Elliptische Kurven

Vortrag zum Seminar zur Funktionentheorie, 12.11.2007

Martin Raum

Elliptische Funktionen beziehungsweise die Weierstraßsche $\wp$-Funktion und ihre Eigenschaften geben Anlass dazu, gewisse von ihnen induzierte Nullstellengebilde zu untersuchen. Diese, so wird sich herausstellen, besitzen tatsächlich außergewöhnlich schöne Eigenschaften und ermöglichen es mit ihrer Struktur, Fragestellungen aus anderen Gebieten ihrerseits zu untersuchen.

Wir werden die geometrischen Eigenschaften mit einer Gruppenstruktur in Verbindung bringen und einige Ergebnisse für geeignete Teilmengen angeben. Darauf aufbauend sind wir in der Lage, zahlentheoretische Fragestellungen zu betrachten.

§ 1 Geometrische Verknüpfungen auf einer ell. Kurve

Wir wollen zunächst an die Definition einer elliptischen Kurve erinnern. Eine elliptische Kurve $\mathbb{E}$ ist die Nullstellenmenge von $4X^3 - g_2X - g_3 - Y^2 \in \mathbb{C}[X,Y]$ über $\mathbb{C}$ mit $g_2^3 - 27g_3^2 \neq 0$. Es liegt nahe, zunächst Schnitte zu betrachten, zum Beispiel den Schnitt mit Geraden. Wenn wir die Nullstellenmenge projektiv betrachten, wofür $\mathbb{PE}$ schreiben, stellt sich heraus, dass eine projektive Gerade $\mathrm{Null}(aX + bY + cZ) := \{(x : y : z) \in \mathcal{P}(\mathbb{C}^3) : ax + by + cz = 0\}$ genau drei mit Vielfachheit gezählte Schnittpunkte mit $\mathbb{PE}$ besitzt. Im Affinen verschwinden diese Schnittpunkte eventuell, für $a = b = 0$ etwa sogar alle. Dennoch beschränken wir uns auf diesen Fall, um die Rechnung einfach zu gestalten.

Wir wollen im Folgenden zur Vereinfachung der Notation $\mathbb{PE} \subseteq \mathcal{P}(\mathbb{C}^3)$ mit $\overline{\mathbb{E}} \subseteq \mathbb{C}^2 \cup \{\mathcal{O}\}$ identifizieren. Analog benutzen wir ohne weitere Erwähnung die Einbettung von $\mathcal{A}(\mathbb{C}^2) \cong \mathbb{C}^2$ in $\mathcal{P}(\mathbb{C}^3)$.

— *Eine Gerade durch zwei verschiedene Punkte $P, Q \in \mathbb{E}$* —

Sind $\pi_1, \pi_2 : \mathbb{C}^2 \to \mathbb{C}$ die orthogonalen Projektionen auf die erste beziehungsweise zweite Komponente, bezeichnen wir mit $X_P := \pi_1(P)$ und $Y_P := \pi_2(P)$ die entsprechenden Koordinaten zu einem Punkt P. Wir betrachten zwei Punkte $P, Q \in \mathbb{E}$, für die wir $X_P \neq X_Q$ voraussetzen, um den projektiven Fall zu vermeiden. Dann können wir die Gerade $\Gamma := \Gamma_{P,Q}$ durch P, Q als Graph einer Funktion in X angeben:

(1.1) Definition (Gerade durch P, Q)
Seien $P, Q \in \mathbb{E}$ mit $X_P \neq X_Q$. Dann bezeichnen wir mit

$$a_{P,Q} := \frac{Y_P - Y_Q}{X_P - X_Q} \qquad \text{und}$$
$$b_{P,Q} := Y_P - a_{P,Q} X_P = \frac{X_P Y_Q - X_Q Y_P}{X_P - X_Q}$$

die Steigung beziehungsweise den Ordinatenabschnitt einer Geraden durch P und Q und setzen

$$\Gamma_{P,Q} := \text{Graph}\left(f : \mathbb{C} \to \mathbb{C}, x \mapsto a_{P,Q} x + b_{P,Q}\right) \qquad \diamond$$

Unsere nächste Aufgabe ist es, einen weiteren Schnittpunkt von $\Gamma_{P,Q}$ mit $\mathbb{E}$ zu bestimmen, dessen Existenz wir zunächst annehmen. Sei dieser Punkt mit $P \bullet Q$ benannt. Dann wird einerseits $Y_{P\bullet Q} = a_{P,Q} X_{P\bullet Q} + b_{P,Q}$ gelten müssen. Andererseits gilt für $(X, Y) \in \mathbb{E}$ mit $X \in \{X_P, X_Q, X_{P\bullet Q}\}$ stets

$$\begin{aligned} 4X^3 - g_2 X - g_3 = Y^2 &= (a_{P,Q} X + b_{P,Q})^2 \\ &= 4(X - X_P)(X - X_Q)(X - X_{P\bullet Q}) + (a_{P,Q} X + b_{P,Q})^2 \\ &= 4X^3 + X^2 \left(4(-X_P - X_Q - X_{P\bullet Q}) + a_{P,Q}^2\right) \\ &\quad + X\left(4(X_P X_Q + X_P X_{P\bullet Q} + X_Q X_{P\bullet Q}) + 2a_{P,Q} b_{P,Q}\right) \\ &\quad - 4X_P X_Q X_{P\bullet Q} + b_{P,Q}^2. \end{aligned}$$

Dann stimmen die Auswertungen der entsprechenden Polynome an drei Stellen überein und die Polynome haben bereits den höchsten Koeffizienten gemeinsam, so dass sie als Polynome dritten Grades gleich sind. Also können wir als notwendige Bedingung an einen Schnittpunkt $P \bullet Q$ die Übereinstimmung des zweithöchsten Koeffizienten formulieren.

$$\begin{aligned} 0 &= 4(-X_P - X_Q - X_{P\bullet Q}) + a_{P,Q}^2 \\ \Rightarrow X_{P\bullet Q} &= \frac{1}{4} a_{P,Q}^2 - X_P - X_Q. \end{aligned}$$

Dies können wir nun zum Anlass nehmen, den Punkt $P \bullet Q$ zu definieren. Dabei berücksichtigen wir auch den zuvor ausgeschlossenen projektiven Fall.

(1.2) Definition (Der Punkt $P \bullet Q$)
Seien P, Q wie in 1.1. Dann wird $P \bullet Q$ definiert vermöge

$$X_{P\bullet Q} := \frac{1}{4}a_{P,Q}^2 - X_P - X_Q \qquad \text{und}$$
$$Y_{P\bullet Q} := a_{P,Q}X_{P\bullet Q} + b_{P,Q}.$$

Sind $P, Q \in \mathbb{E}$ mit $P \neq Q$ und $X_P = X_Q$, so definieren wir $P \bullet Q := \mathcal{O}$. ◇

Wir müssen nun für den ersten Fall nachrechnen, dass $P \bullet Q \in \mathbb{E}$ gilt. Der Weg dahin wurde schon angedeutet:

(1.3) Lemma
Mit P, Q wie in 1.1 gilt:

$$4X^3 - g_2X - g_3 = 4(X - X_P)(X - X_Q)(X - X_{P\bullet Q}) + (a_{P,Q}X + b_{P,Q})^2. \qquad \diamond$$

Beweis
Die Gleichheit des höchsten Koeffizienten ist klar. Wir haben $X_{P\bullet Q}$ gerade so gewählt, dass auch der zweithöchste Koeffizient übereinstimmt. An zwei verschiedenen Stellen, nämlich X_P und X_Q, ist die Auswertung gleich:

$$\begin{aligned} 4X_P^3 - g_2X_P - g_3 &\overset{P\in\mathbb{E}}{=} Y_P^2 \overset{P\in\Gamma_{P,Q}}{=} (a_{P,Q}X_P + b_{P,Q})^2 \\ &= 4(X_P - X_P)(X_P - X_Q)(X_P - X_{P\bullet Q}) + (a_{P,Q}X_P + b_{P,Q})^2. \end{aligned}$$

Analog für X_Q.

Mit zwei gleichen Koeffizienten und zwei gleichen Auswertungen stimmen die Polynome, die Grad drei haben, überein. □

Unsere anfänglich angestellten Überlegungen führen nun sofort zum gewünschten Ergebnis.

(1.4) Korollar
Für $P, Q \in \mathbb{E}$ mit $X_P \neq X_Q$ gilt $P \bullet Q \in \mathbb{E}$. ◇

— *Eine Tangente durch* $P \in \mathbb{E}$ —

Für $P = Q$ geht obige Konstruktion in die Tangente durch P über. Diese wollen wir hier betrachten. Wir setzen $Y_P \neq 0$ voraus, wieder um den projektiven Fall auszuschließen.

In diesen Punkten können wir die elliptische Kurve lokal als Graphen einer Funktion $f : \mathbb{C} \to \mathbb{C}$ auffassen und können so einen sinnvollen Steigungsbegriff benutzen.

$$\begin{aligned} \left(Y^2\right)' &= \left(4X^3 - g_2X - g_3\right)' \\ \Rightarrow 2YY' &= 12X^2 - g_2 \\ \Rightarrow Y' &= \frac{12X^2 - g_2}{2Y}. \end{aligned}$$

(1.5) Definition (Tangente in *P*)
Seien $P \in \mathbb{E}$ mit $Y_P \neq 0$. Dann bezeichnen wir mit

$$a_P := \frac{12X_P^2 - g_2}{2Y_P} \qquad \text{und}$$
$$b_P := Y_P - a_P X_P$$

die Steigung beziehungsweise den Ordinatenabschnitt einer Tangenten in P an $\mathbb{E}$ und setzen

$$\Gamma_P := \text{Graph}\left(f : \mathbb{C} \to \mathbb{C},\ x \mapsto a_P x + b_P\right). \qquad \diamond$$

Unter der Annahme einer gewissen Stetigkeit macht es Sinn, in den Überlegungen zur Geraden durch P, Q, insbesondere in 1.2, $X_Q = X_P$ zu setzen. Dann ergibt sich als Definition für $P \bullet P$:

(1.6) Definition (Der Punkt *P* • *P*)
Sei P wie in 1.5. Dann wird $P \bullet P$ definiert vermöge:

$$X_{P\bullet P} := \frac{1}{4}a_P^2 - 2X_P \qquad \text{und}$$
$$Y_{P\bullet P} := a_P X_P + b_P.$$

Ist $P \in \mathbb{E}$ mit $Y_P = 0$ so definieren wir $P \bullet P := \mathcal{O}$. $\diamond$

Wieder müssen wir für den ersten Fall beweisen, dass $P \bullet P \in \mathbb{E}$ gilt. Wir kommen mit einer analogen Beweisidee zum Erfolg.

(1.7) Lemma
Mit P wie in 1.5 gilt

$$4X^3 - g_2X - g_3 = 4(X - X_P)^2(X - X_{P\bullet P}) + (a_PX + b_P)^2. \qquad \diamond$$

Beweis
Wieder stimmt der höchste Koeffizient überein. Als zweithöchsten Koeffizienten haben wir auf der rechten Seite $4(-X_{P\bullet P} - 2X_P) + a_P^2$, welcher nach Wahl von $X_{P\bullet P}$ mit 0 übereinstimmt. Analog zur Rechnung in 1.3 gilt Gleichheit der Auswertungen in X_P. Wir betrachten nun die Ableitungen, die übereinstimmen sollen:

$$12X^2 - g_2 = 8(X - X_P)(X - X_{P\bullet P}) + 4(X - X_P)^2 + 2(a_PX + b_P)a_P$$

Bei Einsetzen von X_P geht die rechte Seite über in $2(a_PX_P + Y_P - a_PX_P)a_P = 2Y_Pa_P = 12X_P^2 - g_2$. Wir haben also Gleichheit der Auswertung der Polynome und ihrer Ableitungen in X_P. Zusammen mit der Übereinstimmung der beiden höchsten Koeffizienten ergibt sich hieraus die Gleichheit der beiden Polynome vom Grad drei.□

(1.8) Korollar
Für $P \in \mathbb{E}$ mit $Y_P \neq 0$ gilt $P \bullet P \in \mathbb{E}$. $\diamond$

Beweis
Indem wir die Aussage aus 1.7 benutzen und $X_{P\bullet P}$ einsetzen, erhalten wir

$$4X_{P\bullet P}^3 - g_2X_{P\bullet P} - g_3 = (a_PX_{P\bullet P} + b_P^2)^2 = Y_{P\bullet P}^2 \,,$$

was uns die Behauptung liefert. □

Bisher ist $\bullet$ noch nicht auf ganz $\mathbb{PE}$ definiert. Die fehlenden Fälle ergänzen wir jetzt:

(1.9) Definition (Die Punkte $P \bullet \mathcal{O}$ und $\mathcal{O} \bullet P$)
Für $P = (X_P, Y_P) \in \mathbb{E}$ definieren wir:

$$P \bullet \mathcal{O} := \mathcal{O} \bullet P := (X_P, -Y_P) \quad \text{und darüber hinaus}$$
$$\mathcal{O} \bullet \mathcal{O} := \mathcal{O}. \qquad \diamond$$

Mit $\bullet : \mathbb{PE} \times \mathbb{PE} \to \mathbb{PE}$ haben wir also einer innere Verknüpfung. Unser natürliches Interesse wird darin liegen, die Struktur dieser oder abgeleiteter Verknüpfungen zu untersuchen.

§ 2 Zusammenhang mit der $\wp$-Funktion

Wir kennen bereits die Bijektion

$$\Phi : \mathbb{C}/\Omega \to \mathbb{PE}(\Omega),\ z+\Omega \mapsto \begin{cases} (\wp(z), \wp'(z)) & \text{für } z \notin \Omega, \\ \mathcal{O} & \text{für } z \in \Omega, \end{cases}$$

die uns erlaubt, für diesen Abschnitt folgende Vereinbarung für $u, v \in \mathbb{C}$ zu treffen:

$$P := \Phi(u+\Omega),\ Q := \Phi(v+\Omega).$$

Nun können wir einen ersten strukturellen Zusammenhang zwischen $\mathbb{C}/\Omega$ und $\mathbb{PE}$ vermöge Φ beweisen.

(2.1) Lemma (Zusammenhang von $+$ und $\bullet$)
Seien $u, v, w \in \mathbb{C} \setminus \Omega$ mit $u+v+w \in \Omega$, so dass $u+\Omega$, $v+\Omega$, $w+\Omega$ paarweise verschieden sind. Dann gilt

$$P \bullet Q = \Phi(u+\Omega) \bullet \Phi(v+\Omega) = \Phi(w+\Omega) = \Phi(-u-v+\Omega). \qquad \diamond$$

Beweis
Wir zeigen, dass $a_{P,Q}$ und $b_{P,Q}$ definiert sind. Gilt $\wp(u) = X_P = X_Q = \wp(v)$, so folgt $u - v \in \Omega$ oder $w = u + v \in \Omega$. Letzeres ist ein Widerspruch zu den Voraussetzungen. Aus dem Ersten folgt $u + \Omega = v + \Omega$, was ebenfalls ein Widerspruch ist.

Wir können also die Funktion $f : z \mapsto \wp'(z) - (a_{P,Q}\wp(z) + b_{P,Q})$ betrachten, die als Summe elliptischer Funktionen zum gleichen Gitter elliptisch ist. Darüber hinaus hat $\wp'$ einen Pol dritter Ordnung in 0 und die beiden anderen Summanden haben höchstens Pole von Ordnung zwei. Mithin besitzt f einen Pol dritter Ordung in 0. Auf der Grundmasche sind alle Summanden holomorph außer in Null und mithin ist dies der einzige Pol von f. Folglich besitzt f genau drei mit Vielfachheit gezählte Nullstellen in $\mathbb{C}/\Omega$.

Wir haben

$$f(u) = \wp'(u) - (a_{P,Q}p(u) + b_{P,Q}) = Y_P - (a_{P,Q}X_P + b_{P,Q}) = 0 \quad \text{und}$$
$$f(v) = \wp'(v) - (a_{P,Q}p(v) + b_{P,Q}) = Y_Q - (a_{P,Q}X_Q + b_{P,Q}) = 0.$$

Nun haben wir bereits bewiesen, dass für eine Grundmasche M gilt:

$$\sum_{c \in M} c \cdot \operatorname{ord}(c) \in \Omega.$$

Nennen wir also die drei Nullstellen, die wir in der Grundmasche zu erwarten haben, u, v, n, die zunächst nicht notwendigerweise verschieden seien müssen. Dann ergibt sich durch Einsetzen:

$$\begin{aligned} & 0 \cdot (-3) + u \cdot 1 + v \cdot 1 + n \cdot 1 \in \Omega \\ \Rightarrow\ & w + \Omega = n + \Omega \\ \Rightarrow\ & f(w) = 0. \end{aligned}$$

Wenn wir $R := \Phi(w + \Omega)$ setzen, erhalten wir so $0 = f(w) = Y_R - (a_{P,Q} X_R + b_{P,Q})$ und mithin R als Schnittpunkt von der Geraden durch P und Q mit $\mathbb{E}$. Wir wollen nun zeigen, dass $R = P \bullet Q$ gilt. Dazu reicht es zu zeigen, dass $P \bullet Q$ von P und Q verschieden ist, denn wir können, da sich durch das Gleichsetzen der Y-Koordinaten eine Polynomegleichung dritten Grades in einer Variablen ergibt, maximal drei Schnittpunkte erwarten, und da $R \neq P \neq Q \neq R$ gilt, müssen dann folglich die Schnittpunkte R und $P \bullet Q$ übereinstimmen.

Angenommen, es gilt $P \bullet Q = P$. Dann auch insbesondere $X_P = X_{P \bullet Q}$. Es muss $Y_P \neq 0$ gelten, denn sonst folgt $\wp'(u) = 0$ und auch $u + v = 2u \in \Omega$ also $w \in \Omega$ mit Widerspruch zur Voraussetzung. Wir erhalten weiter aus den Polynomgleichheiten 1.3 und 1.7 durch Vergleich der Koeffizienten von X^2 und X^1:

$$\begin{aligned} & 4(X - X_P)(X - X_Q)(X - X_{P \bullet Q}) + (a_{P,Q} X + b_{P,Q})^2 \\ & \quad = 4(X - X_P)^2 (X - X_{P \bullet P}) + (a_P X + b_P)^2 \\ \Rightarrow\ & 4(-X_P - X_Q - X_{P \bullet Q}) + a_{P,Q}^2 = 4(-2X_P - X_{P \bullet P}) + a_P^2 \\ & \quad \wedge\ 4(X_P X_Q + X_P X_{P \bullet Q} + X_Q X_{P \bullet Q}) + 2a_{P,Q} b_{P,Q} = 4(X_P^2 + 2X_P X_{P \bullet P}) + 2a_P b_P \\ \Rightarrow\ & 4(-X_P - X_Q - X_{P \bullet Q}) + a_{P,Q}^2 = 4(-2X_P - X_{P \bullet P}) + a_P^2 \\ & \quad \wedge\ 4(X_P X_Q + X_P X_{P \bullet Q} + X_Q X_{P \bullet Q}) + 2a_{P,Q}(Y_P - a_{P,Q} X_P) \\ & \quad\quad = 4(X_P^2 + 2X_P X_{P \bullet P}) + 2a_P(Y_P - a_P X_P) \\ \Rightarrow\ & 4(-2X_P - X_Q) + a_{P,Q}^2 = 4(-2X_P - X_{P \bullet P}) + a_P^2 \\ & \quad \wedge\ 4(X_P X_Q + X_P X_P + X_Q X_P) + 2a_{P,Q}(Y_P - a_{P,Q} X_P) \\ & \quad\quad = 4(X_P^2 + 2X_P X_{P \bullet P}) + 2a_P(Y_P - a_P X_P), \end{aligned}$$

wenn wir nun $X_P = X_{P \bullet Q}$ verwenden. Schließlich erhalten wir unter Berücksichtigung von $Y_P \neq 0$:

$$\begin{aligned}
&\Rightarrow -4X_Q + a_{P,Q}^2 = -4X_{P\bullet P} + a_P^2 \\
&\quad \wedge X_P(8X_Q - 2a_{P,Q}^2) + 2a_{P,Q}Y_P = X_P(8X_{P\bullet P} - 2a_P^2) + 2a_P Y_P \\
&\Rightarrow 2a_{P,Q}Y_P = 2a_P Y_P \qquad \text{nach Einsetzen} \\
&\Rightarrow a_{P,Q} = a_P \Rightarrow b_{P,Q} = b_P.
\end{aligned}$$

Mithin handelt es sich um eine Tangente an P und es existieren höchstens zwei verschiedene Schnittpunkte im Widerspruch zur Existenz von R, also gilt $P \bullet Q \neq P$. Aus Symmetriegründen folgt nun auch $P \bullet Q \neq Q$ und wir sind fertig. □

Auf $(\mathbb{C}/\Omega, +)$ haben wir eine kanonisch von $\mathbb{C}$ induzierte Gruppenstruktur, die sich vermöge Φ auf $\mathbb{PE}$ überträgt. Mit dem Lemma 2.1 wollen wir diese geometrisch verstehen. Dazu definieren wir zunächst:

(2.2) Definition
Für $P = (X_P, Y_P) \in \mathbb{C} \times \mathbb{C}$ setzen wir

$$P^* := (X_P, -Y_P).$$

Für $P = \mathcal{O}$ definieren wir darüber hinaus $P^* = P = \mathcal{O}$. ◇

Nun erhalten wir folgende Aussage.

(2.3) Satz (Geometrische Addition auf $\mathbb{PE}$)
Für $P, Q \in \mathbb{PE}$ gilt:

$$\begin{aligned}
&P + Q = (P \bullet Q)^* \quad \text{und weiterhin} \\
&-P = P^*.
\end{aligned}$$

◇

Beweis
Wir beweisen zunächst die zweite Aussage. Vermöge der durch Φ definierten Addition erhalten wir:

$$\begin{aligned}
&-P = (\wp(-u), \wp'(-u)) = (\wp(u), -\wp'(u)) = P^* \quad \text{für } P \neq \mathcal{O} \\
&-\mathcal{O} = \mathcal{O} = \mathcal{O}^*, \quad \text{da } \mathcal{O} \text{ neutrales Element ist.}
\end{aligned}$$

Wir betrachten zunächst den Fall $P, Q \in \mathbb{E} \subset \mathbb{PE}$. Wenn $P, Q, P \bullet Q$ paarweise verschieden sind, erhalten wir nach 2.1

$$\begin{aligned} P + Q &= \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)) = \Phi(u + v + \Omega) = \Phi(-w + \Omega) \\ &= (\wp(w), -\wp'(w)) = (\Phi(w + \Omega))^* = (P \bullet Q)^*. \end{aligned}$$

Nun sind $\wp, \wp'$ auf $\mathbb{C} \setminus \Omega$ stetig und offen und mithin ist das bijektive Φ Homöomorphismus, also ist $+$ auf $M := \mathbb{E}^2 \setminus \{(P, P) : Y_P = 0\}$ stetig. Gleiches gilt für $\bullet$. Als homöomorphes Bild von $\mathbb{C}^2 \setminus \{(u, u) : u \in \frac{1}{2}\Omega\}$ hat M keine isolierten Punkte, die Menge der Punkte, für die wir bereits den Zusammenhang bewiesen haben, liegt dicht und mithin gilt obiger Zusammenhang auf ganz M.

Sei nun P mit $Y_P = 0$ gegeben. Dann gilt $u \in \frac{1}{2}\Omega \setminus \Omega$, also

$$P + P = \Phi(2u + \Omega) = \Phi(\Omega) = \mathcal{O} = \mathcal{O}^* = (P \bullet P)^*.$$

Für $P = \mathcal{O}$ oder $Q = \mathcal{O}$ folgt die Behauptung sofort aus den Definitionen. □

Das Additionstheorem ist von grundlegendem Interesse. Wir wollen einen weiteren Beweis angeben, der im Licht des letzten Satzes eine geometrische Interpretation erlaubt.

(2.4) Satz (Additionstheorem)
Für alle $u, v \in \mathbb{C}$ mit $u, v, u \pm v \notin \Omega$ gilt

$$\wp(u + v) + \wp(u) + \wp(v) = \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2. \qquad \diamond$$

Beweis
Aus 2.1 folgt für $u, v, w = -u - v \in \mathbb{C} \setminus \Omega$, wenn $u + \Omega, v + \Omega, w + \Omega$ paarweise verschieden sind, unter Beachtung der Definitionen 1.1 und 1.2 :

$$\begin{aligned} &\wp(u + v) = \wp(-w) = \wp(w) \\ &= X_{P \bullet Q} = \frac{1}{4}a_{P,Q}^2 - X_P - X_Q \\ &= \frac{1}{4}\left(\frac{Y_P - Y_Q}{X_P - X_Q}\right)^2 - X_P - X_Q \\ &= \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v), \end{aligned}$$

was nach Umformung sofort zur behaupteten Formel führt.

Aus $u, v, u+v \notin \Omega$ und der paarweisen Verschiedenheit der $u+\Omega, v+\Omega, w+\Omega$ folgt, dass $u - v \notin \Omega$ gilt, denn sonst würde $u + \Omega = v + \Omega$ gelten, und so erhalten wir auch $\wp(u) \neq \wp(v)$ und der Bruch ist wohldefiniert.

Nun sind beide Seiten der zu beweisenden Gleichung stetig auf ihrem Definitionsbereich, denn die $\wp$-Funktion ist dies. Gilt also die geforderte paarweise Verschiedenheit nicht, sondern wie in der Voraussetzung schwächer $u, v, u \pm v \notin \Omega$, so folgt die Formel daraus, dass wir in jeder Umgebung des betrachteten Paares $(u, v) \in \mathbb{C}^2$ ein entsprechendes Paar $(u+\varepsilon, v+\tilde{\varepsilon}) \in \mathbb{C}^2$ finden, das alle Voraussetzungen des schon bewiesenen Teils erfüllt. □

(2.5) Bemerkung
Drei Punkte $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in \mathbb{C}^2$ sind kollinear genau dann, wenn

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} = 0$$

zutrifft. Da wir $P, Q, P \bullet Q$ so definiert haben, dass sie auf einer Gerade liegen, folgt mit 2.1 für $u, v, w \in \mathbb{C} \setminus \Omega$ mit $u + v + w \in \Omega$

$$\det \begin{pmatrix} 1 & 1 & 1 \\ \wp(u) & \wp(v) & \wp(w) \\ \wp'(u) & \wp'(v) & \wp'(w) \end{pmatrix} = 0,$$

denn für nicht paarweise verschiedene $u+\Omega, v+\Omega, w+\Omega$ ist dies offensichtlich. ⋄

§ 3 Rationale Punkte und eine Anwendung

— $\mathbb{PE}_{\mathbb{Q}} \leq \mathbb{PE}$ —

Wenn Ω ein Gitter zu $g_2, g_3 \in \mathbb{Q}$ ist, so gilt $4X^3 - g_2 X - g_3 - Y^2 \in \mathbb{Q}[X, Y]$, also können wir die bisher betrachtete Nullstellenmenge $\mathbb{PE}$ auch über $\mathbb{Q}$ untersuchen, das heißt die Punkte untersuchen, die rationale Koordinaten besitzen, und bezeichnen sie dann mit $\mathbb{PE}_{\mathbb{Q}}$. Wir konnten im letzten Abschnitt für $P, Q \in \mathbb{E}$ mit $P \neq Q$ oder $Y_P \neq 0$ die Koordinaten X_{P+Q} und Y_{P+Q} rational in X_P, X_Q, Y_P, Y_Q und g_2 darstellen. Mithin ist $\mathbb{PE}_{\mathbb{Q}}$ Untergruppe von $\mathbb{PE}$. Diese besitzt Eigenschaften, die von großem Vorteil sind, so ist sie beispielsweise stets endlich erzeugt.

Wir betrachten zunächst einige Beispiele, bevor wir zu einer Anwendung kommen.

(3.1) Beispiele

a) Es lässt sich zeigen, dass gilt

$$\mathbb{F}_{\mathbb{Q}} := \{(u,v) \in \mathbb{Q}^2 : u^3 + v^3 = 1\} = \{(1,0),(0,1)\}.$$

Vermöge $(u,v) \mapsto \left(\frac{12}{u+v}, 72\frac{u-v}{u+v}\right)$ mit Umkehrung $(x,y) \mapsto \left(\frac{72+y}{12x}, \frac{72-y}{12x}\right)$ lässt sich $\mathbb{F}_{\mathbb{Q}}$ nun birational auf

$$\mathbb{E}_{\mathbb{Q}} := \{(x,y) \in \mathbb{Q}^2 : y^2 = 4x^3 - 1728\} = \{(12,72),(12,-72)\}$$

abbilden. Mithin ist $\mathbb{PE}_{\mathbb{Q}}$ von Ordnung 3 und zyklisch.

b) Wenn wir

$$\mathbb{E} := \{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - 4x + 4\}$$

betrachten, sehen wir, dass $P := (1,2) \in \mathbb{E}_{\mathbb{Q}}$. Wir rechnen für $2P$ nach:

$$a_P = \frac{12 \cdot 1^2 - 4}{2 \cdot 2} = 2,$$
$$b_P = 2 - 2 \cdot 1 = 0,$$
$$X_{2P} = \frac{1}{4}2^2 - 2 \cdot 1 = -1,$$
$$Y_{2P} = 2 \cdot 1 + 0 = 2,$$

also $2P = (-1,2)$. Weitere Punkte sind:

$$3P = (0,-2),\ \ 4P = (3,-10),\qquad 5P = (5,22)$$
$$6P = \left(\tfrac{1}{4}, \tfrac{7}{4}\right),\ \ 7P = \left(-\tfrac{11}{9}, \tfrac{34}{27}\right),\ \ 8P = \left(\tfrac{19}{25}, -\tfrac{206}{125}\right).$$

Man kann nun zeigen, dass als Gruppen $\mathbb{PE}_{\mathbb{Q}} = \langle P \rangle \cong \mathbb{Z}$ gilt. ◇

(3.2) Bemerkung

Die Eigenschaften von $\mathbb{PE}$ lassen sich zur Faktorisierung einer natürlichen Zahl n benutzen. Dieses Verfahren, das H. W. Lenstra entwickelt hat, hat sich als sehr effektiv herausgestellt.

Man erzeugt natürliche Zahlen x, y, g_2 und setzt $g_3 := 4x^3 - g_2x - y^2$. Gilt nun $g_2^3 - 27g_3^2 \neq 0$, so haben wir

$$P := (x,y) \in \mathbb{E}_{\mathbb{Q}} := \{(u,v) : v^2 = 4u^3 - g_2u - g_3\}.$$

Wir berechnen nun die Vielfachen kP in $\mathbb{Z}/n\mathbb{Z}$ solange die Nenner in 1.5 beziehungsweise 1.1 teilerfremd zu n sind. So erhalten wir entweder die Punkte kP auf $\mathbb{E}_{\mathbb{Q}} (\text{mod } n)$ oder einen Teiler von n. ◇

— *Eine Anwendung in der Zahlentheorie* —

(3.3) Definition (Dreieckszahlen)
Eine positive ganze Zahl $f \in \mathbb{Z}_{>0}$ heißt *Dreieckszahl* oder HERON-*Zahl*, genau dann wenn es ein rechtwinkliges Dreieck mit rationalen Seitenlängen $a, b, c \in \mathbb{Q}$ und Fläche f gibt. ◇

(3.4) Bemerkung
Wir können ohne Einschränkung annehmen, dass $c > a, b$ gilt. Für die Untersuchung der Dreieckszahlen, kann man ohne weitere Einschränkung annehmen, dass f quadratfrei ist, da für $n \in \mathbb{N}$ gilt:

$$n^2 f = \frac{1}{2}(na)(nb) \quad \text{mit } na, nb \in \mathbb{Q},$$
$$\frac{f}{n^2} = \frac{1}{2}\frac{a}{n}\frac{b}{n} \quad \text{mit } \frac{a}{n}, \frac{b}{n} \in \mathbb{Q}.$$

◇

Mit rechtwinkligen Dreiecken in direktem Zusammenhang stehen pythagoreische Tripel.

(3.5) Definition (Pythagoreische Tripel)
Ein Tripel $(a, b, c) \in \mathbb{N}^3$ heißt pythagoreisch, wenn gilt $a^2 + b^2 = c^2$. Gilt darüber hinaus $\mathrm{ggT}(a, b, c) = 1$, nennen wir dieses Tripel primitiv. ◇

Es ist nun eine erste Idee, pythagoreische Tripel zur Lösung des Problems heranzuziehen. Wir beweisen zunächst ein Ergebnis zu diesen Tripeln, mit dem wir das betrachtete Problem beschreiben können.

(3.6) Lemma
Sei $(a, b, c) \in \mathbb{Z}^3$ ein primitives pythagoreisches Tripel mit $2 \mid b$. Dann existieren $u, v \in \mathbb{Z}$ mit

$$a = u^2 - v^2, \;\; b = 2uv, \;\; c = u^2 + v^2.$$

Es gilt $u > v > 0$, $u \not\equiv v \pmod 2$. ◇

Beweis
Wir zeigen zuerst, dass $\frac{c \pm a}{2}$ eine Quadratzahl ist.

Bezeichne $\mathrm{n}_p(z)$ für p prim und $z \in \mathbb{N}$ die Potenz von p in der Primfaktorzerlegung von z. Dass $2 \mid c \pm a$ gilt, ist klar, da $2 \nmid a, c$.

Wir haben $(c+a)(c-a) = c^2 - a^2 = b^2$. Angenommen, es gilt $4 \mid c+a, c-a$. Dann erhalten wir durch Addition beziehungsweise Subtraktion:

$$\begin{aligned} &\frac{c \pm a}{4} \in \mathbb{Z} \\ \Rightarrow &\frac{c+a}{4} + \frac{c-a}{4} = \frac{2c}{4} = \frac{c}{2},\ \frac{a}{2} \in \mathbb{Z}. \end{aligned}$$

Dann aber ist $(a/2, b/2, c/2)$ ein pythagoreisches Tripel und (a,b,c) war nicht primitiv, also gilt $\mathrm{n}_2(c+a) = 1$ oder $\mathrm{n}_2(c-a) = 1$, und da $2 \mid \mathrm{n}_2(b^2)$ gilt mit $\mathrm{n}_2(b^2) = \mathrm{n}_2(c+a) + \mathrm{n}_2(c-a)$, folgt $2 \mid \mathrm{n}_2(\frac{c \pm a}{2})$.

Sei nun $p \neq 2$ eine Primzahl. Angenommen, es gilt $p \mid c+a, c-a$, dann folgt analog zum obigen Vorgehen

$$\begin{aligned} &\frac{c \pm a}{p} \in \mathbb{Z} \\ \Rightarrow &\frac{2c}{p}, \frac{2a}{p} \in \mathbb{Z} \\ \Rightarrow &\frac{c}{p}, \frac{a}{p} \in \mathbb{Z}. \end{aligned}$$

Wegen $a^2 + b^2 = c^2$ gilt darüber hinaus $p \mid b$ und (a,b,c) wäre nicht primitiv. Folglich haben wir $\mathrm{n}_p(c+a) = 0$ oder $\mathrm{n}_p(c-a) = 0$, und da $2 \mid \mathrm{n}_p(b^2)$ gilt, folgt schließlich $2 \mid \mathrm{n}_p\left(\frac{c \pm a}{2}\right)$.

Die Zahlen $(c \pm a)/2$ sind also tatsächlich Quadratzahlen und wir können definieren

$$u := \sqrt{\frac{c+a}{2}}, \quad v := \sqrt{\frac{c-a}{2}}.$$

Dann sind u, v positive ganze Zahlen. Man rechnet direkt nach, dass 3.6 gilt. Da $a = u^2 - v^2$ und $2 \nmid a$ gilt, folgt daraus auch $u \not\equiv v \pmod 2$ und $u > v > 0$. □

(3.7) Proposition
Eine positive ganze, quadratfreie Zahl f ist genau dann eine Dreieckszahl, wenn es eine ganze Zahl q und teilerfremde ganze Zahlen u, v gibt mit

$$q^2 f = uv(u^2 - v^2) \quad \wedge \quad u > v, u \not\equiv v \pmod 2. \qquad \diamond$$

Beweis
Sei f Dreieckszahl. Man wähle a, b, c nach der Definition 3.3 und $q \in \mathbb{N}$, so dass qa, qb, qc ein primitives pythagoreisches Tripel ist. Wir wollen ohne Einschränkung annehmen, dass qb gerade ist.

Um zu zeigen, dass dies möglich ist, nehmen wir an, es gilt $2 \nmid qa, qb$. Dann folgt $2 \mid (qc)^2$ und mithin $4 \mid (qc)^2$. Wegen $2 \nmid qa, qb$ gilt $(qa)^2, (qb)^2 \equiv 1 \pmod 4$. Schließlich ist $2 \equiv (qa)^2 + (qb)^2 \equiv (qc)^2 \equiv 0 \pmod 4$ ein Widerspruch. Wir können also tatsächlich ohne Einschränkung qb als gerade voraussetzen.

Nun können wir u, v nach 3.6 zu (qa, qb, qc) wählen und erhalten $q^2 f = \frac{1}{2} qaqb = uv(u^2 - v^2)$, was gefordert war.

Ist umgekehrt eine Darstellung nach 3.7 gegeben, so setzen wir

$$a := \tfrac{u^2 - v^2}{q}, \quad b := \tfrac{2uv}{q}, \quad c := \tfrac{u^2 + v^2}{q}$$

und erhalten $a^2 + b^2 = \frac{u^4 + v^4 - 2u^2v^2 + 4u^2v^2}{q^2} = c^2$ und $f = \frac{1}{q^2} uv(u^2 - v^2) = \frac{1}{2} ba$. □

Damit haben wir allerdings nur bewiesen, dass es sich um ein Semi-Entscheidungsverfahren für die Dreieckszahlen handelt. Dieses ist darüber hinaus nicht sonderlich effektiv, da sehr große q, u, v auftreten können.

(3.8) Beispiel
Die 19 quadratfreien Dreieckszahlen ≤ 50 sind 5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47. Für 47 erhalten wir bereits $q = 12111037689240 \approx 10^{13}$, $u = 14561856 \approx 10^7$, $v = 2289169 \approx 10^6$. Eine Dreieckszahl mit großem q, u, v ist 157. Hier er gibt sich

$$q = 89123322689288595880255351789671635700164808 30 \approx 10^{42},$$
$$u = 44362401899742989970992 5 \approx 10^{23},$$
$$v = 16613623166818526754080 4 \approx 10^{23}.$$

◇

Folgender Zusammenhang stellt dagegen eine Möglichkeit dar, das Problem mit anderen Methoden zu behandeln.

(3.9) Lemma
Für eine positive, quadratfreie ganze Zahl f sind äquivalent:

(i) f ist eine Dreieckszahl

(ii) Es existiert ein rationaler Punkt (x, y) auf der elliptischen Kurve $Y^2 = 4X^3 - 4f^2X$, so dass x ein Quadrat in $\mathbb{Q}$ mit geradem $\nu(x)$ und $\mathrm{ggT}(\zeta(x), f) = 1$ ist, wo $\nu(q)$ den Nenner und $\zeta(q)$ den Zähler einer Zahl $0 \neq q \in \mathbb{Q}$ in gekürzter Darstellung angibt. ◇

Beweis
(i) $\Rightarrow$ (ii) : Seien $a, b, c \in \mathbb{Q}$ aus der Definition der Dreieckszahlen 3.3 entnommen und $q = \mathrm{kgV}(\nu(a), \nu(b))$. Da f quadratfrei ist, ist (qa, qb, qc) primitives pythagoreisches Tripel. Um dies zu zeigen, stellen wir a, b dar als $a = a_\mathrm{R}/(a_\mathrm{N} \cdot g_\mathrm{N}), b = b_\mathrm{R}/(b_\mathrm{N} \cdot g_\mathrm{N})$ mit teilerfremden a_N und b_N, weiter a_R teilerfremd zu a_N und g_N und schließlich b_R teilerfremd zu b_N und g_N. Dann gilt $qa = a_\mathrm{R} b_\mathrm{N}$ und $qb = b_\mathrm{R} a_\mathrm{N}$. Gilt nun $n \mid qa, qb$ für ein $n \in \mathbb{N}$, erhalten wir wegen der verlangten Teilerfremdheiten hieraus $n \mid a_\mathrm{R}, b_\mathrm{R}$. Ist $2 \neq n$, gelangen wir wieder wegen der geforderten Teilerfremdheiten und $n^2 \mid f = a_\mathrm{R} b_\mathrm{R}/(2 a_\mathrm{N} b_\mathrm{N} g_\mathrm{N}^2)$ zu einem Widerspruch.

Wir beweisen nun noch, dass aus $2 \mid qa, qb$ auch $4 \mid f$ folgt. Es gilt $q^2a^2 \equiv 0 (\mathrm{mod}\ 16)$ oder $q^2a^2 \equiv 4 (\mathrm{mod}\ 16)$ und dann auch $q^2a^2 + q^2b^2 \equiv q^2c^2 \in \{0, 4, 8\} + \mathbb{Z}/16\mathbb{Z}$. Da es sich aber um eine Quadratzahl handelt, fällt 8 als Möglichkeit weg. Dann galt aber für mindestens einer der beiden Zahlen qa, qb bereits, dass sie von 4 geteilt wird. Da nun für $n = 2$ bereits $2 \nmid a_\mathrm{N}, b_\mathrm{N}, g_\mathrm{N}$ gilt, erhalten wir $4 \mid f = a_\mathrm{R} b_\mathrm{R}/(2 a_\mathrm{N} b_\mathrm{N} g_\mathrm{N}^2)$ als Widerspruch zur Quadratfreiheit von f.

Daher ist (qa, qb, qc) primitiv und wir können nach 3.6 $u, v \in \mathbb{Z}$ zu diesem Tripel wählen.

Nun ist $qc = u^2 + v^2$ ungerade und mithin auch $\zeta(c)$. Dann aber ist $\nu(x)$ für $x := (\frac{c}{2})^2$ gerade, weil sich der Faktor zwei nicht herauskürzt. Da $\mathrm{ggT}(qa, qb) = 1$ und wegen $a_\mathrm{R} \mid qa$ und $b_\mathrm{R} \mid qb$ auch insbesondere $\mathrm{ggT}(a_\mathrm{R}, b_\mathrm{R}) = 1$ gilt, erhalten wir

$$\begin{aligned}\mathrm{ggT}(\zeta(x), f) &= \mathrm{ggT}\left(\zeta\left(\frac{a^2+b^2}{4}\right), \zeta\left(\frac{ab}{2}\right)\right) \\ &= \mathrm{ggT}(\underbrace{\zeta(a^2+b^2)}_{\cdot | a_\mathrm{R}^2 b_\mathrm{N}^2 + a_\mathrm{N}^2 b_\mathrm{R}^2}, \underbrace{\zeta(ab)}_{\cdot | a_\mathrm{R} b_\mathrm{R}}) = 1,\end{aligned}$$

denn ein gemeinsamer Primteiler, der a_R teilt, würde auch $a_\mathrm{N}^2 b_\mathrm{R}^2$ teilen, was nicht möglich ist. Für gemeinsame Teiler, die b_R teilen, folgt analog ein Widerspruch.

Wir haben schließlich

$$\begin{aligned}x \pm f &= \frac{a^2+b^2}{4} \pm \frac{1}{2}ab = \left(\frac{a \pm b}{2}\right)^2, \\ 4x^3 - 4f^2x &= 4x(x^2 - f^2) = 4x(x+f)(x-f) \\ &= \frac{c^2(a+b)^2(a-b)^2}{16} =: y^2 \in \mathbb{Q}^2.\end{aligned}$$

(ii) $\Rightarrow$ (i) : Seien $\alpha := \sqrt{x} \in \mathbb{Q}$, $\beta := \frac{y}{\alpha}$. Da (x, y) auf der elliptischen Kurve liegt, gilt

$$\beta^2 = 4x^2 - 4f^2 \Leftrightarrow \beta^2 + 4f^2 = 4x^2.$$

Nach Voraussetzung ist $\nu(x)$ und dann auch $t := \nu(\alpha)$ gerade. Da f ganz ist, erhalten wir aus der letzten Gleichung $\nu(\beta^2) = \nu(4x^2) = t^4/4$. Dann ist also $(t^2\beta/2, t^2 f, t^2 x)$ wegen $t^2 x = \zeta(x)$, $t^2 = \nu(x)$ und $\mathrm{ggT}(\nu(x)f, \zeta(x)) = 1$ ein primitives pythagoreisches Tripel und wir können u, v nach 3.6 wählen, was zu

$$\frac{t^2\beta}{2} = u^2 - v^2, \;\; t^2 f = 2uv, \;\; t^2\alpha^2 = u^2 + v^2$$

führt. Nach der letzten Gleichung ist $(u, v, t\alpha)$ pythagoreisch und mithin auch $(\frac{2u}{t}, \frac{2v}{t}, 2\alpha)$. Es ergibt sich ein Flächeninhalt des entsprechenden Dreiecks zu $\frac{1}{2}\frac{2u}{t}\frac{2v}{t} = \frac{2uv}{t^2} = f$. □