Universelle elliptische Gauß-Summen und der Algorithmus von Schoof

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Christian Johannes Berghoff

aus
Münster

Bonn, September 2016

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter:	Prof. Dr. Jens Franke
2. Gutachter:	Prof. Dr. Preda Mihăilescu
Tag der Promotion:	13. 4. 2017
Erscheinungsjahr:	2017

Für meine Eltern

Danksagung

An erster Stelle danke ich meinem Betreuer Herrn Prof. Jens Franke für den interessanten Themenvorschlag und die fachliche Unterstützung während meiner Promotionszeit. Großer Dank geht an Herrn Prof. Preda Mihăilescu, der mich sowohl bei der Bewerbung um die Promotionsstelle in Bonn als auch bei der Anbahnung meines Forschungsaufenthalts an der École polytechnique unterstützt und der sich weiterhin bereit erklärt hat, das Zweitgutachten für diese Arbeit zu erstellen. Mein besonderer Dank gilt Jan Büthe, der es mir leicht gemacht hat, mich am Institut in Bonn einzuleben, und der mich zu zahlreichen Fragen persönlicher und fachlicher Natur klug beraten hat.

Je remercie toute l'équipe GRACE de m'avoir permis de passer six mois enrichissants à Paris et de m'avoir aussi chaleureusement accueilli.

In meiner Zeit an Schule und Universität hatte ich das Glück, von einigen sehr guten Lehrern zu lernen. Unter ihnen allen heraus ragt mein Lateinlehrer Dr. Markus Schmitz, der mein Leben rückblickend entscheidend geprägt hat. Von seinem viel zu frühen Tod habe ich erst kürzlich mit großer Bestürzung erfahren.

Die Erstellung dieser Arbeit wurde ermöglicht durch die großzügige Förderung im Rahmen der BIGS, wofür ich den Verantwortlichen herzlich danke. Weiterhin bin ich Frau Bingel, Frau Schmidt und Frau Sievert für die stets nette und schnelle Hilfe bei allen Formalitäten dankbar.

Schließlich gilt mein großer Dank meiner Familie: Manfred und Veronika danke ich für die Umzugshilfe und Unterstützung beim Start in Bonn. Meinen Schwestern Julia und Carolin danke ich für unseren tollen Familienzusammenhalt.
Ganz besonders danke ich meinen Eltern Gabriele und Reinhard für die fortwährende Unterstützung, die ich von ihnen bekommen habe, seit ich denken kann. Ihnen widme ich diese Arbeit.

Inhaltsverzeichnis

Einleitung **11**

1 Elliptische Kurven **15**
1.1 Definitionen und Fakten . . . 15
1.2 Der Algorithmus von Schoof . . . 18
1.2.1 Ursprünglicher Algorithmus . . . 18
1.2.2 Der SEA-Algorithmus . . . 19
1.2.3 Weitere Verbesserungen . . . 20

2 Universelle elliptische Gauß-Summen **23**
2.1 Modulfunktionen . . . 23
2.1.1 Definition . . . 23
2.1.2 Untergruppen . . . 26
2.1.3 Aussagen über Modulfunktionen von Gewicht 0 . . . 28
2.2 Die Tate-Kurve . . . 32

3 Berechnung der universellen elliptischen Gauß-Summen **39**
3.1 Definitionen . . . 39
3.2 Laurentreihen . . . 40
3.2.1 Allgemeine Bemerkungen . . . 40
3.2.2 Verbesserung des Algorithmus . . . 41
3.3 Rationaler Ausdruck . . . 44
3.3.1 Allgemeines . . . 44
3.3.2 Verwendung von m_ℓ . . . 45
3.3.3 Verwendung von a_ℓ . . . 50
3.3.4 Weitere Betrachtungen . . . 55

4 Punktezählen im Elkies-Fall **57**
4.1 Bestimmung des Eigenwerts . . . 57
4.2 Verwendung von m_ℓ . . . 58
4.3 Verwendung von a_ℓ . . . 60
4.4 Jacobi-Summen . . . 61
4.4.1 Definition . . . 61
4.4.2 Implementierung . . . 63
4.5 Weitere Überlegungen . . . 64
4.6 Laufzeit und Speicherbedarf . . . 65
4.7 Vergleich von m_ℓ und a_ℓ . . . 68

5 Verwendung von Primzahlpotenzen **73**
5.1 Universelle elliptische Gauß-Summen . . . 73
5.2 Berechnung . . . 76

6 Universelle elliptische Gauß-Summen im Atkin-Fall **81**
6.1 Definition . . . 81
6.2 Rationale Darstellung . . . 84
6.3 Anwendung . . . 88

6.4 Laufzeit 90

7 Polynomiell zyklische Algebren **93**
7.1 Definitionen 93
7.2 Anwendung 95
7.2.1 Verbesserungen 98
7.3 Laufzeit 100
7.3.1 Bestimmung von $\beta(\chi_q)$ 100
7.3.2 Berechnung von α 101
7.3.3 Berechnung von t 102
7.3.4 Gesamtlaufzeit 102

Notation **105**

Literaturverzeichnis **107**

Κτῆμά τε ἐς αἰεὶ μᾶλλον ἢ ἀγώνισμα ἐς τὸ παραχρῆμα ἀκούειν ξυγκείμενον εἴη.
– frei nach Θουκυδίδης 1, 22

Einleitung

Diese Arbeit untersucht verschiedene auf der Grundidee von Schoof basierende Algorithmen im Kontext des Punktezählens auf elliptischen Kurven über endlichen Körpern $\mathbb{F}_p$ mit großer Charakteristik.

In der algorithmischen Zahlentheorie werden elliptische Kurven bei der Lösung einer Vielzahl von Problemen verwendet. Die größte praktische Relevanz weist hierbei ihr Einsatz in der Kryptographie auf (vgl. [Was08, S. 169–188]), wie er erstmalig von Koblitz in [Kob87] als Alternative zu Verfahren, die auf der multiplikativen Gruppe endlicher Körper basieren, vorgeschlagen wurde. Die heute verwendeten kryptographischen Routinen unter Verwendung elliptischer Kurven (Elliptic Curve Cryptography, ECC) basieren im Wesentlichen darauf, dass für die Berechnung diskreter Logarithmen in der Gruppe der Punkte $E(\mathbb{F}_p)$ einer allgemeinen elliptischen Kurve E bis heute kein Algorithmus existiert, dessen Komplexität subexponentiell in $\log p$ ist. In endlichen Körpern ist hingegen mit dem Index-Calculus-Algorithmus ein solches Verfahren gegeben. Dies hat zur Folge, dass bei Verwendung von ECC erheblich kürzere Schlüssellängen als in traditionellen Verfahren wie RSA ausreichend sind, um dasselbe Niveau an Sicherheit zu garantieren. Insbesondere in Situationen, in denen Speicher- und Rechenkomplexität begrenzt sind, beispielsweise auf Chipkarten wie im neuen deutschen Personalausweis (vgl. [LM09]), kommen daher ECC-Verfahren in zunehmendem Maße zur Anwendung.
Da für verschiedene spezielle Klassen elliptischer Kurven Algorithmen zur Berechnung diskreter Logarithmen mit deutlich geringerer Laufzeit bekannt sind (vgl. [Was08, S. 143–168]), muss sichergestellt werden, dass die verwendeten Kurven für diese Angriffe nicht anfällig sind. Dies ist der Fall, wenn $\#E(\mathbb{F}_p)$ bestimmte Eigenschaften erfüllt, beispielsweise wenn $\#E(\mathbb{F}_p)$ eine von p verschiedene Primzahl ist. Zur Bestimmung von $\#E(\mathbb{F}_p)$ für eine (zufällig erzeugte) Kurve E werden seit 1985 der Algorithmus von Schoof und seine verbesserten Varianten eingesetzt. Für Kurven über Körpern $\mathbb{F}_{p^n}$ mit großem Erweiterungsgrad n und kleiner Charakteristik p, die in der Praxis aus Sicherheitsgründen jedoch wenig Verwendung finden, existiert gemäß [BSS05, S. 103–115] seit 1999 mit dem Algorithmus von Satoh ein alternativer Ansatz mit besserer Laufzeit. Mithilfe der Theorie der komplexen Multiplikation ist es weiterhin in gewissen Fällen möglich, Kurven mit vorgegebener Anzahl an Punkten zu erzeugen [Sch10, S. 266–287].

Neben der Anwendung im Rahmen von ECC werden elliptische Kurven beispielsweise in Algorithmen zur Faktorisierung ganzer Zahlen (nach der Elliptic Curve Factorization Method von Lenstra) oder für Primalitätstests (aufbauend auf dem Goldwasser-Kilian-Test) eingesetzt [Was08, S. 189–197]. Neue Ansätze zur Verwendung elliptischer Kurven in Primalitätstests wurden in [Mih06b] vorgeschlagen und in [FKDG12] weiter ausgearbeitet. Vielen dieser Algorithmen ist gemein, dass sie die multiplikative Gruppe endlicher Körper oder diejenige der Einheitswurzeln in Kreisteilungskörpern, auf denen frühere Algorithmen basieren, durch die Gruppe der Punkte auf einer elliptischen Kurve oder deren Torsionspunkte ersetzen, was in Zwischenschritten eine höhere Flexibilität und letztlich bessere Laufzeiten ermöglicht. Diesem Ansatz folgen auch die Ideen aus [BDD$^+$] zur Berechnung expliziter Isomorphismen zwischen

endlichen Körpern.

Wir geben zunächst eine kurze Einführung zu elliptischen Kurven, dem Algorithmus von Schoof sowie seinen Verbesserungen durch Elkies und Atkin mit einigen Varianten. Dabei erinnern wir insbesondere an die erstmals in [Mih06c] eingeführten elliptischen Gauß-Summen, auf der ein Großteil der in dieser Arbeit vorgestellten Ansätze aufbaut.

Im folgenden zweiten Kapitel führen wir zuerst die für unsere Untersuchungen notwendigen Begriffe aus der Theorie der Modulfunktionen ein. Anschließend beweisen wir durch galoistheoretische Überlegungen den wichtigen Satz 2.1.11 über die Gestalt gewisser Körper von Modulfunktionen, der die Grundlage für unsere neuen Algorithmen bildet. Hierauf folgen verschiedene Verbesserungen der Aussage dieses Satzes, die durch die praktische Effizienz der Algorithmen motiviert sind. Ausgehend von der Weierstraßschen $\wp$-Funktion und der Tate-Kurve, die die Isomorphieklassen elliptischer Kurven über $\mathbb{C}$ parametrisiert, definieren wir die universellen elliptischen Gauß-Summen und zeigen mithilfe der vorigen Ergebnisse, dass ihre Eigenschaften es erlauben, sie als rationale Funktion R in der j-Invarianten und einer weiteren Modulfunktion darzustellen.

Das dritte Kapitel ist der detaillierten Ausarbeitung dieser allgemeinen Aussage gewidmet. Wir betrachten und lösen verschiedene praktische Probleme, worauf wir konkrete Algorithmen zur Berechnung der rationalen Funktion R angeben, die wir mit der Programmiersprache C implementiert haben (die Programme sind in diese Arbeit nicht eingebunden, jedoch auf Wunsch vom Verfasser erhältlich). Als zweite neben der j-Invarianten zu verwendende Modulfunktion untersuchen wir die Alternativen m_ℓ und a_ℓ, die bereits aus früheren Arbeiten zum Algorithmus von Schoof bekannt sind [Mül95]. Es stellt sich heraus, dass die Algorithmen auf Basis von a_ℓ aus Laufzeitgründen vorzuziehen sind.

Im vierten Kapitel befassen wir uns mit der Anwendung der zuvor berechneten Ergebnisse zum Punktezählen auf einer konkreten elliptischen Kurve für Elkies-Primzahlen ℓ. Die vorgestellten Ansätze haben wir ebenfalls in C implementiert. Die Grundidee besteht darin, dass aufgrund der Eigenschaften der Tate-Kurve die Darstellungen der universellen elliptischen Gauß-Summen auf eine konkrete Kurve E spezialisiert werden können, wodurch sich Formeln zur Berechnung der elliptischen Gauß-Summen in Abhängigkeit von anderen effizient zu berechnenden Werten auf E ergeben. Eine Laufzeitanalyse zeigt, dass mithilfe der neuen Algorithmen die elliptischen Gauß-Summen schneller berechnet werden können als direkt anhand ihrer Definition, was gemäß [Fra16] ihre Verwendung im Rahmen der in [Mih06b, FKDG12] ausgearbeiteten Ansätze für Primalitätstests sinnvoll erscheinen lässt. Eine effiziente Verwendung als Teilroutine des Algorithmus von Schoof bleibt gleichwohl unwahrscheinlich, da andere bereits existierende Verbesserungen eine geringere Laufzeit aufweisen. Abschließend quantifizieren wir anhand der von uns durchgeführten Rechnungen die Unterschiede bei Verwendung der Modulfunktionen m_ℓ sowie a_ℓ.

Nachfolgend zeigen wir, dass die elliptischen Gauß-Summen aus [Mih06c] und damit auch die universellen elliptischen Gauß-Summen von Primzahlen ℓ auf Primzahlpotenzen ℓ^i verallgemeinert werden können. Im Fall $i = 2$ untersuchen wir ähnlich zu den vorherigen Abschnitten die Berechnung und praktische Anwendung der universellen elliptischen Gauß-Summen.

Das sechste Kapitel behandelt die Verwendung universeller elliptischer Gauß-Summen im Fall von Atkin-Primzahlen ℓ. Dafür modifizieren wir die Definition auf geeignete Weise, zeigen erneut Resultate zur Darstellbarkeit der Gauß-Summen als rationale Funktionen in anderen Modulfunktionen und führen abschließend aus, wie die Resultate im Atkin-Fall praktisch verwendet werden können.

Das letzte Kapitel ist unabhängig von der übrigen Arbeit. In ihm werden Ansätze zur Behandlung des Atkin-Falls auf der Grundlage sogenannter polynomiell zyklischer Algebren, wie sie bereits in [Ber13, Á14] ausführlich untersucht wurden, weitergeführt und leicht verbessert. Eine detaillierte Laufzeitanalyse zeigt jedoch auch hier, dass die Ergebnisse im Rahmen des Algorithmus von Schoof keine praktische Verbesserung zu erwirken vermögen.

1 Elliptische Kurven

Das mathematische Objekt, das die in dieser Arbeit vorgestellten Ideen motiviert, ist eine elliptische Kurve E über einem endlichen Körper $K = \mathbb{F}_p$ mit einer Primzahl p. In diesem Abschnitt stellen wir die für uns relevanten Eigenschaften elliptischer Kurven dar, wobei wir im Wesentlichen [Sil09], [Was08] benutzen und eng [Ber13] folgen.

1.1 Definitionen und Fakten

Wir arbeiten mit elliptischen Kurven nicht in größtmöglicher Allgemeinheit und beginnen daher mit der folgenden

Definition 1.1.1. [Sil09, S. 42] Sei K ein beliebiger Körper. Dann ist eine *elliptische Kurve* E über K gegeben durch

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad \text{mit} \quad a_i \in K,\ i = 1, \ldots, 6,$$

zusammen mit $\mathcal{O}$, dem Punkt bei Unendlich.

Ist $\mathrm{char}(K) \neq 2, 3$, so erhält man durch geeignete Substitutionen die Gleichung

$$E : Y^2 = X^3 + aX + b \quad \text{mit} \quad a, b \in K.$$

Wir werden im Folgenden diese Gleichung benutzen, da wir nur Primzahlen $p > 3$ betrachten werden. Weiterhin werden wir die elliptische Kurve E mit der Menge der Punkte

$$E(\overline{K}) = \{P = (X, Y) \in \overline{K} \times \overline{K} \colon\ Y^2 = X^3 + aX + b\} \cup \{\mathcal{O}\}$$

identifizieren, die im algebraischen Abschluss $\overline{K}$ von K auf ihr liegen. Wir nennen einen Punkt $P = (P_x, P_y)$ der Kurve E *rational*, wenn seine Koordinaten in K liegen. Die Menge dieser Punkte zusammen mit dem Punkt bei Unendlich bezeichnen wir als $E(K)$. Im Rahmen dieser Arbeit sind wir daran interessiert, die rationalen Punkte auf elliptischen Kurven über endlichen Körpern $K = \mathbb{F}_p$ zu bestimmen. Bekanntlich sind zu einer elliptischen Kurve die folgenden Größen definiert:

Definition 1.1.2. [Was08, S. 46] Sei E eine elliptische Kurve über K mit der Gleichung $E : Y^2 = X^3 + aX + b$. Dann definieren wir die *Diskriminante* von E als

$$\Delta(E) := -16(4a^3 + 27b^2). \tag{1.1}$$

Im Rahmen dieser Arbeit werden wir annehmen, dass $\Delta \neq 0$ gilt, anderenfalls heißt die Kurve E *singulär*. Weiterhin definieren wir die *j-Invariante* von E mittels

$$j(E) := 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{1.2}$$

Offenbar ist die j-Invariante wegen $\Delta \neq 0$ wohldefiniert.

Mit der gut bekannten Operation zur Addition von Punkten weist eine elliptische Kurve E die Struktur einer abelschen Gruppe mit neutralem Element $\mathcal{O}$ auf [Sil09, S. 51–54]. Aus den

Formeln für die Addition in [Was08, S. 14] folgt sofort, dass $E(K)$ eine Untergruppe von E ist.

Einer der für den Algorithmus von Schoof (s. Abschnitt 1.2) zentralen Begriffe wird durch folgende Definition gegeben:

Definition 1.1.3. Sei E eine elliptische Kurve über K und $m \in \mathbb{N}$. Dann definieren wir die *m-Torsion* von E als

$$E[m] := \{P \in E : mP = \mathcal{O}\}.$$

$E[m]$ enthält also die Punkte auf E, deren Ordnung m teilt. $E[m]$ ist offenbar eine Untergruppe von E.

Auf der m-Torsion ist die Weil-Paarung

$$e_m : E[m] \times E[m] \to \mu_m$$

definiert (für die genaue Definition s. [Sil09, S. 95–96]), die unter anderem die folgenden Eigenschaften aufweist:

Proposition 1.1.4. *[Sil09, S. 96] Seien $S, T, S_i, T_i \in E[m]$, $i = 1, 2$. Dann gilt*

1. $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$,
   $e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$.
2. $e_m(T, T) = 1$, *insbesondere* $e_m(S, T) = e_m(T, S)^{-1}$.

Laut [Sil09, S. 86–87] gilt für die m-Torsion einer elliptischen Kurve E über einem endlichen Körper $\mathbb{F}_p$ mit $p \neq m$ die Aussage

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}. \tag{1.3}$$

Im Algorithmus von Schoof werden Rechnungen in der ℓ-Torsion für eine Primzahl ℓ ausgeführt, während $K = \mathbb{F}_p$ mit einer großen Primzahl p ist. Daher gilt immer $\ell < p$ und die Voraussetzung ist somit erfüllt. Als Nächstes benötigen wir die folgende

Definition 1.1.5. Seien E_1 und E_2 zwei elliptische Kurven. Eine *Isogenie* von E_1 nach E_2 ist ein Morphismus

$$\psi : E_1 \to E_2 \quad \text{mit} \quad \psi(\mathcal{O}) = \mathcal{O}.$$

Gemäß [Sil09, S. 20] sind Morphismen zwischen algebraischen Kurven, also insbesondere zwischen elliptischen Kurven, entweder konstant oder surjektiv. Daher gilt für eine Isogenie

$$\psi(E_1) = \mathcal{O} \quad \text{oder} \quad \psi(E_1) = E_2.$$

Weitere Eigenschaften von Isogenien finden sich in [Sil09, S. 45] sowie [Sil09, S. 71].
Die Menge der Isogenien zwischen zwei elliptischen Kurven schreiben wir mit der üblichen Notation als

$$\mathrm{Hom}(E_1, E_2) = \{\text{Isogenien } \psi : E_1 \to E_2\} \quad \text{und} \quad \mathrm{End}(E) = \mathrm{Hom}(E, E).$$

Wir zitieren noch den folgenden wichtigen Satz nach [Sil09, S. 74].

Satz 1.1.6. *Sei E eine elliptische Kurve und $\mathcal{C}$ eine endliche Untergruppe von E. Dann gibt es eine eindeutig bestimmte elliptische Kurve E' und eine Isogenie*

$$\psi : E \to E'$$

mit $\ker(\psi) = \mathcal{C}$. *In diesem Fall schreiben wir statt E' auch $E/\mathcal{C}$.*

Definition 1.1.7. Sei E eine elliptische Kurve über einem Körper K und $\psi : E \to E'$ eine Isogenie. Wenn $\deg(\psi) = m$ ist, so wird ψ als *m-Isogenie* bezeichnet. Die allgemeine Definition von $\deg(\psi)$ findet sich in [Sil09, S. 21]. Wenn $\mathrm{ggT}(m, \mathrm{char}(K)) = 1$ gilt, was in den von uns betrachteten Fällen erfüllt ist, folgt aus [Sil09, S. 26–27, 72], dass ψ genau dann vom Grad m ist, wenn $\#\ker(\psi) = m$ gilt. Ist also in Satz 1.1.6 die Gruppe $\mathcal{C}$ von Ordnung m, so ist ψ eine m-Isogenie.

Weiterhin benutzen wir beim Übergang zwischen elliptischen Kurven über Zahlkörpern und endlichen Körpern folgenden Satz von Deuring

Satz 1.1.8. *[Lan87, S. 184] Sei E eine elliptische Kurve über einem endlichen Körper von Charakteristik p mit einem nicht-trivialen Endomorphismus α. Dann existiert eine elliptische Kurve E_0 über einem Zahlkörper K, ein Endomorphismus α_0 von E_0 und ein Primideal $\mathfrak{P} \subset \mathcal{O}_K$ über (p), sodass die durch Reduktion modulo $\mathfrak{P}$ entstehende Kurve $\bar{E}_0$ nicht-singulär und isomorph zu E ist und $\bar{\alpha_0}$ unter diesem Isomorphismus α entspricht. E_0 wird auch als* Deuring-Lift *von E bezeichnet.*

Abgesehen von den sich aus der Addition ergebenden Abbildungen

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

die Elemente von $\mathrm{End}(E)$ sind, enthält der Endomorphismenring einer Kurve E über einem endlichen Körper $\mathbb{F}_p$ den sogenannten *Frobenius-Homomorphismus* ϕ_p, der im Zentrum des Algorithmus von Schoof steht.

Bekanntlich wirkt dieser auf einer Kurve E über $\mathbb{F}_p$ gemäß

$$\phi_p : E \to E, \quad P = (X, Y) \mapsto (X^p, Y^p) = (\varphi_p(X), \varphi_p(Y)), \tag{1.4}$$

wobei $\varphi_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, $x \mapsto x^p$ der aus der Theorie der endlichen Körper bekannte Frobenius-Homomorphismus ist. Durch Einschränkung wird ϕ_p zu einem Element von $\mathrm{End}(E[\ell])$.

Möchte man die Anzahl $\#E(\mathbb{F}_p)$ bestimmen, so erhält man zunächst die triviale obere Schranke $\#E(\mathbb{F}_p) \leqslant 2p + 1$: Für einen Punkt $P = (X, Y) \in E(\mathbb{F}_p)$ existieren a priori p Möglichkeiten für X sowie für jeden dieser Werte zwei Möglichkeiten für Y. Dazu kommt noch der Punkt $\mathcal{O}$.

Unter Verwendung von Eigenschaften des Frobenius-Homomorphismus erhält man jedoch eine sehr viel bessere Abschätzung. Wesentlich für deren Beweis ist die folgende einfache Beobachtung: Die Punkte, die vom Frobenius-Homomorphismus fixiert werden, sind genau diejenigen, die in $E(\mathbb{F}_p)$ liegen, was direkt aus der Definition folgt. Damit ergibt sich der folgende Satz, der 1934 von Hasse gezeigt wurde.

Satz 1.1.9. *[Sil09, S. 138] Sei E eine elliptische Kurve über $\mathbb{F}_p$. Dann gilt*

$$p + 1 - 2\sqrt{p} \leqslant \#E(\mathbb{F}_p) \leqslant p + 1 + 2\sqrt{p}.$$

Somit erhält man $\#E(\mathbb{F}_p) = p + 1 - t$ mit $t \in \mathbb{Z}$ und $|t| \leqslant 2\sqrt{p}$.

Der folgende Satz nutzt weitere Eigenschaften des Frobenius-Homomorphismus und liefert eine explizite Bedingung an t und damit $\#E(\mathbb{F}_p)$.

Satz 1.1.10. *[Sil09, S. 142] Der Frobenius-Homomorphismus erfüllt im Endomorphismenring von E die quadratische Gleichung*

$$\chi(\phi_p) := \phi_p^2 - t\phi_p + p = 0.$$

1.2 Der Algorithmus von Schoof

Der Algorithmus von Schoof, der im Jahr 1985 in [Sch85] veröffentlicht wurde, berechnet die Anzahl der Punkte auf einer gegebenen Kurve E über $\mathbb{F}_p$. Er weist im Gegensatz zu den zuvor verwendeten Algorithmen eine polynomielle Laufzeit in $\log p$ auf. Für die Berechnung bedient er sich der in den Sätzen 1.1.9 und 1.1.10 genannten Eigenschaften des Frobenius-Homomorphismus. Wir geben nur eine grobe Übersicht über die zugrundeliegenden Ideen, Details finden sich in [Sch95] sowie [Mül95, Mor95, BSS99, Was08].

1.2.1 Ursprünglicher Algorithmus

Die Idee des Algorithmus von Schoof besteht darin, die Spur $\bar{t} = t \bmod \ell$ des Frobenius-Homomorphismus mithilfe von Satz 1.1.10 für kleine Primzahlen ℓ zu berechnen, sodass für deren Produkt

$$\prod_{\ell} \ell > 4\sqrt{p}$$

erfüllt ist und somit wegen der Hasse-Schranke $|t| \leqslant 2\sqrt{p}$ aus diesen Informationen der Wert von t mithilfe des Chinesischen Restsatzes eindeutig bestimmt werden kann, woraus sich mit Satz 1.1.9 direkt $\#E(\mathbb{F}_p)$ ergibt. Bekanntlich reicht es aus, den Wert von t modulo Primzahlen ℓ in der Größenordnung $O(\log p)$ zu bestimmen, was direkt aus dem Primzahlsatz folgt.

Zur Bestimmung des Wertes modulo einer Primzahl ℓ werden im Algorithmus von Schoof die sogenannten *Divisionspolynome* ψ_ℓ verwendet. Diese bilden eine rekursiv definierte Folge von Polynomen mit den Eigenschaften, dass Vielfache eines Punktes P auf E sich als rationaler Ausdruck in bestimmten Divisionspolynomen und den Koordinaten von P darstellen lassen und dass für einen Punkt $P = (X, Y) \in E$ und ℓ ungerade

$$(X, Y) \in E[\ell] \Leftrightarrow \psi_\ell(X) = 0 \tag{1.5}$$

gilt und $\deg(\psi_\ell) = \frac{\ell^2-1}{2}$ ist [Was08, S. 80–86, 123–127]. Mit ihrer Hilfe wird nun für einen Punkt $P = (X, Y) \in E[\ell], P \neq \mathcal{O}$, überprüft, für welchen Wert von $t \mod \ell$ die Gleichung

$$\phi_p^2(P) + \bar{p}P = t\phi_p(P) \tag{1.6}$$

erfüllt ist, wobei $\bar{p} = p \mod \ell$ gilt.

Der Algorithmus von Schoof weist unter Verwendung von schneller Arithmetik eine Laufzeit von $\tilde{O}(\log^5 p)$ Bitoperationen auf [BSS99, S. 111]. Der die Laufzeit dominierende Schritt ist dabei die Auswertung des Frobenius-Homomorphismus zur Berechnung von (X^p, Y^p) und (X^{p^2}, Y^{p^2}) in der Erweiterung $\mathbf{F} := \mathbb{F}_p[X,Y]/(\psi_\ell(X), Y^2 - X^3 - aX - b)$. Zur Verbesserung der Laufzeit des Algorithmus von Schoof ist es daher wünschenswert, die Auswertung des Frobenius-Homomorphismus in kleinere Erweiterungen von $\mathbb{F}_p$ zu verlagern.

1.2.2 Der SEA-Algorithmus

Eine solche Verbesserung ist als Algorithmus von Schoof, Elkies und Atkin, abgekürzt als SEA-Algorithmus, bekannt und wurde 1995 veröffentlicht [Sil09, S. 375].

Dafür untersucht man die Wirkung des Frobenius-Homomorphismus auf den Vektorraum $E[\ell] = \mathbb{F}_\ell^2$ (s. Gleichung (1.3)). Wie im letzten Abschnitt ausgeführt, wird der Wert von $t \mod \ell$ mithilfe der Gleichung

$$0 = \chi_\ell(\phi_p) := \phi_p^2 - t\phi_p + p \mod \ell \tag{1.7}$$

ermittelt. Die Diskriminante dieser quadratischen Gleichung ist $\Delta = t^2 - 4p$, mittels deren wir die drei Fälle $\Delta \equiv 0 \mod \ell$, $\left(\frac{\Delta}{\ell}\right) = 1$ sowie $\left(\frac{\Delta}{\ell}\right) = -1$ unterscheiden. Im ersten Fall besitzt die Gleichung eine doppelte Nullstelle, daher gilt

$$t \equiv \pm 2\sqrt{p} \mod \ell,$$

somit kann der Wert $t \mod \ell$ direkt bis auf sein Vorzeichen bestimmt werden. Offenbar ist dies ein Spezialfall für endlich viele Primzahlen ℓ. Im zweiten Fall wird ℓ als *Elkies-Primzahl*, im dritten als *Atkin-Primzahl* bezeichnet.

Im Elkies-Fall $\left(\frac{\Delta}{\ell}\right) = 1$ besitzt ϕ_p zwei verschiedene Eigenwerte $\lambda, \mu \in \mathbb{F}_\ell^*$. Die charakteristische Gleichung zerfällt somit in die Linearfaktoren $\chi_\ell(\phi_p) = (\phi_p - \lambda)(\phi_p - \mu)$ und es gilt

$$t \equiv \lambda + \mu \equiv \lambda + p\lambda^{-1} \mod \ell. \tag{1.8}$$

Mittels zweier Sätze von Atkin (vgl. hierfür [Sch95, S. 236–239]), die mithilfe von Satz 1.1.6 einen Zusammenhang zwischen dem Wert von $\left(\frac{\Delta}{\ell}\right)$ und dem Zerfällungstyp des sogenannten *ℓ-ten Modularpolynoms* Φ_ℓ (s. auch Abschnitt 2.1.3 hinter Korollar 2.1.20) im Ring $\mathbb{F}_p[X]$ herstellen, kann leicht ermittelt werden, ob eine gegebene Primzahl vom Elkies- oder vom Atkin-Typ ist. Grundlage dieser Aussagen bildet die Tatsache, dass für eine elliptische Kurve $E/\mathbb{F}_p$ die Nullstellen des Modularpolynoms $\Phi_\ell(X, j(E))$ genau die j-Invarianten der elliptischen Kurven E' sind, für die eine ℓ-Isogenie $\psi : E \to E'$ existiert. Wegen $|\ker(\psi)| = \ell$ nach Satz 1.1.6 ist $\ker(\psi)$ offenbar eine Untergruppe $\mathcal{C}$ von $E[\ell]$, deren Verhalten unter Anwendung von ϕ_p mit dem Wert von $\left(\frac{\Delta}{\ell}\right)$ in Verbindung steht. Genauer gelten die folgenden Äquivalenzen, die eine Unterscheidung zwischen den drei genannten Fällen durch Berechnung von $\mathrm{ggT}(X^p - X, \Phi_\ell(X, j(E)))$ ermöglichen.

1. $\ell \mid \Delta \Leftrightarrow \Phi_\ell(X, j(E))$ hat genau eine oder mehr als zwei Nullstellen in $\mathbb{F}_p$.

2. ℓ ist Elkies-Primzahl $\Leftrightarrow \Phi_\ell(X, j(E))$ hat genau zwei Nullstellen in $\mathbb{F}_p$.

3. ℓ ist Atkin-Primzahl $\Leftrightarrow \Phi_\ell(X, j(E))$ hat keine Nullstelle in $\mathbb{F}_p$.

In [Mül95] wurden sogenannte äquivalente Polynome untersucht, die statt des Modularpolynoms verwendet werden können und aus Laufzeitgründen in der Praxis zu bevorzugen sind. Auch auf diese werden wir später in Abschnitt 2.1.3 genauer eingehen.

Im Elkies-Fall ist nun der Wert $\lambda \in \{1, \ldots, \ell - 1\}$ zu bestimmen, für den

$$\phi_p(P) = \lambda P$$

für einen Punkt P in einer bestimmten Untergruppe von $E[\ell]$ gilt. Bei der Auswertung dieser Gleichung kann statt des ℓ-ten Divisionspolynoms ψ_ℓ, das bei der Konstruktion der Erweiterung $\mathbf{F}$ verwendet wird, ein Teiler $F_{\ell,\lambda}$ von ψ_ℓ genutzt werden, der lediglich von Grad $\frac{\ell-1}{2}$ gegenüber $\frac{\ell^2-1}{2}$ ist. Damit kann die Laufzeit für die Bestimmung von t modulo ℓ für festes $\ell \in O(\log p)$ von $\tilde{O}(\log^4 p)$ auf $\tilde{O}(\log^3 p)$ Bitoperationen reduziert werden. Im Rahmen des üblichen Vorgehens, bei dem die Werte des ℓ-ten Modularpolynoms $\Phi_\ell(X, Y)$ bzw. des verwendeten äquivalenten Polynoms allgemein vorberechnet sind (vgl. [Mor95, Eng09]), stellt dies weiter den die Laufzeit dominierenden Schritt dar.

Für Atkin-Primzahlen wurde von Atkin ein Verfahren von gleicher Laufzeit vorgeschlagen, dessen Nachteil jedoch darin besteht, dass es nicht den exakten Wert von t modulo ℓ zu bestimmen vermag, sondern lediglich eine Menge an Kandidaten, die anschließend mithilfe einer nicht-trivialen Baby-Step-Giant-Step-Methode (s. [Mül95, S. 144–148]) überprüft werden müssen, was insgesamt zu einer exponentiellen Laufzeit führt.

Im Schoof-Elkies-Atkin-Algorithmus werden die beiden Ansätze kombiniert. Neben den Elkies-Primzahlen werden dabei auch einige Atkin-Primzahlen verwendet, für die die Kandidatenmenge relativ klein ist. In [SS14] wird gezeigt, dass für fast alle Primzahlen p ausreichend viele kleine Elkies-Primzahlen existieren, sodass der SEA-Algorithmus eine erwartete Laufzeit von $\tilde{O}(\log^4 p)$ gegenüber $\tilde{O}(\log^5 p)$ Bitoperationen für den ursprünglichen Algorithmus von Schoof aufweist.

1.2.3 Weitere Verbesserungen

In zahlreichen Forschungsarbeiten wurden weitere Verbesserungen des Vorgehens im Elkies-Fall vorgeschlagen. So ermöglichen die in [Eng09] vorgestellten Ansätze wie diejenigen in [BLS12] und insbesondere [Sut13], die Ideen aus [FM02, BMSS08] weiterentwickeln, eine Beschleunigung der mit dem Modularpolynom Φ_ℓ verbundenen Rechnungen. Weiterhin erlauben die Algorithmen aus [MM01, GM06] eine schnellere Bestimmung des Eigenwertes λ, [MSS16] ersetzt den Frobenius-Homomorphismus ϕ_p auf bestimmten Kurven durch einen anderen Homomorphismus, der in diesem Fall effizienter ausgewertet werden kann, berechnet dessen Spur und rekonstruiert daraus die Spur t von ϕ_p.

In [MMS07] wurde eine größere Modifikation des Vorgehens im Elkies-Fall eingeführt. Mithilfe des dort vorgestellten Algorithmus reicht es aus, den Frobenius-Homomorphismus in

Erweiterungen von $\mathbb{F}_p$ von Grad n, wobei n die maximalen Primpotenzteiler von $\ell - 1$ durchläuft, auszuwerten. Dabei werden sogenannte *elliptische Gaußsche Perioden* verwendet, um den Index des Eigenwerts λ in der Gruppe $(\mathbb{Z}/\ell\mathbb{Z})^*$ zunächst modulo den verschiedenen Primpotenzteilern von $\ell - 1$ zu bestimmen, bevor der Chinesische Restsatz angewendet wird.

Weiterhin wurde in [Mih06c] und [MV10] eine Variante dieses neuen Ansatzes vorgestellt, bei der sogenannte *elliptische Gauß-Summen* Verwendung finden. Sie sind für einen Charakter $\chi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mu_n = \langle \zeta_n \rangle$ von Ordnung n mit $n \mid \ell - 1$ in Analogie zu den klassischen zyklotomischen Gauß-Summen definiert als

$$G_{\ell,n,\chi}(E) = \sum_{a=1}^{\ell-1} \chi(a)(aP)_V \tag{1.9}$$

für einen ℓ-Torsionspunkt P auf E, wobei $V = y$ für gerades sowie $V = x$ für ungerades n gilt. Wie in [Mih06c] gezeigt wird, gilt nun

$$G_{\ell,n,\chi}(E)^n, \frac{G_{\ell,n,\chi}(E)^m}{G_{\ell,n,\chi^m}(E)} \in \mathbb{F}_p[\zeta_n] \quad \text{für} \quad m < n. \tag{1.10}$$

Außerdem lässt sich der Index von λ modulo n direkt mithilfe der Gleichung

$$G_{\ell,n,\chi}(E)^p = \chi^{-p}(\lambda) G_{\ell,n,\chi^p}(E) \quad \Rightarrow \quad \frac{G_{\ell,n,\chi}(E)^m}{G_{\ell,n,\chi^m}(E)} (G_{\ell,n,\chi}(E)^n)^q = \chi^{-m}(\lambda) \tag{1.11}$$

für $p = nq+m$ mit $0 \leqslant m < n$ bestimmen. Sind die verschiedenen Größen aus Gleichung (1.10) berechnet, so sind damit zur Ermittlung des Index von λ modulo n nur noch Rechnungen in der Erweiterung $\mathbb{F}_p[\zeta_n]$ von Grad $\varphi(n)$ nötig. Wir befassen uns in den folgenden Abschnitten damit, wie diese Größen mittels sogenannter *universeller elliptischer Gauß-Summen*, die wir schließlich in Gleichung (2.19) definieren werden, bestimmt werden können, statt sie direkt anhand der Definition (1.9) zu berechnen.

Wir bemerken noch, dass die elliptischen Gauß-Summen und Gleichung (1.11) ebenfalls eine wichtige Rolle in dem in [Mih06a, Mih06b] vorgeschlagenen Primzahltest CIDE (Cyclotomy Initialized by Dual Elliptic tests) spielen, der in [FKDG12] weiter ausgearbeitet wurde. Auch wenn diese Anwendung nicht Gegenstand dieser Arbeit ist und wir daher nicht näher auf sie eingehen werden, möchten wir gleichwohl anmerken, dass die in den folgenden Abschnitten hergeleiteten algorithmischen Resultate zur Berechnung der universellen elliptischen Gauß-Summen gemäß [Fra16] die Laufzeit dieses Algorithmus zu reduzieren vermögen.

2 Universelle elliptische Gauß-Summen

Bei der Beschäftigung mit den universellen elliptischen Gauß-Summen bedienen wir uns ausführlich der Theorie der Modulfunktionen für Untergruppen von $\mathrm{SL}_2(\mathbb{Z})$, die wir daher im Folgenden in dem Maße einführen, in dem wir sie benötigen. Wir folgen dabei insbesondere [Kob93], [Apo76] und [Shi71].

2.1 Modulfunktionen

2.1.1 Definition

Wir beginnen mit der Definition der oberen Halbebene $\mathbb{H} \subseteq \mathbb{C}$. Diese ist gegeben als

$$\mathbb{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}.$$

Elemente $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma := \mathrm{SL}_2(\mathbb{Z})$ wirken als Möbius-Transformationen mittels

$$\gamma : \mathbb{H} \to \mathbb{H}, \quad \tau \mapsto \frac{a\tau + b}{c\tau + d}$$

auf Elemente von $\mathbb{H}$. Sei $N \in \mathbb{N}$. Γ besitzt unter anderem die Untergruppen

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N \right\} \text{ und}$$
$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1 \mod N, b \equiv c \equiv 0 \mod N \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\},$$

die wir im Folgenden verwenden werden.

Definition 2.1.1. [Kob93, S. 108] Seien $f(\tau)$ eine auf der oberen Halbebene $\mathbb{H}$ meromorphe Funktion und $k \in \mathbb{Z}$. Weiterhin erfülle $f(\tau)$ die folgenden Bedingungen:

1. $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ für alle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

   Insbesondere gilt dann

   $$f(\tau + 1) = f\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau\right) = f(\tau)$$

   für alle $\tau \in \mathbb{H}$. Daher lässt sich $f(\tau)$ als Laurentreihe in

   $$q = q(\tau) = e^{2\pi i \tau}$$

   schreiben. Dies führt uns auf Bedingung

2. In der Fourierreihe

   $$f(\tau) = \sum_{n \in \mathbb{Z}} a_n q^n$$

   gilt $a_n = 0$ für $n < n_0$, $n_0 \in \mathbb{Z}$; in ihr treten also nur endlich viele Potenzen von q mit negativem Exponenten auf. Man sagt in diesem Fall auch, dass f meromorph bei Unendlich ist.

Dann nennt man $f(\tau)$ eine *Modulfunktion von Gewicht k für* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Für die Menge aller solchen Modulfunktionen schreiben wir $\mathbf{A}_k(\Gamma)$.
Ist $f(\tau)$ sogar holomorph auf $\mathbb{H}$ und bei Unendlich (d. h., gilt in der zweiten Bedingung $n_0 = 0$), dann nennt man $f(\tau)$ eine *Modulform von Gewicht k für* Γ.
Gilt zusätzlich $a_0 = 0$, verschwindet die Modulform also bei Unendlich, so nennt man sie eine *Spitzenform von Gewicht k für* Γ.

Bevor wir diese Definition auf Untergruppen von Γ verallgemeinern, wollen wir zunächst einige Bemerkungen anbringen und Beispiele angeben, die wir später noch vielfach verwenden werden.

Bemerkung 2.1.2.

1. Für ungerade k gibt es keine nicht-trivialen Modulfunktionen von Gewicht k für Γ. Dies folgt sofort durch Betrachten der Wirkung von $\gamma = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

2. Die Bedingungen aus Definition 2.1.1 bleiben unter Addition und skalarer Multiplikation erhalten, sodass die Menge der Modulfunktionen, Modulformen und Spitzenformen von festem Gewicht einen Vektorraum bilden.
   Weiterhin ist das Produkt zweier Modulfunktionen (bzw. -formen) von Gewicht k_1 und k_2 eine Modulfunktion (bzw. -form) von Gewicht $k_1 + k_2$; der Quotient einer Modulfunktion von Gewicht k_1 und einer nicht-trivialen Modulfunktion von Gewicht k_2 ist eine Modulfunktion von Gewicht $k_1 - k_2$. Insbesondere ist damit $\mathbf{A}_0(\Gamma)$, die Menge der Modulfunktionen von Gewicht 0, ein Körper.

Beispiel 2.1.3.

1. Eine wichtige Familie von Modulformen von Gewicht $2k$ für $k > 1$ ist gegeben durch die Eisensteinreihen $E_{2k}(\tau)$, die definiert sind als

$$E_{2k}(\tau) = \frac{1}{2\zeta(2k)} {\sum_{m,n\in\mathbb{Z}}}' \frac{1}{(m\tau + n)^{2k}}.$$

   Sei $\sigma_k(n) = \sum_{d|n} d^k$. Gemäß [Kob93, S. 111] ist die q-Entwicklung von E_{2k} gegeben durch

$$E_{2k}(\tau) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \frac{n^{2k-1} q^n}{1 - q^n},$$

   wobei B_k die k-te Bernoulli-Zahl, definiert durch

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!},$$

   bezeichnet. Im Folgenden werden wir die Reihen $E_4(\tau)$ sowie $E_6(\tau)$ benötigen, deren q-Entwicklungen

$$E_4(\tau) = E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}, \tag{2.1}$$

$$E_6(\tau) = E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n} \tag{2.2}$$

lauten.

2. Aus diesen beiden Modulfunktionen konstruieren wir zwei weitere, die eine wichtige Rolle in der Theorie der elliptischen Kurven spielen. Zunächst definieren wir die Diskriminante der zum Gitter $\langle 1, \tau \rangle_{\mathbb{Z}}$ zugehörigen elliptischen Kurve E_τ (vgl. Satz 2.2.3) als
$$\Delta(\tau) = \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728}. \tag{2.3}$$
Aus den q-Entwicklungen der beiden Eisensteinreihen folgt sofort, dass in dieser Reihe der konstante Term verschwindet, weshalb $\Delta(\tau)$ eine Spitzenform von Gewicht 12 für Γ ist. Des Weiteren ist $\Delta(\tau) \neq 0$ auf $\mathbb{H}$ [Kob93, S. 118].
Weiterhin setzen wir die j-Invariante von E_τ als
$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)}. \tag{2.4}$$
Dies ist offenbar eine Modulfunktion von Gewicht 0. Die Funktion $j(\tau) : \mathbb{H} \to \mathbb{C}$ ist zudem surjektiv [Cox89, S. 121].

3. Die Dedekindsche η-Funktion besitzt die q-Entwicklung
$$\eta(\tau) = \eta(q) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n).$$
Für $\tau \in \mathbb{H}$ konvergiert das Produkt absolut und ist ungleich Null. Wie schon Weber in [Web08, S. 112] zeigte, lässt sich die q-Entwicklung von η umformen zu
$$\eta(q) = q^{\frac{1}{24}} \left(1 + \sum_{n=1}^{\infty} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right). \tag{2.5}$$
Mit den obigen Definitionen gilt gemäß [Apo76, S. 51]
$$\eta(q)^{24} = \Delta(q).$$
Dies liefert eine weitere Möglichkeit zur Berechnung der q-Entwicklung von $\Delta(q)$.

Bemerkung 2.1.4. Wir weichen bei der Normierung der Funktion $\Delta(\tau)$ von derjenigen in [Apo76] und [Kob93] ab und verwenden stattdessen diejenige, die in [Sch95] und [BSS99] benutzt wird. Dies ist dem Umstand geschuldet, dass diese Normierung für die Berechnung der universellen elliptischen Gauß-Summen, die wir später ausführen wollen, günstiger ist.

Die folgende Aussage zeigt die fundamentale Bedeutung der j-Invarianten $j(\tau)$ in der Theorie der Modulfunktionen.

Satz 2.1.5. *[Cox89, S. 226]*

1. *Es gilt*
$$\mathbf{A}_0(\Gamma) = \mathbb{C}(j(\tau)),$$
die Modulfunktionen von Gewicht 0 *sind also genau die rationalen Funktionen in* j*.*

2. Bezeichnen wir mit $\mathbf{H}_0(\Gamma)$ *die Teilmenge der holomorphen Funktionen, dann gilt*

$$\mathbf{H}_0(\Gamma) = \mathbb{C}[j(\tau)],$$

diese Funktionen können also sogar als Polynome in j *dargestellt werden.*

2.1.2 Untergruppen

Wir übertragen nun Definition 2.1.1 auf Untergruppen von Γ.

Definition 2.1.6. [Kob93, S. 125] Seien $f(\tau)$ eine auf der oberen Halbebene $\mathbb{H}$ meromorphe Funktion und $k \in \mathbb{Z}$ sowie $\Gamma' \leqslant \Gamma$, sodass $\Gamma' \supseteq \Gamma(N)$ für ein $N \in \mathbb{N}$ gilt. Des Weiteren erfülle $f(\tau)$ folgende Bedingungen:

1. $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ für alle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$. Wegen $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma(N)$ gilt dann
$$f(\tau + N) = f(\tau)$$
und $f(\tau)$ lässt sich als Laurentreihe in
$$q_N = q^{\frac{1}{N}} = e^{\frac{2\pi i \tau}{N}}$$
schreiben.

2. In der Fourierreihe
$$f(\gamma\tau) = \sum_{n \in \mathbb{Z}} a_n q_N^n$$
gilt $a_n = 0$ für $n < n_0$, $n_0 \in \mathbb{Z}$, für alle $\gamma \in \Gamma$. Man sagt auch, dass $f(\tau)$ meromorph an den Spitzen ist.

Dann nennt man $f(\tau)$ eine *Modulfunktion von Gewicht* k *für* Γ'. Für die Menge aller solchen Modulfunktionen schreiben wir $\mathbf{A}_k(\Gamma')$.
Ist $f(\tau)$ holomorph auf $\mathbb{H}$ und kann man $n_0 = 0$ für alle $\gamma \in \Gamma$ wählen, so nennt man $f(\tau)$ entsprechend eine *Modulform von Gewicht* k *für* Γ'.
Gilt zusätzlich $a_0 = 0$ für alle $\gamma \in \Gamma$, so bezeichnet man die Funktion als *Spitzenform von Gewicht* k *für* Γ'.

Bemerkung 2.1.7. [Kob93, S. 126] Es reicht, die zweite Bedingung für ein Repräsentantensystem $\{\gamma_1, \ldots, \gamma_r\}$ von Γ/Γ' (also $\Gamma = \bigcup_{i=1}^r \Gamma'\gamma_i$) zu prüfen.

Definition 2.1.8. [Iwa97, S. 112] Sei $f(q) = f(\tau)$ eine Modulfunktion für $\Gamma' \subseteq \Gamma$. Dann definieren wir die Fricke-Atkin-Lehner-Involution durch

$$w_\ell : f(\tau) \mapsto f\left(\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}\tau\right) = f\left(-\frac{1}{\ell\tau}\right) =: f^*(\tau).$$

Bemerkung 2.1.9. Für $f(\tau) \in \mathbf{A}_0(\Gamma)$ ergibt sich

$$f^*(\tau) = f\left(-\frac{1}{\ell\tau}\right) = f\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\ell\tau\right) = f(\ell\tau).$$

Für unsere Rechnungen werden wir Modulfunktionen für die Untergruppe $\Gamma_0(N)$ verwenden, weiterhin wird dabei $N = \ell$ eine Primzahl sein. Wir geben erneut als Beispiele diejenigen Funktionen an, deren wir uns später noch bedienen werden.

Beispiel 2.1.10.

1. Eine geringfügige Modifikation (vgl. [Kob93, S. 112]) der Definition für die Eisensteinreihen für $k > 2$ in Beispiel 2.1.3 liefert die Eisensteinreihe

$$E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n = 1 - 24 \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}. \tag{2.6}$$

   Die so definierte Reihe ist keine Modulfunktion für Γ, denn es gilt beispielsweise

$$E_2\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tau\right) = E_2\left(\frac{-1}{\tau}\right) = \tau^2 E_2(\tau) + \frac{12\tau}{2\pi i}.$$

   Jedoch ist durch

$$p_1(q) = \frac{1}{12} \ell (E_2(q) - \ell E_2(q^\ell)) \tag{2.7}$$

   eine Modulfunktion von Gewicht 2 für $\Gamma_0(\ell)$ gegeben, wie wir später in Korollar 2.2.9 zeigen werden.

2. $j(\ell\tau)$ ist eine Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$. Dies folgt aus

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b\ell \\ c/\ell & d \end{pmatrix} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \quad \text{für beliebige} \quad a, b, c, d \in \mathbb{Z},$$

   wie man leicht nachrechnet. Wählt man nun $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\ell)$, so gilt $c \equiv 0 \mod \ell$ und es folgt $\tilde{\gamma} = \left(\begin{smallmatrix} a & b\ell \\ c/\ell & d \end{smallmatrix}\right) \in \Gamma$. Damit gilt

$$j(\ell\gamma\tau) = j(\tilde{\gamma}\ell\tau) = j(\ell\tau),$$

   weil $j(\tau)$ unter Γ invariant ist. Weiterhin kann man nachrechnen, dass $j(\ell\tau)$ meromorph an den Spitzen ist [Cox89, S. 229].
   Für Modulformen (Spitzenformen) $A(\tau)$ für Γ gilt allgemeiner, dass $A(\ell\tau)$ eine Modulform (Spitzenform) für $\Gamma_0(\ell)$ ist.

3. Die in [Mül95] ausführlich untersuchte Funktion

$$m_\ell(q) = \ell^s \left(\frac{\eta(q^\ell)}{\eta(q)}\right)^{2s} \quad \text{mit} \quad s = \frac{12}{\mathrm{ggT}(12, \ell - 1)} \tag{2.8}$$

   ist eine Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$. Dies wird in [Mül95, S. 59] direkt durch Nachrechnen für diesen Spezialfall gezeigt, folgt jedoch ebenfalls aus den weitaus allgemeineren Resultaten [Rad42, S. 619] und [New57, S. 336] über sogenannte Eta-Quotienten.

2.1.3 Aussagen über Modulfunktionen von Gewicht 0

Wir wollen nun folgenden Satz beweisen, der sich als essentiell für die späteren Rechnungen herausstellen wird:

Satz 2.1.11. *Sei $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))\backslash\mathbf{A}_0(\Gamma)$ eine Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$, aber nicht für Γ. Dann gilt*

$$\mathbf{A}_0(\Gamma_0(\ell)) = \mathbf{A}_0(\Gamma)(f(\tau)) = \mathbb{C}(f(\tau), j(\tau)),$$

insbesondere existieren für beliebiges $g(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))$ also Polynome $P_1, P_2 \in \mathbb{C}[X, Y]$ mit

$$g(\tau) = \frac{P_1(f(\tau), j(\tau))}{P_2(f(\tau), j(\tau))}.$$

Für den Beweis werden wir in mehreren Schritten vorgehen. Zunächst zeigen wir folgenden

Satz 2.1.12. *Sei $\Gamma' \trianglelefteq \Gamma$ ein Normalteiler von endlichem Index in $\mathrm{SL}_2(\mathbb{Z})$. Dann ist die Körpererweiterung $\mathbf{A}_0(\Gamma')/\mathbf{A}_0(\Gamma)$ eine Galoiserweiterung mit*

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma')/\mathbf{A}_0(\Gamma)) \leqslant \Gamma/\Gamma'.$$

Beweis. Sei $f(\tau) \in \mathbf{A}_0(\Gamma')$, dann gilt $f(\gamma\tau) \in \mathbf{A}_0(\Gamma')$ für alle $\gamma \in \Gamma$: Da Γ' ein Normalteiler in Γ ist, gilt nämlich für $\delta \in \Gamma'$ die Gleichung $\gamma\delta\gamma^{-1} = \tilde{\delta} \in \Gamma'$. Wir folgern

$$f(\gamma\delta\tau) = f(\tilde{\delta}\gamma\tau) = f(\gamma\tau) \quad \text{für alle} \quad \delta \in \Gamma',$$

zudem ist $f(\gamma\tau)$ meromorph an den Spitzen, da dies für $f(\tau)$ gilt. Ersetzt man γ durch γ^{-1}, so sieht man, dass durch

$$\gamma^* : \mathbf{A}_0(\Gamma') \to \mathbf{A}_0(\Gamma'), \quad f \mapsto f \circ \gamma$$

eine Bijektion gegeben ist. Wegen der Invarianz der Elemente von $\mathbf{A}_0(\Gamma')$ unter $\pm\Gamma'$ (man beachte, dass die von $-I$ induzierte Möbius-Transformation die Identität ist) und von $\mathbf{A}_0(\Gamma)$ unter Γ folgt, dass die endliche Gruppe $\Gamma/(\pm\Gamma')$ als Automorphismengruppe auf $\mathbf{A}_0(\Gamma')$ wirkt und $\mathbf{A}_0(\Gamma)$ fixiert. Aus der Galois-Theorie ergibt sich nun die Behauptung. □

Als Spezialfall ergibt sich

Lemma 2.1.13. *[Shi71, S. 134] Für $N \in \mathbb{N}$ ist $\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma)$ eine Galoiserweiterung und es gilt*

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma)) \cong \Gamma/(\pm\Gamma(N)).$$

Wir bemerken noch, dass aufgrund der Identität $\Gamma(N) = \ker\{\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\mod N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\}$ offenbar $\Gamma/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ und somit

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

gilt.

Korollar 2.1.14. *Sei Γ' eine Untergruppe von Γ mit $\Gamma(N) \leqslant \Gamma'$, dann gilt*

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma')) \cong (\pm\Gamma')/(\pm\Gamma(N)).$$

Insbesondere ist $\mathbf{A}_0(\Gamma')$ *eine endliche Erweiterung von* $\mathbf{A}_0(\Gamma) = \mathbb{C}(j)$ *von Grad* $[\Gamma : \pm\Gamma']$.

Beweis. Weil $\Gamma(N)$ der Kern der Reduktionsabbildung modulo N ist, gilt $\Gamma(N) \trianglelefteq \Gamma'$. Nun ergibt sich $(\pm\Gamma')/(\pm\Gamma(N)) \leqslant \Gamma/(\pm\Gamma(N)) = \mathrm{Gal}(\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma))$. Da weiterhin

$$\mathbf{A}_0(\Gamma(N))^{\Gamma'} = \{f \in \mathbf{A}_0(\Gamma(N)) : f \circ \gamma = f \ \forall \gamma \in \Gamma'\} = \mathbf{A}_0(\Gamma')$$

gilt, folgt die Aussage über die Galoisgruppe aus der Galois-Theorie. Damit ergibt sich $[\mathbf{A}_0(\Gamma(N)) : \mathbf{A}_0(\Gamma')] = [\pm\Gamma' : \pm\Gamma(N)]$ und $[\mathbf{A}_0(\Gamma') : \mathbf{A}_0(\Gamma)] = [\Gamma : \pm\Gamma']$. □

Für $\Gamma' = \Gamma_0(N)$ erhält man nun

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma(N))/\mathbf{A}_0(\Gamma_0(N))) \cong (\pm\Gamma_0(N))/(\pm\Gamma(N)) \cong \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\} /\{\pm 1\}.$$

Bevor wir Satz 2.1.11 beweisen, benötigen wir noch das folgende

Lemma 2.1.15. *Sei* K *ein Körper,* $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in K^*, b \in K \right\} \subseteq G = \mathrm{SL}_2(K)$. *Dann ist durch*

$$\begin{aligned} G/B &\to \mathbb{P}^1(K), \\ g \cdot B &\mapsto g \cdot \infty = g \cdot [1,0] \text{ mit } g \cdot [v] \mapsto [gv], \\ \text{d. h., } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot B &\mapsto [a, c] \end{aligned}$$

eine Bijektion gegeben und es gibt keine Zwischengruppen zwischen G *und* B.

Beweis. Die erste Aussage ist trivial, da die Wirkung von G auf $\mathbb{P}^1(K)$ transitiv und B der Stabilisator von ∞ ist. Wegen

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} [0,1] \mapsto [b,1]$$

wirkt B auf $\mathbb{P}^1(K)\backslash\{\infty\}$ transitiv.

Seien nun $g, h \in G\backslash B$. Dann sind $h\cdot\infty$ und $g\cdot\infty$ in $\mathbb{P}^1(K)\backslash\{\infty\}$ enthalten, da B der Stabilisator von ∞ ist. Aus diesem Grund existiert ein $b \in B$ mit

$$h \cdot \infty = b \cdot g \cdot \infty,$$

also gilt $h^{-1}bg \in B$ oder $h \in BgB$. Somit erzeugen B und g ganz G, weshalb zwischen B und G keine Zwischengruppen existieren können. □

Beweis von Satz 2.1.11. Sei ℓ eine Primzahl. Aus obigen Überlegungen wissen wir

$$G = \mathrm{Gal}(\mathbf{A}_0(\Gamma(\ell))/\mathbf{A}_0(\Gamma)) \cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm 1\}$$

sowie

$$B = \mathrm{Gal}(\mathbf{A}_0(\Gamma(\ell))/\mathbf{A}_0(\Gamma_0(\ell))) \cong \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \right\} /\{\pm 1\}.$$

Daher entsprechen die Zwischenkörper der Erweiterung $\mathbf{A}_0(\Gamma_0(\ell))/\mathbf{A}_0(\Gamma)$ nach Galois-Theorie genau den Zwischengruppen von G und B. Wendet man nun Lemma 2.1.15 mit $K = \mathbb{F}_\ell$ an und beachtet, dass $-1 \in B$ gilt, so folgt, dass keine Zwischengruppen zwischen G und B und damit keine Zwischenkörper zwischen $\mathbf{A}_0(\Gamma_0(\ell))$ und $\mathbf{A}_0(\Gamma)$ existieren, woraus sofort folgt, dass $\mathbf{A}_0(\Gamma_0(\ell)) = \mathbb{C}(f(\tau), j(\tau))$ für beliebiges $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))\backslash\mathbf{A}_0(\Gamma)$. □

Somit können Modulfunktionen von Gewicht 0 für $\Gamma_0(\ell)$, wie insbesondere die in Korollar 2.2.10 definierten universellen elliptischen Gauß-Summen, als rationaler Ausdruck in $j(\tau)$ und einer weiteren Modulfunktion $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))\backslash\mathbf{A}_0(\Gamma)$ dargestellt werden. Satz 2.1.11 liefert jedoch lediglich eine Existenzaussage. Um einen effizienten Algorithmus zur Bestimmung des rationalen Ausdrucks zu erhalten, sind noch weitere Resultate nötig. Weiterhin muss auch die Wahl der zweiten Funktion $f(\tau)$ diskutiert werden. Wir orientieren uns für die beiden folgenden Resultate stark an [Cox89, S. 228–231], verallgemeinern die dortigen Überlegungen jedoch leicht.

Lemma 2.1.16. *Sei $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))\backslash\mathbf{A}_0(\Gamma)$ holomorph auf $\mathbb{H}$. Dann existiert ein irreduzibles Polynom $Q_f(X, Y) \in \mathbb{C}[X, Y]$ mit*

$$Q_f(f(\tau), j(\tau)) = 0.$$

Beweis. Wir bemerken zunächst, dass durch $\{S_k, k = 0, \ldots, \ell\}$ mit

$$S_k = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \quad \text{für} \quad 0 \leqslant k < \ell, \quad S_\ell = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.9}$$

ein Repräsentantensystem für $\Gamma/\Gamma_0(\ell)$ gegeben ist, wie in [Mül95, S. 54] gezeigt wird. Nun betrachten wir das Polynom in X

$$Q_f(X, \tau) = \prod_{k=0}^{\ell} (X - f(S_k\tau))$$

und untersuchen seine Koeffizienten. Als elementar-symmetrische Polynome in $f(S_k\tau)$ sind sie offensichtlich holomorph auf $\mathbb{H}$. Sei $\gamma \in \Gamma$. Da die S_k ein Repräsentantensystem von $\Gamma/\Gamma_0(\ell)$ bilden, sind die Werte $f(S_k\gamma\tau)$, $k = 0, \ldots, \ell$, genau eine Permutation der Werte $f(S_k\tau)$. Somit sind die Koeffizienten von $Q_f(X, \tau)$ invariant unter $\mathrm{SL}_2(\mathbb{Z})$. Als Modulfunktion ist $f(\tau)$ meromorph an den Spitzen, aus dem Beweis von Satz 2.1.12 folgt, dass dies auch für $f(S_k\tau)$ gilt. Daher sind die Koeffizienten meromorph an den Spitzen und somit Funktionen in $\mathbf{H}_0(\Gamma)$. Nach Satz 2.1.5 sind sie daher Polynome in $j(\tau)$. Es existiert also ein Polynom $Q_f(X, Y) \in \mathbb{C}[X, Y]$ mit

$$Q_f(X, j(\tau)) = \prod_{k=0}^{\ell} (X - f(S_k\tau)),$$

das offenbar $f(\tau)$ als Nullstelle besitzt. Da es, wie wir gesehen haben, zwischen $\mathbf{A}_0(\Gamma_0(\ell))$ und $\mathbf{A}_0(\Gamma)$ keine Zwischenkörper gibt, muss $Q_f(X, j(\tau))$ irreduzibel sein. □

Die folgende Aussage, die man durch eine Verallgemeinerung der Überlegungen aus [Cox89, S. 230–231] zeigen kann, liefert schließlich einen ersten Ansatz für einen effizienten Algorithmus.

Satz 2.1.17. *Sei $g(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))$ eine Modulfunktion und $f(\tau) \in \mathbf{H}_0(\Gamma_0(\ell))\backslash\mathbf{H}_0(\Gamma)$. Dann hat man die Darstellung*

$$g(\tau) = \frac{Q(f(\tau), j(\tau))}{\frac{\partial Q_f}{\partial X}(f(\tau), j(\tau))},$$

wobei $Q(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$ ein Polynom in X ist, das in Abhängigkeit von

$$\{g(S_k\tau), f(S_k\tau), i = 0, \ldots, \ell\}$$

explizit angegeben werden kann.
Ist $g(\tau)$ holomorph, so gilt sogar $Q(X, j(\tau)) \in \mathbb{C}[j(\tau)][X]$, der Zähler des rationalen Ausdrucks in dieser Darstellung ist also ein Polynom in f und j.

Bemerkung 2.1.18. Der für uns relevante Fall, wenn die Funktion $g(\tau)$ holomorph ist, folgt auch direkt aus dem im folgenden angeführten Lemma 2.1.19 aus [Neu07, S. 206–208].

Die Darstellung aus Satz 2.1.17 ist unter algorithmischen Gesichtspunkten noch nicht optimal, da sie keine guten Schranken an die im Zähler auftretenden Potenzen der j-Invarianten $j(q) = q^{-1} + \sum_{k=0}^{\infty} c_k q^k$, deren Koeffizienten c_k gemäß [Pet32, BP05] exponentiell in $\sqrt{k}$ und somit sehr schnell wachsen, ermöglicht. Vielmehr stellen sich die folgenden Aussagen als nützlich heraus.

Lemma 2.1.19. *[Neu07, S. 206–208] Sei L/K eine Körpererweiterung, $\mathcal{O} \subseteq K$ ein Ring. Sei $\alpha \in L\backslash K$ mit Minimalpolynom $f(X) \in K[X]$ von Grad n. Dann besitzt der $\mathcal{O}$-Modul*

$$C_\alpha = \{x \in L \mid \mathrm{Tr}_{L/K}(x\mathcal{O}[\alpha]) \subseteq \mathcal{O}\}$$

die $\mathcal{O}$-Basis

$$\left\{\frac{\alpha^i}{f'(\alpha)}, i = 0, \ldots, n-1\right\}.$$

Korollar 2.1.20. *Sei $g(\tau) \in \mathbf{H}_0(\Gamma_0(\ell))\backslash\mathbf{H}_0(\Gamma)$ eine holomorphe Modulfunktion und es sei $f(\tau) \in \mathbf{H}_0(\Gamma_0(\ell))\backslash\mathbf{H}_0(\Gamma)$ mit Minimalpolynom $Q_f(X, j)$ mit $\deg_j(Q_f) = v$. Dann besitzt $g(\tau)$ eine Darstellung der Form*

$$g(\tau) = \frac{\sum_{i=0}^{v-1} a_i j(\tau)^i}{\frac{\partial Q_f}{\partial Y}(f(\tau), j(\tau))}$$

mit

$$a_i \in \{h(\tau) \in \mathbb{C}(f(\tau)) : h(\tau) \text{ holomorph}\}.$$

Beweis. Wir verwenden Lemma 2.1.19 für $K = \mathbb{C}(f(\tau))$, $L = K(j(\tau)) = \mathbf{A}_0(\Gamma_0(\ell))$ sowie $\alpha = j(\tau)$ und somit $f(X) = Q_f(f(\tau), X)$. Weiterhin wählen wir

$$\mathcal{O} = \{h(\tau) \in K : h(\tau) \text{ holomorph}\}.$$

Offensichtlich sind dann alle Elemente z von $\mathcal{O}[j]$ und somit $g(\tau)z$ sowie $\mathrm{Tr}_{L/K}(g(\tau)z)$ holomorph. Also gilt $g(\tau) \in C_j$. Mit Lemma 2.1.19 folgt die Behauptung. □

Wir betrachten nun spezielle Werte für $f(\tau)$.

1. Die nächstliegende und historisch zuerst verwendete Wahl ist $f(\tau) = j(\ell\tau)$. In diesem Fall schreiben wir $Q_f(X, Y) = \Phi_\ell(X, Y)$ und nennen Φ_ℓ das ℓ-te Modularpolynom.

Das Modularpolynom hat Koeffizienten in $\mathbb{Z}$ und ist symmetrisch in X und Y [Cox89, S. 229–234]. Das Problem bei seiner Verwendung besteht darin, dass seine Koeffizienten exponentiell in ℓ wachsen [Coh84].

2. In [Mül95] wurde die Wahl $f(\tau) = m_\ell(\tau)$, wobei $m_\ell(\tau)$ wie in Beispiel 2.1.10 ist, ausführlich untersucht und nutzbar gemacht. Aus der Konstruktion von $m_\ell(\tau)$ und der Beziehung zwischen $\eta(\tau)$ und $\Delta(\tau)$ folgt, dass auch $m_\ell(\tau)$ holomorph auf $\mathbb{H}$ ist. In diesem Fall schreiben wir $Q_f(X,Y) = M_\ell(X,Y)$. Das Polynom M_ℓ besitzt ebenfalls Koeffizienten in $\mathbb{Z}$ und der Grad in der zweiten Variablen ist gegeben durch $v = v(m_\ell) := \frac{\ell-1}{\mathrm{ggT}(\ell-1,12)}$, wie in [Mül95, S. 61–62] gezeigt wird. Dies führt dazu, dass seine Koeffizienten deutlich langsamer wachsen als diejenigen von Φ_ℓ.

3. Eine weitere in [Mül95] untersuchte Alternative ist $f(\tau) = a_\ell(\tau)$, wobei $a_\ell(\tau)$ später in Lemma 3.3.9 definiert wird. Die Funktion $a_\ell(\tau)$ ist ebenfalls holomorph. Hier schreiben wir $Q_f(X,Y) = A_\ell(X,Y)$. Auch dieses Polynom besitzt Koeffizienten in $\mathbb{Z}$ und sein Grad in der zweiten Variablen ist im Allgemeinen noch geringer als der von M_ℓ, was es asymptotisch zu der besten Alternative macht.

Durch diese Spezialisierung erhalten wir die folgende

Proposition 2.1.21. *Sei $g(\tau) \in \mathbf{H}_0(\Gamma_0(\ell))\backslash\mathbf{H}_0(\Gamma)$ eine holomorphe Modulfunktion. Dann besitzt $g(\tau)$ die folgenden Darstellungen:*

1.
$$g(\tau) = \frac{Q(m_\ell(\tau), j(\tau))}{m_\ell(\tau)^k \frac{\partial M_\ell}{\partial Y}(m_\ell(\tau), j(\tau))}$$
für ein $k \geqslant 0$ und ein Polynom $Q(X,Y) \in \mathbb{C}[X,Y]$ mit $\deg_Y(Q) < v = \deg_Y(M_\ell)$,

2.
$$g(\tau) = \frac{Q(a_\ell(\tau), j(\tau))}{\frac{\partial A_\ell}{\partial Y}(a_\ell(\tau), j(\tau))}$$
für ein Polynom $Q(X,Y) \in \mathbb{C}[X,Y]$ mit $\deg_Y(Q) < \deg_Y(A_\ell)$.

Beweis. 1. Wir wenden Korollar 2.1.20 mit $f(\tau) = m_\ell(\tau)$ an. Wie angemerkt, ist $m_\ell(\tau)$ holomorph, analog gilt dies auch für $m_\ell(\tau)^{-1}$. In Korollar 3.3.2 wird weiterhin gezeigt, dass $m_\ell(\mathbb{H}) = \mathbb{C}^*$ ist. Daher sind die holomorphen Funktionen in $\mathbb{C}(m_\ell(\tau))$ gegeben durch $\mathcal{O} = \mathbb{C}[m_\ell(\tau), m_\ell(\tau)^{-1}]$. Nun ergibt sich mit Korollar 2.1.20 die Behauptung.

2. Wir wählen $f(\tau) = a_\ell(\tau)$. Die Funktion ist nach Lemma 3.3.9 holomorph und nach Korollar 3.3.13 surjektiv auf $\mathbb{C}$. Somit gilt in diesem Fall $\mathcal{O} = \mathbb{C}[a_\ell(\tau)]$, was mit Korollar 2.1.20 die Behauptung impliziert.

□

2.2 Die Tate-Kurve

In diesem Abschnitt werden wir die universellen elliptischen Gauß-Summen, deren Berechnung wir uns später widmen werden, definieren. Zunächst erinnern wir an die Weierstraßsche $\wp$-Funktion:

Definition 2.2.1. [Cox89, S. 200] Sei $\Lambda = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}} \subset \mathbb{C}$ und seien ω_1, ω_2 über $\mathbb{R}$ linear unabhängig. In diesem Fall bezeichnen wir Λ als *Gitter*. Die *Weierstraßsche $\wp$-Funktion* zu Λ ist definiert als

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Für die speziellen Gitter $\langle 1, \tau \rangle_{\mathbb{Z}}$ mit $\tau \in \mathbb{H}$ schreiben wir

$$\wp(z, \tau) := \wp(z, \langle 1, \tau \rangle_{\mathbb{Z}}) = \frac{1}{z^2} + \sum_{n^2+m^2 \neq 0} \left(\frac{1}{(z-(m+n\tau))^2} - \frac{1}{(m+n\tau)^2} \right).$$

Bemerkung 2.2.2.

1. Die Weierstraßsche $\wp$-Funktion ist von fundamentaler Bedeutung für die Theorie der meromorphen doppelt-periodischen Funktionen in der komplexen Ebene. Wir werden im Rahmen dieser Arbeit darauf jedoch nicht näher eingehen.

2. Die Ableitung der Weierstraßschen $\wp$-Funktion ist gegeben durch

$$\wp'(z, \tau) = -\frac{2}{z^3} - 2 \sum_{n^2+m^2 \neq 0} \frac{1}{(z-(m+n\tau))^3}.$$

Satz 2.2.3. *[Sil09, S. 159–161] Sei $E/\mathbb{C}$ eine elliptische Kurve. Dann existiert ein $\tau \in \mathbb{H}$ und ein $\alpha \in \mathbb{C}$, sodass mit $\Lambda = \langle 1, \tau \rangle_{\mathbb{Z}}$*

$$\psi_1 : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad z \mapsto \begin{cases} (\wp(\alpha z, \alpha\Lambda), \wp'(\alpha z, \alpha\Lambda)), & z \notin \Lambda, \\ \mathcal{O}, & z \in \Lambda, \end{cases}$$

ein komplex-analytischer Isomorphismus ist.

Die folgende Reihenentwicklung der Weierstraßschen $\wp$-Funktion werden wir mehrfach verwenden:

Lemma 2.2.4. *[Sil94, S. 50] Seien $q = e^{2\pi i \tau}$, $w = e^{2\pi i z}$. Dann gelten für $|q| < |w| < |q^{-1}|$ die folgenden Gleichungen:*

$$\frac{1}{(2\pi i)^2} \wp(z, \tau) = \frac{1}{12} - 2 \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} + \sum_{n \in \mathbb{Z}} \frac{q^n w}{(1-q^n w)^2} =: x(w, q), \tag{2.10}$$

$$\frac{1}{(2\pi i)^3} \wp'(z, \tau) = \sum_{n \in \mathbb{Z}} \frac{q^n w (1+q^n w)}{(1-q^n w)^3} =: 2y(w, q). \tag{2.11}$$

Bemerkung 2.2.5. Unter Verwendung verschiedener Identitäten lassen sich die Reihenentwicklungen für $x(w, q)$ und $y(w, q)$ umschreiben, was sowohl für den Beweis theoretischer Aussagen als auch für die tatsächliche Berechnung dieser Werte von großer Nützlichkeit ist. Wir erinnern an die Gleichung für die geometrische Reihe

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i \quad \text{für} \quad |x| < 1.$$

Gliedweises Differenzieren liefert

$$\frac{1}{(1-x)^2} = \sum_{i=0}^{\infty}(i+1)x^i \quad \text{und} \quad \frac{2}{(1-x)^3} = \sum_{i=0}^{\infty}(i+1)(i+2)x^i.$$

Daneben benutzen wir noch die Identität

$$(1-x^{-1})^{-1} = (-x^{-1}(1-x))^{-1} = -x(1-x)^{-1}.$$

Damit erhalten wir für $|q| < |w| < |q^{-1}|$ die Formeln

$$x(w,q) = \frac{1}{12} + \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} mq^{nm}(w^m + w^{-m}) - 2mq^{nm}, \tag{2.12}$$

$$y(w,q) = \frac{w+w^2}{2(1-w)^3} + \frac{1}{2}\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{m(m+1)}{2}\left(q^{nm}(w^m - w^{-m}) + q^{n(m+1)}(w^{m+1} - w^{-(m+1)})\right). \tag{2.13}$$

In den von uns betrachteten Fällen wird w eine Einheitswurzel sein, sodass wegen $|q(\tau)| < 1$ für $\tau \in \mathbb{H}$ die Reihenentwicklungen in dieser Form angegeben werden können.

Proposition 2.2.6. *[Sch95, S. 245] Seien $E_4(q), E_6(q)$ die in Beispiel 2.1.3 definierten Eisensteinreihen und $E_2(q)$ wie in Beispiel 2.1.10. Dann gelten folgende Gleichungen:*

$$y(w,q)^2 = x(w,q)^3 - \frac{E_4(q)}{48}x(w,q) + \frac{E_6(q)}{864}, \tag{2.14}$$

$$\sum_{\zeta\in\mu_\ell,\zeta\neq 1} x(\zeta,q) = \frac{1}{12}\ell(E_2(q) - \ell E_2(q^\ell)) = p_1(q). \tag{2.15}$$

Durch Gleichung (2.14) wird die sogenannte Tate-Kurve E_q definiert, die in [Tat95] eingeführt wurde. Sie besitzt die folgenden wichtigen Eigenschaften:

Satz 2.2.7. *[Sil94, S. 410–411]*

1. *Die Tate-Kurve E_q ist eine elliptische Kurve und es gilt*

$$\Delta(E_q) = \Delta(q), \quad j(E_q) = j(q),$$

   wobei $\Delta(q)$, $j(q)$ genau die entsprechenden Modulfunktionen aus Abschnitt 2.1.1 sind.

2. *Es gibt einen komplex-analytischen Isomorphismus*

$$\psi_2 : \mathbb{C}^*/q^{\mathbb{Z}} \to E_q(\mathbb{C}), \quad w \mapsto \begin{cases}(x(w,q), y(w,q)), & w \notin q^{\mathbb{Z}},\\ \mathcal{O}, & w \in q^{\mathbb{Z}}.\end{cases}$$

3. *Für jede elliptische Kurve $E/\mathbb{C}$ existiert ein $q \in \mathbb{C}^*$ mit $|q| < 1$, sodass*

$$E_q \cong E(\mathbb{C})$$

   gilt. Dieses q ist durch $q = q(\tau) = \exp(2\pi i\tau)$ für das τ aus Satz 2.2.3 gegeben. Wie in Satz 2.2.3 schreiben wir $\Lambda = \langle 1, \tau\rangle_{\mathbb{Z}}$. Für den Isomorphismus $\psi : E_q \to E(\mathbb{C})$ gilt

$\psi = \psi_1 \circ \theta^{-1} \circ \psi_2^{-1}$ mit ψ_1 aus Satz 2.2.3 und

$$\theta : \mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}^*/q^{\mathbb{Z}}, \quad z \mapsto w = \exp(2\pi i z).$$

Damit ist ψ gegeben als

$$(x(w,q), y(w,q)) \mapsto (\wp(\alpha z, \alpha\Lambda), \wp'(\alpha z, \alpha\Lambda)), \quad \mathcal{O} \mapsto \mathcal{O}$$

mit α wie in Satz 2.2.3.

Die Tate-Kurve parametrisiert somit die Isomorphieklassen elliptischer Kurven über $\mathbb{C}$. Dies stellt die Grundidee der von uns ausgeführten Rechnungen dar: Wir berechnen nämlich die gesuchten Objekte, die elliptischen Gauß-Summen, mithilfe der Tate-Kurve als formale Potenzreihen in q. Die Spezialisierung auf eine konkrete elliptische Kurve $E \cong E_{q(\tau)}$ über $\mathbb{C}$ oder (nach Reduktion) über $\mathbb{F}_p$ geschieht dann, indem die formale Variable q durch den konkreten Wert $q(\tau)$ ersetzt wird, wie dies in Abschnitt 4.1 ausgeführt wird.

Wir untersuchen nun das Verhalten von $\wp(z,\tau)$ und $\wp'(z,\tau)$ unter Transformationen aus Γ. Mittels Lemma 2.2.4 wird dies zu Aussagen über das Verhalten von $x(w,q)$ sowie $y(w,q)$ führen. Es gilt folgendes

Lemma 2.2.8. *Sei $\tau \in \mathbb{H}$ und $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Dann gelten*

$$\wp(z, \gamma\tau) = (c\tau + d)^2 \wp((c\tau + d)z, \tau), \tag{2.16}$$
$$\wp'(z, \gamma\tau) = (c\tau + d)^3 \wp'((c\tau + d)z, \tau). \tag{2.17}$$

Beweis. Wir rechnen nach

$$\begin{aligned}
\wp\left(z, \frac{a\tau+b}{c\tau+d}\right) &= \frac{1}{z^2} + \sum_{n^2+m^2\neq 0} \left(\frac{1}{(z - (m + n\frac{a\tau+b}{c\tau+d}))^2} - \frac{1}{(m + n\frac{a\tau+b}{c\tau+d})^2} \right) \\
&= (c\tau + d)^2 \cdot \frac{1}{((c\tau + d)z)^2} \\
&\quad + (c\tau + d)^2 \sum_{m^2+n^2\neq 0} \left(\frac{1}{((c\tau + d)z - S_{a,b,c,d}(m,n))^2} - \frac{1}{(S_{a,b,c,d}(m,n))^2} \right) \\
&= (c\tau + d)^2 \wp((c\tau + d)z, \tau),
\end{aligned}$$

wobei wir die Abkürzung $S_{a,b,c,d}(m,n) = m(c\tau + d) + n(a\tau + b)$ benutzen und die letzte Gleichung aus $ad - bc = 1$ folgt. Die Identität für die Ableitung von $\wp$ zeigt man völlig analog. □

Korollar 2.2.9. *Sei $\gamma \in \Gamma_0(\ell)$.*

1. *Sei $\zeta_\ell \in \mu_\ell$ eine ℓ-te Einheitswurzel. Dann gilt*

$$x(\zeta_\ell, q(\gamma\tau)) = (c\tau + d)^2 x(\zeta_\ell^d, \tau) \quad \text{und} \quad y(\zeta_\ell, q(\gamma\tau)) = (c\tau + d)^3 y(\zeta_\ell^d, \tau).$$

2. *Die in Formel (2.7) definierte Funktion $p_1(q)$ transformiert sich unter der Wirkung von γ mittels $p_1(q(\gamma\tau)) = (c\tau + d)^2 p_1(q)$.*

3. *Sei n ein Teiler von $\ell-1$, $\chi : \mathbb{F}_\ell^* \to \mu_n$ ein Dirichlet-Charakter von Ordnung n und seien*
$$V = \begin{cases} x, & n \equiv 1 \mod 2, \\ y, & n \equiv 0 \mod 2, \end{cases} \quad \textit{sowie} \quad e = \begin{cases} 2n, & n \equiv 1 \mod 2, \\ 3n, & n \equiv 0 \mod 2. \end{cases}$$
Dann transformiert sich die von χ abhängige n-te Potenz der Funktion
$$G_{\ell,n,\chi}(q) = G_{\ell,n}(q) := \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda) V(\zeta_\ell^\lambda, q) \tag{2.18}$$
unter γ mittels $G_{\ell,n}(q(\gamma\tau))^n = (c\tau+d)^e G_{\ell,n}(q)^n$.

4. *Die Funktionen $p_1(q)$ und $G_{\ell,n}(q)^n$ sind meromorph an den Spitzen und somit Modulfunktionen vom jeweils angegebenen Gewicht für $\Gamma_0(\ell)$. Weiterhin ist $G_{\ell,n}(q)^n$ unabhängig von der Wahl der primitiven ℓ-ten Einheitswurzel $\zeta_\ell \in \mu_\ell$.*

Beweis. 1. Für $k = \frac{1}{(2\pi i)^2}$ gilt
$$x(\zeta_\ell, q(\tau)) = k\wp\left(\frac{v}{\ell}, \tau\right)$$
für ein $v \in \mathbb{Z}$. Damit folgt
$$\begin{aligned} x(\zeta_\ell, q(\gamma\tau)) &= k\wp\left(\frac{v}{\ell}, \gamma\tau\right) = k(c\tau+d)^2\wp\left(\frac{(c\tau+d)v}{\ell}, \tau\right) \\ &= (c\tau+d)^2 x\left(\exp\left(\frac{2\pi i(c\tau+d)v}{\ell}\right), q\right) = (c\tau+d)^2 x\left(\exp\left(\frac{2\pi i dv}{\ell}\right), q\right) \\ &= (c\tau+d)^2 x(\zeta_\ell^d, q), \end{aligned}$$
wobei die vorletzte Gleichheit wegen $c \equiv 0 \mod \ell$ direkt aus der Reihenentwicklung (2.10) von $x(w,q)$ folgt. Die Gleichung für y wird wieder analog gezeigt.

2. Wegen $\gamma \in \Gamma_0(\ell)$ ist $d \not\equiv 0 \mod \ell$, daher permutiert die Wirkung von γ die Summanden in Gleichung (2.15) bei gleichzeitiger Multiplikation mit $(c\tau+d)^2$.

3. Ohne Beschränkung der Allgemeinheit sei n ungerade. Es ist
$$\begin{aligned} G_{\ell,n}(q(\gamma\tau)) &= \sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda) x(\zeta_\ell^\lambda, q(\gamma\tau)) = (c\tau+d)^2 \sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda) x(\zeta_\ell^{d\lambda}, q(\tau)) \\ &= (c\tau+d)^2 \chi^{-1}(d) \sum_{a\in\mathbb{F}_\ell^*} \chi(a) x(\zeta_\ell^a, q(\tau)) = (c\tau+d)^2 \chi^{-1}(d) G_{\ell,n}(q). \end{aligned}$$
Die Behauptung folgt sofort, da χ Werte in μ_n annimmt.

4. Wir erinnern an das Repräsentantensystem für $\Gamma/\Gamma_0(\ell)$, das durch $\{S_k, k = 0, \ldots, \ell\}$ mit
$$S_k = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \quad \text{für} \quad 0 \leqslant k < \ell, \quad S_\ell = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
gegeben ist. Wir berechnen nun gemäß Bemerkung 2.1.7 für alle S_k die Fourierreihen-

entwicklung von $x(\zeta_\ell, q(S_k\tau))$. Für $k < \ell$ gilt

$$x(\zeta_\ell, q(S_k\tau)) = (\tau+k)^2 x\left(\exp\left(\frac{2\pi i(\tau+k)v}{\ell}\right), q\right) = (\tau+k)^2 x(\zeta_\ell^k q^{\frac{v}{\ell}}, q).$$

Berechnet man $x(\zeta_\ell^k q^{\frac{v}{\ell}}, q)$ mit Formel (2.12), so ist offensichtlich, dass in dieser q-Entwicklung nur endlich viele negative Exponenten auftreten. Eine analoge Aussage lässt sich für $y(w,q)$ zeigen. Aus der Konstruktion von $p_1(q)$ sowie $G_{\ell,n}(q)^n$ ist nun ersichtlich, dass diese Modulfunktionen meromorph an den Spitzen sind.
Die Unabhängigkeit von $G_{\ell,n}(q)^n$ von der Wahl von ζ_ℓ folgt direkt aus dem bereits Gezeigten, denn danach gilt für $d \not\equiv 0 \mod \ell$

$$\sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda) x(\zeta_\ell^{d\lambda}, q) = \chi^{-1}(d) \sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda) x(\zeta_\ell^{\lambda}, q).$$

□

Wir kommen schließlich zur Konstruktion der *universellen elliptischen Gauß-Summen*, mit deren konkreter Berechnung wir uns ausgiebig beschäftigen werden.

Korollar 2.2.10. *Seien ℓ, n, χ wie in Korollar 2.2.9. Weiterhin gelte*

$$r = \begin{cases} \min\left\{r : \frac{n+r}{6} \in \mathbb{N}\right\}, & n \equiv 1 \mod 2, \\ 3, & n = 2, \\ 0, & \textit{sonst}, \end{cases} \quad \textit{und} \quad e_\Delta = \begin{cases} \frac{n+r}{6}, & n \equiv 1 \mod 2, \\ 1, & n = 2, \\ \frac{n}{4}, & \textit{sonst}. \end{cases}$$

Dann ist

$$\tau_{\ell,n}(q) := \frac{G_{\ell,n}(q)^n p_1(q)^r}{\Delta(q)^{e_\Delta}} \tag{2.19}$$

eine auf $\mathbb{H}$ holomorphe Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$ mit Koeffizienten in $\mathbb{Q}[\zeta_n]$.

Beweis. Ohne Beschränkung der Allgemeinheit sei n ungerade. Aus Korollar 2.2.9 wissen wir, dass $G_{\ell,n}(q)^n$ und $p_1(q)$ Modulfunktionen für $\Gamma_0(\ell)$ von Gewicht $2n$ bzw. 2 sind. Weiterhin ist bekannt, dass die Diskriminante eine Modulfunktion von Gewicht 12 für Γ, also auch für Untergruppen, ist. Da außerdem $\Delta(q) \neq 0$ gilt, ist der betrachtete Ausdruck ebenfalls eine Modulfunktion für $\Gamma_0(\ell)$, deren Gewicht offenbar durch

$$2n + 2r - 12\frac{n+r}{6} = 0$$

gegeben ist.
Mithilfe der Formel (2.10) lassen sich die Polstellen von $x(\zeta_\ell, q(\tau))$ einfach bestimmen. Offenbar liegt genau dann eine Polstelle vor, wenn $q^n = 1$ oder $q^n = \zeta_\ell$ für ein n gilt. In beiden Fällen folgt $|q| = |\exp(2\pi i\tau)| = 1$, was $\tau \in \mathbb{H}$ widerspricht. Damit sind die Funktionen im Zähler nach Konstruktion holomorph. Analoges gilt bei Verwendung von $y(\zeta_\ell, q(\tau))$. Außerdem gilt $\Delta(\tau) \neq 0$ auf $\mathbb{H}$, womit $\tau_{\ell,n}(q)$ holomorph ist.
Um die Aussage über die Koeffizienten zu zeigen, bemerken wir zunächst, dass die Koeffizienten von $p_1(q)$ sowie $\Delta(q)$ in $\mathbb{Z}$ liegen. Da der führende Koeffizient von Δ eine Eins ist, gilt dies auch für die Koeffizienten von $\Delta(q)^{-1}$. Weiterhin ist aus der Definition der Gauß-Summe

in Korollar 2.2.9 unmittelbar ersichtlich, dass ihre Koeffizienten in $\mathbb{Q}[\zeta_n, \zeta_\ell]$ liegen. Sei nun c ein Erzeuger von $\mathbb{F}_\ell^*$ und $\sigma : \zeta_\ell \mapsto \zeta_\ell^c$, sodass $\mathrm{Gal}(\mathbb{Q}[\zeta_n, \zeta_\ell]/\mathbb{Q}[\zeta_n])$ von σ erzeugt wird. Nun gilt

$$\begin{aligned}\sigma(G_{\ell,n}(q)) &= \sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda)\sigma(V(\zeta_\ell^\lambda, q)) = \sum_{\lambda\in\mathbb{F}_\ell^*} \chi(\lambda)V(\zeta_\ell^{c\lambda}, q)\\ &= \chi^{-1}(c)\sum_{\lambda\in\mathbb{F}_\ell^*} \chi(c\lambda)V(\zeta_\ell^{c\lambda}, q) = \chi^{-1}(c)G_{\ell,n}(q),\end{aligned}$$

wobei die zweite Gleichung aus Formel (2.12) bzw. (2.13) folgt, weil σ ein Homomorphismus ist. Es folgt sofort, dass $G_{\ell,n}(q)^n$ unter σ invariant ist, weshalb die Koeffizienten dieses Ausdrucks in $\mathbb{Q}[\zeta_n]$ liegen. □

Bemerkung 2.2.11. Setzt man $f = 6$ für ungerades, $f = 4$ für gerades n und $o = \frac{f}{\mathrm{ggT}(n,f)}$, so ist auch die Funktion $\frac{G_{\ell,n}(q)^{no}}{\Delta^{no/f}}$ eine Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$. Da wir jedoch letztendlich daran interessiert sind, den Wert von $G_{\ell,n}(q(\tau))^n$, spezialisiert auf eine konkrete elliptische Kurve $E_{q(\tau)}$, zu bestimmen, stellt diese potenzielle Variante keine gangbare Alternative dar, da sie nur eine Potenz des gesuchten Wertes liefert und dieser demnach noch durch Ziehen einer o-ten Wurzel gewonnen werden muss, was unter algorithmischen Gesichtspunkten nicht vernachlässigbare Kosten verursacht.

3 Berechnung der universellen elliptischen Gauß-Summen

3.1 Definitionen

In diesem Kapitel widmen wir uns der Vorstellung unserer Algorithmen zunächst zur Bestimmung der Laurentreihen der universellen elliptischen Gauß-Summen, anschließend zur Berechnung der rationalen Ausdrücke in Abhängigkeit von anderen Modulfunktionen gemäß Proposition 2.1.21. Dazu benötigen wir die folgenden Definitionen:

Definition 3.1.1. Sei $f(q)$ durch eine Laurentreihe $\sum_{i=o}^{\infty} a_i q^i$ gegeben. Dann nennen wir o die *Ordnung* und a_o den *Leitkoeffizienten* von $f(q)$. Wir schreiben auch $\mathrm{ord}(f) := o$, $\mathrm{lk}(f) := a_o$.

Bemerkung 3.1.2. Seien $f_1(q), f_2(q)$ durch Laurentreihen mit $\mathrm{ord}(f_1) = o_1, \mathrm{ord}(f_2) = o_2$ gegeben. Dann gilt

1. $\mathrm{ord}(f_1 f_2) = o_1 + o_2$.
2. $\mathrm{ord}(f_1 \pm f_2) = \min\{o_1, o_2\}$ für $o_1 \neq o_2$.
3. Gilt $o := o_1 = o_2$, so erhält man $\mathrm{ord}(f_1 \pm f_2) \geqslant o$ mit Gleichheit genau dann, wenn sich die Leitkoeffizienten der Reihen nicht aufheben.
4. $\mathrm{ord}(f_1^{-1}) = -o_1$. Um dies einzusehen, schreibe $f_1(q) = q^{o_1}\tilde{f}_1(q)$ mit $\mathrm{ord}(\tilde{f}_1) = 0$.

Im Rahmen der Rechnungen können wir nur endlich viele Terme der betrachteten Laurentreihen bestimmen. Dies führt uns zu

Definition 3.1.3. 1. Sei $f(q) = \sum_{i=o}^{\infty} a_i q^i$ durch eine Laurentreihe gegeben. Wir sagen, dass wir f bis zur Präzision p berechnen, wenn wir die Teilsumme $\sum_{i=o}^{o+p-1} a_i q^i$ bestimmen.

2. Sei

$$\mathrm{prec} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (\ell, n) \mapsto \mathrm{prec}(\ell, n) \tag{3.1}$$

eine Abbildung, die einem Tupel (ℓ, n) einen Wert $\mathrm{prec}(\ell, n)$ zuordnet, sodass mit dem betrachteten Algorithmus der rationale Ausdruck zur Darstellung von $\tau_{\ell,n}(q)$ ermittelt werden kann, wenn die auftretenden Laurentreihen bis zu dieser Genauigkeit berechnet werden. Wir werden mögliche Werte für $\mathrm{prec}(\ell, n)$ später untersuchen.

Bei der Analyse der Laufzeit der in diesem Abschnitt und im weiteren Verlauf der Arbeit vorgeschlagenen Algorithmen verwenden wir die folgenden Konventionen und Resultate:

Lemma 3.1.4. *[vG03, MMS07] Wir bezeichnen mit $\mathsf{M}(n)$ den Aufwand zum Multiplizieren zweier Polynome in $\mathbb{Z}[X]$ bzw. $\mathbb{F}_p[X]$ von Grad kleiner als n und mit $\mathsf{C}(n)$ den für die Berechnung von $g(h) \mod f$ für Polynome $f, g, h \in \mathbb{F}_p[X]$ von Grad kleiner als n. Unter Verwendung von schneller Arithmetik können diese Rechnungen in*

$$\mathsf{M}(n) = \tilde{O}(n), \quad \mathsf{C}(n) = O(n^{(\omega+1)/2})$$

Multiplikationen im jeweiligen Grundkörper ausgeführt werden. Dabei besagt die Notation $\tilde{O}(n)$, dass logarithmische Faktoren unterdrückt werden. Der Wert ω ist so gewählt, dass $n \times n$-Matrizen über $\mathbb{F}_p$ mit $O(n^\omega)$ Operationen multipliziert werden können. Der beste bekannte Wert für ω aus [CW90] liegt bei $\omega \approx 2{,}38$.

3.2 Laurentreihen

3.2.1 Allgemeine Bemerkungen

Zunächst bemerken wir, dass bei der Berechnung der Laurentreihen der universellen elliptischen Gauß-Summen aufgrund der bekannten Eigenschaften von Charaktersummen der von w unabhängige Teil in den Formeln (2.12) verschwindet und somit nicht berechnet werden muss. Einen zusätzlichen Ansatz zur Beschleunigung der Berechnung der Gauß-Summen liefert

Lemma 3.2.1. *Sei ℓ eine ungerade Primzahl, $n \mid \frac{\ell-1}{2}$ und sei $\langle c \rangle = \mathbb{F}_\ell^*$. Dann gilt*

$$\{\ell a + nc^a \mod n\ell,\ 0 \leqslant a \leqslant \ell - 2\} = \{\ell a - nc^a \mod n\ell,\ 0 \leqslant a \leqslant \ell - 2\}.$$

Beweis. Da c ein Erzeuger von $\mathbb{F}_\ell^*$ ist, gilt $c^{\frac{\ell-1}{2}} \equiv -1 \mod \ell$. Mit $n \mid \frac{\ell-1}{2}$ folgt dann

$$\ell\left(a + \frac{\ell-1}{2}\right) + nc^{a+\frac{\ell-1}{2}} \equiv \ell a + \frac{\ell(\ell-1)}{2} + nc^a \cdot c^{\frac{\ell-1}{2}} \equiv \ell a - nc^a \mod n\ell.$$

Daher erhält man die Werte auf der rechten Seite der Identität durch Verschiebung von a um $\frac{\ell-1}{2}$ auf der linken Seite. □

Es folgt nun

$$\sum_{a=0}^{\ell-2} \zeta_n^a (\zeta_\ell^{c^a} - \left(\zeta_\ell^{c^a}\right)^{-1}) = \sum_{a=0}^{\ell-2} \zeta_{n\ell}^{\ell a + nc^a} - \zeta_{n\ell}^{\ell a - nc^a} = 0.$$

Wir nutzen die Beobachtungen aus, indem wir für die ℓ-ten Einheitswurzeln ζ jeweils statt

$$x(\zeta, q) = \frac{1}{12} + \frac{\zeta}{(1-\zeta)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} mq^{nm}(\zeta^m + \zeta^{-m}) - 2mq^{nm}$$

lediglich die Reihe

$$\tilde{x}(\zeta, q) = \frac{\zeta}{(1-\zeta)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} 2mq^{nm}\zeta^m \tag{3.2}$$

bis zur gewünschten Präzision berechnen, denn für ungerades n gilt

$$G_{\ell,n}(q) = \sum_{a=0}^{\ell-2} \zeta_n^a x(\zeta_\ell^{c^a}, q) = \sum_{a=0}^{\ell-2} \zeta_n^a \tilde{x}(\zeta_\ell^{c^a}, q).$$

Hierdurch reduziert sich die Laufzeit zur Berechnung von $G_{\ell,n}(q)$ etwa um den Faktor 2.

Weiterhin möchten wir aus Effizienzgründen in unserer Implementierung mit der Bibliothek GMP [Gra15] für die auftretenden Koeffizienten so lange wie möglich den Datentyp für ganze Zahlen verwenden und die Koeffizienten der Reihen erst im letzten Schritt durch Division

in rationale Zahlen umwandeln. Um dieses Vorhaben zu verwirklichen, müssen die in den Laurentreihen der universellen elliptischen Gauß-Summen auftretenden Nenner untersucht werden.

Zunächst bemerken wir, dass mit Ausnahme des konstanten, von q unabhängigen Terms in der für die x-Koordinate verwendeten Formel (3.2) alle Koeffizienten in $\mathbb{Z}[\zeta_\ell]$ und in der zu y gehörigen Formel (2.13) in $\frac{1}{2}\mathbb{Z}[\zeta_\ell]$ liegen. Der konstante Term liefert eine Potenz ℓ^{c_ℓ}, die den Nenner der Ausdrücke teilen kann. Der genaue Wert von c_ℓ ergibt sich gemäß

Lemma 3.2.2. *Sei*

$$c_\ell = \begin{cases} \lceil \frac{2n}{\ell-1} \rceil, & n \text{ ungerade,} \\ \lceil \frac{3n}{\ell-1} \rceil, & n \text{ gerade.} \end{cases}$$

Dann gilt $v_\ell(\ell^{c_\ell} \cdot \tau_{\ell,n}(q)) \geqslant 0$, wobei v_ℓ die ℓ-adische Bewertung bezeichnet.

Beweis. Bekanntlich gilt

$$(\ell) = (1-\zeta_\ell)^{\ell-1},$$

wenn beide Seiten als Ideale in $\mathbb{Z}[\zeta_\ell] = \mathcal{O}(\mathbb{Q}[\zeta_\ell])$ betrachtet werden, und damit

$$v_\ell((1-\zeta_\ell)^{-k}) = -\frac{k}{\ell-1}.$$

Aus der Gestalt der konstanten Terme in den Formeln (3.2) sowie (2.13) und Korollar 2.2.10 ergibt sich mit $k = 2n$ für die x- bzw. $k = 3n$ für die y-Koordinaten die Behauptung. □

Wir bemerken noch, dass wegen Formel (2.7) die Koeffizienten von $12p_1(q)$ ebenfalls ganz sind. Weil $\Delta(q)$ Leitkoeffizienten 1 hat, sind auch die Koeffizienten von $\Delta(q)^{-1}$ ganze Zahlen. Aus diesen Überlegungen und der Definition von $\tau_{\ell,n}(q)$ in Korollar 2.2.10 folgt

Korollar 3.2.3. *Sei ℓ eine Primzahl und es gelte $n \mid \ell - 1$. Sei $r = \min\{r : \frac{n+r}{6} \in \mathbb{N}\}$ für $n \equiv 1 \mod 2$ wie in Korollar 2.2.10 und c_ℓ wie in Lemma 3.2.2. Definiere*

$$c = \begin{cases} 12^r \ell^{c_\ell}, & n \equiv 1 \mod 2, \\ 2^2 \cdot 12^3 \ell^{c_\ell}, & n = 2, \\ 2^n \ell^{c_\ell}, & \text{sonst.} \end{cases}$$

Dann liegen alle Koeffizienten von $c \cdot \tau_{\ell,n}(q)$ in $\mathbb{Z}[\zeta_n]$.

3.2.2 Verbesserung des Algorithmus

Wie aus der Formel in Korollar 2.2.9 leicht ersichtlich ist, gilt $G_{\ell,n}(q) \in \mathbb{Q}[\zeta_n, \zeta_\ell]((q))$. Zur Berechnung von $\tau_{\ell,n}(q)$ bis zur Präzision $\operatorname{prec}(\ell, n)$ muss also insbesondere die n-te Potenz eines Elements dieses Körpers bestimmt werden, was, wenn wir das Vielfache von $\tau_{\ell,n}(q)$ aus Korollar 3.2.3 verwenden, eine Laufzeit von

$$O(\log n \, \mathsf{M}(\ell n \operatorname{prec}(\ell, n)))$$

Multiplikationen in $\mathbb{Z}$ erfordert. Dabei gilt $\operatorname{prec}(\ell, n) = O((v + e_\Delta)\ell))$ gemäß Proposition 3.3.4 bzw. Gleichung (3.16) mit $v = \operatorname{ord}(m_\ell)$ bzw. $v = -\operatorname{ord}(a_\ell)$. Im ungünstigsten Fall gilt

$n, v \in O(\ell)$, womit sich für diesen Schritt eine schnell wachsende Laufzeit von $O(\log n\, \mathsf{M}(\ell^4))$ ergibt. Im Folgenden soll gezeigt werden, wie die Zeitkomplexität deutlich reduziert werden kann.

Wir benutzen dazu insbesondere das folgende

Lemma 3.2.4. *Es bezeichne $G_\chi(\zeta_\ell) = \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda)\zeta_\ell^\lambda$ die gewöhnliche zyklotomische Gauß-Summe. Dann gilt*

$$G_{\ell,n,\chi}(q) G_{\chi^{-1}}(\zeta_\ell) \in \mathbb{Q}[\zeta_n]((q)).$$

Beweis. Nach Definition liegt der gesuchte Ausdruck in $\mathbb{Q}[\zeta_\ell, \zeta_n]((q))$. Wir betrachten die Wirkung der Galoisgruppe G der Körpererweiterung $\mathbb{Q}[\zeta_\ell, \zeta_n]/\mathbb{Q}[\zeta_n]$ auf den Ausdruck. Da $(\ell, n) = 1$ gilt, ist $G = \langle \sigma : \zeta_\ell \mapsto \zeta_\ell^c \rangle$, wobei c ein Erzeuger von $\mathbb{F}_\ell^*$ ist. Wie schon im Beweis von Korollar 2.2.10 gezeigt wurde, gilt

$$\sigma(G_{\ell,n,\chi}(q)) = \chi^{-1}(c) G_{\ell,n,\chi}(q).$$

Analog kann man

$$\sigma(G_\chi(\zeta_\ell)) = \chi^{-1}(c) G_\chi(\zeta_\ell)$$

zeigen, woraus sofort die Invarianz des betrachteten Ausdrucks unter σ und damit die Behauptung folgt. □

Aufgrund dieses Lemmas modifizieren wir den Algorithmus zur Bestimmung von $\tau_{\ell,n}(q)$, der sich aus den Formeln (3.2), (2.13), (2.18) und (2.19) ergibt, wie folgt. Anstatt direkt die n-te Potenz von $G_{\ell,n,\chi}(q)$ zu berechnen, rechnen wir:

Algorithmus 1. Schnelle Berechnung von $G_{\ell,n,\chi}(q)^n$

Eingabe: $\ell, n, \mathrm{prec}(\ell, n)$
Ausgabe: $G_{\ell,n,\chi}(q)^n$

1. Berechne $G_{\ell,n,\chi}(q)$ mit den Formeln (3.2), (2.13), (2.18) bis zur Präzision $\mathrm{prec}(\ell, n)$.
2. $T_1 := G_{\ell,n,\chi}(q) G_{\chi^{-1}}(\zeta_\ell)$.
3. $T_2 := T_1^n$.
4. $T_3 := G_{\chi^{-1}}(\zeta_\ell)^n$.
5. Gib $T_4 = T_2 T_3^{-1}$ aus.

Es ist offensichtlich, dass dann $T_4 = G_{\ell,n,\chi}(q)^n$ gilt und somit das gewünschte Ergebnis ermittelt wird. Aufgrund von Lemma 3.2.4 liegt die Laufzeit für Schritt 2 lediglich bei

$$O(\log n\, \mathsf{M}(n \,\mathrm{prec}(\ell, n))) = O(\log n\, \mathsf{M}(\ell^3)),$$

sodass im Grad der zu multiplizierenden Polynome eine ganze Potenz von ℓ eingespart werden kann. Ebenso überlegt man sich leicht, dass T_3 mit Laufzeit $O(\log n\, \mathsf{M}(\ell n))$ und T_4 in Laufzeit $O(\mathrm{prec}(\ell, n)\, \mathsf{M}(n))$ berechnet werden können, was vernachlässigbar ist.

Die Bestimmung von T_1 erfordert bei naiver Implementierung $O(\mathrm{prec}(\ell, n)\, \mathsf{M}(\ell n))$ Operationen. Wir zeigen nun jedoch, wie sich der Aufwand deutlich reduzieren lässt. Dazu rechnen wir

$$G_{\ell,n,\chi}(q) G_{\chi^{-1}}(\zeta_\ell) = \sum_{\lambda_1, \lambda_2 \in \mathbb{F}_\ell^*} \chi(\lambda_1) V(\zeta_\ell^{\lambda_1}, q) \chi^{-1}(\lambda_2) \zeta_\ell^{\lambda_2} = \sum_{c = \lambda_1 \lambda_2^{-1} \in \mathbb{F}_\ell^*} \chi(c) \sum_{\lambda_1 \in \mathbb{F}_\ell^*} \zeta_\ell^{\lambda_1 c^{-1}} V(\zeta_\ell^{\lambda_1}, q).$$

Bevor wir die innere Summe weiter umformen, bemerken wir

$$V(\zeta_\ell, q) = \sum_{i=0}^{\infty} q^i \sum_{k=0}^{\ell-1} a_{i,k}\zeta_\ell^k \Rightarrow V(\zeta_\ell^{\lambda_1}, q) = \sum_{i=0}^{\infty} q^i \sum_{k=0}^{\ell-1} a_{i,k}\zeta_\ell^{\lambda_1 k}$$

mit $a_{i,k} \in \mathbb{Q}$, wie sich durch Anwendung der passenden Potenz von $\sigma : \zeta_\ell \mapsto \zeta_\ell^c$ ergibt. Damit erhält man

$$\begin{aligned}
\sum_{\lambda_1 \in \mathbb{F}_\ell^*} \zeta_\ell^{\lambda_1 c^{-1}} V(\zeta_\ell^{\lambda_1}, q) &= \sum_{i=0}^{\infty} q^i \sum_{\lambda_1 \in \mathbb{F}_\ell^*} \zeta_\ell^{\lambda_1 c^{-1}} \sum_{k=0}^{\ell-1} a_{i,k}\zeta_\ell^{\lambda_1 k} = \sum_{i=0}^{\infty} q^i \sum_{\lambda_1 \in \mathbb{F}_\ell^*} \sum_{k=0}^{\ell-1} a_{i,k}\zeta_\ell^{\lambda_1(k+c^{-1})} \\
&= \sum_{i=0}^{\infty} q^i \left(\sum_{\lambda_1 \in \mathbb{F}_\ell^*} a_{i,-c^{-1}} + \sum_{\substack{k=0 \\ k \neq -c^{-1}}}^{\ell-1} a_{i,k} \sum_{\lambda_3 = \lambda_1(k+c^{-1}) \in \mathbb{F}_\ell^*} \zeta_\ell^{\lambda_3} \right) \\
&= \sum_{i=0}^{\infty} q^i \left((\ell-1) a_{i,-c^{-1}} + \sum_{\substack{k=0 \\ k \neq -c^{-1}}}^{\ell-1} a_{i,k} \sum_{\lambda_3 = 1}^{\ell-1} \zeta_\ell^{\lambda_3} \right) \\
&= \sum_{i=0}^{\infty} q^i \underbrace{\left((\ell-1) a_{i,-c^{-1}} - \sum_{\substack{k=0 \\ k \neq -c^{-1}}}^{\ell-1} a_{i,k} \right)}_{=:b_i(c)},
\end{aligned}$$

wobei die letzte Umformung wegen $\sum_{i=0}^{\ell-1} \zeta_\ell^i = 0$ gilt. Insgesamt ergibt sich damit

$$G_{\ell,n,\chi}(q) G_{\chi^{-1}}(\zeta_\ell) = \sum_{i=0}^{\infty} q^i \sum_{c \in \mathbb{F}_\ell^*} \chi(c) b_i(c)$$

mit $b_i(c) \in \mathbb{Q}$. Weiterhin gilt offenbar für $c_1, c_2 \in \mathbb{F}_\ell^*$

$$b_i(c_1) = b_i(c_2) + \ell(a_{i,-c_1^{-1}} - a_{i,-c_2^{-1}}), \tag{3.3}$$

weshalb die Berechnung von $b_i(c), c \in \mathbb{F}_\ell^*$, für festes i nur ℓ Multiplikationen in $\mathbb{Q}$ erfordert. Um T_1 bis zur nötigen Präzision zu bestimmen, gehen wir also folgendermaßen vor:

Algorithmus 2. Beschleunigung von Schritt 1 in Algorithmus 1

Eingabe: $\ell, n, \operatorname{prec}(\ell, n)$

Ausgabe: $G_{\ell,n,\chi}(q) G_{\chi^{-1}}(\zeta_\ell)$

1. Bestimme die Koeffizienten $a_{i,k}$ von $V(\zeta_\ell, q)$ mit Formel (3.2) bzw. (2.13) im Bereich $i = 0, \ldots, \operatorname{prec}(\ell, n), k = 0, \ldots, \ell - 1$.
2. Für $i = 0, \ldots, \operatorname{prec}(\ell, n)$ bestimme die Werte $b_i(c), c \in \mathbb{F}_\ell^*$, mithilfe von (3.3).
3. Gib $\sum_{i=0}^{\operatorname{prec}(\ell,n)} q^i \sum_{c \in \mathbb{F}_\ell^*} \chi(c) b_i(c)$ aus.

Damit kann der Wert T_1 mit $O(\ell \operatorname{prec}(\ell, n))$ Operationen bestimmt werden und ist für große n gegenüber dem zweiten Schritt des neuen Algorithmus vernachlässigbar.

Um bei der Berechnung von T_4 in Algorithmus 1 den, wie schon weiter oben erwähnt, deutlich langsameren GMP-Datentyp für rationale Zahlen zu umgehen, wird wieder untersucht, mit welchem Faktor die Zwischenergebnisse multipliziert werden müssen, damit alle Koeffizienten ganzzahlig sind. Die benötigte Aussage bezüglich der Größe T_3^{-1} liefert folgendes

Lemma 3.2.5. *Sei ℓ eine Primzahl und χ ein Charakter von Ordnung $n \mid \ell - 1$. Dann gilt*

$$\ell^n G_\chi(\zeta_\ell)^{-n} \in \mathbb{Z}[\zeta_n].$$

Beweis. Wie aus der in Lemma 3.2.4 gezeigten Identität

$$\sigma(G_\chi(\zeta_\ell)) = \chi^{-1}(c) G_\chi(\zeta_\ell)$$

mit $\sigma : \zeta_\ell \mapsto \zeta_\ell^c$ und $\langle c \rangle = \mathbb{F}_\ell^*$ folgt, gilt

$$G_\chi(\zeta_\ell)^n \in \mathbb{Q}[\zeta_n].$$

Aus der Definition der Gauß-Summen ist direkt ersichtlich, dass $G_\chi(\zeta_\ell)^n$ sogar in $\mathbb{Z}[\zeta_n]$ liegt. Eine allgemeine Eigenschaft von Gauß-Summen (s. beispielsweise [Shi71, S. 91]) ist weiterhin gegeben durch

$$G_\chi(\zeta_\ell) G_{\chi^{-1}}(\zeta_\ell) = \chi(-1)\ell.$$

Durch Exponentiation mit n folgt, da $\chi(-1)^n = 1$ gilt,

$$G_\chi(\zeta_\ell)^n G_{\chi^{-1}}(\zeta_\ell)^n = \ell^n$$

und damit

$$\ell^n G_\chi(\zeta_\ell)^{-n} = G_{\chi^{-1}}(\zeta_\ell)^n \in \mathbb{Z}[\zeta_n].$$

□

Korollar 3.2.6. *Die universelle elliptische Gauß-Summe $\tau_{\ell,n}(q)$ kann mit*

$$O(\log n \, \mathsf{M}(n \operatorname{prec}(\ell, n)))$$

Multiplikationen in $\mathbb{Z}$ berechnet werden.

3.3 Rationaler Ausdruck

3.3.1 Allgemeines

In diesem Abschnitt sollen Algorithmen vorgestellt werden, mit deren Hilfe später aus den zuvor berechneten Laurentreihen der universellen elliptischen Gauß-Summen auf konkreten elliptischen Kurven die gewünschten Werte bestimmt werden können. In Korollar 2.2.10 haben wir gezeigt, dass die Größen $\tau_{\ell,n}(q)$ holomorphe Modulfunktionen von Gewicht 0 für $\Gamma_0(\ell)$ sind. Die Aussagen aus Abschnitt 2.1.3 eröffnen nun zunächst zwei mögliche Wege, wie die elliptischen Gauß-Summen schließlich auf einer konkreten elliptischen Kurve E bestimmt werden können:

1. Nach Lemma 2.1.16 existiert ein irreduzibles Polynom $Q_\tau(X, Y) \in \mathbb{C}[X, Y]$ von Grad $\deg_X(Q_\tau) = \ell + 1$, sodass $Q_\tau(\tau_{\ell,n}(q), j(q)) = 0$ gilt. Hat man dieses Polynom bestimmt,

so findet man den Wert von $\tau_{\ell,n}(E)$ auf der Kurve E als Nullstelle von $Q_\tau(X, j(E))$, wobei $j(E)$ die j-Invariante der Kurve E bezeichnet.

2. Nach Satz 2.1.17 bzw. Proposition 2.1.21 ist $\tau_{\ell,n}(q)$ als rationaler Ausdruck in $j(q)$ und $m_\ell(q)$ bzw. $a_\ell(q)$ darstellbar. Weiterhin ist der Nenner des rationalen Ausdrucks genau bekannt. Ist dieser Ausdruck bestimmt, so erhält man $\tau_{\ell,n}(E)$ durch Einsetzen der Werte $j(E)$ sowie $m_\ell(E)$ bzw. $a_\ell(E)$.

Ist $\tau_{\ell,n}(E)$ berechnet, so kann durch Multiplizieren mit der passenden Potenz der Werte $p_1(E)$, $\Delta(E)$ die elliptische Gauß-Summe $G_{\ell,n}(E)^n$ bestimmt werden, wie in Abschnitt 4 im Detail ausgeführt wird.

Bezüglich der ersten Möglichkeit ist anzumerken, dass die Bestimmung derartiger Polynome vielfältig untersucht und verbessert wurde. Allgemeine Überlegungen finden sich beispielsweise in [Mor95], spezifische optimierte Algorithmen im Kontext des Punktezählens auf elliptischen Kurven werden in [Eng09] und [Sut13] behandelt. Zu beachten ist jedoch, dass wir in unseren Anwendungen den Wert von $\tau_{\ell,n}(E)$ auf einer elliptischen Kurve $E/\mathbb{F}_p$ bestimmen wollen. Da $\tau_{\ell,n}(q)$ nach Korollar 2.2.10 Koeffizienten in $\mathbb{Q}[\zeta_n]$ besitzt, wird dies auch für das Polynom Q_τ gelten. Weiterhin wird $\tau_{\ell,n}(E)$ nicht in $\mathbb{F}_p$, sondern in $\mathbb{F}_p[\zeta_n]$ liegen. Die Bestimmung der Nullstellen eines Polynoms von Grad d in diesem Körper erfordert jedoch einen Aufwand von $O(dn^2 \log p)$ Operationen in $\mathbb{F}_p$ (vgl. [vG03, S. 382]), was diesen Ansatz unattraktiv gegenüber bereits bestehenden macht. Daher befassen wir uns im Folgenden mit der zweiten Methode.

3.3.2 Verwendung von m_ℓ

Wir befassen uns zunächst mit der Darstellung von $\tau_{\ell,n}(q)$ mithilfe von $m_\ell(q)$. In diesem Fall erhalten wir nach Proposition 2.1.21 die Darstellung

$$\tau_{\ell,n}(q) = \frac{Q(m_\ell(q), j(q))}{\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q))}, \tag{3.4}$$

wobei $Q(X,Y) = \sum_{i=i_{min}}^{i_{max}} \sum_{k=0}^{v-1} c_{i,k} X^i Y^k$ mit $v = v(m_\ell) = \deg_Y(M_\ell) = \frac{\ell-1}{\mathrm{ggT}(\ell-1,12)}$ gemäß [Mül95, S. 61–62] und $c_{i,k} \in \mathbb{Q}[\zeta_n]$ gilt. Das Polynom M_ℓ kann dabei mit Algorithmus 5.8 aus [Mül95] bestimmt werden. Umformen ergibt die Gleichung

$$\tau_{\ell,n}(q) \frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q)) = Q(m_\ell(q), j(q)), \tag{3.5}$$

deren linke Seite mittels der bekannten q-Entwicklungen bis zu einer gewissen Präzision berechnet werden kann. Wie man anhand der Definition von m_ℓ sowie η sieht, hat $m_\ell(q)$ genau die Ordnung v. Weiterhin gilt $\mathrm{ord}(j) = -1$. Damit folgt $\mathrm{ord}(m_\ell^i j^k) = iv - k$. Somit haben alle Summanden des Ausdrucks

$$Q(m_\ell(q), j(q)) = \sum_{i=i_{min}}^{i_{max}} \sum_{k=0}^{v-1} c_{i,k} m_\ell^i j^k$$

verschiedene Ordnungen, was den folgenden Algorithmus zur Bestimmung von Q liefert:

Algorithmus 3. Bestimmung von Q aus Gleichung (3.4)

Eingabe: $\ell, n, \mathrm{prec}(\ell, n)$
Ausgabe: $Q(X, Y)$ aus Gleichung (3.4)

1. Berechne $\tau_{\ell,n}(q)$, $m_\ell(q)$, $j(q)$ mit Algorithmus 1 sowie den Formeln (2.1)-(2.8) und (2.19) bis zur Präzision $\mathrm{prec}(\ell, n)$.
2. Bestimme $M_\ell(X, Y)$ mit Algorithmus 5.8 aus [Mül95].
3. Berechne $s(q) = \tau_{\ell,n}(q)\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q))$, setze $Q := 0$.
4. **while** $s \neq 0$ **do**
5. Bestimme $o = ord(s)$ und (i, k) mit $iv - k = o$ und $0 \leqslant k < v$.
6. Berechne $s := s - \frac{\mathrm{lk}(s)}{\mathrm{lk}(m_\ell^i j^k)} m_\ell^i j^k$. Setze $Q := Q + \frac{\mathrm{lk}(s)}{\mathrm{lk}(m_\ell^i j^k)} X^i Y^k$.
7. **end while**
8. Gib Q aus.

Die vorausgegangenen Überlegungen implizieren, dass die Ordnung von s in jedem Iterationsschritt wächst und somit verschiedene Summanden des Polynoms Q berechnet werden. Wenn wir eine obere Schranke an die benötigte Präzision $\mathrm{prec}(\ell, n)$ angeben können, können wir sicherstellen, dass wir tatsächlich das korrekte Polynom Q bestimmt haben.

Zur Herleitung einer derartigen Schranke werden wir uns im Wesentlichen der Ordnungen der verschiedenen auftretenden Laurentreihen bedienen. Wir wissen, dass

$$\mathrm{ord}(m_\ell) = v, \quad \mathrm{ord}(j) = -1 \quad \text{sowie} \quad \mathrm{ord}(\tau_{\ell,n}) = -e_\Delta$$

gilt, wobei die letzte Aussage aus $\mathrm{ord}(\Delta) = 1$ folgt. Um eine Schranke an die benötigte Präzision zu erhalten, wenden wir insbesondere auf Gleichung (3.5) die Fricke-Atkin-Lehner-Involution w_ℓ aus Definition 2.1.8 an. Zuvor benötigen wir noch einige Aussagen.

Lemma 3.3.1. *Sei*

$$M_\ell(X, Y) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} a_{i,k} X^i Y^k$$

das zu m_ℓ gehörige Polynom mit $a_{i,k} \in \mathbb{Z}$. Dann gilt

$$a_{i,k} \neq 0 \quad \Rightarrow \quad k \leqslant iv \leqslant (v - k)\ell + v.$$

Beweis. Wir wissen, dass

$$0 = M_\ell(m_\ell(q), j(q)) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} a_{i,k} m_\ell(q)^i j(q)^k$$

gilt. Um die Behauptung zu zeigen, betrachten wir die Ordnungen der verschiedenen Summanden. Es gilt $\mathrm{ord}(m_\ell(q)^i j(q)^k) = iv - k$. Wir suchen zunächst den Summanden mit der geringsten Ordnung n_0. Damit die rechte Summe verschwindet, muss es mindestens einen weiteren Summanden mit derselben Ordnung n_0 geben. Daher betrachten wir für $0 \leqslant i_1, i_2 \leqslant \ell + 1$, $0 \leqslant k_1, k_2 \leqslant v$ die Gleichung

$$i_1 v - k_1 = i_2 v - k_2 \quad \Rightarrow \quad (i_1 - i_2)v = (k_1 - k_2).$$

Aufgrund der Einschränkungen gilt für Lösungen modulo Symmetrie $i_1 = i_2 + 1$ sowie $(k_1, k_2) = (v, 0)$ und es folgt direkt $n_0 \geqslant 0$. Es können nur die Koeffizienten derjenigen

Summanden ungleich Null sein, deren Ordnung größer oder gleich n_0 ist. Falls $a_{i,k} \neq 0$ ist, so folgt also

$$iv - k \geqslant 0 \quad \Rightarrow \quad k \leqslant iv.$$

Für die zweite Ungleichung wenden wir auf die Ursprungsgleichung w_ℓ an und gehen analog vor. Verwenden wir, dass $w_\ell(j(q)) = j(q^\ell)$ sowie $w_\ell(m_\ell(q)) = \frac{\ell^s}{m_\ell(q)}$ nach [Mül95, S. 64] gilt, so ergibt sich

$$0 = M_\ell(m_\ell^*(q), j(q^\ell)) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} a_{i,k} m_\ell^*(q)^i j(q^\ell)^k.$$

Nun ist $\operatorname{ord}(m_\ell^*(q)^i j(q^\ell)^k) = -iv - k\ell$. Analog zu den vorangegangenen Überlegungen erhalten wir $n_0 \geqslant -(\ell+1)v$, weshalb $a_{i,k} \neq 0$ die Beschränkung

$$-iv - k\ell \geqslant -(\ell+1)v \quad \Rightarrow \quad iv \leqslant (v-k)\ell + v$$

impliziert. □

Korollar 3.3.2. *Die Modulfunktion $m_\ell(\tau)$ besitzt die Wertemenge $m_\ell(\mathbb{H}) = \mathbb{C}^*$.*

Beweis. Die Ungleichungen aus Lemma 3.3.1 implizieren $a_{i,v} = 0$ für $i \neq 1$. Weiterhin folgt aus [Mül95, S. 63], dass $a_{1,v} \neq 0$ ist. Für $c \in \mathbb{C}^*$ ist damit $M_\ell(c, Y)$ ein Polynom in Y von Grad v. Wegen der Surjektivität von $j(\tau)$ existiert nun ein τ mit $M_\ell(c, j(\tau)) = 0$. Damit folgt, dass für eine der in Lemma 2.1.16 eingeführten Transformationen S_k die Identität $c = m_\ell(S_k\tau)$ erfüllt ist. Somit nimmt m_ℓ auf $\mathbb{H}$ alle Werte $c \in \mathbb{C}^*$ an. □

Lemma 3.3.3. *Es gilt* $\operatorname{ord}(\tau_{\ell,n}^*) \geqslant n - \ell e_\Delta$.

Beweis. Offenbar gilt $w_\ell(\Delta(q)) = (\ell\tau)^{12}\Delta(q^\ell)$ und $\operatorname{ord}(\Delta(q^\ell)) = \ell$. Wir untersuchen nun das Transformationsverhalten des Zählers von $\tau_{\ell,n}$. Aufgrund der Eigenschaften der Ordnung betrachten wir dazu das Verhalten von $x(\zeta, q)$ (bzw. analog $y(\zeta, q)$) unter w_ℓ. Aus Lemma 2.2.8 folgt für t mit $\zeta = \exp\left(\frac{2\pi i t}{\ell}\right)$

$$w_\ell(x(\zeta,\tau)) = x\left(\zeta, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ell\tau\right) = (\ell\tau)^2 x\left(\exp\left(\frac{2\pi i t \ell\tau}{\ell}\right), \ell\tau\right) = (\ell\tau)^2 x(q^t, q^\ell).$$

Gemäß Formel (2.12) ist

$$x(q^t, q^\ell) = \frac{1}{12} + \frac{q^t}{(1-q^t)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} m q^{\ell nm}(q^{tm} + q^{-tm}) - 2mq^{\ell nm}. \tag{3.6}$$

Die Ordnung des zweiten Summanden ist nun offenbar t, während die Ordnung der unendlichen Summe durch $\ell - t$ gegeben ist. Eine analoge Aussage gilt auch für $y(q^t, q^\ell)$. Da wir bei der Berechnung von $p_1(q)$ und $G_{\ell,n}(q)$ über die verschiedenen ℓ-ten Einheitswurzeln summieren, läuft t im Bereich $\{1, \ldots, \ell-1\}$. Damit folgt $\operatorname{ord}(p_1^*/(\ell\tau)^2) = 0$ wegen des konstanten Terms $\frac{1}{12}$ und, da dieser Term aufgrund der Eigenschaften von Charaktersummen in $G_{\ell,n}(q)$ verschwindet, $\operatorname{ord}(G_{\ell,n}^*/(\ell\tau)^2) \geqslant 1$. Die auftretenden Potenzen von $\ell\tau$ verschwinden in $\tau_{\ell,n}^*(q)$, weil dies genau als Modulfunktion von Gewicht 0 konstruiert ist. Insgesamt folgt $\operatorname{ord}(\tau_{\ell,n}^*) \geqslant n - \ell e_\Delta$. □

Proposition 3.3.4. *In unserem Algorithmus können wir*

$$\mathrm{prec}(\ell, n) = (v - 1 + e_\Delta)\ell + v + e_\Delta - n - \overline{e_\Delta - n - 1}$$

wählen, wobei $0 \leqslant \overline{a} < v$ *den Repräsentanten der Restklasse* $a \mod v$ *bezeichnet.*

Beweis. Gemäß Gleichung (3.5) gilt

$$\tau_{\ell,n}(q)\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q)) = Q(m_\ell(q), j(q)). \tag{3.7}$$

Wir schreiben $Q(m_\ell(q), j(q)) = \sum_{i=o}^{\infty} c_i q^i = \sum_{i=i_{min}}^{i_{max}} \sum_{k=0}^{v-1} c_{i,k} m_\ell(q)^i j(q)^k$. Mit den Bezeichnungen aus Lemma 3.3.1 ist nun

$$\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q)) = \sum_{i=0}^{\ell+1}\sum_{k=0}^{v-1}(k+1)a_{i,k+1}m_\ell(q)^i j(q)^k,$$

womit sich

$$a_{i,k+1} \neq 0 \quad \Rightarrow \quad iv \geqslant k+1 \quad \Rightarrow \quad iv - k \geqslant 1$$

und somit $\mathrm{ord}\left(\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q))\right) \geqslant 1$ ergibt. Wegen $\mathrm{ord}(\tau_{\ell,n}) = -e_\Delta$ folgt $o \geqslant 1 - e_\Delta$ und damit impliziert $c_{i,k} \neq 0$, dass $iv - k \geqslant 1 - e_\Delta$ gilt. Wie man sich leicht überlegt, gilt $e_\Delta \leqslant v$, woraus man insbesondere $i_{min} \geqslant 0$ schließt. Es treten also in Q keine negativen Potenzen von $m_\ell(q)$ auf.
Um eine obere Schranke an die Größe $iv - k$ zu finden, wenn $c_{i,k} \neq 0$ gilt, wenden wir auf Gleichung (3.5) die Fricke-Atkin-Lehner-Involution aus Definition 2.1.8 an und erhalten

$$\tau^*_{\ell,n}(q)\frac{\partial M_\ell}{\partial Y}(m^*_\ell(q), j(q^\ell)) = Q(m^*_\ell(q), j(q^\ell)). \tag{3.8}$$

Die in der Ableitung des Polynoms M_ℓ auftretenden Summanden haben jeweils die Ordnung $\mathrm{ord}(m^*_\ell(q)^i j(q^\ell)^k) = -iv - k\ell$. Wir verwenden erneut Lemma 3.3.1 und erhalten

$$a_{i,k+1} \neq 0 \quad \Rightarrow \quad iv \leqslant (v - (k+1))\ell + v \quad \Rightarrow \quad -iv - k\ell \geqslant -(v-1)\ell - v,$$

also $\mathrm{ord}\left(\frac{\partial M_\ell}{\partial Y}(m^*_\ell(q), j(q^\ell))\right) \geqslant -(v-1)\ell - v$. Mit $\mathrm{ord}(\tau^*_{\ell,n}) \geqslant n - \ell e_\Delta$ folgt

$$\mathrm{ord}(Q(m^*_\ell(q), j(q^\ell))) \geqslant -(v - 1 + e_\Delta)\ell - v + n =: o'.$$

Wenn $c_{i,k} \neq 0$ ist, muss somit

$$-iv - \ell k \geqslant o' \quad \Rightarrow \quad iv - k \leqslant iv + \ell k \leqslant -o'$$

gelten. Wegen $\ell \equiv 1 \mod v$ ist $-o' \equiv e_\Delta - n - 1 \mod v$. Bezeichnen wir mit $0 \leqslant \overline{a} < v$ den Repräsentanten der Restklasse $a \mod v$, erhalten wir somit

$$iv - k \leqslant iv \leqslant -o' - \overline{e_\Delta - n - 1}.$$

Eine Abschätzung an die benötigte Präzision ergibt sich nun direkt als Differenz aus der

oberen und unteren Schranke an $iv - k$ als

$$\operatorname{prec}(\ell, n) \leqslant -o' - \overline{e_\Delta - n - 1} - (1 - e_\Delta) + 1 = (v - 1 + e_\Delta)\ell + v + e_\Delta - n - \overline{e_\Delta - n - 1}.$$

□

Bemerkung 3.3.5.

1. Wegen $e_\Delta \leqslant v$, $v \leqslant \frac{\ell-1}{2}$ kann in der Implementierung die einfachere Schranke $\operatorname{prec}(\ell, n) = (v + e_\Delta)\ell$ verwendet werden, ohne dass dies einen asymptotischen Einfluss auf die Laufzeit hat.

2. Eine Alternative für die Bestimmung des rationalen Ausdrucks liefert die Beobachtung, dass $m_\ell(q) = \frac{\ell^s}{m_\ell^*(q)}$ gilt. Damit erhält man unter Verwendung des Polynoms M_ℓ die Gleichung
$$0 = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} a_{i,k} \left(\frac{\ell^s}{m_\ell^*(q)} \right)^i j(q)^k,$$
woraus sich durch Multiplikation mit $m_\ell^*(q)^{\ell+1}$
$$0 = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} \ell^{si} a_{i,k} m_\ell^*(q)^{\ell+1-i} j(q)^k = \sum_{i=0}^{\ell+1} \sum_{k=0}^{v} b_{i,k} m_\ell^*(q)^i j(q)^k =: M_\ell^c(m_\ell^*(q), j(q))$$
mit $b_{i,k} = \ell^{s(\ell+1-i)} a_{\ell+1-i,k}$ ergibt. Somit ist eine Variante des Polynoms M_ℓ durch $M_\ell^c(X, Y)$ gegeben und man kann auch einen rationalen Ausdruck unter Verwendung von $m_\ell^*(q)$ statt von $m_\ell(q)$ berechnen. In diesem Fall erhält man durch analoge Überlegungen die Ungleichungen
$$-(\ell + 1)v - e_\Delta + 1 \leqslant o \leqslant \ell(e_\Delta - 1) - n - \overline{e_\Delta - n - 1},$$
wobei $o = -iv - k$ die Ordnung der Summanden $m_\ell^*(q)^i j(q)^k$ von $Q(m_\ell^*(q), j(q))$ bezeichnet, die nicht verschwinden.
Insgesamt ergibt sich die gleiche Schranke an die benötigte Präzision. Wie sich aus der oberen Schranke ergibt, können jedoch negative Potenzen von $m_\ell^*(q)$ in Q auftreten, sofern $e_\Delta > 1$ gilt.

Proposition 3.3.4 legt nun nahe, eine Form für $\tau_{\ell,n}$ zu wählen, in der e_Δ möglichst klein ist. Dies ist zusätzlich zu dem dort angeführten Argument ein Grund dafür, dass die Variante aus Bemerkung 2.2.11 nicht verwendet wird.

Korollar 3.3.6. *Algorithmus 3 berechnet Q mit $\tilde{O}((v + e_\Delta)^2 \ell^2)$ Multiplikationen in $\mathbb{Z}$.*

Beweis. In jedem Durchlauf von Schleife 4 wird $\operatorname{ord}(s)$ aufgrund der Wahl der Exponenten i und k echt kleiner. Da die Berechnung der Reihen bis zur Präzision $\operatorname{prec}(\ell, n) = (v + e_\Delta)\ell$ nach Bemerkung 3.3.5 hinreichend ist, wird die Schleife höchstens so oft durchlaufen. Es ist klar, dass, wenn wir wenige Zwischenergebnisse speichern, in jedem Schleifendurchlauf eine konstante Menge von Multiplikationen von Laurentreihen durchgeführt werden muss, denen gegenüber die ebenfalls durchzuführenden Multiplikationen mit Konstanten vernachlässigbar sind. Da die zu multiplizierenden Reihen bis zur Präzision $\operatorname{prec}(\ell, n)$ berechnet sind, werden insgesamt
$$O(\operatorname{prec}(\ell, n)\, \mathsf{M}(\operatorname{prec}(\ell, n))) = \tilde{O}((v + e_\Delta)^2 \ell^2)$$

Multiplikationen in $\mathbb{Z}$ benötigt. Dabei benutzen wir erneut die Tatsache, dass wir für die tatsächlichen Rechnungen das in Korollar 3.2.3 angegebene Vielfache von $\tau_{\ell,n}(q)$ verwenden. Die nach Abschluss der Rechnungen noch notwendigen $\mathrm{prec}(\ell, n)$ Divisionen durch den konstanten Faktor aus Korollar 3.2.3 sind gegenüber den beschriebenen Kosten gleichfalls vernachlässigbar. □

3.3.3 Verwendung von a_ℓ

In [Mül95, S. 66–76] wird eine weitere Modulfunktion $a_\ell(\tau)$ vorgestellt, die als Alternative zu $m_\ell(\tau)$ verwendet werden kann. In der Tat weist das Minimalpolynom $A_\ell(X, j)$ von $a_\ell(\tau)$ einen deutlich geringeren Grad in j und deutlich geringere Koeffizienten auf als $M_\ell(X, j)$, weshalb derartige Polynome laut [Eng09] unter anderem beim Erzielen des damaligen Rekordwertes für das Punktezählen auf elliptischen Kurven [EM06] genutzt wurden.

Bevor wir die Funktion $a_\ell(\tau)$ definieren können, benötigen wir die folgende

Definition 3.3.7. Sei $f(\tau)$ eine Modulfunktion von Gewicht 1 und sei r eine Primzahl. Dann wirkt der r-te Hecke-Operator T_r auf f gemäß

$$T_r(f)(\tau) = \frac{1}{r} \sum_{k=0}^{r-1} f\left(\frac{\tau + k}{r}\right) + f(r\tau).$$

Bemerkung 3.3.8. Dies ist ein Spezialfall einer weitaus allgemeineren Definition für Hecke-Operatoren, die man beispielsweise in [Ser73, S. 98–100] finden kann. In [Hec37] zeigte Hecke verschiedene wichtige Eigenschaften dieser bereits zuvor bekannten Operatoren und benutzte sie erstmals, um Aussagen über Modulfunktionen zu beweisen.

Lemma 3.3.9. *[Mül95, S. 74] Sei $\ell > 3$, $s = \frac{24}{\mathrm{ggT}(24,\ell+1)}$ und sei r eine ungerade Primzahl mit*

$$s \mid r - 1, \quad \left(\frac{r}{\ell}\right) = 1, \quad \left(\frac{\ell}{r}\right) = 1.$$

Dann ist die Funktion

$$a_\ell(\tau) = \frac{T_r(\eta(\tau)\eta(\ell\tau))}{\eta(\tau)\eta(\ell\tau)} \tag{3.9}$$

eine auf $\mathbb{H}$ holomorphe Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$. Weiterhin ist $a_\ell(\tau)$ invariant unter w_ℓ.

Für die tatsächlichen Rechnungen unter Verwendung von $a_\ell(\tau)$ benötigen wir zunächst deren Laurentreihe bis zur erforderlichen Präzision. Zu ihrer Bestimmung benutzen wir Formel (2.5) für die Laurentreihe der η-Funktion und bedienen uns anschließend der folgenden

Proposition 3.3.10. *[Mül95, S. 74] Sei die Laurentreihe einer Funktion $a(\tau)$ gegeben als*

$$a(\tau) = \exp\left(2\pi i \tau \frac{z}{s}\right) \sum_{k=0}^{\infty} a_k \exp(2\pi i k \tau)$$

mit $\mathrm{ggT}(z,s)=1$. *Dann gilt*

$$T_r(a(\tau)) = \exp\left(2\pi i\tau\frac{z}{s}\right)\left(\sum_{\substack{k=0\\ r\mid ks+z}}^{\infty} a_k \exp\left(2\pi i\tau\frac{ks+(1-r)z}{rs}\right) + \sum_{k=0}^{\infty} a_k \exp\left(2\pi i\tau kr+\frac{(r-1)z}{s}\right)\right). \tag{3.10}$$

Wir schreiben nun $v = v(a_\ell) := -\operatorname{ord}(a_\ell)$. Wie man leicht nachrechnet, ergibt sich nach Bestimmung der Werte s,z,r aus der Kongruenz $ks+z\equiv 0 \mod r$, dass $v=0$ für $\ell<29$ sowie für $\ell\in\{37,43,67,163\}$ gilt. Das Minimalpolynom $A_\ell(X,j)$ von a_ℓ weist nach [Mül95, S. 77] den Grad $2v$ in j auf. Für diese Werte von ℓ ist der Grad in j also 0. Folglich ist $a_\ell(\tau)\in\mathbb{C}$ und für diese (vorwiegend kleinen) Werte von ℓ kann die Funktion a_ℓ nicht wie gewünscht verwendet werden, sodass in diesem Fall keine Alternative zur Verwendung von m_ℓ besteht.

Zur Bestimmung des Minimalpolynoms von $a_\ell(\tau)$ verwenden wir den in [Mül95, S. 79] vorgestellten Algorithmus. Im Sonderfall $v=1$, d. h. für $\ell\in\{29,31,41,47\}$ kann dieser deutlich vereinfacht werden, diesbezügliche Überlegungen finden sich in [Mor95, S. 267].

Versuchen wir, die Methode zur Bestimmung des rationalen Ausdrucks aus Abschnitt 3.3.2 zu übertragen und dabei statt $m_\ell(\tau)$ die Funktion $a_\ell(\tau)$ zu verwenden, stoßen wir auf ein Problem: Gemäß Proposition 2.1.21 ist nämlich der Zähler des rationalen Ausdrucks unter Verwendung von a_ℓ wegen $\deg_j(A_\ell)=2v$ aus Monomen der Form $a_\ell^i j^k$ mit $0\leqslant k\leqslant 2v-1$ zusammengesetzt. Offenbar gilt aber $\operatorname{ord}(a_\ell^i j^k) = -iv-k = \operatorname{ord}(a_\ell^{i-1}j^{k+v})$, falls $k<v$ ist. Somit gibt es stets zwei Monome derselben Ordnung. Daher können nicht wie in Algorithmus 3 die Koeffizienten der verschiedenen Monome sukzessiv berechnet werden, da das zugrundeliegende lineare Gleichungssystem nicht mehr die Form einer Dreiecksmatrix aufweist. Selbstverständlich kann das System weiter durch Invertieren der Matrix gelöst werden, der Rechenaufwand dafür ist jedoch bedeutend höher.

Um dieses Problems Herr zu werden, benutzen wir folgendes

Lemma 3.3.11. *Sei $f(\tau)$ eine unter w_ℓ anti-invariante Funktion, d. h., es gelte $f^*=-f$. Sei $g(\tau)\in\mathbf{A}_0(\Gamma_0(\ell))$ unter w_ℓ nicht invariant. Dann gilt*

$$g(\tau) = \frac{g(\tau)+g^*(\tau)}{2} + \frac{(g(\tau)-g^*(\tau))f(\tau)}{2f(\tau)} =: g^{(1)}(\tau) + \frac{g^{(2)}(\tau)}{f(\tau)},$$

sofern $f(\tau)\neq 0$ gilt, und $g^{(1)}(\tau), g^{(2)}(\tau)$ sind unter w_ℓ invariant.

Beweis. Die Invarianz unter w_ℓ ist offensichtlich, denn es gilt

$$w_\ell(g(\tau)+g^*(\tau)) = g^*(\tau)+g(\tau), \quad w_\ell(g(\tau)-g^*(\tau)) = -(g(\tau)-g^*(\tau)),$$

woraus nach der Voraussetzung an f die Behauptung folgt. □

Um den rationalen Ausdruck für $\tau_{\ell,n}(q)$ zu bestimmen, gehen wir nun wie folgt vor:

Algorithmus 4. Bestimmung des rationalen Ausdrucks für $\tau_{\ell,n}$ mit a_ℓ

Eingabe: $\ell, n, \mathrm{prec}(\ell, n)$
Ausgabe: Rationaler Ausdruck für $\tau_{\ell,n}(q)$

1. Bestimme $g \in \mathbf{A}_0(\Gamma_0(\ell))$ mit $g^* = -g$.
2. Bestimme $\tau_{\ell,n}$ und $\tau^*_{\ell,n}$ mit Algorithmus 1 sowie den Formeln (2.1)-(2.8), (2.19) und (3.6) bis zur Präzision $\mathrm{prec}(\ell, n)$.
3. Berechne $\tau^{(1)}_{\ell,n}, \tau^{(2)}_{\ell,n}$ gemäß Lemma 3.3.11.
4. Bestimme für beide Funktionen einen rationalen Ausdruck R_1, R_2 in Abhängigkeit von a_ℓ und j.
5. Berechne $\tau_{\ell,n} := R_1(a_\ell, j) + \frac{R_2(a_\ell, j)}{g}$.

Wir müssen noch genauer angeben, wie wir die Schritte 1 und 4 realisieren. Bezüglich der Bestimmung von g bemerken wir, dass $g(\tau) := m^*_\ell(\tau) - m_\ell(\tau)$ unter w_ℓ anti-invariant ist und daher die gewünschten Bedingungen erfüllt. Zudem besitzt es eine relativ kleine Ordnung, was aus Komplexitätsgründen relevant ist. Weiterhin gilt offenbar für jedes g mit den geforderten Eigenschaften $w_\ell(g^2) = g^2$. Daher können wir mit Algorithmus 5 einen rationalen Ausdruck in Abhängigkeit von a_ℓ und j für g^2 berechnen. Den Wert für g selbst erhält man auf der konkreten elliptischen Kurve, wie dies in Abschnitt 4.3 ausgeführt wird.

Bevor wir einen Algorithmus für Schritt 4 angeben, untersuchen wir zunächst ähnlich wie in Abschnitt 3.3.2 die Ordnungen verschiedener Laurentreihen.

Lemma 3.3.12. *Sei $A_\ell(X, j)$ das Minimalpolynom von a_ℓ, sodass gemäß [Mül95, S. 77]*

$$0 = A_\ell(a_\ell, j) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{2v} a_{i,k} a_\ell^i j^k$$

mit $a_{i,k} \in \mathbb{Z}$ gilt, wobei $\mathrm{ord}(a_\ell) = -v$ ist. Dann gelten folgende Aussagen:

1. $\mathrm{ord}\left(\frac{\partial}{\partial Y} A_\ell(a_\ell, j)\right) \geqslant -(\ell+1)v + 1$.
2. $\mathrm{ord}\left(\frac{\partial}{\partial Y} A_\ell(a_\ell, j(q^\ell))\right) \geqslant -(2v-1)\ell$.

Beweis. 1. Wir betrachten zunächst, welche Koeffizienten von A_ℓ nicht verschwinden und gehen dafür analog zu Lemma 3.3.1 vor. Es gilt $\mathrm{ord}(a_\ell^i j^k) = -iv - k$. Suchen wir zwei Summanden $a_\ell^{i_1} j^{k_1}$, $a_\ell^{i_2} j^{k_2}$ mit gleicher Ordnung, so führt dies auf die Gleichung

$$(i_2 - i_1)v = (k_1 - k_2).$$

Da dies $v \mid k_1 - k_2$ impliziert, hat diese Gleichung abhängig vom Wert von k_1, k_2 die Lösungen $(i, 0), (i-1, v), (i-2, 2v)$ bzw. $(i, k), (i-1, k+v)$ für $0 < k < v$. Unter Beachtung der Einschränkungen an mögliche Werte von i und k ergibt sich direkt, dass $\mathrm{ord}(a_\ell^i j^k) \geqslant -(\ell+1)v$ für alle Summanden mit nicht verschwindenden Koeffizienten gelten muss. Somit ergibt sich

$$a_{i,k} \neq 0 \quad \Rightarrow \quad -iv - k \geqslant -(\ell+1)v. \tag{3.11}$$

Nun untersuchen wir

$$\frac{\partial}{\partial Y} A_\ell(a_\ell, j) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{2v-1} (k+1) a_{i,k+1} a_\ell^i j^k.$$

Aus (3.11) folgt sofort

$$a_{i,k+1} \neq 0 \quad \Rightarrow \quad -iv-(k+1) \geqslant -(\ell+1)v \quad \Rightarrow \quad \operatorname{ord}(a_\ell^i j^k) = -iv-k \geqslant -(\ell+1)v+1.$$

2. Für den Beweis der zweiten Behauptung gehen wir analog vor. Durch Anwendung von w_ℓ erhalten wir

$$0 = A_\ell(a_\ell^*, j^*) = A_\ell(a_\ell, j(q^\ell)) = \sum_{i=0}^{\ell+1} \sum_{k=0}^{2v} a_{i,k} a_\ell^i j(q^\ell)^k.$$

Hier gilt $\operatorname{ord}(a_\ell^i j(q^\ell)^k) = -iv - k\ell$ und wir erhalten durch einfache Überlegungen

$$a_{i,k} \neq 0 \quad \Rightarrow \quad -iv - k\ell \geqslant -2v\ell \tag{3.12}$$

und damit

$$a_{i,k+1} \neq 0 \quad \Rightarrow \quad -iv-(k+1)\ell \geqslant -2v\ell \quad \Rightarrow \quad \operatorname{ord}(a_\ell^i j(q^\ell)^k) = -iv - k\ell \geqslant -(2v-1)\ell.$$

□

Korollar 3.3.13. *Die Modulfunktion $a_\ell : \mathbb{H} \to \mathbb{C}$ ist surjektiv.*

Beweis. Unter Benutzung von (3.12) sehen wir sofort $a_{i,2v} = 0$ für $i > 0$. Weiterhin implizieren die Überlegungen aus [Mül95, S. 77], dass $a_{0,2v} \neq 0$ gilt. Damit ergibt sich, dass $A_\ell(c, Y)$ für $c \in \mathbb{C}$ ein Polynom in Y von Grad $2v$ ist. Wegen der Surjektivität der j-Invariante existiert ein $\tau \in \mathbb{H}$ mit $A_\ell(c, j(\tau)) = 0$. Somit ist nach Definition von $A_\ell(X, Y)$ für eine der in Lemma 2.1.16 eingeführten Transformationen S_k die Identität $c = a_\ell(S_k\tau)$ erfüllt und a_ℓ also surjektiv. □

Sei nun $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))$ holomorph und unter w_ℓ invariant. Gemäß Proposition 2.1.21 gilt dann für ein Polynom $Q \in \mathbb{C}[X, Y]$ mit $\deg_Y(Q) < 2v$

$$f(\tau)\frac{\partial}{\partial Y} A_\ell(a_\ell, j) = Q(a_\ell, j) \quad \text{sowie} \quad f(\tau)\frac{\partial}{\partial Y} A_\ell(a_\ell, j(q^\ell)) = Q(a_\ell, j(q^\ell)), \tag{3.13}$$

wobei die zweite Gleichung durch Anwendung von w_ℓ auf die erste entsteht. Zur Bestimmung des rationalen Ausdrucks unter Verwendung von a_ℓ und j benutzen wir daher den folgenden

Algorithmus 5. Bestimmung des rationalen Ausdrucks für $f(\tau)$ mit a_ℓ

Eingabe: $\ell, n, f(\tau)$

Ausgabe: $Q(X, Y) = \sum_i \sum_k q_{i,k} X^i Y^k$ aus Gleichung (3.13)

1. Setze $Q := 0$, $\operatorname{prec}(\ell, n) := -\operatorname{ord}(f) + (\ell+1)v$.
2. Berechne $a_\ell(q)$, $j(q)$ mit den Formeln (2.1)-(2.4), (2.5), (3.9) und (3.10) bis zur Präzision $\operatorname{prec}(\ell, n)$.
3. Berechne $A_\ell(X, Y)$ mit Algorithmus 5.26 aus [Mül95].

4. Berechne $s_1 := f(\tau)\frac{\partial}{\partial Y}A_\ell(a_\ell, j)$, $s_2 := f(\tau)\frac{\partial}{\partial Y}A_\ell(a_\ell, j(q^\ell))$ bis zur Präzision $\mathrm{prec}(\ell, n)$.
5. Setze $p_1 := \mathrm{ord}(s_1)$, $p_2 := \mathrm{ord}(s_2)$.
6. **while** $s_1 \neq 0$ **do**
7. $o_1 := p_1, o_2 := p_2$.
8. **while** $p_1 < o_1 + \ell - 1$ **do**
9. Bestimme $(i_1, k_1), (i_2, k_2)$ mit $\mathrm{ord}(a_\ell^{i_s} j^{k_s}) = p_1$, $s = 1, 2$, mit $0 \leqslant k_1 < v$, $k_2 = k_1 + v$.
10. Berechne $s_1 := s_1 - q_{i_2,k_2} a_\ell^{i_2} j^{k_2}$.
11. Berechne $s_1 := s_1 - \frac{\mathrm{lk}(s_1)}{\mathrm{lk}(a_\ell^{i_1} j^{k_1})} a_\ell^{i_1} j^{k_1}$. Setze $Q := Q + \frac{\mathrm{lk}(s_1)}{\mathrm{lk}(a_\ell^{i_1} j^{k_1})} X^{i_1} Y^{k_1}$.
12. $p_1 := p_1 + 1$.
13. **end while**
14. **while** $p_2 < o_2 + \ell - 1$ **do**
15. Bestimme $(i_1, k_1), (i_2, k_2)$ mit $\mathrm{ord}(a_\ell^{i_s} j(q^\ell)^{k_s}) = p_2$, $s = 1, 2$, mit $0 \leqslant k_1 < v$ und $k_2 = k_1 + v$.
16. Berechne $s_2 := s_2 - q_{i_1,k_1} a_\ell^{i_1} j(q^\ell)^{k_1}$.
17. Berechne $s_2 := s_2 - \frac{\mathrm{lk}(s_2)}{\mathrm{lk}(a_\ell^{i_2} j(q^\ell)^{k_2})} a_\ell^{i_2} j(q^\ell)^{k_2}$. Setze $Q := Q + \frac{\mathrm{lk}(s_2)}{\mathrm{lk}(a_\ell^{i_2} j(q^\ell)^{k_2})} X^{i_2} Y^{k_2}$.
18. $p_2 := p_2 + 1$.
19. **end while**
20. **end while**
21. Gib Q aus.

Die Idee des Algorithmus besteht darin, abwechselnd die beiden Gleichungen $s_1 = Q(a_\ell, j)$ sowie $s_2 = s_1^* = Q(a_\ell, j^*)$ zu betrachten. Aufgrund der Einschränkungen an die Ordnungen der Laurentreihen können jeweils $\ell - 1$ Koeffizienten durch sukzessive Eliminierung berechnet werden, da jeweils für einen der zwei Summanden mit gleicher Ordnung der Koeffizient entweder bereits bekannt ist oder verschwindet. Im Detail zeigt dies

Lemma 3.3.14. *Algorithmus 5 arbeitet korrekt.*

Beweis. Um dies zu beweisen, müssen wir folgendes zeigen:

1. Die angegebene Präzision ist ausreichend, um das Polynom Q zu finden.
2. Die in Schritt 10 bzw. 16 verwendeten Koeffizienten q_{i_2,k_2} bzw. q_{i_1,k_1} wurden bereits berechnet, sofern sie nicht verschwinden.

Zum ersten Punkt bemerken wir erneut, dass gemäß Proposition 2.1.21 $Q(X, Y)$ unter Verwendung von a_ℓ ein Polynom ist und also nur positive Potenzen von a_ℓ umfasst. Daher gilt für die Ordnung o seiner Summanden

$$\mathrm{ord}\left(f(\tau)\frac{\partial}{\partial Y}A_\ell(a_\ell, j)\right) = \mathrm{ord}(f) - (\ell + 1)v + 1 \leqslant o \leqslant 0, \tag{3.14}$$

wobei die Gleichheit nach Lemma 3.3.12 folgt. Da der Wert p_1, der über die Ordnung von s_1 iteriert, bei jedem Durchlauf von Schleife 8 echt größer wird, ist die angegebene Präzision

$$\mathrm{prec}(\ell, n) = -\mathrm{ord}(f) + (\ell + 1)v$$

ausreichend.
Zur zweiten Frage bemerken wir zunächst, dass gemäß Lemma 3.3.12 nach t Iterationen von

Schleife 6

$$o_1 \geqslant o_1(t) := \operatorname{ord}(f) - (\ell+1)v + 1 + (\ell-1)t, \quad o_2 \geqslant o_2(t) := \operatorname{ord}(f) - (2v-1)\ell + (\ell-1)t$$

gilt. Weiterhin sieht man durch Nachrechnen $o_1(t) = o_2(t) + (\ell-1)(v-1)$. In Schritt 9 gelte für p_1 nun $o_1(t) \leqslant p_1 = -i_2 v - k_2 < o_1(t) + \ell - 1$. Daraus ergibt sich mit $k_2 = k_1 + v$

$$\begin{aligned} & o_1(t) - (\ell-1)k_2 \leqslant -i_2 v - k_2\ell < o_1(t) - (\ell-1)(k_2-1) \\ \overset{k_2=k_1+v}{\Rightarrow} \; & o_2(t) - (\ell-1)(k_1+1) \leqslant -i_2 v - k_2\ell < o_2(t) - (\ell-1)k_1. \end{aligned}$$

Wegen $k_1 \geqslant 0$ muss also bereits in einer früheren Iteration $-i_2 v - k_2\ell = p_2$ gegolten haben, sofern der Koeffizient nicht a priori verschwindet (falls $o_2(t) - (\ell-1)k_1 \leqslant o_2(0)$ gilt). Damit ist der Koeffizient q_{i_2,k_2} bereits bekannt.
Analog gelte in Schritt 15 $o_2(t) \leqslant p_2 = -i_1 v - k_1\ell < o_2(t) + \ell - 1$. Damit folgt

$$\begin{aligned} & o_2(t) + (\ell-1)k_1 \leqslant -i_1 v - k_1 < o_2(t) + (\ell-1)(k_1+1) \\ \Rightarrow \quad & o_1(t) + (\ell-1)(k_1+1-v) \leqslant -i_1 v - k_1 < o_1(t) + (\ell-1)(k_1+2-v). \end{aligned}$$

Wegen $k_1 \leqslant v-1$ gilt $k_1 + 2 - v \leqslant 1$ und damit muss spätestens in der $t+1$-ten Iteration $-i_1 v - k_1 = p_1$ gelten. Da Schleife 8 mit den Rechnungen zu s_1 vor Schleife 14 ausgeführt wird, ist der Koeffizient q_{i_1,k_1} bereits bekannt, sofern er nicht verschwindet. □

Zur Berechnung des rationalen Ausdrucks unter Verwendung von a_ℓ wenden wir nun Algorithmus 5 auf die Funktionen $\tau^{(1)}_{\ell,n}, \tau^{(2)}_{\ell,n}$ an. Aus Lemma 3.3.3 folgt dabei

$$\operatorname{ord}\left(\tau^{(1)}_{\ell,n}\right) \geqslant n - \ell e_\Delta, \quad \operatorname{ord}\left(\tau^{(2)}_{\ell,n}\right) \geqslant n - \ell e_\Delta - \operatorname{ord}(m_\ell). \tag{3.15}$$

Korollar 3.3.15. *Algorithmus 5 berechnet Q mit $\tilde{O}((v+e_\Delta)^2\ell^2)$ Multiplikationen in $\mathbb{Z}$.*

Beweis. Der Beweis verläuft analog zu demjenigen von Korollar 3.3.6. In jedem Durchlauf von Schleife 8 wird die Ordnung von s_1 nach Konstruktion des Algorithmus echt kleiner, weshalb die Schleife höchstens $\operatorname{prec}(\ell,n)$-mal durchlaufen wird. Weiterhin sind wiederum bei jedem Durchlauf von Schleife 8 und 14 eine konstante Menge von Multiplikationen erforderlich, wenn einige Zwischenergebnisse gespeichert werden. Wir bemerken, dass zur effizienten Implementierung aufgrund der Werte, die i und k in Schleife 14 annehmen, ein etwas geschickteres Vorgehen als bei Algorithmus 3 vonnöten ist. Mit

$$\operatorname{prec}(\ell,n) = \ell e_\Delta - n + \operatorname{ord}(m_\ell) + (\ell+1)v = O(\ell(e_\Delta + v)) \tag{3.16}$$

gemäß (3.15) und Schritt 1 des Algorithmus folgt die Behauptung analog zu Korollar 3.3.6. □

3.3.4 Weitere Betrachtungen

Sowohl Proposition 3.3.4 als auch Lemma 3.3.14 zeigen, dass die für das Auffinden des rationalen Ausdrucks notwendige Präzision und damit die Laufzeit aller Teilrechnungen vom Wert v abhängt. Neben den in [Mül95] ausführlich untersuchten und im Kontext des Punktezählens (vgl. [Eng09]) vielfältig verwendeten Funktionen m_ℓ und insbesondere a_ℓ ist auch

der Einsatz weiterer Alternativen denkbar. Einen gemäß kurzer Erwähnung im Text auf einer Idee von Atkin beruhenden Ansatz zur Bestimmung anderer Funktionen findet man in [Mor95, S. 262–265]. Die dort vorgestellte Methode ist insbesondere deshalb interessant, weil mit ihr gezielt eine Modulfunktion $f_\ell(q)$ von Gewicht 0 für $\Gamma_0(\ell)$ gefunden werden kann, für die $v = -\operatorname{ord}(f_\ell)$ minimal für das gegebene ℓ ist. Nach der Bestimmung einer derartigen Funktion kann ihr Minimalpolynom mit den verschiedenen Ansätzen aus demselben Artikel oder den Ideen aus [Mül95, S. 76–79] berechnet werden. Aus [Mül95, S. 77] folgt wiederum, dass der Grad des Minimalpolynoms in j maximal $2v$ ist. In der Praxis ist das Verfahren aus [Mor95] jedoch nicht verwendet worden, da es relativ kompliziert ist und sich daraus schlecht ein allgemeiner Algorithmus ableiten lässt.
Bei der Verwendung des von Morain vorgestellten Vorgehens folgt direkt aus der Konstruktion und den Formeln in [Mor95, S. 257–258] und [Maz77, S. 98], dass

$$v \leqslant 2\left(\frac{g(\ell)+1}{2} - \frac{a(\ell)}{4}\right) - 1 = g(\ell) - \frac{a(\ell)}{2} \tag{3.17}$$

gilt. Dabei bezeichnet $g(\ell)$ das Geschlecht der riemannschen Fläche $X_0(\ell) = \mathbb{H}^*/\Gamma_0(\ell)$ (für $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$) mit $g(\ell) = \frac{\ell}{12} + O(1)$ (vgl. [Mor95, S. 257] und [Sch74, S. 100–103]), während $a(\ell) = c \cdot h(-\ell)$ mit $h(-\ell) = h(\mathbb{Q}(\sqrt{-\ell}))$ und $c \in \{1, 2, 4\}$ von ℓ abhängig ist [Mor95, S. 258]. Nach der Klassenzahlformel für imaginär-quadratische Zahlkörper, die man etwa in [Rib01, S. 574] findet, gilt

$$h(-\ell) = \frac{w\sqrt{|\delta|}}{2\pi} L(1, \chi_\ell),$$

wobei w die Anzahl der Einheitswurzeln in $\mathbb{Q}(\sqrt{-\ell})$ und $\delta \in \{\ell, 4\ell\}$ die Diskriminante dieses Körpers bezeichnet sowie χ_ℓ ein bestimmter dem Körper zugeordneter Charakter ist. Für Primzahlen $\ell > 3$ ist $w = 2$. Weiterhin gilt $L(1, \chi_\ell) = O(\log \ell)$, wie man leicht durch partielle Summation zeigt. Insgesamt erhält man also die Abschätzung

$$h(-\ell) = O(\sqrt{\ell} \log \ell)$$

und mit (3.17) ergibt sich asymptotisch

$$v \leqslant \frac{\ell}{12} + O(\sqrt{\ell} \log \ell).$$

Bemerkung 3.3.16. Die Überlegungen liefern eine obere Schranke an den Wert von v, wenn die genannten Methoden zur Konstruktion von $f_\ell(q)$ verwendet werden. In der Praxis liegen die Werte, die man für v erhält, jedoch schon bei Verwendung von a_ℓ deutlich unter dieser groben oberen Schranke. In [Abr96] wird weiterhin

$$v \geqslant \frac{7}{800}\ell \tag{3.18}$$

als untere Schranke für die bestmöglichen Werte gezeigt.

4 Punktezählen im Elkies-Fall

4.1 Bestimmung des Eigenwerts

Um mittels der vorberechneten universellen elliptischen Gauß-Summen $\tau_{\ell,n}(q)$ die Ordnung der Gruppe der Punkte auf einer konkreten elliptischen Kurve $E : Y^2 = X^3 + aX + b$ über einem Körper $\mathbb{F}_p$ zu bestimmen, erinnern wir an einige Aussagen aus Abschnitt 1.2.

Wir nehmen im Folgenden an, dass die j-Invariante der betrachteten Kurve E verschieden von 0 und 1728 ist, und betrachten Elkies-Primzahlen ℓ, für die die charakteristische Gleichung

$$\phi_p^2 - t\phi_p + p = 0$$

des Frobenius-Homomorphismus ϕ_p gemäß Abschnitt 1.2.2 über $\mathbb{F}_\ell$ in Linearfaktoren zerfällt. Wie üblich bezeichnen wir einen Teiler von $\ell - 1$ mit n und $\chi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mu_n$ ist ein Charakter von Ordnung n. Weiter sei λ ein Eigenwert von ϕ_p modulo ℓ, womit direkt

$$t \equiv \lambda + \frac{p}{\lambda} \mod \ell$$

folgt. Mithilfe der in Gleichung (1.9) eingeführten elliptischen Gauß-Summen

$$G_{\ell,n,\chi}(E) = \sum_{a=1}^{\ell-1} \chi(a)(aP)_V$$

aus [Mih06c], wobei P ein ℓ-Torsionspunkt auf E ist und $V = y$ für gerades sowie $V = x$ für ungerades n gilt, erhalten wir nach [Mih06c] die bereits in Gleichung (1.11) angeführte Identität

$$\frac{G_{\ell,n,\chi}(E)^m}{G_{\ell,n,\chi^m}(E)}(G_{\ell,n,\chi}(E)^n)^q = \chi^{-m}(\lambda), \tag{4.1}$$

wobei $p = nq + m$ mit $0 \leqslant m < n$ gilt.

Aus den Berechnungen der universellen elliptischen Gauß-Summen in Abschnitt 3 ist nun der Wert

$$\tau_{\ell,n}(q) = \frac{G_{\ell,n,\chi}(q)^n p_1^r(q)}{\Delta(q)^{e_\Delta}} \tag{4.2}$$

gemäß Gleichung (3.4) bzw. (3.13) als rationaler Ausdruck $R(m_\ell(q), j(q))$ bzw. $R(a_\ell(q), j(q))$ in den entsprechenden Laurentreihen bekannt, wobei r und e_Δ wie in Korollar 2.2.10 definiert sind.

Wir liften die betrachtete Kurve $E/\mathbb{F}_p$ mittels Satz 1.1.8 zu ihrem Deuring-Lift E_0 über einem Zahlkörper K. Dann gibt es ein Primideal $\mathfrak{P} \subset \mathcal{O}_K$ mit $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_p$, sodass die durch Reduktion modulo $\mathfrak{P}$ entstehende elliptische Kurve nicht-singulär und isomorph zu E ist. Nun übertragen wir die unter Verwendung der Tate-Kurve berechnete Darstellung für $\tau_{\ell,n}(q)$ durch die Spezialisierung $q \mapsto q(\tau) = \exp(2\pi i\tau)$, wobei τ den zu E_0/K gehörigen Wert τ aus Satz 2.2.3 bezeichnet, auf die spezielle Kurve $E_{q(\tau)}$. Anschließend benutzen wir den in Satz 2.2.7 definierten Isomorphismus $\psi : E_{q(\tau)} \xrightarrow{\sim} E_0$. Berücksichtigen wir dabei den Übergang von

der multiplikativen zur additiven Struktur (vgl. Satz 2.2.7), so sehen wir für $a \in \mathbb{Z}$

$$\psi(x(\zeta_\ell^a, q(\tau))) = (aP)_x, \quad \psi(y(\zeta_\ell^a, q(\tau))) = (aP)_y$$

für einen ℓ-Torsionspunkt P auf E_0. Weiterhin entspricht $\Delta(q) = \Delta(E_q)$ (s. Satz 2.2.7) dem Wert $\Delta(E_0)$ sowie $j(q) = j(E_q)$ der Größe $j(E_0)$. Damit folgt $\psi(G_{\ell,n,\chi}(q(\tau))) = G_{\ell,n,\chi}(E_0)$ und wir können die allgemein berechnete rationale Darstellung von $\tau_{\ell,n}$ für die Bestimmung der elliptischen Gauß-Summe $G_{\ell,n,\chi}(E_0)$ und, wie in den folgenden Abschnitten gezeigt wird, auch $G_{\ell,n,\chi}(E)$ verwenden.

4.2 Verwendung von m_ℓ

Da in den Fällen, die für uns von Interesse sind, $\ell = O(\log p)$ gilt, schließt man aus der Aussage von Korollar 3.2.3 über die Koeffizienten des Ausdrucks, dass deren Nenner modulo p invertierbar sind und also alle Rechnungen auch modulo p reduziert werden können. Bei Verwendung von m_ℓ erhalten wir somit schließlich durch Reduktion modulo dem Primideal $\mathfrak{P} \mid (p)$ die Formel

$$\frac{G_{\ell,n,\chi}(E)^n p_1(E)^r}{\Delta(E)^{e_\Delta}} = R(m_\ell(E), j(E)) \tag{4.3}$$

auf $E/\mathbb{F}_p$. Die einzelnen Größen sind nun die der untersuchten Kurve E zugehörigen. Mithilfe der Formeln (1.1) und (1.2) für $\Delta(E)$ und $j(E)$ sowie der Formeln (vgl. insbesondere [Mül95, S. 99])

$$E_2^* = -\frac{12E_6DJ}{sE_4DF}, \tag{4.4}$$

$$p_1(E) = -\ell E_2^* \tag{4.5}$$

mit gemäß [Mül95, S. 91]

$$E_4 = -\frac{a}{3}, \qquad E_6 = -\frac{b}{2},$$
$$DF = m_\ell(E)\frac{\partial M_\ell}{\partial X}(m_\ell(E), j(E)),$$
$$DJ = j(E)\frac{\partial M_\ell}{\partial Y}(m_\ell(E), j(E)),$$

womit man durch Einsetzen

$$E_2^* = -18\frac{bDJ}{saDF}$$

erhält, können diese Größen auf E bestimmt werden.

Bemerkung 4.2.1. Beim üblichen Verfahren für Elkies-Primzahlen wird aus dem Wert von $p_1(E)$ das bereits in Abschnitt 1.2.2 erwähnte Polynom $F_{\ell,\lambda}(X)$ berechnet, dessen Nullstellen genau die x-Koordinaten der Punkte sind, die im Kern der $m_\ell(E)$ entsprechenden ℓ-Isogenie $\psi : E \to E'$ (s. Abschnitt 1.2.2) liegen, und das damit das Divisionspolynom $\psi_\ell(X)$ teilt. Eine ausführliche Darstellung dieser Rechnungen findet sich in [Mül95, S. 89–106].
Wir bemerken noch, dass in [Mül95, Mor95] et al. die Konvention

$$p_1(E) = -\frac{\ell}{2}E_2^*$$

benutzt wird. Der Unterschied zu (4.5) ergibt sich daraus, dass wir gemäß Formel (2.15) bei der Berechnung von p_1 auf der Tate-Kurve über die ganze Gruppe $\mathbb{F}_\ell^*$ summieren, während in [Mül95, Mor95] über $\mathbb{F}_\ell^*/\{-1,1\}$ summiert wird.

Zur Bestimmung von $p_1(E)$ muss offenbar zunächst der Wert von $m_\ell(E)$ ermittelt werden. Nach Definition ist $m_\ell(E)$ eine Nullstelle des Polynoms $M_\ell(X, j(E))$, es gilt

$$M_\ell(m_\ell(E), j(E)) = 0.$$

Liegt das Polynom $M_\ell(X, Y)$ vor, so muss also lediglich für die Variable Y der zuvor berechnete Wert von $j(E)$ eingesetzt werden, um $m_\ell(E)$ zu erhalten. Ist ℓ eine Elkies-Primzahl, so liegt $m_\ell(E)$ in $\mathbb{F}_p$ und kann daher als Nullstelle von $\mathrm{ggT}(X^p - X, M_\ell(X, j(E)))$ bestimmt werden. Die möglichen Werte für $m_\ell(E)$ entsprechen den unter ϕ_p invarianten Untergruppen von $E[\ell]$, die wiederum mit den beiden Eigenwerten λ und μ von ϕ_p korrespondieren (vgl. Abschnitt 1.2.2). Da das Polynom $M_\ell(X, j(E))$ laut [Mül95, S. 42, 47] keine doppelten Nullstellen besitzt, erhalten wir für Elkies-Primzahlen stets zwei verschiedene mögliche Werte für $m_\ell(E)$.

Nun kann Gleichung (4.3) umgestellt werden zu

$$G_{\ell,n,\chi}(E)^n = \frac{R(m_\ell(E), j(E))\Delta(E)^{e_\Delta}}{p_1(E)^r}. \tag{4.6}$$

Bemerkung 4.2.2.

1. Falls das n-te zyklotomische Polynom über $\mathbb{F}_p$ irreduzibel ist, kann man die Korrektur durch Multiplikationen mit $p_1(E)$, $\Delta(E)$ auf der Kurve auslassen, da diese Werte in $\mathbb{F}_p$ liegen und die letztlich in Gleichung (4.1) betrachteten Einheitswurzeln $\mathbb{F}_p$-linear unabhängig sind. Somit kann insbesondere die recht aufwändige Berechnung von $p_1(E)$ eingespart werden.

2. Als Nenner des rationalen Ausdrucks wird gemäß Proposition 2.1.21 die Größe

$$\frac{\partial M_\ell}{\partial Y}(m_\ell(E), j(E))$$

verwendet. Man beachte, dass dieser Wert in Einzelfällen 0 sein kann, wie auch schon in [Mül95, S. 110] angemerkt. In einem solchen Fall kann mittels des vorliegenden zweiten Wertes für $m_\ell(E)$ der Ausdruck erneut berechnet werden. Ergibt sich wieder der Wert 0, so kann die Primzahl ℓ nicht verwendet werden. In der Praxis ist dieser Fall jedoch nie aufgetreten.

Wir müssen ebenfalls sicherstellen, dass der in Gleichung (4.6) im Nenner auftauchende Wert von p_1 modulo p ungleich Null ist. Da wir Kurven betrachten, deren j-Invarianten ungleich 0 oder 1728 sind, gilt $a \cdot b \neq 0$, woraus direkt $E_4 \cdot E_6 \neq 0$ folgt. Weiterhin kann man zeigen, dass das Absolutglied von $M_\ell(X, j(E))$ den Wert ℓ^s aufweist [EM02, S. 254] und somit modulo p nicht verschwindet. Daher folgt auch $m_\ell(E) \neq 0$ und, weil $M_\ell(X, j(E))$ gemäß [Mül95] keine doppelten Nullstellen besitzt, auch $DF \neq 0$. Damit

kann aus Formel (4.4) geschlossen werden, dass

$$p_1 = 0 \Leftrightarrow \frac{\partial M_\ell}{\partial Y}(m_\ell(E), j(E)) = 0$$

gilt. Sofern der rationale Ausdruck für einen Wert von $m_\ell(E)$ bestimmt werden konnte, kann also auch Formel (4.6) angewendet werden.

Berechnet man nun die q-te Potenz $(G_{\ell,n}(E)^n)^q$, so kann für Primzahlen $p \equiv 1 \mod n$ mit Gleichung (4.1) der Index von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n bestimmt werden. Abschnitt 4.4 zeigt, wie wir diese Gleichung für beliebige große Primzahlen p benutzen können.

4.3 Verwendung von a_ℓ

Gemäß den in Abschnitt 3.3.3 vorgestellten Algorithmen erhalten wir in diesem Fall auf $E/\mathbb{F}_p$ die Formel

$$\frac{G_{\ell,n,\chi}(E)^n p_1(E)^r}{\Delta(E)^{e_\Delta}} = R_1(a_\ell(E), j(E)) + \frac{R_2(a_\ell(E), j(E))}{g(E)}. \tag{4.7}$$

Dabei bestimmen wir $j(E)$ und $\Delta(E)$ wieder mithilfe der Formeln (1.1) und (1.2). Danach erhalten wir $a_\ell(E)$ analog zu $m_\ell(E)$ als Nullstelle des Polynoms $A_\ell(X, j(E))$, es ergeben sich wieder zwei mögliche Werte. Haben wir für Gleichung (4.7) $g = \frac{\ell^s}{m_\ell} - m_\ell$ gewählt und g^2 als rationalen Ausdruck in a_ℓ und j vorberechnet, so erhalten wir durch Einsetzen der Werte $a_\ell(E)$ und $j(E)$ den Wert $g(E)^2$ und daraus durch Wurzelziehen zwei mögliche Werte für $g(E)$. Der korrekte unter den beiden Kandidaten $\pm g(E)$ kann dabei bestimmt werden, indem man die Gleichungen

$$\frac{\ell^s}{x} - x = \pm g(E) \tag{4.8}$$

löst und für alle Lösungen x überprüft, ob sie Nullstellen von $M_\ell(X, j(E))$ sind. Dies liefert gleichzeitig auch den $g(E)$ entsprechenden Wert von $m_\ell(E)$.

Bemerkung 4.3.1. Es wäre auch denkbar, den Wert $g(E)$ direkt aus $m_\ell(E)$ zu berechnen (man beachte, dass gemäß Bemerkung 4.2.2 $m_\ell(E) \neq 0$ gilt). Es zeigt sich jedoch, dass die Bestimmung von $m_\ell(E)$ als Nullstelle von $M_\ell(X, j(E))$ eine deutlich höhere Laufzeit erfordert als der Ansatz, den gewünschten Wert aus dem vorberechneten Ausdruck für g^2 durch Wurzelziehen zu gewinnen.

Anschließend kann der Wert $p_1(E)$ mit Formel (4.4) aus dem Wert von $m_\ell(E)$ oder alternativ mithilfe der Ausführungen in [Mül95, S. 102–106] aus $a_\ell(E)$ bestimmt werden. Letzteres Vorgehen erfordert jedoch die Bestimmung von Nullstellen in $\mathbb{F}_p$ eines Polynoms in $\mathbb{F}_p[X]$ und das Testen mehrerer möglicher Werte, weshalb wir aus Laufzeitgründen die erste Variante vorziehen. Nun können wir Gleichung (4.7) analog zum vorigen Abschnitt umstellen und durch Einsetzen der berechneten Werte die Größe $G_{\ell,n,\chi}(E)^n$ bestimmen.

Bemerkung 4.3.2.

1. Es kann vorkommen, dass beide in (4.8) genannten Gleichungen eine Lösung besitzen, die Nullstelle von $M_\ell(X, j(E))$ ist. So hat für die elliptische Kurve $E : Y^2 = X^3 + 8X + 16$ über $\mathbb{F}_{83}$ mit $j(E) = 44$ das Polynom $M_5(X, j(E))$ in $\mathbb{F}_{83}$ die beiden Nullstellen $m_{5,1}(E) = 23$ und $m_{5,2}(E) = 74$ mit (für $\ell = 5$ ist $s = 3$) $\frac{125}{m_{5,1}(E)} - m_{5,1}(E) = 51 = -\left(\frac{125}{m_{5,2}(E)} - m_{5,2}(E)\right)$.
   In solch einem Fall ergibt sich, wenn man die beiden möglichen Werte für $g(E)$ in Gleichung (4.7) einsetzt, nach $G_{\ell,n,\chi}(E)^n$ umstellt und mit (4.10) weiter rechnet, jedoch

in der Regel auf der rechten Seite von (4.10) nur für den zu $a_\ell(E)$ gehörigen Wert von $m_\ell(E)$ eine Einheitswurzel $\zeta_n^i, 0 \leqslant i < n$, sodass der korrekte Wert von $g(E)$ dennoch bestimmt werden kann. Falls man in beiden Fällen eine Einheitswurzel erhält, ergeben sich für die betrachtete Primzahl ℓ zwei Möglichkeiten für den Wert der Spur $t \mod \ell$, sodass sie nicht verwendet werden sollte.

2. Der als Nenner der verschiedenen rationalen Ausdrücke verwendete Wert

$$\frac{\partial A_\ell}{\partial Y}(a_\ell(E), j(E))$$

kann erneut in Einzelfällen verschwinden. Wir verwenden dann wie schon für m_ℓ beschrieben den zweiten möglichen Wert für $a_\ell(E)$. Die gleichen Aussagen treffen auf $g(E) = \frac{\ell^s}{m_\ell(E)} - m_\ell(E)$ zu. Beispielsweise hat die Kurve $E : Y^2 = X^3 + 125X + 125$ über $\mathbb{F}_{131}$ die j-Invariante $j(E) = 62$ und für $\ell = 5$ ist eine Nullstelle von $M_\ell(X, j(E))$ durch $m_\ell(E) = 16$ gegeben, für die $g(E) = 0$ gilt, bei Verwendung der zweiten Nullstelle $m_\ell(E) = 101$ ergibt sich jedoch $g(E) = 4$.

4.4 Jacobi-Summen

4.4.1 Definition

Um den Ansatz aus [Mih06c] allgemein benutzen zu können, müssen gemäß Gleichung (4.1) auch die Jacobi-Summen $\frac{G_{\ell,n,\chi}(E)^m}{G_{\ell,n,\chi^m}(E)}$ bestimmt werden. Wie man analog zu den Aussagen in Korollar 2.2.9 zeigen kann, ist der Ausdruck $\frac{G_{\ell,n,\chi}(q)^m}{G_{\ell,n,\chi^m}(q)}$ ebenfalls eine Modulfunktion für $\Gamma_0(\ell)$, aus der man wie in Korollar 2.2.10 mithilfe von $p_1(q)$ und $\Delta(q)$ eine Modulfunktion von Gewicht 0 konstruieren kann. Anders als der in Korollar 2.2.10 definierte Ausdruck für die universellen elliptischen Gauß-Summen ist diese Funktion jedoch nicht holomorph auf $\mathbb{H}$, da $G_{\ell,n,\chi^m}(q)$ hier Nullstellen besitzt, weshalb der Nenner der rationalen Darstellung zusätzlich durch ein Polynom in j teilbar ist.

Wir können dieses Problem jedoch umgehen, indem wir die Schlüsselgleichung (4.1) leicht umformen. Dazu bemerken wir, dass mit $m' = n - m$

$$p = n(q+1) - m', \quad m \equiv -m' \mod n \tag{4.9}$$

gilt, womit wir die neue Gleichung

$$\chi^{-m}(\lambda) = \frac{(G_{\ell,n,\chi}(E)^n)^{q+1}}{G_{\ell,n,\chi}(E)^{m'} G_{\ell,n,\chi^{-m'}}(E)} \tag{4.10}$$

erhalten. Aus dem Beweis von Korollar 2.2.9 ist bekannt, dass für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\ell)$

$$G_{\ell,n,\chi}(q(\gamma\tau))^k = (c\tau + d)^{ek} \chi^{-k}(d) G_{\ell,n,\chi}(q)^k$$

gilt, wobei $e = 2$ für ungerades und $e = 3$ für gerades n gilt. Aus diesem Grund ist analog zu Korollar 2.2.9 durch den Ausdruck

$$G_{\ell,n,\chi}(q)^k G_{\ell,n,\chi^{-k}}(q)$$

eine Modulfunktion von Gewicht $e(k+1)$ für $\Gamma_0(\ell)$ gegeben. Insbesondere erhalten wir folgendes

Lemma 4.4.1. *Seien ℓ, n, χ wie gewohnt und $k \in \mathbb{N}$. Falls n gerade ist, so sei k ungerade. Weiterhin gelte*

$$r = \begin{cases} \min\{r : \frac{k+1+r}{6} \in \mathbb{N}\}, & n \equiv 1 \mod 2, \\ \min\{r : \frac{3(k+1)+2r}{12} \in \mathbb{N}\}, & n \equiv 0 \mod 2, \end{cases} \quad \textit{und} \quad e_\Delta = \begin{cases} \frac{k+1+r}{6}, & n \equiv 1 \mod 2, \\ \frac{3(k+1)+2r}{12}, & n \equiv 0 \mod 2. \end{cases}$$

Dann ist

$$J_{\ell,n,\chi,k}(q) = J_{\ell,n,k}(q) := \frac{G_{\ell,n,\chi}(q)^k G_{\ell,n,\chi^{-k}}(q) p_1(q)^r}{\Delta(q)^{e_\Delta}}$$

eine auf $\mathbb{H}$ holomorphe Modulfunktion von Gewicht 0 für $\Gamma_0(\ell)$ mit Koeffizienten in $\mathbb{Q}[\zeta_n]$. Wir bezeichnen $J_{\ell,n,k}(q)$ als universelle elliptische Jacobi-Summe.

Beweis. Der Beweis verläuft mit den vorangegangenen Überlegungen völlig analog zu demjenigen von Korollar 2.2.10. Für gerades n stellt dabei die Bedingung an k sicher, dass ein passender Wert für r existiert. □

Aufgrund der dargelegten Theorie kann nun $J_{\ell,n,k}(q)$ als rationaler Ausdruck R_k in $j(q)$ sowie $m_\ell(q)$ bzw. $a_\ell(q)$ dargestellt werden. Dieser Ausdruck kann in analoger Weise mit dem in Abschnitt 3.3.2 bzw. 3.3.3 für die universellen elliptischen Gauß-Summen vorgestellten Algorithmus bestimmt werden. Aus den Beweisen von Lemma 3.3.3 und Proposition 3.3.4 ist direkt ersichtlich, dass dabei $\operatorname{ord}(J^*_{\ell,n,k}) \geqslant (k+1) - \ell e_\Delta$ gilt. Hieraus ergibt sich mit $v = \operatorname{ord}(m_\ell)$ bei Verwendung von a_ℓ und Anwendung von Algorithmus 5 direkt

$$\operatorname{ord}\left(J^{(1)}_{\ell,n,k}\right) \geqslant (k+1) - \ell e_\Delta, \quad \operatorname{ord}\left(J^{(2)}_{\ell,n,k}\right) \geqslant (k+1) - \ell e_\Delta - v, \tag{4.11}$$

bei der Berechnung mit m_ℓ kann

$$\operatorname{prec}(\ell, n, k) = (v - 1 + e_\Delta)\ell + v + e_\Delta - (k+1) - \overline{e_\Delta - k - 2} \tag{4.12}$$

gewählt werden. Liegt der rationale Ausdruck R_k vor, so kann analog zu Abschnitt 4.2 bzw. 4.3 der Wert

$$J_{\ell,n,\chi,k}(E) = G_{\ell,n,\chi}(E)^k G_{\ell,n,\chi^{-k}}(E)$$

ermittelt werden. Um den Index von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n zu bestimmen, gehen wir also folgendermaßen vor:

Algorithmus 6. Bestimmung des Index von λ modulo n

Eingabe: ℓ, n, E

Ausgabe: Index von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n

1. Bestimme $G_{\ell,n,\chi}(E)^n$ mit Gleichung (4.6) bzw. (4.7).
2. Bestimme analog $J_{\ell,n,\chi,m'}(E)$ mit m' aus Gleichung (4.9).
3. Bestimme den Index von λ mit Gleichung (4.10).

Wir bemerken noch, dass in der Darstellung $p = nq + m$ offenbar $(m, n) = 1$ gilt. Insbesondere sind m bzw. m' ungerade, wenn n gerade ist, sodass wir den zweiten Schritt nur für Werte

von m' ausführen, die durch Lemma 4.4.1 gedeckt sind.

Wenden wir dieses Vorgehen für die verschiedenen koprimen Teiler n von $\ell-1$ an, so erhalten wir mit dem Chinesischen Restsatz den Wert von λ und damit von t modulo ℓ. Ist dieser Wert für genügend viele Primzahlen ℓ bekannt, so kann wie im Algorithmus von Schoof mithilfe des Chinesischen Restsatzes der Wert von t und somit schließlich $\#E(\mathbb{F}_p)$ bestimmt werden. Wir merken an, dass die Korrektheit eines berechneten Ergebnisses mithilfe des in [Mül95, S. 155–161] beschriebenen Algorithmus verifiziert werden kann. Der dort angegebene Algorithmus basiert im Wesentlichen auf der Schranke von Hasse an $\#E(\mathbb{F}_p)$ aus Satz 1.1.9 sowie auf der Tatsache, dass $\#E(\mathbb{F}_p) + \#E^t(\mathbb{F}_p) = 2p + 2$ gilt, wobei E^t den sogenannten quadratischen Twist von E bezeichnet, der einfach zu bestimmen ist [BSS99, S. 36–37, 104].

4.4.2 Implementierung

Bei der Implementierung der Berechnung der Laurentreihen der Jacobi-Summen sowie beim Auffinden des rationalen Ausdrucks benutzen wir wieder die in Abschnitt 3.2 dargestellten Ideen. Insbesondere multiplizieren wir die Ausdrücke G_{ℓ,n,χ^k} mit passenden zyklotomischen Gauß-Summen, bevor wir sie miteinander multiplizieren. Auf diese Weise können erneut alle Multiplikationen in $\mathbb{Q}[\zeta_n]$ statt in $\mathbb{Q}[\zeta_\ell, \zeta_n]$ ausgeführt und somit die benötigte Laufzeit deutlich reduziert werden.
Für festes ℓ, n berechnen wir alle nötigen Jacobi-Summen $J_{\ell,n,\chi,k}(q)$ sukzessiv. Wie angemerkt, müssen wir diese nur für zu n teilerfremde k betrachten. Weiterhin sieht man aus Gleichung (4.1) direkt, dass für $m = 1$, also $m' = n-1$, keine Jacobi-Summen nötig sind. Für die Berechnung nutzen wir daher

Algorithmus 7. Berechnung der Jacobi-Summen zu ℓ und n

Eingabe: $\ell, n, \mathrm{prec}(\ell, n)$
Ausgabe: Jacobi-Summen $J_{\ell,n,\chi,k}$ für $1 \leqslant k \leqslant n-2$ und $(k,n) = 1$

1. Berechne $T = T_1 := G_{\ell,n,\chi}(q)G_{\chi^{-1}}(\zeta_\ell)$ bis zur Präzision $\mathrm{prec}(\ell, n)$, $S = S_1 := G_{\chi^{-1}}(\zeta_\ell)$.
2. **for** $k = 1$ **to** $n-2$ **do**
3. Falls $(k,n) > 1$, gehe zu Schritt 8.
4. Bestimme $T_2 := G_{\ell,n,\chi^{-k}}(q)G_{\chi^k}(\zeta_\ell)$, $S_2 := G_{\chi^k}(\zeta_\ell)$.
5. $T_3 := TT_2$, $S_3 := SS_2$.
6. $T_4 := T_3S_3^{-1}$.
7. Berechne $J_{\ell,n,\chi,k}(q)$ durch Multiplikation von T_4 mit passenden Potenzen von $p_1(q)$ und $\Delta(q)$.
8. $T := TT_1$, $S := SS_1$.
9. **end for**

Offenbar stellt Schritt 8 sicher, dass in jeder Iteration in Schritt 5 $T = T_1^k$ sowie $S = S_1^k$ gilt, was die Korrektheit zeigt. Sei c ein Erzeuger von $(\mathbb{Z}/n\mathbb{Z})^*$. Wegen $(\ell, n) = 1$ gilt dann $\mathrm{Gal}(\mathbb{Q}[\zeta_\ell, \zeta_n]/\mathbb{Q}[\zeta_\ell]) = \langle \sigma : \zeta_n \mapsto \zeta_n^c \rangle$. Da σ ein Homomorphismus ist, folgt nun

$$\sigma(G_{\ell,n,\chi}(q)) = G_{\ell,n,\chi^c}(q) \quad \text{und} \quad \sigma(G_{\chi^{-1}}(\zeta_\ell)) = G_{\chi^{-c}}(\zeta_\ell).$$

Somit können wir die Ausdrücke in Schritt 4 ohne nennenswerten Aufwand aus den vorberechneten Werten T_1, S_1 gewinnen, indem wir jeweils den Homomorphismus $\zeta_n \mapsto \zeta_n^k$ anwenden.

Der aufwändigste Schritt innerhalb der Schleife sind dabei offenbar die Bestimmung von T_3 sowie die Aktualisierung von T_1. Diese erfordern jeweils $O(\mathsf{M}(n\,\mathrm{prec}(\ell,n)))$ Operationen. Wir bemerken, dass wegen Gleichung (4.12) bei Verwendung von m_ℓ für alle Werte k die Wahl $\mathrm{prec}(\ell,n) = (v(m_\ell) + e_\Delta)\ell$ ausreichend ist, damit anschließend der rationale Ausdruck bestimmt werden kann. Weiterhin folgt aus (3.14) und (4.11) analog zu (3.16), dass mit der Wahl $\mathrm{prec}(\ell,n) = (v(a_\ell) + e_\Delta + 1)\ell$ der rationale Ausdruck in Abhängigkeit von a_ℓ und j mit Algorithmus 5 berechnet werden kann.

4.5 Weitere Überlegungen

Die folgenden Überlegungen erlauben es, ganz auf die Berechnung der Jacobi-Summen zu verzichten. In diesem Fall wird der resultierende Algorithmus allerdings eine deutlich höhere Laufzeit aufweisen als bestehende Methoden.

Analog zu Gleichung (1.11) kann man auch

$$G_{\ell,n,\chi}(E)^{p^u} = \chi^{-p^u}(\lambda) G_{\ell,n,\chi^{p^u}}(E)$$

mit $u \geqslant 1$ zeigen. Wählt man hierbei $u = \mathrm{ord}_n(p)$, so gilt $p^u \equiv 1 \mod n$ und damit erhält man

$$G_{\ell,n,\chi}(E)^{p^u} = \chi^{-1}(\lambda) G_{\ell,n,\chi}(E) \Rightarrow G_{\ell,n,\chi}(E)^{p^u-1} = \chi^{-1}(\lambda). \tag{4.13}$$

Benutzt man diese Formel, so kann man den Index von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n bestimmen, ohne die Jacobi-Summen zu benutzen. Allerdings benötigt man dann

$$O(\mathsf{M}(n)\log(p^u)) = \tilde{O}(nu\log p) = \tilde{O}(n^2 \log p)$$

Multiplikationen in $\mathbb{F}_p$, um die linke Seite von (4.13) zu berechnen, was wohl unattraktiv ist.

Wie in [FKDG12] schreiben wir $n = q^k$ und $k_1 = \max\{k : q^k \mid p^u - 1\}$. Damit gilt $\mathrm{ggT}(\frac{p^u-1}{q^{k_1}}, q) = 1$ und somit ist $d := \frac{p^u-1}{q^{k_1}}$ modulo n invertierbar. Exponenzieren wir beide Seiten der Gleichung (4.13) mit d^{-1}, so folgern wir

$$G_{\ell,n,\chi}(E)^{q^{k_1}} = \chi^{-d^{-1}}(\lambda)\zeta, \tag{4.14}$$

wobei ζ eine d-te Einheitswurzel ist. Die zugrundeliegende Idee besteht darin, dass man statt der $p-m$-ten Potenz der Gauß-Summe $G_{\ell,n,\chi}(E)$ wie in Gleichung (4.6) mittels dieser Formel lediglich die q^{k_1}-te Potenz benötigt, wobei in den meisten Fällen q^{k_1} viel kleiner als p sein sollte.
Bei den Rechnungen mit elliptischen Gauß-Summen erhalten wir Gleichung (4.14) jedoch in $\mathbb{F}_p[\zeta_n] = \mathbb{F}_{p^u}$, was offenbar die $p^u - 1$-ten Einheitswurzeln enthält. Daher müssen wir in Gleichung (4.14) tatsächlich mit einer Einheitswurzel vom Grad $d = \frac{p^u-1}{q^{k_1}}$ rechnen. Wählen wir einen Erzeuger g von $\mathbb{F}_{p^u}^*$, so können wir $g^{iq^{k_1}} = \zeta$ für ein i mit $0 \leqslant i \leqslant d-1$ schreiben. Analog gilt die Darstellung $\chi^{-d^{-1}}(\lambda) = g^{j\frac{p^u-1}{n}}$ mit $0 \leqslant j \leqslant n-1$, womit wir Gleichung (4.14) als Diskreter-Logarithmus-Problem

$$\log_g(G_{\ell,n,\chi}(E)^{q^{k_1}}) = iq^{k1} + j\frac{p^u-1}{n}$$

und

$$\log_g(G_{\ell,n,\chi}(E)^{q^{k_1}}) \equiv j\frac{p^u-1}{n} \mod q^{k_1}$$

schreiben können. Eine Lösung dieser Kongruenz liefert aufgrund der Definition von k_1 dann direkt den Wert von j, woraus sich der Index von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n ergibt. Da die schnellsten bekannten Algorithmen zur Lösung des Diskreter-Logarithmus-Problems subexponentielle Laufzeit in $\log p$ haben, ist dieser Ansatz offenbar nicht praktikabel.

4.6 Laufzeit und Speicherbedarf

In den folgenden beiden Abschnitten benutzen wir, um Verwirrung zu vermeiden, die Notation $v(m_\ell) = \operatorname{ord}(m_\ell)$ sowie $v(a_\ell) = -\operatorname{ord}(a_\ell)$. Bei Verwendung von m_ℓ berechnen wir $G_{\ell,n,\chi}(E)^n$ mithilfe von Gleichung (4.6). Die Auswertung der rechten Seite dieser Gleichung erfordert, wenn die Werte von j, m_ℓ, Δ und p_1 auf E bekannt sind, noch $\operatorname{prec}(\ell, n)$ Multiplikationen, um $R(m_\ell, j)$ auszuwerten. Wie sich aus Proposition 3.3.4 ergibt, kann man für den Wert $\operatorname{prec}(\ell, n)$, der eine Schranke an den Grad von Zähler und Nenner von R in j und m_ℓ darstellt,

$$\operatorname{prec}(\ell, n) = (v(m_\ell) + e_\Delta)\ell$$

verwenden. Da der Ausdruck $R(m_\ell, j)$ in $\mathbb{F}_p[\zeta_n]$ liegt, sind somit $O((v(m_\ell)+e_\Delta)\ell\,\mathsf{M}(n))$ Multiplikationen in $\mathbb{F}_p$ erforderlich, um $G_{\ell,n,\chi}(E)^n$ mit (4.6) zu berechnen. Die Berechnung von $J_{\ell,n,\chi,m'}(E)$ erfordert laut Abschnitt 4.4.2 einen vergleichbaren Aufwand. Man überlegt sich leicht, dass dies den Aufwand für die Vorberechnungen der Werte j, m_ℓ, Δ, p_1 dominiert. Danach ist gemäß Gleichung (4.10) im Wesentlichen die Potenz $(G_{\ell,n,\chi}(E)^n)^{q+1}$ zu bestimmen, was $O(\mathsf{M}(n)\log q) = O(\mathsf{M}(n)\log p)$ Operationen benötigt, da $n \mid \ell-1$ gilt und somit gegenüber p vernachlässigbar klein ist. Insgesamt ergibt sich $O(\mathsf{M}(n)((v(m_\ell)+e_\Delta)\ell+\log p))$ als Laufzeit.

Unter Verwendung von a_ℓ können wir nach Lemma 3.3.14 und Gleichung (3.15)

$$\operatorname{prec}(\ell, n) = (v(a_\ell) + e_\Delta)\ell + v(a_\ell) + v(m_\ell) - n \leqslant (v(a_\ell) + e_\Delta + 1)\ell$$

wählen und erhalten so die Laufzeit $O(\mathsf{M}(n)((v(a_\ell) + e_\Delta + 1)\ell + \log p))$.

Wir vergleichen dies mit dem in [MMS07] vorgestellten Algorithmus, der die im ursprünglichen Vorgehen nach Elkies für die Bestimmung von t modulo ℓ erforderlichen $O(\ell \log p)$ Operationen in $\mathbb{F}_p$ weiter verbessert und dessen Laufzeit für ein $n \mid \ell - 1$ mit der in diesem Artikel eingeführten Notation $\mathsf{C}_{\sqrt{n}}(.)$ durch

$$O\left(\mathsf{C}(\ell)\log\frac{\ell}{n} + \mathsf{M}(n)\log p + \mathsf{C}_{\sqrt{n}}(n)\right)$$

gegeben ist. Dabei gilt

$$O\left(\mathsf{C}(\ell)\log\frac{\ell}{n} + \mathsf{C}_{\sqrt{n}}(n)\right) = \tilde{O}\left(\ell^{\frac{\omega+1}{2}} + n^{\frac{3\omega+1}{4}}\right) \tag{4.15}$$

mit ω wie in Lemma 3.1.4.

Vergleichen wir dies mit der entsprechenden Laufzeit

$$O((v(m_\ell) + e_\Delta)\ell\,\mathsf{M}(n)) \quad \text{bzw.} \quad O((v(a_\ell) + e_\Delta + 1)\ell\,\mathsf{M}(n)), \tag{4.16}$$

so stellen wir fest, dass unser Ansatz, sofern n und v vergleichsweise klein sind (also vor allem im Fall der Verwendung von a_ℓ, vgl. Abschnitt 4.7), durchaus konkurrenzfähig ist. Ein Vergleich von (4.15) und (4.16) zeigt wegen $e_\Delta \approx \frac{n}{6}$, dass man hierfür mindestens $n \leqslant \sqrt{\ell}$ fordern sollte. Die Anzahl

$$\Psi(x, y) = \#\{z \leqslant x : p \mid z \Rightarrow p \leqslant y\}$$

der y-glatten Zahlen $\leqslant x$ wurde verschiedentlich untersucht, so wurde in [Dic30] und [de 66]

$$\Psi(x, y) \sim x\rho(u) \quad \text{für } x \to \infty \quad \text{mit } x = y^u$$

gezeigt, wobei $\rho(u)$ die in [Dic30] definierte Dickmann-Funktion bezeichnet. In [Ten15] wird bewiesen, dass die Asymptotik die gleiche bleibt, wenn statt für Primteiler für alle Primpotenzteiler $p^k \mid\mid z$ die Beschränkung durch y erfüllt sein soll. Für $u = 2$ gilt nun $\rho(u) \approx 0{,}307$ (s. etwa [Gra08, S. 288]). Somit können wir erwarten, dass für ca. 30% der betrachteten Primzahlen ℓ die Werte von n klein genug sind, dass eine Laufzeitverbesserung möglich scheint.
Es ist jedoch zu beachten, dass nach Gleichung (3.18) asymptotisch in jedem Fall $\ell = O(v)$ gilt, womit unser Algorithmus asymptotisch eine Laufzeit von $O(\ell^2\,\mathsf{M}(n))$ aufweist und mit dem aus [MMS07] nicht kompetitiv ist.

Es bleibt noch anzumerken, dass die Laufzeit für die Berechnung der q-ten Potenz von $G_{\ell,n}(E)^n$ sich reduziert, wenn das n-te zyklotomische Polynom über $\mathbb{F}_p$ reduzibel ist. In diesem Fall hat die Erweiterung $\mathbb{F}_p[\zeta_n]/\mathbb{F}_p$ nur den Grad $\min\{k : p^k \equiv 1 \mod n\} = \mathrm{ord}_n(p)$.
Gilt $n = q^k$ mit einer Primzahl $q > 2$, $n = 2$ oder $n = 4$, so ist jedoch zu berücksichtigen, dass die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ bekanntermaßen zyklisch von Ordnung $\varphi(n)$ ist und somit genau $\varphi(\varphi(n))$ Erzeuger besitzt, weshalb die Wahrscheinlichkeit, dass $\mathrm{ord}_n(p) = \varphi(n)$ gilt, mit $\frac{\varphi(\varphi(n))}{\varphi(n)}$ sehr hoch ist: Wir bemerken nämlich, dass gemäß [MV07, S. 55] für $n \geqslant 3$

$$\varphi(n) \geqslant \frac{n}{\log\log n}(e^{-\gamma} + O(1/\log\log n))$$

gilt, wobei γ die Euler-Konstante und $e^{-\gamma} \approx 0{,}57$ ist.
Falls $n = 2^k$ mit $k > 2$ ist, so gilt $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ und die zweite Gruppe hat 2^{k-3} Erzeuger. Daher liegt die Wahrscheinlichkeit, dass $\mathrm{ord}_p(n) = 2^{k-2} = \frac{n}{4}$ gilt, bei $\frac{2^{k-2}}{2^{k-1}} = \frac{1}{2}$. Somit kann die Ausnutzung der genannten Tatsache nur für wenige Fälle eine signifikante Verbesserung der Laufzeit erwirken.

Schließlich wollen wir die Bestimmung von $G_{\ell,n,\chi}(E)^n$ mithilfe der vorberechneten universellen elliptischen Gauß-Summen mit der Laufzeit vergleichen, die bei einer direkten Berechnung anhand der Definition (1.9) anfällt. Bezeichnen wir mit c einen Erzeuger von $\mathbb{F}_\ell^*$, so bemerken wir zunächst, dass mit der übrigen Notation aus (1.9) wegen $\mathrm{ord}(\chi) = n$

$$G_{\ell,n,\chi}(E) = \sum_{a=1}^{\ell-1} \chi(c^a)(c^a P)_V = \sum_{a=0}^{n-1} \chi(c^a) \sum_{j=1}^{(\ell-1)/n} (c^{a+jn} P)_V =: \sum_{a=0}^{n-1} \chi(c^a)\eta_a(P)$$

gilt. Wie in [MMS07, S. 5] ausgeführt, erfordert die Bestimmung von $\eta_0(P)$ zunächst eine Laufzeit von $O\left(\mathsf{C}(\ell)\log\frac{\ell}{n}\right)$, wonach die übrigen η_a jeweils in Laufzeit $O(\mathsf{C}(\ell))$ bestimmt werden können, womit die Laufzeit für die direkte Berechnung von $G_{\ell,n,\chi}(E)$ bei $O(n\,\mathsf{C}(\ell))$ liegt. Zur Berechnung von $G_{\ell,n,\chi}(E)^n$ sind nun $\log n$ Multiplikationen in der Erweiterung $\mathbb{F}_p[\zeta_n][X]/(F_{\ell,\lambda}(X))$ nötig, wobei $F_{\ell,\lambda}(X)$ der zu P gehörige Elkies-Faktor von $\psi_\ell(X)$ ist (s. Abschnitt 1.2.2 oder etwa [Mül95, Mor95, MMS07]), für den $\deg(F_{\ell,\lambda}) = O(\ell)$ gilt. Somit ergibt sich insgesamt eine asymptotische Laufzeit von $O(n\,\mathsf{C}(\ell) + \log n\,\mathsf{M}(n\ell)) = O(n\,\mathsf{C}(\ell))$ Multiplikationen in $\mathbb{F}_p$, was zu vergleichen ist mit der am Anfang dieses Abschnitts hergeleiteten Laufzeit $O((v+e_\Delta)\ell\,\mathsf{M}(n))$. Wegen $\mathsf{C}(\ell) = O(\ell^{\frac{\omega+1}{2}})$ mit $\omega \geqslant 2{,}38$ und $\ell = O(v)$ nach (3.18) könnte die mit den Algorithmen aus [MMS07] optimierte direkte Berechnung zwar asymptotisch schneller sein. Nehmen wir jedoch an, dass $v \leqslant \ell^{0{,}69}$ oder äquivalent

$$\frac{\ell}{v} \geqslant \ell^{0{,}31} \tag{4.17}$$

ist, so sollte unser neuer Ansatz effizienter sein. Unter Verwendung von m_ℓ erhalten wir im Fall $\ell \equiv 1 \mod 12$ den Wert $\frac{\ell}{v} = 12$, was mit (4.17) $\ell < 3000$ ergibt, während bei Verwendung von a_ℓ im Durchschnitt $\frac{\ell}{v} = 15$ gilt (vgl. Abbildung 1 in Abschnitt 4.7), woraus $\ell < 6200$ folgt, was für alle praktischen Rechnungen, gemäß [Fra16] insbesondere für die benötigten Werte von ℓ im Rahmen von CIDE wie in [FKDG12], erfüllt ist. Wir bemerken, dass eine genauere Analyse der Konstanten in der O-Notation nötig wäre, um diese groben Überlegungen zu präzisieren. In diesem Fall erwarten wir jedoch eine noch stärkere Überlegenheit unseres neuen Ansatzes, da die Konstante in dessen Laufzeit gemäß Proposition 3.3.4 bei 1 liegt.

Weit einschränkender als die Laufzeit ist für praktische Anwendungen im Bereich des Punktezählens auf elliptischen Kurven jedoch der nötige Speicherbedarf. Wie aus den Überlegungen in den Abschnitten 3.3.2 und 3.3.3 folgt, ist das Polynom Q zu $\tau_{\ell,n}(q)$ durch $\operatorname{prec}(\ell,n)$ Koeffizienten aus $\mathbb{Q}[\zeta_n]$ gegeben. Die im nächsten Abschnitt diskutierten durch unsere Rechnungen erhaltenen Ergebnisse, die nahelegen, dass die Höhe (der Logarithmus des maximalen Absolutbetrags) dieser Koeffizienten im Wesentlichen proportional zu v und damit nach (3.18) asymptotisch zu ℓ ist, implizieren somit, dass

$$\tilde{O}(\operatorname{prec}(\ell,n)n\ell) = \tilde{O}((v+e_\Delta)n\ell^2)$$

Byte Speicherplatz benötigt werden, um alle Koeffizienten von Q zu speichern. Unter erneuter Verwendung von $\ell = O(v)$ gemäß Gleichung (3.18) sowie $n = O(\ell)$ im ungünstigsten Fall erhalten wir damit einen Platzbedarf von $\tilde{O}(\ell^4)$ Bytes. Damit rechnen wir im ungünstigsten Fall für $\ell \approx 100$ mit einem Speicherbedarf von etwa 100 MB zur Darstellung *eines* Polynoms Q, was durch unsere Rechnungen bestätigt wird. Der erwartete Speicherbedarf steigt für $\ell \approx 200$ bereits auf 1,6 GB und für $\ell \approx 1000$ auf etwa 1 TB. Berücksichtigen wir noch, dass das Polynom Q zu festem ℓ und n gemäß Abschnitt 4.4 für $\varphi(n) - 1$ verschiedene Jacobi-Summen vorberechnet werden muss, um die Punkte für elliptische Kurven $E/\mathbb{F}_p$ für beliebige Primzahlen p zählen zu können, so ist ersichtlich, dass die vorgeschlagene Methode hier schnell an die Grenzen des Möglichen stößt. Im Kontext des Punktezählens auf elliptischen Kurven werden ähnliche Speicherprobleme bereits in [Inr09, S. 9] geschildert. Wir bemerken, dass für die Rekordrechnungen in [EM06] Primzahlen bis zu $\ell \approx 4000$ und für diejenigen in [Sut13] sogar bis zu $\ell \approx 11000$ verwendet wurden.

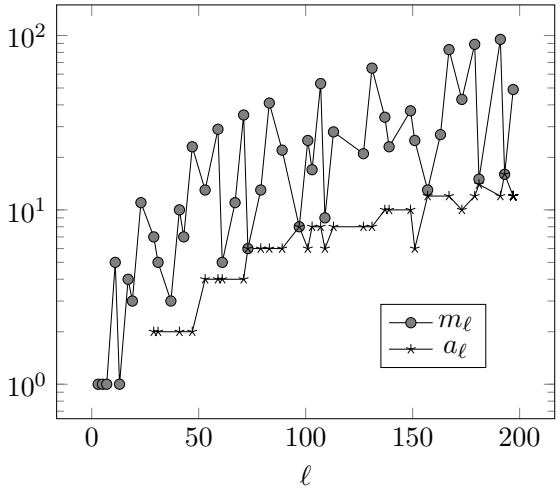


Abbildung 1: Grad des Minimalpolynoms in j

4.7 Vergleich von m_ℓ und a_ℓ

In den Abschnitten 3.3.2 bzw. 3.3.3 sowie 4.2 bzw. 4.3 wurde das Vorgehen zur Bestimmung der universellen elliptischen Gauß-Summen und ihrer Anwendung zum Punktezählen im Elkies-Fall unter Benutzung der Modulfunktionen m_ℓ bzw. a_ℓ vorgestellt. Wir wollen im Folgenden die bereits getätigte Aussage, dass die Wahl von a_ℓ aus Laufzeitgründen vorzuziehen ist, genauer quantifizieren. Dazu verwenden wir die Daten aus den von uns unter Verwendung von sowohl m_ℓ als auch a_ℓ durchgeführten Berechnungen der universellen elliptischen Gauß-Summen $\tau_{\ell,n}$ für die Primzahlen $\ell \leqslant 197$ und alle Primpotenzteiler $n \mid\mid \ell - 1$.

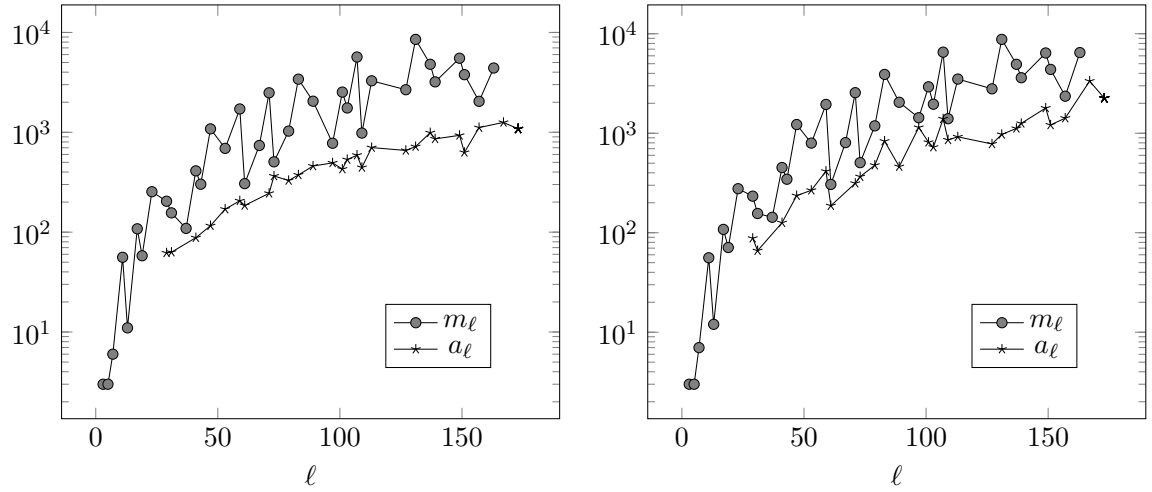
Der Vorteil von a_ℓ gegenüber m_ℓ besteht im Wesentlichen darin, dass der Wert $v(a_\ell)$ für die meisten Primzahlen ℓ deutlich kleiner ist als $v(m_\ell)$. Dies wirkt sich folgendermaßen aus:

Zunächst hat das Minimalpolynom $A_\ell(X, j)$ von a_ℓ gemäß [Mül95, S. 77] den Grad $2v(a_\ell)$ in j, während das Minimalpolynom $M_\ell(X, j)$ von m_ℓ laut [Mül95, S. 61–62] den Grad $v(m_\ell)$ aufweist. Mit Proposition 2.1.21 ist der Grad des Zählers der rationalen Darstellung in j jeweils durch diese Werte nach oben beschränkt. Abbildung 1 zeigt einen Vergleich der Werte $\deg_j(M_\ell)$ und $\deg_j(A_\ell)$ (man beachte die logarithmische Skalierung). Aufgrund der Definition von $v(m_\ell)$, die von der Restklasse von ℓ modulo 12 abhängt, oszilliert diese Größe relativ stark. Wie man in Abbildung 1 sieht, ergibt sich unter Verwendung von a_ℓ immer ein Vorteil, außer wenn $\ell \equiv 1 \mod 12$ gilt. Im dargestellten Bereich ist der Wert unter Verwendung von a_ℓ im Durchschnitt etwa um den Faktor 4 geringer.

Weiterhin ergeben sich aus den Werten $v(m_\ell)$ bzw. $v(a_\ell)$ gemäß Proposition 3.3.4 bzw. Lemma 3.3.14 und Formel (3.15) die Werte

$$\operatorname{prec}(\ell, n) = (v(m_\ell) + e_\Delta)\ell \quad \text{bzw.} \quad \operatorname{prec}(\ell, n) = (v(a_\ell) + e_\Delta + 1)\ell \tag{4.18}$$

als Schranken an die nötige Präzision. Da die Präzision in den Formeln für die Laufzeit aller wesentlichen Teilschritte der Rechnungen (s. die Korollare 3.2.6, 3.3.6 und 3.3.15 sowie Abschnitt 4.6) mindestens als linearer Faktor auftritt, rechnen wir damit, dass der Unterschied



(a) Minimale Präzision für festes ℓ

(b) Maximale Präzision für festes ℓ

Abbildung 2: Benötigte Präzision

von $v(a_\ell)$ und $v(m_\ell)$ um einen konstanten Faktor die Beschleunigung der Algorithmen mindestens um eben diesen Faktor bewirkt. Dies gilt zumindest im Fall, dass $e_\Delta \approx \frac{n}{6}$ im Vergleich zu den Werten von v klein ist, was für den von uns praktisch verwendeten Bereich $\ell < 200$ sehr häufig gegeben ist.

Abbildung 2 zeigt einen Vergleich der Werte von $\operatorname{prec}(\ell, n)$. In Grafik 2a sind für festes ℓ die Werte $\min_{n||\ell} \operatorname{prec}(\ell, n)$ dargestellt, in Abbildung 2b die Größe $\max_{n||\ell} \operatorname{prec}(\ell, n)$. Man sieht, dass die Verwendung von a_ℓ stets kleinere Werte ergibt. Bei Betrachtung der Minima sind diese im Durchschnitt um den Faktor 5 geringer, bei den Maxima, für die in Formel (4.18) die von der Wahl zwischen m_ℓ und a_ℓ unabhängige Größe e_Δ einen wichtigeren Beitrag leistet, immerhin noch um den Faktor 3,5.

Schließlich sind auch die in den Ausdrücken auftretenden Koeffizienten unter Verwendung von a_ℓ deutlich geringer. Um dies genauer zu quantifizieren, definieren wir die (logarithmische) Höhe eines bivariaten Polynoms $P(X, Y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{i,j} X^i Y^j \in \mathbb{Z}[X, Y]$ als

$$\mathrm{h}(P) := \log \max_{i,j} |a_{i,j}|. \tag{4.19}$$

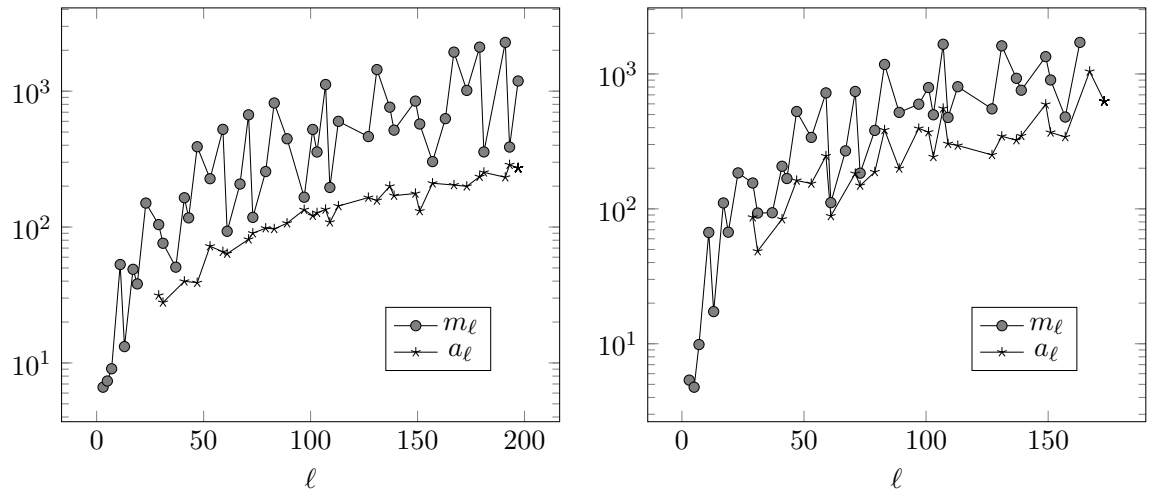
Für das Modularpolynom Φ_ℓ wurde von Cohen in [Coh84]

$$\mathrm{h}(\Phi_\ell) = 6(\ell + 1)\left(\left(1 - \frac{2}{\ell}\right)\log \ell + O(1)\right)$$

gezeigt. In [BS10] wurde in Cohens Beweis der Fehlerterm explizit gemacht und damit die Schranke

$$\mathrm{h}(\Phi_\ell) \leqslant 6\ell \log \ell + 18\ell \tag{4.20}$$

hergeleitet. Für die Minimalpolynome anderer Modulfunktionen, die in der Praxis anstelle von $\Phi_\ell(X, j)$ verwendet werden, lassen numerische Ergebnisse und eine Untersuchung der



(a) Höhe des Minimalpolynoms

(b) Maximale Höhe von Q für festes ℓ

Abbildung 3: Höhe der auftretenden Polynome

Grundideen von [Coh84] analoge Schranken in Abhängigkeit von ihrem Grad in j vermuten. Für die Minimalpolynome $M_\ell(X, j)$ bzw. $A_\ell(X, j)$ von m_ℓ bzw. a_ℓ rechnet man so mit

$$\mathrm{h}(M_\ell) = c_1 v(m_\ell) \log \ell + c_2 v(m_\ell) \quad \text{bzw.} \quad \mathrm{h}(A_\ell) = d_1 v(a_\ell) \log \ell + d_2 v(a_\ell) \tag{4.21}$$

für gewisse Konstanten $c_i, d_i, i = 1, 2$. Der Beweis für die Schranken in [Coh84] benutzt jedoch in starkem Ausmaße verschiedene spezifische Eigenschaften der j-Funktion und konnte daher bisher nicht auf andere Modulfunktionen übertragen werden (vgl. [Eng09]). Unter der durch empirische Daten gestützten Hypothese (4.21) folgert man wiederum, dass die im Nenner der gemäß Proposition 2.1.21 berechneten rationalen Darstellung für die universellen elliptischen Gauß-Summen auftretenden Koeffizienten unter Verwendung von a_ℓ deutlich geringer sind. Abbildung 3a vergleicht die Höhen von M_ℓ und A_ℓ. Im betrachteten Bereich ist diejenige von A_ℓ durchschnittlich um den Faktor 5 geringer als die von M_ℓ, d. h., es gilt $m_{A_\ell} \approx m_{M_\ell}^{1/5}$, wenn m_{A_ℓ} bzw. m_{M_ℓ} den maximalen Absolutbetrag der Koeffizienten des jeweiligen Polynoms bezeichnen.

Definieren wir für das den Zähler der Darstellung für die universelle elliptische Gauß-Summe bestimmende Polynom $Q = \sum_{i=0}^{n} \sum_{j=0}^{m} \sum_{k=0}^{r-1} a_{i,j,k} \zeta_r^k X^i Y^j$ mit $a_{i,j,k} = \frac{p_{i,j,k}}{q_{i,j,k}} \in \mathbb{Q}$ die Höhe als

$$h(Q) := \log \max_{i,j,k} |p_{i,j,k}| + |q_{i,j,k}|,$$

so können wir anhand der berechneten Darstellungen empirisch das Wachstum der Koeffizienten untersuchen, die im Zählerpolynom $Q(m_\ell, j)$ bzw. $Q(a_\ell, j)$ des Ausdrucks für $\tau_{\ell,n}$ (bzw. $\tau_{\ell,n}^{(1)}, \tau_{\ell,n}^{(2)}$ in Abschnitt 3.3.3) auftreten. Auch hier ergibt sich das Bild, dass die Höhe unter Verwendung von a_ℓ deutlich geringer ist. Diese nimmt in beiden Fällen bei Vergrößerung von n stark zu, ein genau quantifizierbarer Bezug zu $h(M_\ell)$ bzw. $h(A_\ell)$ lässt sich aus den Daten nicht ableiten, der Wert von $\mathrm{h}(Q)$ ist in beiden Fällen grob doppelt so groß. Abbildung 3b zeigt die Werte $\max_{n||\ell} h(Q)$, die im betrachteten Bereich unter Verwendung von a_ℓ etwa um

den Faktor 2,5 geringer ausfallen.

Aus den verschiedenen bei Verwendung von a_ℓ kleineren Werten ergibt sich insgesamt eine Verbesserung der benutzten Algorithmen um einen für praktische Anwendungen beträchtlichen Faktor, der jedoch stark von der Restklasse von ℓ modulo 12 und der Größe der Teiler n von ℓ abhängt.

5 Verwendung von Primzahlpotenzen

5.1 Universelle elliptische Gauß-Summen

Im Kontext des Algorithmus von Schoof wurde für den Elkies-Fall erforscht, wie der Wert der Spur t des Frobenius-Homomorphismus ϕ_p auf einer elliptischen Kurve $E/\mathbb{F}_p$ nicht nur modulo Primzahlen ℓ, sondern auch modulo Primzahlpotenzen ℓ^i bestimmt werden kann. Ein eher theoretischer Abschnitt dazu findet sich in [Mül95, S. 124–129]. In [CDM96] wird ein effizienterer Ansatz dargestellt, der Folgen von Isogenien konstruiert, um einen Faktor des ℓ^i-ten Divisionspolynoms $\psi_{\ell^i}(X)$ von kleinem Grad zu berechnen. Die Verwendung von Primzahlpotenzen ermöglicht offenbar die Benutzung kleinerer Primzahlen ℓ und wirkt sich im SEA-Algorithmus bei sorgfältiger Wahl der benutzten Primzahlpotenzen und unter Verwendung der Methoden aus [CDM96] insgesamt positiv auf die Laufzeit aus.

Solche Rechnungen lassen sich jedoch auch durch eine Verallgemeinerung zunächst der elliptischen Gauß-Summen aus [Mih06c] realisieren. Für eine Elkies-Primzahl ℓ erhält man nämlich, wenn das charakteristische Polynom $\chi(\phi_p) = \phi_p^2 - t\phi_p + p$ in $\mathbb{F}_\ell^*$ zwei verschiedene Nullstellen λ und μ besitzt, mittels des Henselschen Lemmas für $i \geqslant 2$ jeweils genau zwei verschiedene Nullstellen λ_i, μ_i in $(\mathbb{Z}/\ell^i\mathbb{Z})^*$. Dies sind die Eigenwerte der Wirkung von ϕ_p auf die ℓ^i-Torsion. Nach (1.3) gilt $E[\ell^i] \cong \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$. Nun gibt es gemäß [CDM96] wieder einen Eigenpunkt $P_i \in E[\ell^i] \backslash E[\ell^{i-1}]$ mit

$$\phi_p(P_i) = \lambda_i P_i,$$

der eine Untergruppe von $E[\ell^i]$ erzeugt.

Bemerkung 5.1.1. Falls $\chi(\phi_p) = \phi_p^2 - t\phi_p + p$ eine doppelte Nullstelle λ modulo ℓ hat, also $\chi'(\lambda) \equiv 0 \mod \ell$ gilt, kann λ nicht eindeutig zu einer Nullstelle modulo ℓ^i für $i > 1$ geliftet werden. Dieser Fall tritt für $p \neq 2$ stets für $\ell = 2$ auf, allgemein lässt er sich mithilfe des Modularpolynoms Φ_ℓ leicht erkennen, wie in Abschnitt 1.2.2 ausgeführt, und die Bestimmung von $t \mod \ell$ selbst ist besonders einfach durchzuführen. Besitzt $\chi(\phi_p)$ modulo ℓ eine doppelte Nullstelle, so lässt sie sich entweder zu mehreren Lösungen modulo ℓ^i liften oder aber $\chi(\phi_p)$ besitzt keine Nullstelle modulo ℓ^i [Eis95, S. 207]. Selbst wenn $\chi(\phi_p)$ Nullstellen modulo ℓ^i besitzt, ist die Ordnung der zugehörigen Eigenpunkte im Allgemeinen nur ein Teiler $\ell^k, k \leqslant i$, von ℓ^i, wie in [CDM96] angemerkt wird, und damit kann der Eigenwert nur modulo dieser Ordnung und im Allgemeinen nicht modulo ℓ^i bestimmt werden.

Da der Wert von t, von dem dies abhängt, nicht bekannt ist und überhaupt erst berechnet werden soll, lässt sich das Verhalten zur Laufzeit nicht vorhersagen. Man könnte zwar die auf den folgenden Überlegungen basierenden Rechnungen ebenfalls ausführen, müsste jedoch die verschiedenen für λ_i erhaltenen Werte auf ihre Korrektheit prüfen und würde, wenn keine Lösung modulo ℓ^i existiert, dies erst nach Abschluss der recht aufwändigen Berechnungen bemerken. Daher beschränken wir uns im Folgenden auf den Fall, dass die Nullstellen von $\chi(\phi_p)$ modulo ℓ verschieden sind. Wir bemerken, dass der Fall doppelter Nullstellen in [CDM96, S. 13–17] näher betrachtet und seine Behandlung im Rahmen des dort vorgestellten Algorithmus erläutert wurde.

Sei n ein Teiler von $\left|(\mathbb{Z}/\ell^i\mathbb{Z})^*\right| = \varphi(\ell^i) = \ell^{i-1}(\ell-1)$ und sei $\chi : (\mathbb{Z}/\ell^i\mathbb{Z})^* \to \mu_n$ ein Dirichlet-

Charakter von Ordnung n. Dann definieren wir die zugehörige elliptische Gauß-Summe mittels

$$G_{\ell^i,n,\chi}(E) = \sum_{a=1}^{\ell^i-1} \chi(a)(aP_i)_V, \tag{5.1}$$

wobei wie in (1.9) $V = y$ für gerades und $V = x$ für ungerades n und außerdem $\chi(a) = 0$ für $\mathrm{ggT}(a, \ell^i) > 1$ gilt. Analog zu den Ergebnissen aus [Mih06c] erhalten wir folgendes

Lemma 5.1.2. *Mit den genannten Bezeichnungen gelten die folgenden Aussagen:*

1. $G_{\ell^i,n,\chi}(E)^n, \frac{G_{\ell^i,n,\chi}(E)^m}{G_{\ell^i,n,\chi^m}(E)} \in \mathbb{F}_p[\zeta_n]$ $(m \in \mathbb{N})$.

2. $G_{\ell^i,n,\chi}(E)^p = \chi^{-p}(\lambda_i) G_{\ell^i,n,\chi^p}(E)$.

Beweis. Sei $\mathbb{F}_p[\zeta_n] = \mathbb{F}_{p^k}$ (also $k = \mathrm{ord}_n(p)$) und bezeichne $\varphi_{p^k} : x \mapsto x^{p^k}$ die zugehörige Potenz des Frobenius-Homomorphismus. Schreiben wir $\lambda_i^k = b$, so gilt

$$\begin{aligned}\varphi_{p^k}(G_{\ell^i,n,\chi}(E)) &= \varphi_{p^k}\left(\sum_{a=1}^{\ell^i-1} \chi(a)(aP_i)_V\right) = \sum_{a=1}^{\ell^i-1} \varphi_{p^k}(\chi(a))(\phi_p^k(aP_i))_V \\ &= \sum_{a=1}^{\ell^i-1} \chi(a)(a\lambda_i^k P_i)_V = \chi^{-1}(b) \sum_{a=1}^{\ell^i-1} \chi(ab)(abP_i)_V = \chi^{-1}(b) G_{\ell^i,n,\chi}(E).\end{aligned}$$

Wegen $\mathrm{ord}(\chi) = n$ folgt damit die Invarianz der beiden Ausdrücke aus Punkt 1 unter φ_{p^k}, weshalb sie in $\mathbb{F}_p[\zeta_n]$ liegen.

Weiterhin rechnen wir nach

$$G_{\ell^i,n,\chi}(E)^p = \sum_{a=1}^{\ell^i-1} \chi^p(a)(\phi_p(aP_i))_V = \sum_{a=1}^{\ell^i-1} \chi^p(a)(a\lambda_i P_i)_V = \chi^{-p}(\lambda_i) G_{\ell^i,n,\chi^p}(E). \tag{5.2}$$

□

Schreibt man $p = nq + m$ mit $0 \leqslant m < n$, so kann man Gleichung (5.2) wieder umformen zu

$$\frac{G_{\ell^i,n,\chi}(E)^m}{G_{\ell^i,n,\chi^m}(E)} (G_{\ell^i,n,\chi}(E)^n)^q = \chi^{-m}(\lambda_i), \tag{5.3}$$

woraus sich analog zu (1.11) der Index von λ_i in $(\mathbb{Z}/\ell^i\mathbb{Z})^*$ modulo n bestimmen lässt.

Wir übertragen nun den Ansatz zur Berechnung der gesuchten Objekte mittels universeller elliptischer Gauß-Summen aus den Abschnitten 2 und 3. Analog zu Korollar 2.2.9 beginnen wir mit

Lemma 5.1.3. *Seien $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\ell^i)$, $\zeta_{\ell^i} \in \mu_{\ell^i}$ eine primitive ℓ^i-te Einheitswurzel, n ein Teiler von $\varphi(\ell^i)$, $\chi : (\mathbb{Z}/\ell^i\mathbb{Z})^* \to \mu_n$ ein Dirichlet-Charakter von Ordnung n und seien*

$$V = \begin{cases} x, & n \equiv 1 \mod 2, \\ y, & n \equiv 0 \mod 2, \end{cases} \quad \textit{sowie} \quad e = \begin{cases} 2n, & n \equiv 1 \mod 2, \\ 3n, & n \equiv 0 \mod 2. \end{cases}$$

Dann transformiert sich die von χ abhängige n-te Potenz der Funktion

$$G_{\ell^i,n,\chi}(q) = G_{\ell^i,n}(q) := \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)V(\zeta_{\ell^i}^{\lambda}, q) \tag{5.4}$$

unter γ mittels $G_{\ell^i,n}(q(\gamma\tau))^n = (c\tau+d)^e G_{\ell^i,n}(q)^n$. Weiterhin ist diese Funktion meromorph an den Spitzen und somit eine Modulfunktion vom angegebenen Gewicht für $\Gamma_0(\ell^i)$ sowie unabhängig von der Wahl der primitiven ℓ^i-ten Einheitswurzel ζ_{ℓ^i}.

Beweis. Der Beweis verläuft analog zu demjenigen von Korollar 2.2.9. Analog zu ihm rechnen wir zunächst

$$\begin{aligned} x(\zeta_{\ell^i}, q(\gamma\tau)) =& (c\tau+d)^2 x\left(\exp\left(\frac{2\pi i(c\tau+d)}{\ell^i}\right), q\right) = (c\tau+d)^2 x\left(\exp\left(\frac{2\pi i d}{\ell^i}\right), q\right) \\ =& (c\tau+d)^2 x(\zeta_{\ell^i}^d, q), \end{aligned}$$

wobei die vorletzte Gleichheit wegen $\gamma \in \Gamma_0(\ell^i)$, also $c \equiv 0 \mod \ell^i$, aus der Reihenentwicklung (2.10) folgt. Für y zeigt man eine analoge Gleichheit.
Sei nun ohne Beschränkung der Allgemeinheit n ungerade. Dann gilt wegen $\mathrm{ggT}(d,\ell) = 1$

$$\begin{aligned} G_{\ell^i,n}(q(\gamma\tau)) =& \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)x(\zeta_{\ell^i}^{\lambda}, q(\gamma\tau)) = (c\tau+d)^2 \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)x(\zeta_{\ell^i}^{d\lambda}, q(\tau)) \\ =& (c\tau+d)^2\chi^{-1}(d) \sum_{a\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(a)x(\zeta_{\ell^i}^{a}, q(\tau)) = (c\tau+d)^2\chi^{-1}(d)G_{\ell^i,n}(q), \end{aligned}$$

womit die Aussage zum Transformationsverhalten von $G_{\ell^i,n,\chi}(q)^n$ aus $\mathrm{ord}(\chi) = n$ folgt.
Dass diese Funktion meromorph an den Spitzen ist, sieht man analog zu Korollar 2.2.9 durch Betrachten der Laurentreihen $x(\zeta_{\ell^i}, q(S_k\tau))$, wobei S_k, $k = 1,\dots,\ell^{i-1}(\ell+1)$ ein Repräsentantensystem von $\Gamma/\Gamma_0(\ell^i)$ bilden. Die Unabhängigkeit von $G_{\ell^i,n,\chi}(q)^n$ von der Wahl der Einheitswurzel folgt aus dem bereits Gezeigten, denn für $\mathrm{ggT}(d,\ell) = 1$ gilt danach

$$\sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)x(\zeta_{\ell^i}^{d\lambda}, q) = \chi^{-1}(d) \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)x(\zeta_{\ell^i}^{\lambda}, q).$$

□

Nun erhalten wir analog zu Korollar 2.2.10 folgendes

Korollar 5.1.4. *Seien ℓ^i, n, χ wie in Lemma 5.1.3. Weiterhin gelte*

$$r = \begin{cases} \min\left\{r : \frac{n+r}{6} \in \mathbb{N}\right\}, & n \equiv 1 \mod 2, \\ 3, & n = 2, \\ 0, & \textit{sonst}, \end{cases} \quad \textit{und} \quad e_\Delta = \begin{cases} \frac{n+r}{6}, & n \equiv 1 \mod 2, \\ 1, & n = 2, \\ \frac{n}{4}, & \textit{sonst.} \end{cases}$$

Dann ist

$$\tau_{\ell^i,n}(q) := \frac{G_{\ell^i,n}(q)^n p_1(q)^r}{\Delta(q)^{e_\Delta}} \tag{5.5}$$

eine auf $\mathbb{H}$ holomorphe Modulfunktion von Gewicht 0 für $\Gamma_0(\ell^i)$ mit Koeffizienten in $\mathbb{Q}[\zeta_n]$.

Beweis. Der Beweis verläuft völlig analog zu demjenigen von Korollar 2.2.10, da $p_1(q)$ eine Modulfunktion für $\Gamma_0(\ell)$ und damit auch für $\Gamma_0(\ell^i)$ ist. Lediglich die Aussage über die Koeffizienten muss genauer betrachtet werden. Gilt $\mathrm{ggT}(n,\ell)=1$, so überträgt sich der Beweis aus Korollar 2.2.10 direkt. Anderenfalls gelte $\ell^k \mid\mid n$ mit $k<i$, sodass $\mathbb{Q}[\zeta_n]$ die ℓ^k-ten Einheitswurzeln enthält. Dann gilt $G := \mathrm{Gal}(\mathbb{Q}[\zeta_{\ell^i},\zeta_n]/\mathbb{Q}[\zeta_n]) \cong \mathbb{Z}/\ell^{i-k}\mathbb{Z}$. Ist c ein Erzeuger von $(\mathbb{Z}/\ell^i\mathbb{Z})^*$ und $c' = c^{\varphi(\ell^k)}$, so wird G von $\sigma : \zeta_{\ell^i} \mapsto \zeta_{\ell^i}^{c'}$ erzeugt. Nun gilt wie in Korollar 2.2.10

$$\begin{aligned}\sigma(G_{\ell^i,n}(q)) &= \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)\sigma(V(\zeta_{\ell^i}^{\lambda},q)) = \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(\lambda)V(\zeta_{\ell^i}^{c'\lambda},q)\\ &= \chi^{-1}(c') \sum_{\lambda\in(\mathbb{Z}/\ell^i\mathbb{Z})^*} \chi(c'\lambda)V(\zeta_{\ell}^{c'\lambda},q) = \chi^{-1}(c')G_{\ell^i,n}(q).\end{aligned}$$

Somit liegt $G_{\ell^i,n}(q)^n$ in $\mathbb{Q}[\zeta_n]$. □

5.2 Berechnung

Um wie für den Fall von Primzahlen ℓ die universellen elliptischen Gauß-Summen als rationalen Ausdruck in Abhängigkeit von j und einer anderen Modulfunktion f zu berechnen, benötigen wir eine holomorphe Modulfunktion f, sodass $\mathbf{A}_0(\Gamma_0(\ell^i)) = \mathbb{C}(j(\tau),f(\tau))$ gilt. Dann erhält man nämlich völlig analog zu Korollar 2.1.20 das folgende

Lemma 5.2.1. *Sei $g(\tau)\in\mathbf{H}_0(\Gamma_0(\ell^i))$ eine holomorphe Modulfunktion. Sei $f(\tau)\in\mathbf{H}_0(\Gamma_0(\ell^i))$ mit Minimalpolynom $Q_f(X,j)$ mit $\deg_j(Q_f)=v$, sodass $\mathbf{A}_0(\Gamma_0(\ell^i)) = \mathbb{C}(j(\tau),f(\tau))$ gilt. Dann besitzt $g(\tau)$ eine Darstellung der Form*

$$g(\tau) = \frac{\sum_{i=0}^{v-1} a_i j(\tau)^i}{\frac{\partial Q_f}{\partial Y}(f(\tau),j(\tau))}$$

mit

$$a_i \in \{h(\tau)\in\mathbb{C}(f(\tau)) : h(\tau)\ \textit{holomorph}\}.$$

Es liegt nahe, solch eine Modulfunktion f wie im Fall von Primzahlen ℓ aus der Dedekindschen η-Funktion zu konstruieren. Das folgende durch sorgfältige Analyse des wohlbekannten Transformationsverhaltens von η (s. Satz 6.2.3) bewiesene Lemma aus [New57, S. 336] liefert dazu ein allgemeines Werkzeug.

Lemma 5.2.2. *Sei $\phi_\delta(\tau) = \frac{\eta(\delta\tau)}{\eta(\tau)}$. Sei $N>1$, $\mathrm{ggT}(N,6)=1$ und seien $\{r_\delta\}_{\delta\mid N}$ ganze Zahlen, sodass*

$$\frac{1}{24}\sum_{\delta\mid N}(\delta-1)r_\delta \text{ eine ganze Zahl und}$$
$$\prod_{\delta\mid N}\delta^{r_\delta} \text{ ein Quadrat in } \mathbb{Q} \text{ ist.}$$

Dann ist die Funktion

$$g = g(\tau) = \prod_{\delta\mid N}\phi_\delta^{r_\delta}$$

eine Modulfunktion von Gewicht 0 für $\Gamma_0(N)$. (Wegen $\phi_1=1$ wird $r_1=0$ gesetzt.)

Wie bereits in Abschnitt 2.1.2 angemerkt, erhält man die Funktion $m_\ell(q)$ als einfachsten Spezialfall für $N = \ell$. Im Folgenden betrachten wir den Fall $N = \ell^2$, der als einziger im Kontext des Punktezählens algorithmisch interessant scheint, wie wir weiter unten ausführen. Dieser Fall ist in [ES05] eingehend untersucht worden. Der Artikel befasst sich mit der Funktion $\mathfrak{w}^s_{\ell_1,\ell_2}$ mit

$$\mathfrak{w}_{\ell_1,\ell_2}(\tau) = \frac{\eta\left(\frac{\tau}{\ell_1}\right)\eta\left(\frac{\tau}{\ell_2}\right)}{\eta(\tau)\eta\left(\frac{\tau}{\ell_1\ell_2}\right)}$$

und $s = 24/\operatorname{ggT}(24, (\ell_1 - 1)(\ell_2 - 1))$, wobei $\ell_1 = \ell_2$ und $\ell_1 \in \{2, 3\}$ möglich sind. Aus Lemma 5.2.2 folgt, dass

$$\left(\mathfrak{w}_{\ell_1,\ell_2}(S_0^{-1}\tau)\right)^s = \left(\frac{\eta(\ell_1\tau)\eta(\ell_2\tau)}{\eta(\tau)\eta(\ell_1\ell_2\tau)}\right)^s, \quad \text{dabei} \quad S_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

eine Modulfunktion von Gewicht 0 für $\Gamma_0(\ell_1\ell_2)$ ist, sofern $(\ell_1\ell_2, 6) = 1$ gilt. Für die übrigen Fälle ist diese Aussage ebenfalls korrekt, wie man durch Nachrechnen sieht.
Die Gruppe $\Gamma^0(N)$, die später in Gleichung (6.5) definiert wird, erfüllt $\Gamma^0(N) = S_0^{-1}\Gamma_0(N)S_0$ und damit gilt nach (6.7) $f(S_0\tau) \in \mathbf{A}_0(\Gamma^0(N))$ genau dann, wenn $f(\tau) \in \mathbf{A}_0(\Gamma_0(N))$ ist. Verwendet man diese Korrespondenz, so ergibt sich auch, dass $\mathfrak{w}^s_{\ell_1,\ell_2}$ eine Modulfunktion von Gewicht 0 für $\Gamma^0(\ell_1\ell_2)$ ist. Im von uns betrachteten Fall $N = \ell^2$ bedienen wir uns nun der Funktion $m_{\ell^2}(\tau) := \mathfrak{w}_{\ell,\ell}(S_0^{-1}\tau)^s$ mit $s = 24/\operatorname{ggT}(24, (\ell - 1)^2)$.

Aus [ES05, Satz 8] folgt, dass m_{ℓ^2} zusammen mit j den Körper $\mathbf{A}_0(\Gamma_0(\ell^2))$ erzeugt, sodass die Voraussetzungen von Lemma 5.2.1 erfüllt sind und für die universellen elliptischen Gauß-Summen $\tau_{\ell^2,n,\chi}$ eine Darstellung als rationaler Ausdruck in j und m_{ℓ^2} berechnet werden kann. Der Beweis dieser Aussage wird in [ES05] durch sehr konkrete Rechnungen für die Funktion m_{ℓ^2} erbracht und kann, da der Körper $\mathbf{A}_0(\Gamma_0(\ell^2))$ eine Reihe von Teilkörpern besitzt, nicht aus einer allgemeinen Aussage geschlossen werden, wie es im Fall $N = \ell$ mit Satz 2.1.11 möglich war. A fortiori gilt dies für den Fall $N = \ell^i$ mit $i \geqslant 3$.

Aus ähnlichen Gründen ist die effiziente Berechnung des Minimalpolynoms $M_{\ell^2}(X, j)$ der Funktion m_{ℓ^2} oder gegebenenfalls anderer Modulfunktionen, die stattdessen verwendet werden können, nicht-trivial. Dies resultiert daraus, dass zur Bestimmung der Laurentreihen der Konjugierten von m_{ℓ^2} die Wahl eines speziellen Repräsentantensystem für $\Gamma/\Gamma_0(\ell^2)$ nötig ist, das sich teilweise stark vom kanonischen unterscheidet. Dazu sind umfangreiche Ad-hoc-Rechnungen für die betrachtete Funktion erforderlich, die in [ES05], ausgehend von den Erläuterungen Deurings in [Deu58], für m_{ℓ^2} ausgeführt werden. Für $N = \ell^i$ mit $i \geqslant 3$ würde sich dieses Problem erneut verschärfen. Daher wurde in [Eng09] ein anderer Algorithmus zur Bestimmung modularer Polynome vorgestellt, der, anstatt mit Laurentreihen zu arbeiten, die betreffenden Modulfunktionen an verschiedenen Punkten auswertet und anschließend durch Interpolation das gewünschte Ergebnis gewinnt. Durch diesen Ansatz erfordert der Algorithmus keine derartigen Ad-hoc-Rechnungen.

Mit den Ergebnissen erhalten wir nun folgendes Korollar aus Lemma 5.2.1.

Korollar 5.2.3. *Die universellen elliptischen Gauß-Summen $\tau_{\ell^2,n,\chi}$ besitzen eine Darstellung*

der Form

$$\tau_{\ell^2,n,\chi}(\tau) = \frac{Q(m_{\ell^2}(\tau), j(\tau))}{m_{\ell^2}(\tau)^k \frac{\partial M_{\ell^2}}{\partial Y}(m_{\ell^2}(\tau), j(\tau))} \tag{5.6}$$

für ein $k \geqslant 0$ *und ein Polynom* $Q(X,Y) \in \mathbb{C}[X,Y]$ *mit* $\deg_Y(Q) < 2v = \deg_Y(M_{\ell^2})$*, wobei* $v = \frac{(\ell-1)^2}{\mathrm{ggT}((\ell-1)^2, 24)}$ *gilt.*

Beweis. Offenbar haben $\mathfrak{w}^s_{\ell,\ell}$ und m_{ℓ^2} dasselbe Minimalpolynom $M_{\ell^2}(X,j)$, da j invariant unter S_0 ist. [ES05, Satz 9] impliziert daher $2v = \deg_Y(M_{\ell^2})$. Weiterhin folgt aus dem Satz, dass $M_{\ell^2}(c,Y)$ für $c \in \mathbb{C}^*$ ein Polynom in Y von Grad $2v$ ist. Analog zu Korollar 3.3.2 ergibt sich nun, dass m_{ℓ^2} auf $\mathbb{H}$ alle Werte aus $\mathbb{C}^*$ annimmt. Damit sind die holomorphen Funktionen in $\mathbb{C}(m_{\ell^2}(\tau))$ genau durch $\mathbb{C}[m_{\ell^2}(\tau), m_{\ell^2}(\tau)^{-1}]$ gegeben, womit die Aussage aus Lemma 5.2.1 folgt. □

Zur konkreten Berechnung dieses rationalen Ausdrucks ist wie in den Fällen von Primzahlen $N = \ell$ die Kenntnis der Präzision nötig, bis zu der die Laurentreihen der auftretenden Modulfunktionen berechnet werden müssen. Diese Aussage liefert

Proposition 5.2.4. *Seien* v *wie in Korollar 5.2.3 und* e_Δ *wie in Korollar 5.1.4. Zur Bestimmung des Ausdrucks* (5.6) *reicht es aus, die ersten*

$$\mathrm{prec}(\ell^2, n) = (2v + e_\Delta - 1)\ell^2 + \left\lceil (e_\Delta - 1)\frac{\ell}{2} \right\rceil \tag{5.7}$$

Terme der Laurentreihen zu berechnen.

Beweis. Der Beweis verläuft insgesamt sehr ähnlich zu demjenigen von Proposition 3.3.4. Wie dort erhalten wir durch Betrachten der Ordnungen der auftretenden Laurentreihen Schranken an die Ordnungen der Terme von $Q(m_{\ell^2}, j)$. Um die Ergebnisse aus [ES05] direkt verwenden zu können, arbeiten wir statt mit m_{ℓ^2} mit der dort betrachteten Funktion $n_{\ell^2} := \mathfrak{w}^s_{\ell,\ell}$. Aufgrund der genannten Korrespondenz zwischen $\Gamma_0(\ell^2)$ und $\Gamma^0(\ell^2)$ mittels S_0 ist klar, dass sich die Ergebnisse direkt übertragen.
Bei unseren Rechnungen verfolgen wir insbesondere die gleiche Grundidee wie in Proposition 3.3.4, einmal mit der Gleichung (5.6) entsprechenden Gleichung

$$\tau_{\ell^2,n,\chi}(S_0\tau)\frac{\partial M_{\ell^2}}{\partial Y}(n_{\ell^2}(\tau), j(\tau)) = \frac{Q(n_{\ell^2}(\tau), j(\tau))}{n_{\ell^2}(\tau)^k} \tag{5.8}$$

für n_{ℓ^2} zu arbeiten, in der die Ordnung der Laurentreihe $n_{\ell^2}(q(\tau))$ negativ ist und einmal eine Transformation $T \in \Gamma/\Gamma_0(\ell^2)$ darauf anzuwenden, sodass die Ordnung der Konjugierten $n_{\ell^2}(q(T\tau)))$ positiv ist. Wir geben nur einige Zwischenergebnisse der Rechnungen an, die leicht nachzuprüfen sind.

Zunächst betrachten wir die Gleichung

$$0 = M_{\ell^2}(n_{\ell^2}(q), j(q)) = \sum_{i=0}^{\ell^2+\ell} \sum_{k=0}^{2v} a_{i,k} n_{\ell^2}(q)^i j(q)^k \tag{5.9}$$

mit $a_{i,k} \in \mathbb{Z}$. Nach [ES05, Satz 6] gilt $\mathrm{ord}(n_{\ell^2}) = -\frac{v}{\ell^2}$. Vergleicht man die Ordnungen der verschiedenen Summanden wie in Lemma 3.3.1, so erhält man $\mathrm{ord}(n_{\ell^2}(q)^i j(q)^k) \geqslant -\left(2 - \frac{\ell-1}{\ell^2}\right) v$,

sofern $a_{i,k} \neq 0$ gilt, und daraus $\operatorname{ord}\left(\frac{\partial M_{\ell^2}}{\partial Y}(n_{\ell^2}(q), j(q))\right) \geqslant -\left(2 - \frac{\ell-1}{\ell^2}\right) v + 1$. Nun berechnen wir die Ordnung von $\tau_{\ell^2,n,\chi}(S_0\tau)$ in (5.8). Mit Lemma 6.1.1 zum Transformationsverhalten der Weierstraßschen $\wp$-Funktion ergibt sich $x(\zeta_N^a, q)|_{S_0} = x(q^{a/N}, q)$, analog gilt dies für y. Mit Formel (2.12) ergeben sich $\operatorname{ord}\left(p_1(q)|_{S_0}\right) = 0$ und $\operatorname{ord}(G_{\ell^2,n,\chi}(q)\big|_{S_0}) \geqslant \frac{1}{\ell^2}$ und insgesamt $\operatorname{ord}(\tau_{\ell^2,n,\chi}(q)\big|_{S_0}) \geqslant \frac{n}{\ell^2} - e_\Delta$. Für die Terme $n_{\ell^2}(q)^i j(q)^k$ auf der rechten Seite von (5.8) gilt also

$$\operatorname{ord}(n_{\ell^2}(q)^i j(q)^k) \geqslant -\left(2 - \frac{\ell-1}{\ell^2}\right) v - e_\Delta + \frac{n}{\ell^2} + 1 =: s_1. \tag{5.10}$$

Nun wenden wir auf die Gleichungen (5.8) und (5.9) die Transformation $T = \left(\begin{smallmatrix} \ell & -1 \\ 1 & 0 \end{smallmatrix}\right)$ an. Gemäß [ES05, Satz 6] besitzt $n_{\ell^2}(q)|_T$ die positive Ordnung $\frac{2v}{\ell-1}$. Mit $t := \operatorname{ggT}(2v, \ell-1)$ erhält man aus (5.9) die Schranke $\operatorname{ord}\left(\frac{\partial M_{\ell^2}}{\partial Y}(n_{\ell^2}(q), j(q))\Big|_T\right) \geqslant 2v\left(\frac{1}{t} - 1\right) + 1$. Außerdem erhält man $\operatorname{ord}\left(\tau_{\ell^2,n,\chi}(q)\big|_{S_0T}\right) \geqslant \frac{n}{\ell} - e_\Delta$. Dies ergibt wiederum für die Terme $(n_{\ell^2}(q)|_T)^i j(q)^k$ in (5.8) die Schranke

$$\frac{2iv}{\ell-1} - k = \operatorname{ord}((n_{\ell^2}(q)|_T)^i j(q)^k) \geqslant 2v\left(\frac{1}{t} - 1\right) + 1 + \frac{n}{\ell} - e_\Delta =: s_2.$$

Daraus folgt für $k \geqslant 0$

$$-\frac{iv}{\ell^2} - k \leqslant -\frac{iv}{\ell^2} \leqslant -\frac{\ell-1}{2\ell^2}(s_2 + k) \leqslant -\frac{\ell-1}{2\ell^2} s_2 =: s_3.$$

Mit Gleichung (5.10) schließen wir, dass die möglichen Ordnungen von $n_{\ell^2}(q)^i j(q)^k$ auf der rechten Seite von (5.8) in einem Bereich der Länge

$$\begin{aligned} s_3 - s_1 =& \frac{v(\ell-1)}{\ell^2} - \frac{v(\ell-1)}{t\ell^2} - \frac{n}{\ell^2} \cdot \frac{\ell-1}{2\ell} + (e_\Delta - 1)\frac{\ell-1}{2\ell^2} + 2v - \frac{v(\ell-1)}{\ell^2} + e_\Delta - \frac{n}{\ell^2} - 1 \\ =& \left(2 - \frac{\ell-1}{t\ell^2}\right) v + (e_\Delta - 1)\left(1 + \frac{\ell-1}{2\ell^2}\right) - \frac{n}{\ell^2}\left(1 + \frac{\ell-1}{2\ell}\right) \\ <& 2v + (e_\Delta - 1)\left(1 + \frac{1}{2\ell}\right) \end{aligned}$$

enthalten sind. Da $\operatorname{ord}(n_\ell^2(q)^i j(q)^k) = -\frac{iv}{\ell^2} - k = -\frac{iv + k\ell^2}{\ell^2}$ und $v \mid (\ell-1)^2$, also $\operatorname{ggT}(v, \ell) = 1$ gilt, können auch unter der Einschränkung $0 \leqslant k \leqslant 2v - 1$ innerhalb dieses Bereichs alle Ordnungen mit Schrittweite $\frac{1}{\ell^2}$ realisiert werden. Daher müssen höchstens

$$\operatorname{prec}(\ell^2, n) = (2v + e_\Delta - 1)\ell^2 + \left\lceil (e_\Delta - 1)\frac{\ell}{2} \right\rceil$$

Glieder der auftretenden Laurentreihen berechnet werden. □

Bei der Berechnung des Polynoms Q in (5.6) bzw. (5.8) tritt wie bei der Verwendung von a_ℓ für Primzahlen ℓ das Problem auf, dass $\operatorname{ord}(n_{\ell^2}(q)^i j(q)^k) = -\frac{iv}{\ell^2} - k = \operatorname{ord}(n_{\ell^2}(q)^{i-\ell^2} j(q)^{k+v})$ für $0 \leqslant k \leqslant v - 1$ gilt, also jeweils zwei Summanden die gleiche Ordnung aufweisen. Dieses Problem lässt sich jedoch auf die gleiche Weise wie für a_ℓ dadurch lösen, dass man abwechselnd (5.6) und die durch Anwendung der Transformation $T = \left(\begin{smallmatrix} \ell & -1 \\ 1 & 0 \end{smallmatrix}\right)$ daraus entstehende Gleichung betrachtet, womit Q analog zu Algorithmus 5 berechnet werden kann.

Ist der Ausdruck (5.6) berechnet, so kann er analog zu den Ausführungen aus Abschnitt 4 auf eine konkrete elliptische Kurve $E/\mathbb{F}_p$ übertragen werden, um die linke Seite der bereits in (5.3) aufgeführten Gleichung

$$\frac{G_{\ell^i,n,\chi}(E)^m}{G_{\ell^i,n,\chi^m}(E)}(G_{\ell^i,n,\chi}(E)^n)^q = \chi^{-m}(\lambda_i)$$

und damit den Index von λ_i in $(\mathbb{Z}/\ell^i\mathbb{Z})^*$ modulo n (in diesem Fall für $i = 2$) zu bestimmen. Wir bemerken, dass sich nach den Überlegungen aus Abschnitt 5.1 insbesondere Lemma 4.4.1 mit der Definition der universellen elliptischen Jacobi-Summen ebenso auf Primzahlpotenzen ℓ^i verallgemeinern lässt.

Wie in Abschnitt 5.1 ausgeführt, erhält man allgemein λ_i als Hensel-Lift der Nullstelle λ von $\chi(\phi_p)$ modulo ℓ. Sei g ein Erzeuger von $(\mathbb{Z}/\ell^i\mathbb{Z})^*$, sodass $g_1 = g \mod \ell$ ein Erzeuger von $(\mathbb{Z}/\ell\mathbb{Z})^*$ ist. Nun sei $\lambda_i = g^{c(\lambda_i)}$ in $(\mathbb{Z}/\ell^i\mathbb{Z})^*$ und $\lambda \equiv g_1^{c(\lambda)} \mod \ell$. Dann folgt

$$g_1^{c(\lambda)} \equiv \lambda \equiv \lambda_i \equiv g^{c(\lambda_i)} \equiv g_1^{c(\lambda_i)} \mod \ell,$$

also $c(\lambda_i) \equiv c(\lambda) \mod \ell - 1$. Ist der Index $c(\lambda)$ von λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ bekannt, genügt es somit wegen $\varphi(\ell^i) = (\ell-1)\ell^{i-1}$, $c(\lambda_i)$ modulo $n = \ell^{i-1}$ zu bestimmen, um anschließend mithilfe des Chinesischen Restsatzes den Wert $c(\lambda_i)$ und damit t modulo ℓ^i zu berechnen.

Da die Laufzeiten für die Berechnung der universellen elliptischen Gauß-Summen und die Übertragung auf eine konkrete Kurve $E/\mathbb{F}_p$ mindestens linear von $e_\Delta \approx \frac{n}{6}$ abhängen, wie dies in Abschnitt 3.3 und 4.6 für Primzahlen ℓ gezeigt wurde und für Primzahlquadrate ℓ^2 aus Proposition 5.7 folgt, kann man nur für verhältnismäßig kleine Werte von n einen effizienten Algorithmus erwarten, wie in 4.6 ausgeführt. Bei Verwendung der Gauß-Summen für Primzahlen ℓ wurde dort $n \leqslant \sqrt{\ell}$ für notwendig angesehen. Benutzt man Primzahlpotenzen ℓ^i, so erhält man ein solches Verhältnis genau für $i = 2$ und $n = \ell$. Für größere Werte von i muss man offenbar $n = \ell^{i-1}$ wählen, sodass das Verhältnis unter dem Gesichtspunkt der Effizienz zunehmend ungünstiger wird. Abgesehen von den weiter oben angesprochenen Schwierigkeiten bei Rechnungen mit Modulfunktionen für $\Gamma_0(\ell^i)$ mit $i \geqslant 3$ ist dies der Grund, warum wir uns in der genaueren Ausarbeitung auf den Fall $i = 2$ beschränkt haben.
Ist $N = \ell^2$, so ist für die koprimen Primpotenzteiler n von $\varphi(N)$ jedoch stets die Bedingung $n \leqslant \sqrt{N}$ erfüllt. Für $N = \ell$ ist die analoge Bedingung laut den Ausführungen in Abschnitt 4.6 asymptotisch lediglich für ca. 30% der Primzahlen ℓ erfüllt. Somit könnte die Verwendung der Gauß-Summen für Primzahlquadrate $N = \ell^2$ in einigen Fällen eine bessere Laufzeit aufweisen. Dem gegenüberzustellen ist jedoch die Tatsache, dass der Wert v, von dem die Laufzeit ebenfalls abhängt, gemäß seiner Definition in Korollar 5.2.3 im besten Fall den Wert $\frac{(\ell-1)^2}{24}$ aufweist (im Fall $\ell - 1 \equiv 0 \mod 12$). Unter Verwendung der Funktion a_ℓ für Primzahlen ℓ können jedoch durchschnittlich deutlich kleinere Werte des zugehörigen $v(a_\ell)$ erreicht werden. Abgesehen davon ufert der benötigte Speicherplatz gemäß Abschnitt 4.6 bereits für $\ell \approx 200$ aus, sodass ohne bessere neue Ideen im praktikablen Bereich ohnehin nur eine Handvoll Primzahlquadrate verwendet werden könnte.

6 Universelle elliptische Gauß-Summen im Atkin-Fall

In diesem Abschnitt sollen die bisher beschriebenen Ideen zur Bestimmung universeller elliptischer Gauß-Summen in einer Weise modifiziert werden, die es ermöglicht, auch im Atkin-Fall die Spur t des Frobenius-Homomorphismus ϕ_p modulo kleinen Primzahlen zu bestimmen.

6.1 Definition

Wir orientieren uns an den Aussagen in den Abschnitten 2.1.3 und 2.2. Den Ausgangspunkt unserer Überlegungen bildet das folgende Resultat, das Lemma 2.2.8 verallgemeinert.

Lemma 6.1.1. *Seien $\tau \in \mathbb{H}$, $v_1, v_2 \in \mathbb{Z}$ und $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Dann gelten*

$$\wp\left(\frac{v_1\tau + v_2}{\ell}, \tau\right)\Big|_\gamma = (c\tau + d)^2 \wp\left(\frac{v_1(a\tau + b) + v_2(c\tau + d)}{\ell}, \tau\right), \tag{6.1}$$

$$\wp'\left(\frac{v_1\tau + v_2}{\ell}, \tau\right)\Big|_\gamma = (c\tau + d)^3 \wp'\left(\frac{v_1(a\tau + b) + v_2(c\tau + d)}{\ell}, \tau\right). \tag{6.2}$$

Beweis. Es gilt

$$\wp\left(\frac{v_1\tau + v_2}{\ell}, \tau\right)\Big|_\gamma = \wp\left(\frac{v_1\frac{a\tau+b}{c\tau+d} + v_2}{\ell}, \frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 \wp\left(\frac{v_1(a\tau + b) + v_2(c\tau + d)}{\ell}, \tau\right),$$

wobei man die zweite Gleichheit durch Anwendung von Lemma 2.2.8 erhält. Für die Ableitung von $\wp$ geht man analog vor. □

Mithilfe dieser Aussage werden wir eine Modulfunktion für die nun definierte Gruppe $\Gamma_0^0(\ell)$ konstruieren.

Lemma 6.1.2. *Sei ℓ eine Primzahl. Dann ist durch*

$$\Gamma_0^0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv c \equiv 0 \mod \ell \right\} \subseteq \Gamma$$

eine Untergruppe von Γ gegeben und es gilt $\Gamma(\ell) \subseteq \Gamma_0^0(\ell) \subseteq \Gamma_0(\ell)$. Ein Repräsentantensystem für $\Gamma/\Gamma_0^0(\ell)$ ist gegeben durch

$$S_{\lambda,k} = \begin{pmatrix} \lambda & -1 + \lambda k \\ 1 & k \end{pmatrix} \quad \textit{für} \quad 0 \leqslant \lambda, k < \ell, \quad S_{\lambda,\ell} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \textit{für} \quad 0 \leqslant \lambda < \ell.$$

Beweis. Die Tatsache, dass $\Gamma_0^0(\ell)$ eine Gruppe bildet, sowie die Inklusionen sind trivial. Um die Korrektheit des Repräsentantensystems zu zeigen, bemerken wir, dass die Matrizen

$$T_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{für} \quad 0 \leqslant \lambda < \ell \tag{6.3}$$

die Nebenklassen $\Gamma_0(\ell)/\Gamma_0^0(\ell)$ repräsentieren, wie man sich leicht überlegt. Multipliziert man die T_λ mit den Matrizen S_k, $k = 0, \ldots, \ell$, aus [Mül95, S. 54] und Lemma 2.1.16, die ein Repräsentantensystem für $\Gamma/\Gamma_0(\ell)$ bilden, so erhält man genau die Behauptung. □

Korollar 6.1.3. *Seien ℓ eine Primzahl, $n \mid \ell - 1$ und $\chi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mu_n$ ein Dirichlet-Charakter von Ordnung n. Sei ξ die den beiden ℓ-Torsionspunkten $P = (x(\zeta_\ell, q), y(\zeta_\ell, q))$, $Q_0 = (x(q^{\frac{1}{\ell}}, q), y(q^{\frac{1}{\ell}}, q))$ auf der Tate-Kurve vermöge der Weil-Paarung e_ℓ zugeordnete ℓ-te Einheitswurzel und $G_{\chi^{-1}}(\xi)$ die entsprechende zyklotomische Gauß-Summe. Sei $G_{\ell,n,\chi}(q)$ wie in Korollar 2.2.9. Definiere*

$$H_{\ell,n,\chi}(q) = \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda) V(q^{\frac{\lambda}{\ell}}, q) = \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda)(\lambda Q_0)_V \quad \textit{für} \quad V = \begin{cases} x, & n \equiv 1 \mod 2, \\ y, & n \equiv 0 \mod 2. \end{cases}$$

Dann besitzt die Funktion

$$\sigma_{\ell,n,\chi}(q) := \frac{G_{\ell,n,\chi}(q) H_{\ell,n,\chi}(q) p_1(q)^r G_{\chi^{-1}}(\xi)}{\Delta(q)} \quad \textit{für} \quad r = \begin{cases} 4, & n \equiv 1 \mod 2, \\ 3, & n \equiv 0 \mod 2, \end{cases}$$

die wir als universelle elliptische Gauß-Summe (für Atkin-Primzahlen) *bezeichnen, die folgenden Eigenschaften:*

1. *$\sigma_{\ell,n,\chi}(q)$ ist eine Modulfunktion von Gewicht 0 für die Gruppe $\Gamma_0^0(\ell)$.*
2. *$\sigma_{\ell,n,\chi}(q)$ ist holomorph auf $\mathbb{H}$.*
3. *$\sigma_{\ell,n,\chi}(q)$ ist invariant unter Transformationen der Form $(P, Q_0) \mapsto (aP, bQ_0)$ für Werte $a, b \in \mathbb{F}_\ell^*$.*
4. *$\sigma_{\ell,n,\chi}(q)$ hat Koeffizienten in $\mathbb{Q}[\zeta_n]$.*

Beweis. 1. Zunächst rechnen wir unter Benutzung des gerade gezeigten Lemmas 6.1.1 für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0^0(\ell)$ und $v_1 \in \mathbb{F}_\ell^*$ ähnlich wie in Korollar 2.2.9

$$x\left(q^{\frac{v_1}{\ell}}, q\right)\Big|_\gamma = k\wp\left(\frac{v_1\tau}{\ell}, \tau\right)\Big|_\gamma = k(c\tau + d)^2 \wp\left(\frac{v_1(a\tau + b)}{\ell}, \tau\right) = (c\tau + d)^2 x\left(q^{\frac{v_1 a}{\ell}}, q\right).$$

Wir benutzen dabei die Formeln aus Lemma 2.2.4 (mit $k = \frac{1}{(2\pi i)^2}$) für den Übergang zur Weierstraßschen $\wp$-Funktion (man bemerke, dass $|q| < |q^{\frac{v_1}{\ell}}| < 1$ gilt) und verwenden im letzten Schritt $b \equiv 0 \mod \ell$. Analog zeigt man auch

$$y\left(q^{\frac{v_1}{\ell}}, q\right)\Big|_\gamma = (c\tau + d)^3 y\left(q^{\frac{v_1 a}{\ell}}, q\right).$$

Hieraus wiederum lässt sich das Transformationsverhalten von $H_{\ell,n,\chi}(q)$ unter γ bestimmen als

$$\begin{aligned} H_{\ell,n,\chi}(q)|_\gamma &= \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda)\ V\left(q^{\frac{\lambda}{\ell}}, q\right)\Big|_\gamma = (c\tau + d)^e \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda) V\left(q^{\frac{\lambda a}{\ell}}, q\right) \\ &= (c\tau + d)^e \chi^{-1}(a) H_{\ell,n,\chi}(q), \end{aligned}$$

wobei $e = 2$ für $n \equiv 1 \mod 2$ und $e = 3$ sonst gilt. Mit der Kenntnis über das Transformationsverhalten der übrigen in der Definition von $\sigma_{\ell,n,\chi}(q)$ auftauchenden Funktionen

erhalten wir schließlich

$$\sigma_{\ell,n,\chi}(q)|_\gamma = \sigma_{\ell,n,\chi}(q)\frac{(c\tau+d)^{2e+2r}\chi^{-1}(d)\chi^{-1}(a)}{(c\tau+d)^{12}} = \sigma_{\ell,n,\chi}(q)\chi^{-1}(ad) = \sigma_{\ell,n,\chi}(q).$$

Im letzten Schritt haben wir $ad \equiv 1 \mod \ell$ benutzt, was wegen $b \equiv c \equiv 0 \mod \ell$ gilt. Es bleibt noch zu zeigen, dass $\sigma_{\ell,n,\chi}(q)$ meromorph an den Spitzen ist, also in der Fourierreihenentwicklung von $\sigma_{\ell,n,\chi}(q)|_{S_{\lambda,k}}$ mit den Matrizen $S_{\lambda,k}$ aus Lemma 6.1.2 nur endlich viele negative Exponenten auftauchen. Mit Lemma 6.1.1 folgt jedoch für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ allgemein

$$x\left(q^{\frac{v_1}{\ell}}\zeta_\ell^{v_2}, q\right)\Big|_\gamma = (c\tau+d)^2 x\left(q^{\frac{v_1a+v_2c}{\ell}}\zeta_\ell^{v_1b+v_2d}, q\right)$$

und eine analoge Aussage für $y(\cdot, q)$. Berechnet man den entstehenden Ausdruck mit Formel (2.12) bzw. (2.13), so ist offensichtlich, dass in der q-Entwicklung nur endlich viele negative Exponenten auftauchen. Aus der Definition dieser Ausdrücke folgt dies auch für $G_{\ell,n,\chi}(q)|_{S_{\lambda,k}}$, $H_{\ell,n,\chi}(q)|_{S_{\lambda,k}}$ und $p_1(q)|_{S_{\lambda,k}}$ sowie schließlich für $\sigma_{\ell,n,\chi}(q)|_{S_{\lambda,k}}$.

2. Aus Formel (2.10) liest man sofort ab, dass $x(q^{\frac{v}{\ell}}, q)$ genau dann Polstellen aufweist, wenn $q^n = 1$ oder $q^n = q^{\frac{v}{\ell}}$ für ein $n \in \mathbb{Z}$ gilt. Wegen $\tau \in \mathbb{H}$ gilt jedoch $|q| < 1$, die zweite Möglichkeit ist für $0 < v < \ell$ ausgeschlossen. Damit ist $H_{\ell,n,\chi}(q)$ nach Konstruktion holomorph auf $\mathbb{H}$. Nun folgt aus dem Wissen über die übrigen in $\sigma_{\ell,n,\chi}(q)$ auftauchenden Funktionen sofort die Behauptung.

3. Es ist $(aP, bQ_0) = ((x,y)(\zeta_\ell^a, q), (x,y)(q^{\frac{b}{\ell}}, q))$. Offenbar sind $\Delta(q)$ und $p_1(q)$ unter dieser Transformation invariant. Weiterhin gilt

$$\sum_{\lambda\in\mathbb{F}_\ell^*}\chi(\lambda)V(q^{\frac{b\lambda}{\ell}}, q) = \chi^{-1}(b)\sum_{\lambda\in\mathbb{F}_\ell^*}\chi(b\lambda)V(q^{\frac{b\lambda}{\ell}}, q) = \chi^{-1}(b)H_{\ell,n,\chi}(q)$$

und analog $\sum_{\lambda\in\mathbb{F}_\ell^*}\chi(\lambda)V(\zeta_\ell^{a\lambda}, q) = \chi^{-1}(a)G_{\ell,n,\chi}(q)$, wie schon in Korollar 2.2.9 gezeigt wurde. Zusätzlich transformiert sich der Term $G_{\chi^{-1}}(\xi)$ zu

$$G_{\chi^{-1}}(e_\ell(aP, bQ_0)) = G_{\chi^{-1}}(e_\ell(P,Q_0)^{ab}) = G_{\chi^{-1}}(\xi^{ab}) = \chi(ab)G_{\chi^{-1}}(\xi),$$

wie aus den Eigenschaften der Weil-Paarung und zyklotomischer Gauß-Summen folgt. Durch Multiplikation der entstehenden Faktoren sehen wir, dass $\sigma_{\ell,n,\chi}(q)$ unter der Transformation invariant bleibt.

4. Dies folgt aus bereits bewiesenen Tatsachen. Offensichtlich liegen die Koeffizienten von $\sigma_{\ell,n,\chi}(q)$ in $\mathbb{Q}[\zeta_\ell, \zeta_n]$. Wir wählen einen Erzeuger c von $\mathbb{F}_\ell^*$ und betrachten die Wirkung des Homomorphismus $\sigma : \zeta_\ell \mapsto \zeta_\ell^c$, der $\mathrm{Gal}(\mathbb{Q}[\zeta_\ell, \zeta_n]/\mathbb{Q}[\zeta_n])$ erzeugt, auf $\sigma_{\ell,n,\chi}(q)$. Laut Korollar 2.2.10 gilt

$$\sigma(G_{\ell,n,\chi}(q)) = \chi^{-1}(c)G_{\ell,n,\chi}(q)$$

und analog zeigt man

$$\sigma(G_{\chi^{-1}}(\xi)) = \chi(c)G_{\chi^{-1}}(\xi).$$

Da die übrigen Terme in der Definition von $\sigma_{\ell,n,\chi}(q)$ unter σ invariant sind, liegen die

Koeffizienten von $\sigma_{\ell,n,\chi}(q)$ im Fixkörper dieses Homomorphismus.

□

Bemerkung 6.1.4. Auf der elliptischen Kurve $E_\tau \cong \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ gilt gemäß [Lan87]

$$e_\ell\left(\frac{1}{\ell}, \frac{\tau}{\ell}\right) = \exp\left(\frac{2\pi i}{\ell}\right).$$

Über den Isomorphismus $E_q \cong E_\tau$ aus Satz 2.2.7 ergibt sich mit der in Korollar 6.1.3 genannten Wahl der Punkte P, Q_0 für konkrete Rechnungen direkt

$$\xi = e_\ell(P, Q_0) = \exp\left(\frac{2\pi i}{\ell}\right).$$

6.2 Rationale Darstellung

Ähnlich zu unserem Vorgehen für die universellen elliptischen Gauß-Summen $\tau_{\ell,n}(q)$ möchten wir nun die Ausdrücke $\sigma_{\ell,n}(q)$ in Abhängigkeit von $j(\tau)$ und anderen Modulfunktionen darstellen. Tatsächlich wird unsere Darstellung außer von der j-Invarianten von zwei weiteren Modulfunktionen abhängen. Den Ansatz dafür liefert folgendes

Lemma 6.2.1. *Sei $f(\tau) \in \mathbf{A}_0(\Gamma_0(\ell))\backslash\mathbf{A}_0(\Gamma)$ eine Modulfunktion von Gewicht 0 und sei die Matrix $S_0 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ wie in Lemma 2.1.16. Dann gilt*

$$\mathbf{A}_0(\Gamma_0^0(\ell)) = \mathbb{C}(j(\tau), f(\tau), f(S_0\tau)). \tag{6.4}$$

Beweis. Wir bemerken zunächst, dass

$$\Gamma_0^0(\ell) = \Gamma_0(\ell) \cap \Gamma^0(\ell) \quad \text{mit} \quad \Gamma^0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv 0 \mod \ell \right\} \tag{6.5}$$

gilt. Nun folgt mit den galois-theoretischen Aussagen zu den Körpern der Modulfunktionen von Gewicht 0 für gewisse Untergruppen von Γ (insbesondere Korollar 2.1.14)

$$\mathrm{Gal}(\mathbf{A}_0(\Gamma(\ell))/\mathbf{A}_0(\Gamma_0^0(\ell))) = \mathrm{Gal}(\mathbf{A}_0(\Gamma(\ell))/\mathbf{A}_0(\Gamma_0(\ell))) \cap \mathrm{Gal}(\mathbf{A}_0(\Gamma(\ell))/\mathbf{A}_0(\Gamma^0(\ell))),$$

was direkt

$$\mathbf{A}_0(\Gamma_0^0(\ell)) = \mathbf{A}_0(\Gamma_0(\ell))\mathbf{A}_0(\Gamma^0(\ell)) \tag{6.6}$$

impliziert. Weiterhin rechnen wir für $a, b, c, d \in \mathbb{Z}$

$$S_0^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} S_0 = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix},$$

woraus $\Gamma^0(\ell) = S_0^{-1}\Gamma_0(\ell)S_0$ folgt. Aus dieser Beobachtung schließen wir wiederum, dass die Funktion $f(S_0\tau)$ in $\mathbf{A}_0(\Gamma^0(\ell))$ liegt. Schreiben wir $\gamma \in \Gamma^0(\ell)$ als $\gamma = S_0^{-1}\gamma' S_0$ für ein $\gamma' \in \Gamma_0(\ell)$, so ergibt sich nämlich

$$f(S_0\gamma\tau) = f(\gamma' S_0\tau) = f(S_0\tau). \tag{6.7}$$

Nach Satz 2.1.11 gilt $\mathbf{A}_0(\Gamma_0(\ell)) = \mathbb{C}(j(\tau), f(\tau))$ und analog zum dortigen Beweis erhält man nun $\mathbf{A}_0(\Gamma^0(\ell)) = \mathbb{C}(j(\tau), f(S_0\tau))$, was mit Gleichung (6.6) die Behauptung ergibt. □

Analog zu Korollar 2.1.20 erhalten wir weiterhin

Lemma 6.2.2. *Sei $g(\tau) \in \mathbf{H}_0(\Gamma_0^0(\ell))\backslash\mathbf{H}_0(\Gamma_0(\ell))$ eine holomorphe Modulfunktion und sei $k(\tau) \in \mathbf{H}_0(\Gamma_0^0(\ell))\backslash\mathbf{H}_0(\Gamma_0(\ell))$ mit Minimalpolynom $Q_k(X)$ über $\mathbf{A}_0(\Gamma_0(\ell))$ mit $\deg(Q_k) = \ell$. Dann besitzt $g(\tau)$ eine Darstellung der Form*

$$g(\tau) = \frac{\sum_{i=0}^{\ell-1} a_i k(\tau)^i}{\frac{\partial Q_k}{\partial X}(k(\tau))} \tag{6.8}$$

mit $a_i \in \mathbf{H}_0(\Gamma_0(\ell))$.

Beweis. Wir benutzen Lemma 2.1.19 völlig analog zum Beweis von Korollar 2.1.20. Wir wählen $K = \mathbf{A}_0(\Gamma_0(\ell))$, $L = \mathbf{A}_0(\Gamma_0^0(\ell))$ und $\alpha = k(\tau)$ mit Minimalpolynom $f(X) = Q_k(X)$, weiterhin gelte

$$\mathcal{O} = \{h(\tau) \in K : h(\tau) \text{ holomorph}\} = \mathbf{H}_0(\Gamma_0(\ell)).$$

Da k nach Voraussetzung holomorph ist, gilt dies für alle Elemente $z \in \mathcal{O}[k]$ und somit auch für $g(\tau)z$ und $\mathrm{Tr}_{L/K}(g(\tau)z)$. Damit folgt $g(\tau) \in C_k$ (s. Lemma 2.1.19), was die Behauptung impliziert. □

Die vorangehenden Lemmata legen das folgende Vorgehen zur Bestimmung eines Ausdrucks für $\sigma_{\ell,n}$ nahe: Wählen wir eine holomorphe Modulfunktion $f(\tau) \in \mathbf{H}_0(\Gamma_0(\ell))\backslash\mathbf{H}_0(\Gamma)$, so ist aus dem Beweis von Lemma 6.2.1 ersichtlich, dass $f(S_0\tau) \in \mathbf{H}_0(\Gamma_0^0(\ell))\backslash\mathbf{H}_0(\Gamma_0(\ell))$ gilt. Kennen wir das Minimalpolynom $Q_{f,S_0}(X)$ von $f(S_0\tau)$ über $\mathbf{A}_0(\Gamma_0(\ell))$, so können wir zunächst mithilfe von Lemma 6.2.2 eine Darstellung für $\sigma_{\ell,n}$ bestimmen. Da die auftretenden Koeffizienten a_i in $\mathbf{H}_0(\Gamma_0(\ell))$ liegen, lässt sich im zweiten Schritt für jeden dieser Koeffizienten eine Darstellung in Abhängigkeit von $j(\tau)$ und $f(\tau)$ gemäß Korollar 2.1.20 oder Proposition 2.1.21 bestimmen, was insgesamt die gewünschte Darstellung in Abhängigkeit von $j(\tau)$, $f(\tau)$ und $f(S_0\tau)$ ergibt, was wir als

$$\sigma_{\ell,n,\chi}(q) = R(j(\tau), f(\tau), f(S_0\tau)) \tag{6.9}$$

schreiben. Wie in Abschnitt 3.3 müssen wir angeben, bis zu welcher Präzision die Laurentreihen der verschiedenen Modulfunktionen zu berechnen sind, um die Darstellungen ermitteln zu können. Wir führen diese Untersuchung für die Wahl $f(\tau) = m_\ell(\tau)$ durch und schreiben dabei $m_{\ell,2}(\tau) := m_\ell(S_0\tau)$.

Wir benötigen zunächst Aussagen über das Transformationsverhalten der η-Funktion.

Satz 6.2.3. *[Web08, S. 113, 126, 130] Die η-Funktion transformiert sich unter Wirkung von $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ mittels*

$$\eta(\gamma\tau) = \varepsilon \cdot \sqrt{c\tau + d} \cdot \eta(\tau).$$

Die Werte für die 24-te Einheitswurzel ε sind gegeben durch

$$\varepsilon = \begin{cases} \left(\frac{c}{d}\right) i^{(d-1)/2} \exp\left(\frac{\pi i}{12}(d(b-c) - (d^2-1)ac)\right), & d \equiv 1 \mod 2, d > 0, \\ \left(\frac{d}{c}\right) i^{(1-c)/2} \exp\left(\frac{\pi i}{12}(c(a+d) - (c^2-1)bd - 3)\right), & c \equiv 1 \mod 2, c > 0. \end{cases}$$

Korollar 6.2.4. *Es gelten $m_{\ell,2}(\tau) = \ell^s m_\ell\left(\frac{\tau}{\ell}\right)^{-1}$ sowie $w_\ell(m_{\ell,2}(\tau)) = m_\ell(\ell\tau)$.*

Beweis. Wir rechnen

$$\begin{aligned} m_{\ell,2}(\tau) =& m_\ell(S_0\tau) = \ell^s \left(\frac{\eta(\ell S_0\tau)}{\eta(S_0\tau)}\right)^{2s} = \ell^s \left(\frac{\eta\left(S_0\frac{\tau}{\ell}\right)}{\eta(S_0\tau)}\right)^{2s} = \ell^s \left(\frac{-i\sqrt{i\frac{\tau}{\ell}}\cdot\eta\left(\frac{\tau}{\ell}\right)}{-i\sqrt{i\tau}\cdot\eta(\tau)}\right)^{2s} \\ &= \left(\frac{\eta\left(\frac{\tau}{\ell}\right)}{\eta(\tau)}\right)^{2s} = \ell^s m_\ell\left(\frac{\tau}{\ell}\right)^{-1} \end{aligned} \tag{6.10}$$

sowie

$$w_\ell(m_{\ell,2}(\tau)) = \ell^s \left(\frac{\eta\left(\ell S_0 \left(\begin{smallmatrix}0 & -1\\ \ell & 0\end{smallmatrix}\right)\tau\right)}{\eta\left(S_0\left(\begin{smallmatrix}0 & -1\\ \ell & 0\end{smallmatrix}\right)\tau\right)}\right)^{2s} = \ell^s \left(\frac{\eta(\ell^2\tau)}{\eta(\ell\tau)}\right)^{2s} = m_\ell(\ell\tau). \tag{6.11}$$

□

Aus der Definition des Minimalpolynoms in Lemma 2.1.16 sehen wir sofort, dass die Funktion $m_{\ell,2}(\tau) = m_\ell(S_0\tau)$ als Konjugierte von $m_\ell(\tau)$ über $\mathbb{C}(j(\tau))$ dasselbe Minimalpolynom $M_\ell(X, j(\tau))$ hat. Damit ergibt sich das Minimalpolynom von $m_{\ell,2}(\tau)$ über $\mathbf{A}_0(\Gamma_0(\ell))$ als $M_{\ell,2}(X) = \frac{M_\ell(X,j(\tau))}{X-m_\ell(\tau)}$. Nun sind wir in der Lage, die folgende Aussage zu zeigen:

Lemma 6.2.5. *Seien $\sigma_{\ell,n}(q)$, $m_\ell(q)$, $m_{\ell,2}(q)$ sowie $j(q)$ bis zur Präzision*

$$\operatorname{prec}(\ell, n) = (\ell^2 + \ell + 1)v - 1$$

berechnet, wobei $v = \frac{\ell-1}{\operatorname{ggT}(\ell-1,12)} = \operatorname{ord}(m_\ell)$ ist. Dann kann ein rationaler Ausdruck für $\sigma_{\ell,n}(q)$ in Abhängigkeit von den anderen drei Modulfunktionen eindeutig bestimmt werden.

Beweis. Zur Berechnung der benötigten Präzision gehen wir in zwei Schritten vor. Zunächst bestimmen wir Schranken an die Ordnung der Koeffizienten a_i aus Gleichung (6.8), aus denen sich dann analog zu Proposition 3.3.4 Schranken an die erforderliche Präzision ergeben.

Gemäß (6.8) gilt

$$\sigma_{\ell,n}(q) \underbrace{\frac{\partial M_{\ell,2}}{\partial X}(m_{\ell,2}(q))}_{=:N} = \sum_{i=0}^{\ell-1} a_i m_{\ell,2}(q)^i. \tag{6.12}$$

Unter Benutzung von (6.10) erhält man $\operatorname{ord}(m_\ell) = v$, $\operatorname{ord}(m_{\ell,2}) = -\frac{v}{\ell}$ und damit

$$\begin{aligned} \operatorname{ord}(N) &= \operatorname{ord}\left(\frac{\frac{\partial M_\ell}{\partial X}(m_{\ell,2}, j)(m_{\ell,2} - m_\ell) - M_\ell(m_{\ell,2}, j)}{(m_{\ell,2} - m_\ell)^2}\right) \\ &= \min\left(\operatorname{ord}\left(\frac{\partial M_\ell}{\partial X}(m_{\ell,2}, j)\right) - \frac{v}{\ell}, \operatorname{ord}(M_\ell(m_{\ell,2}, j))\right) + \frac{2v}{\ell}. \end{aligned}$$

Aus Lemma 3.3.1 ergibt sich, wenn der Koeffizient $a_{i,k}$ im Polynom M_ℓ nicht verschwindet,

$$iv \leqslant (v-k)\ell + v \quad \Rightarrow \quad -\frac{iv}{\ell} - k \geqslant -v - \frac{v}{\ell} \quad \Rightarrow \quad \operatorname{ord}(M_\ell(m_{\ell,2}, j)) \geqslant -v - \frac{v}{\ell}.$$

Analog erhält man $\operatorname{ord}\left(\frac{\partial M_\ell}{\partial X}(m_{\ell,2}, j)\right) \geqslant -v$, was $\operatorname{ord}(N) \geqslant -v + \frac{v}{\ell}$ ergibt.
Lässt man w_ℓ auf (6.12) wirken, so erhält man unter Verwendung von (6.11) die Aussage

$\operatorname{ord}(m^*_{\ell,2}) = v\ell$, was in ähnlicher Weise $\operatorname{ord}(M_\ell(m^*_{\ell,2}, j^*)) \geqslant 0$, $\operatorname{ord}\left(\frac{\partial M_\ell}{\partial X}(m^*_{\ell,2}, j^*)\right) \geqslant -v\ell$ und damit $\operatorname{ord}(N^*) \geqslant v(1-\ell)$ impliziert.
Benutzt man die Definition von $\sigma_{\ell,n}$, so ergeben sich mit den Überlegungen aus Abschnitt 3.3 und der Definition von $H_{\ell,n}$ weiterhin die Aussagen

$$\begin{aligned}\operatorname{ord}(\sigma_{\ell,n}) &= \operatorname{ord}(G_{\ell,n}) + \operatorname{ord}(H_{\ell,n}) + r\operatorname{ord}(p_1) - \operatorname{ord}(\Delta) \geqslant 0 + \frac{1}{\ell} + 0 - 1 = -1 + \frac{1}{\ell},\\ \operatorname{ord}(\sigma^*_{\ell,n}) &= \operatorname{ord}(G^*_{\ell,n}) + \operatorname{ord}(H^*_{\ell,n}) + r\operatorname{ord}(p^*_1) - \operatorname{ord}(\Delta^*) \geqslant 1 + 0 + 0 - \ell = 1 - \ell,\end{aligned}$$

woraus insgesamt

$$\operatorname{ord}(\sigma_{\ell,n}N) \geqslant -v - 1 + \frac{v+1}{\ell}, \quad \operatorname{ord}(\sigma^*_{\ell,n}N^*) \geqslant 1 - \ell + v(1-\ell)$$

folgt. Aus Gleichung (6.12) erhält man

$$\begin{aligned}\operatorname{ord}(a_i) &\geqslant \operatorname{ord}(\sigma_{\ell,n}Nm_{\ell,2}^{-i}) \geqslant -v - 1 + \frac{v+1}{\ell} + \frac{iv}{\ell} \quad \Rightarrow \quad \operatorname{ord}(a_i) \geqslant -v,\\ \operatorname{ord}(a^*_i) &\geqslant \operatorname{ord}(\sigma^*_{\ell,n}N^*(m^*_{\ell,2})^{-i}) \geqslant 1 - \ell + v(1-\ell) - iv\ell \geqslant v + 1 - v\ell - \ell - (\ell-1)v\ell\\ &= -\ell^2 v - \ell + v + 1. \end{aligned} \tag{6.13}$$

Nun betrachten wir die Gleichung

$$a_i(q)\underbrace{\frac{\partial M_\ell}{\partial Y}(m_\ell(q), j(q))}_{=:M} = \sum_{i=i_1}^{i_2}\sum_{k=0}^{v-1} b_{i,k}m_\ell(q)^i j(q)^k \tag{6.14}$$

laut Proposition 2.1.21, wobei wir völlig analog zu Proposition 3.3.4 vorgehen. Dort wurde bereits $\operatorname{ord}(M) \geqslant 1$, $\operatorname{ord}(M^*) \geqslant -(v-1)\ell - v$ gezeigt, was

$$\operatorname{ord}(a_iM) \geqslant 1 - v, \quad \operatorname{ord}(a^*_iM^*) \geqslant -\ell^2 v - \ell + v + 1 - (v-1)\ell - v = -(\ell^2+\ell)v + 1 =: o$$

ergibt. Daraus folgen für die Ordnungen $iv - k = \operatorname{ord}(m_\ell^i j^k)$ der Summanden auf der rechten Seite in (6.14) die Schranken

$$iv - k \geqslant 1 - v \quad \text{sowie} \quad -iv - \ell k \geqslant o \quad \Rightarrow \quad iv - k \leqslant iv + \ell k \leqslant -o,$$

als deren Differenz man schließlich die behauptete Präzision $\operatorname{prec}(\ell, n) = (\ell^2 + \ell + 1)v - 1$ erhält. □

Bemerkung 6.2.6. Abschätzung (6.13) lässt sich für kleine Werte von i offenbar deutlich verbessern, so ergibt sich beispielsweise für $i = 0$ die Schranke $\operatorname{ord}(a^*_0) \geqslant v + 1 - (v+1)\ell$, womit die Präzision $\operatorname{prec}(\ell, n) = (2\ell+1)v - 1$ ausreicht, um die Darstellung für a_0 zu bestimmen.

Mithilfe des in Lemma 6.2.5 skizzierten Vorgehens erhalten wir somit als Spezialisierung von (6.9) die Gleichung

$$\sigma_{\ell,n,\chi}(\tau) = R(j(\tau), m_\ell(\tau), m_\ell(S_0\tau)). \tag{6.15}$$

Das folgende Lemma liefert äquivalente Formulierungen von (6.15).

Lemma 6.2.7. *Seien für $0 \leqslant k < \ell$ die bereits in Gleichung* (6.3) *eingeführten Matrizen*

$T_k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(\ell)$ gegeben und seien $S_k = \left(\begin{smallmatrix} 0 & -1 \\ 1 & k \end{smallmatrix}\right)$ wie in Gleichung (2.9). Schreiben wir außerdem $P = (x(\zeta_\ell, q), y(\zeta_\ell, q))$ und $Q_k = (x(\zeta_\ell^k q^{\frac{1}{\ell}}, q), y(\zeta_\ell^k q^{\frac{1}{\ell}}, q)), 0 \leqslant k < \ell$, für diese verschiedenen ℓ-Torsionspunkte auf der Tate-Kurve, so transformiert sich durch die Wirkung von T_k Gleichung (6.15) zu

$$\frac{G_{\ell,n,\chi}(q)\left(\sum_{\lambda\in\mathbb{F}_\ell^*}\chi(\lambda)(\lambda Q_k)_V\right)p_1(q)^r G_{\chi^{-1}}(P,Q_k)}{\Delta(q)} = R(j(\tau), m_\ell(\tau), m_\ell(S_k\tau)), \tag{6.16}$$

wobei $V = x$ für n ungerade und $V = y$ für n gerade gilt.

Beweis. Wir betrachten zunächst die rechte Seite der Gleichung. Wegen T_k in $\Gamma_0(\ell)$ sind $m_\ell(\tau)$ sowie $j(\tau)$ unter der Wirkung von T_k invariant. Weiterhin gilt

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$$

und damit $m_\ell(S_0\tau)|_{T_k} = m_\ell(S_0T_k\tau) = m_\ell(S_k\tau)$.
Auf der linken Seite untersuchen wir die verschiedenen Komponenten von $\sigma_{\ell,n,\chi}(\tau)$ gemäß Korollar 6.1.3. Zunächst gilt $\Delta(q)|_{T_k} = \Delta(q)$ sowie laut Korollar 2.2.9 $p_1(q)|_{T_k} = p_1(q)$ und $G_{\ell,n,\chi}(q)|_{T_k} = \chi^{-1}(1)G_{\ell,n,\chi}(q) = G_{\ell,n,\chi}(q)$. Weiterhin folgt mit $c = \frac{1}{(2\pi i)^2}$ aus Lemma 6.1.1

$$x\left(q^{\frac{\lambda}{\ell}}, q\right)\Big|_{T_k} = c\wp\left(\frac{\lambda\tau}{\ell}, \tau\right)\Big|_{T_k} = c\wp\left(\frac{\lambda(\tau+k)}{\ell}, \tau\right) = x\left(\zeta_\ell^{k\lambda}q^{\frac{\lambda}{\ell}}, q\right)$$

und eine analoge Aussage für $y(q^{\frac{\lambda}{\ell}}, q)$. Dies impliziert

$$H_{\ell,n,\chi}(q)|_{T_k} = \sum_{\lambda\in\mathbb{F}_\ell^*}\chi(\lambda)V\left(\zeta_\ell^{k\lambda}q^{\frac{\lambda}{\ell}}, q\right) = \sum_{\lambda\in\mathbb{F}_\ell^*}\chi(\lambda)(\lambda Q_k)_V,$$

wobei wie stets $V = x$ für ungerades und $V = y$ für gerades n gilt. Des Weiteren schließen wir $G_{\chi^{-1}}(e_\ell(P,Q_0))\big|_{T_k} = G_{\chi^{-1}}(e_\ell(P,Q_k))$. □

6.3 Anwendung

Sei ℓ eine Atkin-Primzahl für eine elliptische Kurve E über $\mathbb{F}_p$. Aus den bereits in Abschnitt 1.2.2 erwähnten wichtigen Sätzen aus [Sch95, S. 236–239] zum Zerfällungstyp des Modularpolynoms Φ_ℓ und den Konstruktionen in [Mül95] folgt, dass für ein $r \mid \ell+1$, $r > 1$, eine ℓ-Isogenie $\psi : E \to E'$ existiert, die über $\mathbb{F}_{p^r}$ definiert ist und der eine Nullstelle $m_\ell(E) \in \mathbb{F}_{p^r}\backslash\mathbb{F}_{p^{r-1}}$ von $M_\ell(X, j(E))$ entspricht. Wir nehmen im Folgenden an, dass $r > 2$ gilt. Für $n \mid \ell - 1$, einen Charakter χ von Ordnung n und einen ℓ-Torsionspunkt Q auf E schreiben wir allgemein

$$G_{\ell,n,\chi}(E,Q) := \sum_{a=1}^{\ell-1}\chi(a)(aQ)_V$$

mit $V = x$ für ungerades und $V = y$ für gerades n.

Mit den gleichen Überlegungen wie in Abschnitt 4.1 können wir nun die Formeln (6.15) sowie (6.16) auf die elliptische Kurve $E/\mathbb{F}_p$ spezialisieren. Für den der Kurve E bzw. ihrem Deuring-

Lift E_0 (vgl. Abschnitt 4.1) zugehörigen Wert von τ entspricht $m_\ell(E)$ dann dem Wert $m_\ell(\tau)$ in (6.16). Ebenso entsprechen die Werte $\varphi_p(m_\ell(E))$ und $\varphi_p^2(m_\ell(E))$ als weitere Nullstellen von $M_\ell(X, j(E))$ jeweils einer Konjugierten $m_\ell(S_k\tau)$ für ein passendes k mit $0 \leqslant k < \ell$. Wir benutzen hier, dass wir $r > 2$ angenommen haben und somit $\varphi_p^2(m_\ell(E)) \neq m_\ell(E)$ gilt.
Wie durch Anwendung von φ_p auf die Formeln (4.4), (4.5) und Bemerkung 4.2.1 folgt, entsprechen weiterhin den Werten $\varphi_p(m_\ell(E))$, $\varphi_p^2(m_\ell(E))$ die Isogenien $\phi_p(\psi) : E \to \phi_p(E')$ sowie $\phi_p^2(\psi) : E \to \phi_p^2(E')$. Schreiben wir $P \neq \mathcal{O}$ für einen Punkt in $\ker(\psi)$, dann folgt $\phi_p(P) \in \ker(\phi_p(\psi))$ und $\phi_p^2(P) \in \ker(\phi_p^2(\psi))$. Durch Spezialisierung von Formel (6.16) auf die betrachtete Kurve E ergeben sich also die Gleichungen

$$R(j(E), m_\ell(E), \varphi_p(m_\ell(E))) = \frac{G_{\ell,n,\chi}(E,P)G_{\ell,n,\chi}(E,\phi_p(P))p_1(E)^r G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))}{\Delta(E)},$$
$$R(j(E), m_\ell(E), \varphi_p^2(m_\ell(E))) = \frac{G_{\ell,n,\chi}(E,P)G_{\ell,n,\chi}(E,\phi_p^2(P))p_1(E)^r G_{\chi^{-1}}(e_\ell(P,\phi_p^2(P)))}{\Delta(E)}.$$

Daraus erhalten wir sofort

$$\frac{R(j(E), m_\ell(E), \varphi_p(m_\ell(E)))}{R(j(E), m_\ell(E), \varphi_p^2(m_\ell(E)))} = \frac{G_{\ell,n,\chi}(E,\phi_p(P))G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))}{G_{\ell,n,\chi}(E,\phi_p^2(P))G_{\chi^{-1}}(e_\ell(P,\phi_p^2(P)))}. \tag{6.17}$$

Für $p \equiv 1 \mod n$ rechnen wir weiterhin

$$G_{\ell,n,\chi}(E,\phi_p(P)) = \sum_{a=1}^{\ell-1} \chi(a)(a\phi_p(P))_V = \sum_{a=1}^{\ell-1} \chi^p(a)(aP)_V)^p = G_{\ell,n,\chi}(E,P)^p, \tag{6.18}$$

was direkt $G_{\ell,n,\chi}(E,\phi_p^2(P)) = G_{\ell,n,\chi}(E,P)^{p^2}$ impliziert. Damit ergibt sich

$$\frac{G_{\ell,n,\chi}(E,\phi_p(P))}{G_{\ell,n,\chi}(E,\phi_p^2(P))} = G_{\ell,n,\chi}(E,P)^{p-p^2} = (G_{\ell,n,\chi}(E,P)^n)^{\frac{p(1-p)}{n}}, \tag{6.19}$$

da $n \mid 1-p$ gilt. Mit Gleichung (6.17) folgt

$$\frac{R(j(E), m_\ell(E), \varphi_p(m_\ell(E)))}{R(j(E), m_\ell(E), \varphi_p^2(m_\ell(E)))}(G_{\ell,n,\chi}(E,P)^n)^{\frac{p(p-1)}{n}} = \frac{G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))}{G_{\chi^{-1}}(e_\ell(P,\phi_p^2(P)))}. \tag{6.20}$$

Wie in Abschnitt 4 ausführlich beschrieben, kann der Wert von $G_{\ell,n,\chi}(E,P)^n$ mittels der vorberechneten universellen elliptischen Gauß-Summen für den Elkies-Fall aus den Werten von $j(E)$ und $m_\ell(E)$ bestimmt werden. Damit kann die linke Seite von Gleichung (6.20) mithilfe der vorberechneten rationalen Ausdrücke berechnet werden.

Nach Satz 1.1.10 gilt

$$\phi_p^2(P) = t\phi_p(P) - pP,$$

was mit den Eigenschaften der Weil-Paarung e_ℓ laut Proposition 1.1.4

$$e_\ell(P,\phi_p^2(P)) = e_\ell(P, t\phi_p(P) - pP) = e_\ell(P,\phi_p(P))^t$$

impliziert. Aus den bekannten Eigenschaften der zyklotomischen Gauß-Summen (vgl. den

Beweis von Lemma 3.2.4) folgt damit für die rechte Seite von Gleichung (6.20)

$$\frac{G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))}{G_{\chi^{-1}}(e_\ell(P,\phi_p^2(P)))} = \frac{G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))}{\chi(t)G_{\chi^{-1}}(e_\ell(P,\phi_p(P)))} = \chi^{-1}(t).$$

Somit erlaubt es Gleichung (6.20), den Index von $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$ modulo n zu bestimmen. Wird die Rechnung für die verschiedenen koprimen Teiler n von $\ell - 1$ ausgeführt, erhält man den im Algorithmus von Schoof gesuchten Wert von t modulo ℓ.

Abschließend gehen wir auf die bei der Herleitung der Formeln getroffenen Annahmen ein. Zunächst haben wir $r > 2$ angenommen. Falls $r = 2$ gilt, so sind jedoch keine weiteren Rechnungen nötig, um t modulo ℓ zu bestimmen: Nach [Sch95, S. 236] folgt nämlich für $P \in E[\ell]$ zunächst $\phi_p^2(P) = aP$ für ein $a \in \mathbb{F}_\ell^*$. Setzt man dies in Gleichung (1.6) ein, so ergibt sich

$$(a + p)P = t\phi_p(P).$$

Da ℓ eine Atkin-Primzahl ist, muss die linke Seite verschwinden. Damit erhält man die Kongruenzen $a \equiv -p \mod \ell$ und $t \equiv 0 \mod \ell$.

Weiterhin haben wir in den Gleichungen (6.18) und (6.19) angenommen, dass $p \equiv 1 \mod n$ gilt. Allgemein sei für eine Primzahl p das Inverse modulo n mit p' bezeichnet und es gelte $p = nq_1 + m_1, p^2 = nq_2 + m_2$ mit $0 \leqslant m_1, m_2 < n$. Statt Gleichung (6.18) erhält man dann

$$G_{\ell,n,\chi}(E,\phi_p(P)) = \sum_{a=1}^{\ell-1} \chi(a)(a\phi_p(P))_V = \sum_{a=1}^{\ell-1} \chi^{p'p}(a)(aP)_V)^p = G_{\ell,n,\chi^{p'}}(E,P)^p$$

und daraus $G_{\ell,n,\chi}(E,\phi_p^2(P)) = G_{\ell,n,\chi^{p'2}}(E,P)^{p^2}$. Anstelle von Gleichung (6.19) ergibt sich nun

$$\frac{G_{\ell,n,\chi}(E,\phi_p(P))}{G_{\ell,n,\chi}(E,\phi_p^2(P))} = \frac{(G_{\ell,n,\chi^{p'}}(E,P)^n)^{q_1} G_{\ell,n,\chi^{p'}}(E,P)^{m_1} G_{\ell,n,\chi^{-1}}(E,P)}{(G_{\ell,n,\chi^{p'2}}(E,P)^n)^{q_2} G_{\ell,n,\chi^{p'2}}(E,P)^{m_2} G_{\ell,n,\chi^{-1}}(E,P)}.$$

Der Wert $G_{\ell,n,\chi^{p'}}(E,P)^n$ kann nun wieder mittels der universellen elliptischen Gauß-Summen für den Elkies-Fall bestimmt werden. Wegen $p'm_1 \equiv p'p \equiv 1 \mod n$ lässt sich weiterhin die Größe $G_{\ell,n,\chi^{p'}}(E,P)^{m_1} G_{\ell,n,\chi^{-1}}(E,P)$ direkt mit der universellen elliptischen Jacobi-Summe $J_{\ell,n,\chi^{p'},m_1}$ aus Lemma 4.4.1 berechnen. Analoges gilt für die Ausdrücke im Nenner. Somit kann Gleichung (6.17) auch für allgemeines p in eine Gleichung analog zu (6.20) umgeformt werden, deren linke Seite mittels vorberechneter rationaler Ausdrücke bestimmt werden kann.

6.4 Laufzeit

Wir beschränken uns auf die Betrachtung der Laufzeit für das Auswerten des Ausdrucks $R(j(E), m_\ell(E), \varphi_p(m_\ell(E)))$. Aus der Kombination von Lemma 6.2.2 sowie Proposition 2.1.21 ergibt sich

$$\sigma_{\ell,n}(E) = \frac{\sum_{i_1=0}^{\ell-1} \varphi_p(m_\ell(E))^{i_1} \sum_{i_2=n_0}^{n_1} m_\ell(E)^{i_2} \sum_{i_3=0}^{v-1} a_{i_1,i_2,i_3} j(E)^{i_3}}{\frac{\partial M_{\ell,2}}{\partial X}(\varphi_p(m_\ell(E))) \frac{\partial M_\ell}{\partial Y}(m_\ell(E), j(E))}. \tag{6.21}$$

Aus Lemma 6.2.5 und Gleichung (6.14) folgt, dass im Mittel für festes i_1 die Berechnung des von m_ℓ sowie j abhängenden Terms $O(\ell^2 v)$ Multiplikationen in $\mathbb{F}_{p^r}[\zeta_n]$ erfordert. Wird anschließend über i_1 summiert, so ergibt sich ein Aufwand von $O(\ell^3 v)$ Multiplikationen in $\mathbb{F}_{p^r}[\zeta_n]$. Es ist klar, dass allein die Laufzeit für diesen Schritt für Werte von $\ell \in O(\log p)$ bereits für *ein* festes n deutlich die im ursprünglichen Algorithmus von Schoof für festes ℓ erforderliche Laufzeit $\tilde{O}(\ell^2 \log p)$ Multiplikationen in $\mathbb{F}_p$ übersteigt, ganz zu schweigen von der Laufzeit $\tilde{O}(\ell \log p)$ im Elkies-Fall oder den weiteren in Abschnitt 1.2.3 dargestellten Verbesserungen. Beachten wir überdies, dass asymptotisch laut (3.18) $\ell \in O(v)$ gilt, so sehen wir, dass die vorgestellte Alternative für den Atkin-Fall eine Laufzeit aufweist, die eine tatsächliche Verwendung zum Punktezählen nicht praktikabel macht.
Dies müsste offenbar auch gelten, wenn wir, statt wie in Abschnitt 6.2 eine Darstellung auf Basis von m_ℓ zu bestimmen, ähnliche Überlegungen ausgehend von anderen Modulfunktionen wie a_ℓ durchgeführt hätten. In diesem Fall wäre zwar der Wert von v geringer, aufgrund des Faktors ℓ^3 läge die Laufzeit jedoch weiterhin deutlich über derjenigen bestehender Ansätze.

7 Polynomiell zyklische Algebren

7.1 Definitionen

In diesem vom Rest der Arbeit unabhängigen Abschnitt stellen wir einen weiteren Ansatz vor, mit dem mithilfe der in [MV10] definierten polynomiell zyklischen Algebren die Spur des Frobenius-Homomorphismus modulo Atkin-Primzahlen ℓ berechnet werden kann. Wir nehmen in starkem Maße Bezug auf die Masterarbeit [Ber13], der die meisten hier dargestellten Ergebnisse entstammen. Neue Resultate werden in den Abschnitten 7.2.1 sowie 7.3 präsentiert.

Definition 7.1.1. [MV10, S. 6] Sei $\mathbb{K}$ ein endlicher Körper und $f(X) \in \mathbb{K}[X]$ ein Polynom mit $\deg(f) = n$. Dann nennen wir die $\mathbb{K}$-Algebra $\mathbf{A} = \mathbb{K}[X]/(f(X))$ eine *polynomiell zyklische Algebra* mit *Zyklizitätspolynom* $C(X) \in \mathbb{K}[X]$ und bezeichnen $f(X)$ als *zyklisches Polynom*, wenn die folgenden Bedingungen erfüllt sind:

1. $f(C(X)) \equiv 0 \bmod f(X)$.
2. $C^{(n)}(X) - X \equiv 0 \bmod f(X)$ und $\mathrm{ggT}(C^{(m)}(X) - X, f(X)) = 1$ für $m < n$.

Dabei ist $C^{(m)}(X) = \underbrace{C \circ C \cdots \circ C}_{m\text{-mal}}(X)$.

Bemerkung 7.1.2.
1. Jedes irreduzible Polynom $f \in \mathbb{K}[X]$ ist auch zyklisch mit Zyklizitätspolynom $C(X) = X^q$, wenn $\mathbb{K} = \mathbb{F}_q$ gilt.
2. Wenn ein Polynom $f(X) \in \mathbb{K}[X]$ zyklisch mit Zyklizitätspolynom $C(X)$ ist, gilt dasselbe in allen Erweiterungen $\mathbb{L}$ von $\mathbb{K}$.

Der folgende Satz liefert mehrere Charakterisierungen zyklischer Polynome.

Satz 7.1.3. *[MV10, S. 6] Die folgenden Bedingungen sind äquivalent:*

1. *f ist zyklisch.*
2. *Es gibt ein Polynom $C(X) \in \mathbb{K}[X]$, das die Nullstellen von f zyklisch permutiert, d. h., für jede Nullstelle $\alpha \in \overline{\mathbb{K}}$ von f gilt die Gleichheit $f(C(\alpha)) = 0$ und die Elemente $C^{(i)}(\alpha)$, $i = 1, \ldots, n$, sind paarweise verschieden.*
3. *In der Faktorisierung $f = \prod_{k=1}^{d} h_k$ über $\mathbb{K}[X]$ haben alle Faktoren h_k denselben Grad und sind paarweise verschieden.*

Als nächstes beschreiben wir einige Eigenschaften polynomiell zyklischer Algebren.

Satz 7.1.4. *[MV10, S. 9] Sei $\mathbf{A} = \mathbb{K}[X]/(f(X))$, $\deg(f) = n$, eine polynomiell zyklische Algebra mit Zyklizitätspolynom $C(X)$ und sei $\alpha := X \bmod f(X)$. Dann gelten die folgenden Aussagen:*

1. *Das Zyklizitätspolynom $C(X)$ induziert einen Automorphismus ν von $\mathbb{K}$-Algebren von Ordnung n vermöge*

$$\nu : \mathbf{A} \to \mathbf{A}, \quad \alpha \mapsto C(\alpha).$$

Wir schreiben $\mathrm{Gal}(\mathbf{A}/\mathbb{K}) := \langle \nu \rangle$, $\mathrm{Gal}(\mathbf{A}/\mathbb{K})$ ist also die von ν erzeugte Automorphismengruppe von $\mathbf{A}$, die wir auch als Galoisgruppe von $\mathbf{A}/\mathbb{K}$ bezeichnen.

2. *Es gilt* $\mathbf{A}^{\mathrm{Gal}(\mathbf{A}/\mathbb{K})} = \{x \in \mathbf{A} : \nu(x) = x\} = \mathbb{K}$, *also* $\nu(x) = x \Rightarrow x \in \mathbb{K}$.

Satz 7.1.5. *[MV10, S. 11] Sei* $\mathbf{A} = \mathbb{K}[X]/(f(X))$ *eine polynomiell zyklische Algebra. Dann gelten die folgenden Aussagen:*

1. *Sei* $\tilde{\mathbb{K}}/\mathbb{K}$ *eine Körpererweiterung. Dann ist* $\tilde{\mathbf{A}} := \mathbf{A} \otimes_{\mathbb{K}} \tilde{\mathbb{K}}$ *eine polynomiell zyklische* $\tilde{\mathbb{K}}$*-Algebra und es gibt einen kanonischen Isomorphismus* $\mathrm{Gal}(\tilde{\mathbf{A}}/\tilde{\mathbb{K}}) \cong \mathrm{Gal}(\mathbf{A}/\mathbb{K})$.

2. *Sei* $H \subset \mathrm{Gal}(\mathbf{A}/\mathbb{K})$ *eine Untergruppe. Dann ist die Unteralgebra aller unter* H *invarianten Elemente,*
$$\mathbf{A}^H := \{a \in \mathbf{A} : h(a) = a \ \forall h \in H\},$$
polynomiell zyklisch. Ist umgekehrt $\mathbf{B} \subset \mathbf{A}$ *eine polynomiell zyklische Algebra, dann gibt es eine Untergruppe* $H \subset \mathrm{Gal}(\mathbf{A}/\mathbb{K})$ *mit* $\mathbf{B} = \mathbf{A}^H$.
Die Dimension von $\mathbf{A}^H$ *ist gleich dem Index* $[\mathrm{Gal}(\mathbf{A}/\mathbb{K}) : H]$. *Des Weiteren gibt es einen kanonischen Isomorphismus* $\mathrm{Gal}(\mathbf{A}^H/\mathbb{K}) \cong \mathrm{Gal}(\mathbf{A}/\mathbb{K})/H$.

Wir definieren nun *Lagrange-Resolventen* in polynomiell zyklischen Algebren, wobei wir erneut eng [MV10, S. 12] folgen. Sei $\mathbf{A} = \mathbb{K}[X]/(f(X))$, $\deg(f) = n$, wieder eine polynomiell zyklische Algebra mit $\mathrm{Gal}(\mathbf{A}/\mathbb{K}) = \langle\nu\rangle$. Sei $\zeta_n \in \overline{\mathbb{K}}$ eine primitive n-te Einheitswurzel mit Minimalpolynom $K_n(X) \in \mathbb{K}[X]$. Wir setzen nun $\mathbf{A}_{\zeta_n} := \mathbf{A}[T]/(K_n(T))$. Wegen $\mathbf{A}_{\zeta_n} = \mathbf{A} \otimes_{\mathbb{K}} \mathbb{K}[\zeta_n]$ impliziert Satz 7.1.5, dass $\mathbf{A}_{\zeta_n}$ eine polynomiell zyklische Algebra über $\mathbb{K}[\zeta_n]$ ist und wir mittels des kanonischen Isomorphismus die Gruppen $\mathrm{Gal}(\mathbf{A}_{\zeta_n}/\mathbb{K}[\zeta_n])$ und $\mathrm{Gal}(\mathbf{A}/\mathbb{K})$ identifizieren können. Sei nun $\chi : \mathrm{Gal}(\mathbf{A}/\mathbb{K}) \to \mathbb{K}[\zeta_n]$ ein multiplikativer Charakter. Für $\alpha \in \mathbf{A}$ definieren wir die Lagrange-Resolvente (χ, α) als

$$(\chi, \alpha) = \sum_{\sigma \in \mathrm{Gal}(\mathbf{A}/\mathbb{K})} \chi(\sigma)\sigma(\alpha) = \sum_{i=1}^{n} \chi(\nu^i)\nu^i(\alpha) = \sum_{i=1}^{n} \chi(\nu)^i \nu^i(\alpha) \in \mathbf{A}_{\zeta_n}.$$

Wie aus dem folgenden Satz hervorgeht, können die Lagrange-Resolventen dazu verwendet werden, einen Isomorphismus zwischen zwei polynomiell zyklischen Algebren explizit zu bestimmen, was wir später benutzen werden.

Satz 7.1.6. *[MV10, S. 14] Seien* $\mathbf{A}_i = \mathbb{K}[X]/(f_i(X))$, $\deg(f_i) = n$, $i = 1, 2$, *zwei isomorphe polynomiell zyklische Algebren mit den Zyklizitätspolynomen* $C_1(X), C_2(X)$. *Seien* ν_i *die von* $C_i(X)$ *induzierten Automorphismen und* $G_i := \mathrm{Gal}(\mathbf{A}_i/\mathbb{K}) = \langle\nu_i\rangle$ *und* $\alpha_i := X \mod f_i(X)$, *wobei* α_2 *mit seinen Konjugierten eine normale Basis von* $\mathbf{A}_2$ *bilde. Dann existiert ein Isomorphismus*

$$\varphi : \mathbf{A}_1 \to \mathbf{A}_2, \quad \alpha_1 \mapsto \sum_{i=1}^{n} a_i \nu_2^i(\alpha_2) \quad \textit{mit} \quad a_i \in \mathbb{K} \tag{7.1}$$

mit $\varphi \circ \nu_1 = \nu_2 \circ \varphi$.
Sei weiterhin $\zeta_n \in \overline{\mathbb{K}}$ *eine primitive* n*-te Einheitswurzel und sei* $\mathbf{A}_{i,\zeta_n}$ *wie oben. Seien noch* $\chi_i : G_i \to \mu_n$, $i = 1, 2$, *Charaktere mit* $\chi_1(\nu_1) = \chi_2(\nu_2)$. *Dann gibt es* $\beta(\chi_2) \in \mathbb{K}[\zeta_n]$ *mit*

$$\varphi((\chi_1, \alpha_1)) = (\chi_2, \alpha_2) \cdot \beta(\chi_2).$$

Genauer gilt

$$\beta(\chi_2) = \sum_{i=1}^{n} a_i \chi_2^{-1}(\nu_2^i).$$

Aus dem Satz ergibt sich folgendes Vorgehen zur Bestimmung der Koeffizienten a_i in (7.1) ([MV10, S. 14]): Für $j = 1, \ldots, n$ sei $\chi_{2,j}$ der Charakter mit $\chi_{2,j}(\nu_2) = \zeta_n^j$. Wenn der Wert $\beta(\chi_{2,j})$ bekannt ist, so ergibt sich

$$\beta(\chi_{2,j}) = \sum_{i=1}^{n} a_i \chi_{2,j}^{-1}(\nu_2^i) = \sum_{i=1}^{n} a_i \zeta_n^{-ij},\ j = 1, \ldots, n.$$

Daraus folgt

$$M \cdot \vec{a} = \vec{\beta}$$

mit $M = (\zeta_n^{-ij})_{i,j=1}^n$, $\vec{a} = (a_i)_{i=1}^n$ und $\vec{\beta} = (\beta(\chi_{2,j}))_{j=1}^n$. Somit erhält man ein lineares Gleichungssystem für die Koeffizienten a_i, mit dem sie aufgrund der folgenden Proposition bestimmt werden können.

Proposition 7.1.7. *[Ber13, S. 35] Die Matrix M ist regulär, wenn* $\mathrm{ggT}(n, char(\mathbb{K})) = 1$ *gilt. Genauer ist*

$$(\det(M))^2 = (-1)^{n\cdot(n+1)/2+1} \cdot n^n.$$

7.2 Anwendung

Wir erinnern zunächst an das Strahlenpolynom aus [MV10].

Definition 7.2.1. Sei $E : Y^2 = X^3 + aX + b =: f(X)$ eine elliptische Kurve über $\mathbb{F}_p$, ℓ eine Primzahl und P ein Punkt in $E[\ell], P \neq \mathcal{O}$. Das zu P zugehörige *Strahlenpolynom* ist definiert als

$$E_P(X) = \prod_{a=1}^{(\ell-1)/2} (X - (aP)_x) \in \overline{\mathbb{F}}_p[X].$$

Wir bemerken, dass das Strahlenpolynom nur von dem Teilvektorraum von $E[\ell]$ abhängt, der von P aufgespannt wird. Das Polynom verfügt über die folgenden Eigenschaften:

Lemma 7.2.2. *1. $E_P(X)$ ist ein zyklisches Polynom, dessen Zyklizitätspolynom $G_c(X)$ mithilfe der Divisionspolynome von E leicht berechnet werden kann [MV10, S. 8].*

2. $E_P(X)$ liegt in $\mathbb{F}_{p^r}[X]$, wobei $r \mid \ell + 1$ der Grad eines irreduziblen Faktors in $\mathbb{F}_p[X]$ des ℓ-ten Modularpolynoms $\Phi_\ell(X, j(E))$ ist. Dies folgt aus [Sch95, Satz 6.1, 6.2] und wird in [MV10, S. 3] gezeigt. Im Elkies-Fall stimmt das Strahlenpolynom für passendes P mit dem Elkies-Faktor $F_{\ell,\lambda}$ aus [Sch95, Mor95] überein, es gilt $r = 1$.

Um den Wert von $t \mod \ell$ zu bestimmen, betrachten wir wie üblich die Gleichung $\chi(\phi_p) \mod \ell$ aus Satz 1.1.10. Setzen wir einen ℓ-Torsionspunkt P ein und beschränken uns auf die x-Koordinaten, so erhalten wir

$$(\phi_p^2(P) + pP)_x = G_t(\varphi_p(P_x)), \tag{7.2}$$

wobei $G_t(P_x) = (tP)_x$ gilt und G_t mithilfe der Divisionspolynome definiert ist [Was08, S. 79]. Setzen wir $\mathbf{A} = \mathbb{F}_{p^r}$ wie in Lemma 7.2.2 und $\mathbf{B} = \mathbf{A}[T]/(E_P(T))$, so können alle Rechnungen in $\mathbf{B}$ durchgeführt werden. Lemma 7.2.2 impliziert wiederum, dass $\mathbf{B}$ eine polynomiell zyklische Algebra ist. Wir bezeichnen den vom Zyklizitätspolynom G_c induzierten Erzeuger der Galoisgruppe $\mathrm{Gal}(\mathbf{B}/\mathbf{A})$ mit ν und schreiben $\theta := T + (E_P(T))$. Wie im Algorithmus von

Schoof dominiert die Berechnung der Wirkung von ϕ_p die Laufzeit. Da $\deg(E_P) = \frac{\ell-1}{2}$ gilt, liegt die Gesamtlaufzeit bei $O(r\ell \log p)$ Operationen in $\mathbb{F}_p$ gegenüber $O(\ell^2 \log p)$ Operationen im ursprünglichen Algorithmus von Schoof.

Mithilfe der in Abschnitt 7.1 präsentierten Resultate möchten wir einen Ansatz beschreiben, mit dem die Laufzeit verringert werden kann. Unsere wesentliche Idee besteht, aufbauend auf Ansätzen in [MV10] und detaillierten Überlegungen in [Ber13], darin, eine polynomiell zyklische Algebra $\mathbf{C}$ zu konstruieren, die zu $\mathbf{B}$ isomorph ist und eine effiziente Auswertung des Frobenius-Homomorphismus erlaubt. Danach lösen wir das sich ergebende Diskreter-Logarithmus-Problem in dieser Algebra. Unser Ansatz betrifft Atkin-Primzahlen und unterscheidet sich von den verschiedenen Verbesserungen im Elkies-Fall, die im Wesentlichen darauf basieren, auszuführende Rechnungen in kleinere Erweiterungen von $\mathbb{F}_p$ zu verlagern, was für Atkin-Primzahlen nicht möglich ist. Offensichtlich erfordert unser Ansatz die explizite Berechnung des Isomorphismus zwischen den beiden Algebren.

Wir definieren zunächst die Algebra $\mathbf{C}$.

Proposition 7.2.3. *[Ber13, S. 36] Sei* $G = \left\{b \in \mathbb{F}_\ell^* : \left(\frac{b}{\ell}\right) = 1\right\}$, $\zeta_\ell \in \overline{\mathbb{F}}_p$ *eine primitive* ℓ*-te Einheitswurzel und* $K(U) = \prod_{b \in G}(U - \zeta_\ell^b)$. *Dann ist* $\mathbf{C} = \mathbf{A}[U]/(K(U))$ *eine polynomiell zyklische Algebra mit* $\mathrm{Gal}(\mathbf{C}/\mathbf{A}) = \langle \sigma : \zeta_\ell \mapsto \zeta_\ell^{c^2} \rangle$, *wobei* $\langle c \rangle = \mathbb{F}_\ell^*$ *gilt.*

Lemma 7.2.4. *[Ber13, S. 37] Als Algebren über* $\mathbf{A}$ *sind* $\mathbf{B}$ *und* $\mathbf{C}$ *isomorph.*

Somit existiert ein Isomorphismus

$$\alpha : \mathbf{B} \to \mathbf{C}, \quad \theta \mapsto \sum_{i=1}^{(\ell-1)/2} b_i \zeta_\ell^{c^{2i}} \quad \text{mit} \quad b_i \in \mathbf{A} \tag{7.3}$$

mit $\alpha \circ \nu = \sigma \circ \alpha$.

Bemerkung 7.2.5. Damit die Voraussetzungen von Satz 7.1.6 erfüllt sind, müssen die Elemente $\zeta_\ell^{c^{2i}}, i = 1, \ldots, \frac{\ell-1}{2}$, eine Basis der Algebra $\mathbf{C}$ bilden. Dies kann bei tatsächlichen Rechnungen zur Laufzeit geprüft werden und war in der Praxis stets der Fall.

Zur Bestimmung der Koeffizienten von (7.3) folgen wir den Erläuterungen nach Satz 7.1.6. Sei ρ eine $\frac{\ell-1}{2}$-te Einheitswurzel, $q \mid \frac{\ell-1}{2}$, $\zeta_q = \rho^{(\ell-1)/(2q)}$ und

$$\chi_q : \mathrm{Gal}(\mathbf{B}/\mathbf{A}) \to \mathbf{A}[\zeta_q], \ \nu \mapsto \zeta_q \tag{7.4}$$

ein Charakter von Ordnung q. Wir identifizieren χ_q mit dem Charakter

$$\chi_{q,2} : \mathrm{Gal}(\mathbf{C}/\mathbf{A}) \to \mathbf{A}[\zeta_q], \ \sigma \mapsto \zeta_q.$$

Es gilt folgendes

Lemma 7.2.6. *[Ber13, S. 38–39] Seien*

$$b_i^{(q)} = \sum_{k=1}^{(\ell-1)/(2q)} b_{kq+i}, 1 \leqslant i \leqslant q, \ \textit{und} \ \theta^{(q)} = \sum_{j=1}^{(\ell-1)/(2q)} \nu^{jq}(\theta) \ \textit{und} \ \zeta_\ell^{(q)} = \sum_{j=1}^{(\ell-1)/(2q)} \sigma^{jq}(\zeta_\ell).$$

Seien weiterhin

$$\tau_e(\chi_q) = \sum_{a=1}^{q} \zeta_q^a \nu^a(\theta^{(q)}) \text{ und } \tau(\chi_q) = \sum_{j=1}^{q} \zeta_q^j \sigma^j(\zeta_\ell^{(q)}) \text{ sowie } \beta(\chi_q) = \sum_{i=1}^{q} \zeta_q^{-i} b_i^{(q)}.$$

Dann erhält man

$$\alpha(\tau_e(\chi_q)) = \beta(\chi_q) \cdot \tau(\chi_q).$$

Bemerkung 7.2.7. Die Größen $\tau(\chi_q)$ sind im Wesentlichen klassische zyklotomische Gauß-Summen, während die Werte $\tau_e(\chi_q)$ die in [MV10] eingeführten elliptischen Gauß-Summen sind, die in dieser Arbeit, beginnend mit Gleichung (1.9), bereits vielfach betrachtet wurden.

Die effiziente Berechnung von $\beta(\chi_q)$ geschieht gemäß

Lemma 7.2.8. *[Ber13, S. 39–40] Mit den obigen Bezeichnungen gelten folgende Aussagen:*

1. $\beta(\chi_q)^q = \frac{\tau_e(\chi_q)^q}{\tau(\chi_q)^q}$.
2. *Für $i > 1$ gilt* $\beta(\chi_q^{i+1}) = \beta(\chi_q^i)\beta(\chi_q) \cdot \frac{z_i}{z_{e,i}}$ *mit*

$$z_{e,i} := \frac{\tau_e(\chi_q^i) \cdot \tau_e(\chi_q)}{\tau_e(\chi_q^{i+1})} \in \mathbf{A}[\zeta_q] \quad \text{und} \quad z_i := \frac{\tau(\chi_q^i) \cdot \tau(\chi_q)}{\tau(\chi_q^{i+1})} \in \mathbf{A}[\zeta_q].$$

3. *Sei χ ein Charakter von Ordnung $\frac{\ell-1}{2}$ mit $\chi = \prod_{q||(\ell-1)/2} \chi_q^{e_q}$. Dann gilt*

$$\beta(\chi) = \frac{z_{e,n}}{z_n} \cdot \prod_{q||n} \beta(\chi_q^{e_q})$$

mit $z_{e,n}, z_n \in \mathbf{A}[\rho]$.

Zur Berechnung von $\beta(\chi)$ für alle Charaktere $\chi : \mathrm{Gal}(\mathbf{B}/\mathbf{A}) \to \mathbf{A}[\rho]$ berechnet man also zunächst für maximale Primzahlpotenzen $q \,||\, \frac{\ell-1}{2}$ für den Charakter χ_q den Wert $\beta(\chi_q)$ durch Ziehen einer q-ten Wurzel in $\mathbf{A}[\zeta_q]$, anschließend die Werte von $\beta(\chi_q)$ für Potenzen χ_q^i, woraus man die Werte für allgemeine Charaktere χ erhält. Insbesondere müssen nach Bestimmung der $\beta(\chi_q)$ keine weiteren Wurzeln mehr gezogen werden, was die Laufzeit gegenüber dem naiven Vorgehen wesentlich reduziert. Danach verfügen wir gemäß Satz 7.1.6 über ein lineares Gleichungssystem der Form

$$M \cdot \vec{b} = \vec{\beta} \tag{7.5}$$

mit $M = (\rho^{-ij})_{i,j=1}^{(\ell-1)/2}$, $\vec{b} = (b_i)_{i=1}^{(\ell-1)/2}$ und $\vec{\beta} = (\beta(\chi))$. Wegen $\mathrm{ggT}\left(\frac{\ell-1}{2}, p\right) = 1$ ist die Matrix M laut Proposition 7.1.7 regulär und die Koeffizienten b_i des Isomorphismus α können bestimmt werden.

Zur Berechnung der Spur t modulo ℓ gehen wir wie folgt vor. Zunächst definieren wir mithilfe der Gleichung der betrachteten Kurve E und der x-Koordinate θ den Punkt $P := (\theta, \gamma)$, der auf E liegt. Anstatt $\varphi_p(\theta)$ zu bestimmen, rechnen wir nun wie in [Ber13]

$$\alpha(\varphi_p(\theta)) = \varphi_p(\alpha(\theta)) = \varphi_p\left(\sum_{i=1}^{(\ell-1)/2} b_i \zeta_\ell^{c^{2i}}\right) = \sum_{i=1}^{(\ell-1)/2} b_i^p \zeta_\ell^{pc^{2i}}. \tag{7.6}$$

Offensichtlich gilt $\zeta_\ell^{pc^{2i}} = \zeta_\ell^k$ mit $k \equiv pc^{2i} \mod \ell$. Gegebenenfalls muss die Potenz ζ_ℓ^k mit $k < \ell$ noch modulo $K(U)$ reduziert werden. Es ergibt sich, dass diese Werte mit vernachlässigbaren Kosten berechnet werden können und die Laufzeit dieses Schritts von der Berechnung der p-ten Potenzen der b_i dominiert wird, die jedoch in $\mathbf{A}$ liegen. Gleiches gilt für die Berechnung von $\alpha(\varphi_p^2(\theta))$. Mithilfe des Polynoms G_t können wir die rechte Seite von Gleichung (7.2) bestimmen.
Um die linke Seite zu bestimmen, benutzen wir das Polynom H_p mit $\gamma \cdot H_p(\theta) = (pP)_y$, das analog zu G_t mithilfe der Divisionspolynome definiert ist [Was08, S. 79]. Unter Verwendung der Formeln zur Addition von Punkten auf elliptischen Kurven erhalten wir

$$(\phi_p^2(P) + pP)_x = \left(\frac{\varphi_p^2(\gamma) - (pP)_y}{\varphi_p^2(\theta) - (pP)_x}\right)^2 - \varphi_p^2(\theta) - (pP)_x. \tag{7.7}$$

Dabei nehmen wir an, dass $\phi_p^2(P) \neq \pm pP$ gilt (anderenfalls kann t einfach bestimmt werden). Wegen

$$\begin{aligned}(\varphi_p^2(\gamma) - (pP)_y)^2 &= (\gamma^{p^2} - \gamma \cdot H_p(\theta))^2 = \gamma^2(\gamma^{p^2-1} - H_p(\theta))^2 \\ &= f(\theta)\left(f(\theta)^{(p^2-1)/2} - H_p(\theta)\right)^2\end{aligned} \tag{7.8}$$

mit f wie in Definition 7.2.1 hängen der Zähler des Bruchs und somit der Wert $(\phi_p^2(P)+pP)_x$ nur von θ ab. Nach Bestimmung der Werte $\varphi_p^2(\theta), \varphi_p^2(f(\theta))$ mithilfe der speziellen Struktur von $\mathbf{C}$ sowie $G_p(\theta), H_p(\theta)$ kann die linke Seite von Gleichung (7.2) durch einmaliges Wurzelziehen gewonnen werden.

7.2.1 Verbesserungen

Das in [Ber13] vorgestellte Vorgehen erfordert, wie dargestellt, die Berechnung von $\beta(\chi)$ für alle Charaktere χ von Ordnung $\frac{\ell-1}{2}$. Zur Reduzierung der Laufzeit stellen wir einen alternativen Ansatz zur Bestimmung von α vor.

Unter Benutzung der Definition von α erhalten wir zunächst

$$\alpha(\theta) = \sum_{i=1}^{(\ell-1)/2} b_i\sigma^i(\zeta_\ell) \quad \text{und} \quad \alpha(\nu^k(\theta)) = \sum_{i=1}^{(\ell-1)/2} b_i\sigma^{i+k}(\zeta_\ell).$$

Mithilfe dieser Identitäten rechnen wir

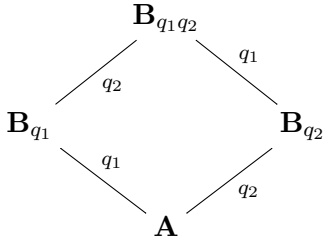
$$\begin{aligned}\alpha(\theta^{(q)}) =& \alpha\left(\sum_{j=1}^{(\ell-1)/(2q)} \nu^{jq}(\theta)\right) = \sum_{j=1}^{(\ell-1)/(2q)} \sum_{i=1}^{(\ell-1)/2} b_i\sigma^{i+jq}(\zeta_\ell) \\ =& \sum_{i=1}^{(\ell-1)/2} b_i\sigma^i \underbrace{\left(\sum_{j=1}^{(\ell-1)/(2q)} \sigma^{jq}(\zeta_\ell)\right)}_{\zeta_\ell^{(q)}} = \sum_{i=1}^{q} \underbrace{\sum_{k=1}^{(\ell-1)/(2q)} b_{kq+i}}_{b_i^{(q)}} \underbrace{\sigma^{kq+i}(\zeta_\ell^{(q)})}_{=\sigma^i(\zeta_\ell^{(q)})} = \sum_{i=1}^{q} b_i^{(q)}\sigma^i(\zeta_\ell^{(q)}).\end{aligned}$$

Wir benötigen also genau die Werte $b_i^{(q)}$, um den Isomorphismus

$$\alpha_q : \mathbf{A}[\theta^{(q)}] \to \mathbf{A}[\zeta_\ell^{(q)}]$$

anzugeben, der die Einschränkung von α auf diese Teilalgebren ist. Zur Bestimmung der $b_i^{(q)}$ müssen die Werte $\beta(\chi_q^i), i = 1, \ldots, q$, gemäß Lemma 7.2.8 berechnet werden, wozu eine q-te Wurzel gezogen werden muss. Anschließend löst man direkt ein lineares Gleichungssystem, anstatt $\beta(\chi)$ für Charaktere von größerer Ordnung zu bestimmen. Unser neuer Ansatz besteht darin, den Isomorphismus α_q für $q \mid\mid \frac{\ell-1}{2}$ zu bestimmen und aus den Zwischenergebnissen induktiv den Isomorphismus α zu konstruieren.

Seien $q_1, q_2 \mid \frac{\ell-1}{2}$ mit $(q_1, q_2) = 1$. Wir nehmen an, dass die Isomorphismen $\alpha_{q_1}, \alpha_{q_2}$ bekannt sind, und geben eine Methode zur Berechnung von $\alpha_{q_1 q_2}$ an. Zu diesem Zweck setzen wir $\mathbf{B}_q := \mathbf{A}[\theta^{(q)}], \mathbf{C}_q := \mathbf{A}[\zeta_\ell^{(q)}]$ und betrachten das folgende Diagramm:



Mittels der allgemeinen Theorie aus [MV10] erhalten wir $\mathrm{Gal}(\mathbf{B}/\mathbf{B}_q) = \langle \nu^q \rangle$, wobei ν wie bisher ein Erzeuger von $\mathrm{Gal}(\mathbf{B}/\mathbf{A})$ ist. Das Polynom

$$M_1(X) = \prod_{i=1}^{q_2} X - \nu^{q_1 i}(\theta^{(q_1 q_2)})$$

verschwindet bei $\theta^{(q_1 q_2)}$, und weil seine Nullstellen von ν^{q_1} permutiert werden, liegt es laut Satz 7.1.5 in $\mathbf{B}_{q_1}[X]$. Weiterhin ist $\theta^{(q_2)}$ eine Nullstelle von

$$M_2(X) = \prod_{i=1}^{q_2} X - \nu^i(\theta^{(q_2)}).$$

Wir betrachten die Wirkung von ν^{q_1} auf die Nullstellen von $M_2(X)$ und erhalten

$$\nu^{jq_1}(\nu^i(\theta^{(q_2)})) = \nu^{jq_1+i}(\theta^{(q_2)}) = \nu^{j(i)}(\theta^{(q_2)})$$

mit $j(i) \equiv jq_1 + i \mod q_2$, da $\nu^{q_2}(\theta^{(q_2)}) = \theta^{(q_2)}$ gilt. Wegen $(q_1, q_2) = 1$ folgert man $jq_1 \not\equiv 0 \mod q_2$ für $j < q_2$. Somit permutiert ν^{q_1} die Nullstellen von $M_2(X)$, das somit ebenfalls in $\mathbf{B}_{q_1}[X]$ liegt.
Da wegen $(q_1, q_2) = 1$ die Elemente $x \in \mathbf{B}_{q_1}[X]/(M_2(X))$ genau unter $\nu^{q_1 q_2}$ invariant sind, schließen wir mit Satz 7.1.5

$$\mathbf{B}_{q_1}[X]/(M_2(X)) \cong \mathbf{B}_{q_1 q_2} \cong \mathbf{B}_{q_1}[X]/(M_1(X)). \tag{7.9}$$

Da $\theta^{(q_1 q_2)} = X \mod \mathbf{B}_{q_1}[X]M_1(X)$ und $\theta^{(q_2)} = X \mod \mathbf{B}_{q_1}[X]M_2(X)$ gilt, existiert auf-

grund von Isomorphismus (7.9) ein Polynom $W(X) \in \mathbf{B}_{q_1}[X]$ mit $\deg(W(X)) < q_2$, sodass $W(\theta^{(q_2)}) = \theta^{(q_1 q_2)}$ gilt. Da der Isomorphismus

$$\alpha_{q_2} : \mathbf{B}_{q_2} \to \mathbf{C}_{q_2}, \quad \theta^{(q_2)} \mapsto \sum_{i=0}^{q_2-1} a_i \sigma^i(\zeta_\ell^{(q_2)})$$

als bekannt angenommen wird, erhalten wir

$$\alpha_{q_1 q_2}(\theta^{(q_1 q_2)}) = \alpha(\theta^{(q_1 q_2)}) = \alpha(W(\theta^{(q_2)})) = \alpha(W) \left(\sum_{i=0}^{q_2-1} a_i \sigma^i(\zeta_\ell^{(q_2)}) \right).$$

Wegen $W(X) \in \mathbf{B}_{q_1}[X]$ hängen die Koeffizienten von W von $\theta^{(q_1)}$ ab. Unter Benutzung des Isomorphismus α_{q_1}, der ebenfalls als bekannt angenommen wird, können wir sie in Abhängigkeit von ζ_ℓ angeben, was schließlich $\alpha_{q_1 q_2}(\theta^{(q_1 q_2)})$ in Abhängigkeit von ζ_ℓ ergibt.

Wir geben noch eine verbesserte Methode zur Bestimmung der Spur t an. Der in [Ber13] vorgestellte Ansatz erfordert das Ziehen einer Wurzel in Gleichung (7.8) in der Algebra $\mathbf{C}$, was hohe Kosten verursacht. Wir zeigen, wie wir dies umgehen können. Schreiben wir

$$A(\theta) = \varphi_p^2(\theta) - G_p(\theta), \; C(\theta) = \varphi_p^2(\theta) + G_p(\theta),$$

so erhalten wir aus (7.7) und (7.8)

$$\begin{aligned} G_t(\varphi_p(\theta)) &= \frac{\varphi_p^2(f(\theta)) - 2f(\theta)^{(p^2+1)/2} H_p(\theta) + f(\theta) H_p^2(\theta)}{A^2(\theta)} - C(\theta) \\ \Rightarrow & \underbrace{(G_t(\varphi_p(\theta)) + C(\theta)) A^2(\theta) - \varphi_p^2(f(\theta)) - f(\theta) H_p^2(\theta)}_{B(t,\theta)} = 2f(\theta)^{(p^2+1)/2} H_p(\theta) \\ \Rightarrow & B(t,\theta)^2 = 4f(\theta)^{p^2+1} H_p^2(\theta) = 4\varphi_p^2(f(\theta)) f(\theta) H_p^2(\theta). \end{aligned} \tag{7.10}$$

Offenbar können beide Seiten dieser Gleichung ohne Wurzelziehen berechnet werden und nach Anwendung von α auf (7.10) muss lediglich der Wert von t, der diese Gleichung erfüllt, bestimmt werden.

Da wir nur die x-Koordinaten betrachten, erhalten wir zwei Lösungen $\pm t$. In manchen Fällen erlaubt es [Dew98, S. 1251], das Vorzeichen von t zu bestimmen.

7.3 Laufzeit

7.3.1 Bestimmung von $\beta(\chi_q)$

Zunächst müssen die elliptischen Gauß-Summen $\tau_e(\chi_q)$ bestimmt werden. Aus dem Absatz vor Gleichung (4.17), in dem ihre direkte Berechnung für Elkies-Primzahlen analysiert wurde, ergibt sich direkt ein Aufwand von $O(q\,\mathsf{C}(\ell))$ Operationen in $\mathbf{A}$ oder

$$O(q\,\mathsf{C}(r\ell)) \tag{7.11}$$

Operationen in $\mathbb{F}_p$. Die zyklotomischen Gauß-Summen $\tau(\chi_q)$ können analog in ähnlicher Laufzeit bestimmt werden. Als nächstes sind die q-ten Potenzen der Größen $\tau_e(\chi_q), \tau(\chi_q)$ zu berechnen, was $\log q$ Multiplikationen in $\mathbf{A}[\zeta_q, \theta^{(q)}]$ und somit

$$O(\mathsf{M}(rq^2) \log q) \tag{7.12}$$

Operationen in $\mathbb{F}_p$ entspricht. Anschließend muss eine q-te Wurzel gezogen werden, was laut [DS14] mit

$$O(\mathsf{M}(q)\,\mathsf{M}(rq) \log p + q\,\mathsf{C}(rq) + \mathsf{C}(q)\,\mathsf{M}(rq) \log rq) \tag{7.13}$$

Operationen zu Buche schlägt. Damit ist der Wert $\beta(\chi_q)$ bestimmt. Wegen $q \in O(p)$ werden die Kosten aus (7.12) von denen aus (7.13) dominiert. Da $\beta(\chi_q)$ für alle $q \mid\mid \frac{\ell-1}{2}$ berechnet werden muss, erhalten wir eine Gesamtlaufzeit von

$$\sum_{q \mid\mid \frac{\ell-1}{2}} (7.11) + (7.13). \tag{7.14}$$

für diesen Schritt. Da $\frac{\ell-1}{2}$ höchstens $\log \ell$ verschiedene Primteiler hat, können wir die Kosten mit

$$\begin{aligned} &O(\log \ell (q\,\mathsf{C}(r\ell) + \mathsf{M}(q)\,\mathsf{M}(rq) \log p + q\,\mathsf{C}(rq) + \mathsf{C}(q)\,\mathsf{M}(rq) \log rq)) \\ &= \tilde{O}(q\,\mathsf{C}(r\ell) + rq^2 \log p) \end{aligned} \tag{7.15}$$

abschätzen, wo nun $q = \max_i\{q_i \mid\mid \frac{\ell-1}{2}\}$ gilt.

7.3.2 Berechnung von α

Mit dem Ansatz aus Abschnitt 7.2.1 erhalten wir folgende Kosten für die Bestimmung von α. Zunächst berechnen wir den Isomorphismus α_q. Sobald der Wert $\beta(\chi_q)$ für $q \mid\mid \frac{\ell-1}{2}$ bekannt ist, sind die Werte $\beta(\chi_q^j), j = 2, \ldots, q$, zu berechnen, was gemäß Lemma 7.2.8 $O(q)$ Multiplikationen in $\mathbf{A}[\zeta_q, \theta^{(q)}]$ erfordert. Anschließend lösen wir ein lineares Gleichungssystem von Dimension q über $\mathbf{A}[\zeta_q]$, wobei die zu invertierende Matrix zu einer diskreten Fouriertransformation gehört, weshalb dieser Schritt $O(q \log q)$ Multiplikationen in $\mathbf{A}[\zeta_q]$ erfordert. Bezeichnen wir mit q die maximale Primzahlpotenz, die $\frac{\ell-1}{2}$ teilt, erhalten wir insgesamt Kosten von

$$\tilde{O}(q\,\mathsf{M}(rq^2) + q \log q\,\mathsf{M}(rq)) = \tilde{O}(rq^3). \tag{7.16}$$

Für die induktive Berechnung von α aus den verschiedenen α_q müssen in jedem Schritt die Polynome M_1, M_2, W bestimmt werden. Dafür sollte man den Algorithmus aus [MMS07, S. 4–5] anpassen können, was die Laufzeit

$$O(q_2^{1/2}\,\mathsf{M}(r\ell) + q_2^{(\omega-1)/2} r\ell)$$

liefert. Da $\omega > 2$ gilt, kann die Laufzeit durch

$$\tilde{O}(q_2^{(\omega-1)/2} r\ell) \tag{7.17}$$

abgeschätzt werden. Nun verfügen wir über ein Polynom $W = \sum_{k=0}^{q_2-1} w_k X^k \in \mathbf{B}_{q_1}[X]$, sodass $W(\theta^{(q_2)}) = \theta^{(q_1 q_2)}$. Da die Terme, die man bei der Berechnung von Potenzen von

$\alpha_{q_2}(\theta^{(q_2)}) = \sum_{i=0}^{q_2-1} a_i \sigma^i(\zeta_\ell^{(q_2)})$ erhält, in der Regel nicht direkt in derselben Form geschrieben werden können, benutzen wir von Anfang an die Darstellung $\alpha_{q_2}(\theta^{(q_2)}) = \sum_{i=0}^{\ell-1} a_i \zeta_\ell^i$, die man leicht durch Ausschreiben der $\zeta_\ell^{(q_2)}$ erhält.
Da W den Grad q_2-1 aufweist, müssen die Potenzen bis zu diesem Exponenten berechnet werden, was $O(q_2\,\mathsf{M}(r\ell))$ Operationen ergibt. Danach muss noch $\sum_{k=0}^{q_2-1} w_k \alpha_{q_2}(\theta^{(q_2)})^k$ bestimmt werden. Die w_k sind Polynome in Potenzen von $\alpha_{q_1}(\theta^{(q_1)})$, die in $O(q_1\,\mathsf{M}(r\ell))$ Operationen berechnet werden können. Abschließend sind die Terme in $O(q_2\,\mathsf{M}(r\ell))$ Operationen zu multiplizieren, womit $\alpha_{q_1 q_2}$ bestimmt ist. Insgesamt ergibt sich zusätzlich

$$\tilde{O}((q_1 + q_2)r\ell), \tag{7.18}$$

was (7.17) dominiert, da $\omega \leqslant 3$ gilt, sodass dies die Laufzeit eines induktiven Schritts ist.

Offensichtlich müssen höchstens $O(\log \ell)$ induktive Schritte durchgeführt werden, bis α bestimmt ist. Damit ist die Gesamtlaufzeit gleich (7.18), wobei q_1, q_2 mit $q_1 q_2 = \frac{\ell-1}{2}$ die maximalen Werte bei der iterativen Bestimmung von α sind. Im besten Fall können q_1, q_2 von Ordnung $O(\sqrt{\ell})$ gewählt werden, was eine Laufzeit von $O(r\ell^{3/2})$ Operationen ergibt, wohingegen die Laufzeit bei $O(r\ell^2)$ liegt, wenn der größte Primpotenzteiler $q \mid\mid \frac{\ell-1}{2}$ von Ordnung $O(\ell)$ ist.

7.3.3 Berechnung von t

Aufgrund der speziellen Struktur von $\mathbf{C}$ kann die Berechnung von φ_p in dieser Algebra sehr schnell durchgeführt werden, wie bereits angemerkt. Um den Homomorphismus φ_p effizient auf beliebige $b = \sum_{i=0}^{\ell-1} a_i \zeta_\ell^i$ anwenden zu können, reicht es aus, die Wirkung von φ_p auf einer Basis von $\mathbf{A}$ zu kennen. Wählt man eine Potenzbasis $\{1, x, \ldots x^{r-1}\}$, dann ist es hinreichend, $\varphi_p(x)$ in $\mathbf{A}$ zu berechnen, woraus man direkt $\varphi_p(x^k) = (\varphi_p(x))^k$ erhält. Somit liegen die Kosten für die Vorberechnungen bei $O(\mathsf{M}(r)\log p)$ Operationen. Anschließend kann der Wert $\varphi_p(a) = \sum_{j=0}^{r-1} c_j \varphi_p(x)^j$ für $a = \sum_{j=0}^{r-1} c_j x^j \in \mathbf{A}$ mit $O(r^2)$ Multiplikationen in $\mathbb{F}_p$ ermittelt werden. Um $\varphi_p(b)$ zu bestimmen, muss diese Rechnung ℓ-mal ausgeführt werden. Somit können die durch Wirkung des Frobenius-Homomorphismus entstehenden Werte in Laufzeit $O(r^2\ell)$ berechnet werden.

Abschließend muss t durch das Testen möglicher Werte bestimmt werden, was $O(\ell\,\mathsf{M}(r\ell))$ Operationen erfordert. Insgesamt ergibt sich für diesen Schritt eine Laufzeit von

$$O(\mathsf{M}(r)\log p + r^2\ell + \ell\,\mathsf{M}(r\ell)) = \tilde{O}(r\log p + r\ell^2). \tag{7.19}$$

7.3.4 Gesamtlaufzeit

Die Kombination der verschiedenen Abschätzungen (7.15), (7.16), (7.18), (7.19) aus den vorangehenden Abschnitten ergibt

$$\begin{aligned} &\tilde{O}(q\,\mathsf{C}(r\ell) + rq^2\log p + rq^3 + (q_1+q_2)r\ell + r\log p + r\ell^2) \\ &= \tilde{O}(rq^2\log p + q\,\mathsf{C}(r\ell) + rq^3 + r\ell^2). \end{aligned} \tag{7.20}$$

Wir vergleichen dies mit der Laufzeit für den Elkies-Fall, die $\tilde{O}(\ell\log p)$ Operationen be-

trägt, wohingegen die entsprechenden Rechnungen im ursprünglichen Algorithmus von Schoof $\tilde{O}(\ell^2 \log p)$ Operationen benötigten. Da wir erwarten, dass die größte zu betrachtende Primzahl ℓ von Ordnung $O(\log p)$ ist, erlaubt der ursprüngliche Algorithmus die Verwendung von Atkin-Primzahlen $\ell \in \tilde{O}(\sqrt{\log p})$. Wir untersuchen nun die Bedingungen dafür, dass unsere Laufzeit $\tilde{O}(\log^2 p)$, d. h. die Kosten für Elkies-Primzahlen $\ell \in O(\log p)$, nicht überschreitet.

Wir erhalten die folgenden Einschränkungen:

$$\begin{aligned} rq^2 &\in \tilde{O}(\log p), \\ q\,\mathsf{C}(r\ell) \in \tilde{O}(\log^2 p), \quad rq^3 &\in \tilde{O}(\log^2 p), \quad r\ell^2 \in \tilde{O}(\log^2 p). \end{aligned}$$

Die erste Bedingung impliziert dabei die mittlere in der zweiten Zeile. Nehmen wir an, dass r klein ist, so ergibt sich

$$q \in \tilde{O}(\sqrt{\log p}), \quad q\,\mathsf{C}(\ell) \in \tilde{O}(\log^2 p),$$

sodass, wenn die Teiler q von $\frac{\ell-1}{2}$ klein genug sind, Atkin-Primzahlen mit $\mathsf{C}(\ell) \in \tilde{O}((\log p)^{1,5})$, also $\ell \in \tilde{O}((\log p)^{0,89})$ für den besten bekannten Wert von $\omega \approx 2{,}38$, benutzt werden können. Allerdings kann, wenn r klein ist, genau so gut die bestehende generische Methode für Atkin-Primzahlen aus [Sch95, Mül95] benutzt werden, die in diesem Fall effizient ist.
Gibt man die Annahme, dass r klein ist, auf und nimmt nur $r \in O(\ell)$ an, muss offenbar erstens q kleinere Werte annehmen und zweitens wird $O(q\,\mathsf{C}(r\ell))$ zum dominierenden Term in der zweiten Zeile. Falls q klein ist, erhält man für ℓ die Schranke

$$\ell \in \tilde{O}((\log p)^{\frac{2}{\omega+1}}),$$

was $\ell \in \tilde{O}\left((\log p)^{0,59}\right)$ statt $\ell \in \tilde{O}\left((\log p)^{0,5}\right)$ im Algorithmus von Schoof ergibt.

Somit könnte die Methode es erlauben, wenn die Werte von r und q nicht zu groß werden, etwas größere Atkin-Primzahlen ℓ zu verwenden. Ihr praktischer Nutzen ist jedoch als gering einzuschätzen.

Notation

$\mathbb{N}$	natürliche Zahlen
$\mathbb{Z}$	ganze Zahlen
$\mathbb{C}$	komplexe Zahlen
$\mathbb{H}$	obere Halbebene
$\mathbb{F}_{p^r}$	endlicher Körper mit p^r Elementen
ζ_ℓ	primitive ℓ-te Einheitswurzel
μ_ℓ	Gruppe der ℓ-ten Einheitswurzeln
φ_p	Frobenius-Homomorphismus über $\mathbb{F}_p$
ϕ_p	Frobenius-Homomorphismus auf elliptischer Kurve $E/\mathbb{F}_p$ → S. 17
t	Spur von ϕ_p im Endomorphismenring von E
e_ℓ	Weil-Paarung → S. 16
O	$f \in O(g)$ äquivalent zu $\exists C : \lvert f\rvert \leqslant C\lvert g\rvert$
$\tilde{O}$	$f(x) \in \tilde{O}(g(x))$ äquivalent zu $\exists N : f(x) \in O(g(x)\log^N x)$
$\mathsf{M}(n)$	Aufwand zur Multiplikation von Polynomen f, g von Grad $< n$
$\mathsf{C}(n)$	Aufwand zur Berechnung von $g(h) \mod f$ für $f, g, h \in \mathbb{F}_p[X]$ von Grad $< n$
$\mathrm{ord}(f)$	Ordnung der Laurentreihe f → S. 39
$\mathrm{lk}(f)$	Leitkoeffizient der Laurentreihe f → S. 39
Γ	$\mathrm{SL}_2(\mathbb{Z})$
$\Gamma_0(\ell), \Gamma(\ell)$	Untergruppen von Γ → S. 23
$\mathbf{A}_0(G)$	Modulfunktionen von Gewicht 0 für G
$\mathbf{H}_0(G)$	holomorphe Modulfunktionen von Gewicht 0 für G
q, $q(\tau)$	$\exp(2\pi i\tau)$ für $\tau \in \mathbb{H}$
Δ	Diskriminante → S. 25
j	j-Invariante → S. 25
η	Dedekindsche η-Funktion → S. 25
p_1, m_ℓ, a_ℓ	Modulfunktionen für $\Gamma_0(\ell)$ → S. 27, 50
M_ℓ, A_ℓ	Minimalpolynome von m_ℓ, a_ℓ → S. 31
w_ℓ	Fricke-Atkin-Lehner-Involution → S. 26
f^*	äquivalente Notation für $w_\ell(f)$
$\wp$	Weierstraßsche $\wp$-Funktion → S. 33
$\tau_{\ell,n,\chi}$	universelle elliptische Gauß-Summe → S. 37
$J_{\ell,n,\chi,k}$	universelle elliptische Jacobi-Summe → S. 62

Literaturverzeichnis

[Á14] Álvarez Martínez, Irene: *Polynomially cyclic algebras and Kummer theory in point counting on elliptic curves*, Georg-August-Universität Göttingen, Masterarbeit, 2014

[Abr96] Abramovich, Dan: A linear lower bound on the gonality of modular curves. In: *Internat. Math. Res. Notices* (1996), Nr. 20, S. 1005–1011

[Apo76] Apostol, Tom M.: *Graduate Texts in Mathematics*. Bd. 41: *Modular functions and Dirichlet series in number theory*. Springer-Verlag, New York, Heidelberg, 1976

[BDD+] Brieulle, Ludovic ; De Feo, Luca ; Doliskani, Javad ; Flori, Jean-Pierre ; Schost, Éric: *Computing isomorphisms and embeddings of finite fields*. `https://github.com/defeo/ffisom`

[Ber13] Berghoff, Christian: *Elliptische Gauss-Summen und algebraische Verbesserungen des Schoof-Algorithmus*, Georg-August-Universität Göttingen, Masterarbeit, 2013

[BLS12] Bröker, Reinier ; Lauter, Kristin ; Sutherland, Andrew V.: Modular polynomials via isogeny volcanoes. In: *Math. Comp.* 81 (2012), Nr. 278, S. 1201–1231

[BMSS08] Bostan, Alin ; Morain, François ; Salvy, Bruno ; Schost, Éric: Fast algorithms for computing isogenies between elliptic curves. In: *Math. Comp.* 77 (2008), Nr. 263, S. 1755–1778

[BP05] Brisebarre, Nicolas ; Philibert, Georges: Effective lower and upper bounds for the Fourier coefficients of powers of the modular invariant j. In: *J. Ramanujan Math. Soc.* 20 (2005), Nr. 4, S. 255–282

[BS10] Bröker, Reinier ; Sutherland, Andrew V.: An explicit height bound for the classical modular polynomial. In: *Ramanujan J.* 22 (2010), Nr. 3, S. 293–313

[BSS99] Blake, Ian F. ; Seroussi, Gadiel ; Smart, Nigel P.: *Elliptic curves in cryptography*. Cambridge University Press, 1999

[BSS05] Blake, Ian F. (Hrsg.) ; Seroussi, Gadiel (Hrsg.) ; Smart, Nigel P. (Hrsg.): *London Mathematical Society Lecture Note Series*. Bd. 317: *Advances in elliptic curve cryptography*. Cambridge University Press, Cambridge, 2005

[CDM96] Couveignes, Jean-Marc ; Dewaghe, Laurent ; Morain, François: Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research report LIX/RR/96/03 / École Polytechnique. 1996. – Forschungsbericht. – Verfügbar unter `http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/isog-cycles.pdf`

[Coh84] Cohen, Paula: On the coefficients of the transformation polynomials for the elliptic modular function. In: *Math. Proc. Cambridge Philos. Soc.* 95 (1984), Nr. 3, S. 389–402

[Cox89] Cox, David A.: *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, Inc., New York, 1989

[CW90] Coppersmith, Don ; Winograd, Shmuel: Matrix multiplication via arithmetic progressions. In: *J. Symbolic Comput.* 9 (1990), Nr. 3, S. 251–280

[de 66] de Bruijn, Nicolaas G.: On the number of positive integers $\leqslant x$ and free of prime factors $> y$. II. In: *Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math.* 28 (1966), S. 239–247

[Deu58] Deuring, Max: *Enzyklopädie der mathematischen Wissenschaften mit Einschluß ihrer Anwendungen.* Bd. I 2, Heft 10, Teil II: *Die Klassenkörper der komplexen Multiplikation.* B. G. Teubner Verlagsgesellschaft, Stuttgart, 1958

[Dew98] Dewaghe, Laurent: Remarks on the Schoof-Elkies-Atkin algorithm. In: *Math. Comp.* 67 (1998), Nr. 223, S. 1247–1252

[Dic30] Dickmann, Karl: On the frequency of numbers containing prime factors of a certain relative magnitude. In: *Ark. Mat. Astr. Fys.* 2 (1930), S. 1–14

[DS14] Doliskani, Javad ; Schost, Éric: Taking roots over high extensions of finite fields. In: *Math. Comp.* 83 (2014), Nr. 285, S. 435–446

[Eis95] Eisenbud, David: *Graduate Texts in Mathematics.* Bd. 150: *Commutative algebra – With a view toward algebraic geometry.* Springer-Verlag, New York, 1995

[EM02] Enge, Andreas ; Morain, François: Comparing invariants for class fields of imaginary quadratric fields. In: *Lecture Notes in Comput. Sci.* Bd. 2369. Springer-Verlag, Berlin, 2002, S. 252–266

[EM06] Enge, Andreas ; Morain, François: *SEA in genus 1: 2500 decimal digits.* Posting to the Number Theory List, 2006

[Eng09] Enge, Andreas: Computing modular polynomials in quasi-linear time. In: *Math. Comp.* 78 (2009), Nr. 267, S. 1809–1824

[ES05] Enge, Andreas ; Schertz, Reinhard: Modular curves of composite level. In: *Acta Arith.* 118 (2005), Nr. 2, S. 129–141

[FKDG12] Franke, Jens ; Kleinjung, Thorsten ; Decker, Andreas ; Grosswendt, Anna: *Format of the certificate (version 0.1).* Verfügbar unter `http://www.math.uni-bonn.de/people/franke/ptest/fmt-0.1.pdf`, 2012

[FM02] Fouquet, Mireille ; Morain, François: Isogeny volcanoes and the SEA algorithm. In: *Lecture Notes in Comput. Sci.* Bd. 2369. Springer-Verlag, Berlin, 2002, S. 276–291

[Fra16] Franke, Jens: *Private Mitteilungen.* 2014–2016

[GM06] Gaudry, Pierrick ; Morain, François: Fast algorithms for computing the eigenvalue in the Schoof-Elkies-Atkin algorithm. In: *ISSAC 2006.* ACM, New York, 2006, S. 109–115

[Gra08] Granville, Andrew: Smooth numbers: computational number theory and beyond. In: *Math. Sci. Res. Inst. Publ.* Bd. 44. Cambridge Univ. Press, Cambridge, 2008, S. 267–323

[Gra15] Granlund, Torbjörn et al.: *GNU Multiple Precision Arithmetic Library 6.1.0.* `https://gmplib.org/`. Version: November 2015

[Hec37] Hecke, Erich: Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. II. In: *Math. Ann.* 114 (1937), Nr. 1, S. 316–351

[Inr09] Inria Project-Team TANC: Activity Report 2009 / Inria Saclay. 2009. – Forschungsbericht. – Verfügbar unter `http://raweb.inria.fr/rapportsactivite/RA2009/tanc/tanc.pdf`

[Iwa97] Iwaniec, Henryk: *Graduate Studies in Mathematics*. Bd. 17: *Topics in classical automorphic forms*. American Mathematical Society, Providence, RI, 1997

[Kob87] Koblitz, Neal: Elliptic curve cryptosystems. In: *Math. Comp.* 48 (1987), S. 203–209

[Kob93] Koblitz, Neal: *Graduate Texts in Mathematics*. Bd. 97: *Introduction to elliptic curves and modular forms*. 2. Auflage. Springer-Verlag, New York, 1993

[Lan87] Lang, Serge: *Graduate Texts in Mathematics*. Bd. 112: *Elliptic functions*. 2. Auflage. Springer-Verlag, New York, 1987

[LM09] Lochter, Manfred ; Merkle, Johannes: *Ein neuer Standard für elliptische Kurven*. 11. Deutscher IT-Sicherheitskongress des BSI, 2009

[Maz77] Mazur, Barry: Modular curves and the Eisenstein ideal. In: *Inst. Hautes Études Sci. Publ. Math.* (1977), Nr. 47, S. 33–186

[Mih06a] Mihăilescu, Preda: Cyclotomy Primality Proofs and their Certificates. In: *Mathematica Gottingensis* (2006)

[Mih06b] Mihăilescu, Preda: Dual Elliptic Primes and applications to cyclotomic primality proving. In: *Mathematica Gottingensis* (2006)

[Mih06c] Mihăilescu, Preda: Elliptic curve Gauss sums and counting points. In: *Mathematica Gottingensis* (2006)

[MM01] Maurer, Markus ; Müller, Volker: Finding the eigenvalue in Elkies' algorithm. In: *Experiment. Math.* 10 (2001), Nr. 2, S. 275–285

[MMS07] Mihăilescu, Preda ; Morain, François ; Schost, Éric: Computing the eigenvalue in the Schoof-Elkies-Atkin algorithm using Abelian lifts. In: *ISSAC 2007*. ACM, New York, 2007, S. 285–292

[Mor95] Morain, François: Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. In: *J. Théor. Nombres Bordeaux* 7 (1995), Nr. 1, S. 255–282. – Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993)

[MSS16] Morain, François ; Scribot, Charlotte ; Smith, Benjamin: Computing cardinalities of Q-curve reductions over finite fields. In: *ANTS-XII – Twelfth Algorithmic Number Theory Symposium*, 2016

[Mül95] Müller, Volker: *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*, Universität des Saarlandes, Diss., 1995

[MV07] Montgomery, Hugh L. ; Vaughan, Robert C.: *Cambridge Studies in Advanced Mathematics*. Bd. 97: *Multiplicative number theory. I. Classical theory*. Cambridge University Press, Cambridge, 2007

[MV10] Mihăilescu, Preda ; Vuletescu, Victor: Elliptic Gauss sums and applications to point counting. In: *Journal of Symbolic Computation* 45 (2010), S. 825–836

[Neu07] Neukirch, Jürgen: *Algebraische Zahlentheorie.* Nachdruck des Originals von 1992. Springer-Verlag, Berlin, 2007

[New57] Newman, Morris: Construction and application of a class of modular functions. In: *Proc. London. Math. Soc.* 7 (1957), Nr. 3, S. 334–350

[Pet32] Petersson, Hans: Über die Entwicklungskoeffizienten der automorphen Formen. In: *Acta Math.* 58 (1932), Nr. 1, S. 169–215

[Rad42] Rademacher, Hans: The Ramanujan identities under modular substitutions. In: *Trans. Amer. Math. Soc.* 51 (1942), S. 609–636

[Rib01] Ribenboim, Paulo: *Classical theory of algebraic numbers*. Springer-Verlag, New York, 2001 (Universitext)

[Sch74] Schoeneberg, Bruno: *Elliptic modular functions: an introduction*. Springer-Verlag, New York, Heidelberg, 1974

[Sch85] Schoof, René: Elliptic curves over finite fields and the computation of square roots mod p. In: *Math. Comp.* 44 (1985), Nr. 170, S. 483–494

[Sch95] Schoof, René: Counting points on elliptic curves over finite fields. In: *J. Théor. Nombres Bordeaux* 7 (1995), Nr. 1, S. 219–254. – Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993)

[Sch10] Schertz, Reinhard: *New Mathematical Monographs*. Bd. 15: *Complex multiplication*. Cambridge University Press, Cambridge, 2010

[Ser73] Serre, Jean-Pierre: *Graduate Texts in Mathematics*. Bd. 7: *A course in arithmetic*. Springer-Verlag, New York, Heidelberg, 1973

[Shi71] Shimura, Goro: *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. – Kanô Memorial Lectures, No. 1

[Sil94] Silverman, Joseph H.: *Graduate Texts in Mathematics*. Bd. 151: *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994

[Sil09] Silverman, Joseph H.: *Graduate Texts in Mathematics*. Bd. 106: *The arithmetic of elliptic curves*. 2. Auflage. Springer-Verlag, Dordrecht, 2009

[SS14] Shparlinski, Igor E. ; Sutherland, Andrew V.: On the distribution of Atkin and Elkies primes. In: *Found. Comput. Math.* 14 (2014), Nr. 2, S. 285–297

[Sut13] Sutherland, Andrew V.: On the evaluation of modular polynomials. In: *ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium* Bd. 1. Math. Sci. Publ., Berkeley, CA, 2013, S. 531–555

[Tat95] Tate, John: A review of non-Archimedean elliptic functions. In: *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*. Int. Press, Cambridge, MA, 1995 (Ser. Number Theory, I), S. 162–184

[Ten15] Tenenbaum, Gérald: On ultrafriable integers. In: *Q. J. Math.* 66 (2015), Nr. 1, S. 333–351

[vG03] von zur Gathen, Joachim ; Gerhard, Jürgen: *Modern computer algebra*. 2. Auflage. Cambridge University Press, New York, 2003

[Was08] Washington, Lawrence C.: *Elliptic curves: Number theory and Cryptography*. 2. Auflage. Chapman & Hall/CRC, Boca Raton, FL, 2008 (Discrete Mathematics and its Applications (Boca Raton))

[Web08] Weber, Heinrich: *Lehrbuch der Algebra*. Bd. III. 3. Auflage. Chelsea Publishing Company, 1908