Universität Duisburg-Essen, Campus Essen
Fakultät für Mathematik
Master-Studiengang für das Lehramt an Gymnasien und Gesamtschulen

MASTERARBEIT

Primzahltests mit elliptischen Kurven

Autor:
Julian Söhngen
Am Dickelsbach 51
47269 Duisburg
julian.soehngen@stud.uni-duisburg-essen.de
Telefon: 0203 765898
Matrikelnummer: 2272320

Betreuer, Erstgutachter: Prof. Dr. Ulrich Görtz
Zweitgutachter: Dr. Ingo Janiszczak

10. Februar 2017

Inhalt

1 Einleitung

Es gibt unendlich viele Primzahlen. Die bisher größte bekannte Primzahl ist die Mersenne'sche Primzahl $M_{74207281} = 2^{74207281} - 1$. Sie besitzt 22338618 Dezimalstellen und wurde 2016 im Rahmen des Projekts *GIMPS* (Great Internet Mersenne Prime Search) auf einem Computer des US-amerikanischen Mathematikers Curtis Cooper entdeckt. Für Zahlen spezieller Gestalt gibt es spezielle Primzahltests, etwa den *Lucas-Test* für Mersenne'sche Zahlen (siehe zum Beispiel [3] Satz 17.5), das sind Zahlen der Form $2^n - 1$, $n \in \mathbb{N}$. Wie aber kann man zeigen, dass eine Zahl, die keine besondere Gestalt aufweist, prim ist? Eine Zahl $n \in \mathbb{N}$ kann schlicht auf Primalität getestet werden, indem für jede Primzahl $p \leq \sqrt{n}$ geprüft wird, ob sie n teilt. Falls kein solches p ein Teiler von n ist, so ist n prim. Dieser Test ist für große Zahlen natürlich viel zu aufwendig. Mit dem *kleinen Satz von Fermat* können Zahlen von vornherein als Kandidaten für Primzahlen ausgeschlossen werden. Der Satz sagt aus, dass wenn p eine Primzahl ist und es eine ganze Zahl a mit $\mathrm{ggT}(a,p) = 1$ gibt, dann die Kongruenz $a^{p-1} \equiv 1 \pmod{p}$ gilt. Finden wir also ein a mit $\mathrm{ggT}(a,n) = 1$, so dass $a^{n-1} \not\equiv 1 \pmod{n}$, dann kann n keine Primzahl sein. Gilt jedoch $a^{n-1} \equiv 1 \pmod{n}$ für einige beliebige Wahlen von a, so liegt die Vermutung nahe, dass n eine Primzahl ist. Fermats kleiner Satz liefert uns damit einen probabilistischen Primzahltest. Doch wir interessieren uns für einen deterministischen Primzahltest, mit dem wir Kandidaten n, die womöglich tausend Dezimalstellen oder mehr besitzen, effizient auf Primalität prüfen können. Die gängigste Methode, die in dieser Arbeit vorgestellt werden soll, arbeitet mit elliptischen Kurven.

Wir werden uns, genauer gesagt, mit einem Primzahltest befassen, der auf Shafrira Goldwasser und Joe Kilian (1986) zurückgeht. Um die Primalität einer Zahl $n \in \mathbb{N}$ zu zeigen, werden elliptische Kurven über dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ benutzt. Der erste Teil der Arbeit (Kapitel 2) dient dem Zweck, die Theorie der elliptischen Kurven über Ringen in einem für den Primzahltest relevanten Umfang bereitzustellen. Unser Ziel wird es sein, ein fundamentales Theorem zu beweisen: Wenn R ein kommutativer Ring mit 1 ist, der gewisse Bedingungen erfüllt, und eine elliptische Kurve E über R durch eine Weierstraß-Gleichung der Form $y^2z = x^3 + axz^2 + bz^3$ mit $a,b \in R$ gegeben ist, dann bildet die Menge $E(R)$ von Punkten $(x : y : z)$ auf E im projektiven Raum $\mathbb{P}^2(R)$ eine abelsche Gruppe, die additiv geschrieben wird und deren neutrales Element $(0 : 1 : 0)$ ist, wobei 0 das Nullelement von R bezeichnet. Wir werden den Fall betrachten, dass R ein Körper K ist. Die Addition von Punkten in $E(K)$ ist durch eine geometrische Konstruktion erklärt, mit der $E(K)$ die Struktur einer abelschen Gruppe erhält. Aus den Formeln dieser geometrisch begründeten Punktaddition wollen wir Formeln entwickeln, mit denen eine Addition von Punkten in $E(R)$ definiert werden kann, und sodann zeigen, dass $E(R)$ mit dieser Addition zu einer abelschen Gruppe wird. Der Beweis des Theorems stützt sich

auf die Idee, die Gruppeneigenschaften von $E(R)$ durch Rückführung auf den bekannten Körperfall zu zeigen. Der zweite Teil der Arbeit (Kapitel 3) zielt auf den *Goldwasser-Kilian-Primzahltest*. Die erworbene Theorie wird benötigt, um den Satz, auf dem der Primzahltest beruht, zu beweisen. Dieser Satz zeichnet sich dadurch aus, dass wenn man Punkte in $E(\mathbb{Z}/n\mathbb{Z})$ mit bestimmten Eigenschaften gefunden hat, sogleich auf die Primalität einer Zahl $n \in \mathbb{N}$ schließen kann und durch die Angabe der elliptischen Kurve sowie der Punkte mit ihren Eigenschaften ein Zertifikat für die Primalität von n ausstellt, das schnell überprüft werden kann. Wie der Primzahltest genau funktioniert, soll in Form eines Algorithmus festgehalten werden. Die Frage nach der Effizienz des Tests ist eine Frage danach, mit welchem Aufwand die Suche nach einer geeigneten elliptischen Kurve bzw. nach Punkten mit den gewünschten Eigenschaften verbunden ist. Je effizienter die Methoden sind, desto effizienter wird der Test. Ein Beispiel soll den Primzahltest veranschaulichen und bringt die Arbeit zum Abschluss.

Die Zeichnungen in dieser Arbeit wurden mit dem Programm *GeoGebra* erstellt. In dem Abschlussbeispiel zur Veranschaulichung des Primzahltests wurde das mathematische Software-System *SageMath* als Hilfsmittel benutzt.

2 Elliptische Kurven über Ringen

2.1 Grundlegende Definitionen

Die folgenden Ausführungen orientieren sich an [8] Ch. 2 Sec. 2.11.
In diesem Kapitel ist R stets ein kommutativer Ring mit 1, dessen Nullelement wir mit 0 bezeichnen.

Ein Tupel $(x_1, x_2, ...)$ von Elementen aus R heißt *primitiv*, wenn das von ihnen erzeugte Ideal das Einsideal R ist, d.h. wenn es Elemente $r_1, r_2, ... \in R$ gibt, so dass $r_1x_1 + r_2x_2 + ... = 1$. Wir nennen eine $m \times n$-Matrix $(a_{ij})_{1\leq i\leq m,\ 1\leq j\leq n}$ mit Einträgen aus R primitiv, wenn das Tupel $(a_{11}, a_{12}, ..., a_{mn})$, das aus allen Einträgen von M besteht, primitiv ist.

Die Einheitengruppe von R bezeichnen wir mit R^*. Um mit elliptischen Kurven über R arbeiten und später eine Gruppenstruktur einführen zu können, verlangen wir, dass R folgende zwei Bedingungen erfüllt:

1. $6 \in R^*$.
2. Für jede primitive $m \times n$-Matrix $M = (a_{ij})_{1\leq i\leq m,\ 1\leq j\leq n}$ über R, deren 2×2-Unterdeterminanten alle verschwinden, d.h. $a_{ij}a_{kl} - a_{il}a_{kj} = 0$ für alle i, j, k, l mit $1 \leq i < k \leq m$ und $1 \leq j < l \leq n$, gibt es eine R-Linearkombination der Zeilen von M, die als n-Tupel primitiv ist.

Für den Rest des Kapitels erfülle R die Bedingungen 1 und 2.

Die auf der Menge aller primitiven Tripel von Elementen aus R durch

$$(x, y, z) \sim (x', y', z') \iff \exists u \in R^* :\ (x', y', z') = u(x, y, z) = (ux, uy, uz)$$

definierte Relation ist eine Äquivalenzrelation. Für die Äquivalenzklasse von (x, y, z) schreiben wir $(x : y : z)$. Die Menge der Äquivalenzklassen bezeichnen wir mit $\mathbb{P}^2(R)$.

$$\mathbb{P}^2(R) := \left\{(x, y, z) \in R^3 \mid (x, y, z) \text{ ist primitiv}\right\} / \sim$$

ist der zweidimensionale *projektive Raum* über R. Ist $(x, y, z) \in R^3$ primitiv, so ist auch $(ux, uy, uz) \in R^3$ primitiv für jedes $u \in R^*$. Denn seien $u \in R^*$, $v \in R$ mit $uv = 1$ und $r, s, t \in R$ mit $rx + sy + tz = 1$, dann ist $rv \cdot ux + sv \cdot uy + tv \cdot uz = uv = 1$.

Eine *elliptische Kurve* über R ist durch eine homogene Gleichung der Form

$$y^2z = x^3 + axz^2 + bz^3$$

mit $a, b \in R$ gegeben, so dass $4a^3 + 27b^2 \in R^*$. Wir bezeichnen die durch a und b festgelegte elliptische Kurve mit $E_{a,b}$ oder einfach mit E. Die Gleichung $y^2z = x^3 + axz^2 + bz^3$ ist eine vereinfachte

Weierstraß-Gleichung. Weil R die Bedingungen 1 und 2 erfüllt, entspricht die obige Definition dem aus der algebraischen Geometrie bekannten Begriff einer elliptischen Kurve über dem Ring R. In der gesamten Arbeit verstehen wir unter einer elliptischen Kurve $E = E_{a,b}$ über R stets eine durch $y^2z = x^3 + axz^2 + bz^3$ gegebene elliptische Kurve.

Sei $E = E_{a,b}$ eine elliptische Kurve über R.

$$E(R) := \left\{(x : y : z) \in \mathbb{P}^2(R) \mid y^2z = x^3 + axz^2 + bz^3\right\}$$

ist die *Menge von Punkten* auf E im projektiven Raum $\mathbb{P}^2(R)$. Wir sehen schnell, dass $E(R)$ wohldefiniert ist: Wir betrachten $F(x,y,z) = x^3 + axz^2 + bz^3 - y^2z$, ein homogenes Polynom vom Grad 3 in x,y,z, d.h. $F(\lambda x, \lambda y, \lambda z) = \lambda^3 F(x,y,z)$ für alle $\lambda \in R$. Seien $(x',y',z'), (x'',y'',z'')$ zwei verschiedene Repräsentanten von $(x : y : z) \in E(R)$. Dann gibt es ein $u \in R^*$, so dass $(x',y',z') = (ux'', uy'', uz'')$. Da $u^3 \in R^*$, existiert ein $v \in R^*$ mit $u^3v = 1$. Damit gilt

$$F(x',y',z') = 0 \quad \Leftrightarrow \quad u^3F(x'',y'',z'') = 0 \quad \Leftrightarrow \quad vu^3F(x'',y'',z'') = v0 \quad \Leftrightarrow \quad F(x'',y'',z'') = 0.$$

Die Kurvengleichung von E gilt also unabhängig von der Wahl des Repräsentanten von $(x : y : z)$, d.h. jeder Repräsentant erfüllt die Kurvengleichung. Die Punktmenge $E(R)$ ist also wohldefiniert.

Unser Ziel ist es, auf $E(R)$ eine Addition einzuführen, mit der $E(R)$ die Struktur einer abelschen Gruppe bekommt. Wir stellen zunächst das Gruppengesetz vor.

2.2 Das Gruppengesetz von $E(R)$

Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1), P_2 = (x_2 : y_2 : z_2) \in E(R)$. Wir wählen $p_1 = (x_1, y_1, z_1)$ als Repräsentanten von P_1 und $p_2 = (x_2, y_2, z_2)$ als Repräsentanten von P_2 und stellen zusammen mit den Koeffizienten a, b der Kurvengleichung drei Formeln I, II und III auf:

I.

$$\begin{aligned}
x_3^I &= (x_1y_2 - x_2y_1)(y_1z_2 + y_2z_1) + (x_1z_2 - x_2z_1)y_1y_2 - a(x_1z_2 + x_2z_1)(x_1z_2 - x_2z_1) \\
&\quad -3b(x_1z_2 - x_2z_1)z_1z_2 \\
y_3^I &= -3x_1x_2(x_1y_2 - x_2y_1) - y_1y_2(y_1z_2 - y_2z_1) - a(x_1y_2 - x_2y_1)z_1z_2 \\
&\quad +a(x_1z_2 + x_2z_1)(y_1z_2 - y_2z_1) + 3b(y_1z_2 - y_2z_1)z_1z_2 \\
z_3^I &= 3x_1x_2(x_1z_2 - x_2z_1) - (y_1z_2 + y_2z_1)(y_1z_2 - y_2z_1) + a(x_1z_2 - x_2z_1)z_1z_2
\end{aligned}$$

II.

$$x_3^{II} = (x_1^2z_2^2 + x_1x_2z_1z_2 + x_2^2z_1^2 + az_1^2z_2^2)^2(y_1z_2 + y_2z_1) - (x_1z_1z_2^2 + x_2z_1^2z_2)(y_1z_2 + y_2z_1)^3$$

$$\begin{aligned}
y_3^{II} &= (x_1^2z_2^2+x_1x_2z_1z_2+x_2^2z_1^2+az_1^2z_2^2)(x_1z_2(y_1z_2+y_2z_1)^2-x_1y_1^2z_2^3-x_2y_2^2z_1^3-2x_1^2x_2^2z_1z_2\\
&\quad +a(x_1^2z_1z_2^3+x_2^2z_1^3z_2)+b(x_1z_1^2z_2^3+x_2z_1^3z_2^2)-2(x_1^2z_2^2+x_2^2z_1^2)(x_1x_2+az_1z_2)\\
&\quad -(x_1x_2+az_1z_2)^2z_1z_2+(x_1z_2+x_2z_1)(y_1z_2+y_2z_1)^2)-y_1z_1z_2^2(y_1z_2+y_2z_1)^3\\
z_3^{II} &= (y_1z_2+y_2z_1)^3z_1^2z_2^2
\end{aligned}$$

III.

$$\begin{aligned}
x_3^{III} &= y_1y_2(x_1y_2+x_2y_1)-ax_1x_2(y_1z_2+y_2z_1)-a(x_1y_2+x_2y_1)(x_1z_2+x_2z_1)\\
&\quad -3b(x_1y_2+x_2y_1)z_1z_2-3b(x_1z_2+x_2z_1)(y_1z_2+y_2z_1)+a^2(y_1z_2+y_2z_1)z_1z_2\\
y_3^{III} &= y_1^2y_2^2+3ax_1^2x_2^2+9bx_1x_2(x_1z_2+x_2z_1)-a^2x_1z_2(x_1z_2+2x_2z_1)-a^2x_2z_1(2x_1z_2+x_2z_1)\\
&\quad -3ab(x_1z_2+x_2z_1)z_1z_2-(a^3+9b^2)z_1^2z_2^2\\
z_3^{III} &= 3x_1x_2(x_1y_2+x_2y_1)+y_1y_2(y_1z_2+y_2z_1)+a(x_1y_2+x_2y_1)z_1z_2\\
&\quad +a(x_1z_2+x_2z_1)(y_1z_2+y_2z_1)+3b(y_1z_2+y_2z_1)z_1z_2
\end{aligned}$$

(Die Formeln I und III finden sich in [8] Ch. 2 Sec. 2.11.)

Wir definieren eine Matrix

$$M(p_1,p_2) := \begin{pmatrix} x_3^I & y_3^I & z_3^I \\ x_3^{II} & y_3^{II} & z_3^{II} \\ x_3^{III} & y_3^{III} & z_3^{III} \end{pmatrix}$$

über R und werden später sehen, dass $M(p_1,p_2)$ primitiv ist und all ihre 2×2-Unterdeterminanten verschwinden. Da R die Bedingung 2 erfüllt, gibt es eine Linearkombination der Zeilen von $M(p_1,p_2)$, die als Tripel (x_3,y_3,z_3) primitiv ist. Die Addition $+' : E(R)\times E(R)\to E(R)$ auf $E(R)$ ist nun durch

$$(x_1:y_1:z_1)+'(x_2:y_2:z_2) := (x_3:y_3:z_3)$$

definiert. Für $+'$ schreiben wir auch einfach nur $+$. Die Verknüpfung kann unabhängig von der Wahl der als Tripel primitiven Linearkombination definiert werden und ist auch unabhängig von den Wahlen der Repräsentanten von P_1 und P_2 und damit wohldefiniert. Auch dies werden wir später noch sehen. Wir definieren

$$-(x:y:z) := (x:-y:z)$$

für jeden Punkt $(x:y:z)\in E(R)$, wobei $-y$ das Inverse von y bezüglich der Addition in R ist. Ein Beispiel soll die Punktaddition veranschaulichen.

Beispiel 2.1. *Sei* $R=\mathbb{Z}/10\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},...,\overline{9}\}$ *der Restklassenring modulo* 10*. Durch*

$$y^2z \equiv x^3-xz^2+3z^3 \ (mod\ 10)$$

ist eine elliptische Kurve $E = E_{\overline{-1},\overline{3}}$ *gegeben, denn* $ggT(4\cdot(-1)^3+27\cdot 3^2,10) = ggT(239,10) = 1$, *d.h.* $\overline{4\cdot(-1)^3+27\cdot 3^2} \in (\mathbb{Z}/10\mathbb{Z})^*$.

$$P_1 = (\overline{2} : \overline{3} : \overline{1}) \quad \textit{und} \quad P_2 = (\overline{7} : \overline{3} : \overline{1})$$

sind Punkte in $E(\mathbb{Z}/10\mathbb{Z})$, *denn* $\overline{2}^3 - \overline{2} + \overline{3} = \overline{9} = \overline{3}^2$ *und* $\overline{7}^3 - \overline{7} + \overline{3} = \overline{339} = \overline{9} = \overline{3}^2$. *Wir wählen die Repräsentanten* $p_1 = (\overline{2},\overline{3},\overline{1})$ *und* $p_2 = (\overline{7},\overline{3},\overline{1})$ *von* P_1 *und* P_2 *und berechnen mit den Formeln I, II und III die Matrix*

$$M(p_1,p_2) = \begin{pmatrix} x_3^I & y_3^I & z_3^I \\ x_3^{II} & y_3^{II} & z_3^{II} \\ x_3^{III} & y_3^{III} & z_3^{III} \end{pmatrix} = \begin{pmatrix} \overline{5} & \overline{5} & \overline{5} \\ \overline{2} & \overline{2} & \overline{6} \\ \overline{7} & \overline{7} & \overline{1} \end{pmatrix}.$$

Enthält eine Zeile der Matrix eine Einheit des Rings, so ist sie primitiv. Wir sehen sofort, dass die dritte Zeile von $M(p_1,p_2)$ *primitiv ist. Also*

$$P_1 + P_2 = (\overline{7} : \overline{7} : \overline{1}).$$

Theorem 2.2. *Sei* $E = E_{a,b}$ *eine elliptische Kurve über R. Dann bildet* $E(R)$ *zusammen mit der durch die Formeln I, II und III definierten Addition eine abelsche Gruppe. Das neutrale Element ist*

$$\infty := (0 : 1 : 0).$$

Die inversen Elemente sind durch $-(x : y : z) = (x : -y : z)$ *gegeben.*

Der Beweis erfordert einige Vorarbeit. Zuerst wollen wir erklären, wie die Formeln I, II und III zustande kommen. Dafür betrachten wir den Fall, dass R ein Körper ist.

2.3 Herleitung der Additionsformeln

Sei in diesem Unterkapitel R ein Körper K.

Die Bedingung 1 bedeutet, dass die Charakteristik von K ungleich 2 und 3 ist. Jeder Körper erfüllt die Bedingung 2. Denn sei $M = (a_{ij})_{1\le i\le m,\ 1\le j\le n}$ eine $m\times n$-Matrix über K, die primitiv ist, d.h. es gibt einen Eintrag $a_{ij} \neq 0$, und deren 2×2-Unterdeterminanten alle verschwinden, d.h. die Zeilen von M sind proportional zueinander. Wenn $a_{ij} \neq 0$, so ist die i-te Zeile von M primitiv. Wir wollen nun etwas mehr über elliptische Kurven über einem Körper K der Charakteristik ungleich 2 und 3 erfahren und die durch geometrische Konstruktion erklärte Addition von Punkten in $E(K)$ vorstellen, um daraus die Formeln I, II und III herleiten zu können.

Sei $(x : y : z) \in \mathbb{P}^2(K)$. Falls $z \neq 0$, so ist $(x : y : z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right)$. Punkte dieser Form heißen die *endlichen Punkte* in $\mathbb{P}^2(K)$. Ist $z = 0$, dann können wir uns das Dividieren durch z so vorstellen, als

ginge die x- oder y-Koordinate ins Unendliche. Punkte der Form $(x : y : 0)$ werden die *unendlichen Punkte* in $\mathbb{P}^2(K)$ genannt. Die *affine Ebene*

$$\mathbb{A}^2(K) := \left\{(x,y) \in K^2\right\}$$

über K wird durch die injektive Abbildung

$$\mathbb{A}^2(K) \to \mathbb{P}^2(K), \quad (x,y) \mapsto (x : y : 1)$$

bijektiv auf $\mathbb{P}^2(K) \setminus \left\{(x : y : z) \in \mathbb{P}^2(K) \mid z = 0\right\}$ abgebildet, d.h. jedem Punkt (x,y) der affinen Ebene $\mathbb{A}^2(K)$ entspricht genau ein endlicher Punkt $(x : y : 1)$ im projektiven Raum $\mathbb{P}^2(K)$. Wir könnten sagen, dass die affine Ebene durch Hinzunahme der unendlichen Punkte zu $\mathbb{P}^2(K)$ ergänzt wird, und $\mathbb{P}^2(K)$ als projektive Vervollständigung der affinen Ebene auffassen. Dass die Abbildung injektiv ist, sehen wir schnell: Seien $(x_1,y_1),(x_2,y_2) \in \mathbb{A}^2(K)$ mit $(x_1 : y_1 : 1) = (x_2 : y_2 : 1)$. Dann existiert ein $u \in K \setminus \{0\}$, so dass $(ux_2, uy_2, u) = (x_1, y_1, 1)$. Also $u = 1$ und folglich $(x_1,y_1) = (x_2,y_2)$. Damit ist die Injektivität gezeigt.

Sei $E = E_{a,b}$ eine elliptische Kurve über K — gegeben durch $y^2z = x^3 + axz^2 + bz^3$. Welche unendlichen Punkte enthält $E(K)$? Sei $(x : y : z) \in E(K)$ mit $z = 0$. Dann ist $x^3 = 0$, und weil K ein Körper ist, folgt, dass $x = 0$. Da aber $(x,y,z) \in K^3$ primitiv ist, kann y nicht auch noch 0 sein. Damit ist $(0 : 1 : 0)$ der einzige unendliche Punkt in $E(K)$, den wir bereits mit ∞ bezeichnet haben und von nun an den *Punkt im Unendlichen* nennen. $E(K)$ können wir schließlich schreiben als

$$E(K) = \left\{(x : y : 1) \in \mathbb{P}^2(K) \mid y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

und uns eine elliptische Kurve in der affinen Ebene vorstellen und den Punkt im Unendlichen einfach als ein formales Merkmal ansehen. $E(K)$ kann, so betrachtet, als projektive Fortsetzung der durch $y^2 = x^3 + ax + b$ gegebenen Kurve in der affinen Ebene $\mathbb{A}^2(K)$ verstanden werden.

Die inhomogene Gleichung $y^2 = x^3 + ax + b$ können wir auf die homogene Form $y^2z = x^3 + axz^2 + bz^3$ bringen, indem wir x und y durch $\frac{x}{z}$ und $\frac{y}{z}$ ersetzen und dann mit z^3 durchmultiplizieren. $y^2z = x^3 + axz^2 + bz^3$ ist eine vereinfachte Weierstraß-Gleichung. Ihre allgemeine Form lautet

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

$a_1, a_2, a_3, a_4, a_6 \in K$. Da die Charakteristik von K ungleich 2 und 3 ist, können wir die allgemeine Weierstraß-Gleichung vereinfachen. Wir betrachten dafür ihre inhomogene Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Da die Charakteristik von K ungleich 2 ist, können wir y durch $\frac{1}{2}(y - a_1x - a_3)$ ersetzen und die Gleichung vereinfachen zu

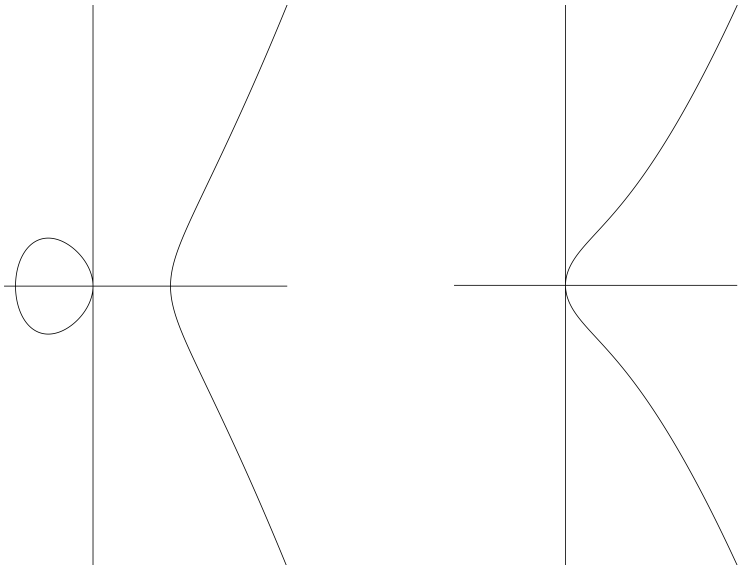
$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

mit $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$. Da die Charakteristik von K auch ungleich 3 ist, können wir x und y durch $\frac{1}{36}(x - 3b_2)$ und $\frac{1}{108}y$ ersetzen und erhalten schließlich

$$y^2 = x^3 + ax + b$$

mit $a = 27(24b_4 - b_2^2)$ und $b = 54(b_2^3 - 36b_2b_4 + 216b_6)$.

Um eine anschauliche Vorstellung von elliptischen Kurven zu bekommen, betrachten wir den Körper $\mathbb{R}$ der reellen Zahlen und zwei elliptische Kurven in der affinen Ebene $\mathbb{A}^2(\mathbb{R})$, die durch $y^2 = x^3 - x$ und $y^2 = x^3 + x$ gegeben sind (die Beispiele sind entnommen aus [8] Ch. 2 Sec. 2.1):



$y^2 = x^3 - x$ $y^2 = x^3 + x$

So sehen die Grundformen elliptischer Kurven in der affinen Ebene über $\mathbb{R}$ aus. Das Polynom $p_1(x) = x^3 - x$ besitzt drei verschiedene reelle Nullstellen und das Polynom $p_2(x) = x^3 + x$ hat nur eine reelle Nullstelle. Damit die Addition von Punkten in $E(K)$ auf eindeutige Weise eingeführt werden kann, möchten wir ausschließen, dass $p(x) = x^3 + ax + b$ mehrfache Nullstellen besitzt.

Lemma 2.3 ([3] Lemma 19.1)**.** *Sei $p(x) = x^3 + ax + b \in K[x]$ ein Polynom mit Koeffizienten $a, b \in K$ — K ist ein Körper der Charakteristik ungleich 2 und 3. Hat p eine mehrfache Nullstelle n_0 in einem Erweiterungskörper $L \supset K$, so ist $n_0 \in K$. Genau dann hat p keine mehrfachen Nullstellen, wenn*

$$4a^3 + 27b^2 \neq 0.$$

Beweis. Wir argumentieren wie in [3] §19. Sei n_0 eine zweifache Nullstelle von p. Dann besitzt p noch eine weitere Nullstelle n_1. Es gilt

$$x^3 + ax + b = p(x) = (x - n_0)^2(x - n_1) = x^3 - (2n_0 + n_1)x^2 + (n_0^2 + 2n_0n_1)x - n_0^2n_1.$$

Ein Koeffizientenvergleich ergibt

(1) $2n_0 + n_1 = 0$,

(2) $n_0^2 + 2n_0n_1 = a$,

(3) $-n_0^2n_1 = b$.

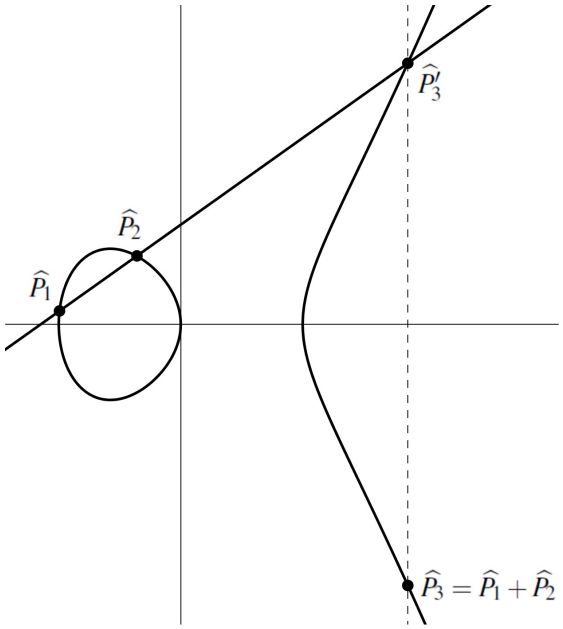
Aus (1) folgt $n_1 = -2n_0$ und damit aus (2) $n_0^2 = -\frac{a}{3}$. Falls $a = 0$, so sehen wir sofort, dass $n_0 = 0 \in K$ und folglich $n_1 = 0 \in K$, womit dann $4a^3 + 27b^2 = 0$. Falls $a \neq 0$, so erhalten wir mit $n_0^2 = -\frac{a}{3}$ aus (3) $n_1 = \frac{3b}{a} \in K$ und damit aus (1) $n_0 = -\frac{3b}{2a} \in K$. Mit diesen Identitäten können wir (2) umformen zu $4a^3 + 27b^2 = 0$.

Sei umgekehrt $4a^3 + 27b^2 = 0$. Falls $a = 0$, so ist $b = 0$ und damit $p(x) = x^3$. D.h. $n_0 = 0$ ist eine dreifache Nullstelle. Falls $a \neq 0$, dann ist, wie gerade gesehen, $n_0 = -\frac{3b}{2a}$ eine zweifache und $n_1 = \frac{3b}{a}$ eine einfache Nullstelle von p. □

Nun wollen wir die Addition von Punkten in $E(K)$ durch eine geometrische Konstruktion erklären. Sei $E = E_{a,b}$ eine elliptische Kurve über K und seien $P_1, P_2 \in E(K)$ endliche Punkte. Dann können wir P_1, P_2 auf die Form $P_1 = (x_1 : y_1 : 1), P_2 = (x_2 : y_2 : 1)$ bringen. Diesen Punkten entsprechen die Punkte $\widehat{P_1} = (x_1, y_1), \widehat{P_2} = (x_2, y_2)$ auf der elliptischen Kurve $\widehat{E}$ — gegeben durch $y^2 = x^3 + ax + b$ — in der affinen Ebene $\mathbb{A}^2(K)$. Wir beginnen mit dem Fall, dass $P_1 \neq -P_2$ bzw. $(x_1, y_1) \neq (x_2, -y_2)$. Um $\widehat{P_1}$ und $\widehat{P_2}$ zu addieren, legen wir eine Gerade durch $\widehat{P_1}$ und $\widehat{P_2}$, die, falls $\widehat{P_1} = \widehat{P_2}$, die Tangente an E in $\widehat{P_1}$ ist. Sei $\widehat{P_3'} = (x_3, y_3)$ der dritte Schnittpunkt der Geraden mit $\widehat{E}$. Dann ist die Summe von $\widehat{P_1}$ und $\widehat{P_2}$ durch

$$\widehat{P_1} + \widehat{P_1} := -\widehat{P_3'} = (x_3, -y_3),$$

die Spiegelung von $\widehat{P_3'}$ an der x-Achse, definiert. Das folgende Bild veranschaulicht die geometrische Konstruktion der Punktaddition, wobei $\widehat{P_3} := -\widehat{P_3'}$:



Die Gerade ist durch $y = \lambda(x - x_1) + y_1$ gegeben, wobei λ die Form

$$\lambda_1 = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{oder} \quad \lambda_2 = \frac{x_2^2 + x_2 x_1 + x_1^2 + a}{y_2 + y_1}$$

hat (vgl. [5] 105). Mindestens eine dieser Versionen von λ ist wohldefiniert, da $\widehat{P_1} \neq -\widehat{P_2}$, und sie sind identisch, falls beide wohldefiniert sind. Die Summe $\widehat{P_3} = \widehat{P_1} + \widehat{P_2}$ ist durch $\widehat{P_3} = (x_3, y_3)$ mit

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

gegeben. Im projektiven Raum $\mathbb{P}^2(K)$ erhalten wir

$$P_1 + P_2 = P_3 = (x_3 : y_3 : 1).$$

Falls $P_1 = -P_2$, so setzen wir $P_1 + P_2 = \infty$, und legen $P + \infty = \infty$ für alle Punkte $P \in E(K)$ fest.

Mit der so definierten Punktaddition bildet $E(K)$ eine abelsche Gruppe, deren neutrales Element $\infty = (0 : 1 : 0)$ ist. Die Kommutativität ergibt sich schon aus geometrischer Betrachtung, denn die Gerade durch $\widehat{P_1}$ und $\widehat{P_2}$ ist dieselbe wie die Gerade durch $\widehat{P_2}$ und $\widehat{P_1}$. Anhand der Formeln sehen wir sofort, dass die Koordinaten von $\widehat{P_1} + \widehat{P_2}$ wieder in K liegen. Nach Konstruktion erfüllt $\widehat{P_1} + \widehat{P_2}$ auch die Kurvengleichung. Somit ist $E(K)$ abgeschlossen unter der Addition. Per Definition spielt ∞ die Rolle des neutralen Elements. Das Inverse $-P = (x : -y : 1)$ eines endlichen Punktes $P = (x : y : 1)$ ist durch den Spiegelpunkt $(x, -y)$ von (x, y) bezüglich der Spiegelung an der x-Achse gegeben. Die Assoziativität kann nicht so leicht begründet werden. Es ist keinesfalls offensichtlich, dass wenn $\widehat{P'}$ der dritte Schnittpunkt der Geraden durch $\widehat{P_1} + \widehat{P_2}$ und $\widehat{P_3}$ mit der elliptischen Kurve ist und $\widehat{P''}$ der dritte Schnittpunkt der Geraden durch $\widehat{P_1}$ und $\widehat{P_2} + \widehat{P_3}$ mit der elliptischen Kurve ist, dann $-\widehat{P'} = -\widehat{P''}$. Die Assoziativität folgt aus $-((\widehat{P_1} + \widehat{P_2}) + \widehat{P_3}) = -(\widehat{P_1} + (\widehat{P_2} + \widehat{P_3}))$. Um dies zu zeigen, konstruiert man bestimmte Geraden und betrachtet deren Schnittpunkte untereinander und mit der elliptischen Kurve. Hier treten verschiedene Fälle auf, die dann zu untersuchen sind. Der Beweis der Assoziativität sowie eine genauere Herleitung der soeben aufgestellten Formeln finden sich in [8] Ch. 2.

Legen wir einen Ring zugrunde, der kein Körper ist, so kann es passieren, dass der Nenner von λ_1 oder λ_2 nicht invertierbar ist und die Formeln sonach nicht wohldefiniert sind. Im Körperfall sind sie stets wohldefiniert, weshalb wir sie von nun an die *Körperformeln* nennen. Aus den Körperformeln wollen wir nun die bereits vorgestellten Formeln I, II und III herleiten. Wir kommen zu einem Lemma, das für den Beweis des Theorems 2.2 fundamental ist.

Lemma 2.4. *Seien P_1 und P_2 Punkte in $E(K)$ — K ist ein Körper der Charakteristik ungleich 2 und 3 — mit Repräsentanten $p_1 = (x_1, y_1, z_1)$ und $p_2 = (x_2, y_2, z_2)$. Sei $M(p_1, p_2)$ die auf den Formeln I, II und III beruhende Matrix. Dann gilt:*

(i) Mindestens eine der Formeln I, II, III liefert ein Ergebnis ungleich $(0,0,0)$. *(D.h. die Matrix* $M(p_1,p_2)$ *ist primitiv.)*

(ii) Jedes von $(0,0,0)$ *verschiedene Ergebnis aus I, II, III liefert als Punkt in* $\mathbb{P}^2(K)$ *das korrekte Ergebnis der Addition von* P_1 *und* P_2. *(Insbesondere gilt: Alle* 2×2*-Unterdeterminanten von* $M(p_1,p_2)$ *verschwinden.)*

Beweis. Wir entwickeln die Formeln I, II und III aus den Körperformeln. Seien $P_1=(x_1:y_1:z_1), P_2=(x_2:y_2:z_2)\in E(K)$ endlich. Wir schreiben

$$P_1=\left(\frac{x_1}{z_1}:\frac{y_1}{z_1}:1\right) \quad \text{und} \quad P_2=\left(\frac{x_2}{z_2}:\frac{y_2}{z_2}:1\right)$$

und benutzen ebendiese x- und z-Koordinaten, um mit den Körperformeln x_3 und y_3 zu berechnen und so $(x_3:y_3:1)=P_3=P_1+P_2$ zu erhalten.

Formel I. Es gelte $x_2z_1-x_1z_2\neq 0$. Dann ist

$$\lambda_1=\frac{\frac{y_2}{z_2}-\frac{y_1}{z_1}}{\frac{x_2}{z_2}-\frac{x_1}{z_1}}=\frac{y_2z_1-y_1z_2}{x_2z_1-x_1z_2}$$

wohldefiniert und x_3,y_3 sind durch

$$x_3=\lambda_1^2-\frac{x_1}{z_1}-\frac{x_2}{z_2} \quad \text{und} \quad y_3=\lambda_1\left(\frac{x_1}{z_1}-x_3\right)-\frac{y_1}{z_1}$$

gegeben. Multiplizieren wir x_3 und y_3 mit $\frac{(x_2z_1-x_1z_2)^3}{z_1z_2}$, wobei $z_1,z_2\neq 0$, da P_1,P_2 endlich sind, und ersetzen x_i^3 durch $y_i^2z_i-ax_iz_i^2-bz_i^3$ für $i=1,2$, dann erhalten wir — nach mühsamem Rechnen —

$$\frac{(x_2z_1-x_1z_2)^3}{z_1z_2}\cdot(x_3,y_3,1)=(x_3^I,y_3^I,z_3^I),$$

d.h. die Formel I. Da $\frac{(x_2z_1-x_1z_2)^3}{z_1z_2}\neq 0$, ist $P_3=(x_3^I:y_3^I:z_3^I)$.

Formel II. Es gelte $y_1z_2+y_2z_1\neq 0$. Dann ist

$$\lambda_2=\frac{(\frac{x_2}{z_2})^2+\frac{x_2x_1}{z_1z_2}+(\frac{x_1}{z_1})^2+a}{\frac{y_2}{z_2}+\frac{y_1}{z_1}}=\frac{x_2^2z_1^2+x_1x_2z_1z_2+x_1^2z_2^2+az_1^2z_2^2}{(y_1z_2+y_2z_1)z_1z_2}$$

wohldefiniert und

$$x_3=\lambda_2^2-\frac{x_1}{z_1}-\frac{x_2}{z_2} \quad \text{und} \quad y_3=\lambda_2\left(\frac{x_1}{z_1}-x_3\right)-\frac{y_1}{z_1}.$$

Wir multiplizieren x_3 mit $(y_1z_2+y_2z_1)^2z_1^2z_2^2$, ersetzen x_i^3 durch $y_i^2z_i-ax_iz_i^2-bz_i^3$ für $i=1,2$ und dividieren den entstandenen Term durch $z_1z_2\neq 0$. Dies führt auf einen neuen Term q ohne Nenner. Wir multiplizieren y_3 mit $z_3^{II}=(y_1z_2+y_2z_1)^3z_1^2z_2^2$ und ersetzen $x_3(y_1z_2+y_2z_1)^2z_1z_2$ durch q. So entsteht y_3^{II}. Multiplizieren wir x_3 mit z_3^{II}, verschwinden auch hier die Nenner und wir erhalten

$$z_3^{II}(x_3,y_3,1)=(x_3^{II},y_3^{II},z_3^{II}),$$

also die Formel II. Da $z_3^{II} \neq 0$, gilt $P_3 = (x_3^{II} : y_3^{II} : z_3^{II})$.

Formel III. Sei

$$r := \frac{x_1z_2 + x_2z_1}{z_1z_2} + \frac{x_1y_2 + x_2y_1}{x_1z_2 - x_2z_1} - \left(\frac{y_1z_2 + y_2z_1}{x_1z_2 - x_2z_1}\right)^3$$

(vgl. [2] Ch. 5) wohldefiniert. Multiplizieren wir (x_3^I, y_3^I, z_3^I) mit r, führt dies nach mühsamem Rechnen auf die Formel III, d.h. es gilt

$$r(x_3^I, y_3^I, z_3^I) = (x_3^{III}, y_3^{III}, z_3^{III}).$$

So gehen die Formeln I und II aus den auf λ_1 bzw. λ_2 beruhenden Körperformeln hervor und III entsteht aus I. Daraus folgt, dass wenn P_1, P_2 endliche Punkte sind mit $P_1 \neq -P_2$, dann jedes aus I, II, III entstehende Tripel ungleich $(0,0,0)$ als Punkt in $\mathbb{P}^2(K)$ stets das korrekte Ergebnis $P_3 = P_1 + P_2$ liefert, d.h. alle Tripel ungleich $(0,0,0)$ definieren denselben Punkt in $\mathbb{P}^2(K)$. Falls $P_1 = -P_2$, so führt I mit den Repräsentanten $(x_1, y_1, 1)$ und $(x_1, -y_1, 1)$ von P_1 und P_2 auf das Tripel $(0, y_3^I, 0)$. Die Formel II liefert $(0, y_3^{II}, 0)$ und die Formel III bringt $(0, y_3^{III}, 0)$ hervor. Also definiert jedes dieser drei Tripel, das ungleich $(0,0,0)$ ist, denselben Punkt $(0:1:0) = \infty$ und liefert damit das korrekte Ergebnis der Addition von P_1 und P_2, wenn $P_1 = -P_2$. Ist P_1 weiterhin ein endlicher Punkt, P_2 aber der Punkt im Unendlichen, dann bringt I mit den Repräsentanten (x_1, y_1, z_1) und $(0,1,0)$ von P_1 und ∞ das Tripel $z_1(x_1, y_1, z_1)$ hervor. Da $z_1 \neq 0$, erhalten wir das korrekte Ergebnis $(z_1x_1 : z_1y_1 : z_1z_1) = (x_1 : y_1 : z_1) = P_1$ der Addition von P_1 und ∞. Die Formel II führt auf $(0,0,0)$ und die Formel III liefert $y_1(x_1, y_1, z_1)$, also ebenfalls das korrekte Ergebnis $(x_1 : y_1 : z_1) = P_1$, wenn $y_1 \neq 0$. Falls $P_1 = \infty = P_2$, so bringt III mit dem Repräsentanten $(0,1,0)$ von ∞ das Tripel $(0,1,0)$ hervor und damit das korrekte Ergebnis $(0:1:0) = \infty$ der Addition von ∞ mit sich selbst. Die Formeln I und II führen beide auf das Tripel $(0,0,0)$. Daraus folgt (ii).

Wir haben gesehen, dass wenn P_1, P_2 endliche Punkte mit $P_1 \neq -P_2$ sind oder P_1 endlich und $P_2 = \infty$ ist oder $P_1 = \infty = P_2$, dann mindestens eine der Formeln I, II, III das Ergebnis $P_3 = P_1 + P_2$ liefert. Daher muss mindestens ein Tripel, das bei der Berechnung von P_3 aus I, II, III entsteht, ungleich $(0,0,0)$ sein. Wenn P_1, P_2 endliche Punkte mit $P_1 = -P_2$ sind, dann bringen die Formeln I, II und III mit den Repräsentanten $(x_1, y_1, 1)$ und $(x_1, -y_1, 1)$ von P_1 und P_2 die Tripel $(0, y_3^I, 0)$, $(0, y_3^{II}, 0)$ und $(0, y_3^{III}, 0)$ hervor. Wir wollen zeigen, dass nicht alle drei Tripel zugleich $(0,0,0)$ sein können. Wir betrachten

$$y_3^I = y_1(6(x_1^3 + ax_1 + b) + 2y_1^2) = y_1(6y_1^2 + 2y_1^2) = 8y_1^2.$$

Wenn $y_1 \neq 0$, dann ist $y_3^I \neq 0$, denn die Charakteristik von K ist ungleich 2, also $8 \neq 0$. In diesem Fall liefert I also das Ergebnis $(0 : y_3^I : 0) = (0:1:0) = \infty$. Ist aber $y_1 = 0$, stellt sich die Frage, mit welcher Formel $(x_1 : 0 : 1) + (x_1 : 0 : 1)$ berechnet werden kann. Mit dem Repräsentanten $(x_1, 0, 1)$ von $(x_1 : 0 : 1)$ liefert III das Tripel $(0, y_3^{III}, 0)$. Wir wissen, dass x_1 eine Nullstelle des Polynoms

$p(x) = x^3 + ax + b$ ist, denn aus $(x_1 : 0 : 1) \in E(K)$ folgt, dass $0 = x_1^3 + ax_1 + b$. Damit können wir y_3^{III} wie folgt umformen:

$$\begin{aligned} y_3^{III} &= 3ax_1^4 + 18bx_1^3 - 6a^2x_1^2 - 6abx_1 - a^3 - 9b^2 \\ &= 3ax_1^4 + 18(-x_1^3 - ax_1)x_1^3 - 6a^2x_1^2 - 6a(-x_1^3 - ax_1)x_1 - a^3 - 9(-x_1^3 - ax_1)^2 \\ &= -27x_1^3(x_1^3 + ax_1) - 9a^2x_1^2 - a^3 \\ &= 27bx_1^3 - 9a^2x_1^2 - a^3 \\ &= 27b(-ax_1 - b) - 9a^2x_1^2 - a^3 \\ &= -9a^2x_1^2 - 27abx_1 - a^3 - 27b^2. \end{aligned}$$

Wenn $a = 0$, so ist $b \neq 0$, denn sonst wäre $4a^3 + 27b^2 = 0$ und dieser Fall kann nicht eintreten, da das Gegenteil vorausgesetzt ist. Mit $a = 0$ und $b \neq 0$ ist $y_3^{III} = -27b^2 \neq 0$, denn $27 \neq 0$, da die Charakteristik von K ungleich 3 ist. In diesem Fall bringt III also das Ergebnis $(0 : y_3^{III} : 0) = (0 : 1 : 0) = \infty$ der Addition von $(x_1 : 0 : 1)$ mit sich selbst hervor. Sei nun $a \neq 0$. Wir nehmen an, dass $y_3^{III} = 0$, d.h.

$$-9a^2x_1^2 - 27abx_1 - a^3 - 27b^2 = 0.$$

Wir lösen die Gleichung nach x_1 auf und erhalten

$$x_1 = -\frac{3b}{2a} \pm \sqrt{-\frac{4a^3 + 27b^2}{36a^2}}.$$

Um x_1 einfacher darzustellen, setzen wir $c := \frac{3b}{2a}$ und $d := -\frac{4a^3+27b^2}{36a^2}$. Damit ist $x_1 = -c \pm \sqrt{d}$. Setzen wir x_1 in $p(x)$ ein, führt dies auf

$$p(x_1) = (-c \pm \sqrt{d})^3 + a(-c \pm \sqrt{d}) + b = -c^3 \pm \sqrt{d}(3c^2 + d + a) - 3cd - ac + b.$$

Wir möchten a und b mit c und d ausdrücken:

$$\begin{aligned} a &= \tfrac{4a^3}{4a^2} = \tfrac{-27b^2+4a^3+27b^2}{4a^2} = -3\tfrac{9b^2}{4a^2} + 9\tfrac{4a^3+27b^2}{36a^2} = -3c^2 - 9d, \\ b &= \tfrac{2a}{3} \cdot \tfrac{3b}{2a} = \tfrac{2a}{3}c = \tfrac{2ac}{3} = \tfrac{2(-3c^2-9d)c}{3} = -2c(c^2 + 3d). \end{aligned}$$

Mit $a = -3c^2 - 9d$ und $b = -2c(c^2 + 3d)$ erhalten wir schließlich

$$p(x_1) = -c^3 \pm \sqrt{d}(3c^2 + d - 3c^2 - 9d) - 3cd - (-3c^2 - 9d)c - 2c(c^2 + 3d) = \mp 8d\sqrt{d}.$$

Nach Voraussetzung gilt, dass $4a^3 + 27b^2 \neq 0$ und $a \neq 0$. Da die Charakteristik von K ungleich 2 und 3 ist, folgt, dass $36 \neq 0$ und $8 \neq 0$. Daher ist $d = -\frac{4a^3+27b^2}{36a^2} \neq 0$. Daraus folgt, dass $p(x_1) = \mp 8d\sqrt{d} \neq 0$ im Widerspruch dazu, dass x_1 eine Nullstelle von p ist. Also war die Annahme falsch, d.h. $y_3^{III} \neq 0$. Die Formel III liefert auch in diesem Fall wieder das Ergebnis $(0 : y_3^{III} : 0) = (0 : 1 : 0) = \infty$ der Addition von $(x_1 : 0 : 1)$ mit sich selbst. Daraus folgt (i). □

2.4 Beweis der Gruppeneigenschaften von $E(R)$

Wir kommen nun zu dem Beweis des Theorems 2.2, der wie folgt strukturiert ist. Zuerst zeigen wir, dass $+ : E(R) \times E(R) \to E(R)$ eine wohldefinierte Verknüpfung ist. Dafür sollten wir uns klarmachen, dass die Punktaddition sowohl unabhängig von der Wahl der Linearkombination definiert werden kann, dass also jede als Tripel primitive Linearkombination denselben Punkt in $\mathbb{P}^2(R)$ hervorbringt, als auch unabhängig von den Wahlen der Punktrepräsentanten ist, d.h. dass jedes Repräsentantenpaar (p_1, p_2) von $(P_1, P_2) \in E(R) \times E(R)$ denselben Punkt $P_3 = P_1 + P_2$ in $\mathbb{P}^2(R)$ definiert. Wenn die Matrix $M(p_1, p_2)$ primitiv ist und all ihre 2×2-Unterdeterminanten verschwinden, so gibt es Bedingung 2 zufolge ein primitives Tripel (x_3, y_3, z_3) als Linearkombination der Zeilen von $M(p_1, p_2)$. Wenn (x_3, y_3, z_3) zudem die Kurvengleichung von E erfüllt, ist $(x_3 : y_3 : z_3) \in E(R)$. Daraus folgt, dass $E(R)$ unter der wohldefinierten Addition abgeschlossen ist. Anschließend beweisen wir die Eigenschaften, die $E(R)$ zu einer abelschen Gruppe machen. Entsprechend dieser Struktur baut sich der Beweis in mehreren Schritten auf.

Schritt 1. *Die Verknüpfung $+ : E(R) \times E(R) \to E(R)$ kann unabhängig von der Wahl der als Tripel primitiven Linearkombination definiert werden.*

Lemma 2.5. *Sei S ein Ring (kommutativ mit 1) und sei $M = (a_{ij})_{1 \le i \le m,\ 1 \le j \le n}$ eine $m \times n$-Matrix über S, deren 2×2-Unterdeterminanten alle verschwinden, d.h. $a_{ij}a_{kl} - a_{il}a_{kj} = 0$ für alle i, j, k, l mit $1 \le i < k \le m$ und $1 \le j < l \le n$. Seien $(b_1, ..., b_n), (b'_1, ..., b'_n) \in S^3$ primitive n-Tupel, die jeweils als Linearkombination der Zeilen von M darstellbar sind. Dann gibt es ein $u \in S^*$, so dass $b'_j = ub_j$ für alle $j = 1, ..., n$. (D.h. die Linearkombination ist eindeutig bis auf Multiplikation mit Einheiten. Erfüllt S zusätzlich die Bedingung 2, so definieren $(b_1, ..., b_n), (b'_1, ..., b'_n)$ denselben Punkt in $\mathbb{P}^{n-1}(S)$.)*

Beweis. Zunächst wollen wir zeigen, dass alle 2×2-Unterdeterminanten von

$$M' := \begin{pmatrix} b_1 & ... & b_n \\ b'_1 & ... & b'_n \end{pmatrix}$$

verschwinden, d.h. $b_j b'_l - b_l b'_j = 0$ für alle j, l mit $1 \le j < l \le n$. Wir stellen $(b_1, ..., b_n), (b'_1, ..., b'_n)$ jeweils als Linearkombination der Zeilen von M dar:

$$\begin{aligned} (b_1, ..., b_n) &= \textstyle\sum_{i=1}^m r_i (a_{i1}, ..., a_{in}) = (\sum_{i=1}^m r_i a_{i1}, ..., \sum_{i=1}^m r_i a_{in}), \\ (b'_1, ..., b'_n) &= \textstyle\sum_{k=1}^m r'_k (a_{k1}, ..., a_{kn}) = (\sum_{k=1}^m r'_k a_{k1}, ..., \sum_{i=1}^m r'_k a_{kn}), \end{aligned}$$

$r_i, r'_k \in R'$ für alle i, k. Dann gilt

$$\begin{aligned} b_j b'_l - b_l b'_j &= (\textstyle\sum_{i=1}^m r_i a_{ij}) \cdot (\sum_{k=1}^m r'_k a_{kl}) - (\sum_{i=1}^m r_i a_{il}) \cdot (\sum_{k=1}^m r'_k a_{kj}) \\ &= \textstyle\sum_{i=1}^m \sum_{k=1}^m r_i r'_k (a_{ij}a_{kl} - a_{il}a_{kj}) = \sum_{i=1}^m \sum_{k=1}^m r_i r'_k \cdot 0 \\ &= 0 \end{aligned}$$

für alle j,l. Da $(b_1,...,b_n)$ primitiv ist, gibt es $s_1,...,s_n \in S$, so dass $\sum_{l=1}^n s_l b_l = 1$. Sei $u := \sum_{l=1}^n s_l b'_l$. Dann ist $ub_j = b'_j$ für alle $j = 1,...,n$, denn mit $b'_l b_j = b'_j b_l$ gilt

$$\begin{aligned} ub_j - b'_j &= (\textstyle\sum_{l=1}^n s_l b'_l b_j) - b'_j = (\sum_{l=1}^n s_l b'_j b_l) - b'_j = b'_j(\sum_{l=1}^n s_l b_l) - b'_j \\ &= b'_j((\textstyle\sum_{l=1}^n s_l b_l) - 1) = b'_j(1-1) = b'_j \cdot 0 \\ &= 0. \end{aligned}$$

Es bleibt zu zeigen, dass u eine Einheit von S ist. Da $(b'_1,...,b'_n)$ primitiv ist, existieren $t_1,...,t_n \in S$, so dass $\sum_{j=1}^n t_j b'_j = 1$. Mit $v := \sum_{j=1}^n t_j b_j$ und $ub_j = b'_j$ für alle $j = 1,...,n$ ist dann $uv = \sum_{j=1}^n t_j u b_j = \sum_{l=1}^n t_j b'_j = 1$. □

Schritt 1. Sei E eine elliptische Kurve über R und seien P_1 und P_2 Punkte in $E(R)$ mit Repräsentanten p_1 und p_2. Aus den Formeln I, II und III entsteht die Matrix $M(p_1,p_2)$. Nach Lemma 2.5 definiert jede als Tripel primitive Linearkombination der Zeilen von $M(p_1,p_2)$ denselben Punkt in $\mathbb{P}^2(R)$. Wählen wir also eine Linearkombination der Zeilen von $M(p_1,p_2)$, die als Tripel $(x_3,y_3,z_3) \in R^3$ primitiv ist, so ist (x_3,y_3,z_3) eindeutig bis auf Multiplikation mit Einheiten von R. □

Schritt 2. *Die Verknüpfung $+ : E(R) \times E(R) \to E(R)$ kann unabhängig von der Wahl des Repräsentantenpaares von $(P_1,P_2) \in E(R) \times E(R)$ definiert werden.*

Beweis. Sei $E = E_{a,b}$ eine elliptische Kurve über R und sei $(P_1,P_2) = ((x_1 : y_1 : z_1),(x_2 : y_2 : z_2)) \in E(R) \times E(R)$. Seien $(p_1,p_2) = ((x_1,y_1,z_1),(x_2,y_2,z_2))$ und $(p'_1,p'_2) = ((x'_1,y'_1,z'_1),(x'_2,y'_2,z'_2))$ Repräsentantenpaare von (P_1,P_2). Dann gibt es $u,v \in R^*$, so dass $(x'_1,y'_1,z'_1) = (ux_1,uy_1,uz_1)$ und $(x'_2,y'_2,z'_2) = (vx_2,vy_2,vz_2)$. Aus den Formeln I, II und III entstehen die Matrizen

$$M(p_1,p_2) = \begin{pmatrix} x_3^I & y_3^I & z_3^I \\ x_3^{II} & y_3^{II} & z_3^{II} \\ x_3^{III} & y_3^{III} & z_3^{III} \end{pmatrix} \quad \text{und} \quad M(p'_1,p'_2) = \begin{pmatrix} u^2v^2 \cdot x_3^I & u^2v^2 \cdot y_3^I & u^2v^2 \cdot z_3^I \\ u^5v^5 \cdot x_3^{II} & u^5v^5 \cdot y_3^{II} & u^5v^5 \cdot z_3^{II} \\ u^2v^2 \cdot x_3^{III} & u^2v^2 \cdot y_3^{III} & u^2v^2 \cdot z_3^{III} \end{pmatrix}.$$

Sei $(x_3,y_3,z_3) \in R^3$ bzw. $(x'_3,y'_3,z'_3) \in R^3$ primitiv und als Linearkombination der Zeilen von $M(p_1,p_2)$ bzw. $M(p'_1,p'_2)$ darstellbar. Da sich die Zeilen von $M(p'_1,p'_2)$ nur durch Multiplikation mit Einheiten von den Zeilen von $M(p_1,p_2)$ unterscheiden, ist auch (x'_3,y'_3,z'_3) als Linearkombination der Zeilen von $M(p_1,p_2)$ darstellbar. Nach Lemma 2.5 definieren (x_3,y_3,z_3) und (x'_3,y'_3,z'_3) also denselben Punkt $(x_3 : y_3 : z_3)$ in $\mathbb{P}^2(R)$. □

Schritt 3. *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1)$ und $P_2 = (x_2 : y_2 : z_2)$ Punkte in $E(R)$ mit Repräsentanten $p_1 = (x_1,y_1,z_1)$ und $p_2 = (x_2,y_2,z_2)$. Dann ist die Matrix $M(p_1,p_2)$ primitiv.*

Beweis. Wir nehmen an, dass $M(p_1,p_2)$ nicht primitiv ist. Dann ist das von allen Einträgen $x_3^I, y_3^I, \ldots, z_3^{III}$ von $M(p_1,p_2)$ erzeugte Ideal ungleich R, also in einem maximalen Ideal $\mathfrak{m}$ enthalten. Der surjektive Ringhomomorphismus

$$\pi : R \to R/\mathfrak{m}, \quad x \mapsto \overline{x} = x + \mathfrak{m} = \{x + m \mid m \in \mathfrak{m}\}$$

wird als die *kanonische Projektion* bezeichnet und induziert eine Abbildung

$$\tilde{\pi} : E(R) \to \tilde{E}(R/\mathfrak{m}), \quad (x : y : z) \mapsto (\overline{x} : \overline{y} : \overline{z}).$$

Die elliptische Kurve E ist durch $F(x,y,z) = x^3 + axz^2 + bz^3 - y^2z = 0$ gegeben, wobei $4a^3 + 27b^2 \in R^*$. Die Addition bzw. Multiplikation auf $R/\mathfrak{m}$ ist durch $\overline{r} + \overline{s} := \overline{r+s}$ bzw. $\overline{r} \cdot \overline{s} := \overline{rs}$ definiert. Daraus folgt direkt, dass $\overline{4a^3 + 27b^2} \in (R/\mathfrak{m})^*$ und $\tilde{F}(\overline{x},\overline{y},\overline{z}) = \overline{x}^3 + \overline{a} \cdot \overline{x} \cdot \overline{z}^2 + \overline{b} \cdot \overline{z}^3 - \overline{y}^2 \cdot \overline{z} = \overline{0}$. So verstehen wir $\tilde{E} = \tilde{E}_{\overline{a},\overline{b}}$ als eine elliptische Kurve über $R/\mathfrak{m}$. Sei $P = (x : y : z) \in E(R)$, dann ist $\tilde{\pi}(P) = (\overline{x} : \overline{y} : \overline{z}) \in \tilde{E}(R/\mathfrak{m})$. Denn so wie sich die Eigenschaften von E auf $\tilde{E}$ übertragen, übertragen sich die Eigenschaften von $(x,y,z) \in R^3$, primitiv zu sein und die Kurvengleichung $F(x,y,z) = 0$ von E zu erfüllen, auf $(\overline{x},\overline{y},\overline{z}) \in (R/\mathfrak{m})^3$, d.h. $(\overline{x},\overline{y},\overline{z})$ ist primitiv und erfüllt die Kurvengleichung $\tilde{F}(\overline{x},\overline{y},\overline{z}) = \overline{0}$ von $\tilde{E}$. Seien $(x,y,z) \neq (x',y',z')$ Repräsentanten von $(x : y : z) \in E(R)$ und $u \in R^*$, so dass $(x,y,z) = (ux', uy', uz')$. Dann ist $(\overline{x},\overline{y},\overline{z}) = (\overline{ux'},\overline{uy'},\overline{uz'}) = (\overline{u} \cdot \overline{x'}, \overline{u} \cdot \overline{y'}, \overline{u} \cdot \overline{z'})$ mit $\overline{u} \in (R/\mathfrak{m})^*$, d.h. $(\overline{x'} : \overline{y'} : \overline{z'}) = (\overline{x} : \overline{y} : \overline{z}) = \tilde{\pi}((x : y : z))$. Also ist $\tilde{\pi}$ wohldefiniert.

Da $\mathfrak{m}$ maximal ist, ist $R/\mathfrak{m}$ ein Körper, den wir mit $K_{\mathfrak{m}}$ bezeichnen. Seien $\tilde{P}_1 = \tilde{\pi}(P_1)$ und $\tilde{P}_2 = \tilde{\pi}(P_2)$ die Bilder von P_1, P_2 unter $\tilde{\pi}$ mit Repräsentanten $\tilde{p_1} = (\overline{x_1},\overline{y_1},\overline{z_1})$ und $\tilde{p_2} = (\overline{x_2},\overline{y_2},\overline{z_2})$. Aus den Formeln I, II und III entsteht die zu $\tilde{p_1}, \tilde{p_2}$ gehörende Matrix

$$M(\tilde{p_1},\tilde{p_2}) = \begin{pmatrix} \overline{x_3^I} & \overline{y_3^I} & \overline{z_3^I} \\ \overline{x_3^{II}} & \overline{y_3^{II}} & \overline{z_3^{II}} \\ \overline{x_3^{III}} & \overline{y_3^{III}} & \overline{z_3^{III}} \end{pmatrix}.$$

Da R die Bedingung 1 erfüllt, also $2,3 \in R^*$, sind $\overline{2},\overline{3} \in (R/\mathfrak{m})^*$ und damit ungleich $\overline{0}$. Daher ist die Charakteristik von $K_{\mathfrak{m}}$ ungleich 2 und 3. Nach Lemma 2.4 ist die Matrix $M(\tilde{p_1},\tilde{p_2})$ primitiv, d.h. mindestens ein Eintrag ist ungleich $\overline{0}$. Da aber das von $x_3^I, y_3^I, \ldots, z_3^{III}$ erzeugte Ideal in $\mathfrak{m}$ enthalten ist, folgt, dass $\overline{x_3^I} = \overline{0}$, $\overline{y_3^I} = \overline{0}, \ldots, \overline{z_3^{III}} = \overline{0}$, d.h. $M(\tilde{p_1},\tilde{p_2})$ ist die Nullmatrix. Das ist ein Widerspruch. □

Schritt 4. *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1)$ und $P_2 = (x_2 : y_2 : z_2)$ Punkte in $E(R)$ mit Repräsentanten $p_1 = (x_1,y_1,z_1)$ und $p_2 = (x_2,y_2,z_2)$. Dann verschwinden alle 2×2-Unterdeterminanten von $M(p_1,p_2)$.*

Um dies wieder mit Hilfe des Lemmas 2.4 zeigen zu können, wenden wir folgende Methode an: Sei E eine elliptische Kurve über R. Dann konstruieren wir einen Integritätsring T und einen Ringhomomorphismus $\varphi : T \to R$, der eine Abbildung $\tilde{\varphi} : \tilde{E}(T) \to E(R)$ induziert, so dass wir jeden Punkt

$P \in E(R)$ als das Bild eines Punktes $\tilde{P} \in \tilde{E}(T)$ unter $\tilde{\varphi}$ auffassen können, wobei $\tilde{E}$ eine elliptische Kurve über T ist. Sei K_T der Quotientenkörper von T und sei $\alpha : T \to K_T$ der injektive Ringhomomorphismus, der T in K_T einbettet. Dann können wir $\tilde{E}$ auch als eine elliptische Kurve über K_T auffassen. Wenn nun die Charakteristik von K_T ungleich 2 und 3 ist, kann das Lemma 2.4 zur Anwendung gebracht werden. Die skizzierte Methode ist in diesem und den nächsten Beweisschritten von entscheidender Bedeutung. Wir sprechen von nun an von der *Rückführung auf den Körperfall*. Das folgende Diagramm veranschaulicht das Grundmuster der Methode:

$$\begin{array}{ccc} T & \overset{\alpha}{\hookrightarrow} & K_T \\ {\scriptstyle\varphi}\downarrow & & \\ R & & \end{array}$$

Wir wollen nun einen Integritätsring T sowie einen Ringhomomorphismus $\varphi : T \to R$ mit den gewünschten Eigenschaften konstruieren.

Lemma 2.6. *Sei T' ein Integritätsring. Wir betrachten das Polynom $f := X^3 + AXZ^2 + BZ^3 - Y^2Z \in T'[X,Y,Z]$ mit $A,B \in T'$. Dann ist der Restklassenring $T'(X,Y,Z)/(f)$ nach dem Ideal, das von f erzeugt wird, ein Integritätsring.*

Beweis. Sei $K_{T'}$ der Quotientenkörper von T'. Der Polynomring $T'[X,Y,Z]$ ist ein Integritätsring, da T' ein Integritätsring ist. Also ist $T'[X,Y,Z]/(f)$ genau dann ein Integritätsring, wenn f ein Primelement ist. Seien $g,h \in T'[X,Y,Z]$ mit $gh \in (f)$. Dann ist zu zeigen, dass $g \in (f)$ oder $h \in (f)$. Nach [6] genügt es dafür zu zeigen, dass f im Ring $K_{T'}[X,Y,Z]$ irreduzibel ist, d.h. ist $f = gh$ mit $g,h \in K_{T'}[X,Y,Z]$, so ist g konstant oder h konstant. Wir nehmen an, dass g und h nicht konstant sind. Da f homogen vom Grad 3 in X,Y,Z ist, sind auch g und h homogen in X,Y,Z. O.B.d.A. können wir g und h in folgender Form schreiben:

$$\begin{aligned} g &= X + C_1Y + C_2Z, \\ h &= X^2 + D_1Y^2 + D_2Z^2 + D_3XY + D_4XZ + D_5YZ \end{aligned}$$

mit Koeffizienten $C_i, D_j \in K_{T'}$ für $i = 1,2$, $j = 1,...,5$. Dann gilt

$$\begin{aligned} gh \;=\; & X^3 + C_1D_1Y^3 + C_2D_2Z^3 + (C_1 + D_3)X^2Y + (C_2 + D_4)X^2Z + (C_1D_5 + C_2D_1)Y^2Z \\ & + (C_1D_3 + D_1)XY^2 + (C_2D_4 + D_2)XZ^2 + (C_1D_2 + C_2D_5)YZ^2 \\ & + (C_1D_4 + C_2D_3 + D_5)XYZ \\ =\; & f = X^3 + AXZ^2 + BZ^3 - Y^2Z. \end{aligned}$$

Ein Koeffizientenvergleich führt auf $C_1D_5 + C_2D_1 = -1$ und $C_1D_1 = C_1D_3 + D_1 = C_1 + D_3 = 0$. Aus $C_1D_1 = 0$ folgt, dass

$$(C_1 = 0 \;\wedge\; D_1 \neq 0) \;\vee\; (C_1 \neq 0 \;\wedge\; D_1 = 0) \;\vee\; (C_1 = 0 = D_1).$$

Aus dem ersten Fall folgt, dass $D_1 = C_1D_3 + D_1 = 0$, aber $D_1 \neq 0$, ein Widerspruch. Aus dem zweiten Fall folgt, dass $C_1D_3 = C_1D_3 + D_1 = 0$. Da $C_1 \neq 0$, muss $D_3 = 0$ sein. Dann gilt $C_1 = C_1 + D_3 = 0$, aber $C_1 \neq 0$, ein Widerspruch. Aus dem letzten Fall folgt, dass $0 = C_1D_5 + C_2D_1 = -1$, ein Widerspruch. Die Annahme muss also falsch gewesen sein, d.h. h ist konstant oder g ist konstant. Damit ist f irreduzibel in $K_{T'}[X,Y,Z]$. □

Korollar 2.7. *Wir betrachten das Polynom* $f_j := X_j^3 + AX_jZ_j^2 + BZ_j^3 - Y_j^2Z_j$ *aus* $\mathbb{Z}[A,B,X_i,Y_i,Z_i;\ i = 1,...,r]$ *für* $j = 1,...,r$. *Dann ist*

$$\mathbb{Z}[A,B,X_i,Y_i,Z_i;\ i = 1,...,r]/(f_1,...,f_r)$$

ein Integritätsring.

Beweis. Der Polynomring $\mathbb{Z}[A,B]$ ist ein Integritätsring, da $\mathbb{Z}$ ein Integritätsring ist. Wir betrachten das Polynom $f_1 = X_1^3 + AX_1Z_1^2 + BZ_1^3 - Y_1^2Z_1$ aus $(\mathbb{Z}[A,B])[X_1,Y_1,Z_1] = \mathbb{Z}[A,B,X_1,Y_1,Z_1]$. Nach Lemma 2.6 ist

$$\mathbb{Z}[A,B,X_1,Y_1,Z_1]/(f_1)$$

ein Integritätsring. Wir betrachten das Polynom $f_2 = X_2^3 + AX_2Z_2^2 + BZ_2^3 - Y_2^2Z_2$ aus $(\mathbb{Z}[A,B,X_1,Y_1,Z_1]$ $/(f_1))[X_2,Y_2,Z_2]$. Nach Lemma 2.6 ist

$$(\mathbb{Z}[A,B,X_1,Y_1,Z_1]/(f_1))[X_2,Y_2,Z_2]/(f_2) = \mathbb{Z}[A,B,X_1,X_2,Y_1,Y_2,Z_1,Z_2]/(f_1,f_2)$$

ein Integritätsring. So folgt die Behauptung nach r-facher Anwendung des Lemmas 2.6. □

Lemma 2.8. *Sei* $E = E_{a,b}$ *eine elliptische Kurve über* R *und seien* $P_1,...,P_r$ *Punkte von* $E(R)$. *Für jedes* $i \in \{1,...,r\}$ *sei* $(x_i,y_i,z_i) \in R^3$ *ein primitiver Repräsentant von* $P_i = (x_i : y_i : z_i)$. *(Dieser erfüllt die Kurvengleichung* $y^2z = x^3 + axz^2 + bz^3 - y^2z$ *von E.) Dann gibt es einen Integritätsring* T *und Elemente* $A,B,X_i,Y_i,Z_i \in T$ *für* $i = 1,...,r$, *so dass* $4A^3 + 27B^2 \in T^*$ *und für jedes* $i \in \{1,...,r\}$ *das Tripel* $(X_i,Y_i,Z_i) \in T^3$ *primitiv ist sowie die Gleichung* $Y^2Z = X^3 + AXZ^2 + BZ^3$ *in* T *erfüllt — d.h.* $\tilde{E} = \tilde{E}_{A,B}$ *ist eine durch* $Y^2Z = X^3 + AXZ^2 + BZ^3$ *gegebene elliptische Kurve über* T *und* $(X_i : Y_i : Z_i) \in \tilde{E}(T)$ *— und es existiert ein Ringhomomorphismus*

$$\varphi : T \to R \quad mit \quad A \mapsto a,\ B \mapsto b,\ X_i \mapsto x_i,\ Y_i \mapsto y_i,\ Z_i \mapsto z_i$$

für alle $i = 1,...,r$.

Beweis. Wir betrachten den Ring

$$T_0 := \mathbb{Z}[A,B,X_i,Y_i,Z_i,U_i,V_i,W_i;\ i = 1,...,r]/(f_1,...,f_r),$$

wobei $f_j := X_j^3 + AX_jZ_j^2 + BZ_j^3 - Y_j^2Z_j$ für $j = 1,...,r$. Wir bezeichnen das Ideal $(f_1,...,f_r)$ mit $\mathfrak{I}$. Nach Korollar 2.7 ist T_0 ein Integritätsring. Sein Nullelement ist $0+\mathfrak{I}$ und sein Einselement ist $1+\mathfrak{I}$. Sei K_0 der Quotientenkörper von T_0. Die Idee ist nun, den gewünschten Ring T als Lokalisierung von T_0 zu erhalten. Wir definieren eine Teilmenge

$$S := \left\{ D^d \prod_{i=1}^{r} R_i^{d_i} \mid d, d_1, ..., d_r \geq 0 \right\} \subseteq T_0,$$

wobei

$$D := (4A^3 + 27B^2) + \mathfrak{I} \in T_0 \quad \text{und} \quad R_i := (U_iX_i + V_iY_i + W_iZ_i) + \mathfrak{I} \in T_0$$

für $i = 1,...,r$. Die Menge S ist eine multiplikative Teilmenge, denn für $d = d_i = 0$ ist $D^0 \prod_{i=1}^{r} R_i^0 = 1+\mathfrak{I}$, also $1 \in S$, und wenn $s, s' \in S$ mit

$$s = D^d \prod_{i=1}^{r} R_i^{d_i}, \quad s' = D^{d'} \prod_{i=1}^{r} R_i^{d_i'},$$

dann ist

$$ss' = D^{d+d'} \prod_{i=1}^{r} R_i^{d_i+d_i'},$$

also $ss' \in S$.

$$T := \left\{ \frac{g}{D^d \prod_{i=1}^{r} R_i^{d_i}} \mid g \in T_0,\, d, d_1, ..., d_r \geq 0 \right\} \subseteq K_0$$

ist zusammen mit dem Ringhomomorphismus

$$\tau : T_0 \to T, \quad g \mapsto \frac{g}{1}$$

die Lokalisierung von T_0 nach S. Die Schreibweise $\frac{g}{s}$ bezeichnet die Äquivalenzklasse von $(g,s) \in T_0 \times S$, wobei (g,s) in Relation zu $(g',s') \in T_0 \times S$ steht, wenn $gs' = g's$. Für die Äquivalenzklasse $\frac{g}{1}$ von $(g,1)$ schreiben wir auch einfach nur g. Mit den Verknüpfungen

$$\frac{g}{s} + \frac{g'}{s'} := \frac{gs' + g's}{ss'} \quad \text{und} \quad \frac{g}{s} \cdot \frac{g'}{s'} := \frac{gg'}{ss'}$$

ist T ein kommutativer Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$. Nach Konstruktion ist T ein Unterring von K_0 und damit insbesondere ein Integritätsring. Da $\tau(S) \subseteq T^*$, ist $D\prod_{i=1}^{r} R_i$ eine Einheit von T. Daraus folgt, dass $D \in T^*$ sowie $R_i \in T^*$ für jedes $i \in \{1,...,r\}$, womit jedes Tripel $(X_i+\mathfrak{I}, Y_i+\mathfrak{I}, Z_i+\mathfrak{I}) \in T^3$ primitiv ist. Für jedes $j \in \{1,...,r\}$ ist $f_j + \mathfrak{I} = 0 + \mathfrak{I} = 0$ in T_0, da $f_j \in \mathfrak{I}$, und damit

$$\frac{f_j + \mathfrak{I}}{1} = \tau(f_j + \mathfrak{I}) = \tau(0) = 0,$$

d.h. jedes Tripel $(X_i+\mathfrak{I}, Y_i+\mathfrak{I}, Z_i+\mathfrak{I}) \in T^3$ erfüllt die Gleichung $Y^2Z = X^3 + AXZ^2 + BZ^3$ in T. Für ein Element $h+\mathfrak{I} \in T_0$ bzw. $\frac{h+\mathfrak{I}}{1} \in T$, $h \in \mathbb{Z}[A,B,X_i,Y_i,Z_i,U_i,V_i,W_i;\ i = 1,...,r]$, schreiben wir auch

einfach nur h und wissen an entsprechenden Stellen, dass damit ein Element von T_0 bzw. T gemeint ist. So können wir $4A^3+27B^2$ sowie X_i, Y_i, Z_i als Elemente von T auffassen.

Wir wollen nun die universelle Eigenschaft der Lokalisierung nutzen, um den gewünschten Ringhomomorphismus $\varphi : T \to R$ zu erhalten. Dafür müssen wir einen Ringhomomorphismus $\varphi' : T_0 \to R$ mit $\varphi'(S) \subseteq R^*$ konstruieren. Nach Voraussetzung ist für jedes $i \in \{1,...,r\}$ das Tripel $(x_i, y_i, z_i) \in R^3$ primitiv, d.h. es existieren Elemente $u_i, v_i, w_i \in R$ mit $u_i x_i + v_i y_i + w_i z_i = 1$. Wir definieren einen Ringhomomorphismus

$$\psi : \mathbb{Z}[A, B, X_i, Y_i, Z_i, U_i, V_i, W_i;\ i = 1,...,r] \to R$$

durch die Vorschriften

$$A \mapsto a,\ B \mapsto b,\ X_i \mapsto x_i,\ Y_i \mapsto y_i,\ Z_i \mapsto z_i,\ U_i \mapsto u_i,\ V_i \mapsto v_i,\ W_i \mapsto w_i \tag{1}$$

für $i = 1,...,r$. Das Ideal $\mathfrak{I}$ ist im Kern $\operatorname{Ker}\psi$ von ψ enthalten. Denn für jedes $j \in \{1,...,r\}$ ist $\psi(f_j) = x_j^3 + a x_j z_j^2 + b z_j^3 - y_j z_j^2 = 0$, da (x_j, y_j, z_j) als Repräsentant von $P_j = (x_j : y_j : z_j) \in E(R)$ die Kurvengleichung von E erfüllt. Für jedes $j \in \{1,...,r\}$ und $\lambda_j \in \mathbb{Z}[A, B, X_i, Y_i, Z_i, U_i, V_i, W_i;\ i = 1,...,r]$ ist deshalb $\psi(\sum_{j=1}^r \lambda_j f_j) = \sum_{j=1}^r \psi(\lambda_j)\psi(f_j) = \sum_{j=1}^r \psi(\lambda_j) \cdot 0 = 0$. Also $\mathfrak{I} \subseteq \operatorname{Ker}\psi$. Nach der universellen Eigenschaft des Restklassenrings gibt es nun einen eindeutig bestimmten Ringhomomorphismus

$$\varphi' : T_0 \to R \quad \text{mit} \quad \psi = \varphi' \circ \pi,$$

wobei $\pi : \mathbb{Z}[A, B, X_i, Y_i, Z_i, U_i, V_i, W_i;\ i = 1,...,r] \to T_0$ die kanonische Projektion ist. Die Abbildungsvorschrift von φ' ist durch (1) festgelegt. Es gilt $\varphi'(S) \subseteq R^*$, denn für jedes $d, d_1, ..., d_r \geq 0$ gilt

$$\begin{aligned}&\varphi'(D^d \textstyle\prod_{i=1}^r R_i^{d_i}) = \varphi'(D)^d \prod_{i=1}^r \varphi'(R_i)^{d_i} = (4a^3+27b^2)^d \prod_{i=1}^r (u_i x_i + v_i y_i + w_i z_i)^{d_i} \\ &= (4a^3+27b^2)^d \textstyle\prod_{i=1}^r 1^{d_i} = (4a^3+27b^2)^d\end{aligned}$$

und $(4a^3+27b^2)^d \in R^*$, da $4a^3+27b^2 \in R^*$ nach Voraussetzung. Nach der universellen Eigenschaft der Lokalisierung existiert nun ein eindeutig bestimmter Ringhomomorphismus

$$\varphi : T \to R \quad \text{mit} \quad \varphi \circ \tau = \varphi'.$$

Die Abbildungsvorschrift von φ ist wieder durch (1) gegeben. □

Bemerkung 2.9. *Mit den obigen Notationen und dem Lemma 2.8 halten wir Folgendes fest: Durch die Gleichung $Y^2Z = X^3 + AXZ^2 + BZ^3$ ist eine elliptische Kurve $\tilde{E} = \tilde{E}_{A,B}$ über T gegeben. Sei $P_i = (x_i : y_i : z_i) \in E(R)$ für ein $i \in \{1,...,r\}$. Dann existieren $X_i, Y_i, Z_i \in T$, so dass $\tilde{P}_i := (X_i : Y_i : Z_i) \in \tilde{E}(T)$ und $(\varphi(X_i) : \varphi(Y_i) : \varphi(Z_i)) = (x_i : y_i : z_i) \in E(R)$. D.h. $\varphi : T \to R$ induziert eine Abbildung*

$$\tilde{\varphi} : \tilde{E}(T) \to E(R), \quad (X : Y : Z) \mapsto (\varphi(X) : \varphi(Y) : \varphi(Z)),$$

so dass wir jeden Punkt in $E(R)$ als das Bild eines Punktes in $\tilde{E}(T)$ unter $\tilde{\varphi}$ auffassen können. Sei $(X : Y : Z) \in \tilde{E}(T)$, dann ist $(X,Y,Z) \in T^3$ primitiv und erfüllt die Kurvengleichung von $\tilde{E}$. Also existieren $S_1,S_2,S_3 \in T$, so dass $S_1X + S_2Y + S_3Z = 1$, und es gilt $X^3 + AXZ^2 + BZ^3 - Y^2Z = 0$. Da φ ein Ringhomomorphismus ist, folgt, dass $\varphi(S_1)\varphi(X)+\varphi(S_2)\varphi(Y)+\varphi(S_3)\varphi(Z) = \varphi(S_1X+S_2Y+S_3Z) = \varphi(1) = 1$, wobei $\varphi(S_1),\varphi(S_2),\varphi(S_3) \in R$, und $\varphi(X)^3+a\varphi(X)\varphi(Z)^2+b\varphi(Z)^3-\varphi(Y)^2\varphi(Z) = \varphi(X^3)$ $+\varphi(A)\varphi(X)\varphi(Z^2)+\varphi(B)\varphi(Z^3)-\varphi(Y^2)\varphi(Z) = \varphi(X^3+AXZ^2+BZ^3-Y^2Z) = \varphi(0) = 0$. Sei $U \in T^*$, dann existiert ein $V \in T$ mit $UV = 1$, weshalb $\varphi(U)\varphi(V) = \varphi(UV) = \varphi(1) = 1$ mit $\varphi(V) \in R$, d.h. $\varphi(U) \in R^*$. Daraus folgt, dass zwei verschiedene Repräsentanten eines Punktes $\tilde{P} \in \tilde{E}(T)$ stets denselben Punkt $\tilde{\varphi}(\tilde{P}) \in E(R)$ hervorbringen. Also ist $\tilde{\varphi}$ eine wohldefinierte Abbildung. Sei

$$\alpha : T \to K_T, \quad h \mapsto \frac{h}{1}$$

der injektive Ringhomomorphismus, der T in seinen Quotientenkörper K_T einbettet. Für $\frac{h}{1}$ schreiben wir einfach nur h. Da $2+\mathfrak{I} \neq 0+\mathfrak{I}$ und $3+\mathfrak{I} \neq 0+\mathfrak{I}$, ist die Charakteristik von K_T ungleich 2 und 3, d.h. wir können das Lemma 2.4 anwenden. Im Folgenden übernehmen wir die obigen Notationen.

Schritt 4. Wir wollen Schritt 4 nun durch Rückführung auf den Körperfall zeigen. Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1)$ und $P_2 = (x_2 : y_2 : z_2)$ Punkte in $E(R)$ mit Repräsentanten $p_1 = (x_1,y_1,z_1)$ und $p_2 = (x_2,y_2,z_2)$. Nach Lemma 2.8 existieren Punkte $\tilde{P_1} = (X_1 : Y_1 : Z_1)$ und $\tilde{P_2} = (X_2 : Y_2 : Z_2) \in \tilde{E}(T)$ mit Repräsentanten $\tilde{p_1} = (X_1,Y_1,Z_1)$ und $\tilde{p_2} = (X_2,Y_2,Z_2)$, so dass $(\varphi(X_1),\varphi(Y_1),\varphi(Z_1)) = (x_1,y_1,z_1)$ und $(\varphi(X_2),\varphi(Y_2),\varphi(Z_2)) = (x_2,y_2,z_2)$, d.h. $\tilde{\varphi}(\tilde{P_1}) = P_1$ und $\tilde{\varphi}(\tilde{P_2}) = P_2$. Sei

$$M_T(\tilde{p_1},\tilde{p_2}) := \begin{pmatrix} X_3^I & Y_3^I & Z_3^I \\ X_3^{II} & Y_3^{II} & Z_3^{II} \\ X_3^{III} & Y_3^{III} & Z_3^{III} \end{pmatrix}$$

die zu $\tilde{p_1},\tilde{p_2}$ gehörende Matrix über T. Wir stellen die 2×2-Unterdeterminanten von $M_T(\tilde{p_1},\tilde{p_2})$ durch $A_{ij}A_{kl} - A_{il}A_{kj}$, $1 \le i < k \le 3$, $1 \le j < l \le 3$, dar. Betten wir T durch α in seinen Quotientenkörper K_T ein, so können wir die Matrix $M_T(\tilde{p_1},\tilde{p_2})$ über T als eine Matrix $M_{K_T}(\tilde{p_1},\tilde{p_2})$ über einem Körper auffassen. Nach Lemma 2.4 verschwinden nun alle 2×2-Unterdeterminanten von $M_{K_T}(\tilde{p_1},\tilde{p_2})$, d.h. $A_{ij}A_{kl} - A_{il}A_{kj} = 0$ in K_T für alle i,j,k,l. Da α ein injektiver Ringhomomorphismus ist, folgt, dass $A_{ij}A_{kl} - A_{il}A_{kj} = 0$ in T. Somit ist $\varphi(A_{ij}A_{kl} - A_{il}A_{kj}) = \varphi(0) = 0$. Nach Konstruktion von φ gilt $\varphi(X_3^I) = x_3^I$, der erste Eintrag der zu p_1,p_2 gehörenden Matrix $M(p_1,p_2)$. Entsprechendes trifft für alle Matrixeinträge zu. Mit $\varphi(A_{ij}A_{kl} - A_{il}A_{kj}) = \varphi(A_{ij})\varphi(A_{kl}) - \varphi(A_{il})\varphi(A_{kj}) = a_{ij}a_{kl} - a_{il}a_{kj}$ beschreiben wir also alle 2×2-Unterdeterminanten von

$$M(p_1,p_2) = \begin{pmatrix} x_3^I & y_3^I & z_3^I \\ x_3^{II} & y_3^{II} & z_3^{II} \\ x_3^{III} & y_3^{III} & z_3^{III} \end{pmatrix}.$$

Aus $a_{ij}a_{kl} - a_{il}a_{kj} = 0$ für alle i,j,k,l folgt schließlich, dass alle 2×2-Unterdeterminanten von $M(p_1,p_2)$ verschwinden. □

Schritt 5. *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1)$ und $P_2 = (x_2 : y_2 : z_2)$ Punkte in $E(R)$ mit Repräsentanten $p_1 = (x_1,y_1,z_1)$ und $p_2 = (x_2,y_2,z_2)$. Dann gibt es eine Linearkombination der Zeilen von $M(p_1,p_2)$, die als Tripel $(x_3,y_3,z_3) \in R^3$ primitiv ist, und (x_3,y_3,z_3) erfüllt die Kurvengleichung $y^2z = x^3 + axz^2 + bz^3$ von E. (D.h. $(x_3 : y_3 : z_3) \in E(R)$.)*

Da $M(p_2,p_2)$ primitiv ist und all ihre 2×2-Unterdeterminanten verschwinden, existiert nach Bedingung 2, die R erfüllt, eine primitive Linearkombination $(x_3,y_3,z_3) \in R^3$ der Zeilen von $M(p_1,p_2)$. Die zu zeigende Behauptung ist also, dass (x_3,y_3,z_3) die Kurvengleichung von E erfüllt.

Lemma 2.10. *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1)$ und $P_2 = (x_2 : y_2 : z_2)$ Punkte in $E(R)$ mit Repräsentanten $p_1 = (x_1,y_1,z_1)$ und $p_2 = (x_2,y_2,z_2)$. Dann erfüllt jede Linearkombination der Zeilen von $M(p_1,p_2)$ die Kurvengleichung von E.*

Beweis. Wir wollen die Behauptung wieder durch Rückführung auf den Körperfall zeigen. Sei

$$(x_3,y_3,z_3) = a_1(x_3^I,y_3^I,z_3^I) + a_2(x_3^{II},y_3^{II},z_3^{II}) + a_3(x_3^{III},y_3^{III},z_3^{III}),$$

$a_1,a_2,a_3 \in R$, eine Linearkombination der Zeilen von $M(p_1,p_2)$. Wir passen T_0 unserer Situation an. Die Aussagen ändern sich dadurch formal, inhaltlich jedoch nicht. Deshalb und für eine bessere Übersicht behalten wir die gewohnten Notationen bei. Wir betrachten im Folgenden

$$T_0 = \mathbb{Z}[A,A_1,A_2,A_3,B,X_i,Y_i,Z_i,U_i,V_i,W_i;\ i=1,2]/(f_1,f_2),$$

$$T = \left\{ \frac{g}{D^d R_1^{d_1} R_2^{d_2}} \mid g \in T_0,\, d,d_1,d_2 \geq 0 \right\} \subseteq K_0,$$

$$\varphi : T \to R \quad mit \quad A \mapsto a,\ A_1 \mapsto a_1,\ A_2 \mapsto a_2,\ A_3 \mapsto a_3,\ B \mapsto b,\ X_i \mapsto x_i,\ Y_i \mapsto y_i,\ Z_i \mapsto z_i$$

für $i = 1,2$. Nach Lemma 2.8 existieren Punkte $\tilde{P}_1 = (X_1 : Y_1 : Z_1)$ und $\tilde{P}_2 = (X_2 : Y_2 : Z_2)$ in $\tilde{E}(T)$ mit Repräsentanten $\tilde{p_1} = (X_1,Y_1,Z_1)$ und $\tilde{p_2} = (X_2,Y_2,Z_2)$, so dass $(\varphi(X_1),\varphi(Y_1),\varphi(Z_1)) = (x_1,y_1,z_1)$ und $(\varphi(X_2),\varphi(Y_2),\varphi(Z_2)) = (x_2,y_2,z_2)$, d.h. $\tilde{\varphi}(\tilde{P}_1) = P_1$ und $\tilde{\varphi}(\tilde{P}_2) = P_2$.

$$(X_3,Y_3,Z_3) = A_1(X_3^I,Y_3^I,Z_3^I) + A_2(X_3^{II},Y_3^{II},Z_3^{II}) + A_3(X_3^{III},Y_3^{III},Z_3^{III})$$

ist die Linearkombination der Zeilen von $M_T(\tilde{p_1},\tilde{p_2})$, die unter Anwendung von φ gerade (x_3,y_3,z_3) ergibt, d.h. $\varphi((X_3,Y_3,Z_3)) = (x_3,y_3,z_3)$. Wir betten T durch α in seinen Quotientenkörper K_T ein. Nach Lemma 2.4 sind die Zeilen von $M_{K_T}(\tilde{p_1},\tilde{p_2})$ proportional zueinander. Sei o.B.d.A. die erste Zeile von $M_{K_T}(\tilde{p_1},\tilde{p_2})$ primitiv. Dann gibt es ein $r \in K_T$, so dass $(X_3,Y_3,Z_3) = r(X_3^I,Y_3^I,Z_3^I)$ in K_T^3. Da $(X_3^I,Y_3^I,Z_3^I) \in K_T^3$ die Kurvengleichung $X^3+AXZ^2+BZ^3-Y^2Z=0$ in K_T erfüllt und die Gleichung homogen in X,Y,Z ist, erfüllt auch $r(X_3^I,Y_3^I,Z_3^I) = (X_3,Y_3,Z_3)$ die Kurvengleichung in K_T, d.h. $\alpha(X_3^3+AX_3Z_3^2+BZ_3^3-Y_3^2Z_3)=0$. Da α injektiv ist, folgt, dass $X_3^3+AX_3Z_3^2+BZ_3^3-Y_3^2Z_3=0$ in T. Damit gilt schließlich $x_3^3+ax_3z_3^2+bz_3^3-y_3^2z_3 = \varphi(X_3^3+AX_3Z_3^2+BZ_3^3-Y_3^2Z_3) = \varphi(0) = 0$. Also erfüllt (x_3,y_3,z_3) die Kurvengleichung von E. □

Schritt 5. Ist $(x_3,y_3,z_3) \in R^3$ nun eine primitive Linearkombination der Zeilen von $M(p_1,p_2)$, so erfüllt (x_3,y_3,z_3) nach Lemma 2.10 die Kurvengleichung von E, womit $(x_3:y_3:z_3) \in E(R)$. □

Somit ist $E(R)$ abgeschlossen unter der wohldefinierten Verknüpfung $+ : E(R)\times E(R) \to E(R)$.

Schritt 6 (Assoziativität)**.** *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1:y_1:z_1), P_2 = (x_2:y_2:z_2), P_3 = (x_3:y_3:z_3) \in E(R)$. Dann gilt*

$$(P_1+P_2)+P_3 = P_1+(P_2+P_3).$$

Beweis. Wir bezeichnen die Matrix, aus der die Summe $P+Q$ zweier Punkte $P,Q \in E(R)$ berechnet wird, mit $M_R(P,Q)$ — und unterschlagen dabei die Wahl der Repräsentanten von P und Q. Es genügt zu zeigen, dass alle 2×2-Unterdeterminanten der 6×3-Matrix

$$M_{Ass} := \begin{pmatrix} M_R(P_1+P_2,P_3) \\ M_R(P_1,P_2+P_3) \end{pmatrix}$$

verschwinden. Denn sei $(x_4:y_4:z_4) = (P_1+P_2)+P_3$ und sei $(x_4':y_4':z_4') = P_1+(P_2+P_3)$, dann ist $(x_4,y_4,z_4) \in R^3$ bzw. $(x_4',y_4',z_4') \in R^3$ primitiv und als Linearkombination der ersten bzw. letzten drei Zeilen von M_{Ass} darstellbar. Wenn nun alle 2×2-Unterdeterminanten von M_{Ass} verschwinden, so folgt aus Lemma 2.5, dass $(x_4:y_4:z_4) = (x_4':y_4':z_4')$. Dass alle 2×2-Unterdeterminanten von M_{Ass} verschwinden, wollen wir nun durch Rückführung auf den Körperfall zeigen. Dafür betrachten wir im Folgenden

$$T_0 = \mathbb{Z}[A,B,X_i,Y_i,Z_i,U_i,V_i,W_i;\ i=1,2,3]/(f_1,f_2,f_3),$$

$$T = \left\{ \frac{g}{D^d R_1^{d_1} R_2^{d_2} R_3^{d_3}} \mid g \in T_0,\ d,d_1,d_2,d_3 \geq 0 \right\} \subseteq K_0,$$

$$\varphi : T \to R \quad mit \quad A \mapsto a, B \mapsto b,\ X_i \mapsto x_i,\ Y_i \mapsto y_i,\ Z_i \mapsto z_i$$

für $i = 1,2,3$. Nach Lemma 2.8 existieren Punkte $\tilde{P}_i = (X_i : Y_i : Z_i) \in \tilde{E}(T)$ mit $\tilde{\varphi}(\tilde{P}_i) = (\varphi(X_i) : \varphi(Y_i) : \varphi(Z_i)) = (x_i : y_i : z_i) = P_i$ für $i = 1,2,3$. Sei

$$M_{Ass}(T) := \begin{pmatrix} M_T(\tilde{P}_1 + \tilde{P}_2, \tilde{P}_3) \\ M_T(\tilde{P}_1, \tilde{P}_2 + \tilde{P}_3) \end{pmatrix}.$$

Betten wir T durch α in seinen Quotientenkörper K_T ein, so können wir die Matrizen $M_T(\tilde{P}_1 + \tilde{P}_2, \tilde{P}_3)$ und $M_T(\tilde{P}_1, \tilde{P}_2 + \tilde{P}_3)$ über T als Matrizen $M_{K_T}(\tilde{P}_1 + \tilde{P}_2, \tilde{P}_3)$ und $M_{K_T}(\tilde{P}_1, \tilde{P}_2 + \tilde{P}_3)$ über einem Körper auffassen und folglich $M_{Ass}(T)$ als Matrix $M_{Ass}(K_T)$ über K_T ansehen. Nach Lemma 2.4 verschwinden nun alle 2×2-Unterdeterminanten von $M_{Ass}(K_T)$, d.h. $A_{ij}A_{kl} - A_{il}A_{kj} = 0$ in K_T für alle $1 \leq i < k \leq 6$, $1 \leq j < l \leq 3$. Da α injektiv ist, folgt, dass jede Determinante $A_{ij}A_{kl} - A_{il}A_{kj} = 0$ in T ist. Seien $a_{ij}a_{kl} - a_{il}a_{kj}$ die 2×2-Unterdeterminanten von M_{Ass}. Für alle i, j, k, l gilt dann

$$a_{ij}a_{kl} - a_{il}a_{kj} = \varphi(A_{ij})\varphi(A_{kl}) - \varphi(A_{il})\varphi(A_{kj}) = \varphi(A_{ij}A_{kl} - A_{il}A_{kj}) = \varphi(0) = 0,$$

d.h. es verschwinden alle 2×2-Unterdeterminanten von M_{Ass}. □

Schritt 7 (Kommutativität)**.** *Sei $E = E_{a,b}$ eine elliptische Kurve über R und seien $P_1 = (x_1 : y_1 : z_1), P_2 = (x_2 : y_2 : z_2) \in E(R)$. Dann gilt*

$$P_1 + P_2 = P_2 + P_1.$$

Beweis. Ganz analog zu obigem Beweis zeigt man, dass alle 2×2-Unterdeterminanten von

$$M_{Komm} := \begin{pmatrix} M_R(P_1, P_2) \\ M_R(P_2, P_1) \end{pmatrix}$$

verschwinden. Daraus folgt die Kommutativität der Punktaddition. □

Schritt 8 (Neutrales Element)**.** *Sei $E = E_{a,b}$ eine elliptische Kurve über R. Dann gilt für jeden Punkt $P \in E(R)$*

$$P + \infty = \infty + P = \infty. \tag{2}$$

Beweis. Seien $p = (x, y, z)$ und $p_\infty = (0, 1, 0)$ Repräsentanten von P und ∞. Aus den Formeln I, II und III entsteht die Matrix

$$M(p, p_\infty) = \begin{pmatrix} zx & zy & z^2 \\ 0 & 0 & 0 \\ yx & y^2 & yz \end{pmatrix}.$$

Sei $r(x, y, z)$ eine Linearkombination der Zeilen von $M(p, p_\infty)$, $r \in R$, die als Tripel primitiv ist. Dann gibt es $s_1, s_2, s_3 \in R$, so dass $r(s_1x + s_2y + s_3z) = 1$. Also ist r eine Einheit von R, d.h. in $\mathbb{P}^2(R)$ gilt $(rx : ry : rz) = (x : y : z) = P$. Aus der Kommutativität der Addition folgt, dass $P + \infty = \infty + P$. □

Schritt 9 (Inverse Elemente)**.** *Sei $E = E_{a,b}$ eine elliptische Kurve über R. Dann gilt für jeden Punkt $P = (x : y : z) \in E(R)$ mit $-P = (x : -y : z)$*

$$P - P = -P + P = \infty,$$

wobei $P - P$ für $P + (-P)$ steht.

Beweis. Seien $p = (x, y, z)$ und $p' = (x, -y, z)$ Repräsentanten von P und $-P$. Aus den Formeln I, II und III entsteht die Matrix

$$M(p, p') = \begin{pmatrix} 0 & y_3^I & 0 \\ 0 & y_3^{II} & 0 \\ 0 & y_3^{III} & 0 \end{pmatrix}.$$

Sei $r(0,1,0)$ eine Linearkombination der Zeilen von $M(p, p')$, $r \in R$, die als Tripel primitiv ist. Dann gibt es ein $s \in R$ mit $sr = 1$, d.h. $r \in R^*$. In $\mathbb{P}^2(R)$ gilt daher $(0 : r : 0) = (0 : 1 : 0) = \infty$. Aus der Kommutativität der Addition folgt, dass $P - P = -P + P$. □

Wir haben schließlich gezeigt, dass $E(R)$ zusammen mit der Verknüpfung $+ : E(R) \times E(R) \to E(R)$ eine abelsche Gruppe bildet, deren neutrales Element $\infty = (0 : 1 : 0)$ ist. Die inversen Elemente sind durch $-(x : y : z) = (x : -y : z)$ gegeben. Das Theorem ist somit bewiesen.

Addieren wir einen Punkt $P \in E(R)$ k-mal zu sich selbst, kürzen wir $P + P + ... + P = \sum_{i=1}^{k} P$ durch die Schreibweise $k \cdot P$ bzw. kP ab. Wir kommen nun zu dem Primzahltest nach Goldwasser und Kilian, der auf der entwickelten Theorie aufbaut. Um eine Zahl $n \in \mathbb{N}$ auf Primalität zu testen, werden elliptische Kurven über dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ betrachtet.

3 Goldwasser-Kilian-Primzahltest

3.1 Der grundlegende Satz und sein Beweis

Satz 3.1 (Goldwasser-Kilian-Primzahltest; [8] Theorem 7.3)**.** *Sei* $3 < n \in \mathbb{N}$ *eine nicht durch* 2 *und* 3 *teilbare Zahl und sei* $E = E_{a,b}$ *eine elliptische Kurve über* $\mathbb{Z}/n\mathbb{Z}$*. Wenn verschiedene Primzahlen* $l_1, ..., l_r$ *und endliche Punkte* $P_1, ..., P_r \in E(\mathbb{Z}/n\mathbb{Z})$ *existieren, so dass*

(i) $l_i P_i = \infty$ *für alle* $i = 1, ..., r$*,*
(ii) $\prod_{i=1}^{r} l_i > (\sqrt[4]{n}+1)^2$*,*

dann ist n eine Primzahl.

Ein Punkt $P = (\overline{x} : \overline{y} : \overline{z}) \in E(\mathbb{Z}/n\mathbb{Z})$ ist ein endlicher Punkt, wenn $z \not\equiv 0 \pmod{m}$ für alle Teiler m von n.

Wir bereiten den Beweis des Satzes 3.1 vor. Zuerst sollten wir zeigen, dass der Ring $\mathbb{Z}/n\mathbb{Z}$ auch die Bedingungen 1 und 2 erfüllt. Da $\mathrm{ggT}(2,n) = 1 = \mathrm{ggT}(3,n)$, ist $\overline{6} = 6 + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$, womit die Bedingung 1 erfüllt ist. Es bleibt zu zeigen, dass $\mathbb{Z}/n\mathbb{Z}$ die Bedingung 2 erfüllt.

Lemma 3.2. *Seien* R_1, R_2 *Ringe (jeweils kommutativ mit Eins). Dann erfüllt das Produkt* $R_1 \times R_2$ *genau dann die Bedingung 2, wenn* R_1 *und* R_2 *die Bedingung 2 erfüllen.*

Beweis. $R_1 \times R_2$ erfülle die Bedingung 2. Sei $M_{R_1} = (a_{ij})_{1 \le i \le m,\ 1 \le j \le n}$ eine primitive $m \times n$-Matrix über R_1 und sei $M_{R_2} = (b_{ij})_{1 \le i \le m,\ 1 \le j \le n}$ eine primitive $m \times n$-Matrix über R_2, deren 2×2-Unterdeterminanten alle verschwinden, d.h. $(a_{ij}a_{kl} - a_{il}a_{kj}, b_{ij}b_{kl} - b_{il}b_{kj}) = (0,0)$ für alle i, j, k, l mit $1 \le i < k \le m$ und $1 \le j < l \le n$. Wir können beide Matrizen als $m \times n$-Matrizen annehmen, denn wenn die Anzahl der Einträge von M_{R_1} und M_{R_2} verschieden ist, so können wir die Matrizen durch Hinzufügen von Nullen zu Matrizen mit gleich vielen Zeilen und Spalten erweitern. Die folgenden Argumentationsschritte werden sich dadurch inhaltlich nicht ändern, jede Aussage über die erweiterten Matrizen ist hauptsächlich eine Aussage über die nicht erweiterten Matrizen. Es gilt

$$(a_{ij}a_{kl} - a_{il}a_{kj}, b_{ij}b_{kl} - b_{il}b_{kj}) = (0,0) \quad \Leftrightarrow \quad (a_{ij}, b_{ij}) \cdot (a_{kl}, b_{kl}) - (a_{il}, b_{il}) \cdot (a_{kj}, b_{kj}) = (0,0)$$

für alle i, j, k, l. Da M_{R_1} und M_{R_2} primitiv sind, gibt es $\lambda_{ij} \in R_1$, $\mu_{ij} \in R_2$, so dass

$$\left(\sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{ij}a_{ij}, \sum_{i=1}^{m}\sum_{j=1}^{n} \mu_{ij}b_{ij}\right) = (1,1).$$

Wir formen die linke Seite um und erhalten

$$\sum_{i=1}^{m}\sum_{j=1}^{n} (\lambda_{ij}, \mu_{ij}) \cdot (a_{ij}, b_{ij}) = (1,1).$$

Somit ist $M_{R_1\times R_2} := ((a_{ij},b_{ij}))_{1\leq i\leq m,\ 1\leq j\leq n}$ eine primitive $m\times n$-Matrix über $R_1\times R_2$, deren 2×2-Unterdeterminanten alle verschwinden. Da $R_1\times R_2$ die Bedingung 2 erfüllt, existiert eine Linearkombination

$$\sum_{i=1}^{m}(r_i,s_i)\cdot((a_{i1},b_{i1}),...,(a_{in},b_{in})) = \sum_{i=1}^{m}((r_ia_{i1},s_ib_{i1}),...,(r_ia_{in},s_ib_{in}))$$

der Zeilen von $M_{R_1\times R_2}$, die als n-Tupel $((c_1,d_1),...,(c_n,d_n))\in(R_1\times R_2)^n$ primitiv ist, $(r_i,s_i)\in R_1\times R_2$ für alle $i=1,...,m$. D.h. es gibt $(\nu_j,\xi_j)\in R_1\times R_2$, so dass

$$\sum_{j=1}^{n}(\nu_j,\xi_j)\cdot(c_j,b_j) = (1,1),$$

also

$$(\sum_{j=1}^{n}\nu_jc_j,\sum_{j=1}^{n}\xi_jd_j) = (1,1).$$

Mit $\sum_{i=1}^{m}r_i(a_{i1},...,a_{in})$ bzw. $\sum_{i=1}^{m}s_i(b_{i1},...,b_{in})$ ist eine Linearkombination der Zeilen von M_{R_1} bzw. M_{R_2} beschrieben, die als n-Tupel $(c_1,...,c_n)\in R_1^n$ bzw. $(d_1,...,d_n)\in R_2^n$ primitiv ist.

Erfüllen umgekehrt R_1 und R_2 die Bedingung 2, so folgt mit denselben Rechnungen ganz analog, dass $R_1\times R_2$ die Bedingung 2 erfüllt. □

Per Induktion folgt direkt

Korollar 3.3. *Seien $R_1,...,R_m$ Ringe (jeweils kommutativ mit Eins). Dann erfüllt $R_1\times...\times R_m$ genau dann die Bedingung 2, wenn $R_1,...,R_m$ die Bedingung 2 erfüllen.*

Lemma 3.4. *Sei $1\leq n\in\mathbb{N}$. Dann erfüllt der Ring $\mathbb{Z}/n\mathbb{Z}$ die Bedingung 2.*

Beweis. Sei $n = p_1^{k_1}\cdot...\cdot p_r^{k_r}$ die Primfaktorzerlegung von n. Aus dem chinesischen Restsatz folgt

$$\mathbb{Z}/n\mathbb{Z}\cong(\mathbb{Z}/p_1^{k_1}\mathbb{Z})\times...\times(\mathbb{Z}/p_r^{k_r}\mathbb{Z}).$$

Nach Korollar 3.3 genügt es zu zeigen, dass $\mathbb{Z}/p_t^{k_t}\mathbb{Z}$ die Bedingung 2 für alle $t=1,...,r$ erfüllt. Sei für ein $t\in\{1,...,r\}$ $M_t = (\overline{a_{ij}})_{1\leq i\leq m,\ 1\leq j\leq n'}$ eine primitive $m\times n'$-Matrix über $\mathbb{Z}/p_t^{k_t}\mathbb{Z}$. Dann existiert ein Eintrag $\overline{0}\neq\overline{a_{ij}}\in\mathbb{Z}/p_t^{k_t}\mathbb{Z}$ mit $p_t\nmid a_{ij}$, denn sonst gälte $p_t\mid a_{ij}$ für alle $i=1,...,m$ und $j=1,...,n'$ und folglich $\mathrm{ggT}(a_{11},a_{12},...,a_{mn'},n)\neq 1$, womit M_t dann nicht mehr primitiv wäre. Also ist a_{ij} kein Vielfaches von p_t und da p_t prim ist, ist $\mathrm{ggT}(a_{ij},p)=1$, d.h. $\overline{a_{ij}}\in(\mathbb{Z}/p_t^{k_t}\mathbb{Z})^*$. Also ist die i-te Zeile von M_t primitiv. □

Somit erfüllt der Ring $\mathbb{Z}/n\mathbb{Z}$ die Bedingungen 1 und 2, sofern $3<n\in\mathbb{N}$ eine nicht durch 2 und 3 teilbare Zahl ist. Für den Beweis des Satzes 3.1 benötigen wir noch zwei Hilfssätze.

Lemma 3.5. *Sei p ein Primteiler von $1 < n \in \mathbb{N}$ und sei $E = E_{\overline{a},\overline{b}}$ eine durch $y^2z \equiv x^3 + axz^2 + bz^3 \pmod{n}$ gegebene elliptische Kurve über $\mathbb{Z}/n\mathbb{Z}$. Durch Reduktion modulo p kann E auch als eine elliptische Kurve E_p über $\mathbb{Z}/p\mathbb{Z}$ aufgefasst werden. Die Abbildung*

$$\rho : E(\mathbb{Z}/n\mathbb{Z}) \to E_p(\mathbb{Z}/p\mathbb{Z}), \quad \big((x+n\mathbb{Z}) : (y+n\mathbb{Z}) : (z+n\mathbb{Z})\big) \mapsto \big((x+p\mathbb{Z}) : (y+p\mathbb{Z}) : (z+p\mathbb{Z})\big)$$

ist ein Gruppenhomomorphismus.

Beweis. Da $p \mid n$, folgt aus $y^2z \equiv x^3 + axz^2 + bz^3 \pmod{n}$ und $(4a^3 + 27b^2) + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$ sofort, dass $y^2z \equiv x^3 + axz^2 + bz^3 \pmod{p}$ und $(4a^3 + 27b^2) + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$. Daher können wir E auch als eine elliptische Kurve E_p über $\mathbb{Z}/p\mathbb{Z}$ auffassen. Sei $P = (\overline{x} : \overline{y} : \overline{z}) \in E(\mathbb{Z}/n\mathbb{Z})$. Dann ist $(\overline{x},\overline{y},\overline{z}) \in (\mathbb{Z}/n\mathbb{Z})^3$ primitiv, d.h. es existieren $\overline{r_1},\overline{r_2},\overline{r_3} \in \mathbb{Z}/n\mathbb{Z}$, so dass $r_1x + r_2y + r_3z \equiv 1 \pmod{n}$. Weiter erfüllt $(\overline{x},\overline{y},\overline{z})$ die Kurvengleichung von E, also $y^2z \equiv x^3 + axz^2 + bz^3 \pmod{n}$. Da $p \mid n$, folgt, dass $r_1x + r_2y + r_3z \equiv 1 \pmod{p}$ und $y^2z \equiv x^3 + axz^2 + bz^3 \pmod{p}$. D.h. $(x + p\mathbb{Z}, y + p\mathbb{Z}, z + p\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z})^3$ ist primitiv und erfüllt die Kurvengleichung in $\mathbb{Z}/p\mathbb{Z}$. Also $\rho(P) \in E_p(\mathbb{Z}/p\mathbb{Z})$. Seien $(\overline{x},\overline{y},\overline{z}) \neq (\overline{x'},\overline{y'},\overline{z'}) \in (\mathbb{Z}/n\mathbb{Z})^3$ Repräsentanten von P. Dann gibt es ein $\overline{u} \in (\mathbb{Z}/n\mathbb{Z})^*$, so dass $(\overline{x},\overline{y},\overline{z}) = (\overline{ux'},\overline{uy'},\overline{uz'})$. Da $p \mid n$, folgt, dass $(x+p\mathbb{Z}, y+p\mathbb{Z}, z+p\mathbb{Z}) = (ux'+p\mathbb{Z}, uy'+p\mathbb{Z}, uz'+p\mathbb{Z}) = ((u+p\mathbb{Z})(x'+p\mathbb{Z}), (u+p\mathbb{Z})(y'+p\mathbb{Z}), (u+p\mathbb{Z})(z'+p\mathbb{Z}))$ mit $u + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$. Daraus folgt, dass $\big((ux'+p\mathbb{Z}) : (uy'+p\mathbb{Z}) : (uz'+p\mathbb{Z})\big) = \big((x+p\mathbb{Z}) : (y+p\mathbb{Z}) : (z+p\mathbb{Z})\big) = \rho(P) \in E_p(\mathbb{Z}/p\mathbb{Z})$. Also ist ρ wohldefiniert.

Seien $P_1 = (\overline{x_1} : \overline{y_1} : \overline{z_1}), P_2 = (\overline{x_2} : \overline{y_2} : \overline{z_2}) \in E(\mathbb{Z}/n\mathbb{Z})$. Um P_1 und P_2 zu addieren, wählen wir die Repräsentanten $p_1 = (\overline{x_1},\overline{y_1},\overline{z_1})$ und $p_2 = (\overline{x_2},\overline{y_2},\overline{z_2}) \in (\mathbb{Z}/n\mathbb{Z})^3$ von P_1 und P_2 und berechnen mit den Formeln I, II und III die Matrixeinträge $x_3^I, y_3^I, ..., z_3^{III}$ modulo n. Sei $(\overline{x_3},\overline{y_3},\overline{z_3}) \in (\mathbb{Z}/n\mathbb{Z})^3$ eine primitive Linearkombination der Zeilen von $M(p_1,p_2)$. Dann ist die Summe $P_3 = P_1 + P_2$ durch $(\overline{x_3} : \overline{y_3} : \overline{z_3})$ gegeben. Für die Addition von $\rho(P_1)$ und $\rho(P_2)$ wählen wir die Repräsenten $q_1 = (x_1 + p\mathbb{Z}, y_1 + p\mathbb{Z}, z_1 + p\mathbb{Z})$ und $q_2 = (x_2 + p\mathbb{Z}, y_2 + p\mathbb{Z}, z_2 + p\mathbb{Z})$ und erhalten dieselben Ergebnisse $x_3^I, y_3^I, ..., z_3^{III}$ modulo p. Es folgt, dass $(x_3 + p\mathbb{Z}, y_3 + p\mathbb{Z}, z_3 + p\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z})^3$ ein primitives Tripel ist und als Linearkombination der Zeilen von $M(q_1,q_2)$ dargestellt werden kann. Also $\rho(P_1) + \rho(P_2) = \big((x_3 + p\mathbb{Z}) : (y_3 + p\mathbb{Z}) : (z_3 + p\mathbb{Z})\big)$. Damit gilt

$$\rho(P_1 + P_2) = \rho(P_3) = \rho((\overline{x_3} : \overline{y_3} : \overline{z_3})) = \big((x_3 + p\mathbb{Z}) : (y_3 + p\mathbb{Z}) : (z_3 + p\mathbb{Z})\big) = \rho(P_1) + \rho(P_2).$$

Also ist ρ ein Gruppenhomomorphismus. □

Sei $P = (\overline{x} : \overline{y} : \overline{z}) \in E(\mathbb{Z}/n\mathbb{Z})$. Wir bezeichnen $\rho(P) = \big((x+p\mathbb{Z}) : (y+p\mathbb{Z}) : (z+p\mathbb{Z})\big) \in E_p(\mathbb{Z}/p\mathbb{Z})$ mit P_p. Insbesondere gilt

$$\rho(\infty) = \infty \quad \text{und} \quad \rho(-P) = -P_p$$

für jeden Punkt $P \in E(\mathbb{Z}/n\mathbb{Z})$.

Für den Beweis des Satzes 3.1 müssen wir die Anzahl der Punkte in $E(\mathbb{Z}/p\mathbb{Z})$, p prim, zumindest abschätzen können. Der *Satz von Hasse* hilft uns weiter:

Satz 3.6 (Hasse)**.** *Sei p eine Primzahl und sei E eine elliptische Kurve über $\mathbb{Z}/p\mathbb{Z}$. Dann gilt*

$$|p+1-|E(\mathbb{Z}/p\mathbb{Z})|| \leq 2\sqrt{p}.$$

Für den Beweis verweisen wir auf [8] Ch. 4 Sec. 4.2. Aus dem Satz von Hasse folgt direkt

$$|E(\mathbb{Z}/p\mathbb{Z})| \leq (\sqrt{p}+1)^2.$$

Nun sind wir bereit, Satz 3.1 zu beweisen.

Satz 3.1. Wir argumentieren wie in [8] Ch. 7 Sec. 7.2. Sei p ein Primteiler von n. Wir betrachten einen endlichen Punkt $P_i = (\overline{x_i} : \overline{y_i} : \overline{z_i}) \in E(\mathbb{Z}/n\mathbb{Z})$, der die Voraussetzungen des Satzes erfüllt. Nach (i) ist $l_i P_i = \infty$. Daraus folgt mit Lemma 3.5, dass $l_i \cdot \rho(P_i) = \infty$ in $E(\mathbb{Z}/p\mathbb{Z})$. Wir bezeichnen $\rho(P_i) = \big((x_i + \mathbb{Z}/p\mathbb{Z}) : (y_i + \mathbb{Z}/p\mathbb{Z}) : (z_i + \mathbb{Z}/p\mathbb{Z})\big)$ mit $P_{i,p}$. Da $P_i \in E(\mathbb{Z}/n\mathbb{Z})$ endlich ist, ist auch $P_{i,p} \in E(\mathbb{Z}/p\mathbb{Z})$ endlich, und weil $l_i P_{i,p} = \infty$ und l_i prim ist, ist l_i die Ordnung von $P_{i,p}$ in $E(\mathbb{Z}/p\mathbb{Z})$. Daraus folgt

$$l_i \mid |E(\mathbb{Z}/p\mathbb{Z})| \quad \forall i = 1, ..., r.$$

Nun sind $l_1, ..., l_r$ verschiedene Primzahlen, daher gilt

$$\prod_{i=1}^{r} l_i \mid |E(\mathbb{Z}/p\mathbb{Z})|.$$

Mit (ii) und dem Satz von Hasse folgt, dass

$$(\sqrt[4]{n}+1)^2 < \prod_{i=1}^{r} l_i \leq |E(\mathbb{Z}/p\mathbb{Z})| \leq (\sqrt{p}+1)^2,$$

also $p > \sqrt{n}$. Jeder Primteiler von n ist demnach größer als $\sqrt{n}$. Wäre n eine zusammengesetzte Zahl, könnten wir n schreiben als $n = mpq$, wobei p, q prim sind mit $p, q > \sqrt{n}$ und $m \geq 1$. Dann gälte $n > mn \geq n$. Das ist ein Widerspruch. Also ist n eine Primzahl. □

Der Goldwasser-Kilian-Primzahltest ist insofern sehr elegant, als dass er es erlaubt, sofort auf die Primalität einer Zahl n zu schließen, sobald man endliche Punkte in $E(\mathbb{Z}/n\mathbb{Z})$ sowie Primzahlen gefunden hat, die (i) und (ii) erfüllen. Satz 3.1 sagt uns allerdings noch nicht, wie der Primzahltest genau funktionieren soll. Wir wollen nun einen Algorithmus aufstellen, der uns erklärt, wie wir mit Satz 3.1 eine Zahl auf Primalität testen können. Der Algorithmus soll anschließend durch ein Beispiel veranschaulicht werden.

3.2 Algorithmus mit Beispiel

Um eine Zahl $n > 3$ auf Primalität zu testen, gehe wie folgt vor.

Algorithmus 3.7 (Goldwasser-Kilian-Primzahltest)**.**

1. Wähle eine elliptische Kurve über $\mathbb{Z}/n\mathbb{Z}$, d.h. wähle $a, b \in \mathbb{Z}$ so, dass $\mathrm{ggT}(4a^3 + 27b^2, n) = 1$. Dann ist durch $y^2 z \equiv x^3 + axz^2 + bz^3 \pmod{n}$ eine elliptische Kurve $E = E_{\overline{a},\overline{b}}$ über $\mathbb{Z}/n\mathbb{Z}$ gegeben. Falls $\mathrm{ggT}(4a^3 + 27b^2, n) \neq 1$ und $4a^3 + 27b^2 \not\equiv 0 \pmod{n}$, findet man einen echten Teiler von n und der Algorithmus kann abgebrochen werden. Am besten wählt man a, b so, dass bereits ein Punkt in $E(\mathbb{Z}/n\mathbb{Z})$ bekannt ist.
2. Berechne die Ordnung von $E(\mathbb{Z}/n\mathbb{Z})$ mit dem *Algorithmus von Schoof* (siehe zum Beispiel [8] Ch. 4 Sec. 4.5) unter der Annahme, dass n prim ist. Geht dabei etwas schief, kann $\mathbb{Z}/n\mathbb{Z}$ kein Körper gewesen sein, d.h. n ist nicht prim und der Algorithmus kann abgebrochen werden.
3. Falls $|E(\mathbb{Z}/n\mathbb{Z})| = kl$ und $l > (\sqrt[4]{n} + 1)^2$ prim ist — l sollte eine bekannte Primzahl sein, ansonsten muss auch die Primalität von l nachgewiesen werden —, dann gehe weiter zu Schritt 4. Siehe anderenfalls Bemerkung 3.8 und gehe ggf. zu Schritt 1 zurück, um eine andere elliptische Kurve auszuprobieren.
4. Wähle einen Punkt $P \in E(\mathbb{Z}/n\mathbb{Z})$ der Form $P = (\overline{x} : \overline{y} : \overline{1})$. Falls nicht schon ein Punkt bekannt ist, wähle x so lange, bis $x^3 + ax + b$ ein quadratischer Rest modulo n ist, d.h. bis es ein y gibt, so dass $y^2 \equiv x^3 + ax + b \pmod{n}$, dann ist $(\overline{x} : \overline{y} : \overline{1}) \in E(\mathbb{Z}/n\mathbb{Z})$.
5. Berechne kP. Sei $M(tP)$ die Matrix, die aus den Formeln I, II und III entsteht und aus der tP berechnet wird, wobei $2 \leq t \leq k$ — die Wahl der Punktrepräsentanten wurde wieder unterschlagen. Sei $\overline{a_{ij}} \neq \overline{0}$ ein Eintrag von $M(tP)$. Ist $\overline{a_{ij}}$ eine Einheit von $\mathbb{Z}/n\mathbb{Z}$ — d.h. $\mathrm{ggT}(a_{ij}, n) = 1$ —, dann ist die i-te Zeile von $M(tP)$ primitiv und liefert als Punkt Q in $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ das Ergebnis der Addition, d.h. $Q = tP$. Ist $\overline{a_{ij}} \neq \overline{0}$ keine Einheit, so ist $\mathrm{ggT}(a_{ij}, n)$ ein echter Teiler von n und der Algorithmus kann abgebrochen werden. Ist man bei der Berechnung von $P' = kP$ auf keinen Eintrag $\overline{a_{ij}} \neq \overline{0}$ gestoßen, der keine Einheit ist, so untersuche die z-Koordinate $\overline{z}$ von P':

   Falls $\overline{z}$ eine Einheit ist, lässt sich P' in der Form $P' = (\overline{x} : \overline{y} : \overline{1})$ darstellen, d.h. P' ist endlich. Gehe weiter zu Schritt 6.

   Falls $\overline{z} \neq \overline{0}$ keine Einheit ist, so ist $\mathrm{ggT}(z, n)$ ein echter Teiler von n und der Algorithmus kann abgebrochen werden.

   Falls $\overline{z} = \overline{0}$, aber $P' \neq \infty$, d.h. die x-Koordinate von P' ist ungleich $\overline{0}$ oder die y-Koordinate ist keine Einheit, so kann $\mathbb{Z}/n\mathbb{Z}$ kein Körper und n damit nicht prim sein.

Der Algorithmus kann abgebrochen werden.

Falls $\overline{z} = \overline{0}$ und $P' = \infty$, so gehe zurück zu Schritt 4 und wähle einen neuen Punkt P.

6. Berechne lP'. Wenn bei der Berechnung ein Eintrag $\overline{a_{ij}} \neq \overline{0}$ generiert wird, der keine Einheit ist, kann n nicht prim sein. Der Algorithmus kann dann abgebrochen werden. Ansonsten ist entweder $lP' = kl \cdot P = \infty$ und n nach Satz 3.1 eine Primzahl oder $lP' \neq \infty$, dann ist kl aber nicht die Ordnung von $E(\mathbb{Z}/n\mathbb{Z})$, d.h. $\mathbb{Z}/n\mathbb{Z}$ kann kein Körper und n damit nicht prim sein.

Bemerkung 3.8. *Lässt sich im dritten Schritt keine Primzahl l mit $l > (\sqrt[4]{n}+1)^2$ finden, aber eine kleinere Primzahl l_i und in den folgenden Schritten 4 bis 6 ein endlicher Punkt P_i mit $l_i P_i = \infty$, dann suche so lange solche l_i, P_i, bis $\prod l_i > (\sqrt[4]{n}+1)^2$. Nach Satz 3.1 ist n dann eine Primzahl. Es empfiehlt sich, zuerst diesen Weg einzuschlagen, bevor man eine neue elliptische Kurve ausprobiert und den aufwendigen Algorithmus von Schoof anwenden muss.*

Bemerkung 3.9. *Man kann den Algorithmus auch so formulieren, dass keine elliptischen Kurven über Ringen benötigt werden und man schon mit den Körperformeln auskommt: Geht bei der Berechnung der Summe zweier Punkte mit den Körperformeln etwas schief, kann n keine Primzahl gewesen sein. Gelingt die Berechnung aber — dieser Fall kann auch dann eintreten, wenn n keine Primzahl ist —, so liefern die Körperformeln stets das richtige Ergebnis der Addition, denn so wie die Formeln I, II und III aus den Körperformeln entstehen, führen die Formeln I, II und III durch umgekehrte Multiplikation — wieder zurück — auf die Körperformeln.*

Wenn der Algorithmus für eine Zahl n bis zum letzten Schritt mit Erfolg durchlaufen werden konnte, so liefert er nicht nur das Ergebnis, dass n eine Primzahl ist, sondern hat darüber hinaus ein Zertifikat für die Primalität von n generiert, das aus den Koeffizienten a, b der Kurvengleichung der elliptischen Kurve sowie den Punkten P_i zusammen mit den Primzahlen l_i besteht. Sind a, b, P_i, l_i bekannt, kann man die Primalität von n schnell beweisen. Der Algorithmus soll nun durch ein Beispiel veranschaulicht werden.

Beispiel 3.10.

Wir wollen die Zahl 180547 auf Primalität testen.

1. Wir wählen $a = 1$ und $b = -1$. Dann ist $4 \cdot 1^3 + 27 \cdot (-1)^2 = 31$ und $\mathrm{ggT}(31, 180547) = 1$. D.h. mit $a = 1$ und $b = -1$ ist eine elliptische Kurve E über $\mathbb{Z}/180547\mathbb{Z}$ gegeben.
2. Der Algorithmus von Schoof liefert uns $|E(\mathbb{Z}/180547\mathbb{Z})| = 180316$.
3. $180316 = 244 \cdot 739$ und $(\sqrt[4]{180547}+1)^2 \approx 467,13$. Es gilt $739 > (\sqrt[4]{180547}+1)^2$ und 739 ist eine Primzahl. Wir setzen $l = 739$ und $k = 244$.

4. Es gilt $1^2 \equiv 1^3 + 1 \cdot 1 - 1 \pmod{180547}$, also $P = (\overline{1} : \overline{1} : \overline{1}) \in E(\mathbb{Z}/180547\mathbb{Z})$.
5. $244 \cdot P = (\overline{80174} : \overline{86559} : \overline{1}) = P'$.
6. $739 \cdot P' = \infty$. Daraus folgt, dass 180547 eine Primzahl ist.

Natürlich müssen wir noch wissen, dass 739 eine Primzahl ist. Das zeigen wir wieder mit dem Goldwasser-Kilian-Primzahtest:

1. Wir wählen $a = 2$ und $b = -2$. Dann ist $4 \cdot 2^3 + 27 \cdot (-2)^2 = 140$ und $\mathrm{ggT}(140, 739) = 1$. D.h. mit $a = 2$ und $b = -2$ ist eine elliptische Kurve E über $\mathbb{Z}/739\mathbb{Z}$ gegeben.
2. Der Algorithmus von Schoof liefert uns $|E(\mathbb{Z}/739\mathbb{Z})| = 759$.
3. $759 = 3 \cdot 11 \cdot 23$ und $(\sqrt[4]{739} + 1)^2 \approx 38,61$. Es gilt $3 \cdot 23 = 69 > (\sqrt[4]{739} + 1)^2$ und die Zahlen 3 und 23 sind Primzahlen. Wir setzen $l_1 = 3$, $l_2 = 23$, $k_1 = 11 \cdot 23 = 253$ und $k_2 = 3 \cdot 11 = 33$.
4. Es gilt $1^2 \equiv 1^3 + 2 \cdot 1 - 2 \pmod{739}$, also $P = (\overline{1} : \overline{1} : \overline{1}) \in E(\mathbb{Z}/739\mathbb{Z})$.
5. $253 \cdot P = (\overline{552} : \overline{480} : \overline{1}) = P'_1$ und $33 \cdot P = (\overline{69} : \overline{23} : \overline{1}) = P'_2$.
6. $3 \cdot P'_1 = \infty$ und $23 \cdot P'_2 = \infty$. Daraus folgt, dass 739 eine Primzahl ist.

(Als Hilfsmittel diente SageMath, siehe [7].)

Die schwierigste Aufgabe besteht darin, eine geeignete elliptische Kurve E zu finden, so dass Punkte $P_i \in E(\mathbb{Z}/n\mathbb{Z})$ mit den gewünschten Eigenschaften generiert werden können. Man kann zufällig vorgehen, muss ggf. aber mehrere elliptische Kurven ausprobieren, läuft also Gefahr, den aufwendigsten Teil des Tests, den Algorithmus von Schoof, mehrmals anwenden zu müssen. Atkin und Elkies haben die Effizienz des Algorithmus von Schoof mit Hilfe von Isogenien zwischen elliptischen Kurven verbessert (eine gute Zusammenfassung findet sich in [8] Ch. 12 Sec. 12.4). Eine noch effizientere Methode geht auf Atkin und Morain zurück und benutzt die Theorie der komplexen Multiplikation (siehe [1]). Der Vorteil liegt darin, dass von vornherein eine elliptische Kurve E so gewählt wird, dass die Ordnung von $E(\mathbb{Z}/n\mathbb{Z})$ bereits bekannt ist. Der Goldwasser-Kilian-Primzahltest gestaltet sich durch diese Verbesserungen noch effizienter. Er stellt die gängigste Methode dar, die Primalität großer Zahlen zu beweisen. Mit ihm wurde schon die Primalität von Zahlen bewiesen, die über 20000 Dezimalstellen besitzen.

Literatur

[1] Atkin, A. O. L. / Morain, F.: Elliptic curves and primality proving. In: *Math. Comp., 61(203), 1993*, 29-68.

[2] Bosma, W. / Lenstra, H. W. Jr.: Complete Systems of Two Addition Laws for Elliptic Curves. In: *Journal of Number Theory, 53, 1995*, 229-240.

[3] Forster, Otto: *Algorithmische Zahlentheorie*. Braunschweig/Wiesbaden: Vieweg, Springer, 1996.

[4] Hohenwarter, Markus / Hohenwarter, Judith: *GeoGebra Hilfe. Offizielles Handbuch 3.2*, 2009. Online verfügbar unter: https://app.geogebra.org/help/docude.pdf (10.02.2017). GeoGebra Website: www.geogebra.org.

[5] Lenstra, H. W. Jr.: Elliptic Curves and Number-Theoretic Algorithms. In: Gleason, Andrew M. (Hg.): *Proceedings of the International Congress of Mathematicians, August 3-11, 1986, Berkeley, California*. Providence: American Mathematical Society, 1987, 99-120.

[6] Tang, Hwa Tsang: Gauss' Lemma. In: *Proceedings of the American Mathematical Society, Vol. 35, No. 2, 1972*, 372-376.

[7] The Sage Development Team: *Sage Tutorial. Release 7.5*, 2017. Online verfügbar unter: http://doc.sagemath.org/pdf/en/tutorial/SageTutorial.pdf (10.02.2017). SageMath Website: www.sagemath.com.

[8] Washington, Lawrence C.: *Elliptic Curves: Number Theory and Cryptography*. *Discrete Mathematics and Its Applications*. Boca Raton: Chapman & Hall/CRC, 2008.

Eigenständigkeitserklärung

Hiermit versichere ich, Julian Söhngen, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Duisburg, den 10. Februar 2017

Julian Söhngen