Nennerfreie Gleichungen für elliptische Kurven mit Torsionspunkt der Ordnung 4 bis 20

Patrick Reichert

14. Juni 2017

Zusammenfassung

Die von Andrew Sutherland optimierten Darstellungen elliptischer Kurven vorgegebener Torsion werden so umgeformt, dass die Koeffiziententerme nennerfrei sind. Es wird ein Algorithmus angegeben, der eine möglichst kompakte Faktorisierung der Diskriminante in nicht-faktoriellen Polynomringen bestimmt.

Mathematical Subject Classification 2010: 11G05, 14H52 (primary), 14H10 (secondary)

Inhaltsverzeichnis

1 Elliptische Kurven mit Torsionspunkt

Definition 1.1 (Torsionspunkt) *Sei E eine über $\mathbb{C}$ definierte elliptische Kurve mit Basispunkt $\mathcal{O}$ und $n \geq 2$ eine natürliche Zahl. Ein Punkt $P \in E$ heißt n-**Torsionspunkt**, falls $nP = \mathcal{O}$ und $mP \neq \mathcal{O}$ für alle natürlichen Zahlen m mit $1 \leq m < n$ gilt.*

Theorem 1.2 (Tate-Normalform, Definition 4.1 in [Hus2004], Tabelle 3 in [Kub1976]) *Sei E eine über $\mathbb{C}$ definierte elliptische Kurve mit Basispunkt $\mathcal{O}$. Ist $P = (0,0) \in E$ ein n-Torsionspunkt mit $n \geq 4$, so lässt sich die Gleichung der elliptischen Kurve in **Tate-Normalform***

$$E(b,c)\colon y^2 + (1-c)xy - by = x^3 - bx^2$$

für zwei Parameter $b, c \in \mathbb{C}$ schreiben.

Beweis. Die Weierstraß-Normalform einer über $\mathbb{C}$ definierten elliptischen Kurve lautet

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

für Parameter $a_1, a_2, a_3, a_4, a_6 \in \mathbb{C}$. Aus $(0,0) \in E$ folgt $a_6 = 0$. Weiterhin gilt $a_3 \neq 0$, da ansonsten $-P = P$ und damit $2P = \mathcal{O}$ folgen würde. Die Substitution

$$y \mapsto y + \left(\frac{a_4}{a_3}\right) x$$

ergibt

$$y^2 + \frac{a_1a_3 + 2a_4}{a_3}\, xy + a_3y = x^3 + \frac{a_2a_3^2 - a_4^2 - a_1a_3a_4}{a_3^2}\, x^2$$

und zeigt damit, dass es ohne Beschränkung der Allgemeinheit genügt, nur Weierstraß-Formen mit $a_4 = 0$ zu betrachten, da sich der lineare Term stets durch diese Substitution entfernen lässt. Somit genügt es, die reduzierte Gleichung

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2$$

zu betrachten. Hier gilt $a_2 \neq 0$, da ansonsten $2P = (-a_2, -a_1a_2 - a_3) = (0, -a_3) = -P$ und damit $3P = \mathcal{O}$ folgen würde. Die Substitution

$$x \mapsto \left(\frac{a_3}{a_2}\right)^2 x, \qquad y \mapsto \left(\frac{a_3}{a_2}\right)^3 y$$

reduziert die Anzahl der Parameter von drei (a_1, a_2, a_3) auf zwei (α, β):

$$\begin{aligned} &y^2 + \frac{a_1a_2}{a_3}\, xy + \frac{a_2^3}{a_3^2}\, y = x^3 + \frac{a_2^3}{a_3^2}\, x^2 \\ &y^2 + \alpha xy + \beta y = x^3 + \beta x^2 \end{aligned}$$

Klassischerweise bezeichnet man die Parameter in der Form $\alpha = 1-c$ und $\beta = -b$ und erhält damit die angegebene Tate-Normalform einer elliptischen Kurve mit n-Torsionspunkt $(0,0)$ für $n \geq 4$. □

Theorem 1.3 (Vielfache des Torsionspunktes, [Rei1986], [Sut2012]) *Sei $E(b,c)\colon y^2+(1-c)xy-by = x^3 - bx^2$ eine in Tate-Normalform gegebene elliptische Kurve über $\mathbb{C}$ mit Basispunkt $\mathcal{O}$ und n-Torsionspunkt $P = (0,0) \in E(b,c)$ mit $n \geq 4$. Dann besitzt P die folgenden Vielfachen:*

$$\begin{aligned} P &= (0,0), \\ 2P &= (b, bc), \\ 3P &= (c, b-c), \\ 4P &= (r(r-1), r^2(c+r-1)) \text{ mit } r = \frac{b}{c}, \\ 5P &= (rs(s-1), rs^2(r-s)) \text{ mit } s = \frac{c^2}{b-c}, \\ 6P &= \left(\frac{s(r-1)(r-s)}{(s-1)^2}, \frac{s^2(r-1)^2(rs-2r+1)}{(s-1)^3}\right), \\ 7P &= \left(\frac{rs(r-1)(s-1)(rs-2r+1)}{(r-s)^2}, \frac{r^2s(r-1)^2(r-s^2+s-1)(s-1)^2}{(r-s)^3}\right). \end{aligned}$$

Für $c = 0$ gilt $4P = \mathcal{O}$, für $b = c$ gilt $5P = \mathcal{O}$, für $s = 1$ gilt $6P = \mathcal{O}$, für $r = s$ gilt $7P = \mathcal{O}$. Die Rücksubstitution der in der Literatur üblichen Hilfsvariablen erfolgt gemäß

$$b = rs(r-1) \text{ und } c = s(r-1). \qquad \square$$

Theorem 1.4 (Gleichungen für rationale Torsionskurven) *Die folgende Tabelle beschreibt für $n \in \{4, \ldots, 10, 12\}$ die allgemeine Gleichung einer elliptischen Kurve über $\mathbb{C}$, die den n-Torsionspunkt $P = (0,0)$ besitzt:*

n	*Darstellung und Diskriminante der elliptischen Kurve mit n-Torsionspunkt $P=(0,0)$*
4	$E_4\colon y^2+xy+cy=x^3+cx^2$, $c\in\mathbb{C}\setminus\left\{0,\ \frac{1}{16}\right\}$, $\operatorname{disc}(E_4)=-(16c-1)\,c^4$
5	$E_5\colon y^2+(c+1)xy+cy=x^3+cx^2$, $c\in\mathbb{C}\setminus\left\{0,\ -\frac{11}{2}\pm\frac{5}{2}\sqrt{5}\right\}$, $\operatorname{disc}(E_5)=-(c^2+11c-1)\,c^5$
6	$E_6\colon y^2+(1-c)xy-c(c+1)y=x^3-c(c+1)x^2$, $c\in\mathbb{C}\setminus\left\{0,\ -1,\ -\frac{1}{9}\right\}$, $\operatorname{disc}(E_6)=(c+1)^3(9c+1)c^6$
7	$E_7\colon y^2+(1-c-c^2)xy+(c+1)c^2y=x^3+(c+1)c^2x^2$, $c\in\mathbb{C}\setminus\left\{0,\ -1,\ \frac{14}{3}\sin\left(\frac{1}{3}\arctan\left(\frac{13}{14}\right)\right)-\frac{8}{3},\ -\frac{14}{3}\sin\left(\frac{1}{3}\arcsin\left(\frac{13}{14}\right)+\frac{\pi}{3}\right)-\frac{8}{3}\right.$, $\left.\frac{14}{3}\cos\left(\frac{1}{3}\arcsin\left(\frac{13}{14}\right)+\frac{\pi}{6}\right)-\frac{8}{3}\right\}$, $\operatorname{disc}(E_7)=-(c^3+8c^2+5c-1)(c+1)^7c^7$
8	$E_8\colon y^2+(1-2c^2)xy-(2c+1)(c+1)^3cy=x^3-(2c+1)(c+1)^2cx^2$, $c\in\mathbb{C}\setminus\left\{0,\ -1,\ -\frac{1}{2},\ -\frac{1}{2}\pm\frac{1}{4}\sqrt{2}\right\}$, $\operatorname{disc}(E_8)=(8c^2+8c+1)(2c+1)^4(c+1)^8c^8$
9	$E_9\colon y^2+(c^3+c^2+1)xy+(c^2+c+1)(c+1)c^2y=x^3+(c^2+c+1)(c+1)cx^2$, $c\in\mathbb{C}\setminus\left\{0,\ -1,\ -\frac{1}{2}\pm\frac{1}{2}i\sqrt{3},\ 2\sqrt{3}\sin\left(\frac{\pi}{9}\right)-2,\ 2\sqrt{3}\sin\left(\frac{2\pi}{9}\right)-2,\ -2\sqrt{3}\cos\left(\frac{\pi}{18}\right)-2\right\}$, $\operatorname{disc}(E_9)=-(c^3+6c^2+3c-1)(c^2+c+1)^3(c+1)^9c^9$
10	$E_{10}\colon y^2+(-c^3-2c^2+4c+4)xy+(c+1)(c+2)(c^2+6c+4)c^3y$ $\quad=x^3+(c+1)(c+2)c^3x^2$, $c\in\mathbb{C}\setminus\left\{0,\ -1,\ -2,\ -\frac{1}{2}\pm\frac{1}{2}\sqrt{5},\ -3\pm\sqrt{5}\right\}$, $\operatorname{disc}(E_{10})=-(c^2+6c+4)^2(c^2+c-1)(c+2)^{10}(c+1)^5c^{10}$
12	$E_{12}\colon y^2+(-c^4-2c^2+8c+27)xy+32(c+3)(1-c^2)(c^2+3)(c^2+2c+5)y$ $\quad=x^3+4(1-c^2)(c^2+3)(c^2+2c+5)x^2$, $c\in\mathbb{C}\setminus\left\{1,\ -1,\ -3,\ \pm i\sqrt{3},\ 3\pm2\sqrt{3},\ -1\pm2i\right\}$, $\operatorname{disc}(E_{12})=4096(c^2+2c+5)^3(c^2-6c-3)(c^2+3)^4(c+3)^2(c+1)^{12}(c-1)^6$

Beweis. Die in der Tabelle angegebenen Gleichungen erhält man aus den Koordinaten der Vielfachen des Torsionspunktes gemäß Theorem 1.3. Für einen Punkt Q einer elliptischen Kurve bezeichne x_Q dessen x-Koordinate. Aus dem Additionstheorem für Punkte elliptischer Kurven folgt, dass zwei vom Basispunkt $\mathcal{O}$ verschiedene Punkte $Q\neq R$ einer elliptischen Kurve genau dann dieselbe x-Koordinate besitzen, wenn $Q+R=\mathcal{O}$ gilt.

Für $n=4$ gilt somit $x_P=x_{3P}$ und damit $c=0$ in der Tate-Normalform $E(b,c)$. Die allgemeine Gleichung einer elliptischen Kurve mit 4-Torsionspunkt $(0,0)$ lautet somit

$$y^2+xy-by=x^3-bx^2.$$

Die Substitution $b\mapsto -c$ liefert daraus die in der Tabelle angegebene Darstellungsform E_4.

Für $n = 5$ gilt $x_{2P} = x_{3P}$ und damit $b = c$. Die Tate-Normalform einer elliptischen Kurve mit 5-Torsionspunkt $(0, 0)$ lautet somit

$$y^2 + (1 - c)xy - cy = x^3 - cx^2.$$

Die Substitution $c \mapsto -c$ ergibt die Darstellung E_5 in der Tabelle.

Für $n = 6$ gilt $x_{2P} = x_{4P}$ und damit $b = r(r - 1)$. Mit $r = bc^{-1}$ folgt daraus $b = c(c+1)$ und die Gleichung einer elliptischen Kurve mit 6-Torsionspunkt $(0, 0)$ lautet

$$E_6 \colon y^2 + (1 - c)xy - c(c + 1)y = x^3 - c(c + 1)x^2.$$

Für $n = 7$ gilt $x_{3P} = x_{4P}$ und damit $c = r(r - 1)$. Zusammen mit $b = c \cdot r = r^2(r - 1)$ erhält man daraus als Gleichung einer elliptischen Kurve mit 7-Torsionspunkt $(0, 0)$:

$$y^2 + (1 + r - r^2)xy - (r - 1)r^2y = x^3 - (r - 1)r^2x^2.$$

Die Substitution $r \mapsto -c$ liefert die in der Tabelle angegebene Darstellung E_7.

Für $n = 8$ gilt $x_{3P} = x_{5P}$ und damit $c = rs(s - 1)$. Mit $c = s(r - 1)$ folgt daraus $s = 2 - r^{-1}$. Damit erhält man

$$\begin{aligned} b &= rs(r - 1) = (2r - 1)(r - 1) \quad \text{und} \\ c &= s(r - 1) = \frac{(2r - 1)(r - 1)}{r}. \end{aligned}$$

Die elliptische Kurvengleichung besitzt dann die Gestalt

$$y^2 + \left(1 - \frac{(2r - 1)(r - 1)}{r}\right) xy + (2r - 1)(1 - r)y = x^3 + (2r - 1)(1 - r)x^2.$$

Die Darstellung wird nennerfrei durch die Transformation

$$\begin{aligned} x &\mapsto \frac{x}{r^2}, \\ y &\mapsto \frac{y}{r^3}; \end{aligned}$$

man erhält dann

$$y^2 + (r - (2r - 1)(r - 1))xy + (2r - 1)(1 - r)r^3y = x^3 + (2r - 1)(1 - r)r^2x^2.$$

Die Substitution $r \mapsto c + 1$ erzeugt daraus die Darstellung E_8 in der Tabelle.

Für $n = 9$ gilt $x_{4P} = x_{5P}$ und damit $r(r - 1) = rs(s - 1)$. Daraus folgt

$$\begin{aligned} r &= s^2 - s + 1, \\ b &= rs(r - 1) = (s^2 - s + 1)(s - 1)s^2 \quad \text{und} \\ c &= s(r - 1) = (s - 1)s^2. \end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 9-Torsionspunkt $(0, 0)$ lautet somit

$$y^2 + (-s^3 + s^2 + 1)xy - (s^2 - s + 1)(s - 1)s^2y = x^3 - (s^2 - s + 1)(s - 1)s^2x^2.$$

Die Substitution $s \mapsto -c$ erzeugt daraus die in der Tabelle angegebene Darstellung E_9.

Für $n = 10$ gilt $x_{4P} = x_{6P}$ und damit $r(r - 1) = s(r - 1)(r - s)(s - 1)^{-2}$. Daraus folgt

$$\begin{aligned} r &= \frac{s^2}{-s^2 + 3s - 1}, \\ b &= rs(r - 1) = \frac{(s - 1)(2s - 1)s^3}{(-s^2 + 3s - 1)^2} \quad \text{und} \\ c &= s(r - 1) = \frac{(s - 1)(2s - 1)s}{-s^2 + 3s - 1}. \end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 10-Torsionspunkt $(0, 0)$ lautet somit

$$y^2 + \left(1 - \frac{(s - 1)(2s - 1)s}{-s^2 + 3s - 1}\right) xy - \frac{(s - 1)(2s - 1)s^3}{(-s^2 + 3s - 1)^2}\, y = x^3 - \frac{(s - 1)(2s - 1)s^3}{(-s^2 + 3s - 1)^2}\, x^2.$$

Eine nennerfreie Darstellung erhält man durch die Substitution

$$x \mapsto \frac{x}{(-4)^2(-s^2+3s-1)^2},$$
$$y \mapsto \frac{y}{(-4)^3(-s^2+3s-1)^3};$$

es gilt dann

$$y^2 + (8s^3 - 8s^2 - 8s + 4)xy + 64(s-1)(2s-1)s^3(-s^2+3s-1)y = x^3 - 16(s-1)(2s-1)s^3x^2.$$

Die Substitution $s \mapsto -\frac{1}{2}c$ überführt diese Gleichung in die in der Tabelle angegebene Form E_{10}.

Für $n = 12$ gilt $x_{5P} = x_{7P}$ und damit

$$rs(s-1) = \frac{rs(r-1)(s-1)(rs-2r+1)}{(r-s)^2} \quad \Rightarrow \quad r^2(s-3) + r(s+3) - s^2 - 1 = 0.$$

Um Wurzeln zu vermeiden, wird

$$s = \frac{a^2+3}{4}$$

substituiert, damit gilt entweder

$$r = r_1 = \frac{a^2+2a+5}{2(a+3)} \quad \text{oder} \quad r = r_2 = \frac{a^2-2a+5}{2(3-a)}.$$

Hier genügt es, die erste Parametrisierung für r zu betrachten. Durchläuft a_1 alle Elemente von $\mathbb{C}$, so wird $r = r_1$ für $a = a_1$ und $r = r_2$ für $a = -a_1$ angenommen. Mit $r = \frac{1}{2}(a^2+2a+5)(a+3)^{-1}$ erhält man

$$b = rs(r-1) = \frac{(a^2-1)(a^2+3)(a^2+2a+5)}{16(a+3)^2} \quad \text{und}$$
$$c = s(r-1) = \frac{(a^2-1)(a^2+3)}{8(a+3)}.$$

Eine nennerfreie Darstellung der elliptischen Kurve $E(b,c)\colon y^2 + (1-c)xy - by = x^3 - bx^2$ erhält man durch die Substitution

$$x \mapsto \frac{x}{8^2(a+3)^2},$$
$$y \mapsto \frac{y}{8^3(a+3)^3};$$

es gilt dann

$$E_{12}\colon y^2 + (-a^4 - 2a^2 + 8a + 27)\,xy + 32(a+3)(1-a^2)(a^2+3)(a^2+2a+5)\,y$$
$$= x^3 + 4(1-a^2)(a^2+3)(a^2+2a+5)\,x^2.$$

Für die andere mögliche Wahl $r = r_2$ erhält man dieselbe Parametrisierung einer 12-Torsionskurve; es findet lediglich der Vorzeichenwechsel $a \mapsto -a$ statt. □

2 Algorithmen zur Faktorisierung von Polynomen in Idealen

In Polynomringen ohne eindeutige Primfaktorzerlegung ist das multiplikative Zerlegen von Termen aufwendig, selbst wenn die Menge der möglichen Faktoren vorgegeben ist. Sei T ein polynomieller Term und $\{F_1, \ldots, F_n\}$ eine endliche Menge von Polynomen. Gesucht sind Exponenten $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$, so dass in der Faktorisierung

$$T = P \cdot \prod_{i=1}^{n} F_i^{\alpha_i}$$

das Polynom P eine möglichst geringe Anzahl von Monomen besitzt. Im Optimalfall $P \equiv 1$ wäre der Term T komplett faktorisiert.

Um die Komplexität der Aufgabenstellung zu verdeutlichen, soll das Beispielpolynom

$$T = (e+f)^3 \cdot (e+1)^2 \cdot e^2 \cdot f^6 \cdot (e^3 + 2e^2 - ef - f^2 + 2e + f)^8$$

bezüglich der Faktorenmenge $\{F_1, \ldots, F_8\} = \{e+f,\ e+1,\ e,\ f,\ e-f+1,\ f-1,\ e^2+e-f+1,\ e^3+2e^2-ef-f^2+2e+f\}$ multiplikativ zerlegt werden, wobei die Variablen e und f auf der Kurve

$$\begin{aligned} X_1(19)\colon\ & f^5 - (e^2+2)f^4 - (2e^3+2e^2+2e-1)f^3 + (e^5+3e^4+7e^3+6e^2+2e)f^2 \\ & - (e^5+2e^4+4e^3+3e^2)f + (e^3+e^2) = 0 \end{aligned}$$

liegen sollen. Dieses Beispiel soll aufzeigen, dass ein sogenannter Greedy-Algorithmus nicht in der Lage ist, die vollständige Faktorisierung $(\alpha_1, \ldots, \alpha_8) = (3,2,2,6,0,0,0,8)$ zu ermitteln. Ein solcher Greedy-Algorithmus iteriert einmalig in einer festen Reihenfolge über die Faktorenmenge $\{F_1, \ldots, F_8\}$ und wählt für jedes Polynom F_i den maximal möglichen Exponenten α_i aus. Für die Reihenfolge $(F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8)$ erhält man die partielle Faktorisierung

$$T = (e+f)^7 \cdot (e+1) \cdot e^8 \cdot (e-f+1)^6 \cdot P_1,$$

wobei das verbleibende Polynom P_1 durch keinen Faktor aus $\{F_1, \ldots, F_8\}$ mehr teilbar ist. Für andere Faktorenreihenfolgen liefert der Greedy-Algorithmus:

$$\begin{aligned} T &= (e+1)^5 \cdot e^{12} \cdot (e^3 + 2e^2 - ef - f^2 + 2e + f) \cdot (f-1)^{10} \cdot P_2, \\ T &= e^{12} \cdot f \cdot (e+1)^4 \cdot (e-f+1) \cdot (f-1)^{12} \cdot P_3, \\ T &= f^{10} \cdot (e^3 + 2e^2 - ef - f^2 + 2e + f)^8 \cdot (e+f) \cdot (f-1) \cdot P_4, \end{aligned}$$

wobei die verbleibenden nicht weiter faktorisierbaren Polynome P_2, P_3, P_4 jeweils sehr viele Monome besitzen. Man erhält sogar Faktorisierungen, wenn der Greedy-Algorithmus mit Faktoren startet, die in der initialen Bildungsvorschrift von T gar nicht enthalten sind:

$$\begin{aligned} T &= (e-f+1)^9 \cdot (e+f)^7 \cdot f \cdot P_5, \\ T &= (f-1)^{22} \cdot e^5 \cdot f^{10} \cdot P_6, \\ T &= (e^2+e-f+1)^{13} \cdot (e+1)^3 \cdot e \cdot f^4 \cdot P_7. \end{aligned}$$

Ein Greedy-Algorithmus erreicht nicht das Ziel, Exponenten $(\alpha_1, \ldots, \alpha_n)$ zu bestimmen, so dass das nicht weiter faktorisierbare Polynom

$$P = \frac{T}{\prod_{i=1}^{n} F_i^{\alpha_i}}$$

möglichst wenig Monome besitzt. Zum einen wird nur eine einzelne feste Faktorenreihenfolge berücksichtigt, zum anderen wird für jedes Polynom F_i stets der maximal mögliche Exponent α_i ausgewählt.

Behoben werden diese beiden Nachteile mit einem Algorithmus, der alle für T auswählbaren Exponentenvektoren $(\alpha_1, \ldots, \alpha_n)$ und somit auch alle Faktorenreihenfolgen betrachtet.

Algorithmus 2.1 (Optimale Faktorisierung)

- ***Eingabe:***
  - *Polynom T in zwei Variablen e, f, welches im Polynomring $R = \mathbb{C}[e,f]/I$ bezüglich eines Ideals I liegt*
  - *Endliche duplikatfreie Faktorenmenge $\{F_1, \ldots, F_n\} \subset R$*
- ***Ausgabe:***
  - *Exponentenvektor $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, so dass T durch $\prod_{i=1}^{n} F_i^{\alpha_i}$ teilbar ist und das Polynom $T / \prod_{i=1}^{n} F_i^{\alpha_i}$ die geringste Anzahl von Monomen besitzt (unter allen für T auswählbaren Exponentenvektoren)*
- ***Algorithmus:***

Schritt	Art der Optimierung
Schritt 1 [Entfernen von 1-Monom-Faktoren]: Aus der Faktorenmenge $\{F_1, \ldots, F_n\}$ werden alle Polynome entfernt, die nur aus einem Monom bestehen, also $\alpha \cdot e^m$ und $\alpha \cdot f^m$ für $\alpha \in \mathbb{C}$, $m \in \mathbb{N}$.	Die rekursive Suche würde deutlich länger dauern, wenn Monome nicht mit Maximalpotenz aus dem Term entfernt werden.
Schritt 2 [Rekursive Iteration über alle Exponentenvektoren $(\alpha_1, \ldots, \alpha_n)$**]:** Wenn dieser Schritt mit dem noch zu zerlegendem Restpolynom T und der verbleibenden Faktorenmenge $\{F_s, \ldots F_n\}$ aufgerufen wird:	
(2.a) Aus $\{F_s, \ldots, F_n\}$ werden alle Faktoren entfernt, durch die T nicht mehr teilbar ist.	Vermeidung überflüssiger Teilbarkeitstests in allen weiteren rekursiven Aufrufen
(2.b) Für jeden verbliebenen Faktor $F_i \in \{F_s, \ldots, F_n\}$ wird Schritt 2 rekursiv mit den Parametern $(T/F_i, \{F_i, \ldots, F_n\})$ aufgerufen.	Wenn T bereits durch $\{F_1, \ldots, F_{i-1}\}$ geteilt wurde, müssen nur noch die Faktoren $\{F_i, \ldots, F_n\}$ betrachtet werden. Die Faktorisierungsreihenfolge „Erst F_b, dann F_a“ ist überflüssig, wenn vorher „Erst F_a, dann F_b“ betrachtet wurde.
(2.c) [Vollständige Faktorisierung gefunden ?]: Hat einer der rekursiven Aufrufe von **(2.b)** eine Faktorisierung gefunden, in der das nicht-faktorisierbare Restpolynom nur noch aus einem Monom besteht, kann der gesamte **Schritt 2** vorzeitig beendet werden.	Abbruch weiterer rekursiver Aufrufe, da das Ergebnis des Gesamtalgorithmus feststeht; die optimale Faktorisierung wurde gefunden.
(2.d) [Bestes Ergebnis nach oben zurückgeben]: Unter allen durchgeführten rekursiven Aufrufen T/F_i, $i \in \{s, \ldots, n\}$ und $T/1$ wird derjenige an den Aufrufer zurückgeliefert, für den der nicht weiter faktorisierbare Restterm die geringste Anzahl an Monomen besitzt.	Bedeutung von $T/1$: Hier wird der Fall berücksichtigt, dass $T/1 = T$ weniger Monome besitzt als jede fortgesetzte Faktorisierung von T/F_i.
Schritt 3 [Behandlung der 1-Monom-Faktoren]: Aus dem Restterm der gefundenen optimalen Faktorisierung werden die in **Schritt 1** entfernten 1-Monom-Faktoren (αe^m, αf^m) mit maximaler Potenz herausfaktorisiert.	

3 Die 11-Torsionskurve

Theorem 3.1 (Nennerfreie 11-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 11-Torsionspunkt $(0, 0)$ *lautet*

$$\begin{aligned} E_{11}\colon y^2 &+ (1 - (e+f)(f+1))\, xy - (ef+1)(e+f)(f+1)\, y \\ &= x^3 - (ef+1)(e+f)(f+1)\, x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$*, die auf der Kurve*

$$X_1(11)\colon \chi_{11}(e,f) \stackrel{def}{:=} f^2 + (e^2+1)f + e = 0$$

liegen.

(b) Die Diskriminante

$$\operatorname{disc}(E_{11}) = e^{11} \cdot (e-1)^2 \cdot (ef+1)^7 \cdot (e^2 - ef - 4e - 2f - 1)$$

verschwindet unter der Nebenbedingung $\chi_{11}(e,f)=0$ genau für die 8 Parameterpaare

$$(e,f)\in\{(0,0),(0,-1),(1,-1),(e_1,f_1),\ldots,(e_5,f_5)\}.$$

Die reellen Zahlen $e_1,\ldots,e_5$ sind dabei die Nullstellen von $e^5-e^4-15e^3+14e^2+3e-1$, die zugehörigen Werte $f_1,\ldots,f_5$ bestimmen sich gemäß $f_i=\varphi(e_i)$ für $i\in\{1,\ldots,5\}$ mit

$$\varphi(e)\overset{def}{:=}\frac{1}{11}(-e^4+3e^3+9e^2-21e-5)$$

und sind damit die Nullstellen des Polynoms $f^5+18f^4+35f^3+16f^2-2f-1$.

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 11-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\ & b=rs(r-1)\\ & c=s(r-1)\\ & r=ef+1\\ & s=-e+1\\ & X_1(11)\colon\ f^2+(e^2+1)f+e=0\end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned}1-c&=1-(e+f)(f+1)\\ -b&=-(ef+1)(e+f)(f+1)\end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 11-Torsionspunkt $(0,0)$ lautet also

$$\begin{aligned}E_{11}\colon\ & y^2+(1-(e+f)(f+1))\,xy-(ef+1)(e+f)(f+1)\,y\\ &=x^3-(ef+1)(e+f)(f+1)\,x^2\end{aligned}$$

mit der Nebenbedingung

$$\chi_{11}(e,f)=f^2+(e^2+1)f+e=0.$$

Für die Diskriminante $\operatorname{disc}(E_{11})$ liefert der Algorithmus 2.1 folgende optimierte Faktorisierung:

$$\operatorname{disc}(E_{11})=e^{11}\cdot(e-1)^2\cdot(ef+1)^7\cdot(e^2-ef-4e-2f-1).$$

Um zu bestimmen, wann diese Diskriminante unter der Nebenbedingung $\chi_{11}(e,f)=0$ verschwindet, werden die Resultanten bezüglich der Variablen e und f betrachtet:

$$\begin{aligned}\operatorname{res}_e(\operatorname{disc}(E_{11}),\chi_{11})&=-(e-1)^{11}\cdot e^{22}\cdot(e^5-e^4-15e^3+14e^2+3e-1)\\ \operatorname{res}_f(\operatorname{disc}(E_{11}),\chi_{11})&=f^{17}\cdot(f+1)^{22}\cdot(f^5+18f^4+35f^3+16f^2-2f-1)\end{aligned}$$

Die Resultanten besitzen folgende Nullstellen:

$$\begin{aligned}e_1&\approx-3.823 & f_1&\approx-15.857\\ e_2&\approx-0.325 & f_2&\approx 0.241\\ e_3&\approx 0.194 & f_3&\approx-0.793\\ e_4&\approx 1.067 & f_4&\approx-1.346\\ e_5&\approx 3.886 & f_5&\approx-0.245\\ e_6&=0 & f_6&=0\\ e_7&=1 & f_7&=-1\end{aligned}$$

Unter den 49 Paaren (e_i,f_j), $i,j\in\{1,\ldots,7\}$ lassen nur die folgenden 8 Paare sowohl die Diskriminante $\operatorname{disc}(E_{11})$ als auch die Kurvengleichung $\chi_{11}(e,f)$ verschwinden:

$$(e,f)\in\{(0,0),(0,-1),(1,-1),(e_1,f_1),\ldots,(e_5,f_5)\}.$$

Aus dem Diskriminantenfaktor $(e^2 - ef - 4e - 2f - 1)$ erhält man die Parametrisierung

$$f_i = T(e_i) \quad \text{für alle } i \in \{1, \ldots, 5\}$$

mit

$$T(e) = T_1(e) \stackrel{\text{def}}{=} \frac{e^2 - 4e - 1}{e + 2}.$$

Da $e_1, \ldots, e_5$ Nullstellen des Polynoms $e^5 - e^4 - 15e^3 + 14e^2 + 3e - 1$ sind, kann die Transformation T auch nennerfrei dargestellt werden, indem man $T_1(e)$ modulo $e^5 - e^4 - 15e^3 + 14e^2 + 3e - 1$ reduziert:

$$T(e) = T_2(e) \stackrel{\text{def}}{=} \frac{1}{11}(-e^4 + 3e^3 + 9e^2 - 21e - 5).$$

Damit erhält man insgesamt: Ist $\overline{e}$ eine Nullstelle von $e^5 - e^4 - 15e^3 + 14e^2 + 3e - 1$, dann ist $T_1(\overline{e})$ eine Nullstelle von $f^5 + 18f^4 + 35f^3 + 16f^2 - 2f - 1$ wegen

$$\begin{aligned}
&T_1(\overline{e})^5 + 18T_1(\overline{e})^4 + 35T_1(\overline{e})^3 + 16T_1(\overline{e})^2 - 2T_1(\overline{e}) - 1 \\
&= \frac{1}{(\overline{e}+2)^5} \cdot (\overline{e}^5 - \overline{e}^4 - 15\overline{e}^3 + 14\overline{e}^2 + 3\overline{e} - 1) \cdot (\overline{e}^5 - \overline{e}^4 - 48\overline{e}^3 + 179\overline{e}^2 - 151\overline{e} - 23) = 0.
\end{aligned}$$

Für die Darstellung T_2 erhält man analog

$$\begin{aligned}
&T_2(\overline{e})^5 + 18T_2(\overline{e})^4 + 35T_2(\overline{e})^3 + 16T_2(\overline{e})^2 - 2T_2(\overline{e}) - 1 \\
&= -\frac{1}{161051} \cdot (\overline{e}^5 - \overline{e}^4 - 15\overline{e}^3 + 14\overline{e}^2 + 3\overline{e} - 1) \cdot (\overline{e}^{15} - 14\overline{e}^{14} + 46\overline{e}^{13} + 197\overline{e}^{12} - 1568\overline{e}^{11} \\
&+ 2079\overline{e}^{10} + 10560\overline{e}^9 - 49093\overline{e}^8 + 49555\overline{e}^7 + 231737\overline{e}^6 - 735218\overline{e}^5 + 182525\overline{e}^4 + 1864560\overline{e}^3 \\
&- 2462764\overline{e}^2 + 757359\overline{e} + 109009) = 0.
\end{aligned}$$

Faktorisiert man die Diskriminante in der Form

$$\begin{aligned}
\operatorname{disc}(E_{11}) = -(f+1)^{11}[&e(f^7 + 8f^6 - 9f^5 - 20f^4 + 6f^3 + 11f^2 - 2f - 1) + \\
&(f^7 - 13f^6 - 10f^5 + 13f^4 + 8f^3 - 3f^2 - f)],
\end{aligned}$$

so lässt sich aus $\operatorname{disc}(E_{11}) = 0$ die Beziehung

$$e = -\frac{f^7 - 13f^6 - 10f^5 + 13f^4 + 8f^3 - 3f^2 - f}{f^7 + 8f^6 - 9f^5 - 20f^4 + 6f^3 + 11f^2 - 2f - 1}$$

ableiten. Wählt man für f nur Nullstellen von $f^5 + 18f^4 + 35f^3 + 16f^2 - 2f - 1$, so lässt sich dieser Bruch modulo $f^5 + 18f^4 + 35f^3 + 16f^2 - 2f - 1$ reduzieren zu

$$e = H(f) \stackrel{\text{def}}{=} \frac{1}{11}(-10f^4 - 177f^3 - 298f^2 - 86f + 37).$$

Ist $\overline{f}$ eine Nullstelle von $f^5 + 18f^4 + 35f^3 + 16f^2 - 2f - 1$, dann ist $H(\overline{f})$ eine Nullstelle von $e^5 - e^4 - 15e^3 + 14e^2 + 3e - 1$ wegen

$$\begin{aligned}
&H(\overline{f})^5 - H(\overline{f})^4 - 15H(\overline{f})^3 + 14H(\overline{f})^2 + 3H(\overline{f}) - 1 \\
&= -\frac{1}{161051} \cdot (\overline{f}^5 + 18\overline{f}^4 + 35\overline{f}^3 + 16\overline{f}^2 - 2\overline{f} - 1) \cdot (100000\overline{f}^{15} + 7050000\overline{f}^{14} + 197790000\overline{f}^{13} \\
&+ 2795883000\overline{f}^{12} + 20913034050\overline{f}^{11} + 82408707557\overline{f}^{10} + 183096368114\overline{f}^9 + 233299607123\overline{f}^8 \\
&+ 154699317850\overline{f}^7 + 23893332331\overline{f}^6 - 31375760625\overline{f}^5 - 15033616144\overline{f}^4 + 1146616072\overline{f}^3 \\
&+ 1261211278\overline{f}^2 - 63054876\overline{f} - 16232963) = 0.
\end{aligned}$$

Die Transformationen $e \mapsto T(e)$ und $f \mapsto H(f)$ sind sogar echte Umkehrfunktionen: es gilt $H(f_i) = e_i$ für alle $i \in \{1, \ldots, 5\}$. □

Beispiel 3.2 (11-Torsionskurven)

(a) Die Parameter $e = -1, f = \sqrt{2} - 1$ liefern die elliptische Kurve

$$y^2 + (2\sqrt{2} - 1)\,xy + (6\sqrt{2} - 8)\,y = x^3 + (6\sqrt{2} - 8)\,x^2$$

mit 11-Torsionspunkt $(0, 0)$.

(b) Die Parameter $e = 3, f = \sqrt{22} - 5$ liefern die elliptische Kurve

$$y^2 + (6\sqrt{22} - 29)\,xy + (816 - 174\sqrt{22})\,y = x^3 + (816 - 174\sqrt{22})\,x^2$$

mit 11-Torsionspunkt $(0, 0)$.

4 Die 13-Torsionskurve

Theorem 4.1 (Nennerfreie 13-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 13-Torsionspunkt $(0, 0)$ lautet

$$\begin{aligned} E_{13}\colon\ & y^2 + ((f+1)(ef+1) - e^2f^2)\,xy + ef(f+1)^2(ef-1)(ef-f-1)\,y \\ & = x^3 + ef(f+1)(ef-1)(ef-f-1)\,x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$, die auf der Kurve

$$X_1(13)\colon\ \chi_{13}(e, f) \overset{\text{def}}{=} f^2 + (e^3 + e^2 + 1)f - e^2 - e = 0$$

liegen.

(b) Die Diskriminante

$$\operatorname{disc}(E_{13}) = e^2 \cdot (e+1)^2 \cdot f^{11} \cdot (f+1)^5 \cdot (ef-1) \cdot (ef-f-1)^6 \cdot (e^3 + 4e^2 + e - 1)$$

verschwindet unter der Nebenbedingung $\chi_{13}(e, f) = 0$ genau für die 10 Parameterpaare

$$(e, f) \in \{(0,0),\ (0,-1),\ (-1,0),\ (-1,-1),\ (e_1, f_{4/5}),\ (e_2, f_{1/2}),\ (e_3, f_{3/6})\},$$

wobei e_1, e_2, e_3 die drei Nullstellen von $e^3 + 4e^2 + e - 1$ sind:

$$\begin{aligned} e_1 &= \frac{2}{3}\sqrt{13}\,\sin\left(\frac{1}{3}\arctan\left(\frac{5}{9}\sqrt{3}\right)\right) - \frac{4}{3}, \\ e_2 &= -\frac{2}{3}\sqrt{13}\,\sin\left(\frac{1}{3}\arctan\left(\frac{5}{9}\sqrt{3}\right) + \frac{\pi}{3}\right) - \frac{4}{3}, \\ e_3 &= \frac{2}{3}\sqrt{13}\,\cos\left(\frac{1}{3}\arctan\left(\frac{5}{9}\sqrt{3}\right) + \frac{\pi}{6}\right) - \frac{4}{3}. \end{aligned}$$

Dabei sind f_5, f_1, f_6 Nullstellen von $f^3 + (-16 - 5\sqrt{13})f^2 + (-10 - 3\sqrt{13})f + \frac{1}{2}(11 + 3\sqrt{13})$:

$$f_5 = \varphi(e_1), \quad f_1 = \varphi(e_2), \quad f_6 = \varphi(e_3) \quad \textit{mit } \varphi(e) \overset{\text{def}}{=} \frac{1}{2}(e+1)(3e-2) + \frac{1}{2}\sqrt{13}\,e(e+1).$$

Weiterhin sind f_4, f_2, f_3 Nullstellen von $f^3 + (-16 + 5\sqrt{13})f^2 + (-10 + 3\sqrt{13})f + \frac{1}{2}(11 - 3\sqrt{13})$:

$$f_4 = \psi(e_1), \quad f_2 = \psi(e_2), \quad f_3 = \psi(e_3) \quad \textit{mit } \psi(e) \overset{\text{def}}{=} \frac{1}{2}(e+1)(3e-2) - \frac{1}{2}\sqrt{13}\,e(e+1).$$

Die Umkehrfunktion $e_{1/1/2/2/3/3} = \Phi(f_{4/5/1/2/3/6})$ wird vermittelt durch das Polynom

$$\Phi(f) \overset{\text{def}}{=} \frac{1}{13}\,(32f^5 - 1033f^4 - 2558f^3 - 1151f^2 + 415f + 109).$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 13-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}
E(b,c)\colon\ & y^2 + (1-c)xy - by = x^3 - bx^2 \\
& b = rs(r-1) \\
& c = s(r-1) \\
& r = -ef + 1 \\
& s = 1 - \frac{ef}{f+1} \\
& X_1(13)\colon\ f^2 + (e^3+e^2+1)f - e^2 - e = 0
\end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned}
1 - c &= -\frac{e^2f^2 - ef^2 - ef - f - 1}{f+1} \\
-b &= \frac{ef(ef-1)(ef-f-1)}{f+1}
\end{aligned}$$

Eine nennerfreie Darstellung von $E(b,c)$ erhält man durch Substitution

$$\begin{aligned}
x &\mapsto \frac{x}{(f+1)^2} \\
y &\mapsto \frac{y}{(f+1)^3}
\end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 13-Torsionspunkt $(0,0)$ lautet also

$$\begin{aligned}
E_{13}\colon\ & y^2 + ((f+1)(ef+1) - e^2f^2)\,xy + ef(f+1)^2(ef-1)(ef-f-1)\,y \\
&= x^3 + ef(f+1)(ef-1)(ef-f-1)\,x^2
\end{aligned}$$

mit der Nebenbedingung

$$\chi_{13}(e,f) = f^2 + (e^3+e^2+1)f - e^2 - e = 0.$$

Für die Diskriminante $\operatorname{disc}(E_{13})$ liefert der Algorithmus 2.1 folgende optimierte Faktorisierung:

$$\operatorname{disc}(E_{13}) = e^2 \cdot (e+1)^2 \cdot f^{11} \cdot (f+1)^5 \cdot (ef-1) \cdot (ef-f-1)^6 \cdot (e^3+4e^2+e-1)$$

Um zu bestimmen, wann diese Diskriminante unter der Nebenbedingung $\chi_{13}(e,f) = 0$ verschwindet, werden die Resultanten bezüglich der Variablen e und f betrachtet:

$$\begin{aligned}
\operatorname{res}_e(\operatorname{disc}(E_{13}), \chi_{13}) &= (e+1)^{26} \cdot e^{38} \cdot (e^3+4e^2+e-1)^2 \\
\operatorname{res}_f(\operatorname{disc}(E_{13}), \chi_{13}) &= (f+1)^{38} \cdot f^{56} \cdot (f^6 - 32f^5 - 89f^4 - 59f^3 + 2f^2 + 7f + 1) \\
&= (f+1)^{38} \cdot f^{56} \cdot \left[f^3 + (-16-5\sqrt{13})f^2 + (-10-3\sqrt{13})f + \frac{1}{2}(11+3\sqrt{13})\right] \\
&\qquad \cdot \left[f^3 + (-16+5\sqrt{13})f^2 + (-10+3\sqrt{13})f + \frac{1}{2}(11-3\sqrt{13})\right]
\end{aligned}$$

Die Resultanten besitzen die folgenden Nullstellen:

$$\begin{aligned}
e_1 &= \ \ \frac{2}{3}\sqrt{13}\,\sin\left(\frac{1}{3}\,\arctan\left(\frac{5}{9}\sqrt{3}\right)\right) - \frac{4}{3}, \\
e_2 &= -\frac{2}{3}\sqrt{13}\,\sin\left(\frac{1}{3}\,\arctan\left(\frac{5}{9}\sqrt{3}\right) + \frac{\pi}{3}\right) - \frac{4}{3}, \\
e_3 &= \ \ \frac{2}{3}\sqrt{13}\,\cos\left(\frac{1}{3}\,\arctan\left(\frac{5}{9}\sqrt{3}\right) + \frac{\pi}{6}\right) - \frac{4}{3}, \\
e_4 &= -1, \\
e_5 &= 0,
\end{aligned}$$

$$f_{5/1/6} = \varphi(e_{1/2/3}) \quad \text{mit } \varphi(e) \overset{\text{def}}{=} \frac{1}{2}(e+1)(3e-2) + \frac{1}{2}\sqrt{13}\,e(e+1),$$

$$f_{4/2/3} = \psi(e_{1/2/3}) \quad \text{mit } \psi(e) \overset{\text{def}}{=} \frac{1}{2}(e+1)(3e-2) - \frac{1}{2}\sqrt{13}\,e(e+1),$$

$$\begin{aligned}
f_7 &= -1, \\
f_8 &= 0.
\end{aligned}$$

Ist $e \in \{e_1, e_2, e_3\}$ eine Nullstelle von e^3+4e^2+e-1, dann ist $\varphi(e) = \frac{1}{2}(e+1)(3e-2)+\frac{1}{2}\sqrt{13}\,e(e+1)$ eine Nullstelle von $f^3 + (-16 - 5\sqrt{13})f^2 + (-10 - 3\sqrt{13})f + \frac{1}{2}(11 + 3\sqrt{13})$: Einsetzen ergibt die Faktorisierung

$$(e^3 + 4e^2 + e - 1) \cdot \frac{1}{2} \cdot (18 + 5\sqrt{13}) \cdot (2e^3 + (7 - 3\sqrt{13})e^2 + (19 - 7\sqrt{13})e + (11 - 3\sqrt{13})) = 0.$$

Ist $e \in \{e_1, e_2, e_3\}$ eine Nullstelle von e^3+4e^2+e-1, dann ist $\psi(e) = \frac{1}{2}(e+1)(3e-2)-\frac{1}{2}\sqrt{13}\,e(e+1)$ eine Nullstelle von $f^3 + (-16 + 5\sqrt{13})f^2 + (-10 + 3\sqrt{13})f + \frac{1}{2}(11 - 3\sqrt{13})$: Einsetzen ergibt die Faktorisierung

$$(e^3 + 4e^2 + e - 1) \cdot \frac{1}{2} \cdot (18 - 5\sqrt{13}) \cdot (2e^3 + (7 + 3\sqrt{13})e^2 + (19 + 7\sqrt{13})e + (11 + 3\sqrt{13}) = 0.$$

Unter den 40 Paaren (e_i, f_j), $i \in \{1, \ldots, 5\}$, $j \in \{1, \ldots, 8\}$ lassen nur die folgenden 10 Paare sowohl die Diskriminante $\operatorname{disc}(E_{13})$ als auch die Kurvengleichung $\chi_{13}(e, f)$ verschwinden:

$$(e, f) \in \{(0, 0),\ (0, -1),\ (-1, 0),\ (-1, -1),\ (e_1, f_{4/5}),\ (e_2, f_{1/2}),\ (e_3, f_{3/6})\}.$$

Die Koeffizienten des Polynoms Φ erhält man durch Interpolation durch die 6 Punkte $(e_1, f_{4/5})$, $(e_2, f_{1/2})$, $(e_3, f_{3/6})$. □

Beispiel 4.2 (13-Torsionskurve) *Die Parameterwerte*

$$e = 1,\ f = \frac{1}{2}\sqrt{17} - \frac{3}{2}$$

ergeben folgende elliptische Kurve mit 13-Torsionspunkt $(0, 0)$*:*

$$E\colon y^2 + (\sqrt{17} - 2)\,xy + (13\sqrt{17} - 53)\,y = x^3 + (21 - 5\sqrt{17})\,x^2$$

5 Die 14-Torsionskurve

Theorem 5.1 (Nennerfreie 14-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 14-Torsionspunkt $(0, 0)$ *lautet*

$$\begin{aligned} &E_{14}\colon y^2 + (2f + (e+1)(f+1)^2)\,xy + (e+1)(e+f+1)(ef+f+1)f(f+1)^2\,y \\ &= x^3 + (1-e)(e+1)(ef+f+1)f\,x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$*, die auf der Kurve*

$$X_1(14)\colon \chi_{14}(e, f) \stackrel{def}{=} f^2 + (e^2 + e)f + e = 0$$

liegen.

(b) Die Diskriminante

$$\operatorname{disc}(E_{14}) = (e+1)^7 \cdot (e-1)^3 \cdot (e+f+1)^2 \cdot f^{14} \cdot (-2ef + f^2 + 2f - 1)$$

verschwindet unter der Nebenbedingung $\chi_{14}(e, f) = 0$ *genau für die 7 Parameterpaare*

$$(e, f) \in \{(0,\ 0),\ (1,\ -1),\ (-1,\ 1),\ (-1,\ -1), (e_7,\ -e_7 - 1), (e_8,\ -e_8 - 1), (e_9,\ -e_9 - 1)\},$$

wobei e_7*,* e_8*,* e_9 *die drei Nullstellen von* $e^3 + e^2 - 2e - 1$ *sind:*

$$\begin{aligned} e_7 &= -\frac{2}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right) + \frac{\pi}{6}\right) - \frac{1}{3}, \\ e_8 &= \ \ \frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right) + \frac{\pi}{3}\right) - \frac{1}{3}, \\ e_9 &= -\frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right) - \frac{1}{3}. \end{aligned}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 14-Torsionspunkt $(0,0)$ an:

$$\begin{aligned} E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\ & b=rs(r-1)\\ & c=s(r-1)\\ & r=1-\frac{e+f}{(1+f)(e+f+1)}\\ & s=\frac{1-e}{1+f}\\ & X_1(14)\colon\ f^2+(e^2+e)f+e=0 \end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned} 1-c&=-\frac{e^2-ef^2-ef-2e-f^3-3f^2-4f-1}{(e+f+1)(f+1)^2}\\ -b&=\frac{(1-e)(e+f)(ef+f^2+f+1)}{(e+f+1)^2(f+1)^3} \end{aligned}$$

Eine nennerfreie Darstellung von $E(b,c)$ erhält man durch Substitution

$$\begin{aligned} x&\mapsto\frac{x}{(f+1)^4(e+f+1)^2}\\ y&\mapsto\frac{y}{(f+1)^6(e+f+1)^3} \end{aligned}$$

Eine erste nennerfreie Darstellung der 14-Torsionskurve lautet also:

$$\begin{aligned} &y^2+((e+f+1)(f^2+2f+3-e)-f-2)\,xy\\ &+(1-e)(e+f)(e+f+1)(f+1)^3(ef+f^2+f+1)\,y\\ &=x^3+(1-e)(e+f)(f+1)(ef+f^2+f+1)\,x^2 \end{aligned}$$

Ersetzt man in den Koeffizienten

$$f^n=f^{n-2}f^2=f^{n-2}(-e^2f-ef-e)\quad\text{für } n\geq 2$$

und anschließend

$$e^ne^2f=e^n(-f^2-ef-e)\quad\text{für } n\geq 0,$$

so erhält man die zweite nennerfreie Darstellung

$$\begin{aligned} &y^2+(1-e)(e(f+1)^2+f^2+4f+1)\,xy\\ &+(1-e)^3(e+1)f(e+f+1)(f+1)^2(ef+f+1)\,y\\ &=x^3+(1-e)^3(e+1)f(ef+f+1)\,x^2. \end{aligned}$$

Die Potenzen von $(1-e)$ können aus den Koeffizienten entfernt werden:

$$\begin{aligned} x&\mapsto x(1-e)^2\\ y&\mapsto y(1-e)^3 \end{aligned}$$

Die allgemeine Darstellung einer elliptischen Kurve mit 14-Torsionspunkt $(0,0)$ lautet somit

$$\begin{aligned} &E_{14}\colon\ y^2+(2f+(e+1)(f+1)^2)\,xy+(e+1)(e+f+1)(ef+f+1)f(f+1)^2\,y\\ &=x^3+(1-e)(e+1)(ef+f+1)f\,x^2 \end{aligned}$$

unter der Nebenbedingung $\chi_{14}(e,f)=f^2+(e^2+e)f+e=0$. Der Algorithmus 2.1 liefert als optimierte Faktorisierung der Diskriminante:

$$\operatorname{disc}(E_{14})=(e+1)^7\cdot(e-1)^3\cdot(e+f+1)^2\cdot f^{14}\cdot(-2ef+f^2+2f-1)$$

Um zu bestimmen, wann diese Diskriminante unter der Nebenbedingung $\chi_{14}(e,f)=0$ verschwindet, werden die Resultanten bezüglich der Variablen e und f betrachtet:

$$\begin{aligned}\operatorname{res}_e(\operatorname{disc}(E_{14}),\chi_{14}) &= (e-1)^7\cdot e^{14}\cdot(e+1)^{14}\cdot(e^3+e^2-9e-1)\cdot(e^3+e^2-2e-1)^2\\ \operatorname{res}_f(\operatorname{disc}(E_{14}),\chi_{14}) &= (f-1)^7\cdot f^{23}\cdot(f+1)^{14}\cdot(f^3+9f^2-f-1)\cdot(f^3+2f^2-f-1)^2\end{aligned}$$

Die f-Resultante besitzt die Nullstellen

$$\begin{aligned}f_1 &= 1,\quad f_2=-1,\quad f_3=0,\\ f_4 &= \frac{4}{3}\sqrt{21}\sin\left(\frac{1}{3}\arctan\left(3\sqrt{3}\right)\right)-3,\\ f_5 &= -\frac{4}{3}\sqrt{21}\sin\left(\frac{1}{3}\arctan\left(3\sqrt{3}\right)+\frac{\pi}{3}\right)-3,\\ f_6 &= \frac{4}{3}\sqrt{21}\cos\left(\frac{1}{3}\arctan\left(3\sqrt{3}\right)+\frac{\pi}{6}\right)-3,\\ f_7=H(f_4) &= \frac{2}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{6}\right)-\frac{2}{3},\\ f_8=H(f_5) &= -\frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{3}\right)-\frac{2}{3},\\ f_9=H(f_6) &= \frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right)-\frac{2}{3}\qquad \text{mit } H(f)\stackrel{\text{def}}{=}-\frac{1}{4}f^2-2f+\frac{1}{4};\end{aligned}$$

ist nämlich $\overline{f}$ eine Nullstelle von f^3+9f^2-f-1, dann ist $H(\overline{f})$ eine Nullstelle von f^3+2f^2-f-1 wegen

$$H(\overline{f})^3+2H(\overline{f})^2-H(\overline{f})-1=-\frac{1}{64}\cdot(\overline{f}^3+9\overline{f}^2-\overline{f}-1)\cdot(\overline{f}^3+15\overline{f}^2+47\overline{f}-71)=0.$$

Die e-Resultante besitzt die Nullstellen

$$\begin{aligned}e_1 &= 1,\quad e_2=0,\quad e_3=-1,\\ e_4=T(f_4) &= \frac{4}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{6}\right)-\frac{1}{3},\\ e_5=T(f_5) &= -\frac{4}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{3}\right)-\frac{1}{3},\\ e_6=T(f_6) &= \frac{4}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right)-\frac{1}{3}\qquad \text{mit } T(f)\stackrel{\text{def}}{=}-\frac{1}{2}f^2-4f+\frac{3}{2},\\ e_7=L(e_4) &= -\frac{2}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{6}\right)-\frac{1}{3},\\ e_8=L(e_5) &= \frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{3}\right)-\frac{1}{3},\\ e_9=L(e_6) &= -\frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right)-\frac{1}{3}\qquad \text{mit } L(e)\stackrel{\text{def}}{=}-\frac{1}{2}e-\frac{1}{2}.\end{aligned}$$

Die Beziehungen $e_{4/5/6}=T(f_{4/5/6})$ entstehen wie folgt: Ist $\overline{f}$ eine Nullstelle von f^3+9f^2-f-1, dann ist $T(\overline{f})$ eine Nullstelle von e^3+e^2-9e-1 wegen

$$T(\overline{f})^3+T(\overline{f})^2-9T(\overline{f})-1=-\frac{1}{8}\cdot(\overline{f}^3+9\overline{f}^2-\overline{f}-1)\cdot(\overline{f}^3+15\overline{f}^2+47\overline{f}-71)=0.$$

Die Definition $e=T(f)=-\frac{1}{2}f^2-4f+\frac{3}{2}$ ist modulo f^3+9f^2-f-1 identisch zu $e=T(f)=(f^2+2f-1)(2f)^{-1}$, und dieser Zusammenhang folgt aus dem Diskriminantenfaktor $-2ef+f^2+2f-1$. Die Beziehungen $e_{7/8/9}=L(e_{4/5/6})$ folgen aus dem linearen Zusammenhang $Q(L(e))\equiv-\frac{1}{8}P(e)$ für die Resultantenfaktoren $P(e)\stackrel{\text{def}}{=}e^3+e^2-9e-1$ und $Q(e)\stackrel{\text{def}}{=}e^3+e^2-2e-1$.

Unter den 81 Paaren (e_i,f_j) für $i,j\in\{1,\ldots,9\}$ lassen nur 7 Paare sowohl die Diskriminante

$\operatorname{disc}(E_{14})$ als auch die Kurvengleichung $\chi_{14}(e,f)$ verschwinden:

$$
\begin{aligned}
&(e_2, f_3) = (0,\ 0),\\
&(e_1, f_2) = (1,\ -1),\\
&(e_3, f_1) = (-1,\ 1),\\
&(e_3, f_2) = (-1,\ -1),\\
&(e_7, f_7) = \left(-\frac{2}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{6}\right)-\frac{1}{3},\quad \frac{2}{3}\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{6}\right)-\frac{2}{3}\right),\\
&(e_8, f_8) = \left(\ \frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{3}\right)-\frac{1}{3},\ -\frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)+\frac{\pi}{3}\right)-\frac{2}{3}\right),\\
&(e_9, f_9) = \left(-\frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right)-\frac{1}{3},\ \frac{2}{3}\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{1}{9}\sqrt{3}\right)\right)-\frac{2}{3}\right). \qquad \square
\end{aligned}
$$

Beispiel 5.2 (14-Torsionskurve) *Eine Beispielkurve aus dieser Familie erhält man für*

$$e = 2,\ f = \sqrt{7} - 3;$$

die elliptische Kurve

$$y^2 + (27 - 10\sqrt{7})\,xy + (2913\sqrt{7} - 7707)\,y = x^3 + (51\sqrt{7} - 135)\,x^2$$

besitzt den 14-Torsionspunkt $(0,0)$.

6 Die 15-Torsionskurve

Theorem 6.1 (Nennerfreie 15-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 15-Torsionspunkt $(0,0)$ *lautet*

$$
\begin{aligned}
E_{15}\colon\ & y^2 + (1 - (e+f+1)(e^2+ef+2e+f+2))\,xy\\
& - e(e+1)^2(e+f+1)^2(1-e^2f)\,y = x^3 + e(e+1)(1-e^2f)\,x^2
\end{aligned}
$$

für Parameter $e, f \in \mathbb{C}$*, die auf der Kurve*

$$X_1(15)\colon\ \chi_{15}(e,f) \overset{def}{:=} e^2 + f^2 + (e^2+e+1)f = 0$$

liegen.

(b) Die Diskriminante

$$
\begin{aligned}
\operatorname{disc}(E_{15}) = {} & (e+1)^5\cdot(f+1)^{15}\cdot(1-e^2f)^3\cdot(e^2+e+f)^{11}\cdot(e+f)^2\cdot f\\
& \cdot(ef+2e-2f-1)
\end{aligned}
$$

verschwindet unter der Nebenbedingung $\chi_{15}(e,f) = 0$ *genau für die folgenden 10 Parameterpaare:*

$$
\begin{aligned}
(e,f) \in \Bigg\{ & (0,\ 0),\ (0,\ -1),\ \left(-1,\ -\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\ \left(-1,\ -\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right),\\
& \left(\frac{1}{2}+\frac{1}{2}i\sqrt{3},\ -\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right),\ \left(\frac{1}{2}-\frac{1}{2}i\sqrt{3},\ -\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\\
& \left(-\frac{1}{4}+\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}-\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}}\right),\\
& \left(-\frac{1}{4}+\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}-\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}}\right),\\
& \left(-\frac{1}{4}-\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}+\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}}\right),\\
& \left(-\frac{1}{4}-\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}+\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}}\right)\Bigg\}.
\end{aligned}
$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 15-Torsionspunkt $(0,0)$ an:

$$\begin{aligned} E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\ & b=rs(r-1)\\ & c=s(r-1)\\ & r=1+\frac{ef+f^2}{e^2(e+f+1)}\\ & s=1+\frac{f}{e(e+1)}\\ & X_1(15)\colon\ e^2+f^2+(e^2+e+1)f=0 \end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned} 1-c&=\frac{e^5+e^4(f+2)+e^3-e^2f(f+1)-2ef^2-f^3}{e^3(e+1)(e+f+1)}\\ -b&=\frac{-f(e+f)(e^2+e+f)(e^3+e^2(f+1)+ef+f^2)}{e^5(e+1)(e+f+1)^2} \end{aligned}$$

Der Zähler von $(1-c)$ lässt sich modulo $e^2+f^2+(e^2+e+1)f=0$ faktorisieren:

$$1-c=\frac{-f(e^2+e+f)(e^3+ef^2+e^2+2ef-f^2+4e+f+1)}{e^3(e+1)(e+f+1)}$$

Diese Darstellung wird noch kompakter, wenn man $f^2=-e^2-(e^2+e+1)f$ ersetzt:

$$1-c=\frac{f(e^2+e+f)(e^3f-2e^2-2e(f+2)-2f-1)}{e^3(e+1)(e+f+1)}$$

Modulo $e^2+f^2+(e^2+e+1)f=0$ gibt es verschiedene Darstellungen von $-b$. Gewählt wird eine Form, in der Faktoren von $(1-c)$ kubisch ausgeklammert werden können. Im Zähler kann $f^3(e^2+e+f)^3$ ausgeklammert werden, wenn man im Nenner zusätzliche Terme hinzufügt:

$$-b=\frac{-f^3(e^2+e+f)^3(e^3+2ef^2+f^3-e^2+e+1)}{e^8(e+1)(e+f+1)^2}$$

Eine nennerfreie und um den gemeinsamen Faktor $f(e^2+e+f)$ reduzierte Darstellung von $E(b,c)$ erhält man durch Substitution

$$\begin{aligned} x&\mapsto x\cdot\frac{f^2(e^2+e+f)^2}{e^6(e+1)^2(e+f+1)^2}\\ y&\mapsto y\cdot\frac{f^3(e^2+e+f)^3}{e^9(e+1)^3(e+f+1)^3} \end{aligned}$$

Eine nennerfreie Darstellung der 15-Torsionskurve lautet somit:

$$\begin{aligned} &y^2+(e^3f-2e^2-2ef-4e-2f-1)\,xy\\ &-e(e+1)^2(e+f+1)(e^3+2ef^2+f^3-e^2+e+1)\,y\\ &=x^3+(e^4-ef^2-f^3+e^2-f^2+e)\,x^2 \end{aligned}$$

Der erste Koeffizient lässt sich additiv schreiben:

$$e^3f-2e^2-2ef-4e-2f-1=1-(e+f+1)(e^2+ef+2e+f+2)$$

Der zweite Koeffizient lässt sich faktorisieren in:

$$\begin{aligned} &-e(e+1)^2(e+f+1)(e^3+2ef^2+f^3-e^2+e+1)\\ &=-e(e+1)^2(e+f+1)^2(e^2+ef+f^2+f+1)\\ &=-e(e+1)^2(e+f+1)^2(1-e^2f) \end{aligned}$$

Ersetzt man im dritten Koeffizienten

$$f^2 = -e^2 - (e^2+e+1)f \quad \text{und}$$
$$f^3 = f \cdot f^2 = e^4 f + e^4 + 2e^3 f + e^3 + 2e^2 f + e^2 + 2ef + f,$$

so erhält man die Faktorisierung

$$e^4 - ef^2 - f^3 + e^2 - f^2 + e = e(e+1)(1-e^2 f).$$

Die Gleichung einer elliptischen Kurve mit 15-Torsionspunkt $(0,0)$ lautet also

$$\begin{aligned} E_{15}\colon\, & y^2 + (1-(e+f+1)(e^2+ef+2e+f+2))\,xy - e(e+1)^2(e+f+1)^2(1-e^2 f)\,y \\ & = x^3 + e(e+1)(1-e^2 f)\,x^2 \end{aligned}$$

mit der Nebenbedingung

$$\chi_{15}(e,f) = e^2 + f^2 + (e^2+e+1)f = 0.$$

Der Algorithmus 2.1 liefert als optimierte Faktorisierung der Diskriminante:

$$\operatorname{disc}(E_{15}) = (e+1)^5 \cdot (f+1)^{15} \cdot (1-e^2 f)^3 \cdot (e^2+e+f)^{11} \cdot (e+f)^2 \cdot f \cdot (ef+2e-2f-1)$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{15})$ unter der Nebenbedingung $\chi_{15}(e,f) = 0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned} \operatorname{res}_e(\operatorname{disc}(E_{15}), \chi_{15}) = & -(e+1)^{10} \cdot e^{30} \cdot (e^2-e+1)^5 \cdot (e^4+e^3-9e^2+e+1) \\ & \cdot (e^4+e^3+e^2+e+1)^3 \\ \operatorname{res}_f(\operatorname{disc}(E_{15}), \chi_{15}) = & (f+1)^{22} \cdot f^{15} \cdot (f^2+f+1)^{10} \cdot (f^4+11f^3+21f^2+11f+1) \\ & \cdot (f^4+f^3+f^2+f+1)^3 \end{aligned}$$

Die Resultanten besitzen die Nullstellen

$$\begin{aligned} e_1 = -1, \qquad e_2 = 0, \qquad e_{3/4} &= \frac{1}{2} \pm \frac{1}{2} i\sqrt{3}, \\ e_{5/6} &= -\frac{1}{4} - \frac{3}{4}\sqrt{5} \pm \sqrt{\frac{15}{8} + \frac{3}{8}\sqrt{5}}, \\ e_{7/8} &= -\frac{1}{4} + \frac{3}{4}\sqrt{5} \pm \sqrt{\frac{15}{8} - \frac{3}{8}\sqrt{5}}, \\ e_{9/10} &= -\frac{1}{4} + \frac{1}{4}\sqrt{5} \pm i\sqrt{\frac{5}{8} + \frac{1}{8}\sqrt{5}}, \\ e_{11/12} &= -\frac{1}{4} - \frac{1}{4}\sqrt{5} \pm i\sqrt{\frac{5}{8} - \frac{1}{8}\sqrt{5}}; \\ f_1 = 0, \qquad f_2 = -1, \qquad f_{3/4} &= -\frac{1}{2} \pm \frac{1}{2} i\sqrt{3}, \\ f_{5/6} &= -\frac{11}{4} - \frac{3}{4}\sqrt{5} \pm \sqrt{\frac{75}{8} + \frac{33}{8}\sqrt{5}}, \\ f_{7/8} &= -\frac{11}{4} + \frac{3}{4}\sqrt{5} \pm \sqrt{\frac{75}{8} - \frac{33}{8}\sqrt{5}}, \\ f_{9/10/11/12} &= e_{9/10/11/12}. \end{aligned}$$

Unter den 144 Paaren (e_i, f_j) für $i,j \in \{1,\ldots,12\}$ lassen nur die folgenden 10 Paare sowohl die

Diskriminante $\operatorname{disc}(E_{15})$ als auch die Kurvengleichung $\chi_{15}(e,f)$ verschwinden:

$$
\begin{aligned}
(e_2, f_1) &= (0,\ 0),\\
(e_2, f_2) &= (0,\ -1),\\
(e_1, f_3) &= \left(-1,\ -\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\\
(e_1, f_4) &= \left(-1,\ -\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right),\\
(e_3, f_4) &= \left(\frac{1}{2}+\frac{1}{2}i\sqrt{3},\ -\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right),\\
(e_4, f_3) &= \left(\frac{1}{2}-\frac{1}{2}i\sqrt{3},\ -\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right),\\
(e_9, f_{12}) &= \left(-\frac{1}{4}+\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}-\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}}\right),\\
(e_{10}, f_{11}) &= \left(-\frac{1}{4}+\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}-\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}}\right),\\
(e_{11}, f_9) &= \left(-\frac{1}{4}-\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}+\frac{1}{4}\sqrt{5}+i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}}\right),\\
(e_{12}, f_{10}) &= \left(-\frac{1}{4}-\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}-\frac{1}{8}\sqrt{5}},\ -\frac{1}{4}+\frac{1}{4}\sqrt{5}-i\sqrt{\frac{5}{8}+\frac{1}{8}\sqrt{5}}\right). \qquad \square
\end{aligned}
$$

Beispiel 6.2 (15-Torsionskurve) *Eine Beispielkurve aus dieser Familie erhält man für die Parameter*

$$e = 1,\ f = \frac{1}{2}\sqrt{5}-\frac{3}{2};$$

die elliptische Kurve

$$y^2 - \left(\frac{3}{2}\sqrt{5}+\frac{5}{2}\right)xy - \left(2\sqrt{5}+10\right)y = x^3 + \left(5-\sqrt{5}\right)x^2$$

besitzt den 15-Torsionspunkt $(0,0)$.

Beweis. Es handelt sich um einen echten 15-Torsionspunkt, da

$$
\begin{aligned}
3\cdot(0,0) &= \left(-1-\sqrt{5},\ 2-2\sqrt{5}\right),\\
5\cdot(0,0) &= \left(-\frac{5}{2}-\frac{1}{2}\sqrt{5},\ -\frac{5}{2}-\frac{1}{2}\sqrt{5}\right),\\
15\cdot(0,0) &= \mathcal{O}. \qquad \square
\end{aligned}
$$

7 Die 16-Torsionskurve

Theorem 7.1 (Nennerfreie 16-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 16-Torsionspunkt $(0,0)$ *lautet*

$$
\begin{aligned}
E_{16}\colon\ & y^2 + (e^2f^2 + 2e^2f - e^2 + f^2 + 2f + 1)\,xy\\
&\quad + (e-f)(e-f-1)e^2(f+1)f(e^2+e-f-1)\,y\\
&\quad = x^3 - (e-f)(e-f-1)e^2(f+1)f\,x^2
\end{aligned}
$$

für Parameter $e, f \in \mathbb{C}$*, die auf der Kurve*

$$X_1(16)\colon \chi_{16}(e,f) \overset{\text{def}}{=} e^2 + f^2 + (e^3+e^2-e+1)f = 0$$

liegen.

(b) Die Diskriminante

$$\begin{aligned}\operatorname{disc}(E_{16}) = &-(e-f)^4\cdot(e-f-1)^9\cdot f^6\cdot(f+1)^4\cdot(e-1)^2\cdot(e^2-2e-1)\\ &\cdot(e^2+2e-1)\cdot(e^2f+2ef+e+1)\end{aligned}$$

verschwindet unter der Nebenbedingung $\chi_{16}(e,f)=0$ genau für die folgenden 12 Parameterpaare:

$$\begin{aligned}(e,f)\in\{&(0,\,0),\,(0,\,-1),\,(1,\,-1),\,(-1,\,-1),\,(i,\,i),\,(-i,\,-i),\\ &(-1+\sqrt{2},\,1-\sqrt{2}),\,(-1-\sqrt{2},\,1+\sqrt{2}),\\ &\left(1+\sqrt{2},\,-5-3\sqrt{2}+\sqrt{40+28\sqrt{2}}\right),\,\left(1+\sqrt{2},\,-5-3\sqrt{2}-\sqrt{40+28\sqrt{2}}\right),\\ &\left(1-\sqrt{2},\,-5+3\sqrt{2}+\sqrt{40-28\sqrt{2}}\right),\,\left(1-\sqrt{2},\,-5+3\sqrt{2}-\sqrt{40-28\sqrt{2}}\right)\Big\}.\end{aligned}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 16-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\ & b=rs(r-1)\\ & c=s(r-1)\\ & r=\frac{e^2-ef+f^2+f}{e^2+e-f-1}\\ & s=\frac{e-f}{e+1}\\ & X_1(16)\colon\ e^2+f^2+(e^3+e^2-e+1)f=0\end{aligned}$$

Damit erhält man folgende Koeffizienten:

$$1-c=\frac{e^3+e^2(f+3)-e(2f^2+4f+1)+(f+1)(f^2+f-1)}{(e+1)(e^2+e-f-1)}$$

Ein Faktor im Nenner fällt modulo $X_1(16)$ weg:

$$1-c=-\frac{e^2f^2+2e^2f-e^2+f^2+2f+1}{e^2+e-f-1}$$

Für den anderen Koeffizienten gilt:

$$-b=\frac{(e-f)(e-f-1)(e^2-ef+f^2+f)(f+1)}{(e+1)(e^2+e-f-1)^2}$$

Auch hier fällt modulo $X_1(16)$ derselbe Faktor weg:

$$-b=\frac{(e-f)(-1)(e-f-1)e^2(f+1)f}{(e^2+e-f-1)^2}$$

Eine nennerfreie Darstellung erhält man durch Substitution

$$\begin{aligned}x&\mapsto\frac{x}{(e^2+e-f-1)^2(-1)^2}\\ y&\mapsto\frac{y}{(e^2+e-f-1)^3(-1)^3}\end{aligned}$$

Eine nennerfreie Darstellung einer elliptischen Kurve mit 16-Torsionspunkt $(0,0)$ lautet also

$$\begin{aligned}E_{16}\colon\ & y^2+(e^2f^2+2e^2f-e^2+f^2+2f+1)\,xy\\ &+(e-f)(e-f-1)e^2(f+1)f(e^2+e-f-1)\,y\\ &=x^3-(e-f)(e-f-1)e^2(f+1)f\,x^2\end{aligned}$$

mit der Nebenbedingung

$$\chi_{16}(e,f) = e^2 + f^2 + (e^3 + e^2 - e + 1)f = 0.$$

Der Algorithmus 2.1 liefert als optimierte Faktorisierung der Diskriminante:

$$\begin{aligned}\operatorname{disc}(E_{16}) = &-(e-f)^4 \cdot (e-f-1)^9 \cdot f^6 \cdot (f+1)^4 \cdot (e-1)^2 \cdot (e^2-2e-1) \cdot (e^2+2e-1) \\ &\cdot (e^2 f + 2ef + e + 1)\end{aligned}$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{16})$ unter der Nebenbedingung $\chi_{16}(e,f) = 0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned}\operatorname{res}_e(\operatorname{disc}(E_{16}), \chi_{16}) &= e^{56} \cdot (e-1)^8 \cdot (e+1)^8 \cdot (e^2-2e-1)^2 \cdot (e^2+2e-1)^2 \cdot (e^2+1)^4 \\ \operatorname{res}_f(\operatorname{disc}(E_{16}), \chi_{16}) &= -f^{29} \cdot (f+1)^{56} \cdot (f^2-2f-1)^2 \cdot (f^2+1)^4 \\ &\quad \cdot (f^4 + 20f^3 + 34f^2 + 12f + 1)\end{aligned}$$

Die Resultanten besitzen die Nullstellen

$$\begin{aligned}&e_1 = 0, \qquad e_{2/3} = \pm 1, \qquad e_{4/5} = 1 \pm \sqrt{2}, \qquad e_{6/7} = -1 \pm \sqrt{2}, \qquad e_{8/9} = \pm i; \\ &f_1 = 0, \qquad f_2 = -1, \qquad f_{3/4} = 1 \pm \sqrt{2}, \qquad f_{5/6} = \pm i, \\ &f_{7/8} = -5 - 3\sqrt{2} \pm \sqrt{40 + 28\sqrt{2}}, \qquad f_{9/10} = -5 + 3\sqrt{2} \pm \sqrt{40 - 28\sqrt{2}}.\end{aligned}$$

Unter den 90 Paaren (e_i, f_j), $i \in \{1,\dots,9\}$, $j \in \{1,\dots,10\}$ lassen nur die folgenden 12 Paare sowohl die Diskriminante $\operatorname{disc}(E_{16})$ als auch die Kurvengleichung $\chi_{16}(e,f)$ verschwinden:

$$\begin{aligned}(e_1, f_1) &= (0,\ 0), \\ (e_1, f_2) &= (0,\ -1), \\ (e_2, f_2) &= (1,\ -1), \\ (e_3, f_2) &= (-1,\ -1), \\ (e_8, f_5) &= (i,\ i), \\ (e_9, f_6) &= (-i,\ -i), \\ (e_6, f_4) &= (-1+\sqrt{2},\ 1-\sqrt{2}), \\ (e_7, f_3) &= (-1-\sqrt{2},\ 1+\sqrt{2}), \\ (e_4, f_7) &= \left(1+\sqrt{2},\ -5-3\sqrt{2}+\sqrt{40+28\sqrt{2}}\right), \\ (e_4, f_8) &= \left(1+\sqrt{2},\ -5-3\sqrt{2}-\sqrt{40+28\sqrt{2}}\right), \\ (e_5, f_9) &= \left(1-\sqrt{2},\ -5+3\sqrt{2}+\sqrt{40-28\sqrt{2}}\right), \\ (e_5, f_{10}) &= \left(1-\sqrt{2},\ -5+3\sqrt{2}-\sqrt{40-28\sqrt{2}}\right). \qquad \square\end{aligned}$$

Beispiel 7.2 (16-Torsionskurve) *Eine Beispielkurve aus dieser Familie erhält man für die Parameter*

$$e = 2,\ f = \frac{1}{2}\sqrt{105} - \frac{11}{2};$$

die elliptische Kurve

$$y^2 + \left(\frac{449}{2} - \frac{45}{2}\sqrt{105}\right) xy + (468720 - 45744\sqrt{105})\, y = x^3 + (2928\sqrt{105} - 30000)\, x^2$$

besitzt den 16-Torsionspunkt $(0,0)$.

Beweis. Es handelt sich um einen echten 16-Torsionspunkt, da

$$\begin{aligned}2 \cdot (0,0) &= (30000 - 2928\sqrt{105},\ -14121120 + 1378080\sqrt{105}), \\ 4 \cdot (0,0) &= (7128 - 696\sqrt{105},\ -2915712 + 284544\sqrt{105}), \\ 8 \cdot (0,0) &= (-496 + 48\sqrt{105},\ -121984 + 11904\sqrt{105}), \\ 16 \cdot (0,0) &= \mathcal{O}. \qquad \square\end{aligned}$$

8 Die 17-Torsionskurve

Theorem 8.1 (Nennerfreie 17-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 17-Torsionspunkt $(0,0)$ lautet

$$\begin{aligned} E_{17}\colon\, & y^2 + (e^3+e^2(3f+2) - e(f^2-2f-1) - f(f^2+3f+1))\,xy \\ & + f(e+1)(e-f)(e+f+1)^2(e^2+e-f)(e^2+ef+e-f^2-f)\,y \\ & = x^3 + f(e+1)(e-f)(e+f+1)(e^2+e-f)\,x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$, die auf der Kurve

$$X_1(17)\colon\, \chi_{17}(e,f) \overset{\text{def}}{=} f^4 + (e^3+e^2-e+2)f^3 + (e^3-3e+1)f^2 - (e^4+2e)f + (e^3+e^2) = 0$$

liegen.

(b) Die Diskriminante

$$\begin{aligned} \operatorname{disc}(E_{17}) = {} & (f+1)^6\cdot(e^2+e-f)^7\cdot(e+f+1)^3\cdot(e-f)^7\cdot(4e^2f^6+ef^7+7e^2f^5 \\ & + 6ef^6 - f^7 - 4e^4f^2 - 2e^2f^4 + ef^5 - 12f^6 + 9e^3f^2 - 7e^2f^3 - 18ef^4 \\ & - 30f^5 + 12e^3f + 3e^2f^2 - 17ef^3 - 16f^4 - 4e^2f - 11ef^2 + 25f^3 - 8e^2 \\ & - 17ef + 32f^2 - 9e + 10f) \end{aligned}$$

verschwindet unter der Nebenbedingung $\chi_{17}(e,f) = 0$ genau für die folgenden 12 Parameterpaare:

$$\begin{aligned} (e,f) \in \{ & (0,\,0),(0,\,-1),(-1,\,0),(-1,\,-1),(e_1,\,f_5),(e_2,\,f_7), \\ & (e_3,\,f_2),(e_4,\,f_4),(e_5,\,f_6),(e_6,\,f_3),(e_7,\,f_1),(e_8,\,f_8)\}. \end{aligned}$$

Dabei sind die Parameterwerte e_1, e_3, e_6 und e_8 die Nullstellen von

$$\begin{aligned} & e^4 + \left(-\frac{5}{2} - \frac{1}{2}\sqrt{17}\right)e^3 + (-12-2\sqrt{17})\,e^2 + \left(-\frac{7}{2} - \frac{1}{2}\sqrt{17}\right)e + (4+\sqrt{17}): \\ & e_1 \approx -2.374, \quad e_3 \approx -0.942, \quad e_6 \approx 0.492, \quad e_8 \approx 7.385. \end{aligned}$$

Weiterhin sind die Parameterwerte e_2, e_4, e_5 und e_7 die Nullstellen von

$$\begin{aligned} & e^4 + \left(-\frac{5}{2} + \frac{1}{2}\sqrt{17}\right)e^3 + (-12+2\sqrt{17})\,e^2 + \left(-\frac{7}{2} + \frac{1}{2}\sqrt{17}\right)e + (4-\sqrt{17}): \\ & e_2 \approx -1.480, \quad e_4 \approx -0.282, \quad e_5 \approx -0.127, \quad e_7 \approx 2.327. \end{aligned}$$

Die Werte f_{1-8} sind definiert durch $f_{5/7/2/4/6/3/1/8} = \varphi(e_{1/2/3/4/5/6/7/8})$ mit

$$\varphi(e) \overset{\text{def}}{=} \frac{1}{17}\,(-e^7 + 4e^6 + 29e^5 - 8e^4 - 146e^3 - 102e^2 + 37e + 4).$$

Die Parameterwerte f_2, f_3, f_5 und f_8 sind damit die Nullstellen von

$$\begin{aligned} & f^4 + (9-2\sqrt{17})\,f^3 + \left(-\frac{3}{2} - \frac{1}{2}\sqrt{17}\right)f^2 + \left(-\frac{13}{2} + \frac{1}{2}\sqrt{17}\right)f - 1: \\ & f_2 \approx -1.393, \quad f_3 \approx -1.145, \quad f_5 \approx -0.301, \quad f_8 \approx 2.085. \end{aligned}$$

Weiterhin sind die Parameterwerte f_1, f_4, f_6 und f_7 die Nullstellen von

$$\begin{aligned} & f^4 + (9+2\sqrt{17})\,f^3 + \left(-\frac{3}{2} + \frac{1}{2}\sqrt{17}\right)f^2 + \left(-\frac{13}{2} - \frac{1}{2}\sqrt{17}\right)f - 1: \\ & f_1 \approx -17.185, \quad f_4 \approx -0.670, \quad f_6 \approx -0.119, \quad f_7 \approx 0.728. \end{aligned}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 17-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}
E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\
& b=rs(r-1)\\
& c=s(r-1)\\
& r=\frac{e^2+e-f}{e^2+ef+e-f^2-f}\\
& s=\frac{e+1}{e+f+1}\\
& X_1(17)\colon\ f^4+(e^3+e^2-e+2)f^3+(e^3-3e+1)f^2-(e^4+2e)f+e^3+e^2=0
\end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned}
1-c&=-\frac{f^3+f^2(e+3)+f(e+1)(1-3e)-e(e+1)^2}{(e+f+1)(e^2+ef+e-f^2-f)}\\
-b&=\frac{f(e+1)(e-f)(e^2+e-f)}{(e+f+1)(e^2+ef+e-f^2-f)^2}
\end{aligned}$$

Eine nennerfreie Darstellung von $E(b,c)$ erhält man durch Substitution

$$\begin{aligned}
x&\mapsto\frac{x}{(e+f+1)^2(e^2+ef+e-f^2-f)^2}\\
y&\mapsto\frac{y}{(e+f+1)^3(e^2+ef+e-f^2-f)^3}
\end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 17-Torsionspunkt $(0,0)$ lautet also

$$\begin{aligned}
E_{17}\colon\ & y^2+(e^3+e^2(3f+2)-e(f^2-2f-1)-f(f^2+3f+1))\,xy\\
&+f(e+1)(e-f)(e+f+1)^2(e^2+e-f)(e^2+ef+e-f^2-f)\,y\\
&=x^3+f(e+1)(e-f)(e+f+1)(e^2+e-f)\,x^2
\end{aligned}$$

mit der Nebenbedingung

$$\chi_{17}(e,f)=f^4+(e^3+e^2-e+2)f^3+(e^3-3e+1)f^2-(e^4+2e)f+(e^3+e^2)=0.$$

Der Algorithmus 2.1 liefert als optimale Faktorisierung der Diskriminante:

$$\begin{aligned}
\operatorname{disc}(E_{17})=&(f+1)^6\cdot(e^2+e-f)^7\cdot(e+f+1)^3\cdot(e-f)^7\cdot(4e^2f^6+ef^7+7e^2f^5+6ef^6\\
&-f^7-4e^4f^2-2e^2f^4+ef^5-12f^6+9e^3f^2-7e^2f^3-18ef^4-30f^5+12e^3f\\
&+3e^2f^2-17ef^3-16f^4-4e^2f-11ef^2+25f^3-8e^2-17ef+32f^2-9e+10f)
\end{aligned}$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{17})$ unter der Nebenbedingung $\chi_{17}(e,f)=0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned}
&\operatorname{res}_e(\operatorname{disc}(E_{17}),\chi_{17})=e^{99}\cdot(e+1)^{58}\cdot(e^8-5e^7-22e^6+19e^5+93e^4+47e^3-20e^2-11e-1)\\
&=e^{99}(e+1)^{58}\cdot\left[e^4+\left(-\frac{5}{2}-\frac{1}{2}\sqrt{17}\right)e^3+(-12-2\sqrt{17})\,e^2+\left(-\frac{7}{2}-\frac{1}{2}\sqrt{17}\right)e+(4+\sqrt{17})\right]\\
&\qquad\cdot\left[e^4+\left(-\frac{5}{2}+\frac{1}{2}\sqrt{17}\right)e^3+(-12+2\sqrt{17})\,e^2+\left(-\frac{7}{2}+\frac{1}{2}\sqrt{17}\right)e+(4-\sqrt{17})\right]
\end{aligned}$$

$$\begin{aligned}
&\operatorname{res}_f(\operatorname{disc}(E_{17}),\chi_{17})\\
&=f^{118}\cdot(f+1)^{51}\cdot(f^8+18f^7+10f^6-74f^5-87f^4+10f^3+41f^2+13f+1)\\
&=f^{118}\cdot(f+1)^{51}\cdot\left[f^4+(9-2\sqrt{17})\,f^3+\left(-\frac{3}{2}-\frac{1}{2}\sqrt{17}\right)f^2+\left(-\frac{13}{2}+\frac{1}{2}\sqrt{17}\right)f-1\right]\\
&\qquad\cdot\left[f^4+(9+2\sqrt{17})\,f^3+\left(-\frac{3}{2}+\frac{1}{2}\sqrt{17}\right)f^2+\left(-\frac{13}{2}-\frac{1}{2}\sqrt{17}\right)f-1\right]
\end{aligned}$$

Die Resultanten besitzen die Nullstellen

$$\begin{array}{lllll} e_1 \approx -2.374, & e_2 \approx -1.480, & e_3 \approx -0.942, & e_4 \approx -0.282, & e_5 \approx -0.127, \\ e_6 \approx 0.492, & e_7 \approx 2.327, & e_8 \approx 7.385, & e_9 = 0, & e_{10} = -1; \\ f_1 \approx -17.185, & f_2 \approx -1.393, & f_3 \approx -1.145, & f_4 \approx -0.670, & f_5 \approx -0.301, \\ f_6 \approx -0.119, & f_7 \approx 0.728, & f_8 \approx 2.085, & f_9 = 0, & f_{10} = -1. \end{array}$$

Unter den 100 Parameterpaaren (e_i, f_j), $i, j \in \{1, \dots, 10\}$ lassen nur die folgenden 12 Paare sowohl die Diskriminante $\operatorname{disc}(E_{17})$ als auch die Kurvengleichung $\chi_{17}(e, f)$ verschwinden:

$$\begin{aligned}(e, f) \in \{&(0,\ 0), (0,\ -1), (-1,\ 0), (-1,\ -1), (e_1,\ f_5), (e_2,\ f_7),\\ &(e_3,\ f_2), (e_4,\ f_4), (e_5,\ f_6), (e_6,\ f_3), (e_7,\ f_1), (e_8,\ f_8)\}.\end{aligned}$$

Die Koeffizienten der Transformation φ erhält man durch Interpolation durch die Punkte $(e_1,\ f_5)$, $(e_2,\ f_7)$, $(e_3,\ f_2)$, $(e_4,\ f_4)$, $(e_5,\ f_6)$, $(e_6,\ f_3)$, $(e_7,\ f_1)$, $(e_8,\ f_8)$. □

Beispiel 8.2 (17-Torsionskurve) *Ein Beispiel aus dieser Kurvenfamilie findet man durch den Ansatz* $e = f + 1$*:*

$$\begin{aligned} e &= \frac{1}{4}\sqrt{2\sqrt{41} + 10} + \frac{1}{2} + \frac{1}{4}i\sqrt{2\sqrt{41} - 10}, \\ f &= \frac{1}{4}\sqrt{2\sqrt{41} + 10} - \frac{1}{2} + \frac{1}{4}i\sqrt{2\sqrt{41} - 10}; \end{aligned}$$

damit besitzt die elliptische Kurve

$$\begin{aligned} &y^2 + \frac{1}{4}\left(30 + 24i + \sqrt{106\sqrt{41} + 226} + i\sqrt{106\sqrt{41} - 226}\right) xy \\ &+ \left(-92 + 236i - \sqrt{5008\sqrt{41} + 23360} + i\sqrt{5008\sqrt{41} + 23360}\right) y \\ &= x^3 + \left(5 + 15i + \sqrt{17\sqrt{41} - 100} + i\sqrt{17\sqrt{41} + 100}\right) x^2 \end{aligned}$$

den 17-Torsionspunkt $(0, 0)$*.*

Beweis. Es handelt sich um einen 17-Torsionspunkt, da

$$\begin{aligned} 4 \cdot (0,0) = \Big(&-4 - 16i - \sqrt{40\sqrt{41} - 248} - i\sqrt{40\sqrt{41} + 248}\,, \\ &-48 + 52i - \sqrt{232\sqrt{41} - 200} + i\sqrt{232\sqrt{41} + 200}\Big), \\ 8 \cdot (0,0) = \Big(&-10 - 18i - \sqrt{36\sqrt{41} - 144} - i\sqrt{36\sqrt{41} + 144}, \\ &16 + 72i + \sqrt{416\sqrt{41} - 2336} + i\sqrt{416\sqrt{41} + 2336}\Big), \\ 9 \cdot (0,0) = \Big(&-10 - 18i - \sqrt{36\sqrt{41} - 144} - i\sqrt{36\sqrt{41} + 144}, \\ &10 + 82i + \sqrt{548\sqrt{41} - 3440} + i\sqrt{548\sqrt{41} + 3440}\Big), \\ 17 \cdot (0,0) = \mathcal{O}. \qquad \square \end{aligned}$$

9 Die 18-Torsionskurve

Theorem 9.1 (Nennerfreie 18-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 18-Torsionspunkt $(0, 0)$ *lautet*

$$\begin{aligned} E_{18}\colon\ &y^2 + (e^3 - 2e^2 f - ef^2 - 6e^2 + f^2 + 5e + f - 1)\, xy \\ &+ e(e+f)(-e^2 + ef + 3e - 1)(e-1)^4(ef+1)\, y \\ &= x^3 + e(e+f)(-e^2 + ef + 3e - 1)(e-1)\, x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$, die auf der Kurve

$$X_1(18)\colon \chi_{18}(e,f) \stackrel{\text{def}}{=} f^2 + (e^3 - 2e^2 + 3e + 1)f + 2e = 0$$

liegen.

(b) Die Diskriminante

$$\begin{aligned}\operatorname{disc}(E_{18}) = e \cdot (e-1)^5 \cdot (f+1)^{10} \cdot (e^2 - 2e - f) \cdot (e+f)^2 \cdot (e^2 - e + 1)^3 \cdot (e^3 - 3e^2 + 1) \\ \cdot (-e^2 f - e^2 + 2e + f) \cdot (-e^6 + ef^2 + e^2 + 4ef + f^2 + 2e + f)\end{aligned}$$

verschwindet unter der Nebenbedingung $\chi_{18}(e,f) = 0$ genau für die folgenden 11 Parameterpaare:

$$\begin{aligned}(e,f) \in \Bigg\{ &(0,\ 0), (0,\ -1), (1,\ -1), (1,\ -2), \left(\frac{1}{2} + \frac{1}{2}i\sqrt{3},\ -2\right), \left(\frac{1}{2} - \frac{1}{2}i\sqrt{3},\ -2\right), \\ &\left(\frac{1}{2} + \frac{1}{2}i\sqrt{3},\ -\frac{1}{2} - \frac{1}{2}i\sqrt{3}\right), \left(\frac{1}{2} - \frac{1}{2}i\sqrt{3},\ -\frac{1}{2} + \frac{1}{2}i\sqrt{3}\right), \\ &\left(1 + 2\cos\left(\frac{\pi}{9}\right),\ -2\sin\left(\frac{\pi}{18}\right)\right), \left(1 - 2\cos\left(\frac{2\pi}{9}\right),\ 2\cos\left(\frac{\pi}{9}\right)\right), \\ &\left(1 - 2\sin\left(\frac{\pi}{18}\right),\ -2\cos\left(\frac{2\pi}{9}\right)\right)\Bigg\}.\end{aligned}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 18-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}E(b,c)\colon\ & y^2 + (1-c)xy - by = x^3 - bx^2 \\ & b = rs(r-1) \\ & c = s(r-1) \\ & r = \frac{e^2 - ef - 3e + 1}{(e-1)^2(ef+1)} \\ & s = \frac{e^2 - 2e - f}{e^2 - ef - 3e - f^2 - 2f} \\ & X_1(18)\colon\ f^2 + (e^3 - 2e^2 + 3e + 1)f + 2e = 0\end{aligned}$$

Damit erhält man für den ersten Koeffizienten:

$$1 - c = \frac{e^4 - e^2f^2 + 3ef^3 + f^4 - 8e^3 + 15ef^2 + 4f^3 + 15e^2 + 25ef + 6f^2 + 5e + 2f}{(e-1)^2(e^2 - ef - 3e - f^2 - 2f)(ef+1)}$$

Modulo $X_1(18)$ lässt sich der mittlere Nennerfaktor entfernen, wenn die Potenz des ersten Nennerfaktors erhöht wird:

$$1 - c = \frac{e^3 - 2e^2f - ef^2 - 6e^2 + f^2 + 5e + f - 1}{(e-1)^3(ef+1)}$$

Für den zweiten Koeffizienten erhält man:

$$-b = \frac{e(e^2 - 2e - f)(e^2 - ef - 3e + 1)(e^2f - 2ef + 2f + 1)}{(e-1)^4(e^2 - ef - 3e - f^2 - 2f)^1(ef+1)^2}$$

Auch hier lässt sich der mittlere Nennerfaktor entfernen, wenn die Potenz des ersten Nennerfaktors erhöht wird:

$$-b = \frac{e(e+f)(-e^2 + ef + 3e - 1)}{(e-1)^5(ef+1)^2}$$

Man erhält eine nennerfreie Darstellung der elliptischen Kurve durch die Transformation

$$\begin{aligned}x &\mapsto \frac{x}{(e-1)^6(ef+1)^2} \\ y &\mapsto \frac{y}{(e-1)^9(ef+1)^3}\end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 18-Torsionspunkt $(0,0)$ lautet somit

$$\begin{aligned} E_{18}\colon\, & y^2 + (e^3 - 2e^2f - ef^2 - 6e^2 + f^2 + 5e + f - 1)\,xy \\ & + e(e+f)(-e^2 + ef + 3e - 1)(e-1)^4(ef+1)\,y \\ & = x^3 + e(e+f)(-e^2 + ef + 3e - 1)(e-1)\,x^2 \end{aligned}$$

mit der Nebenbedingung

$$\chi_{18}(e,f) = f^2 + (e^3 - 2e^2 + 3e + 1)f + 2e = 0.$$

Der Algorithmus 2.1 liefert als optimierte Faktorisierung der Diskriminante:

$$\begin{aligned} \operatorname{disc}(E_{18}) = {} & e \cdot (e-1)^5 \cdot (f+1)^{10} \cdot (e^2 - 2e - f) \cdot (e+f)^2 \cdot (e^2 - e + 1)^3 \cdot (e^3 - 3e^2 + 1) \\ & \cdot (-e^2f - e^2 + 2e + f) \cdot (-e^6 + ef^2 + e^2 + 4ef + f^2 + 2e + f) \end{aligned}$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{18})$ unter der Nebenbedingung $\chi_{18}(e,f) = 0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned} \operatorname{res}_e(\operatorname{disc}(E_{18}), \chi_{18}) = {} & e^{27}(e-1)^{39}(e^2 - e + 1)^9(e^3 - 3e^2 + 1)^3 \\ \operatorname{res}_f(\operatorname{disc}(E_{18}), \chi_{18}) = {} & f^{14}(f+1)^{48}(f+2)^{15}(f^2 + f + 1)^6(f^3 + 18f^2 + 24f + 8)(f^3 - 3f - 1)^2 \end{aligned}$$

Die Resultanten besitzen die Nullstellen

$$\begin{aligned} & e_1 = 0, \qquad e_2 = 1, \qquad e_{3/4} = \frac{1}{2} \pm \frac{1}{2}i\sqrt{3}, \\ & e_5 = 1 - 2\sin\left(\frac{\pi}{18}\right), \qquad e_6 = 1 + 2\cos\left(\frac{\pi}{9}\right), \qquad e_7 = 1 - 2\cos\left(\frac{2\pi}{9}\right), \\ & f_1 = 0, \qquad f_2 = -1, \qquad f_3 = -2, \qquad f_{4/5} = -\frac{1}{2} \pm \frac{1}{2}i\sqrt{3}, \\ & f_6 = \quad 4\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{37}{3}\sqrt{3}\right)\right) - 6, \\ & f_7 = -4\sqrt{7}\sin\left(\frac{1}{3}\arctan\left(\frac{37}{3}\sqrt{3}\right) + \frac{\pi}{3}\right) - 6, \\ & f_8 = \quad 4\sqrt{7}\cos\left(\frac{1}{3}\arctan\left(\frac{37}{3}\sqrt{3}\right) + \frac{\pi}{6}\right) - 6, \\ & f_9 = -2\sin\left(\frac{\pi}{18}\right), \qquad f_{10} = 2\cos\left(\frac{\pi}{9}\right), \qquad f_{11} = -2\cos\left(\frac{2\pi}{9}\right). \end{aligned}$$

Unter den 77 Paaren (e_i, f_j), $i \in \{1,\dots,7\}$, $j \in \{1,\dots,11\}$ lassen nur die folgenden 11 Paare sowohl die Diskriminante $\operatorname{disc}(E_{18})$ als auch die Kurvengleichung $\chi_{18}(e,f)$ verschwinden:

$$\begin{aligned} & (e_1, f_1) = (0,\ 0), \\ & (e_1, f_2) = (0,\ -1), \\ & (e_2, f_2) = (1,\ -1), \\ & (e_2, f_3) = (1,\ -2), \\ & (e_3, f_3) = \left(\frac{1}{2} + \frac{1}{2}i\sqrt{3},\ -2\right), \\ & (e_4, f_3) = \left(\frac{1}{2} - \frac{1}{2}i\sqrt{3},\ -2\right), \\ & (e_3, f_5) = \left(\frac{1}{2} + \frac{1}{2}i\sqrt{3},\ -\frac{1}{2} - \frac{1}{2}i\sqrt{3}\right), \\ & (e_4, f_4) = \left(\frac{1}{2} - \frac{1}{2}i\sqrt{3},\ -\frac{1}{2} + \frac{1}{2}i\sqrt{3}\right), \\ & (e_6, f_9) = \left(1 + 2\cos\left(\frac{\pi}{9}\right),\ -2\sin\left(\frac{\pi}{18}\right)\right), \\ & (e_7, f_{10}) = \left(1 - 2\cos\left(\frac{2\pi}{9}\right),\ 2\cos\left(\frac{\pi}{9}\right)\right), \\ & (e_5, f_{11}) = \left(1 - 2\sin\left(\frac{\pi}{18}\right),\ -2\cos\left(\frac{2\pi}{9}\right)\right). \qquad \square \end{aligned}$$

Beispiel 9.2 (18-Torsionskurve) *Ein Beispiel aus dieser Kurvenfamilie erhält man für*

$$e = 2,\ f = \frac{1}{2}\sqrt{33} - \frac{7}{2};$$

die elliptische Kurve

$$y^2 - 3xy + (105\sqrt{33} - 603)\, y = x^3 + (51 - 9\sqrt{33})\, x^2$$

hat den 18-Torsionspunkt $(0, 0)$.

Beweis. Es handelt sich um einen echten 18-Torsionspunkt, da

$$\begin{aligned} 6 \cdot (0,0) &= (3\sqrt{33} - 17,\ 586 - 102\sqrt{33}), \\ 9 \cdot (0,0) &= \left(\frac{81}{8}\sqrt{33} - \frac{465}{8},\ \frac{3429}{16} - \frac{597}{16}\sqrt{33}\right), \\ 18 \cdot (0,0) &= \mathcal{O}. \qquad \square \end{aligned}$$

10 Die 19-Torsionskurve

Theorem 10.1 (Nennerfreie 19-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 19-Torsionspunkt $(0, 0)$ *lautet*

$$\begin{aligned} E_{19}\colon\ & y^2 + (e^5 - 3e^4 f - e^3 f^2 + e^2 f^3 + 6e^4 - 6e^3 f - 2e^2 f^2 + 3ef^3 + 10e^3 - 6e^2 f \\ & \quad - 6ef^2 + f^3 + 8e^2 + ef - 2f^2 + 2e + f)\, xy \\ & + e(e+1)^4 (f-1)^2 (e^2 + e - f + 1)(e^3 + 2e^2 - ef - f^2 + 2e + f)^2 \\ & \quad \cdot (e^2 f - f^2 + e + f)\, y \\ & = x^3 - e(e+1)(f-1)(e^2 + e - f + 1)(e^3 + 2e^2 - ef - f^2 + 2e + f)(e + f) \\ & \quad \cdot (e - f + 1)\, x^2 \end{aligned}$$

für Parameter $e, f \in \mathbb{C}$*, die auf der Kurve*

$$\begin{aligned} X_1(19)\colon\ & \chi_{19}(e,f) \overset{def}{=} f^5 - (e^2+2)f^4 - (2e^3 + 2e^2 + 2e - 1)f^3 \\ & + (e^5 + 3e^4 + 7e^3 + 6e^2 + 2e)f^2 - (e^5 + 2e^4 + 4e^3 + 3e^2)f + (e^3 + e^2) = 0 \end{aligned}$$

liegen.

(b) Die Diskriminante

$$\begin{aligned} \operatorname{disc}(E_{19}) = {} & e^7 \cdot (e+1)^7 \cdot (e+f)^5 \cdot (e - f + 1)^5 \cdot (f-1)^9 \cdot (e^2 + e - f + 1)^4 \\ & \cdot (e^3 + 2e^2 - ef - f^2 + 2e + f)^3 \cdot (e^2 - ef - f^2 + 2e + f)^2 \\ & \cdot (e^5 f + 4e^4 f^2 - e^3 f^3 - e^4 f + 7e^3 f^2 - 8e^2 f^3 - 2e^3 f + 18e^2 f^2 \\ & \quad - 5ef^3 - e^3 - 11e^2 f + 10ef^2 + f^3 + 2e^2 - 7ef - 2f^2 + 2e + f) \end{aligned}$$

verschwindet unter der Nebenbedingung $\chi_{19}(e, f) = 0$ *genau für die folgenden 13 Parameterpaare:*

$$\begin{aligned} (e,f) \in \{ & (0,\ 0), (0,\ 1), (-1,\ 0), (-1,\ 1), (e_1,\ f_7), (e_2,\ f_8), (e_3,\ f_4), \\ & (e_4,\ f_1), (e_5,\ f_5), (e_6,\ f_2), (e_7,\ f_6), (e_8,\ f_3), (e_9,\ f_9)\}. \end{aligned}$$

Dabei sind die Parameterwerte e_{1-9} *die Nullstellen des Polynoms* $e^9 + e^8 - 27e^7 - 64e^6 + 59e^5 + 243e^4 + 170e^3 + 9e^2 - 14e + 1$*:*

$$\begin{aligned} & e_1 \approx -3.252, \quad e_2 \approx -2.846, \quad e_3 \approx -1.156, \quad e_4 \approx -0.783, \quad e_5 \approx -0.716, \\ & e_6 \approx 0.084, \quad e_7 \approx 0.178, \quad e_8 \approx 2.049, \quad e_9 \approx 5.443. \end{aligned}$$

Die Werte f_{1-9} *sind definiert durch* $f_{7/8/4/1/5/2/6/3/9} = \varphi(e_{1/2/3/4/5/6/7/8/9})$ *mit*

$$\varphi(e) \overset{def}{=} \frac{1}{19}\,(14e^8 + 6e^7 - 380e^6 - 677e^5 + 1171e^4 + 2640e^3 + 1008e^2 - 119e - 4)$$

und sind damit die Nullstellen des Polynoms $f^9-23f^8+157f^7-369f^6+322f^5-27f^4-87f^3+22f^2+6f-1$*:*

$$\begin{array}{llll} f_1\approx -0.396, & f_2\approx -0.277, & f_3\approx 0.135, & f_4\approx 0.649, \quad f_5\approx 0.692,\\ f_6\approx 1.184, & f_7\approx 1.488, & f_8\approx 6.630, & f_9\approx 12.895. \end{array}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 19-Torsionspunkt $(0,0)$ an:

$$\begin{aligned} E(b,c)\colon\ & y^2+(1-c)xy-by=x^3-bx^2\\ & b=rs(r-1)\\ & c=s(r-1)\\ & r=1+\frac{e(e+f)(f-1)}{(e+1)(e^2-ef+2e-f^2+f)}\\ & s=1+\frac{e(f-1)}{(e+1)(e-f+1)}\\ & X_1(19)\colon\ f^5-(e^2+2)f^4-(2e^3+2e^2+2e-1)f^3+(e^5+3e^4+7e^3+6e^2+2e)f^2\\ & \qquad -(e^5+2e^4+4e^3+3e^2)f+(e^3+e^2)=0 \end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned} 1-c=&\frac{e^5+(6-3f)e^4-(f^2+6f-10)e^3+(f^3-2f^2-6f+8)e^2}{(e+1)^2(e-f+1)(e^2-ef+2e-f^2+f)}\\ &+\frac{(f-1)(3f^2-3f-2)e+f(f-1)^2}{(e+1)^2(e-f+1)(e^2-ef+2e-f^2+f)}\\ -b=&\frac{e(1-f)(e+f)(e^2+e-f+1)(e^3+2e^2-ef+2e-f^2+f)}{(e+1)^3(e-f+1)(e^2-ef+2e-f^2+f)^2} \end{aligned}$$

Man erhält eine nennerfreie Darstellung der elliptischen Kurve durch die Transformation

$$\begin{aligned} x&\mapsto \frac{x}{(e+1)^4(e-f+1)^2(e^2-ef+2e-f^2+f)^2}\\ y&\mapsto \frac{y}{(e+1)^6(e-f+1)^3(e^2-ef+2e-f^2+f)^3} \end{aligned}$$

Die Gleichung einer elliptischen Kurve mit 19-Torsionspunkt $(0,0)$ lautet somit

$$\begin{aligned} E_{19}\colon\ & y^2+(e^5-3e^4f-e^3f^2+e^2f^3+6e^4-6e^3f-2e^2f^2+3ef^3+10e^3-6e^2f\\ &\qquad -6ef^2+f^3+8e^2+ef-2f^2+2e+f)\,xy\\ &+e(e+1)^4(f-1)^2(e^2+e-f+1)(e^3+2e^2-ef-f^2+2e+f)^2\\ &\qquad \cdot(e^2f-f^2+e+f)\,y\\ &=x^3-e(e+1)(f-1)(e^2+e-f+1)(e^3+2e^2-ef-f^2+2e+f)(e+f)\\ &\qquad \cdot(e-f+1)\,x^2 \end{aligned}$$

mit der Nebenbedingung

$$\begin{aligned} \chi_{19}(e,f)=&f^5-(e^2+2)f^4-(2e^3+2e^2+2e-1)f^3+(e^5+3e^4+7e^3+6e^2+2e)f^2\\ &-(e^5+2e^4+4e^3+3e^2)f+(e^3+e^2)=0. \end{aligned}$$

Der Algorithmus 2.1 liefert als optimierte Faktorisierung der Diskriminante:

$$\begin{aligned} \operatorname{disc}(E_{19})=&e^7\cdot(e+1)^7\cdot(e+f)^5\cdot(e-f+1)^5\cdot(f-1)^9\cdot(e^2+e-f+1)^4\\ &\cdot(e^3+2e^2-ef-f^2+2e+f)^3\cdot(e^2-ef-f^2+2e+f)^2\\ &\cdot(e^5f+4e^4f^2-e^3f^3-e^4f+7e^3f^2-8e^2f^3-2e^3f+18e^2f^2\\ &\quad -5ef^3-e^3-11e^2f+10ef^2+f^3+2e^2-7ef-2f^2+2e+f) \end{aligned}$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{19})$ unter der Nebenbedingung $\chi_{19}(e,f)=0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned}\operatorname{res}_e(\operatorname{disc}(E_{19}),\chi_{19}) &= -e^{158}\cdot(e+1)^{129}\\ &\quad\cdot(e^9+e^8-27e^7-64e^6+59e^5+243e^4+170e^3+9e^2-14e+1)\\ \operatorname{res}_f(\operatorname{disc}(E_{19}),\chi_{19}) &= -f^{71}\cdot(f-1)^{234}\\ &\quad\cdot(f^9-23f^8+157f^7-369f^6+322f^5-27f^4-87f^3+22f^2+6f-1)\end{aligned}$$

Die Resultanten besitzen die Nullstellen

$$\begin{array}{llllll} e_1\approx -3.252, & e_2\approx -2.846, & e_3\approx -1.156, & e_4\approx -0.783, & e_5\approx -0.716, & e_6\approx 0.084,\\ e_7\approx 0.178, & e_8\approx 2.049, & e_9\approx 5.443; & e_{10}=0, & e_{11}=1; & \\ f_1\approx -0.396, & f_2\approx -0.277, & f_3\approx 0.135, & f_4\approx 0.649, & f_5\approx 0.692, & f_6\approx 1.184,\\ f_7\approx 1.488, & f_8\approx 6.630, & f_9\approx 12.895, & f_{10}=0, & f_{11}=1. & \end{array}$$

Unter den 121 Parameterpaaren (e_i,f_j), $i,j\in\{1,\dots,11\}$ lassen nur die folgenden 13 Paare sowohl die Diskriminante $\operatorname{disc}(E_{19})$ als auch die Kurvengleichung $\chi_{19}(e,f)$ verschwinden:

$$\begin{aligned}(e,f)\in\{&(0,\,0),(0,\,1),(-1,\,0),(-1,\,1),(e_1,\,f_7),(e_2,\,f_8),(e_3,\,f_4),\\ &(e_4,\,f_1),(e_5,\,f_5),(e_6,\,f_2),(e_7,\,f_6),(e_8,\,f_3),(e_9,\,f_9)\}.\end{aligned}$$

Die Koeffizienten der Transformation φ erhält man durch Interpolation durch die Punkte $(e_1,\,f_7)$, $(e_2,\,f_8)$, $(e_3,\,f_4)$, $(e_4,\,f_1)$, $(e_5,\,f_5)$, $(e_6,\,f_2)$, $(e_7,\,f_6)$, $(e_8,\,f_3)$, $(e_9,\,f_9)$. □

Es ist momentan kein Beispiel einer 19-Torsionskurve mit radikalen Koeffizienten bekannt, da bisher keine radikalen Punkte auf der Kurve $X_1(19)$ bestimmt werden konnten. Der Nachweis, dass der Punkt $(0,0)$ tatsächlich ein 19-Torsionspunkt von E_{19} ist, lässt sich also nur durch symbolische Verifikation von $19\cdot(0,0)=\mathcal{O}$ mittels [SAGE] erbringen.

11 Die 20-Torsionskurve

Theorem 11.1 (Nennerfreie 20-Torsionskurve)

(a) Die allgemeine Gleichung einer elliptischen Kurve mit 20-Torsionspunkt $(0,0)$ lautet

$$\begin{aligned}E_{20}\colon\, &y^2+(-e^3+e^2f+2ef^2+f^3+4e^2+2ef+3f^2-2e+5f+4)\,xy\\ &-e\cdot(e-1)^3\cdot(e^2-e+f+1)\\ &\cdot(e^2f^2+ef^3-e^2f-2ef^2-2f^3-e^2-2ef-4f^2-4f-2)\,y\\ &=x^3-e\cdot(e-1)\cdot(e^3+3ef+f^2+3e+f)\,x^2\end{aligned}$$

für Parameter $e,f\in\mathbb{C}$, die auf der Kurve

$$X_1(20)\colon\,\chi_{20}(e,f)\overset{def}{=}f^3+(e^2+3)f^2+(e^3+4)f+2=0$$

liegen.

(b) Die Diskriminante

$$\begin{aligned}\operatorname{disc}(E_{20})=\frac{1}{2}&\cdot e^5\cdot(e-1)^6\cdot(e^2-e+f+2)\cdot(e^2-e+f+1)\cdot(f+1)^3\cdot(f+2)\\ &\cdot(e^2f^2+ef^3-e^2f-2ef^2-2f^3-e^2-2ef-4f^2-4f-2)^2\\ &\cdot(e^2f+ef^2-f^2-e-2f-1)^2\cdot(-e^5-11e^2f^3-12ef^4-2f^5-6e^4\\ &-19e^2f^2-21ef^3+9f^4-12e^3-33e^2f+7ef^2+75f^3-4e^2+44ef\\ &+168f^2+28e+176f+72)\end{aligned}$$

verschwindet unter der Nebenbedingung $\chi_{20}(e,f) = 0$ genau für die folgenden 13 Parameterpaare:

$$\begin{aligned}(e,f) \in \{&(0,\ -1), (0,\ -1+i), (0,\ -1-i), (1,\ -1), (1,\ -2),\\ &(1+i,\ -1+i), (1-i,\ -1-i), \left(\frac{1}{2}+\frac{1}{2}\sqrt{5},\ -2\right), \left(\frac{1}{2}-\frac{1}{2}\sqrt{5},\ -2\right),\\ &\left(\frac{1}{2}+\frac{1}{2}\sqrt{-5+2\sqrt{5}},\ -\frac{3}{4}-\frac{1}{4}\sqrt{5}-\frac{1}{2}\sqrt{-\frac{5}{2}-\frac{1}{2}\sqrt{5}}\right),\\ &\left(\frac{1}{2}-\frac{1}{2}\sqrt{-5+2\sqrt{5}},\ -\frac{3}{4}-\frac{1}{4}\sqrt{5}+\frac{1}{2}\sqrt{-\frac{5}{2}-\frac{1}{2}\sqrt{5}}\right),\\ &\left(\frac{1}{2}+\frac{1}{2}\sqrt{-5-2\sqrt{5}},\ -\frac{3}{4}+\frac{1}{4}\sqrt{5}-\frac{1}{2}\sqrt{-\frac{5}{2}+\frac{1}{2}\sqrt{5}}\right),\\ &\left(\frac{1}{2}-\frac{1}{2}\sqrt{-5-2\sqrt{5}},\ -\frac{3}{4}+\frac{1}{4}\sqrt{5}+\frac{1}{2}\sqrt{-\frac{5}{2}+\frac{1}{2}\sqrt{5}}\right)\Bigg\}.\end{aligned}$$

Beweis. Sutherland ([Sut2012], Tabelle 7) gibt als Parametrisierung einer elliptischen Kurve mit 20-Torsionspunkt $(0,0)$ an:

$$\begin{aligned}E(b,c)\colon\ & y^2 + (1-c)xy - by = x^3 - bx^2\\ & b = rs(r-1)\\ & c = s(r-1)\\ & r = 1 + \frac{e^3+ef+e}{(e-1)^2(e^2-e+f+1)}\\ & s = 1 + \frac{e^2+f+1}{(e-1)(e^2-e+f+2)}\\ & X_1(20)\colon\ f^3 + (e^2+3)f^2 + (e^3+4)f + 2 = 0\end{aligned}$$

Damit erhält man die folgenden Koeffizienten:

$$\begin{aligned}1-c &= 1 + \frac{e(e^2+f+1)(e^3-e^2+ef+3e-1)}{(1-e)^3(e^2-e+f+1)(e^2-e+f+2)}\\ -b &= \frac{e(e^2+f+1)(e^3-e^2+ef+3e-1)(e^2f-ef+f+e^4-2e^3+4e^2-2e+1)}{(1-e)^5(e^2-e+f+2)(e^2-e+f+1)^2}\end{aligned}$$

Die Transformation auf die nennerfreie Darstellung erfolgt durch:

$$\begin{aligned}x &\mapsto \frac{x}{(1-e)^6(e^2-e+f+1)^2(e^2-e+f+2)^2}\\ y &\mapsto \frac{y}{(1-e)^9(e^2-e+f+1)^3(e^2-e+f+2)^3}\end{aligned}$$

Man erhält die 20-Torsionsgleichung

$$\begin{aligned}&y^2 + [-f^2(e^3-4e^2+3e-1) - f(2e^5-10e^4+16e^3-21e^2+12e-3)\\ &\qquad - e^7+6e^6-14e^5+26e^4-27e^3+22e^2-10e+2]\,xy\\ &+ e(e-1)^4(e^2-e+f+1)(e^2-e+f+2)^2(e^2+f+1)(e^3-e^2+ef+3e-1)\\ &\quad\cdot(e^4-2e^3+e^2f+4e^2-ef-2e+f+1)\,y\\ &= x^3 - e(e-1)(e^2-e+f+2)(e^2+f+1)(e^3-e^2+ef+3e-1)\\ &\qquad\cdot(e^4-2e^3+e^2f+4e^2-ef-2e+f+1)\,x^2\end{aligned}$$

Der Koeffizient vor xy lässt sich wie folgt faktorisieren:

$$\begin{aligned}&(e^4-2e^3+e^2f+4e^2-ef-2e+f+1)\\ &\cdot(-e^3+e^2f+2ef^2+f^3+4e^2+2ef+3f^2-2e+5f+4)\end{aligned}$$

Der Koeffizient vor y lässt sich passend kubisch faktorisieren:

$$(e^4 - 2e^3 + e^2f + 4e^2 - ef - 2e + f + 1)^3 \cdot (-1) \cdot e \cdot (e-1)^3 \cdot (e^2 - e + f + 1)$$
$$\cdot (e^2f^2 + ef^3 - e^2f - 2ef^2 - 2f^3 - r^2 - 2ef - 4f^2 - 4f - 2)$$

Der Koeffizient vor x^2 lässt sich passend quadratisch faktorisieren:

$$(e^4 - 2e^3 + e^2f + 4e^2 - ef - 2e + f + 1)^2 \cdot (-1) \cdot e \cdot (e-1) \cdot (e^3 + 3ef + f^2 + 3e + f)$$

Somit führt die Transformation

$$x \mapsto (e^4 - 2e^3 + e^2f + 4e^2 - ef - 2e + f + 1)^2 \cdot x$$
$$y \mapsto (e^4 - 2e^3 + e^2f + 4e^2 - ef - 2e + f + 1)^3 \cdot y$$

auf die 20-Torsionskurve

$$\begin{aligned} E_{20}\colon\, & y^2 + (-e^3 + e^2f + 2ef^2 + f^3 + 4e^2 + 2ef + 3f^2 - 2e + 5f + 4)\, xy \\ & - e(e-1)^3(e^2 - e + f + 1)(e^2f^2 + ef^3 - e^2f - 2ef^2 - 2f^3 - e^2 - 2ef - 4f^2 - 4f - 2)\, y \\ & = x^3 - e(e-1)(e^3 + 3ef + f^2 + 3e + f)\, x^2 \end{aligned}$$

Für die Diskriminante $\operatorname{disc}(E_{20})$ hat der Algorithmus 2.1 die folgende optimierte Faktorisierung ermittelt, in der der nicht-faktorisierbare Restterm die geringste Anzahl von Monomen besitzt:

$$\begin{aligned} \operatorname{disc}(E_{20}) = \frac{1}{2} & \cdot e^5 \cdot (e^2 - e + f + 2) \cdot (e^2 - e + f + 1) \cdot (e^2f + ef^2 - f^2 - e - 2f - 1)^2 \\ & \cdot (e-1)^6 \cdot (e^2f^2 + ef^3 - e^2f - 2ef^2 - 2f^3 - e^2 - 2ef - 4f^2 - 4f - 2)^2 \\ & \cdot (f+1)^3 \cdot (f+2) \cdot (-e^5 - 11e^2f^3 - 12ef^4 - 2f^5 - 6e^4 - 19e^2f^2 - 21ef^3 \\ & + 9f^4 - 12e^3 - 33e^2f + 7ef^2 + 75f^3 - 4e^2 + 44ef + 168f^2 + 28e + 176f + 72) \end{aligned}$$

Die Nullstellen der Diskriminante $\operatorname{disc}(E_{20})$ unter der Nebenbedingung $\chi_{20}(e,f) = 0$ erhält man durch Betrachtung der Resultanten bezüglich der Variablen e und f:

$$\begin{aligned} \operatorname{res}_e(\operatorname{disc}(E_{20}), \chi_{20}) = & -e^{30} \cdot (e-1)^{30} \cdot (e^2 - e - 1)^2 \cdot (e^2 - 2e + 2)^5 \\ & \cdot (e^4 - 2e^3 - 6e^2 + 12e - 4) \cdot (e^4 - 2e^3 + 4e^2 - 3e + 1)^4 \\ \operatorname{res}_f(\operatorname{disc}(E_{20}), \chi_{20}) = & f^6 \cdot (f+2)^{14} \cdot (f+1)^{40} \cdot (f^2 + 2f + 2)^{10} \cdot (f^4 + 8f^3 + 4f^2 - 8f - 4) \\ & \cdot (f^4 + 3f^3 + 4f^2 + 2f + 1)^4 \end{aligned}$$

Die Resultanten besitzen die folgenden Nullstellen:

$$\begin{aligned} & e_1 = 0, && e_2 = 1, \\ & e_{3/4} = \frac{1}{2} \pm \frac{1}{2}\sqrt{5}, && e_{5/6} = 1 \pm i, \\ & e_{7/8} = \frac{1}{2} + \frac{1}{2}\sqrt{5} \pm \frac{1}{2}\sqrt{10 - 2\sqrt{5}}, && e_{9/10} = \frac{1}{2} - \frac{1}{2}\sqrt{5} \pm \frac{1}{2}\sqrt{10 + 2\sqrt{5}}, \\ & e_{11/12} = \frac{1}{2} \pm \frac{1}{2}\sqrt{-5 + 2\sqrt{5}}, && e_{13/14} = \frac{1}{2} \pm \frac{1}{2}\sqrt{-5 - 2\sqrt{5}}; \\ & f_1 = 0, && f_2 = -2, \\ & f_3 = -1, && f_{4/5} = -1 \pm i, \\ & f_{6/7} = -2 + \sqrt{5} \pm \frac{1}{2}\sqrt{20 - 8\sqrt{5}}, && f_{8/9} = -2 - \sqrt{5} \pm \frac{1}{2}\sqrt{20 + 8\sqrt{5}}, \\ & f_{10/11} = -\frac{3}{4} + \frac{1}{4}\sqrt{5} \pm \frac{1}{2}\sqrt{-\frac{5}{2} + \frac{1}{2}\sqrt{5}}, && f_{12/13} = -\frac{3}{4} - \frac{1}{4}\sqrt{5} \pm \frac{1}{2}\sqrt{-\frac{5}{2} - \frac{1}{2}\sqrt{5}}. \end{aligned}$$

Unter den 182 Paaren (e_i, f_j), $i \in \{1, \ldots, 14\}$, $j \in \{1, \ldots, 13\}$ lassen nur die folgenden 13 Paare

sowohl die Diskriminante $\operatorname{disc}(E_{20})$ als auch die Kurvengleichung $\chi_{20}(e,f)$ verschwinden:

$$
\begin{aligned}
(e_1, f_3) &= (0,\ -1),\\
(e_1, f_4) &= (0,\ -1+i),\\
(e_1, f_5) &= (0,\ -1-i),\\
(e_2, f_3) &= (1,\ -1),\\
(e_2, f_2) &= (1,\ -2),\\
(e_5, f_4) &= (1+i,\ -1+i),\\
(e_6, f_5) &= (1-i,\ -1-i),\\
(e_3, f_2) &= \left(\frac{1}{2}+\frac{1}{2}\sqrt{5},\ -2\right),\\
(e_4, f_2) &= \left(\frac{1}{2}-\frac{1}{2}\sqrt{5},\ -2\right),\\
(e_{11}, f_{13}) &= \left(\frac{1}{2}+\frac{1}{2}\sqrt{-5+2\sqrt{5}},\ -\frac{3}{4}-\frac{1}{4}\sqrt{5}-\frac{1}{2}\sqrt{-\frac{5}{2}-\frac{1}{2}\sqrt{5}}\right),\\
(e_{12}, f_{12}) &= \left(\frac{1}{2}-\frac{1}{2}\sqrt{-5+2\sqrt{5}},\ -\frac{3}{4}-\frac{1}{4}\sqrt{5}+\frac{1}{2}\sqrt{-\frac{5}{2}-\frac{1}{2}\sqrt{5}}\right),\\
(e_{13}, f_{11}) &= \left(\frac{1}{2}+\frac{1}{2}\sqrt{-5-2\sqrt{5}},\ -\frac{3}{4}+\frac{1}{4}\sqrt{5}-\frac{1}{2}\sqrt{-\frac{5}{2}+\frac{1}{2}\sqrt{5}}\right),\\
(e_{14}, f_{10}) &= \left(\frac{1}{2}-\frac{1}{2}\sqrt{-5-2\sqrt{5}},\ -\frac{3}{4}+\frac{1}{4}\sqrt{5}+\frac{1}{2}\sqrt{-\frac{5}{2}+\frac{1}{2}\sqrt{5}}\right). \qquad \square
\end{aligned}
$$

Beispiel 11.2 (20-Torsionskurven)

(a) Unter der Nebenbedingung $f = 4e$ erhält man die Parameter

$$
\begin{aligned}
e &= \frac{1}{10}\cdot\sqrt[4]{216}+\frac{2}{5}\cdot\sqrt[4]{6}-\frac{1}{5}\cdot\sqrt{6}-\frac{4}{5},\\
f &= \frac{2}{5}\cdot\sqrt[4]{216}+\frac{8}{5}\cdot\sqrt[4]{6}-\frac{4}{5}\cdot\sqrt{6}-\frac{16}{5};
\end{aligned}
$$

diese Parameter erzeugen die elliptische Kurve

$$
\begin{aligned}
&y^2+\left(\frac{7527}{125}\cdot\sqrt[4]{216}+\frac{37011}{250}\cdot\sqrt[4]{6}-\frac{11844}{125}\cdot\sqrt{6}-\frac{28621}{125}\right)xy\\
&+\left(-\frac{19943363887}{1562500}\cdot\sqrt[4]{216}-\frac{24424481529}{781250}\cdot\sqrt[4]{6}+\frac{31211475639}{1562500}\cdot\sqrt{6}+\frac{76456430901}{1562500}\right)y\\
&=x^3+\left(\frac{739933}{12500}\cdot\sqrt[4]{216}+\frac{907911}{6250}\cdot\sqrt[4]{6}-\frac{290694}{3125}\cdot\sqrt{6}-\frac{1415667}{6250}\right)x^2
\end{aligned}
$$

mit 20-Torsionspunkt $(0,0)$. Die Transformation

$$x \mapsto \frac{x}{250^2}, \quad y \mapsto \frac{y}{250^3}$$

erzeugt daraus die folgende nennerfreie Darstellung

$$
\begin{aligned}
&y^2+\left(15054\cdot\sqrt[4]{216}+37011\cdot\sqrt[4]{6}-23688\cdot\sqrt{6}-57242\right)xy\\
&+\left(-199433638870\cdot\sqrt[4]{216}-488489630580\cdot\sqrt[4]{6}+312114756390\cdot\sqrt{6}+764564309010\right)y\\
&=x^3+\left(3699665\cdot\sqrt[4]{216}+9079110\cdot\sqrt[4]{6}-5813880\cdot\sqrt{6}-14156670\right)x^2.
\end{aligned}
$$

Auf dieser elliptischen Kurve lauten die Vielfachen des 20-Torsionspunkt dann

$$\begin{aligned}
4 \cdot (0,0) &= (1125365 \cdot \sqrt[4]{216} - 2792910 \cdot \sqrt[4]{6} + 1785530 \cdot \sqrt{6} + 4316520, \\
&\quad - 825591600 \cdot \sqrt[4]{216} - 2016640650 \cdot \sqrt[4]{6} + 1293302700 \cdot \sqrt{6} + 3153369300), \\
5 \cdot (0,0) &= (8369635 \cdot \sqrt[4]{216} + 20412090 \cdot \sqrt[4]{6} - 13073220 \cdot \sqrt{6} - 32005980, \\
&\quad 2121643133400 \cdot \sqrt[4]{216} + 5196996259350 \cdot \sqrt[4]{6} - 3320556147300 \cdot \sqrt{6} \\
&\quad - 8133725743200), \\
20 \cdot (0,0) &= \mathcal{O}.
\end{aligned}$$

(b) Parameter für eine zweite elliptische Kurve mit 20-Torsionspunkt $(0,0)$ *erhält man aus der Zusatzbedingung* $f = e - 1$*:*

$$\begin{aligned}
e &= \sqrt[3]{\frac{1}{36}\sqrt{114} - \frac{8}{27}} - \sqrt[3]{\frac{1}{36}\sqrt{114} + \frac{8}{27}} + \frac{1}{3}, \\
f &= \sqrt[3]{\frac{1}{36}\sqrt{114} - \frac{8}{27}} - \sqrt[3]{\frac{1}{36}\sqrt{114} + \frac{8}{27}} - \frac{2}{3}.
\end{aligned}$$

Literatur

[Hus2004] D. Husemöller, *Elliptic curves*, Second edition, Springer Verlag, New York, 2004

[Kub1976] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), pp. 193–237

[Rei1986] M.A. Reichert, *Explicit Determination of Torsion Structures of Elliptic Curves Over Quadratic Number Fields*, Math. Comp. **46** (1986), no. 2, pp. 637–658

[SAGE] The Sage Notebook v7.0, Computer-Algebra-System, `http://www.sagenb.org/`

[Sil2009] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Springer Verlag, New York, 2009

[Sut2012] A.V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), pp. 1131–1147