Vom Verhältnis von Dreiecken und Zahlen – ein Jahrhundertproblem wird besichtigt

Jürg Kramer
Humboldt-Universität zu Berlin

1. Die Millenniums-probleme

Im Mai 2000 wurden in Paris folgende sieben mathematischen Probleme zu Millenniumsproblemen erklärt, für deren Lösung jeweils eine Million Dollar Preisgeld ausgesetzt ist:

- Die Riemannsche Vermutung
- P versus NP
- Die Poincaré-Vermutung
- Navier-Stokes-Gleichungen
- Die Vermutung von Birch und Swinnerton-Dyer
- Die Hodge-Vermutung
- Yang-Mills-Gleichungen

2. Das Kongruenzzahl-problem

Pythagoreische Tripel

Gesucht: Rechtwinklige Dreiecke mit ganzzahligen Seiten, d.h. $a, b, c \in \mathbb{N}$ mit

$$a^2 + b^2 = c^2 \,.$$

Lösung: Man erhält alle pythagoreischen Tripel wie folgt:

- Wähle beliebige positive ganze Zahlen m, n mit $m > n$.

- Setze:

  $$a = m^2 - n^2, b = 2mn, c = m^2 + n^2 .$$

Kongruenzzahlproblem

Gegeben: Eine positive ganze Zahl F.

Gesucht: Rechtwinklige Dreiecke mit rationalzahligen Seiten und Flächeninhalt F, d.h. $a, b, c \in \mathbb{N}$ mit

$$a^2 + b^2 = c^2 \quad \text{und} \quad \frac{a \cdot b}{2} = F\,.$$

Beispiele

- $F = 6$:

  Wähle z.B. $a = 3, b = 4, c = 5$.

- $F = 5$:

  Diese Lösung werden wir später finden.

- Gibt es für jedes F eine Lösung?

- $F = 2$: Hängt mit dem Fermat-Problem zusammen:
  Falls es eine Lösung gäbe, so fände man positive rationale Zahlen a, b, c mit

$$a^2 + b^2 = c^2 \quad \text{und} \quad b = 4/a\,.$$

  Eingesetzt erhielte man

$$a^2 + \frac{16}{a^2} = c^2\,,$$

  d.h.

$$a^4 + 2^4 = (a \cdot c)^2\,.$$

  Dies ist aber nicht möglich aufgrund der Fermat-Vermutung für den Exponenten 4.

3. Irrationalität von $\sqrt{2}$

Beweis durch Widerspruch

Annahme:

$\sqrt{2} \in \mathbb{Q}$, d.h., $\exists\, x, y \in \mathbb{Z}_{\neq 0} : \sqrt{2} = \frac{x}{y}$.

Leite daraus einen Widerspruch her!

Methoden:

- Eindeutige Primfaktorzerlegung
- Unendlicher Abstieg

Unendliche Abstiegsmethode

$$\sqrt{2} = \frac{x}{y} \Rightarrow x^2 = 2y^2.$$

$$2|2y^2 \Rightarrow 2|x^2 \Rightarrow 2|x \Rightarrow$$
$$\exists x_1 \in \mathbb{Z}_{\neq 0} : x = 2x_1 \Rightarrow$$
$$2x_1^2 = y^2.$$

$$2|2x_1^2 \Rightarrow 2|y^2 \Rightarrow 2|y \Rightarrow$$
$$\exists y_1 \in \mathbb{Z}_{\neq 0} : y = 2y_1 \Rightarrow$$
$$x_1^2 = 2y_1^2.$$

Schlussfolgerung:

$\exists x, y \in \mathbb{Z}_{\neq 0}$:

$x^2 = 2y^2$.

$\Rightarrow$

$\exists x_1, y_1 \in \mathbb{Z}_{\neq 0}; |x_1| < |x|, |y_1| < |y|$:

$x_1^2 = 2y_1^2$.

$\Rightarrow$

$\exists x_2, y_2 \in \mathbb{Z}_{\neq 0}; |x_2| < |x_1|, |y_2| < |y_1|$:

$x_2^2 = 2y_2^2$.

$\Rightarrow$

etc. . . . ad infinitum.

Widerspruch!

4. Das allgemeine Problem

Zwei Fragen

Gegeben

$$P = P(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n].$$

Frage A:

$\exists (x_1, ..., x_n) \in \mathbb{Q}^n : P(x_1, ..., x_n) = 0$?

Falls die Antwort positiv ist

Frage B:

Gibt es *endlich viele* oder *unendlich viele* rationale Lösungen?

- Wir beginnen mit:

  $P = P(X, Y) \in \mathbb{Z}[X, Y]$.

- P definiert eine Kurve C in der affinen (resp. projektiven) X, Y-Ebene.

- Wir definieren:

$$C(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid P(x, y) = 0\} .$$

- Frage A:

$$C(\mathbb{Q}) = \emptyset \quad \text{or} \quad C(\mathbb{Q}) \neq \emptyset \, ?$$

- Frage B:

$$\#C(\mathbb{Q}) < \infty \quad \text{or} \quad \#C(\mathbb{Q}) = \infty \, ?$$

Kurven vom Grad 1

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

$$(a, b, c \in \mathbb{Q};\, a \neq 0)\,.$$

$$C(\mathbb{Q}) = \left\{(x,y) \,\middle|\, x = -\frac{b\lambda + c}{a}, y = \lambda : \lambda \in \mathbb{Q}\right\}\,.$$

$$\Rightarrow \quad \#C(\mathbb{Q}) = \infty\,.$$

Kurven vom Grad 2

Ohne Beschränkung der Allgemeinheit können wir annehmen:

$$P(X,Y) = aX^2 + bY^2 - 1$$

$$(a, b \in \mathbb{Q} : a, b \neq 0).$$

Zu Frage A

Dies kann nicht so einfach erklärt werden (lokal-global Prinzip von Minkowski-Hasse).

Zu Frage B

Annahme: $C(\mathbb{Q}) \neq \emptyset$, d.h., $\exists Q \in C(\mathbb{Q})$.

$$\Rightarrow \quad C(\mathbb{Q}) \cong L(\mathbb{Q}) \,.$$

$$\Rightarrow \quad \#C(\mathbb{Q}) = \infty \,.$$

Kurven vom Grad > 3

Ohne Beschränkung der Allgemeinheit können wir annehmen:

$P = P(X, Y)$ definiert eine glatte (projektive) Kurve C vom Geschlecht > 1.

Theorem (G. Faltings, 1983).

$$\#C(\mathbb{Q}) < \infty.$$

5. Elliptische Kurven

Zu Frage A

Hierzu ist die Antwort schwierig!

Z.B. gibt es kein lokal-global Prinzip.

Zu Frage B

- Sei $O \in C(\mathbb{Q})$; wir wählen O als den "unendlich fernen Punkt".

- Weierstraßsche Normalform:

$$C : Y^2 = X^3 + aX^2 + bX + c$$

$$(a, b, c \in \mathbb{Z}).$$

- Falls C glatt ist, wird C **elliptische Kurve** genannt.

- $C(\mathbb{Q})$ hat die Struktur einer abelschen Gruppe:

- Ist die abelsche Gruppe $C(\mathbb{Q})$ endlich erzeugt?

Definition. Eine abelsche Gruppe G heißt **endlich erzeugt**, wenn Elemente $x_1, \ldots, x_n \in G$ existieren, so dass für alle $x \in G$ gilt

$$x = \sum_{j=1}^{n} c_j \cdot x_j$$

mit Koeffizienten $c_1, ..., c_n \in \mathbb{Z}$.

Beispiele.

- $G = \mathbb{Z}^r = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r-\text{mal}}$

  G heißt **freie abelsche Gruppe vom Rang** r.

- $G =$ endliche abelsche Gruppe

Theorem. Falls G eine endlich erzeugte abelsche Gruppe ist, so haben wir

$$G \cong G_{\text{frei}} \oplus G_{\text{endl.}};$$

wobei

$G_{\text{frei}} =$

freie abelsche Gruppe vom Rang r,

$G_{\text{endl.}} =$

endliche abelsche Gruppe.

Abstiegslemma. Es sei G eine abelsche Gruppe mit $|G/2G| < \infty$. Weiter gebe es eine Funktion $h : G \longrightarrow \mathbb{R}_{\geq 0}$ (Höhenfunktion) mit den Eigenschaften:

(i) für alle $M \in \mathbb{R}_{\geq 0}$ gilt:
$\#\{x \in G \,|\, h(x) \leq M\} < \infty$;

(ii) für jedes $x_0 \in G$ gibt es eine Konstante $c_0 = c(x_0) > 0$:
$h(x + x_0) \leq 2h(x) + c_0$;

(iii) es gibt eine Konstante $c > 0$:
$h(2x) \geq 4h(x) - c$.

Dann ist G endlich erzeugt, d.h. i.e., $G \cong \mathbb{Z}^r \oplus G_{\text{endl.}}$.

Anwendung auf elliptische Kurven

Theorem (Mordell, Weil).

Sei

$$C : Y^2 = X^3 + aX^2 + bX + c$$

eine elliptische Kurve. Dann ist die Gruppe $C(\mathbb{Q})$ der rationalen Punkte C endlich erzeugt, d.h.

$$C(\mathbb{Q}) \cong \mathbb{Z}^{r_C} \oplus C(\mathbb{Q})_{\text{endl.}} .$$

Insbesondere stellen wir fest

$$\#C(\mathbb{Q}) = \infty \Longleftrightarrow r_C > 0 .$$

Beweisskizze:

(1) Man zeige, dass die Faktorgruppe

$$C(\mathbb{Q})/2C(\mathbb{Q})$$

endlich ist.

(2) Man zeige, dass $h : C(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$, gegeben durch

$$(x, y) \mapsto \log\left(\max\left(|N(x)|, |D(x)|\right)\right)$$

($N(x) =$ Zähler von x, $D(x) =$ Nenner von x), eine **Höhenfunktion** definiert, d.h. h erfüllt die Bedingungen (i)–(iii) des Abstieglemmas. □

Zwei Beispiele

(1) $C : Y^2 = X^3 + 4X$,

$C(\mathbb{Q}) = \langle Q \rangle \cong \mathbb{Z}/4\mathbb{Z}$,

$Q = (2, 4)$.

(2) $C : Y^2 = X^3 + X + 1$,

$C(\mathbb{Q}) = \langle Q \rangle \cong \mathbb{Z}$,

$Q = (0, 1)$.

6. Vermutung von Birch und Swinnerton-Dyer

- C elliptische Kurve

- p Primzahl

Definiere:

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

Beobachtung:

$$r_C > 0 \Longleftrightarrow \prod_{\substack{p \text{ prim} \\ p \leq x}} \frac{N_p}{p} \longrightarrow \infty$$

L-Reihe einer elliptischen Kurve C

Mit einer (komplexen) Variablen s setzt man:

$$L_C(s) = \prod_{p \,\text{prim}} \frac{1}{1 - (p + 1 - N_p)p^{-s} + p^{1-2s}}$$

Dieses unendliche Produkt konvergiert für $\text{Re}(s) >> 0$.

Vermutung von Birch und Swinnerton-Dyer

- Die L-Reihe $L_C(s)$ von C lässt sich zu einer holomorphen Funktion auf die ganze komplexe Ebene $\mathbb{C}$ fortsetzen.

- Für die Verschwindungsordnung $\mathrm{ord}_{s=1} L_C(s)$ von $L_C(s)$ an der Stelle $s = 1$ gilt:

$$r_C = \mathrm{ord}_{s=1} L_C(s).$$

Hinweis auf aktuelle Ergebnisse

- J. Coates, A. Wiles (1977):
  $C/\mathbb{Q}$ elliptische Kurve mit komplexer Multiplikation und $L_C(1) \neq 0$
  $\Longrightarrow r_C = 0$.

- B. Gross, D. Zagier (1985)/
  V.A. Kolyvagin (1989):
  $C/\mathbb{Q}$ (modulare) elliptische Kurve mit $L_C(1) = 0$ und $L'_C(1) \neq 0$
  $\Longrightarrow r_C = 1$.

7. Das Kongruenzzahl-problem, revisited

Kongruenzzahlproblem

Gegeben:

$F \in \mathbb{N}_{>0}$

Gesucht:

$a, b, c \in \mathbb{Q} : a^2 + b^2 = c^2, a \cdot b = 2 \cdot F$

Zusammenhang mit elliptischen Kurven

- $C_F : Y^2 = X^3 - F^2 X = X(X-F)(X+F)\,.$

- $\mathcal{P}_F := \{a, b, c \in \mathbb{Q}_{\neq 0} \mid a^2 + b^2 = c^2,\ a \cdot b = 2 \cdot F\}\,.$

- $\varphi : \mathcal{P}_F \longrightarrow \{(x, y) \in C_F(\mathbb{Q}) \mid y \neq 0\}$, gegeben durch $(a, b, c) \mapsto \left(x = -\frac{F \cdot b}{a+c}, y = \frac{2 \cdot F^2}{a+c}\right).$

- φ ist surjektiv: Urbild von (x, y)

$$a = \frac{F^2 - x^2}{y}, b = \frac{2Fx}{y}, c = \frac{F^2 + x^2}{y}\,.$$

Beachte:

$$\{(x,y) \in C_F(\mathbb{Q}) \mid y \neq 0\}$$
$$= C_F(\mathbb{Q}) \setminus C_F(\mathbb{Q})_{\text{endl.}}.$$

Theorem. $\mathcal{P}_F \neq \emptyset \iff r_{C_F} > 0$.

Beispiele

- $F = 1, 2, 3$:

  $r_{C_F} = 0$, i.e., $\mathcal{P}_F = \emptyset$.

- $F = 6$:

  $r_{C_F} = 1$, $(-3, 9) \in C_F(\mathbb{Q}) \backslash C_F(\mathbb{Q})_{\text{endl.}}$,
  $(3, 4, 5) \in \mathcal{P}_F$.

- $F = 5$:

  $r_{C_F} = 1$, $(-5/9, 100/27) \in C_F(\mathbb{Q}) \setminus$
  $C_F(\mathbb{Q})_{\text{endl.}}$, $(20/3, 3/2, 41/6) \in \mathcal{P}_F$.

Aktuelle Ergebnisse

- B. Gross, D. Zagier:

  F Primzahl, $F \equiv 5, 7 \bmod 8$

  $\Rightarrow \mathcal{P}_F \neq \emptyset$.

- Allgemeiner:

  $F \equiv 5, 6, 7 \bmod 8 : L'_{C_F}(1) \neq 0$

  $\Rightarrow \mathcal{P}_F \neq \emptyset$.

- F Primzahl, $F \equiv 3 \bmod 8$

  $\Rightarrow \mathcal{P}_F = \emptyset$.

- Vermutung:

  $F \equiv 1, 2, 3 \bmod 8$

  $\Rightarrow \mathcal{P}_F = \emptyset$.