Punkte auf elliptischen Kurven über $\mathbb{Q}$ in quadratischen Zahlkörpern

von

Michael Laska

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D - 5300 Bonn 3

MPI/SFB 83-13

Inhalt

0. Einführung.

Sei K ein quadratischer Zahlkörper, $K = \mathbb{Q}(\theta)$, $\theta^2 = z \in \mathbb{Z}$ quadratfrei; O_z sei der Ring der ganzen Zahlen in K .

Sei E eine elliptische Kurve über $\mathbb{Q}$ mit Weierstraß-Gleichung

$$\Gamma_{A,B} : \quad y^2 = x^3 + Ax + B \quad ,$$

$A,B \in \mathbb{Z}$, $\Delta = 4A^3+27B^2 \neq 0$. Sei E^* die elliptische Kurve über $\mathbb{Q}$ mit Weierstraß-Gleichung

$$\Gamma_{Az^2,Bz^3} : \quad y^2 = x^3 + Az^2x + Bz^3 \quad .$$

Seien $E(\mathbb{Q})$ und $E^*(\mathbb{Q})$ die Mordell-Weil-Gruppen von E bzw. E^* über $\mathbb{Q}$ und sei $E(K)$ die Mordell-Weil-Gruppe von E über K . Für die abelsche Gruppe $E(K)$ hat man den Automorphismus $Q \mapsto Q'$, der induziert wird von der Konjugation (über $\mathbb{Q}$) in K . Sei

$$\sigma : \quad E(K) \to E(\mathbb{Q})$$

der Spurhomomorphismus von $E(K)$; er ist gegeben durch $\sigma(Q) = Q + Q'$, wo $+$ die Addition auf der elliptischen Kurve E bedeutet.

In der vorliegenden Arbeit benutzen wir den Spurhomomorphismus und beweisen im ersten Teil folgende Sätze über die Struktur von $E(K)$.

Satz (1.3). $\mathrm{Rang}(E(K)) = \mathrm{Rang}(E(\mathbb{Q})) + \mathrm{Rang}(E^*(\mathbb{Q}))$.

Satz (1.6). Sei $Q \in E(K)$ ein Punkt der Ordnung p, p Primzahl. Dann ist $p = 2,3,5$ oder 7.

Satz 1.3 ergibt sich als Folgerung aus der BIRCH-SWINNERTON-DYER-Vermutung.

Im zweiten Teil der Arbeit betrachten wir das diophantische Objekt $\Gamma_{A,B}$. Für einen Teilring R von K sei

$$\Gamma_{A,B}(R)$$

die Menge der Lösungen (x,y) von $\Gamma_{A,B}$ mit $x,y \in R$. Für $R \not\subset \mathbb{Q}$ setzen wir

$$\overline{\Gamma_{A,B}(R)} = \Gamma_{A,B}(R) \setminus \Gamma_{A,B}(\mathbb{Q}) \quad .$$

$\Gamma_{A,B}(R)$ ist also gegeben durch $\Gamma_{A,B}(R \cap \mathbb{Q})$ und $\overline{\Gamma_{A,B}(R)}$. Wir zeigen mit Hilfe des Spurhomomorphismus, daß man die Menge $\overline{\Gamma_{A,B}(R)}$ vollständig beschreiben kann, wenn man $E(\mathbb{Q})$ kennt. Und zwar induziert σ eine Abbildung

$$\sigma_R : \overline{\Gamma_{A,B}(R)} \to \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\} \quad ,$$
$$\sigma_R(Q) = Q + Q' \quad ,$$

wo ∞ der eindeutig bestimmte Punkt von $\Gamma_{A,B}$ im Unendlichen ist, und wir beschreiben die Fasern $\sigma_R^{-1}(P)$. Dabei interessieren uns vor allem die Fälle in denen $R = K$ oder R ein S-arithmetischer Ring in K ist.

Für $R = K$ beweisen wir den folgenden

Satz (3.1). Die Fasern $\sigma_K^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$, mit $\sigma_K^{-1}(P) \neq \emptyset$ werden parametrisiert durch

$$\Gamma_{Az^2,Bz^3}(\mathbb{Q})$$

Der Satz kann zum Beispiel benutzt werden, um K-rationale Punkte auf $\Gamma_{A,B}$

zu konstruieren, die nicht schon $\mathbb{Q}$-rational sind.

Sei R ein S-arithmetischer Ring in K,

$$R = O_Z[S^{-1}] \quad ,$$

wo S eine endliche Menge von Primstellen in O_Z ist. Nach Sätzen von SIEGEL [Si], MAHLER [Mah], BAKER [Ba], COATES [Coa] ist $\Gamma_{A,B}(R)$ endlich. Wir nehmen an, daß O_Z Hauptidealring ist und daß ohne Einschränkung $\theta^{-1} \in R$ ist. Mit T bezeichnen wir die Menge der rationalen Primzahlen, die von den Primelementen in S geteilt werden. Wir beweisen den folgenden

Satz (4.1). Sei $Q = (s,t)$, $s,t \in R$. Die folgenden Aussagen (i) und (ii) sind äquivalent.

(i) $Q \in \sigma_R^{-1}(\infty)$.

(ii) $(s,t) = (p\theta^{-2}, q\theta^{-3})$ mit $(p,q) \in \Gamma_{Az^2,Bz^3}(\mathbb{Z}[T^{-1}])$, $q \neq 0$.

Für $P \neq \infty$ beweisen wir den folgenden

Satz (4.2). Sei $P \in \Gamma_{A,B}(\mathbb{Z})$, $P = (u,v)$. Sei S derart, daß jedes Primelement in S assoziiert zu seinem Konjugierten ist. Dann gilt für $(s,t) \in \sigma_R^{-1}(P)$:

(i) $s,t \in O_Z$.

(ii) Sei $s = \frac{e}{2} + \frac{f}{2}\theta$, $t = \frac{g}{2} + \frac{h}{2}\theta$ mit $e,f,g,h \in \mathbb{Z}$, $\lambda = hf^{-1}$. Dann ist (λ,f) ganzahliger Punkt (x,y) auf der elliptischen Kurve

$$zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2$$

und $e = \lambda^2 - u$, $g = (e - 2u)\lambda - 2v$.

Mit den beiden obigen Sätzen ist die Bestimmung von $\overline{\Gamma_{A,B}(R)}$ vollständig

auf diophantische Probleme über $\mathbb{Q}$ zurückgeführt. Falls nun $E(\mathbb{Q})$ endlich ist, hat man insbesondere nur endlich viele Fasern $\sigma_R^{-1}(P)$ und für jedes $P \in \Gamma_{A,B}(\mathbb{Q})$ gilt: $P \in \Gamma_{A,B}(\mathbb{Z})$. Damit ist $\Gamma_{A,B}(R)$ gegeben einerseits durch $\Gamma_{A,B}(R \cap \mathbb{Q}) = \Gamma_{A,B}(\mathbb{Q})$, andererseits durch $\overline{\Gamma_{A,B}(R)}$, das sich mit den beiden obigen Sätzen in vielen Fällen explizit bestimmen läßt.

In Kapitel 1 beweisen wir die beiden Sätze über die Struktur von $E(K)$ und diskutieren den Zusammenhang mit der BIRCH-SWINNERTON-DYER-Vermutung. In Kapitel 2 stellen wir die wesentlichen Eigenschaften der Spurabbildung zusammen, die wir für das Studium der diophantischen Gleichung $\Gamma_{A,B}$ benötigen. In Kapitel 3 behandeln wir die Lösungen von $\Gamma_{A,B}$ in K , in Kapitel 4 die Lösungen in S-arithmentischen Teilringen von K . In Kapitel 5 zeigen wir, wie man in konkreten Fällen unsere Ergebnisse zur Lösung der Gleichung $\Gamma_{A,B}$ benutzt. Als Beispiele konstruieren wir die Lösungen von

$$y^2 = x^3 - 1 \quad \text{in} \quad O_{-2}[\tfrac{1}{\sqrt{-2}}] \quad ,$$

$$y^2 = x^3 + x \quad \text{in} \quad O_3[\tfrac{1}{\sqrt{3}}] \quad .$$

Die Gleichung $x^3 - y^2 = r$ ist mit den Methoden der Spurabbildung in einer früheren Arbeit [La] behandelt worden. Dort sind auch wichtige Anwendungen und zahlreiche Beispiele angegeben. Die Resultate in der vorliegenden Arbeit lassen sich ohne weiteres auf eine beliebige quadratische Erweiterung $K:k$ von Zahlkörpern mit $A,B \in O_k$ übertragen.

In der gesamten Arbeit seien der quadratische Zahlkörper K , die elliptische Kurve E über $\mathbb{Q}$ und die Gleichung $\Gamma_{A,B}$ für E , $A,B \in \mathbb{Z}$, fest gewählt; E^* sei wie oben der z-twist von E .

1. Zur Struktur von $E(K)$.

Sei $Q \mapsto Q'$ der Automorphismus der abelschen Gruppe $E(K)$, der induziert wird von der Konjugation in K; also für $Q \in E(K)$, $Q = (s,t) \in \Gamma_{A,B}(K)$ ist $Q' = (s',t')$, wo s' das Konjugierte (über $\mathfrak{Q}$) von $s \in K$ ist. Sei $\sigma : E(K) \to E(\mathfrak{Q})$, $\sigma(Q) = Q + Q'$, der Spurhomomorphismus von $E(K)$. Sei

$$\alpha : E^*(\mathfrak{Q}) \to E(K)$$

der Gruppenhomomorphismus, der folgendermaßen definiert ist: Für $U \in E^*(\mathfrak{Q})$, $U = (p,q) \in \Gamma_{Az^2,Bz^3}(\mathfrak{Q})$ sei $\alpha U = (pz^{-1},qz^{-2}\theta) \in \Gamma_{A,B}(K)$. α hat die Eigenschaft

$$(1.1) \qquad (\alpha U)' = -\alpha U \quad , U \in E^*(\mathfrak{Q}) \quad .$$

Sei nun $(P,U) \in E(\mathfrak{Q}) \times E^*(\mathfrak{Q})$. Wir definieren

$$\tau(P,U) = P + \alpha U \quad .$$

Seien $E(\mathfrak{Q})_2$, $E^*(\mathfrak{Q})_2$ die Untergruppen der 2-Teilungspunkte von $E(\mathfrak{Q})$ bzw. $E^*(\mathfrak{Q})$.

(1.2) Proposition. $\tau : E(\mathfrak{Q}) \times E^*(\mathfrak{Q}) \to E(K)$ ist ein Homomorphismus abelscher Gruppen mit folgenden Eigenschaften:

(i) $\tau((0,E^*(\mathfrak{Q})) = \alpha(E^*(\mathfrak{Q})) = \text{Kern } \sigma$.

(ii) $\text{Kern } \tau \subseteq E(\mathfrak{Q})_2 \times E^*(\mathfrak{Q})_2$.

(iii) $2E(K) \subseteq \text{Bild } \tau$.

Beweis. τ ist offensichtlich ein Homomorphismus. Zu (i). Das erste Gleichheitszeichen folgt aus der Definition von τ. Für $Q \in E(K)$ bedeutet $Q \in \text{Kern } \sigma$ offensichtlich $Q = -Q'$. Also folgt wegen 1.1, daß $\alpha(E^*(\mathfrak{Q})) \subseteq \text{Kern } \sigma$ ist. Schreibe $Q = (s,t) \in \Gamma_{A,B}(K)$. Aus $Q \in \text{Kern } \sigma$ folgt $s = s'$, $t = -t'$, also $s = a \in \mathfrak{Q}$, $t = d\theta$ mit $d \in \mathfrak{Q}$. Für $U = (az, dz^2)$ gilt $U \in \Gamma_{Az^2,Bz^3}(\mathfrak{Q})$ und $\alpha(U) = Q$. Also ist $\text{Kern } \sigma \subseteq \alpha(E^*(\mathfrak{Q}))$. Damit ist (i) bewiesen. Zu (ii). Aus $P + \alpha U = 0$ für $(P,U) \in E(\mathfrak{Q}) \times E^*(\mathfrak{Q})$ folgt $P = -\alpha U$ und wegen 1.1 $P = P' = \alpha U$. Daraus folgt $2P = 0$ und $2(\alpha U) = 0$ und weiter $2U = 0$. Also ist $(P,U) \subseteq E(\mathfrak{Q})_2 \times E^*(\mathfrak{Q})_2$ und (ii) ist bewiesen. Zu (iii). Für $Q \in E(K)$ können wir schreiben $2Q = \sigma(Q) + (Q - Q')$. Offensichtlich ist $Q - Q' \in \text{Kern } \sigma$, also wegen (i) ist $Q - Q' = \alpha U$ für ein $U \in E^*(\mathfrak{Q})$. Daraus folgt $2Q = \tau(P,U)$ mit $P = \sigma(Q) \in E(\mathfrak{Q})$, $U \in E^*(\mathfrak{Q})$. Damit ist $2Q \in \text{Bild } \tau$, und (iii) ist bewiesen. ∎

Aus der Existenz der Abbildung τ folgen die Strukturssätze für $E(K)$.

(1.3) Satz. $\text{Rang}(E(K)) = \text{Rang}(E(\mathfrak{Q})) + \text{Rang}(E^*(\mathfrak{Q}))$.

Beweis. Aus Proposition 1.2, Teil (ii) folgt, daß $\text{Kern } \tau$ endlich ist. Andererseits ist nach dem Satz von Mordell-Weil $|E(K) : 2E(K)|$ endlich. Also ist nach Teil (iii) auch $|E(K) : \text{Bild } \tau|$ endlich. τ ist also eine Isogenie abelscher Gruppen. Daraus folgt $\text{Rang}(E(K)) = \text{Rang}(E(\mathfrak{Q}) \times E^*(\mathfrak{Q}))$ und damit die Behauptung des Satzes. ∎

Sei $L_K(E,s)$ die L-Reihe von E über K, und seien $L_{\mathfrak{Q}}(E,s)$, $L_{\mathfrak{Q}}(E^*,s)$ die L-Reihen von E bzw. E^* über $\mathfrak{Q}$:

$$L_K(E,s) = \prod_{\substack{\mathfrak{p} \\ \text{gut}}} \frac{1}{1 - a_K(\mathfrak{p}) \|\mathfrak{p}\|^{-s} + \|\mathfrak{p}\|^{1-2s}} \quad ,$$

$$L_{\mathbb{Q}}(E,s) = \prod_{\substack{p \\ \text{gut}}} \frac{1}{1 - a_{\mathbb{Q}}(p) p^{-s} + p^{1-2s}} \quad ,$$

$$L_{\mathbb{Q}}(E^*,s) = \prod_{\substack{p \\ \text{gut}}} \frac{1}{1 - a^*_{\mathbb{Q}}(p) p^{-s} + p^{1-2s}} \quad .$$

Dabei ist

$$a_K(\mathfrak{p}) = \|\mathfrak{p}\| + 1 - |E_{\mathfrak{p}}(k_{\mathfrak{p}})| \quad ,$$

$$a_{\mathbb{Q}}(p) = p + 1 - |E_p(\mathbb{F}_p)| \quad ,$$

$$a^*_{\mathbb{Q}}(p) = p + 1 - |E^*_p(\mathbb{F}_p)| \quad ,$$

wobei $\mathfrak{p}$ in O_Z ein gutes Primideal für E über K ist, d.h. ein Primideal, für das die Reduktion $E_{\mathfrak{p}}$ von E über K an der Stelle $\mathfrak{p}$ eine elliptische Kurve über $k_{\mathfrak{p}} = O_Z/\mathfrak{p}$, $\|\mathfrak{p}\| = |k_{\mathfrak{p}}|$, ist, und wobei p eine gute rationale Primzahl für E bzw. E^* ist, d.h. eine Primzahl, für die die Reduktion E_p , E^*_p von E bzw. E^* an der Stelle p eine elliptische Kurve über $\mathbb{F}_p$ ist.

Unter der Annahme, daß $L_K(E,s)$, $L_{\mathbb{Q}}(E,s)$, $L_{\mathbb{Q}}(E^*,s)$ analytisch fortsetzbar nach ganz $\mathbb{C}$ sind, sagt die BIRCH-SWINNERTON-DYER-Vermutung:

$$\operatorname{ord}_{s=1} L_K(E,s) = \operatorname{Rang}(E(K)) \quad ,$$

$$\operatorname{ord}_{s=1} L_{\mathbb{Q}}(E,s) = \operatorname{Rang}(E(\mathbb{Q})) \quad ,$$

$$\operatorname{ord}_{s=1} L_{\mathbb{Q}}(E^*,s) = \operatorname{Rang}(E^*(\mathbb{Q})) \quad .$$

Sei nun $\mathfrak{p}$ ein gutes Primideal für E über K , das nicht verzweigt ist.

(1.4) Lemma. Sei $\mathfrak{p}\mathfrak{p}' = (p)$. Dann gilt

$$a_K(\mathfrak{p}) = a_K(\mathfrak{p}') = a_{\mathbb{Q}}(p) = a^*_{\mathbb{Q}}(p) \quad .$$

Beweis. Es ist $k_{\mathfrak{p}} = k_{\mathfrak{p}'} = \mathbb{F}_p$, $x^2 - z$ reduzibel modulo p . Also ist E_p isomorph zu E^*_p über $\mathbb{F}_p$. Es folgt $|E_{\mathfrak{p}}(k_{\mathfrak{p}})| = |E_{\mathfrak{p}'}(k_{\mathfrak{p}'})| = |E_p(\mathbb{F}_p)| = |E^*_p(\mathbb{F}_p)|$ und damit die Behauptung. ∎

Sei $\mathfrak{p}\mathfrak{p}' = (p)$. Dann besagt Lemma 1.4:

$$\frac{1}{1 - a_K(\mathfrak{p})\|\mathfrak{p}\|^{-s} + \|\mathfrak{p}\|^{1-2s}} \cdot \frac{1}{1 - a_K(\mathfrak{p}')\|\mathfrak{p}'\|^{-s} + \|\mathfrak{p}'\|^{1-2s}}$$

$$= \frac{1}{1 - a_{\mathbb{Q}}(p)p^{-s} + p^{1-2s}} \cdot \frac{1}{1 - a^*_{\mathbb{Q}}(p)p^{-s} + p^{1-2s}} \quad .$$

(1.5) Lemma. Sei $\mathfrak{p} = (p)$. Dann gilt

(i) $a_K(\mathfrak{p}) = a_{\mathbb{Q}}(p)^2 - 2p$.

(ii) $a_{\mathbb{Q}}(p) = - a^*_{\mathbb{Q}}(p)$.

Beweis. Es ist $k_{\mathfrak{p}} = \mathbb{F}_{p^2}$, $x^2 - z$ irreduzibel modulo p und $E_{\mathfrak{p}}$ über $\mathbb{F}_p$ definiert. Teil (i) folgt aus der Rekursion $E_{\mathfrak{p}}(\mathbb{F}_{p^2}) = p^2 + 1 - \pi^2 - \overline{\pi}$ wobei $p = \pi\overline{\pi}$, $a_{\mathbb{Q}}(p) = \pi + \overline{\pi}$. Für Teil (ii) sei $L := \Gamma_{\overline{A},\overline{B}}(\mathbb{F}_p)$ und $L^* := \Gamma_{\overline{Az}^2,\overline{Bz}^2}(\mathbb{F}_p)$, wobei $\overline{A},\overline{B},\overline{z}$ die Reduktion modulo p bedeutet. Wir betrachten die Abbildung

$$\psi : L \dot{\cup} L^* \to \mathbb{F}_p \quad ,$$

die folgendermaßen definiert ist: Ist $Q = (x,y) \in L$, dann sei

$$\psi(Q) = x \quad .$$

Ist $Q = (x,y) \in L^*$, dann sei

$$\psi(Q) = x\overline{z}^{-1} \quad .$$

Wir zeigen zunächst: ψ ist surjektiv. Sei $x_o \in \mathbb{F}_p$. Falls $x_o^3 + \overline{A}x_o + \overline{B}$ ein Quadrat in $\mathbb{F}_p$ ist, so ist man fertig: Es existiert ein $y_o \in \mathbb{F}_p$, so daß $(x_o,y_o) \in L$ und $\psi(x_o,y_o) = x_o$ ist. Sei also $x_o^3 + \overline{A}x_o + \overline{B}$ kein Quadrat in $\mathbb{F}_p$. Da $\overline{z}$ und somit $\overline{z}^3$ kein Quadrat in $\mathbb{F}_p$ ist, muß $\overline{z}^3(x_o^3 + \overline{A}x_o + \overline{B})$ ein Quadrat in $\mathbb{F}_p$ sein. Also gibt es ein $y_o \in \mathbb{F}_p$, so daß $(x_o\overline{z},y_o) \in L^*$ ist. Es ist $\psi(x_o\overline{z},y_o) = x_o$. Also ist ψ surjektiv.
Sei $x_o \in \mathbb{F}_p$. Wir zeigen: $|\psi^{-1}(x_o)| = 2$.
1.Fall: $x_o^3 + \overline{A}x_o + \overline{B} = 0$. In L liegt genau ein Punkt (x,y) mit $x = x_o$, nämlich $(x_o,0)$. In L^* liegt genau ein Punkt (x,y) mit $x_oz = x$, nämlich $(x_oz,0)$.
2.Fall: $x_o^3 + \overline{A}x_o + \overline{B} \neq 0$, $x_o + \overline{A}x_o + \overline{B}$ ist Quadrat in $\mathbb{F}_p$. In L gibt es zwei Punkte (x,y) mit $x = x_o$, nämlich (x_o,y_o) und $(x_o,-y_o)$, wobei $y_o^2 = x_o^3 + \overline{A}x_o + \overline{B}$. In L^* gibt es keinen Punkt (x,y) mit $x = x_o\overline{z}$, denn $(x_o\overline{z})^3 + \overline{A}\overline{z}^2(x_o\overline{z}) + \overline{B}\overline{z}^3 = \overline{z}^3(x_o^3 + \overline{A}x_o + \overline{B})$ ist kein Quadrat in $\mathbb{F}_p$.
3.Fall: $x_o^3 + \overline{A}x_o + \overline{B} \neq 0$, $x_o^3 + \overline{A}x_o + \overline{B}$ ist kein Quadrat in $\mathbb{F}_p$. In L gibt es keinen Punkt (x,y) mit $x_o = x$. In L^* gibt es genau zwei Punkte (x,y) mit $x = x_o\overline{z}$. In jedem Falle hat man $|\psi^{-1}(x_o)| = 2$. Aus den Eigenschaften von ψ folgt: $|E_p(\mathbb{F}_p)| + |E_p^*(\mathbb{F}_p)| = 2p + 2$. Daraus folgt $a_Q(p) = -a_Q^*(p)$. Teil (ii) ist damit bewiesen. ∎

Sei $\mathfrak{p} = (p)$. Dann folgt aus Lemma 1.5:

$$\frac{1}{1 - a_K(\mathfrak{p})\|\mathfrak{p}\|^{-s} + \|\mathfrak{p}\|^{1-2s}} = \frac{1}{1 - a_Q(p)p^{-s} + p^{1-2s}} \cdot \frac{1}{1 - a_Q^*(p)p^{-s} + p^{1-2s}} \quad .$$

Insgesamt haben wir gezeigt: Die Euler-Faktoren von $L_K(E,s)$ sind bis auf endlich viele Ausnahmen genau die Faktoren im Produkt $L_{\mathbb{Q}}(E,s) \cdot L_{\mathbb{Q}}(E^*,s$

Daraus folgt

$$\operatorname{ord}_{s=1} L_K(E,s) = \operatorname{ord}_{s=1} L_{\mathbb{Q}}(E,s) + \operatorname{ord}_{s=1} L_{\mathbb{Q}}(E^*,s) \quad .$$

Damit sieht man: Aus der BIRCH-SWINNERTON-DYER-Vermutung folgt Satz 1.3.

(1.6) Satz. Sei $Q \in E(K)$ ein Punkt der Ordnung p, p Primzahl. Dann ist $p = 2,3,5$ oder 7.

Beweis. Wir betrachten die Abbildung τ aus Proposition 1.2. Wir nehmen zunächst an, daß $Q \notin$ Bild τ ist. Es ist $|E(K) : 2E(K)| = 2^r |E(K)_2|$ wo r der Rang von $E(K)$ ist. Aus Teil (iii) in Proposition 1.2 folgt $|E(K) : \text{Bild } \tau| = 2^{r'}$, und daraus folgt $p = 2$. Sei $Q \in$ Bild τ, $\tau(V) = Q$, $V \in E(\mathbb{Q}) \times E^*(\mathbb{Q})$. Es folgt $pV \in$ Kern τ. Aus Teil (ii) in Proposition 1.2 folgt $2pV = 0$. Nun sind die Torsionsgruppen $E(\mathbb{Q})_{\text{Tor}}$ bzw. $E^*(\mathbb{Q})_{\text{Tor}}$ isomorph zu einer der folgenden Gruppen [Maz]: $\mathbb{Z}/m\mathbb{Z}$ mit $1 \leq m \leq 10$ oder $m = 12$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ mit $1 \leq n \leq 4$. Daraus folgt $p = 2,3,5$ oder 7. Damit ist der Satz bewiesen. ∎

2. Eigenschaften der Spurabbildung.

In den folgenden Kapiteln betrachten wir speziell die Gleichung $\Gamma_{A,B}$ für E und interessieren uns für die Lösungsmenge $\Gamma_{A,B}(R)$, wobei R ein Teilring von K ist. Sei $R \not\subset \mathbb{Q}$ und $\overline{\Gamma_{A,B}(R)} := \Gamma_{A,B}(R) \setminus \Gamma_{A,B}(\mathbb{Q}) \neq \emptyset$. Der Spurhomomorphismus $\sigma : E(K) \to E(\mathbb{Q})$, gegeben an dem Modell $\Gamma_{A,B}$, induziert eine Abbildung

$$\sigma_R : \overline{\Gamma_{A,B}(R)} \to \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\} ,$$

$\sigma_R(Q) = Q + Q'$, wobei $\infty = (0:1:0)$ der eindeutig bestimmte Punkt von $\Gamma_{A,B}$ im Unendlichen ist. Wir zeigen in diesem Kapitel, daß die Fasern $\sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$, durch geeignete $\mathbb{Q}$-rationale Punkte einer (zu P) passenden elliptischen Kurve über $\mathbb{Q}$ parametrisiert werden. Außerdem geben wir für $(s,t) \in \sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q})$, eine Abschätzung der Ordnung des Nenners von s und t an unzerlegten Primstellen von O_Z an. Der Einfachheit halber, aber ohne Einschränkung, machen wir im folgenden stets die Annahme: $\theta^{-1} \in R$.

Zunächst erinnern wir an die Additionsformeln für E, dargestellt an dem Modell $\Gamma_{A,B}$. Seien $P_1, P_2 \in E(K)$, $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2) \in \Gamma_{A,B}(K)$. Sei $P_3 = P_1 + P_2$. Dann ist $P_3 = \infty$ genau dann, wenn $(x_1,y_1) = (x_2,-y_2)$. Sei $P_3 \neq \infty$, $P_3 = (x_3,y_3) \in \Gamma_{A,B}(K)$. Dann ist

$$x_3 = \lambda^2 - x_1 - x_2 , \quad y_3 = -\lambda(x_3 - x_1) - y_1 ,$$

mit

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & , \text{ falls } P_1 \neq P_2 . \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & , \text{ falls } P_1 = P_2 . \end{cases}$$

Wir behandeln zunächst den Fall $P = \infty$. Die Faser $\sigma_R^{-1}(\infty)$ wird parametrisiert durch $\Gamma_{Az^2,Bz^3}(R \cap \mathfrak{Q})$:

(2.1) Proposition. Sei $Q = (s,t)$, $s,t \in R$. Die folgenden Aussagen (i) und (ii) sind äquivalent.

(i) $Q \in \sigma_R^{-1}(\infty)$.

(ii) $(s,t) = (p\theta^{-2}, q\theta^{-3})$ mit $(p,q) \in \Gamma_{Az^2,Bz^3}(R \cap \mathfrak{Q})$, $q \neq 0$.

Beweis. Der Fall $R = K$ folgt unmittelbar aus Teil (i) in Proposition 1.2. Im Allgemeinen hat man folgende Kette von Äquivalenzen:

(i) $(s,t) \in \sigma_R^{-1}(\infty)$.

(i') $(s,t) \in \overline{\Gamma_{A,B}(R)}$, $s = s'$, $t = -t'$.

(i'') $t^2 = s^3 + As + B$, $s = a \in R \cap \mathfrak{Q}$, $t = d\theta$, $d \in R \cap \mathfrak{Q}$, $d \neq 0$.

(i''') $(d\theta^4)^2 = (a\theta^2)^3 + Az^2(a\theta^2) + Bz^3$, $a,d \in R \cap \mathfrak{Q}$, $d \neq 0$.

(ii) $s = a = p\theta^{-2}$, $t = q\theta^{-3}$ mit $(p,q) \in \Gamma_{Az^2,Bz^3}(R \cap \mathfrak{Q})$, $q \neq 0$.

Damit ist das Lemma bewiesen. ∎

Als nächstes behandeln wir den Fall $P \neq \infty$. Dazu beweisen wir zunächst zwei Lemmata, die sich auch später noch als nützlich erweisen werden.

(2.2) Lemma. Sei $P \in \Gamma_{A,B}(\mathfrak{Q})$, $P = (u,v)$. Sei $Q = (s,t)$, $s,t \in R$, $s = a + b\theta$, $t = c + d\theta$ mit $a,b,c,d \in \mathfrak{Q}$. Die folgenden Aussagen (i) und (ii) sind äquivalent.

(i) $Q \in \sigma_R^{-1}(P)$.

(ii) $b \neq 0$ und die folgenden Gleichungen sind erfüllt:

(1) $a^3 + 3ab^2z + Aa + B - c^2 - d^2z = 0$,

(2) $3a^2 + b^2z + A - 2c\lambda = 0$,

(3) $u + 2a - \lambda^2 = 0$.

(4) $v + c + (u - a)\lambda = 0$, wobei $\lambda := db^{-1}$.

Beweis. Sei $Q \in \sigma_R^{-1}(P)$, also $Q \in \overline{\Gamma_{A,B}(R)}$ und $\sigma_R(Q) = P$.
$Q = (s,t) \in \Gamma_{A,B}(R)$ ist äquivalent zu

$$a^3 + 3ab^2z + Aa + B - c^2 - d^2z = 0 \quad ,$$
$$3a^2b + b^3z + Ab - 2cd = 0 \quad .$$

$Q \in \Gamma_{A,B}(\mathfrak{Q})$ und $\sigma_R(Q) = P \neq \infty$ ist äquivalent zu $b \neq 0$, $u + 2a - \lambda^2 = 0$,
$v + c + (u - a)\lambda = 0$ mit $\lambda := db^{-1}$. Damit ist das Lemma bewiesen. ∎

Sei $N = \| \ \|$ die Normabbildung von K über $\mathfrak{Q}$.

(2.3) Lemma. Sei $P \in \Gamma_{A,B}(\mathfrak{Q})$, $P = (u,v)$. Sei $(s,t) \in \sigma_R^{-1}(P)$,
$s = a + b\theta$, $t = c + d\theta$ mit $a,b,c,d \in \mathfrak{Q}$, $\lambda := db^{-1}$. Dann gilt

$$N(s) = 2au + 2u^2 + A + 2\lambda v \quad ,$$
$$N(t) = 3v^2 + 2cv + 2cu\lambda - 4ub^2z - 3u^3 - 4Au + \lambda^2 A \quad .$$

Beweis. Wir benutzen die Gleichungen (2), (3), (4) aus Lemma 2.2.
Aus (2) folgt $N(s) = a^2 - b^2z = 4a^2 + A - 2c\lambda$. Aus (3) und (4) folgt
$2c\lambda = -2v\lambda - 2u^2 - 2au + 4a^2$. Insgesamt folgt $N(s) = 2au + 2u^2 + A + 2\lambda v$
wie behauptet.
Aus (4) folgt: $3(v + c)^2 = 3(u - a)^2\lambda^2$.
Aus (3) folgt: $3(v + c)^2 = 6a^3 - 9a^2u + 3u^3$.
Aus (2) folgt: $6a^3 = -2ab^2z - 2Aa + 4ac\lambda$.
Aus (2) folgt: $-9a^2u = 3b^2uz + 3Au - 6ca\lambda$.
Aus (2) folgt: $-2Aa = uA - \lambda^2 A$.
Aus (3) folgt: $-2ab^2z = zub^2 - d^2z$.
Aus (4) folgt: $4ac\lambda = 4vc + 4c^2 + 4cu\lambda$.
Sukzessives Einsetzen ergibt: $3(v + c)^2 = 4ub^2z - d^2z + 4Au - \lambda^2 A + 4cv$
$+ 4c^2 - 2cu\lambda + 3u^3$ und damit die Gleichung für $N(t)$ wie behauptet. ∎

Zu $P \in \Gamma_{A,B}(\mathbb{Q})$, $P = (u,v)$ assoziieren wir nun die Kurve $C_P = C_P(x,y)$:

$$\boxed{C_P : \quad zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2} \quad .$$

C_P hat Geschlecht 1 . Falls C_P im projektiven Raum $\mathbb{P}^2(\mathbb{Q})$ einen Punkt besitzt, definiert C_P also insbesondere eine elliptische Kurve über $\mathbb{Q}$ Wir zeigen nun, daß die Faser $\sigma_R^{-1}(P)$ durch geeignete $\mathbb{Q}$-rationale Punkte auf C_P parametrisiert wird.

(2.4) Proposition. Sei $P \in \Gamma_{A,B}(\mathbb{Q})$, $P = (u,v)$. Sei $(s,t) \in \sigma_R^{-1}(P)$ $s = a + b\theta$, $t = c + d\theta$ mit $a,b,c,d \in \mathbb{Q}$, $\lambda = db^{-1}$. Dann gilt: $(\lambda,2b)$ ist ein Punkt (x,y) auf der Kurve C_P .

Beweis. Wir betrachten die Gleichung für $N(s)$ aus Lemma 2.3. Wir erhalten daraus zunächst $(a - u)^2 - b^2z = A + 3u^2 + 2\lambda v$. Nach Gleichung (3) in Lemma 2.2 ist $a = (\lambda^2 - u)/2$. Daraus folgt $z4b^2 = \lambda^4 - 6\lambda^2u - 8\lambda v - 4A - 3u^2$, d.h. $(\lambda,2b)$ ist ein Punkt auf der Kurve C_P . ∎

Man beachte, daß (s,t) vollständig durch $(\lambda,2b)$ bestimmt ist: Aus Gleichung (3) und (4) in Lemma 2.2 folgt $a = (\lambda^2 - u)/2$, $c = (a - u)\lambda$ -

Sei nun O_Z Hauptidealring. Sei $P \in \Gamma_{A,B}(\mathbb{Q})$, $P = (u,v)$, $(s,t) \in \sigma_R^{-1}(P)$. Sei p eine rationale Primzahl, die nicht zerlegt ist in O_Z , also

$$p = \varepsilon\pi^{\delta}$$

für ein Primelement π in O_Z , $\varepsilon \in O_Z^*$, $\delta \in \{1,2\}$. Im folgenden schätzen wir die Ordnung des Nenners von s und t an der Stelle π ab

durch die Ordnung des Nenners von u und v an der Stelle p . Sei ν_p die p-adische Bewertung auf $\mathbb{Q}$.

Es lassen sich u und v schreiben als

$$u = \frac{r}{p^{2\beta} q_1^2} \quad , \quad v = \frac{w}{p^{3\beta} q_2^3} \tag{2.5}$$

mit $r,w,q_1,q_2 \in \mathbb{Z}$, $\beta \in \mathbb{N}_0$, $(r,q_1) = (w,q_2) = 1$, $p \nmid q_1,q_2$ und, falls $\beta > 0$, $p \nmid r,w$. Ebenso läßt sich (s,t) schreiben als

$$s = \frac{e}{\pi^{2\alpha} d_1^2} \quad , \quad t = \frac{g}{\pi^{3\alpha} d_2^3} \tag{2.6}$$

mit $e,g,d_1,d_2 \in O_{\mathbb{Z}}$, $\alpha \in \mathbb{N}_0$, $(e,d_1) = (g,d_2) = 1$, $\pi \nmid d_1,d_2$ und, falls $\alpha > 0$, $\pi \nmid e,f$.

(2.7) Proposition. (i) Sei $(p,\delta) \neq (2,2)$. Dann ist $\alpha \leq \beta\delta$.

(ii) Sei $p = \delta = 2$. Dann ist $\alpha \leq 2\beta + 1$, wobei $\alpha = 0$, falls $\beta = 0$.

Beweis. Setze $f = \pi^{2\alpha} d_1^2$, also $s = e/f$, $e,f \in O_{\mathbb{Z}}$ mit $(e,f) = 1$. Wir können schreiben

$$e = \frac{e_1}{2} + \frac{e_2}{2}\theta \quad , \quad f = \frac{f_1}{2} + \frac{f_2}{2}\theta$$

mit $e_1,e_2,f_1,f_2 \in \mathbb{Z}$, $e_1 \equiv e_2 \bmod 2$, $f_1 \equiv f_2 \bmod 2$ und, falls $z \equiv 2,3 \bmod 4$ ist, mit $e_1 \equiv f_1 \equiv 0 \bmod 2$. Sei $s = a + b\theta$, $t = c + d\theta$ mit $a,b,c,d \in \mathbb{Q}$. Dann ist

$$a = \frac{e_1 f_1 - e_2 f_2 z}{4N(f)} \quad , \quad b = \frac{e_2 f_1 - e_1 f_2}{4N(f)} \quad .$$

Wir wenden die Gleichung für $N(s)$ aus Lemma 2.3 an:

$$(*) \qquad N(e) = N(s)N(f) = \frac{e_1f_1 - e_2f_2z}{2}u + 2N(f)u^2 + AN(f) + 2v\lambda_o \quad .$$

Dabei erfüllt $\lambda_o = \lambda N(f)$ die Gleichung

$$(**) \qquad (\lambda_o)^2 = N(f)^2u + N(f)\frac{e_1f_1 - e_2f_2z}{2}$$

(siehe Gleichung (3) in Lemma 2.2). Wir haben $e_1f_1 - e_2f_2z \in 2\mathbb{Z}$ und, falls $z \equiv 2,3 \bmod 4$ ist, sogar $e_1f_1 - e_2f_2z \in 4\mathbb{Z}$.

Zu (i). Sei $(p,\delta) \neq (2,2)$. Annahme: $\alpha > \beta\delta$.

Aus $N(f) = N(\varepsilon)p^{4\alpha/\delta}N(d_1)^2$ mit $p \nmid N(d_1)$ folgt $\nu_p(N(f)^2u) > 0$ und $\nu_p(\frac{e_1f_1 - e_2f_2z}{2}N(f)) > 0$ und wegen Gleichung (**) somit $\nu_p(\lambda_o) > 0$. Außerdem ist $\nu_p(AN(f)) > 0$ und $\nu_p(2N(f)u^2) > 0$. Aus $f = \pi^{2\alpha}d_1^2$ folgt $p^{2\beta+1} \mid f$ in O_Z , wobei $2^{2\beta+2} \mid f$ in O_Z . Damit folgt $p^{2\beta+1} \mid f_1, f_2$ in $\mathbb{Z}$, wobei $2^{2\beta+2} \mid f_1, f_2$ in $\mathbb{Z}$. Also ist $\nu_p(\frac{e_1f_1 - e_2f_2z}{2}u) > 0$. Insgesamt haben wir wegen Gleichung (*) damit $p \mid N(e)$, also $\pi \mid e$. Andererseits folgt aus unserer Annahme $\alpha > 0$. Das ist ein Widerspruch. Also ist $\alpha \leq \beta\delta$.

Zu (ii). Sei $(p,\delta) = (2,2)$. Dann ist $z \equiv 2,3 \bmod 4$. Aus $\alpha > 2\beta + 1$ würde wie im obigen Fall folgen $2 \mid N(e)$, was ein Widerspruch zu $\alpha > 0$ ist. Also ist $\alpha \leq 2\beta + 1$. Sei $\beta = 0$. Wegen $\frac{e_1f_1 - e_2f_2z}{2} \equiv 0 \bmod 2$ würde mit Gleichung (*) aus $\alpha > 0$ folgen: $2 \mid N(e)$, also $\pi \mid e$, was ein Widerspruch ist. Also ist $\alpha = 0$. Die Proposition ist bewiesen. ∎

3. K-rationale Lösungen von $\Gamma_{A,B}$.

Wir setzen $R = K$ und betrachten

$$\Gamma_{A,B}(K) \quad ,$$

die Menge der K-rationalen Punkte auf $\Gamma_{A,B}$. Wir beweisen, daß die Fasern der Spurabbildung

$$\sigma_K : \overline{\Gamma_{A,B}(K)} \to \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$$

durch die $\mathbb{Q}$-rationalen Punkte einer universellen elliptischen Kurve über $\mathbb{Q}$ parametrisiert werden:

(3.1) Satz. Die Fasern $\sigma_K^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$, mit $\sigma_K^{-1}(P) \neq \emptyset$ werden parametrisiert durch

$$\Gamma_{Az^2,Bz^3}(\mathbb{Q}) \quad .$$

Beweis. Wir geben für jedes $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$ explizit eine passende Parametrisierung an. Sei $P = \infty$. Nach Proposition 2.1 gilt für $Q = (s,t)$, $s,t \in K$, daß $Q \in \sigma_K^{-1}(\infty)$ genau dann, wenn (s,t) von der Form $(s,t) = (p\theta^{-2}, q\theta^{-3})$ ist mit $(p,q) \in \Gamma_{Az^2,Bz^3}(\mathbb{Q})$, $q \neq 0$. Damit hat man eine gewünschte Parametrisierung für $\sigma_K^{-1}(\infty)$. Sei $P \neq \infty$, $P = (u,v)$. Sei $(s,t) \in \sigma_K^{-1}(P) \neq \emptyset$, $s = a + b\theta$, $t = c + d\theta$ mit $a,b,c,d \in \mathbb{Q}$, $\lambda := db^{-1}$. Nach Proposition 2.4 ist $(\lambda, 2b)$ Punkt (x,y) auf der Kurve

$$C_P : \quad zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2 \quad ,$$

die damit insbesondere einen $\mathbb{Q}$-rationalen Punkt besitzt, also elliptische

Kurve über $\mathbb{Q}$ ist. Wir identifizieren diese elliptische Kurve als Γ_{Az^2,Bz^3}. Dazu seien h_1, h_2 die Invarianten von C_p :

$$h_1 = -\frac{1}{4}(\alpha\varepsilon - 4\beta\delta + 3\gamma^2)$$

$$h_2 = \frac{1}{4}\begin{vmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \delta \\ \gamma & \delta & \varepsilon \end{vmatrix}$$

mit $\alpha = z$, $\beta = 0$, $\gamma = -zu$, $\delta = -2zv$, $\varepsilon = -z(4A + 3u^2)$. Man rechnet nach:

$$h_1 = Az^2 \quad , \quad h_2 = Bz^3 \quad ,$$

d.h. C_p ist birational äquivalent (über $\mathbb{Q}$) zu Γ_{Az^2,Bz^3} . Eine birationale Transformation

$$\Psi_p : \Gamma_{Az^2,Bz^3} \to C_p$$

konstruiert man auf folgende Weise [Mo,Seite 77].Wir geben eine Folge von birationalen Transformationen an, die C_p in Γ_{Az^2,Bz^3} überführt. Sei (ξ,η) $\mathbb{Q}$-rationaler Punkt auf $C_p = C_p(x,y)$.

$$\boxed{x = x_1 + \xi \quad , \quad y = z^{-1}y_1} \quad .$$

(x_1,y_1) erfüllen die Gleichung $y_1^2 = a_1x_1^4 + b_1x_1^3 + c_1x_1^2 + d_1x_1 + e_1$ mit

$$a_1 = z$$

$$b_1 = 4z\xi$$

$$c_1 = 6z\xi^2 - 6zu$$

$$d_1 = 4z\xi^3 - 12zu - 8zv$$

$$e_1 = z^2\eta^2 \quad .$$

$$\boxed{x_1 = \frac{1}{x_2} \quad , \quad y = \frac{y_2}{x_2}}$$

(x_2,y_2) erfüllen die Gleichung $y_2^2 = e_1x_2^4 + d_1x_2^3 + c_1x_2^2 + b_1x_2 + a_1$.

Falls $e_1 = 0$, wählt man eine Substitution, die c_1 zu Null macht. Man bekommt als Gleichung Γ_{Az^2,Bz^3} . Sei also $e_1 \neq 0$.

$$\boxed{x_2 = \frac{x_3}{z\eta} \quad , \quad y_2 = \frac{y_3}{z\eta}}$$

(x_3,y_3) erfüllen die Gleichung $y_3^2 = x_3^4 + b_3x_3^3 + c_3x_3^2 + d_3x_3 + e_3$ mit

$$b_3 = \frac{d_1}{z\eta}$$
$$c_3 = c_1$$
$$d_3 = b_1z\eta$$
$$e_3 = a_1z^2\eta^2 \quad .$$

$$\boxed{x_3 = x_4 - \frac{1}{4}b_3 \quad , \quad y_3 = y_4}$$

(x_4,y_4) erfüllen die Gleichung $y_4^2 = x_4^4 - 6c_4x_4^2 + 4d_4x_4 + e_4$ mit

$$c_4 = -\frac{1}{6}(c_3 - \frac{3}{8}b_3^2)$$
$$d_4 = \frac{1}{4}(d_3 + \frac{1}{8}b_3^2 - \frac{1}{2}c_3b_3)$$
$$e_4 = -\frac{3}{256}b_3^4 + \frac{1}{16}b_3^2c_3 - \frac{1}{4}b_3d_3 + e_3 \quad .$$

$$\boxed{x_4 = \frac{2\overline{y} - d_4}{2(\overline{x} - c_4)} \quad , \quad y_4 = -x_4^2 + 2\overline{x} + c_4}$$

$(\overline{x},\overline{y})$ erfüllen die Gleichung

$$\Gamma_{Az^2,Bz^3} \quad : \quad \overline{y}^2 = \overline{x}^3 + h_1\overline{x} + h_2 \quad .$$

Sukzessives Einsetzen liefert eine birationale Transformation $\Psi_p = (\Psi_1,\Psi_2)$,

$$x = \Psi_1(\overline{x},\overline{y}) \quad , \quad y = \Psi_2(\overline{x},\overline{y})$$

von Γ_{Az^2,Bz^3} nach C_p und damit die gewünschte Parametrisierung der $\mathbb{Q}$-rationalen Punkte auf C_p (bis auf endlich viele Ausnahmen) und damit

eine Parametrisierung von $\sigma_K^{-1}(P)$ durch $\mathbb{Q}$-rationale Punkte auf Γ_{Az^2,Bz^3}.
Damit ist der Beweis vollständig. ∎

Kennt man $\mathbb{Q}$-rationale Punkte auf $\Gamma_{A,B}$ und Γ_{Az^2,Bz^3}, so kann man mit Satz 3.1 und der im Beweis explizit angegebenen birationalen Abbildung Ψ_P Punkte auf $\Gamma_{A,B}$ konstruieren, die K-rational, aber nicht schon $\mathbb{Q}$-rational sind.

4. Lösungen von $\Gamma_{A,B}$ in S-arithmetischen Ringen.

Sei O_Z Hauptidealring. Sei R ein S-arithmetischer Ring in K,

$$R = O_Z[S^{-1}] \quad ,$$

wo S eine endliche Menge von (paarweise nicht assoziierten) Primelementen in O_Z ist. Ohne Einschränkung nehmen wir an: $\theta^{-1} \in R$.
Es ist $\Gamma_{A,B}(R)$ endlich. Wir beschreiben die Fasern der Spurabbildung

$$\sigma_R : \overline{\Gamma_{A,B}(R)} \to \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\} \quad .$$

Unsere Ergebnisse gestatten es, $\Gamma_{A,B}(R)$ in vielen Fällen explizit zu bestimmen (siehe Kapitel 5).

Sei T die Menge der rationalen Primzahlen, die von den Primelenten in S geteilt werden. Dann ist $R \cap \mathbb{Q} = \mathbb{Z}[T^{-1}]$. Mit Proposition 2.1 haben wir folgende Beschreibung für $\sigma_R^{-1}(\infty)$.

(4.1) Satz. Sei $Q = (s,t)$, $s,t \in R$. Die folgenden Aussagen (i) und (ii) sind äquivalent.

(i) $Q \in \sigma_R^{-1}(\infty)$.

(ii) $(s,t) = (p\theta^{-2}, q\theta^{-3})$ mit $(p,q) \in \Gamma_{Az^2,Bz^3}(\mathbb{Z}[T^{-1}])$, $q \neq 0$.

∎

Für $P \neq \infty$ haben wir den folgenden Satz.

(4.2) Satz. Sei $P \in \Gamma_{A,B}(\mathbb{Z})$, $P = (u,v)$. Sei S derart, daß jedes Primelement in S assoziiert zu seinem Konjugierten ist. Dann gilt für $(s,t) \in \sigma_R^{-1}(P)$:

(i) $s,t \in O_z$.

(ii) Sei $s = \frac{e}{2} + \frac{f}{2}\theta$, $t = \frac{g}{2} + \frac{h}{2}\theta$ mit $e,f,g,h \in \mathbb{Z}$, $\lambda = hf^{-1}$. Dann ist (λ,f) ganzzahliger Punkt (x,y) auf der elliptischen Kurve

$$C_P : \quad zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2 \quad ,$$

und $e = \lambda^2 - u$, $g = (e - 2u)\lambda - 2v$.

Beweis. Sei $(s,t) \in \sigma_R^{-1}(P)$. Zu (i). Sei $\pi \in S$. Dann ist $\varepsilon\pi^\delta = p$ für eine rationale Primzahl p , $\varepsilon \in O_z^*$, $\delta \in \{1,2\}$. Da $u,v \in \mathbb{Z}$, folgt für die Darstellung 2.5 von u und v : $\beta = 0$. Aus Proposition 2.7 folgt für die Darstellung 2.6 von s und t : $\alpha = 0$. Somit sind $s,t \in R$ ganz an der Stelle π . Da $\pi \in S$ beliebig gewählt war, folgt $s,t \in O_z$. Zu (ii). Nach (i) können wir s,t schreiben in der Form $s = \frac{e}{2} + \frac{f}{2}\theta$, $t = \frac{g}{2} + \frac{h}{2}\theta$ mit $e,f,g,h \in \mathbb{Z}$, $e \equiv f \bmod 2$, $g \equiv h \bmod 2$ und $e \equiv g \equiv 0 \bmod 2$, falls $z \equiv 2,3 \bmod 4$ ist. Sei $\lambda := hf^{-1}$. (Man beachte, daß stets $f \neq 0$ ist.) Nach Proposition 2.4 ist (λ,f) Punkt (x,y) auf der Kurve C_P . Aus Gleichung (3) und (4) in Lemma 2.2 folgt $e = \lambda^2 - u$, $g = (e - 2u)\lambda - 2v$, insbesondere folgt $\lambda \in \mathbb{Z}$. Damit ist (ii) bewiesen. ∎

$P \in \Gamma_{A,B}(\mathbb{Z})$ ist für $P \in \Gamma_{A,B}(\mathbb{Q})$ stets dann erfüllt, falls $E(\mathbb{Q})$ endlich ist (Satz von NAGELL-LUTZ). In diesem Falle hat man insbesondere nur endlich viele Fasern $\sigma_R^{-1}(P)$. Damit ist $\Gamma_{A,B}(R)$ gegeben einerseits durch $\Gamma_{A,B}(R \cap \mathbb{Q}) = \Gamma_{A,B}(\mathbb{Q}) = \Gamma_{A,B}(\mathbb{Z})$, andererseits durch die endlich vielen Fasern $\sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$. In vielen Fällen kann man die Fasern mit Satz 4.1 und Satz 4.2 explizit bestimmen. Dabei liegen nach Satz 4.2 Lösungen $(s,t) \in \overline{\Gamma_{A,B}(R)}$ mit $s,t \notin O_z$ notwendig in $\sigma_R^{-1}(\infty)$.

5. Anwendungen.

Sei $R = O_Z[S^{-1}]$ ein S-arithmetischer Ring in K. Dann ist $\Gamma_{A,B}(R)$ endlich. Im allgemeinen bereitet es große Mühe, die Lösungen in $\Gamma_{A,B}(R)$ explizit anzugeben. Aus BAKERS Linearformenresultat (für K) folgt zwar die Existenz eines Algorithmus zur Auffindung der Lösungen, dieser Algorithmus ist jedoch wegen der Größenordnung der vorkommenden reellen Schranken völlig unbrauchbar für explizite Rechnungen.

Unter geeigneten Voraussetzungen können wir nun die Resultate in Kapitel 3 und 4 benutzen und in Fällen, in denen man die Lösungen gewisser diophantischer Gleichungen über $\mathbb{Q}$ kennt, die Lösungen in $\Gamma_{A,B}(R)$ explizit konstruieren.

Die <u>Voraussetzungen</u> an $\Gamma_{A,B}$ und $R = O_Z[S^{-1}]$ sind:

(5.1) O_Z ist Hauptidealring. Jedes Primelement in S ist assoziiert zu seinem Konjugierten. (S endlich). $\theta^{-1} \in R$.

(5.2) $E(\mathbb{Q})$ ist endlich.

$\Gamma_{A,B}(R)$ ist gegeben durch $\Gamma_{A,B}(R \cap \mathbb{Q})$ und $\overline{\Gamma_{A,B}(R)}$. Es ist

$$\Gamma_{A,B}(R \cap \mathbb{Q}) = \Gamma_{A,B}(\mathbb{Q}) = \Gamma_{A,B}(\mathbb{Z}) \quad .$$

<u>Bestimmung von $\overline{\Gamma_{A,B}(R)}$</u>. Dazu bestimmt man die endlich vielen Fasern $\sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) \cup \{\infty\}$.

Ist $E^*(\mathbb{Q})$ <u>endlich</u>, so ist $E(K)$ endlich nach Satz 1.3. In diesem Falle

bestimmt man $\Gamma_{A,B}(K) \supseteq \Gamma_{A,B}(R)$. Die Fasern $\sigma_K^{-1}(P)$ lassen sich aus $\Gamma_{Az^2,Bz^3}(\mathbb{Q})$ mit Hilfe der im Beweis von Satz 3.1 angegebenen rationalen Transformation Ψ_P explizit konstruieren. Nehmen wir also an, daß $E^*(\mathbb{Q})$ unendlich ist.

(i) Bestimmung von $\sigma_R^{-1}(\infty)$. Für die Bestimmung von $\sigma_R^{-1}(\infty)$ hat man die Gleichung

$$y^2 = x^3 + Az^2x + Bz^3 \quad \text{in} \quad \mathbb{Z}[T^{-1}]$$

zu betrachten, wobei T die Menge der rationalen Primzahlen ist, die von den Primelementen in S geteilt werden. Genauer: Nach Satz 4.1 ist $\sigma_R^{-1}(\infty)$ genau durch folgende Elemente (s,t) gegeben: $(s,t) = (p\theta^{-2}, q\theta^{-3})$ mit $(p,q) \in \Gamma_{Az^2,Bz^3}(\mathbb{Z}[T^{-1}])$, $q \neq 0$. Es gibt zahlreiche Beispiele für $a,b \in \mathbb{Z}$ und $T \subset \mathbb{P}$ endlich, in denen die Gleichung $y^2 = x^3 + ax + b$ in $\mathbb{Z}[T^{-1}]$ gelöst worden ist bzw. man die Lösungen mit Standard-Methoden leicht finden kann. (Siehe zum Beispiel [Mo] und [Stro & Ti] , wo auch ausführliche Literturhinweise zu finden sind.)

(ii) Bestimmung von $\sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q})$. Für die Bestimmung von $\sigma_R^{-1}(P)$, $P \in \Gamma_{A,B}(\mathbb{Q}) = \Gamma_{A,B}(\mathbb{Z})$, $P = (u,v)$, hat man die Gleichung

$$zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2 \quad \text{in} \quad \mathbb{Z}$$

zu betrachten. Genauer: Sei $(s,t) \in \sigma_R^{-1}(P)$. Nach Satz 4.2 sind $s,t \in O_z$ und, falls $s = \frac{e}{2} + \frac{f}{2}\theta$, $t = \frac{g}{2} + \frac{h}{2}\theta$ mit $e,f,g,h \in \mathbb{Z}$, gilt: $f \neq 0$, (λ,f) ist ganzzahliger Punkt (x,y) auf der Kurve C_P : $zy^2 = x^4 - 6ux^2 - 8vx - 4A - 3u^2$ und $e = \lambda^2 - u$, $g = (e - 2u)\lambda - 2v$, $h = \lambda f$.

Die diophantische Gleichung $ky^2 = ax^4 + bx^3 + cx^2 + dx + e$

mit $k,a,b,c,d,e \in \mathbb{Z}$ ist in vielen Spezialfällen gelöst worden. Zahlreiche Beispiele dafür findet man in [Mo], wo auch weitere umfangreiche Literatur angegeben ist. Betrachten wir zum Beispiel genauer den

Fall $P = (u,0)$. Sei (x,y) ganzzahliger Punkt auf C_P , sei $w = x^2 - 3u$. Dann gilt

$$(*) \qquad w^2 - zy^2 = 4A + 12u^2 \quad .$$

Für $z < 0$ lassen sich die ganzzahligen Lösungen (w,y) von (*) leicht finden, denn es gilt

$$|w| \leq \sqrt{|4A + 12u^2|} \quad , \quad |y| \leq \sqrt{-z^{-1}|4A + 12u^2|} \quad .$$

Für $z > 0$ ist (*) eine Pellsche Gleichung. Sie besitzt nur endlich viele Lösungen (w,y) , so daß $w = x^2 - 3u$, $x \in \mathbb{Z}$. Wie man diese findet, ist in [Mo,Seite 63] angegeben. Im Falle $A = 0$ hat man wegen Gleichung (*) noch folgendes nützliches Kriterium [La,Corollary 1.8]: Falls $\sigma_R^{-1}(P) \neq \emptyset$, so besitzt O_z ein Element der Norm 3 .

Betrachten wir auch noch den Fall $A = 0$, $P = (0,v)$. In diesem Fall hat man für $(s,t) \in \sigma_R^{-1}(P)$, $s = \frac{e}{2} + \frac{f}{2}\theta$, $t = \frac{g}{2} + \frac{h}{2}\theta$ folgende Bedingung [La,Proposition 1.7] :

(i) $(g - 2v)^2 - zh^2 = 16v^2$ und $h \neq 0$.

(ii) $ef^2 = h^2$.

Gleichung (i) folgt direkt aus der Gleichung für $N(t)$ in Lemma 2.3. Für $z < 0$ kann man die Lösungen der Gleichung $\bar{x}^2 - z\bar{y}^2 = 16v^2$ sofort angeben, für $z > 0$ sucht man gewisse Lösungen einer Pellschen Gleichung.

Die Fasern $\sigma_R^{-1}(P)$, wo $P \in \Gamma_{A,B}(\mathbb{Z})$ von der Form $P = (u,v)$ mit $u = 0$ oder $v = 0$ ist, lassen sich also ohne weiteres bestimmen. Damit ist es

insbesondere ohne weiteres möglich, $\overline{\Gamma_{A,B}(R)}$ vollständig anzugeben, wenn $\Gamma_{A,B}(\mathbb{Q})$ von der Form $\Gamma_{A,B}(\mathbb{Q}) = \{(u,v)\}$ ist mit $u = 0$ oder $v = 0$.

(5.3) Beispiel. Wir betrachten die Gleichung

$$\Gamma_{0,-1}: \quad y^2 = x^3 - 1 \quad .$$

Wir setzen $z = -2$ und bestimmen $\Gamma_{0,-1}(R)$ für

$$R = O_{-2}[\tfrac{1}{\sqrt{-2}}] \quad .$$

Es ist

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{mit} \quad \Gamma_{0,-1}(\mathbb{Q}) = \{(1,0)\} \quad .$$

$$E^*(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad .$$

Die Voraussetzungen 5.1 und 5.2 sind erfüllt. $\Gamma_{0,-1}(R)$ setzt sich zusammen aus $\Gamma_{0,-1}(R \cap \mathbb{Q})$ und $\overline{\Gamma_{0,-1}(R)}$. Es ist $\Gamma_{0,-1}(R \cap \mathbb{Q}) = \{(1,0)\}$. Um $\overline{\Gamma_{0,-1}(R)}$ zu bestimmen, bestimmt man die Fasern $\sigma_R^{-1}(P)$, $P \in \Gamma_{0,-1}(\mathbb{Q}) \cup \{\infty\}$. Dazu muß man die Gleichungen

$$y^2 = x^3 + 2^3 \qquad \text{in } \mathbb{Z}[\tfrac{1}{2}] \quad .$$

$$(x^2 - 3)^2 + 2y^2 = 12 \qquad \text{in } \mathbb{Z} \quad .$$

lösen. Genauer:

(i) Sei $P = \infty$. Nach Satz 4.1 sind die Elemente (s,t) in $\sigma_R^{-1}(\infty)$ gegeben durch $(s,t) = (p\sqrt{-2}^{-2}, q\sqrt{-2}^{-3})$ mit $(p,q) \in \Gamma_{0,2^3}(\mathbb{Z}[\frac{1}{2}])$, $q \neq 0$. Mit Standard-Methoden über $\mathbb{Q}$ beweist man:

$$\Gamma_{0,2^3}(\mathbb{Z}[\tfrac{1}{2}]) = \{(-2,0), (1,\pm 3), (2,\pm 4), (46,\pm 312), (-7\cdot 2^{-2}, \pm 13\cdot 2^{-3})\} \quad .$$

(ii) Sei $P = (1,0)$. Sei $(s,t) \in \sigma_R^{-1}((1,0))$. Nach Satz 4.2 sind $s,t \in O_{-2}$ und für $s = e_o + f_o\sqrt{-2}$, $t = g_o + h_o\sqrt{-2}$ mit $e_o,f_o,g_o,h_o \in \mathbb{Z}$ gilt: $(\lambda,2f_o)$ ist ganzzahliger Punkt auf der Kurve $C_{(1,0)}$: $-2y^2 = x^4 - 6x^2 - 3$ und $2e_o = \lambda^2 - 1$, $g_o = (e_o - 1)\lambda$, $h_o = \lambda f_o$. $C_{(1,0)}$ läßt sich schreiben als $(x^2 - 3)^2 + 2y^2 = 12$. Damit findet man als ganzzahlige Punkte auf $C_{(1,0)}$ sofort: $(x,y) = (\pm 1,\pm 2)$. Daraus folgt $(s,t) = (\sqrt{-2},\pm(1 - \sqrt{-2}))$ oder $(s,t) = (-\sqrt{-2},\pm(1 + \sqrt{-2}))$.

Wir fassen zusammen:

Lösungen von $\Gamma_{0,-1}$: $y^2 = x^3 - 1$ in $R = O_{-2}[\frac{1}{\sqrt{-2}}]$		
$\Gamma_{0,-1}(R \cap \mathbb{Q})$	$\overline{\Gamma_{0,-1}(R)}$	
	$\sigma_R^{-1}(\infty)$	$\sigma_R^{-1}((1,0))$
$(1,0)$	$(-7\sqrt{-2}^{-6},\pm 13\sqrt{-2}^{-9})$ $(\sqrt{-2}^{-2},\pm 3\sqrt{-2}^{-3})$ $(-1,\pm\sqrt{-2})$ $(-23,\pm 8\sqrt{-2})$	$(\sqrt{-2},\pm(1-\sqrt{-2}))$ $(-\sqrt{-2},\pm(1+\sqrt{-2}))$

(5.4) Beispiel. Wir betrachten die Gleichung

$$\Gamma_{1,0} : \quad y^2 = x^3 + x \quad .$$

Wir setzen $z = 3$ und bestimmen $\Gamma_{1,0}(R)$ für

$$R = O_3[\tfrac{1}{\sqrt{3}}] \quad .$$

Es ist

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{mit} \quad \Gamma_{1,0}(\mathbb{Q}) = \{(0,0)\} \quad .$$

$$E^*(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad .$$

Die Voraussetzungen 5.1 und 5.2 sind erfüllt. $\Gamma_{1,0}(R)$ setzt sich zusammen aus $\Gamma_{1,0}(R \cap \mathbb{Q})$ und $\overline{\Gamma_{1,0}(R)}$. Es ist $\Gamma_{1,0}(R \cap \mathbb{Q}) = \{(0,0)\}$. Um $\overline{\Gamma_{1,0}(R)}$ zu bestimmen, bestimmt man die Fasern $\sigma_R^{-1}(P)$, $P \in \Gamma_{1,0}(\mathbb{Q}) \cup \{\infty\}$. Dazu muß man die Gleichungen

$$y^2 = x^3 + 3^2x \qquad \text{in} \quad \mathbb{Z}[\tfrac{1}{3}] \quad ,$$

$$3y^2 = x^4 - 4 \qquad \text{in} \quad \mathbb{Z} \quad .$$

lösen. Genauer:

(i) Sei $P = \infty$. Nach Satz 4.1 sind die Elemente (s,t) in $\sigma_R^{-1}(\infty)$ gegeben durch $(s,t) = (p\sqrt{3}^{-2}, q\sqrt{3}^{-3})$ mit $(p,q) \in \Gamma_{3^2,0}(\mathbb{Z}[\frac{1}{3}])$, $q \neq 0$. Mit Standard-Methoden über $\mathbb{Q}$ beweist man:

$$\Gamma_{3^2,0}(\mathbb{Z}[\tfrac{1}{3}]) = \{(0,0), (4,\pm 10)\} \quad .$$

(ii) Sei $P = (0,0)$. Sei $(s,t) \in \sigma_R^{-1}((0,0))$. Nach Satz 4.2 sind $s,t \in O_3$ und für $s = e_o + f_o\sqrt{3}$, $t = g_o + h_o\sqrt{3}$ mit $e_o, f_o, g_o, h_o \in \mathbb{Z}$ gilt: $(\lambda, 2f_o)$ ist ganzzahliger Punkt auf der Kurve $C_{(0,0)}$: $3y^2 = x^4 - 4$ und $2e_o = \lambda^2$, $g_o = e_o\lambda$, $h_o = \lambda f_o$. Betrachtet man $C_{(0,0)}$ modulo 4 , so folgt $x \equiv y \equiv 0 \bmod 2$, $x,y \in \mathbb{Z}$. Also hat man die Lösungen $(\overline{x},\overline{y})$ der Pel Gleichung $\overline{x}^2 - 3\overline{y}^2 = 1$ zu bestimmen, die von der Form $2\overline{x} = x^2$, $2\overline{y} = y$ sind [Mo,Seite 63] . Als ganzzahlige Punkte auf $C_{(0,0)}$ findet man $(x,y) = (\pm 2, \pm 2)$. Daraus folgt $(s,t) = (2 + \sqrt{3}, \pm(4 + 2\sqrt{3}))$ oder $(2 - \sqrt{3}, \pm(4 - 2\sqrt{3}))$. Wir fassen zusammen:

Lösungen von $\Gamma_{1,0}$: $y^2 = x^3 + x$ in $R = O_3[\frac{1}{\sqrt{3}}]$		
$\Gamma_{1,0}(R \cap \mathbb{Q})$	$\overline{\Gamma_{1,0}(R)}$ $\sigma_R^{-1}(\infty)$	$\sigma_R^{-1}((0,0))$
(0,0)	$(4\sqrt{3}^{-2}, \pm 10\sqrt{3}^{-3})$	$(2+\sqrt{3}, \pm(4+2\sqrt{3}))$ $(2-\sqrt{3}, \pm(4-2\sqrt{3}))$

Wir zeigen nun abschließend, wie man in gewissen Fällen die angegebenen Methoden benutzt, um die Gleichung $\Gamma_{A,B}$: $y^2 = x^3 + Ax + B$ zu lösen, wenn $A,B \in O_{\mathbb{Z}}$ und nicht notwendig $A,B \in \mathbb{Z}$ sind.

Sei R zunächst ein beliebiger Teilring von K, R^* die Einheitengruppe von R.

(5.5) Definition. Eine Transformation $x \to u^2x$, $y \to u^3y$ der Variablen x und y mit $u \in R^*$ heißt zulässige Transformation. Die Gleichung Γ_{A_1,B_1} mit $A_1,B_1 \in O_{\mathbb{Z}}$ heißt äquivalent zur Gleichung Γ_{A_2,B_2} mit $A_2,B_2 \in O_{\mathbb{Z}}$, falls Γ_{A_2,B_2} aus Γ_{A_1,B_1} durch eine zulässige Transformation hervorgeht.

Auf diese Weise ist auf der Menge der Gleichungen Γ_{A_1,B_1} mit $A_1,B_1 \in O_{\mathbb{Z}}$ offensichtlich eine Äquvalenzrelation im abstrakten Sinne gegeben. Sind Γ_{A_1,B_1} und Γ_{A_2,B_2} äquivalent, so ist die von Γ_{A_1,B_1} über K definierte elliptische Kurve E_1 isomorph (über K) zu der von Γ_{A_2,B_2} definierten elliptischen Kurve E_2. Mehr noch: Die zulässige Transformation zwischen Γ_{A_1,B_1} und Γ_{A_2,B_2} induziert eine Bijektion zwischen den Lösungsmengen $\Gamma_{A_1,B_1}(R)$ und $\Gamma_{A_2,B_2}(R)$. Mit anderen Worten: Kennt man $\Gamma_{A_1,B_1}(R)$ für

für eine einzelne Gleichung Γ_{A_1,B_1} , so kennt man $\Gamma_{A_2,B_2}(R)$ für alle Gleichungen Γ_{A_2,B_2} , die äquivalent sind zu Γ_{A_1,B_1} .

Sei nun R ein S-arithmetischer Ring in K , $R = O_Z[S^{-1}]$, und R erfülle die Voraussetzung 5.1. Für eine zulässige Transformation ist $u \in R^*$ gleichbedeutend damit, daß u von der Form $u = \delta \pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$ ist mit $\delta \in O_Z^*$, $\alpha_i \in \mathbb{Z}$, $1 \leq i \leq n$, wobei $S = \{\pi_1, \ldots, \pi_n\}$. Sei Γ_{A_1,B_1} eine gegebene Gleichung mit $A_1, B_1 \in O_Z$, so daß folgendes gilt: Γ_{A_1,B_1} ist äquivalent zu einer Gleichung $\Gamma_{A,B}$ mit folgenden Eigenschaften:

(i) $A,B \in \mathbb{Z}$.

(ii) $E(\mathbb{Q})$ ist endlich (Voraussetzung 5.2).

In diesem Falle kann man $\Gamma_{A_1,B_1}(R)$ bestimmen, indem man $\Gamma_{A,B}(R)$ bestimmt, wie in diesem Kapitel angegeben. In [La] sind die obigen Überlegungen für eine große Klasse von Gleichungen Γ_{A_1,B_1} explizit ausgeführt.

Literaturverzeichnis.

[Ba] A. Baker, Effective Methods in Diophantine Problems. Proc. Symp. Pure Math.,Amer. Math. Soc., Providence, R.I., Vol.20 (1971), 195 - 209, Vol. 24(1974), 1 - 7 .

[Coa] J.Coates, An effective p-adic analogue of a theorem of Thue, I. Acta Arithm. 15(1969), 279 - 305 . II, The greatest prime factor of a binary form. Acta Aritm. 16(1970), 399 - 412. III, The diophantine equation $y^2 = x^3 + k$. Acta Arithm. 16(1970), 425 - 435.

[La] M. Laska, Solving the equation $x^3 - y^2 = r$ in number fields. J. reine u. angew. Math. Band 333(1982), 73 - 85.

[Mah] K. Mahler, Über die rationalen Punkte auf Kurven von Geschlecht 1 . J. reine u. angew. Math. Band 170(1933), 168 - 178.

[Maz] B. Mazur, Rational isogenie of prime degree. Inv. Math. 44(1978), 129 - 162.

[Mo] L.J. Mordell, Diophantine Equations. Academic Press, London, New York 1969.

[Si] C.L. Siegel, Über einige Anwendungen diophantischer Approximationen. Abh. der Preuß. Akad. der Wiss., Physik.-math. Klasse 1929, Nr.1.

[Stro & Ti] R.J. Stroeker, R. Tijdeman, Diophantine Equations. Computational Methods in Number Theory, 154, 155.

[Ta] J. Tate, The arithmetic of elliptic curves. Inv. Math. v. 23(1974), 179 - 206.