Addition von Punkten auf elliptischen Kurven

Winterschule 2001

Prof. Dr. Annette Huber-Klawitter huber@mathematik.uni-leipzig.de
Augustusplatz 10/11
04109 Leipzig

Definition: Eine *elliptische Kurve* ist

$$\{(x, y) \in \mathbf{R}^2 \mid E(x, y) = 0\}$$

wobei E ein (nicht-singuläres) Polynom dritten Grades in den Variablen x und y ist.

Beispiele: $y^3 + x^3 - 1$, $y^2 = x(x+1)(x+2)$, $27x^3 - x^2y + y - 2001$.

Satz: In der projektiven Ebene schneiden sich eine Gerade und eine elliptische Kurve in einem oder in drei Punkten (mit Vielfachheiten gezählt).

Definition: Wir fixieren einen Punkt O auf E. Seien P und Q beliebige Punkte auf E. Dann wird

$$P \oplus Q$$

konstruiert:

- Sei H der dritte Schnittpunkt der elliptischen Kurve mit der Geraden durch P und Q.
- Sei $P \oplus Q$ der dritte Schnittpunkt der elliptischen Kurve mit der Geraden durch H und O.

Regenregeln:

$$O \oplus P = P \tag{1}$$

$$P \oplus Q = Q \oplus P \tag{2}$$

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R) \tag{3}$$

Für jedes P gibt es ein Q mit $P \oplus Q = O$. Wir schreiben $Q = \ominus P$. Die Punkte der elliptischen Kurve bilden eine *kommutative Gruppe* mit der Addition $\oplus$.

Wir wollen das Assoziativgesetz (3) beweisen.

Theorem: Sei E eine elliptische Kurve, $P_1 = P$, $P_3 = Q$, $P_8 = R$, $P_6 = O$. Wie im Bild ergeben sich weitere Punkte auf E aus der Addition $P \oplus (Q \oplus R)$ und $(P \oplus Q) \oplus R$, z.B. $P_7 = P \oplus Q$, $P_4 = Q \oplus R$. Seien L_1, L_2, L_3 und G_1, G_2, G_3 die Geraden mit

$$\begin{aligned} P_1, P_2, P_3 &\in L_1 \cap E \\ P_4, P_5, P_6 &\in L_2 \cap E \\ P_7, P_8 &\in L_3 \cap E \\ P_2, P_6, P_7 &\in G_1 \cap E \\ P_3, P_5, P_8 &\in G_2 \cap E \\ P_1, P_4 &\in G_3 \cap E \end{aligned}$$

Sei L die Gleichung für $L_1 \cup L_2 \cup L_3$, G die Gleichung für $G_1 \cup G_2 \cup G_3$. (Es handelt sich um Polynome dritten Grades.) Dann gibt es Zahlen a und b mit

$$L = aE + bG.$$

Folgerung: Sei S der dritte Schnittpunkt der Geraden G_3 mit E. Dann gilt

$$L(S) = aE(S) + bG(S) = a \cdot 0 + b \cdot 0 = 0$$

Also liegt S auf $L_1 \cup L_2 \cup L_3$. Also muss S mit dem dritten Schnittpunkt von L_3 mit E übereinstimmen. Das beweist das Assoziativgesetz. q.e.d.

Zu zeigen ist also das Theorem. Hierfür überlegen wir zuerst:

Hilfssatz: Seien L_1, L_2 zwei Geraden, Q eine Quadrik (d.h. Nullstellenmenge einer quadratischen Gleichung). Seien $P_1, \ldots P_5$ verschiedene Punkte mit $P_1, P_2, P_3 \in L_1 \cap Q$, $P_4, P_5 \in L_2 \cap Q \setminus L_1$. Dann ist $Q = L_1 \cup L_2$.

Beweis: Ohne Einschränkung hat L_1 die Gleichung $x = 0$. Q hat die Gleichung

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Also hat $Q \cap L_1$ die Gleichung

$$0 + 0 + cy^2 + 0 + ey + f.$$

Nach der Lösungsformel für quadratische Gleichungen gibt es höchstens zwei Lösungen. Da der Schnitt aber drei Punkte enthalten soll, gilt $c = e = f = 0$ d.h. $L_1 \subset Q$. Demnach hat Q die Gleichung

$$0 = ax^2 + bxy + dx = x(ax + by + d)$$

P_4, P_5 sind zwei weiter Nullstellen von Q, liegen aber nicht auf $x = 0$. Also sind sie Nullstellen der Geraden $ax + by + d$. Diese Gerade hat mit L_2 zwei Punkte gemeinsam, ist also gleich L_2. q.e.d.

Beweis des Theorems: Wir wählen weitere Punkte $H_1 \in L_1$, $H_2 \notin L_1 \cup L_2 \cup L_3$. Wir bestimmen ein Polynom

$$K = \alpha E + \beta L + \gamma G$$

mit Nullstellen H_1 und H_2. Dafür betrachtet man das Gleichungssystem

$$\alpha E(H_1) + \beta L(H_1) + \gamma G(H_1) = 0 \tag{4}$$
$$\alpha E(H_2) + \beta L(H_2) + \gamma G(H_2) = 0 \tag{5}$$

Es gilt $E(H_1) \neq 0$, da $H_1 \in L_1$ und $E \cap L_1 = \{P_1, P_2, P_3\}$. Also können wir die erste Gleichung nach α auflösen und in die zweite einsetzen. Nun brauchen wir nur noch β oder γ zu wählen und sind fertig.

Angenommen K ist nicht das Nullpolynom. Dann schneiden sich K und L_1 in P_1, P_2, P_3, H_1. Eine Gerade und eine Gleichung dritten Grades schneiden sich aber nur in drei Punkten. Wie im Beweis des Hilfsatzes folgt, dass $K = L_1 \cup Q$, wobei Q eine Quadrik ist. Q und $L_2 \cup L_3$ schneiden sich in $\{P_4, P_5, P_6, P_7, P_8\}$. Nach dem Hilfsatz gilt dann $Q = L_2 \cup L_3$, insgesamt also $K = L_1 \cup L_2 \cup L_3$. Dies ist nicht möglich, da $H_2 \notin L_1 \cup L_2 \cup L_3$ und $H_2 \in K$.

Also haben wir gezeigt, dass es Zahlen α, β und γ gibt mit

$$\alpha E + \beta L + \gamma G = 0$$

Wenn $\beta = 0$, so ist $\alpha E = \gamma G$. G besteht aus drei Geraden, E ist nicht-singulär, also ist das unmöglich. Es gilt also $\beta \neq 0$, und wir können auflösen:

$$L = -\frac{\alpha}{\beta} L - \frac{\gamma}{\beta} G.$$

q.e.d.

Anwendungen:

- Beweis der Fermatschen Vermutung durch Wiles: Die Gleichung $x^n + y^n = z^n$ hat für $n > 2$ keine Lösung in natürlichen Zahlen.
- Kryptografie, z.B. auf der Geldkarte.
- Konstruktion von guten Grafen, z.B. für Telefonnetze.

Satz von Mordell: Sei E eine elliptische Kurve mit rationalen Koeffizienten. Dann gibt es Punkte $P_1, \ldots P_r$ auf E, so dass sich jede rationale Lösung von E eindeutig als

$$P = n_1 P_1 \oplus n_2 P_2 \ldots n_r P_r \oplus T$$

schreiben lässt. Dabei sind $n_1, \ldots n_r$ ganze Zahlen, T ein Torsionspunkt von E (d.h. es gibt eine natürliche Zahl N mit $NT = O$).

Die Zahl r ist eindeutig bestimmt. Sie heißt *Mordell-Rang* von E. Die Vermutung von Birch und Swinnterton-Dyer gibt eine Formel für r an, die aber unbewiesen ist. Für den Beweis hat ein amerikanischer Millionär eine Million Dollar ausgesetzt!