Fermats letzter Satz und Modularität

1.Teil: Spezialfälle und Modularität

Christian Geyer

Technische Universität Kaiserslautern
Fachbereich Mathematik
AG Algebra, Geometrie und Computeralgebra

27.Juni 2011

Inhalt

Fall $n \in \{1,2\}$

Lemma

Für $n \in \{1,2\}$ existieren $x,y,z \in \mathbb{Z}\backslash\{0\}$ welche die Gleichung

$$x^n + y^n = z^n$$

lösen. $\square$

Fall $n = 3$

Lemma

Die Fläche eines ganzzahligen, rechtwinkligen Dreiecks ist nie eine Quadratzahl $\square$

Satz

Es gibt kein Tripel $(x, y, z) \in \mathbb{Z}^3$ *mit* $xyz \neq 0$ *welches die Gleichung* $x^3 + y^3 = z^3$ *erfüllt.* $\square$

Fall $n = 4$

Satz

Es gibt kein Tripel $(x, y, z) \in \mathbb{Z}^3$ *mit* $xyz \neq 0$ *welches die Gleichung* $x^4 + y^4 = z^4$ *erfüllt.* $\square$

Reduktion auf Primzahlen

Lemma

Um Fermats letzten Satz zu zeigen, genügt es die Fälle $n \in \{1,2,3,4\}$ *und* $n \in \mathbb{P}\backslash\{2\}$ *zu betrachten.*

Reduktion auf Primzahlen

Lemma

Um Fermats letzten Satz zu zeigen, genügt es die Fälle $n \in \{1,2,3,4\}$ *und* $n \in \mathbb{P}\backslash\{2\}$ *zu betrachten.*

Beweis.

Ist $n \in \mathbb{N}$ mit $n \geq 3$, so wird n entweder von 4 oder von $p \in \mathbb{P}\backslash\{2\}$ geteilt. Daher gilt:

$$x^n + y^n = z^n \Leftrightarrow \begin{cases} (x^m)^4 + (y^m)^4 = (z^m)^4 \text{ für } 4|n \\ (x^m)^p + (y^m)^p = (z^m)^p \text{ für } p|n \end{cases}$$

□

weitere Reduktion des Problems

Lemma

Sei $p \in \mathbb{P}$ *ungerade und seien* $a,b,c \in \mathbb{Z}\backslash\{0\}$ *mit* $a^p + b^p = c^p$, *dann existieren* $a',b',c' \in \mathbb{Z}\backslash\{0\}$ *mit* $a'^p + b'^p = c'^p$ *sowie* $\mathrm{ggt}(a',b',c') = 1$ *und* $b \equiv 0 \mod 2$, $a \equiv 3 \mod 4$

Beweis.

Ist $ggt(a,b,c) = h \neq 1$, so können und das teilerfremde Tripel $(a',b',c') = (\frac{a}{h}, \frac{b}{h}, \frac{c}{h})$ betrachten.

Beweis.

Ist $ggt(a,b,c) = h \neq 1$, so können und das teilerfremde Tripel $(a',b',c') = (\frac{a}{h}, \frac{b}{h}, \frac{c}{h})$ betrachten. Ferner können nicht alle drei Zahlen a',b',c' gerade sein.
Betrachte daher die folgenden Fälle:

i) a',b' ungerade und c' gerade

ii) b' gerade und a',c' ungerade

Beweis.

Ist $ggt(a,b,c) = h \neq 1$, so können und das teilerfremde Tripel $(a',b',c') = (\frac{a}{h}, \frac{b}{h}, \frac{c}{h})$ betrachten. Ferner können nicht alle drei Zahlen a',b',c' gerade sein.
Betrachte daher die folgenden Fälle:

i) a',b' ungerade und c' gerade

ii) b' gerade und a',c' ungerade

diese Fälle sind jedoch äquvalent, denn

$$a'^p + b'^p = c'^p \Leftrightarrow b'^p = c'^p - a'^p = c'^p + (-a')^p$$

also ist oBdA $b' \equiv 0 \mod 2$

Beweis.

Ist $ggt(a,b,c) = h \neq 1$, so können und das teilerfremde Tripel $(a',b',c') = (\frac{a}{h}, \frac{b}{h}, \frac{c}{h})$ betrachten. Ferner können nicht alle drei Zahlen a', b', c' gerade sein.
Betrachte daher die folgenden Fälle:

i) a', b' ungerade und c' gerade

ii) b' gerade und a', c' ungerade

diese Fälle sind jedoch äquvalent, denn

$$a'^p + b'^p = c'^p \Leftrightarrow b'^p = c'^p - a'^p = c'^p + (-a')^p$$

also ist oBdA $b' \equiv 0 \mod 2$
Gilt nun $a' \equiv 3 \pmod 4$, so sind wir fertig.

Beweis.

Ist $ggt(a,b,c) = h \neq 1$, so können und das teilerfremde Tripel $(a',b',c') = (\frac{a}{h}, \frac{b}{h}, \frac{c}{h})$ betrachten. Ferner können nicht alle drei Zahlen a', b', c' gerade sein.
Betrachte daher die folgenden Fälle:

i) a', b' ungerade und c' gerade

ii) b' gerade und a', c' ungerade

diese Fälle sind jedoch äquvalent, denn

$$a'^p + b'^p = c'^p \Leftrightarrow b'^p = c'^p - a'^p = c'^p + (-a')^p$$

also ist oBdA $b' \equiv 0 \mod 2$
Gilt nun $a' \equiv 3 \pmod 4$, so sind wir fertig. Anderenfalls gilt $a' \equiv 1 \pmod 4$. Dann betrachte das Tripel $(-a', -b', -c')$, welches natürlich auch eine Lösung ist. Nun gilt aber:
$-b' \equiv 0 \pmod 2$ und $-a' \equiv -1 = 3 \pmod 4$ □

Frey-Kurve

Definition

Sei $p \in \mathbb{P}$ ungerade, dann heißt die elliptische Kurve

$$E_{Frey}: \; y^2 = x(x - a^p)(x + b^p)$$

mit $a, b \in \mathbb{Z}$ teilerfremd und $b \equiv 0 \pmod 2$, $a \equiv 3 \pmod 4$,
***Frey-Kurve**. Ihre Diskriminante ist gegeben duch*

$$\Delta = (a^p(-b^p)(a^p + b^p))^2 \tag{1}$$

Diskriminante von E_{Frey}

Bemerkung

Exististiert eine Lösung von $x^p + y^p = z^p$ über $\mathbb{Z}$, so existiert die Kurve E_{Frey}. In diesem Fall wird (1) zu $\Delta = (abc)^{2p}$. Jedoch muss dieser Ausdruck aus „technischen Gründen“ modifiziert werden, so dass die ***minimale Diskriminante*** *folgende Form erhält*

$$\Delta = 2^{-8}(abc)^{2l}$$

Eigenform

Bemerkung

Sei E eine Elliptische Kurve über einem Körper $\mathbb{K}$ so kann man jede elliptische Kurve durch Variablentransformation auf die Form

$$E: \ y^2 = x^3 + Ax + B \tag{2}$$

bringen. Insbesondere kann jede elliptische Kurve über $\mathbb{Q}$ auf diese Form mit $A, B \in \mathbb{Z}$ gebracht werden.
Ferner muss E glatt sein, d.h. falls E gegeben durch $y^2 = f(x)$ gilt:

$$E \text{ glatt} \ \Leftrightarrow \ \operatorname{disc}(f) \neq 0 \ \Leftrightarrow \ f \text{ hat keine mehrfache Nullstelle}$$

gute und schlechte Reduktion

Definition

Sei $p \in \mathbb{P}$. Wir reduzieren die Gleichung (2) modulo p.

a) *Falls $E \mod p$ eine elliptische Kurve ist, sagt man E hat eine **gute Reduktion** $\mod p$.*

b) *Falls $E \mod p$ eine mehrfache Nullstelle hat, sagt man E hat eine **schlechte Reduktion** $\mod p$.*

gute und schlechte Reduktion

Definition

Sei $p \in \mathbb{P}$. Wir reduzieren die Gleichung (2) modulo p.

a) *Falls $E \mod p$ eine elliptische Kurve ist, sagt man E hat eine **gute Reduktion** $\mod p$.*

b) *Falls $E \mod p$ eine mehrfache Nullstelle hat, sagt man E hat eine **schlechte Reduktion** $\mod p$.*

   i) *Wenn E eine dreifache Nullstelle besitzt, so sagt man E hat eine **additive Reduktion** $\mod p$.*

   ii) *Wenn E eine zweifache Nullstelle besitzt, so sagt man E hat eine **multiplikative Reduktion** $\mod p$.*

gute und schlechte Reduktion

Definition

Sei $p \in \mathbb{P}$. Wir reduzieren die Gleichung (2) modulo p.

a) *Falls $E \mod p$ eine elliptische Kurve ist, sagt man E hat eine* ***gute Reduktion*** $\mod p$.

b) *Falls $E \mod p$ eine mehrfache Nullstelle hat, sagt man E hat eine* ***schlechte Reduktion*** $\mod p$.

   i) *Wenn E eine dreifache Nullstelle besitzt, so sagt man E hat eine* ***additive Reduktion*** $\mod p$.

   ii) *Wenn E eine zweifache Nullstelle besitzt, so sagt man E hat eine* ***multiplikative Reduktion*** $\mod p$.

Im Falle der multiplikativen Reduktion hat E

- ***zerfallende*** *multiplikative Reduktion, wenn die Steigungen der Tangenten an E im singulären Punkt aus $\mathbb{F}_p$ sind*
- *sonst* ***nicht-zerfallende*** *multiplikative Reduktion*

Lemma

Primzahlen mit schlechter Reduktion
Sei E eine elliptische Kurve und Δ die zugehörige Diskriminante, dann gilt:

$$E \text{ hat schlechte Reduktion modulo } p \Rightarrow p|\Delta$$

Lemma

Primzahlen mit schlechter Reduktion
Sei E eine elliptische Kurve und Δ die zugehörige Diskriminante, dann gilt:

$$E \text{ hat schlechte Reduktion modulo } p \;\Rightarrow\; p|\Delta$$

Beweis.

Sei I eine Indexmenge, $\{a_i \mid i \in I\}$ die Menge aller Nullstellen von E und p eine Primzahl mit schlechter Reduktion, d.h. E hat eine mehrfache Nullstelle modulo p, dann gilt:

$$\Delta = \prod_{i<j}(a_i - a_j) \equiv 0 \bmod p$$

also gilt $p|\Delta$ □

notwendiges und hinreichendes Kriterium für schlechte Reduktion

Bemerkung

a) *Für elliptische Kurven der Form* $y^2 = x^3 + Ax + B$ *mit* $A, B \in \mathbb{Z}$ *gibt es meist mehrere mögliche Werte für* A, B *welche die selbe Kurve definieren. Man kann zeigen, dass es immer eine Wahl von* $A, B \in \mathbb{Z}$ *gibt, so dass für alle* $p \in \mathbb{P}$ *die Anzahl der verschiedenen Nullstellen von* $E \bmod p$ *größtmöglich ist. Die Gleichung dieser Wahl nennt man* ***minimale Weierstrassgleichung*** *von* E *und die zugehörige Diskriminante* Δ *heißt* ***Minimaldiskriminante*** *von* E.

b) *Ersetzt man im Lemma die Diskriminante durch die Minimaldiskriminante, so gilt die Äquivalenz.*

Beispiel

Betrachte E gegeben durch

$$y^2 = x^3 - 270000x + 128250000$$

Substitution	*E gegeben durch*	Δ / *Bemerkung*

Beispiel

Betrachte E gegeben durch

$$y^2 = x^3 - 270000x + 128250000$$

Substitution	*E gegeben durch*	Δ / *Bemerkung*
—	$y^2 = x^3 - 270000x + 128250000$	$-2^8 3^{12} 5^{12} 11$

Beispiel

Betrachte E gegeben durch

$$y^2 = x^3 - 270000x + 128250000$$

Substitution	*E gegeben durch*	Δ / *Bemerkung*
—	$y^2 = x^3 - 270000x + 128250000$	$-2^8 3^{12} 5^{12} 11$
$x = 25x_1$ $y = 125y_1$	$y_1^2 = x_1^3 - 432x_1 + 8208$	$-2^8 3^{12} 11$

Beispiel

Betrachte E gegeben durch

$$y^2 = x^3 - 270000x + 128250000$$

Substitution	*E gegeben durch*	Δ / *Bemerkung*
—	$y^2 = x^3 - 270000x + 128250000$	$-2^8 3^{12} 5^{12} 11$
$x = 25x_1$ $y = 125y_1$	$y_1^2 = x_1^3 - 432x_1 + 8208$	$-2^8 3^{12} 11$
$x_1 = 9x_2 - 12$ $y_1 = 27y_2$	$y_2^2 = x_2^3 - 4x_2^2 + 16$	$-2^8 11$

Beispiel

Betrachte E gegeben durch

$$y^2 = x^3 - 270000x + 128250000$$

Substitution	*E gegeben durch*	Δ / *Bemerkung*
—	$y^2 = x^3 - 270000x + 128250000$	$-2^8 3^{12} 5^{12} 11$
$x = 25x_1$ $y = 125y_1$	$y_1^2 = x_1^3 - 432x_1 + 8208$	$-2^8 3^{12} 11$
$x_1 = 9x_2 - 12$ $y_1 = 27y_2$	$y_2^2 = x_2^3 - 4x_2^2 + 16$	$-2^8 11$
$x_2 = 4x_3$ $y_2 = 8y_3 + 4$	$y_3^2 + y_3 = x_3^3 - x_3^2$	*nicht-singulär modulo* 2

semistabile Kurven

Definition

*Eine elliptische Kurve heißt **semistabil**, wenn sie für alle $p \in \mathbb{P}$ eine gute oder multiplikative Reduktion besitzt.*

semistabile Kurven

Definition

*Eine elliptische Kurve heißt **semistabil**, wenn sie für alle $p \in \mathbb{P}$ eine gute oder multiplikative Reduktion besitzt.*

Lemma

Sei $p \in \mathbb{P}$, dann ist E_{Frey} semistabil.

Definition

Sei $p \in \mathbb{P}$, dann definiere

$$a_p = \begin{cases} p+1-\#E(\mathbb{F}_p) & \text{gute Reduktion mod p} \\ 0 & \text{additive Reduktion mod p} \\ 1 & \text{zerfallende mult. Reduktion mod p} \\ -1 & \text{nicht-zerfallende mult. Reduktion mod p} \end{cases}$$

Definition

Sei $p \in \mathbb{P}$, dann definiere

$$a_p = \begin{cases} p+1-\#E(\mathbb{F}_p) & \text{gute Reduktion mod p} \\ 0 & \text{additive Reduktion mod p} \\ 1 & \text{zerfallende mult. Reduktion mod p} \\ -1 & \text{nicht-zerfallende mult. Reduktion mod p} \end{cases}$$

und setze für $n = \prod_j p_j^{n_j}$ PFZ

$$a_n := \prod_j a_{p_j}^{n_j}$$

Definition

Sei $p \in \mathbb{P}$, dann definiere

$$a_p = \begin{cases} p+1-\#E(\mathbb{F}_p) & \text{gute Reduktion mod p} \\ 0 & \text{additive Reduktion mod p} \\ 1 & \text{zerfallende mult. Reduktion mod p} \\ -1 & \text{nicht-zerfallende mult. Reduktion mod p} \end{cases}$$

und setze für $n = \prod_j p_j^{n_j}$ PFZ

$$a_n := \prod_j a_{p_j}^{n_j}$$

sowie für $\tau \in \mathscr{H}$ und $q = \mathrm{e}^{2\pi \mathrm{i} \tau}$

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n$$

Bemerkung

Man beachte:

a) *Die Reihe $f_E(\tau)$ konvergiert und stellt nichts anderes als eine kodierung der Anzahl der Punkte auf E modulo der verschiedenen Primzahlen dar.*

Bemerkung

Man beachte:

a) *Die Reihe $f_E(\tau)$ konvergiert und stellt nichts anderes als eine kodierung der Anzahl der Punkte auf E modulo der verschiedenen Primzahlen dar.*

b) *Die Abbildung*

$$\begin{array}{ccc} \mathbb{N}^+ & \longrightarrow & \mathbb{R} \\ n & \longmapsto & a_n \end{array}$$

ist offensichtlich eine zahlentheoretisch multiplikative Funktion

Galois-Darstellungen

Sei E eine elliptische Kurve über $\mathbb{Q}$, dann gilt

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$$

Galois-Darstellungen

Sei E eine elliptische Kurve über $\mathbb{Q}$, dann gilt

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$$

Sei nun $\{\beta_1, \beta_2\}$ eine Basis von $E[m]$ und sei $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dann ist auch $\sigma\beta_i \in E[m]$ und es gilt

$$\sigma\beta_1 = a\beta_1 + c\beta_2$$
$$\sigma\beta_2 = b\beta_1 + d\beta_2$$

wobei $a, b, c, d \in \mathbb{Z}_m$.

Galois-Darstellungen

Sei E eine elliptische Kurve über $\mathbb{Q}$, dann gilt

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$$

Sei nun $\{\beta_1, \beta_2\}$ eine Basis von $E[m]$ und sei $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dann ist auch $\sigma\beta_i \in E[m]$ und es gilt

$$\sigma\beta_1 = a\beta_1 + c\beta_2$$
$$\sigma\beta_2 = b\beta_1 + d\beta_2$$

wobei $a, b, c, d \in \mathbb{Z}_m$. Somit erhält man den Isomorphismus

$$\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_m) \ : \ \sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Galois-Darstellungen

Sei E eine elliptische Kurve über $\mathbb{Q}$, dann gilt

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$$

Sei nun $\{\beta_1, \beta_2\}$ eine Basis von $E[m]$ und sei $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dann ist auch $\sigma\beta_i \in E[m]$ und es gilt

$$\sigma\beta_1 = a\beta_1 + c\beta_2$$
$$\sigma\beta_2 = b\beta_1 + d\beta_2$$

wobei $a, b, c, d \in \mathbb{Z}_m$. Somit erhält man den Isomorphismus

$$\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_m) \ : \ \sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Definition

Ist $m = p \in \mathbb{P}$, so nennen wir ρ_p die mod p ***Galoisdarstellung*** *von E*

Bemerkung

Die Galoisdarstellungen lässt sich auf $m = p^n$ mit $n \in \mathbb{N}^+$ verallgemeinern, wobei dann $\rho_{p^n} \equiv \rho_{p^{n+1}} \pmod{p^n}$ gilt.

Bemerkung

Die Galoisdarstellungen lässt sich auf $m = p^n$ mit $n \in \mathbb{N}^+$ verallgemeinern, wobei dann $\rho_{p^n} \equiv \rho_{p^{n+1}} \pmod{p^n}$ gilt. Ferner erhält man auf diese Weise auch

$$\rho_{p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_p)$$

wobei $\mathcal{O}_p$ ein Ring ist, der die p-adischen Zahlen enthält und Charakteristik 0 besitzt.

Bemerkung

Die Galoisdarstellungen lässt sich auf $m = p^n$ mit $n \in \mathbb{N}^+$ verallgemeinern, wobei dann $\rho_{p^n} \equiv \rho_{p^{n+1}} \pmod{p^n}$ gilt. Ferner erhält man auf diese Weise auch

$$\rho_{p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathscr{O}_p)$$

wobei $\mathscr{O}_p$ ein Ring ist, der die p-adischen Zahlen enthält und Charakteristik 0 besitzt.

Durch die Betrachtung geeigneter Elemente $\mathrm{Frob_r} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ für eine Primzahl r, deren Anwendung auf $E(\overline{\mathbb{Q}})$ der Anwendung von ϕ_r auf $E(\overline{\mathbb{F}}_r)$ entspricht, erhält man unter gewissen Voraussetzungen für die Darstellung

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathscr{O}_p)$$

dass $a_r = \mathrm{Spur}(\rho(\mathrm{Frob_r}))$. Hierbei erhält man, dass a_r das a_p aus Definition von f_E ist.