Galoisdarstellungen von elliptischen Kurven mit komplexer Multiplikation

Ernst Kani
Queen's University at Kingston

Tübinger Seminar, Erlangen
5. Mai 2018

Outline

1. Einleitung

- Es sei:

  E/k eine elliptische Kurve über einem Zahlkörper k,

  $N \geq 3$ eine Primzahl,

  $\rho_{E/k,N}$: $G_k = \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

  die zugehörige Galoisdarstellung.

- Vermutung 1 (Frey). Es gibt eine Konstante $c_{E/k}$ derart, daß $\forall$ Primzahlen $N > c_{E/k}$ und alle elliptischen Kurven E'/k gilt:

  (1) $$\rho_{E/k,N} \simeq \rho_{E'/k,N} \quad \Rightarrow \quad E \sim_k E'.$$

- Bemerkung: Nach Frey (1995) besteht ein enger Zusammenhang zwischen Vermutung 1 und der asymptotischen Fermat Vermutung.

1. Einleitung – 2

- Vermutung 2 (Darmon, 1995). Es gibt eine Konstante c_k derart, daß für alle elliptischen Kurven E/k und E'/k und alle Primzahlen $N > c_k$ gilt:

$$\rho_{E/k,N} \simeq \rho_{E'/k,N} \quad \Rightarrow \quad E \sim_k E'. \tag{2}$$

- Bemerkung: Vermutung 2 wird oft die Frey-Mazur Vermutung genannt. Besser: Darmon-Frey-Mazur Vermutung.
- Frage 1: Kann man diese Vermutungen für CM-Kurven beweisen?
- Erinnerung: Eine CM-Kurve ist eine elliptische Kurve E/k mit $\mathrm{End}(E) := \mathrm{End}_{\overline{k}}(E) \neq \mathbb{Z}$.

1. Einleitung – 3

- Vermutung 3 (Serre, 1972). Es gibt eine Konstante s_k mit der Eigenschaft, daß für alle Primzahlen $N > s_k$ und alle elliptischen Kurven E/k ohne CM gilt:

$$|\mathrm{Im}(\rho_{E/k,N})| = |\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})|. \tag{3}$$

- Bemerkung: Serre bewies 1972, daß es zu jeder elliptischen Kurve E/k ohne CM eine Konstante $s_{E/k}$ gibt, derart, daß (3) für $N > s_{E/k}$ gilt.
- Frage 2: Wie sieht die Serresche Vermutung für CM Kurven aus?

1. Einleitung – 4

- Bemerkung. Ist E/k eine CM-Kurve mit CM Körper K, und ist N eine Primzahl, so gilt stets, daß

$$|\mathrm{Im}(\rho_{E/k,N})| \leq |\mathcal{E}_N^\times|[Kk : k], \tag{4}$$

wobei $\mathcal{E}_N^\times = (\mathrm{End}(E)/N\,\mathrm{End}(E))^\times$. Serre bewies 1972, daß es eine Konstante $s'_{E/k}$ gibt so, daß für $N > s'_{E/k}$ (und $K \subset k$) die Gleichheit in (4) gilt.

- Nebenmerkung: Ist E/k eine CM-Kurve mit CM Körper K, so ist $\mathrm{End}(E)$ isomorph zu einer Ordnung in K. Ist $D < 0$ die Diskriminante dieser Ordnung und ist N eine Primzahl, so gilt

$$|\mathcal{E}_N^\times| = (N-1)\left(N - \left(\frac{D}{N}\right)\right),$$

wobei $\left(\frac{D}{N}\right)$ das Legendre-Kronecker Symbol bedeutet.

- Frage 2*: Gibt es eine Konstante s'_k derart, daß für jede CM-Kurve E/k und jede Primzahl $N > s'_k$ die Formel

$$|\mathrm{Im}(\rho_{E/k,N})| \;=\; |\mathcal{E}(E)_N^{\times}|[K_E k : k] \tag{5}$$

gilt? Hierbei ist $\mathcal{E}(E)_N^{\times} = (\mathrm{End}(E)/N\,\mathrm{End}(E))^{\times}$ und $K_E \simeq \mathrm{End}(E) \otimes \mathbb{Q}$ der CM-Körper von E.

2. Hauptresultate

- Satz 1: Die Darmon-Frey-Mazur Vermutung gilt für CM-Kurven. Mit anderen Worten: es gibt eine Konstante c'_k derart, dass für alle Primzahlen $N > c'_k$ die Implikation

$$\rho_{E/k,N} \simeq \rho_{E'/k,N} \quad \Rightarrow \quad E \sim_k E' \tag{6}$$

  für alle CM-Kurven E/k und E'/k gilt.

- Bemerkung: Der Beweis dieser Aussage benützt ein schönes Resultat von Frey/Jarden (2002) (und mehr).
- Satz 2: Ist $k = \mathbb{Q}$, so gilt Satz 1 mit $c'_{\mathbb{Q}} = 5$.

2. Hauptresultate - 2

- Korollar: Gilt die Serre Vermutung für k, so gilt auch die Frey Vermutung für CM-Kurven E/k.
- Frage 1*: Kann man die Frey Vermutung für CM-Kurven E/k beweisen (ohne Benützung der Serre Vermutung)?

2. Hauptresultate - 3

- Satz 3: Es kann keine Konstante s'_k geben, die den Bedingungen von Frage 2* genügt.
- Dies folgt aus der folgenden genaueren Aussage:
- Satz 4: Es sei $N \geq 5$ eine Primzahl mit $N \not\equiv \pm 1 \mod 9$. Dann gibt es eine elliptische Kurve $E/\mathbb{Q}$ mit $j(E) = 0$ derart, daß (5) für dieses N nicht gilt, d.h. es ist

$$|\mathrm{Im}(\rho_{E/\mathbb{Q},N})| < 2(N-1)\left(N - \left(\frac{-3}{N}\right)\right).$$

2. Hauptresultate - 4

- Satz 5: Es sei k ein Zahlköper mit mindestens einer reellen Einbettung (d.h., $r_k \geq 1$). Dann gibt es eine Konstante s_k'' derart, daß die Gleichung (5) gilt für alle Primzahlen $N > s_k''$ und alle CM-Kurven E/k mit $j(E) \neq 0$.
- Satz 6: Für $K = \mathbb{Q}$ gilt Satz 5 mit $s_k'' = 163$.

3. Beweistechnik I: CM-Körper

- Bezeichnung: Es sei

$$k(E[N]) \;=\; \overline{k}^{\mathrm{Ker}(\rho_{E/k,N})}$$

der N-Teilungskörper von E/k.

- Satz 7 (Frey/Jarden[FJ], 2002). Es seien $K_1 \neq K_2$ zwei verschiedene imaginär-quadratische Zahlkörper. Dann gibt es zu jedem Zahlkörper k eine Konstante $c_{k,K_1,K_2} > 0$ derart, daß

$$[k(E_1[N])k(E_2[N]) : k(E_1[N])] \;\geq\; c_{k,K_1,K_2} N, \tag{7}$$

für alle elliptischen Kurven E_i/k mit $\mathrm{End}(E_i) \simeq \mathfrak{O}_{K_i}$ und alle Primzahlen $N \geq 3$.

- Bemerkung: Satz 7 wird implizit im Beweis von Theorem 3.5 von [FJ] bewiesen.

3. Beweistechnik I: CM-Körper - 2

- Definition. Es sei k ein Zahlkörper. Ein imaginär-quadratischer Körper K heißt *CM-Körper von k*, wenn es eine elliptische Kurve E/k mit $\mathrm{End}(E) \simeq \mathfrak{O}_K$ gibt.
- Satz 8 (Heilbronn, 1934). Ein Zahlkörper k besitzt nur endlich viele CM-Körper.
- Bemerkung: Nach Heilbronn[H] (1934) gibt es nur endlich viele imaginär-quadratische Zahlkörper K mit beschränkter Klassenzahl h_K, und daraus folgt Satz 8, da $h_K | [k : \mathbb{Q}]$ für jeden CM-Körper K von k. Aus den Sätzen 7 und 8 folgt:

3. Beweistechnik I: CM-Körper - 3

- Satz 9. Es gibt eine Konstante c_k'' derart, daß für alle CM-Kurven E_i/k mit $\mathrm{End}(E_i) \simeq \mathfrak{O}_{K_i}$ gilt:

  (8) $$\rho_{E_1/k,N} \simeq \rho_{E_2/k,N},\ N > c_k'' \ \Rightarrow\ K_1 = K_2.$$

- Satz 10. Für $k = \mathbb{Q}$ gilt die Aussage von Satz 7 mit $c_{\mathbb{Q}}'' = 3$.
- Bemerkung: Der Beweis von Satz 10 benützt weder Satz 7 noch Satz 8.

4. Beweistechnik II: Galoisdarstellungen von Twists

- Satz 11. Es seien E_1/k und E_2/k zwei CM-Kurven mit $j(E_1) = j(E_2)$, und sei K der gemeinsame CM-Körper von E_1 und E_2. Ist $K \subset k$ und ist

$$|\mathrm{Im}(\rho_{E/k,N})| \ > \ (N-1)|\mathrm{Aut}(E_1)|, \tag{9}$$

wobei $N \geq 5$ eine Primzahl ist, so gilt

$$\rho_{E_1/k,N} \simeq \rho_{E_2/k,N} \ \Rightarrow \ E_1 \simeq_k E_2. \tag{10}$$

4. Beweistechnik II: Galoisdarstellungen von Twists - 2

- Bemerkung: Satz 11 ist relativ einfach zu beweisen, wenn $j(E_i) \neq 0, 1728$, da in diesem Fall $E_2 \simeq (E_1)_\psi$ ein quadratischer Twist von E_1 ist, und dann gilt

$$\rho_{E_2/k,N} \simeq \rho_{E_1/k,N} \otimes \psi.$$

Für die Ausnahmefälle $j(E_i) = 1728$ bzw. $j(E_i) = 1728$ muß man aber auch quartische bzw. sextische Twists in Betracht ziehen, und für diese ist die Beziehung zwischen $\rho_{E_1/k,N}$ und $\rho_{E_2/k,N}$ wesentlich komplizierter.

5. Beweistechnik III: Die Größe des Bildes

- Satz 12. Es sei k Zahlkörper und K ein CM-Körper von k. Ist $N \geq 3$ eine Primzahl mit $N \nmid d_{Kk} := \mathrm{disc}(Kk/\mathbb{Q})$, so gilt

$$(11)\quad |\mathrm{Im}(\rho_{E/k,N})| \;\geq\; (N-1)(N-(\frac{d_K}{N}))[Kk:k]/|\operatorname{Aut}(E)|,$$

  für alle E/k mit $\mathrm{End}(E) \simeq \mathfrak{O}_K$.
- Bemerkung. Dies benützt die (analytische) Theorie der komplexen Multiplikation. (Klassifikation der Weber Körper.)
- Korollar: Ist N eine Primzahl mit $N > \max(d_{Kk}, 37)$, so gilt die Voraussetung (9) von Satz 11 (falls $K \subset k$).

6. Beweistechnik IV: Die Existenz von Isogenien

- Vorbemerkung 1. Sei E/k eine CM-Kurve mit CM-Körper K.
(a) Ist $K \subset k$, so liefert nach Deuring[D] jedes Ideal $\mathfrak{a}$ von $\mathrm{End}(E)$ eine k-Isogenie

$$\pi_{\mathfrak{a}} : E \to E' \quad \text{mit Kern} \quad E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \mathrm{Ker}(\alpha).$$

Ferner gilt (vgl. [PCM]):

$$\deg(\pi_{\mathfrak{a}}) \;=\; [\mathrm{End}(E) : \mathfrak{a}].$$

(b) Ist $K \not\subset k$, so gelten die Aussagen von (a) noch für diejenigen Ideale $\mathfrak{a}$, die unter der kanonischen Involution (= der komplexen Konjugation) von $\mathrm{End}(E)$ invariant sind: $\overline{\mathfrak{a}} = \mathfrak{a}$.

6. Beweistechnik IV: Die Existenz von Isogenien - 2

- Vorbemerkung 2. Für uns ist es wichtig, etwas über der Grad einer k-Isogenie $\phi : E \to E'$ zu wissen, denn es gilt

$$N \nmid \deg(\phi) \Rightarrow \rho_{E/k,N} \simeq \rho_{E'/k,N}. \tag{12}$$

- Satz 13. Es sei E/k eine CM-Kurve mit $\mathrm{End}(E) \simeq \mathcal{O}_D$ und CM-Köper $K = \mathbb{Q}(\sqrt{D})$. Ist $f = [\mathfrak{O}_K : \mathcal{O}_D]$ der Führer von $\mathcal{O}_D$, so gibt es eine k-Isogenie

$$\phi : E \to E'$$

vom Grad f derart, daß $\mathrm{End}(E') \simeq \mathfrak{O}_K$ ist.

6. Beweistechnik IV: Die Existenz von Isogenien - 3

- Satz 14. Es seien E_i/k zwei CM-Kurven mit $\mathrm{End}(E_1) \simeq \mathrm{End}(E_2)$. Ist $K \subset k$, so gibt es eine Kurve E_2'/k mit

$$E_2' \sim_k E_1 \quad \text{und} \quad j(E_2') = j(E_2).$$

  Ferner kann man die Isogenie $\phi : E_1 \to E_2'$ so wählen, daß ihr Grad prim zu einer vorgegebenen Zahl m ist.

- Satz 15. Es seien E_i/k zwei CM-Kurven mit gemeinsamen CM-Körper $K \not\subset k$. Dann gilt:

$$E_1 \sim_{Kk} E_2 \;\Rightarrow\; E_1 \sim_k E_2.$$

7. Beweisskizze von Satz 1

- Behauptung: Satz 1 gilt mit

$$c'_k \;=\; \max(37, d_{K_1 k}, \ldots, d_{K_t k}, c''_k),$$

wobei $K_1, \ldots, K_t$ die endlich vielen CM-Körper von k sind (vgl. Satz 8) und c''_k die Konstante von Satz 9 ist.

- Beweisskizze. Es sei $N > c'_k$ eine Primzahl und seien E_1/k und E_2/k zwei CM-Kurven mit

$$\rho_{E_1/k,N} \simeq \rho_{E_2/k,N}.$$

- 1. Schritt: Es sei K_i der CM-Körper von E_i/k. Nach Satz 13 gibt es E'_i/k mit $\mathrm{End}(E'_i) \simeq \mathfrak{O}_{K_i}$ und eine k-Isogenie $\phi_i : E_i \to E'_i$ mit $N \nmid \deg(\phi_i)$. Nach (12) gilt also $\rho_{E_i/k,N} \simeq \rho_{E'_i/k,N}$ für $i = 1, 2$, und daher ist

(13)
$$\rho_{E'_1/k,N} \simeq \rho_{E'_2/k,N}.$$

7. Beweisskizze von Satz 1 - 2

- 2. Schritt: Nach Satz 9 folgt aus (13), daß $K_1 = K_2$ ist, und daher gilt $\mathrm{End}(E_1') \simeq \mathfrak{O}_{K_i} \simeq \mathrm{End}(E_2')$. Sei $k' = K_1 k = K_2 k$. Nach Satz 14 gibt es daher eine Twistkurve E_2''/k' von E_2/k' und eine k'-Isogenie $\psi : E_1' \to E_2''$ mit $N \nmid \deg(\psi)$.
- 3. Schritt: Aus (13) und dem vorherigen Schritt folgt:

$$\rho_{E_2'/k',N} \simeq \rho_{E_1'/k',N} \simeq \rho_{E_2''/k',N}.$$

  Da $j(E_2') = j(E_2'')$ ist, so folgt aus Satz 11 (zusammen mit dem Korollar von Satz 12), daß $E_2'' \simeq_{k'} E_2'$. Somit ist $E_1' \sim_{k'} E_2'$.
- 4. Schritt: Aus dem vorherigen Schritt und Satz 15 folgt, daß $E_1' \sim_k E_2'$, und daher ist $E_1 \sim_k E_1' \sim_k E_2' \sim_k E_2$. Somit gilt also (6). ■

8. Beweisskizze der Sätze 2, 5, 6 und 10

- Satz 16: Es sei $E/\mathbb{Q}$ eine CM-Kurve mit CM-Diskriminante $D \neq -3$. Ist $N \geq 5$ eine Primzahl mit $N \nmid D$, so ist $G := \mathrm{Im}(\rho_{E/\mathbb{Q},N})$ eine Gruppe der Ordnung

$$|G| = 2(N-1)N_D,$$

  wobei $N_D := N - \left(\frac{D}{N}\right)$, und $G/Z(G)$ ist eine Diedergruppe der Ordnung $2N_D$, wobei $Z(G)$ das Zentrum von G bezeichnet.

- Bemerkungen: 1) Satz 16 folgt aus der Theorie der komplexen Multiplication (Weber Körper) zusammen mit einem genauen Studium der Galoiswirkung auf $E[N]$.
  2) Satz 16 + Satz von Heegner $\Rightarrow$ Satz 6.
  3) Die Beweismethode von Satz 1 (zusammen mit der von Satz 16) ergibt einen Beweis von Satz 5.

8. Beweisskizze der Sätze 2, 5, 6 und 10 - 2

- Zusatz: In der Situation von Satz 16 sei

$$L := \overline{\mathbb{Q}}^{\rho_{E/\mathbb{Q},N}^{-1}(Z(G))} \subset \mathbb{Q}(E[N]).$$

  Dann ist $L/\mathbb{Q}$ eine Diedererweiterung, die den CM-Körper K von E enthält, und L/K ist zyklisch vom Grad N_D.

- Bemerkung: 1) Ist $N_D \geq 3$, so beinhaltet der Zusatz eine darstellungstheorische Kennzeichnung des CM-Körpers K von E, und daraus erhält man leicht die Aussage von Satz 10. (Man muß aber einige Ausnahmefälle separat behandeln.)
  2) Mithilfe der schärferen Sätze 6 und 10 kann man dann Satz 2 mit einer ähnlichen Methode beweisen, wie mit der vom Beweis von Satz 1.

9. Beweisskizze der Sätze 3 und 4

- Bemerkung: Es ist klar (nach Dirichlet), daß Satz 3 aus Satz 4 folgt. Es reicht also, Satz 4 zu beweisen.
- 1. Schritt: Es sei $K = \mathbb{Q}(\sqrt{-3})$. Dann gibt es eine CM-Kurve $E/\mathbb{Q}$ mit $j(E) = 0$ derart, daß für jede Primzahl $N \geq 5$ die Gruppe $H = \mathrm{Im}(\rho_{E/K,N})$ die folgende Struktur hat:

$$H \simeq \begin{cases} \mathbb{F}_N^\times \times \mathbb{F}_N^\times & \text{falls } N \equiv 1 \mod 3 \\ \mathbb{F}_{N^2}^\times & \text{falls } N \equiv 2 \mod 3 \end{cases}$$

In der Tat: sei $E_1/\mathbb{Q}$ eine Kurve mit CM-Diskriminante $D = -12$. Nach Satz 13 gibt es eine CM-Kurve $E/\mathbb{Q}$ mit $j(E) = 0$ und eine $\mathbb{Q}$-Isogenie $\phi : E_1 \to E$ vom Grad 2. Da $\rho_{E/\mathbb{Q},N} \simeq \rho_{E_1/\mathbb{Q},N}$ ist, so folgt die Aussage aus Satz 16.

9. Beweisskizze der Sätze 3 und 4 - 2

- 2. Schritt: Ist $N \geq 5$ eine Primzahl mit $N \not\equiv \pm 1 \mod 9$, so gibt es einen Homomorphimsm

$$h : H = \mathrm{Im}(\rho_{E/K,N}) \to \mathrm{Aut}(E) \simeq \mathbb{Z}/6\mathbb{Z}$$

der Ordnung 6 mit der folgenden Eigenschaft. Ist E'/K der Twist von E/K bezüglich

$$\chi := h \circ \rho_{E/K,N} : G_K \to \mathrm{Aut}(E),$$

so ist $[\mathrm{Ker}(\rho_{E'/K,N}) : \mathrm{Ker}(\rho_{E/K,N})] = 3$ und daher ist

$$|\mathrm{Im}(\rho_{E'/K,N})| = \frac{1}{3}|\mathrm{Im}(\rho_{E/K,N})|.$$

9. Beweisskizze der Sätze 3 und 4 - 3

- 3. Schritt: Es sei $G = \mathrm{Im}(\rho_{E/\mathbb{Q},N})$. Dann weist man nach, daß die Restriktionsabbildung

$$H^1(G, \mathrm{Aut}(E)) \to \mathrm{Hom}(H, \mathrm{Aut}(E))^{G/H}$$

surjektiv ist, und daraus sieht man leicht, daß es zu dem obigen h ein $h' \in H^1(G, \mathrm{Aut}(E))$ mit $(h')_{|H} = h$ gibt. Somit ist $\chi' = h' \circ \rho_{E/\mathbb{Q},N} \in H^1(G_{\mathbb{Q}}, \mathrm{Aut}(E))$, und der Twist $E''/\mathbb{Q}$ von $E/\mathbb{Q}$ bezüglich χ' erfüllt die gewünschte Eigenschaft, denn

$$|\mathrm{Im}(\rho_{E''/\mathbb{Q},N})| = \frac{1}{3}|\mathrm{Im}(\rho_{E/\mathbb{Q},N})|.$$

10. Literatur

[D] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.

[FK] G. Frey, E.K., Curves of genus 2 and associated Hurwitz spaces. *Contemp. Math.* **487** (2009), 33–81.

[FJ] G. Frey, M. Jarden, Horizontal isogeny theorems. *Forum Math.* **14** (2002), 931–952.

[H] H. Heilbronn, On the class-number in imaginary quadratic fields. *Quart. J. Math.* **5** (1934), 150–160.

[PCM] E.K., Products of CM elliptic curves. *Collect. Math.* **62** (2011), 297–339.