Die Ordnung von Tate-Shafarevich Gruppen modulo Quadrate

S. Keil, R. N. Kloosterman
(Humboldt-Universität zu Berlin)

keil@math.hu-berlin.de
klooster@math.hu-berlin.de

Lokale und globale Lösungen

Eine der ältesten Problemstellungen der Zahlentheorie ist das Beschreiben der Lösungsmenge von diophantischen Gleichungen. Eine algebraische Gleichung heißt *diophantisch*, wenn alle in ihr vorkommenden Koeffizienten ganze Zahlen sind. Eine allgemeine diophantische Gleichung vom Grad 2 in zwei Variablen hat die Gestalt

$$a_1X^2 + a_2Y^2 + a_3XY + a_4X + a_5Y + a_6 = 0,$$

wobei die sechs Koeffizienten a_i aus $\mathbb{Z}$ sind. In Grad 3 erhalten wir somit die allgemeine Formel

$$a_1X^3 + a_2Y^3 + a_3X^2Y + a_4XY^2 + a_5X^2 + a_6Y^2$$

$$+a_7XY + a_8X + a_9Y + a_{10} = 0.$$

Üblicherweise interessiert man sich nun für ganzzahlige oder rationale Lösungen solcher diophantischer Gleichungen. In diesem Abschnitt werden wir uns am meisten mit diophantischen Gleichungen in zwei Unbekannten beschäftigen.

Gibt es eine rationale Lösung einer diophantischen Gleichung, so gibt es natürlich auch eine reelle Lösung für diese Gleichung, d. h., gibt es keine reelle Lösung, so kann es auch keine rationale Lösung geben. Zum Beispiel hat die Gleichung $X^2 + Y^2 + 1 = 0$ keine rationale Lösung, was man leicht überprüft, indem man zeigt, dass es keine reelle Lösung gibt. Eine Variante der obigen Fragestellung erhält man, indem man *homogene* diophantische Gleichungen in der projektiven Ebene $\mathbb{P}^2_{\mathbb{Q}}$ betrachtet, d. h., man sucht die Nullstellenmenge von Polynomen $f \in \mathbb{Q}[X, Y, Z]$, wobei die Grade der einzelnen Monome alle gleich sind. In Grad 2 erhalten wir demnach die allgemeine Formel

$$a_1X^2 + a_2Y^2 + a_3XY + a_4XZ + a_5YZ + a_6Z^2 = 0$$

mit $a_i \in \mathbb{Q}$. Durch entsprechendes Durchmultiplizieren mit dem Hauptnenner der Koeffizienten a_i ändert sich die Lösungsmenge nicht und man erhält stets ein Polynom aus $\mathbb{Z}[X, Y, Z]$. Ist ein Tripel (x_0, y_0, z_0) eine rationale Lösung eines solchen Polynoms $f(X, Y, Z)$, so ist auch jedes rationale Vielfache davon eine rationale Lösung. Die so erhaltenen Tripel interpretieren wir als eine projektive Lösung $(x_0 : y_0 : z_0)$. Den Nullvektor wollen wir dabei allerdings nicht als gültige Lösung akzeptieren. O.B.d.A. können wir also stets für eine projektive Lösung $(x_0 : y_0 : z_0)$ annehmen, dass $x_0, y_0, z_0 \in \mathbb{Z}$ und $\mathrm{ggT}(x_0, y_0, z_0) = 1$ gilt. Dies ermöglicht uns über eine Lösung modulo p^n zu sprechen, für eine Primzahl p und ein $n \in \mathbb{N}$.

Umgekehrt können wir auch die Gleichung $f \equiv 0 \bmod p^n$ betrachten und nach Lösungen in $\mathbb{Z}/p^n\mathbb{Z}$ fragen. Aus Hensels Lemma lässt sich folgern, dass es für jede Primzahl p ein berechenbares $n_p \in \mathbb{N}$ gibt, so dass für jedes $n \geq n_p$ gilt, dass wenn $f = 0$ eine Lösung modulo p^n hat, dann hat $f = 0$ auch eine Lösung modulo p^{n+1}. Dabei ist die ursprüngliche Lösung aus der späteren rekonstruierbar, indem man einfach wieder modulo p^n rechnet. Man sagt, dass die Lösungen *geliftet* werden können. Gibt es für eine feste Primzahl p ab $n = 1$ eine ununterbrochene Kette solcher Hensel-Lifte, so nennen wir dies eine *p-adische Lösung* der Gleichung $f = 0$. Beschreibt die Gleichung $f = 0$ überdies eine glatte Kurve in $\mathbb{P}^2_{\mathbb{Q}}$, so ist $n_p = 1$, für alle bis auf endlich viele Primzahlen p. Mit weiteren Mitteln der algebraischen Geometrie lässt sich zeigen, dass es eine untere Schranke $m \in \mathbb{N}$ gibt, so dass für alle Primzahlen $p > m$ gilt, dass $f \equiv 0 \bmod p$ eine Lösung hat. Dieses m lässt sich effektiv bestimmen. Für fast alle Primzahlen p weiß man also im glatten Falle bereits *a priori*, dass es eine p-adische Lösung gibt. Und für die endlich vielen verbleibenden Primzahlen lässt sich die Existenz einer p-adischen Lösung durch die Kenntnis der n_p ebenfalls in endlicher Zeit auf einem Rechner überprüfen. Hat eine Gleichung eine reelle Lösung, sowie für jede Primzahl p eine p-adische Lösung, so sagen wir, sie habe *überall lokale Lösungen*.

Für eine diophantische Gleichung ist es eine notwendige Bedingung überall lokale Lösungen zu haben,

um eine tatsächliche Lösung (*globale Lösung*) zu haben. (Falls eine globale Lösung existiert, dann liefert diese Lösung modulo p^n p-adische Lösungen.)

Beispiel 1 (i) Sei $f = X^2 + Y^2 + 5Z^2 \in \mathbb{Q}[X, Y, Z]$. Es ist klar, dass $(0, 0, k)$ eine Lösung von $f \equiv 0 \bmod 5$ ist, für $k \in \mathbb{Z}\setminus\{0\}$. Diese können wir jedoch nicht zu einer Lösung modulo 5^2 liften. Da man aus einem solchen Lift (x_0, y_0, z_0) die alte Lösung rekonstruieren können muss, folgt, dass x_0 und y_0 beide durch 5 teilbar sein müssen. Dies impliziert sofort, dass auch z_0 durch 5 teilbar sein muss, um $f(x_0, y_0, z_0) \equiv 0 \bmod 5^2$ zu erhalten. Damit hätten wir $\text{ggT}(x_0, y_0, z_0) = 5$, bzw. $k = 0$, und somit einen Widerspruch. Die Lösung $(1, 2, 2)$ modulo 5 lässt sich dagegen liften, z. B. zu $(1, 2, 7)$ modulo 5^2. Nun ist hier $n_5 = 2$, so dass mit Hensels Lemma gefolgert werden kann, dass es eine 5-adische Lösung gibt.

(ii) Sei $f = X^2 + Y^2 + 7Z^2 \in \mathbb{Q}[X, Y, Z]$. Man sieht schnell, dass für jede Lösung (x_0, y_0, z_0) modulo 7 gilt, dass x_0 und y_0 durch 7 teilbar sein müssen. Wie im ersten Beispiel bereits gesehen, können derartige Lösungen aber nicht geliftet werden. Da jede Lösung modulo 7^2 stets ein Lift irgendeiner Lösung modulo 7 ist, folgt sofort, dass es gar keine Lösung modulo 7^2 gibt und demnach auch keine 7-adische Lösung.

Das bereits erwähnte Hasse-Prinzip beschäftigt sich mit der Frage, inwieweit die Existenz von überall lokalen Lösungen ausreicht, um die Existenz einer globalen Lösung zu garantieren. Für Gleichungen vom Grad 2 ist dies tatsächlich so:

Satz 2 (Hasse-Prinzip / Satz von Hasse-Minkowski) *Sei $f \in \mathbb{Q}[X, Y, Z]$ ein homogenes Polynom vom Grad 2 und die Gleichung $f = 0$ habe überall eine lokale Lösung. Dann hat die Gleichung $f = 0$ auch eine globale Lösung.*

Falls man eine globale Lösung einer Gleichung vom Grad 2 kennt, so kann man damit relativ einfach alle weiteren globalen Lösungen finden.

Selmer- und Tate-Shafarevich-Gruppen

Ist der Grad gleich 3, so gilt Hensels Lemma noch immer, jedoch das Hasse-Prinzip nicht mehr. Eines der ersten Gegenbeispiele wurde durch Selmer konstruiert: die Gleichung

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

hat überall lokale Lösungen. Selmer bewies, dass sie aber keine globale Lösung hat. Man benötigt also eine andere Strategie als das Hasse-Prinzip, um für Gleichungen dritten Grades entscheiden zu können, ob sie rationale Lösungen haben. Und falls es eine globale Lösung gibt, dann sagt diese Lösung auch wenig über die weiteren Lösungen der Gleichung. (Man kann aus ihr zwar oft weitere globale Lösungen konstruieren, aber dies sind im Allgemeinen nicht alle Lösungen.)

Wir beschäftigen uns nun mit dem Bestimmen aller globalen Lösungen einer diophantischen Gleichung vom Grad 3, wenn man schon mindestens eine Lösung gefunden hat. Dazu macht man sich eine wichtige geometrische Eigenschaft zu Nutze. Derartige Gleichungen beschreiben nämlich eine Kurve in der projektiven Ebene, welche eine sogenannte elliptische Kurve E über $\mathbb{Q}$ ist. Entscheidend ist, dass die rationalen Punkte von E, im Zeichen $E(\mathbb{Q})$, eine abelsche Gruppe bilden, und jede elliptische Kurve $E/\mathbb{Q}$ lässt sich affin als folgende Weierstraß-Gleichung schreiben

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

mit $a_i \in \mathbb{Q}$. In diesem affinen Modell fehlt genau ein Punkt im Unendlichen $(0 : 1 : 0)$, welcher der neutrale Punkt des Gruppengesetzes ist. Eine Gerade schneidet E in genau drei Punkten (mit Vielfachheit) und die Addition ist so definiert, dass die Summe solcher dreier Schnittpunkte gleich dem neutralen Punkt ist. Da wir auf $E(\mathbb{Q})$ addieren können, gibt es also für jedes $n \in \mathbb{N}$ eine natürliche Multiplikation-mit-n-Abbildung. Nach dem Satz von Mordell-Weil ist $E(\mathbb{Q})$ als Gruppe endlich erzeugt, somit ist der Kokern $E(\mathbb{Q})/nE(\mathbb{Q})$ endlich. Überdies ist bei elliptischen Kurven $E/\mathbb{Q}$ der Torsionsanteil von $E(\mathbb{Q})$ leicht zu berechnen. Um $E(\mathbb{Q})$ als abstrakte Gruppe zu kennen, reicht es somit aus, für ein beliebiges $n \geq 2$ den Kokern $E(\mathbb{Q})/nE(\mathbb{Q})$ zu bestimmen.

Folgender traditioneller Ansatz wurde für diesen Zweck versucht. Der Kokern $E(\mathbb{Q})/nE(\mathbb{Q})$ lässt sich in die sogenannte *n-Selmer-Gruppe* $\text{Sel}^{(n)}(E/\mathbb{Q})$ einbetten. Es führt hier zu weit diese Gruppe zu definieren, jedoch weiß man, dass sie endlich ist, und ihre Ordnung ist berechenbar. Die Elemente der *n-Selmer-Gruppe* korrespondieren mit Kurven $C/\mathbb{Q}$, die über einer Körpererweiterung isomorph zu E sind (sogenannte *Twists* von E), und die überall lokale Punkte haben. Außerdem gilt, dass das Bild von $E(\mathbb{Q})/nE(\mathbb{Q})$ in $\text{Sel}^{(n)}(E/\mathbb{Q})$ genau denjenigen Kurven $C/\mathbb{Q}$ entspricht, die mindestens einen rationalen Punkt haben. Diese Kurven erfüllen also das Hasse-Prinzip, da sie überall lokale Lösungen haben und auch eine globale Lösung. Die Einbettung von $E(\mathbb{Q})/nE(\mathbb{Q})$ in die n-Selmer-Gruppe ist im Allgemeinen nicht surjektiv. Die Abweichung zur Surjektivität misst die sogenannte *Tate-Shafarevich-Gruppe* $Ш(E/\mathbb{Q})$. Die Elemente der Tate-Shafarevich-Gruppe entsprechen also den Twists aus der Selmer-Gruppe, die das Hasse-Prinzip nicht erfüllen. Es ist bekannt, dass $Ш(E/\mathbb{Q})$ eine abelsche Torsionsgruppe ist, d. h., jedes Element hat endliche Ordnung. Die n-Torsion von $Ш(E/\mathbb{Q})$, im Zeichen $Ш(E/\mathbb{Q})[n]$, ist eine endliche Gruppe und ist mittels der folgenden kurzen exakten Sequenz definiert

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \text{Sel}^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0.$$

Insgesamt ist über die Tate-Shafarevich-Gruppe wenig bekannt und es gibt keinen Algorithmus, um sie zu berechnen. Dies entspricht ja auch der eingangs gestellten Frage, festzustellen, ob eine Gleichung dritten Gerades einen rationalen Punkt hat. Dies ist auch heute noch ein offenes Problem. Häufig kann jedoch

die Gruppenstruktur von $E(\mathbb{Q})$ trotzdem bestimmt werden, indem man mit Hilfe eines Rechners endlich viele Punkte $P_1, \ldots, P_k$ findet, und zeigt, dass für eine natürliche Zahl n deren Bilder in $\text{Sel}^{(n)}$ die ganze n-Selmer-Gruppe erzeugen. Es wird vermutet, dass die Tate-Shafarevich-Gruppe eine endliche Gruppe ist. Damit wäre $Ш(E/\mathbb{Q})[p]$ bis auf endlich viele Primzahlen p trivial und somit $E(\mathbb{Q})/nE(\mathbb{Q})$ fast immer identisch zur n-Selmer-Gruppe. Basierend auf dieser Vermutung kann mit dem soeben beschriebenen Verfahren die Gruppenstruktur von $E(\mathbb{Q})$ bestimmt werden, indem für hinreichend viele n die n-Selmer-Gruppe bestimmt wird und lange genug nach Punkten gesucht wird.

Eines der bekannten Ergebnisse über die Tate-Shaferevich-Gruppe ist, dass, die Ordnung von $\#Ш(E/\mathbb{Q})$, wenn $Ш(E/\mathbb{Q})$ endlich ist, immer eine Quadratzahl ist. Dies beweist man mit Hilfe einer Paarung auf $Ш(E/\mathbb{Q})$.

Abelsche Varietäten

Wir betrachten nun die höherdimensionalen Verallgemeinerungen von elliptischen Kurven, die sogenannten *abelschen Varietäten*. Die genaue Definition ist ziemlich technisch, jedoch ist im Wesentlichen eine abelsche Varietät eine glatte projektive Varietät A (d. h. eine (glatte) Nullstellenmenge von endlich vielen homogenen Polynomen), so dass auf A eine Gruppenstruktur auf algebraische Weise definiert werden kann.

Im eindimensionalen Fall sind dies genau die elliptischen Kurven. Man erhält sofort Beispiele von n-dimensionalen abelschen Varietäten, indem man das Produkt von n elliptischen Kurven betrachtet. Zwei elliptische Kurven E_1 und E_2 'spannen' also eine abelsche Fläche $E_1 \times E_2$ auf. Die natürlichen Abbildungen zwischen projektiven Varietäten sind rationale Funktionen. Eine solche Abbildung zwischen zwei abelschen Varietäten gleicher Dimension, die gleichzeitig ein Gruppenhomomorphismus ist und einen endlichen Kern hat, nennen wir eine *Isogenie*. Die Definitionen der Selmer- und Tate-Shafarevich-Gruppe lassen sich für abelsche Varietäten beliebiger Dimension verallgemeinern.

Eine konkrete Bestimmung der Tate-Shafarevich-Gruppe ist, wie im Falle der elliptischen Kurven, nur in wenigen Einzelfällen möglich. Anders als im Fall der elliptischen Kurven kann jetzt die Ordnung der Tate-Shafarevich-Gruppe auch eine Nicht-Quadratzahl sein. Fälschlicherweise wurde jedoch für über 30 Jahre angenommen, dass $\#Ш(A/\mathbb{Q})$ immer ein Quadrat ist (sofern endlich). Erst Ende der 1990er Jahren wurde das erste Beispiel einer endlichen Tate-Shafarevich-Gruppe mit nicht-quadratischer Ordnung gefunden [4]. Es handelt sich dabei um eine abelsche Fläche $B/\mathbb{Q}$ mit $\#Ш(B/\mathbb{Q}) = 2\square$, wobei wir mit $\square$ eine passende Quadratzahl meinen. Etwas später wurde ein Beispiel einer abelschen Fläche $B/\mathbb{Q}$ gefunden mit $\#Ш(B/\mathbb{Q}) = 3\square$, sowie andere Beispiele in höheren Dimensionen. Wir werden nun beschreiben, wie man mit Hilfe der Computeralgebra viele Beispiele von abelschen Flächen konstruieren kann, deren Tate-Shafarevich-Gruppe als Ordnung keine Quadratzahl hat.

Abelsche Flächen $B/\mathbb{Q}$ mit $\#Ш(B/\mathbb{Q}) = 5\square$

Nicht nur bei der Bestimmung der rationalen Punkte einer abelschen Varietät spielt die Tate-Shafarevich-Gruppe eine entscheidende Rolle, sondern auch in einem der sieben Millennium-Probleme, der sogenannten *Vermutung von Birch und Swinnerton-Dyer* aus den 1960er Jahren. Auf die Kernaussage dieser bedeutenden Vermutung werden wir später noch eingehen. Zunächst sei erwähnt, dass Cassels und Tate bewiesen haben, dass diese Vermutung invariant unter Isogenien ist, das heißt, es ist bekannt, dass wenn sie für eine abelsche Varietät A zutrifft, so gilt sie auch für jede zu A isogene abelsche Varietät B. Dazu bewiesen Cassels und Tate eine Gleichung, in der viele wichtige Invarianten zweier isogener abelscher Varietäten zueinander in Beziehung gestellt werden. Diese Invarianten sind der Regulator R, die Periode P, die duale abelsche Varietät $A^\vee$, der Torsionsanteil $A(\mathbb{Q})_{\text{tors}}$ der rationalen Punkte und für jede Primzahl p die lokale Tamagawazahl c_p. Das Produkt im nachstehenden Satz ist wohldefiniert, da $c_p = 1$ gilt, für alle bis auf endlich viele Primzahlen.

Satz 3 (Gleichung von Cassels und Tate) *[1] [5] Sei $\varphi : A \to B$ eine Isogenie zwischen zwei abelschen Varietäten A und B über $\mathbb{Q}$. Sind $Ш(A/\mathbb{Q})$ und $Ш(B/\mathbb{Q})$ endlich, so lässt sich der Quotient der Ordnungen der Tate-Shafarevich-Gruppen $\frac{\#Ш(A/\mathbb{Q})}{\#Ш(B/\mathbb{Q})}$ wie folgt berechnen:*

$$\frac{R_B}{R_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}}\,\#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}}\,\#B^\vee(\mathbb{Q})_{\text{tors}}} \cdot \frac{P_B}{P_A} \cdot \prod_{p \text{ prim}} \frac{c_{B,p}}{c_{A,p}} \quad (1)$$

Wir haben diese Gleichung benutzt, um Beispiele von abelschen Flächen mit Tate-Shafarevich-Gruppe der Ordnung 5 mal ein Quadrat zu konstruieren. Seien dazu E_1 und E_2 zwei elliptische Kurven über $\mathbb{Q}$, die einen rationalen Torsionspunkt der Ordnung 5 haben; nennen wir diesen P_1 bzw. P_2. Nun bilden wir das Produkt dieser beiden elliptischen Kurven, d. h., wir erhalten eine abelsche Fläche und betrachten die folgende Isogenie

$$\varphi : E_1 \times E_2 \to B,$$

wobei der Kern von φ von dem Punkt (P_1, P_2) erzeugt wird, dass heißt, er ist eine zyklische Gruppe der Ordnung 5. Die abelsche Fläche $B/\mathbb{Q}$ ist also der Quotient $(E_1 \times E_2)/\langle(P_1, P_2)\rangle$. Da die Tate-Shafarevich-Gruppe eines Produktes das Produkt der beiden Tate-Shafarevich-Gruppen ist, erhalten wir dass

$$\#Ш(E_1 \times E_2) = \#Ш(E_1) \cdot \#Ш(E_2) = \square,$$

sofern die Kardinalitäten endlich sind, was wir ab jetzt immer annehmen wollen. Desweiteren ist der Grad der Isogenie φ gleich 5, weswegen sich die Ordnung von $Ш(B/\mathbb{Q})$ nur um eine 5-Potenz von der von $Ш(E_1 \times E_2)$ unterscheiden kann. Somit wissen wir *a priori*, dass

$\#Ш(B/\mathbb{Q}) = \square$ oder $5\square$ ist. Um dies konkret entscheiden zu können, reicht es also (1) modulo Quadraten zu bestimmen. Dazu zerlegen wir dieses Produkt erneut in zwei Teile, und zwar in den Regulator- und Torsionsquotienten

$$\frac{R_B}{R_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}} \#B^\vee(\mathbb{Q})_{\text{tors}}},$$

welches wir den *globalen Quotienten* nennen, und in den Perioden- und Tamagawazahlenquotienten

$$\frac{P_B}{P_A} \cdot \prod_{p \text{ prim}} \frac{c_{B,p}}{c_{A,p}},$$

welches wir den *lokalen Quotienten* nennen. Nun nutzen wir die Tatsache, dass sich alle elliptischen Kurven $E/\mathbb{Q}$, die einen rationalen 5-Torsionspunkt haben, mittels einer rationalen Zahl $d \in \mathbb{Q} \setminus \{0\}$ parametrisieren lassen. Diese elliptischen Kurven entsprechen nämlich genau den Weierstraß-Gleichungen

$$E : Y^2 + (d+1)XY + dY = X^3 + dX^2.$$

Wir identifizieren also unser Produkt $E_1 \times E_2$ mit dem Paar (d_1, d_2), wobei wir wiederum $d_i = u_i/v_i$ als Quotient zweier ganzer, teilerfremder Zahlen $u_i, v_i \in \mathbb{Z}$ schreiben. Der lokale Quotient und auch der Torsionsquotient lassen sich nun sehr einfach aus der Primfaktorzerlegung der u_i und v_i und aus dem Verhalten der d_i modulo 5-ter Potenzen bestimmen. Dafür definieren wir für alle Primzahlen p eine rationale Zahl lokal_p. Gilt $p \mid u_1v_1u_2v_2$, so ist $\text{lokal}_p = 1/5$. Falls $p \equiv 1(5)$ ist und p ist ein Teiler von $\text{ggT}(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2)$ dann ist lokal_p gleich 5. Falls $p = 5$ und 25 teilt $u_1 - 7v_1 \equiv u_2 - 7v_2$ dann ist lokal_5 gleich 5. Für die übrigen Fälle gilt $\text{lokal}_p = 1$.

Satz 4 *[2, Thm. 4.3] Der lokale Quotient lässt sich als folgendes endliches Produkt berechnen:*

$$\frac{1}{5} \cdot \prod_{p \text{ prim}} \text{lokal}_p.$$

Der Torsionsquotient läßt sich ebenso sehr einfach bestimmen.

Satz 5 *[2, Prop. 4.6] Der Torsionsquotient hat den Wert*

$$\begin{cases} 1 \text{ oder } 5, & d_1, d_2 \in \mathbb{Q}^{*5}, \\ 5^2, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j, \\ 5^2, & \langle 1\rangle \neq \langle d_1\rangle = \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}, \\ 5^3, & \langle 1\rangle \neq \langle d_1\rangle \neq \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}. \end{cases}$$

Der Einfachheit halber haben wir im Torsionsquotienten den Fall, dass beide d_i 5-te Potenzen sind, nicht weiter spezifiziert.

Beispiel 6 Seien $E_1/\mathbb{Q}$ und $E_2/\mathbb{Q}$ gegeben durch $d_1 = u_1/v_1 = 1/11$ und $d_2 = u_2/v_2 = 2/9$. Mit den obigen Sätzen rechnet man leicht nach, dass der lokale Quotient $1/5^4$ ist: Für die drei Primzahlen $p = 2, 3, 11$ gilt $\text{lokal}_p = 1/5$ und für alle anderen Primzahlen gilt $\text{lokal}_p = 1$. Der Torsionsquotient ist gleich 5^3. Mit dem Computer bestimmt man nun den sogenannten analytischen Rang der beiden elliptischen Kurven, welcher in beiden Fällen gleich 0 ist. Dies impliziert sofort, dass der Regulatorquotient gleich 1 ist. Außerdem ist dies einer der wenigen bewiesenen Fälle, bei denen wir wissen, dass die Tate-Shafarevich-Gruppen endlich sind. Wir erhalten also vollkommen unkonditionell die Gleichung

$$\#Ш(B) = 5 \cdot \#Ш(E_1 \times E_2) = 5\square.$$

Regulatorquotient & Computer-Algebra

Es bleibt somit noch übrig den Regulatorquotienten $R_B/R_{E_1\times E_2}$ zu berechnen. Für diesen Quotienten gibt es nach unseren Kentnissen keine einfache Formel, wie für die anderen beiden Quotienten. Wir können allerdings einen Algorithmus angeben, mit welchem er in vielen Fällen mit Hilfe des Computers berechnet werden kann. Dazu müssen wir zunächst die Gruppen $E_1(\mathbb{Q})$ und $E_2(\mathbb{Q})$ bestimmen. Eine Möglichkeit wäre es hier für geeignete n, die n-Selmer-Gruppen zu bestimmen und hinreichend viele Punkte auf $E_1(\mathbb{Q})$ zu finden, wie wir oben bereits erwähnt haben. In viele Fällen kann man dies jedoch umgehen, indem man entweder bewiesene Fälle der Birch und Swinnerton-Dyer-Vermutung ausnutzt oder diese Vermutung annimmt. Da $E(\mathbb{Q})$ eine endlich erzeugte Gruppe ist, gilt abstrakt $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$, für eine nicht-negative ganze Zahl r, genannt der *Mordell-Weil-Rang* von $E/\mathbb{Q}$. Die Kernaussage der Birch und Swinnerton-Dyer-Vermutung betrifft den analytischen Rang und besagt, dass dieser gleich dem Mordell-Weil-Rang ist. Es ist bewiesen, dass wenn der analytische Rang gleich 0 oder 1 ist, dann gleicht er tatsächlich dem Mordell-Weil-Rang. In diesem Fall weiß man zudem noch, dass die Tate-Shafarevich-Gruppe endlich ist.

Dieser analytische Rang ist die Ordnung einer Nullstelle einer holomorphen Funktion. Falls diese Ordnung höchstens drei ist (was für die meisten Beispiele gilt), so kann man diesen analytischen Rang vergleichsweise einfach und schnell (auf einem Rechner) bestimmen.

Ist der analytische Rang 0, so weiß man, dass $E(\mathbb{Q})$ endlich ist. Falls der analytische Rang 1 ist, dann braucht unser Algorithmus einen einzigen beliebigen Punkt unendlicher Ordnung. Solch einen Punkt zu finden ist allerdings keine triviale Aufgabe, denn die Zähler und Nenner der Koeffizienten dieser Punkte können sehr groß werden. Nimmt man z. B. die elliptische Kurve mit $d = 83/74$, welche analytischen Rang 1 hat, so dauert es sehr lange den ersten Punkt unendlicher Ordnung zu finden, wenn man systematisch alle rationalen X-Werte durchläuft und prüft ob es dazu einen rationalen Y-Wert gibt. Der 'kleinste' X-Wert

dieses Beispiels hat einen negativen Zähler mit 44 Ziffern und einen Nenner mit 40 Ziffern. Das Berechnen von Selmer-Gruppen stellt sich hier zusätzlich als sehr hilfreich heraus, da man mit deren Kenntnis auch den Punktesuch-Algorithmus deutlich beschleunigen kann. Im Falle dass der Rang gleich 1 ist, kann auch mit der Theorie der Heegner-Punkte auf einem Computer ein Punkt unendlicher Ordnung auf der elliptischen Kurve gefunden werden.

Falls der analytische Rang größer als eins ist, dann ist die Birch und Swinnerton-Dyer-Vermutung noch offen. Für diese Kurven nehmen wir stets an, dass der analytische Rang mit dem Mordell-Weil-Rang übereinstimmt.

Hat man nun eine 'Basis' von $E_1(\mathbb{Q})$ und $E_2(\mathbb{Q})$ bestimmt, so kann daraus der Regulatorquotient $R_B/R_{E_1\times E_2}$ berechnet werden. Falls beide Gruppen endlich sind, so ist der Regulatorquotient gleich 1. Sonst benutzt man die Erzeuger von $E_i(\mathbb{Q})$ (modulo Torsionspunkten) um endlich viele Zahlen in $\mathbb{Q}^*/\mathbb{Q}^{*5}$ und in $\mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*5}$ zu bestimmen. Dann muss man die Ordnung der durch diese Zahlen erzeugten Untergruppen bestimmen. Nun kann man mit Hilfe der Theorie abelscher Varietäten zeigen, dass der Regulatorquotient genau dann ein Quadrat ist, wenn das Produkt dieser Ordnungen ein Quadrat ist.

Ergebnisse

Das oben beschriebene Verfahren haben wir auf alle Paare von elliptischen Kurven E_1 und E_2 angewendet, für deren Parameter d_1 und d_2 die Zähler und Nenner betragsmäßig durch 100 beschränkt sind. Daraus resultierten ungefähr $18,5$ Millionen abelsche Flächen, wovon $49,31\%$ eine Tate-Shafarevich-Gruppe mit Ordnung $5\square$ haben. Jedoch ist dieses Ergebnis bedingt durch Annahme der Birch und Swinnerton-Dyer-Vermutung.

Betrachtet man davon nur die abelschen Flächen, so dass beide zugehörigen elliptischen Kurven analytischen Rang 0 oder 1 haben, (d. h., die Birch und Swinnerton-Dyer-Vermutung ist schon bewiesen für E_1 und E_2), so ergibt dies $14,7$ Millionen abelsche Flächen von denen $49,95\%$ eine Tate-Shafarevich-Gruppe mit Ordnung $5\square$ haben [3].

Insbesondere zeigt dies, dass man häufig in der Lage ist, zu unterscheiden, ob die Ordnung der Tate-Shafarevich-Gruppe ein Nicht-Quadrat ist, ohne deren Ordnung selbst zu berechnen.

Literatur

[1] Cassels, J. W. S. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[2] Keil, Stefan. Examples of abelian varieties with non-square Tate-Shafarevich group. Preprint 2012, *arXiv:1206.1822v1*.

[3] Keil, Stefan and Kloosterman, Remke N. On the density of abelian surfaces with Tate-Shafarevich group of order five times a square. Erscheint in: *Algorithmic number theory, 10th international symposium, ANTS-X Proceedings*, 2013.

[4] Poonen, Bjorn and Stoll, Michael. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150:1109–1149, 1999.

[5] Tate, John. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki, Vol. 9*, 9:415–4401, 1995.