^2 = 1, \sigma\varphi = \varphi\sigma^3 > .$$

Der zu $(K, \{1, \varphi\})$ duale CM-Typ ist $(\mathbb{Q}(\xi + \xi^{\varphi}), \{1, \sigma\varphi\})$. Der Reflexivkörper $K^* = \mathbb{Q}(\xi+\xi^{\varphi})$ ist selbst ein CM-Körper vom Grad 4 mit reellem Teilkörper $K_0^* = \mathbb{Q}(\sqrt{a^2 - b^2 d})$. Falls wir den CM-Typ $(K, \{1, \rho\varphi\})$ betrachten, erhalten wir $(\mathbb{Q}(\xi - \xi^{\varphi}), 1, \sigma^3\varphi)$. Es gilt $\xi - \xi^{\varphi} \notin \mathbb{Q}(\xi + \xi^{\varphi})$, aber die beiden Körper $\mathbb{Q}(\xi + \xi^{\varphi})$ und $\mathbb{Q}(\xi - \xi^{\varphi})$ sind isomorph. Insbesondere ist das Zerfällungsverhalten von Primzahlen in beiden Körpern identisch.

Einheiten in CM-Körpern vom Grad 4

Es sei U_{K_0} bzw. U_K die Einheitengruppen von K_0 bzw. K.

Lemma 3.1.1. *Sei ϵ_0 die Fundamentaleinheit von K_0 und $N(\epsilon_0) = 1$. Falls $K = \mathbb{Q}(i\sqrt{\epsilon_0})$, dann ist K Galoissch mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insbesondere existiert kein primitiver CM-Typ zu K.*

Beweis. Sei $K = \mathbb{Q}(\sqrt{-a})$ für ein total positives $a \in K_0$, und σ bezeichne die reelle Konjugation. Nach Spallek ([56], S. 80) ist K genau dann Galoissch, wenn ein $q \in K_0$ existiert, so daß $\frac{\sigma(a)}{a} = q^2$. In unserer Situation gilt $a = \epsilon_0$ und $q = \epsilon_0^{\sigma}$.
Weiter ist nach Spallek $Gal(K, \mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, falls $\sigma(q)q = 1$. Daraus folgt die Behauptung. □

Bemerkung 3.1.2. Sei $K = \mathbb{Q}(i\sqrt{a})$ mit total positivem a in $K_0 = \mathbb{Q}(\sqrt{d})$ ein zyklischer CM-Körper. Weiter sei die Klassenzahl h_{K_0} des reell-quadratischen Teilkörpers gleich eins. Die Eindeutigkeit der Primfaktorzerlegung impliziert, daß jede Normgleichung bezüglich $K_0/\mathbb{Q}$, die rational lösbar ist, bereits in ganzen Zahlen lösbar ist.
Da K Galoissch ist K_0 in eine zyklische Erweiterung einbettbar. Dafür muß d mit $K_0 = \mathbb{Q}(\sqrt{d})$ die Summe von zwei Quadraten sein ([46]).
Aus der Gleichung $d = a^2 + b^2$ folgt $(\frac{a}{b})^2 - (\frac{1}{b})^2 d = -1$. Somit ist die Normgleichung $N_{K_0/\mathbb{Q}}(\alpha) = -1$ rational lösbar, und dann wie oben erläutert auch ganzzahlig lösbar.
Somit ergibt sich für K Galoissch und $h_{K_0} = 1$ stets $N(\epsilon_0) = -1$.

Die Einheitengruppen U_{K_0} und U_K haben beide stets den gleichen Rang. Wir zeigen nun, daß sie in den für uns interessanten Fällen sogar identisch sind. Dadurch läßt sich die Berechnung des Repräsentantensystem noch vereinfachen.

Satz 3.1.3. *Sei $K/\mathbb{Q}$ ein CM-Körper vom Grad vier mit trivialer Torsionseinheitengruppe ($\mu_K = \{\pm 1\}$), für den ein primitiver CM-Typ existiert, d.h. $Gal(K/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ oder K nicht Galoissch.*
Dann gilt $U_K = U_{K_0}$.

Beweis. Sei ρ die komplexe Konjugation. Die Normabbildung $N_{K/K_0} = 1 + \rho$ definiert einen Homomorphismus $U_K \to U_{K_0}$. Falls $\eta\eta^{\rho} = 1$, dann gilt auch $\eta^{\tau}(\eta^{\tau})^{\tau^{-1}\rho\tau}$ für alle Einbettungen τ von K nach $\mathbb{C}$. Somit gilt $Kern(1+\rho) = \mu_K$. Aus dem Homomorphiesatz folgt $\text{Bild}(N_{K/K_0}) \simeq U_K/\{\pm 1\}$.
Falls für die Fundamentaleinheit ϵ_0 von K_0 gilt, daß $\epsilon_0 \neq \epsilon\bar{\epsilon}$, dann folgt wegen $\text{Bild}(N_{K/K_0}) \leq U_{K_0}$ die Behauptung.

Wir nehmen also $\epsilon_0 = \epsilon\epsilon^\rho$ für ein $\epsilon \in K$ an. Dann ergibt sich $N(\epsilon_0) = 1$ und $K = \mathbb{Q}(\epsilon)$. Wir schreiben

$$\epsilon_0 = \epsilon\epsilon^\rho = \epsilon^2\epsilon^{-1}\epsilon^\rho = \epsilon^2\eta.$$

Es gilt $\eta \in Kern(1+\rho)$, also $\eta = \pm 1$.
Daraus folgt $K = \mathbb{Q}(\sqrt{\epsilon_0})$ bzw. $K = \mathbb{Q}(i\sqrt{\epsilon_0})$. Der erste Körper ist kein CM-Körper, der zweite besitzt nach Lemma 3.1.1 keinen primitiven CM-Typ. □

Somit tritt der Fall, daß die Fundamentaleinheit $\epsilon_0 \in U_1$ liegt, nicht auf.

3.1.2 Dichte von Primzahlen

Wie wir bereits in den Abschnitten 1.1.3 und 2.5 erläutert haben, interessieren wir uns für Primzahlen $p \in \mathbb{Z}$, die bezüglich K/K_0 relative Normgleichungen erfüllen. Diese führen uns auf die Primkörper, über denen die Kurve definiert ist.
Wir widmen uns nun dem Zerlegungsverhalten von Primzahlen in $K/\mathbb{Q}$ und untersuchen, mit welcher Häufigkeit Primzahlen auftreten, die eine relative Normgleichung erfüllen.
Weiter gehen wir in diesem Abschnitt auf die Gruppenordnung von Jacobischen mit komplexer Multiplikation ein.

Mit Hilfe des Dichtesatzes von Cebotarev (Satz 1.1.7) können wir nun einige Sätze für den CM-Fall zeigen. K sei ein CM-Körper vom Grad 4 über $\mathbb{Q}$ und K_0 sein reeller Teilkörper.

Satz 3.1.4. *Sei $K/\mathbb{Q}$ Galoissch mit primitivem CM-Typ. Es sei S die Menge aller in K unverzweigten Primstellen $(p) \in \mathbb{Z}$, so daß*

$$(p) = \mathfrak{A}\overline{\mathfrak{A}} \in \mathcal{O}_K.$$

Dann gilt $\delta(S) = \frac{1}{4}$.
Insbesondere gilt (bis auf eine Primstellenmenge der Dichte 0), daß jede Primzahl p, die bezüglich K/K_0 eine relative Normgleichung erfüllt, bereits in $K/\mathbb{Q}$ total zerlegt ist.

Beweis. Wir haben

$$Gal(K, \mathbb{Q}) = \{1, \varphi, \rho, \varphi^3\} \simeq \mathbb{Z}/4\mathbb{Z},$$

wobei ρ die komplexe und φ die reelle Konjugation bezeichne. Es gibt in $Gal(K, \mathbb{Q})$ nur ein Element der Ordnung zwei, nämlich ρ, das aber zu den Primstellen gehört, die bezüglich der imaginär quadratischen Erweiterung K/K_0 träge sind. □

Satz 3.1.5. *Sei $K/\mathbb{Q}$ nicht Galoissch und L der Galoisabschluß von K. Dann fallen die Primstellen in $\mathbb{Z}$ (bis auf eine Primstellenmenge der Dichte 0) in folgende fünf Klassen:*

1. *$S_1 = \{p$ total zerlegt in $L\}$, $\delta(S_1) = \frac{1}{8}$,*
2. *$S_2 = \{p$ nur träge bezüglich $K_0/\mathbb{Q}\}$, $\delta(S_2) = \frac{1}{4}$,*

3. $S_3 = \{p$ *hat Trägheitsindex vier in* $L\}$, $\delta(S_3) = \frac{1}{4}$,

4. $S_4 = \{p$ *nur träge bezüglich* $K/K_0\}$, $\delta(S_4) = \frac{1}{8}$ *und*

5. $S_5 = \{p$ *nur träge bezüglich* $K_0^*/\mathbb{Q}\}$, $\delta(S_5) = \frac{1}{4}$.

Beweis. Wir haben hier

$$Gal(K, \mathbb{Q}) =< \tau, \sigma : \tau^2 = \sigma^4 = 1, \tau\sigma = \sigma^3\tau >\simeq D_4,$$

wobei τ der reellen und σ^2 der komplexen Konjugation entspricht. Wir ordnen die fünf Mengen den Konjugationsklassen von $Gal(K, \mathbb{Q})$ zu. Die total zerlegten Primzahlen entsprechen der Konjugationsklasse $< 1 >$, die Konjugationsklasse $< \sigma^2 >$ entspricht den Primzahlen, die bezüglich der imaginär quadratischen Erweiterung K/K_0 träge sind. Die Primzahlen, die in der Galoisschen Erweiterung L/K_0 träge sind, korrespondieren zu dem Element σ, also zu der Konjugationsklasse $< \sigma >= \{\sigma, \sigma^3\}$. Die Menge S_2 kann $< \tau >= \{\tau, \sigma\tau\}$ und die Menge S_5 der Klasse $< \sigma\tau >= \{\sigma\tau, \sigma^3\tau\}$ zugeordnet werden. Die Behauptung ergibt sich nun aus dem Satz von Cebotarev. □

Falls p in S_1, dann zerfällt p in K in vier Ideale. Falls p in S_2 oder in S_4, dann zerfällt p in zwei Ideale. Im Fall S_3 zerfällt p in K in zwei Ideale, die reell konjugiert sind, und im Fall S_5 liegen genau drei Ideale über p.
Damit ergibt sich das nächste Ergebnis, daß den Zusammenhang zwischen Zerlegtheit bezüglich K/K_0 und dem reellen Teilkörper des Reflexivkörpers K^* aufzeigt.

Korollar 3.1.6. *Angenommen* $p \in \mathbb{Z}$ *ist nicht verzweigt in* L *und* $p = \mathfrak{P}\overline{\mathfrak{P}}$ *mit* $\mathfrak{P}$ *in* K, *dann gilt (bis auf eine Primzahlmenge der Dichte 0), daß* p *in* K_0^* *zerlegt ist.*

Beweis. K_0^* ist der reelle Teilkörper von K^* und somit in L enthalten. Falls K Galoissch, dann ist $K = K^*$ und die Behauptung folgt aus Satz 3.1.4.
Falls K nicht Galoissch und $p = \mathfrak{P}\overline{\mathfrak{P}}$, dann folgt insbesondere, daß p in L in mindestens vier zueinander konjugierte (nicht notwendigerweise prime) Ideale zerfällt. Daraus ergibt sich aber (da in diesem Fall $K_0 \neq K_0^*$ und $L = KK_0^*$), daß p in K_0^* zerlegt ist. □

Damit ist die Dichte der Primzahlen $p \in \mathbb{Z}$ mit $p = \mathfrak{P}\overline{\mathfrak{P}}$ in $\mathcal{O}_K$ gleich $\frac{1}{4}$ im Galoisschen Fall und $\frac{3}{8}$, falls K nicht Galoissch. Falls die Klassenzahl von K gleich eins ist, ist dies der zu erwartende Anteil von Primzahlen in $\mathbb{Z}$, die bezüglich K/K_0 eine relative Normgleichung erfüllen. Allgemein ist die Frage nach der Häufigkeit von Primzahlen, die relative Normgleichungen erfüllen, schwer zu beantworten. Die Bedingung, daß $\mathfrak{p}$ ein Hauptideal ist, bedeutet, daß $\mathfrak{p}$ im Hilbertschen Klassenkörper von K total zerfällt. Die Tabelle zeigt einige experimentelle Ergebnisse. Diese stimmen im Fall $h_K = 1$ mit unseren theoretischen Überlegungen überein.

Anzahl der Primzahlen, die eine relative Normgleichung erfüllen (von 10000 zufällig gewählten Primzahlen)							
D	a	b	Anzahl der Primzahlen	D	a	b	Anzahl der Primzahlen
5	6	2	2484	5	35	8	764
8	2	1	2496	8	3	1	2483
8	6	1	642	8	15	4	765
12	6	1	3667	24	17	6	1153
24	9	2	1805	28	7	2	2416
33	7	2	3806	41	10	2	1237
44	67	20	1861	57	5	1	2524

Wir begründen die Häufigkeiten in zwei Beispielen:
Vergleiche die beiden CM-Körper K_1 gegeben durch $D = 33$, $a = 7$ und $b = 2$ und K_2 gegeben durch $D = 8$, $a = 3$ und $b = 1$. Beide sind nicht Galoissch und haben Klassenzahl zwei. Dennoch sind die Dichten der Primzahlen, die in K_1/K_{01} bzw. K_2/K_{02} eine relative Normgleichung erfüllen, verschieden.
Nehmen wir zunächst den Körper K_1. Mit dem Zahlentheorie-System KANT (siehe S. 129) erhalten wir das Minimalpolynom des Hilbertschen Klassenkörpers L_1. Das Minimalpolynom ist $x^2 + 3$ und definiert damit den total reellen Teilkörper K_{01}^* des Reflexivkörpers von K_1. Somit ist L_1 der Galoissche Abschluß von K_1. Weiter haben wir gesehen, daß (bis auf eine Menge der Dichte 0) jede Primzahl, die in $K_1/\mathbb{Q}$ total zerfällt oder nur in $K_{01}/\mathbb{Q}$ träge ist, in K_{01}^* zerfällt (siehe Satz 3.1.5). Da die Primideale $\mathfrak{p}|p$ in K also in diesem Fall im Hilbertschen Klassenkörper total zerfallen, sind sie Hauptideale. Alle p mit $p = \mathfrak{A}\overline{\mathfrak{A}}$ in K erfüllen somit bezüglich K_1/K_{01} eine relative Normgleichung. Somit ergibt sich die Dichte $\frac{3}{8}$.
Für den CM-Körper K_2 erfüllen alle Primzahlen, die in $K/\mathbb{Q}$ total zerfallen, eine relative Normgleichung. Denn falls $p = \mathfrak{A}\overline{\mathfrak{A}}$ mit $\mathfrak{A} = \mathfrak{p}_1\mathfrak{p}_2$, dann sind $\mathfrak{p}_1$ und $\mathfrak{p}_2$ zueinander konjugiert und haben in der Klassengruppe die gleiche Ordnung. Also ist $\mathfrak{A}$ ein Hauptideal. (Dies erklärt auch das Phänomen aus [59], daß das Klassenpolynom bei Galoisschen CM-Körpern mit Klassenzahl zwei entweder über $\mathbb{Q}$ oder spätestens über K_0 in Linearfaktoren zerfällt.)
Wir betrachten also die Primzahlen, die genau in $K_0/\mathbb{Q}$ träge sind.
Sei $\alpha \in K_2$ mit $\alpha^4 + 6\alpha^2 + 7 = 0$. Mit KANT (siehe Seite 129) erhalten wir für den Hilbertschen Klassenkörper L_2 von K_2 das Minimalpolynom $x^2 + (-2 - \alpha^2)$. Über $\mathbb{Q}$ wird L_2 durch $f(x) = x^8 + 2x^6 + x^4 + 2x^2 + 1$ definiert. Die Galoisgruppe G von f hat Ordnung 32. Das Zentrum von G ist isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Weiter gibt es sechs Konjugationsklassen der Länge zwei mit Elementen der Ordnung zwei, eine Konjugationsklasse der Länge vier mit Elementen der Ordnung zwei und drei Konjugationsklassen der Länge vier mit Elementen der Ordnung vier (unter Verwendung von Magma, siehe Seite 129). Betrachten wir nun die Menge der Primzahlen p mit $p = \mathfrak{p}\overline{\mathfrak{p}}$, die *keine* relative Normgleichung erfüllen. Diese zerfallen in L_2 nach Satz 1.1.9 nur in zwei Primideale. Sie haben also im Galoisschen Abschluß von L_2 einen Trägheitsindex größer gleich vier, und

nach der Liste der Konjugationsklassen ist dieser gleich vier. Damit sind diese Primzahlen durch ihr Zerfällungsverhalten in $L/\mathbb{Q}$ vollständig bestimmt, und wir müssen inbesondere nur eine Konjugationsklasse betrachten. Die Dichte dieser Primzahlen ist nach dem Satz von Cebotarev (Satz 1.1.7) $\frac{4}{32} = \frac{1}{8}$. Für die Primzahlen p mit $p = \mathfrak{p}\overline{\mathfrak{p}}$, die eine relative Normgleichung erfüllen, ergibt sich dann ebenfalls $\frac{1}{8}$. Als Gesamtdichte aller Primzahlen, die eine relative Normgleichung erfüllen, erhalten wir $\frac{1}{8} + \frac{1}{8} = \frac{1}{4}$.

Da wir nun eine Vorstellung davon haben, wie das Ideal p in K zerfällt, widmen wir uns den möglichen Gruppenordnungen über $\mathbb{F}_p$ definierter Abelscher Varietäten mit komplexer Multiplikation.

Lemma 3.1.7. *Sei K ein CM-Körper vom Grad vier mit primitivem CM-Typ. Weiter sei $p = w\overline{w}$ für ein $w \in \mathcal{O}_K$ mit $K = \mathbb{Q}(w)$. Dann gilt*

$$\prod_{i=1}^{4}(1 - w_i) \neq \prod_{i=1}^{4}(1 + w_i),$$

wobei w_i die zu w konjugierten Nullstellen des Minimalpolynoms von w sind. Jede mögliche Lösung einer Normgleichung führt also zu zwei unterschiedlichen Gruppenordnugen.

Beweis. Angenommen es gelte

$$\prod_{i=1}^{4}(1 - w_i) = \prod_{i=1}^{4}(1 + w_i),$$

dann hat w ein Minimalpolynom der Form

$$X^4 + a_2X^2 + p^2.$$

Sei K_0 der quadratische Teilkörper, der durch das Minimalpolynom

$$q(Y) = Y^2 + a_2Y + p^2$$

beschrieben wird. Dann ist K über K_0 durch die Gleichung $X^2 = Y$ gegeben.
Da K ein primitiver CM-Körper ist, muß dieser quadratische Körper der reell-quadratische Teilkörper K_0 von K sein. Sei β eine Nullstelle von q und φ die reelle Konjugation. Dann gilt wegen $\beta\beta^{\varphi} = p$ entweder $\beta = \pm p$ oder $\beta = \pm w^2$ mit $ww^{\varphi} = p$. Im ersten Fall ist $q \in \mathbb{Q}[Y]$, im anderen Fall definiert q keinen reell-quadratischen Zahlkörper. Dies führt zu einem Widerspruch unserer Annahme. □

Satz 3.1.8. *Sei A eine Abelsche Varietät mit komplexer Multiplikation mit $\mathcal{O}_K$ und sei K ein CM-Körper vom Grad vier über $\mathbb{Q}$ mit primitivem CM-Typ, der keine nicht-trivialen Einheitswurzeln enthält. Sei p eine Primzahl, die bezüglich K/K_0 eine relative Normgleichung erfüllt. Dann gibt es*

$$\begin{cases} \text{genau 2 Gruppenordnungen,} & \text{falls } K \text{ Galoissch} \\ & \textbf{oder} \text{ die relative Normgleichung } p = w\overline{w} \\ & \text{(abgesehen vom Vorzeichen) nur eine Lösung hat,} \\ \text{3 oder 4 Gruppenordnungen,} & \text{sonst.} \end{cases}$$

Beweis. Falls die relative Normgleichung

$$p = w\overline{w}$$

(abgesehen von der Wahl des Vorzeichens) nur eine Lösung hat, dann gibt es genau zwei mögliche Gruppenordnungen

$$\prod_{i=1}^{4}(1 - w_i) \text{ und } \prod_{i=1}^{4}(1 + w_i),$$

wobei w_i die zu w konjugierten Nullstellen des charakteristischen Polynoms sind (siehe Lemma 3.1.7).
Nehmen wir nun an, daß es für die relative Normgleichungen zwei Lösungen gibt, die sich nicht nur im Vorzeichen unterscheiden. In diesem Fall muß p in K total zerlegt sein. Sei K^* der Reflexivkörper von K. Dann gilt

$$p = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}}_1\overline{\mathfrak{p}}_2$$

in $\mathcal{O}_{K^*}$. Die Ideale

$$\mathfrak{p}_1\mathfrak{p}_2 \text{ und } \overline{\mathfrak{p}_1}\mathfrak{p}_2$$

sind dann zwei Hauptideale in K, deren Erzeugende $w^{(1)}$ und $w^{(2)} = \overline{\omega_1}\omega_2$ die relative Normgleichung lösen.
Falls K Galoissch, sind $w^{(1)}$ und $w^{(2)}$ über K zueinander konjugiert, und die beiden Gruppenordnungen stimmen überein.
Sei nun K nicht Galoissch. Dann gilt $K \neq K^*$, und die beiden Hauptideale $(w^{(1)})$ und $(w^{(2)})$ sind in diesem Fall nicht zueinander konjugiert. Somit sind auch die beiden Minimalpolynome $P_{w^{(1)}}$ und $P_{w^{(2)}}$ unterschiedlich. Da aus

$$P_{w^{(1)}}(1) = P_{w^{(2)}}(1) \text{ und } P_{w^{(1)}}(-1) = P_{w^{(2)}}(-1)$$

die Gleichheit der Minimalpolynome folgt, gibt es in diesem Fall mindestens drei, im allgemeinen sogar vier verschiedene mögliche Gruppenordnungen. □

Bemerkung 3.1.9. Wenn K nicht Galoissch ist, möchten wir in Analogie zu Lemma 3.1.7 zeigen, daß stets

$$P_{w^{(1)}}(1) \neq P_{w^{(2)}}(1).$$

Wir haben viele Experimente durchgeführt, und in der Praxis ist dies **immer** der Fall.
Sei

$$P_{w^{(1)}}(X) = X^4 + a_1X^3 + a_2X^2 + a_1p + p^2$$

das Minimalpolynom für $w^{(1)}$ und

$$P_{w^{(2)}}(X) = X^4 + b_1X^3 + b_2X^2 + b_1p + p^2$$

das Minimalpolynom von $w^{(2)}$. Die Bedingung

$$P_{w^{(1)}}(1) = P_{w^{(2)}}(1)$$

ist gleichbedeutend mit

$$b_1(p+1)+b_2 = a_1(p+1)+a_2,$$

also

$$b_2 = a_2 - k(p+1) \text{ und } b_1 = a_1 + k$$

für ein $k \in \mathbb{Z}$. Weiter müssen $P_{w^{(1)}}(X)$ und $P_{w^{(2)}}(X)$ den gleichen CM-Körper erzeugen. Dies sind starke Einschränkungen an die Koffizienten a_1 und a_2. Wir konnten dennoch keinen Widerspruch zur Existenz eines CM-Körpers K und einer solchen Primzahl p ableiten.

3.1.3 Der Fall $N(\epsilon_0) = 1$

In diesem Abschnitt zeigen wir, daß die Anzahl der Isomorphieklassen prinzipal polarisierter Abelscher Varietäten für die möglichen CM-Typen identisch sind. Auch dies vereinfacht die Berechnung des Repräsentantensystems in Abschnitt 2.1.

Sei $\mathcal{K}_{1,\varphi}$ die Menge der Isomorphieklassen prinzipal polarisierter Abelscher Varietäten mit CM-Typ $(K, \{1, \varphi\})$.
Falls $K/\mathbb{Q}$ Galoissch, so gilt nach Spallek ([56], S.59) $\mathcal{K}_{1,\varphi} = \mathcal{K}_{1,\rho\varphi}$.
Falls $K/\mathbb{Q}$ nicht Galoissch und $N(\epsilon_0) = -1$, dann haben die beiden Klassen $\mathcal{K}_{1,\varphi}$ und $\mathcal{K}_{1,\rho\varphi}$ gleiche Kardinalität, da mit $(tau, tau^{\varphi}) \in \mathcal{K}_{1,\varphi}$ das Tupel$(\epsilon_0\tau_j, \epsilon_0\tau_j^{\varphi})$ eine Abelsche Varietät aus $\mathcal{K}_{1,\rho\varphi}$ beschreibt.
Nach Abschnitt 3.1.1 ist der Fall $\epsilon_0 = \epsilon\overline{\epsilon}$ für ein $\epsilon \in U_K$ für uns nicht von Interesse.

Wir beschränken uns hier nun auf K nicht Galoissch und $N(\epsilon_0) = 1$ und $|U^+/U_1| = 2$ mit den Bezeichnung aus dem ersten Abschnitt des letzten Kapitels. Wir wollen auch in diesem Fall für $h_K \geq 2$ zeigen, daß die Kardinalität der beiden Klassen $\mathcal{K}_{1,\varphi}$ und $\mathcal{K}_{1,\rho\varphi}$ gleich ist. Dies ist nach Satz 2.1.1 dazu äquivalent, daß für $h_K \geq 2$ mindestens eine Idealklasse $< \mathfrak{A} >$ existiert, so daß $\mathfrak{A}\overline{\mathfrak{A}} = \alpha$ für ein nicht total positives $\alpha \in K_0$. Dies wiederum ist gleichbedeutend damit, daß ein Primideal $\mathfrak{p}$ in K mit $< \mathfrak{p} >< \overline{\mathfrak{p}} >= \alpha$ für ein nicht total positives α existiert.
In der engeren Klassengruppe $Cl(M)^+$ eines Zahlkörpers M sind zwei Elemente $\mathfrak{A}$, $\mathfrak{B}$ genau dann äquivalent, wenn

$$\alpha\mathfrak{A} = \beta\mathfrak{B}, \quad \alpha, \beta \in M$$

und zusätzlich $\frac{\beta}{\alpha}$ für alle reellen Einbettungen von M nach $\mathbb{C}$ positiv ist. Es gilt:

Lemma 3.1.10. *Sei K_0 reell-quadratisch mit $N(\epsilon_0) = 1$. Dann gilt $h^+ = 2h$, wobei h^+ die Ordnung der engeren Klassengruppe bezeichne.*

Wir wollen zeigen, daß die Primzahlmenge

$$S = \{p \in \mathbb{Z} : p \text{ zerfällt in } K/\mathbb{Q} \text{ total}, \mathfrak{p}|(p) \in I_{K_0}, < \mathfrak{p} > \neq < 1 > \text{ in } Cl(K_0)^+\}$$

eine positive Dichte hat.

Lemma 3.1.11. *Sei K_0 wie oben mit $h_{K_0} = 1$. Dann ist der Hilbertsche Klassenkörper $H^+_{K_0}$ bezüglich der engeren Klassengruppe von K_0 ein Galoisscher Körper vom Grad 4 über $\mathbb{Q}$ mit*

$$Gal(H^+_{K_0}, \mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Beweis. Sei $\hat{\sigma}$ eine Fortsetzung der reellen Konjugation σ, dann gilt $(H^+_{K_0})^{\hat{\sigma}}$ ist der Hilbertsche Klassenkörper zu $(K_0^{\sigma}) = K_0$. Aus der Eindeutigkeit der Hilbertschen Klassenkörpers folgt dann, daß $H^+_{K_0}$ Galoissch ist.
Sei p ein Primideal, das in K_0 träge ist, so liegt p in der trivialen Klasse in $Cl(K_0)^+$. Damit ist p in $H^+_{K_0}$ zerlegt, und es gibt keine absolut trägen Primideale in $H^+_{K_0}/\mathbb{Q}$. Die Galoisgruppe kann somit kein Element der Ordnung vier haben. □

Da $Gal(H^+_{K_0}, \mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, gilt $H^+_{K_0} = K_0 Q$ für einen über $\mathbb{Q}$ quadratischen Körper Q.

Satz 3.1.12. *Sei K_0 wie oben. Falls $h_K = 1$, dann existiert zu K kein primitiver CM-Typ.*

Beweis. Sei p eine Primzahl, die in $K/\mathbb{Q}$ total zerfällt und (w) ein Hauptideal über p. Dann liegt $w\overline{w}$ in der trivialen Klasse von $Cl(K_0)^+$. Somit zerfällt p in $H^+_{K_0}/\mathbb{Q}$. Aus Satz 1.1.8 folgt dann, daß $H^+_{K_0} \subseteq K$, und da beide Grad vier über $\mathbb{Q}$ haben, die Gleichheit. Damit ist K Galoissch mit nicht-zyklischer Galoisgruppe. □

Sei nun K ein nicht Galoisscher CM-Körper über K_0 mit Klassenzahl $h_K \geq 2$ und L der Galoisabschluß von K. Da in $H^+_{K_0}/K_0$ nach Definition der engeren Klassengruppe ∞ verzweigt ist, ist $H^+_{K_0}/K_0$ eine imaginär quadratische Erweiterung. Somit folgt $H^+_{K_0} \neq K_0 K_0^*$, und aus der Existenz eines primitiven CM-Typs zu K ergibt sich $L \cap H^+_{K_0} = K_0$.

Satz 3.1.13. *Die Menge der Primzahlen p, die in $K/\mathbb{Q}$ total zerlegt sind, für die aber $< \mathfrak{p} >$ mit $\mathfrak{p}|p$ nicht die triviale Klasse in $Cl(K_0)^+$ ist, hat eine positive Dichte.*

Beweis. Sei $H^+_{K_0} = K_0 Q$ für einen quadratischen Zahlkörper Q und L der Galoissche Abschluß von K. Dann ist LQ Galoissch mit

$$Gal(LQ/\mathbb{Q}) \simeq Gal(L/\mathbb{Q}) \times Gal(Q/\mathbb{Q}) \simeq D_4 \times \mathbb{Z}/2\mathbb{Z}.$$

Sei τ die Fortsetzung des nicht-trivialen Elements von $Gal(Q/\mathbb{Q})$, die auf $Gal(L, \mathbb{Q})$ trivial operiert. Dann gilt für $\mathfrak{p}$ in LQ mit Artinsymbol $\left(\frac{LQ/\mathbb{Q}}{\mathfrak{p}}\right) = \tau$, daß $\mathfrak{p}$ über einer Primzahl $p \in \mathbb{Z}$ liegt, die in D_4 total zerfällt und in Q träge ist. Diese hat dann die gewünschte Eigenschaft. □

Korollar 3.1.14. *Sei K ein primitiver CM-Körper vom Grad 4. Dann gilt*

$$|\mathcal{K}_{1,\varphi}| = |\mathcal{K}_{1,\rho\varphi}|.$$

Beweis. Falls K Galoissch ist, sind die Klassen identisch. Falls $N(\epsilon_0) = -1$ haben wir bereits auf S. 54 erläutert, warum die Behauptung gilt.
Sei also K nicht Galoissch.
Da ein Primideal $\mathfrak{p}$ mit der Eigenschaft aus Satz 3.1.13 existiert, gibt es eine Idealklasse in K, in der alle Ideale in K_0 eine nicht total positive Norm haben. Da die Menge dieser Idealklassen eine Untergruppe bildet, folgt, daß die Anzahl der Idealklassen mit Idealen mit total positiver Norm gleich der Idealklassen mit Idealen mit nicht total positiver Norm ist. Da für $N(\epsilon_0) = 1$ und K nicht Galoissch diese Idealklassen jeweils zu unterschiedlichen CM-Typen führen, folgt die Aussage. □

Wir erreichen nun eine Verschärfung des Satzes 5.8. in [56]. Wie sich später zeigt (Satz 3.1.20), können wir mit diesem Korollar zeigen, daß das Klassenpolynom für alle p, die bezüglich K/K_0 eine relative Normgleichung erfüllen, mindestens eine Nullstelle modulo p hat.

Korollar 3.1.15. *Sei K nicht Galoissch und seien $H_i(X)$ die Klassenpolynome über $\mathbb{Q}$. Dann zerfällt $H_i(X)$ über K_0 in zwei (nicht notwendigerweise irreduzible) Faktoren gleichen Grades. Insbesondere können wir die Nullstellen jedes Klassenpolynoms so nummerieren, daß $j_i \in k_0^*$ für $1 \leq i \leq \frac{\deg(H_i)}{2}$ und $j_i \in (k_0^*)'$ für $\frac{\deg(H_i)}{2} + 1 \leq i \leq \deg(H_i)$, wobei k_0^* der Klassenkörper zu H_0 bezüglich $(K, \{1, \varphi\})$ und $(k_0^*)'$ der Klassenkörper zu H_0 bezüglich $(K, \{1, \rho\varphi\})$ ist.*

Aus dem vorhergehenden Satz folgt zusammen mit der Tatsache, daß für $K/\mathbb{Q}$ zyklisch und h_{K_0} stets $N(\epsilon_0) = -1$ (siehe Bemerkung 3.1.2), das folgende Korollar.

Korollar 3.1.16. *Sei K ein CM-Körper vom Grad vier über $\mathbb{Q}$ mit primitivem CM-Typ und einem reell-quadratischen Zahlkörper mit Klassenzahl eins. Dann gilt*

$$\deg H_i(X) = \begin{cases} h_K, & \text{falls } K/\mathbb{Q} \text{ Galoissch,} \\ 2h_K, & \text{falls } K/\mathbb{Q} \text{ nicht Galoissch.} \end{cases}$$

Dies deckt sich mit der Tabelle auf Seite 40.

3.1.4 Zerfällungsverhalten der Klassenpolynome

Als nächstes wenden wir uns dem Zerfällungsverhalten der Klassenpolynome zu. Für das Zerfällungsverhalten der Klassenpolynome möchten wir noch einmal daran erinnern, daß die Koeffizienten der normierten Klassenpolynome im allgemeinen nicht ganz sind. Wir bezeichnen das kleinste gemeinsame Vielfache der Nenner aller Klassenpolynome in Anspielung an den Zusammenhang zum Reduktionsverhalten mit Δ_K. Es macht nur Sinn, Primzahlen p zu betrachten, die den Nenner Δ_K nicht teilen.

Satz 3.1.17. *Sei $K/\mathbb{Q}$ ein CM-Körper vom Grad vier, L der Galoissche Abschluß von K und p ($p \nmid \Delta_K$) ein in L unverzweigtes Primideal, das in $K/\mathbb{Q}$ total in Hauptideale zerfällt und bezüglich K/K_0 eine relative Normgleichung erfüllt. Dann zerfällt das Klassenpolynom mod p in Linearfaktoren.*

Beweis. Falls p in $K/\mathbb{Q}$ total zerlegt ist, dann auch in $L/\mathbb{Q}$ wobei L der Galoissche Abschluß von K ist. Insbesondere ist p dann auch in K^* total zerlegt.
Sei (K, Φ) ein beliebiger CM-Typ und k_0^* der zu H_0 gehörige Klassenkörper (für die Bezeichnung siehe Satz 1.1.10). Wir wollen zeigen, daß für alle $\mathfrak{p}|p$ in K^* gilt, daß $\mathfrak{p}$ in k_0^* total zerfällt. Nach dem Zerlegungssatz der Klassenkörpertheorie 1.1.9 müssen wir zeigen, daß für $\mathfrak{p}|p$ gilt, daß $\mathfrak{p} \in H_0$.
Nach Proposition 3.6. in [56] gilt, falls $\{1, \psi\}$ der duale CM-Typ, dann

$$\mathfrak{p}\mathfrak{p}^{\psi} = \mathfrak{b}$$

für ein Ideal $\mathfrak{b}$ in K mit $\mathfrak{b}\overline{\mathfrak{b}} = p$. Da p eine relative Normgleichung erfüllt, folgt $\mathfrak{b} = (w)$. Also ist $\mathfrak{b}$ ein Hauptideal, und $\mathfrak{p}$ liegt in der Idealgruppe H_0. Da wir einen beliebigen CM-Typ gewählt haben, ist dies vom CM-Typ unabhängig, und das Klassenpolynom zerfällt modulo p vollständig in Linearfaktoren. □

Analog zeigen wir auch die folgende Aussage:

Korollar 3.1.18. *Sei $K/\mathbb{Q}$ ein CM-Körper vom Grad vier mit $h_K \leq 2$, L der Galoissche Abschluß von K und p ($p \nmid \Delta_K$) ein in L unverzweigtes Primideal, das in $K/\mathbb{Q}$ total zerlegt ist. Dann zerfällt das Klassenpolynom mod p in Linearfaktoren.*

Falls $h_K \geq 3$ und p in K nicht in Hauptideale zerfällt, scheitert der Beweis von Satz 3.1.17. Wir erklären dies an einem Beispiel.

Beispiel 3.1.19. Sei K der CM-Körper beschrieben durch $D = 8$, $a = 13$ und $b = 6$. Sei p eine Primzahl (z.B. $p = 241$), die in K vollständig, aber **nicht** in Hauptideale, zerfällt und bezüglich K/K_0 eine relative Normgleichung erfüllt.
Die Klassenpolynome zerfallen in einen Faktor vom Grad 3 und drei Faktoren vom Grad 1. Es gilt $h_K = 3$. Nach Satz 3.1.15 besteht das Klassenpolynom aus zwei Faktoren, die den Klassenkörper zur Idealgruppe H_0 für den jeweiligen CM-Typ $(K, \{1, \varphi\})$ oder $(K, \{1, \rho\varphi\})$ erzeugen.
Da $p = 241$ eine relative Normgleichung erfüllt, gilt

$$p = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_1\mathfrak{p}_2},$$

wobei entweder $\mathfrak{p}_1\mathfrak{p}_2$ oder $\mathfrak{p}_1\overline{\mathfrak{p}_2}$ ein Hauptideal ist.
Sei nun p ein Primideal in K^* und $(K^*, \{1, \psi\})$ bzw. $(K^*, \{1, \rho\psi\}$ der zu $(K, \{1, \varphi\})$ bzw. $(K, \{1, \rho\varphi\})$ gehörige CM-Typ von K^*. Dann sehen wir, daß $\mathfrak{P}|p$ in K^* entweder in H_0 bezüglich $(K^*, \{1, \psi\})$ oder in H_0 bezüglich $(K^*, \{1, \rho\psi\})$, aber nicht in beiden Idealgruppen gleichzeitig liegt. Nach den Sätzen 1.1.10 und 1.1.9 ergibt sich damit das angegebene Zerfällungsverhalten des Klassenpolynoms.

Der nächste Satz ist zentral für die Korrektheit unserer Methode, denn wir haben in Abschnitt 2.6 vorausgesetzt, daß die Klassenpolynome in $\mathbb{F}_p$ mindestens eine Nullstelle haben. Im Gegensatz zu 3.1.17 fordern wir nicht, daß p in K total zerfällt.

Satz 3.1.20. *Sei $K/\mathbb{Q}$ ein CM-Körper. Sei nun p ($p \nmid \Delta_K$) ein Primideal in $\mathbb{Z}$, das eine relative Normgleichung erfüllt. Dann besitzt jedes der drei Klassenpolynome modulo p mindestens eine Nullstelle.*

Beweis. Wir müssen zeigen, daß in K^* ein Primideal $\mathfrak{p}|p$ existiert, das bezüglich einer der beiden möglichen CM-Typen in H_0 liegt. Nach Satz 1.1.9 gibt es dann ein Primideal $\mathfrak{P}$ in k_0K^*, das über $\mathfrak{p}$ liegt und Grad eins hat. Es gilt somit

$$\mathcal{O}_{k_0K^*}/\mathfrak{P} \simeq \mathbb{F}_p.$$

Die j-Invarianten, also die Nullstellen der Klassenpolynome, liegen in k_0K^*. Somit haben die Klassenpolynome modulo p eine Nullstelle.
Sei zunächst $p = w\overline{w}$ für ein Primideal w in K, d.h. p ist in $K_0/\mathbb{Q}$ träge. Da p eine relative Normgleichung erfüllt, gibt es das gewünschte Primideal $\mathfrak{p}|p$ vom Grad eins in K^* mit $\mathfrak{p} \in H_0$.
Betrachte nun $p = \mathfrak{p}_1\overline{\mathfrak{p}_1}\mathfrak{p}_2\overline{\mathfrak{p}}$ mit $\mathfrak{p}_1 = \mathfrak{p}_2^{\varphi}$, wobei φ eine Fortsetzung der reellen Konjugation auf K bezeichne. Da $p = w\overline{w}$ für ein w gilt entweder $(w) = \mathfrak{p}_1\mathfrak{p}_2$ oder $(w) = \mathfrak{p}_1\overline{\mathfrak{p}_2}$. Wir nehmen o.B.d.A. $(w) = \mathfrak{p}_1\mathfrak{p}_2$ an. Es gilt $< \mathfrak{p}_1 >=< \mathfrak{p}_2 >^{-1}$.
Sei K Galoissch und $\{1, \psi\} = \{1, \overline{\varphi}\}$ der duale CM-Typ. Dann gilt $\mathfrak{p}_2\mathfrak{p}_2^{\psi} = \mathfrak{p}_2\mathfrak{p}_1$, also ist $\mathfrak{p}_2 \in H_0$.
Sei nun K nicht Galoissch, $\mathfrak{P}|p$ ein Primideal in K^* und $(K^*, \{1, \psi\})$. Es gilt nach Proposition 3.6 in [56] $\mathfrak{A} = \mathfrak{P}\mathfrak{P}^{\psi} \in I_K$. Es folgt, daß $\mathfrak{P}\mathfrak{P}^{\psi}$ gleich $\mathfrak{p}_1\mathfrak{p}_2$ oder $\mathfrak{p}_1\mathfrak{p}_2$ ist.
Falls $\mathfrak{P}\mathfrak{P}^{\psi} = \mathfrak{p}_1\mathfrak{p}_2$ liegt $\mathfrak{P}$ in der Idealgruppe H_0 bezüglich $(K^*, \{1, \psi\})$. Sonst liegt $\mathfrak{P}$ in der Idealgruppe H_0 bezüglich des zweiten CM-Typs $(K^*, \{1, \rho\psi\})$. Daraus folgt mit Satz 3.1.15 die Behauptung. □

Falls p eine relative Normgleichung erfüllt, werden somit immer Nullstellen der Klassenpolynome gefunden. Diese Nullstellen korrespondieren zu der j-Invarianten einer hyperelliptischen Kurven über $\mathbb{F}_p$.

Bemerkung 3.1.21. Eine vollständige Klassifizierung des Zerfällungsverhalten der Klassenpolynome modulo p ist für $g = 2$ kompliziert, da bereits das Zerfällungsverhalten des über $\mathbb{Q}$ definierten Polynoms über K_0^* sehr unterschiedlich ist. Die CM-Körper K_1 gegeben durch $D = 5$, $a = 18$ und $b = 6$ und K_2 gegeben durch $D = 5$, $a = 12$ und $b = -6$ sind beide Galoissch und haben eine Klassengruppe isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sei (K_i, Φ) ein beliebiger CM-Typ (da K Galoissch ist die Wahl des CM-Typs unbedeutend). Dann gilt im ersten Fall $|I_K/H_0| = 2$ und im zweiten Fall $I_K = H_0$. Dies hat zur Folge, daß die Klassenpolynome im zweiten Fall schon über K^* (tatsächlich sogar über K_0) total zerfallen.
In der Tabelle auf Seite 59 erfüllt p stets eine Normgleichung bezüglich K/K_0, $\mathfrak{p}$ sei ein Primideal in K über p, und $< \mathfrak{p} >$ bezeichne die Klasse von $\mathfrak{p}$ in der Idealklassengruppe von K. Der Index $[I_K : H_0]$ sei durch $i_{H/K}$ gegeben.

Eine weitere interessante Frage besteht darin, ob Van Wamelen in [59] alle über $\mathbb{Q}$ definierten Kurven mit komplexer Multiplikation konstruiert hat. Alle seine Kurven entstanden durch Wahl eines Galoisschen CM-Körpers K mit Klassenzahl $h_K \leq 2$.

Satz 3.1.22. *Sei K ein CM-Körper mit primitivem CM-Typ und einem reellen Teilkörper mit Klassenzahl eins. Sei C eine über $\mathbb{Q}$ definierte hyperelliptische Kurve vom Geschlecht zwei, deren Jacobische komplexe Multiplikation mit dem Ganzheitsring $\mathcal{O}_K$ hat. Dann ist C zu einer der Kurven in [59] isomorph.*

Der folgende Beweis basiert auf unserem Programm, ist also kein streng mathematischer Beweis.

Zerfällungsverhalten des Klassenpolynoms für Primzahlen, die bzgl. K/K_0 eine relative Normgleichung erfüllen

Klassenzahl	Erweiterung $K/\mathbb{Q}$	Primzahl p	Zerfällungsverhalten
$h_K = 1$	**Gal.**	bel.	$[1]$
	nicht Gal.	bel.	$[1,1]$
$h_K = 2$	**Gal.**	bel.	$[1,1]$
	nicht Gal.	zerfällt total	$[1,1,1,1]$
		p in $K_0/\mathbb{Q}$ träge	$[1,1,2]$
$h_K = 3$	**Gal.**	bel.	$[1,1,1]$
	nicht Gal.	zerfällt total,$<\mathfrak{p}>\neq id$	$[1,1,1,3]$
		zerfällt total,$<\mathfrak{p}>= id$	$[1,1,1,1,1,1]$
		p in $K_0/\mathbb{Q}$ träge	$[1,1,1,1,2]$
$h_K = 4$	**Gal.**		
	$I_K \simeq \mathbb{Z}/4\mathbb{Z}$	$ord <\mathfrak{p}>\leq 2$	$[1,1,1,1]$
		$ord <\mathfrak{p}>= 4$	$[1,1,2]$
	$I_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$<\mathfrak{p}>= id$ oder $i_{H/K} = 1$	$[1,1,1,1]$
		$<\mathfrak{p}>\neq id$ und $i_{H/K} = 2$	$[1,1,2]$
	nicht.Gal.		
	$I_K \simeq \mathbb{Z}/4\mathbb{Z}$	p zerfällt total	$[1,1,1,1,1,1,1,1]$
			$[1,1,1,1,2,2]$
			$[1,1,1,1,4]$
		p in $K_0/\mathbb{Q}$ träge	$[1,1,1,1,1,1,2]$
			$[1,1,1,1,2,2]$
	$I_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	p zerfällt total	$[1,1,1,1,1,1,1,1]$
			$[1,1,1,1,2,2]$
		p in $K_0/\mathbb{Q}$ träge	$[1,1,1,1,1,1,2]$
			$[1,1,1,1,2,2]$

Beweis. Aus Proposition 5.17 in [49] folgt, daß der Definitionskörper der Kurve für einen nicht Galoisschen CM-Körper $K/\mathbb{Q}$ stets den Körper K_0^* enthält. Somit kann in diesem Fall die Kurve nicht über $\mathbb{Q}$ definiert sein.
Für $K/\mathbb{Q}$ Galoissch gilt wegen $h_{K_0} = 1$ nach Bemerkung 3.1.2, daß $N(\epsilon_0) = -1$. Jedes Ideal $\mathfrak{A}$ hat eine total positive Norm bezüglich K/K_0. Für jede Abelsche Varietät $A(\mathfrak{A})$ existiert eine prinzipale Polarisierung bezüglich der beiden CM-Typen $(K, \{1, \varphi\})$ bzw. $(K, \{1, \rho\varphi\})$.
Wir nehmen zunächst an, daß der Exponent der Klassengruppe ≥ 2 ist. Dann gibt es ein

Ideal in $\mathcal{A}$ mit Ordnung ≥ 2 und für dieses Ideal gibt es einen CM-Typ $((K, \{1, \varphi\}))$, so daß $\mathcal{A}$ nicht in H_0 liegt. Wir erhalten dann mit Proposition 3.24 aus [56] mindestens zwei prinzipal polarisierte Abelsche Varietäten, die über K^* konjugiert sind. Diese können insbesondere nicht über $\mathbb{Q}$ definiert sein.
Damit verbleiben wir mit der Situation, daß der Exponent der Klassengruppe ≤ 2 ist. Loubatin hat in [31], S.339, alle 33 zyklischen CM-Körper mit dieser Eigenschaft aufgelistet. Unser Programm zeigt nun, daß nur die Körper in [59] zu Klassenpolynomen führen, die über $\mathbb{Q}$ zerfallen. □

3.2 Erweiterungskörper

Unsere Methode eignet sich, um Kurven über Erweiterungkörpern $\mathbb{F}_q = \mathbb{F}_{p^n}$ für $n \geq 1$ zu konstruieren. Zunächt einmal gibt es verschiedene Ansätze, von denen nur einer zu kryptographisch geeigneten Kurven führt. Wir betrachten erst die erfolglosen Versuche:

1. Wir können eine Primzahl p wählen, die in K^* träge ist. Diese erfüllt keine relative Normgleichung bezüglich K/K_0 (siehe Sätze über das Zerfällungsverhalten). Betrachten wir etwa den Fall $h_K = 1$, ist es nun möglich, die Kurve über $\mathcal{O}_{K_0}^*/(p) \simeq \mathbb{F}_{p^2}$ zu definieren. Die Gruppenordnung ist allerdings durch

$$\#J_C(\mathbb{F}_{p^2}) = (p-1)^4$$

   gegeben, da $\pi^2 = p\overline{p}$ gilt. Diese Kurven sind also für die Kryptographie ungeeignet, d.h. der größte Primfaktor ist verglichen mit der Gruppenordnung zu klein.

2. Wir können eine Primzahl p wählen, die eine relative Normgleichung erfüllt, für die aber das Klassenpolynom nicht in Linearfaktoren zerfällt. Ein Beispiel hierfür findet sich auf Seite 38 in Bemerkung 2.6.1. Hier zerfällt das Klassenpolynom in zwei Linearfaktoren und einen Faktor vom Grad zwei. Mit diesem Faktor lassen sich hyperelliptische Kurven über $\mathbb{F}_q = \mathbb{F}_{p^2}$ definieren. Betrachten wir aber die Gruppenordnung, dann ergibt sich

$$p^2 = w^2\overline{w}^2 \text{ in } \mathcal{O}_K,$$

   also

$$\#J_C(\mathbb{F}_{p^2}) = \prod_{i=1}^{4}(1 - w_i^2) = \prod_{i=1}^{4}(1 - w_i)\prod_{i=1}^{4}(1 + w_i).$$

   Auch hier ist der größte Primfaktor der Gruppenordnung relativ klein.

Als dritte Möglichkeit können wir eine Primzahl p wählen, die bezüglich K/K_0 zerlegt ist, aber nicht in ein Hauptideal zerfällt.

Satz 3.2.1. *Sei $K/\mathbb{Q}$ ein CM-Körper, L der Galoissche Abschluß und p ($p \nmid \Delta_K$) eine in L unverzweigte Primzahl, die in K/K_0 zerfällt. Weiter sei $\mathfrak{A}$ ein Ideal (nicht notwendigerweise prim) mit $\mathfrak{A}\overline{\mathfrak{A}}$, das über p liegt, und $f \in \mathbb{N}$ minimal, so daß*

$$\mathfrak{A}^f = (w), w \in \mathcal{O}_K$$

ein Hauptideal ist.
Dann gibt es eine über $\mathbb{F}_{p^f}$ definierte hyperelliptische Kurve mit komplexer Multiplikation, deren Gruppenordnung durch

$$J_C(\mathbb{F}_{p^f}) = \prod_{i=1}^{4}(1 - w_i) \text{ oder } J_C(\mathbb{F}_{p^f}) = \prod_{i=1}^{4}(1 + w_i)$$

gegeben ist. Hier sei $w_1 = w$ und w_i, $i \geq 1$, die Konjugierten zu w.

Beweis. Da $p = \mathfrak{A}\overline{\mathfrak{A}}$ in $\mathcal{O}_K$, gibt es ein Primideal $\mathfrak{p}$ in K^* vom Grad eins über p. Da nun $\mathfrak{A}^f$ mit f minimal ein Hauptideal, folgt $\mathfrak{p}^f \in H_0$. Somit gibt es ein Primideal $\mathfrak{P}$ in k_0K^* vom Grad f über $\mathfrak{p}$ (siehe Satz 1.1.9). Es gilt dann

$$\mathcal{O}_{k_0K^*}/\mathfrak{P} \simeq \mathbb{F}_{p^f}.$$

Gegeben sei nun eine Kurve über $\mathbb{C}$ mit komplexer Multiplikation mit $\mathcal{O}_K$ und drei j-Invarianten j_1, j_2, $j_3 \in \mathcal{O}_{k_0K^*}(\Delta_K^{-1})$. Da $p \nmid \Delta_K$ und $\mathfrak{P}$ über p liegt, können wir dann die j-Invarianten modulo $\mathfrak{P}$ reduzieren und erhalten $j_i \in \mathbb{F}_{p^f}$. Diese definieren uns eine Kurve über $\mathbb{F}_{p^f}$. □

Satz 3.2.2. *Sei $K/\mathbb{Q}$ nicht Galoissch und p eine Primzahl, die in drei Ideale zerfällt, d.h.*

$$p = \mathfrak{p}_1\overline{\mathfrak{p}_2}\mathfrak{p}_2.$$

Dann gibt es ein Ideal $\mathfrak{A}$, so daß

$$p^2 = \mathfrak{A}\overline{\mathfrak{A}} \text{ und } \mathfrak{A} \neq (p).$$

Beweis. Setze $\mathfrak{A} = \mathfrak{p}_1\mathfrak{p}_2^2$. □

Diese beiden Aussagen können wir verknüpfen, um damit im Optimalfall Kurven zu erzeugen, die über ein Körper mit Erweiterungsgrad $f = 2h_K$ definiert sind. Das Beispiel illustriert diese Methode. Wir betrachten den CM-Körper

$$K = \mathbb{Q}\left(i\sqrt{35 + 8\frac{-1+\sqrt{5}}{2}}\right).$$

Dieser hat Klassenzahl 5, und für jede Abelsche Varietät ergeben sich zwei mögliche Polarisierungen.
Wir nehmen nun die Primzahl $p = 911$, die über dem Körper K wie in Satz 3.2.2 in drei

Primideale zerfällt. Für das Ideal $\mathfrak{A} = \mathfrak{p}_1\mathfrak{p}_2^2$ gilt, daß $f = 5$ der kleinste Exponent ist, so daß $\mathfrak{A}^f$ Hauptideal ist.
Wir geben die Elemente in $\mathbb{F}_{911^{10}}$ durch Polynome vom Grad neun an. Dazu führen wir die folgende Notation (aus der NTL-Bibliothek) ein:

$$a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^9 = [a_0 \quad a_1 \ldots \quad a_9].$$

Die Klassenpolynome von $\mathcal{O}_K$ sind modulo p irreduzibel:

$$H_0(X) \equiv 701X^{10}+401X^9+322X^8+712X^7+125X^6+774X^5+513X^4+869X^3+474X^2+49X+680 \mod p,$$
$$H_1(X) \equiv 186X^{10}+895X^9+453X^8+86X^7+180X^6+47X^5+811X^4+339X^3+887X^2+296X+371 \mod p \text{ und}$$
$$H_2(X) \equiv 75X^{10}+280X^9+616X^8+737X^7+511X^6+179X^5+623X^4+533X^3+616X^2+697X+700 \mod p.$$

Wir können somit eine Kurve über $\mathbb{F}_{911^{10}}$ konstruieren. Es ergeben sich zwei mögliche Gruppenordnugen:

$$n_1 = 155012792308846128138632814006095268154658315370266774539376 \text{ und}$$
$$n_2 = 155012792308846046374979954330693046736810307187589966188400.$$

Wir finden die Kurve $y^2 = f(x)$ mit

$$\begin{aligned} f(x) = x^5 &+ [9 \quad 703 \quad 722 \quad 261 \quad 507 \quad 119 \quad 164 \quad 322 \quad 684 \quad 741]x^4 \\ &+ [715 \quad 508 \quad 396 \quad 153 \quad 661 \quad 164 \quad 513 \quad 167 \quad 892 \quad 156]x^3 \\ &+ [548 \quad 810 \quad 311 \quad 54 \quad 483 \quad 636 \quad 130 \quad 899 \quad 845101]x^2 \\ &+ [550 \quad 294 \quad 663 \quad 157 \quad 288 \quad 697 \quad 710 \quad 60 \quad 475 \quad 608]x \\ &+ [301 \quad 385 \quad 355 \quad 533 \quad 347 \quad 763 \quad 659 \quad 163 \quad 720 \quad 665]. \end{aligned}$$

Diese hat Gruppenordung

$$n_2 = 400 \cdot q,$$

wobei q eine Primzahl mit 57 Dezimalstellen ist.

Bemerkung 3.2.3. Dieser Abschnitt ist besonders von theoretischem Interesse. In der Praxis ist die Wahl von Kurven über kleinen Erweiterungkörpern gefährlich. Mittels Weil-Restriktion können wir einer Jacobischen über $\mathbb{F}_{p^n}$ einer Kurve vom Geschlecht g eine Abelsche Varietät der Dimension $g \cdot n$ zuordnen. Wenn diese Abelsche Varietät ein Faktor einer Jacobischen einer Kurve von kleinem Geschlecht ist, dann können wir ab $n \cdot g \geq 4$ Gaudrys Algorithmus einsetzen. Das diskrete Logarithmusproblem ist dann einfacher als auf einer sorgfältig gewählten Kurve über einem vergleichbar großen Primkörper (siehe auch die Diskussion in der Einleitung und [16],[9]).

Kapitel 4

Die CM-Methode für Geschlecht drei

4.1 Vom CM-Körper zur Periodenmatrix

Sei K ein CM-Körper mit $[K : \mathbb{Q}] = 6$. Der erste Schritt des Konstruktionsverfahrens besteht aus der Bestimmung eines Repräsentantensystems aller Isomorphieklassen der prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit der Maximalordnung $\mathcal{O}_K$.

4.1.1 CM-Typen

Für CM-Körper vom Grad 6 über $\mathbb{Q}$ ist der reelle Teilkörper meist nicht mehr Galoissch über $\mathbb{Q}$. Falls er Galoissch ist, dann gilt $G_0 = Gal(K_0/\mathbb{Q}) = \{id, \sigma, \sigma^2\} \simeq \mathbb{Z}/3\mathbb{Z}$. Sonst hat der Galoissche Abschluß L_0 Grad 2 über K_0 und $G_0 = Gal(L_0/\mathbb{Q}) \simeq S_3$. Es ergeben sich nun die folgenden Möglichkeiten für die Galoisgruppe $G = \mathrm{Gal}(L, \mathbb{Q})$ des Galoisschen Abschlusses L von K:

1. $G = Gal(K, \mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ (siehe oben, $K/\mathbb{Q}$ Galoissch),
2. $G \simeq \mathbb{Z}/2\mathbb{Z} \times S_3$,
3. $G \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times_s \mathbb{Z}/3\mathbb{Z}$ und
4. $G \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times_s S_3$.

Für die ersten zwei Körper ist nicht jeder CM-Typ primitiv. Wir können hier folgende Aussage zeigen:

Lemma 4.1.1. *Wir verwenden die Bezeichnungen L, K, G und G_0 wie oben.*

1. *Sei $G \simeq \mathbb{Z}/6\mathbb{Z}$ und sei H die Untergruppe von G mit 3 Elementen. Dann ist (K, Φ) genau dann nicht primitiv, wenn Φ gleich einer Nebenklasse von H in G ist.*
2. *Sei $G \simeq \mathbb{Z}/2\mathbb{Z} \times S_3$ und sei H die Untergruppe von S_3 mit 3 Elementen. Dann ist (K, Φ) genau dann nicht primitiv, wenn Φ gleich $H|_K$ oder $\rho H|_K$ ist, wobei ρ die komplexe Multiplikation bezeichne.*

Beweis. 1. Da die komplexe Konjugation die Ordnung zwei hat, sind keine zwei Elemente in H bzw. $\rho H, \rho \notin H$ zueinander konjugiert. Also sind H und ρH zulässige CM-Typen.
Für H prüft man nach, daß $S \simeq H$, also $H' = S \neq \{id\} = Gal(L, K) = H$. Also ist dieser CM-Typ nicht primitiv. Analog zeigt man, daß $\rho H, \rho \notin H$ nicht primitiv ist. Für jeden anderen CM-Typ erhalten wir hingegen auch $H' = \{id\}$.

2. Falls $\Phi = H$, dann ergibt sich $S \simeq G_0 \simeq S_3$ und somit $H' \simeq S_3$. Für die Galoisgruppe $H = Gal(L, K)$ gilt aber $H \simeq \mathbb{Z}/2\mathbb{Z}$. Also ist dieser CM-Typ nicht primitiv.
Analog zeigen wir die Aussage für ρH.
Für alle anderen CM-Typen rechnet man leicht nach, daß diese primitiv sind.

□

Für die Fälle 3. und 4. auf Seite 63 sind **alle** CM-Typen primitiv.
Für CM-Körper vom Grad 8 über $\mathbb{Q}$, die bei einfachen Abelschen Varietäten der Dimension 4 auftreten, gibt es für den Galoisschen Abschluß L von K 38 Möglichkeiten ([10]). Unter diesen gibt es genau eine Klasse von CM-Körpern, die keinen primitiven CM-Typ besitzen. Es gilt nämlich der folgende Satz ([44]):

Satz 4.1.2. *Ein CM-Körper K besitzt genau dann keinen primitiven CM-Typ, falls $K/\mathbb{Q}$ Galoissch ist und $Gal(K, \mathbb{Q})$ entweder die Kleinsche Vierergruppe oder die Diedergruppe der Ordnung 8 ist.*

4.1.2 Repräsentantensystem für U^+/U_1

Es sei wie in Abschnitt 2.1 U^+ die Gruppe der total positiven Einheiten in K_0. Dies sind die Einheiten mit positiver Norm. Weiter sei U_1 die Untergruppe von U^+ mit Einheiten der Form $\epsilon\overline{\epsilon}$ für eine Einheit ϵ in K.
Der Körper K_0 ist total reell. Falls $[K_0 : \mathbb{Q}] = g$, dann gilt nach dem Dirichletschen Einheitensatz für die Einheitengruppe U_{K_0}

$$U_{K_0} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{g-1},$$

da außer ± 1 alle Einheitswurzeln komplex sind.

Der Fall g=3

Falls ϵ_1 und ϵ_2 die beiden positiven Fundamentaleinheiten sind, dann gilt

$$U_{K_0} = \{\pm\epsilon_1^n\epsilon_2^m : n, m \in \mathbb{Z}\}.$$

Zunächst bestimmen wir die beiden Erzeugenden u_1, u_2 der freien Untergruppe U^+ von U_{K_0}.
Fall 1: Falls beide Fundamentaleinheiten total positiv sind, setzen wir $u_1 := \epsilon_1$ und $u_2 := \epsilon_2$.

Fall 2: Falls ϵ_1 total positiv ist und ϵ_2 nicht (oder umgekehrt), dann setzen wir $u_1 := \epsilon_1$ und $u_2 := \epsilon_2^2$ (bzw. umgekehrt).
Fall 3: Falls beide Fundamentaleinheiten nicht total positiv sind, so sind es aber ϵ_i^2 und $\epsilon_1\epsilon_2$. Wir setzen $u_1 := \epsilon_1\epsilon_2$ und $u_2 := \epsilon_2^2$.
Es gilt nun

$$U^+ = \{u_1^n u_2^m : n, m \in \mathbb{Z}\}.$$

Als nächstes wenden wir uns der Bestimmung von U^+/U_1 zu. Sei $\alpha = u_1^n u_2^m$ ein Element in U^+. Falls n und m beide gerade sind, dann gilt $\alpha \in U_1$, also haben wir $|U^+/U_1| \leq 4$. Allgemein ergibt sich der folgende Algorithmus (wobei K der CM-Körper ist):

Berechnung eines Repräsentantensystems für U^+/U_1 im Fall $g = 3$
Input: Erzeugende u_1, u_2 von U^+
Output: Repräsentantensystem $\mathcal{R}$ für U^+/U_1 und $d = |U^+/U_1|$.
$\mathcal{R} = \{1\}$.
for $i = 1$ to 2 **do**
Teste, ob u_1 Norm bezgl. $\mathcal{O}_K$.
Wenn ja, setze $t_i := 1$, sonst $t_i := 0$.
end for
if $t_1 = t_2 = 1$ **then**
$d := 1$.
else if $t_1 = 1, t_2 = 0$ **then**
$d := 2$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_2\}$.
else if $t_1 = 0, t_2 = 1$ **then**
$d := 2$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_1\}$.
else
if $\epsilon_1 \cdot \epsilon_2$ Norm bezgl. $\mathcal{O}_K$ **then**
$d := 2$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_1\}$.
else
$d := 4$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_1, \epsilon_2, \epsilon_1\epsilon_2\}$.
end if
end if
Return $\mathcal{R}$ und d.

Der Fall g = 4

In diesem Fall gibt es drei Fundamentaleinheiten $\epsilon_1, \epsilon_2, \epsilon_3$.
1. Fall: Alle drei Fundementaleinheiten sind total positiv. Wir setzen $u_1 := \epsilon_1$, $u_2 := \epsilon_2$ und $u_3 := \epsilon_3$.
2. Fall: Genau zwei Fundamentaleinheiten (o.B.d.A ϵ_1 und ϵ_2) sind total positiv. Dann setzen wir $u_1 := \epsilon_1$, $u_2 := \epsilon_2$ und $u_3 := \epsilon_3^2$.
3. Fall: Genau eine Fundamentaleinheit (o.B.d.A. ϵ_1) ist total positiv. Wir setzen $u_1 := \epsilon_1$, $u_2 := \epsilon_2^2$ und $u_3 := \epsilon_2\epsilon_3$.

4. Fall: Falls keine Fundamentaleinheit total positiv ist, wählen wir $u_1 := \epsilon_1^2$, $u_2 := \epsilon_1\epsilon_2$ und $u_3 := \epsilon_1^2\epsilon_2\epsilon_3$.
Das Repräsentantensystem für $|U^+/U_1|$ besteht aus höchstens acht Elementen:

Berechnung eines Repräsentantensystems für U^+/U_1 für $g = 4$
Input: Erzeugende u_1, u_2, u_3 von U^+
Output: Repräsentantensystem $\mathcal{R}$ für U^+/U_1 und $d = |U^+/U_1|$.
$\mathcal{R} := \{1\}$.
for $i = 1$ to 3 **do**
Teste, ob u_1 Norm bezgl. $\mathcal{O}_K$.
Wenn ja, setze $t_i := 1$, sonst $t_i := 0$.
end for
Setze $t := (t_1, t_2, t_3)$.
if $t = (1,1,1)$ **then**
$d := 1$.
else if $t = (1,1,0)$ (analog $(1,0,1)$ und $(0,1,1)$) **then**
$d := 2$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_3\}$.
else if $t = (1,0,0)$ (analog $(0,1,0)$ und $(0,0,1)$) **then**
if $\epsilon_2\epsilon_3$ Norm bezgl. $\mathcal{O}_K$ **then**
$d := 2$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_2\}$.
else
$d := 4$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_2, \epsilon_3, \epsilon_2\epsilon_3\}$
end if
else
if $\epsilon_1\epsilon_2$ ist Norm, $\epsilon_2\epsilon_3$ nicht (analoge Fälle ebenso) **then**
$d := 4$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_1, \epsilon_3, \epsilon_1\epsilon_3\}$
else if $\epsilon_i\epsilon_j$ ist Norm **then**
$d := 2$ und $\mathcal{R} := \{\epsilon_1\}$
else
$d := 8$ und $\mathcal{R} := \mathcal{R} \cup \{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_1\epsilon_2, \epsilon_2\epsilon_3, \epsilon_1\epsilon_3, \epsilon_1\epsilon_2\epsilon_3\}$
end if
end if
Return $\mathcal{R}$ und d.

4.1.3 Bestimmung eines geeigneten CM-Typs

Notation: Statt $\varphi(x)$ schreiben wir im folgenden auch abkürzend x^φ.
Wie wir bereits erwähnt haben, existiert zu jedem CM-Körper, dessen reeller Teilkörper Klassenzahl eins hat, ein geeigneter CM-Typ, so daß eine prinzipal polarisierte Abelsche Varietät $A(\mathcal{O}_K)$ zu diesem CM-Typ existiert. Seien $\{\varphi_1, \ldots, \varphi_g\}$ g verschiedene Einbettungen von K nach $\mathbb{C}$, die nicht zueinander konjugiert sind. Weiter sei die Differente von K über $\mathbb{Q}$ ein Hauptideal (γ). Dann finden wir den CM-Typ wie folgt:

$\Phi := \{\}$
for $i = 1$ to g **do**
  if Im $\gamma^{\varphi_i} < 0$ **then**
    $\Phi := \Phi \cup \{\varphi_i\}$
  else
    $\Phi := \Phi \cup \{\overline{\varphi_i}\}$
  end if
end for
Return (K, Φ)

Wir werden nun genauer auf die Fälle $[K : \mathbb{Q}] = 6$ und $[K : \mathbb{Q}] = 8$ eingehen.

Der Fall $[K : \mathbb{Q}] = 6$

Der CM-Körper K enthält den reellen Teilkörper K_0 mit $[K : K_0] = 2$ bzw. $[K_0 : \mathbb{Q}] = 3$. Wir beschränken uns hier und für den Rest der Konstruktion auf den Fall, daß K_0 monogen ist, d.h. eine Potenz-Ganzheitsbasis besitzt. Dies bedeutet, daß

$$\mathcal{O}_{K_0} = \mathbb{Z} + \mathbb{Z}w + \mathbb{Z}w^2 = \mathbb{Z}[w] \text{ für ein } w \in K_0.$$

Insbesondere gilt, $K_0 = \mathbb{Q}(w)$.
Weiter fordern wir, daß $K = K_0(i\sqrt{b})$ für ein total positives Element b in K_0 gilt. Total positiv bedeutet, daß das Minimalpolynom von b über $\mathbb{Q}$ nur reelle positive Wurzeln hat. Nach der Definition der Differente gilt

$$\delta_{K_0/\mathbb{Q}} = (f'(w)).$$

Weiter gilt für die Relativdifferente

$$\delta_{K/K_0} = (\eta - \overline{\eta}),$$

falls $\mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$.
Daraus ergibt sich

$$\delta_{K/\mathbb{Q}} = (f'(w)(\eta - \overline{\eta}))\,.$$

Eine algebraische Zahl ist durch ihr Minimalpolynom gegeben. Durch die Wahl einer Nullstelle fixieren wir eine Einbettung des Zahlkörpers in $\mathbb{C}$. Wir legen nun für den Rest des Abschnittes eine Einbettung des total reellen Zahlkörpers K_0 fest, die sich an der Pari-Bibliothek orientiert.
Sei f mit $f(w) = 0$ das Minimalpolynom des total reellen Zahlkörpers $\mathbb{Q}(w)$ vom Grad drei. Wir betten K_0 mit der kleinsten Nullstelle w in $\mathbb{R}$ ein. Da das Minimalpolynom normiert ist und somit der höchste Koffizient positiv ist, gilt $f'(w) > 0$.
Die mittlere Nullstelle sei $\sigma_1(w)$, die größte der Nullstellen $\sigma_2(w)$. Damit haben wir die drei reellen Einbettungen $\{id, \sigma_1, \sigma_2\}$ von K_0 festgelegt.
Sei nun $K = K_0(i\sqrt{b})$ der CM-Körper. Dann setzen wir

$$\hat{\sigma}_i(i\sqrt{b}) = i\sqrt{\sigma_i(b)}$$

wobei $\sqrt{\sigma_i(b)}$ die positive Wurzel der reellen Zahl $\sigma(b)$ ist. Die sechs Einbettungen des CM-Körpers nach $\mathbb{C}$ sind dann durch $\{\hat{id}, \hat{\sigma}_1, \hat{\sigma}_2, \rho\hat{id}, \rho\hat{\sigma}_1, \rho\hat{\sigma}_2\}$ gegeben, wobei ρ die komplexe Konjugation bezeichnet. Wir bezeichnen $\hat{id}$ auch abkürzend mit 1 und $\rho(x)$ mit $\overline{x}$.
Wir können η dann so wählen, daß

$$\text{Im } \eta > 0 \text{ und Im } \eta^{\hat{\sigma}_i} > 0 \text{ für } i = 1, 2.$$

Bei der von uns gewählten Einbettung gilt

$$f'(w) > 0, \quad f'(w^{\sigma_1}) < 0 \text{ und } f'(w^{\sigma_2}) > 0.$$

Wir wählen $\gamma = -f'(w)(\eta - \overline{\eta})$, und es gilt:

$$\begin{aligned} \text{Im } \gamma^{\rho\hat{\sigma}_1} &= \text{Im } (-f'(w^{\sigma_1})(\overline{\eta}^{\hat{\sigma}_1} - \eta^{\hat{\sigma}_1})) < 0 \text{ und} \\ \text{Im } \gamma^{\hat{\sigma}_2} &= \text{Im } (-f'(w^{\sigma_2})(\eta^{\hat{\sigma}_2} - \overline{\eta}^{\hat{\sigma}_2})) < 0. \end{aligned}$$

Nach Satz 1.1.4 definiert $\xi = \gamma^{-1} = -(f'(w)(\eta - \overline{\eta}))^{-1}$ eine prinzipale Polarisierung auf $A(\mathcal{O}_K)$ vom CM-Typ $\Phi = \{1, \rho\hat{\sigma}_1, \hat{\sigma}_2\}$.

Der Fall $[K : \mathbb{Q}] = 8$

Sei K_0 eine Körpererweiterung vom Grad 4 über $\mathbb{Q}$ und f das Minimalpolynom von K_0. Weiter sei $\mathcal{O}_{K_0}$ monogen, d.h. $\mathcal{O}_{K_0} = \mathbb{Z} + \mathbb{Z}w + \mathbb{Z}w^2 + \mathbb{Z}w^3$.
Für die Differente des CM-Körpers K über $\mathbb{Q}$ gilt dann

$$\begin{aligned} \delta_{K/\mathbb{Q}} &= -(f'(w)(\eta - \overline{\eta})) \\ &= -(f'(w)(2 \text{ Im } \eta). \end{aligned}$$

Wir fixieren wieder eine Einbettung für $w \in \mathbb{R}$.
Falls wir $\gamma = -f'(w)(\eta - \overline{\eta})$ setzen und $\{\varphi_1, \ldots, \varphi_4\}$ nicht zueinander, konjugierte Einbettungen von K nach $\mathbb{C}$ sind, dann wählen wir den CM-Typ so, daß

$$\begin{aligned} \varphi_i &\in \Phi, \quad \text{falls } f'(w^{\varphi_i}) > 0, \text{ und} \\ \overline{\varphi}_i &\in \Phi, \quad \text{falls } f'(w^{\varphi_i}) < 0. \end{aligned}$$

4.1.4 Prinzipale Polarisierungen auf $A(\mathfrak{A}_\tau)$

Wir prüfen nun, ob sich Satz 4.2 aus [56] auf höheres Geschlecht übertragen läßt. In der Tat ändert sich hier nichts, denn für den Satz 4.2 ist es nur wichtig, daß K_0 Klassenzahl eins hat und K eine imaginär quadratische Erweiterung von K_0 ist. Der Vollständigkeit halber geben wir hier trotzdem den Satz und eine Beweisskizze an.
Da wir annehmen, daß die Klassenzahl des reell-quadratischen Teilkörpers K_0 gleich eins ist, ist die relative Norm N_{K/K_0} eines Ideales in K ein Hauptideal in K_0. Die Untergruppe der Idealklassengruppe, für deren Elemente Repräsentanten $\mathfrak{A}$ existieren, so daß $N_{K/K_0}(\mathfrak{A}) = (\alpha)$ für ein total positives Element $\alpha \in K_0$ ist, bezeichenen wir mit c'_K.
Die Funktion sign(x) gibt uns das Vorzeichen von x an.

Satz 4.1.3. *Sei $(K, \{1, \varphi_1, \varphi_2)$ ein primitiver CM-Typ und $\mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$ mit η wie in Abschnitt 4.1.3.*
Dann gibt es zu jeder Idealklasse von c'_K ein Ideal $\mathfrak{A}_\tau$ der Form $\mathfrak{A}_\tau = \mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}$ mit sign(Im (τ)) =sign(Im (η)) und sign(Im (τ^{φ_1})) =sign(Im (η^{φ_2})). Weiter gilt $\mathfrak{A}_\tau\overline{\mathfrak{A}}_\tau$ für das total positive Element

$$\alpha_\tau = \frac{Im\ (\tau)}{Im\ (\eta)}.$$

Falls

$$\xi = -f'(w)(\eta - \overline{\eta})^{-1}$$

eine prinzipale Polarisierung auf $A(\mathcal{O}_K)$ ist, dann definiert

$$\xi_\tau = -f'(w)(\tau - \overline{\tau})^{-1}$$

eine prinzipale Polarisierung auf $A(\mathcal{A}_\tau)$.

Eine analoge Aussagen können wir zeigen, falls

$$\xi = f'(w)(\eta - \overline{\eta})^{-1}$$

eine prinzipale Polarisierung auf $A(\mathcal{O}_K)$ definiert.

Beweis. Sei $\mathfrak{A} \in c'_K$ ein ganzes Ideal. Da K_0 Klassenzahl eins hat, existiert eine $\mathcal{O}_{K_0}$-Basis von $\mathfrak{A}$ mit nur zwei Elementen. Wir können also schreiben:

$$\mathfrak{A} = (\alpha\eta + \beta)\mathcal{O}_{K_0} + (\gamma\eta + \delta)\mathcal{O}_{K_0}.$$

Weiter haben wir

$$\mathfrak{A}\overline{\mathfrak{A}} = (\alpha\delta - \beta\gamma),$$

und da $\mathfrak{A} \in c'_K$, folgt, daß $\alpha\delta - \beta\gamma$ in K_0 total positiv ist.
Wir ordnen $\mathfrak{A}$ die Zahl

$$\tau = \frac{\alpha\eta + \beta}{\gamma\eta + \delta}$$

zu. Man rechnet leicht nach, daß die Imaginärteile von η und τ stets das gleiche Vorzeichen haben, da $\alpha\delta - \gamma\eta$ total positiv ist.
Für $\mathfrak{A}_\tau = \mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}$ ist $\mathfrak{A}_\tau\overline{\mathfrak{A}_\tau} = \alpha_\tau = \frac{\text{Im } \tau}{\text{Im } \eta}$ die Relativnorm. Somit ist α_τ stets positiv.
Wir setzen $\xi_\tau := (\gamma\alpha_\tau)^{-1} = \left(\gamma\frac{\text{Im } \tau}{\text{Im } \eta}\right)^{-1}$. Für $\gamma = (-f'(w)(\eta - \overline{\eta}))^{-1}$ ergibt sich, z.B.

$$\xi_\tau = (-(\tau - \overline{\tau})f'(w))^{-1}.$$

□

Bemerkung 4.1.4. Betrachten wir nun den CM-Typ

$$(K, \Phi) = (K, \{1, \varphi_1, \varphi_2\}) = (K, \{1, \rho\hat{\sigma}_1, \hat{\sigma}_2).$$

Dann ist eine Abelsche Varietät zu diesem CM-Typ durch ein Tripel komplexer Zahlen $(\tau, \tau^{\varphi_1}, \tau^{\varphi_2})$ gegeben mit

$$\begin{aligned} &\mathrm{Im}\tau > 0, \\ &\mathrm{Im}\tau^{\varphi_1} < 0 \text{ und} \\ &\mathrm{Im}\tau^{\varphi_2} > 0. \end{aligned}$$

4.1.5 Das Repräsentantensystem

Sei $(K, \Phi) = (K, \{\varphi_1, \dots, \varphi_g\})$ ein geeigneter CM-Typ und $\epsilon_1, \dots, \epsilon_d$ ein Repräsentantensystem von U^+/U_1. Weiter sei $\{\tau_1, \dots \tau_{h'}\}$ ein Repräsentantensystem von c'_K mit τ_i wie in (4.1.4). Dann ist das Repräsentantensystem aller Isomorphieklassen prinzipal polarisierter Abelscher Varietäten durch

$$K_\Phi = \{(\epsilon_j \tau_i^{\varphi_1}, \dots, \epsilon_j \tau_i^{\varphi_g}) : i = 1, \dots, h', j = 1, \dots, d\}$$

gegeben (siehe auch S. 6).

Wir betrachten nun den Fall $g = 3$ genauer. Es seinen ϵ_1, ϵ_2 die zwei Fundamentaleinheiten und $u_1, \dots, u_d$ ein Repräsentantenssystem von U^+/U_1.
Weiter legen wir (wie auf Seite 67 beschrieben) die drei Einbettungen $\{id, \sigma_1, \sigma_2\}$ von K_0 nach $\mathbb{R}$ festgelegt. Die beiden Fundamentaleinheiten wählen wir so, daß sie in K_0 einen positiven Absolutbetrag haben.
Wir setzen $d = |U^+/U_1|$.
Sei nun $\alpha \in K_0$ bezüglich einer Ganzheitsbasis gegeben und $\alpha > 0$. Dann können wir sagen, was wir unter dem Einbettungstyp von α verstehen: Der **Einbettungstyp** sei

gleich 1,	falls α total positiv ist,
gleich 2,	falls $\alpha^{\sigma_1} < 0$ und $\alpha^{\sigma_2} > 0$,
gleich 3,	falls $\alpha^{\sigma_1} > 0$ und $\alpha^{\sigma_2} < 0$,
und gleich 4,	falls $\alpha^{\sigma_1} < 0$ und $\alpha^{\sigma_2} < 0$.

Wir wollen nun folgende Beobachtungen festhalten:

1. Falls ϵ_1, ϵ_2 beide nicht total positiv sind und ϵ_1, ϵ_2 unterschiedlichen Einbettungstyp haben, dann gilt $d = 1$.

2. Falls ϵ_i einen Einbettungstyp $\neq 1$ hat, dann gilt $|c'_K| \geq \frac{1}{2}|c_K|$ und $d \leq 2$.

3. Falls ϵ_1, ϵ_2 beide vom Typ 1 sind, können wir vorab keine besseren Aussagen als $|c'_K| \geq \frac{1}{4}|c_K|$ machen.

Angenommen $(K, \{1, \varphi_1, \varphi_2\})$ ist ein geeigneter CM-Typ, ϵ_1, ϵ_2 seien Fundamentaleinheiten von K_0 und $\tau_1, \dots \tau_{h'}$ ein Repräsentantensystem von c'_k mit Im $\tau_i > 0$ und Im $\tau_i^{\varphi_2} < 0$ und Im $\tau_i^{\varphi_2} > 0$.

Wir möchten nun ein vollständiges Repräsentantensystem für alle CM-Typen (K, Φ) zu K angeben. Zunächst einmal gibt es $2^3 = 8$ mögliche CM-Typen. Falls die Galoisgruppe des Galoisschen Abschlusses L von K isomorph zu $\mathrm{Gal}(L_0, \mathbb{Q}) \times \mathbb{Z}/2\mathbb{Z}$ ist, sind nur sechs Typen davon primitiv. In diesem Fall entfernen wir die zwei nicht-primitiven CM-Typen aus dem Repräsentantensystem.
Weiter gilt, daß die Repräsentantensysteme von (K, Φ) und $(K, \overline{\Phi})$ übereinstimmen, da mit $\mathfrak{A} \in c'_K$ auch $\overline{\mathfrak{A}} \in c'_K$. Wir können uns also auf die Bestimmung von Repräsentantensystemen Abelscher Varietäten zu CM-Typen der Form $(K, \{\psi_1, \psi_2, \psi_3\})$ beschränken, wobei $\psi_1 = 1$.
Analog zu $g = 2$ ([56]) läßt sich noch der folgende Satz zeigen:

Satz 4.1.5. *Falls K Galoissch ist, dann sind die Repräsentantensysteme aller primitiven CM-Typen identisch.*

Beweis. Sei G die Galoisgruppe von K über $\mathbb{Q}$ und $H = \{\psi_1, \psi_2, \psi_3\}$ die Untergruppe der Ordnung drei. Nach den Bemerkungen oben und Lemma 4.1.1 können wir den Beweis auf die folgenden drei primitiven CM-Typen reduzieren:

1. $\Phi_1 = \{\psi_1, \rho\psi_2, \psi_3\}$
2. $\Phi_2 = \{\psi_1, \psi_2, \rho\psi_3\}$
3. $\Phi_3 = \{\psi_1, \rho\psi_2, \rho\psi_3\}$.

O.B.d.A. zeigen wir, daß die prinzipal polarisierten Abelschen Varietäten vom Typ 1 mit den prinzipal polarisierten Abelschen Varietäten vom Typ 2 übereinstimmen.
Es seien

$$\Psi_1(\mathfrak{A}) = \{(\alpha^{\psi_1}, \alpha^{\rho\psi_2}, \alpha^{\psi_3}) : \alpha \in \mathfrak{A}\} \text{ und } \Psi_2(\mathfrak{A}) = \{(\alpha^{\psi_1}, \alpha^{\psi_2}, \alpha^{\rho\psi_3}) : \alpha \in \mathfrak{A}\}.$$

Setze $\beta := \alpha^{\rho\psi_2}$. Dann gilt

$$\Psi_1(\mathfrak{B}) = \{(\alpha^{\rho\psi_2}, \alpha^{\psi_3}, \alpha^{\rho\psi_1}) : \alpha \in \mathfrak{A}\} = \{(\alpha^{\psi_2}, \alpha^{\rho\psi_3}, \alpha^{\psi_1}) : \alpha \in \overline{\mathfrak{A}}\}.$$

Somit sind die Gitter $\Psi_1(\mathfrak{B})$ und $\Psi_2(\mathfrak{A})$ äquivalent. Da die Definition des CM-Typs von der gewählten Polarisierung unabhängig ist, gibt es eine zu $\Psi_2(\mathfrak{A})$ äquivalente Matrix vom Typ Ψ_2, die zu $\Psi_1(\mathfrak{B})$ isomorph ist. Damit sind die Mengen der Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten von beiden Typen gleich. □

Wir zeigen exemplarisch, wie wir für den CM-Typ $(K, \{1, \hat{\sigma}_1, \hat{\sigma}_2\})$ ein Repräsentantensystem finden:

FALL 1: Es existiert eine Fundamentaleinheit $\epsilon_j \in K_0$ mit $\epsilon_j > 0$, $\epsilon_j^{\sigma_1} < 0$, $\epsilon_j^{\sigma_2} > 0$. Falls dann $\tau_i \in c'_K$, dann gilt

$$\text{Im } (\epsilon_j \tau_i) > 0, \text{Im } (\epsilon_j \tau_i)^{\hat{\sigma}_1} < 0 \text{ und Im } (\epsilon_j \tau_i)^{\hat{\sigma}_2} > 0,$$

und das Tripel $((\epsilon_j \tau_i), (\epsilon_j \tau_i)^{\hat{\sigma}_1}), (\epsilon_j \tau_i)^{\hat{\sigma}_2})$ definiert eine prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K, \{1, \hat{\sigma}_1, \hat{\sigma}_2\})$.

FALL 2: Es existiert keine solche Fundamentaleinheit. Dann gibt es keine prinzipale Polarisierung auf $A(\mathcal{O}_K)$. Falls $c_K = c'_K$, dann gibt es auch kein anderes Ideal $\mathfrak{A}$, so daß es zu $A(\mathfrak{A})$ eine prinzipale Polarisierung gibt.
Angenommen, es existiert ein $\tilde{\tau}_i \in c_K - c'_K$ mit

$$\text{Im } \tilde{\tau}_i > 0, \text{Im } \tilde{\tau}_i^{\hat{\sigma}_1} < 0 \text{ und Im } \tilde{\tau}_i^{\hat{\sigma}_2} > 0,$$

dann gilt

$$\text{Im } \tilde{\tau}_i > 0, \text{Im } \tilde{\tau}_i^{\hat{\sigma}_1} < 0 \text{ und Im } \tilde{\tau}_i^{\hat{\sigma}_2} > 0.$$

Also definiert das Tripel $(\tilde{\tau}_i, \tilde{\tau}_i^{\hat{\sigma}_1}, \tilde{\tau}_i^{\hat{\sigma}_2})$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K, \{1, \hat{\sigma}_1, \hat{\sigma}_2\})$.

Analog bestimmen wir die Repräsentantenysteme zu den restlichen CM-Typen.

So ergibt sich das folgende Resultat:
Es seien ϵ_1, ϵ_2 die Fundamentaleinheiten von K_0, $\tilde{\epsilon}_i$, $i = 1, \ldots d$, ein Fundamentalsystem von U^+/U_1, $\tau_i, i = 1, \ldots h'$ ein Repräsentantensystem der total positiven Klassengruppe von K und $\tilde{\tau}_i$ ein Repräsentantensystem von $h - h'$. Dann ist ein Repräsentantensystem aller Isomorphieklassen prinzipal polarisierter Abelscher Varietäten mit Endomorphismenring $\mathcal{O}_K$ durch

$$\mathcal{K} = \bigcup_{i=1}^{4} \mathcal{K}_i, \text{ falls } K \text{ nicht Galoissch}$$

gegeben, wobei

$$\mathcal{K}_1 = \{(\tilde{\epsilon}_j\tau_i, (\tilde{\epsilon}_j\tau_i)^{\varphi_1}, (\tilde{\epsilon}_j\tau_i)^{\varphi_2}), i = 1, \dots, h', j = 1, \dots, d\}$$

$$\mathcal{K}_2 = \begin{cases} \{(\tilde{\epsilon}_j\epsilon_k\tau_i, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\overline{\varphi_1}}, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\varphi_2}), i = 1, \dots, h', j = 1, \dots, d\} & \text{falls } \epsilon_k \text{ ex. mit } \epsilon_k > 0, \\ & \epsilon_k^{\varphi_1} < 0 \text{ und } \epsilon_k^{\varphi_2} > 0. \\ \{(\tilde{\epsilon}_j\tilde{\tau}_i, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\overline{\varphi_1}}, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\varphi_2}), j = 1, \dots, d\} & \text{falls } \tilde{\tau}_i \in c_K - c'_K \text{ ex.} \\ & \text{mit } N_{K/K_0}(\tilde{\tau}_i) \text{ vom} \\ & \text{Einbettungstyp 2.} \end{cases}$$

$$\mathcal{K}_3 = \begin{cases} \{(\tilde{\epsilon}_j\epsilon_k\tau_i, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\varphi_1}, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\overline{\varphi_2}}), i = 1, \dots, h', j = 1, \dots, d\} & \text{falls } \epsilon_k \text{ ex. mit } \epsilon_k > 0, \\ & \epsilon_k^{\varphi_1} > 0 \text{ und } \epsilon_k^{\varphi_2} < 0. \\ \{(\tilde{\epsilon}_j\tilde{\tau}_i, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\varphi_1}, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\overline{\varphi_2}}), j = 1, \dots, d\} & \text{falls } \tilde{\tau}_i \in c_K - c'_K \text{ ex.} \\ & \text{mit } N_{K/K_0}(\tilde{\tau}_i) \text{ vom} \\ & \text{Einbettungstyp 3.} \end{cases}$$

$$\mathcal{K}_4 = \begin{cases} \{(\tilde{\epsilon}_j\epsilon_k\tau_i, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\overline{\varphi_1}}, (\tilde{\epsilon}_j\epsilon_k\tau_i)^{\overline{\varphi_2}}), i = 1, \dots, h', j = 1, \dots, d\} & \text{falls } \epsilon_k \text{ ex. mit } \epsilon_k > 0, \\ & \epsilon_k^{\varphi_1} < 0 \text{ und } \epsilon_k^{\varphi_2} < 0. \\ \{(\tilde{\epsilon}_j\tilde{\tau}_i, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\overline{\varphi_1}}, (\tilde{\epsilon}_j\tilde{\tau}_i)^{\overline{\varphi_2}}), j = 1, \dots, d\} & \text{falls } \tilde{\tau}_i \in c_K - c'_K \text{ ex.} \\ & \text{mit } N_{K/K_0}(\tilde{\tau}_i) \text{ vom} \\ & \text{Einbettungstyp 4.} \end{cases}$$

Bemerkung 4.1.6.

- Das oben angegebene Repräsentantensystem kann auch nicht-einfache Abelsche Varietäten enthalten. Um nur einfache prinzipal polarisierte Abelsche Varietäten zu erhalten, müssen wir noch den nicht-primitiven CM-Typ ausschließen.
  Falls K Galoissch, ergibt sich das Repräsentantensystem nach Satz 4.1.5 schon aus einem einzigen CM-Typ.

- Bei unserem Repräsentantensystem haben wir angenommen, daß die Ideale der Klassengruppe vorher in die Nebenklassen bezüglich c'_K aufgeteilt wurde. Wenn etwa eine Fundamentaleinheit vom Einbettungstyp zwei existiert, dann gibt es nur noch zwei Nebenklassen. Eine Nebenklasse enthält τ_i mit $N_{K/K_0}(\tau_i)$ total positiv. Die andere Nebenklasse enthält nur Elemente τ_i mit $N_{K/K_0}(\tau_i)$ vom Einbettungstyp drei (oder vom Einbettungstyp vier).
  Dies ist programmiertechnisch sehr aufwendig, deshalb geht man bei der Implementierung anders vor. Wir teilen die Elemente τ_i der Klassengruppe gemäß des Einbettungstyps ihrer relativen Normen $N_{K/K_0}(\tau_i)$ in vier Klassen ein. Dies bedeutet, wir erhalten unter Umständen auch dann vier Klassen, wenn der Index von c'_K in c_K kleiner als vier ist.
  Das Repräsentantensystem berechnen wir dann ähnlich wie oben. Allerdings muß noch folgende Situation berücksichtigt werden:

Angenommen es gibt ein Element τ_i, dessen relative Norm $N_{K/K_0}(\tau_i)$ Einbettungstyp vier hat und es gibt eine Fundamentaleinheit ϵ_i, dessen Einbettungstyp gleich drei ist. Dann erhalten wir eine weitere Abelsche Varietät vom CM-Typ $(K, \{1, \overline{\varphi_1}, \varphi_2\})$, nämlich $(\epsilon_i\tau_i, (\epsilon_i\tau_i)^{\overline{\varphi_1}}, (\epsilon_i\tau_i)^{\varphi_2})$.

4.1.6 Berechnung der Periodenmatrix

Der Fall $[K : \mathbb{Q}] = 6$

Sei $f(x) = x^3+a_1x^2+a_2x+a_3$ das Minimalpolynom, das den reellen Teilkörper $K_0 = \mathbb{Q}(w)$ vom Grad 3 über $\mathbb{Q}$ erzeugt. Dann gilt

$$\begin{aligned} w^3 &= -a_1w^2 - a_2w - a_3 \text{ und} \\ w^4 &= ((a_1^2 - a_2)w^2 + (a_1a_2 - a_3)w + a_3a_1. \end{aligned} \tag{4.1}$$

Wir nehmen an, daß wir für den CM-Typ

$$(K, \{\varphi_1, \varphi_2, \varphi_3\}) = (K, \{1, \rho\hat{\sigma_1}, \hat{\sigma_2}\})$$

gewählt haben, so daß

$$\xi = -(f'(w)(\tau - \overline{\tau}))^{-1}$$

eine prinzipale Polarisierung definiert.
Wir wählen als Basis

$$\begin{array}{lll} \alpha_1 = \tau(w^2 + a_1w + a_2), & \alpha_2 = \tau w, & \alpha_3 = \tau, \\ \alpha_4 = 1, & \alpha_5 = w, & \alpha_6 = w^2 + a_1w. \end{array} \tag{4.2}$$

Dies ist offensichtlich eine $\mathbb{Z}$-Basis. Sei

$$E_\xi(x, y) = \sum_{i=1}^{3} \xi^{\varphi_i}(\overline{x}_iy_i - \overline{y}_ix_i) \text{ mit } x_i = x^{\varphi_i}.$$

Wir zeigen nun, daß die Basis (4.2) $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$ eine symplektische Basis bezüglich E_ξ ist. Dabei schreiben wir statt $E(\Phi(\alpha_i), \Phi(\alpha_j))$ mit $\Phi(\alpha_i) = (\varphi_1(\alpha_i), \varphi_2(\alpha_i), \varphi_3(\alpha_i))^t$ abkürzend $E(\alpha_i, \alpha_j)$.
In der Tat gilt offensichtlich

$$\begin{aligned} &E_\xi(\alpha_1, \alpha_2) = E_\xi(\alpha_1, \alpha_3) = E_\xi(\alpha_2, \alpha_3) = E_\xi(\alpha_4, \alpha_5) \\ &= E_\xi(\alpha_4, \alpha_6) = E_\xi(\alpha_5, \alpha_6) = E_\xi(\alpha_i, \alpha_i) = 0, \end{aligned}$$

weil hier alle Summanden gleich 0 sind.
Für die anderen Werte weisen wir auf folgende Identitäten hin:

$$\begin{aligned} \frac{1}{f'(w)} + \frac{1}{f'(w^{\sigma_1})} + \frac{1}{f'(w^{\sigma_2})} &= 0 \\ \frac{w}{f'(w)} + \frac{w^{\sigma_1}}{f'(w^{\sigma_1})} + \frac{w^{\sigma_2}}{f'(w^{\sigma_2})} &= 0 \\ \frac{(w)^2}{f'(w)} + \frac{(w^{\sigma_1})^2}{f'(w^{\sigma_1})} + \frac{(w^{\sigma_2})^2}{f'(w^{\sigma_2})} &= 0. \end{aligned} \tag{4.3}$$

Aus den Gleichungen (4.3) folgt nun einfach

$$E_\xi(\alpha_1,\alpha_4) = 1 = -E_\xi(\alpha_4,\alpha_1)$$
$$E_\xi(\alpha_2,\alpha_5) = 1 = -E_\xi(\alpha_5,\alpha_2)$$
$$E_\xi(\alpha_3,\alpha_6) = 1 = -E_\xi(\alpha_6,\alpha_3).$$

Unter Verwendung von (4.3) und (4.1) läßt sich schließlich noch

$$E_\xi(\alpha_1,\alpha_5) = E_\xi(\alpha_1,\alpha_6) = 0$$

zeigen.
Das Gitter $\Lambda(\mathfrak{A}_\tau)$ für das Ideal $\mathfrak{A}_\tau = \mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}$ wird also durch $\mathcal{A}_1\mathbb{Z}^3 + \mathcal{A}_2\mathbb{Z}^3$ mit

$$\mathcal{A}_1 = \begin{pmatrix} \tau^{\varphi_1}((w^{\varphi_1})^2 + a_1w^{\varphi_1} + a_2) & \tau^{\varphi_1}w^{\varphi_1} & \tau^{\varphi_1} \\ \tau^{\varphi_2}((w^{\varphi_2})^2 + a_1w^{\varphi_2} + a_2) & \tau^{\varphi_2}w^{\varphi_2} & \tau^{\varphi_2} \\ \tau^{\varphi_3}((w^{\varphi_3})^2 + a_1w^{\varphi_3} + a_2) & \tau^{\varphi_3}w^{\varphi_3} & \tau^{\varphi_3} \end{pmatrix}$$

und

$$\mathcal{A}_2 = \begin{pmatrix} 1 & w^{\varphi_1} & ((w^{\varphi_1})^2 + a_1w^{\varphi_1} + a_2) \\ 1 & w^{\varphi_2} & ((w^{\varphi_2})^2 + a_1w^{\varphi_2} + a_2) \\ 1 & w^{\varphi_3} & ((w^{\varphi_3})^2 + a_1w^{\varphi_3} + a_2) \end{pmatrix}$$

beschrieben.
Die Gitter

$$\mathcal{A}_1\mathbb{Z}^3 + \mathcal{A}_2\mathbb{Z}^3 \text{ und } \mathcal{A}_2^{-1}\mathcal{A}_1\mathbb{Z}^3 + \mathbb{Z}^3$$

sind äquivalent. Da wir die Basis symplektisch gewählt haben, liegt $\mathcal{A}_2^{-1}\mathcal{A}_1$ in der Siegelschen oberen Halbebene $\mathbb{H}_3$ ([29], Seite 134).
Um die Periodenmatrix anzugeben, vereinfachen wir zunächst die Schreibweise. Wir führen folgende Abkürzungen ein:

$$\begin{aligned} w_i &:= w^{\varphi_i}, \\ \tau_i &:= \tau^{\varphi_i}, \\ \alpha_{1,i} &:= w_i^2 + a_1w_i + a_2, \\ w_{ij} &:= w_i - w_j, \\ s_{ij} &:= w_i + w_j + a_1 = -w_k + 2a_1 \text{ für } k \neq i,j, \\ wt_{ij} &:= w_{ij}\tau_k \text{ für } k \neq i,j, \\ W_{ij} &:= wt_{ij} \cdot w_i \cdot w_j \text{ und} \\ S_{ij} &:= wt_{ij}s_{ij}. \end{aligned}$$

Damit ergibt sich nun

$$\begin{aligned} \mathcal{A}_2^{-1}\mathcal{A}_1 &= \frac{1}{(w_1-w_2)(w_1-w_3)(w_2-w_3)}\mathcal{B} \\ &= \frac{1}{w_{12}w_{13}w_{23}}\mathcal{B} \end{aligned}$$

mit

$$\mathcal{B} = \begin{pmatrix} W_{23}\alpha_{11} + W_{31}\alpha_{12} + W_{12}\alpha_{13} & a_3 \cdot (wt_{23} + wt_{31} + wt_{21}) & W_{23} + W_{31} + W_{12} \\ S_{32}\alpha_{11} + S_{13}\alpha_{12} + S_{12}\alpha_{13} & S_{32}w_1 + S_{13}w_2 + S_{21}w_3 & S_{32} + S_{13} + S_{21} \\ wt_{23}\alpha_{11} + wt_{31}\alpha_{12} + wt_{12}\alpha_{13} & wt_{23}w_1 + wt_{31}w_2 + wt_{12}w_3 & wt_{23} + wt_{31} + wt_{12} \end{pmatrix}.$$

Bemerkung 4.1.7. 1. Falls die prinzipale Polarisierung durch

$$\xi = (f'(w)(\tau - \overline{\tau}))^{-1}$$

gegeben ist, dann ergibt sich als Periodenmatrix gerade $-\frac{1}{(w_1-w_2)(w_1-w_3)(w_2-w_3)}\mathcal{B}$.

2. Die Periodenmatrix liegt stets in der Siegelschen oberen Halbebene $\mathbb{H}_3$, d.h. sie ist symmetrisch. Dies sieht man der vorliegenden Matrix nicht ohne weiteres an. Wir wollen exemplarisch nachrechnen, daß $\mathcal{B}_{13} = \mathcal{B}_{31}$:
Es gilt

$$\begin{aligned} \mathcal{B}_{13} &= (w_2 - w_3)\tau_1 w_2 w_3 + (w_3 - w_1)\tau_2 w_1 w_3 + (w_1 - w_2)\tau_3 w_2 w_1 \text{ und} \\ \mathcal{B}_{31} &= (w_2 - w_3)\tau_1(w_1^2 + a_1 w_1 + a_2) + (w_3 - w_1)\tau_2(w_2^2 + a_1 w_2 + a_2) \\ &\quad + (w_1 - w_2)\tau_3(w_3^2 + a_1 w_3 + a_2). \end{aligned}$$

Nun haben wir

$$w_1^2 + a_1 w_1 + a_2 = \frac{f(w_1) - a_3}{w_1} = -\frac{a_3}{w_1} = w_2 w_3.$$

Daraus ergibt sich die Gleichheit.

Der Fall $[K : \mathbb{Q}] = 8$

Wir nehmen hier wieder an, daß der CM-Typ so gewählt ist, daß $\xi = -(f'(w)(\tau - \overline{\tau}))^{-1}$ eine prinzipale Polarisierung ist. Diesmal gilt dann,

$$\begin{aligned} \sum_{i=1}^{n} \frac{(w^{\varphi_i})^k}{f'(w^{\varphi_i})} &= 0 \text{ für } k = 0, 1, 2 \text{ und} \\ \sum_{i=1}^{n} \frac{(w^{\varphi_i})^3}{f'(w^{\varphi_i})} &= 1. \end{aligned}$$

Durch das Minimalpolynom lassen sich Potenzen von w vom Grad größer als vier durch ein Polynom vom Grad kleiner als drei ausdrücken. Damit zeigt man, daß die folgende Basis bezüglich E_ξ symplektisch ist [1]:

$$\begin{aligned} &\alpha_1 = \tau(w^3 + a_1 w^2 + a_2 w + a_3), \alpha_2 = \tau w^2, \alpha_3 = \tau w, \alpha_4 = \tau, \\ &\alpha_5 = 1, \alpha_6 = w, \alpha_7 = w^2, \alpha_8 = w^3 + a_1 w^2 + a_2 w. \end{aligned}$$

[1] Analog können wir in höheren Dimensionen die Periodenmatrix bestimmen, falls $\mathcal{O}_{K_0}$ monogen ist.

Das Gitter $\mathfrak{A}_\tau = \mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}$ wird durch das Gitter $\mathcal{A}_1\mathbb{Z}^4 + \mathcal{A}_2\mathbb{Z}^4$ beschrieben, wobei

$$\mathcal{A}_1 := \begin{pmatrix} \tau^{\varphi_1}((w^{\varphi_1})^3 + a_1(w^{\varphi_1})^2 + a_2w^{\varphi_1} + a_3 & \tau^{\varphi_1}(w^{\varphi_1})^2 & \tau_{\varphi_1}w^{\varphi_1} & \tau_{\varphi_1} \\ \tau^{\varphi_2}((w^{\varphi_2})^3 + a_1(w^{\varphi_2})^2 + a_2w^{\varphi_2} + a_3 & \tau^{\varphi_2}(w^{\varphi_2})^2 & \tau_{\varphi_1}w^{\varphi_2} & \tau_{\varphi_2} \\ \tau^{\varphi_3}((w^{\varphi_3})^3 + a_1(w^{\varphi_3})^2 + a_2w^{\varphi_3} + a_3 & \tau^{\varphi_3}(w^{\varphi_3})^2 & \tau_{\varphi_3}w^{\varphi_3} & \tau_{\varphi_3} \\ \tau^{\varphi_4}((w^{\varphi_4})^3 + a_1(w^{\varphi_4})^2 + a_2w^{\varphi_4} + a_3 & \tau^{\varphi_4}(w^{\varphi_4})^2 & \tau_{\varphi_4}w^{\varphi_4} & \tau_{\varphi_4} \end{pmatrix}$$

und

$$\mathcal{A}_2 := \begin{pmatrix} 1 & w^{\varphi_1} & (w^{\varphi_1})^2 & (w^{\varphi_1})^3 + a_1(w^{\varphi_1})^2 + a_2w^{\varphi_1} \\ 1 & w^{\varphi_2} & (w^{\varphi_2})^2 & (w^{\varphi_2})^3 + a_1(w^{\varphi_2})^2 + a_2w^{\varphi_2} \\ 1 & w^{\varphi_3} & (w^{\varphi_3})^2 & (w^{\varphi_3})^3 + a_1(w^{\varphi_3})^2 + a_2w^{\varphi_3} \\ 1 & w^{\varphi_4} & (w^{\varphi_4})^2 & (w^{\varphi_4})^3 + a_1(w^{\varphi_4})^2 + a_2w^{\varphi_4} \end{pmatrix}.$$

Wir führen nun wieder einige abkürzende Bezeichnungen ein:

$$\begin{aligned} w_i &:= w^{\sigma_i}, \\ \tau_i &:= \tau^{\varphi_i}, \\ w_{ij} &:= w_i - w_j, \\ \alpha_{1,i} &:= (w_i^{\varphi})^3 + a_1(w_i^{\varphi})^2 + a_2(w_i^{\varphi}) + a_3, \\ p_i &:= \prod_{k\neq i} w_k, \text{ z.B. } p_1 = w_1w_3w_4 \\ P_i &:= \prod_{\substack{j,k\neq i \\ j<k}} w_{jk} = \prod_{\substack{j,k\neq i \\ j<k}} (w_j - w_k), \\ s_i &:= \prod_{\substack{j,k\neq i \\ j<k}} w_{jk} - a_2 \text{ und} \\ \sigma_i &:= \sum_{k\neq i} w_k + a_1. \end{aligned}$$

Dann gilt

$$\mathcal{A}_2^{-1}\mathcal{A}_1 = \frac{1}{\prod\limits_{1\leq i<j\leq 4} w_{ij}}\mathcal{B}$$

mit

$$\mathcal{B} = \begin{pmatrix} \sum\limits_{i=1}^{4}(-1)^iP_ip_i\tau_i\alpha_{1,i} & a_4\sum\limits_{i=1}^{4}(-1)^iP_iw_i\tau_i & a_4\sum\limits_{i=1}^{4}(-1)^iP_i\tau_i & \sum\limits_{i=1}^{4}(-1)^iP_ip_i\tau_i \\ \sum\limits_{i=1}^{4}(-1)^{i+1}P_is_i\tau_i\alpha_{1,i} & \sum\limits_{i=1}^{4}(-1)^{i+1}P_is_i\tau_iw_i^2 & \sum\limits_{i=1}^{4}(-1)^{i+1}P_is_i\tau_iw_i & \sum\limits_{i=1}^{4}(-1)^{i+1}P_is_i\tau_i \\ \sum\limits_{i=1}^{4}(-1)^iP_i\sigma_i\tau_i\alpha_{1,i} & \sum\limits_{i=1}^{4}(-1)^iP_i\sigma_i\tau_iw_i^2 & \sum\limits_{i=1}^{4}(-1)^iP_i\sigma_i\tau_iw_i & \sum\limits_{i=1}^{4}(-1)^iP_i\sigma_i\tau_i \\ \sum\limits_{i=1}^{4}(-1)^{i+1}P_i\tau_i\alpha_{1,i} & \sum\limits_{i=1}^{4}(-1)^iP_i\tau_iw_i^2 & \sum\limits_{i=1}^{4}(-1)^iP_i\tau_iw_i & \sum\limits_{i=1}^{4}(-1)^iP_i\tau_i \end{pmatrix}.$$

4.2 Von der Periodenmatrix zum Rosenhain-Modell

In diesem Abschnitt führen wir die Arbeit von Weber ([61]) weiter und leiten für den Fall Geschlecht $g = 3$ ein konkretes Kriterium ab, wann eine Periodenmatrix $\Omega \in \mathbb{H}_3$ die Jacobi-Varietät einer hyperelliptischen Kurve über $\mathbb{C}$ definiert (Satz 4.2.1).
Schließlich können wir für Geschlecht $g = 3$ sogar explizite Formeln für das Modell der hyperelliptischen Kurve über $\mathbb{C}$ angeben.
Wir verwenden die Notation aus Abschnitt 1.1.6.

4.2.1 Hyperelliptische Charakterisierung für Geschlecht drei

Aus Satz 1.1.15 ergibt sich, daß das azygetische Fundamentalsystem so gewählt werden muß, daß *die ungeraden Thetanullwerte den geraden Teilmengen T mit $\#(T \circ U) \neq g+1$ entsprechen*. Dies ist eine Einschränkung, die es uns ermöglicht hat, die Menge möglicher azygetischer Fundamentalsysteme zu reduzieren.
Wir nennen ein azygetisches Fundementalsystem $\{\eta_i\}$ mit $\eta_i \in (\mathbb{Z}/2\mathbb{Z})^{2g} - \{0\}$ **zulässig**, wenn die ungeraden Thetacharakteristiken in der Menge

$$M = \{\theta[\eta_T] : \#T \equiv 0 \mod 2, \#(T \circ U) \neq g+1\}$$

(siehe Satz 1.1.15) enthalten sind. Für jedes zulässige Fundamentalsystem gibt es dann genau eine gerade Thetacharakteristik, die in der Menge M enthalten ist.
Eine Periodenmatrix der Dimension drei ist nach Satz 1.1.15 genau dann hyperelliptisch, wenn es ein azgygetisches Fundamentalsystem mit

$$M = \left\{\theta[\eta] : \theta[\eta](0,\Omega) = 0, \eta = \begin{bmatrix}\delta\\ \epsilon\end{bmatrix}\right\}$$

gibt. Dies ist äquivalent dazu, daß genau ein gerader Thetanullwert $\theta[\eta]$ in Ω verschwindet und daß ein zulässiges azygetisches Fundamentalsystem existiert, so daß $\theta[\eta]$ in M.
Um dieses Kriterium zu konkretisieren, ermitteln wir die geraden Thetanullwerte $\theta[\eta]$, für die ein zulässiges azygetisches Fundamentalsystem mit $\theta[\eta] \in M$ existiert. Dies erreichen wir, indem wir die Elemente der Gruppe $Sp_6(\mathbb{F}_2)$ aufzählen und auf Mumfords azygetischem Fundamentalsystem auf Seite 13 operieren lassen.
Mit der Hilfe der Bibliothek Magma (siehe S. 129) können wir die Gruppe $Sp_6(\mathbb{F}_2)$ einfach beschreiben. Wir erreichten damit ein hinreichendes Kriterium, das schnell überprüft werden kann:

Satz 4.2.1. *Sei $\Omega \in \mathbb{H}_3$ eine beliebige Periodenmatrix. Dann sind folgende Aussagen äquivalent:*

1. *Ω ist hyperelliptisch.*
2. *Genau ein gerader Thetanullwert verwindet in Ω.*

Gestützt auf einige Beispiele, die wir berechnet haben, können wir die folgende Vermutung formulieren:

Vermutung 4.2.2. *Eine Periodenmatrix $\Omega \in \mathbb{H}_3$ mit komplexer Multiplikation gehört zu einer nicht-einfachen Abelschen Varietät, falls sechs bzw. neun Thetanullwerte (je nachdem, ob der CM-Körper nicht-triviale Einheitswurzeln enthält oder nicht) verschwinden.*

4.2.2 Das Rosenhain-Modell

Aus den Thetanullwerten kann das Rosenhain-Modell

$$y^2 = x(x-1)(x-\lambda_3)(x-\lambda_4)(x-\lambda_5)(x-\lambda_6)(x-\lambda_7)$$

berechnet werden. Wir geben nun explizite Formeln an, die davon abhängen, welcher der Thetanullwerte verschwindet.
Betrachte eine Aufzählung $t_1, \ldots, t_{36}$ der geraden Thetanullwerte:

$$\theta_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \theta_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \theta_4 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$\theta_5 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \theta_6 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \theta_7 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad \theta_8 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\theta_9 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{10} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \theta_{11} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \theta_{12} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

$$\theta_{13} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{14} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \theta_{15} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \theta_{16} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\theta_{17} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{18} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad \theta_{19} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \theta_{20} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\theta_{21} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{22} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \theta_{23} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad \theta_{24} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\theta_{25} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{26} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \theta_{27} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \theta_{28} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\theta_{29} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{30} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \theta_{31} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \theta_{32} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\theta_{33} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \theta_{34} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \theta_{35} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \theta_{36} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Wir setzen

$$\lambda_3 = \frac{(\alpha_{15}\alpha_3)^4 + (\alpha_{12}\alpha_1)^4 - (\alpha_{14}\alpha_2)^4}{2(\alpha_{15}\alpha_3)^4} =< \alpha_{15}, \alpha_3, \alpha_{12}, \alpha_1, \alpha_{14}, \alpha_2 >$$
$$\lambda_4 = \frac{(\alpha_4\alpha_9)^4 + (\alpha_6\alpha_{11})^4 - (\alpha_{13}\alpha_8)^4}{2(\alpha_4\alpha_9)^4} =< \alpha_4, \alpha_9, \alpha_6, \alpha_{11}, \alpha_{13}, \alpha_8 >$$
$$\lambda_5 = \frac{(\alpha_{10}\alpha_9)^4 + (\alpha_6\alpha_5)^4 - (\alpha_7\alpha_8)^4}{2(\alpha_{10}\alpha_9)^4} =< \alpha_{10}, \alpha_9, \alpha_6, \alpha_5, \alpha_7, \alpha_8 >$$
$$\lambda_6 = \frac{(\alpha_{10}\alpha_3)^4 + (\alpha_{12}\alpha_5)^4 - (\alpha_{14}\alpha_7)^4}{2(\alpha_{10}\alpha_3)} =< \alpha_{10}, \alpha_3, \alpha_{12}, \alpha_5, \alpha_{14}, \alpha_7 >$$
$$\lambda_7 = \frac{(\alpha_{15}\alpha_4)^4 + (\alpha_{11}\alpha_1)^4 - (\alpha_{13}\alpha_2)^4}{2(\alpha_{15}\alpha_4)^4} =< \alpha_{15}, \alpha_4, \alpha_{11}, \alpha_1, \alpha_{13}, \alpha_2 > .$$

Abhängig von dem Thetanullwert, der in Ω verschwindet, können wir nun die α_i festlegen:
1. Thetanullwert:

$$\alpha_1 = \theta_{33}, \alpha_2 = \theta_{23}, \alpha_3 = \theta_{30}, \alpha_4 = \theta_5, \alpha_5 = \theta_3, \alpha_6 = \theta_{22}, \alpha_7 = \theta_{17}, \alpha_8 = \theta_{34},$$
$$\alpha_9 = \theta_{16}, \alpha_{10} = \theta_{31}, \alpha_{11} = \theta_{29}, \alpha_{12} = \theta_6, \alpha_{13} = \theta_{26}, \alpha_{14} = \theta_{20}, \alpha_{15} = \theta_{11}.$$

2. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{35}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{12}, \alpha_5 = \theta_{36}, \alpha_6 = \theta_{19}, \alpha_7 = \theta_7, \alpha_8 = \theta_{22},$$
$$\alpha_9 = \theta_{15}, \alpha_{10} = \theta_{31}, \alpha_{11} = \theta_{14}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_{34}, \alpha_{14} = \theta_{27}, \alpha_{15} = \theta_9.$$

3. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{18}, \alpha_3 = \theta_{35}, \alpha_4 = \theta_{15}, \alpha_5 = \theta_{17}, \alpha_6 = \theta_{20}, \alpha_7 = \theta_4, \alpha_8 = \theta_5,$$
$$\alpha_9 = \theta_{25}, \alpha_{10} = \theta_{28}, \alpha_{11} = \theta_{24}, \alpha_{12} = \theta_{10}, \alpha_{13} = \theta_{33}, \alpha_{14} = \theta_{14}, \alpha_{15} = \theta_{32}.$$

4. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{16}, \alpha_3 = \theta_{11}, \alpha_4 = \theta_{29}, \alpha_5 = \theta_{31}, \alpha_6 = \theta_{15}, \alpha_7 = \theta_{24}, \alpha_8 = \theta_2,$$
$$\alpha_9 = \theta_{19}, \alpha_{10} = \theta_{36}, \alpha_{11} = \theta_{33}, \alpha_{12} = \theta_5, \alpha_{13} = \theta_{27}, \alpha_{14} = \theta_{14}, \alpha_{15} = \theta_9.$$

5. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{28}, \alpha_3 = \theta_{35}, \alpha_4 = \theta_{31}, \alpha_5 = \theta_{26}, \alpha_6 = \theta_{34}, \alpha_7 = \theta_6, \alpha_8 = \theta_{25},$$
$$\alpha_9 = \theta_{10}, \alpha_{10} = \theta_{28}, \alpha_{11} = \theta_8, \alpha_{12} = \theta_4, \alpha_{13} = \theta_{25}, \alpha_{14} = \theta_{24}, \alpha_{15} = \theta_{30}.$$

6.Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{30}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{23}, \alpha_5 = \theta_{31}, \alpha_6 = \theta_{29}, \alpha_7 = \theta_8, \alpha_8 = \theta_2,$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_{36}, \alpha_{11} = \theta_{26}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_{18}, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_9.$$

7.Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{28}, \alpha_3 = \theta_{18}, \alpha_4 = \theta_{23}, \alpha_5 = \theta_{25}, \alpha_6 = \theta_{27}, \alpha_7 = \theta_8, \alpha_8 = \theta_3,$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_{35}, \alpha_{11} = \theta_{32}, \alpha_{12} = \theta_{12}, \alpha_{13} = \theta_{17}, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_{16}.$$

8. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{16}, \alpha_3 = \theta_{21}, \alpha_4 = \theta_{11}, \alpha_5 = \theta_{12}, \alpha_6 = \theta_{33}, \alpha_7 = \theta_{18}, \alpha_8 = \theta_{27},$$
$$\alpha_9 = \theta_{29}, \alpha_{10} = \theta_7, \alpha_{11} = \theta_5, \alpha_{12} = \theta_{25}, \alpha_{13} = \theta_{14}, \alpha_{14} = \theta_{35}, \alpha_{15} = \theta_9.$$

9. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_6, \alpha_3 = \theta_{30}, \alpha_4 = \theta_{20}, \alpha_5 = \theta_4, \alpha_6 = \theta_{34}, \alpha_7 = \theta_7, \alpha_8 = \theta_{36},$$
$$\alpha_9 = \theta_{21}, \alpha_{10} = \theta_{17}, \alpha_{11} = \theta_5, \alpha_{12} = \theta_{26}, \alpha_{13} = \theta_2, \alpha_{14} = \theta_{28}, \alpha_{15} = \theta_{18}.$$

10. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{24}, \alpha_3 = \theta_6, \alpha_4 = \theta_{19}, \alpha_5 = \theta_{17}, \alpha_6 = \theta_{28}, \alpha_7 = \theta_{34}, \alpha_8 = \theta_{11},$$
$$\alpha_9 = \theta_{25}, \alpha_{10} = \theta_{20}, \alpha_{11} = \theta_{18}, \alpha_{12} = \theta_3, \alpha_{13} = \theta_{33}, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_8.$$

11. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{20}, \alpha_3 = \theta_6, \alpha_4 = \theta_{31}, \alpha_5 = \theta_{23}, \alpha_6 = \theta_4, \alpha_7 = \theta_{35}, \alpha_8 = \theta_{19},$$
$$\alpha_9 = \theta_3, \alpha_{10} = \theta_{24}, \alpha_{11} = \theta_{32}, \alpha_{12} = \theta_5, \alpha_{13} = \theta_{25}, \alpha_{14} = \theta_{18}, \alpha_{15} = \theta_2.$$

12. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{32}, \alpha_3 = \theta_4, \alpha_4 = \theta_{26}, \alpha_5 = \theta_{25}, \alpha_6 = \theta_{35}, \alpha_7 = \theta_{20}, \alpha_8 = \theta_{10},$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_{27}, \alpha_{11} = \theta_{28}, \alpha_{12} = \theta_7, \alpha_{13} = \theta_{17}, \alpha_{14} = \theta_{30}, \alpha_{15} = \theta_6.$$

13. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_8, \alpha_3 = \theta_{10}, \alpha_4 = \theta_{24}, \alpha_5 = \theta_{31}, \alpha_6 = \theta_{26}, \alpha_7 = \theta_{30}, \alpha_8 = \theta_{27},$$
$$\alpha_9 = \theta_9, \alpha_{10} = \theta_{15}, \alpha_{11} = \theta_2, \alpha_{12} = \theta_{25}, \alpha_{13} = \theta_7, \alpha_{14} = \theta_{28}, \alpha_{15} = \theta_{23}.$$

14. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{35}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{31}, \alpha_5 = \theta_{23}, \alpha_6 = \theta_{25}, \alpha_7 = \theta_{20}, \alpha_8 = \theta_{16},$$
$$\alpha_9 = \theta_{21}, \alpha_{10} = \theta_{26}, \alpha_{11} = \theta_{36}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_4, \alpha_{14} = \theta_{27}, \alpha_{15} = \theta_9.$$

15. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{20}, \alpha_3 = \theta_{27}, \alpha_4 = \theta_7, \alpha_5 = \theta_{10}, \alpha_6 = \theta_{18}, \alpha_7 = \theta_{16}, \alpha_8 = \theta_5,$$
$$\alpha_9 = \theta_{26}, \alpha_{10} = \theta_{34}, \alpha_{11} = \theta_{32}, \alpha_{12} = \theta_{19}, \alpha_{13} = \theta_{25}, \alpha_{14} = \theta_4, \alpha_{15} = \theta_{30}.$$

16. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_8, \alpha_3 = \theta_{11}, \alpha_4 = \theta_{21}, \alpha_5 = \theta_{26}, \alpha_6 = \theta_{19}, \alpha_7 = \theta_{27}, \alpha_8 = \theta_{18},$$
$$\alpha_9 = \theta_{15}, \alpha_{10} = \theta_{23}, \alpha_{11} = \theta_{25}, \alpha_{12} = \theta_5, \alpha_{13} = \theta_{28}, \alpha_{14} = \theta_4, \alpha_{15} = \theta_9.$$

17. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{26}, \alpha_3 = \theta_{22}, \alpha_4 = \theta_7, \alpha_5 = \theta_{31}, \alpha_6 = \theta_{23}, \alpha_7 = \theta_{19}, \alpha_8 = \theta_9,$$
$$\alpha_9 = \theta_{24}, \alpha_{10} = \theta_{32}, \alpha_{11} = \theta_8, \alpha_{12} = \theta_{21}, \alpha_{13} = \theta_{27}, \alpha_{14} = \theta_{10}, \alpha_{15} = \theta_2.$$

18. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_6, \alpha_3 = \theta_{23}, \alpha_4 = \theta_{11}, \alpha_5 = \theta_7, \alpha_6 = \theta_{36}, \alpha_7 = \theta_4, \alpha_8 = \theta_{34},$$
$$\alpha_9 = \theta_{31}, \alpha_{10} = \theta_{12}, \alpha_{11} = \theta_5, \alpha_{12} = \theta_{26}, \alpha_{13} = \theta_2, \alpha_{14} = \theta_{28}, \alpha_{15} = \theta_9.$$

19. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{32}, \alpha_3 = \theta_6, \alpha_4 = \theta_{12}, \alpha_5 = \theta_{10}, \alpha_6 = \theta_{34}, \alpha_7 = \theta_{35}, \alpha_8 = \theta_{11},$$
$$\alpha_9 = \theta_{26}, \alpha_{10} = \theta_{18}, \alpha_{11} = \theta_{20}, \alpha_{12} = \theta_{15}, \alpha_{13} = \theta_{25}, \alpha_{14} = \theta_{24}, \alpha_{15} = \theta_{14}.$$

20. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{30}, \alpha_3 = \theta_{33}, \alpha_4 = \theta_3, \alpha_5 = \theta_{11}, \alpha_6 = \theta_{13}, \alpha_7 = \theta_{35}, \alpha_8 = \theta_{22},$$
$$\alpha_9 = \theta_{17}, \alpha_{10} = \theta_5, \alpha_{11} = \theta_{10}, \alpha_{12} = \theta_{29}, \alpha_{13} = \theta_{34}, \alpha_{14} = \theta_2, \alpha_{15} = \theta_9.$$

21. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_8, \alpha_3 = \theta_{35}, \alpha_4 = \theta_{12}, \alpha_5 = \theta_{31}, \alpha_6 = \theta_{32}, \alpha_7 = \theta_{30}, \alpha_8 = \theta_{29},$$
$$\alpha_9 = \theta_{23}, \alpha_{10} = \theta_{24}, \alpha_{11} = \theta_{18}, \alpha_{12} = \theta_{25}, \alpha_{13} = \theta_{19}, \alpha_{14} = \theta_{28}, \alpha_{15} = \theta_{16}.$$

22. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{16}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{26}, \alpha_5 = \theta_{10}, \alpha_6 = \theta_5, \alpha_7 = \theta_{20}, \alpha_8 = \theta_{14},$$
$$\alpha_9 = \theta_{11}, \alpha_{10} = \theta_3, \alpha_{11} = \theta_{23}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_{32}, \alpha_{14} = \theta_6, \alpha_{15} = \theta_9.$$

23. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{34}, \alpha_3 = \theta_{27}, \alpha_4 = \theta_5, \alpha_5 = \theta_{17}, \alpha_6 = \theta_{28}, \alpha_7 = \theta_{24}, \alpha_8 = \theta_{15},$$
$$\alpha_9 = \theta_{25}, \alpha_{10} = \theta_{20}, \alpha_{11} = \theta_4, \alpha_{12} = \theta_{26}, \alpha_{13} = \theta_{33}, \alpha_{14} = \theta_{14}, \alpha_{15} = \theta_8.$$

24. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{35}, \alpha_3 = \theta_{29}, \alpha_4 = \theta_{26}, \alpha_5 = \theta_{10}, \alpha_6 = \theta_7, \alpha_7 = \theta_{32}, \alpha_8 = \theta_{34},$$
$$\alpha_9 = \theta_{12}, \alpha_{10} = \theta_3, \alpha_{11} = \theta_{23}, \alpha_{12} = \theta_{33}, \alpha_{13} = \theta_{20}, \alpha_{14} = \theta_6, \alpha_{15} = \theta_9.$$

25. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_2, \alpha_3 = \theta_{34}, \alpha_4 = \theta_{19}, \alpha_5 = \theta_5, \alpha_6 = \theta_{14}, \alpha_7 = \theta_6, \alpha_8 = \theta_{13},$$
$$\alpha_9 = \theta_{10}, \alpha_{10} = \theta_{20}, \alpha_{11} = \theta_8, \alpha_{12} = \theta_{21}, \alpha_{13} = \theta_7, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_{18}.$$

26. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{24}, \alpha_3 = \theta_{35}, \alpha_4 = \theta_5, \alpha_5 = \theta_{17}, \alpha_6 = \theta_{32}, \alpha_7 = \theta_{34}, \alpha_8 = \theta_{15},$$
$$\alpha_9 = \theta_{25}, \alpha_{10} = \theta_8, \alpha_{11} = \theta_{18}, \alpha_{12} = \theta_{23}, \alpha_{13} = \theta_{33}, \alpha_{14} = \theta_2, \alpha_{15} = \theta_{20}.$$

27. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{14}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{23}, \alpha_5 = \theta_{36}, \alpha_6 = \theta_{29}, \alpha_7 = \theta_{28}, \alpha_8 = \theta_{22},$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_{31}, \alpha_{11} = \theta_{26}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_{34}, \alpha_{14} = \theta_2, \alpha_{15} = \theta_9.$$

28. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{35}, \alpha_3 = \theta_{21}, \alpha_4 = \theta_5, \alpha_5 = \theta_7, \alpha_6 = \theta_{33}, \alpha_7 = \theta_{34}, \alpha_8 = \theta_6,$$
$$\alpha_9 = \theta_{29}, \alpha_{10} = \theta_{12}, \alpha_{11} = \theta_{11}, \alpha_{12} = \theta_{25}, \alpha_{13} = \theta_{30}, \alpha_{14} = \theta_{16}, \alpha_{15} = \theta_9.$$

29. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{24}, \alpha_3 = \theta_{35}, \alpha_4 = \theta_{26}, \alpha_5 = \theta_3, \alpha_6 = \theta_4, \alpha_7 = \theta_{22}, \alpha_8 = \theta_{21},$$
$$\alpha_9 = \theta_7, \alpha_{10} = \theta_8, \alpha_{11} = \theta_{28}, \alpha_{12} = \theta_{33}, \alpha_{13} = \theta_{11}, \alpha_{14} = \theta_{18}, \alpha_{15} = \theta_6.$$

30. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{16}, \alpha_3 = \theta_{17}, \alpha_4 = \theta_{36}, \alpha_5 = \theta_{23}, \alpha_6 = \theta_{25}, \alpha_7 = \theta_{32}, \alpha_8 = \theta_{35},$$
$$\alpha_9 = \theta_{21}, \alpha_{10} = \theta_{26}, \alpha_{11} = \theta_{31}, \alpha_{12} = \theta_{13}, \alpha_{13} = \theta_{24}, \alpha_{14} = \theta_6, \alpha_{15} = \theta_9.$$

31. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{20}, \alpha_3 = \theta_{34}, \alpha_4 = \theta_3, \alpha_5 = \theta_{25}, \alpha_6 = \theta_{35}, \alpha_7 = \theta_{32}, \alpha_8 = \theta_{23},$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_{27}, \alpha_{11} = \theta_8, \alpha_{12} = \theta_{36}, \alpha_{13} = \theta_{17}, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_6.$$

32. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{14}, \alpha_3 = \theta_{33}, \alpha_4 = \theta_3, \alpha_5 = \theta_5, \alpha_6 = \theta_{13}, \alpha_7 = \theta_{16}, \alpha_8 = \theta_2,$$
$$\alpha_9 = \theta_{17}, \alpha_{10} = \theta_{11}, \alpha_{11} = \theta_{10}, \alpha_{12} = \theta_{29}, \alpha_{13} = \theta_{18}, \alpha_{14} = \theta_{22}, \alpha_{15} = \theta_9.$$

33. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_8, \alpha_3 = \theta_{22}, \alpha_4 = \theta_{10}, \alpha_5 = \theta_{26}, \alpha_6 = \theta_{28}, \alpha_7 = \theta_{27}, \alpha_8 = \theta_{25},$$
$$\alpha_9 = \theta_{36}, \alpha_{10} = \theta_{34}, \alpha_{11} = \theta_{18}, \alpha_{12} = \theta_{29}, \alpha_{13} = \theta_{19}, \alpha_{14} = \theta_{32}, \alpha_{15} = \theta_{14}.$$

34. Thetanullwert

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{22}, \alpha_3 = \theta_5, \alpha_4 = \theta_{25}, \alpha_5 = \theta_{23}, \alpha_6 = \theta_{19}, \alpha_7 = \theta_4, \alpha_8 = \theta_{35},$$
$$\alpha_9 = \theta_{15}, \alpha_{10} = \theta_{26}, \alpha_{11} = \theta_{21}, \alpha_{12} = \theta_{11}, \alpha_{13} = \theta_2, \alpha_{14} = \theta_{27}, \alpha_{15} = \theta_9.$$

35. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{28}, \alpha_3 = \theta_{21}, \alpha_4 = \theta_5, \alpha_5 = \theta_{12}, \alpha_6 = \theta_{29}, \alpha_7 = \theta_{22}, \alpha_8 = \theta_{20},$$
$$\alpha_9 = \theta_{33}, \alpha_{10} = \theta_7, \alpha_{11} = \theta_{11}, \alpha_{12} = \theta_{25}, \alpha_{13} = \theta_{24}, \alpha_{14} = \theta_8, \alpha_{15} = \theta_9.$$

36. Thetanullwert:

$$\alpha_1 = \theta_1, \alpha_2 = \theta_{21}, \alpha_3 = \theta_5, \alpha_4 = \theta_{32}, \alpha_5 = \theta_{25}, \alpha_6 = \theta_3, \alpha_7 = \theta_9, \alpha_8 = \theta_{23},$$
$$\alpha_9 = \theta_6, \alpha_{10} = \theta_{28}, \alpha_{11} = \theta_{29}, \alpha_{12} = \theta_4, \alpha_{13} = \theta_{13}, \alpha_{14} = \theta_{24}, \alpha_{15} = \theta_8.$$

4.3 Probleme für Geschlecht drei

Für $g = 3$ sind alle prinzipal polarisierten Abelschen Varietäten Jacobische von Kurven, aber im allgemeinen nicht mehr Jacobische von hyperelliptischen Kurven. Der Modulraum der hyperelliptischen Kurven von Geschlecht 3 hat Kodimension eins im Modulraum der Kurven vom Geschlecht 3. Wenn wir mit einem zufälligen CM-Körper K starten, ist es deshalb unwahrscheinlich, daß das Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit $\mathcal{O}_K$ Periodenmatrizen enthält, die die Bedingung von Satz 4.2.1 erfüllen, also hyperelliptisch sind.

S. Loubatin und R. Okazaki haben uns eine vollständige Liste von CM-Körpern K mit Galoisabschluß L übersandt, für die $h_K = 1$ und $G = \#Gal(L, \mathbb{Q}) = 24$.
Es ist $P_{K_0}(y)$ das Minimalpolynom des reellen Teilkörpers von K. Das Minimalpolynom von K ist dann durch $P_K = -P_{K_0}(-x^2)$ gegeben.

CM-Körper K mit Galoisabschluß L (Gal$(L, \mathbb{Q})$=24) und $h_K = 1$

Fall	Diskr(K)	P_{K_0}
1	$-7^4 \cdot 167$	$y^3 - 18y^2 + 101y - 167$
2	$-7^4 \cdot 239$	$y^3 - 19y^2 + 118y - 239$
3	$-7^4 \cdot 251$	$y^3 - 22y^2 + 145y - 251$
4	$-7^4 \cdot 379$	$y^3 - 26y^2 + 181y - 379$
5	$-7^4 \cdot 491$	$y^3 - 26y^2 + 209y - 491$
6	$-7^4 \cdot 547$	$y^3 - 27y^2 + 222y - 547$
7	$-7^4 \cdot 1051$	$y^3 - 34y^2 + 341y - 1051$
8	$-13^4 \cdot 47$	$y^3 - 15y^2 + 62y - 47$
9	$-13^4 \cdot 79$	$y^3 - 14y^2 + 61y - 79$
10	$-19^4 \cdot 31$	$y^3 - 11y^2 + 34y - 31$
11	$-19^4 \cdot 83$	$y^3 - 18y^2 + 89y - 83$
12	$-31^4 \cdot 2^3$	$y^3 - 12y^2 + 17y - 2$
13	$-37^4 \cdot 11$	$y^3 - 10y^2 + 21y - 11$
14	$-61^4 \cdot 3$	$y^3 - 15y^2 + 14y - 3$
15	$-9^4 \cdot 71$	$y^3 - 30y^2 + 117y - 71$
16	$-9^4 \cdot 199$	$y^3 - 39y^2 + 318y - 199$
17	$-9^4 \cdot 379$	$y^3 - 30y^2 + 237y - 379$
18	$-9^4 \cdot 523$	$y^3 - 57y^2 + 507y - 523$
19	$-9^4 \cdot 739$	$y^3 - 33y^2 + 315y - 739$

Wir haben mit unserem Proramm getestet, ob es eine hyperelliptische Kurve gibt, deren Jacobische komplexe Multiplikation mit $\mathcal{O}_K$ hat.
Keiner dieser CM-Körper führt zu einer hyperelliptischen Kurve. Somit kann es auch keine hyperelliptische Kurve geben, deren Jacobische komplexe Multiplikation mit der maximalen Ordnung in einem CM-Körper hat, dessen Galoisabschluß Grad 24 über $\mathbb{Q}$ besitzt.
Weiter haben wir hyperelliptische Kurven C über $\mathbb{F}_p$ mit $p = 7, 11, 13, 17$ berechnet. Wir

ermittelten $K = \mathbb{Q}(\pi_p)$, wobei π_p dem Frobenius entspricht. Falls die Jacobische von C einfach ist, ist K ein CM-Körper vom Grad sechs über $\mathbb{Q}$. Der Endomorphismenring muß allerdings nicht die Maximalordnung in K sein. In der Tat war die Methode, auf diese Weise einen geeigneten CM-Körper zu finden, erfolglos.
Die Bestimmung des Endomorphismenringes der Jacobischen, d.h. die Bestimmung der Ordnung $\mathcal{O} \subseteq \mathcal{O}_K$ mit $End(J_C) \simeq \mathcal{O}$, einer über $\mathbb{F}_p$ definierten Kurve, ist ein nicht-triviales Problem. Nur für den Fall $g = 1$ existiert ein Algorithmus (siehe [27]).

4.4 Automorphismen von hyperelliptischen Kurven

Alle CM-Körper, für die wir hyperelliptische Kurven finden konnten, enthielten den Körper $\mathbb{Q}(i)$.
Aus dem Satz von Torelli 1.1.1 folgt, daß die Automorphismengruppe einer hyperelliptischen Kurve mit der Automorphismengruppe der zur Kurve gehörigen prinzipal polarisierten Abelschen Varietät übereinstimmt.
Ein Automorphismus muß die Jacobische und ihre Polarisierung in sich überführen. In unserem Fall ist die Riemannsche Form durch $E_\xi(x, y)$ für $\xi \in K$ gegeben. Sei $\alpha \in \mathcal{O}_K$ ein Automorphismus. Es gilt

$$(\alpha E_\xi)(x, y) = E_\xi(S_\Phi(\alpha)x, S_\Phi(\alpha)y) = E_\xi(S_\Phi(\alpha\overline{\alpha})x, y).$$

Nun wissen wir, daß

$$E_\xi(S_\Phi(\alpha\overline{\alpha})x, y) = E_\xi(x, y)$$

genau dann, wenn $\xi = \alpha\overline{\alpha}\xi$ also $\alpha\overline{\alpha} = 1$ ist. Somit ist α eine Einheitswurzel, und jede Einheitswurzel auf der prinzipal polarisierten Jacobischen Varietät J_C induziert einen Automorphismus.
Somit haben alle über $\mathbb{C}$ definierten Kurven, die wir mit der CM-Methode konstruieren konnten, einen nicht-trivialen Automorphismus (siehe Korollar 1.1.2). Dies verbietet die Anwendung von Mestres Algorithmus, der voraussetzt, daß die Kurve neben der hyperelliptischen Involution keine weiteren Automorphismen besitzt.

4.4.1 CM-Körper und Automorphismen

Wir betrachten nun CM-Körper vom Grad vier und sechs, die Einheitswurzeln enthalten.
Fall i: Sei zunächst $[K : \mathbb{Q}] = 4$.
Der Fall $K = \mathbb{Q}(\zeta_5)$, der auf die Gleichung $y^2 = x^5 - 1$ führt, ist allgemein bekannt. Hier verschwinden alle drei j-Invarianten.
Nun nehmen wir an, daß $K \neq \mathbb{Q}(\zeta_5)$. Der Körper K enthält entweder $M = \mathbb{Q}(i)$ oder $M = \mathbb{Q}(\sqrt{-3})$. Dann gilt $K = K_0M$, da $K_0 \cap M = \mathbb{Q}$. Somit folgt $K = \mathbb{Q}(\sqrt{d}, \sqrt{-3})$ bzw. $K = \mathbb{Q}(\sqrt{d}, i)$ für $K_0 = \mathbb{Q}(\sqrt{d})$ und $Gal(K, \mathbb{Q}) \simeq \mathbb{Z}_2 \bowtie \mathbb{Z}_2$. In diesem Fall gibt es keinen primitiven CM-Typ zu K.
Fall ii: Wir betrachten $[K : \mathbb{Q}] = 6$. Wie oben kann der Fall $K = \mathbb{Q}(\zeta_7)$ leicht abgehandelt

werden. In diesem Fall ist K natürlich Galoissch.
Außerdem sind wieder die Fälle $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3}) \subset K$ möglich.
Angenommen $\mathbb{Q}(i) \subset K$, dann ergibt sich $K = K_0\mathbb{Q}(i)$, da K_0 total reell ist. Sei L_0 der Galoissche Abschluß von K_0. Dann gilt $L = L_0\mathbb{Q}(i)$ ist Galoissch. Wir haben nämlich

$$L_0\mathbb{Q}(i)/\mathbb{Q}(i) \simeq L_0/\mathbb{Q},$$

also ist $L/\mathbb{Q}(i)$ Galoissch. Da $\rho L \subset L$ (ρ komplexe Konjugation), ist auch $L/\mathbb{Q}$ Galoissch. Wir können für $\mathbb{Q}(\sqrt{-3}) \subset K$ eine analoge Aussage zeigen.
Wir erhalten damit das folgende Lemma:

Lemma 4.4.1. *Sei K ein CM-Körper mit primitivem CM-Typ, der nicht-triviale Einheitswurzeln enthält. Falls $[K : \mathbb{Q}] = 4$, dann gilt $K = \mathbb{Q}(\xi_5)$. Falls $[K : \mathbb{Q}] = 6$ und L der Galoissche Abschluß von K ist, folgt $[L : \mathbb{Q}] = 6$ oder 12.*

Allerdings ergibt sich aus $Gal(L, \mathbb{Q}) = 6, 12$ noch nicht, daß L nicht-trivial Einheitswurzeln hat. Wir geben hier zwei einfache Beispiele an:

$K_{01}/\mathbb{Q}$	definiert durch $y^3 + y^2 - 2y - 1$
K_1/K_{01}	definiert durch $x^2 + 5$
und	
$K_{02}/\mathbb{Q}$	definiert durch $y^3 + y^2 - 3y - 1$
K_2/K_{02}	definiert durch $x^2 + 5$.

Der Körper K_1 ist Galoissch. Der Körper K_2 hat einen Galoisabschluß vom Grad 12 über $\mathbb{Q}$.

CM-Körper vom Grad 6, die $\mathbb{Q}(i)$ enthalten, führen stets auf hyperelliptische Kurven.

Satz 4.4.2. *Es sei C eine Kurve vom Geschlecht g, deren prinzipal polarisierte Jacobische J_C einfach ist. Weiter habe J_C komplexe Multiplikation mit $\mathcal{O}_K$, wobei $\mathbb{Q}(i) \subset K$. Dann ist C hyperelliptisch.*

Beweis. Die Jacobische J_C besitzt eine Automorphismengruppe der Ordnung vier. Aus Satz 1.1.2 folgt dann, daß C einen echten Automorphismus α der Ordnung zwei besitzt. Da J_C einfach ist, hat $C/\langle\alpha\rangle$ Geschlecht 0. Somit ist C eine Überlagerung vom Grad zwei von $\mathbb{P}_1$. Damit ist C hyperelliptisch. □

4.4.2 Invariantentheorie für Geschlecht drei

In diesem Abschnitt führen wir Invariantensysteme von hyperelliptischen Kurven vom Geschlecht 3 ein. Sei $\overline{\kappa}$ ein beliebiger algebraisch abgeschlossener Körper.
Es sei f eine binäre Form vom Grad 8 über $\overline{\kappa}$. Wir definieren zunächst acht Kovarianten.

Die Schreibweise $(xy)_k$ bezeichne die k-te Überschiebung der binären Formen x und y (siehe S. 15 für die Definition).

$$\begin{array}{llll} H=(ff)_2, & g=(ff)_4, & k=(ff)_6, & m=(fk)_4 \\ n=(fh)_4, & p=(gk)_4, & q=(gh)_4, & h=(kk)_2. \end{array}$$

Nun führen wir neun Invarianten der binären Form f ein

$$\begin{array}{lllll} I_2=(ff)_8, & I_3=(fg)_8, & I_4=(kk)_4, & I_5=(mk)_4, & I_6=(kh)_4 \\ I_7=(mh)_4, & I_8=(ph)_4, & I_9=(nh)_4, & I_{10}=(qh)_4. & \end{array}$$

Shioda [51] zeigte den folgenden Satz:

Satz 4.4.3. *Es seien $C_i, i=1,2$ zwei über $\overline{\kappa}$ definierte hyperelliptische Kurven der Form $y^2=f_i(x), i=1,2$. Die Kurven sind genau dann isomorph, wenn es ein $r\in\overline{\kappa}$ gibt, so daß $I_k^{(f_1)}=r^kI_k^{(f_2)}$ für $k=2,\dots 10$.*

Shepherd-Barron gibt in einem Artikel [48] sogar erzeugende absolute Invarianten $j_1,\dots,j_5$ für hyperelliptische Kurven vom Geschlecht drei an. Leider sind diese vom algorithmischen Standpunkt aus unbrauchbar. Wir benötigen absolute Invarianten, die bis auf einen glatten Nenner ganze Zahlen sind. Genauer möchten wir, daß der Nenner nur die Diskriminante enthält. Für Geschlecht drei ist dies eine Invariante vom Gewicht 14. Sie läßt sich durch die zehn Invarianten I_k ausdrücken. Es ist nicht klar, wie man die absoluten Invarianten von Barron in dieser Form ausdrückt.
Wir haben uns deshalb einer anderen Technik bedient und aus den Invarianten eigene absolute Invarianten abgeleitet. Wir betrachten die folgenden neun absoluten Invarianten

$$\begin{array}{llll} j_1=\frac{I_2^5}{\Delta}, & j_2=\frac{I_2I_3^4}{\Delta}, & j_3=\frac{I_2I_4^3}{\Delta}, & j_4=\frac{I_2^2I_5^2}{\Delta}, \quad j_5=\frac{I_2I_6^2}{\Delta}, \\ j_6=\frac{I_7^2}{\Delta}, & j_7=\frac{I_2^3I_8}{\Delta}, & j_8=\frac{I_5I_9}{\Delta} \text{ und} & j_9=\frac{I_2^2I_{10}}{\Delta} \quad . \end{array} \tag{4.4}$$

Satz 4.4.4. *Es seien $C_i, i=1,2$ zwei über $\overline{\kappa}$ definierte hyperelliptische Kurven der Form $y^2=f_i(x), i=1,2$. Die Kurven sind genau dann isomorph, wenn $j_k^{(f_1)}=j_k^{(f_2)}$.*

Beweis. Falls C_i isomorph sind, haben die Kurven wegen Satz 4.4.3 die gleichen absoluten Invarianten.
Nehmen wir nun an, daß die absoluten Invarianten übereinstimmen. Es sei $I_2^{(f_1)}=s\cdot I_2^{(f_2)}$. Dann setze $r=\sqrt{s}$. Es folgt dann $I_k^{(f_1)}=r^kI_k^{(f_2)}$. Mit Satz 4.4.3 folgt die Behauptung. □

Natürlich ist das von uns angegebene System absoluter Invarianten nicht minimal. Wie wir im nächsten Abschnitt sehen werden, lassen sich die neun absoluten Invarianten in (4.4) im Fall $\mathbb{Q}(i)\subset K$ auf fünf reduzieren.

4.4.3 Kurven mit Automorphismen über $\mathbb{C}$

In diesem Abschnitt betrachten wir Kurven über $\mathbb{C}$.
Sei C eine hyperelliptische Kurve vom Geschlecht drei. Mit $Aut(C)^*$ bezeichnen wir die reduzierte Automorphismengruppe $Aut(C)/\{\pm 1\}$ wobei -1 für die hyperelliptische Involution steht. Für alle Kurven, die wir erhalten haben, gilt $Aut(C)\simeq\mathbb{Z}/4\mathbb{Z}$ und $|Aut^*(C)|=2$.

Ein Automorphismus α operiert als Permutation auf den Weierstraßpunkten der Kurve. Außerdem läßt er sich durch eine lineare projektive Transformation, also eine Möbius-Transformation, auf den Weierstraßpunkten beschreiben. Wir unterscheiden zwei Fälle:

1. Die zwei Fixpunkte der Möbius-Transformation liegen in der Menge der Weierstraßpunkte. Durch eine geeignete projektive Transformation können wir sie nach 0 und ∞ schieben. Damit wird der Automorphismus α durch

   $$\lambda \mapsto -\lambda$$

   beschrieben. Die Kurve hat dann die Form

   $$y^2 = x(x^2 - a)(x^2 - b)(x^2 - c). \tag{4.5}$$

   Weiter können wir a gleich eins setzen oder $a+b+c = -1$ annehmen, was bedeutet, daß der Koeffizient von x^5 gleich eins ist.

2. Die zwei Fixpunkte sind keine Weierstraßpunkte. Wieder können wir annehmen, daß der Automorphismus wie oben gegeben ist. Die Kurve kann dann auf die Form

   $$y^2 = (x^2 - a)(x^2 - b)(x^2 - c)(x^2 - d). \tag{4.6}$$

   gebracht werden.

Im ersten Fall ist die Automorphismengruppe offensichtlich zu $\mathbb{Z}_4$ isomorph. Das erzeugende Element ist durch

$$(x, y) \mapsto (-x, iy)$$

gegeben. Im zweiten Fall erhalten wir die Kleinsche Vierergruppe mit den Erzeugenden

$$(x, y) \mapsto (-x, y) \text{ und } (x, y) \mapsto (x, -y).$$

Demnach besitzen alle Kurven, die wir erzeugt haben, die Form (4.5). Dies bestätigt auch eine Berechnung der Invarianten. Für Modell (4.5) verschwinden I_3, I_5, I_7 und I_9. Das gleiche Phänomen beobachten wir, wenn wir für die von uns konstruierten Kurven über $\mathbb{C}$ die Invarianten zu einer festgelegten Genauigkeit bestimmen.

Korollar 4.4.5. *Es seien C_1 und C_2 zwei hyperelliptische Kurven vom Geschlecht drei der Form*

$$y^2 = f_i(x), \quad i = 1, 2,$$

deren Jacobi-Varietät komplexe Multiplikation mit $\mathcal{O}_K$ für einen Körper K hat. Weiter enthalte K den Körper $\mathbb{Q}(i)$. Dann verschwinden alle ungeraden Invarianten von C_i. Die Kurven genau dann isomorph, wenn ihre j_i für $i = 1, 3, 5, 7, 9$ in (4.4) übereinstimmen.

4.4.4 Klassenpolynome für ausgewählte CM-Körper

Wir geben in diesem Abschnitt CM-Körper K an, für die das Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten mit komplexer Multiplikation mit $\mathcal{O}_K$ hyperelliptische Kurven enthielt. Außerdem führen die zugehörigen j-Invarianten bzw. deren Klassenpolynome an. Wie bereits erwähnt, enthalten alle unsere Körper den imaginär quadratischen Körper $\mathbb{Q}(i)$. Somit sind sie nach Abschnitt 4.4.1 entweder selbst Galoissch oder haben einen Galoisschen Abschluß vom Grad 12 über $\mathbb{Q}$.

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - w^2 - 2w + 1}$ $(d_{K_0} = 49)$:
K Galoissch mit Klassenzahl 1
$j_1 = 2187/1048576$,
$j_3 = 24373629/131072$,
$j_5 = -11632436487/16384$,
$j_7 = -2952169653573/16384000000000$,
$j_9 = 1168038669244419/2048000000000000$,

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - 3w - 1}$ $(d_{K_0} = 81)$:
K Galoissch mit Klassenzahl 1
$j_1 = 3142742836021/5665734653902848$,
$j_3 = 2623678442719129/43360214188032$,
$j_5 = -75785498250080047/258096513024$,
$j_7 = -8906335571231211275/1024192512$,
$j_9 = 257463692629950254825/6096384$,

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - w^2 - 3w + 1}$ $(d_{K_0} = 148)$:
K nicht Galoissch mit Klassenzahl 1
$H_1(X) = 157216684084675597457479111278592X^3 - 208980303832303241435692400 64X^2$
$+ 189152338400413070721024X + 410338673$,
$H_3(X) = 704699876308155165761863 68X^3 - 551685627939501598977294336X^2$
$+ 187419969157662252372566016X - 1449930370552879723$,
$H_5(X) = 148619689657095946 24X^3 + 191181142158432644628480X^2$
$- 866131960927730373606912 0X - 4404273769237556715911$,
$H_7(X) = 677021181018112X^3 + 125014720557174497280000X^2$
$- 347006107182666931729682400000X - 230106745388473261048492322343 75$,
$H_9(X) = 7710244864X^3 + 925838963848158151680 0X^2$
$+ 637730438128434794146944550680000X + 146304155906485680553936265241809704687 5$,

$K = \mathbb{Q}(i)K_0,\ K_0$ definiert durch $\mathbf{w^3 - w^2 - 4w - 1}$ $(d_{K_0} = 169)$:
K Galoissch mit Klassenzahl 3
$H_1(X) = 2^{60}7^{21}X^3 - 2^{40}7^{14}13394183218463911X^2$
$- 2^{20}7^8576832592944243257715X - 32936214446567570566377458 1,$
$H_3(X) = 2^{51}7^{15}3^2X^3 - 2^{34}7^{10}38074756187254019539X^2$
$- 2^{17}7^6220485155493244961499348955X - 393906234475647994618890864629750732,$
$H_5(X) = 2^{42}7^{12}X^3 + 2^{28}7^8148703899096183273861X^2$
$- 2^{14}7^6123539019249154551407110769 89X + 157126821950345315799920933723745558743 1,$
$H_7(X) = 2^{36}7^9X^3 + 2^{24}7^6116522431109649488491425X^2$
$- 2^{12}7^4504429129293913901754555871732918 75X$
$+ 14606874302471877561211308668443713398310619218 75,$
$H_9(X) = 2^{27}7^6X^3 - 2^{18}7^4293406671229128315542102 5X^2$
$- 2^97^3107503557570970280749650292503533718 75X$
$- 32412419132093893937638230043042547648454683264892187 5,$

$K = \mathbb{Q}(i)K_0,\ K_0$ definiert durch $\mathbf{w^3 - 4w - 1}$ $(d_{K_0} = 229)$:
K nicht Galoissch mit Klassenzahl 2
$H_1(X) = 2^{84}7^{14}X^3 - 1143428955145023779139325 27^7X^2$
$+ 47819463875643137141607922881709011 * 2^{27}X$
$+ 22828654144835368941572243418054 53,$
$H_2(X) = 2^{75}3^37^{10}X^3 - 2^{46}7^53^3228397238031092583528151 9X^2$
$+ 2^{24}3^271529982115053435723692448104299719522 37X$
$- 7^4969928047498503633061293046134433259824 7,$
$H_3(X) = 2^{66}7^8X^3 + 2^{40}7^4124794432811366957536271251X^2$
$+ 2^{21}10109327077294996381509046885054025083944039X$
$+ 7^6169016862473141462792640178486416127893489804 7,$
$H_4(X) = 2^{60}7^6X^3 + 2^{36}7^3970445452431995195900487711 75X^2$
$+ 2^{19}77962875975965128035532714775490130727578534068 75X$
$+ 7^6633040402496664989002612083068449060204370796138112031 25,$
$H_5(X) = 2^{51}7^4X^3 - 2^{30}7^2226908643553599184408617034782 5X^2$
$+ 2^{16}13432860670531632327899492497978085987240429155119375X$
$- 7^4898431194714052982576794056452567297925276746019101527632357812 5,$

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - w^2 - 4w + 2}$ ($d_{K_0} = 316$) :
K nicht Galoissch mit Klassenzahl 1
$H_1(X) = 2^{66}7^{21}X^3 - 2^{44}7^{14}16977077X^2 - 2^{20}7^7 18538036861403X + 4424930743202406821,$
$H_3(X) = 2^{51}3^37^{15}X^3 - 2^{34}3^27^{10}2956110587X^2 - 2^{17}3 \cdot 7^5 289420249457554127X$
$+ 54348504427072832171412461,$
$H_5(X) = 2^{40}7^{12}X^3 + 2^{26}7^872469877141X^2 - 2^{17}7^4 6662197493027064589X$
$- 28272918222745965 1593901157063,$
$H_7(X) = 2^{32}7^9X^3 + 2^{20}7^671985633469425X^2 - 2^{12}7^3 11801267248526243263293 75X$
$- 406606358212606847513925108848754843 75,$
$H_9(X) = 2^{25}7^6X^3 - 2^{16}7^45204937342630825X^2 + 2^{10}7^2 18715672573404905721538956937 5X$
$- 155774592214793352282682538004318800654531 25,$

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - w^2 - 4w + 1}$ ($d_{K_0} = 321$) :
K nicht Galoissch mit Klassenzahl 1

$H_1(X)=2^{60}3^{48}7^{45}11^{12}X^3$

$-2^{40}3^{24}7^{14}44253233996980876934205054737160334461916685004707369448729152623X^2$

$+1146368552739664866385250094709091783709770356530053242441285997863636604985933716322^{0}3^{12}7^7X$

$-13051277044011795726799639855549757097588117623523414970899937285430100293587328127260064682415190 1,$

$H_3(X)=2^{51}3^{51}7^{39}11^{12}X^3$

$-2^{34}3^{26}7^{10}26421165969961701147668293519718014885204998828103164607733422412827X^2$

$+2^{17}3^{13}7^5543418419370694983704257530590941672913122696791163056332782949523028603867062248486776 3X$

$-46390738996916679276457787153642518769365762929441418072069532080969830505786493384014976036249442740457049,$

$H_5(X)=2^{42}3^{48}7^{36}11^{12}X^3+2^{28}3^{12}7^4477942539212098711211083497209404740366640223095726095355128923536061X^2$

$+2^{14}3^{12}7^4271306479328480506810709066970280420171594374733423239186310221259373640561043723468777478 7X$

$+57865234174262185380381185992183279851594207550611270740069007983154623691528087104075502214295708278975 5201343,$

Die Koeffizienten der Polynome $H_7(X)$ und $H_9(X)$ wurden so groß,
daß wir sie nicht mehr berechnen konnten.

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 + w^2 - 6w - 7}$ ($d_{K_0} = 361$) :
K Galoissch mit Klassenzahl 1

$$j_1 = \frac{26306585108110544858216556909420391465632875181}{5192199555002209410349871709851706308197089 28},$$

$$j_3 = \frac{78214160055044361736199456755916852470144941841 23}{13245407028066860740688448239417618133155 84},$$

$$j_5 = -\frac{68992305147150188074492339359997775212370190061736 7}{23652512550119394179800800427531460952064},$$

$$j_7 = -\frac{64271513708788894539153823528612853096509521619680225}{76793871915972059025327274115361886208},$$

$$j_9 = \frac{60129069453603978761009691053766575022551915963706979275}{15084510554923083022832143129803227648},$$

$K = \mathbb{Q}(i)K_0$, K_0 definiert durch $\mathbf{w^3 - w^2 - 5w - 1}$ ($d_{K_0} = 404$) :
K nicht Galoissch mit Klassenzahl 1

$$H_1(X) = 2^{48}3^{24}7^{26}X^3 - 2^{32}7^{14}3561172547061023380786378056 1X^2$$
$$- 2^{16}3 \cdot 7^7781161077659372891670339465009339 3X$$
$$+ 1515445684423679960010517248997423231823,$$

$$H_3(X) = 2^{39}3^{27}7^{21}X^3 - 2^{26}3^27^{10}135220980534148949983356286252573X^2$$
$$- 2^{13}3^27^52475565386049789726501871312466100516750 1X$$
$$+ 1320465532093023873209754785281260609283098714989,$$

$$H_5(X) = 2^{30}3^{24}7^{18}X^3 + 2^{20}7^8202291055667330128462111686232953 9X^2$$
$$- 9127017439743196227840030143775673641214649 2^{10}37^4X$$
$$+ 2171344025981164785469005929036941691906096815121 77,$$

$$H_7(X) = 2^{24}3^{22}7^{16}X^3 + 1068224448400628590365226645008886475 2^{16}7^6X^2$$
$$- 3802306327482541949244076242679981531777882495625 2^87^33X$$
$$+ 3240535406573304401696425657196106704007099785667603573437 53^2,$$

$$H_9(X) = 2^{16}3^{21}7^{13}X^3 + 2^{11}7^4425269939401494313739952682523047782 5X^2$$
$$+ 2^67^23^2204567785491246226981356894934530015991158607276875X$$
$$+ 3^46146845279589393223463306391481735900291515118680902430907343 75,$$

4.4.5 Berechnung der Kurvengleichung über $\mathbb{F}_p$

Da unsere Kurven alle nicht-triviale Automorphismen haben, können wir Mestres Algorithmus nicht anwenden. Wir müssen zu einer anderen Methode greifen.
Falls ein CM-Körper K den Körper $\mathbb{Q}(i)$ enthält, gibt es mit jeder Lösung w der relativen Normgleichung $p = w\overline{w}$ bereits vier verschiedene Lösungen, nämlich w, $-w$, iw und $-iw$. Diese führen auf die vier verschiedenen Twists der hyperelliptischen Kurve über $\mathbb{F}_p$.

Satz 4.4.6. *Sei $K = \mathbb{Q}(i)K_0$ ein CM-Körper vom Grad 6 über $\mathbb{Q}$ mit total reellem Teilkörper K_0. Sei C eine über $\mathbb{F}_p$ definierte hyperelliptische Kurve, deren Jacobische komplexe Multiplikation mit $\mathcal{O}_K$ hat. Dann besitzt entweder C oder einer der drei anderen Twists $\tilde{C}$ von C über $\mathbb{F}_p$ ein Modell der Form*

$$y^2 = x^7 + x^5 + c_3x^3 + c_1x \text{ mit } c_1, c_3 \in \mathbb{F}_p.$$

Beweis. Wir betrachten die Überlagerung $X_1 = C/\{\pm 1\}$ vom Grad zwei von C. Diese ist isomorph zu $\mathbb{P}_1/\mathbb{F}_p$, hat also Geschlecht 0. Die acht Verzweigungspunkte sind die acht Weierstrasspunkte von C.
Der Automorphismus i auf C induziert auf X_1 einen Automorphismus α der Ordnung zwei. Dadurch erhalten wir eine Überlagerung

$$\phi : X_1 = C/\{\pm 1\} \to X_2 = C/\{\pm 1, \pm i\}.$$

Nach der Riemann-Hurwitz Formel hat ϕ zwei Verzweigungspunkte. Da die Automorphismengruppe von C zyklisch ist, entsprechen die beiden Verzweigungspunkte von ϕ Weierstrasspunkten von C. Sie sind Fixpunkte des Automorphismus α.
Wir behaupten nun, daß diese Fixpunkte bereits über $\mathbb{F}_p$ definiert sind. Sei nämlich $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$ ein Automorphismus der Ordnung zwei. Dann muß $d = -a$ gelten. Sei nun $z \in \overline{\mathbb{F}_p}$ ein Fixpunkt. Es gilt

$$\begin{aligned} az + b &= (cz - a)z, \quad \text{also} \\ 0 &= cz^2 - 2az - b. \end{aligned}$$

Dies ist äquivalent zu

$$\begin{aligned} 0 &= (z - \frac{a}{c})^2 - (\frac{bc + a^2}{c^2}) \\ &= (z - \frac{a}{c})^2 + \frac{1}{c^2}. \end{aligned}$$

Da -1 in $\mathbb{F}_p$ quadratischer Rest ist (sonst kann die Kurve nicht komplexe Multiplikation mit $\mathcal{O}_K$ haben), sind die Lösungen dieser Gleichung bereits über $\mathbb{F}_p$ definiert.
Wir können die beiden Fixpunkte damit nach 0 und ∞ schieben. Der Automorphismus wird dann durch $z \mapsto \gamma z$ für ein $\gamma \in \mathbb{F}_p$ beschrieben. Da α die Ordnung zwei hat, folgt $\gamma = -1$. Damit erhalten wir für C über $\mathbb{F}_p$ ein Modell der Form

$$y^2 = x^7 + cx^5 + ax^3 + bx.$$

Setze nun

$$k = \sqrt{\frac{1}{c}} \in \mathbb{F}_{p^2}.$$

Dann ist

$$\tilde{C} : y^2 = k(x^7 + cx^5 + ax^3 + bx)$$

über $\mathbb{F}_{p^4}$ zu C isomorph. Die Kurve $\tilde{C}$ hat komplexe Multiplikation mit $\mathcal{O}_K$ und ist ein Twist von C. Nun überführt die Transformation

$$x' = \frac{1}{k}x \text{ und } y' = \frac{1}{k^3}y$$

die Kurvengleichung $y^2 = kf(x)$ auf die über $\mathbb{F}_p$ definierte Gleichung

$$y^2 = x^7 + x^3 + ak^4x^3 + k^6bx.$$

□

Wir können also annehmen, daß unsere Kurve über $\mathbb{F}_p$ von der Form

$$y^2 = x^7 + x^5 + c_3x^3 + c_1x$$

ist. Die fünf j-Invarianten lassen sich durch multivariate Polynome in c_3 und c_1 beschreiben:

$$\begin{aligned}
\Delta &= -17280\,{c_1}^5{c_3}^2 + 9216\,{c_1}^5c_3 - 1024\,{c_1}^5 - 4352\,{c_1}^4{c_3}^3 + 512\,{c_1}^4{c_3}^2 + 9216\,{c_1}^4{c_3}^4, \\
&\quad + 62208\,{c_1}^6c_3 - 13824\,{c_1}^5{c_3}^3 - 64\,{c_1}^3{c_3}^4 - 13824\,{c_1}^6 - 1024\,{c_1}^3{c_3}^6 + 512\,{c_1}^3{c_3}^5 - 46656\,{c_1}^7, \\
I_2 &= -1/4\,c_1 - 1/28\,c_3, \\
I_4 &= \frac{1}{288}\,(-504\,c_3 - 120)\left(-504\,c_1 - 120\,{c_3}^2\right) + \frac{1}{96}\,(-196\,c_1 + 68\,c_3)^2\,, \\
I_6 &= -900375\,{c_1}^2c_3 - 185220\,{c_3}^3c_1 + 268275\,{c_3}^2c_1 + 64260\,{c_3}^4 - 185220\,{c_1}^2 + 64260\,c_1c_3 \\
&\quad + 10387\,{c_3}^3 + 117649\,{c_1}^3, \\
I_8 &= -4976552700\,{c_1}^3c_3 + 655473000\,{c_1}^2{c_3}^3 + 1297080225\,{c_1}^4 - 7899975\,{c_3}^4 - 70875000\,{c_3}^5 \\
&\quad + 10290000\,{c_1}^2c_3 - 13230000\,{c_1}^2 - 602714700\,{c_3}^3c_1 - 70875000\,{c_3}^2c_1 - 13230000\,{c_3}^6 \\
&\quad + 10290000\,c_1{c_3}^4 + 3776172750\,{c_1}^2{c_3}^2 + 655473000\,{c_1}^3, \\
I_{10} &= 1611556002000\,{c_1}^3c_3 + 1154471629500\,{c_1}^2{c_3}^3 - 1230373242000\,{c_1}^4 - 285070050\,{c_3}^5 \\
&\quad - 11827620000\,{c_1}^2c_3 - 13298418000\,{c_3}^3c_1 - 13298418000\,{c_3}^6 - 161577659250\,c_1{c_3}^4 \\
&\quad - 79453206000\,{c_1}^2{c_3}^2 + 120578220000\,{c_1}^3 + 381341586150\,{c_1}^5 - 11827620000\,{c_3}^7 \\
&\quad - 1230373242000\,{c_1}^3{c_3}^3 + 120578220000\,{c_3}^6c_1 - 79453206000\,{c_3}^5c_1 - 1361934236250\,{c_1}^4c_3 \\
&\quad + 1011722575500\,{c_1}^3{c_3}^2 + 1611556002000\,{c_3}^4{c_1}^2.
\end{aligned}$$

Wir können nun die Gleichungen

$$\begin{aligned}\Delta j_1 &= I_2^5,\\ \Delta j_3 &= I_2 I_4^3,\\ \Delta j_5 &= I_2 I_6^2,\\ \Delta j_7 &= I_2^3 I_8,\\ \Delta j_9 &= I_2^2 I_{10}.\end{aligned} \tag{4.7}$$

durch Gröbner-Basen bezüglich der lexikographischen Ordnung auflösen. Die Gröbner-Basis enthält ein univariates Polynom in c_1 von der Form $c_1^m g(c_1)$. Wir bestimmen eine Nullstelle von $g(c_1)$. Diese Nullstelle substituieren wir in die anderen Polynome der Gröbner-Basis. So erhalten wir die korrekten Werte für c_1 und c_3.
Gröbner-Basen sind im allgemeinen PSPACE-vollständig. Für Polynomideale in zwei Variablen lassen sich aber effizient bestimmen [4].
Sei F das Erzeugendensystems des Ideals I bei Eingabe und $\deg_{\min}(F)$ bzw. $\deg_{\max}(F)$ der kleinste bzw. größte Grad der Elemente in F. Dann berechnet der Algorithmus eine Gröbner-Basis G von I. Sei D der maximale, während der Berechnung auftretende Grad. Dann gilt [4]

$$\#G \leq \deg_{\min}(F) + 1 \text{ und } D \leq 2\deg_{\max}(F) - 1.$$

Damit erhält man als obere Schranke für die Anzahl der Schritte zur Berechnung einer Gröbner-Basis (siehe dazu auch [3])

$$\frac{3}{2}\left(|F| + 2(\deg_{\max}(F)+2)^2\right)^4.$$

4.4.6 Der Algorithmus für $\mathbb{Q}(i) \subset K$

Wir beschreiben zur Übersicht den gesamten Algorithmus.
Die möglichen Gruppenordnung für einen CM-Körper $\mathbb{Q}(i) \subset K$ und p erhalten wir durch Anwendung der Pari-Funktion $< bnfisintnorm >$ auf p^3.

Input: CM-Körper K mit $\mathbb{Q}(i) \subset K$, $h_{K_0} = 1$ und $\mathcal{O}_{K_0}$ monogen, eine Primzahl p und eine mögliche Gruppenordnungen n.
Output: Eine hyperelliptische Kurve der Form $y^2 = x^7 + kx^5 + c_3x^3 + c_1x$.

1: Bestimme ein vollständiges Repräsentantensystem von Periodenmatrizen Ω_i aller Isomorphieklassen einfacher prinzipal polarisierter Abelscher Varietäten, die komplexe Multiplikation mit $\mathcal{O}_K$ haben (siehe Abschnitt 4.1) . Sei s die Anzahl der Isomorphieklassen.
2: Berechne für jede Periodenmatrix Ω_i die geraden Thetanullwerte.
3: Abhängig vom dem geraden Thetanullwert, der in Ω_i verschwindet, berechne die Kurvengleichung der hyperelliptischen Kurve (siehe Abschnitt 4.2).

4: Berechne die fünf absoluten Invarianten $j_1^{(i)}, j_3^{(i)}, \ldots, j_9^{(i)}$ für alle Ω_i.
5: Berechne die Klassenpolynome

$$H_k(X) = \prod_{i=1}^{s}(X - j_k^{(i)}), \quad k = 1, 3, \ldots, 9.$$

6: Finde den Nenner und berechne die Polynome $H_k'(X) \in \mathbb{Z}[X]$.
7: **for** alle 5-Tupel $(a_1, a_2, a_3, a_4, a_5)$ mit $H_k'(a_k) = 0 \mod p$ **do**
8: Setze

$$j_1 := a_1, \quad j_3 := a_2, \quad j_5 := a_3, \quad j_7 := a_4 und \quad j_9 := a_5.$$

9: Löse die Gleichungen 4.7 mit dem Buchberger-Algorithmus und erhalte c_1, c_3.
10: Setze $C: \ y^2 = x^7 + x^5 + c_3x^3 + c_1x$.
11: Teste, ob J_C oder die Jacobische $J_{\tilde{C}}$ eines Twists von C die gewünschte Gruppenordnung hat.
12: **end for**

4.4.7 Kurven über $\mathbb{Q}$ mit einer CM-Jacobischen

Wir interessieren uns für Kurven über $\mathbb{Q}$, deren Jacobischen komplexe Multiplikation hat. Wenn eine Kurve über $\mathbb{Q}$ definiert ist, müssen die j-Invarianten in $\mathbb{Q}$ liegen.
Kandidaten für solche Kurven sind Kurven, deren Jacobische komplexe Multiplikation mit einem CM-Körper mit Klassenzahl eins hat, der nur wenige Polarisierungen zuläßt. Wir konnten zwei Kurven über $\mathbb{Q}$ mit komplexer Multiplikation mit einem Galoisschen CM-Körper bestimmen.

CM-Körper		Kurven über $\mathbb{Q}$
K_0	imaginäre Erweiterung	
$y^3 - y^2 - 2y + 1$	$x^2 + 1$	$y^2 = x^7 + 7x^5 + 14x^3 + 7x$
$y^3 - 3y - 1$	$x^2 + 1$	$y^2 = x^7 + 6x^5 + 9x^3 + x$

4.4.8 Kryptographisch relevante Beispiele

Reduktion des globalen Modells

Neben dem Algorithmus in Abschnitt 4.4.6 gibt es auch die Möglichkeit eine der in Abschnitt 4.4.7 angegebenen Kurven bezüglich einer geeigneten Primzahl zu reduzieren.
Wir wählen die Primzahl $p = 123456776543211236173$ und betrachten die Kurve

$$C: y^2 = x^7 + 7x^5 + 14x^3 + 7x.$$

Wir wissen bereits, daß C über $\mathbb{Q}$ komplexe Multiplikation mit $K = \mathbb{Q}(i)K_0$ hat, wobei K_0 durch das Minimalpolynom $w^3 - w^2 - 2w + 1$ definiert ist.

Nun berechnen wir die verschiedenen Möglichkeiten für das charakteristische Polynom des Frobeniusendomorphismus, indem wir die absolute Normgleichung

$$p^3 = N_{K/\mathbb{Q}}(\mathfrak{p})$$

lösen.
Die Pari-Bibliothek liefert das charakteristische Polynom des Frobenius-Endomorphismus:

$$\begin{aligned}
&x^6 + 6037355552x^5 + 19987507920573934619 9x^4 \\
&+ 96686854925517942362044041502 0x^3 + 16144304186644136965139712689430946630299x^2 \\
&- 28250845179418138299807981946041564531211593736 44x \\
&+ 18816758022058315767795492254184951858568706339377174759097 17.
\end{aligned}$$

Daraus ergeben sich zwei Möglichkeiten für die Gruppenordnung.
Durch Test mit einem zufälligen Element in der Jacobischen erhalten wir die richtige Ordnung

$$n = 188167580186437989111433953556453880527469259476859068821184 8 = 8q,$$

wobei q eine Primzahl mit 60 Stellen ist. Die Ordnung von p in $\mathbb{F}_q$ ist gleich

$$11760473761652374319464622097278367532966828717303691801324 0,$$

also ist die Kurve gegen die Tate-Paarung resistent [13]. Nach dem heutigen Stand ist C über $\mathbb{F}_p$ eine kryptographisch sichere hyperelliptische Kurve.

Lösung durch Reduktion der Klassenpolynome

Wir geben nun ein Beispiel für den Algorithmus in Abschnitt 4.4.6 an.
Wir wählen die Primzahl $p = 99037184507501969$. Diese liefert uns für den Körper

$$K = \mathbb{Q}(i)K_0 \text{ mit } K_0 = \mathbb{Q}(w) \text{ für } w^3 - w^2 - 3w + 1$$

eine gute kryptographisch Gruppenordnung, nämlich

$$n = 971392753190745941126493757635007515188486994011624.$$

Es gilt $n = 8q$, wobei q eine Primzahl mit 51 Dezimalstellen ist.
Die Klassenpolynome für K sind über $\mathbb{Q}$ irreduzibel. Wir reduzieren sie modulo p und setzen eine Kurvengleichung der Form

$$C : y^2 = x^7 + x^5 + c_3x^3 + c_1x$$

an (siehe Lemma 4.4.6). Mit dem Buchberger-Algorithmus unter Verwendung der Magma-Bibliothek (siehe Seite 129) erhalten wir

$$c_1 = 8683773159487505 \text{ und } c_3 = 6218231719898953.$$

Kapitel 5

Statistiken

In diesem Abschnitt untersuchen wir die Punktegruppe von Jacobischen mit komplexer Multiplikation. Dabei gilt auch hier stets, daß die Charakteristik unseres Grundkörpers **ungleich zwei** ist.

5.1 Elliptische CM-Kurven

5.1.1 Über die Gruppenstruktur

Die Punktegruppe der $\mathbb{F}_q$-rationalen Punkte einer über einem endlichen Körper definierten elliptischen Kurve ist entweder zyklisch oder direktes Produkt zweier zyklischer Faktoren. Genauer gilt

$$\#E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \bowtie \mathbb{Z}/n_2\mathbb{Z}$$

mit $n_2 \mid n_1$ und $n_2 \mid q-1$ [43].
Wir können noch mehr über die Gruppenstruktur sagen.

Satz 5.1.1. *Sei π_q der Frobeniusendomorphismus auf der über $\mathbb{F}_q$ definierten elliptischen Kurve E mit komplexer Multiplikation. Dann ergibt sich*

$$E(\mathbb{F}_q) \simeq EndE/(\pi_q - id).$$

als $EndE/(\pi_q - id)$-Moduln.

Daraus können wir den folgenden Satz ableiten:

Satz 5.1.2. *Sei eine über $\mathbb{F}_q$ definierte elliptische Kurve E mit komplexer Multiplikation gegeben, und die Abbildung $\pi_q - 1$ in $End(E) = \mathbb{Z}[\alpha]$ werde durch $a + b\alpha$, $a, b \in \mathbb{Z}$ beschrieben. Dann gilt:*
a) Falls $ggT(a,b) = 1$, dann ist $E(\mathbb{F}_q)$ zyklisch.
b) Wenn $ggT(a,b) > 1$, dann ist $E(\mathbb{F}_q)$ nicht zyklisch oder $\mathcal{O} = ggT(a,b)\mathcal{O}_K$.

Für einen Beweis siehe [63].
Uns interessiert die Gruppenstruktur elliptischer Kurven, die mit der CM-Methode erzeugt wurden. Dabei beschränken wir uns auf elliptische Kurven, deren Endomorphismus die Hauptordnung im jeweiligen imaginär quadratischen Zahlkörper ist. Dies macht Sinn, da zwei über $\mathbb{F}_q$ definierte elliptische Kurven mit einem Endomorphismenring im gleichen imaginär quadratischen Zahlkörper zueinander isogen sind. Zwar kann es passieren, daß die Gruppenstrukturen unterschiedlich sind, aber für kryptographische Anwendungen zählt allein die Gruppenordnung, und diese ist identisch.
Im folgenden nehmen wir außerdem an, daß wir die Punktegruppe über einem Primkörper $\mathbb{F}_p$ betrachten. Sei nun D stets die Diskriminante einer Hauptordnung. Insbesondere gelte entweder $D \equiv 1 \mod 4$ oder $D \equiv 0 \mod 4$ und $D/4 \equiv 2, 3 \mod 4$.

Satz 5.1.3. *Elliptische Kurven mit komplexer Multiplikation mit einer Hauptordnung in einem imaginär quadratischen Zahlkörper mit Diskriminante $D \equiv 1 \mod 8$ enthalten stets die volle 2-Torsionsgruppe, insbesondere sind sie immer nicht-zyklisch.*

Beweis. Aus Satz 5.1.2 ergibt sich, daß wir dazu nur die imaginär quadratische Zahl, die dem Endomorphismus $\pi_q - id$ entspricht, betrachten müssen.
Angenommen, es gelte $4p = a^2 - Db^2$ mit $D \equiv 1 \mod 8$. Dann folgt daraus, daß $a \equiv 0 \mod 2$ und $b \equiv 0 \mod 2$ und weiter $a - b \equiv 2 \mod 4$.
Nun wird der Frobenius durch $\pi_p = \frac{a-b}{2} + b(\frac{1+\sqrt{D}}{2})$ beschrieben. Es folgt $\frac{a-b}{2} - 1 \equiv 0 \mod 2$, und daraus ergibt sich nun die Behauptung. □

Die 2-Torsionsgruppe tritt auch bei den Punktegruppen von Kurven mit komplexer Multiplikation mit einer anderen Diskriminante häufig auf. Falls $D \equiv 0 \mod 4$ und $p = a^2 - D/4b^2$, dann ist sie immer genau dann in der Gruppe der $\mathbb{F}_p$-rationalen Punkte enthalten, falls a gerade ist. Falls $D \equiv 5 \mod 8$ und $4p = a^2 - Db^2$, dann ist sie ebenfalls immer genau dann in der Gruppe der $\mathbb{F}_p$-rationalen Punkte enthalten, falls a gerade ist.
Wir haben jeweils 10000 Kurven untersucht. Für die Größenordnung des Grundkörpers wurde 2^{160} gewählt. In der vierten Spalte ist die Anzahl der Kurven von Primzahlordnung festgehalten.

Gruppenstruktur von $E(\mathbb{F}_p)$ für Diskriminante $D \equiv 5 \mod 8$
(p durchläuft 10000 Primzahlen der Größe 2^{160})

D	Zyklisch	Nicht-zykl.	prim	D	Zyklisch	Nicht-zykl.	prim
-11	4441	5559	18	-19	5199	4801	48
-35	4408	5592	17	-43	5314	4686	76
-51	4890	5110	36	-59	4413	5587	15
-67	5266	4734	99	-83	4536	5464	17
-91	5241	4759	41	-107	4580	5420	20
-115	5268	4732	61	-123	5058	4942	47
-131	4334	5666	16	-139	5117	4883	37
-147	5138	4862	50	-155	4490	5510	22
-163	5291	4709	145	-179	4407	5593	14

D	Zyklisch	Nicht-zykl.	prim	D	Zyklisch	Nicht-zykl.	prim
-187	5222	4778	68	-195	5002	4998	41
-203	4464	5536	25	-211	5094	4906	47
-219	4970	5030	34	-227	4506	5494	21
-235	5176	4824	77	-251	4384	5616	10
-259	5005	4995	34	-267	5055	4945	65
-283	5290	4710	67	-291	4972	5028	38
-299	4538	5462	13	-307	5311	4689	65
-323	4482	5518	34	-331	5097	4903	58
-339	4817	5183	16	-347	4452	5548	20
-355	5302	4698	52	-363	4476	5524	50
-371	4462	5538	16	-379	5146	4854	64
-395	4462	5538	14	-403	5364	4636	110
-411	4900	5100	24	-419	4366	5634	9
-427	5288	4712	130	-435	4994	5006	39
-443	4565	5435	23	-451	5130	4870	40
-467	4439	5561	14	-483	5069	4931	44
-491	4490	5510	8	-499	5187	4813	71
-507	4628	5372	36	-515	4464	5536	17
-523	5199	4801	59	-547	5276	4724	102
-555	5141	4859	57	-563	4457	5543	17
-571	5230	4770	52	-579	4861	5139	17
-587	4488	5512	28	-595	5394	4606	72
-611	4372	5628	19	-619	5121	4879	52
-627	4972	5028	78	-635	4501	5499	19
-643	5507	4493	109	-651	4844	5156	21
-659	4475	5525	7	-667	5145	4855	65
-683	4554	5446	31	-691	5146	4854	49
-699	4940	5060	23	-707	4410	5590	39
-715	5203	4797	70	-723	5067	4933	56
-731	4424	5576	12	-739	5116	4884	55
-755	4421	5579	17	-763	5305	4695	85
-771	4821	5179	40	-779	4449	5551	18
-787	5217	4783	56	-795	4957	5043	63
-803	4484	5516	13	-811	5122	4878	44
-827	4701	5299	23	-835	5199	4801	45
-843	4993	5007	41	-851	4545	5455	19
-859	5217	4783	38	-867	4709	5291	38
-883	5276	4724	99	-891	2926	7074	24
-899	4424	5576	12	-907	5184	4816	121
-915	4949	5051	41	-923	4589	5411	18
-931	4496	5504	46	-939	4877	5123	35
-947	4437	5563	44	-955	5194	4806	77
-971	4444	5556	12	-979	5259	4741	42
-987	5078	4922	41	-995	4463	5537	25

Als nächstes betrachten wir den Fall $D \equiv 0 \mod 4$. Für $D \equiv 0 \mod 4$ ist die Gruppenordnung nie eine Primzahl, da sie stets durch zwei teilbar ist. Denn falls $p = x^2 + D/4y^2$, dann ist $\#E(\mathbb{F}_p) = p + 1 - 2a \equiv 0 \mod 2$. Wir prüfen zusätzlich, wann die Gruppenordnung von der Form $2 \cdot q$ mit q prim ist.

Gruppenstruktur von $E(\mathbb{F}_p)$ für Diskriminante $D \equiv 0 \mod 4$
(p durchläuft 10000 Primzahlen der Größe 2^{160})

D	Zyklisch	Nicht-zykl.	2· prim	D	Zyklisch	Nicht-zykl.	2· prim
-8	3328	6672	14	-20	3295	6705	13
-24	3674	6326	25	-40	3811	6189	34
-52	3914	6086	45	-56	3270	6730	10
-68	3489	6511	22	-104	3308	6692	6
-116	3365	6635	12	-120	3744	6256	29
-124	3889	6111	0	-132	3759	6241	21
-136	3824	6176	36	-148	3893	6107	70
-152	3411	6589	8	-164	3331	6669	16
-168	3740	6260	32	-184	3941	6059	43
-212	3410	659	22	-228	3751	6249	36
-232	4089	5911	114	-244	3792	6208	37
-248	3372	6628	12	-260	3323	6677	17
-264	3690	6310	17	-276	3598	6402	15
-280	3944	6056	40	-292	3963	6037	53
-296	3270	6730	53	-308	3386	6614	16
-312	3929	6071	47	-328	3939	6061	66
-340	3958	6042	66	-344	3341	6659	12
-356	3230	6770	7	-372	3787	6213	42
-376	3869	6131	33	-388	3980	6020	74
-404	3293	6707	13	-408	3704	6296	57
-420	3767	6233	29	-424	3909	6091	29
-436	3997	6003	39	-440	3401	6599	13
-456	3671	6329	23	-472	3890	6110	49
-488	3407	6593	22	-516	3665	6335	21
-520	3874	6126	79	-532	3986	6014	71
-536	3364	6636	5	-548	3394	6606	26
-552	3783	6217	24	-564	3706	6294	20
-568	3940	6060	78	-580	3901	6099	37
-584	3275	6725	9	-596	3334	6666	11
-616	3872	6128	36	-628	3898	6102	41
-632	3361	6639	22	-644	3459	6541	9
-660	3622	6378	37	-664	3842	6158	34
-680	3396	6604	17	-692	3457	6543	16

D	Zyklisch	Nicht-zykl.	2· prim	D	Zyklisch	Nicht-zykl.	2· prim
-696	3714	6286	11	-708	3778	6222	76
-712	3916	6084	38	-724	3866	6134	26
-728	3410	6590	14	-740	3415	6585	9
-744	3642	6358	18	-760	4001	5999	96
-772	3913	6087	78	-776	3329	6671	6
-788	3317	6683	24	-792	4293	5707	38
-804	3580	6420	20	-808	4008	5992	64
-820	3943	6057	47	-824	3322	6678	8
-836	3395	6605	17	-840	3780	6220	37
-852	3800	6200	38	-856	3785	6215	52
-868	3960	6040	40	-872	3426	6574	18
-884	3360	6640	13	-888	3757	6243	23
-904	3874	6126	40	-916	3875	6125	35
-920	3362	6638	9	-932	3357	6643	33
-948	3652	6348	17	-964	3834	6166	32
-984	3700	6300	22	-996	3688	6312	21

5.1.2 Heuristiken über Primordnungen

In diesem Abschnitt sei D wieder die Diskriminante einer Hauptordnung in einem CM-Körper. Insbesondere gelte wieder $D \equiv 1 \mod 4$ oder $D \equiv 0 \mod 4$ mit $D/4 \equiv 2, 3 \mod 4$. Sei E eine elliptische Kurve mit komplexer Multiplikation mit $\mathcal{O}_K$ für einen imaginär quadratischen Zahlkörper K. Wir können o.B.d.A. annehmen, daß E über dem Hilbertschen Klassenkörper F von K definiert ist.
Wir nehmen zunächst an, daß $E(F)$ keine Torsionspunkte enthält. Wir möchten die Menge

$$\{p \text{ prim} : p \neq n, p \nmid \Delta_E, p \text{ zerfällt total in } F, |E \mod \mathfrak{p}|, \text{ ist prim für ein } (\mathfrak{p}|p), \}$$

untersuchen und ihre Kardinalität abschätzen. Dabei bedienen wir uns der gleichen Heuristik wie Koblitz [23] für über $\mathbb{Q}$ definierte Kurven mit komplexer Multiplikation.
Nach dem Primzahlsatz erwarten wir, daß eine Zahl der Größe n mit Wahrscheinlichkeit $\frac{1}{\log n}$ prim ist. Hier suchen wir zwei Primzahlen - für den Definitionskörper und die Gruppenordnung - dieser Größe. Wir erwarten, daß es etwa $\frac{n}{\log^2 n}$ solcher Primzahltupel gibt. Nun beachte noch zwei Korrekturen:

1. Nicht jede Primzahl ist in K zerlegt. Nach Cebotarev ist ein Anteil von $\frac{1}{2h_k}$ aller Primzahlen in K zerlegt.

2. Der Primzahlsatz geht davon aus, daß jede Zahl mit Wahrscheinlichkeit $\frac{1}{l}$ durch l teilbar ist.

   Satz 5.1.4. *Sei E/F eine elliptische Kurve. Für eine Primzahl $p \neq l$ von guter Reduktion hat $\overline{E}(\mathbb{F}_p)$ eine durch l teilbare Ordnung genau dann, wenn der Frobenius π_p dargestellt als Element in $Gal(F(E[l]) \mid F) = G_l$ Eigenwert 1 hat.*

Beweis. Der Frobenius π_p hat genau dann Eigenwert eins, wenn er $l-1$ Elemente von $E[l] \simeq \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ festläßt. Dies bedeutet aber genau, daß $E(\mathbb{F}_p)$ eine Untergruppe der Ordnung l hat. □

Nach dem Satz von Cebotarev sind die Frobeniuselemente gleichverteilt. Eine Kurve wird also in

$$p_l := \frac{|\{g \in G_l : g \text{ hat Eigenwert eins}|}{|G_l|}$$

aller Fälle eine durch l teilbare Gruppenordnung haben.
Der Anteil der Kurven, deren Gruppenordnung nicht durch l teilbar ist, ist somit durch $(1-p_l)$ und nicht durch $(1-\frac{1}{l})$ gegeben, wie man es für eine zufällige Zahl annehmen würde.
Wir müssen für jedes l den Korrekturterm

$$a_l := \left(1 - \frac{|\{g \in G_l : g \text{ hat Eigenwert eins}|}{|G_l|}\right) \Big/ \left(1 - \frac{1}{l}\right)$$

berücksichtigen. Das ergibt den Korrekturfaktor

$$C = \prod_{l \text{ prim}} a_l.$$

Damit diese Heuristik sinnvoll ist, muß das Produkt konvergieren.

Wir widmen uns nun den Faktoren a_l.

Satz 5.1.5. *Sei E/F eine elliptische Kurve mit komplexer Multiplikation mit $\mathcal{O}_K$ und $\mathcal{A}$ ein Ideal in $\mathcal{O}_K$. Dann existiert eine Injektion*

$$G_{\mathcal{A}} = Gal(F(E[\mathcal{A}])|F) \to (\mathcal{O}/\mathcal{A})^*.$$

Insbesondere ist $F(E[\mathcal{A}])|F$ abelsch.

Für einen Beweis siehe [53].
Somit ist $\mathrm{Gal}(F(E[\mathcal{A}])|F)$ eine Untergruppe von $(\mathcal{O}/\mathcal{A})^*$.
Es gilt nun

$$(\mathcal{O}/(l))^* = \begin{cases} \mathbb{F}_{l^2}^* & \text{falls } l \text{ träge,} \\ \mathbb{F}_l^* \oplus \mathbb{F}_l^* & \text{falls } l \text{ zerfällt,} \\ \mathbb{F}_l^* \oplus \mathbb{Z}/l\mathbb{Z} & \text{falls } l \text{ verzweigt.} \end{cases}$$

Für die Anzahl der Elemente mit Eigenwert eins in G_l ergibt sich in den drei Fällen 1, $2l-3$ bzw. l [23]. Falls nun $G_l = (\mathcal{O}/\mathcal{A})^*$, dann erhalten wir für a_l

$$\frac{(1-\frac{1}{l^2-1})}{(1-\frac{1}{l})}, \frac{(1-\frac{2l-3}{(l-1)^2})}{(1-\frac{1}{l})} \text{ und } \frac{(1-\frac{1}{l-1})}{(1-\frac{1}{l})}.$$

Tatsächlich konvergiert das Produkt $C = \prod a_l$ [23].
Da für $D \equiv 0 \mod 4$ die Zahl 2 in K verzweigt und für $D \equiv 1 \mod 8$ die Zahl 2 in K zerlegt ist, ergibt sich für diese Fälle, daß die Gruppenordnung immer durch 2 teilbar ist und somit niemals eine Primzahl sein kann. Das deckt sich auch mit unseren Beobachtungen im letzten Abschnitt. In diesen beiden Fällen werden wir untersuchen, wann $\#E(\mathbb{F}_p) = 2 \cdot prim$ bzw. $\#E(\mathbb{F}_p) = 4 \cdot prim$ ist.
Falls $D \equiv 0 \mod 4$ haben wir bewiesen, daß die Gruppenordnung stets durch 2 teilbar ist. Für alle Primzahlen $l \neq 2$ berechnen wir a_l wie oben. So bleibt zu klären, wann $\#E(\mathbb{F}_p)$ durch 4 teilbar ist. Wir haben die folgende Beobachtung gemacht:

Lemma 5.1.6. *Sei E eine elliptische Kurve mit komplexer Multiplikation mit der Maximalordnung in $K = \mathbb{Q}(\sqrt{D})$ für $D \equiv 0 \mod 4$, $D/4 \equiv 2, 3 \mod 4$. Falls $\#E(\mathbb{F}_q)$ durch 4 teilbar ist, dann enthält $E(\mathbb{F}_q)$ bereits die ganze 2-Torsionsgruppe.*

Beweis. Das Ideal (2) ist in $K = Q(\sqrt{D})$ mit $D \equiv 0 \mod 4$ verzweigt. Falls $4 \mid \#E(\mathbb{F}_q)$, dann gilt $2 \mid \pi_q - 1$ und somit $2 \mid a, b$ aus Satz 5.1.2. Daraus folgt die Behauptung. □

Wir können uns nun überlegen, wie wahrscheinlich dieser Fall ist. Falls $E(\mathbb{F}_p)$ die ganze 2-Torsionsgruppe enthält, dann gilt, daß der Frobenius π_p die gesamte Gruppe $E[2]$ festläßt. Es gibt jeweils ein Element mit dieser Eigenschaft in $(\mathcal{O}/l\mathcal{O})^*$. Die Zahl 2 ist in O_K verzweigt. Da die Gruppenordnung immer durch 2 teilbar ist, läßt der Frobenius immer bereits eine Untergruppe der Ordnung 2 fest. Somit ergibt sich für die Wahrscheinlichkeit hier $\frac{1}{2}$, also $a_2 = 1$.
Nun wenden wir uns dem letzten verbliebenen Fall $D \equiv 1 \mod 8$ zu. Hier enthält $E(\mathbb{F}_p)$ bereits die ganze 2-Torsionsgruppe. Wir müssen die Wahrscheinlichkeit bestimmen, daß die Gruppenordnung durch 8 teilbar ist. Experimentelle Ergebnisse zeigen, daß diese bei $\frac{3}{4}$ liegt.
Wir können nun folgende Vermutung über die Anzahl von Primordnungen für elliptische CM-Kurven aufstellen.

Vermutung 5.1.7. *Sei F der Hilbertsche Klassenkörper eines imaginär quadratischen Zahlkörpers K mit Diskriminante D. Die elliptische Kurve E sei über F definiert und habe komplexe Multiplikation mit $\mathcal{O}_K$. Setze*

$$t(D) = \begin{cases} 1 & \text{für } D \equiv 5 \mod 8, \\ 2 & \text{für } D \equiv 0 \mod 4, \\ 4 & \text{für } D \equiv 1 \mod 8. \end{cases}$$

Dann ist die Anzahl der Elemente in der Menge

$$\{p \text{ prim} : p \neq n, p \nmid \Delta_E, p \text{ zerfällt total in } F, (|E \mod \mathfrak{p}|)/t(D) \text{ ist prim für } \mathfrak{p}|p\}$$

asymptotisch durch

$$\prod_{l \text{ prim}} a_l \frac{n}{2h_K(\log n \log(n/t(D)))}$$

gegeben.

Wir haben nun speziell für diese Formel einige Statistiken erstellt. Sei f_D eine Funktion auf der Menge der primen Hauptideale von Trägheitsgrad 1 in $\mathcal{O}_K$, die wie folgt definiert ist:

$$f_D(w) = \begin{cases} 1 & \text{falls } (w-1)(\overline{w}-1) \text{ prim} \\ 0 & \text{sonst.} \end{cases} \qquad \text{für } D \equiv 5 \mod 8$$

$$f_D(w) = \begin{cases} 1 & \text{falls } \frac{1}{2}(w-1)(\overline{w}-1) \text{ prim} \\ 0 & \text{sonst.} \end{cases} \qquad \text{für } D \equiv 0 \mod 4$$

$$f_D(w) = \begin{cases} 1 & \text{falls } \frac{1}{4}(w-1)(\overline{w}-1) \text{ prim} \\ 0 & \text{sonst.} \end{cases} \qquad \text{für } D \equiv 1 \mod 8$$

Falls $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$ bestimmen wir nun die Zahl

$$\sum_{\substack{p \text{ prim, } p \leq n, p \nmid D \\ p = w\overline{w},\ w \in \mathcal{O}_K}} \frac{1}{2}(f(w) + f(-w))$$

durch einfaches Lösen von Normgleichungen. Für $K = \mathbb{Q}(\sqrt{-4}), \mathbb{Q}(\sqrt{-3})$ gewichten wir entsprechend über die vier, bzw. sechs möglichen Gruppenordnungen. Dies gibt uns den Wert für die zu erwartende Anzahl von Primzahlordnungen, falls der gewählte Grundkörper $\leq n$ Elemente hat.
Wir vergleichen das Ergebnis mit dem heuristischen Wert

$$C \sum_{\substack{p \text{ prim, } p \leq n, \chi(p)=1 \\ p \text{ zerfällt total in } F}} (\log(p/t(D)))^{-1}.$$

Bemerkung 5.1.8. Koblitz hat für den Fall $h_K = 1$ Berechnungen angestellt. Allerdings hat er zur Ermittlung der tatsächlichen Gruppenordnung keine Normgleichung gelöst, sondern die Punkte auf einer Parameterfamilie von Kurven gezählt.

Zunächst betrachten wir die CM-Körper mit Klassenzahl eins und $D \equiv 5 \mod 8$. Für den tatsächlichen Wert haben wir Normgleichungen in K gelöst. Es ergeben sich dann immer zwei (bzw. für $D = -3$ sechs) Gruppenordnungen.

	$D=-3$		$D=-11$		$D=-19$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	14,66	14,8	8,5	7,1	18	14,9
10^4	77,66	78,8	35,5	35,6	82,5	75,2
10^5	469,5	472,8	220,5	212,3	448,5	453,5
10^6	3149,5	3147,9	1427,5	1410	2992,5	3013
	$D=-43$		$D=-67$		$D=-163$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	31,5	26,8	43	35,1	39,5	43,6
10^4	124,5	132,4	193	172,9	274	265,5
10^5	799	807	1050	1030,9	1649	1646
10^6	5386,5	5372,8	6954	6882,2	11007	10990

Nun betrachten wir einige CM-Körper mit höheren Klassenzahlen:

	$D=-35,\ h_K=2$		$D=-51,\ h_K=2$		$D=-59,\ h_K=3$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	3	2,8	1,5	4,1	0	1,4
10^4	16,5	15,4	24	23,9	7,5	8,0
10^5	106,5	94,7	154,5	145,7	62	50,6
10^6	642	635	979,5	977,5	337,5	342,7
	$D=-83,\ h_K=3$		$D=-347,\ h_K=5$		$D=-467,\ h_K=7$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	2	1,7	1,5	1,4	0	0,5
10^4	9,5	8	7	7,6	4,5	4,6
10^5	66	66,7	53	52,3	34,5	29,6
10^6	471	452,2	366,5	350,6	206	197,1

Als nächstes wenden wir uns $D \equiv 0 \mod 4$ zu. Zur Erinnerung: Hier betrachten wir die Gruppenordnung, die bis auf den Faktor 2 prim sind.

	$D=-8,\ h_K=2$		$D=-20,\ h_K=2$		$D=-24,\ h_K=2$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	10	9,2	3	2,9	4,5	3,6
10^4	40,5	42,4	14	15,2	21,5	19,8
10^5	247	245,4	87	89,3	119,5	118,1
10^6	1617	1600,8	579	588,1	781	775,4
	$D=-68,\ h_K=2$		$D=-52,\ h_K=2$		$D=-84,\ h_K=4$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	0,5	1,3	7	7,9	1,5	1,3
10^4	7	6,7	45	43,3	9,5	8,8
10^5	44,5	40,8	258,5	252,4	54	54,3
10^6	275,5	271,8	1665	1665	371,5	365,0

Für $D=4$ erhalten wir für jede Primzahl, die einer Normgleichung genügt, vier mögliche Gruppenordnungen.

	$D=-4,\ h_K=1$	
n	tats. Wert	Heuristik
10^3	16,25	18,6
10^4	86,5	92,0
10^5	528,25	537,1
10^6	3503,75	3516,8

Der letzte verbliebene Fall ist $D \equiv 1 \mod 8$. Hier interessieren wir uns für die Anzahl der Gruppenordnungen, die bis auf den Faktor 4 prim sind.

	$D=-7$, $h_K=1$		$D=-15$, $h_K=2$		$D=-23$, $h_K=2$	
n	tats. Wert	Heuristik	tats. Wert	Heuristik	tats. Wert	Heuristik
10^3	14,5	16,7	3	3,7	1	1,7
10^4	74	75,4	18	19,8	6	8,4
10^5	413,5	423,9	106	114,0	48,5	49,5
10^6	2718,5	2727,7	732	739,3	315,5	323,9

5.2 CM-Kurven vom Geschlecht zwei

5.2.1 Wahrscheinlichkeit für eine fast prime Gruppenordnung

Zunächst geben wir eine von unserem Programm errechnete Statistik an. Sie gibt Aufschluß darüber, wie häufig eine kryptographisch geeignete Gruppenordnung auftritt. Falls wir fordern, daß die Ordnung der Jacobischen bis auf einen Kofaktor der Größe maximal 1000 prim ist, dann ist nach unseren experimentellen Ergebnissen etwa jede zwanzigste Kurve kryptographisch geeignet.
Für jeden CM-Körper, den wir unten angegeben haben, wählten wir 5001 Primzahlen, die eine relative Normgleichung erfüllen.
Wir ermittelten die Anzahlen der Gruppenordnungen der Form

$$k \cdot q_{prim}$$

mit $k = 1, \ldots, 9$, $k \leq 1000$ und $k > 1000$. Die erste Spalte gibt die Parameter D, a und b des CM-Körpers an.

Verteilung der Gruppenordnungen in der Form $k = 1, \ldots, 9$, $k \leq 1000$ und $k > 1000$

CM-Körper	1	2	3	4	5	6	7	8	9	10	11 -1000	> 1000	Bem.
$5,5,1$	0	0	0	136	0	0	0	0	0	0	413	9453	
$5,4,1$	0	0	0	76	0	0	0	0	0	0	424	9500	
$5,6,1$	0	0	0	250	0	0	0	0	0	0	399	9351	
$5,7,1$	158	0	0	0	71	0	0	0	0	0	477	9296	
$5,6,2$	0	0	0	130	0	0	0	0	0	0	431	9439	
$5,35,8$	135	0	0	0	94	0	0	0	0	0	421	9350	

CM-Körper	1	2	3	4	5	6	7	8	9	10	11 −1000	> 1000	Bem.
8, 3, 1	0	0	0	0	0	0	0	93	0	0	374	9533	
8, 5, 2	0	0	0	147	0	0	0	0	0	0	431	9424	
8, 6, 1	0	0	0	149	0	0	0	0	0	0	438	9458	
8, 6, 3	0	0	0	146	0	0	0	0	0	0	402	9452	
8, 15, 4	0	0	0	98	0	0	0	0	0	0	404	9498	
8, 10, 2	0	0	0	0	0	0	0	185	0	0	392	9423	
8, 19, 8	255	0	0	76	0	0	0	0	0	0	422	9257	
12, 6, 1	0	0	0	95	0	0	0	36	0	0	403	9468	
12, 6, 2	0	0	0	59	0	0	0	0	0	0	442	9499	
13, 3, 1	0	0	0	52	0	0	0	0	0	0	365	9583	
13, 8, 3	47	0	0	0	0	0	0	0	106	0	397	9450	
13, 5, 1	55	0	99		0	0	0	0	75	0	360	9411	
13, 7, 1	0	0	0	62	0	0	0	0	0	0	407	9531	
13, 75, 20	170	0	0	0	0	0	0	0	37	0	448	9345	
13, 16, 6	0	0	0	237	0	0	0	0	0	0	464	9299	
13, 11, 4	57	0	90	0	0	0	0	0	71	0	378	9404	
17, 3, 1	0	0	0	0	0	0	0	0	0	0	411	9424	$16 \mid \#J_C(\mathbb{F}_p)$
17, 11, 4	0	0	0	60	0	0	0	67	0	0	427	9446	
17, 6, 1	0	0	0	0	0	0	0	108	0	0	436	9458	
17, 147, 56	183	0	0	139	0	0	0	0	0	0	441	9237	
19, 5, 1	0	0	0	90	0	0	0	0	0	0	484	9426	
19, 9, 2	0	23	0	13	0	37	0	7	0	5	425	9490	
19, 279, 64	0	0	0	32	0	0	0	0	0	0	371	9597	
21, 5, 1	0	0	0	59	0	0	0	0	0	0	423	9520	
21, 7, 1	34	0	52	0	24	0	11	0	42	0	394	9443	
21, 22, 7	60	0	81	0	15	0	0	0	85	0	369	9390	
21, 15, 4	112	0	0	0	78	0	39	0	9	0	395	9367	
24, 9, 2	0	0	0	73	0	0	0	0	0	0	385	9542	
24, 17, 6	0	0	0	45	0	0	0	0	0	0	439	9516	
28, 7, 2	0	33	0	24	0	24	0	14	0	0	421	9484	
28, 43, 16	65	0	56	23	0	0	0	0	35	0	391	9432	
29, 7, 2	0	0	0	55	0	0	0	0	0	0	328	9617	
29, 5, 1	92	0	0	0	51	0	31	0	0	14	441	9373	
29, 17, 5	160	0	0	0	0	0	105	0	0	0	406	9329	
29, 24, 7	70	0	0	0	50	0	55	0	0	0	392	9433	
29, 12, 3	76	0	0	0	51	0	31	0	7	0	390	9447	
29, 4, 1	0	0	0	163	0	0	0	0	0	0	405	9434	
33, 7, 2	0	0	0	0	0	0	0	116	0	0	325	9559	
33, 95, 28	0	0	0	31	0	0	0	41	0	0	392	9538	
37, 43, 12	134	0	0	0	0	0	97	0	36	0	401	9332	

CM-Körper	1	2	3	4	5	6	7	8	9	10	11 −1000	> 1000	Bem.
41, 10, 2	0	0	0	0	0	0	0	0	0	0	400	9602	$16 \mid \#J_C(\mathbb{F}_p)$
44, 67, 20	0	0	0	125	0	0	0	0	0	0	383	9492	
53, 5, 1	0	0	0	113	0	0	0	0	0	0	375	9512	
53, 55, 4	331	0	0	0	0	0	0	0	0	0	527	9142	
61, 5, 1	11	0	15	0	37	0	0	0	12	0	384	9541	
73, 6, 1	0	0	0	0	0	0	0	73	0	0	216	9668	
88, 5, 1	0	0	0	0	0	0	0	77	0	0	432	9491	
88, 85, 18	142	0	0	40	0	0	53	0	32	0	445	9288	
92, 29, 6	0	67	0	50	0	0	0	28	0	0	436	9419	
113, 6, 1	0	0	0	0	0	0	0	39	0	0	333	9628	
113, 7, 1	0	107	0	50	0	0	0	77	0	0	453	9313	
152, 13, 2	120	0	0	30	0	0	0	0	0	0	452	9398	
233, 10, 1	0	105	0	56	0	0	0	101	0	0	372	9366	

Wir möchten einige Erklärungen für obige Daten liefern. Auf den ersten Blick mag es erstaunlich sein, daß die Tabelle so viele Nullen aufweist. Es ist jedoch sofort einsichtig, daß es CM-Körper K gibt, bei denen die Gruppenordnung mit l bereits durch l^2 (bzw. l^4) teilbar ist. Dies hängt mit dem Zerfällungsverhalten von l in K zusammen. Umgekehrt folgt aus der Existenz von Gruppenordnung, bei denen l nur in erster Potenz auftritt, daß in K ein Primideal vom Grad eins über l liegt.

Lemma 5.2.1. *Sei $\mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$ mit η rein imaginär. Dann ist die Gruppenordnung $\#J_C(\mathbb{F}_q)$ immer durch 4 teilbar.*

Beweis. Setze $q = w\overline{w}$ mit $w = \alpha + \beta\eta$. Falls φ die reelle Konjugation ist, folgt

$$\begin{aligned} \#J_C(\mathbb{F}_p) &= (w-1)(w^\varphi - 1)\overline{(w-1)(w^\varphi - 1)} \\ &= (q+1)^2 - 2(q+1)(\alpha + \alpha^\varphi) + 4N_{K_0/\mathbb{Q}}(\alpha) \\ &\equiv 0 \mod 4. \end{aligned}$$

□

Da der von uns entworfene Algorithmus in Abschnitt 2.5 Weil-Zahlen liefert, die in der Ordnung $\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$ für rein imaginäres η liegen, erhalten wir dort stets Gruppenordnungen, die durch 4 teilbar sind.
Der nächste Satz gilt analog natürlich auch für elliptische Kurven.

Lemma 5.2.2. *Falls in $\mathcal{O}_K$ ein Primideal $\mathfrak{p} \mid 2$ vom Trägheitsgrad eins existert, dann ist die Gruppenordnung immer durch zwei teilbar.*

Beweis. Sei $\mathfrak{l}$ das Ideal vom Grad eins über $l = 2$ in $\mathcal{O}_K$. Es gilt $\mathcal{O}_K/\mathfrak{l} \simeq \mathbb{F}_2$.
Weiter sei $p \neq 2$ die Charakteristik des Definitionskörpers. Für w mit $w\overline{w} = q = p^n$ gilt $w \equiv 1 \mod \mathfrak{l}$. Somit ergibt sich $w - 1 \equiv 0 \mod \mathfrak{l}$, und die Gruppenordnung ist durch zwei teilbar. □

5.2.2 Heuristiken über Primordnungen

Wir möchten nun analog zu elliptischen Kurven untersuchen, wie oft eine prime Gruppenordnung auftritt. Dazu geben wir auch hier wieder eine Heuristik an.

Sei K ein primitiver CM-Körper vom Grad vier über $\mathbb{Q}$ und $p \neq 2$ eine in K unverzweigte Primzahl, die bezüglich K/K_0 eine relative Normgleichung erfüllt. Weiter soll p nicht Teiler des kleinsten gemeinsamen Vielfaches Δ_K der Nenner aller Klasssenpolynome $H_i(X)$ sein. Dann ist es nach Kapitel 2 möglich, eine über $\mathbb{F}_p$ definierte hyperelliptische Kurve zu konstruieren, deren Jacobische komplexe Multiplikation mit $\mathcal{O}_K$ hat. Eine solche Primzahl nennen wir in diesem Abschnitt eine Primzahl **von guter Reduktion**. Man beachte, daß diese Definition **nicht** mit der gängigen Definition von guter Reduktion übereinstimmt. Sie bezieht sich zunächst nicht auf eine Abelsche Varietät über einem Zahlkörper, sondern hängt vom gewählten CM-Körper ab.
Im Fall Geschlecht $g = 1$ haben wir eine elliptische Kurve über dem Hilbertschen Klassenkörper betrachtet. Für hyperelliptische Kurven müssen wir unsere Aussagen etwas modifizieren. Falls der CM-Körper K nicht Galoissch ist, gibt es zwei verschiedene CM-Typen, die zu unterschiedlichen Körpern k_0^* führen (siehe Abschnitte 1.1.5 und 3.1.1). Wir können im allgemeinen keine prinzipal polarisierte Abelsche Varietät mit komplexer Multiplikation mit $\mathcal{O}_K$ angeben, die über einem Zahlkörper F definiert ist, so daß für alle p von guter Reduktion ein Primideal $\mathfrak{P} \mid p$ vom Grad eins in F existiert. Wir betrachten also für jedes p einen anderen Definitionskörper F und dazu eine über F definierte Abelsche Varietät.
Sei p eine Primzahl von guter Reduktion und n eine der möglichen Gruppenordnungen für die Divisorklassengruppe vom Grad 0 über $\mathbb{F}_p$. Mit unserem Konstruktionsverfahren in Kapitel 2 können wir dazu eine hyperelliptische Kurve C_p über $\mathbb{F}_p$ mit komplexer Multiplikation mit $\mathcal{O}_K$ und einer Jacobischen mit Gruppenordnung $\#J_C(\mathbb{F}_p) = n$ konstruieren. Mit dem gleichen Konstruktionsverfahren erhalten wir, indem wir die Klassenpolynome nicht modulo p reduzieren, sondern mit den Nullstellen in k_0^* arbeiten, eine hyperelliptische Kurve $\tilde{C}$, die über einer höchstens quadratischen Erweiterung F/k_0^* definiert ist. Nach Bemerkung 1.1.18 können wir F so wählen, daß ein Primideal $\mathfrak{P} \mid p$ vom Grad eins in F existiert (auch Bemerkung 1.1.18). Es gilt dann $\tilde{C} \mod \mathfrak{P} \simeq C_p$. Somit können wir jedem CM-Körper K vom Grad vier und jeder Primzahl von guter Reduktion bezüglich K eine über einem Zahlkörper F definierte Abelsche Varietät A mit komplexer Multiplikation mit $\mathcal{O}_K$ zuordnen, so daß $A \mod \mathfrak{P}$ für eine Primstelle $\mathfrak{P} \mid p$ eine über $\mathbb{F}_p$ definierte prinzipal polarisierte Abelsche Varietät mit komplexer Multiplikation ist.

Wie im elliptischen Fall betrachten wir wieder die Galoisgruppe $G_l = Gal(F(A[l])|F)$ der abelschen Körpererweiterung, die man erhält, wenn man den Definitionskörper der l-Torsionspunkte von A zu F adjungiert.

Satz 5.2.3. *Sei $p \neq l$ von guter Reduktion bezüglich K (nach der Definition oben) und A eine über F definierte Abelsche Varietät (wie oben beschrieben), so daß ein Primideal $\mathfrak{P}|p$ vom Grad eins in F existiert. Dann hat $A \mod \mathfrak{P}$ eine durch l teilbare Ordnung genau*

dann, wenn der Frobenius π_p dargestellt als Element in $Gal(F(A[l]) \mid F) = G_l$ Eigenwert 1 hat.

Der Beweis läuft hier analog zu Satz 5.1.4.
Sei $\mathcal{A}$ ein Ideal in $\mathcal{O}_K$ und $A[\mathcal{A}]$ die Menge der Punkte $x \in A$, so daß $\mathcal{A}x = 0$. Dann gilt der folgende Satz (siehe [30], S. 112, Proposition 5.3)

Satz 5.2.4. *$A[\mathcal{A}]$ ist als Modul isomorph zu $\mathcal{O}_K/\mathcal{A}$.*

Damit ergibt sich dann der nächste Satz.

Satz 5.2.5. *Es existiert eine Injektion*

$$G_{\mathcal{A}} = Gal(F(A[\mathcal{A}])|F) \to (\mathcal{O}_{\mathcal{K}}/\mathcal{A})^*.$$

Insbesondere ist $F(A[\mathcal{A}])|F$ abelsch.

Beweis. Die Beweisidee verläuft fast analog zu Satz 5.1.5.
Sei $\beta \in \mathcal{O}_K$, $\sigma \in G_{\mathcal{A}}$ und $P \in E(\overline{F})$. Da A einfach ist, ist der CM-Typ (K, Φ) von A primitiv. Weiter gilt, A ist definiert über F und F enthält K^*. Nach [30], Satz 1.1. ist β dann über F definiert. Somit gilt $\sigma(\beta P) = \beta(\sigma P)$. Die Galoisgruppe verträgt sich also mit der $\mathcal{O}_K$-Modulstruktur von $A[\mathcal{A}]$. Somit erhalten wir eine injektive Abbildung

$$Gal(F(A[\mathcal{A}]|F) \to Aut_{O_K}(A[\mathcal{A}]),$$

wobei $Aut_{O_K}(A[\mathcal{A}])$ die Automorphismen des $\mathcal{O}_K$-Moduls $(A[\mathcal{A}])$ sind. Nach dem vorherigen Satz gilt

$$Aut_{O_K}(A[\mathcal{A}]) \simeq Aut_{O_K}(\mathcal{O}_K/\mathcal{A}) = (\mathcal{O}_K/\mathcal{A})^*.$$

□

Wir interessieren uns deshalb für die Gruppe $(\mathcal{O}_{\mathcal{K}}/(l))^*$ für verschiedene Primzahlen l. Wir nehmen an, daß l unverzweigt ist. Es gilt

$$(\mathcal{O}_{\mathcal{K}}/l)^* = \begin{cases} (\mathbb{F}_l^*)^4 & \text{falls } l \text{ total zerlegt ist,} \\ (\mathbb{F}_{l^2}^*)^2 & \text{falls } l \text{ in } K \text{ in zwei Primideale zerfällt,} \\ \mathbb{F}_{l^2}^* \times (\mathbb{F}_l^*)^2 & \text{falls } l \text{ in } K \text{ in drei Primideale zerfällt,} \\ \mathbb{F}_{l^4}^* & \text{falls } l \text{ in } K \text{ total träge ist.} \end{cases}$$

Falls l in $(\mathcal{O}_{\mathcal{K}}/l)$ verzweigt ist, ist die Situation etwas komplizierter.

Lemma 5.2.6. *Sei $\mathfrak{l}$ ein Primideal über l mit Verzweigungsindex e und Grad f und sei k eine natürliche Zahl. Dann gilt*

$$(\mathcal{O}_K/\mathfrak{l}^k)^* \simeq \mathbb{Z}/(p^f - 1)\mathbb{Z} \times G_{\mathfrak{l}} \text{ mit } G_{\mathfrak{l}} = \prod_{i=1}^{k-1} (\mathbb{Z}/p^i\mathbb{Z})^{b_i}$$

für nicht-negative ganze Zahlen b_i, die von p und e abhängig sind.

In [7] sind für den Fall $k \leq 4$ (also für unsere Zwecke ausreichend) die genauen Werte für die Zahlen b_i angegeben.

Wir können die Operation der Galoisgruppe G_l auf dem vier-dimensionalen $\mathbb{F}_l$-Vektorraum der l-Torsionpunkte durch Matrizen beschreiben. Da die Elemente in G_l die Polarisierung erhalten, ist G_l eine Untergruppe der **allgemeinen symplektischen Gruppe**

$$GSp(2,\mathbb{F}_l) = \{M \in Gl(4,\mathbb{F}_l) : M^t J M = \alpha J, \alpha \in \mathbb{F}_l^*\} \text{ mit } J = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

Die Untergruppe mit Elementen $M \in Gl(4,\mathbb{F}_l)$, für die $M^t J M = J$ gilt, ist die **symplektische Gruppe** $Sp(2,\mathbb{F}_l)$. Für alle Matrizen $M \in GSp(2,\mathbb{F}_l)$ gilt stets $M^{l-1} \in Sp(2,\mathbb{F}_l)$.

Bemerkung 5.2.7. Falls die Jacobische Endomorphismenring $\mathbb{Z}$ hat, also keine komplexe Multiplikation, hat Serre [47] gezeigt, daß fast immer $G_l = GSp(2,l)$. Darauf basierend berechnete Kuhlman [28] die Wahrscheinlichkeit, daß die Gruppenordnung der Jacobischen einer über $\mathbb{Q}$ definierten hyperelliptischen Kurve vom Geschlecht zwei mit $End(J_C) \simeq \mathbb{Z}$ modulo p eine Primzahl ist.

Analog zum elliptischen Fall möchten wir nun den Korrekturterm

$$a_l := \left(1 - \frac{|\{g \in G_l : \ g \text{ hat Eigenwert eins}\}|}{|G_l|}\right)\left(1 - \frac{1}{l}\right)^{-1}$$

bestimmen.

Bestimmung der a_l

Wir betrachten die Fälle, in denen l unverzweigt ist.
Sei zunächst l träge in $K/\mathbb{Q}$. Dann wissen wir bereits, daß G_l zyklisch ist. Falls $|G_l|$ nicht (l^2-1) teilt, folgt, daß G_l auf $J_C[l]$ irreduzibel operiert.

Satz 5.2.8. *Sei $\langle A\rangle$ eine zyklische, irreduzible Untergruppe von $GSp(2,\mathbb{F}_l)$. Falls die Ordnung von $\langle A\rangle$ nicht $2(l^2-1)$ teilt, dann ist $\langle A\rangle^{l-1}$ eine zyklische, irreduzible Untergruppe von $Sp(2,\mathbb{F}_l)$. Insbesondere folgt*

$$|\langle A\rangle| \leq (l-1)(l^2+1).$$

Beweis. Sei c ein Eigenwert von A. Dann ist c^{l-1} ein Eigenwert von A^{l-1}. Angenommen $\langle A^{l-1}\rangle$ wäre nicht irreduzibel. Dann gilt

$$\begin{aligned} \text{ord } c^{l-1} &\mid (l^2-1) \text{ und} \\ \text{ord } c &\mid (l-1)(l^2-1). \end{aligned}$$

Da $c \in \mathbb{F}_{l^4}^*$ ergibt sich aber auch

$$\begin{aligned} &\text{ord } c | (l^4-1) \text{ also} \\ &\text{ord } c | \left((l^2-1)ggT(l-1,l^2+1)\right) = 2(l^2-1). \end{aligned}$$

Falls nun $\langle A^{l-1}\rangle$ eine irreduzible Untergruppe von $Sp(2,l)$ ist, dann gilt nach Satz 5 in [18], daß $|\langle A^{l-1}\rangle|$ die Zahl l^2+1 teilt. Daraus ergibt sich die Behauptung, da der Index $[\langle A\rangle : \langle A^{l-1}\rangle] \leq l-1$ ist. □

Bemerkung 5.2.9. Wir haben die Gruppenordnung G_l für kleine l experimentell bestimmt. Dabei erhielten wir fast immer $G_l = (l^2+1)(l-1)$.
Wir erläutern das Programm, das wir hierfür geschrieben haben.
Sei p eine Primzahl von guter Reduktion in K und sei (A,E) eine über einem Zahlkörper F definierte prinzipal polarisierte Abelsche Varietät, so daß $(A_{\mathfrak{P}}, E_{\mathfrak{P}}) := (A,E) \mod \mathfrak{P}$ zu einer über $\mathbb{F}_p$ definierte prinzipal polarisierten Abelsche Varietät isomorph ist. Weiter sei $\mathcal{A}$ ein Ideal prim zu $\mathfrak{P}$. Es gilt $End((A,E)) = End((A_{\mathfrak{P}}, E_{\mathfrak{P}})$ ([50], S. 100) und $A[\mathcal{A}] \simeq A_{\mathfrak{p}}[\mathcal{A}]$ als $\mathcal{O}_K$-Modul. Dies bedeutet nach Satz 5.2.4 insbesondere, daß auch $A_{\mathfrak{p}}[\mathcal{A}] \simeq \mathcal{O}_K/\mathcal{A}$.

Lemma 5.2.10. *Sei A eine über $\mathbb{F}_p$ definierte Abelsche Varietät mit komplexer Multiplikation mit $\mathcal{O}_K$. Weiter sei π der Frobeniusendomorphismus von A. Dann gilt $A[\mathcal{A}] \subseteq A(\mathbb{F}_p)$ genau dann, wenn $\pi - 1 \equiv 0 \mod \mathcal{A}$.*

Beweis. Wir haben $A[\mathcal{A}] \simeq \mathcal{O}_K/(\mathcal{A})$ und $A(\mathbb{F}_p) = A[\pi-1] \simeq \mathcal{O}_K/(\pi-1)$. Also gilt $A[\mathcal{A}] \subseteq A(\mathbb{F}_p)$ genau dann, wenn $(\pi-1) \subseteq \mathcal{A}$, also $\pi - 1 \equiv 0 \mod \mathcal{A}$. □

Insbesondere gilt $A[l] \subset A(\mathbb{F}_p)$, falls $(\pi-1) \in (l)$. Wir können nun mit einer geeigneten Zahlentheorie-Bibliothek (z.B. Pari) testen, wie oft dieser Fall auftritt. Für diese Primzahlen p gilt, daß der Frobenius dargestellt als Element in G_l die Identität ist. Nach Cebotarev (Satz 1.1.7) haben diese Primzahlen die Dichte $\frac{1}{G_l}$.
Für l träge haben wir eine Ausnahme beobachtet, für die $G_l \neq (l^2+1)(l-1)$. Betrachte den CM-Körper mit $D=13$, $a=8$, $b=3$. Hier ergibt sich für $l=11$ experimentell ein Anteil von $\frac{1}{3660}$ statt $\frac{1}{1220}$.

Satz 5.2.11. *Sei l in $K/\mathbb{Q}$ total zerlegt. Dann gilt $|G_l| \leq (l-1)^3$.*

Beweis. Falls l in $K/\mathbb{Q}$ total zerlegt ist, gilt

$$G_l \leq (\mathbb{F}_l^*)^4.$$

Wir können die Gruppe G_l durch Diagonalmatrizen beschreiben. Es läßt sich leicht nachprüfen, daß jede Gruppe von Diagonalmatrizen in $GSp(2,l)$ zu einer Untergruppe von

$$\left\{ \begin{pmatrix} e_1 & & & \\ & e_2 & & \\ & & e_1^{-1}\lambda & \\ & & & e_2^{-1}\lambda \end{pmatrix} : e_i, \lambda \in \mathbb{F}_l^* \right\}. \tag{5.1}$$

konjugiert ist. Da die Gruppe (5.1) $(l-1)^3$ Elemente hat, ergibt sich die Behauptung. □

Tatsächlich gilt für unsere experimentellen Ergebnisse auch hier, daß $G_l = (l-1)^3$.

Satz 5.2.12. *Sei l total zerlegt, und $G_l \simeq (\mathbb{F}_l^*)^3$. Dann ist*

$$p_l = (l-1)^2 + (l-1)(l-2) + (l-2)^2 + (l-2)(l-3)$$

die Anzahl der Elemente mit Eigenwert eins in G_l.

Beweis. In diesem Fall ist G_l zur Gruppe 5.1 konjugiert. Wenn wir nun die Elemente mit Eigenwert eins in der Menge 5.1 abzählen, ergibt sich p_l. □

Nun betrachten wir den Fall, daß l in K in zwei Primideale vom Grad zwei zerfällt. Hier ist G_l eine Untergruppe von

$$\mathbb{F}_{l^2}^* \times \mathbb{F}_{l^2}^*.$$

Jede Matrix von G_l besitzt also Eigenwerte in $\mathbb{F}_{l^2}^*$, und da die Darstellung halbeinfach ist [11], können wir die Gruppe durch Matrizen der Form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{5.2}$$

beschreiben.
Es ist nun einfacher, zu einer zu $GSp(2, \mathbb{F}_l)$ konjugierten Gruppe in $Gl(4, \mathbb{F}_l)$ überzugehen. Wir betrachten

$$G = \{N \in Gl(4, \mathbb{F}_l) : N^t \tilde{J} N = \alpha \tilde{J}, \alpha \in \mathbb{F}_l^*\} \text{ mit } \tilde{J} = \begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & 0 \\ & & 0 & 1 \\ 0 & & -1 & 0 \end{pmatrix}.$$

Durch Übergang zu der konjugierten Gruppe können wir auch hier weiterhin annehmen, daß die Gruppe G_l in G durch Matrizen der Form (5.2) beschrieben wird.

Satz 5.2.13. *Die Primzahl l zerfalle in K in zwei verschiedene Primideale vom Grad zwei. Dann gilt $|G_l| \leq (l+1)^2(l-1)$.*

Beweis. Damit die Matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ in $GSp(2, \mathbb{F}_l)$ liegt, müssen $A, B \in Gl(2, \mathbb{F}_l)$ liegen und die Identität $\det(A) = \det(B)$ gelten. Die größte zyklische Untergrupe in $Gl(2, \mathbb{F}_l)$ hat $l^2 - 1$ Elemente. Davon haben jeweils $l+1$ Elemente die gleiche Determinante (siehe [19], Kapitel 2, Abschnitt 7). Für die Wahl der Matrix A haben wir somit höchstens $l^2 - 1$ Möglichkeiten und für B dann weitere $l+1$ Möglichkeiten. Daraus ergibt sich die Behauptung. □

In unseren experimentellen Ergebnissen gilt für $l \neq 2$ immer $G_l = (l+1)^2(l-1)$.

Satz 5.2.14. *Sei l eine Primzahl, die in K in zwei verschiedene Primideale vom Grad zwei zerfällt. Weiter gelte $|G_l| = (l+1)^2(l-1)$. Dann ist $p_l = (l+1) + l$ die Anzahl der Elemente mit Eigenwert eins in G_l.*

Beweis. Sei $M = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ mit $A, B \in Gl(2, \mathbb{F}_l)$ ein Element aus G_l mit Eigenwert eins. Dann gilt $\det(A) = \det(B) = 1$ und entweder $A = I_2$ oder $B = I_2$, wobei I_2 die zwei-dimensionale Einheitsmatrix bezeichne. Somit gibt es $(l+1) + l = 2l + 1$ Elemente mit Eigenwert eins. □

Für $l = 2$ gilt (nach Experiment) stets $|G_l| = l + 1 = 3$. Die Gruppe G_l ist in diesem Fall zyklisch und besitzt nur ein Element mit Eigenwert eins, die Identität.
Nun wenden wir uns dem letzten Fall zu, daß l in drei Primideale zerfällt. Auch hier nehmen wir an, daß G_l eine Untergruppe der zu $GSp(2, \mathbb{F}_l)$ konjugierten Gruppe G ist.

Satz 5.2.15. *Sei l eine Primzahl, die in K unverzweigt ist und in drei Primideale zerfällt. Dann gilt $|G_l| \leq (l+1)(l-1)^2$.*

Beweis. Der Beweis verläuft wie in dem Fall, in dem l in K in zwei verschiedene Primideale zerfällt (siehe Satz 5.2.13). Wir wählen A wie oben. Die Matrix B ist diesmal aber eine Diagonalmatrix in $Gl(2, \mathbb{F}_l)$ mit $\det(B) = \det(A)$. □

Wieder gilt in unseren Berechnungen stets, daß $G_l = (l+1)(l-1)^2$.

Satz 5.2.16. *Sei l eine Primzahl, die in K unverzweigt ist und in drei Primideale zerfällt. Weiter gelte $G_l = (l+1)(l-1)^2$. Dann hat G_l genau $p_l = 2l^2 - 5$ Elemente mit einem Eigenwert eins.*

Beweis. Die Elemente in G_l können wir durch

$$\begin{pmatrix} A & 0 \\ 0 & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\det(A) \end{pmatrix} \end{pmatrix}$$

mit $\lambda \in \mathbb{F}_l^*$ und $A \in Gl(2, \mathbb{F}_l)$ beschreiben. Die Matrizen A liegen alle in einer zyklischen Untergruppe der Ordnung $l^2 - 1$ in $Gl(2, \mathbb{F}_l)$.
Es gibt $(l-1)$ Matrizen mit $A = I_2$ in G_l. Weiter gibt es $(l^2 - 2)$ Matrizen mit $\lambda = 1$ und $A \neq I_2$.
Falls $\lambda^{-1}\det(A) = 1$, ergibt sich $\det(A) = \lambda$. Wir können also A frei wählen, bestimmen aber mit der Wahl von A dann das Element in G_l eindeutig. Für $\lambda^{-1}\det(A) = 1$ mit $\lambda \neq 1$ gibt es $(l^2 - 1) - (l + 1) = l^2 - l - 2$ Möglichkieten.
Insgesamt erhalten wir also $2l^2 - 5$ Matrizen mit Eigenwert eins. □

Nach dem Satz von Cebotarev gilt, daß die Frobeniuselemente in G_l gleichverteilt sind. Somit ist die Wahrscheinlichkeit p_l, mit der eine Gruppenordnung $J_C(\mathbb{F}_p)$ durch l teilbar ist, durch

$$\frac{|\{g \in G_l : g \text{ hat Eigenwert eins}\}|}{|G_l|}$$

gegeben. Für die unverzweigten Primzahlen in K erhalten wir damit folgende Tabelle für die Wahrscheinlichkeit p_l, daß l die Gruppenordnung $J_C(\mathbb{F}_p)$ teilt:

Zerfällungsverhalten	Wahrscheinlichkeit p_l
träge	$\frac{1}{(l^2+1)(l-1)}$
zwei Primideal über p	$\frac{2l+1}{(l+1)^2(l-1)}$ $\left(l=2,\frac{1}{3}\right)$
total zerlegt	$\frac{(l-1)^2+(l-1)(l-2)+(l-2)^2+(l-2)(l-3)}{(l-1)^3}$
drei Primideale über p	$\frac{2l^2-5}{(l+1)(l-1)^2}$

Man beachte, daß für K Galoissch der letzte Fall nicht auftreten kann.

Die Heuristik

Satz 5.2.17. *Sei K ein zyklischer CM-Körper vom Grad vier. Das Produkt*

$$C = \prod_{\substack{l \text{ prim,} \\ l \text{ unverzweigt in } K/\mathbb{Q}}} a_l, \qquad a_l = (1-p_l)/(1-1/l)$$

(mit p_l aus der Tabelle auf S. 117) konvergiert gegen einen endlichen Grenzwert ≥ 0.

Für die Beweisidee danken wir K. Murty, der uns in diesem Zusammenhang auf die folgende Version des Primzahlsatzes aufmerksam gemacht hat:

Satz 5.2.18. *Sei L eine beliebige Primzahlmenge der Dichte δ. Dann gilt*

$$\sum_{l \leq x, \in L} \frac{1}{l} = \delta \log\log x + c(L) + O\left(\frac{1}{\log x}\right)$$

für eine nur von L abhängige Konstante $c(L)$.

Beweis. (von Satz 5.2.17) Das Produkt $\prod(1+\frac{1}{l})$ konvergiert nicht. Wir müssen also die Vorzeichen beachten.
Durch Umformung erhalten wir

$$a_l = \begin{cases} 1 + \frac{1}{l-1} - \frac{1}{(l^2+1)(l-1)} & \text{für } l \text{ in } K/\mathbb{Q} \text{ träge,} \\ 1 + \frac{1}{l-1} - \frac{l}{(l+1)^2(l-1)} & \text{für } l \text{ nur in } K/K_0 \text{ träge,} \\ 1 - \frac{3}{l-1} - \frac{2l^2-l-4}{(l-1)^4} & \text{für } l \text{ total zerlegt in } K/\mathbb{Q}. \end{cases}$$

Für l träge, gilt

$$\frac{1+\frac{1}{l-1}}{a_l} = 1 + O\left(\frac{1}{l^2}\right).$$

Da das Produkt $\prod_{l \text{ prim}} (1+O(\frac{1}{l^2}))$ konvergiert, können wir statt a_l auch den Faktor $(1+\frac{1}{l-1}) = (1-\frac{1}{l})^{-1}$ ansetzen. Analog verfahren wir in den anderen Fällen. Es ist also ausreichend das Produkt $\prod c_l$ mit

$$c_l = \begin{cases} (1-\frac{1}{l})^3 & \text{für } l \text{ in } K/\mathbb{Q} \text{ total zerlegt,} \\ (1-\frac{1}{l})^{-1} & \text{sonst,} \end{cases}$$

abzuschätzen.
Wir betrachten das Produkt für alle $l \leq x$. Wir logarithmieren das Produkt. Wegen der Ungleichung $r \geq (\ln(r+1))$ für alle $r \in (-1, \infty]$ genügt es die Konvergenz der Reihe

$$-3 \sum_{l \text{ total zerlegt}} \frac{1}{l} + \sum_{l \text{ sonst}} \frac{1}{l}.$$

zu zeigen.
Nun wenden wir Satz 5.2.18 zusammen mit Satz 3.1.4 über die Dichte in zyklischen CM-Körpern vom Grad vier an. Wir erhalten, daß die Terme der Ordnung $\frac{1}{l}$ sich gegeneinander aufheben. Für $l \to \infty$ ergibt sich die Konvergenz. □

Satz 5.2.19. *Sei K ein nicht Galoisscher CM-Körper vom Grad vier. Das Produkt*

$$C = \prod_{\substack{l \text{ prim,} \\ l \text{ unverzweigt in } K/\mathbb{Q}}} a_l, \qquad a_l = (1-p_l)/(1-1/l)$$

(mit p_l aus der Tabelle auf S. 117) konvergiert gegen einen endlichen Grenzwert ≥ 0.

Beweis. Der Beweis verläuft analog zu Satz 5.2.17. Für die Primzahlen l, die in drei Primideale zerfallen, ergibt sich

$$a_l = 1 - \frac{1}{l-1} - \frac{2l^2-l-2}{(l-1)^3(l+1)}.$$

Nach Umformungen wenden wir wieder Satz 5.2.18 zusammen mit Satz 3.1.5 über die Dichte in nicht Galoisschen CM-Körpern an und erhalten die Behauptung. □

Bemerkung 5.2.20. Bisher haben wir nur die unverzweigten Primzahlen behandelt. Für jeden CM-Körper K gibt es nur endlich viele verzweigte Primzahlen. Insbesondere ändern diese nichts am Konvergenzverhalten des Produktes $\prod a_l$. Die folgende (unvollständige) Liste stützt sich allein auf unsere experimentellen Daten.

Verzweigungsverhalten	Wahrscheinlichkeit p_l
$l = \mathfrak{p}^4$	$\frac{2}{(l-1)}$
$l = \mathfrak{p}^2$ l träge in $K_0/\mathbb{Q}$	$\frac{1}{(l^2-1)}$
$l = \mathfrak{p}_1\mathfrak{p}_2^2$	$\frac{1}{l^2-1}$
$l = \mathfrak{p}_1^2\mathfrak{p}_2^2$	$\frac{2l+1}{(l^2-1)}$

Wir würden nun eigentlich gerne die Ordnung der Menge

$$\left\{ p \text{ prim: } p \leq n, w\overline{w} = p, \prod_{i=1}^{4}(w_i - 1) \text{ prim} \right\}$$

abschätzen. Hier müssen wir allerdings beachten, daß es für ein $p \in S_K$ zwei bzw. sogar vier mögliche Frobeniuselemente w und damit vier unterschiedliche Gruppenordnungen gibt. Wir werden die Primzahlen also entsprechend gewichten.

Vermutung 5.2.21. *Sei K ein CM-Körper und S_K die Menge aller Primzahlen in $\mathbb{Z}$ mit guter Reduktion bezüglich K (für unsere Definition von guter Reduktion siehe S. 111). Für $w \in \mathcal{O}_K$ seien $w_1 = w$, $w_i, i = 2, \ldots 4$ die vier verschiedenen Einbettungen von w. Setze*

$$N = \#\{\textit{mögliche Gruppenordnungen zu } p \textit{ und } K\}$$

und

$$\chi(p) = \frac{1}{N} \left| \{ \prod_{i=1}^{4}(w_i - 1) \textit{ prim } : w\overline{w} = p \} \right|.$$

Dann ist die Anzahl der Elemente in der Menge

$$\{\chi(p) : p \leq n, p \in S_K\} \tag{5.3}$$

asymptotisch durch

$$\prod_{l \textit{ prim}} a_l \left(\delta(S_K) \frac{n}{\log^2 n} \right)$$

gegeben, wobei $\delta(S_K)$ die Dichte von S_K ist.

Es stellt sich nun die natürliche Frage, wie die Menge (5.3) zu interpretieren ist. Es sei nochmal daran erinnert, daß wir hier im allgemeinen keine Abelsche Varietät über einem Zahlkörper F haben, so daß für alle $p \in S_K$ ein Primideal $\mathfrak{P}$ vom Grad eins über p existiert. Wir können die Menge (5.3) wie folgt verstehen: Wir wählen für jede Primzahl eine eigene Abelsche Varietät wie auf S. 111 beschrieben. Dann zählen wir die primen Gruppenordnungen bei Reduktion.

Statistiken

Wir haben einige Statistiken erstellt, die unsere Heuristik im Fall $h_K = 1$ unterstützen sollen.
Analog zu den elliptischen Kurven definieren wir wieder eine Funktion. Die Funktion f ist auf der Menge der Elemente $w \in \mathcal{O}_K$ definiert, für die $w\overline{w} = p$ für eine Primzahl $p \in \mathbb{Z}$ ist. Es gelte

$$f(w) = \begin{cases} 1 & \text{falls } \prod(w_{(i)} - 1) \text{ prim}, \\ 0 & \text{sonst}, \end{cases}$$

wobei $w_{(i)}, i = 1, \ldots, 4$, die vier zu w konjugierten Elemente in $\mathcal{O}_K$ sind.
Betrachten wir zunächst den Galoisschen Fall. Hier bestimmen wir die Mächtigkeit der Menge 5.3 durch die Summe

$$\sum_{\substack{p \text{ gute Reduktion} \\ p=w\overline{w}}} \frac{1}{2}(f(w) + f(-w)).$$

Wir vergleichen diese mit dem heuristischen Wert

$$C \sum_{p \text{ hat gute Reduktion}} (2 \log p)^{-1}.$$

Wir untersuchen zunächst den CM-Körper $D = 13$, $a = 8$ und $b = 3$. Wie bereits auf S. 114 hingewiesen, gilt für $p_{11} = 13660$. Für die anderen p_l setzen wir die Werte aus Tabelle auf S. 117 an. Die Primzahl 13 ist total verzweigt. Wir setzen $p_{13} = \frac{1}{6}$. Wir erhalten dann für die Kardinalität der Menge 5.3 folgende Tabelle ($C = \prod a_l$):

	$13, 8, 3$	
n	tats. Wert	Prognose
10^3	1,5	1,6
10^4	9,3	9,1
10^5	58	55,3
10^6	369	369,0
$\approx C$	0,47	

Die nächste Tabelle enthält einige weitere Galoissche CM-Körper mit $h_K = 1$. Die zweite Zeile gibt jeweils die Primzahl an, die in $K/\mathbb{Q}$ verzweigt ist.

	$29, 17, 5$		$37, 43, 12$		$53, 55, 4$	
	$l = 29, p_l = \frac{1}{14}$		$l = 37, p_l = \frac{1}{18}$		$l = 53, p_l = \frac{1}{26}$	
n	tats. Wert	Prognose	tats. Wert	Prognose	tats. Wert	Prognose
10^3	7	6,0	5,5	6,0	14	10,5
10^4	29,5	32,3	30,5	32,2	75,5	69,0
10^5	194	195,1	197,5	193,5	451	437,9
10^6	1312,5	1313,4	1309,5	1291,7	3018	2982,4
$\approx C$	1,69		1,66		3,85	

Nun wenden wir uns dem Fall zu, daß K nicht Galoissch ist.
Die Funktion f ist mit der Funktion im Galoisschen Fall identisch. Sie ist auf den Elementen $w \in \mathcal{O}_K$ mit $w\overline{w} = p$ definiert. In diesem Fall kann das Element w auch prim sein. Wir errechnen wieder die Mächtigkeit der Menge 5.3 durch den Wert

$$\sum_{\substack{p \le n, \text{ Normgl. eine Lösung} \\ p = w\overline{w},\ w \in \mathcal{O}_K}} \frac{1}{2}(f(w) + f(-w)) + \sum_{\substack{p \le n,\ w_1 \neq \pm w_2 \\ p = w_1\overline{w_1} = w_2\overline{w_2}}} \frac{1}{4}(f(w_1) + f(-w_1) + f(w_2) + f(-w_2)).$$

Wir vergleichen ihn mit dem heuristischen Wert

$$\prod_{l \text{ prim,unverzweigt}} a_l \sum_{\substack{p = w\overline{w},\ w \in \mathcal{O}_K \\ p \le n}} \frac{1}{2 \log p}.$$

Die folgenden Tabellen geben die experimentellen Ergebnisse in vier nicht Galoisschen CM-Körper mit $h_K = 1$ wieder. Die zweite Zeile gibt jeweils die verzweigten Primstellen an, und die Wahrscheinlichkeit, mit der diese die Gruppenordnung teilen. In der letzten Spalte steht eine Approximation von $\prod a_l$ über alle l (auch die in $K/\mathbb{Q}$ verzweigten).

	$D = 109, a = 9, b = 1$		$D = 5, a = 10, b = 3$	
	$p_5 = \frac{1}{4}, p_{109} = \frac{219}{109^2-1}$		$p_5 = \frac{11}{(5^2-1)}, p_{61} = \frac{1}{62}$ $p_3 = \frac{3}{16}$	
n	tats. Wert	Prognose	tats. Wert	Prognose
10^3	2	2,2	10,25	8,4
10^4	13,5	11,7	49,25	43,3
10^5	67,25	71,4	263,75	256,8
10^6	477,5	474,9	1715,75	1701,2
$\approx C$	0,41		1,46	

	$D = 29, a = 15, b = 4$		$D = 13, a = 25, b = 9$	
	$p_{29} = \frac{59}{(29^2-1)}$, $p_{53} = \frac{1}{54}$		$p_5 = \frac{27}{13^2-1}$, $p_{157} = \frac{1}{156}$	
n	tats. Wert	Prognose	tats. Wert	Prognose
10^3	16,75	13,2	18,75	15,3
10^4	71,25	68,4	83	84,2
10^5	397,75	402,5	496,5	489,2
10^6	2668	2667,5	3279,75	3274,1
$\approx C$	2,29		2,81	

Bemerkung 5.2.22. Die Implikation dieses Abschnittes für praktische Anwendungen läßt sich einfach zusammenfassen: CM-Körper, in denen die kleinen Primzahlen möglichst träge sind, führen eher zu primen Ordnungen. Als Beispiel betrachte den CM-Körper $D = 53, a = 55, b = 4$. Hier gibt es auffällig viele prime Gruppenordnungen. Tatsächlich sind die Primzahlen 2, 3 und 5 träge, 7 und 11 zerfallen nur in zwei Primideale und erst 13 ist total zerlegt.

Anhang A

Elliptische Kurven mit komplexer Multiplikation

In diesem Kapitel gehen wir kurz auf den allgemein bekannten Fall $g = 1$ ein. Dieser ist in der Literatur bereits vollständig untersucht. Es existieren detailierte Programmbeschreibungen [38]. Wir widmen uns hier nur den folgenden zwei Fragestellungen:

1. Wie lange dauert in etwa die Berechnung des Klassenpolynoms in Abhängigkeit von der Klassenzahl?

2. Was ist die maximale Klassenzahl, die wir mit dem CM-Verfahren für elliptischen Kurven erreichen können?

Die Tabelle auf Seite 124 gibt einige Zeiten an. Die Berechnungen wurden auf einem Pentium III with 650 Mhz durchgeführt.
Man beachte, daß die Laufzeit zur Berechnung des Klassenpolynoms nicht nur von der Klassenzahl, sondern auch von der Diskriminante des CM-Körpers abhängt. Je größer die Diskriminante desto höher ist die von uns gewählte Präzision.
Wir haben bewußt besonders viele CM-Körper mit Klassenzahl zwischen 200 und 300 in die Tabelle aufgenommen, da der CM-Körper - nach den Vorgaben des BSI - mindestens Klassenzahl 200 haben sollte. Wir sehen, daß solche Klassenpolynome sehr schnell berechnet werden können.

Um die maximale Klassenzahl zu bestimmen, für die die CM-Methode von praktischer Bedeutung ist, vergleichen wir die Laufzeit des CM-Verfahrens mit dem Schoof-Atkin-Elkies-Algorithmus.
Bei der CM-Methode wählen wir zunächst einen imaginär quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{D})$ gegeben durch seine Diskriminante D. Wir suchen Primzahlen, die bezüglich $K/\mathbb{Q}$ eine Normgleichung erfüllen. Dabei gehen wir so vor, daß wir zufällige Elemente $w \in \mathcal{O}_K$ wählen und testen, ob deren Norm prim ist. Dies ist schneller als die zufällige Wahl von Primzahlen in $\mathbb{Z}$ und Anwendung des Algorithmus von Cornaccia. Inbesondere ist diese Vorgehensweise von der Klassenzahl $h(\mathcal{O}_K)$ unabhängig.

Wenn wir eine Primzahl p mit $p = w\overline{w}$ gefunden haben, testen wir, ob eine der beiden resultierenden Gruppenordnungen $(1 \pm w)(1 \pm \overline{w})$ prim ist. Der Schritt von der Diskriminante des CM-Körpers zu einer geeigneten Primzahl mit kryptographisch geeigneter Gruppenordnung dauert weniger als eine Sekunde. Untenstehende Tabelle gibt die Zeiten an, um **1000** Primzahlen der Größenordnung 2^{160} zu finden, die in $K/\mathbb{Q}$ eine Normgleichung erfüllen und für die $\#E(\mathbb{F}_p)) = k \cdot prim$ mit $k \leq 1000$ und .

D	Zeit, um **1000** Primzahlen p mit **kryptographisch geeigneter Ordnung** $\#E(\mathbb{F}_p)$ zu finden	D	Zeit, um **1000** Primzahlen p mit **kryptographisch geeigneter Ordnung** $\#E(\mathbb{F}_p)$ zu finden
-53444	476.25s	-973496	437.32s
-345124	292.89s	-2128136	424.44s
-17111	734.06s	-900311	698.49s
-19631	733.88s	-1139519	807.23s
-19031	521.46s	-2155919	876.61s
-56696	293.71s	-3300359	836.26s
-698472	521.44s	-4145951	904.15s
-98276	293.99s	-5154551	817.52s
-180164	327.60s	-6077111	1013.19s
-237236	345.40s	-7032119	994.38s
-326504	365.75s	-8282039	928.72s

Als nächstes konstruieren wir zu K und p und der geeigneten Gruppenordnung $n = n(K, p)$ eine elliptische Kurve über $\mathbb{F}_p$ mit komplexer Multiplikation mit $\mathcal{O}_K$. Da die Klassenpolynome vorberechnet und bei Bedarf aus einer Datei abgerufen werden können, muß für die tatsächliche Rechenzeit zur Konstruktion einer elliptische Kurve dann nur noch die **einmalige** Faktorisierung des Klassenpolynoms modulo p berücksichtigt werden.
Für das Punktezählen auf einer zufälligen Kurve nach Schoof, Atkin und Elkies benötigt man ungefähr 30 Sekunden. Da etwa nur jede zwanzigste elliptische Kurve kryptographisch geeignet ist, d.h. eine fast prime Gruppenordnung hat, finden wir mit dem SEA-Algorithmus in etwa zehn Minuten eine kryptographisch geeigente Kurve.
In zehn Minuten können wir ein Klassenpolynom vom Grad 5000 faktorisieren. Somit wird erst bei $h_K = 5000$ das Limit der CM-Methode erreicht.

D bezeichne die Diskriminante des Zahlkörpers $K = \mathbb{Q}(\sqrt{D})$ und h_K die Klassenzahl. Die dritte Spalte gibt jeweils die Zeit an, die wir für die Berechnung des Klassenpolynoms benötigten. In der vierten Spalte steht die Zeit für die Berechnung einer Nullstelle modulo p und der dazugehörigen Kurve. Sie gibt also die tatsächliche Laufzeit der CM-Methode wieder.

Komplexität der CM-Methode für $g = 1$ abhängig von Diskriminante und Klassenzahl

D	h_K	Zeit (in s.) f. Polynom	**Zeit (in s.) f. Kurve**	D	h_K	Zeit (in s.) f. Polynom	**Zeit (in s.) f. Kurve**
-53444	200	3	14	-345124	200	4	9
-17111	202	1	8	-19631	208	2	14
-19031	203	1	9	-395652	204	16	10
-56696	204	3	10	-18119	205	1	9
-345624	208	20	20	-690072	208	23	9
-57944	210	3	10	-58484	210	6	11
-159416	212	3	9	-52664	212	3	9
-18191	213	1	9	-55844	216	3	10
-698472	224	26	10	-698772	228	91	10
-128456	236	5	10	-158036	242	11	9
-124004	248	5	15	-78536	252	4	10
-699752	264	9	16	-113636	284	7	16
-98276	304	7	18	-132404	332	24	23
-120056	340	10	20	-144836	352	13	20
-160676	380	16	20	-168164	384	18	19
-180164	400	19	101	-185624	402	32	76
-247796	466	75	24	-248804	468	31	24
-237236	476	78	25	-283076	520	43	35
-318776	540	184	49	-326504	578	60	39
-399944	612	75	39	-434216	630	84	42
-442196	644	218	41	-450056	676	103	44
-512984	714	135	43	-607844	752	161	142
-650744	832	211	192	-727256	866	246	170
-803864	914	291	45	-914744	972	367	48
-973496	1044	460	69	-1202984	1126	599	81
-1319876	1188	728	93	-1435496	1218	803	89
-1514036	1250	2201	93	-1561544	1280	966	98
-1617656	1324	1134	99	-1890776	1404	1467	102
-2128136	1500	1724	99	-701399	1581	566	92

D	h_K	Zeit (in s.) f. Polynom	**Zeit (in s.) f. Kurve**	D	h_K	Zeit (in s.) f. Polynom	**Zeit (in s.) f. Kurve**
-900311	1626	626	94	-1139519	2027	1306	109
-1238639	2150	1595	176	-1614311	2421	3465	193
-1884791	2669	3407	211	-2155919	2968	5373	223
-2336879	3036	5883	212	-3300359	3531	9458	250
-3190151	3593	10034	272	-3312839	3632	10424	269
-3524351	3714	11585	262	-3983591	3918	13694	293
-4145951	4065	16008	281	-4305479	4227	17515	479
-4972679	4498	21830	507	-5154551	4551	22698	521
-5652071	4802	28634	501	-5892311	4913	29785	550
-6077111	5092	34459	509	-6606599	5180	35831	529
-7032119	5424	45254	615	-7651199	5628	52417	589
-7741439	5686	54300	641	-8282039	5819	59305	668

Anhang B

Schlechte Reduktion

Falls die hyperelliptische Kurve in der Form

$$y^2 = f(x) = \sum_{i=0}^{6} a_i x^i \tag{B.1}$$

gegeben ist, lassen sich die Invarianten I_2, I_4, I_6 und I_{10} als Polynome in $\mathbb{Z}[\frac{1}{2}, a_i]$ beschreiben [21].
Sei nun $\mathcal{C}$ ein Modell der Kurve über einem Ganzheitsring $\mathcal{O}_M$ in der oben angegebenen Form (B.1). Falls $j_i \mod \mathfrak{P}$ nicht definiert ist, dann muß $\mathfrak{P}$ den Nenner der Invariante j_i teilen, d.h. es muß ein Teiler der Invariante I_{10}, also der Diskriminante der Kurve sein. In diesem Fall hat das Modell $\mathcal{C}$ schlechte Reduktion in $\mathfrak{P}$.
Die folgende Tabelle, in der die Nenner einiger CM-Körper in ihrer Faktorisierung explizit aufgelistet sind, ist von theoretischem Interesse. Sie stützt zahlentheoretische Vermutungen, die aussagen, daß die Norm einer Primstelle, an der die Kurve schlechte Reduktion hat, für einen CM-Körper mit kleiner Diskriminante nicht zu groß wird.

D, a, b	$Nenner$	D, a, b	$Nenner$	D, a, b	$Nenner$
$5, 3, 1$	1	$5, 4, 1$	7^{12}	$5, 5, 1$	$3^7 5^{12}$
$5, 6, 1$	$5^{12}7^{12}23^{12}$	$5, 7, 1$	2^3	$5, 11, 1$	$3^7 5^{12}$
$5, 6, 2$	11^{12}	$5, 8, 1$	$3^5 11^6 13^{12}$	$5, 8, 2$	$5^{12}7^{12}11^6 19^{12}$
$5, 10, 3$	3^7	$5, 18, 7$	$5^{12}7^{12}$	$5, 16, 7$	$7^{12}19^6 31^{12}71^{12}$
$5, 91, 52$	$11^{12}31^{12}41^{12}$	$5, 119, 68$	$11^{12}41^{12}61^{12}71^{12}$	$5, 35, 8$	$2^{10}11^{12}13^{12}$
$5, 18, 6$	$2^3 11^{12}19^{12}31^{12}139^{12}$	$8, 2, 1$	1	$8, 3, 1$	3^4
$8, 4, 1$	$5^{12}7^6$	$8, 5, 1$	$7^{12}11^{12}$	$8, 6, 1$	$3^5 5^{10}17^6$
$8, 6, 3$	7^{12}	$8, 5, 2$	1	$8, 7, 2$	$2^5 5^{11}$
$8, 9, 2$	3^7	$8, 11, 4$	5^{12}	$8, 13, 4$	$2^{17}7^{12}11^{12}17^{11}$
$8, 13, 6$	3^7	$8, 19, 4$	$5^{12}13^{12}19^{12}$	$8, 15, 4$	3^7
$8, 10, 2$	$7^{12}11^{12}$	$12, 6, 1$	$2^3 11^6 17^{12}29^{12}$	$12, 9, 4$	2^3

D, a, b	$Nenner$	D, a, b	$Nenner$	D, a, b	$Nenner$
$12, 11, 4$	3^{7}	$12, 5, 2$	3^{7}	$12, 17, 8$	3^{7}
$13, 5, 1$	2^{3}	$13, 3, 1$	1	$13, 8, 3$	1
$13, 11, 4$	5^{12}	$13, 16, 6$	$3^{7}23^{12}131^{12}$	$13, 7, 1$	$3^{7}5^{12}7^{11}19^{12}$
$13, 75, 20$	$3^{7}53^{12}$	$17, 6, 1$	$2 \cdot 5^{12}11^{12}23^{12}$	$17, 3, 1$	1
$17, 9, 1$	$2^{4}47^{12}$	$17, 4, 1$	1	$17, 11, 4$	3^{7}
$21, 15, 4$	$3^{6}19^{12}$	$21, 22, 7$	$3^{7}7^{12}19^{12}$	$21, 7, 1$	$3 \cdot 11^{12}$
$21, 5, 1$	$7^{11}11^{12}71^{12}$	$17, 147, 56$	$2^{23}7^{6}43^{12}179^{12}$	$24, 3, 1$	11^{12}
$24, 4, 1$	$3^{7}5^{6}31^{12}$	$24, 9, 2$	7^{11}	$24, 31, 12$	$3^{4}11^{12}$
$24, 17, 6$	$3 \cdot 19^{12}$	$28, 3, 1$	7^{6}	$28, 43, 16$	7^{11}
$28, 7, 2$	$5^{12}7^{3}$	$29, 7, 2$	1	$29, 5, 1$	3^{7}
$29, 17, 5$	5^{12}	$29, 4, 1$	$5^{6}31^{12}$	$29, 9, 1$	$5^{6}7^{11}$
$29, 15, 4$	$11^{12}13^{12}17^{12}$	$29, 24, 7$	13^{6}	$29, 12, 3$	$3^{2}19^{12}$
$29, 31, 4$	5^{12}	$33, 7, 2$	1	$33, 95, 28$	$7^{12}11^{12}23^{12}$
$33, 15, 4$	$3^{7}7^{12}$	$37, 15, 4$	5^{11}	$37, 7, 1$	$2 \cdot 3$
$37, 19, 5$	5^{12}	$37, 43, 12$	$3^{7}11^{12}$	$37, 26, 7$	$17^{12}19^{12}$
$37, 4, 1$	$3 \cdot 23^{12}$	$41, 4, 1$	7^{12}	$41, 5, 1$	3^{7}
$41, 9, 2$	$7^{10}11^{12}19^{12}23^{6}$	$41, 10, 2$	$3^{7}5^{6}$	$44, 4, 1$	$5^{6}11^{12}19^{12}$
$44, 7, 2$	11^{6}	$44, 67, 20$	$5^{12}11^{12}$	$53, 5, 1$	$3^{5}7^{6}29^{12}$
$53, 55, 4$	$17^{12}29^{12}$	$56, 4, 1$	$7^{6}23^{12}$	$56, 43, 14$	$2^{10}7^{6}13^{6}29^{1}2$
$57, 5, 1$	5^{12}	$57, 9, 2$	$3\dot{7}^{6}$	$61, 5, 1$	1
$61, 67, 12$	$3^{19}5^{12}41^{12}$	$62, 9, 2$	$3 \cdot 11^{12}23^{12}$	$69, 6, 1$	$3^{7}13^{6}53^{12}103^{12}$
$73, 6, 1$	11^{12}	$76, 9, 2$	$5^{6}11^{12}19^{6}$	$73, 5, 1$	7^{12}
$76, 5, 1$	$3 \cdot 5^{12}23^{12}71^{12}$	$76, 279, 64$	19^{6}	$88, 5, 1$	$3^{7}11^{12}47^{12}$
$88, 85, 18$	$3^{19}11^{6}43^{12}89^{12}$	$89, 6, 1$	1	$89, 11, 2$	$5^{12}7^{12}11^{6}$
$92, 5, 1$	$7^{12}23^{6}31^{12}$	$92, 29, 6$	$3^{5}17^{12}23^{6}$	$92, 77, 16$	$2^{23}5^{12}23^{11}$
$97, 9, 1$	1	$101, 7, 1$	2^{2}	$109, 9, 1$	5^{6}
$97, 8, 1$	7^{12}	$109, 10, 1$	$3^{4}19^{12}47^{12}167^{12}$	$113, 7, 1$	$5^{12}11^{12}13^{12}31^{12}$
$124, 39, 7$	$7^{12}31^{6}47^{12}$	$124, 23, 4$	$3^{7}17^{12}$	$124, 45, 8$	$2^{11}5^{9}31^{6}37^{12}$
$129, 13, 2$	$7^{12}11^{11}17^{12}$	$133, 9, 3$	$3^{19}7^{2}47^{12}167^{12}199^{12}$	$137, 7, 1$	$7^{11}23^{12}31^{12}47^{12}$
$137, 10, 1$	$5^{12}103^{12}$	$141, 9, 1$	$3^{7}7^{12}53^{12}$	$149, 7, 1$	11^{12}
$157, 13, 1$	$3^{19}17^{12}23^{12}$	$152, 13, 2$	19^{6}	$233, 10, 1$	$7^{12}23^{12}$
$269, 9, 1$	$5^{6}11^{12}$				

Anhang C

Verwendete Programme

Für diese Arbeit haben wir eine Reihe von Computerprogrammen und -bibliotheken verwendet.

- **Pari/GP**
  Eine Zahlentheorie-Bibliothek, die unter anderem Funktionen zur Berechnung in relativen Zahlkörpern enthält. Frei erhältlich unter

  `ftp://megrez.math.u-bordeaux.fr/pub/pari`.

- **Magma**
  Ein riesiges kommerzielles Computeralgebra-System, das wir zum Beispiel für Berechnungen von Gröbner-Basen über $\mathbb{F}_p$ verwendet haben. Informationen findet man unter

  `http://www.maths.usyd.edu.au:8000/u/magma/`.

- **Kant/Kash**
  Ein Zahlentheorie-System, das unter anderem Funktionen zur Berechnung von Strahlklassengruppen enthält. Frei erhältlich unter

  `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`.

- **NTL**
  Eine C++-Bibliothek für effiziente Polynomarithmetik.

  `http://www.shoup.net/ntl/`.

- **CLN**
  Eine weitere C++-Bibliothek mit Langzahlarithmetik.

  `http://clisp.cons.org/~ haible/packages-cln.html`.

Literaturverzeichnis

[1] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *unpublished manuscript*, 1991.

[2] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[3] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Groebner bases. *Springer LNCS*, 72:3–21, 1979.

[4] B. Buchberger. A note on the complexity of constructing Gröbner bases. *Springer LNCS*, 162:137–145, 1983.

[5] J.W.S. Cassels. *Lecture on Elliptic Curves*. Cambridge University Press, 1991.

[6] A. Clebsch. *Theorie der binären algebraischen Formen*. Teubner, 1873.

[7] H. Cohen. *Advanced Topics in Computational Number Theory*. Springer, 2000.

[8] D.A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[9] C. Diem. *A study of theoretical and practical aspects of Weil-restriction of varieties*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 2001.

[10] B. Dodson. The structure of galois groups of CM-fields. *Trans. AMS*, 283:1–32, 1984.

[11] G. Faltings and G. Wüstholz. *Rational points*. Vieweg, 1984.

[12] G. Frey, M. Müller, and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1718, 1999.

[13] G. Frey and H.-G. Rück. A remark concerning m-divisbility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[14] J. von zur Gathen and Victor Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2:187–224, 1992.

[15] P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. *ANTS IV*, 2000.

[16] P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *to appear in J.Cryptology*, 2000.

[17] W.-D. Geyer. Invarianten binärer Formen. *Lecture Notes in Math.*, 412:36–69, 1978.

[18] B. Huppert. Singer-Zyklen in klassischen Gruppen. *Math. Z.*, 117:141–150, 1970.

[19] B. Huppert. *Endliche Gruppen I.* Springer, 1983.

[20] J. Igusa. *Theta Functions.* Springer, 1972.

[21] J.-I. Igusa. The arithmetic variety of genus two. *Ann. Math.*, 72:612–649, 1960.

[22] D.E. Knuth. *The Art of Computer Programming Vol.2, Seminumerical Algorithms.* Addison-Weseley, 1981.

[23] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.*, 131:157–165, 1988.

[24] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.

[25] N. Koblitz. CM-curves with good cryptographic properties. *Advances in Cryptology, Crypto 91, LNCS*, 576:203–209, 1992.

[26] N. Koblitz. *Algebraic Aspects of Cryptology.* Springer, 1998.

[27] D. Kohel. *Endomorphisms of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.

[28] D. Kuhlman. *On the Orders of Jacobians of Hyperelliptic Curves.* PhD thesis, University of Illinois at Urbana-Champaign, 2000.

[29] S. Lang. *Introduction to Algebraic and Abelian Functions.* Springer-Verlag, 2nd edition, 1982.

[30] S. Lang. *Complex Multiplication.* Springer-Verlag, 1983.

[31] S. Louboutin. Determination of all nonquadratic imaginary cyclic quartic number fields of 2-power degrees with ideal class groups of exponents ≤ 2. *Math. Comp.*, pages 323–340, 1995.

[32] J.-F. Mestre. Construction des courbes de genre 2 a partir de leurs modules. *Prog.Math., Birkhäuser*, 94:313–334, 1991.

[33] J.-S. Milne. Abelian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 103–150. Springer-Verlag, 1986.

[34] J.-S. Milne. Jacobian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer-Verlag, 1986.

[35] D. Mumford. *Tata Lecture on Theta, Band I.* Birkhäuser, 1983.

[36] D. Mumford. *Tata Lecture on Theta, Band II.* Birkhäuser, 1984.

[37] J. Neukirch. *Class Field Theory.* Springer, 1986.

[38] IEEE P1363. Standard specifications for public key cryptography. *http://grouper.ieee.org/groups/1363/*, 2000.

[39] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. *ANTS III, LNCS*, 1423:576–591, 1998.

[40] S. Pohlig and M. Hellmann. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory*, IT-24:106–110, 1978.

[41] E. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory.* Cambridge University Press, 1989.

[42] C. Poor. The hyperelliptic locus. *Duke Math. J.*, 76:809–884, 1994.

[43] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, pages 301–304, 1987.

[44] N. Schappacher. Zur Existenz einfacher Abelscher Varietäten mit komplexer Multiplikation. *J. Reine Angew. Math.*, 292:186–190, 1977.

[45] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7, 1995.

[46] J.-P. Serre. *Topics in Galois Theory.* Springer, 1992.

[47] J. P. Serre. Lettre á Marie-France Vignéras. In *Collected Papers*, pages 38–55. Springer-Verlag, 2000.

[48] N.I. Shepherd-Barron. Apolarity and its applications. *Inv. Math.*, 97:433–444, 1989.

[49] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, 1971.

[50] G. Shimura. *Abelian Varieties with complex multiplication and modular functions.* Princeton University Press, revised edition, 1998.

[51] T. Shioda. On the graded ring of binary octavics. *Am.J. Math.*, 89:1022–1046, 1967.

[52] V. V. Shokurov. Riemann surfaces and algebraic curves. In I.R. Shafarevich, editor, *Algebraic Geometry I*, pages 1–168. Springer-Verlag, 1991.

[53] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[54] J.A. Solinas. Generalized Mersenne numbers. *Technical Reports, CACR, Waterloo*, 1999.

[55] A.-M. Spallek. Konstuktion einer elliptischen Kurve über einem endlichen Körper zu gegebener Punktegruppe. Master's thesis, Institut für Experimentelle Mathematik Universität GH Essen, 1992.

[56] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen.* PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

[57] A. Stein and E. Teske. The parallelized pollard's kangaroo method in real quadratic function fields. *to appear in Math. Comp.*, 2000.

[58] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[59] P. Van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68, 1999.

[60] X. Wang. 2-dimensional simple factors of $J_0(N)$. *Manuscr. Math.*, 87:179–197, 1995.

[61] H.-J. Weber. *Algorithmische Konstruktion hyperelliptischer Kurven mit kryptographischer Relevanz und einem Endomorphismenring echt grösser als* $\mathbb{Z}$. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1997.

[62] H.J. Weber. Hyperelliptic simple factors of $J_0(N)$ with dimension at least 3. *Experimental Math.*, 6:273–287, 1997.

[63] Annegret Weng. Das diskrete Logarithmusproblem auf elliptischen Kurven mit einem Endomorphismenring kleiner Klassenzahl. Master's thesis, Universität Frankfurt, 1999.