Annette Huber: Was wir alles für Gleichungen vom Grad drei (nicht) wissen – elliptische Kurven und die Vermutung von Birch und Swinnerton-Dyer

0.1 Einleitung

Worum es gehen wird

Zur Jahrtausendwende stellte die Clay-Foundation die ihrer Meinung nach wichtigsten sieben mathematischen Fragen vor, die Milleniumsprobleme. Auf die Lösung ist jeweils eine Million Dollar ausgesetzt. In der Liste findet sich auch eine der berühmtesten Vermutungen der modernen Zahlentheorie. Ich will sie formulieren und zeigen, wie sie sich in den Kontext der Dinge einbettet, die wir wissen. Hier ist sie:

Vermutung 0.1.1 (Birch und Swinnerton-Dyer, 1965)**.** *Es sei E eine elliptische Kurve über $\mathbb{Q}$. Dann stimmt die Nullstellenordnung der L-Funktion $L(E,s)$ in $s = 1$ mit dem Rang der Gruppe $E(\mathbb{Q})$ überein.*

Hoffentlich ist bis zum Ende unseres Crashkurses (einigermaßen) klar, was alle diese Wörter bedeuten. Schon in die Formulierung geht nämlich einiges an spannender und schwieriger Mathematik ein!

Zahlentheorie

Zahlentheorie ist der Teil der Mathematik, der sich mit den Eigenschaften von Zahlen beschäftigt. Gemeint sind Zahlen wie

$$1,2,3,\dots .$$

Das Gebiet ist uralt. Viele sehr interessante Sachverhalte waren bereits in der Antike bekannt.

In diesem Artikel soll der Zahlbegriff etwas allgemeiner gefasst werden. Es geht auch um Zahlen wie

$$0,-4,\frac{1}{3},-\frac{97}{312},\dots .$$

Präzise: um die rationalen[1] Zahlen.

Wir wollen uns mit Gleichungen und ihren Lösungsmengen beschäftigen.

[1] **Ganze Zahlen:** $\mathbb{Z} = \{0,\pm1,\pm2,\pm3,\dots\}$; **Rationale Zahlen:** $\mathbb{Q} = \left\{\frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0\right\}$

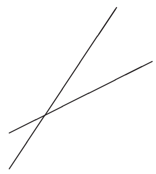
Lineare und quadratische Gleichungen

Lineare Gleichungen sind gut verstanden: Die Gleichung

$$3x = 7$$

hat eine einzige Lösung, nämlich $\frac{7}{3}$. Auch mit Gleichungssystemen in mehreren Variablen können wir gut umgehen. Zum Beispiel hat

$$\begin{aligned} \frac{9}{2}x - 3y &= 1 \;, \\ -2x + 4y &= 0 \end{aligned}$$



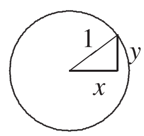
genau eine Lösung, deren Bestimmung hier eine Übungsaufgabe für den Leser oder die Leserin ist. Sie liegt auf jeden Fall in $\mathbb{Q}$, da die Koeffizienten $9/2$, 3, -2 und 4 rationale Zahlen sind. Schöner ist der geometrische Standpunkt: Jede der beiden Gleichungen beschreibt eine Gerade. Diese beiden Geraden schneiden sich in genau einem Punkt, denn sie sind nicht parallel.

Quadratische Gleichungen in einer Variablen sind ebenfalls vertraut. Die Lösungsformel ist unter vielen Namen bekannt (a,b,c-Formel, p,q-Formel, Mitternachtsformel). Das Beispiel

$$x^2 = 3$$

zeigt, dass manche Gleichungen mit rationalen Koeffizienten keine Lösung in den rationalen Zahlen haben. Für quadratische Gleichungen in zwei Variablen kommt uns wieder die Geometrie zu Hilfe. Die Gleichung

$$x^2 + y^2 = 1$$



beschreibt einen Kreis. Allgemeiner trifft man auf die Kegelschnitte: Ellipsen, Parabeln und Hyperbeln. Konstruktionen mit Zirkel und Lineal – der Gegenstand der Schulgeometrie – sind nur ein Spezialfall. Mehr lernt man in der Schule meist nicht. Überraschenderweise kommt aber auch die höhere Mathematik bei Gleichungen höheren Grades sehr schnell an ihre Grenzen.

Übersicht

In diesem Artikel soll es hauptsächlich um Gleichungen dritten Grades in zwei Variablen gehen, zum Schluss ein wenig um Gleichungen höheren Grades in nur einer Variablen.

- Gleichungen vom Grad drei beschreiben eine elliptische Kurve. Dies ist der erste Begriff, den wir vorstellen werden.

- Danach lernen wir $E(\mathbb{Q})$ und seinen Rang kennen. Dafür müssen wir zunächst das Gruppengesetz auf der elliptischen Kurve vorstellen und den Satz von Mordell formulieren.

- Nun fehlt uns noch die L-Funktion. Danach sind wir so weit: Die Vermutung von Birch und Swinnerton-Dyer kann hingeschrieben werden.

- Zum Ausklang wird der Zusammenhang zu der analogen Vermutung für Gleichungen in einer Variablen hergestellt, meinem eigenen Forschungsgebiet.

0.2 Elliptische Kurven

Unsere Gleichungen: Grad drei in zwei Variablen

Wir wollen uns nun auf Gleichungen konzentrieren wie

$$\frac{1}{2}x^3 - 2x^2y + y^2 + 3xy - 5y = \frac{5}{8} .$$

Diese Gleichung hat zwei Variablen x, y, rationale Koeffizienten (wie $\frac{1}{2}$) und Grad 3; das heißt, wenn man in jedem Summanden die Exponenten von x und y addiert, so erhält man höchstens 3. Wir zeichnen die Lösungspaare (x, y) der Gleichung in der Ebene ein und erhalten eine Kurve. Ein typisches Beispiel ist auf Seite XVII zu sehen. Wir werden meist nicht zwischen der Gleichung und der Kurve unterscheiden.

Der Einfachheit halber beschränken wir uns auf Gleichungen der Form

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma .$$

Hierbei sind $\alpha, \beta, \gamma \in \mathbb{Q}$ feste Koeffizienten, während x, y die Variablen der Gleichung sind.[2]

Die Frage nach der Lösbarkeit in den rationalen Zahlen ist alles andere als offensichtlich!

Beispiel 0.2.1. Nehmen wir

$$y^2 = x^3 + 17 .$$

Für die meisten rationalen x wird y eine echte Quadratwurzel sein, zum Beispiel ist für $x = 0$ der Wert $y = \pm\sqrt{17}$ nicht rational. Rationale Lösungen erhalten wir nur, wenn zufällig die Wurzel aus einer Quadratzahl gezogen wird. Einige kleine ganzzahlige Lösungen kann man raten, zum Beispiel

$$(-1, 4) \quad (-2, 3) \quad (2, 5) \quad (4, 9) \quad (8, 23) .$$

Insgesamt gibt es 16 ganzzahlige Lösungen, zum Beispiel auch

$$(52, 375) \quad (5234, 378661) .$$

Hinzu kommen viele rationale Punkte, zum Beispiel

$$\left(\frac{137}{64}, -\frac{2651}{512}\right) .$$

Kurven vom Grad drei sind fast das Gleiche wie elliptische Kurven. Um zu verstehen, warum deren Definition komplizierter ausfällt, wollen wir erst untersuchen, was beim Schneiden mit Geraden passiert.

[2] Die Einschränkung ist nicht groß, durch elementare lineare Variablentransformationen wie zum Beispiel $x = x' + y'$, $y = 2y' - 1$ kann jede Gleichung dritten Grades, also jede Gleichung der Form

$$a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} = 0$$

auf diese Form gebracht werden.

Schneiden mit Geraden

Wie viele Schnittpunkte hat eine Gerade mit einer Kurve vom Grad 3?

Geometrisch kann man sich das mit der Kurve auf Seite XVII und einem Lineal anschauen. (Am besten probieren Sie es aus, bevor Sie weiterlesen.) Alternativ wollen wir ein Beispiel rechnen.[3]

Wir betrachten wieder die Kurve mit der Gleichung

$$y^2 = x^3 + 17\,. \tag{$\star$}$$

Auf der Kurve liegen die Punkte $P = (-1,4)$ und $Q = (2,5)$, denn es gilt

$$4^2 = 16 = (-1)^3 + 17 \text{ und } 5^2 = 25 = 2^3 + 17\,.$$

Zwei Punkte legen eine Gerade fest, in diesem Fall hat sie die Gleichung

$$y = \frac{1}{3}x + \frac{13}{3}\,.$$

Gibt es weitere Schnittpunkte der Geraden mit der Kurve? Dafür setzen wir die Geradengleichung in die Gleichung ($\star$) ein:

$$\left(\frac{1}{3}x + \frac{13}{3}\right)^2 = x^3 + 17 \quad \Leftrightarrow \quad 0 = x^3 - \frac{1}{9}x^2 - \frac{26}{9}x - \frac{16}{9}\,.$$

Das ist eine Gleichung vom Grad drei in einer Variablen x. Zum Glück kennen wir zwei Nullstellen: die x-Koordinaten von P und Q. Das Polynom ist also durch $(x+1)(x-2) = x^2 - x - 2$ teilbar. Eine Polynomdivision später, mit

$$\left(x^3 - \frac{1}{9}x^2 - \frac{26}{9}x - \frac{16}{9}\right) \,:\, \left(x^2 - x - 2\right) = x + \frac{8}{9},$$

kennen wir die dritte Nullstelle, nämlich $x = -\frac{8}{9}$. Der Punkt $R = (-\frac{8}{9}, \frac{11881}{729})$ ist der eindeutige dritte Schnittpunkt der Kurve dritten Grades mit der Geraden durch P und Q.

Die Methode funktioniert offensichtlich auch für andere Zahlenwerte. Aus zwei Schnittpunkten berechnen wir genau einen dritten.

Ganz stimmt das aber nicht, wie man mit Experimentieren in dem Bild auf Seite XVII sehen kann. Was kann schiefgehen?

1. Es könnte sein, dass das Polynom dritten Gerades mehrfache Nullstellen hat. Geometrisch bedeutet dies, dass die Gerade eine Tangente an die Kurve ist. Dieses Problem lösen wir, indem wir vereinbaren, dass Schnittpunkte mit *Vielfachheit* gezählt werden müssen.

2. Senkrechte Geraden wie $x = 2$ schneiden die Kurve auch mit Vielfachheit gezählt nur in maximal zwei Punkten, genauer: gar nicht oder zweimal. Beim Einsetzen der Geradengleichung bleibt nämlich nur ein quadratisches Polynom übrig, dessen beiden Lösungen

[3] Wenn es zu kompliziert wird, bitte gleich in den nächsten Abschnitt springen und exotische Grenzfälle ignorieren.

wir schon kennen. Wir gehen daher zur Lösungsmenge in der *projektiven Ebene*[4] über. Wir fügen einfach zur Kurve einen *unendlich fernen* Punkt ∞ hinzu, der auf allen senkrechten Geraden (und keiner anderen) liegt. Die Gerade $x = 2$ schneidet also die Kurve $(\star)$ in den Punkten $(2,5),(2,-5),\infty$. (Es würde zu weit führen, hier die projektive Ebene systematisch zu diskutieren. Es ist aber weder Zauberei noch Willkür.)

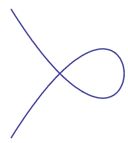
Elliptische Kurven

Definition 0.2.2. Es sei E_0 die Kurve mit der Gleichung $y^2 = x^3 + \alpha x^2 + \beta x + \gamma$ für $\alpha, \beta, \gamma \in \mathbb{Q}$, so dass $x^3 + \alpha x^2 + \beta x + \gamma$ keine doppelten Nullstellen hat. Dann heißt

$$E = E_0 \cup \{\infty\}$$

elliptische Kurve über $\mathbb{Q}$. Mit $E(\mathbb{Q})$ bezeichnen wir die Menge der Punkte (x,y) von E mit rationalen Koordinaten x und y (einschließlich ∞).

Warum die Bedingung, die doppelte Nullstellen ausschließt? Sie verhindert Kurven wie die Schlinge mit der Gleichung $y^2 = -x^2(x-1)$ im Bild rechts. Im Kreuzungspunkt gibt es mehr als eine Tangente, und das würde uns im Weiteren stören.



Beispiel 0.2.3. Für die Gleichung $y^2 = x^3 + 17$ liegen $P = (-1,4)$, $Q = (2,5)$, $R = (-\frac{8}{9}, \frac{11881}{729})$ in $E(\mathbb{Q})$.

Bemerkung 0.2.4. Gleichungen von elliptischen Kurven tauchen auf, wenn man die Kurvenlänge von Ellipsen berechnet. Für unsere Fragestellung ist das unwichtig.

Und nun korrekt:

Satz 0.2.5. *Es sei E eine elliptische Kurve. Hat eine Gerade zwei Schnittpunkte P und Q mit E, dann hat sie genau einen dritten Schnittpunkt R mit E. Dabei werden Schnittpunkte mit Vielfachheit gezählt.*

Korollar 0.2.6. *Es sei E eine elliptische Kurve über $\mathbb{Q}$ und $P, Q \in E(\mathbb{Q})$. Dann liegt auch der dritte Schnittpunkt der Geraden durch P und Q mit E in $E(\mathbb{Q})$.*

Beweis. Wie bei der Rechnung im obigen Beispiel tauchen in jedem Schritt nur rationale Zahlen auf. $\square$

Beim Blick in die Vermutung 0.1.1 sollten nun die Begriffe elliptische Kurve über $\mathbb{Q}$ und die Menge $E(\mathbb{Q})$ vertraut sein. Außerdem wissen wir aus Korollar 0.2.6, was passiert, wenn man Punkte aus $E(\mathbb{Q})$ mit Geraden verbindet.

[4] Die projektive Ebene entsteht aus der Ebene, indem man für jede Geradenrichtung formal einen zusätzlichen Punkt hinzufügt. Dies ist ein „unendlich ferner“ Punkt, in dem sich alle parallelen Geraden mit gleicher Richtung schneiden. Alle unendlich fernen Punkte liegen auf der unendlich fernen Geraden. In der projektiven Ebene haben je zwei Geraden genau einen Schnittpunkt.

0.3 Das Gruppengesetz

Die Definition der Verknüpfung $\star$

Unser nächstes Ziel ist die Definition des Rangs von $E(\mathbb{Q})$. Dafür führen wir ein *Gruppengesetz* auf E ein, also eine Art Addition. Deren Existenz ist es, was elliptische Kurven so interessant für viele Anwendungen macht.

Definition 0.3.1. Es sei E eine elliptische Kurve. Wir definieren eine Abbildung

$$\begin{aligned} \star : E \times E &\to E \\ (P,Q) &\mapsto P \star Q \end{aligned}$$

wie folgt: Seien $P,Q \in E$ Punkte der Kurve. Sei G_1 die eindeutig bestimmte Gerade durch P und Q. Sei H_1 der dritte Schnittpunkt von G_1 mit E. Weiter sei G_2 die senkrechte Gerade durch H_1. Sei H_2 der dritte Schnittpunkt von G_2 mit E. Wir setzen

$$P \star Q := H_2 \ .$$

Es sind hier noch allerlei Sonderfälle zu berücksichtigen:

1. Ist $P = Q$, so ist G_1 die eindeutige Tangente in P, analog für G_2.
2. Ist $P = \infty$, so ist G_1 die senkrechte Gerade durch Q, analog für $Q = \infty$ für G_2.
3. Wir setzen $\infty \star \infty = \infty$.

Wichtig ist, dass die Operation $\star$ nichts mit dem Addieren der Koordinaten von Punkten zu tun hat. Mit einem hübschen Programm meines Kollegen Stefan Kebekus (siehe Literaturverzeichnis) kann die Rechenvorschrift ausprobiert werden (oder natürlich mit Bleistift und Papier).

Diese etwas seltsame Vorschrift hat sehr gute Eigenschaften, analog zu den Rechenregeln für ganze oder rationale Zahlen. Wir können addieren und subtrahieren.

Satz 0.3.2. *Die Punkte von E bilden bezüglich der Addition $\star$ eine* abelsche Gruppe *mit neutralem Element ∞. Das heißt, es gilt für alle $P,Q,R \in E$:*

1. $P \star Q = Q \star P$,
2. $(P \star Q) \star R = P \star (Q \star R)$,
3. $P \star \infty = P$,
4. *zu jedem Punkt P gibt es einen eindeutigen Punkt Q mit $P \star Q = \infty$; wir schreiben $Q = [-1]P$ und sagen, dass Q das Inverse von P ist.*

Der Leser oder die Leserin ist herzlich eingeladen, sich Beweise für diese Aussagen zu überlegen. Eigenschaft 1. ist ganz leicht, 3. und 4. kann man sich geometrisch überlegen. Die Eigenschaft 2. jedoch ist alles andere als offensichtlich. Um sie zu beweisen, muss man erst Sätze der algebraischen Geometrie herleiten (Satz von Bézout oder Satz von Riemann-Roch).

Korollar 0.3.3. *Es sei E eine elliptische Kurve über $\mathbb{Q}$. Dann ist $E(\mathbb{Q})$ bezüglich der Addition $\star$ eine abelsche Gruppe mit neutralem Element ∞.*

Beweis: Alle Eigenschaften gelten nach dem letzten Satz. Zu zeigen bleibt, dass für $P,Q \in E(\mathbb{Q})$ auch $P \star Q \in E(\mathbb{Q})$. Das folgt aus Korollar 0.2.6 und der Konstruktionsvorschrift. □

Der Satz von Mordell und der Rang von $E(\mathbb{Q})$

$E(\mathbb{Q})$ haben wir eingeführt als die Menge der rationalen Lösungen einer (fast) beliebigen Gleichung dritten Grades in zwei Variablen. Wir haben jetzt gesehen, dass diese Lösungsmenge eine sehr interessante Struktur hat. Aber gibt es überhaupt Lösungen? Manchmal ja, manchmal nein. Manchmal unendlich viele, manchmal nur endlich viele.

Zur Formulierung einer präziseren Antwort brauchen wir noch etwas Notation.

Definition 0.3.4. Es sei E eine elliptische Kurve, P ein Punkt der Kurve. Dann definieren wir

$$[0]P = \infty, \quad [1]P = P, \quad [2]P = P \star P, \quad [3]P = ([2]P) \star P, \quad \dots ,$$

$[-1]P$ wie in der Eigenschaft 4. von $\star$ in Satz 0.3.2 und

$$[-2]P = [-1]([2]P), \quad [-3]P = [-1]([3]P), \quad \dots .$$

Damit gilt automatisch

$$[n]P \star [m]P = [n+m]P, \quad [n]P \star [-n]P = \infty, \quad [n]([m]P) = [nm]P$$

für alle $n,m \in \mathbb{Z}$.

Theorem 0.3.5 (Mordell, 1922)**.** *Es sei E eine elliptische Kurve über $\mathbb{Q}$. Dann ist $E(\mathbb{Q})$ eine endlich erzeugte abelsche Gruppe, das heißt, es gibt Punkte*

$$P_1, \dots, P_r, F_1, \dots, F_t \in E(\mathbb{Q}) ,$$

so dass es für jedes $P \in E(\mathbb{Q})$ eindeutig bestimmte Zahlen $n_1, n_2, \dots, n_r \in \mathbb{Z}$ und ein eindeutiges $i \in \{1, \dots, t\}$ gibt mit

$$P = [n_1]P_1 \star [n_2]P_2 \star \dots [n_r]P_r \star F_i .$$

Beispiel 0.3.6. Für die bereits vorher betrachtete Kurve mit der Gleichung $y^2 = x^3 + 17$ gilt $r = 2$, $t = 0$ mit den Punkten $P_1 = (-2,3)$ und $P_2 = (2,5)$. Also sind die Elemente P von $E(\mathbb{Q})$ genau von der Form

$$P = [n_1]P_1 \star [n_2]P_2 .$$

Der endliche Anteil (das sind die F_i) ist auch allgemein gut verstanden:

Theorem 0.3.7 (Mazur, 1977)**.** *Es sei E eine elliptische Kurve über $\mathbb{Q}$, und es sei t die Zahl aus dem Satz von Mordell. Dann gilt $t \leq 16$.*

Schwieriger ist der unendliche Anteil, wie wir im Folgenden sehen werden.

Definition 0.3.8. Die Zahl r in Theorem 0.3.5 heißt *Rang* von $E(\mathbb{Q})$. Der Fall $r = 0$ ist erlaubt, das heißt $P_1, \dots, P_r$ tauchen dann in der Darstellung gar nicht auf.

Korollar 0.3.9. *Es sei E eine elliptische Kurve über $\mathbb{Q}$. Dann hat E genau dann endlich viele Punkte mit rationalen Koeffizienten, wenn der Rang r von $E(\mathbb{Q})$ gleich null ist. In diesem Fall enthält E höchstens* 16 *rationale Punkte.*

Wir kennen Beispiele von Kurven mit endlich vielen rationalen Punkten und solche mit unendlich vielen. Wie unterscheiden wir die Fälle? Gibt es eine Formel für den Rang r?

Die Antwort ist vermutungsweise ja, eben die Formel von Birch und Swinnerton-Dyer, deren erste Hälfte wir jetzt verstehen. Übrigens ist bis heute unbekannt, ob es elliptische Kurven mit beliebig großem Rang gibt.

0.4 Die L-Funktion einer elliptischen Kurve

Elliptische Kurven über Restklassen modulo p

Für die Definition der L-Funktion einer elliptischen Kurve brauchen wir für (fast) jede Primzahl p eine natürliche Zahl t_p, an deren Definition wir uns nun wagen.

In diesem Abschnitt ist p eine Primzahl.[5] Wir wollen mit den Restklassen[6] modulo p rechnen. Das heißt, es geht um ganze Zahlen, aber wir interessieren uns immer nur für den Rest, der nach ganzzahliger Division durch p bleibt. Wir schreiben $a \equiv b \mod p$, wenn die beiden Zahlen denselben Rest haben. Diese Art des Rechnens wurde von Gauß 1801 eingeführt.

Beispiel 0.4.1. $p = 5$. Dann ist

$$2 + 4 \equiv 1 \mod 5 ,$$

denn 6 hat bei Division durch 5 den Rest 1:

$$6 = 1 \cdot 5 + 1 .$$

Oder:

$$3 \cdot 3 \equiv -1 \mod 5 ,$$

denn 9 und -1 haben beide bei Division durch 5 den gleichen Rest, nämlich 4:

$$9 = 1 \cdot 5 + 4 \qquad -1 = -1 \cdot 5 + 4 .$$

Es gibt genau p Restklassen modulo p, die durch die Zahlen $0, 1, 2, \dots, p-1$ repräsentiert werden.

Definition 0.4.2. Die Menge der Restklassen modulo p wird mit $\mathbb{Z}/p\mathbb{Z}$ bezeichnet.

[5] Ein natürliche Zahl ungleich 1 heißt Primzahl, wenn sie nur durch 1 und sich selbst teilbar ist.

[6] Zwei Zahlen gehören genau dann zur selben Restklasse, wenn ihre Differenz durch p teilbar ist. Wir sagen dann, sie haben denselben Rest modulo p.

Nun zurück zu unseren elliptischen Kurven. Um einfachere Formeln zu erhalten, betrachten wir ab jetzt nur Gleichungen E_0 der Form

$$y^2 = x(x-1)(x-\mu)$$

mit $\mu \in \mathbb{Z}$, $\mu \neq 1,0$. Wie bisher ist $E = E_0 \cup \{\infty\}$. Diese Gleichung können wir jetzt auch modulo p betrachten, indem wir von μ zu seiner Restklasse übergehen. Wir suchen nun nach Lösungen modulo p.

Beispiel 0.4.3. Die elliptische Kurve $y^2 \equiv x(x-1)(x-2) \mod 5$ hat beispielsweise die Lösung $(3,4)$, denn

$$4^2 \equiv 1 \mod 5 \;\text{ und }\; 3(3-1)(3-2) \equiv 1 \mod 5\;.$$

Die vollständige Liste aller Lösungen modulo 5 ist

$$(0,0),(1,0),(2,0),(3,1),(3,4),(4,2),(4,3)\;.$$

Rechnen mit Restklassen ist viel einfacher als mit rationalen Zahlen!

Definition 0.4.4. Mit $E(\mathbb{Z}/p\mathbb{Z})$ bezeichnen wir die Menge der Punkte von E mit Koordinaten in $\mathbb{Z}/p\mathbb{Z}$, das heißt

$$E(\mathbb{Z}/p\mathbb{Z}) = \left\{(x,y) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \mid y^2 \equiv x(x-1)(x-\mu)\right\} \cup \{\infty\}\;.$$

Die Anzahl der Elemente von $E(\mathbb{Z}/p\mathbb{Z})$ wird mit a_p bezeichnet.

In Beispiel 0.4.3 hatten wir $a_5 = 8$ (bitte ∞ nicht vergessen!). Die Zahl der Elemente von $E(\mathbb{Z}/p\mathbb{Z})$ ist endlich, denn es gibt für x und für y jeweils nur p Möglichkeiten. Außerdem gibt es wieder ∞, insgesamt also

$$a_p \leq p^2 + 1\;.$$

Tatsächlich wissen wir mehr:

Satz 0.4.5 (Hasse, 1933)**.** *Es sei E eine elliptische Kurve der obigen Form. Es sei p kein Teiler von μ und $\mu - 1$. Dann gilt*

$$|p + 1 - a_p| \leq 2\sqrt{p}\;.$$

Bemerkung 0.4.6. Wir stellen hier eine Bedingung an p, durch die für jedes E endlich viele Primzahlen ausgeschlossen werden. In der Definition einer elliptischen Kurve hatten wir verlangt, dass

$$x^3 + \alpha x^2 + \beta x + \gamma$$

keine mehrfachen Nullstellen hat. In unserer spezielleren Form $x(x-1)(x-\mu)$ bedeutet das einfach $\mu \neq 0,1$. Wenn p ein Teiler von μ oder $\mu - 1$ ist, so wird die Gleichung aber modulo p zu

$$y^2 \equiv x^2(x-1) \quad \text{bzw.} \quad y^2 \equiv x(x-1)^2\;.$$

Das sind keine elliptischen Kurven! Daher betrachten wir diese „Ausnahmeprimzahlen“ nicht.

Das rein geometrisch definierte Gruppengesetz auf E funktioniert auch modulo p. Dies benötigt eigentlich eine geeignete Sprache von Geometrie über Restklassen. Oder konkret: Die Vorschrift aus Definition 0.3.1 für $(P,Q) \mapsto P \star Q$ läuft auf das Lösen von Gleichungen hinaus. Diese Gleichungen können auch modulo p gelöst werden.

Auf jeden Fall gilt:

Satz 0.4.7. *Es sei E eine elliptische Kurve über $\mathbb{Z}/p\mathbb{Z}$. Dann ist $E(\mathbb{Z}/p\mathbb{Z})$ bezüglich der Addition $\star$ eine abelsche Gruppe mit endlich vielen Elementen.*

Gruppen mit endlich vielen Elementen werden bei bestimmten Public-Key-Verschlüsselungsverfahren benötigt, daher erfreuen sich elliptische Kurven auch bei Banken einer gewissen Beliebtheit.

Für das Weitere ist aber nur die Zahl a_p wichtig bzw. die Größe

$$t_p := p + 1 - a_p,$$

die auch im Satz von Hasse vorkam.

In Beispiel 0.4.3 hatten wir $a_5 = 8$ und $t_5 = -2$.

Definition der L-Funktion und Eigenschaften

Es sei nun E die elliptische Kurve mit der Gleichung

$$y^2 = x(x-1)(x-\mu)\ ,$$

wobei $\mu \in \mathbb{Z}$, $\mu \neq 0, 1$. Jeder solchen Kurve wollen wir eine differenzierbare Funktion zuordnen, wir benutzen ab jetzt die Techniken der Differentialrechnung. Wir erinnern uns an die Zahl

$$t_p = p + 1 - a_p\ ,$$

die im Satz von Hasse vorkam.

Definition 0.4.8. Die *(restringierte) L-Funktion von E* an der Stelle s ist definiert durch das unendliche Produkt

$$L(E,s) = \prod_{p \nmid \mu(\mu-1)} \frac{1}{1 - t_p p^{-s} + p^{1-2s}}\ .$$

Wir haben es hier mit einem unendlichen Produkt zu tun: für jede Primzahl, die μ und $\mu - 1$ nicht teilt, ein Faktor. Das Produkt konvergiert für $s > 3/2$, und wir erhalten eine differenzierbare Funktion in der Variablen s.

In der Vermutung von Birch und Swinnerton-Dyer geht es um die L-Funktion in der Nähe von 1. Leider konvergiert das Produkt dort nicht! Der Ausweg benutzt die komplexe Differentialrechnung, übersteigt also die Schulmathematik.

Theorem 0.4.9. *$L(E,s)$ setzt sich zu einer eindeutigen komplex differenzierbaren Funktion für alle $s \in \mathbb{C}$ fort.*

Hinter diesem Theorem steckt die sogenannte Modularität von elliptischen Kurven, die in Wiles' Beweis der Fermat'schen Vermutung eine Schlüsselrolle spielte. Es ist wohl das tiefste Ergebnis, das wir ansprechen.

Wir betrachten ab jetzt $L(E,s)$ als Funktion auf ganz $\mathbb{C}$, interessieren uns aber nur für $s = 1$. Dort hat die Funktion im Allgemeinen eine Nullstelle. Wie bei der Kurvendiskussion in der reellen Differentialrechnung hat die Nullstelle eine Vielfachheit. Formal führt man sie so ein:

Definition 0.4.10. Die *Nullstellenordnung* von $L(E,s)$ in 1 ist die eindeutig bestimmte Zahl $n \geq 0$, so dass der Grenzwert

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^n}$$

existiert und ungleich 0 ist.

Die Existenz und Eindeutigkeit dieser Zahl folgt aus der Theorie der komplex differenzierbaren Funktionen.

Die Vermutung von Birch und Swinnerton-Dyer

Und damit noch einmal:

Vermutung 0.4.11 (Birch und Swinnerton-Dyer, 1965)**.** *Es sei E eine elliptische Kurve über $\mathbb{Q}$. Dann stimmt die Nullstellenordnung n der L-Funktion von E in* 1 *mit dem Rang r der Gruppe $E(\mathbb{Q})$ überein.*

Die beiden Engländer formulierten auch eine präzise Formel für den Wert des Grenzwertes in der Definition der Nullstellenordnung.

Da die Formulierung so kompliziert ist, überrascht es, dass man die Vermutung in expliziten Beispielen numerisch überprüfen kann. Das geht tatsächlich und wurde in unzähligen Fällen durchgeführt. Allgemein bewiesen sind nur die Spezialfälle $r = 0$ und $r = 1$ durch Arbeiten von Gross/Zagier (1983) und Kolyvagin (1990).

Immerhin wissen wir damit:

Korollar 0.4.12. *$E(\mathbb{Q})$ ist genau dann endlich, wenn $L(E,1) \neq 0$.*

0.5 Die Bloch-Kato-Vermutung

Mit diesem Ausblick will ich den Zusammenhang mit meiner eigenen Forschung herstellen. Elliptische Kurven sind Beispiele für sogenannte algebraische Varietäten über $\mathbb{Q}$. Eine allgemeine Varietät ist ein System von Polynomgleichungen in mehreren Variablen. Die Koeffizienten sollen weiter in $\mathbb{Q}$ liegen. Der Grad und die Anzahl der Variablen ist also nun beliebig. Jeder solchen Varietät (und sogar allgemeiner jedem „Motiv“, das sind gewisse Bausteine von Varietäten) wird ebenfalls eine L-Funktion zugeordnet. Die Gruppe $E(\mathbb{Q})$ lässt sich verallgemeinern durch die sogenannten *motivischen Kohomologiegruppen*.

Die *Vermutung von Beilinson (1984)* drückt die Nullstellenordnung (bzw. die Polstellenordnung) der L-Funktion in Zahlen $r \in \mathbb{Z}$ aus durch die Dimension der motivischen Kohomologiegruppen der Varietät. Die *Vermutung von Bloch und Kato (1990)* gibt auch eine sehr komplizierte

Formel für den führenden Koeffizienten (so heißt der Grenzwert analog zu Definition 0.4.10). Beide verallgemeinern die Vermutung von Birch und Swinnerton-Dyer.

In meiner eigenen Forschung geht es um den „Babyfall“ von Gleichungen in einer Variablen. Dies sind die algebraischen Varietäten der Dimension 0 (vulgo: Punkte).

Beispiel 0.5.1. Es sei V die Varietät, die durch die Gleichung $x = 1$ definiert ist. Dann ist die zugehörige L-Funktion die Riemannsche ζ-Funktion

$$\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1-p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots .$$

(Man beachte die formale Ähnlichkeit mit der L-Funktion einer elliptischen Kurve.)

Theorem 0.5.2 (Borel, 1974)**.** *Die Beilinson-Vermutung gilt für Varietäten der Dimension* 0.

Theorem 0.5.3 (Huber-Kings, 2003)**.** *Die Bloch-Kato-Vermutung gilt für Gleichungen der Form*

$$x^N = 1 .$$

Dabei wurde der Fall $N = 1$, also der Riemannschen ζ-Funktion, weitgehend von Bloch und Kato selbst bewiesen. Für beliebiges N gibt es noch einen alternativen Beweis von Burns und Greither.

In der Einleitung des Artikels habe ich argumentiert, dass wir lineare und quadratische Gleichungen sehr gut verstehen. Dann habe ich mit den elliptischen Kurven den Fall einer Gleichung in zwei Variablen vom Grad 3 betrachtet, wo noch tiefe Vermutungen offen sind. Nun stellt sich heraus, dass selbst für Gleichungen in nur einer Variablen, aber von beliebigem Grad, noch keineswegs alle zahlentheoretischen Probleme gelöst sind!

Danksagung

Herzlicher Dank geht an Stefan Kebekus, Holger Klawitter und Stephen Meagher für Hinweise und Kommentare.

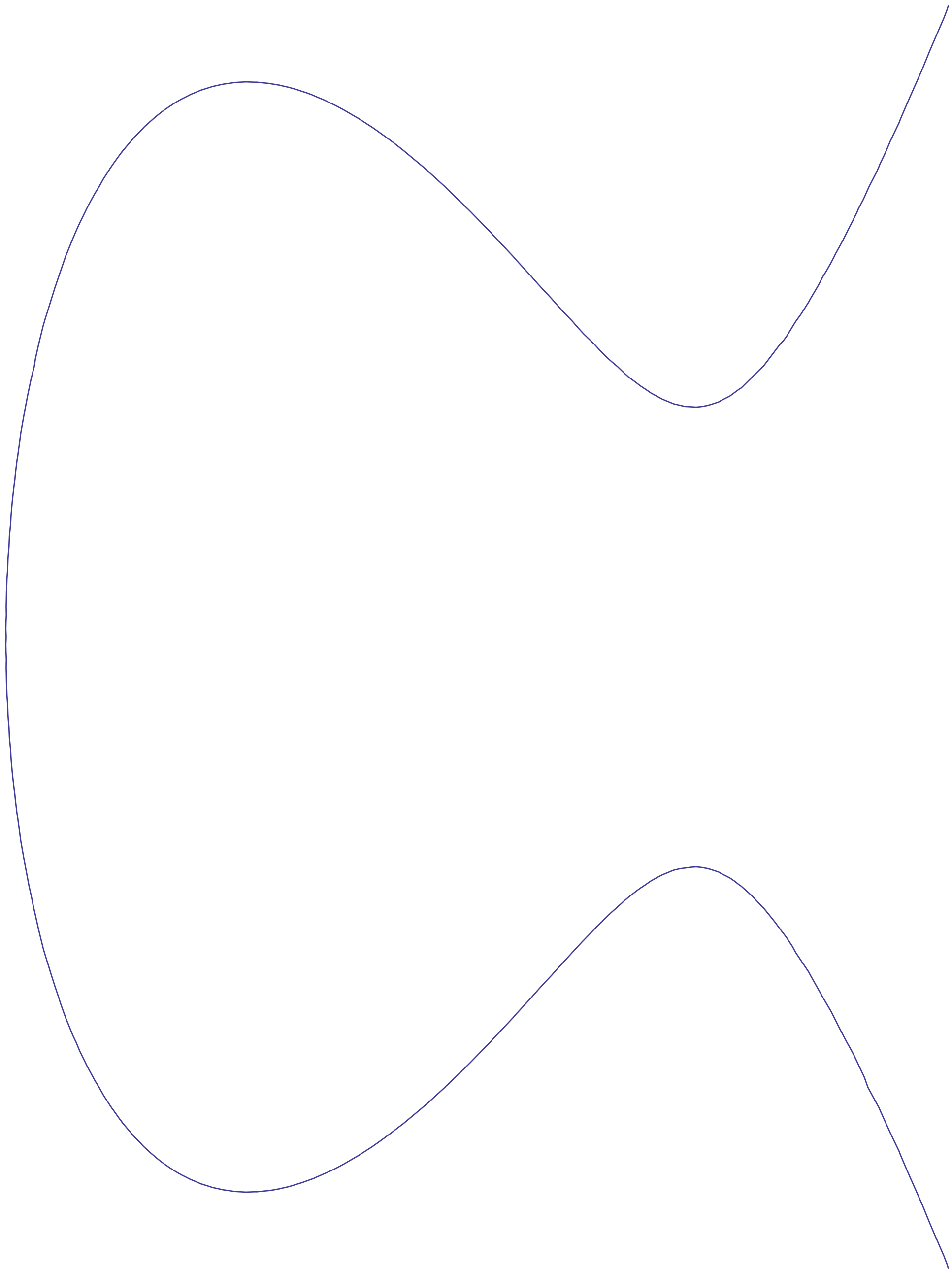


Abbildung 0.1: Die elliptische Kurve $y^2 = x^2 - 6x + 8$

Literaturverzeichnis

[1] B.J.Birch, H.P.F. Swinnerton-Dyer, Notes on elliptic curves. II. J. Reine Angew. Math. 218 (1965) S. 79–108. *(Der Originalartikel, in dem die Vermutung formuliert wird.)*

[2] S. Singh, Fermats letzter Satz: Die abenteuerliche Geschichte eines mathematischen Rätsels, DTV 2000. *(Sehr gut geschriebene populärwissenschaftliche Darstellung eines anderen großen Problems, bei dessen Lösung die elliptischen Kurven eine Schlüsselrolle gespielt haben.)*

[3] A. Wiles, The Birch and Swinnerton-Dyer Conjecture, erhältlich auf

`http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/`

(Die Clay-Foundation hat 1 Million USD auf die Lösung der Vermutung ausgesetzt. Dies ist die offizielle Website mit der Problemstellung.)

[4] S. Kebekus, Elliptic Curve Plotter, Programmpaket erhältlich unter

`http://home.mathematik.uni-freiburg.de/kebekus/software/ellipticcurve-de.html`

Eine graphische Applikation, mit der man elliptische Kurven zeichnen und mit dem Gruppengesetz experimentieren kann

[5] A. Werner, Elliptische Kurven in der Kryptographie, Springer Verlag 2002. *(Eigentlich für Studierende im Grundstudium.)*

[6] J.S. Milne, Elliptic curves. BookSurge Publishers, Charleston, SC, 2006.

`http://www.jmilne.org/math/Books/ectext.html`

(Lehrbuch für Studierende im Hauptstudium)

[7] J.H. Silverman, J. Tate, Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. *(Ebenfalls, aber viel stärker auf den rationalen Fall konzentriert)*

[8] J.H. Silverman, The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *(Dito, für Leser mit Vorkenntnissen in algebraischer Geometrie. Meine Hauptreferenz, zum Beispiel für die Punkte von $y^2 = x^3 + 17$ oder die Formel für die L-Funktion)*