Die Gleichung $x^2 + y^3 = z^7$

Michael Stoll
International University Bremen

In Zusammenarbeit mit

Bjorn Poonen, UC Berkeley
und
Ed Schaefer, University of Santa Clara

Verallgemeinerung der Fermatschen Gleichung

Wir alle kennen die Fermatsche Gleichung

$$\boxed{x^n + y^n = z^n\,.}$$

Wiles (und viele Andere):
Es gibt keine *nichttrivialen ganzzahligen* Lösungen für $n \geq 3$.

Verallgemeinerte Fermatsche Gleichung:

$$\boxed{x^p + y^q = z^r}$$

Hier sind p, q und r ganze Zahlen ≥ 2.

Viele ganzzahlige Lösungen, zum Beispiel

$$(a^{11}\,b^7\,c^3)^2 + (a^7\,b^5\,c^2)^3 = (a^3\,b^2\,c)^7$$

sobald $a + b = c$ ist.
Deshalb: Suche nach *primitiven* Lösungen, d.h. Lösungen in *teilerfremden* ganzen Zahlen.

Eine „Lösung“ sei hier stets
eine primitive nichttriviale ganzzahlige Lösung.

Allgemeine Theorie

Sei $$\boxed{\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1\,.}$$

Die Gestalt der Lösungsmenge hängt vom Vorzeichen von χ ab.

Satz (Beukers, Darmon-Granville)**:**

(1) $\chi > 0 \Rightarrow$ unendlich viele primitive Lösungen in endlich vielen polynomialen Familien.

(2) $\chi = 0 \Rightarrow$ einzige nichttriviale primitive Lösung ist $2^3 + 1^6 = 3^2$.

(3) $\chi < 0 \Rightarrow$ nur endlich viele primitive Lösungen.

Der Prototyp für Fall (1) ist die bekannte Parametrisierung der Pythagoreischen Tripel.

Fall (2): Nur endlich viele Tripel (p, q, r).

Fall (3): Lösungen sind parametrisiert durch rationale Punkte auf endlich vielen *Twists* einer Kurve vom Geschlecht ≥ 2.
Jeder Twist hat nur endlich viele rationale Punkte.

Lösungen

Im uns interessierenden Fall $\chi < 0$
hat man folgende Lösungen gefunden:

- $$2^3 + 1^r = 3^2\,, \qquad r \geq 7$$
  $$7^2 + 2^5 = 3^4$$
  $$13^2 + 7^3 = 2^9$$
- $$17^3 + 2^7 = 71^2$$
  $$11^4 + 3^5 = 122^2$$
  $$1\,549\,034^2 + 33^8 = 15\,613^3$$
- $$2\,213\,459^2 + 1\,414^3 = 65^7$$
- $$15\,312\,283^2 + 9\,262^3 = 113^7$$
- $$76\,271^3 + 17^7 = 21\,063\,928^2$$
  $$96\,222^3 + 43^8 = 30\,042\,907^2$$

Mit Ausnahme der ersten Lösung fällt auf,
dass als Exponententripel nur Permutationen von
$(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$ auftreten.

Sie tragen jeweils 4, 2, 2 und 1 Lösung(en) bei
und entsprechen den vier größten negativen
Werten von χ:
$-\dfrac{1}{42}$, $-\dfrac{1}{24}$, $-\dfrac{1}{20}$ und $-\dfrac{1}{18}$.

Vermutungen

Das gibt Anlass zu verschiedenen Vermutungen.

Vermutung 1:
Es gibt insgesamt für $\chi < 0$
nur endlich viele Lösungen.

Das würde aus der ABC-Vermutung folgen.

Vermutung 2:
Es gibt keine Lösungen für $p, q, r \geq 3$.

Ein amerikanischer Ingenieur namens Beal hat für einen Beweis oder Gegenbeispiel einen Geldpreis von 100 000 $ ausgesetzt.
Die Vermutung wurde allerdings schon früher von Tijdeman und Zagier geäußert.

Vermutung 3:
Es gibt keine Lösungen für andere Exponententripel als die vier angegebenen.

Vermutung 4:
Die Liste enthält bereits alle Lösungen.

Sätze (für $\chi < 0$)

Satz (Wiles etc.)**:**
Es gibt keine Lösungen
für $(p, q, r) = (n, n, n)$ mit $n \geq 4$.

Satz (Darmon-Merel, Poonen)**:**
Es gibt keine Lösungen
für $(p, q, r) = (n, n, 2)$ mit $n \geq 5$ und
für $(p, q, r) = (n, n, 3)$ mit $n \geq 4$.

Satz (Kraus)**:**
Es gibt keine Lösungen
für $(p, q, r) = (3, 3, n)$ mit $17 \leq n \leq 10000$, n prim.

Satz (Ellenberg)**:**
Es gibt keine Lösungen
für $(p, q, r) = (2, 4, n)$ mit $n \geq 211$, n prim.

Satz (Bruin)**:**
Es gibt keine Lösungen für Permutationen von
$(2, 4, 6)$, $(3, 3, 4)$ und $(3, 3, 5)$.

Satz (Bruin)**:**
Die Liste enthält alle Lösungen für
Permutationen von $(2, 3, 8)$, $(2, 4, 5)$ und $(2, 3, 9)$.

Unser Spezialfall

Unser Spezialfall $(p, q, r) = (2, 3, 7)$ ist interessant:

- Er ist *extremal*:
  χ hat den größten negativen Wert.

- Die Exponenten sind verschiedene Primzahlen, so dass sich bekannte Methoden/Ergebnisse nicht unmittelbar anwenden lassen.

- Er trägt (vermutlich) die meisten Lösungen für $\chi < 0$ bei.

- Er ist der letzte Fall, für den interessante Lösungen bekannt sind, aber nicht, ob die Liste komplett ist.

Außerdem ist es eine reizvolle Aufgabe,
die endlich vielen Lösungen einer Gleichung explizit zu bestimmen,
besonders dann, wenn sie nicht offensichtlich sind.
(Und sich andere daran schon die Zähne ausgebissen haben. . .)

Endlich viele Twists

In unserem Fall gibt es endlich viele Twists der *Kleinschen Quartik*

$$\boxed{x^3y + y^3z + z^3x = 0},$$

deren rationale Punkte unsere Lösungen parametrisieren.

Ein *Twist* ist hier eine glatte ebene Kurve,
die durch ein Polynom vom Grad 4
mit rationalen Koeffizienten beschrieben wird,
so dass es eine lineare Transformation
mit i. a. irrationalen Koeffizienten gibt,
die beide Gleichungen ineinander überführt.

Ein einfaches Beispiel ist $x^3y + 2\,y^3z + 3\,z^3x = 0$.

Invariantentheorie liefert Formeln,
die einem rationalen Punkt
auf einem Twist der Kleinschen Quartik eine
(nicht notwendig primitive oder nichttriviale)
Lösung von $x^2 + y^3 = z^7$ zuordnen.

Problem: Finde die relevanten Twists!

Elliptische Kurven, Frey, Ribet, Wiles und Co.

Wir ordnen einer Lösung $a^2 + b^3 = c^7$
eine elliptische Kurve zu:

$$\boxed{E : y^2 = x^3 + 3\lambda^2 b\, x - 2\lambda^3 a}$$

wobei $\lambda \in \{\pm 1, \pm 3\}$ geeignet zu wählen ist.

Die 7-Torsionsuntergruppe $E[7]$ liefert dann eine Darstellung der absoluten Galoisgruppe von $\mathbb{Q}$, die kleinen „Führer“ hat: Er teilt $2^6 \cdot 3^3$.
Wir nehmen an, diese Darstellung sei *irreduzibel*.

Nach Wiles und Breuil, Conrad, Diamond und Taylor ist E und damit $E[7]$ „modular“.

Nach Ribet folgt (im konkreten Fall), dass $E[7]$ bis auf qudratischen Twist isomorph ist zu $E'[7]$ für eine elliptische Kurve E' aus einer expliziten Liste von 13 Kurven.

Nach Halberstadt und Kraus werden für gegebenes E' die Kurven E durch zwei explizit hinschreibbare Twists der Kleinschen Quartik parametrisiert.

Die 10 Kurven

Diese Überlegungen, zusammen mit einer Sonderbetrachtung des reduziblen Falls, führen zu einer endlichen Liste von Twists.

Viele davon lassen sich durch Kongruenzbetrachtungen eliminieren.

Es bleiben die folgenden 10 Kurven übrig.

$$C_1 : 6x^3y + y^3z + z^3x = 0$$

$$C_2 : 3x^3y + y^3z + 2z^3x = 0$$

$$C_3 : 3x^3y + 2y^3z + z^3x = 0$$

$$C_4 : 7x^3z + 3x^2y^2 - 3xyz^2 + y^3z - z^4 = 0$$

$$\begin{aligned} C_5 : -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 \\ - xz^3 + 3y^3z - yz^3 = 0 \end{aligned}$$

$$\begin{aligned} C_6 : x^4 + 2x^3y + 3x^2y^2 + 2xy^3 \\ + 18xyz^2 + 9y^2z^2 - 9z^4 = 0 \end{aligned}$$

$$\begin{aligned} C_7 : -3x^4 - 6x^3z + 6x^2y^2 - 6x^2yz + 15x^2z^2 - 4xy^3 \\ - 6xyz^2 - 4xz^3 + 6y^2z^2 - 6yz^3 = 0 \end{aligned}$$

$$\begin{aligned} C_8 : 2x^4 - x^3y - 12x^2y^2 + 3x^2z^2 - 5xy^3 - 6xy^2z \\ + 2xz^3 - 2y^4 + 6y^3z + 3y^2z^2 + 2yz^3 = 0 \end{aligned}$$

$$\begin{aligned} C_9 : 2x^4 + 4x^3y - 4x^3z - 3x^2y^2 - 6x^2yz + 6x^2z^2 \\ - xy^3 - 6xyz^2 - 2y^4 + 2y^3z - 3y^2z^2 + 6yz^3 = 0 \end{aligned}$$

$$\begin{aligned} C_{10} : x^3y - x^3z + 3x^2z^2 + 3xy^2z + 3xyz^2 + 3xz^3 - y^4 \\ + y^3z + 3y^2z^2 - 12yz^3 + 3z^4 = 0 \end{aligned}$$

Die Punkte

Auf diesen Kurven finden wir die folgenden rationalen Punkte.

C_1 : $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:-1:2)$

C_2 : $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:-1)$, $(1:-2:-1)$

C_3 : $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:-1)$

C_4 : $(1:0:0)$, $(0:1:0)$, $(0:1:1)$

C_5 : $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:1)$

C_6 : $(0:1:0)$, $(1:-1:0)$, $\boxed{(0:1:1)}$, $\boxed{(0:1:-1)}$

C_7 : $(0:1:0)$, $\boxed{(0:0:1)}$, $\boxed{(0:1:1)}$

C_8 : $\boxed{(0:0:1)}$, $(2:-1:0)$

C_9 : $(0:0:1)$, $(1:1:0)$

C_{10} : $\boxed{(1:0:0)}$, $(1:1:0)$

Die eingerahmten Punkte ergeben Lösungen unserer Gleichung; sie sind alle schon bekannt.

Es bleibt zu zeigen, dass es keine weiteren rationalen Punkte auf den Kurven gibt,
oder jedenfalls keine,
die zu weiteren Lösungen führen könnten.

Rationale Punkte mit Chabauty

Zur Bestimmung der rationalen Punkte
gibt es eine gute Methode.

Sei C eine algebraische Kurve
vom Geschlecht $g \geq 2$.
Zu C gehört eine abelsche Varietät J,
die *Jacobische Varietät* von C;
ihre rationalen Punkte bilden
eine endlich erzeugte abelsche Gruppe.
Der Rang r dieser Gruppe heißt
Mordell-Weil-Rang von J oder C.

Ist $r < g$, dann liefert die Methode von Chabauty
eine obere Schranke für die Anzahl der Punkte,
die oft scharf ist.

Gut verstanden ist der Fall $g = 2$,
und allgemeiner, wenn C hyperelliptisch ist.

Abstieg für Twists der Kleinschen Quartik

Unsere Kurven haben jedoch $g = 3$
und sind nicht hyperelliptisch.

Um die Chabauty-Methode anzuwenden, braucht man Informationen über die Mordell-Weil-Gruppe. Diese sind für allgemeine Kurven vom Geschlecht 3 sehr schwierig zu bekommen.

Unsere Twists sind aber sehr speziell
und verhalten sich fast
wie hyperelliptische Kurven.

Wir haben deshalb den „2-Abstieg“,
mit dem man den Rang r
nach oben abzuschätzen kann,
auf diesen Typ von Kurven verallgemeinert.

Die Hoffnung ist nun,
dass dieser Rang jeweils höchstens 2 ist,
damit sich Chabauty anwenden lässt.

Rangberechnungen

Wir haben für alle Kurven in unserer Liste den Rang bestimmt.

Für alle Kurven *mit Ausnahme von* C_5 ist der Rang höchstens 2.

Auf diese neun Kurven haben wir die Chabauty-Methode angewandt und bewiesen, dass sie keine weiteren Lösungen liefern.

Für C_5 ist der Rang 3;
die Gruppe $J_5(\mathbb{Q})$ hat die Form $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

Hier kommt uns zu Hilfe, dass wir keine primitiven Lösungen von dieser Kurve erwarten.

Jeder rationale Punkt auf C_5,
der eine primitive Lösung liefern würde,
ergäbe ein Element $(n_1, n_2, n_3) \in \mathbb{Z}^3 \cong J_5(\mathbb{Q})$.
Betrachtung modulo p für $p = 2, 3, 13, 23, 97$
liefert Kongruenzen mod 14 für n_1, n_2, n_3,
die schließlich zu einem Widerspruch führen.

Damit ist gezeigt, dass die Liste der bekannten Lösungen vollständig ist.

Rück- und Ausblick

Das Ergebnis an sich mag vielleicht
nicht so sehr interessant sein.

Worum es mir hierbei geht, ist zu demonstrieren,
dass wir heute in der Lage sind,
solche Probleme erfolgreich zu lösen.

Bei der Lösung war es nötig, sowohl
neuere theoretische Ergebnisse (Ribet, Wiles)
zu verwenden,
als auch eher praktisch orientierte Fortschritte
auf der algorithmischen Seite zu machen.

Dass auch einiges an Computer-Schweiß
geflossen ist, soll nicht unerwähnt bleiben.

Ein Projekt für die Zukunft ist, mit ähnlichen
Methoden alle Gleichungen $x^2 + y^3 = z^p$
(mit $p \geq 7$ prim) zu behandeln.

Vielleicht können wir dann sogar zeigen,
dass die Liste aller bekannten Lösungen von
$x^2 + y^3 = \pm z^n$ $(n \geq 6)$ vollständig ist.