S-ganze Punkte auf elliptischen Kurven

Diplomarbeit
von
Doris Kern

betreut von
Prof. Dr. M. Pohst

angefertigt am Institut für Mathematik der
Technischen Universität Berlin

März 2009

Eidesstattliche Versicherung

Ich versichere, dass ich diese Diplomarbeit selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

Berlin, den 30. April 2009

Inhaltsverzeichnis

Einleitung **7**

1 Grundlagen **11**

1.1 Elliptische Kurven 11

1.2 Besondere Eigenschaften elliptischer Kurven 15

1.3 p-adische Zahlen und Bewertungen 16

1.3.1 Bewertungen 16

1.3.2 p-adische Bewertungen 17

1.3.3 p-adische Zahlen 19

1.4 Höhen auf elliptischen Kurven 20

1.5 Algorithmen zum Berechnen wichtiger Größen 24

1.5.1 Perioden und elliptische Logarithmen 24

1.5.2 p-adische elliptische Logarithmen 27

1.5.3 Test auf S-Ganzheit 31

2 Schranken **33**

2.1 Schranken über $\mathbb{Q}$ 33

2.2 Schranken über Zahlkörpern 35

2.2.1 Einige notwendige Sätze 37

2.2.2 Schranken für Einheitengleichungen 39

2.2.3 Schranken für $h_n(P)$ 49

3 Reduktion der Schranken **55**

3.1 Grundlagen zur LLL-Reduktion 56

3.2 Aufstellen der Linearformen 62

3.2.1 Die unendlichen Stellen 62
3.2.2 Die endliche Stelle im Fall $\mathbb{K}_\mathfrak{p} = \mathbb{Q}_p$ 65
3.2.3 Die endliche Stelle über $\mathbb{K}_\mathfrak{p} \neq \mathbb{Q}_\mathfrak{p}$ 66

4 Suche nach S-ganzen Punkten 69
4.1 Die Reduktion einer elliptischen Kurve 69
4.2 Suche durch Reduktion der Kurve 72
4.2.1 Reduktion modulo $\mathfrak{p} \notin S$ 73
4.2.2 Reduktion modulo $\mathfrak{p} \in S$ 77
4.3 Ausschluss von Vielfachen 84
4.4 Torsionspunkte 85

Zusammenfassung 89

A Beispiele 91
A.1 Eine Kurve über $\mathbb{Q}$ 92
A.2 Kurven über Zahlkörpern 98

B Algorithmen 107

Literaturverzeichnis 122

Einleitung

Das Ziel dieser Arbeit ist es, die Suche nach S-ganzen Punkten auf elliptischen Kurven über einem algebraischen Zahlkörper in dem Verfahren von Herrmann [Her02] zu verbessern und effizienter zu gestalten. Dabei können S-ganze Punkte als Verallgemeinerung der ganzen Punkte aufgefasst werden: Die Menge der S-ganzen Punkte umfasst zusätzlich zu den ganzen Punkten auch die, die nur bestimmte Stellen im Nenner enthalten. Welche Stellen das sein dürfen wird in der Menge S festgelegt. Die ganzen Punkte erhält man folglich, wenn die Menge S genau die archimedischen Stellen umfasst. Deshalb sind die Fortschritte bei der Bestimmung der S-ganzen Punkte meist eng mit denen zur Berechnung ganzer Punkte verbunden.

Bereits 1929 zeigte Siegel in [Sie29], dass die Anzahl der ganzen Punkte auf einer elliptischen Kurve über einem algebraischen Zahlkörper endlich ist, und 1934 verallgemeinerte Mahler in [Mah34] diese Aussage auf S-ganze Punkte. Beide Beweise sind allerdings nicht konstruktiv und liefern keine Hinweise zur Bestimmung der Punkte. Etwa 30 Jahre später konnte Baker in [Bak68] mit Hilfe von Linearformen in elliptischen Logarithmen erstmals Schranken für die Höhe ganzzahliger Lösungen elliptischer Kurven angeben. Bakers Schranken wurden in den darauffolgenden Jahren immer wieder verbessert und verallgemeinert. Es wurde dabei stets algebraisch zahlentheoretisch vorgegangen.

Im Gegensatz dazu stellten Lang [Lan78] und Zagier [Zag87] einen ersten Ansatz zum Bestimmen ganzer Punkte mit Hilfe der Gruppenstruktur der elliptischen Kurve vor. Daraus entwickelten Stroeker und Tzanakis in [ST94] und Gebel, Pethő und Zimmer in [GPZ94] einen Algorithmus zum Finden ganzer Punkte auf elliptischen Kurven über den rationalen Zahlen. Dieser Ansatz setzt voraus, dass die Mordell-Weil-Basis der Kurve bekannt ist, wobei deren Berechnung allerdings nach wie vor ein Problem darstellt und besonders über Zahlkörpern oft nicht möglich ist. In diesem Verfahren zum Bestimmen der ganzen Punkte werden Schranken für Linearformen mit komplexen elliptischen Logarithmen benötigt. Diese konnten mit Hilfe der Ergebnisse von David aus [Dav95] angegeben werden. Smart stellte in [Sma94] eine Erweiterung des Algorithmus für S-ganze Punkte vor, ohne jedoch die entsprechen-

den Schranken für die nun auftretenden p-adisch elliptischen Logarithmen zu kennen, weshalb sein Verfahren nur auf geschätzten Schranken beruhte. Gleichzeitig gab er in dieser Arbeit einen Hinweis, wie das Testen aller verbleibenden Möglichkeiten nach dem Bestimmen der Schranken effizienter gestaltet werden könnte, allerdings nur für ein Beispiel mit Mordell-Weil-Basis der Länge zwei. Dies wird unter anderem in der vorliegenden Arbeit aufgegriffen und für beliebige Basen erweitert.

Pethő, Zimmer, Gebel und Herrmann verknüpften schließlich in [PHZH99] den zahlentheoretischen Ansatz mit dem über die Gruppenstruktur und konnten so die Notwendigkeit der Schranken von Linearformen in p-adisch elliptischen Logarithmen umgehen. Ein Verfahren zur Bestimmung aller ganzen Punkte einer elliptischen Kurve über einem Zahlkörper mit Darstellung nur in Weierstraß-Form wurde von Smart und Stephens beschrieben. Herrmann gibt in [Her02] ein Verfahren zum Bestimmen der S-ganzen Punkte über elliptischen Kurven in weiteren Darstellungen über Zahlkörpern an. Um Abschätzungen für die auftretenden Linearformen zu erhalten, greift Herrmann auf die Arbeit [Bug97] von Bugeaud zurück. Dazu berechnet er die dort auftretenden Konstanten effektiv. In der vorliegenden Arbeit werden unter anderem einige darin enthaltene Fehler beseitigt.

Die Arbeit gliedert sich in fünf Kapitel. Im ersten Kapitel werden die Grundlagen über elliptische Kurven und Bewertungstheorie bereitgestellt, die für das weitere Vorgehen benötigt werden. Dabei sind besonders die Höhenfunktionen von Bedeutung. Außerdem werden einige Algorithmen angegeben, um p-adische elliptische Logarithmen und die Perioden der Kurve zu berechnen.

In Kapitel 2 wird eine Schranke für die Koeffizienten in der Darstellung eines S-ganzen Punktes mittels der Mordell-Weil-Basis hergeleitet. Dabei wird überwiegend die Beweisführung Herrmanns aus [Her02] übernommen. Allerdings werden vor allem bei der Abschätzung von Lösungen von Einheitengleichungen einige Lücken in der Beweisführung von Herrmann geschlossen und einige Abschätzungen verschärft.

Da die Schranke aus Kapitel 2 im Allgemeinen viel zu groß wird, um damit weiter zu arbeiten, wird sie mit Hilfe der LLL-Reduktion verkleinert. Die entsprechenden Verfahren sind in Kapitel 3 beschrieben. Dazu müssen Linearformen in elliptischen, p-adisch elliptischen und pseudo p-adisch elliptischen Logarithmen aufgestellt werden.

Durch die reduzierte Schranke wird die Anzahl der Möglichkeiten von Linearkombinationen, die als S-ganze Punkte in Frage kommen, deutlich eingeschränkt. Um alle Möglichkeiten durchprobieren zu können, sind es aber oft noch zu viele. In Kapitel 4 werden deshalb Möglichkeiten vorgestellt, um Linearkombinationen a priori auszuschließen. Dabei werden die Eigenschaften einer elliptischen Kurve bei der Reduktion nach einer Stelle ausgenutzt.

Im Anhang werden die Ergebnisse der Berechnung einiger Beispiele dargestellt. Ein großes Problem ist dabei, dass als Eingabe die Mordell-Weil-Basis der Kurve benötigt wird, deren Berechnung über Zahlkörpern allerdings äußerst problematisch ist. Außerdem wird der Pseudocode, auf den in den einzelnen Kapiteln Bezug genommen wird, im Anhang angegeben. In Kapitel 1 findet sich eine Ausnahme, wo zum besseren Verständnis der Code direkt im Text angegeben wurde.

Kapitel 1

Grundlagen

1.1 Elliptische Kurven

Definition 1.1. Eine *elliptische Kurve* ist eine nicht-singuläre algebraische Kurve E der Ordnung 3 und mit Geschlecht 1, auf der mindestens ein rationaler Punkt liegt.
Nicht-singulär bedeutet hierbei, dass es keinen Punkt auf der Kurve gibt, an dem beide Ableitungen verschwinden.

Elliptische Kurven kann man über einem Körper $\mathbb{K}$ durch verschiedene Gleichungen darstellen.

Definition 1.2.

- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ heißt *Weierstraß-Form* der Kurve.
- $y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{K},$ heißt *kurze Weierstraß-Form.*
- $\xi^2 = \eta(\eta - 1)(\eta - \kappa), \quad \kappa, \eta, \xi \in \mathbb{K}, \kappa \neq 0, 1,$ heißt *Legendre-Form.*

Über einem beliebigen Körper $\mathbb{K}$ gibt es für jede elliptische Kurve eine Transformation, die die Kurve in Weierstraß-Form überführt. Eine Transformation in kurze Weierstraß-Form oder Legendre-Form ist über Körpern mit einer Charakteristik $\neq 2, 3$ immer möglich.

Satz 1.3. *Eine Koordinatentransformation von langer in kurze Weierstraß-Form ist gegeben durch die Substitiution*

$$y := Y - \frac{a_1}{2}x - \frac{a_3}{2}, \quad x := X - \frac{1}{3}\left(a_2 + \frac{a_1^2}{4}\right).$$

Eine Transformation von kurzer Weierstraß-Form in Legendre-Form ist gegeben durch die Substitution

$$X := (e_2 - e_1)\eta + e_1, \quad Y := 2(e_2 - e_1)^{3/2}\xi.$$

Dabei ist $\kappa = \frac{e_3 - e_1}{e_2 - e_1}$. *Die* e_i, *die Nullstellen der rechten Seite der kurzen Weierstraß-Form, sind so nummeriert, dass* $|\kappa| < 1$ *gilt.*

Beweis: [Sil86] □

Im Bezug auf die lange Weierstraß-Form lassen sich einige nützliche Invarianten angeben, die im Laufe der Arbeit in verschiedenen Zusammenhängen verwendet werden.

Definition 1.4.

- *b-Invariante*

$$\begin{aligned} b_2 &:= a_1^2 + 4a^2, \\ b_4 &:= 2a_4 + a_1a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2; \end{aligned}$$

- *c-Invariante*

$$\begin{aligned} c_4 &:= b_2^2 - 24b_4, \\ c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6; \end{aligned}$$

- *Diskriminante*

$$\Delta := -b_2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6;$$

- *j-Invariante*

$$j := \frac{c_4^3}{\Delta};$$

- *invariantes Differential*

$$\frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Bemerkung 1.5. Eine Gleichung in Weierstraß-Form beschreibt genau dann eine elliptische Kurve, d.h. ist nicht-singulär, wenn ihre Diskriminante $\neq 0$ ist.

Im Folgenden bezeichne eine elliptische Kurve immer die Menge der Punkte, die die Gleichung der Kurve erfüllen:

$$E(\mathbb{K}) := \left\{(x, y) \in \mathbb{K}^2 \,|\, y^3 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{\mathcal{O}_E\}$$

Diese Punktmenge bildet zusammen mit einem weiteren Punkt $\mathcal{O}_E$ eine additive Gruppe. $\mathcal{O}_E$ entspricht dem Punkt im Unendlichen und bildet das neutrale Element der Gruppe. Die Verknüpfung „+“ ist dabei folgendermaßen definiert:

Seien $P_1, P_2 \in E(\mathbb{K})$:

- $P_1 + \mathcal{O}_E = \mathcal{O}_E + P_1 = P_1$,
- $P_1 + (-P_1) = \mathcal{O}_E$, wobei

$$-P_1 = \begin{cases} \mathcal{O}_E & \text{falls } P_1 = \mathcal{O}_E, \\ (x_1, -y_1 - a_1x_1 - a_3) & \text{falls } P_1 = (x_1, y_1) \neq \mathcal{O}_E. \end{cases}$$

- Falls $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ mit $P_1 \neq -P_2$ und $P_1, P_2 \neq \mathcal{O}_E$ sind, so ist

$$P_1 + P_2 = (x_3, y_3),$$

mit

$$(x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2,\ -(\lambda + a_1)x_3 - \nu - a_3),$$

$$\lambda = \begin{cases} \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{falls } P_1 = P_2, \\ \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P_1 \neq P_2 \end{cases}$$

und

$$\nu = \begin{cases} \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{falls } P_1 = P_2, \\ \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{falls } P_1 \neq P_2. \end{cases}$$

Geometrisch betrachtet bedeutet dies, dass man zunächst P_1 und P_2 mit einer Geraden verbindet. Gilt $P_1 = P_2$, so nimmt man die Tangente in dem Punkt an die Kurve. Dann ermittelt man einen weiteren Schnittpunkt dieser Geraden mit der Kurve. Da jede Gerade mit der Kurve genau drei Schnittpunkte hat, in ihrer Vielfachheit gezählt, existiert dieser Punkt eindeutig. Zuletzt spiegelt man diesen Punkt auf den anderen Ast der Kurve. Der so erhaltene Punkt entspricht der Addition von P_1 und P_2.

Bemerkung 1.6. Eine singuläre Kurve bildet keine Gruppe. In dem singulären Punkt P ist die Tangente nicht eindeutig bestimmt und folglich ist die Verknüpfung $P + P$ nicht definiert.

Da die Berechnung von kP sehr langsam wird für große $k \in \mathbb{Z}$, verwendet man das Verfahren „double and add“. Dabei berechnet man zunächst die Binärdarstellung von k und addiert anschließend die entsprechenden Vielfachen von P, s. Algorithmus 2. Dadurch müssen statt k lediglich $2 \ln k$ Gruppenoperationen durchgeführt werden, vgl. [JS92].

Die elliptische Kurve kann auch in der projektiven Ebene betrachtet werden:

Definition 1.7. Eine *projektive Ebene* $\mathbb{P}^2(\overline{\mathbb{K}})$ über einem Körper $\mathbb{K}$ mit algebraischem Abschluss $\overline{\mathbb{K}}$ ist die Menge

$$\{[x,y,z] \in \overline{\mathbb{K}}^3 \,|\, x,y,z \text{ nicht alle } 0\}/_\sim$$

mit der Äquivalenzrelation $(x,y,z) \sim (u,v,w) \Leftrightarrow \exists \lambda \in \overline{\mathbb{K}}^*$ mit $x = \lambda u,\ y = \lambda v,\ z = \lambda w$.

Um aus den affinen die projektiven Koordinaten zu erhalten dient die Abbildung

$$\begin{aligned} \mathbb{K}^2 &\to \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) &\mapsto [x,y,1]. \end{aligned}$$

Für die andere Richtung lautet eine Abbildung

$$\begin{aligned} \mathbb{P}^2(\overline{\mathbb{K}}) &\to \mathbb{K}^2 \\ [x,y,z] &\mapsto \left(\frac{x}{z}, \frac{y}{z}\right). \end{aligned}$$

Wird die Kurve in projektiven Koordinaten betrachtet, kommt also noch eine weitere Koordinate Z hinzu. Die Gleichung der Kurve muss dann homogen sein. Sie lautet:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Der Punkt im Unendlichen erhält dann die Koordinaten $\mathcal{O}_E = [0,1,0]$.

Weiterhin kann man eine elliptische Kurve über $\mathbb{C}$ auch mit einem Gitter identifizieren.

Definition 1.8. Ein *Gitter* ist eine Menge

$$\omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \{n_1\omega_1 + n_2\omega_2 \,|\, n_1, n_2 \in \mathbb{Z}\}.$$

Dabei werden $\omega_1, \omega_2 \in \mathbb{C}$, $\mathbb{R}$-linear unabhängig, als die *Perioden* des Gitters bezeichnet.
Die Menge

$$\{t_1\omega_1 + t_2\omega_2 \,|\, t_1, t_2 \in [0,1]\}$$

heißt *Fundamentalmasche* des Gitters.

Satz 1.9. *Sei $E : y^2 = 4x^3 - Ax - B$ eine elliptische Kurve über $\mathbb{C}$. Dann existiert ein Gitter L, so dass gilt:*

$$\mathbb{C}/L \cong E$$

mit

$$g_2(L) = 60 \sum_{\omega \in L, \omega \neq 0} \omega^{-4} = A$$

$$g_3(L) = 140 \sum_{\omega \in L, \omega \neq 0} \omega^{-6} = B$$

Folglich lassen sich jeder elliptischen Kurve über $\mathbb{C}$ die Perioden des zu der Kurve isomorphen Torus zuordnen. Zur genauen Berechnung der Perioden einer elliptischen Kurve kann man den Algorithmus von Carlson verwenden, siehe Abschnitt 1.5.1.

Folglich kann zwischen jeder elliptischen Kurve und dem dazu isomorphen Gitter eine Abbildung definiert werden, die jedem Punkt der Kurve einen Punkt der Fundamentalmasche zuordnet. Diese Abbildung heißt elliptischer Logarithmus und ist über ein elliptisches Integral definiert.

Definition 1.10. Sei $P = (x, y)$ ein Punkt auf einer elliptischen Kurve in kurzer Weierstraß-Form. Der *elliptische Logarithmus* ist dann definiert als

$$\Psi_\infty(P) := \sigma \int_{\mathcal{O}_E}^{P} \frac{dx}{\sqrt{x^3 + Ax + B}}.$$

Dabei ist $\sigma = \pm 1$ so gewählt, dass $\wp(\Psi_\infty(P)) = x$, $\wp'(\Psi_\infty(P)) = y$ gilt, wobei $\wp$ die Weierstraß-Funktion bezeichnet. Der Integrationsweg verläuft dabei beliebig von $\mathcal{O}_E$ nach P in der Riemannschen Ebene.

1.2 Besondere Eigenschaften elliptischer Kurven

Satz 1.11 (Mordell-Weil)**.** *Sei $\mathbb{K}$ ein Zahlkörper. Die Gruppe $E(\mathbb{K})$ ist abelsch und endlich erzeugt. Es gibt eine Darstellung*

$$E(\mathbb{K}) = \langle B_1 \rangle \times \cdots \langle B_r \rangle \times E(\mathbb{K})_{\text{tors}}.$$

Dabei sind $B_1, \ldots, B_r$ Punkte der Kurve und $E(\mathbb{K})_{\text{tors}}$ bezeichnet die Torsionsgruppe, also die Untergruppe aller Punkte der Kurve E mit endlicher Ordnung.

Beweis: [Sil86] □

$B_1, \ldots, B_r$ wird dabei als Mordell-Weil-Basis bezeichnet. r ist der Rang der Kurve. Die Torsionsgruppe ist im allgemeinen problemlos zu bestimmen, die Mordell-Weil-Gruppe und der Rang dagegen nicht. Es gibt einige Verfahren, die auf bestimmte Fälle angewendet werden können, aber ein allgemein

gültiges Verfahren gibt es nicht. In dem Computeralgebraprogramm Magma kann man, falls möglich, mit dem Befehl `PseudoMordellWeilGroup()` eine Untergruppe der Mordell-Weil-Gruppe berechnen und über einen booleschen Parameter bestimmen, ob diese Untergruppe gleich viele Erzeuger hat wie die Gruppe selbst.

Sind die Erzeuger, $\{B_1, \cdots, B_r\}$, der Mordell-Weil-Gruppe bekannt, so lässt sich jeder Punkt P auf der Kurve durch

$$P = n_1 B_1 + \cdots + n_r B_r + T, \qquad n_1, \ldots, n_r \in \mathbb{Z}, \quad T \in E(\mathbb{K})_{tors}$$

darstellen. Um eine torsionsfreie Darstellung zu erreichen, kann man diese Gleichung mit der Ordnung g der Torsionsgruppe multiplizieren:

$$\begin{aligned} gP &= gn_1 B_1 + \cdots + gn_r B_r + gT = gn_1 B_1 + \cdots + gn_r B_r + \mathcal{O}_E = \\ &= gn_1 B_1 + \cdots + gn_r B_r. \end{aligned}$$

Über einem endlichen Körper $\mathbb{F}_p$ wird die elliptische Kurve zu einer endlichen Gruppe. Um die Grösse der Gruppe abzuschätzen, dient der Satz von Hasse.

Satz 1.12 (Hasse)**.** *Sei $E(\mathbb{F}_p)$ eine elliptische Kurve und p prim. Dann gilt:* $|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$.

Beweis: [Coh93] □

In Kapitel 4 wird genauer auf die Eigenschaften von elliptischen Kurven über endlichen Körpern eingegangen.

1.3 p-adische Zahlen und Bewertungen

1.3.1 Bewertungen

Definition 1.13. Eine *Bewertung* eines Körpers $\mathbb{K}$ ist eine Funktion

$$|\cdot| : \mathbb{K} \to \mathbb{R}$$

mit den Eigenschaften, dass für alle x, y aus $\mathbb{K}$ gilt:

- $|x| \geq 0$ und $|x| = 0 \Leftrightarrow x = 0$,
- $|xy| = |x||y|$,
- $|x + y| \leq |x| + |y|$ „Dreiecksungleichung“.

Definition 1.14. Mit Hilfe der Bewertung kann der Abstand zwischen zwei Elementen aus $\mathbb{K}$ definiert werden als

$$d(x, y) = |x - y|.$$

Damit wird eine Topologie auf $\mathbb{K}$ induziert.
Zwei Bewertungen von $\mathbb{K}$ heißen *äquivalent*, wenn sie die gleiche Topologie auf $\mathbb{K}$ definieren.

Bewertungen werden nun in zwei große Gruppen eingeteilt:

Definition 1.15. Die Bewertung $|\cdot|$ heißt *nicht-archimedisch*, wenn $|n|$ beschränkt ist, für alle $n \in \mathbb{N}$. Sonst heißt sie *archimedisch*.

Der gewöhnliche Absolutbetrag gehört folglich zu den archimedischen Bewertungen, da für $n \to \infty$ auch $|n| \to \infty$.

Ein wichtiger Unterschied zwischen archimedischen und nicht-archimedischen Bewertungen ist die folgende Eigenschaft, die oft auch zur Definition der nicht-archimedischen Bewertung verwendet wird:

Satz 1.16. *Die Bewertung $|\cdot|$ ist genau dann nicht-archimedisch, wenn sie die verschärfte Dreiecksungleichung erfüllt:*

$$|x + y| \leq \max\{|x|, |y|\} \qquad x, y \in \mathbb{K}.$$

Beweis: [Neu92] □

Die verschärfte Dreiecksungleichung impliziert stets die normale Dreiecksungleichung, wegen $\max\{|x|, |y|\} \leq |x| + |y|$.
Des weiteren folgt aus ihr sofort

$$|x| \neq |y| \Rightarrow |x + y| = \max\{|x|, |y|\} \quad \forall x, y \in \mathbb{K}.$$

1.3.2 p-adische Bewertungen

Zu jeder Primzahl p und Zahl x aus $\mathbb{Q}\backslash\{0\}$ gibt es eine eindeutige Darstellung

$$x = \frac{a}{b} p^n \qquad \text{mit } \ a, n \in \mathbb{Z},\ b \in \mathbb{N}, \ \text{ und } a, b, p \text{ teilerfremd.}$$

Damit lassen sich die p-adische Exponentialbewertung und der p-adische Betrag definieren als

Definition 1.17.

- $v_p(x) = n \quad$ mit $v_p(0) = \infty$ heißt *p-adische Exponentialbewertung* von x.

- $|x|_p = p^{-n}$ mit $|0|_p = 0$ heißt *p-adischer Betrag* von x.

Der p-adische Betrag ist offensichtlich eine nicht-archimedische Bewertung, da er auf $\mathbb{N}$ durch 1 beschränkt ist.

Der normale Absolutbetrag wird daher oft mit $|\cdot|_\infty$ bezeichnet.

Satz 1.18. *Jede Bewertung von $\mathbb{Q}$ ist äquivalent zu einer der Bewertungen $|\cdot|_p$ oder $|\cdot|_\infty$.*

Beweis: [Neu92] □

Satz 1.19. *Die p-adische Exponentialbewertung hat folgende Eigenschaften:*

- $v_p(x) = \infty \Leftrightarrow x = 0$
- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

mit den Konventionen $a + \infty = \infty$ und $\infty + \infty = \infty$ für $a \in \mathbb{R}$.

Beweis: folgt unmittelbar aus der Definition der Exponentialbewertung [Neu92] □

Die Definitionen sind auf Zahlkörper übertragbar:

Definition 1.20. Sei $x \in \mathbb{K}^*$. Hat das Hauptideal (x) die eindeutige Primidealzerlegung

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}.$$

so heißt die Abbildung

$$\begin{aligned} v_\mathfrak{p} : \mathbb{K}^* &\rightarrow \mathbb{Z} \\ v_\mathfrak{p}(x) &= \nu_\mathfrak{p} \end{aligned}$$

Exponentialbewertung.

Ausgehend davon kann man nun zu jeder endlichen Stelle mit Hilfe der Normfunktion des Körpers $\mathbb{K}$ eine Bewertung definieren.

Definition 1.21. Sei ν die zu dem Primideal $\mathfrak{p}$ korrespondierende Stelle und $N_{\mathbb{K}/\mathbb{Q}}$ die zu $\mathbb{K}$ gehörende Normfunktion, dann ist für alle $x \in \mathbb{K}^*$

$$|x|_\nu := N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

1.3.3 p-adische Zahlen

Analog zur Konstruktion reeller Zahlen als Äquivalenzklassen von Cauchy-Folgen bezüglich des gewöhnlichen Absolutbetrags, kann man auch die p-adischen Zahlen als Äquivalenzklassen von Cauchy-Folgen bezüglich des p-adischen Betrags definieren: Eine Folge $(a_i)_i$ heißt Cauchy-Folge, wenn für alle $\epsilon > 0$ ein N existiert, so dass $|a_i - a_j|_p < \epsilon$ für alle $i, j > N$. Zwei Cauchy-Folgen $(a_i)_i$ und $(b_i)_i$ heißen äquivalent, wenn $|a_i - b_i|_p \to 0$ für $i \to \infty$.

Definition 1.22. $\mathbb{Q}_p$ ist die Menge der Äquivalenzklassen bezüglich $|\cdot|_p$.

Satz 1.23. *Sei $x \in \mathbb{Q}_p$, $|x| \leq 1$. Dann existiert für jedes $i \in \mathbb{N}$ eine ganze Zahl a_i mit $p^i - 1 \geq a_i \geq 0$, so dass*

$$|a_i - x|_p \leq p^{-i}.$$

Beweis: [Kob77] □

Bemerkung 1.24. Ist $|x|_p > 1$, so kann man x schreiben als $x = (xp^m)p^{-m} = x'p^{-m}$ mit $|x'|_p < 1$, mit $m \in \mathbb{N}$ minimal. Nach [Kob77] ist diese Darstellung eindeutig.

Das bedeutet, dass jedes $x \in \mathbb{Q}_p$ mit einer Folge $(a_i)_i$, $0 \leq a_i \leq p-1$, identifiziert werden kann. Daraus ergibt sich für p-adische Zahlen die Darstellung

$$x = p^{-m}(a_0 + a_1 p + a_2 p^2 + \cdots) = \sum_{i=-m}^{\infty} a_{i+m} p^i$$

Ist $m = 0$, so handelt es sich um eine ganze p-adische Zahl, und ist außerdem noch $a_0 \neq 0$, so spricht man auch von einer p-adischen Einheit.

Die p-adische Bewertung von x lässt sich dann unmittelbar an dem niedrigsten auftretenden Exponenten mit Koeffizienten $\neq 0$ in dieser Darstellung ablesen.

Die Menge $\mathbb{Q}_p$ bildet einen Körper und dieser ist nach Konstruktion vollständig. Analog lässt sich auch die p-adische Vervollständigung eines Körpers $\mathbb{K}$ bzüglich einer Stelle $\mathfrak{p}$ als Menge der Äquivalenzklassen von Cauchyfolgen bezüglich $|\cdot|_{\mathfrak{p}}$ definieren.

1.4 Höhen auf elliptischen Kurven

Als Maß zum Vergleich von Punkten auf einer elliptischen Kurve gibt es verschiedene Höhenfunktionen.

Definition 1.25 (Nach [Her02])**.** Es habe $P \in E(\mathbb{K})$ die Darstellung $P = n_1B_1 + \cdots + n_rB_r + T$ bezüglich einer Mordell-Weil-Basis. Dann ist

$$h_n(P) := \max_{1\leq i\leq r}\{|n_i|\}.$$

Zum bestimmen S-ganzer Punkte ist es in einem ersten Schritt notwendig, den größten Koeffizienten in der Darstellung eines S-ganzen Punktes mittels der Mordell-Weil-Basis abzuschätzen. Die Höhe h_n eignet sich folgendermaßen zum Beschreiben des Problems: Es ist eine Konstante N gesucht, so dass

$$N \geq h_n(P).$$

Zur weiteren Berechnung ist es aber hilfreich, eine Höhe zu haben, die von der Wahl der Mordell-Weil-Basis unabhängig ist. Dazu definiert man zunächst die absolute Höhe für ein Körperelement:

Definition 1.26. Sei $\mathbb{K}$ eine Körpererweiterung über $\mathbb{Q}$ vom Grad d, n_ν der Index $[\mathbb{K}_\nu : \mathbb{Q}_\nu]$ der ν-adischen Vervollständigung $\mathbb{K}_\nu$ von $\mathbb{K}$ in $\mathbb{Q}_\nu$ und $M_\mathbb{K}$ die Menge aller endlichen und unendlichen Stellen von $\mathbb{K}$. Für $\alpha \in \mathbb{K}$ heißt

$$H(\alpha) = \left(\prod_{\nu\in M_\mathbb{K}} \max\{1, |\alpha|_\nu\}^{n_\nu}\right)^{1/d}$$

die *absolute Höhe* von α.

In der Definition wird benötigt, dass man jeder Stelle des Zahlkörpers $\mathbb{K}$ eine Bewertung zuordnen kann. Für endliche Stellen werden einfach die Bewertungen aus Definition 1.21 verwendet. Für die unendlichen Stellen bettet man zunächst das Element, dessen Bewertung bestimmt werden soll, in die komplexen Zahlen ein und wendet dann den gewöhnlichen Absolutbetrag an:

Sei $\sigma : \mathbb{K} \to \mathbb{C}$ die zu der unendlichen Stelle ν korrespondierende Einbettung, dann gilt für alle $x \in \mathbb{K}$:

$$|x|_\nu = |\sigma(x)|.$$

Um die Höhe auch für einen Punkt $P = (x, y)$ auf einer Kurve $E(\mathbb{K})$ zu definieren, setzt man einfach

$$H(P) := H(x).$$

Für den Umgang mit der absoluten Höhe werden folgende Regeln benötigt:

Satz 1.27. *Seien* $\alpha, \beta, \alpha_1, \ldots, \alpha_n \in \mathbb{K}$

- $H(\alpha) = H(-\alpha)$
- $H(\alpha) = H(1/\alpha)$
- $H(\alpha_1 \cdots \alpha_n) \leq H(\alpha_1) \cdots H(\alpha_n)$
- $H(\alpha + \beta) \leq H(\alpha) + H(\beta)$

Beweis: [Lan78], [Sma98] □

Ausgehend von der absoluten Höhe kann man nun die logarithmische Höhe definieren:

Definition 1.28. Die Bezeichnungen seien die gleichen wie für die absolute Höhe. Dann heißt

$$h(\alpha) = \log H(\alpha)$$

bzw. für den Punkt auf einer elliptischen Kurve

$$h(P) = \log H(x)$$

logarithmische Höhe von α bzw. P.

Mit dieser Definition gilt für die logarithmische Höhe:

$$h(\alpha) = \log \left(\prod_{\nu \in M_{\mathbb{K}}} \max\{1, |\alpha|_\nu\}^{n_\nu} \right)^{1/d} = \frac{1}{d} \sum_{\nu \in M_{\mathbb{K}}} n_\nu \log \max\{1, |\alpha|_\nu\}.$$

Aufbauend auf der logarithmischen Höhe lässt sich nun noch die Néron-Tate-Höhe definieren. Herrmann gibt diese in [Her02] folgendermaßen an:

Definition 1.29. Sei P ein Punkt der Kurve $E(\mathbb{K})$.

$$\hat{h}(P) := \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$$

heißt *Néron-Tate-Höhe.*

Die Néron-Tate-Höhe hat folgende Eigenschaften:

Satz 1.30. *Sei* $E(\mathbb{K})$ *eine elliptische Kurve in langer Weierstraß-Form. Seien* $P, P_1, P_2 \in E(\mathbb{K})$ *drei beliebige Punkte auf* $E(\mathbb{K})$ *und* $n \in \mathbb{Z}$. *Dann gilt:*

1. *Die Néron-Tate-Höhe ist eine positiv semidefinite quadratische Form auf* $E(\mathbb{K})$ *mit Kern* $E_{\text{tors}}(\mathbb{K})$. *D.h.*

(i) $\hat{h}(P) \geq 0$ *und* $\hat{h}(P) = 0 \Leftrightarrow P \in E_{\text{tors}}(\mathbb{K})$,
(ii) $\hat{h}(P) = \hat{h}(-P)$,
(iii) $\hat{h}(P_1 + P_2) = 2\hat{h}(P_1) + 2\hat{h}(P_2) - \hat{h}(P_1 - P_2)$,
(iv) $\hat{h}(nP) = n^2\hat{h}(P)$.

Es wird eine symmetrische Bilinearform induziert:

$$\langle P_1, P_2 \rangle = \frac{1}{2}(\hat{h}(P_1 + P_2) - \hat{h}(P_1) - \hat{h}(P_2)).$$

2. *Der Abstand zwischen der Néron-Tate-Höhe und der logarithmischen Höhe ist beschränkt, d.h. es existieren zwei positive reelle Zahlen* u_1 *und* u_2*, so dass*

$$-u_1 \leq \hat{h}(P) - h(P) \leq u_2 \text{ für alle } P \in E(\mathbb{K}).$$

Dabei hängen die Werte von u_1 *und* u_2 *nur von der elliptischen Kurve, nicht aber von dem Punkt* P *ab.*

Beweis: [Sil86] □

Für die Konstanten u_2 und u_1 gibt es verschiedene Abschätzungen. Ich verwende im Laufe der Arbeit folgende:

Satz 1.31. *Sei* $\mathbb{K}$ *ein Körper,* $M_{\mathbb{K}}$ *die Menge aller Stellen über* $\mathbb{K}$*,* $E(\mathbb{K})$ *eine elliptische Kurve in Weierstraß-Form über* $\mathbb{K}$ *und* $v_{\mathfrak{p}}$ *die zur Stelle* $\mathfrak{p} \in M_{\mathbb{K}}$ *gehörende Exponentialbewertung. Weiter sei*

$$\mu_{\mathfrak{p}} := \min\left\{v_{\mathfrak{p}}(b_2), \frac{v_{\mathfrak{p}}(b_4)}{2}, \frac{v_{\mathfrak{p}}(b_6)}{3}, \frac{v_{\mathfrak{p}}(b_8)}{4}\right\},$$

mit b_i *die* b_i*-Invarianten aus Definition 1.4, und*

$$\mu_l := -\frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\mathfrak{p} \in M_{\mathbb{K}}} n_{\mathfrak{p}} \min\{0, \mu_{\mathfrak{p}}\},$$

$$\mu_h := \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{\mathfrak{p} \in M_{\mathbb{K}}} n_{\mathfrak{p}} \max\{0, \mu_{\mathfrak{p}}\}.$$

Dann gilt für alle $P \in E(\overline{\mathbb{K}})$*:*

$$u_2 \leq \mu_l + \log 2$$

und

$$u_1 \geq -2\mu_l + \mu_h - \frac{8}{3}\log 2$$

Beweis: [SZ03], [Uch06] □

Diese Abschätzung in [SZ03] ist besser als die in [Sil86], die Herrmann in [Her02] angibt. Uchida gibt in [Uch06] eine Schranke an, die noch besser als die beiden anderen ist. Da diese aber deutlich aufwändiger zu berechnen ist, verzichte ich darauf, sie zu verwenden.

Weiterhin werden im Laufe der Arbeit die Regulatormatrix und der Regulator $\mathcal{R}_E$ einer Kurve verwendet.

Definition 1.32. Seien $\langle \cdot, \cdot \rangle$ die über die Néron-Tate-Höhe definierte Bilinearform und $\{B_1, \ldots, B_r\}$ eine Basis modulo Torsion von $E(\mathbb{K})$. Dann heißt

$$R_E = \begin{pmatrix} \langle B_1, B_1 \rangle & \ldots & \langle B_1, B_r \rangle \\ \vdots & & \vdots \\ \langle B_r, B_1 \rangle & \ldots & \langle B_r, B_r \rangle \end{pmatrix}$$

Regulatormatrix. Der *Regulator* $\mathcal{R}_E$ ist durch $\mathcal{R}_E = \det(R_E)$ definiert. Falls $r = 0$, setzt man $\mathcal{R}_E = 1$.

Sei $\lambda_{\min}$ der kleinste Eigenwert der Regulatormatrix, so stehen die Höhen nach [GPZ94] miteinander in Zusammenhang durch die Ungleichung

$$\hat{h}(P) \geq \lambda_{\min}(h_n(P))^2$$

Mit dieser Ungleichung und Satz 1.30 folgt nun [Her02]:

$$\lambda_{\min}(h_n(P))^2 - h(P) \leq \hat{h}(P) - h(P) \leq u_2.$$

Ist es also möglich, eine obere Schranke für $h(P)$ anzugeben, so erhält man direkt auch eine gewünschte Schranke N für die Koeffizienten in der Darstellung mittels der Mordell-Weil-Basis: Sei $N' \geq h(P)$. Aus

$$\lambda_{\min}(h_n(P))^2 - h(P) \leq u_2 \Leftrightarrow h_n(P) \leq \sqrt{\frac{u_2 + h(P)}{\lambda_{\min}}}$$

folgt

$$N := \sqrt{\frac{u_2 + N'}{\lambda_{\min}}} \geq h_n(P).$$

Deshalb geht es zunächst darum eine Schranke für $h(P)$ zu bestimmen, falls P S-ganz ist.

Sei $M_{\mathbb{K}}$ die Menge aller endlichen und unendlichen Stellen über $\mathbb{K}$ und $S \subset M_{\mathbb{K}}$ eine endliche fest gewählte Teilmenge, die alle unendlichen Stellen enthält.

Definition 1.33. $\alpha \in \mathbb{K}$ heißt *S-ganz*, wenn

$$v_{\mathfrak{p}}(\alpha) \geq 0 \text{ für alle } \mathfrak{p} \notin S.$$

Der Ring der S-ganzen Zahlen des Zahlkörpers $\mathbb{K}$ wird dann mit $\mathbb{Z}_{\mathbb{K},S}$ bezeichnet.
Ein Punkt auf einer elliptischen Kurve heißt somit *S-ganz*, wenn seine Koordinaten S-ganz sind.

Bemerkung 1.34. Ist $\alpha \in \mathbb{K}$ S-ganz, so gilt:

$$\prod_{\nu \in M_{\mathbb{K}}, \nu \notin S} \max\{1, |\alpha|_\nu\}^{n_\nu} \leq 1,$$

wobei $n_\nu = [\mathbb{K}_\nu : \mathbb{Q}_\nu]$.

Über $\mathbb{Q}$ ist S eine endliche Menge von Primzahlen. Eine Zahl $\in \mathbb{Q}$ ist genau dann S-ganz, wenn in der Faktorisierung ihres Nenners nur Primzahlen aus S auftreten.

Satz 1.35 (Siegel-Mahler)**.** *Sei E eine elliptische Kurve in Weierstraß-Form, welche über einem algebraischen Zahlkörper $\mathbb{K}$ definiert ist. Fixiert man eine endliche Menge von Stellen aus $\mathbb{K}$, welche alle unendlichen Stellen enthält, so existieren in der Gruppe $E(\mathbb{K})$ nur endlich viele S-ganze Punkte P.*

Beweis: [Sil86] □

Dieser Satz selbst gibt zwar noch keine Schranke für $h_n(P)$ mit S-ganzem P an, aber er zeigt, dass es eine solche Schranke gibt. Mit dem Bestimmen expliziter Schranken beschäftigt sich Herrmann in seiner Doktorarbeit [Her02] und wird in dieser Arbeit in Kapitel 2 nochmals aufgegriffen.

1.5 Algorithmen zum Berechnen wichtiger Größen

1.5.1 Perioden und elliptische Logarithmen

Im Laufe dieser Arbeit werden Linearformen in elliptischen Logarithmen und den Perioden der elliptischen Kurve aufgestellt, um darauf die LLL-Reduktion, siehe Kapitel 3, anwenden zu können. Sowohl über $\mathbb{Q}$ als auch über Zahlkörpern gibt es in Magma eine Funktion, um die elliptischen Logarithmen zu berechnen. Zur Berechnung der Perioden gibt es aber nur eine Funktion über $\mathbb{Q}$. Über Zahlkörpern müssen diese mit Hilfe des Algorithmus von Carlson [Car95] berechnet werden. Carlson gibt darin an, wie elliptische Integrale numerisch bestimmt werden können.

Definition 1.36. Das *elliptische Integral erster Gattung* ist

$$R_F(x,y,z) = \frac{1}{2}\int_0^\infty \frac{dt}{\sqrt{(t+x)(t+y)(t+z)}},$$

wobei maximal einer der Werte x, y, z null sein darf und außerdem gilt:

$$-\pi < arg(x) < \pi, \quad -\pi < arg(y) < \pi, \quad -\pi < arg(z) < \pi.$$

Dieses Integral kann nun mit folgender Iteration und den Startwerten $x_0 = x$, $y_0 = y$ und $z_0 = z$ approximiert werden:

$$x_{n+1} = \frac{1}{4}(x_n + \lambda_n), \quad y_{n+1} = \frac{1}{4}(y_n + \lambda_n), \quad z_{n+1} = \frac{1}{4}(z_n + \lambda_n)$$

mit $\lambda_n = \sqrt{x_n}\sqrt{y_n} + \sqrt{x_n}\sqrt{z_n} + \sqrt{y_n}\sqrt{z_n}$.
Dann lautet mit

$$A_0 = \frac{x_0 + y_0 + z_0}{3}$$

$$A_{n+1} = \frac{A_n + \lambda_n}{4},$$

und

$$X = \frac{A_0 - x}{4^n A_n}, \quad Y = \frac{A_0 - y}{4^n A_n}, \quad Z = -X - Y,$$

$$E_2 = XY - Z^2, \quad E_3 = XYZ$$

die Approximation des Integrals

$$R_F(x_n, y_n, z_n) = A_n^{-\frac{1}{2}}\left(1 - \frac{1}{10}E_2 + \frac{1}{14}E_3 + \frac{1}{24}E_2^2 - \frac{3}{44}E_2E_3\right).$$

Der Fehlerterm r_n lässt sich abschätzen durch

$$|r_n| < \frac{1}{3}\left(\frac{\max\{|A_0 - x|, |A_0 - y|, |A_0 - z|\}}{4^n|A_n|}\right)^6.$$

Bei diesem Verfahren nimmt der Fehler etwa mit Faktor 4^6 in jedem Schritt ab. Dadurch können sehr schnell auch sehr hohe Genauigkeiten von einigen tausend Stellen erreicht werden. Der genaue Algorithmus findet sich im Anhang , s. Algorithmus 3

Um das elliptische Integral über einer Kurve in Legendre-Form $F(\Phi, k)$ zu berechnen, gibt Carlson [Car95] folgenden Zusammenhang an, so dass der gleiche Algorithmus verwendet werden kann:

$$F(\Phi, k) = (\sin\Phi)R_F(\cos^2\Phi, 1 - k^2\sin^2\Phi, 1).$$

Die Perioden einer elliptischen Kurve in Legendre-Form sind nach [Hus87] gegeben durch

$$\omega_{1,L}(\kappa) = 2iF(\frac{\pi}{2}, \sqrt{1-\kappa}), \qquad \omega_{2,L}(\kappa) = 2F(\frac{\pi}{2}, \sqrt{2\kappa}).$$

Um die Perioden auch über einer Kurve in Weierstraß-Form zu berechnen, gilt:

Satz 1.37.

$$\begin{aligned} \omega_1 &= \frac{1}{2}\frac{\omega_{1,L}(\kappa)}{\sqrt{e_2-e_1}} = i\frac{F(\frac{\pi}{2}, \sqrt{1-\kappa})}{\sqrt{e_2-e_1}}, \\ \omega_2 &= \frac{1}{2}\frac{\omega_{2,L}(\kappa)}{\sqrt{e_2-e_1}} = \frac{F(\frac{\pi}{2}, \sqrt{2\kappa})}{\sqrt{e_2-e_1}}. \end{aligned}$$

Beweis: Mit Satz 1.3 gilt

$$\frac{dx}{y} = \frac{d((e_2-e_1)\eta + e_1)}{2(e_2-e_1)^{3/2}\xi} = \frac{(e_2-e_1)d\eta}{2(e_2-e_1)^{3/2}\xi} = \frac{d\eta}{2(e_2-e_1)^{1/2}\xi}$$

Damit gilt

$$\int \frac{dx}{y} = \int \frac{1}{2}(e_2-e_1)^{-1/2}\frac{d\eta}{\xi} = \frac{1}{2}\frac{\int \frac{d\eta}{\xi}}{\sqrt{e_2-e_1}}.$$

Durch Einsetzen der entsprechenden Integralgrenzen folgt die Behauptung. □

Mit Hilfe des elliptischen Integrals kann auch der elliptische Logarithmus berechnet werden. Der elliptische Logarithmus ist definiert als das elliptische Integral von $\mathcal{O}_E$ nach P. Im Algorithmus von Carlson wird aber das elliptische Integral von 0 bis ∞ berechnet.

Herrmann gibt in [Her02] eine Beziehung des elliptischen Logarithmus zu $F(\Phi, k)$ an:

Satz 1.38. *Sei $P = (x, y)$ ein Punkt auf einer elliptischen Kurve in Weierstraß-Form und Λ das dazu isomorphe Gitter. Der elliptische Logarithmus von P ist dann gegeben durch:*

$$\Psi_\infty(P) = \begin{cases} \frac{F(\Phi,\sqrt{\kappa})}{\sqrt{e_2-e_1}} \ (\mathrm{mod}\Lambda) & & x \neq e_1, e_2 \\ \frac{\omega_1}{2} & \textit{falls} & x = e_1 \\ \frac{\omega_2}{2} & & x = e_2 \end{cases}$$

wobei $\Phi = \arcsin\sqrt{\frac{e_2-e_1}{x-e_1}}$ *und* $\kappa = \frac{e_3-e_1}{e_2-e_1}$ *mit* $|\kappa| < 1$.

1.5.2 p-adische elliptische Logarithmen

Neben dem Fall der Linearformen in elliptischen Logarithmen werden zur Suche von S-ganzen Punkten auch Linearformen in p-adisch elliptischen Logarithmen verwendet. Um den p-adischen elliptischen Logarithmus zu erklären, muss man zunächst den Begriff minimales Modell einer Kurve definieren [SZ03]:

Definition 1.39. Die Gleichung einer Kurve in Weierstraß-Form über dem Körper $\mathbb{K}$ heißt *minimales Modell* der Kurve bezüglich einer Stelle $\mathfrak{p}$ aus $\mathbb{K}$, wenn ihre Koeffizienten a_i $\mathfrak{p}$-ganz sind, das heißt, $v_\mathfrak{p}(a_i) \geq 0$ für alle i, und außerdem gilt:

$$v_\mathfrak{p}(\Delta) \geq 0 \quad \text{und} \quad v_\mathfrak{p}(\Delta) \text{ minimal}$$

Ist die Gleichung der Kurve minimal für alle Stellen aus $\mathbb{K}$, dann heißt sie *global minimales Modell.*

Satz 1.40. *Für jede elliptische Kurve über einem Körper $\mathbb{K}$ gibt es zu jeder Stelle aus $\mathbb{K}$ ein minimales Modell.*

Beweis: [SZ03] □

Bemerkung 1.41. Über $\mathbb{Q}$ existiert auch stets ein global minimales Modell einer Kurve, über einem Zahllörper nicht notwendiger Weise.

Ein solches Modell lässt sich über den Algorithmus von Tate [Tat75] bestimmen. Dies ist notwendig, da der p-adisch elliptische Logarithmus nur über minimalen Modellen berechnet werden kann. Eine genaue Ausarbeitung des Algorithmus findet sich bei [Cre97].

Die x- und y- Koordinate eines Punktes können als Reihen entwickelt werden. Es lässt sich ebenfalls eine Reihenentwicklung des invarianten Differentials, siehe 1.4, angeben, mit deren Hilfe der p-adische elliptische Logarithmus definiert wird [Sil86]: Dazu wird zunächst eine Substitution vorgenommen:

$$z := -\frac{x}{y} \quad \text{und} \quad w := -\frac{1}{y}.$$

Setzt man diese nun in die lange Weierstraß-Form ein, so ergibt sich:

$$\begin{aligned} w &= z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = \\ &= z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 =: f(z, w(z)). \end{aligned}$$

Setzt man diese Gleichung rekursiv in sich selbst ein, so erhält man eine

Potenzreihe in z:

$$\begin{aligned} w &= z^3 + (a_1z + a_2z^2)[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3] + \\ &\quad +(a_3 + a_4z)[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3]^2 = \\ &\quad +a_6[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3]^3 = \\ &= \cdots = \\ &= z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6) + \\ &\quad +(a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)z^7 + \cdots = \\ &= z^3(1 + A_1z + A_2z^2 + \cdots), \end{aligned}$$

mit $A_n \in \mathbb{Z}[a_1, \ldots, a_6]$ nur von den Koeffizienten von E abhängig. [Sil86] zeigt, dass durch diesen Vorgang eine Potenzreihe eindeutig bestimmt wird. Mit Hilfe dieser Potenzreihe können nun auch x, y und das invariante Differential W als Potenzreihen ausgedrückt werden:

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^3 + \ldots$$

$$y(z) = \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z^+ \ldots$$

und

$$\begin{aligned} W(z) &= (1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + 2a_3)z^3 + \\ &\quad +(a_1^4 + 3a_1a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \ldots)dz = \\ &= 1 + A_1z + A_2z^2 + \ldots \end{aligned}$$

Die Addition zweier Punkte auf einer elliptischen Kurve lässt sich auch auf die Potenzreihen übertragen. Die zu diesem Gruppengesetz gehörige Gruppe heißt *formale Gruppe* $\hat{E}(\mathcal{M})$ mit $\mathcal{M} := \{\alpha \in \mathbb{K} \mid v_\mathfrak{p}(\alpha) > 0\}$.

Definition 1.42.

$$E_m(\mathbb{K}_\mathfrak{p}) := \{P = (x, y) \in E(\mathbb{K}_\mathfrak{p}) \mid v_\mathfrak{p}(x) \leq -2m\}$$

Dabei sei $\mathbb{K}_\mathfrak{p}$ die $\mathfrak{p}$-adische Vervollständigung von $\mathbb{K}$.

Bemerkung 1.43. Satz 4.6 beinhaltet, dass aus $v_\mathfrak{p}(x) \leq -2m$ folgt, dass $v_\mathfrak{p}(y) \leq -3m$. Es folgt sogar: Ist $v_\mathfrak{p}(x) \leq 0$, so ist sein Wert immer gerade: $v_\mathfrak{p}(x) = -2m$, und $v_\mathfrak{p}(y) = -3m$.

Der p-adische elliptische Logarithmus kann nun wie folgt definiert werden:

Definition 1.44. Sei E eine minimale Kurve über $\mathbb{K}$, $e_{\mathfrak{p}|p}$ der Verzweigungsindex von $\mathfrak{p}|p$, $P = (x, y) \in E_{e_{\mathfrak{p}|p}}(\mathbb{K}_{\mathfrak{p}})$ und $\hat{\mathbb{G}}_a$ die additive Gruppe über dem algebraischen Abschluss der Vervollständigung von $\mathbb{Q}$. Setze $z_P := -\frac{x}{y}$, dann heißt

$$\begin{aligned} \Psi_{\mathfrak{p}} : E_{e_{\mathfrak{p}|p}}(\mathbb{K}_{\mathfrak{p}}) &\rightarrow \hat{\mathbb{G}}_a \\ P &\mapsto \int_0^{z_P} W(T)dT = z_P + \frac{A_1}{2} z_P^2 + \frac{A_2}{3} z_P^3 + \cdots \end{aligned}$$

$\mathfrak{p}$-*adisch elliptischer Logarithmus.* Im Fall $\mathbb{K} = \mathbb{Q}$ ersetzt man $E_{e_{\mathfrak{p}|p}}(\mathbb{K}_{\mathfrak{p}})$ durch $E_1(\mathbb{Q}_{\mathfrak{p}})$.

Die Einschränkung des Definitionsbereichs auf $E_{e_{\mathfrak{p}|p}}(\mathbb{K}_{\mathfrak{p}})$ ist notwendig, um die Konvergenz der Potenzreihe zu gewährleisten. Bei der Berechnung der elliptischen Logarithmen muss also immer ein Punkt auf $E_{e_{\mathfrak{p}|p}}$ bestimmt werden. Dazu wird ein Vielfaches des Punktes berechnet, so dass $p^{e_{\mathfrak{p}|p}} m_{\mathfrak{p}} P$ nach der Lutzfiltrierung [Lut37] ein Element von $E_{e_{\mathfrak{p}|p}}$ ist. Dabei berechnet sich der Faktor $m_{\mathfrak{p}}$ durch

$$m_{\mathfrak{p}} = kgV(c_{\mathfrak{p}} \mathcal{N}_{\mathfrak{p}}, g)$$

Dabei bezeichnet g die Ordnung der Torsionsgruppe und wird mit einbezogen, damit $m_{\mathfrak{p}} P$ torsionsfrei ist, vgl. 1.2. $N_{\mathfrak{p}}$ bezeichnet die Anzahl der Punkte der elliptischen Kurve modulo $\mathfrak{p}$, und $c_{\mathfrak{p}}$ steht für den Index $[E(\mathbb{K}_{\mathfrak{p}}) : E_0(\mathbb{K}_{\mathfrak{p}})]$ und entspricht damit der Tamagawazahl. Diese lässt sich mit Hilfe des Algorithmus von Tate berechnen [Tat75].

Um eine Approximation des p-adischen elliptischen Logarithmus $\widehat{\Psi_{\mathfrak{p}}(P)}$ nun konkret zu einer gegebenen Genauigkeit t_0 zu berechnen, also

$$v_{\mathfrak{p}} \left(\Psi_{\mathfrak{p}}(P) - \widehat{\Psi_{\mathfrak{p}}(P)} \right) \geq t_0,$$

geht man folgendermaßen vor [PHZH99]:

1. Berechnung eines minimalen Modells von E bezüglich der Stelle $\mathfrak{p}$.
2. Berechnung des Polynoms $\tilde{\Psi}_{\mathfrak{p}}(T) = \sum_{i=1}^{t_1} \frac{A_i}{i} T^i$ bis zu einem Grad $t_1 \leq t_0$.
3. Bestimmung des Vielfachen des Punktes P, das in $E_{e_{\mathfrak{p}|p}}(\mathbb{K}_{\mathfrak{p}})$ liegt: $P' = p^{e_{\mathfrak{p}|p}} m_{\mathfrak{p}} P$
4. Bestimmung des Vielfachen des Punktes P', so dass dieses in E_{V+1} liegt [Lut37]: $\hat{P} = p^V P'$ mit $V := \left[\frac{t_0}{t_1} \right]$.

Algorithmus 1 : Polynom zur Bestimmung des p-adisch elliptischen Logarithmus

Eingabe : elliptische Kurve E, Grad des Polynoms t_1
Ausgabe : Polynom $\tilde{\Psi}_{\mathfrak{p}}(T)$
$a :=$ Koeffizienten(E);
$w_0 := z$;
$w_1 := z$;
$w_2 := z$;
für $i = 1, \ldots, t_1$ **tue**
  $w_3 := (z^3 + (a_1 z + a_2 z^2) w_0 + (a_3 + a_4 z) w_1^2 + a_6 w_2^3) \bmod z^{t_1+1}$;
  $w_2 := w_1$;
  $w_1 := w_0$;
  $w_0 := w_3$;
Ende
zurück w_3;

Aus der Additionsformel für Punkte einer elliptischen Kurve ergibt sich, dass die Anzahl der Dezimalstellen in Nenner und Zähler in jedem Schritt jeweils um bis zu dem Vierfachen zunimmt. Das bedeutet, bei der Berechnung von mP ist mit bis zu 4^m Stellen in Nenner und Zähler zu rechnen. Dadurch wird bereits für relativ kleine m die exakte Berechnung unmöglich. Deshalb berechnet man den Quotienten der Komponenten von $p^V P'$ nicht exakt, sondern lediglich auf t_0 Stellen genau. Dazu werden die Koordinaten p-adisch mit gewünschter Präzision dargestellt. Anschließend wird eine Approximation durch Anwenden der Additionsformeln und des „double and add“ Verfahrens berechnet. So ist es möglich, P' auch mit sehr hohen Faktoren zu multiplizieren, wobei der Aufwand etwa linear mit der gewünschten Präzision ansteigt.

5. Berechnung von $z_P = \frac{x_{\hat{P}}}{y_{\hat{P}}}$, wobei $\hat{P} = (x_{\hat{P}}, y_{\hat{P}})$.

6. Die gewünschte Approximation erhält man dann durch

$$\widehat{\Psi_{\mathfrak{p}}(P)} = \frac{\tilde{\Psi}_{\mathfrak{p}}(z_P)}{p^V}.$$

   Da diese Approximation lediglich auf t_0 Stellen genau sein soll, ist es unerheblich, ob z_P selbst exakt bekannt ist oder nur eine entsprechend gute Näherung ist.

Theoretisch ist der Aufwand für die Berechnung des Polynoms $\tilde{\Psi}_{\mathfrak{p}}(T)$ linear im Grad, praktisch werden die Koeffizienten sehr schnell sehr groß. Deshalb ist das Verfahren insgesammt deutlich langsamer als linear. Es ist daher kaum möglich, das Polynom bis zu einem Grad größer als einige hundert

zu bestimmen, was in dieser Arbeit aber benötigt wird. Man berechnet es also nur bis zu einem kleineren Grad t_1 und erreicht die geforderte Präzision dann durch die Schritte 4 - 6. Trotz näherungsweiser Berechnung der Punktmultiplikation kann diese für große Faktoren sehr langsam werden. Deshalb muss durch Probieren ein Kompromiss bei der Dauer der Berechnung des Polynoms und der Dauer der Multiplikation der einzelnen Punkte gefunden werden. Da meist der p-adische Logarithmus zu einer Kurve in mehreren Punkten bestimmt werden muss, berechnet man einmal das Polynom und speichert dieses dann. Nur die Schritte 3 - 6. müssen für jeden Punkt einzeln wiederholt werden.

1.5.3 Test auf S-Ganzheit

Man kann einen Punkt auf S-Ganzheit testen, indem man die Primidealzerlegung seiner Koordinaten bestimmt. Will man allerdings mehrere Punkte testen, dauert es sehr lange, für jeden Punkt einzeln die Primidealzerlegung zu bestimmen. Das kann man mit dem folgenden Verfahren aus [Her02] umgehen: Zu jeder endlichen Stelle $\mathfrak{p} \in S$ wird zunächst ein zufälliges Element $\alpha_\mathfrak{p} \in \mathbb{Z}_\mathbb{K}$ mit der Eigenschaft $v_\mathfrak{p}(\alpha_\mathfrak{p}) \geq 1$ gewählt. Diese Elemente $\alpha_\mathfrak{p}$ werden nun einmalig faktorisiert. Alle Faktoren, die nicht bereits in S enthalten sind, werden in einer zweiten Menge $\mathcal{P}$ gespeichert. Diese Schritte werden einmal für alle zu testenden Punkte durchgeführt.

Um nun einen bestimmten Punkt $P = (x, y)$ zu testen, prüft man im ersten Schritt, ob für eine Stelle $\mathfrak{q} \in \mathcal{P}$ gilt: $v_\mathfrak{q}(x) < 0$. Ist das der Fall, so enthält der Punkt auch das zur Stelle $\mathfrak{q}$ korrespondierende Primideal im Nenner, was bei S-Ganzheit nicht sein dürfte, und der Punkt P ist somit nicht S-ganz.

Tritt dieser Fall nicht ein, so bildet man im zweiten Schritt das Produkt

$$A := x \prod_{\substack{\mathfrak{p} \in S, \\ v_\mathfrak{p}(x) < 0}} \alpha_\mathfrak{p}^{-v_\mathfrak{p}(x)}.$$

Da $\mathfrak{p} | \alpha_\mathfrak{p}$ nach Konstruktion, kürzen sich somit alle Faktoren aus S im Nenner von x weg. Ist x S-ganz, hat also außerhalb von S keine weiteren Faktoren im Nenner, so muss das Produkt eine ganze Zahl sein, sonst bleibt ein Faktor im Nenner, der sich nicht kürzen lässt, s. Algorithmus 4 und Algorithmus 5

Kapitel 2

Schranken

Nach 1.11 lässt sich jeder Punkt P mit Hilfe einer Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$ darstellen:

$$P = n_1 B_1 + \cdots + n_r B_r + T.$$

Dabei bezeichnet T einen Torsionspunkt. Um alle S-ganzen Punkte einer elliptischen Kurve zu bestimmen, schätzt man die Koeffizienten n_i ab. Das heißt, es ist ein $N \in \mathbb{N}$ gesucht, so dass $N \geq \max\{|n_i|\} = h_n(P)$.

2.1 Schranken über $\mathbb{Q}$

In [PHZH99] werden explizite Schranken für N im Falle einer elliptischen Kurve über $\mathbb{Q}$ angegeben.

Satz 2.1. *Sei E eine elliptische Kurve in langer Weierstraß-Form und $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}, \infty\}$ eine endliche Menge von Stellen aus $\mathbb{Q}$, die die unendliche Stelle enthält. Dann ist $s-1$ die Anzahl der endlichen Stellen, und $\mathcal{P}$ die größte endliche Stelle. Für den Fall, dass S keine endliche Stelle enthält, sei $\mathcal{P} = 1$. Ist E minimal für jede endliche Stelle aus S, so gilt für einen S-ganzen Punkt $P = (x, y) \in E(\mathbb{Q})$:*

$$h_n(P) \leq N(E, \lambda_{\min}, S) := \sqrt{\frac{1}{\lambda_{\min}} \left(\frac{k_1}{2} + k_2 \right)}$$

mit

$$\begin{aligned}
k_2 &:= \log\left(\max\left\{|b_2|, |b_4|^{1/2}, |b_6|^{1/3}, |b_8|^{1/4}\right\}\right),\\
k_1' &:= 7\cdot 10^{38s+49} s^{20s+15} \mathcal{P}^{24} (\log^* \mathcal{P})^{4s-2} k_3 (\log k_3)^2 ((20s-19)k_3 + \log(ek_4)),\\
k_1 &:= k_1' + 2\log(2\max\{|a_1|, |a_2|\} + 6),\\
k_3 &:= \frac{32}{3}\sqrt{|2^8 3^{12}\Delta|}(8 + \frac{1}{2}\log|2^8 3^{12}\Delta|)^4,\\
k_4 &:= 20^4 \max\{3^6(b_2^2 - 24b_4)^2, 16\sqrt{s^8 3^{12}\Delta}^3\}.
\end{aligned}$$

Beweis: [PHZH99] □

Für den Fall, dass die Kurve E kurze Weierstraß-Form und Rang kleiner oder gleich 2 hat, gibt Herrmann in [Her02] eine niedrigere Schranke an:

Satz 2.2. *Sei E eine elliptische Kurve in kurzer Weierstraß-Form mit Rang ≤ 2. Sei S eine Stellenmenge wie in 2.1. Bezeichne ω_i, $i = 1, 2$ die Perioden der Kurve, $u_{i,\infty}$ den elliptischen Logarithmus des i-ten Basiselements und $u_{i,\mathfrak{p}}$ den $\mathfrak{p}$-adischen elliptischen Logarithmus des i-ten Elements. Man setzt $u'_{i,\infty} := g\frac{u_{i,\infty}}{\omega_1}$, $u'_{i,\mathfrak{p}} := g\frac{u_{i,\mathfrak{p}}}{\omega_1}$ und $\tau := \frac{\omega_1}{\omega_2}$. Dabei ist g die Ordnung der Torsionsgruppe. j_1 und j_2 bezeichnen Zähler und Nenner der j-Invarianten. Dann gilt:*

$$h_n(P) \leq N_1 := \max\{N_\mathfrak{p} : \mathfrak{p} \in S\},$$

mit

$$N_\mathfrak{p} = \begin{cases} 2^5\sqrt{k_{6,\infty}k_{7,\infty}}(\log 5^5 k_{7,\infty})^{5/2}, & \textit{falls } \mathfrak{p} = \infty,\\ 2^4\sqrt{k_{6,\mathfrak{p}}k_{7,\mathfrak{p}}}(\log 4^4 k_{7,\mathfrak{p}})^2, & \textit{falls } \mathfrak{p} \in S\backslash\{\infty\}, \end{cases}$$

wobei für die unendliche Stelle gilt:

$$\begin{aligned}
h &:= \log\max\{4|a_4 j_2|, 4|a_6 j_2|, |j_1|\},\\
\log V_i &:= \max\left\{\hat{h}(B_i), h, \frac{3\pi|u'_{i,\infty}|^2}{\mathrm{Im}(\tau)}\right\}, \quad i = 1, 2,\\
\log V_0 &:= \max\left\{h, \frac{3\pi}{\mathrm{Im}(\tau)}\right\},\\
k_{6,\infty} &:= \frac{1}{\lambda_{\min}}(\log\max\{|2a_4|^{1/2}, |4a_6|^{1/3}\} + s\log(2g/(3\omega_1))),\\
k_{7,\infty} &:= \frac{2\cdot 10^{68} s h^5}{\lambda_{\min}}\prod_{i=0}^{2}\log V_i.
\end{aligned}$$

Und für die endlichen Stellen $\mathfrak{p} \in S$ gilt:

$$\begin{aligned}
\alpha_{\mathfrak{p}} &:= \begin{cases} 3, & \textit{falls } \mathfrak{p} = 2, \\ \frac{1}{\mathfrak{p}-1}, & \textit{sonst,} \end{cases} \\
\sigma_{\mathfrak{p}} &:= (\mathfrak{p}^{\alpha_{\mathfrak{p}}} \max\{|u'_{1,\mathfrak{p}}|_{\mathfrak{p}}, |u'_{2,\mathfrak{p}}|_{\mathfrak{p}}\})^{-1}, \\
d_{\mathfrak{p}} &:= \max\{1, 1/\log \sigma_{\mathfrak{p}}\}, \\
\rho_i &:= \max\{1, \hat{h}(B_i)\}, \quad i = 1, 2, \\
\beta &:= \max\{\log N_0(E, \lambda_{\min}, S), \log|a_4|, \log|a_6|, \rho_1, \rho_2, d_{\mathfrak{p}}\}, \\
\gamma &:= \max\{\log|a_4|, \log|a_6|, \log\beta\}, \\
k_{6,\infty} &:= \frac{1}{\lambda_{\min}} \log \max\{|2a_4|^{1/2}, |4a_6|^{1/3}\}, \\
k_{7,\mathfrak{p}} &\geq \frac{1}{\lambda_{\min}} (3.6 \cdot 10^{25} s \rho_1 \rho_2 d_{\mathfrak{p}}^6 \log \sigma_{\mathfrak{p}}).
\end{aligned}$$

Beweis: [Her02] □

2.2 Schranken über Zahlkörpern

Im folgenden Kapitel richte ich mich großteils nach dem Vorgehen von [Her02]. Allerdings erhalte ich in Lemma 2.10 zum Abschätzen von Einheitengleichungen ein anderes Ergebnis. Danach arbeite ich zwar mit diesem Ergebnis weiter, ändere aber nichts am prinzipiellen Vorgehen Herrmanns [Her02].
Um Schranken für S-ganze Punkte über einem Zahlkörper herzuleiten, ist es zunächst notwendig, einige Bezeichnungen einzuführen:

Sei

- $\mathbb{K} = \mathbb{Q}(\theta)$ ein Zahlkörper vom Grad $d \geq 2$,
- $E : y^2 = f(x) := x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}_{\mathbb{K}}$, eine elliptische Kurve über $\mathbb{K}$,
- Δ_f die Diskriminante von f,
- S eine endliche Menge von Stellen aus $\mathbb{K}$, die alle unendlichen Stellen enthält,
- s die Mächtigkeit von S und t die Anzahl der endlichen Stellen in S,
- $M_{\mathbb{K}}$ die Menge aller Stellen aus dem Körper $\mathbb{K}$,
- $h_{\mathbb{K}}$ die Klassenzahl, $\mathcal{R}_{\mathbb{K}}$ der Regulator und $D_{\mathbb{K}}$ die Diskriminante von $\mathbb{K}$,
- $\mathcal{P} := \begin{cases} 1, & \text{falls } t = 0, \\ \max_{1 \leq i \leq t}\{p : \mathfrak{p}_i | p, p \in M_{\mathbb{Q}} \backslash \{\infty\}\}, & \text{sonst,} \end{cases}$

- $H(f) = \left(\prod_{\nu \in M_{\mathbb{K}}} \max\{1, |a_2|_\nu, |a_4|_\nu, |a_6|_\nu\}^{n_\nu}\right)^{1/d}$ mit $n_\nu = [\mathbb{H}_\nu : \mathbb{Q}_\nu]$, die Höhe des Polynoms f,
- $\mathcal{H}_f := \max\{H(f), e^e\}$,
- $\delta_d > 0$ eine Konstante mit der Eigenschaft $h(\alpha) \geq \frac{\delta_d}{d}$ für alle $\alpha \neq 0$ für die gilt, dass sie algebraisch, vom Grad $\leq d$ und keine Einheitswurzeln sind. Als Beispiel ist in [Her02] $\delta_d = \frac{2}{(\log(3d))^3}$ gegeben. Außerdem gelten folgende zwei Abschätzungen: $\delta_d \leq 1/2$ und $2 \leq \delta_d^{-1} \leq 3d$,
- $R_S = |\det(\log|\varepsilon_i|_{\nu_j})_{1 \leq i,j \leq s-1}|$, der S-Regulator, wobei $\nu_i \in S$, $i = 1, \ldots, s-1$, und $\{\varepsilon_1, \ldots \varepsilon_{s-1}\}$ ein S-Grundeinheitensystem in $\mathbb{K}$ ist. Falls S keine endliche Stelle enthält, entspricht der S-Regulator dem Regulator des Zahlkörpers.

Ziel dieses Kapitels ist es, eine Schranke N für $h_n(P)$ mit S-ganzem P zu erhalten. Das Ergebnis ist in folgendem Satz formuliert und wird in diesem Kapitel bewiesen:

Satz 2.3. *Sei P ein S-ganzer Punkt der elliptischen Kurve E der Form $y^2 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}_{\mathbb{K}}$. Dann gilt folgende Ungleichung:*

$$h_n(P) \leq \sqrt{\frac{u_2 + 12\log 2 + 2\log H_f + 2T_1(\log 2 + \log(2\log H_f + T_2 \log T_2))}{\lambda_{\min}}}$$

mit $T_2 = 31/30 \cdot T_1$ und

$$\begin{aligned}
T_1 &:= 30c_{13}(15\log(e|D_{\mathbb{K}}||N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|)) + c_{12}(d)c_a(12d, 12d-1)M_2 \\
&\quad +60tM_2 \log^* \mathcal{P}), \\
M_2 &= M_1 \frac{(\log M_1)^{6d-1}(12d - 1 + \log M_1)^{6d}}{(12d-1)!}, \\
M_1 &= \left(\frac{2}{\Pi}\right)^{6d} 2^{6d} e^6 |D_{\mathbb{K}}|^{15} |N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|^{10}, \\
c_{13} &= c(24d, 24(d+t)) \frac{\mathcal{P}^{24d}}{(\log^* \mathcal{P})^2} M_2^2 (12d \log^* \mathcal{P})^{24dt} \log^*(M_2(12\log^* \mathcal{P})^{12dt}), \\
c(d,s) &= c_6 \cdot \max\{c_5, c_{10}\} \log c_2 2\delta_d^{1-s} \log((20s-10)dc_7) \log^* \mathcal{P}^2, \\
c_2 &= (s-1)\delta_d^{-1} \frac{((s-1)!)^2}{2^{s-2}}, \\
c_5 &= 35.2 \cdot (s-1)c_M(2s-1)d^{4s-1}5^{2s-1}((s-1)!)^2 \log(ed), \\
c_6 &= \delta_d^{-2s+2} c_{L_1}(d,s)^2 d^{2s-2} \left(\frac{1}{d\log^* P} + 1\right)^{2s-2}, \\
c_7 &= 4\delta_d^{1-s} c_{L_2}(d,s) + (0.2052\log 2)^{-1}, \\
c_{10} &= \frac{s-1}{d} c_{Yu}(2s-1)d^{4s+1} \log(c_{Yu}(2s-1)d^{4s}).
\end{aligned}$$

Die Konstanten $c_i, c_{L_2}, c_M, c_{Yu}, c_a$, und c_{12} stammen aus den Sätzen des nachfolgenden Kapitels 2.2.1 und aus Satz 2.11.

Zwar werden die Schranken für einen Zahlkörper zunächst nur für Kurven der Form $y^2 = f(x)$ hergeleitet, aber das stellt keine Einschränkung dar, denn über die Transformation

$$y = \frac{1}{2}(\frac{1}{4}y' - a_1x' - a_3) \quad \text{und} \quad x = \frac{1}{4}x'$$

lässt sich jede Gleichung in langer Weierstraß-Form in eine Gleichung der Form $y^2 = f(x)$ überführen. Für die Höhen der Punkte gilt dann:

$$h(4x) = h(x').$$

2.2.1 Einige notwendige Sätze

Lemma 2.4. *Es existiert ein $\mathcal{S}$-Grundeinheitensystem $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$, so dass gilt:*

i) $\prod_{j=1}^{s-1} h(\varepsilon_j) \leq c_{L_1}(d,s) \cdot \mathcal{R}_{\mathcal{S}}$, *mit* $c_{L_1}(d,s) = \frac{((s-1)!)^2}{2^{s-2}d^{s-1}}$.

ii) $h(\varepsilon_j) \leq c_{L_2}(d,s) \cdot \mathcal{R}_{\mathcal{S}}$, $j = 1, \ldots, s-1$, *mit* $c_{L_2}(d,s) = c_{L_1}(d,s)\left(\frac{\delta_d}{d}\right)^{2-s}$.

iii) Die Einträge der inversen Matrix von $(\log|\varepsilon_i|_{\nu_j})_{i,j=1,\ldots,s-1}$ *sind betragsmäßig kleiner als* $c_{L_3}(d,s) = c_{L_1}(d,s) \cdot d^{s-1}\delta_d^{-1}$.

Beweis: Vgl. [BG96] □

Satz 2.5 (Matveev)**.** *Sei* $\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n \neq 0$ *mit* $\alpha_i \in \mathbb{K}^*$, $i = 1, \ldots, n$ *und* $b_i \in \mathbb{Z}$, $i = 1, \ldots, n$. *Außerdem wähle Zahlen* A_i *so, dass*

$$A_i \geq \max\{dh(\alpha_i), |\log(\alpha_i)|, 0.16\},\ i = 1, \ldots, n.$$

Mit $B = \max\{|b_1|, \ldots, |b_n|\}$ *gilt dann*

$$|\Lambda| > \exp\{-c_M(n)d^2 \prod_{i=1}^{n} A_i \log(ed)\log(eB)\}.$$

Dabei ist $c_M(n) = \min\left\{\left(\frac{1}{2}en\right)^2 30^{n+3}n^{3.5}, 2^{6n+20}\right\}$

Beweis: [Mat00] □

Satz 2.6 (Yu). *Sei* $\Gamma = \alpha_1^{\varrho_1} \cdots \alpha_n^{\varrho_n} - 1 \neq 1$ *und seien* $A_1, \ldots, A_n$ *positive reelle Zahlen mit*

$$\log A_i \geq \max\left\{h(\alpha_i), \frac{|\log \alpha_i|}{10d}, \log p\right\}, \ i = 1, \ldots, n.$$

Sei weiterhin

$$\Phi = c_{Yu}(n)\left(\frac{d}{\sqrt{\log p}}\right)^{2(n+1)} p^d \log A_1 \cdots \log A_n \log(10nd \log A)$$

mit $c_{Yu} = 22000(9.5(n+1))^{2(n+1)}$ *und* $A = \max\{A_1, \ldots, A_n, e\}$. *Dann ist*

$$|\Gamma|_\nu \geq \exp\{-d(\log p)\Phi \log(dB)\}.$$

Ist zusätzlich noch $\rho_n = 1$ *und* $A_n \geq A_i$ *für* $i = 1, \ldots, n-1$, *so kann* A *durch* $\max\{A_1, \ldots, A_{n-1}, e\}$ *ersetzt werden, und für jedes* $0 < \delta \leq 1$ *gilt*

$$|\Gamma|_\nu \geq \exp\left\{-d(\log p)\max\left\{\Phi \log\left(\frac{\delta^{-1}\Phi}{\log A_n}\right), \delta B\right\}\right\}.$$

Beweis: Vgl. [Yu94] □

Lemma 2.7. *Wenn* $t > 0$, *die Anzahl der endlichen Stellen in der Menge* S *ist, dann gilt*

$$\mathcal{R}_\mathcal{S} \leq \mathcal{R}_\mathbb{K} h_\mathbb{K} \prod_{i=1}^{t} \log N(\mathfrak{p}_i) \leq \mathcal{R}_\mathbb{K} h_\mathbb{K} (d \log^* \mathcal{P})^t$$

und

$$\mathcal{R}_\mathcal{S} \geq \mathcal{R}_\mathbb{K} \prod_{i=1}^{t} \log N(\mathfrak{p}_i) \geq 0.2052(\log 2)(\log^* \mathcal{P}).$$

Beweis: Vgl. [BG96] □

Lemma 2.8. *Sei* $\mathbb{K}$ *ein Zahlkörper vom Grad* d *über* $\mathbb{Q}$ *und* r_2 *die Anzahl der komplexen Einbettungen von* $\mathbb{K}$. *Dann gilt für den Regulator* $\mathcal{R}_\mathbb{K}$ *und die Klassenzahl* $h_\mathbb{K}$ *von* $\mathbb{K}$*:*

$$\mathcal{R}_\mathbb{K} h_\mathbb{K} \leq \left(\frac{2}{\pi}\right)^{r_2} |D_\mathbb{K}|^{1/2} \frac{\left(\log\left(\left(\frac{2}{\pi}\right)^{r_2} |D_\mathbb{K}|^{1/2}\right)\right)^{d-1-r_2} \left(d - 1 + \log\left(\left(\frac{2}{\pi}\right)^{r_2} |D_\mathbb{K}|^{1/2}\right)\right)^{r_2}}{(d-1)!}.$$

Beweis: [Len92] □

Lemma 2.9. *Seien $l_1, l_2 > 0, l_3 \geq 1$ reelle Zahlen und bezeichne $x_{\max} \in \mathbb{R}$ die größte reelle Lösung der Gleichung*

$$x_0 = l_1 + l_2(\log x_0)^{l_3}.$$

Ist $l_2 > (\frac{\exp\{2\}}{l_3})^{l_3}$, dann gilt

$$x_{\max} \leq 2^{l_3}(l_1^{1/l_3} + l_2^{1/l_3} \log(l_3^{l_3} l_2))^{l_3}.$$

Ist die Bedingung für l_2 nicht erfüllt, so ist

$$x_{\max} \leq 2^{l_3}(l_1^{1/l_3} + 2\exp\{2\})^{l_3}.$$

Beweis: [Sma98] □

2.2.2 Schranken für Einheitengleichungen

Aus [Her02].

Lemma 2.10. *Sei $\mathbb{K} = \mathbb{Q}(\theta)$ ein algebraischer Zahlkörper vom Grad $d \geq 2$ über $\mathbb{Q}$. $\mathbb{K}_1, \mathbb{K}_2$ seien Teilkörper von $\mathbb{K}$ vom Grade d_1 und d_2. Weiter seien $\mathcal{S}, \mathcal{S}_1, \mathcal{S}_2$ endliche Stellenmengen von $\mathbb{K}, \mathbb{K}_1, \mathbb{K}_2$ mit den Mächtigkeiten s, s_1, s_2, die alle unendlichen Stellen enthalten.*
Angenommen, es gilt $\mathbb{Z}^*_{\mathbb{K}_1,\mathcal{S}_1} \subset \mathbb{Z}^*_{\mathbb{K},\mathcal{S}}$ und $\mathbb{Z}^*_{\mathbb{K}_2,\mathcal{S}_2} \subset \mathbb{Z}^*_{\mathbb{K},\mathcal{S}}$.
Für $i = 1, 2$ bezeichne $\mathcal{R}_i$ den $\mathcal{S}_i$-Regulator von $\mathbb{K}_i$. Seien $n_1, n_2, n_3 \in \mathbb{K} \setminus \{0\}$ mit $H(n_i) \leq \mathcal{H}$, wobei H die Höhe bezeichnet und $\mathcal{H}$ eine Konstante kleiner e ist.
Für die Gleichung

$$n_1\varepsilon_1 + n_2\varepsilon_2 + n_3\varepsilon_3 = 0$$

mit $\varepsilon_1 \in \mathbb{Z}^*_{\mathbb{K}_1,\mathcal{S}_1}, \varepsilon_2 \in \mathbb{Z}^*_{\mathbb{K}_2,\mathcal{S}_2}, \varepsilon_3 \in \mathbb{Z}^*_{\mathbb{K},\mathcal{S}}$ unbekannt, gilt nun

$$H\left(\frac{n_i\varepsilon_i}{n_3\varepsilon_3}\right) < \exp\left\{c(d,s)\frac{\mathcal{P}^d}{(\log^* \mathcal{P})^2}\mathcal{R}_1\mathcal{R}_2 \log^* \max\{\mathcal{R}_1, \mathcal{R}_2\} \cdot \right.$$

$$\left. \cdot \log \mathcal{H} \log^* \log^* \max\{H(\varepsilon_1), H(\varepsilon_2)\}\right\}, \ i = 1, 2,$$

wobei die Konstante $c(d,s)$ durch

$$\begin{aligned}
c(d,s) &= c_6 \cdot \max\{c_5, c_{10}\} \log c_2 2\delta_d^{1-s} \log((20s-10)dc_7) \log^* \mathcal{P}^2 \\
c_2 &= (s-1)\delta_d^{-1}\frac{((s-1)!)^2}{2^{s-2}} \\
c_5 &= 35.2 \cdot (s-1)c_M(2s-1)d^{4s-1}5^{2s-1}((s-1)!)^2 \log(ed) \\
c_6 &= \delta_d^{-2s+2}c_{L_1}(d,s)^2 d^{2s-2}\left(\frac{1}{d\log^* P} + 1\right)^{2s-2} \\
c_7 &= 4\delta_d^{1-s}c_{L_2}(d,s) + (0.2052\log 2)^{-1} \\
c_{10} &= (s-1)c_{Yu}(2s-1)d^{4s}\log(c_{Yu}(2s-1)d^{4s})
\end{aligned}$$

gegeben ist, mit c_i, c_{L_2}, c_M, und c_{Yu} aus den Sätzen in Kapitel 2.2.1.

Herrmann gibt dieses Lemma in [Her02] mit einem anderen Wert für c an. In seinem Beweis ist aber im letzten Schritt die Abschätzung ungültig. Außerdem verwendet er bei einer Fallunterscheidungen den Satz von Waldschmidt, der dafür jedoch nicht geeignet ist, da er zu starke Voraussetzungen verlangt. Diesen Satz habe ich durch Satz 2.5 ersetzt. Behebt man diese Fehler, so wird die Konstante größer. Ich habe nun im Laufe des Beweises einige Abschätzungen verschärft, um dieser Verschlechterung entgegen zu wirken. D.h., die Beweisführung läuft überwiegend analog zu der Herrmanns, enthält jedoch einige schärfere Abschätzungen und Verbesserungen.

Beweis: Angenommen $\mathcal{S} = \mathcal{S}_\infty$ mit $s < 2$, dann wäre $\mathbb{K}$ ein imaginärer quadratischer Zahlkörper und hätte somit Einheitenrang 0. Entsprechend hätten aber auch die Zwischenkörper $\mathbb{K}_1, \mathbb{K}_2$ den Einheitenrang 0. Folglich kann man annehmen, dass $s \geq 2$.

Seien $E_1 = \{\mu_1, \ldots, \mu_{s_1-1}\}$ ein $\mathcal{S}_1$-Grundeinheitensystem in $\mathbb{K}_1$ und $E_2 = \{\rho_1, \ldots \rho_{s_2-1}\}$ ein $\mathcal{S}_2$-Grundeinheitensystem in $\mathbb{K}_2$. Damit kann man ε_1 und ε_2 darstellen als

$$\varepsilon_1 = \zeta_1 \mu_1^{\varrho_1} \cdots \mu_{s_1-1}^{\varrho_{s_1-1}}, \quad \varepsilon_2 = \zeta_2 \rho_1^{\varsigma_1} \cdots \rho_{s_2-1}^{\varsigma_{s_2-1}},$$

wobei $\varrho_i, \varsigma_i \in \mathbb{Z}$ für $i = 1, \ldots, s_1 - 1$ bzw. $s_2 - 1$ und ζ_1, ζ_2 Einheitswurzeln sind. Dann gilt:

$$\begin{pmatrix} \log|\varepsilon_1|_{\nu_1} \\ \vdots \\ \log|\varepsilon_1|_{\nu_{s_1-1}} \end{pmatrix} = \begin{pmatrix} \log|\mu_1|_{\nu_1} & \cdots & \log|\mu_{s_1-1}|_{\nu_1} \\ \vdots & \ddots & \vdots \\ \log|\mu_1|_{\nu_{s_1-1}} & \cdots & \log|\mu_{s_1-1}|_{\nu_{s_1-1}} \end{pmatrix} \begin{pmatrix} \varrho_1 \\ \vdots \\ \varrho_{s_1-1} \end{pmatrix},$$

wobei $\nu_j \in \mathcal{S}_1$, und daraus folgt

$$\begin{pmatrix} \varrho_1 \\ \vdots \\ \varrho_{s_1-1} \end{pmatrix} = \begin{pmatrix} \log|\mu_1|_{\nu_1} & \cdots & \log|\mu_{s_1-1}|_{\nu_1} \\ \vdots & \ddots & \vdots \\ \log|\mu_1|_{\nu_{s_1-1}} & \cdots & \log|\mu_{s_1-1}|_{\nu_{s_1-1}} \end{pmatrix}^{-1} \begin{pmatrix} \log|\varepsilon_1|_{\nu_1} \\ \vdots \\ \log|\varepsilon_1|_{\nu_{s_1-1}} \end{pmatrix},$$

für $\nu_j \in \mathcal{S}_1$.

Nach Lemma 2.4 gilt $|\varrho_i| \leq (s_1 - 1) c_{L_3}(d_1, s_1) h(\varepsilon_1)$. Analog erhält man $|\varsigma_i| \leq (s_2 - 1) c_{L_3}(d_2, s_2) h(\varepsilon_2)$.
Wegen $\varrho_i \neq 0$ und $\varsigma_i \neq 0$ folgt damit $s_1, s_2 \geq 2$.
Weiterhin lässt sich $c_{L_3}(d_i, s_i)$ abschätzen durch:

$$\begin{aligned} c_{L_3}(d_i, s_i) &= \frac{((s_i-1)!)^2}{2^{s_i-2} d_i^{s_i-1}} d_i^{s_i-1} \delta_{d_i}^{-1} = \frac{((s_i-1)!)^2}{2^{s_i-2}} \delta_{d_i}^{-1} \\ &\leq \frac{((s-1)!)^2}{2^{s-2}} \delta_d^{-1} = c_1(s) \delta_d^{-1} \end{aligned}$$

mit $c_1(s) = \frac{((s-1)!)^2}{2^{s-2}}$.
Folglich ist mit $B = \max\{|\varrho_i|, |\varsigma_i|, 3\}$:

$$B \leq c_2 \log^* \max\{H(\varepsilon_1), H(\varepsilon_2)\}, \text{ mit } c_2 = (s-1)c_1(s)\delta_d^{-1}.$$

Man wählt nun $\nu \in \mathcal{S}$, so dass $|\frac{\varepsilon_3}{\varepsilon_1}|_\nu$ minimal ist.
Betrachte zunächst $|\frac{n_3\varepsilon_3}{n_1\varepsilon_1}|_\nu$. Dies lässt sich darstellen als

$$\left|\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right|_\nu = \left|-\frac{n_2\varepsilon_2}{n_1\varepsilon_2} - 1\right|_\nu = \left|\alpha_0\mu_1^{-\varrho_1}\cdots\mu_{s_1-1}^{-\varrho_{s_1-1}}\rho_1^{\varsigma_1}\cdots\rho_{s_2-1}^{\varsigma_{s_2-1}} - 1\right|_\nu = |\Gamma|_\nu$$

mit $\alpha_0 = -\frac{n_2\varsigma_2}{n_1\varsigma_1}$.

Nun werden 2 zwei Fälle unterschieden:
1. Fall $\nu|\infty$:
An dieser Stelle verwendet Herrmann einen Satz von Waldschmidt [Wal93], der aber sehr starke Bedingungen enthält, die hier nicht ohne weiteres als erfüllt betrachtet werden können. Ich verwende deshalb Satz 2.5. Dazu definiere ich:

$$\begin{array}{lcll} A_i & = & 10d^2h(\mu_i), & i = 1,\ldots,s_1-1 \\ A_{s_1-1+j} & = & 10d^2h(\rho_j), & j = 1,\ldots,s_2-1 \\ A_0 & = & 20d^2\log\mathcal{H}. & \end{array}$$

Dabei gilt wegen $h(\alpha)\delta_d^{-1} \geq \frac{|\log\alpha|}{3.3d}$, vgl. [Bug97],

$$\begin{array}{lcl} A_i & \geq & \max\{dh(\mu_i), |\log\mu_i|, 0.16\} \\ A_j & \geq & \max\{dh(\rho_j), |\log\rho_j|, 0.16\} \\ A_0 & \geq & \max\{dh(\alpha_0), |\log\alpha_0|, 0.16\}, \end{array}$$

denn $d^2 10h(\mu_i) \geq 3.3d\delta_d^{-1}h(\mu_i) \geq |\log\mu_i|,\ i = 1,\ldots,s_1-1$ und analog für $A_j,\ j = s_1,\ldots,s_1+s_2-2$. Für A_0 gilt dann

$$A_0 = 10d^2\log\mathcal{H}^2 \geq H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right)10d^2 = h\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right)10d^2 \geq \left|\log\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right|.$$

Wegen

$$\left|\alpha_0\mu_1^{-\varrho_1}\cdots\mu_{s_1-1}^{-\varrho_{s_1-1}}\rho_1^{\varsigma_1}\cdots\rho_{s_2-1}^{\varsigma_{s_2-1}} - 1\right|_\nu \geq$$

$1/2\,|\alpha_0(-\varrho_1)\log(\mu_1)\cdots(-\varrho_{s_1-1})\ \log(\mu_{s_1-1})\varsigma_1\log(\rho_1)\cdots\varsigma_{s_2-1}\log(\rho_{s_2-1}) - 1|_\nu$

ergibt sich mit Satz 2.5:

$$|\Gamma|_\nu \geq \frac{1}{2}\exp\left\{-c_M(s_1+s_2-1)d^2\prod_{i=0}^{s_1+s_2-2}\log A_i\log(ed)\log(eB)\right\}$$

Mit Lemma 2.4 gilt dann

$$\begin{aligned}\prod_{i=0}^{s_1+s_2-2} \log A_i &= 2(10d^2)^{s_1+s_2-1} \prod_{i=1}^{s_1-1} h(\mu_i) \prod_{i=1}^{s_2-1} h(\rho_i) \log \mathcal{H} \\ &\leq 2(10d^2)^{2s-1} c_{L_1}(d_1, s_1) c_{L_1}(d_2, s_2) \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \\ &\leq 2(10d^2)^{2s-1} c_1(s)^2 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H}\end{aligned}$$

Es ergibt sich insgesamt:

$$|\Gamma|_\nu = \left|\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right| \geq \frac{1}{2} \exp\{-c_3 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \log(eB)\}$$

mit $c_3 = 2c_M(2s-1)d^{4s}10^{2s-1}c_1(s)^2 \log(ed)$.
Aus der Minimalität von $\left|\frac{\varepsilon_3}{\varepsilon_1}\right|_\nu$ folgt

$$H\left(\frac{\varepsilon_3}{\varepsilon_1}\right) \leq \left|\frac{\varepsilon_3}{\varepsilon_1}\right|_\nu^{\frac{-(s-1)}{d}}$$

und damit

$$\mathcal{H}^{2d}\left|\frac{\varepsilon_3}{\varepsilon_1}\right|_\nu \geq \left|\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right|_\nu = \left|\frac{\varepsilon_3}{\varepsilon_1}\right|_\nu \left|\frac{n_3}{n_1}\right|_\nu \geq \frac{1}{2}\exp\{-c_3\mathcal{R}_1\mathcal{R}_2 \log \mathcal{H} \log(eB)\}.$$

Insgesamt folgt also

$$H\left(\frac{\varepsilon_3}{\varepsilon_1}\right) \leq \mathcal{H}^{2(s-1)} \exp\left\{\frac{s-1}{d} c_3 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H}(\log e + \log B)\right\}.$$

Somit ist

$$\begin{aligned}H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) &\leq \mathcal{H}^{2s} \exp\left\{2\frac{s-1}{d} c_3 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \log B\right\} \\ &= \exp\left\{2s \log \mathcal{H} + 2\frac{s-1}{d} c_3 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \log B\right\}.\end{aligned}$$

Beachtet man außerdem, dass

$$\frac{2s \log \mathcal{H}}{2(s-1)c_3 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \log B} \leq 0.1,$$

so gilt

$$H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) \leq \exp\{c_5 \mathcal{R}_1 \mathcal{R}_2 \log \mathcal{H} \log B\}$$

mit

$$c_5 = 1.1 \cdot \frac{2(s-1)}{d} c_3.$$

2.Fall $\nu \nmid \infty$
Definiere:

$$\begin{aligned} \log A_i &= \delta_d^{-1} h(\mu_i) + \log^* \mathcal{P}, \qquad i = 1, \ldots, s_1 - 1, \\ \log A_{s_1-1+j} &= \delta_d^{-1} h(\rho_j) + \log^* \mathcal{P}, \qquad j = 1, \ldots, s_2 - 1, \\ \log A_0 &= 2\delta_d^{-1} \log \mathcal{H} + \log^* \mathcal{P}. \end{aligned}$$

Dann gilt für das Produkt

$$\prod_{i=1}^{s_1+s_2-2} \log A_i = \prod_{i=1}^{s_1-1} (\delta_d^{-1} h(\mu_i) + \log^* \mathcal{P}) \cdot \prod_{j=1}^{s_2-1} (\delta_d^{-1} h(\rho_j) + \log^* \mathcal{P}).$$

Aus der Definition von δ_d folgt: $h(\alpha) \geq \frac{\delta_d}{d} \Leftrightarrow \frac{\delta_d}{h(\alpha)} \leq d$. Damit gilt für den ersten Faktor:

$$\begin{aligned} & \prod_{i=1}^{s_1-1} (\delta_d^{-1} h(\mu_i) + \log^* \mathcal{P}) = \\ = & \prod_{i=1}^{s_1-1} (\delta_d^{-1} h(\mu_i)) + \sum_{j=1}^{s_1-1} \left(\log^* \mathcal{P} \prod_{i=1, i\neq j}^{s_1-1} \delta_d^{-1} h(\mu_i) \right) \\ & + \sum_{k=1}^{s_1-1} \sum_{j=1, j\neq k}^{s_1-1} \left((\log^* \mathcal{P})^2 \prod_{i=1, i\neq j, k}^{s_1-1} (\delta_d^{-1} h(\mu_i)) \right) + \cdots + (\log^* \mathcal{P})^{s_1-1} \\ = & \prod_{i=1}^{s_1-1} (\delta_d^{-1} h(\mu_i)) \cdot \left(1 + \sum_{j=1}^{s_1-1} \frac{\log^* \mathcal{P}}{\delta_d^{-1} h(\mu_j)} + \sum_{k=1}^{s_1-1} \sum_{j=1, j\neq k}^{s_1-1} \frac{(\log^* \mathcal{P})^2}{\delta_d^{-2} h(\mu_k) h(\mu_j)} + \cdots \right. \\ & \left. + \frac{(\log^* \mathcal{P})^{s_1-1}}{\prod_{i=1}^{s_1-1} \delta_d^{-1} h(\mu_i)} \right) \end{aligned}$$

$$
\begin{aligned}
&\leq \left(\delta_d^{-s_1+1} c_{L_1}(d_1, s_1)\mathcal{R}_1\right) \cdot \left(1 + \binom{s_1-1}{1} d\log^*\mathcal{P} + \binom{s_1-1}{2}(d\log^*\mathcal{P})^2 + \cdots \right.\\
&\quad \left. + \binom{s_1-1}{s_1-1}(d\log^*\mathcal{P})^{s_1-1}\right)\\
&= \left(\delta_d^{-s_1+1} c_{L_1}(d_1, s_1)\mathcal{R}_1\right) \cdot (1 + d\log^*\mathcal{P})^{s_1-1}\\
&= \left(\delta_d^{-s_1+1} c_{L_1}(d_1, s_1)\mathcal{R}_1\right) \cdot (d\log^*\mathcal{P})^{s_1-1} \left(\frac{1}{d\log^*\mathcal{P}} + 1\right)^{s_1-1}.
\end{aligned}
$$

Die Abschätzung für den zweiten Faktor verläuft analog, und für das gesamte Produkt ergibt sich damit:

$$
\begin{aligned}
&\prod_{i=1}^{s_1+s_2-2} \log A_i \leq\\
&\leq \left(\delta_d^{-s_1+1} c_{L_1}(d_1, s_1)\mathcal{R}_1\right) d^{s_1-1}(\log^*\mathcal{P})^{s_1-1} \left(\frac{1}{d\log^*\mathcal{P}} + 1\right)^{s_1-1}\\
&\quad \cdot \left(\delta_d^{-s_2+1} c_{L_1}(d_2, s_2)\mathcal{R}_2\right) d^{s_2-1} (\log^*\mathcal{P})^{s_2-1} \left(\frac{1}{d\log^*\mathcal{P}}\right)^{s_2-1}\\
&\leq \delta_d^{-2s+2} c_{L_1}(d, s)^2 \mathcal{R}_1\mathcal{R}_2 d^{2s-2} \left(\frac{1}{d\log^*\mathcal{P}} + 1\right)^{2s-2} (\log^*\mathcal{P})^{s_1+s_2-2}\\
&= c_6 \mathcal{R}_1\mathcal{R}_2 (\log^*\mathcal{P})^{s_1+s_2-2}
\end{aligned}
$$

mit $c_6 = \delta_d^{-2s+2} c_{L_1}(d, s)^2 d^{2s-2} \left(\frac{1}{d\log^* P} + 1\right)^{2s-2}$.

Herrmann verwendet an dieser Stelle eine andere Abschätzung für die Konstante, nämlich

$$\tilde{c_6} = \frac{15^2}{(\log^* P)^2} \left(\frac{s}{d}((s-1)!)^2 \delta_d^{-s+1} + \frac{1}{0.2052 \log 2}\right)^2.$$

Diese Schranke ist besonders für Werte $s \geq d$ ungünstiger. Das folgt aus dem Vergleich von

$$c_6 \leq \delta_d^{-2s+2}((s-1)!)^4 2^{4-2s} \left(\frac{3}{2}\right)^{2s-2}$$

und

$$\frac{15^2}{(\log^*\mathcal{P})^2} \left(\frac{s}{d}((s-1)!)^2 \delta_d^{-s+1}\right)^2,$$

ohne Berücksichtigung der anderen Terme des Quadrates.

Nun werden erneut zwei Fälle unterschieden:

1. Fall $\log \mathcal{H} < c_{L_2}(d_1, s_1)\mathcal{R}_1 + c_{L_2}(d_2, s_2)\mathcal{R}_2$

Ziel ist es, $\log A = \max_{1 \le i \le s_1+s_2-2}\{\log A_i\}$ abzuschätzen.
Dazu wird $\log A_i$ zunächst im Bereich $0 \le i \le s_1 - 1$, dann im Bereich $s_1 \le i \le s_1 + s_2 - 1$ und zuletzt für $i = 0$ mit Lemma 2.4 und Lemma 2.7 abgeschätzt und anschließend das Maximum genommen:

$$\begin{aligned}
\max_{1 \le i \le s_1-1}\{\log A_i\} &= \max_{1 \le i \le s_1-1}\{\delta_d^{-1} h(\mu_i)\} + \log^* \mathcal{P} \\
&\le \delta_d^{-1} c_{L_2}(d_1, s_1)\mathcal{R}_1 + (0.2052 \log 2)^{-1}\mathcal{R}_1 \\
&= (c_{L_2}(d_1, s_1)\delta_d^{-1} + (0.2052 \log 2)^{-1})\mathcal{R}_1 \\
&\le (\frac{1}{2} c_1(s)\delta_d^{1-s} + (0.2052 \log 2)^{-1})\mathcal{R}_1,
\end{aligned}$$

$$\begin{aligned}
\max_{s_1 \le i \le s_1+s_2-2}\{\log A_i\} &= \max_{s_1 \le i \le s_1+s_2-2}\{\delta_d^{-1} h(\rho_i)\} + \log^* \mathcal{P} \\
&\le \delta_d^{-1} c_{L_2}(d_2, s_2)\mathcal{R}_2 + (0.2052 \log 2)^{-1}\mathcal{R}_2 \\
&= (c_{L_2}(d_2, s_2)\delta_d^{-1} + (0.2052 \log 2)^{-1})\mathcal{R}_2 \\
&\le (\frac{1}{2} c_1(s)\delta_d^{1-s} + (0.2052 \log 2)^{-1})\mathcal{R}_2.
\end{aligned}$$

und

$$\begin{aligned}
\log A_0 &= 2\delta_d^{-1} \log \mathcal{H} + \log^* \mathcal{P} \\
&\le 2\delta_d^{-1}(c_{L_2}(d_1, s_1)\mathcal{R}_1 + c_{L_2}(d_2, s_2)\mathcal{R}_2) + (0.2052 \log 2)^{-1} \max\{\mathcal{R}_1, \mathcal{R}_2\} \\
&\le (2\delta_d^{1-s}(c_{L_2}(d_1, s_1) + c_{L_2}(d_2, s_2)) + (0.2052 \log 2)^{-1}) \max\{\mathcal{R}_1, \mathcal{R}_2\} \\
&\le (4\delta_d^{1-s} c_1(d) + (0.2052 \log 2)^{-1}) \max\{\mathcal{R}_1, \mathcal{R}_2\}
\end{aligned}$$

Aus den drei Abschätzungen folgt:

$$\max_{0 \le i \le s_1+s_2-2}\{\log A_i\} \le (4c_1(s)\delta_d^{1-s} + (0.2052 \log 2)^{-1}) \max\{\mathcal{R}_1, \mathcal{R}_2\}.$$

Damit gilt:

$$\log A \le c_7 \max\{\mathcal{R}_1, \mathcal{R}_2\}$$

mit $c_7 = 4\delta_d^{1-s} c_1(s) + (0.2052 \log 2)^{-1}$.

Nun wendet man Satz 2.6 auf das bereits früher definierte Γ an. Dafür setzt man

$$\Phi = \frac{\mathcal{P}^d}{(\log^* \mathcal{P})^{s_1+s_2}} (\prod_{i=0}^{s_1+s_2-2} \log A_i) \log(10(s_1 + s_2 - 1)d \log A)$$

und erhält somit

$$\left|\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right|_\nu \geq \exp\{-c_{Yu}(s_1+s_2-1)d^{2(s_1+s_2)}d\Phi\log^*\mathcal{P}\log(dB)\} = \exp\{-T\},$$

mit $T := -c_{Yu}(s_1+s_2-1)d^{2(s_1+s_2)}d\Phi\log^*\mathcal{P}\log(dB)$.
Analog zu der Rechnung mit den unendlichen Stellen erhält man

$$H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) \leq \mathcal{H}^{2s}\exp\{\frac{s-1}{d}T\}.$$

Um eine geeignetere Abschätzung zu erhalten, betrachtet man

$$\begin{aligned}
\frac{s-1}{d}T &= \frac{s-1}{d}c_{Yu}(s_1+s_2-1)d^{2(s_1+s_2)}d\Phi\log^*\mathcal{P}\log(dB)\\
&\leq (s-1)c_{Yu}(2s-1)d^{4s}\Phi\log^*\mathcal{P}(\log B+\log d)\\
&\leq (s-1)c_{Yu}(2s-1)d^{4s}\Phi\log^*\mathcal{P}\log B(1+\frac{\log d}{\log B})\\
&\leq 1.2(s-1)c_{Yu}(2s-1)d^{4s}\Phi\log^* P\log B,
\end{aligned}$$

denn $\log\log A_0 > 1$ und damit $\frac{\log d}{\log B} \leq \frac{1}{8}$.
Außerdem gilt

$$\frac{2s\log\mathcal{H}}{1.2(s-1)c_{Yu}(2s-1)d^{4s}\Phi\log^* P\log B} \leq 0.1.$$

Damit erhält man die Abschätzung

$$H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) \leq \exp\{c_8\Phi\log^*\mathcal{P}\log B\}$$

mit $c_8 = 1.3(s-1)c_{Yu}(2s-1)d^{4s}$.

2. Fall $\log\mathcal{H} \geq c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2$
Dann gilt $A_0 \geq A_i, \quad i = 1,\ldots,s_1+s_2-2$ und $\log A \leq c_7\max\{\mathcal{R}_1,\mathcal{R}_2\}$. Sei nun

$$B < \Phi\frac{(\log^*\mathcal{P})}{c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2}.$$

Es wird die Eigenschaft $H(a \pm b) \leq 2H(a)H(b)$ angewendet. Damit ist

$$\begin{aligned}
H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) &= H\left(1+\frac{n_2\varepsilon_2}{n_1\varepsilon_1}\right) \leq 2H(n_1)H(n_2)H(\varepsilon_1)H(\varepsilon_2) \\
&\leq \mathcal{H}^2 \exp\{\log 2 + h(\varepsilon_1) + h(\varepsilon_2)\} \\
&\leq \mathcal{H}^2 \exp\left\{\log 2 + h\left(\prod_{i=1}^{s_2-1}\rho_i^{\varsigma_i}\right) + h\left(\prod_{i=1}^{s_1-1}\mu_i^{\varrho_i}\right)\right\} \\
&\leq \mathcal{H}^2 \exp\left\{\log 2 + \sum_{i=1}^{s_1-1}|\varrho_i|h(\mu_i) + \sum_{i=1}^{s_2-1}|\varsigma_i|h(\rho_i)\right\} \\
&\leq \mathcal{H}^2 \exp\left\{\log 2 + B(s_1-1)c_{L_2}(d_1,s_1)\mathcal{R}_1 + B(s_2-1)c_{L_2}(d_2,s_2)\mathcal{R}_2\right\} \\
&\leq \mathcal{H}^2 \exp\left\{\log 2 + (s-1)B(c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2)\right\} \\
&\leq \mathcal{H}^2 \exp\left\{\log 2 + (s-1)\Phi\log^*\mathcal{P}\right\}
\end{aligned}$$

Wegen $\log A_i \geq \log^*\mathcal{P}$ für $i = 1,\ldots,s_1+s_2-2$, $\log A_0 \geq 2\delta_d^{-1}\log\mathcal{H}$ und

$$\begin{aligned}
&\frac{(2\log\mathcal{H}+\log 2)\log^*\mathcal{P}^{s_1+s_2}}{(s-1)\log^*\mathcal{P}\mathcal{P}^d(\log^*\mathcal{P})^{s_1+s_2-2}2\delta_d^{-1}\log\mathcal{H}c_6\mathcal{R}_1\mathcal{R}_2\log(10(s_1+s_2-1)d\log A)} \\
\leq\ & \frac{\delta_d}{(s-1)\mathcal{P}^{d-1}\log(10(s_1+s_2-1)d)} + \frac{\delta_d}{2(s-1)\mathcal{P}^{d-1}\log(10(s_1+s_2-1)d)} \\
\leq\ & \frac{1.5}{2\cdot 2\cdot 2\log(60)} \leq 0.1
\end{aligned}$$

lässt sich die Höhe durch

$$H\left(\frac{n_3\varepsilon_3}{n_1\varepsilon_1}\right) \leq \exp\{c_9\Phi\log^*\mathcal{P}\}$$

mit $c_9 := 1.1s$ abschätzen.

An dieser Stelle verwendet Herrmann die Abschätzung $c_9' = 1.1s((s-1)!)^2\delta_d^{2-s}$, was aber offensichtlich größer und somit ungünstiger ist.

Sei nun

$$B \geq \Phi\frac{(\log^*\mathcal{P})}{c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2}.$$

Um den zweiten Teil des Satzes 2.6 anwenden zu können setzt man

$$\delta := \frac{\Phi\log^*\mathcal{P}}{B(c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2)}, \quad \Psi := c_{Yu}(s_1+s_2-1)d^{2(s_1+s_2)}\Phi =: k_0\Phi$$

und erhält damit

$$\begin{aligned}
&\Psi\log\left(\frac{B(c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2)}{\Phi\log^*\mathcal{P}\log A_0}\Psi\right) \\
=\ & \Psi\log\left(k_0\frac{B(c_{L_2}(d_1,s_1)\mathcal{R}_1 + c_{L_2}(d_2,s_2)\mathcal{R}_2)}{\log^*\mathcal{P}\log A_0}\right).
\end{aligned}$$

Aus $\log A_0 \geq \log \mathcal{H} > (c_{L_2}(d_1, s_1)\mathcal{R}_1 + c_{L_2}(d_2, s_2)\mathcal{R}_2)$ folgt

$$\Psi \log \left(k_0 \frac{B(c_{L_2}(d_1, s_1)\mathcal{R}_1 + c_{L_2}(d_2, s_2)\mathcal{R}_2)}{\log^* \mathcal{P} \log A_0} \right) < \Psi \log(k_0 B).$$

Daraus ergibt sich

$$\begin{aligned} \left| \frac{\varepsilon_3 n_3}{\varepsilon_1 n_1} \right|_\nu &\geq \exp\{-c_{Yu}(2s-1)d^{4s}\Phi d \log^* \mathcal{P} \log(k_0 B)\} \\ &\geq \exp\{-0.9 c_{Yu}(2s-1)d^{4s+1} \log(c_{Yu}(2s-1)d^{4s})\Phi \log^* \mathcal{P} \log B\}. \end{aligned}$$

Des weiteren ist:

$$\frac{2sd \log \mathcal{H}}{0.9(s-1)\Phi c_{Yu}(2s-1)d^{4s+1} \log(c_{Yu}(2s-1)d^{4s})} \leq 0.1.$$

Da ν so gewählt ist, dass $\left|\frac{\varepsilon_3}{\varepsilon_1}\right|_\nu$ minimal, gilt

$$H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) \leq \left| \frac{\varepsilon_3 n_3}{\varepsilon_1 n_1} \right|_\nu^{\frac{-(s-1)}{d}} \leq \exp\{c_{10}\Phi \log^* \mathcal{P} \log B\}$$

mit $c_{10} = \frac{s-1}{d} c_{Yu}(2s-1)d^{4s+1} \log(c_{Yu}(2s-1)d^{4s})$.
Aus den einzelnen Fällen für $\nu \nmid \infty$ erhält man also folgende Abschätzungen:

$$\begin{aligned} H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) &\leq \exp\{c_8 \Phi \log^* \mathcal{P} \log B\}, \\ H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) &\leq \exp\{c_9 \Phi \log^* \mathcal{P}\}, \\ H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) &\leq \exp\{c_{10} \Phi \log^* \mathcal{P} \log B\}. \end{aligned}$$

Es bleibt nun eine gemeinsame obere Schranke für alle Fälle zu finden. Dabei vergleiche ich zuerst die drei Fälle mit $\nu \nmid \infty$ und danach die mit $\nu|\infty$.

Offensichtlich ist c_9 kleiner als c_8 und c_{10}. Deshalb müssen nur diese beiden untereinander verglichen werden. Es gilt

$$c_{10} = \frac{\log(c_{Yu}(2s-1)d^{4s})}{1.3} c_8.$$

Da aber $c_{Yu}(2s-1)$ schon im kleinsten Fall, für $s = 2$ und $d = 2$, größer als $10^3 \cdot 9$ ist, ist c_{10} damit größer als c_8. D.h.

$$H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) \leq \exp\{c_{10} \log^* \Phi \mathcal{P} \log B\}$$

gilt in allen drei Fällen.

Mit Hilfe aller bisherigen Ergebnisse lässt sich nun auch Φ weiter abschätzen:

$$\begin{aligned}
\Phi &= \frac{\mathcal{P}^d}{(\log^* \mathcal{P})^{s_1+s_2}} \log A_0 \left(\prod_{i=1}^{s_1+s_2-2} \log A_i \right) \log(10(s_1+s_2-1)d\log(A)) \\
&\leq \frac{\mathcal{P}^d}{(\log^* \mathcal{P})^{s_1+s_2}} (2\delta_d^{1-s} \log \mathcal{H} + \log^* \mathcal{P}) c_6 \mathcal{R}_1 \mathcal{R}_2 (\log^* \mathcal{P})^{s_1+s_2-2} \\
&\quad \cdot \log((20s-10)dc_7 \max\{\mathcal{R}_1, \mathcal{R}_2\}) \\
&\leq \mathcal{P}^d (\log^* \mathcal{P})^{-1} 2\delta_d^{1-s} \log \mathcal{H} c_6 \mathcal{R}_1 \mathcal{R}_2 (\log((20s-10)dc_7 \max\{\mathcal{R}_1, \mathcal{R}_2\})).
\end{aligned}$$

Um auch den Fall $\nu|\infty$ einzubeziehen, sei $c_{11} := \max\{c_{10}, c_5\}$. Dann lässt sich auch $H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right)$ abschätzen:

$$\begin{aligned}
H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) &\leq \exp\{c_{11} c_6 \mathcal{P}^d 2\delta_d^{1-s} \log \mathcal{H} \log((20s-10)dc_7) \\
&\quad \cdot \log(\max\{\mathcal{R}_1, \mathcal{R}_2\}) \mathcal{R}_1 \mathcal{R}_2 \log B\}.
\end{aligned}$$

Wegen $B \leq c_2 \log^* \max\{H(\varepsilon_1), H(\varepsilon_2)\}$ folgt schließlich

$$\begin{aligned}
H\left(\frac{\varepsilon_3 n_3}{\varepsilon_1 n_1}\right) &\leq \exp\{c_6 \cdot c_{11} \log c_2 \mathcal{P}^d 2\delta_d^{1-s} \log((20s-10)dc_7) \mathcal{R}_1 \mathcal{R}_2 \\
&\quad \cdot \log(\max\{\mathcal{R}_1, \mathcal{R}_2\}) \log \mathcal{H} \log^* \log^* \max\{H(\varepsilon_1), H(\varepsilon_2)\} \\
&= \exp\{c(d,s) \frac{\mathcal{P}^d}{\log^* \mathcal{P}^2} \mathcal{R}_1 \mathcal{R}_2 \log(\max\{\mathcal{R}_1, \mathcal{R}_2\}) \log \mathcal{H} \\
&\quad \cdot \log^* \log^* \max\{H(\varepsilon_1), H(\varepsilon_2)\}
\end{aligned}$$

mit $c(d,s) = c_6 \cdot c_{11} \log c_2 2\delta_d^{1-s} \log((20s-10)dc_7) \log^* \mathcal{P}^2$.

□

2.2.3 Schranken für $h_n(P)$

Um nun eine Schranke $N \geq h_n(P)$ zu bestimmen, werden einige Körpererweiterungen definiert. Sei die elliptische Kurve

$$y^2 = f(x) = x^3 + a_2 x^2 + a_4 x + a_6 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \in \mathbb{Z}_{\mathbb{K}}[x]$$

mit den Nullstellen $\alpha_1, \alpha_2, \alpha_3$ des Polynoms $f(x)$ gegeben. Setze $x = \frac{X}{z}$ mit $X, z \in \mathbb{Z}_{\mathbb{K}}$. Dann gibt es für $1 \leq i \leq 3$ die Darstellung $X - z\alpha_i = \kappa_i' \xi_i'^2$ mit $\kappa_i' \in \mathbb{Z}_{\mathbb{K}}$ und $\xi_i' \in \mathbb{K}_i$, vgl. [Her02]. Setze dann $\kappa_i := \varepsilon^2 \kappa_i'$ und $\xi_i := \frac{\xi_i'}{\varepsilon}$, wobei $\varepsilon \in \mathbb{Z}_{\mathbb{K}}$ eine Einheit ist. Definiere nun für $1 \leq i, j \leq 3$:

- f_i sei das Minimalpolynom von α_i über $\mathbb{K}$,
- $\mathbb{K}_i = \mathbb{K}(\alpha_i)$,
- $\mathbb{K}_{ij} = \mathbb{K}_i(\alpha_j)$ für $i \neq j$,
- $\mathbb{L}_{ij} = \mathbb{K}_{ij}(\sqrt{\kappa_i\kappa_j})$,
- $\mathbb{M} = \mathbb{K}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3})$.

Für diese Körper gelten die folgenden Abschätzungen:

- $[\mathbb{K}_{ij} : \mathbb{K}_i] \leq 3$,
- $[\mathbb{L}_{ij} : \mathbb{Q}] \leq 12d$,
- $[\mathbb{M} : \mathbb{Q}] \leq 24d$.

Herrmann leitet in [Her02] daraus folgende Gleichungen her:

$$\begin{array}{rclcrcl} \tau_1 + \tau_2 & = & b_3\varepsilon_3 & \text{und} & \tau_1 - \tau_2 & = & g_3\delta_3 \\ \tau_1 + \tau_3 & = & b_2\varepsilon_2 & \text{und} & \tau_1 - \tau_3 & = & g_2\delta_2 \\ \sqrt{\kappa_3/\kappa_1}(\tau_2 + \tau_3) & = & b_1'\varepsilon_1 & \text{und} & \sqrt{\kappa_3/\kappa_1}(\tau_2 - \tau_3) & = & g_1'\delta_1. \end{array}$$

wobei $\tau_1 = \kappa_1\xi_1$, $\tau_2 = \sqrt{\kappa_1\kappa_2}\xi_2$, $\tau_3 = \sqrt{\kappa_1\kappa_3}\xi_3$; ε_i, δ_i sind S_{jk}-Einheiten in $\mathbb{L}_{jk}$, $1 \leq i, j, k \leq 3$, paarweise verschieden. Herrmann gibt dabei auch eine gemeinsame Schranke für die Höhe von $b_1', b_2, b_3, g_1', g_2, g_3$ an.

Setzt man $b_1 = \sqrt{\kappa_1/\kappa_3}b_1'$ und $g_1 = \sqrt{\kappa_1/\kappa_3}g_1'$, so kann man die letzten beiden Gleichungen auch schreiben als $\tau_2 + \tau_3 = b_1\varepsilon_1$ und $\tau_2 - \tau_3 = g_1\delta_1$. Entsprechend muss man die Abschätzung der Höhe anpassen mit Hilfe der Beziehung $H(b_1) = H(b_1')(H(\kappa_1)H(\kappa_3))^{1/2}$.

Satz 2.11. *Für $i = 2, 3$ gilt*

$$\begin{aligned} H(b_i), H(g_i) &\leq (e^{12}D_{\mathbb{K}}^{24}|N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|^{12})^{1/d} \exp\{12t \max_{j,k}\{h_{\mathbb{L}_{j,k}}\} \log^* \mathcal{P} \\ &\quad + c_a(12d, 12d-1) \max_{j,k}\{\mathcal{R}_{\mathbb{L}_{j,k}}\}\} \\ H(b_1), H(g_1) &\leq (e^{15}|D_{\mathbb{K}}|^{57/2}|N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|^{14})^{1/d} \exp\{12t \max_{j,k}\{h_{\mathbb{L}_{j,k}}\} \log^* \mathcal{P} \\ &\quad + c_{12}(d)c_a(12d, 12d-1) \max_{i,j}\{\mathcal{R}_{\mathbb{L}_{j,k}}\}\}. \end{aligned}$$

Dabei ist $c_a(d, r_{\mathbb{K}}) = \frac{1}{2}r_{\mathbb{K}}^{r_{\mathbb{K}}+1}\delta_d^{-(r_{\mathbb{K}}-1)}$ und $c_{12}(d) = 2^2 3^{12d-1} d^{12d-2}(3d-1)^{3d}\delta_{3d}^{-(3d-2)}$, wobei $r_{\mathbb{K}}$ der Einheitenrang und $h_{\mathbb{K}}$ die Klassenzahl von $\mathbb{K}$ ist.

Beweis: [Her02] □

Im Folgenden wird nun schließlich der Satz 2.3 hergeleitet.

Herrmann gibt eine Darstellung für z an: $z = \eta^{-2} z_3$, wobei $z_3 \in \mathbb{Z}_{\mathbb{K}}$ und die Höhe von z_3 beschränkt und η eine S-Einheit ist. Sei $S_{\mathbb{M}}$ die Menge aller Fortsetzungen der Stellen aus S auf $\mathbb{M}$. Die Mächtigkeit von $S_{\mathbb{M}}$ ist dann wegen $[\mathbb{M} : \mathbb{Q}] \leq 24d$ durch $24(d+t)$ begrenzt.

Subtrahiert und addiert man die zuvor angegebenen Gleichungen, so dass sich die τ_i gerade aufheben, und multipliziert man das Ergebnis mit η, so erhält man folgende $S_{\mathbb{M}}$-Einheiten-Gleichungen:

$$\begin{aligned} b_1\varepsilon_1\eta - b_2\varepsilon_2\eta + g_3\delta_3\eta &= 0, \\ b_1\varepsilon_1\eta + g_2\delta_2\eta - b_3\varepsilon_3\eta &= 0, \\ g_1\delta_1\eta + b_2\varepsilon_2\eta - b_3\varepsilon_3\eta &= 0, \\ g_1\delta_1\eta - g_2\delta_2\eta + g_3\delta_3\eta &= 0. \end{aligned}$$

Sei nun

$$H_{\max} := \max_{i,j} \left\{ H\left(\frac{b_i\varepsilon_i}{b_j\varepsilon_j}\right), H\left(\frac{g_i\delta_i}{b_j\varepsilon_j}\right), H\left(\frac{b_i\varepsilon_i}{g_j\delta_j}\right), H\left(\frac{g_i\delta_i}{g_j\delta_j}\right) \right\}.$$

Dann gilt mit Lemma 2.10 die Abschätzung

$$\begin{aligned} H_{\max} \leq\ & \exp\{c(24d, 24(d+t)) \frac{\mathcal{P}^{24d}}{(\log^* \mathcal{P})^2} \max\{\mathcal{R}_{S_{12}}, \mathcal{R}_{S_{13}}, \mathcal{R}_{S_{23}}\}^2 \\ & \cdot \log^* \max\{\mathcal{R}_{S_{12}}, \mathcal{R}_{S_{13}}, \mathcal{R}_{S_{23}}\} \\ & \cdot \log \max\{H(b_1), H(b_2), H(b_3), H(g_1), H(g_2), H(g_3)\} \\ & \cdot \log^* \log^* \max\{H(\varepsilon_1\eta), H(\varepsilon_2\eta), H(\delta_1\eta), H(\delta_2\eta)\}\}. \end{aligned}$$

Die S_{ij}-Regulatoren lassen sich dabei folgendermaßen abschätzen: Für die Diskriminante des Körpers $\mathbb{L}_{ij}$ gibt Herrmann die Abschätzung

$$|D_{\mathbb{L}_{ij}}| \leq 2^{12d} e^{12} |D_{\mathbb{K}}|^{30} |N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|^{20}$$

an. Sei nun $M_1 := \left(\frac{2}{\pi}\right)^{6d} 2^{6d} e^6 |D_{\mathbb{K}}|^{15} |N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|^{10}$. Nach Lemma 2.8 gilt dann

$$h_{\mathbb{L}_{ij}} \mathcal{R}_{\mathbb{L}_{ij}} \leq M_1 \frac{(\log M_1)^{6d-1} (12d - 1 + \log M_1)^{6d}}{(12d-1)!} =: M_2.$$

Damit lassen sich die S-Regulatoren durch Lemma 2.7 abschätzen:

$$\max_{i,j}\{\mathcal{R}_{S_{ij}}\} \leq \max_{i,j}\{h_{\mathbb{L}_{ij}} \mathcal{R}_{\mathbb{L}_{ij}}\} (12d \log^* \mathcal{P})^{12dt} \leq M_2 (12d \log^* \mathcal{P})^{12dt}.$$

Damit lässt sich die Abschätzung für $H_{\max}$ schreiben als

$$H_{\max} \leq \exp\{T_1 \cdot E\}$$

mit

$$\begin{aligned} E &:= \log^* \log^* \max\{H(\varepsilon_1\eta), H(\varepsilon_2\eta), H(\delta_1\eta), H(\delta_2\eta)\}, \\ T_1 &\leq 30c_{13}(15\log(e|D_{\mathbb{K}}||N_{\mathbb{K}/\mathbb{Q}}(\Delta_f)|) + c_{12}(d)c_a(12d, 12d-1)M_2 + \\ &\quad +60tM_2 \log^* \mathcal{P}), \end{aligned}$$

wobei

$$c_{13} := c(24d, 24(d+t))\frac{\mathcal{P}^{24d}}{(\log^* \mathcal{P})^2} M_2^2 (12d \log^* \mathcal{P})^{24dt} \log^*(M_2(12\log^* \mathcal{P})^{12dt}).$$

Um nun eine Abschätzung für E zu erhalten, stellt Herrmann in [Her02] zunächst die Ungleichung

$$H(\varepsilon_1\eta) \leq 4\sqrt{H_f}\exp\{T_2 E\}$$

mit $T_2 = \frac{31}{30}T_1$ auf. Diese gilt ebenfalls für $H(\varepsilon_2\eta)$, $H(\delta_1\eta)$, und $H(\delta_2\eta)$. Herrmann führt nun eine weitere Abschätzung der Konstanten T_2 durch, die aber nicht notwendig ist und das Ergebnis nur unnötig vergrößert. Deshalb werde ich sie nicht verwenden. Für E gilt nun:

$$\exp\{\exp\{E\}\} = \max\{H(\varepsilon_1\eta), H(\varepsilon_2\eta), H(\delta_1\eta), H(\delta_2\eta)\} \leq 4\sqrt{H_f}\exp\{T_2 E\}$$

und damit, wegen $\log 4 < \log H_f$,

$$\exp\{E\} \leq T_2 E + 2\log H_f.$$

Da $\exp\{E\} - T_2 E - 2\log H_f$ monoton wachsend in E ist, nimmt E im Fall der Gleichheit $\exp\{E\} = T_2 E + 2\log H_f$ den maximalen Wert an. Man definiert nun F so, dass $E = \log F$. Dann kann man obige Ungleichung im Fall der Gleichheit auch schreiben als

$$F = T_2 \log F + 2\log H_f.$$

Aus Lemma 2.9 folgt dann, da $T_2 > \exp\{2\}$, dass

$$F < 2(2\log H_f + T_2 \log T_2)$$

Damit gilt für E:

$$E \leq \log 2 + \log(2\log H_f + T_2 \log T_2).$$

Um nun wieder zu einer Abschätzung für $H(x)$ zurück zu kommen, setzt man $\gamma := \frac{b_3\varepsilon_3}{g_3\delta_3}$.
Dann gilt

$$\begin{aligned} (\tau_1 + \tau_2) + (\tau_1 - \tau_2) &= (\tau_1 - \tau_2) + b_3\varepsilon_3 = (\tau_1 - \tau_2)(1 + \frac{b_3\varepsilon_3}{g_3\delta_3}) \\ \Leftrightarrow \qquad 2\tau_1 &= (\tau_1 - \tau_2)(1+\gamma) \end{aligned}$$

und analog

$$2\tau_1 = (\tau_1 + \tau_2)(1 + \gamma^{-1}).$$

Das Produkt dieser beiden Gleichungen ergibt dann

$$4\tau_1^2 = (\tau_1^2 - \tau_2^2)(1 + \gamma)(1 + \gamma^{-1}).$$

Da nach Definition gilt $(X - z\alpha_1) = \kappa_1\xi_1^2$, $\tau_1 = \kappa_1\xi_1$ und $\kappa_1(\alpha_2 - \alpha_1)z = \tau_1^2 - \tau_2^2$, gilt auch die Gleichung

$$4(X - z\alpha_1) = (\alpha_2 - \alpha_1)z(1 + \gamma)(1 + \gamma^{-1})$$

und damit

$$x = \frac{X}{z} = \alpha_1 + \frac{1}{4}(1 + \gamma)(1 + \gamma^{-1})(\alpha_2 - \alpha_1).$$

Damit folgt für die Höhe von x

$$H(x) \leq 2H(\alpha_1)8H(\alpha_2)H(\alpha_1)4H(\gamma)^2 \leq 2^6 \prod_{i=1}^{3} H(\alpha_i)^2 H(\gamma)^2.$$

Die Höhe von γ lässt sich abschätzen durch

$$H(\gamma)^2 \leq H\left(\frac{b_3\varepsilon_3}{g_1\delta_1} \cdot \frac{g_1\delta_1}{g_3\delta_3}\right) \leq \exp\{2T_1E\}.$$

Damit gilt insgesamt

$$H(x) \leq 2^{12} H_f^2 \exp\{2T_1(\log 2 + \log(2\log H_f + T_2 \log T_2))\}.$$

Nun lässt sich die Schranke $N \geq h_n(x)$ mit Hilfe des Zusammenhanges zwischen H und h_n angeben durch

$$N := \sqrt{\frac{u_2 + 12\log 2 + 2\log H_f + 2T_1(\log 2 + \log(2\log H_f + T_2 \log T_2))}{\lambda_{\min}}}.$$

Damit ist das Ziel dieses Kapitels, Satz 2.3 zu beweisen, erreicht. □

Kapitel 3

Reduktion der Schranken

Im vorherigen Kapitel wurde eine Schranke hergeleitet für die Koeffizienten $n_i,\ i = 1, \ldots, r$, eines Punktes einer elliptischen Kurve E in der Darstellung

$$P = n_1 B_1 + n_2 B_2 + \cdots n_r B_r + T$$

wobei die $B_i,\ i = 1, \ldots, r$, eine Mordell-Weil-Basis von E bilden und T ein Torsionspunkt ist. Diese Schranke hängt von der gegebenen Stellenmenge S und der Kurve E ab, wird aber zumeist sehr groß, oft größer als 10^{1000}. Das Ziel dieses Kapitels ist es, die Anzahl der Möglichkeiten so weit einzuschränken, dass die S-ganzen Punkte durch Ausprobieren gefunden werden können. Die Schranken müssen deshalb deutlich verkleinert werden. Zur Reduktion verwendet man den LLL-Algorithmus. Hierbei benötigt man aber ein diophantisches Approximationsproblem. Um das zu erhalten werden im Fall der unendlichen Stellen elliptische Logarithmen und im Fall der endlichen Stellen p-adische elliptische Logarithmen oder pseudo p-adische elliptische Logarithmen verwendet, um Linearformen aufzustellen. Diese haben den Vorteil, dass die Linearität der Darstellung von P erhalten bleibt und der unendlich ferne Punkt $\mathcal{O}_E$ auf die Null abgebildet wird. Dazu muss zunächst noch ein direkter Zusammenhang zwischen der x-Koordinate des Punktes und der Schranke N angegeben werden. In Kapitel 1 ist folgender Zusammenhang angegeben:

$$\lambda_{\min} h_n^2 - h(P) \leq \hat{h}(P) - h(P) \leq c_2.$$

Sei $\mathfrak{p} \in S$ so gewählt, dass

$$|x|_{\mathfrak{p}}^{n_p} = \max_{\nu \in S} \{|x|_\nu^{n_\nu}\}.$$

Dann gilt

$$H(P) = \left(\prod_{\nu \in M_{\mathbb{K}}} \max\{1, |x|_\nu\}^{n_\nu} \right)^{1/d} \leq |x|_{\mathfrak{p}}^{s n_{\mathfrak{p}}/d},$$

wobei $M_{\mathbb{K}}$ die Menge aller Stellen im Zahlkörper $\mathbb{K}$ und d der Grad von $\mathbb{K}$ über $\mathbb{Q}$ bezeichnet. Sei außerdem $N = h_n(P)$ für einen gegebenen S-ganzen Punkt P. Dann gilt weiterhin

$$H(P) = \exp\{h(P)\} \leq |x|_{\mathfrak{p}}^{sn_{\mathfrak{p}}/d}.$$

Dies ist äquivalent zu

$$\frac{1}{|x|_{\mathfrak{p}}^{sn_{\mathfrak{p}}/d}} \leq \exp\{-h(P)\} \leq \exp\{c_2 - \lambda_{\min} N^2\}.$$

Damit lässt sich der folgende Satz formulieren, vgl [Her02]:

Satz 3.1.

$$\frac{1}{|x|_{\mathfrak{p}}} \leq \exp\{-c_{14}N^2 + c_{15}\}$$

mit

$$c_{14} := d\frac{\lambda_{\min}}{sn_{\mathfrak{p}}}, \quad \textit{und} \quad c_{15} := d\frac{c_2}{sn_{\mathfrak{p}}}.$$

Da nicht bekannt ist, bezüglich welcher Stelle der $\mathfrak{p}$-adische Betrag von x das Maximum annimmt und damit die Ungleichung in Satz 3.1 gilt, wird die Reduktion für alle Stellen aus S einzeln durchgeführt und anschließend das Maximum der reduzierten Werte bestimmt. Dabei wird bei der Reduktion nach unendlichen Stellen, endlichen Stellen über $\mathbb{K}_{\mathfrak{p}} = \mathbb{Q}_{\mathfrak{p}}$ und endlichen Stellen über dem Zahlkörper $\mathbb{K}_{\mathfrak{p}} \neq \mathbb{Q}_{\mathfrak{p}}$ unterschieden. Der letzte Fall ist der problematischste, da bei ihm die p-adischen elliptischen Logarithmen zum Einsatz kommen, deren Berechnung speziell im Zahlkörperfall bei großer Stellenzahl schwierig ist.

3.1 Grundlagen zur LLL-Reduktion

Vgl. [Sma98]. Zum Bestimmen S-ganzer Punkte ist es notwendig, aus einer Schranke für den Betrag einer Linearform auf eine Abschätzung für die Unbekannten schließen zu können. Es sei

$$L(\vec{x}) = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n,\ \alpha_i \in \mathbb{R},$$

eine Linearform mit den Unbekannten $\vec{x} = (x_1, \ldots, n_n) \in \mathbb{Z}^n$. Diese heißt homogen falls $\alpha_0 = 0$ und sonst inhomogen. Nun interessiert eine Abschätzung für $\vec{x}$ in Abhängigkeit von $|L(\vec{x})|$. Zu jeder solchen Linearform gibt es eine Matrix

$$A = \begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ \alpha_1 & \cdots & \alpha_{n-1} & \alpha_n \end{pmatrix}.$$

Möchte man gleichzeitig sowohl den Wert von $|L(\vec{x})|$ als auch die Norm von $\vec{x}$ minimieren, so bedeutet das nichts anderes, als ein x zu finden, das möglichst genau eine Lösung der Gleichung

$$A\vec{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\alpha_0 \end{pmatrix}$$

approximiert. Durch die Gleichungen $x_i = 0,\ i = 1, \ldots, n-1$, der ersten $n-1$ Zeilen werden die x_i sehr klein. Die Größe der n-ten Komponente wird dabei nicht berücksichtigt. Damit die Determinante der Matrix die richtige Größenordnung hat, wird die letzte Zeile mit einem Faktor C gewichtet. Man verwendet also die Matrix

$$A = \begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ [C\alpha_1] & \cdots & [C\alpha_{n-1}] & [C\alpha_n] \end{pmatrix}.$$

Dabei steht $[\cdot]$ für die Rundung einer Zahl. Betrachtet man nun die Menge $\{A\vec{x} : \vec{x} \in \mathbb{Z}\}$, so erhält man ein Gitter, das sogenannte Approximationsgitter. Im homogenen Fall $\alpha_0 = 0$ entspricht unser Problem dann der Suche nach dem kleinsten Gittervektor. Möchte man gleichzeitig mehrere Linearformen zusammen mit $\vec{x}$ minimieren, so lässt sich das entsprechend über die Matrix

$$A = \begin{pmatrix} 1 & & 0 & \cdots & 0 \\ & \ddots & & & \\ 0 & & 1 & & 0 \\ [C\alpha_{1,1}] & \cdots & [C\alpha_{1,n-m}] & \cdots & [C\alpha_{1,n}] \\ \vdots & & \vdots & & \vdots \\ [C\alpha_{m,1}] & \cdots & [C\alpha_{m,n-m}] & \cdots & [C\alpha_{m,n}] \end{pmatrix}$$

beschreiben. Daraus lässt sich dann auch sofort die Matrix für eine komplexe Linearform ableiten, indem man diese in ihren Imaginärteil und Realteil aufspaltet.

Definition 3.2. Die Basis $\{\vec{b_1}, \ldots, \vec{b_n}\}$ eines Gitters heißt *LLL-reduziert*, wenn für die zugehörige Gram-Schmidt-Basis $\{\vec{b}_1^*, \ldots, \vec{b}_n^*\}$ und die bei der Berechnung auftretenden Konstanten $\mu_{i,j}$ gilt:

1.
$$|\mu_{i,j}| \leq 1/2,\ 1 \leq j < i \leq n,$$

2.
$$\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\vec{b}_{i-1}^*\|^2,\ 1 < i \leq n.$$

Eine solche reduzierte Basis kann leicht mit Hilfe des LLL-Algorithmus berechnet werden.

Bezeichne $d(\vec{y}, \mathcal{L})$ den Abstand von $\vec{y}$ zum Gitter $\mathcal{L}$ oder die Länge des kürzesten Gittervektors, falls $\vec{y}$ bereits selbst im Gitter liegt. $d(\vec{y}, \mathcal{L})$ lässt sich beispielsweise durch die Länge des kürzesten Gittervektors nach unten abschätzen:

Satz 3.3. *Sei $\{\vec{b}_1, \ldots, \vec{b}_n\}$ eine Basis des Gitters $\mathcal{L}$ und $\{\vec{b}_1^*, \ldots, \vec{b}_n^*\}$ eine reduzierte Gitterbasis. Dann gilt:*

$$d(\vec{y}, \mathcal{L}) = \begin{cases} \min_{\vec{x}\in\mathcal{L}} \|\vec{x} - \vec{y}\| & \geq & c_1^{-1}[\sigma_{i_0}]\|\vec{b}_1\|^2, & \textit{falls } \vec{y} \notin \mathcal{L} \\ \min_{\vec{x}\in\mathcal{L}} \|\vec{x}\| & \geq & c_1^{-1}\|\vec{b}_1\|, & \textit{falls } \vec{y} \in \mathcal{L}, \end{cases}$$

wobei
$$c_1 := \max_{1\leq i\leq n} \left\{ \frac{\|\vec{b}_1\|^2}{\|\vec{b}_i^*\|^2} \right\},$$
$$\vec{\sigma} = (\vec{b}_1, \cdots, \vec{b}_n)^{-1}\vec{y}$$

und i_0 der größte Index mit $[\sigma_{i_0}] \neq 0$ ist.

Beweis: [Sma98] □

Von dem LLL-Algorithmus gibt es verschiedene Varianten. Da der LLL-Algorithmus nur auf Gitter aus $\mathbb{Z}^n$ angewendet werden soll, verwendet man die Variante von de Weger [de 89], siehe Algorithmus 6.

Um eine Linearform abzuschätzen, geht man von folgender Situation aus: Angenommen in der Ungleichung

$$|\alpha_0 + \sum_{i=1}^{n} x_i\alpha_i| \leq c_2 \exp\{-c_3 H^q\}$$

sind die Konstanten $q \in \mathbb{N}$ und $c_2, c_3 \in \mathbb{R}_{\geq 0}$ bereits bekannt. Die $\alpha_i,\ i = 0, \ldots, n$, sind durch die Linearform gegeben. Seien $x_1, \ldots, x_n$ jeweils durch $|x_i| \leq X_i$ begrenzt. Ziel ist es nun, eine obere Grenze für H zu bestimmen. Dazu ordnet man zunächst wieder der Linearform eine Approximationsmatrix zu. Diese wird LLL-reduziert. Der erste Spaltenvektor gibt dann eine gute Abschätzung für den kürzesten Gittervektor $c_4 := \|b_1^*\|$ an.

Satz 3.4. *Sei c_4 die Länge des kürzesten Basisvektors in einem LLL-reduzierten Gitter.*

- *Ist $\alpha_i \in \mathbb{R}$ für $i = 0, \cdots, n$, dann sei $S = \sum_{i=1}^{n-1} X_i^2$ und $T = (1 + \sum_{i=1}^{n} X_i)/2$.*
- *Ist $\alpha_i \in \mathbb{C}$ für $i = 0, \cdots, n$, dann sei $S = \sum_{i=1}^{n-2} X_i^2$ und $T = (1 + \sum_{i=1}^{n} X_i)/\sqrt{2}$.*

Falls $c_4^2 \geq T^2 + S$, dann gilt

$$H \leq \sqrt[q]{\frac{1}{c_3}\left(\log(Cc_2) - \log\left(\sqrt{c_4^2 - S} - T\right)\right)}$$

oder

- *über $\mathbb{R}$: $x_1 = \cdots = x_{n-1} = 0$ und $x_n = -[C\alpha_0]/[C\alpha_n]$*
- *über $\mathbb{C}$: $x_1 = \cdots = x_{n-1} = 0$ und $x_n[C\mathrm{Re}(\alpha_{n-1})] + x_n[C\mathrm{Re}(\alpha_n)] = [C\mathrm{Re}(\alpha_0)]$, $x_n[C\mathrm{Im}(\alpha_{n-1})] + x_n[C\mathrm{Im}(\alpha_n)] = [C\mathrm{Im}(\alpha_0)]$.*

Beweis: [Sma98] □

Dabei wählt man C in der Größenordnung X_0^n für den rein reellen und $X_0^{n/2}$ für den komplexen Fall, damit das Ergebnis des LLL-Algorithmus, c_4, möglichst die Voraussetzungen erfüllt. Ist dies aber trotzdem nicht der Fall und c_4 zu klein, so vergrößert man C in der Approximationsmatrix und versucht es erneut solange, bis die Bedingung erfüllt ist.

Über p-adischen Zahlkörpern geht man analog vor, um eine Abschätzung für H aus der Ungleichung $|\alpha_0 + \sum_{i=1}^{n} x_i\alpha_i|_p \leq c_2 \exp\{-c_3 H^q\}$ zu erhalten. Dabei unterscheidet man, ob die Koeffizienten der Linearform, α_i, aus $\mathbb{Z}_p$ oder $\mathbb{Q}_p(\theta)$ sind.

Angenommen, alle α_i sind aus $\mathbb{Z}_p$ und alle x_i sind jeweils durch eine Schranke X_i beschränkt. Dann bestimmt man zunächst eine Konstante $u \in \mathbb{Z}$, so dass $p^u \geq X_0^{n+1}$. Damit soll erreicht werden, dass die Norm des ersten Gittervektors nach der Reduktion nicht zu klein ausfällt. Sei $\alpha \equiv \alpha^{\{u\}} \bmod p^u$ mit $\alpha^{\{u\}} \in [0, \ldots, p^u - 1]$. Dann lässt sich die Approximationsmatrix festlegen durch

$$A = \begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ \alpha_1^{\{u\}} & \cdots & \alpha_m^{\{u\}} & p^u \end{pmatrix}.$$

Der Vektor, der möglichst genau in dem Gitter dargestellt werden soll, ist dann

$$\vec{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\alpha_o^{\{u\}} \end{pmatrix}.$$

Durch LLL-Reduktion lässt sich eine Abschätzung für H mit Hilfe des folgenden Satzes bestimmen:

Satz 3.5. *Falls $d(\vec{y}, \mathcal{L}) > \sqrt{n}X_0$, dann gilt*

$$H < \sqrt[q]{\left(u + \frac{\log c_2}{\log p}\right)\frac{\log p}{\log c_3}}$$

oder $x_1 = \cdots = x_n = 0$.

Beweis: [Sma98] □

Im allgemeinen Fall, also wenn $\alpha_i \in \mathbb{Q}_p(\theta)$, zerlegt man das Problem zunächst in mehrere Ungleichungen über $\mathbb{Q}_p$ und führt diese dann auf den ersten Fall $\alpha_i \in \mathbb{Z}_p$ zurück. Sei θ eine ganze, p-adisch algebraische Zahl und $m = [\mathbb{Q}_p(\theta) : \mathbb{Q}_p]$ der Grad der Körpererweiterung. Die Zerlegung erfolgt mit Hilfe des folgenden Lemmas:

Lemma 3.6. *Seien $\alpha_i = \sum_{j=0}^{m-1} \alpha_{i,j}\theta^j$ für alle $i = 1, \ldots, n$, mit $\alpha_{i,j} \in \mathbb{Q}$. Falls*

$$v_p\left(\alpha_0 + \sum_{i=1}^{n} x_i\alpha_i\right) \geq \frac{c_3}{\log p}H - \frac{c_2}{\log p}$$

dann gilt für alle $j = 1, \ldots, m$, dass

$$v_p\left(\alpha_{0,j} + \sum_{i=1}^{n} x_i\alpha_{i,j}\right) \geq \frac{c_3}{\log p}H - \frac{c_2}{\log p} - 1/2v_p(\Delta(\theta)),$$

wobei $\Delta(\theta)$ die Diskriminante von θ ist.

Beweis: [Sma98] □

Um nun die Ungleichung auf den Fall $\alpha_i \in \mathbb{Z}_p$ zurückzuführen, definiert man zunächst die Konstante λ, so dass

$$v_p(\lambda) = \min_{1 \leq i \leq n}\left(\min_{0 \leq j \leq m-1}(v_p(\alpha_{i,j}))\right).$$

Nimmt man an, dass $v_p(\lambda) \leq v_p(\alpha_{0,i})$, so folgt, dass

$$\beta_{i,j} = \frac{\alpha_{i,j}}{\lambda} \in \mathbb{Z}_p.$$

Betrachtet man statt des Gitters $\mathcal{L}$ das Gitter $\mathcal{L}/\lambda$, so erhält man eine Linearform über $\mathbb{Z}_p$. Damit wird das System von Ungleichungen zu

$$v_p(\beta_{0,j} + \sum_{i=1}^{n} x_i \beta_{i,j}) \geq \frac{c_3}{\log p} H - \frac{\log c_2}{\log p} - \frac{1}{2} v_p(\Delta(\theta)) - v_p(\lambda)$$

Dann ist die zugehörige Approximationsmatrix durch

$$A = \begin{pmatrix} 1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & 0 & \dots & 0 \\ \beta_{1,0}^{\{u\}} & \dots & \beta_{n,0}^{\{u\}} & p^u & & 0 \\ \vdots & & \vdots & & \ddots & \\ \beta_{1,m-1}^{\{u\}} & \dots & \beta_{n,m-1}^{\{u\}} & 0 & & p^u \end{pmatrix}$$

gegeben und der Vektor, der möglichst genau approximiert werden soll, ist

$$\vec{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\beta_{0,0}^{\{u\}} \\ \vdots \\ -\beta_{0,m-1}^{\{u\}} \end{pmatrix}.$$

Ist $v_p(\lambda) > v_p(\alpha_{0,i})$ für mindestens ein i, so kann man direkt, ohne eine Approximationsmatrix zu berechnen, eine Schranke für H angeben. Für diesen Fall ergibt sich, dass die $\alpha_i \in \mathbb{Q}_p(\theta)$ folgende Abschätzung erfüllen.

Satz 3.7. *H lässt sich folgendermaßen abschätzen, falls gilt*

- $v_p(\lambda) > v_p(\alpha_{0,i})$ *für mindestens ein* i :

$$H < \frac{\log p}{c_3} \left(\frac{\log c_2}{\log p} + v_p(\lambda) + \frac{1}{2} v_p(\Delta(\theta)) \right),$$

- $v_p(\lambda) \leq v_p(\alpha_{0,i})$ *für alle* i :
  Falls $d(\vec{y}, \mathcal{L}) > \sqrt{n} X_0$, *dann gilt*

$$H < \frac{\log p}{\log c_3} \left(u + \frac{\log c_2}{\log p} + v_p(\lambda) + \frac{1}{2} v_p(\Delta(\theta)) \right)$$

  oder $x_1 = \dots = x_n = 0$.

Beweis: [Sma98] □

Sind die Voraussetzungen der Sätze nicht erfüllt, so vergrößert man u in der Approximationsmatrix und versucht es erneut.

3.2 Aufstellen der Linearformen

Um die LLL-Reduktion nun auf die Schranken für S-ganze Punkte anwenden zu können, muss man zunächst Linearformen aufstellen. Dabei unterscheidet man drei Fälle, den der unendlichen Stellen, den der endlichen Stellen mit $\mathbb{K}_\mathfrak{p} = \mathbb{Q}_p$ und den der endlichen Stellen mit $\mathbb{K}_\mathfrak{p} \neq \mathbb{Q}$.

3.2.1 Die unendlichen Stellen

Vgl. [Her02]. Zunächst wird die Kurve in kurze Weierstraß-Form transformiert durch

$$X = x + \frac{b_2}{12} \quad \text{und} \quad Y = \frac{1}{2}(2y + a_1 x + a_3)$$

Herrmann gibt in [Her02] eine andere Transformation an, die aber zu einer nicht normierten Kurve führt. Dies ist jedoch für die Implementierung unter Magma sehr ungünstig, da dort elliptische Kurven immer normiert sein müssen. Die so transformierte Kurve lautet:

$$E_\Lambda : Y^2 = X^3 - \frac{g_2}{4}X - \frac{g_3}{4}, \quad g_2, g_3 \in \mathbb{K}.$$

Dabei sind g_2, g_3 gegeben durch

$$\begin{aligned} g_2 &= \frac{2}{3}a_1 62 a_2 - 2a_1 a_3 + \frac{4}{3}a_2^2 + \frac{1}{12}a_1^4 - 4a_4, \\ g_3 &= -\frac{1}{18}a_1^4 a_2 - \frac{2}{9}a_1^2 a_2^2 + \frac{2}{3}a_1 a_2 a_3 + \frac{4}{3}a_2 a_4 + \frac{1}{3}a_1^2 a_4 - a_3^2 - 4a_6 - \\ &\quad -\frac{1}{216}a_1^6 - \frac{8}{27}a_2^3 + \frac{1}{6}a_1^3 a_3. \end{aligned}$$

Außerdem bezeichne $B_{1,\Lambda}, \ldots, B_{r,\Lambda}$ die Bilder der Mordell-Weil-Basis unter der Abbildung von E nach E_Λ.

Jede unendliche Stelle eines Zahlkörpers korrespondiert eindeutig zu einer Einbettung in die komplexen Zahlen. Denn jeder unendlichen Stelle wird eine Nullstelle $\overline{\theta} \in \mathbb{C}$ des Minimalpolynoms von θ zugeordnet. Diese Nullstelle definiert aber die Einbettung über den Homomorphismus $\sigma : \mathbb{Q}(\theta) \to \mathbb{C}$ mit den Eigenschaften $\sigma(\theta) = \overline{\theta}$ und $\sigma(x) = x$ für alle $x \in \mathbb{Q}$. Sei also σ die zur Stelle p gehörende Einbettung. Im Folgenden kann nun alles mit Hilfe der Einbettung über den komplexen Zahlen betrachtet werden. Bei der Gleichung der Kurve wendet man dazu die Einbettung auf die Koeffizienten und

bei einem Punkt auf die einzelnen Komponenten an. Multipliziert man den Punkt P der Kurve dann mit der Ordnung g der Torsionsgruppe, so entfällt nach Kapitel 1 der Torsionspunkt. Seien ω_1 und ω_2 ein Paar minimaler Perioden der Kurve E_Λ über $\mathbb{C}$ und Λ das zugehörige Gitter. Dann lässt sich der elliptische Logarithmus des Punktes $gP_\Lambda = n_1 gB_{1,\Lambda} + \cdots + n_r gB_{r,\Lambda}$ darstellen durch die Summe

$$\Psi_\infty(gP_\Lambda) \equiv \sum_{i=1}^{r} n_i \Psi_\infty(gB_{i,\Lambda}) (\mathrm{mod}\ \Lambda).$$

Das heißt, es gibt zwei ganze Zahlen n_{r+1} und n_{r+2}, so dass sich der elliptische Logarithmus von P_Λ als Linearkombination der $\Psi_\infty(gB_{i,\Lambda})$, $i = 1, \ldots, r$, und ω_1 und ω_2 mit den Koeffizienten n_i für $i = 1, \ldots, r+2$ darstellen lässt. Mit Hilfe von

$$gu_{i,\infty} := \begin{cases} \Psi_\infty(B_{i,\Lambda}), & i = 1, \ldots, r, \\ \omega_1, & i = r+1, \\ \omega_2, & i = r+2. \end{cases}$$

lässt sich dann eine Linearform in komplexen Zahlen für den elliptischen Logarithmus angeben:

$$|\Psi_\infty(P_\Lambda)| = \left| \sum_{i=1}^{r+2} n_i u_{i,\infty} \right|, \quad \text{mit } |n_i| \leq \begin{cases} N, & 1 \leq i \leq r, \\ rN + g, & \text{sonst} \end{cases}.$$

Der folgende Satz gibt nun eine Abschätzung des elliptischen Logarithmus in Abhängigkeit von der X-Koordinate an.

Satz 3.8. *Es existiert eine Konstante $c_{16} > 0$, so dass für alle Punkte $P = (X, Y) \in E_\Lambda(\mathbb{K})$ mit $|X| > c_{16}$ gilt:*

$$|\Psi_\infty(P)| \leq \begin{cases} 4\sqrt{2}|X|^{-1/2}, & X \in \mathbb{R}_{\geq 0}, \\ 4\sqrt{2}(\pi+1)|X|^{-1/2}, & \text{sonst.} \end{cases}.$$

Beweis: Ein Beweis dazu findet sich in [Her02]. Allerdings wählt Herrmann darin c_{16} zu klein. Es müsste $c_{16} := 2\max\{|\alpha_i|\}$ lauten. Außerdem muss man berücksichtigen, dass wir eine andere Kurve als Herrmann verwenden und deshalb den Ausdruck $|1/\sqrt{t^3 - g_2 t - g_3}|$ mit $2\sqrt{2}|t|^{-3/2}$ abschätzen müssen. □

Aus Satz 3.1 folgt nun, dass

$$|X|_p \geq \exp\{c_{14}N^2 - c_{15}\} \geq c_{16}, \quad \text{falls} \quad N \geq \sqrt{\frac{\log(c_{16} + |b_2|_p/12) + c_{15})}{c_{14}}}.$$

Sei $P_\Lambda = (X, Y)$ ein Punkt auf E_Λ und $P = (x, y)$ der entsprechende Punkt auf E, so gilt nach [Her02], wieder unter Berücksichtigung der abgeänderten Transformation,

$$|x\Psi_\infty(P_\Lambda)^2| \leq 32(1+\pi)^2 + \max\{|\omega_1|, |\omega_2|, |\omega_1+\omega_2|\}^2 |b_2|_p \frac{1}{12} =: c_{17}.$$

Damit gilt wegen Satz 3.1 und der Anforderung an N:

Satz 3.9.

$$|\Psi_\infty(P_\Lambda)| \leq c_{18} \exp\{-c_{14}/2N^2\}$$

mit

$$c_{18} := \sqrt{c_{17}} \exp\{c_{15}/2\}.$$

Beweis: [Her02] □

Die entsprechende Approximationsmatrix ergibt sich nach 3.1 dann zu

$$A = \begin{pmatrix} 1 & & 0 & 0 & 0 \\ & \ddots & & \vdots & \vdots \\ 0 & & 1 & 0 & 0 \\ [C\mathrm{Re}(u_{1,\infty})] & \cdots & \cdots & [C\mathrm{Re}(u_{r+1,\infty})] & [C\mathrm{Re}(u_{r+2,\infty})] \\ [C\mathrm{Im}(u_{1,\infty})] & \cdots & \cdots & [C\mathrm{Im}(u_{r+1,\infty})] & [C\mathrm{Im}(u_{r+2,\infty})] \end{pmatrix}.$$

Dabei werden die $u_{i,\infty}$ so umnummeriert, dass A vollen Rang hat, d.h.

$$\mathrm{Re}(u_{r+2,\infty})\mathrm{Im}(u_{r+1,\infty}) - \mathrm{Re}(u_{r+1,\infty})\mathrm{Im}(u_{r+2,\infty}) \neq 0.$$

C wird in der Größenordnung von $(rN+g)^{(r+2)/2}$ gewählt. Dann gilt nach Satz 3.4, da $\vec{y} = 0$, $X_1 = X_2 = \cdots = X_{r+2} = N$ und die Linearform homogen ist: Falls die Abschätzung für die Länge des kürzesten Basisvektors k_1 die Bedingung $k_1 \geq rN^2 + (1 + 3rN + 2g)/\sqrt{2}$ erfüllt, dann gilt entweder

$$N \leq \sqrt{\frac{2}{c_{14}} \left(\log(Cc_{18}) - \log\left(\sqrt{k_1^2 - rN^2} - \frac{1+3rN+2g}{\sqrt{2}} \right) \right)}$$

oder $n_1 = \cdots n_r = 0$ und $n_{r+1}|C\mathrm{Re}(u_{r+1,\infty})| + n_{r+2}|C\mathrm{Re}(u_{r+2,\infty})| = 0$ und $n_{r+1}|C\mathrm{Im}(u_{r+1,\infty})| + n_{r+2}|C\mathrm{Im}(u_{r+2,\infty})| = 0$.

Ist die Bedingung nicht erfüllt, d.h. k_1 zu klein, so wiederholt man den Vorgang mit einem größeren C. Insgesamt wird diese Reduktion so lange wiederholt, bis sich der Wert für N nicht mehr wesentlich verändert. Das Ergebnis wird als $N^{\mathfrak{p}}$ gespeichert. Damit ist unter der Annahme, dass $|x|_{\mathfrak{p}}$ maximal für $\mathfrak{p} \in S$ ist, eine kleinere Schranke für h_n als in Kapitel 2 bestimmt worden. Eine überblickshafte Darstellung der Reduktion findet sich in Anhang B als Algorithmus 10.

3.2.2 Die endliche Stelle im Fall $\mathbb{K}_\mathfrak{p} = \mathbb{Q}_p$

Ab jetzt muss stets mit einem minimalen Modell der Kurve E gearbeitet werden, da sonst der $\mathfrak{p}$-adisch elliptische Logarithmus nicht definiert ist. Bezeichne also im folgenden $E^{(\mathfrak{p})}$ ein minimales Modell von E. Berechnet werden kann dieses z.B. mit Hilfe des Algorithmus von Tate [Tat75]. Nach [Sil86] gelten dann für Koordinaten der beiden Kurven E und $E^{(\mathfrak{p})}$ die Beziehungen

$$x = u^2 x_\mathfrak{p} + l \text{ und } y = u^3 y_\mathfrak{p} + u^2 d x_\mathfrak{p} + t,$$

wobei u, l, t, d aus dem Ganzheitsring. Dabei gilt: $h(x_\mathfrak{p}) \leq h(u^2)h(x-l) \leq 2h(u^2 l)h(x)$. Da jede Kurve E minimal für fast alle Stellen $\mathfrak{p}$ in $\mathbb{K}$ ist, müssen nur endlich viele Modelle von E betrachtet werden. Für jedes dieser Modelle bestimmt man u und die zugehörige Primidealzerlegung. Dann ergänzt man die Stellenmenge S um alle zusätzlichen Stellen der Primidealzerlegung, die nicht bereits in S enthalten sind. Diese neue Menge heiße S' mit der Mächtigkeit s'. Die Menge aller S'-ganzen Punkte enthält dann auch die Menge aller S-ganzen Punkte. Dann muss mit der neuen Stellenmenge S' eine neue Konstante N' aus Kapitel 2 berechnet werden. Mit $B_1^{(\mathfrak{p})}, \ldots, B_r^{(\mathfrak{p})}$ werden die Bildpunkte der Mordell-Weil-Basis von E unter der Abbildung $E \to E^{(\mathfrak{p})}$ bezeichnet. Sei $m_\mathfrak{p}$ die in Kapitel 1 im Zusammenhang mit dem $\mathfrak{p}$-adisch elliptischen Logarithmus, Definition 1.44, definierte Konstante. Dann gilt, dass in der Darstellung von $m_\mathfrak{p} P$ kein Torsionspunkt mehr auftritt und der elliptische Logarithmus für alle $m_\mathfrak{p} B_i^{(\mathfrak{p})}$ definiert ist. Dieser werde mit $u_{i,\mathfrak{p}} = \Psi_\mathfrak{p}(m_\mathfrak{p} B_i^{(\mathfrak{p})})$ bezeichnet. Damit ergibt sich die Linearform

$$\Psi_\mathfrak{p}(m_\mathfrak{p} P) = \sum_{i=1}^{r} n_i' u_{i,\mathfrak{p}}.$$

Herrmann gibt für diese Linearform die folgende Abschätzung an:

Satz 3.10.

$$\left| \sum_{i=1}^{r} n_i' u_{i,\mathfrak{p}} \right| \leq \sqrt{\exp\left\{ d \frac{\lambda_{\min}^{(\mathfrak{p})}}{s' n_\mathfrak{p}} \right\} \exp\left\{ -\frac{1}{2} d \frac{c_2}{s' n_\mathfrak{p}} N'^2 \right\}}$$

Beweis: [Her02] □

In diesem Fall lautet die Approximationsmatrix nach Kapitel 3.1

$$A = \begin{pmatrix} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ [u_{1,p}']_p & \cdots & [u_{r-1,p}']_p & p^u \end{pmatrix},$$

wobei $u'_{i,p} := -u_{i,p}/u_{r,p}$ und $[z_0]_p$ die eindeutige ganze Zahl mit $0 \leq [z_0]_p < p^C - 1$ und $[z_0]_p \equiv z_0 \bmod p^C$, $C \in \mathbb{N}$ ist. u ist so gewählt, dass p^u die Größenordnung von N'^r hat. Durch die LLL-Reduktion erhält man auch in diesem Fall eine Abschätzung für den kürzesten Gittervektor k_2. Dann gilt mit Satz 3.5

Satz 3.11. *Ist $k_2^2 > rN'^2$, so gilt*

$$N' \leq \sqrt{\frac{2s'n_{\mathfrak{p}} \log p}{dc_2}} \left(u + v_p(u_{r,p}) + \frac{d\lambda_{\min}^{(\mathfrak{p})}}{s'n_{\mathfrak{p}} 2 \log p} \right).$$

Beweis: [Her02] □

Auch hier gilt wieder, dass, falls k_2 die Bedingung nicht erfüllt, die LLL-Reduktion mit größerem u wiederholt und das Verfahren so oft angewendet wird, bis sich N' nicht mehr wesentlich ändert. Das Ergebnis wird als $N^{\mathfrak{p}}$ gespeichert.

3.2.3 Die endliche Stelle über $\mathbb{K}_{\mathfrak{p}} \neq \mathbb{Q}_{\mathfrak{p}}$

Das Problem bei Linearformen über $\mathbb{K}_{\mathfrak{p}}$ besteht darin, dass es keinen Reduktionsalgorithmus gibt. Deshalb kann hier nicht mit einfachen $\mathfrak{p}$-adisch elliptischen Logarithmen gerechnet werden. Wegen dieses Problems wird im Folgenden der pseudo $\mathfrak{p}$-adische elliptische Logarithmus aus [Her02] eingeführt.

Sei $\mathfrak{p}$ das Ideal über der Primzahl p mit dem Verzweigungsindex $e_{\mathfrak{p}|p}$. Dann sei $\alpha \in \mathbb{K}$ ein Element, so dass p und α das Ideal $\mathfrak{p}$ erzeugen. In Magma kann α mit Hilfe des Befehls `Decomposition()` berechnet werden. Ansonsten gibt Cohen in [Coh93] einen Algorithmus zur Berechnung von α an. Es sei also

$$p = \alpha^{e_{\mathfrak{p}|p}}\beta, \quad \beta \in \mathbb{K}, \quad v_{\mathfrak{p}}(\beta) = 0.$$

Außerdem bezeichne $\tilde{\Psi}_{\mathfrak{p}}(T) = \sum_{i=1}^{t_1} d_i/i\, T^i \in \mathbb{K}[T]$ wie in Kapitel 1.5.2 das Polynom zur Näherung des $\mathfrak{p}$-adisch elliptischen Logarithmus $\widehat{\Psi_{\mathfrak{p}}(P)}$. Sei $m_v = m_{\mathfrak{p}} p^{e_{\mathfrak{p}|p}} p^V$, so dass nach Kapitel 1.5.2 der $\mathfrak{p}$-adisch elliptische Logarithmus für $m_v P = (x_v, y_v)$ definiert ist und sich mit $\tilde{\Psi}_{\mathfrak{p}}(-x_v/y_v)$ die gewünschte Approximation ergibt. Da der Faktor m_v meist sehr groß ist, kann der Punkt $m_v P$ nur näherungsweise bestimmt werden, wie in Kapitel 1.5.2 beschrieben. Die Koeffizienten und $-x_v/y_v$ lassen sich darstellen als

$$-\frac{x_v}{y_v} = \alpha^{v_{\mathfrak{p}}(-x_v/y_v)} z'_v \text{ mit } v_{\mathfrak{p}}(z'_v) = 0$$

und

$$\frac{d_i}{i} = \alpha^{v_{\mathfrak{p}}(d_i/i)} d'_i \text{ mit } v_{\mathfrak{p}}(d'_i) = 0.$$

Damit lässt sich das Polynom darstellen als

$$\tilde{\Psi}_{\mathfrak{p}}\left(-\frac{x_v}{y_v}\right) = \sum_{i=1}^{t_1} d_{1,i}\alpha^i, \quad v_{\mathfrak{p}}(d_{1,i}) = 0.$$

Sei $L = \left\lfloor \frac{t_2}{e_{\mathfrak{p}|p}} \right\rfloor$, wobei $\lfloor\cdot\rfloor$ auf die nächste ganze Zahl abrundet. Dann gilt

$$\beta^L \tilde{\Psi}_{\mathfrak{p}}\left(-x_v/y_v\right) = \sum_{i=1}^{t_2} d_{2,i}p^i, \qquad 0 \leq v_{\mathfrak{p}}(d_{2,i}) < e_{\mathfrak{p}|p}.$$

Da das Ganze über dem Zahlkörper $\mathbb{K} = \mathbb{Q}(\theta)$ betrachtet wird, ist jeder Koeffizient Element aus $\mathbb{K}$. Bildet man den p-adischen Abschluss eines Zahlkörpers, so kann es sein, dass der Grad der Körpererweiterung zu d' abnimmt und der neue Körper damit ein Erzeugendenelement θ' kleineren Grades hat. Dann lässt sich auch θ mit Hilfe von θ' darstellen.

Definition 3.12.

$$\Psi_{\mathfrak{p}|p}(P) := \beta^L \tilde{\Psi}_{\mathfrak{p}}\left(-x_v/y_v\right) = \sum_{i=0}^{d'} d_{3,i}\theta'^i, \quad d_{3,i} \in \mathbb{Q}_p$$

heißt *pseudo* $\mathfrak{p}$*-adischer elliptischer Logarithmus* zum Punkt P.

Die Abschätzung für die Linearform in $\mathfrak{p}$-adischen elliptischen Logarithmen lässt sich nach Herrmann [Her02] auf pseudo p-adische elliptische Logarithmen übertragen, mit Hilfe der Ungleichung

$$|\Psi_{\mathfrak{p}}(m_{\mathfrak{p}}P)|_{\mathfrak{p}} = \left|\sum_{i=1}^{r} n_i'\Psi_{\mathfrak{p}}(m_{\mathfrak{p}}B_{\mathfrak{p},i})\right|_{\mathfrak{p}} \geq \left|\sum_{i=1}^{r} n_i'\Psi_{\mathfrak{p}|p}(m_{\mathfrak{p}}B_{\mathfrak{p},i})\right|_p p^{1-e_{\mathfrak{p}|p}-l}.$$

Dabei entsteht l dadurch, dass sich die Bewertung bei der Berechnung des pseudo p-adisch elliptischen Logarithmus im Vergleich zum $\mathfrak{p}$-adisch elliptischen Logarithmus ändern kann. l lässt sich einfach berechnen durch

$$l = v_{\mathfrak{p}}(\beta^L \tilde{\Psi}_{\mathfrak{p}}\left(-x_v/y_v\right)) - v_{\mathfrak{p}}(\Psi_{\mathfrak{p}|p}(P)).$$

Herrmann gibt die Schranke für die Linearform in pseudo-$\mathfrak{p}$-adisch elliptischen Logarithmen an wie folgt:

Satz 3.13.

$$\left|\sum_{i=1}^{r} n_i'\Psi_{\mathfrak{p}|p}(m_{\mathfrak{p}}B_{\mathfrak{p},i})\right|_p \leq p^{e_{\mathfrak{p}|p}-1+l}\sqrt{\exp\left\{\frac{d\lambda_{\min}^{(\mathfrak{p})}}{s'n_{\mathfrak{p}}}\right\}}\exp\left\{-\frac{dc_2}{2s'n_{\mathfrak{p}}}N^{\mathfrak{p}2}\right\}.$$

Damit kann man ein System von Linearformen über $\mathbb{Q}_p(\theta')$ angeben:

$$n'_1 u_{1,p} + \cdots + n'_r u_{i,p}, \quad \text{wobei } u_{i,p} = \sum_{j=0}^{d'-1} d_{3,j,i}\theta'^j,\ d_{3,j,i} \in \mathbb{Q}_p.$$

Das lässt sich auf Linearformen in den $d_{3,j,i}$ zurückführen:

$$n'_1 d_{3,j,1} + \cdots + n'_r d_{3,j,r}, \quad \text{mit } j = 0, \ldots, d'-1 \text{ und } d_{3,j,i} \in \mathbb{Q}_p.$$

Nach Lemma 3.6 kann man für diese entsprechend zu Satz 3.13 Ungleichungen angeben. Analog zu Kapitel 3.1 lässt sich nun $\lambda_\Lambda \in \mathbb{Q}_p$ bestimmen durch

$$v_p(\lambda_\Lambda) = \min_{1\le i\le r}\left\{\min_{0\le j\le d'-1}\{v_p(d_{3,j,i})\}\right\} =: c_\lambda.$$

Setzt man $u'_{j,i,p} = d_{3,j,i}/\lambda_\Lambda \in \mathbb{Z}_p$, so kann man das zugehörige Approximationsgitter angeben:

$$A = \begin{pmatrix} 1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & 0 & \cdots & 0 \\ [u'_{0,1,p}]_p & \cdots & [u'_{0,r,p}] & p^C & & 0 \\ \vdots & & \vdots & & \ddots & \\ [u'_{d'-1,1,p}]_p & \cdots & [u_{d'-1,r,p}]_p & 0 & & p^C \end{pmatrix}.$$

Durch die LLL-Reduktion erhält man eine Abschätzung für den kürzesten Gittervektor k_3. Damit gilt nach Satz 3.7:

Satz 3.14. *Ist $k_3 > \sqrt{r}N'$, dann gilt entweder $n'_1 = \cdots = n'_r = 0$ oder*

$$N' < \sqrt{\left(2C\log p + \log p v_p(\Delta(\theta')) + 2\log\left(p^{e_{\mathfrak{p}|p}-1+l}\sqrt{\exp\left\{\frac{d\lambda^{(\mathfrak{p})}_{\min}}{s' n_\mathfrak{p}}\right\}}\right)\right)} \cdot \sqrt{\left(\frac{s' n_\mathfrak{p}}{d c_2}\right)}$$

Beweis: [Her02] □

Ändert sich das Ergebnis nicht mehr, so wird es als $N^\mathfrak{p}$ gespeichert. Auf diese Weise kann man die Schranke aus Kapitel 2 für jede Primstelle deutlich reduzieren. Da aber nicht bekannt ist bei welcher Primstelle die Annahme $|x|_\mathfrak{p}$ maximal für $\mathfrak{p} \in S$ erfüllt ist und damit die Reduktion eine gültige Schranke für h_n liefert, erhält man schließlich die Abschätzung aus Satz 3.1, indem man $N := \max_\mathfrak{p}\{N^\mathfrak{p}\}$ wählt.

Kapitel 4

Suche nach S-ganzen Punkten

In Kapitel 2 wurde eine Schranke N für die Koeffizienten $m_i, i = 1, \ldots, r$ eines S-ganzen Punktes in der Darstellung mittels Mordell-Weil-Basis hergeleitet:

$$P = m_1 B_1 + \cdots + m_r B_r + T, \quad |m_i| \leq N,\ m_i \in \mathbb{Z},\ i = 1, \ldots, r,$$

wobei $B_1, \ldots, B_r$ die Mordell-Weil-Basis der Kurve bezeichnet und T ein Torsionspunkt ist. In Kapitel 3 wurde die Schranke N mit Hilfe der LLL-Reduktion deutlich verringert. Auch wenn dadurch statt einer Schranke in der Größenordnung von oft deutlich über 10^{1000} nun eine Schranke in einer Größenordnung zwischen 10 und wenigen hundert zu erwarten ist, ist die Anzahl C der auf S-Ganzheit zu testenden Punkte meist noch übermäßig groß. Sie beträgt

$$C = (2N + 1)^r.$$

Gerade im Zahlkörperfall mit langsamer Arithmetik werden schnell Größenordnungen von C erreicht, die eine direkte Suche nach S-ganzen Punkten unmöglich machen. In diesem Kapitel geht es nun darum, die Suche so zu gestalten, dass nicht alle Punkte durchprobiert werden müssen, sondern möglichst viele von vornherein ausgeschlossen werden können. Dazu bedient man sich der Eigenschaften der reduzierten Kurve.

4.1 Die Reduktion einer elliptischen Kurve

Eine elliptische Kurve E über einem lokalen Körper $\tilde{\mathbb{K}}$ kann mittels Reduktion auf eine Kurve $E_{\mathfrak{p}}$ über einem endlichen Körper $\mathbb{F}_{\mathfrak{p}}$ für eine Stelle $\mathfrak{p}$ über $\mathbb{K}$ abgebildet werden, indem jeder der Koeffizienten der Kurve $\bmod \mathfrak{p}$ reduziert wird. Dabei unterscheidet man verschiedene Arten von Reduktion in Abhängigkeit davon ob die reduzierte Kurve singulär ist.

Definition 4.1. Sei $E(\tilde{\mathbb{K}})$ eine elliptische Kurve über einem lokalen Körper $\tilde{\mathbb{K}}$.

- $E(\tilde{\mathbb{K}})$ hat *gute Reduktion* bezüglich der Stelle $\mathfrak{p}$, wenn die reduzierte Kurve nicht singulär ist.
- $E(\tilde{\mathbb{K}})$ hat *schlechte Reduktion* bezüglich der Stelle $\mathfrak{p}$, wenn die reduzierte Kurve singulär ist.
  Dabei unterscheidet man:
  - *additive Reduktion*, wenn die reduzierte Kurve eine Spitze hat,
  - *multiplikative Reduktion*, wenn die reduzierte Kurve einen Doppelpunkt hat.

Bemerkung 4.2. Die Reduktion einer Kurve über einem globalen Körper $\mathbb{K}$ wird auf die Reduktion einer Kurve über einem lokalen Körper $\tilde{\mathbb{K}}$ zurückgeführt, indem man das minimale Modell der Kurve über dem $\mathfrak{p}$-adischen Abschluss von $\mathbb{K}$ betrachtet. Deshalb macht es im folgenden keinen Unterschied, ob man die Reduktion der elliptischen Kurve über einem globalen oder lokalen Körper betrachtet. Allerdings ist bei der konkreten Berechnung im Algorithmus darauf zu achten, dass genauso wie zu Beginn von Abschnitt 3.2.2 wegen der Transformation auf ein minimales Modell die Menge der Stellen unter umständen erweitert werden muß.

Hat eine elliptische Kurve gute Reduktion, so ist die reduzierte Kurve selbst wieder eine elliptische Kurve. Durch die Reduktion wird eine Abbildung $a : E(\mathbb{K}) \to E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ definiert, so dass sich jedem Punkt $P = (x, y)$ auf $E(\mathbb{K})$ ein Bildpunkt $\tilde{P} = (x \bmod \mathfrak{p}, y \bmod \mathfrak{p})$ auf $E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ zuordnen lässt.

Tate unterscheidet in [Tat75] noch weitere Arten von Reduktion. Dort gibt er auch einen Algorithmus zum Bestimmen des Reduktionstyps durch das Kodairasymbol an. Ist dies gleich I_0, so liegt gute Reduktion vor. In allen anderen Fällen ist die Reduktion schlecht. Dieser Algorithmus berechnet außerdem ein minimales Modell der Kurve und die Tamagawazahl.

Definition 4.3. Vgl. [Sil86]

- $E_{ns}(\mathbb{F}_{\mathfrak{p}})$ sei die Menge aller nicht-singulären Punkte der reduzierten Kurve,
- $E_0(\mathbb{K}) = \{P \in E(\mathbb{K}) \mid \tilde{P} \in E_{ns}\}$,
- $E_1(\mathbb{K}) = \{P \in E(\mathbb{K}) \mid \tilde{P} = \tilde{\mathcal{O}}_E\}$,
- $E_s(\mathbb{K}) = \{P \in E(\mathbb{K}) \mid \tilde{P}$ ist singulär$\}$.

Satz 4.4. *E_{ns}, $E_0(\mathbb{K})$ und $E_1(\mathbb{K})$ sind Gruppen, und es gilt $E_1(\mathbb{K}) \subset E_0(\mathbb{K})$.*

Beweis: [Sil86] □

Satz 4.5. *Hat E gute Reduktion bezüglich $\mathfrak{p}$, so ist die Abbildung $a : E(\mathbb{K}) \to E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ mit $P \mapsto \tilde{P}$ ein Gruppenhomomorphismus.*

Beweis: [Sil90] □

Satz 4.6. *Sei E eine elliptische Kurve in Weierstraß-Form mit ganzen Koeffizienten über dem Zahlkörper $\mathbb{K}$. Für einen Punkt $P = (x, y)$ mit Primstelle $\mathfrak{p}$ im Nenner gilt*

$$v_{\mathfrak{p}}(y) < v_{\mathfrak{p}}(x).$$

Beweis: Sei $v_{\mathfrak{p}}(x) < 0$.
Wegen $v_{\mathfrak{p}}(a_i) \geq 0$ gilt $v_{\mathfrak{p}}(x^3 + a_2^2 + a_4x + a_6) = v_{\mathfrak{p}}(x^3) < 0$, daraus folgt $0 > v_{\mathfrak{p}}(y^2 + a_1xy + a_3y) \geq \min\{v_{\mathfrak{p}}(y^2), v_{\mathfrak{p}}(a_1xy), v_{\mathfrak{p}}(a_3y)\}$.
Angenommen $v_{\mathfrak{p}}(y) > 0$:
Dann ist $v_{\mathfrak{p}}(y)^2 > 0$ und $v_{\mathfrak{p}}(a_3y) > 0$, also $v_{\mathfrak{p}}(a_1xy) = v_{\mathfrak{p}}(x^3)$ und damit $v_{\mathfrak{p}}(y) < v_{\mathfrak{p}}(x^2) - v_{\mathfrak{p}}(a_1) < 0$.
Es gilt also, ist $v_{\mathfrak{p}}(x) < 0$ dann auch $v_{\mathfrak{p}}(y) < 0$.
Entsprechend folgt: $v_{\mathfrak{p}}(y) < 0 \Rightarrow v_{\mathfrak{p}}(x) < 0$.

Sei $v_{\mathfrak{p}}(x) := -a < 0$ und $v_{\mathfrak{p}}(y) := -b < 0$.
Dann gilt: $0 > 3a \geq \min\{-2b, -a-b+v_{\mathfrak{p}}(a_1), -b+v_{\mathfrak{p}}(a_3)\} = \min\{-2b, -a-b+v_{\mathfrak{p}}(a_1)\}$, wegen $v_{\mathfrak{p}}(a_i) \geq 0$.
1.Fall: $\min\{-2b, -a-b+v_{\mathfrak{p}}(a_1)\} = -2b \Rightarrow -2b \leq -3a \Rightarrow -b < -a$
2.Fall: $\min\{-2b, -a-b+v_{\mathfrak{p}}(a_1)\} = -a-b+v_{\mathfrak{p}}(a_1) \Rightarrow -2a-v_{\mathfrak{p}}(a_1) \geq -b \Rightarrow -b < -a$. □

Bemerkung 4.7. Ist $\mathbb{K}$ ein Zahlkörper mit Klassenzahl 1 und E eine elliptische Kurve über $\mathbb{K}$ in Weierstraß-Form. Dann gilt für einen echt $\mathbb{K}$-rationalen Punkt P sogar:
P hat die projektive Darstellung $[\frac{x}{s^2}, \frac{y}{s^3}, 1]$ mit $x, y, s \in \mathbb{Z}_{\mathbb{K}}$, $\mathrm{ggT}(s, x) = 1$ und $\mathrm{ggT}(s, y) = 1$.

Beweis: Sei P ein Punkt auf E mit den vollständig gekürzten affinen Koordinaten $\frac{x_1}{x_2}$ und $\frac{y_1}{y_2}$, dann gilt

$$E: \left(\frac{y_1}{y_2}\right)^2 + a_1\frac{x_1}{x_2}\frac{y_1}{y_2} + a_3\frac{y_1}{y_2} = \left(\frac{x_1}{x_2}\right)^3 + a_2\left(\frac{x_1}{x_2}\right)^2 + a_4\frac{x_1}{x_2} + a_6.$$

Sind die Koeffizienten $a_1, \ldots, a_6$ der Kurve nicht ganz, so multipliziere die Gleichung mit dem kleinsten gemeinsamen Vielfachen der Nenner der a_i. Nun werden folgende Fälle unterschieden:

- $ggT(a_1, x_2) = 1$

  - x_2 und y_2 seien teilerfremd. Durch Vergleichen der Hauptnenner der linken und rechte Gleichungsseite erhält man $x_2 y_2^2 = x_2^3 \Leftrightarrow y_2 = \pm x_2$. Widerspruch!
  - Seien x_2 und y_2 nicht teilerfremd mit $x_2 = sy_2, s \in \mathbb{Z}_{\mathbb{K}}$. Durch Vergleichen der Hauptnenner erhält man nun $sy_2^2 = x_2^3 \Leftrightarrow y_2^2 = x_2^2 y_2 \Leftrightarrow x_2^2 = y_2$. Widerspruch!
  - Seien x_2 und y_2 nicht teilerfremd mit $sx_2 = y_2, s \in \mathbb{Z}_{\mathbb{K}}$. Dann erhält man durch Vergleichen der Hauptnenner $x_2^2 s^2 = x_2^3$. Daraus folgt $s^2 = x_2$ und $y_2 = s^3$.

- $a_1 = cx_2, c \in \mathbb{Z}_{\mathbb{K}}$. Durch Vergleichen der Hauptnenner ergibt sich $x_2^3 = y_2^2$. Mit $x_2, y_2 \in \mathbb{Z}_{\mathbb{K}}$ folgt die Behauptung.

- $x_2 = ca_2, c \in \mathbb{Z}_{\mathbb{K}}$. Dieser Fall läuft weitgehend analog zu ggT$(a_1, x_2) = 1$. Mit den gleichen Rechnungen und der Tatsache, dass alle auftretenden Größen aus $\mathbb{Z}_{\mathbb{K}}$ sind folgt die Behauptung.

□

Betrachtet man eine elliptische Kurve über einem endlichen Körper, so entspricht diese einer endlichen Gruppe. Sei p die unter der Stelle $\mathfrak{p}$ liegende Primzahl.

Satz 4.8. *Für eine elliptische Kurve E über einem endlichen Körper $\mathbb{F}_{\mathfrak{p}}$ gilt: $E(\mathbb{F}_{\mathfrak{p}})$ ist entweder zyklisch oder isomorph zu $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ mit $d_1 | d_2$.*

Beweis: [Coh93] □

4.2 Suche der S-ganzen Punkte durch Reduktion der Kurve

Herrmann geht bei seinem Algorithmus [Her02] davon aus, dass die Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$ einer Kurve gegeben ist. Damit ist jeder Punkt P der Kurve als Linearkombination $P = m_1 B_1 + \cdots + m_r B_r + T$, wobei T ein Torsionspunkt ist und $m_i \in \mathbb{Z}, i = 1, \ldots, r$, darstellbar. Im vorherigen Kapitel wurde eine explizite Schranke $N \geq \max\{|m_1|, \ldots, |m_r|\}$ zur Berechnung von S-ganzen Punkten bestimmt. Anschließend sollen nun alle möglichen Linearkombinationen bis zu dieser Schranke auf S-Ganzheit überprüft werden. Bei dieser Suche ist es möglich, die Anzahl der zu testenden Kombinationen deutlich zu reduzieren, indem man das Verhalten der Punkte bei Reduktion

der Kurve betrachtet. Dabei werde ich zunächst zur Vereinfachung annehmen, dass keine Torsionspunkte vorliegen, und erst in Abschnitt 4.4 näher auf die Behandlung der Torsionspunkte eingehen.

Satz 4.9. *Sei $P = (x, y)$ ein Punkt auf der Kurve $E(\mathbb{K})$ und a die Reduktionsabbildung bezüglich der Stelle $\mathfrak{p}$ über $\mathbb{K}$. Dann gilt:*

$$v_{\mathfrak{p}}(x) < 0 \Leftrightarrow a(P) = \tilde{\mathcal{O}}_E.$$

Beweis: Sei P ein Punkt auf der Kurve mit Projektiven Koordinaten $[x, y, 1]$ mit $v_{\mathfrak{p}}(x) < 0$.
Dann gilt nach Satz 4.6 $v_{\mathfrak{p}}(y) < v_{\mathfrak{p}}(x)$. Daraus folgt $v_{\mathfrak{p}}(xy^{-1}) > 0$ und $v_{\mathfrak{p}}(y^{-1}) > 0$. Dann ergibt sich durch Anwenden der Reduktionsabbildung auf den Punkt P mit den projektiven Koordinaten $[x, y, 1]$:
$a(P) = a([xy^{-1}, 1, y^{-1}]) = [xy^{-1} \bmod \mathfrak{p}, 1 \bmod \mathfrak{p}, y^{-1} \bmod \mathfrak{p}] = [0, 1, 0]$.

Gilt andererseits $a(P) = a([\tilde{x}, \tilde{y}, \tilde{z}]) = [0, 1, 0]$ so ist $v_{\mathfrak{p}}(\tilde{x}) > 0, v_{\mathfrak{p}}(\tilde{y}) = 0$ und $v_{\mathfrak{p}}(\tilde{z}) > 0$. Mit $P = [\tilde{x}, \tilde{y}, \tilde{z}] = [\tilde{x}\tilde{z}^{-1}, \tilde{y}\tilde{z}^{-1}, 1] = [x, y, 1]$ folgt dann $v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(\tilde{y}\tilde{z}^{-1}) = v_{\mathfrak{p}}(\tilde{y}) - v_{\mathfrak{p}}(\tilde{z}) < 0$ und damit nach Satz 4.6 $v_{\mathfrak{p}}(x) < 0$. Folglich ist der Punkt

□

4.2.1 Reduktion modulo $\mathfrak{p} \notin S$

Ist P ein Punkt einer elliptischen Kurve E und $\mathfrak{p}$ eine Stelle, die nicht in der Menge S enthalten ist, so ist aus Satz 4.9 bekannt, dass P, falls er bei der Reduktion bezüglich $\mathfrak{p}$ auf den Punkt im Unendlichen abgebildet wird, nicht S-ganz sein kann. Dies kann man folgendermaßen ausnutzen, um bei der Suche nach S-ganzen Punkten einige Möglichkeiten auszuschließen:

Zunächst wählt man eine Stelle $\mathfrak{p} \notin S$. Dabei wählt man zur Vereinfachung die Stelle so, dass E bei ihr gute Reduktion hat. Dies kann man beispielsweise über das Kodairasymbol aus dem Algorithmus von Tate [Tat75] prüfen. Dann bestimmt man die Reduktionsabbildung und die Bildpunkte $\tilde{B}_1, \ldots, \tilde{B}_r$ der Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$. Nach Satz 4.8 hat die reduzierte Kurve $E_{\mathfrak{p}}$ entweder einen oder zwei Erzeuger. Deshalb unterscheidet man, siehe auch Algorithmus 11:

- $E_{\mathfrak{p}}$ hat einen Erzeuger Q.
  Dieser hat die Ordnung o. Man stellt nun $\tilde{B}_1, \ldots, \tilde{B}_r$ mit Hilfe von Q dar:
  $$\tilde{B}_i = \alpha_i Q,\ \alpha_i \in \mathbb{F}_{\mathfrak{p}},\ i = 1, \ldots, r.$$
  Sei $P = \sum_{i=1}^{r} m_i B_i$. Da die Reduktionsabbildung ein Homomorphismus ist, gilt dann $\tilde{P} = \sum_{i=1}^{r} m_i \tilde{B}_i$. Mit Hilfe von Q lässt sich $\tilde{P}$ dar-

stellen als

$$\tilde{P} = \sum_{i=1}^{r} m_i(\alpha_i Q) = (\sum_{i=1}^{r} m_i\alpha_i)Q.$$

Ist $\sum_{i=1}^{r} m_i\alpha_i \bmod o = 0$ so folgt $\tilde{P} = \tilde{\mathcal{O}}_E$. Da $\mathfrak{p}$ nicht aus S ist, kann nach Satz 4.9 P nicht S-ganz sein.

- $E_\mathfrak{p}$ hat zwei Erzeuger Q_1 und Q_2.
  Diese haben die Ordnungen o_1 bzw. o_2. Dann lassen sich die $\tilde{B}_1, \ldots, \tilde{B}_r$ darstellen durch

  $$\tilde{B}_i = \alpha_{i,1}Q_1 + \alpha_{i,2}Q_2,\ \alpha_{i,1}, \alpha_{i,2} \in \mathbb{F}_\mathfrak{p},\ i = 1, \ldots, r.$$

  Damit gilt

  $$\tilde{P} = \sum_{i=1}^{r} m_i(\alpha_{i,1}Q_1 + \alpha_{i,2}Q_2) = (\sum_{i=1}^{r} m_i\alpha_{i,1})Q_1 + (\sum_{i=1}^{r} m_i\alpha_{i,2})Q_2.$$

  Ist nun sowohl $\sum_{i=1}^{r} m_i\alpha_{i,1} \bmod o_1 = 0$ als auch $\sum_{i=1}^{r} m_i\alpha_{i,2} \bmod o_2 = 0$, dann ist $\tilde{P} = \tilde{\mathcal{O}}_E$, und P kann nicht S-ganz sein.

Beim Prüfen der Linearkombinationen der Mordell-Weil-Basis ist es nun möglich, alle Koeffizienten, die obigen Kongruenzen entsprechen, sofort auszuschließen, vgl. Algorithmus 12. Dies ist vor allem deshalb eine deutliche Verbesserung, da diese Entscheidung bereits möglich ist, bevor die Linearkombinationen berechnet werden. Das Berechnen von Vielfachen oder Summen von Punkten auf elliptischen Kurven wird nämlich schnell sehr aufwändig. Das Vorgehen kann man für beliebig viele Stellen wiederholen. Allerdings werden desto weniger Fälle ausgeschlossen, je größer die zugehörige Primzahl ist. Gleichzeitig steigt mit der Größe der Primzahl auch der Aufwand zum Berechnen der $\alpha_1, \ldots, \alpha_r$, da die Ordnung der Gruppe $E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$ nach Satz 1.12 wächst.

Satz 4.10. *Sei E eine elliptische Kurve mit einer Mordell-Weil-Basis der Länge r, N die Schranke für die Koeffizienten in der Darstellung durch die Mordell-Weil-Basis, $\mathfrak{p}$ eine Stelle und $E_\mathfrak{p}$ die modulo $\mathfrak{p}$ reduzierte Kurve. Dann lässt sich die Anzahl A der durch obiges Verfahren ausgeschlossenen Fälle in Abhängigkeit von der Anzahl der Erzeuger von $E_\mathfrak{p}$ folgendermaßen abschätzen:*

- *$E_\mathfrak{p}$ hat einen Erzeuger der Ordnung o:*

  $$\left\lfloor \frac{2N}{o} \right\rfloor (2N - (2N \bmod o))^{r-1} \leq A \leq \left\lfloor \frac{2N}{o} + 1 \right\rfloor (2N + o)^{r-1}.$$

- *$E_\mathfrak{p}$ hat zwei Erzeuger mit den Ordnungen o_1, o_2 für die gilt $o_1 b = o_2$:.*

$$\left\lfloor \frac{2N}{o_2} \right\rfloor \left(\frac{2N - (2N \bmod o_2)}{b} \right)^{r-1} \leq A \leq \left\lfloor \frac{2N}{o_2} + 1 \right\rfloor \left(\frac{2N + o_1}{b} \right)^{r-1}.$$

Dabei bezeichnet $\lfloor n \rfloor$ die größte ganze Zahl kleiner oder gleich n.

Bemerkung 4.11. Die Schranken sind besonders gut für große N und kleine o und r. Für den Fall, dass N kleiner als die Ordnung der reduzierten Kurve ist, sind die Abschätzungen für A wertlos. Wird die Ordnung der Gruppe zu groß, wird aber auch der Aufwand zum Bestimmen aller möglichen Tupel größer als die direkte Suche nach S-ganzen Punkten. Dann bestimmt man nicht alle möglichen Tupel $(m_1, \ldots, m_r)$ mit $0 \leq m_i \leq o - 1$, die die Kongruenzen erfüllen, sondern nur die mit $|m_i| \leq N$ und testet die zugehörigen Punkte auf S-Ganzheit. Diese Vorauswahl geht deutlich schneller als das Berechnen und Testen aller möglicher Punkte.

Beweis: Für den ersten Fall gilt: Jedes der r Basiselemente lässt sich nach der Reduktion durch den Erzeuger von $E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$ und eine Zahl α_i darstellen. Um alle Punkte zu bestimmen, die auf $\mathcal{O}_E$ reduziert werden, werden alle Lösungen der Gleichung $\sum_{i=1}^{r} \alpha_i m_i \bmod o = 0$ bestimmt. Ist o eine Primzahl, d.h. $\mathbb{Z}/o\mathbb{Z}$ ein Körper, so gibt es o^{r-1} Lösungen, nämlich

$$\left(m_1, m_2, \ldots, m_{r-1}, -\frac{1}{\alpha_r} \sum_{i=1}^{r-1} \alpha_i m_i \right),$$

mit $m_1, \ldots, m_{r-1}$ beliebig aus $\mathbb{Z}$.
Ist o keine Primzahl, so gibt es zu α_r unter Umständen kein inverses Element. Dies ist genau dann der Fall, wenn $\mathrm{ggT}(\alpha_r, o) \neq 1$. In diesem Fall vertauscht man die Reihenfolge der Basiselemente so, dass $\mathrm{ggT}(\alpha_r', o) = 1$, und geht wie vorher vor. Die Möglichkeit, dass für alle $i = 1, \ldots, r$ gilt $\mathrm{ggT}(\alpha_i, o) \neq 1$, kann nicht auftreten. Denn dies würde bedeuten, dass die Reduktionsabbildung a lediglich in eine Untergruppe von $E_\mathfrak{p}$ abbildet. Nach [Sil86] ist bei guter Reduktion a aber surjektiv. Also kann dieser Fall ausgeschlossen werden, und es ergeben sich wieder o^{r-1} viele Tupel.
Nun werden aber nicht nur die Tupel $(m_1, \ldots, m_r)$ ausgeschlossen, sondern auch alle Tupel der Form $(k_1 o + m_1, \ldots, k_r o + m_r)$, $k_i \in \mathbb{Z}$. Folglich stellt sich nun noch die Frage, welche Werte die k_i annehmen können. Es gilt

$$|k_i o + m_j| \leq N \text{ für alle } j = 1, \ldots, r.$$

Die Anzahl der möglichen k_j ist dann

$$\left\lfloor \frac{N - m_j}{o} \right\rfloor + \left\lfloor \frac{N + m_j}{o} \right\rfloor + 1.$$

Das heißt durch ein Tupel $(m_1, \ldots, m_r)$ werden

$$\prod_{j=1}^{r} \left(\left\lfloor \frac{N - m_j}{o} \right\rfloor + \left\lfloor \frac{N + m_j}{o} \right\rfloor + 1 \right)$$

viele Möglichkeiten ausgeschlossen. Die Gesamtzahl ergibt sich dann über das Aufsummieren aller möglichen Tupel:

$$A = \sum_{i=1}^{o^{r-1}} \prod_{j=1}^{r} \left(\left\lfloor \frac{N - m_{i,j}}{o} \right\rfloor + \left\lfloor \frac{N + m_{i,j}}{o} \right\rfloor + 1 \right).$$

Nun überlegt man sich, dass gilt:

$$\left\lfloor \frac{2N}{o} \right\rfloor \leq \left\lfloor \frac{N - m_j}{o} \right\rfloor + \left\lfloor \frac{N + m_j}{o} \right\rfloor + 1 \leq \left\lfloor \frac{2N}{o} + 1 \right\rfloor.$$

Damit kann A unabhängig von $m_{i,j}$ abgeschätzt werden:

$$\begin{aligned} A &\leq \sum_{i=1}^{o^{r-1}} \prod_{j=1}^{r} \left\lfloor \frac{2N}{o} + 1 \right\rfloor \leq o^{r-1} \left(\frac{2N}{o} + 1 \right)^{r-1} \left\lfloor \frac{2N}{o} + 1 \right\rfloor \\ &\leq \left\lfloor \frac{2N}{o} + 1 \right\rfloor (2N + o)^{r-1} \end{aligned}$$

und

$$\begin{aligned} A &\geq \sum_{i=1}^{o^{r-1}} \prod_{j=1}^{r} \left\lfloor \frac{2N}{o} \right\rfloor \geq o^{r-1} \left(\frac{2N - (2N \bmod o)}{o} \right)^{r-1} \left\lfloor \frac{2N}{o} \right\rfloor \\ &\geq \left\lfloor \frac{2N}{o} \right\rfloor (2N - (2N \bmod o))^{r-1}. \end{aligned}$$

Der zweite Fall verläuft weitgehend analog. Allerdings muss nun nicht die Anzahl der Lösungen für eine Gleichung bestimmt werden, sondern die Anzahl der Lösungen, die beide Gleichungen $\sum_{i=1}^{r} \alpha_{i,1} m_i \bmod o_1 = 0$ und $\sum_{i=1}^{r} \alpha_{i,2} m_i \bmod o_2 = 0$ erfüllen. Da aber beide Gleichungen zusammen nicht mehr gemeinsame Lösungen haben können als jede einzelne, kann man die Anzahl der Lösungen nach dem ersten Fall über $\min\{o_1^{r-1}, o_2^{r-1}\} = o_1^{r-1}$ abschätzen.
Der nächste Schritt verläuft analog, und man erhält die Ungleichungen

$$\begin{aligned} A &\leq \sum_{i=1}^{o_1^{r-1}} \prod_{j=1}^{r} \left\lfloor \frac{2N}{o_2} + 1 \right\rfloor \leq o_1^{r-1} \left(\frac{2N}{bo_1} + 1 \right)^{r-1} \left\lfloor \frac{2N}{o_2} + 1 \right\rfloor \\ &\leq \left\lfloor \frac{2N}{o_2} + 1 \right\rfloor \left(\frac{2N + o_1}{b} \right)^{r-1} \end{aligned}$$

und

$$\begin{aligned} A &\geq \sum_{i=1}^{o_1^{r-1}} \prod_{j=1}^{r} \left\lfloor \frac{2N}{o_2} \right\rfloor \geq o_1^{r-1} \left(\frac{2N - (2N \bmod o_2)}{bo_1} \right)^{r-1} \left\lfloor \frac{2N}{o_2} \right\rfloor \\ &\geq \left\lfloor \frac{2N}{o_2} \right\rfloor \left(\frac{2N - (2N \bmod o_2)}{b} \right)^{r-1}. \end{aligned}$$

□

4.2.2 Reduktion modulo $\mathfrak{p} \in S$

Aus Satz 4.9 folgt auch, dass genau die Punkte, die bei der Reduktion bezüglich einer Stelle $\mathfrak{p} \in S$ auf den unendlich fernen Punkt abgebildet werden, $\mathfrak{p}$ im Nenner enthalten.

Beschränkt man sich auf die Suche nach S-ganzen Punkten, die aber nicht ganz sind, lässt sich diese Eigenschaft ausnutzen um bereits im Voraus die Anzahl der zu testenden Linearkombinationen deutlich einzuschränken, indem man nur diejenigen testet, die modulo $\mathfrak{p} \in S$ auf $\mathcal{O}_E$ abgebildet werden.

Da nun aber die Stellen durch die Menge S vorgegeben sind, muss sowohl der Fall der guten Reduktion als auch der Fall der schlechten Reduktion berücksichtigt werden.

Gute Reduktion

Sei $\mathfrak{p}$ aus S. Wie im vorherigen Abschnitt bestimmt man nun eine Darstellung der Bilder der Mordell-Weil-Basis durch die Erzeuger von $E_{\mathfrak{p}}$:

$$\tilde{B}_i = \alpha_i Q \text{ bzw. } \tilde{B}_i = \alpha_{i,1} Q_1 + \alpha_{i,2} Q_2, \text{ für } i = 1, \ldots, r.$$

Danach bestimmt man alle Tupel $(m_1, \ldots, m_r)$, die $\sum_{i=1}^{r} m_i \alpha_i \bmod o = 0$ bzw. $\sum_{i=1}^{r} m_i \alpha_{i,1} \bmod o_1 = 0$ und gleichzeitig $\sum_{i=1}^{r} m_i \alpha_{i,2} \bmod o_2 = 0$ erfüllen. Mit den gleichen Überlegungen wie in Abschnitt 4.2.1 erhält man nun, dass genau die Punkte, die sich als Linearkombination mit den Elementen eines dieser Tupel als Koeffizienten darstellen lassen, auf den unendlich fernen Punkt abgebildet werden. Das bedeutet aber nichts anderes als dass sie $\mathfrak{p}$ im Nenner enthalten und somit gute Kandidaten für S-ganze, aber nicht ganze Punkte sind. Da diese unter Umständen noch weitere Primzahlen im Nenner enthalten, die nicht in S enthalten sind, ist es notwendig, nochmals explizit auf S-Ganzheit zu testen. Neben den so bestimmten Tupeln $(m_1, \ldots, m_r)$ liefern auch alle Tupel der Form

$$(k_1 o + m_1, \ldots, k_r o + m_r) \text{ bzw. } (k_1 \operatorname{kgV}(o_1, o_2) + m_1, \ldots, k_r \operatorname{kgV}(o_1, o_2) + m_r)$$

mit $k_i \in \mathbb{Z},\ i = 1, \ldots, r$, gute Kandidaten für S-ganze Punkte. Dabei gilt

$$\left\lfloor \frac{-N - m_i}{o} \right\rfloor \leq k_i \leq \left\lfloor \frac{N - m_i}{o} \right\rfloor$$

bzw.

$$\left\lfloor \frac{-N - m_i}{\mathrm{kgV}(o_1, o_2)} \right\rfloor \leq k_i \leq \left\lfloor \frac{N - m_i}{\mathrm{kgV}(o_1, o_2)} \right\rfloor .$$

Schlechte Reduktion

Im Fall der schlechten Reduktion bildet $E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ keine Gruppe. Deshalb muss man die Abbildung $a : E(\mathbb{K}) \to E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ soweit einschränken, dass wieder ein Gruppenhomomorphismus entsteht. Das Problem bei $E_{\mathfrak{p}}$ entsteht durch die singulären Punkte, für die die Addition nicht definiert ist. Das lässt sich einfach beheben, indem man diese Punkte weglässt.

Satz 4.12. *Die Abbildung $a_1 : E_0 \to E_{ns}$ mit $P \mapsto \tilde{P}$ ist ein Gruppenhomomorphismus.*

Beweis: [Tat75] □

Da $E_1 \subset E_0$, ist diese Einschränkung von a geeignet, um alle echt rationalen S-ganzen Punkte zu finden. Man bestimmt also zunächst die Gruppen E_0 und E_{ns} durch deren Erzeuger.

Um E_0 beschreiben zu können, verwendet man den folgenden Satz:

Satz 4.13. *E_0 ist eine Untergruppe mit endlichem Index in $E(\mathbb{K})$. Es gilt:*

$$[E(\mathbb{K}) : E_0(\mathbb{K})] \leq 4.$$

Beweis: [Tat75] □

Die genaue Ordnung von E/E_0 ist durch die Tamagawazahl $c_{\mathfrak{p}}$ gegeben:

$$c_{\mathfrak{p}} = [E(\mathbb{K}) : E_0(\mathbb{K})].$$

Die Tamagawazahl kann mit Hilfe des Algorithmus von Tate [Tat75] bestimmt werden und hat immer einen ganzzahligen Wert zwischen 1 und 4. Bei guter Reduktion hat sie immer den Wert 1. Die Größe der Faktorgruppe ist also bekannt und sehr klein. Nun bestimmt man ein Repräsentantensystem $\tilde{E}_s$ für die Nebenklassen von E_0 in E. Bis auf das neutrale Element $\mathcal{O}_E$ liegen alle Repräsentanten in E_s: Dazu bestimmt man zunächst alle Elemente der Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$, die nicht in E_0 liegen. Die übrigen Elemente der Mordell-Weil-Basis bilden einen Teil des Erzeugendensystems von E_0. Anschließend überprüft man, ob mehrere dieser Punkte in

der gleichen Nebenklasse liegen, indem man testet, ob die Differenz von je zwei Punkten in E_0 liegt. Reicht die Anzahl der so gefundenen Repräsentanten $B_{i_1}, \ldots, B_{i_j}$ noch nicht aus, überprüft man weiterhin, ob die Summe von je zwei Repräsentanten oder das Vielfache eines Repräsentanten in einer neuen Nebenklasse liegt. Auf diese Weise erhält man $c_\mathfrak{p}$ viele Elemente des Repräsentantensystems. Dabei berücksichtigt man:

- Sei $kP \in E_s, k = 1, \ldots, n \in \mathbb{N}$.
  Wegen $k_iP - k_jP = (k_i - k_j)P \in E_s$ mit $1 \leq k_j < k_i \leq n$ gilt: Alle k_iP, $i = 1, \ldots, n$, liegen in verschiedenen Nebenklassen.

- Sei $k_{n+1}P \notin E_s$.
  Mit $k_l > k_{n+1}$ gilt dann wegen $k_lP = (k_l - k_{n+1})P + k_{n+1}P$: k_lP liegt in der gleichen Nebenklasse wie $(k_l \bmod k_{n+1})P$.

- Sei $P_i, P_j \in E_s$ mit $P_i + P_j \in E_s$.
  Dann liegt die Summe $P_i + P_j$ in einer anderen Nebenklasse als P_i und P_j, wegen $(P_i + P_j) - P_i = P_j \in E_s$ bzw. $(P_i + P_j) - P_j = P_i \in E_s$.

- Sei $P_i, P_j, P_k \in E_s$ mit $P_i + P_j \in E_0$.
  Dann liegt $P_i + P_j + P_k$ in der gleichen Nebenklasse wie P_k.

Um ein geeignetes Repräsentantensystem zu bestimmen, genügt es also, solange die Summe von je zwei Elementen aus $\tilde{E}_s$ zu bilden, bis das Ergebnis in E_0 liegt. Da $\#\tilde{E}_s = c_\mathfrak{p}$ und eine der Nebenklassen immer E_0 selbst ist, kann es maximal 3 Nebenklassen mit Elementen aus E_s geben. Es können also nur folgende Fälle beim Vervollständigen des Erzeugendensystems von E_0 und des Repräsentantensystems von E_s auftreten, siehe dazu Algorithmus 13:

- $j = 3$, d.h. $B_{i_1}, B_{i_2}, B_{i_3} \in \tilde{E}_s$
  Dann bildet $\{B_{i_1}, B_{i_2}, B_{i_3}, \mathcal{O}_E\}$ bereits das vollständige Repräsentantensystem, die Tamagawazahl ist demnach 4, und $B_i, i = 1. \ldots, r,\ i \neq i_1, i_2, i_3$, bildet zusammen mit $B_{i_1} + B_{i_2}$, $B_{i_1} + B_{i_3}$ und $2 * B_{i_1}$ ein Erzeugendensystem von E_0.

- $j = 2$, d.h. $B_{i_1}, B_{i_2} \in \tilde{E}_s$

  - $c_\mathfrak{p} = 4$
    Es fehlt noch ein Repräsentant der letzten Nebenklasse. Dieser kann die Form $2B_{i_1}$ bzw. $2B_{i_2}$ oder $B_{i_1} + B_{i_2}$ haben. Angenommen, er hätte die Form $2B_{i_1}$, dann lägen $2B_{i_2}$ und $B_{i_1} + B_{i_2}$ in E_0. Da E_0 aber eine Gruppe ist, wäre damit auch $2(B_{i_1} + B_{i_2}) - 2B_{i_2} = 2B_{i_1}$ in E_0 enthalten. Das widerspricht aber der Annahme, dass $2B_{i_1}$ der fehlende Repräsentant ist. Analog kann man auch $2B_{i_2}$ als Repräsentant ausschließen. Folglich liegt $B_{i_1} + B_{i_2}$ in E_s, und $2B_{i_1}$ und $2B_{i_2}$ ergänzen das Erzeugendensystem von E_0.

  - $c_\mathfrak{p} = 3$
    Dann ist ein Repräsentantensystem $\tilde{E}_s = \{B_{i_1}, B_{i_2}, \mathcal{O}_E\}$ vollständig bekannt, und $B_{i_1} + B_{i_2}$ und $2B_{i_1}$ vervollständigen das Erzeugendensystem von E_0.

- $j = 1$, d.h. $B_{i_1} \in \tilde{E}_s$

  - $c_\mathfrak{p} = 4$
    Da noch die Repräsentanten von 2 Nebenklassen unbekannt sind und sich diese nur als Vielfache des bekannten Repräsentanten B_{i_1} darstellen lassen, sind $2B_{i_1}$ und $3B_{i_1}$ Elemente von $\tilde{E}_s$. Damit ergänzt $4B_{i_1}$ das Erzeugendensystem von E_0.
  - $c_\mathfrak{p} = 3$
    In diesem Fall ist nur ein Repräsentant unbekannt, der sich als $2B_{i_1}$ darstellen lässt. $3B_{i_1}$ ist demnach der gesuchte Punkt aus E_0.
  - $c_\mathfrak{p} = 2$
    Da bereits alle Nebenklassen bekannt sind, ist der gesuchte Erzeuger von E_0 einfach $2B_{i_1}$.

- $j = 0$, d.h., kein Element der Mordell-Weil-Basis liegt in E_s
  In diesem Fall ist $\mathcal{O}_E$ das einzige in $\tilde{E}_s$ enthaltene Element, und alle Punkte der Mordell-Weil-Basis haben gute Reduktion. Die Gruppe E_0 hat also das gleiche Erzeugendensystem wie E und ist somit die einzige Nebenklasse. Das heißt, es gibt insgesamt keinen Punkt, der bei der Reduktion auf den singulären Punkt abgebildet wird. Die Tamagawazahl muss also gleich 1 sein.

Nun muss die Struktur von $\tilde{E}_{ns}$ bestimmt werden. Dazu dient der folgende Satz:

Satz 4.14. *Sei E eine singuläre elliptische Kurve in Weierstraß-Form über dem Körper $\mathbb{K}$. Dann gilt,*

- *falls E multiplikative Reduktion hat:*
  Die Gleichungen der Tangenten in der Singularität seien $y = a_i x + b_i$, $i = 1, 2$.

  - *Falls $a_1 \in \mathbb{K}$, folgt $a_2 \in \mathbb{K}$ und*

    $$E_{ns} \cong \mathbb{K}^*.$$

  - *Falls $a_1 \notin \mathbb{K}$, sei $\mathbb{L} = \mathbb{K}(a_1, a_2)$, und es folgt*

    $$E_{ns}(\mathbb{K}) \subset E_{ns}(\mathbb{L}) \cong \mathbb{L}^*$$

    und

    $$E_{ns}(\mathbb{K}) \cong \{t \in \mathbb{L}^* : \mathcal{N}_{\mathbb{L}/\mathbb{K}}(t) = 1\}.$$

Die zugehörige Abbildung lautet dann:

$$\begin{aligned} \tilde{a}_m : E_{ns} &\to \mathbb{L}^* \\ (x,y) &\mapsto \frac{y - a_1 x - b_1}{y - a_2 x - b_2}. \end{aligned}$$

- *falls E additive Reduktion hat:*
  Die Gleichung der Tangente in dem singulären Punkt $S = (s_1, s_2)$ sei $y = ax + b$ mit $a, b \in \mathbb{K}$. Es gilt:

$$E_{ns}(\mathbb{K}) \cong \mathbb{K}^+.$$

  Die zugehörige Abbildung lautet:

$$\begin{aligned} \tilde{a}_a : E_{ns} &\to \mathbb{K}^+ \\ (x,y) &\mapsto \frac{x - s_1}{y - ax - b}. \end{aligned}$$

Beweis: [Sil86] □

Das weitere Vorgehen entspricht dem im Falle guter Reduktion, nur dass statt der Erzeuger von E nun die Erzeuger von E_0 verwendet werden. Diese werden mit Hilfe der Abbildungen aus Satz 4.14 auf $\mathbb{K}$ bzw. $\mathbb{L}$ abgebildet. Um dafür die Tangentengleichungen zu bestimmen, ist folgendes Vorgehen möglich:

Satz 4.15. *Die Koeffizienten der Tangentengleichungen im singulären Punkt (s_1, s_2) aus obigem Satz seien $a_i, b_i,\ i = 1, 2$. Die zugehörige elliptische Kurve habe die Weierstraß-Gleichung $f(x,y) = y^2 + c_1xy + c_3y - x^3 - c_2x^2 - c_4x - c_6$. Dann gelten die Gleichungen*

$$\begin{aligned} -c_2 - 3s_1 &= a_1 a_2, \\ c_1 &= -(a_1 + a_2). \end{aligned}$$

Außerdem gilt $b_i = -a_i s_1 + s_2,\ i = 1, 2$.

Beweis: Nach [Sil86] gilt

$$f(x,y) - f(s_1,s_2) + (x - s_1)^3 = [(y - s_2) - a_1(x - s_1)][(y - s_2) - a_2(x - s_1)]$$

Durch Ausmultiplizieren und Koeffizientenvergleich ergeben sich obige Gleichungen.

Gilt $a_1 \neq a_2$, so liegt multiplikative Reduktion vor, bei $a_1 = a_2$ additive Reduktion. Die Tangentengleichungen lauten

$$y - s_2 = a_i(x - s_1),\ i = 1, 2.$$

□

Seien nun $B_{0,1}, \ldots, B_{0,r}$ die Erzeuger von E_0. Bei multiplikativer Reduktion sei die Abbildung $a_m : E(\mathbb{K}) \to \mathbb{L}^*$ die Verkettung zweier Gruppenhomomorphismen, der Reduktionsabbildung a und der Abbildung $\tilde{a}_m$, die von den nicht-singulären Punkten auf die multiplikative Gruppe des Körpers $\mathbb{L}$ abbildet. Damit ist a_m selbst wieder ein Gruppenhomomorphismus,

$$\begin{aligned} E &\to \mathbb{L}^* \\ a_m &:= a \circ \tilde{a}_m, \end{aligned}$$

und analog bei additiver Reduktion

$$\begin{aligned} E &\to \mathbb{K}^+ \\ a_a &:= a \circ \tilde{a}_a. \end{aligned}$$

Eine Zusammenfassung zur Berechnung der Abbildung a_a bzw. a_m findet sich im Anhang B als Algorithmus 15.

Nun bildet man die Erzeuger von E_0 mit Hilfe von a_m bzw. a_a ab, d.h., $a_m(B_{0,i}) = \alpha_i,\ i = 1, \ldots, r$, bzw. $a_a(B_{0,i}) = \alpha_i,\ i = 1, \ldots, r$, in Abhängigkeit davon, ob multiplikative oder additive Reduktion vorliegt, siehe Algorithmus 16. Das neutrale Element $\mathcal{O}_E$ wird dabei auf das jeweils neutrale Element der multiplikativen bzw. additiven Gruppe, 1 bzw. 0, abgebildet. Folglich müssen alle Produkte oder Summen gefunden werden, deren Ergebnis das jeweils neutrale Element ist. Bei multiplikativer Reduktion bestimmt man also alle $\beta_1, \ldots, \beta_r$ mit

$$\prod_{i=1}^{r} (\alpha_i \cdot \beta_i) = \prod_{i=1}^{r} \beta_i \prod_{i=1}^{r} \alpha_i = 1,$$

und bei additiver Reduktion bestimmt man alle $\beta_1, \ldots, \beta_r$ mit

$$\sum_{i=1}^{r} (\alpha_i \cdot \beta_i) = 0.$$

Die Punkte der Form

$$P = \beta_1 B_{0,1} + \cdots + \beta_r B_{0,r}$$

sind dann gute Kandidaten für echt rationale $\mathcal{S}$-ganze Punkte. Denn im Falle multiplikativer Reduktion gilt

$$a_m(P) = a_m(\sum_{i=1}^{r} \beta_i B_{0,i}) = \prod_{i=1}^{r} \beta_i a_m(B_{0,i}) = \prod_{i=1}^{r} \beta_i \alpha_i = 1,$$

und analog für additive Reduktion

$$a_a(P) = a_a(\sum_{i=1}^{r} \beta_i B_{0,i}) = \sum_{i=1}^{r} \beta_i a_a(B_{0,i}) = \sum_{i=1}^{r} \beta_i \alpha_i = 0.$$

Da $\tilde{a}_m$ und $\tilde{a}_a$ injektiv sind, ist $\tilde{O}_E$ der einzige Punkt, der auf 1 bzw. 0 abgebildet wird und damit folgt, dass genau bei den Punkten mit obiger Darstellung die Stelle $\mathfrak{p}$ im Nenner auftritt. Natürlich kommen auch hier alle zu $(\beta_1, \ldots, \beta_r)$ kongruenten Tupel in Frage. Das heißt, es müssen alle Linearkombinationen mit Koeffizienten der Form $(k_1 o + \beta_1, \ldots, k_r o + \beta_r)$ auf S-Ganzheit getestet werden. Dabei gibt o die Anzahl der Elemente von $\mathbb{L}^*$ bzw. $\mathbb{K}^+$ an. Für die $k_i \in \mathbb{Z}$ gilt dann:

$$\left\lfloor \frac{-N - m_i}{o} \right\rfloor \leq |k_i| \leq \left\lfloor \frac{N - m_i}{o} \right\rfloor .$$

Für die zusammengesetzten Erzeuger von E_0 gelten unter Umständen geringere Abschätzungen, da, wenn sie gemeinsame Summanden enthalten, die Summe der entsprechenden k_i obige Ungleichung erfüllen muss.

Folgende Bemerkungen gelten wieder gleichermaßen für gute wie schlechte Reduktion:

Bemerkung 4.16. Da bei diesem Verfahren für jede Stelle aus S ein separater Suchlauf durchgeführt wird, muss nicht für jede Primzahl die maximale Schranke $N = \max_{\mathfrak{p} \in S}\{N^{\mathfrak{p}}\}$ verwendet werden. Sei $S' \subset S$.

Für alle S'-ganzen Punkte gilt, dass ihre Koeffizienten m_i in der Darstellung mittels der Mordell-Weil-Basis kleiner oder gleich $N' \leq N$ sind. Damit gilt für alle S-ganzen Punkte, bei denen mindestens ein Koeffizient $N' < m_i \leq N$ auftritt, dass sie mindestens eine Stelle aus $S \setminus S'$ im Nenner enthalten.

Folglich genügt es bei der Bestimmung der Punkte, deren Nenner Primzahlen aus S' enthält, die kleinere Schranke N' zu verwenden. Die fehlenden Punkte werden dann bei der Suche nach Punkten mit Primzahlen aus $S \setminus S'$ im Nenner mit der Schranke N gefunden. Also kann für jede Stelle $\mathfrak{p}$ die ihr zugehörige Schranke $N^{\mathfrak{p}}$ verwendet werden. Da sich diese Schranken je nach Stelle sehr deutlich unterscheiden, kann so der Suchlauf deutlich beschleunigt werden.

Außerdem ist es so möglich, im Nachhinein eine zusätzliche Stelle zur Menge S zu ergänzen, ohne den kompletten Algorithmus erneut ausführen zu müssen. Stattdessen muss lediglich die Schranke $N = \max_{\mathfrak{p} \in S}\{N^{\mathfrak{p}}\}$ über alle Stellen neu berechnet werden und anschließend nur die Suche bezüglich der neuen Stelle $\mathfrak{p}$ durchgeführt werden. Bei diesem Suchlauf muss man allerdings die maximale Schranke N verwenden.

Bemerkung 4.17. Dadurch, dass für jede Stelle eine eigene Suche durchgeführt wird, werden Punkte, die mehrere Stellen im Nenner enthalten, auch mehrfach gefunden. Deshalb ist es sinnvoll, zunächst zu prüfen, ob ein Tupel von Koeffizienten auch Kongruenzen bezüglich anderer Stellen, nach denen bereits gesucht wurde, erfüllt. Dies ist aber nur dann zu berücksichtigen, wenn die einzelnen Einträge des Tupels nicht größer sind als die Schranken bezüglich der Stellen, nach denen bereits gesucht wurde.

Bemerkung 4.18. Da die ganzen Punkte bei der Reduktion nie auf $\mathcal{O}_E$ abgebildet werden, bietet das Vorgehen keine Möglichkeit, sie zu finden. Man muss sie also zusätzlich bestimmen. Dafür berechnet man beispielsweise die Schranke N für den Fall, dass S nur die unendlichen Stellen enthält. Da N sowohl von der Anzahl der Elemente von S als auch von deren Größe abhängt, erhält man nun einen deutlich geringeren Wert für N, als wenn man alle Primzahlen berücksichtigt. Dadurch und eventuell durch Anwenden der in 4.2.1 und 4.3 beschriebenen Verfahren sollte das Durchprobieren aller verbleibenden Möglichkeiten für ganze Punkte möglich sein. Danach berechnet man die Schranke für alle Primzahlen aus S und ergänzt alle echt rationalen S-ganzen Punkte.

4.3 Ausschluss von Vielfachen

Im vorhergehenden Kapitel wurde ein Punkt P mit Hilfe der Reduktionsabbildung a bezüglich der Stelle $\mathfrak{p}$ auf einen Punkt $\tilde{P}$ abgebildet. Für die Darstellung eines Punktes, der $\mathfrak{p}$ im Nenner enthält, durch die Mordell-Weil-Basis galt dabei

$$a(m_1B_1 + \cdots + m_rB_r) = m_1a(B_1) + \cdots + m_ra(B_r) = \tilde{\mathcal{O}}_E.$$

Betrachtet man nun das Vielfache dieses Punktes, so gilt:

$$a(\lambda(m_1B_1+\cdots+m_rB_r)) = \lambda m_1a(B_1)+\cdots+\lambda m_ra(B_r) = \lambda\tilde{\mathcal{O}}_E = \tilde{\mathcal{O}}_E \ \forall\lambda \in \mathbb{Z}.$$

Das bedeutet: Tritt eine Stelle in der Zerlegung des Nenners von P auf, so auch in der Zerlegung der Nenner aller Vielfachen von P. Ist also P nicht S-ganz, so sind auch alle Vielfachen von P nicht S-ganz und können ohne weitere Tests ausgeschlossen werden.

Um alle relevanten Linearkombinationen zu testen, geht man zunächst nur jene durch, deren Koeffizienten teilerfremd sind, also $\mathrm{ggT}(m_1, \ldots, m_r) = 1$. Wird durch eine dieser Linearkombinationen ein S-ganzer Punkt beschrieben, so müssen auch alle Vielfachen dieses Punktes getestet werden. Dabei verwendet man eine Rekursion, bei der der Punkt zunächst mit allen genügend kleinen Primzahlen multipliziert und getestet wird und bei der dann gegebenenfalls dieses Vorgehen mit dem entsprechenden Vielfachen des Punktes wiederholt wird, siehe Algorithmus 17. Dabei ist anzunehmen, dass die Rekursion meist nach wenigen Schritten abbricht. Denn da bei der Punktaddition die Nenner sehr schnell anwachsen, ist zu erwarten, dass bereits nach wenigen Schritten auch andere Primzahlen als erlaubt im Nenner auftreten. Um also grob abzuschätzen, wie viele Punkte getestet werden müssen, genügt es, die Anzahl der Linearkombinationen anzunähern, deren Koeffizienten teilerfremd sind.

Satz 4.19. *Die Anzahl A der r-Tupel $(m_1, \ldots, m_r)$ mit teilerfremden Komponenten lässt sich für große N näherungsweise durch*

$$A \approx \frac{3}{\pi^2}(2N+1)^r$$

angeben.

Beweis: Die ersten $r-1$ Komponenten des Tupels werden beliebig gewählt. Die letzte Komponente m_r wird dann teilerfremd dazu gewählt, d.h.

$$\mathrm{ggT}(m_r, \mathrm{ggT}(m_1, m_2, \ldots, m_{r-1})) = 1.$$

Die Anzahl der zu $e := \mathrm{ggT}(m_1, \ldots, m_{r-1})$ teilerfremden Zahlen wird durch die Eulersche Phi-Funktion φ gegeben. Es gilt damit

$$A = \sum_{m_1=-N}^{N} \sum_{m_2=-N}^{N} \cdots \sum_{m_{r-1}=-N}^{N} \varphi(e)\frac{2N+1}{e}.$$

Nach [Bun02] lässt sich $\varphi(N)$ für große N im Mittel durch $\frac{3}{\pi^2}N$ approximieren. Damit ergibt sich für A:

$$A \approx \sum_{m_1=-N}^{N} \cdots \sum_{m_{r-1}=-N}^{N} \frac{3}{\pi^2}(2N+1) = \frac{3}{\pi^2}(2N+1)^r.$$

□

Tatsächlich erhält man den größten Gewinn bei der Suche nach S-ganzen Punkte durch die Tatsache, dass $-P$ genau dann S-ganz ist, wenn P S-ganz ist. Folglich reicht es, nur die Hälfte der Punkte zu testen. Damit erhält man automatisch auch die Ergebnisse für die Punkte mit negativem Vorzeichen. Wie man eine solche Suche gestalten kann, wird in Algorithmus 18 vorgestellt.

4.4 Torsionspunkte

Bisher wurden zur Vereinfachung die Torsionspunkte nicht weiter berücksichtigt und lediglich der Fall betrachtet, dass $E(\mathbb{K})$ nur einen freien Anteil hat. Um nun auch die Torsionsgruppe $E(\mathbb{K})_{\mathrm{tors}}$ miteinbeziehen zu können, benötigt man folgenden Satz:

Satz 4.20. *Sei $\mathbb{K}$ ein Zahlkörper. Es existiert eine Konstante $M = M(\mathbb{K})$ so, dass für alle elliptischen Kurven E über $\mathbb{K}$ gilt:*
Die Torsionsgruppe $E(\mathbb{K})_{\mathrm{tors}}$ ist endlich erzeugt mit

$$|E(\mathbb{K})_{\mathrm{tors}}| \leq M.$$

Beweis: [Sil86] □

Über den rationalen Zahlen gilt sogar:

Satz 4.21. *Sei E eine elliptische Kurve über $\mathbb{Q}$. Dann gilt*

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z}$$

oder

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Beweis: [Hus87] □

Bemerkung 4.22. Über quadratischen, multiquadratischen, kubischen und quartischen Zahlkörpern zeigt [SZ03], dass die Torsionsgruppe zyklisch oder das Produkt von zwei zyklischen Gruppen ist.

Die Torsionsgruppe hat also endlich viele Erzeuger, in den oben genannten Fällen sogar maximal 2. Diese werden bei der einfachen Suche nach S-ganzen Punkten wie die Elemente der Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$ behandelt, mit dem Unterschied, dass ihre Koeffizienten nicht durch die Schranke der Mordell-Weil-Basis begrenzt werden, sondern durch ihre Ordnung. Es sind dann also alle Linearkombinationen der Form

$$P = m_1 B_1 + \cdots + m_r B_r + n_1 T_1 + \cdots + n_t T_t$$

mit

$$|m_i| \leq N,\ i = 1, \ldots, n \quad \text{und} \quad 0 \leq n_i \leq \text{ord}(T_i) - 1,\ i = 1, \ldots t,$$

zu testen, wobei $T_1, \ldots, T_t$ Erzeuger von $E(\mathbb{Q})_{\text{tors}}$ sind.

Hat die Kurve an der Stelle $\mathfrak{p}$ gute Reduktion, kann das Verfahren aus Abschnitt 4.2.1 und 4.2.2 ohne Veränderung übernommen werden. Dazu betrachtet man zusätzlich zu den Erzeugern der Mordell-Weil-Gruppe auch die der Torsionsgruppe. Statt der berechneten Schranken für die Koeffizienten der Mordell-Weil-Basis verwendet man zum Abschätzen der Koeffizienten der Torsionspunkte die Ordnungen der Erzeuger. Das übrige Vorgehen bleibt gleich.

Folglich stellt sich nur noch die Frage, wie sich die Torsionspunkte bei schlechter Reduktion verhalten. Die Abbildungen a_a und a_m sind unabhängig vom Auftreten von Torsionspunkten definiert worden. Allerdings muss bei der Bestimmung des Erzeugendensystems von E_0 berücksichtigt werden, dass auch die Erzeuger der Torsionsgruppe Repräsentanten für die Nebenklassen von $E_0(\mathbb{K})/E(\mathbb{K})$ sein können. Dazu bestimmt man zunächst die Anzahl der Elemente der Mordell-Weil-Basis, die in E_s liegen und eine eigene Nebenklasse

repräsentieren. Dann bestimmt man die Elemente der Torsionsgruppe, die in E_s liegen und unterscheidet die gleichen Fälle wie in Abschnitt 4.2.2. Um schneller eine Entscheidung treffen zu können, welche Torsionspunkte in E_s liegen, dient der folgende Satz:

Satz 4.23. *Sei T_i, $i \in \{1, \ldots, t\}$, einer der Erzeuger der Torsionsgruppe. Dann gelten folgende Aussagen:*

- *Liegt T_i nicht in E_s, so ist $\langle T_i \rangle \subset E_0$ und T_i ergänzt das Erzeugendensystem von E_0.*
- *Nur in Untergruppen $\langle T_i \rangle$, deren Ordnung sich durch 2 oder 3 teilen lässt, können Punkte mit schlechter Reduktion auftreten.*

Beweis: Sei T_i ein Erzeuger der Torsionsgruppe $E(\mathbb{K})_{\text{tors}}$ und damit auch der Untergruppe $\langle T_i \rangle$. Da E_0 eine Gruppe ist, gilt: Liegt ein Erzeuger von $\langle T_i \rangle$ in E_0, so folgt $\langle T_i \rangle \subset E_0$.

Liegt T_i nicht in E_s und damit $\langle T_i \rangle \nsubseteq E_0$, so liegt kein Erzeuger der Untergruppe $\langle T_i \rangle$ in E_s. Für Untergruppen, deren Ordnung weder durch 2 noch durch 3 teilbar ist, sind aber T_i, $2T_i$, $3T_i$ und $4T_i$ Erzeuger. Mit der Argumentation von Abschnitt 4.2.2 würden damit 4 verschieden Nebenklassen festgelegt. □

Damit lässt sich das Vorgehen ohne Torsionspunkte direkt auf das Vorgehen mit Torsionspunkten übertragen.

Zusammenfassung

Jeder Punkt P einer elliptischen Kurve $E(\mathbb{K})$, wobei $\mathbb{K}$ ein Zahlkörper ist, kann mit Hilfe der Mordell-Weil-Basis $\{B_1, \ldots, B_r\}$ in folgender Weise dargestellt werden:

$$P = m_1 B_1 + \cdots + m_r B_r + n_1 T_1 + \cdots + n_t T_t,$$

mit $m_i, n_j \in \mathbb{Z}$ und $T_j \in E(\mathbb{K})_{\text{tors}},\ i = 1, \ldots, r,\ j = 1, \ldots, t$. Um alle S-ganzen Punkte zu einer gegebenen Stellenmenge zu bestimmen, berechnet man zunächst die in Kapitel 2 angegebene Schranke N für die Koeffizienten, s.d.

$$h_n(P) \leq N$$

für S-ganze P. Diese Schranke wird mit den in Kapitel 3 beschriebenen Verfahren für jede Stelle $\mathfrak{p}$ aus S reduziert zu $N^{\mathfrak{p}}$. Dazu muss zunächst ein minimales Modell von E berechnet, gegebenenfalls die Stellenmenge S erweitert und damit eine neue Schranke N ermittelt werden. Für die unendlichen Stellen werden Linearformen in elliptischen Logarithmen aufgestellt, für die endlichen Stellen in $\mathfrak{p}$-adischen bzw. pseudo $\mathfrak{p}$-adischen Logarithmen. Durch Anwenden des LLL-Algorithmus wird dann für jede Stelle eine kleinere Schranke berechnet. Anschließend sind alle Linearkombinationen der Form

$$\sum_{i=1}^{r} m_i B_i + \sum_{j=1}^{r} n_i T_i$$

mit $|m_i| \leq \max\{N^{\mathfrak{p}}\}$ und $1 \leq n_i \leq \text{ord}(T_i)$ auf S-Ganzheit zu prüfen.

In dieser Arbeit wurde das Verfahren zum Bestimmen S-ganzer Punkte aus [Her02] verbessert. Dabei wurde die Schranke aus Kapitel 2 korrigiert und die Suche nach S-ganzen Punkte effizienter gestaltet.

Um bei der Suche möglichst viele Punkte a priori auszuschließen, nutzt man folgende Eigenschaften aus:

(a) Punkte mit der Stelle $\mathfrak{p}$ im Nenner werden bei der Reduktion der elliptischen Kurve nach $\mathfrak{p}$ auf $\mathcal{O}_E$ abgebildet,

(b) Vielfache eines Punktes P enthalten mindestens die Primzahlen im Nenner, die der Punkt P selbst im Nenner enthält.

Es wird nun für jede Stelle aus S eine eigene Suche durchgeführt. Bei schlechter Reduktion müssen im Fall von (a) zunächst ein Erzeugendensystem von E_0 und die Struktur von E_{ns} bestimmt werden. Durch die Eigenschaft (a) kann über die ganzen Punkte keine Aussage getroffen werden. Außerdem muss nicht jede Suche mit der maximalen Schranke $N = \max_{\mathfrak{p}}\{N^{\mathfrak{p}}\}$ durchgeführt werden, sondern bei der Suche zur Stelle $\mathfrak{p}$ genügt es, die Schranke $N^{\mathfrak{p}}$ zu verwenden. Mit dem in dieser Arbeit vorgestellten Verbesserungen konnten einige neue Beispiele berechnet werden. Diese werden im Anhang A dargestellt.

Anhang A

Beispiele

Die in den vorhergehenden Kapiteln beschriebenen Verfahren wurden in dem Computeralgebra-System Magma implementiert und getestet. Es wurden alle Beispiele aus [Her02] verifiziert, sowie weitere, neue Beispiele berechnet. Dies wäre ohne die vorgestellten Verbesserungen aufgrund zu langer Rechenzeit nicht möglich gewesen. Eine besondere Schwierigkeit bestand darin, geeignete Kurven zu finden. Da die Bestimmung der Mordell-Weil-Basis über Zahlkörpern im Allgemeinen nicht möglich ist, wurde bei der Berechnung über Zahlkörpern auf die Funktion `PseudoMordellWeilGroup()` zurückgegriffen. Diese bestimmt eine Untergruppe der Mordell-Weil-Gruppe. Ein boolescher Parameter gibt an, ob diese Untergruppe gleich viele Erzeuger hat wie die Kurve selbst. In den aufgeführten Beispielen war dies immer der Fall. Durch die Einschränkung, nur eine Untergruppe der Mordell-Weil-Basis zur Verfügung zu haben, konnten natürlich auch nur Teilmengen aller S-ganzen Punkte bestimmt werden. Ein weiteres Problem bei der Wahl der Kurve bestand darin, dass Kurven mit längerer Basis deutlich seltener sind als solche mit kurzer. So musste eine große Menge an Kurven durchprobiert werden, um eine mit geeigneter Mordell-Weil-Basis zu finden. Das wurde besonders dadurch erschwert, dass die Funktion `PseudoMordellWeilGroup()` teilweise sehr lange Rechenzeiten von mehreren Tagen hatte und oft mit Fehlermeldungen über interne Fehler abbrach. Über den rationalen Zahlen steht in Magma die Funktion `MordellWeilGroup()` zur Verfügung, die, falls möglich, die volle Mordell-Weil-Gruppe berechnet. Da aber auch diese Funktion teilweise sehr lange Rechenzeiten hat, wurde das hier aufgeführte Beispiel aus der Arbeit [GPZ94] übernommen.

Ein weiteres Problem trat bei Zahlkörpern mit höherem Grad auf. Hier wurde die Arithmetik so langsam, dass vor allem das Berechnen der Schranken unverhältnismäßig lange dauerte. Bei der Suche nach S-ganzen Punkten fiel dieses Problem kaum ins Gewicht. Im Gegensatz zu [Her02] wo nur Zahlkörper vom Grad zwei oder drei betrachtet wurden, konnten nun auch Beispiele

über Zahlkörpern mit Grad vier und fünf gerechnet werden. Beispiele mit höherem Grad konnten nicht getestet werden, da hierfür keine Mordell-Weil-Basis gefunden wurde.

Die Anzahl der vorgegebenen Stellen stellte insgesamt die geringste Einschränkung dar. Auch bei relativ vielen Stellen wurden die berechneten Schranken nicht so groß, dass die Suche nicht mehr hätte durchgeführt werden können. So wurde hier meist mit zehn Primstellen gearbeitet, während [Her02] sich im westenlichen auf fünf oder sechs beschränkte. Allerdings musste dabei berücksichtigt werden, dass für jede zusätzliche Primzahl auch eine zusätzliche Schranke berechnet werden musste, sodass dies bei hohem Körpergrad wiederum problematisch wurde. Außerdem gab es immer wieder einzelne Stellen, bei denen die Größe der entsprechenden Schranke überproportional groß wurde. In einem solchen Fall war eine vergleichende Berechnung der S-ganzen Punkte mit dem bisherigen Verfahren aus [Her02], nämlich durch Ausprobieren aller Möglichkeiten ohne Reduktion der Kurve, nicht mehr möglich, da dabei immer mit der maximalen auftretenden Schranke gerechnet werden musste. Bei den Suchverfahren mit Reduktion der Kurve stellte dies jedoch kein Problem dar. Die Auswahl der möglichen Beispiele wurde also vor allem durch die Berechnung der Schranken und die fehlende Mordel-Weil-Basis begrenzt, nicht aber durch das Verhaltens des Algorithmus bei der Suche nach S-ganzen Punkten.

In den folgenden Beispielen wurden die Schranken für die unendlichen Stellen stets mit der Annahme berechnet, dass keine endlichen Stellen enthallt, um diese Schranken möglichst gering zu halten. Es wird nur einer der beiden Punkte P und $-P$ angegeben. Soweit es möglich war, wurden alle Ergebnisse überprüft, indem die S-ganzen Punkte auch durch Ausprobieren aller Möglichkeiten, ohne Reduktion der Kurve, bestimmt wurden. Wurden die Schranken dafür zu groß, so wurde dieser Test zumindest mit angenommenen kleineren Schranken durchgeführt. Eine Vergleich mit der entsprechenden Funktion in Magma war nur über $\mathbb{Q}$ möglich. Für den Zahlkörperfall ist in Magma bislang keine entsprechende Funktion vorhanden. Die Rechenzeit in Zahlkörperfall betrug wenige Tage auf einem herkömmlichen Desktop-PC. Im Rahmen dieser Arbeit stand allerdings die Verbesserung der Algorithmik im Vordergrund, so dass bei einer exakteren Implementierung eine weitere Veringerung der Rechenzeit zu erwarten ist.

A.1 Eine Kurve über $\mathbb{Q}$

Beispiel 1

Die Kurve E ist gegeben durch:

$$E : y^2 = x^3 - 203472x^2 + 18487440.$$

Ein dazu minimales Modell ist gegeben durch:

$$E_{\min} : y^2 = x^3 - 157x + 396.$$

Für die Koordinaten x, y eines Punktes gilt dann:

$$x = 36x_{\min}, \quad y = \frac{1}{2} + 216y_{\min}.$$

Die Menge der vorgegeben Primzahlen S lautet:

$$S := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}.$$

Schlechte Reduktion liegt bei den folgenden Primzahlen vor:

Primzahlen mit schlechter Reduktion		
Primzahl	Reduktionstyp	Tamagawazahl
659	multiplikativ	1
272903	multiplikativ	1

Es wurde folgende Basis verwendet:

$$\begin{aligned} B \quad := \quad & \{(36 : 3348), (-36 : 5076), (432 : 3348), \\ & (-216 : 7236), (468 : 5076)\}. \end{aligned}$$

Die Konstante c_2 aus Kapitel 1 beträgt etwa 10.187, und der minimale Eigenwert der Regulatormatrix ist etwa 0.50204. Die Konstante N beträgt ungefähr $5.26445 \cdot 10^{93}$. Nach der Reduktion aus Kapitel 3 betragen die einzelnen Schranken:

Reduzierte Schranken											
Stelle	∞	2	3	5	7	11	13	17	19	23	29
Schranke	7	12	3	3	3	3	3	3	3	11	11

Die Schranke für die unendliche Stelle wurde dabei mit einer verkleinerten Stellenmenge berechnet. Berücksichtigt man die volle Stellenmenge, so lautet die Schranke 19.

In den folgenden Tabellen werden alle S-ganzen Punkte nach den einzelnen Primzahlen, bezüglich denen die Kurve reduziert wurde, sortiert angegeben. Die angegebenen Ordnungen und Erzeuger beziehen sich dabei immer auf die reduzierte Kurve. Die Koeffizienten werden verwendet um die reduzierten Elemente der Mordell-Weil-Basis durch den Erzeuger der reduzierten Kurve darzustellen. Durch die Transformation auf ein minimales Modell der Kurve und die Rücktransformation werden bei der Reduktion nach 2 und 3 nicht nur Punkte mit 2 und 3 im Nenner gefunden, sondern auch solche, bei denen sich die 2 und 3 gegen den Faktor 36 bei der Transformation herausgekürzt haben.

Primzahl 2	
Ordnung der reduzierten Kurve	5
Erzeuger der reduzierten Kurve	$(1:1)$
Koeffizienten zur Darstellung der Basis	$[1,1,3,3,1]$

$(\frac{6512305}{283024} : \frac{559698506135}{150568768})$	$(\frac{18945}{16} : \frac{2426625}{64})$	$(\frac{268857}{169} : \frac{134018253}{2197})$
$(-279 : 7317)$	$(\frac{-39058767}{83521} : \frac{-81378923319}{24137569})$	$(\frac{457}{9} : \frac{77723}{27})$
$(\frac{-236007}{484} : \frac{-14136579}{10648})$	$(468 : 5076)$	$(\frac{-1287}{49} : \frac{-1673811}{343})$
$(3897 : -241677)$	$(\frac{27441}{49} : \frac{-3071223}{343})$	$(\frac{1521}{16} : \frac{-4023}{64})$
$(\frac{-1062934263}{14992384} : \frac{-331228300982427}{58050510848})$	$(\frac{-4023}{64} : \frac{2852037}{512})$	$(\frac{5172849}{9025} : \frac{8141114007}{857375})$
$(\frac{1529877609}{25600} : \frac{59837395150773}{4096000})$	$(\frac{-16551}{49} : \frac{2393091}{343})$	$(\frac{-1575927}{3364} : \frac{-647008101}{195112})$
$(\frac{2601}{4} : \frac{-101547}{8})$	$(\frac{1593}{4} : \frac{6291}{8})$	$(\frac{-911}{4} : \frac{-58249}{8})$
$(\frac{-4662423}{9604} : \frac{1589610933}{941192})$	$(\frac{22739697}{12544} : \frac{105199797303}{1404928})$	$(\frac{12272121}{132496} : \frac{31843356147}{48228544})$
$(\frac{12681}{25} : \frac{845829}{125})$	$(\frac{-495}{4} : \frac{-51705}{8})$	$(\frac{1939545}{1156} : \frac{-2607188445}{39304})$
$(\frac{-48191}{100} : \frac{-2150623}{1000})$	$(\frac{45081}{100} : \frac{-4286979}{1000})$	$(81 : -1593)$
$(\frac{4380777}{529} : \frac{9155637333}{12167})$	$(\frac{12969}{16} : \frac{1257579}{64})$	$(\frac{1392633}{64} : \frac{1643092749}{512})$
$(433 : 3401)$	$(-351 : -6831)$	$(\frac{217596681}{256036} : \frac{2776818944997}{129554216})$
$(-423 : 5373)$	$(\frac{3537}{4} : \frac{-184167}{8})$	$(\frac{156969}{4} : \frac{-62185941}{8})$
$(\frac{113170201}{3025} : \frac{-1203834089699}{166375})$	$(\frac{10809}{16} : \frac{880659}{64})$	$(\frac{541953}{64} : \frac{398411649}{512})$
$(\frac{-1098351}{13456} : \frac{9175104441}{1560896})$	$(\frac{-52119}{256} : \frac{29386827}{4096})$	$(\frac{1117737}{2704} : \frac{314753067}{140608})$
$(\frac{5791249}{5184} : \frac{12850632071}{373248})$	$(\frac{82161}{169} : \frac{-12899223}{2197})$	$(\frac{39271441}{36} : \frac{-246102042887}{216})$
$(\frac{3750777}{3364} : \frac{-6695853363}{195112})$	$(\frac{505}{9} : \frac{72685}{27})$	$(\frac{7289721}{625} : \frac{-19667260269}{15625})$
$(\frac{143906409}{243049} : \frac{1231216488171}{119823157})$	$(\frac{18244377}{1024} : \frac{77903152893}{32768})$	$(\frac{8780049}{9025} : \frac{23343658407}{857375})$
$(\frac{48579616881}{584043889} : \frac{-20640698520793623}{14114588665463})$	$(\frac{-34218063}{417316} : \frac{-1586210641047}{269586136})$	$(13689 : -1600749)$
$(\frac{90297}{121} : \frac{-22360563}{1331})$	$(\frac{-9999}{64} : \frac{3489993}{512})$	$(\frac{1377}{16} : \frac{81297}{64})$
$(\frac{-6490431}{64009} : \frac{99928911681}{16194277})$	$(\frac{15236449}{36100} : \frac{-19149163793}{6859000})$	$(\frac{-30395511}{67600} : \frac{-76755072987}{17576000})$
$(\frac{-80055}{256} : \frac{29404485}{4096})$	$(\frac{29817}{49} : \frac{-3757293}{343})$	$(\frac{762129}{361} : \frac{650642841}{6859})$
$(\frac{-98480511}{200704} : \frac{39192703551}{89915392})$	$(\frac{26689}{64} : \frac{-1270369}{512})$	$(\frac{417897}{784} : \frac{172119627}{21952})$
$(\frac{-1637145647}{8503056} : \frac{-176245968367079}{24794911296})$	$(\frac{-73295}{289} : \frac{-36028855}{4913})$	$(\frac{848313}{9604} : \frac{1032776109}{941192})$
$(\frac{-1679310855}{6635776} : \frac{125347927237875}{17093758976})$	$(\frac{1850970969}{4648336} : \frac{-7795018647261}{10021812416})$	$(\frac{634729}{15876} : \frac{-6456119221}{2000376})$
$(\frac{3969940657}{23716} : \frac{250134989677847}{3652264})$	$(\frac{2877457}{9} : \frac{-4881045223}{27})$	$(\frac{118017}{4} : \frac{40538367}{8})$
$(\frac{-361584728271}{756250000} : \frac{-52898166550379817}{20796875000000})$	$(\frac{146548033}{1089} : \frac{-1774056929599}{35937})$	$(\frac{3560761}{54756} : \frac{30132770797}{12812904})$
$(\frac{-227083553919}{462465025} : \frac{805151488418271}{9945310362625})$		

Primzahl 3	
Ordnung der reduzierten Kurve	7
Erzeuger der reduzierten Kurve	$(2:2)$
Koeffizienten zur Darstellung der Basis	$[3,1,5,5,4]$

$(\frac{39018443272}{4826809} : \frac{7695473229471052}{10604499373})$	$(\frac{1193068}{529} : \frac{1277900684}{12167})$	$(\frac{-11936}{25} : \frac{-325988}{125})$
$(\frac{-3881468}{64009} : \frac{-89586533348}{16194277})$	$(\frac{-294236}{729} : \frac{-116214076}{19683})$	$(\frac{1752124}{2601} : \frac{-1814489956}{132651})$
$(\frac{-761228}{42849} : \frac{-41694006932}{8869743})$	$(\frac{1114408}{49} : \frac{-1176200164}{343})$	$(\frac{7988944}{7569} : \frac{20609968436}{658503})$
$(\frac{-59936}{225} : \frac{-24751988}{3375})$	$(\frac{11272}{9} : \frac{-1122452}{27})$	$(88 : -1124)$
$(\frac{19890968152}{13689} : \frac{-2805329393227412}{1601613})$	$(\frac{28609828}{3969} : \frac{152732557844}{250047})$	$(\frac{285616}{25} : \frac{152523836}{125})$
$(17452 : 2304748)$	$(\frac{-404}{9} : \frac{141668}{27})$	$(\frac{-716}{169} : \frac{9664156}{2197})$
$(\frac{52564}{81} : \frac{9213364}{729})$	$(\frac{-659348}{1521} : \frac{297953612}{59319})$	$(\frac{192628}{49} : \frac{83997836}{343})$
$(\frac{-350636}{2401} : \frac{789979924}{117649})$	$(\frac{-11156}{121} : \frac{8037244}{1331})$	$(496 : 6292)$
$(\frac{2010645316}{2474329} : \frac{-76836109537468}{3892119517})$	$(\frac{470584}{841} : \frac{217909684}{24389})$	$(-488 : 1252)$
$(\frac{15896314984}{8037225} : \frac{-1953854420359148}{22785532875})$	$(520 : -7300)$	$(\frac{-14852}{121} : \frac{-8586044}{1331})$
$(\frac{4176796}{841} : \frac{-8501571748}{24389})$	$(\frac{3629284}{1225} : \frac{-6835911452}{42875})$	$(\frac{32410204}{3249} : \frac{-184324146956}{185193})$
$(\frac{728103480064}{651015225} : \frac{572979364272021988}{16610653465875})$	$(\frac{20729104}{15625} : \frac{89151542308}{1953125})$	$(\frac{-1661456}{4761} : \frac{2252027836}{328509})$
$(\frac{52332712}{131769} : \frac{27125382772}{47832147})$	$(\frac{32404}{81} : \frac{768844}{729})$	$(\frac{-107852}{289} : \frac{-32008724}{4913})$
$(\frac{-3812}{9} : \frac{-144604}{27})$	$(\frac{-355297076}{804609} : \frac{-3403087665004}{721734273})$	$(748 : -16876)$
$(\frac{458308}{729} : \frac{-232098884}{19683})$	$(4 : -4204)$	$(\frac{-96680}{8281} : \frac{-3441878740}{753571})$
$(\frac{36964054264}{648025} : \frac{-7106501309698412}{521660125})$	$(14176 : -1686988)$	$(\frac{95320}{81} : \frac{-27361340}{729})$
$(\frac{2370166408}{7569} : \frac{115389902796956}{658503})$	$(\frac{544}{9} : \frac{-68356}{27})$	$(\frac{155392}{169} : \frac{-54206972}{2197})$

Primzahl 5	
Ordnung der reduzierten Kurve	10
Erzeuger der reduzierten Kurve	$(2:0)$
Koeffizienten zur Darstellung der Basis	$[8,4,1,4,3]$

$(\frac{-535122936}{10144225} : \frac{1742133501420 12}{32309356625})$	$(\frac{8886564}{21025} : \frac{-8619981012}{3048625})$	$(\frac{961236}{25} : \frac{942356484}{125})$
$(\frac{-862583004}{2640625} : \frac{-303714593719 56}{4291015625})$	$(\frac{6689681496}{180625} : \frac{547111731295044}{76765625})$	$(\frac{298476}{25} : \frac{-162950724}{125})$
$(\frac{180077831064}{257763025} : \frac{-61005811491884988}{4138385366375})$	$(\frac{45396}{25} : \frac{9384444}{125})$	$(\frac{-11196}{25} : \frac{-556092}{125})$
$(\frac{83066724}{180625} : \frac{-361505993868}{76765625})$	$(\frac{1197936}{3025} : \frac{-20268684}{166375})$	$(\frac{2376}{25} : \frac{11124}{125})$
$(\frac{314192124}{5175625} : \frac{-29692316623068}{11774546875})$	$(\frac{10044}{25} : \frac{-157572}{125})$	$(\frac{57096}{625} : \frac{12712356}{15625})$
$(\frac{809244}{13225} : \frac{-3807053028}{1520875})$	$(\frac{1443996}{25} : \frac{-1735144956}{125})$	$(\frac{96156}{1225} : \frac{-74256804}{42875})$
$(\frac{126623414844}{625} : \frac{-45057908880476172}{15625})$	$(\frac{76138344}{180625} : \frac{211872878172}{76765625})$	$(\frac{1832616}{625} : \frac{-2452276836}{15625})$
$(\frac{-8496}{25} : \frac{869508}{125})$	$(\frac{-1836}{625} : \frac{68260212}{15625})$	$(\frac{57024}{625} : \frac{12908268}{15625})$
$(\frac{123264}{25} : \frac{43098588}{125})$	$(\frac{1215864}{3025} : \frac{-213012612}{166375})$	$(\frac{-9864}{25} : \frac{-763884}{125})$
$(\frac{2262963207096}{21025} : \frac{-3404209186866847644}{3048625})$	$\frac{1763064}{4225} : \frac{-686274012}{274625})$	$(\frac{-12276}{25} : \frac{3132}{125})$

Primzahl 7	
Ordnung der reduzierten Kurve	11
Erzeuger der reduzierten Kurve	(5 : 1)
Koeffizienten zur Darstellung der Basis	[5, 2, 1, 6, 2]

$(\frac{1234674648}{2019241} : \frac{-31781424877236}{2869341461})$	$(\frac{-5508}{49} : \frac{-2167668}{343})$	$(\frac{7373808}{49} : \frac{20023306164}{343})$
$(\frac{2702502720}{5764801} : \frac{-70748760738060}{13841287201})$	$(\frac{-2805120}{5929} : \frac{1358168580}{456533})$	$(\frac{3348}{49} : \frac{759564}{343})$
$(\frac{259061150412}{3136441} : \frac{131855109987357828}{5554637011})$	$(\frac{2412972}{5929} : \frac{802121508}{456533})$	$(\frac{20953944}{25921} : \frac{81593615844}{4173281})$
$(\frac{-1628550720}{6385729} : \frac{118351360687860}{16136737183})$	$(\frac{273564}{49} : \frac{-142622964}{343})$	$(\frac{-18828}{49} : \frac{2167668}{343})$
$(\frac{45180}{49} : \frac{-8504460}{343})$	$(\frac{20484}{49} : \frac{-873396}{343})$	$(\frac{68076}{49} : \frac{16864308}{343})$
$(\frac{119254556772}{2305248169} : \frac{315004551082942428}{110681880338197})$	$(\frac{-22284}{49} : \frac{-1412748}{343})$	$(\frac{-1168884}{14161} : \frac{9929596788}{1685159})$
$(\frac{194577921756}{19882681} : \frac{-85739866236588348}{88656874579})$	$(\frac{2279232}{41209} : \frac{-22760705052}{8365427})$	$(\frac{-698256}{2401} : \frac{857020716}{117649})$
$(\frac{8184429324}{693889} : \frac{739890131878764}{578009537})$	$(\frac{32904}{49} : \frac{-4660956}{343})$	$(\frac{563544}{5929} : \frac{36458316}{456533})$
$(\frac{9239237568}{5764801} : \frac{-854260000052724}{13841287201})$	$(\frac{24336}{49} : \frac{-2167668}{343})$	

Primzahl 11	
Ordnung der reduzierten Kurve	16
Erzeuger der reduzierten Kurve	(6 : 10)
Koeffizienten zur Darstellung der Basis	[3, 9, 3, 12, 14]

$(\frac{19319976}{14641} : \frac{80167097628}{1771561})$	$(\frac{-17496}{121} : \frac{-8917236}{1331})$	$(\frac{17943480}{20449} : \frac{66397398300}{2924207})$
$(\frac{-7164252}{14641} : \frac{-1667845836}{1771561})$	$(\frac{43856748}{121} : \frac{-290438578044}{1331})$	$(\frac{10771344}{121} : \frac{-35350802244}{1331})$
$(\frac{-59364}{121} : \frac{-628668}{1331})$	$(\frac{11196}{121} : \frac{-895428}{1331})$	$(\frac{123264}{121} : \frac{-39222684}{1331})$
$(\frac{-22032}{121} : \frac{9364356}{1331})$	$(\frac{70287552}{43681} : \frac{-567007452108}{9129329})$	$(\frac{128844}{121} : \frac{42282756}{1331})$
$(\frac{123564301920}{101761} : \frac{43434967407972660}{32461759})$	$(\frac{-3370428}{14641} : \frac{-12912740172}{1771561})$	$(\frac{136152}{121} : \frac{46379412}{1331})$
$(\frac{4307927134212}{12313081} : \frac{8941330795918728708}{43206601229})$	$(\frac{2593188}{121} : \frac{-4174987644}{1331})$	$(\frac{-5878584}{43681} : \frac{-60165811908}{9129329})$
$(\frac{-58284}{121} : \frac{-2896452}{1331})$		

Primzahl 13	
Ordnung der reduzierten Kurve	16
Erzeuger der reduzierten Kurve	(3 : 5)
Koeffizienten zur Darstellung der Basis	[7, 10, 6, 2, 13]

$(\frac{77511065004}{61009} : \frac{21579706260973836}{15069223})$	$(\frac{288180}{169} : \frac{-149489820}{2197})$	$(\frac{1909584}{169} : \frac{2636723556}{2197})$
$(\frac{3913776}{61009} : \frac{35972701452}{15069223})$	$(\frac{252576}{169} : \frac{-121385412}{2197})$	$(\frac{15948}{169} : \frac{-782244}{2197})$
$(\frac{-638048529756}{14828176441} : \frac{-9410679292903921404}{1805641873397011})$	$(\frac{-53208}{169} : \frac{-15741972}{2197})$	$(\frac{576}{169} : \frac{-9267588}{2197})$
$(\frac{12132}{169} : \frac{4529628}{2197})$	$(\frac{57340908}{169} : \frac{434206644444}{2197})$	$(\frac{142164}{169} : \frac{46220004}{2197})$
$(\frac{69228}{169} : \frac{4324644}{2197})$	$(\frac{18679896}{28561} : \frac{-62035462332}{4826809})$	$(\frac{-28512}{169} : \frac{-15223356}{2197})$
$(\frac{-64620}{169} : \frac{13961700}{2197})$	$(\frac{-9685584}{28561} : \frac{-33611150988}{4826809})$	$(\frac{27267984}{48841} : \frac{95884071516}{10793861})$

Primzahl 17	
Ordnung der reduzierten Kurve	25
Erzeuger der reduzierten Kurve	$(0:7)$
Koeffizienten zur Darstellung der Basis	$[13,6,14,22,15]$

$(\frac{117468}{289} : \frac{8418924}{4913})$	$(\frac{-140184}{289} : \frac{8586108}{4913})$	$(\frac{658368}{289} : \frac{-524048076}{4913})$
$(\frac{27072}{289} : \frac{-2452788}{4913})$	$(\frac{-12816}{289} : \frac{25728084}{4913})$	$(\frac{267480}{289} : \frac{-122628060}{4913})$
$(\frac{10116}{289} : \frac{-16594092}{4913})$	$(\frac{66143772}{152881} : \frac{202189975308}{59776471})$	

Primzahl 19	
Ordnung der reduzierten Kurve	24
Erzeuger der reduzierten Kurve	$(12:3)$
Koeffizienten zur Darstellung der Basis	$[5,8,23,18,6]$

$(\frac{5868}{361} : \frac{26727516}{6859})$	$(\frac{-75301308}{190969} : \frac{510436237572}{83453453})$	$(\frac{192132}{361} : \frac{-53549532}{6859})$
$(\frac{-104616}{361} : \frac{49988556}{6859})$	$(\frac{143352}{361} : \frac{3793932}{6859})$	$(\frac{-1224}{361} : \frac{30036852}{6859})$
$(\frac{64059372}{361} : \frac{-512710973532}{6859})$	$(\frac{-99936}{361} : \frac{-50216004}{6859})$	$(\frac{-140350932}{303601} : \frac{620411929524}{167284151})$
$(\frac{6184872}{361} : \frac{15376103532}{6859})$	$(\frac{1120833572328}{255328441} : \frac{-1180469082502593036}{4079893158739})$	$(\frac{704916}{361} : \frac{576589212}{6859})$
$(\frac{-87372}{361} : \frac{50195484}{6859})$	$(\frac{-177264}{361} : \frac{356508}{6859})$	

Primzahl 23	
Ordnung der reduzierten Kurve	32
Erzeuger der reduzierten Kurve	$(10:7)$
Koeffizienten zur Darstellung der Basis	$[21,14,12,13,23]$

$(\frac{-49104}{529} : \frac{73582452}{12167})$	$(\frac{2827116}{279841} : \frac{-600100301268}{148035889})$	$(\frac{2300832}{529} : \frac{-3471589908}{12167})$
$(\frac{211464}{529} : \frac{12333924}{12167})$	$(\frac{249708276}{444889} : \frac{2672436739068}{296740963})$	$(\frac{-160812}{529} : \frac{87947316}{12167})$
$(\frac{39780}{529} : \frac{-23123340}{12167})$	$(\frac{217008}{529} : \frac{-24491916}{12167})$	

Primzahl 29	
Ordnung der reduzierten Kurve	36
Erzeuger der reduzierten Kurve	$(1:13)$
Koeffizienten zur Darstellung der Basis	$[35,5,33,29,14]$

$(\frac{38772}{841} : \frac{73995228}{24389})$	$(\frac{-52380}{841} : \frac{-135613980}{24389})$	$(\frac{-51480}{841} : \frac{-135162540}{24389})$
$(\frac{446868}{841} : \frac{189532764}{24389})$	$(\frac{-60645511148004}{216778704025} : \frac{738352340523329698044}{100931080700519875})$	$(\frac{-382824}{841} : \frac{99926028}{24389})$

In der Menge S liegen keine Primzahlen mit schlechter Reduktion. Als letztes werden die noch fehlenden ganzen Punkte bestimmt.

ganze Punkte		
(55656 : −13129668)	(45548136 : −307401450948)	(372941316 : −7202126555028)
(1188 : 38124)	(36 : 3348)	(22392 : 3350052)
(−468 : −3348)	(2448 : −119124)	(7092 : −596052)
(576 : 9612)	(720 : −15660)	(3204 : 179604)
(1348776 : −1566425412)	(2916 : −155628)	(−72 : −5724)
(8388 : 767124)	(−36 : 5076)	(163872 : 66336948)
(4320 : 282420)	(396 : 108)	(1526904 : −1886763996)
(7272 : −618948)	(90108 : −27048276)	(53856 : 12497868)
(432 : 3348)	(1404 : −50004)	(−180 : −7020)
(157212 : 62334252)	(72 : −2052)	(−216 : 7236 : 1)
(1944 : −83484)		

Das Programm benötigte ungefähr 17 Minuten zur Berechnung. Etwa 30% der Rechenzeit wurde zum Berechnen der Abschätzung gebraucht und etwa 50% zum Suchen der echt rationalen Punkte. Die restlichen 20% wurden benötigt um die ganzen Punkte zu bestimmen. Das Verfahren brauchte mit einfachem Durchprobieren aller Möglichkeiten etwa 100 mal so lange wie mit den Reduktionsmethoden und etwa 70% der Zeit die die entsprechende Funktion in Magma benötigt.

A.2 Kurven über Zahlkörpern

Beispiel 2

Die Kurve E ist gegeben durch

$$E : y^2 + (\theta^2 - \theta)xy + y = x^3 + \theta^2 x + 1$$

über dem Zahlkörper

$$\mathbb{K} = \mathbb{Q}(\theta) \text{ mit } \theta^4 + \theta^3 + \theta^2 + \theta + 1 = 0.$$

Die Menge der vorgegeben Primzahlen S_1 lautet:

$$S_1 := \{2, 3, 5, 7\}.$$

Die zugehörigen Stellen sind

$$S := \{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7\}.$$

Schlechte Reduktion liegt bei den folgenden Stellen vor:

Primzahlen mit schlechter Reduktion		
Stelle	Reduktionstyp	Tamagawazahl
$\mathfrak{p}_{9873373}$	multiplikativ	1
$\mathfrak{p}_{4231}$	multiplikativ	1

Es wurde folgende Basis verwendet:

$$\begin{aligned} B \;:=\; & \{(0:\theta^3+\theta^2),(\theta^3+\theta^2:-\theta^2-2),\\ & (-5\theta^3-\theta^2-3\theta-4:-4\theta^3-5\theta^2-9)\}. \end{aligned}$$

Die Konstante c_2 aus Kapitel 1 beträgt etwa 0.69315, und der minimale Eigenwert der Regulatormatrix ist etwa 0.32986. Die Konstante N beträgt ungefähr $9.77739 \cdot 10^{4284}$. Nach der Reduktion aus Kapitel 3 lauten die einzelnen Schranken:

Reduzierte Schranken								
Stelle	∞_1	∞_2	∞_3	∞_4	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_5$	$\mathfrak{p}_7$
Schranke	5	5	3	3	6	12	119	10

In der folgenden Tabelle werden alle S-ganzen Punkte nach den einzelnen Primzahlen, bezüglich denen die Kurve reduziert wurde, sortiert angegeben. Die angegebenen Ordnungen und Erzeuger beziehen sich dabei immer auf die reduzierte Kurve. Die Koeffizienten werden verwendet um die reduzierten Elemente der Mordell-Weil-Basis durch den Erzeuger der reduzierten Kurve darzustellen. Bezüglich der Stellen $\mathfrak{p}_3$ und $\mathfrak{p}_7$ wurden keine Punkte gefunden.

Stelle $\mathfrak{p}_2$	
Ordnung der reduzierten Kurve	22
Erzeuger der reduzierten Kurve	$(\theta^3+1:\theta^3+1)$
Koeffizienten zur Darstellung der Basis	$[8,4,17]$
$(1/4(8\theta^3+5\theta^2+\theta+11):1/8(27\theta^3+7\theta^2+13\theta+29)$	

Stelle $\mathfrak{p}_3$	
Ordnung der reduzierten Kurve	72
Erzeuger der reduzierten Kurve	$(0:2\theta^3+2\theta^2+2)$
Koeffizienten zur Darstellung der Basis	$[71,62,33]$

E ist bezüglich der Stelle $\mathfrak{p}_5$ nicht minimal. Ein minimales Modell ist gegeben durch:

$$E_{\min}: y^2 = x^3 + 1/48(77\theta^2-29\theta+5)x + 1/864(251\theta^3+195\theta^2+87\theta+1547).$$

Die Transformation ist gegeben durch

$$x_{\min} := x + \frac{1}{2}(-3\theta^3 - \theta - 1) \text{ und } y_{\min} = y + \frac{1}{2}(\theta^2 - \theta)x + \frac{1}{2}.$$

Deshalb ist es möglich, dass auch ganze Punkte oder Punkte mit einer der anderen Stellen im Nenner bei der Suche bezüglich $\mathfrak{p}_5$ gefunden werden.

Stelle $\mathfrak{p}_5$	
Ordnungen der beiden Erzeuger	2, 2
Erzeuger der reduzierten Kurve	$(0:2), (3:2)$
Koeffizienten zur Darstellung der Basis	$[1,1,1], [2,1,1]$

$(1/5(-2\theta^2 - \theta - 1) : 1/25(-37\theta^3 - 27\theta^2 - 5\theta - 31))$

$(1/5(62\theta^3 + 198\theta^2 + 218\theta + 92) : 1/5(-967\theta^3 - 1421\theta^2 - 736\theta + 144))$

$(1/5(2\theta^3 - 9\theta^2 + 7\theta - 16) : 1/25(186\theta^3 + 101\theta^2 + 55\theta + 183))$

$(1/5(-4\theta^3 + 2\theta + 3) : 1/25(7\theta^3 - 13\theta^2 - 15\theta - 29))$

$(1/5(3\theta^3 + 6\theta + 11) : 1/5(-16\theta^3 - 8\theta^2 + 10\theta - 6))$

$(-5\theta^3 - \theta^2 - 3\theta - 4 : -4\theta^3 - 5\theta^2 - 9)$

Stelle $\mathfrak{p}_7$	
Ordnungen der beiden Erzeuger	$2, 1156$
Erzeuger der reduzierten Kurve	$(6\theta^3 + \theta^2 + 2\theta + 4 : 4\theta^3 + 3\theta + 1)$, $(6\theta^3 + 2\theta^2 + 4\theta + 6 : 3\theta^3 + 2\theta^2 + 6\theta + 1)$
Koeffizienten der Basiselemente	$[1,2,2], [955, 630, 851]$

Es liegt keine Stelle mit schlechter Reduktion in S vor.

Zuletzt werden die ganzen Punkte bestimmt:

ganze Punkte	
$(-116\theta^3 - 183\theta^2 - 106\theta + 7 : -17316\theta^3 - 3226\theta^2 - 2420\theta - 426)$	$(7\theta^3+3\theta^2+3\theta+9 : 24\theta^3+3\theta^2+15\theta+20)$
$(3\theta^3 + 7\theta^2 - 3\theta + 11 : 2\theta^3 - 37\theta^2 + 25\theta - 38)$	$(0 : -\theta^3 - \theta^2 - 1)$
$(8\theta^3 + 2\theta^2 - 8\theta - 9 : -43\theta^3 - 83\theta^2 - 65\theta - 17)$	$(-\theta^3 - \theta^2 : \theta^3 + \theta^2)$
$(\theta^3 + \theta^2 : \theta^3 + \theta^2)$	

Etwa 97% der Rechenzeit wurde zur Bestimmung der Schranken verwendet, und 2% fielen auf die Berechnung der ganzen Punkte. Für die Bestimmung der echt rationalen S-ganzen Punkte wurde nur knapp 1% der Rechenzeit benötigt. Ein Vergleich mit der Rechenzeit für die Suche ohne Reduktion war nicht möglich, weil die maximale Schranke mit 119 dafür zu groß war.

Beispiel 3

Die Kurve E ist gegeben durch

$$E : y^2 + (2\theta^3 - 2\theta^2 - 2)y = x^3 + (-3\theta^3 - \theta + 1)x^2 + (-12\theta^2 - 8\theta - 12)x$$

über dem Zahlkörper

$$\mathbb{K} = \mathbb{Q}(\theta) \text{ mit } \theta^4 - \theta^3 + \theta^2 - \theta + 1 = 0.$$

Die Menge der vorgegeben Primzahlen S_1 lautet:

$$S_1 := \{2, 3, 11\}.$$

Die zugehörigen Stellen sind

$$S := \{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_{11,1}, \mathfrak{p}_{11,2}, \mathfrak{p}_{11,3}, \mathfrak{p}_{11,4}\}.$$

Schlechte Reduktion liegt bei den folgenden Stellen vor:

Primzahlen mit schlechter Reduktion		
Stelle	Reduktionstyp	Tamagawazahl
$\mathfrak{p}_2$	additiv	2
$\mathfrak{p}_{75740880221}$	multiplikativ	1

Es wurde folgende Basis verwendet:

$$\begin{aligned} B \quad := \quad & \{(0:0), (\theta^3 + 2\theta^2 + 2\theta + 2 : -5\theta^3 - 3\theta + 2), \\ & (2\theta^2 + 2 : -6\theta^3 + 2\theta^2 - 2\theta + 6), (2\theta^2 + 2\theta + 2 : -2)\} \end{aligned}$$

Die Konstante c_2 aus Kapitel 1 beträgt etwa 0.69315, und der minimale Eigenwert der Regulatormatrix ist etwa 0.49328. Die Konstante N beträgt ungefähr $1.91993 \cdot 10^{5453}$. Nach der Reduktion aus Kapitel 3 lauten die einzelnen Schranken:

Reduzierte Schranken										
Stelle	∞_1	∞_2	∞_3	∞_4	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{11,1}$	$\mathfrak{p}_{11,2}$	$\mathfrak{p}_{11,3}$	$\mathfrak{p}_{11,4}$
Schranke	3	3	3	3	10	15	2	2	2	121

In der folgenden Tabelle werden alle S-ganzen Punkte nach den einzelnen Primzahlen, bezüglich denen die Kurve reduziert wurde, sortiert angegeben. Die angegebenen Ordnungen und Erzeuger beziehen sich dabei immer auf die reduzierte Kurve. Die Koeffizienten werden verwendet um die reduzierten Elemente der Mordell-Weil-Basis durch den Erzeuger der reduzierten Kurve darzustellen.

Stelle $\mathfrak{p}_3$	
Ordnung der reduzierten Kurve	96
Erzeuger der reduzierten Kurve	$(0:0)$
Koeffizienten zur Darstellung der Basis	$[1, 17, 28, 9]$

$$(1/1089(-244\theta^3 + 2077\theta^2 + 665\theta + 2850) : 1/35937(-210403\theta^3 + 106562\theta^2 - 67030\theta + 235777))$$

Stelle $\mathfrak{p}_{11,1}$	
Ordnung der reduzierten Kurve	12
Erzeuger der reduzierten Kurve	$(3:10)$
Koeffizienten zur Darstellung der Basis	$[3,2,10,11]$

$$(1/121(56449\theta^3 - 138822\theta^2 + 132274\theta - 47486) :$$
$$1/1331(-3781863\theta^3 + 41106144\theta^2 - 6040801 7\theta + 35033426))$$
$$(1/121(-9983\theta^3 + 1454\theta^2 - 5270\theta + 7522) : 1/1331(-958817\theta^3 - 202744\theta^2 - 716247\theta + 390140))$$
$$(1/121(-244\theta^3 - 234\theta^2 - 268\theta - 162) : 1/1331(3526\theta^3 - 9506\theta^2 - 4982\theta - 13990))$$
$$(1/484(-76\theta^3 - 59\theta^2 - 262\theta + 257) : 1/10648(1871\theta^3 + 27001\theta^2 + 18515\theta + 12885))$$
$$(1/1771561(4844526\theta^3 - 525094\theta^2 - 4820729\theta + 2149541) :$$
$$1/2357947691(6188729725\theta^3 + 57281552 93\theta^2 - 217991094 71\theta + 5395746452))$$
$$(1/121(-244\theta^3 - 476\theta^2 - 510\theta - 404) : 1/1331(-27450\theta^3 + 23890\theta^2 - 3046\theta + 40460))$$

Stelle $\mathfrak{p}_{11,2}$	
Ordnung der reduzierten Kurve	12
Erzeuger der reduzierten Kurve	$(1:7)$
Koeffizienten zur Darstellung der Basis	$[2,6,11,8]$

$$(1/484(5684\theta^3 + 125\theta^2 + 4150\theta - 2187) : 1/10648(-488989\theta^3 + 153667\theta^2 - 176445\theta + 478229))$$
$$(1/121(-69\theta^3 + 92\theta^2 - 19\theta + 35) : 1/1331(-5308\theta^3 + 2560\theta^2 - 3096\theta + 4646))$$
$$(1/14641(607246\theta^3 - 453518\theta^2 + 997 35\theta - 814731) :$$
$$1/1771561(-5302400 53\theta^3 - 284933793\theta^2 - 503178333\theta + 42314112))$$
$$(1/121(51\theta^3 - 68\theta^2 - 7\theta - 89) : 1/1331(-2784\theta^3 + 4438\theta^2 + 980\theta + 6168))$$
$$(1/484(-5817\theta^3 + 2553\theta^2 - 2796\theta + 5902) : 1/10648(-585246\theta^3 + 68364\theta^2 - 314488\theta + 441501))$$

Stelle $\mathfrak{p}_{11,3}$	
Ordnung der Reduzierten Kurve	18
Erzeuger der Reduzierten Kurve	$(8:2)$
Koeffizienten zur Darstellung der Basis	$[2,15,1,12]$

$$(1/121(4248\theta^3 - 4720\theta^2 - 202\theta - 7264) : 1/1331(674094\theta^3 + 102282\theta^2 + 478890\theta - 314452))$$
$$(1/121(-212\theta^3 + 370\theta^2 - 159\theta + 270) : 1/1331(-11420\theta^3 + 4192\theta^2 - 2757\theta + 6241))$$

Stelle $\mathfrak{p}_{11,4}$	
Ordnung der Reduzierten Kurve	13
Erzeuger der Reduzierten Kurve	$(5:0)$
Koeffizienten zur Darstellung der Basis	$[10,10,9,5]$

$$(1/484(1325\theta^3 + 665\theta^2 + 1269\theta + 564) : 1/10648(-97975\theta^3 + 1344\theta^2 - 54290\theta + 69794))$$
$$(1/121(284\theta^3 - 178\theta^2 - 50\theta - 318) : 1/1331(1480\theta^3 - 3184\theta^2 - 840\theta - 4326))$$

An der Stelle $\mathfrak{p}_2$ liegt schlechte Reduktion vor. Sie muss also gesondert betrachtet werden.

Für $\mathfrak{p}_2$ ist die Tamagawazahl 2. Der singuläre Punkt ist $(1:1)$. Ein Erzeugendensystem von E_0 ist gegeben durch

$$\begin{aligned}&\{B_2, B_3 - B_1, B_4 - B_1, 2B_1\} = \\ &\{(\theta^3 + 2\theta^2 + 2\theta + 2 : -5\theta^3 - 3\theta + 2),\\ &\ (4\theta^3 - 3\theta^2 + \theta - 6 : -7\theta^3 - 4\theta^2 - 6\theta + 1),\\ &\ (2\theta^3 - 2\theta^2 - \theta - 3 : 3\theta^3 - \theta^2 + \theta - 4),\\ &\ (35\theta^3 + 20\theta^2 + 33\theta - 1 : -464\theta^3 + 10\theta^2 - 280\theta + 296)\}.\end{aligned}$$

Die Reduktionsabbildung lautet:

$$\begin{aligned} a_a : E_0(\mathbb{K}) &\rightarrow \mathbb{F}_{\mathfrak{p}_2} \\ (x, y) &\mapsto \frac{x-1}{y} \end{aligned}$$

Stelle $\mathfrak{p}_2$
$(1/4(\theta^3 - 3\theta^2 + \theta) : 1/8(-11\theta^3 - 12\theta + 2))$

Zuletzt werden die ganzen Punkte bestimmt:

ganze Punkte	
$(35\theta^3 + 20\theta^2 + 33\theta - 1 : 462\theta^3 - 8\theta^2 + 280\theta - 294)$	$(2\theta^2 + 2\theta + 2 : -2\theta^3 + 2\theta^2 + 4)$
$(4\theta^3 - 2\theta^2 - 2\theta - 2 : 8\theta - 2)$	$(3\theta^3 - 5\theta^2 - \theta - 6 : 19\theta^3 - 3\theta^2 + 10\theta - 15)$
$\theta^3 - 2\theta^2 + 2\theta - 6 : -7\theta^3 + 10\theta^2 - 7\theta + 2)$	$(0 : -2\theta^3 + 2\theta^2 + 2)$
$(2\theta^3 - 2\theta^2 - \theta - 3 : 3\theta^3 - \theta^2 + \theta - 4)$	$(4\theta^3 - 3\theta^2 + \theta - 6 : -7\theta^3 - 4\theta^2 - 6\theta + 1)$
$(4\theta^3 + 4\theta^2 - 14\theta + 12 : 2\theta^3 + 54\theta^2 - 82\theta + 52)$	$(4\theta^3 + 2\theta^2 - 7\theta + 6 : -6\theta^3 - 18\theta^2 + 35\theta - 17)$
$(-12\theta^3 + 20\theta^2 + 4\theta + 28 : 64\theta^3 - 128\theta^2 - 40\theta - 168)$	$(\theta^3 + 2\theta^2 + 2\theta + 2 : 3\theta^3 + 2\theta^2 + 3\theta)$
$(-28\theta^3 - 20\theta^2 - 28\theta : -122\theta^3 + 258\theta^2 + 80\theta + 330)$	$(-\theta^3 - \theta^2 + 3\theta + 2 : -11\theta^3 + \theta^2 + 2\theta + 5)$
$(20\theta^3 - 4\theta^2 + 10\theta - 16 : -44\theta^3 + 60\theta^2 + 10\theta + 86)$	$(2\theta^2 + 2 : 4\theta^3 + 2\theta - 4)$
$(-2\theta^3 - 14\theta^2 - 10\theta - 13 : -128\theta^3 + 65\theta^2 - 39\theta + 143)$	$(8\theta^3 - 6\theta^2 + \theta - 10 : -24\theta^3 - 10\theta^2 - 21\theta + 5)$
$(56\theta^3 + 24\theta^2 - 112\theta + 112 : -256\theta^3 - 1168\theta^2 + 2384\theta - 1616)$	

Etwa 60% der Rechenzeit wurde zur Bestimmung der Schranken verwendet. Jeweils 20% fielen auf die Berechnung der ganzen Punkte und der echt rationalen S-ganzen Punkte. Ein Vergleich mit der Rechenzeit für die Suche ohne Reduktion war nicht möglich, weil die maximale Schranke mit 121 dafür zu groß war.

Beispiel 4

Die Kurve E ist gegeben durch

$$E : y^2 = x^3 + (\theta^3 - 1)x + 1$$

über dem Zahlkörper

$$\mathbb{K} = \mathbb{Q}(\theta) \text{ mit } \theta^5 - 2\theta^2 + 1 = 0.$$

Die Menge der vorgegeben Primzahlen S_1 lautet:

$$S_1 := \{2, 3, 5\}.$$

Die zugehörigen Stellen sind

$$S := \{\mathfrak{p}_2, \mathfrak{p}_{3,1}, \mathfrak{p}_{3,2}, \mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}\}.$$

Schlechte Reduktion liegt bei den folgenden Stellen vor:

Primzahlen mit schlechter Reduktion		
Stelle	Reduktionstyp	Tamagawazahl
$\mathfrak{p}_2$	additiv	1
$\mathfrak{p}_{3,1}$	additiv	2
$\mathfrak{p}_{2300279}$	multiplikativ	1

Es wurde folgende Basis verwendet:

$$\begin{aligned} B \quad := \quad & \{(0:1), (\theta + 1 : \theta^2 + \theta + 1), \\ & (2\theta^4 - 3\theta^3 + 3\theta^2 - \theta + 1 : 7\theta^4 - 10\theta^3 + 12\theta^2 - 6\theta + 6)\}. \end{aligned}$$

Die Konstante c_2 aus Kapitel 1 beträgt etwa 0.69315, und der minimale Eigenwert der Regulatormatrix ist etwa 0.26552. Die Konstante N beträgt ungefähr $7.25281 \cdot 10^{5285}$. Nach der Reduktion aus Kapitel 3 lauten die einzelnen Schranken:

Reduzierte Schranken										
Stelle	∞_1	∞_2	∞_3	∞_4	∞_5	$\mathfrak{p}_2$	$\mathfrak{p}_{3,1}$	$\mathfrak{p}_{3,2}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
Schranke	6	4	4	4	4	7	5	649	11	15

In der folgenden Tabelle werden alle S-ganzen Punkte nach den einzelnen Primzahlen, bezüglich denen die Kurve reduziert wurde, sortiert angegeben. Die angegebenen Ordnungen und Erzeuger beziehen sich dabei immer auf die reduzierte Kurve. Die Koeffizienten werden verwendet um die reduzierten Elemente der Mordell-Weil-Basis durch den Erzeuger der reduzierten Kurve

darzustellen. Bezüglich der Stellen $\mathfrak{p}_{3,2}$, $\mathfrak{p}_{5,1}$ und $\mathfrak{p}_{5,2}$ wurden keine S-ganzen Punkte gefunden.

Stelle $\mathfrak{p}_{3,2}$	
Ordnung der reduzierten Kurve	91
Erzeuger der reduzierten Kurve	$(2\theta^2+\theta+1 : 2\theta^3+\theta^2+2\theta+2)$
Koeffizienten zur Darstellung der Basis	$[48, 75, 10]$

Stelle $\mathfrak{p}_{5,1}$	
Ordnung der reduzierten Kurve	36
Erzeuger der reduzierten Kurve	$(1 : 4\theta+1)$
Koeffizienten zur Darstellung der Basis	$[30, 21, 13]$

Stelle $\mathfrak{p}_{5,2}$	
Ordnung der reduzierten Kurve	144
Erzeuger der reduzierten Kurve	$(3\theta^2+3\theta : 4\theta+3)$
Koeffizienten zur Darstellung der Basis	$[138, 52, 17]$

An den Stellen $\mathfrak{p}_2$ und $\mathfrak{p}_{3,1}$ liegt schlechte Reduktion vor. Sie müssen also gesondert betrachtet werden.
Für $\mathfrak{p}_2$ ist die Tamagawazahl 1. Alle Punkte der Kurve werden also mittels der Reduktionsabbildung auf nicht-singuläre Punkte abgebildet. Das Erzeugendensystem von E_0 ist demnach gleich der Mordell-Weil-Basis B. Die Reduktionsabbildung a_a lautet:

$$\begin{aligned} a_a : E_0(\mathbb{K}) &\rightarrow \mathbb{F}_{\mathfrak{p}_2} \\ (x,y) &\mapsto \frac{x-\theta^{30}}{y-\theta^{30}x-\theta^{30}} \end{aligned}$$

Die gefundenen Punkte sind:

Stelle $\mathfrak{p}_2$
$(1/4(16\theta^4-2\theta^3-10\theta^2+19\theta+7) : 1/8(-82\theta^4+37\theta^3+48\theta^2-121\theta+21))$
$(1/4(-3\theta^3-\theta+1) : 1/8(\theta^4-7\theta^3-4\theta-7))$
$(1/36(94\theta^4-26\theta^3-29\theta^2-37\theta-79) : 1/216(-1294\theta^4-1192\theta^3-1180\theta^2-635\theta-350))$
$1/4(891\theta^4-1073\theta^3+1270\theta^2-628\theta+752) : 1/8(74523\theta^4-89007\theta^3+106214\theta^2-52309\theta+62433))$

Für $\mathfrak{p}_{3,1}$ ist die Tamagawazahl 2. Die Basiselemente B_2 und B_3 werden auf den singulären Punkt abgebildet. Ein Erzeugendensystem von E_0 lautet:

$$\begin{aligned} &\{B_1, B_3-B_2, 2B_2\} = \\ &\{(\tfrac{1}{4}(16\theta^4-2\theta^3-10\theta^2+19\theta-1) : \tfrac{1}{8}(-82\theta^4+37\,\theta^3+48\theta^2-121\theta+21)) \\ &\ (\tfrac{1}{361}(-348\theta^4+214\theta^3+246\theta^2-325\theta-296) : \\ &\quad \tfrac{1}{6859}(6696\theta^4+177\theta^3-613\theta^2+15988\theta+2795)), (-2:1)\}. \end{aligned}$$

Die Reduktionsabbildung a_a lautet:

$$\begin{aligned} a_a : E_0(\mathbb{K}) &\rightarrow \mathbb{F}_{\mathfrak{p}_{3,1}} \\ (x,y) &\mapsto \frac{x-1}{y} \end{aligned}$$

Die gefundenen Punkte sind:

Primzahl $\mathfrak{p}_{3,1}$
$(1/6561(-351344\theta^4 - 145760\theta^3 + 302968\theta^2 - 338656\theta - 381952) :$
$1/531441(1404254 72\theta^4 - 3301032 64\theta^3 + 1157696\theta^2 + 3718989 76\theta - 404925677))$
$(1/9(4\theta^4 + 10\theta^3 - 2\theta^2 - \theta + 2) : 1/27(-2\theta^4 - 23\theta^3 + 19\theta^2 + 14\theta - 1))$
$(1/81(493\theta^4 - 392\theta^3 + 487\theta^2 - 211\theta + 314) : 1/729(208336\theta^4 - 238196\theta^3 + 29440\theta^2 - 13315\theta + 17612))$

Als letztes werden die noch fehlenden ganzen Punkte bestimmt.

ganze Punkte
$(0 : -1)$
$(\theta + 1 : -\theta^2 - \theta - 1)$
$(\theta^4 - \theta^2 + \theta + 2 : -3\theta^4 - \theta^3 + 2\theta^2 - 3\theta - 2)$
$(\theta^2 - \theta - 1 : \theta^3 - \theta^2 - \theta + 1)$
$(2\theta^4 - \theta^3 - 2\theta^2 + 3\theta : 3\theta^4 - 3\theta^3 - \theta^2 + 7\theta - 3)$
$(-22\theta^4 - 5\theta^3 + 18\theta^2 + 11\theta + 24 : 159\theta^4 - 3\theta^3 - 193\theta^2 - 127\theta - 205)$
$(2\theta^4 - 3\theta^3 + 3\theta^2 - \theta + 1 : -7\theta^4 + 10\theta^3 - 12\theta^2 + 6\theta - 6)$
$(16\theta^4 - 20\theta^3 + 25\theta^2 - 13\theta + 15 : -198\theta^4 + 235\theta^3 - 279\theta^2 + 137\theta - 165)$

Gut 95% der Rechenzeit wurde zum Berechnen der Abschätzungen gebraucht und der Rest fast ausschließlich zum Suchen der echt rationalen Punkte. Die Zeit zur Bestimmung der ganzen Punkte fiel dabei kaum ins Gewicht, da die Schranken zur Bestimmung der rationalen Punkte wesentlich größer waren. Ein Vergleich zu dem Verfahren mit einfachem Durchprobieren aller Möglichkeiten war nicht möglich, da die maximale Schranke mit 649 dafür einfach zu groß war.

Anhang B

Algorithmen

In diesem Abschnitt werden die wichtigesten Algorithmen, die zur Bestimmung S-ganzer Punkte benötigt werden, als Pseudocode angegeben.

Kapitel 1. Grundlagen – elliptische Kurven

Folgender Algorithmus wird zum Beschleunigen der Punktaddition auf elliptischen Kurven verwendet.

Algorithmus 2 : double and add

Input : Punkt P, Skalar k
Output : kP
t :=Binärdarstellung von k;
$P_1 := \mathcal{O}_E$;
$P_2 := P$;
for $i = 1 \ldots$ Länge(t) **do**
  if $t[i] = 1$ **then**
    $P_1 := P_1 + P_2$;
  end
  $P_2 := 2P_2$;
end
return PP;

Kapitel 1. Grundlagen – wichtige Algorithmen

Folgender Algorithmus dient zur Berechnung des elliptischen Integrals bei der Bestimmung der Perioden und elliptischen Logarithmen einer Kurve.

Algorithmus 3 : Carlson

Input : die Koordinaten des Punktes x, y, z, die gewünschte Präzision r

Output : der Wert des elliptischen Integrals R

$x_0 := x;$
$y_0 := y;$
$z_0 := z;$
$A_0 := (x + y + z)/3;$
$Q := (3r)^{-1/6} \max\{|A_0 - x|, |A_0 - y|, |A_0 - z|\};$
while $4^{-n}Q < |A_n|$ **do**
  $\lambda_n := \sqrt{x_n}\sqrt{y_n} + \sqrt{x_n}\sqrt{z_n} + \sqrt{y_n}\sqrt{z_n};$
  $A_{n+1} := (A_n + \lambda_n)/4;$
  $x_{n+1} := (x_n + \lambda_n)/4;$
  $y_{n+1} := (y_n + \lambda_n)/4;$
  $z_{n+1} := (z_n + \lambda_n)/4;$
end
$X := (A_0 - x)/(4^n A_n);$
$Y := (A_0 - y)/(4^n A_n);$
$Z := -X - Y;$
$E_2 := XY - Z^2;$
$E_3 := XYZ;$
$R := A_n^{-1/2}\left(1 - E_2/10 + E_3/14 + E_2^2/24 - 3E_2E_3/44\right);$
return R;

Mit den nächsten beiden Algorithmen wird getestet, ob ein bestimmter Punkt S-ganz ist.

Algorithmus 4 : Einmalige Bestimmung der $\alpha_{\mathfrak{p}}$

Input : Menge von Stellen S
Output : Menge von Stellen $\mathcal{P}$, Liste mit Zufallselementen α
$\mathcal{P} := \emptyset$;
$\alpha := \emptyset$;
for $\mathfrak{p} \in S$ **do**
  while $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \geq 1$ **do**
    $\alpha_{\mathfrak{p}}$:=Zufallszahl($\mathbb{Z}_{\mathbb{K}}$);
  end
  $\alpha(\mathfrak{p}) := \alpha_{\mathfrak{p}}$;
  a:=Faktorisierung(Ideal($\alpha(\mathfrak{p})$));
  for $i := 1 \ldots \#a$ **do**
    if Stelle($a[i]$) $\notin S$ **then**
      $\mathcal{P} := \{\text{Stelle}(a[i])\} \cup \mathcal{P}$;
    end
  end
end
return $\mathcal{P}$, α;

Algorithmus 5 : Test auf S-Ganzheit

Input : Punkt $P = (x, y)$, Menge mit Stellen S, Menge mit Stellen $\mathcal{P}$ aus Alg. 4, Zufallselemente α aus Alg. 4
Output : $wahr$, wenn P S-ganz oder $falsch$, wenn P nicht S-ganz
for $\mathfrak{q} \in \mathcal{P}$ **do**
  if $v_{\mathfrak{q}}(x) < 0$ **then**
    return $falsch$;
  end
end
$A := x$;
for $\mathfrak{p} \in S$ **do**
  $A := A\alpha(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$;
end
if $A \in \mathbb{Z}_{\mathbb{K}}$ **then**
  return $wahr$;
else
  return $falsch$;
end

Kapitel 3. Reduktion der Schranken – Grundlagen zur LLL-Reduktion

Der folgende Algorithmus dient dazu, die LLL-Reduktion eines Gitters zu berechnen:

Algorithmus 6 : LLL-Algorithmus nach De Weger

Input : Matrix B, mit Basisvektoren als Spalten
Output : Matrix B, mit reduzierten Basisvektoren als Spalten
Λ, D :=Gram-Schmidt(B);
k:=2;
while $k > n$ **do**
  k, l, B, Λ, D :=Bedingung1$(k, k-1, B, \Lambda, D)$;
  if $4D_{k-2}D_k < (3D_{k-1}^2 - 4{\lambda_{k,k-1}}^2)$ **then**
    k, B, Λ, D :=Tausch(k, B, Λ, D);
    if $k > 2$ **then**
      $k := k - 1$;
    end
  else
    for $l = k - 1 \ldots 1$ **do**
      Λ, D :=Gram-Schmidt(B);
    end
    $k := k + 1$;
  end
end
return B;

Der LLL-Algorithmus bedient sich dabei der drei nachfolgenden Algorithmen:

Zum Berechnen der Konstantnen, die bei der Anwendung der Gram-Schmidt Orthonormalisierung auftreten:

Algorithmus 7 : Gram-Schmidt mit ganzzahligen Werten

Input : $n \times n$ Matrix B mit den Basisvektoren $\vec{b}_i$ als Spalten
Output : $n \times n$ Matrix Λ mit den Einträgen $\lambda_{i,j}$; Vektor D mit den Einträgen $D_i = \det(\langle \vec{b}_j, \vec{b}_l \rangle_{1 \leq j,l \leq i})$

$D_0 := 1$;
for $i = 1 \ldots n$ **do**
  $\vec{b}_i^* := \vec{b}_i$;
  for $j = 1 \ldots i-1$ **do**
    $\lambda_{i,j} := \langle \vec{b}_i, \vec{b}_j^* \rangle$;
    $\vec{b}_i^* := (D_j \vec{b}_i^* - \lambda_{i,j} \vec{b}_j^*)/D_{j-1}$;
  end
  $D_i := \langle \vec{b}_i^*, \vec{b}_i^* \rangle / D_{i-1}$;
end
return Λ,D;

Um sicher zu stellen, dass die Bedingung 1, $|\lambda_{k.l}| \leq \frac{1}{2}$, aus Definition 3.2 erfüllt ist:

Algorithmus 8 : Bedingung1

Input : ganze Zahlen k, l; $n \times n$ Matrizen B, Λ: Vektor D
Output : ganze Zahlen k, l; $n \times n$ Matrizen B, Λ: Vektor D
if $2|\lambda_{k,l}| > D_l$ **then**
  $r := [\lambda_{k,l}/D_l]$;
  $\vec{b}_k := \vec{b}_k - r\vec{b}_l$;
  for $j = 1 \ldots l-1$ **do**
    $\lambda_{k,j} = \lambda_{k,j} - r\lambda_{l,j}$
  end
  $\lambda_{k,l} := \lambda_{k,l} - rD_l$;
end
return k, l, B, Λ, D;

Um zwei Vektoren $\vec{b}_k$ und $\vec{b}_{k-1}$ der gegebenen Matrix zu vertauschen:

Algorithmus 9 : Tausch

Input : ganze Zahl k, $n \times n$ Matrizen B, Λ, Vektor D
Output : ganze Zahl k, $n \times n$ Matrizen B, Λ, Vektor D
Vertausche $\vec{b}_k$ und $\vec{b}_{k-1}$;
for $j = 1 \dots k-2$ **do**
  Vertausche $\lambda_{k-1,j}$ und $\lambda_{k,j}$
end
for $i = k+1 \dots n$ **do**
  $t := \lambda_{i,k-1}$;
  $\lambda_{i,k-1} := (\lambda_{i,k-1}\lambda_{k,k-1} + \lambda_{i,k}D_{k-2})/D_{k-1}$;
  $\lambda := (tD_k - \lambda_{i,k}\lambda_{k,k-1})/D_{k-1}$;
end
$D_{k-1} := (D_{k-2}D_k + {\lambda_{k,k-1}}^2)/D_{k-1}$;
return k, B, Λ, D;

.

Kapitel 3. Reduktion der Schranken – die unendlichen Stellen

Im folgenden Algorithmus wird grob das Vorgehen bei der Reduktion über einer unendichen Stelle dargestellt. Im Fall einer endlichen Stelle bleiben die wichtigsten Schritte im Wesentlichen die gleichen, allerdings werden die Logarithmen und Linearformen anders berechnet und aufgestellt.

Algorithmus 10 : Reduktion der Schranke N bei einer unendlichen Stelle

Input : Liste der Basispunkte B, Schranke N, Kurve E
Output : reduzierte Schranke N'
$N' := N$;
$r := \#B$;
$g :=$ ord(Torsionsgruppe(E));
`/* Vorbelegen der Gittermatrix */`
$A := \mathbb{1}_{r+2}$;
`/* Bestimmen der elliptischen Logarithmen */`
$E_\Lambda :=$ minimales Modells von E;
for $i = 1 \dots r$ **do**
  $B_\Lambda[i] := B[i]$ unter der Abbildung von $E \to E_\Lambda$;
  $u_{i,\infty} := \Psi_\infty(B_\Lambda[i])$;
end
$u_{r+1,\infty} := \omega_1$;
$u_{r+2,\infty} := \omega_2$;
`/* Es wird so lange reduziert, bis sich` N `nicht mehr wesentlich ändert. */`
while $N' \approx N$ **do**
  $N := N'$;
  Wähle $C \approx (rN + g)^{(\frac{r+2}{2})}$;
  $k := rN^2 + (1 + 3rN + 2g)/\sqrt{2}$;
  $k_1 := 0$;
  `/* Vergrößere` C `so lange, bis` k_1 `groß genug ist. */`
  while $k_1 < k$ **do**
    $C := C * 10$;
    Belege die letzte Zeile der Matrix A mit den Werten $[Cu_i/g]$, $i = 1, \dots, r+2$;
    $A' :=$LLL(A);
    $k_1 := \|A'[1]\|$;
  end
  `/* Berechnung der neuen Schranke. */`
  $N' := \sqrt{\frac{2}{c_{14}} \left(\log(Cc_{18}) - \log\left(\sqrt{k_1^2 - rN^2} - \frac{1+3rN+2g}{\sqrt{2}}\right)\right)}$;
end
return N';

Kapitel 4. Suche nach S-ganzen Punkten – Reduktion modulo $\mathfrak{p} \notin S$

Der folgende Algorithmus liefert die Informationen, die zum Aufstellen der Kongruenzen bei guter Reduktion benötigt werden.

Algorithmus 11 : Basisdarstellung bei guter Reduktion

Input : Liste mit Mordell-Weil-Basis B, Stellenmenge S, elliptische Kurve E

Output : Liste L_g, die zu jeder Stelle aus S mit guter Reduktion die Erzeuger und die Ordnung von $E_\mathfrak{p}$ enthält sowie die Koeffizienten, die zur Darstellung von B in $E_\mathfrak{p}$ dienen

$L_g := \emptyset$;
for $i := 1 \ldots \#S$ **do**
  $\mathfrak{p} := S[i]$;
  `/* Prüfen, ob gute Reduktion vorliegt */`
  if Kodairasymbol$(E, \mathfrak{p}) = I_0$ **then**
    $E_\mathfrak{p} :=$ Reduktion$(E, \mathfrak{p})$;
    $a :=$ Abbildung von E nach $E_\mathfrak{p}$;
    $P :=$ Erzeuger$(E_\mathfrak{p})$;
    `/* Reduktion des Erzeugendensystems */`
    $B_\mathfrak{p} := \emptyset$;
    for $j := 1 \ldots \#B$ **do**
      $B_\mathfrak{p}[j] := a(B[j])$;
    end
    $L_g[i][1] := P$
    for $j := 1 \ldots \#B_\mathfrak{p}$ **do**
      `/* Unterscheide ob` $E_\mathfrak{p}$ `ein oder zwei Erzeuger hat */`
      if $\#P = 1$ **then**
        Bestimme k_1, so dass $B_\mathfrak{p} = k_1 P[1]$;
        $L_g[i][2] := [k_1]$;
        $L_g[i][3] := [\mathrm{ord}(P[1])]$;
      else
        Bestimme k_1, k_2, so dass $B_\mathfrak{p} = k_1 P[1] + k_2 P[2]$;
        $L_g[i][2] := [k_1, k_2]$;
        $L_g[i][3] := [\mathrm{ord}(P[1]), \mathrm{ord}(P[2])]$;
      end
    end
  end
end
return L_g

Der folgende Algorithmus zeigt, wie eine Vorsauswahl der Punkte möglich ist, ohne sie berechnet zu haben:

Algorithmus 12 : Test mit Vorauswahl

Input : Liste s mit Koeffizienten des zu testenden Punktes, Menge der Stellen S, Liste mit Schranken N, Menge mit Stellen $\mathcal{P}$, Liste mit Zufallselementen α, Liste L_g mit Informationen zu den Stellen aus S, Index i, Liste L_b mit Informationen zu Stellen, die nicht in S enthalten sind, Basispunkte B

Output : *wahr* falls der Punkt S-ganz ist und nicht bereits vorher getested wurde, sonst $falsch$

```
/* Ausschließen von Überschneidungen mit bereits getesteten
   Punkten                                                    */
for t := 1 ... i − 1 do
    sum := 0;
    if N[t] ≥ max{s} then
        for j := 1 ... #s do
            sum := sum + s[j] ∗ L_g[t][j];
        end
        if sum mod ord(L_g[t]) = 0 then
            return falsch;
        end
    end
end
/* Ausschließen aller Überschneidungen mit L_b                */
for t := 1 ... #L_b do
    sum := 0;
    for j := 1 ... #s do
        sum := sum + s[j] ∗ L_b[t][j];
    end
    if sum mod ord(L_b[t]) = 0 then
        return falsch;
    end
end
P := O_E;
/* Berechnung und Test des Punktes                            */
for j := 1...#s do
    P := P + s[j] ∗ B[j];
end
return Test auf S-Ganzheit(P, S, P, α);
```

Kapitel 4. Suche nach S-ganzen Punkten – Reduktion modulo $\mathfrak{p} \in S$

Zum Bestimmen der Gruppe E_0 im Fall von schlechter Reduktion dient folgender Algorithmus, der aus Platzgruenden auf zwei Seiten aufgeteilt wurde:

Algorithmus 13 : Bestimmung Erzeugendensystem von E_0

```
Input : Liste mit Mordell-Weil-Basis B, Stelle p, elliptische Kurve E,
        singulärer Punkt S
Output : Erzeugendensystem E_0
E_0 := ∅;
E_s := ∅;
c_p := Tamagawazahl(E, p);
if c_p = 1 then
 | return B
end
/* Prüfe, welche Basiselemente in E_s und welche in E_0
   liegen                                                    */
for i = 1 ... #B do
 | if B[i] mod p = S then
 | | t := 0;
 | | /* Prüfe, ob zwei Basiselemente in der gleichen
 | |    Nebenklasse liegen                                   */
 | | for j = 1 ... i − 1 do
 | | | if (B[i] − B[j]) mod p = S then
 | | | | t := t + 1;
 | | | end
 | | end
 | | if t = i − 1 then
 | | | E_s[#E_s + 1] := B[i];
 | | end
 | else
 | | E_0[#E_0 + 1] := B[i];
 | end
end
/* Fortsetzung nächste Seite                                 */
```

Algorithmus 13 – Teil 2 : Bestimmung Erzeugendensystem von E_0

```
/* Ergänzen der fehlenden Elemente von E_0                    */
if #E_s = 3 then
    E_0[#E_0 + 1] := E_s[1] + E_s[2];
    E_0[#E_0 + 1] := E_s[1] + E_s[3];
    E_0[#E_0 + 1] := 2E_s[1];
else if #E_s = 2 then
    if c_p = 4 then
        E_0[#E_0 + 1] := 2E_s[1];
        E_0[#E_0 + 1] := 2E_s[2];
    else
        E_0[#E_0 + 1] := E_s[1] + E_s[2];
        E_0[#E_0 + 1] := 2E_s[1];
    end
else if #E_s = 1 then
    if c_p = 4 then
        E_0[#E_0 + 1] := 4E_s[1];
    else if c_p = 3 then
        E_0[#E_0 + 1] := 3E_s[1];
    else if c_p = 2 then
        E_0[#E_0 + 1] := 2E_s[1];
    end
end
return E_0
```

Um im Fall von schlechter Reduktion die Struktur von E_{ns} bestimmen zu können, wird die Abbildung aus folgendem Algorithmus verwendet:

Algorithmus 14 : Reduktionsabbildung bei schlechter Reduktion

Input : elliptische Kurve E, reduzierte Kurve $E_{\mathfrak{p}}$, Stelle $\mathfrak{p}$
Output : Reduktionsabbildung $a_{m,a}$, Reduktionstyp b, Körper $\mathbb{L}$
$Sing :=$ singulärer Punkt$(E_{\mathfrak{p}})$;
$a :=$ Abbildung von E nach $E_{\mathfrak{p}}$;
$c :=$ Koeffizienten von $E_{\mathfrak{p}}$;
$a_1 := 1/2(-c[1] + \sqrt{c[1]^2 + 4(c[2] + 3Sing[1])})$;
$a_2 := 1/2(-c[1] - \sqrt{c[1]^2 + 4(c[2] + 3Sing[1])})$;
$b_2 := -Sing[1]a_2$;
$b_1 := -Sing[1]a_1$;
if $a_1 = a_2$ **then**
  $b :=$ additiv;
  $\tilde{a}_m :=$ Abbildung$((x, y) \mapsto \frac{x-s_1}{y-ax-b})$;
  $a_{m,a} := a \circ \tilde{a}_m$;
  $\mathbb{L} := \mathbb{F}_{\mathfrak{p}}$;
else
  $b :=$ multiplikativ;
  $\tilde{a}_a :=$ Abbildung$((x, y) \mapsto \frac{y-a_1x-b_1}{y-a_2x-b_2})$;
  $a_{m,a} := a \circ \tilde{a}_a$;
  $\mathbb{L} := \mathbb{F}_{\mathfrak{p}}(a_1, a_2)$;
end
return $a_{m,a}, b, \mathbb{L}$;

Um bei schlechter Reduktion die notwendigen Kongruenzen aufzustellen dient der nächste Algorithmus:

Algorithmus 15 : Basisdarstellung bei schlechter Reduktion

Input : Liste mit Mordell-Weil-Basis B, Stellenmenge S, elliptische Kurve E

Output : Liste L_b, die zu jeder Stelle aus S mit schlechter Reduktion die Erzeuger und die Ordnung von $E_{\mathfrak{p}}$ sowie die Koeffizienten, die zur Darstellung von B in $E_{\mathfrak{p}}$ dienen enthält

$L_b := \emptyset$;
for $i := 1 \ldots \#S$ **do**
  $\mathfrak{p} := S[i]$;
  if Kodairasymbol$(E, \mathfrak{p}) \neq I_0$ **then**
    $E_{\mathfrak{p}} :=$ Reduktion$(E, \mathfrak{p})$;
    $Sing :=$ singulärer Punkt$(E_{\mathfrak{p}})$;
    $B :=$ Erzeuger von $E_0(B, S[i], E, Sing)$;
    $a, Reduktionstyp, \mathbb{L} :=$ Reduktionsabbildung bei schlechter Reduktion$(E, E_{\mathfrak{p}}, \mathfrak{p})$;
    if $Reduktionstyp = additiv$ **then**
      $L_b[i][1] := [0]$;
    else
      $L_b[i][1] := [1]$;
    end
    $L_b[i][2] := \emptyset$;
    for $j := 1 \ldots \#B$ **do**
      $L_b[i][2][j] := a(B[j])$;
    end
  end
  $L_b[i][3] := \#\mathbb{L}$;
end
return L_b

Kapitel 4. Suche nach S-ganzen Punkten – Ausschluss von Vielfachen

Der folgende Algorithmus zeigt die Rekursion, die zum Testen aller Vielfacher eines Tupels verwendet wird:

Algorithmus 16 : Test von Vielfachen

Input : Punkt P, Menge der Stellen S, Schranke N, Menge $prim$ der Primzahlen kleiner als N, Primzahl p, bei der der Test erfolgreich war
Output : Liste mit S-ganzen Punkten U
$prim2 := \emptyset$;
$U := \emptyset$;
if P *S-ganz* **then**
  for $i \in prim$, $i \geq p$ **do**
    if iP *S-ganz* **then**
      speichere i in Liste $prim2$;
    end
  end
end
for $j \in prim2$ **do**
  $UU :=$Test von Vielfachen(jP, S, N, $prim2$, j);
  $U := UU \cup U$;
end
return U;

Der folgende Algorithmus dient dazu, nur die Punkte zu testen, deren erste Koordinate positiv ist, und wurde aus Platzgründen auf zwei Seiten aufgeteilt:

Algorithmus 17 : Test von teilerfremden Tupeln

Input : Basis B, vorgegebene Stellenmenge S, Liste mit Zufallselementen α, zugehörige Stellenmenge $\mathcal{P}$, Schranke N

Output : Menge mit S-ganzen Punkten U

```
/* die erste Komponente ≠ 0 der getesteten Tupel ist
   positiv, die S-ganzen Punkte mit negativer Komponente
   erhält man durch Multiplikation mit −1                */
```

for $i_1 := 1 \ldots N$ **do**
  for $i_2 := -N \ldots N$ **do**
    ⋮
    for $i_r := -N \ldots N$ **do**
      if $\mathrm{ggT}(i_1, i_2, \ldots, i_r) = 1$ **then**
        $P := i_1B_1 + i_2B_2 + \cdots + i_rB_r$;
        if Test auf $S-$Ganzheit(P, S, $\mathcal{P}$, α) = *wahr* **then**
          Bestimme Menge *prim* von Primzahlen kleiner N;
          U :=Test von Vielfachen(P, S, N, *prim*, 1)
        end
      end
    end
    ⋮
  end
end

```
/* Fortsetzung nächste Seite                             */
```

Algorithmus 17 – Teil 2 : Test von teilerfremden Tupeln

```
/* die erste Komponente ist null, dann ist die zweite immer
   positiv                                                    */
i_1 := 0;
for i_2 = 1 ... N do
|  ⋮
|  for i_r = −N ... N do
|  |  if ggT(i_2, ..., i_r) = 1 then
|  |  |  P := i_2 B_2 + ··· + i_r B_r;
|  |  |  if Test auf S−Ganzheit(P, S, P, α) = wahr then
|  |  |  |  Bestimme Menge prim von Primzahlen kleiner N;
|  |  |  |  U := Test von Vielfachen(P, S, N, prim, 1)
|  |  |  end
|  |  end
|  end
|  ⋮
end
/* die zweite Komponente ist Null, dann ist die dritte
   immer positiv                                              */
⋮
/* Sind alle Komponenten bis auf die letzte null, so kann
   man direkt die Funktion Vielfache anwenden                 */
if Test auf S−Ganzheit(B_r, S, P, α) = wahr then
|  Bestimme Menge prim von Primzahlen kleiner N;
|  U :=Test von Vielfachen(B_r, S, N, prim, 1)
end
return U
```

Literaturverzeichnis

[Bak68] Baker, A.: *The Diophantine Equation $y^2 = ax^3 + bx^2 + cx + d$.* J. London Math. Soc., 43:1–9, 1968.

[BG96] Bugeaud, Y. und K. Győry: *Bounds for the Solution of Unit Equations.* Acta Arith., 74:67–80, 1996.

[Bug97] Bugeaud, Y.: *Bounds for the Solutions of Superelliptic Equations.* Comp. Math., 107:187–219, 1997.

[Bun02] Bundschuh, P.: *Einführung in die Zahlentheorie.* Springer-Verlag, Berlin-Heidelberg-New York, 2002.

[Car95] Carlson, B.C.: *Numerical Computation of Real or Complex Elliptic Integrals.* Numer. Algorithms, 10 No. 1-2:13–26, 1995.

[Coh93] Cohen, H.: *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[Cre97] Cremona, J.E.: *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1997.

[Dav95] David, S.: *Minorations de formes linéaires de logarithmes elliptiques.* Mém. Soc. Math. France (NS), 62(NS):143pp, 1995.

[de 89] de Weger, B.M.M.: *Algorithms for Diophantine Equationes.* CWI Trac 65, Centre for Mathematics and Computer Sience, Amsterdam, 1989.

[GPZ94] Gebel, J., A. Pethő und H.G. Zimmer: *Computing Integral Points on Elliptic Curves.* Acta. Arith., 68:171–192, 1994.

[Her02] Herrmann, E.: *Bestimmung aller S-ganzen Lösungen auf elliptischen Kurven.* Dissertation, Universität des Saarlandes, 2002.

[Hus87] Husemöller, D.: *Elliptic Curves.* Graduate Texts in Mathematics 111. Springer-Verlag, Berlin-Heidelberg-New York, 1987.

[JS92] J.H. SILVERMAN, J. TATE: *Rational Points on Elliptic Curves.* Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[Kob77] KOBLITZ, N.: *p-adic Numbers, p-adic Analysis and Zeta-Functions.* Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[Lan78] LANG, S.: *Elliptic Curves. Diophantine Analysis.* Springer-Verlag, Berlin-Heidelberg-New York, 1978.

[Len92] LENSTRA, H.W.: *Algorithms in Algebraic Number Theory.* Bull. Amer. Math. Soc., 26:209–219, 1992.

[Lut37] LUTZ, E.: *Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques.* J. reine angew. Math., 177:138–247, 1937.

[Mah34] MAHLER, K.: *Über die rationalen Punkte auf Kurven vom Geschlecht eins.* J. reine angew. Math., 170:168–178, 1934.

[Mat00] MATVEEV, E.M.: *An explicit Lower Bound for a Homogeneous Rational Linear Form in Logarithms of Algebraic Numbers, II.* Izv. Math., 64:1217–1269, 2000.

[Neu92] NEUKIRCH, J.: *Algebraische Zahlentheorie.* Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[PHZH99] PETHŐ, A., J.G. GEBEL H.G. ZIMMER und E. HERRMANN: *Computing all S-Integral Points on Elliptic Curves.* Math. Proc. Camb. Phil. Soc., 127:383–402, 1999.

[Sie29] SIEGEL, C.L.: *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. Wiss, Seiten 1–41, 1929.

[Sil86] SILVERMAN, J.H.: *The Arithmetic of Elliptic Curves.* Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[Sil90] SILVERMAN, J.H.: *The Difference between the Weil Height and the Canonical Height on Elliptic Curves.* Math. Comp., 55:723–743, 1990.

[Sma94] SMART, N.P.: *S-integral Points on Elliptic Curves.* Math. Proc. Camb. Phil. Soc, 116:391–399, 1994.

[Sma98] SMART, N.P.: *The Algorithmic Resolution of Diophantine Equations.* Cambridge Press, 1998.

[ST94] STROEKER, R.J. und N. TZANAKIS: *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms.* Acta Arith., 67:177–196, 1994.

[SZ03] SCHMITT, S. und H.G. ZIMMER: *Elliptic Curves.* de Gruyter, Berlin, 2003.

[Tat75] TATE, J.: *Algorithm for Determining the Type of a Singular Fiber in Elliptic Pensil.* Modular functions of one variable IV, Lecture Notes in Math. 476:33–52, 1975.

[Uch06] UCHIDA, Y.: *On the Difference between the Ordinary Height and the Canonical Height on Elliptic Curves.* Proc. Japan Acad., 82(A):56–60, 2006.

[Wal93] WALDSCHMIDT, M.: *Minorations de combinaisons linéaires de logarithmes de nombres algébriques.* Can. J. Math., 45, No.1:176–224, 1993.

[Yu94] YU, K.: *Linear forms in p-adic Logarithms III.* Compositio Math., 91:241–276, 1994.

[Zag87] ZAGIER, D.: *Large Integral Points on Elliptic Curves.* Comp. Math., 48:425–436, 1987.