Elem. Math. 57 (2002) 115 – 120
0013-6018/02/030115-6

© Birkhäuser Verlag, Basel, 2002

Elemente der Mathematik

Die Vermutung von Birch und Swinnerton-Dyer

Jürg Kramer

1 Ein Problem

Eine positive, natürliche Zahl F sei vorgelegt. Gesucht wird ein rechtwinkliges Dreieck mit *rationalen* Seiten a, b, c und Flächeninhalt F. Das heisst, wir suchen positive, rationale Zahlen a, b, c, welche den Gleichungen

$$a^2 + b^2 = c^2\,, \qquad \frac{a \cdot b}{2} = F$$

genügen. Das pythagoreische Zahlentripel $(3, 4, 5)$ zeigt sofort, dass für $F = 6$ ein entsprechendes rechtwinkliges Dreieck existiert. Es stellt sich unmittelbar die Frage, ob es zum Beispiel auch für $F = 1, 2, 3, 4, 5$ solche Dreiecke gibt.

Falls für ein gegebenes F ein entsprechendes rechtwinkliges Dreieck existiert, so wird F *Kongruenzzahl* genannt. Die Frage, ob ein vorgelegtes F Kongruenzzahl ist oder nicht, heisst *Kongruenzzahlproblem*. Die Vermutung von Birch und Swinnerton-Dyer würde insbesondere eine Antwort auf das klassische Kongruenzzahlproblem geben.

2 Rationale Lösungen polynomialer Gleichungen

Es sei $P = P(X, Y)$ ein Polynom in den beiden Variablen X, Y mit ganzzahligen Koeffizienten, d.h. P ist ein Element des Polynomrings $\mathbb{Z}[X, Y]$. In der Zahlentheorie wird insbesondere die Frage untersucht, ob es rationale Lösungen der Gleichung $P(X, Y) = 0$ gibt, d.h. ob es rationale Zahlen x, y mit der Eigenschaft $P(x, y) = 0$ gibt. Diese Fragestellung kann wie folgt auch geometrisch formuliert werden. Durch die Gleichung

$$P(X, Y) = 0$$

wird eine Kurve C in der X, Y-Ebene definiert. Die Frage nach rationalen Lösungen x, y der polynomialen Gleichung $P(X, Y) = 0$ ist somit gleichbedeutend mit der Frage nach Punkten auf der Kurve C, welche rationale Koordinaten besitzen. Um diese Frage zu studieren, schreiben wir

$$C(\mathbb{Q}) = \{(x, y) \,|\, x, y \in \mathbb{Q}\,, P(x, y) = 0\}$$

und nennen dies *die Menge der rationalen Punkte von* C. Für den Einheitskreis ist z.B. $(3/5, 4/5)$ ein rationaler Punkt.

Die Frage lautet also: Ist die Menge $C(\mathbb{Q})$ leer oder nicht? Zur Beantwortung untersucht man die naheliegende Frage, ob $C(\mathbb{Q})$ endlich oder unendlich ist.

Wir geben im folgenden eine kurze Übersicht über die Antwort auf diese zweite Frage. Dazu schreiten wir im wesentlichen nach aufsteigendem Grad d des Polynoms P voran.

(i) *Grad* 1: Ohne Beschränkung der Allgemeinheit können wir

$$P(X,Y) = aX + bY + c$$

mit $a,b,c \in \mathbb{Z}$ und $a \neq 0$ annehmen. Die Kurve C ist in diesem Fall eine Gerade mit rationaler Steigung. Mit Hilfe einer elementaren Rechnung verifiziert man, dass $C(\mathbb{Q})$ unendlich ist.

(ii) *Grad* 2: Ohne Beschränkung der Allgemeinheit können wir

$$P(X,Y) = aX^2 + bXY + cY^2 + d$$

mit $a,b,c,d \in \mathbb{Z}$ und $a \neq 0$ annehmen. Die durch $P(X,Y) = 0$ definierte Kurve C ist eine sogenannte *Quadrik*. Wie das Beispiel $P(X,Y) = X^2 - 2$ zeigt, brauchen auf Kurven zweiten Grades keine rationalen Punkte zu existieren; dieses Beispiel ist ja gerade gleichbedeutend mit der Irrationalität von $\sqrt{2}$. Wir nehmen also an, dass die Kurve C mindestens einen rationalen Punkt $Q \in C(\mathbb{Q})$ besitzt. Indem wir C von Q aus auf eine Gerade L mit rationaler Steigung projizieren, erhalten wir eine Bijektion zwischen $C(\mathbb{Q})$ und $L(\mathbb{Q})$, woraus mit Hilfe von (i) die Unendlichkeit von $C(\mathbb{Q})$ folgt.

(iii) *Grad grösser als* 3: Ohne Beschränkung der Allgemeinheit können wir

$$P(X,Y) = a_{d,0}X^d + a_{d-1,1}X^{d-1}Y + \ldots + a_{0,d}Y^d + \ldots + a_{0,0}$$

mit $a_{d,0}, a_{d-1,1}, \ldots, a_{0,d}, \ldots, a_{0,0} \in \mathbb{Z}$ und $a_{d,0} \neq 0$ annehmen. Die Gleichung $P(X,Y) = 0$ definiert eine Kurve C vom Grad $d > 3$. Sehen wir von Spezialfällen (Nicht-Glattheit, Reduzibilität) ab, so entnehmen wir der von G. Faltings im Jahr 1983 bewiesenen Vermutung von L. Mordell (siehe [4]), dass die Menge $C(\mathbb{Q})$ der rationalen Punkte von C endlich ist. Es bleibt somit die Frage nach dem Verhalten von $C(\mathbb{Q})$ für Kurven vom Grad $d = 3$.

(iv) *Grad* 3: Ist $P = P(X,Y)$ ein Polynom dritten Grades und C die durch $P(X,Y) = 0$ definierte Kurve, so kann – wie im Fall (ii) – die Menge $C(\mathbb{Q})$ leer sein. Wir nehmen an, dass C mindestens einen rationalen Punkt enthält. Indem man diesen als den unendlich fernen Punkt auf C wählt, kann C ohne Beschränkung der Allgemeinheit in der Form

$$Y^2 = X^3 + aX^2 + bX + c \tag{1}$$

mit $a,b,c \in \mathbb{Z}$ angenommen werden. Indem man zusätzlich annimmt, dass das kubische Polynom rechter Hand keine mehrfachen Nullstellen besitzt, d.h. dass seine Diskriminante Δ nicht verschwindet bzw. dass C keine Singularitäten besitzt, so nennt man C eine *elliptische Kurve*.

Für elliptische Kurven schreiben wir fortan E anstelle von C. Zur Theorie der elliptischen Kurven verweisen wir auf die beiden Lehrbücher [6] und [9]. Im folgenden Abschnitt untersuchen wir die Menge $E(\mathbb{Q})$ nach Endlichkeit bzw. Unendlichkeit.

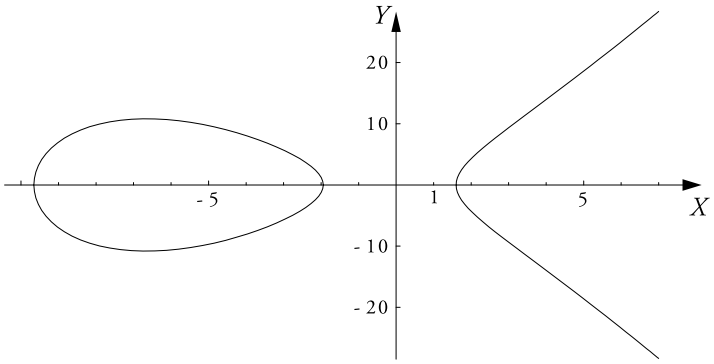

Fig. 1 Elliptische Kurve E: $Y^2 = X^3 + 10X^2 + 0.2X - 30$

3 Rationale Punkte auf elliptischen Kurven

Wir betrachten eine elliptische Kurve E definiert durch die Gleichung (1). Zunächst stellen wir fest, dass die Menge $E(\mathbb{Q})$ der rationalen Punkte auf E die Struktur einer abelschen Gruppe trägt. Die Summe $P + Q$ zweier rationaler Punkte $P, Q \in E(\mathbb{Q})$ ist dabei durch den folgenden rationalen Punkt gegeben: Man verbinde P und Q durch eine Gerade L. Diese hat rationale Steigung und schneidet die Kubik E deshalb in einem weiteren rationalen Punkt R. Indem wir R an der X-Achse spiegeln, erhalten wir den rationalen Punkt $P + Q \in E(\mathbb{Q})$. Die Konstruktion zeigt sofort, dass die auf diese Art definierte Addition kommutativ ist; es ist andererseits aber nicht so einfach, die Assoziativität dieser Addition nachzuweisen.

Der Satz von L. Mordell (siehe [8]) aus dem Jahr 1922 besagt nun, dass die abelsche Gruppe $E(\mathbb{Q})$ *endlich erzeugt* ist. Das heisst, es besteht eine direkte Summenzerlegung der Form

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{frei}} \oplus E(\mathbb{Q})_{\text{endl.}},$$

wobei $E(\mathbb{Q})_{\text{frei}}$ den sogenannten *freien Anteil* und $E(\mathbb{Q})_{\text{endl.}}$ den *endlichen Anteil* (Torsionsanteil) der abelschen Gruppe $E(\mathbb{Q})$ bezeichnet.

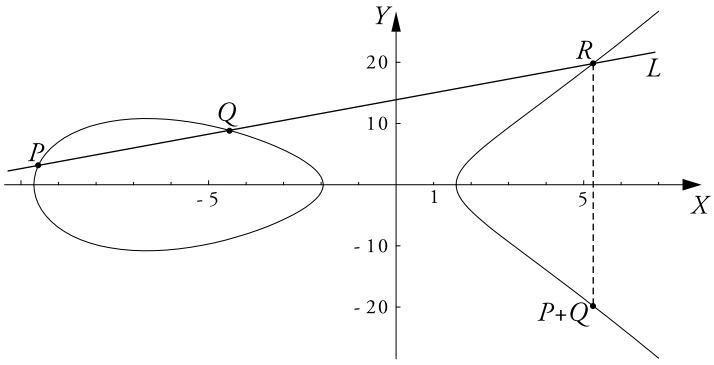

Fig. 2 Addition auf elliptischen Kurven

$E(\mathbb{Q})_{\text{endl.}}$ ist eine endliche abelsche Gruppe, d.h. $E(\mathbb{Q})_{\text{endl.}}$ besteht aus den rationalen Punkten endlicher Ordnung auf E. Nach einem Satz von B. Mazur weiss man, dass $E(\mathbb{Q})_{\text{endl.}}$ zu einer der folgenden 15 Gruppen isomorph ist

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && (N = 1, \ldots, 10, 12)\,, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && (N = 1, \ldots, 4)\,. \end{aligned}$$

Für den freien Anteil besteht die Isomorphie

$$E(\mathbb{Q})_{\text{frei}} \cong \mathbb{Z}^{r_E} = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \qquad (r_E\text{−mal})\,.$$

Die Grösse r_E wird *der Rang von* $E(\mathbb{Q})$ genannt. Ist $r_E = 0$, so besitzt $E(\mathbb{Q})$ also nur endlich viele rationale Punkte. Ist hingegen $r_E > 0$, so besitzt $E(\mathbb{Q})$ rationale Punkte unendlicher Ordnung und somit unendlich viele rationale Punkte. Zusammenfassend haben wir also:

$$r_E = 0 \Longleftrightarrow \#E(\mathbb{Q}) < \infty,$$
$$r_E > 0 \Longleftrightarrow \#E(\mathbb{Q}) = \infty.$$

Das Problem, die Menge $E(\mathbb{Q})$ für elliptische Kurven E zu beschreiben, besteht also in der Bestimmung ihres Rangs r_E.

4 Die Vermutung von Birch und Swinnerton-Dyer

Wir gehen aus von einer elliptischen Kurve E definiert durch die Gleichung (1). Die Vermutung von Birch und Swinnerton-Dyer liefert ein analytisches Werkzeug, um zu entscheiden, ob $r_E = 0$ oder $r_E > 0$ gilt. Zur Formulierung dieses Millenniumsproblems betrachten wir die Gleichung (1) nun auch als Kongruenz modulo einer beliebigen Primzahl p und definieren zunächst

$$N_p := \#\{x, y \in \{0, \ldots, p-1\} \mid y^2 \equiv x^3 + ax^2 + bx + c \bmod p\} + 1\,.$$

Experimentell stellen B. Birch und H.P.F. Swinnerton-Dyer in [1] die Äquivalenz

$$r_E > 0 \Longleftrightarrow \prod_{\substack{p \text{ prim} \\ p \le x}} \frac{N_p}{p} \underset{x\to\infty}{\longrightarrow} \infty \tag{2}$$

fest. Mit Hilfe der L-Reihe $L_E(s)$ der elliptischen Kurve E, welche für $s \in \mathbb{C}$, $\operatorname{Re} s > 3/2$, durch das konvergente Eulerprodukt

$$L_E(s) := \prod_{\substack{p \text{ prim} \\ p \nmid 2\Delta}} \frac{1}{1 - (p + 1 - N_p)p^{-s} + p^{1-2s}}$$

definiert ist, lässt sich (2) – zumindest formal – umschreiben zu

$$r_E > 0 \Longleftrightarrow L_E(1) = 0\,.$$

Diese Heuristik führt jetzt zum folgenden Millenniumsproblem:

Vermutung von Birch und Swinnerton-Dyer: Es sei E eine durch die Gleichung (1) definierte elliptische Kurve. Dann gilt:

- Die L-Reihe $L_E(s)$ von E lässt sich zu einer holomorphen Funktion auf die gesamte komplexe Ebene $\mathbb{C}$ fortsetzen; insbesondere ist also $L_E(1)$ definiert.
- Für die Verschwindungsordnung $\mathrm{ord}_{s=1}L_E(s)$ von $L_E(s)$ an der Stelle $s = 1$ besteht die Gleichheit
$$r_E = \mathrm{ord}_{s=1}L_E(s)\,,$$
und es gibt eine explizite Formel, die den ersten, nicht verschwindenden Koeffizienten der Taylorentwicklung von $L_E(s)$ um $s = 1$ mit der Arithmetik von E in Zusammenhang bringt.

Verallgemeinerungen und Ergebnisse. Die Vermutung von Birch und Swinnerton-Dyer lässt sich auch für die höher dimensionalen Analoga der elliptischen Kurven, die abelschen Varietäten, formulieren. Abgesehen von speziellen Beispielen ist die Vermutung im wesentlichen nur für elliptische Kurven vom Rang 0 und 1 bewiesen. Etwas genauer stellen wir dazu fest: Im Jahr 1977 haben J. Coates und A. Wiles in [3] die Endlichkeit von $E(\mathbb{Q})$ für elliptische Kurven $E/\mathbb{Q}$ mit komplexer Multiplikation und $L_E(1) \neq 0$ bewiesen. 1986 haben B. Gross und D. Zagier in [5] gezeigt, dass (modulare) elliptische Kurven $E/\mathbb{Q}$ mit $L_E(1) = 0$, aber $L'_E(1) \neq 0$ unendlich viele rationale Punkte besitzen. Unter Verwendung dieses Resultats und neuer Ideen hat V.A. Kolyvagin 1989 in [7] bewiesen, dass aus $L_E(1) \neq 0$ sich $r_E = 0$, und aus $L_E(1) = 0$, $L'_E(1) \neq 0$ sich $r_E = 1$ ergibt. Dabei verwendete er eine analytische Voraussetzung, die kurz danach durch D. Bump, S. Friedberg und J. Hoffstein in [2] bewiesen wurde. Wir verweisen den Leser an dieser Stelle auch auf den Übersichtsartikel [11] von A. Wiles.

5 Zusammenhang mit dem Kongruenzzahlproblem

Zum Schluss kommen wir auf das einleitend beschriebene Kongruenzzahlproblem zurück. Dazu ordnen wir der positiven, natürlichen Zahl F die elliptische Kurve

$$E_F:\ Y^2 = X^3 - F^2X$$

zu. Damit lässt sich leicht zeigen, dass F genau dann Kongruenzzahl ist, wenn der Rang r_{E_F} von E_F positiv ist, was nach der Vermutung von Birch und Swinnerton-Dyer wiederum mit dem Verschwinden von $L_{E_F}(1)$ äquivalent ist. Erfüllt F die Kongruenz $F \equiv 5, 6, 7 \bmod 8$, so zeigt die Arbeit [5], dass F Kongruenzzahl ist, falls $L'_{E_F}(1) \neq 0$ gilt; diese Bedingung ist insbesondere erfüllt, wenn F eine Primzahl mit $F \equiv 5, 7 \bmod 8$ ist. Ist hingegen $F \equiv 1, 2, 3 \bmod 8$, so wird vermutet, dass F keine Kongruenzzahl ist; dies lässt sich bestätigen, wenn F eine Primzahl mit $F \equiv 3 \bmod 8$ ist.

Ist nun $r_{E_F} > 0$ und $(x, y) \in E_F(\mathbb{Q})$ ein rationaler Punkt unendlicher Ordnung (o.B.d.A.: $x < 0$, $y > 0$), so bilden $a = (F^2 - x^2)/y$, $b = -2xF/y$, $c = (F^2 + x^2)/y$ ein rechtwinkliges Dreieck mit rationalen Seiten und Flächeninhalt F. Für $F = 5$ hat z.B. der rationale Punkt $(-5/9, 100/27) \in E_F(\mathbb{Q})$ unendliche Ordnung. Damit erhalten wir

das rechtwinklige Dreieck mit den Seiten $a = 20/3$, $b = 3/2$, $c = 41/6$ und Flächeninhalt $F = 5$. Für $F = 6$ erhalten wir mit $(-3, 9) \in E_F(\mathbb{Q})$ das rechtwinklige Dreieck mit den Seiten $a = 3$, $b = 4$, $c = 5$. Für $F = 1, 2, 3$ zeigt man $r_{E_F} = 0$. Somit sind dies keine Kongruenzzahlen. Da $F = 1$ keine Kongruenzzahl ist, gibt es kein rechtwinkliges Dreieck mit rationalen Seiten und Flächeninhalt gleich einer Quadratzahl. Wir verweisen abschliessend auch auf die Arbeit [10] von J. Tunnell zum Kongruenzzahlproblem.

Literatur

[1] Birch, B.; Swinnerton-Dyer, H.P.F.: Notes on elliptic curves I, II. *J. Reine Angew. Math.* 212 (1963), 7–25; 218 (1965), 79–108.

[2] Bump, D.; Friedberg, S.; Hoffstein, J.: Non-vanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.* 102 (1990), 543–618.

[3] Coates, J.; Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* 39 (1977), 223–251.

[4] Faltings, G.: Endlichkeitssätze für abelsche Varietäten. *Invent. Math.* 73 (1983), 349–366.

[5] Gross, B.; Zagier, D.: Heegner points and derivatives of L-series. *Invent. Math.* 84 (1986), 225–320.

[6] Knapp, A.W.: *Elliptic curves*. Math. Notes 40, Princeton University Press. Princeton, New Jersey 1992.

[7] Kolyvagin, V.A.: On the Mordell-Weil and Shafarevich-Tate groups for elliptic Weil curves. *Math. USSR, Izv.* 33 (1989), 473–499.

[8] Mordell, L.J.: *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[9] Silverman, J.H.; Tate, J.: *Rational points on elliptic curves*. Springer-Verlag. Berlin, Heidelberg, New York 1992.

[10] Tunnell, J.: A classical diophantine problem and modular forms of weight $3/2$. *Invent. Math.* 72 (1983), 323–334.

[11] Wiles, A.: The Birch and Swinnerton-Dyer Conjecture. pdf-file unter http://www.claymath.org./prizeproblems/birchsd.htm

Jürg Kramer
Institut für Mathematik
Humboldt-Universität zu Berlin
D–10099 Berlin
e-mail: kramer@mathematik.hu-berlin.de