Florian Kaufhold

Die Beiträge von Levi ben Gershon und Victor A. Lebesgue zur Catalanschen Vermutung

Catalansche Vermutung. *Für die Gleichung*

$$x^p - y^q = 1 \text{ mit } p, q \in \mathbb{N},\ p, q \geq 2,\ x, y \in \mathbb{Z} \setminus \{0\}$$

existieren nur die Lösungen $p = 2,\ q = 3,\ x = \pm 3,\ y = 2.$

Vortrag im Rahmen des Seminars
der WE AℓZAGK im Wintersemester 2008/2009
an der Universität Bremen

1 Einführung

Im Jahre 1844 wandte sich Eugène Charles Catalan hilfesuchend an die mathematische Öffentlichkeit: Er habe die Vermutung, dass 8 und 9 die einzigen beiden echten Potenzen ganzer Zahlen sind, die die Differenz 1 haben, könne dies aber nicht beweisen. Seine Kollegen konnten ihm beim Beweis zunächst auch nicht weiterhelfen. Der vollständige Beweis ließ 160 Jahre auf sich warten und wurde erst 2002 von Preda Mihăilescu geführt.
In dieser Ausarbeitung sollen zwei Spezialfälle der Catalanschen Vermutung vorgestellt werden: Ein Resultat des jüdischen Mathematikers und Philosophen Levi ben Gershon (1288–1344) aus dem Jahre 1343 und eines von Victor A. Lebesgue (1791–1875) aus dem Jahre 1850. Das frühe Resultat von Levi ben Gershon spielt für den Beweis von Mihăilescu keine Rolle, mag aber möglicherweise Catalan zu seiner Vermutung inspiriert haben. Der von Lebesgue betrachtete Spezialfall wird von Mihăilescus Beweis hingegen nicht abgedeckt. Der Beweis dieses Spezialfalls ist also für den Gesamtbeweis der Catalanschen Vermutung von Bedeutung.

2 Levi ben Gershon: $2^k3^l - 2^m3^n = 1$

Bereits 500 Jahre bevor Catalan seine Behauptung aufstellte, beschäftigte sich Levi ben Gershon mit dem Spezialfall der Potenzen von 2 und 3. Aus einem musikalischen Kontext heraus entstand die Frage, ob es außer den Paaren

$$(1,2) \quad (2,3) \quad (3,4) \quad (8,9)$$

noch weitere harmonische Zahlen, das sind Zahlen der Form 2^m3^n, mit Differenz 1 gibt. Levi ben Gershon zeigte, dass die oben angegebenen Paare die einzig möglichen sind. Um dies einzusehen, stellt man zunächst fest, dass lediglich die Paare harmonischer Zahlen in Frage kommen, bei denen die eine eine Potenz von 2 und die andere eine Potenz von 3 ist. Taucht der Faktor 2 (3) in beiden harmonischen Zahlen auf, dann wäre die Differenz mindestens 2 (3) oder 0, wie einfaches Ausklammern zeigt. Levi ben Gershon untersuchte nun, wie sich die Potenzen von 2 und 3 bei Teilung durch 8 verhalten. Er stieß auf die folgenden Teilbarkeitsbeziehungen:

$$3^m \equiv 1 \mod 8 \quad \Leftrightarrow \; m \text{ gerade},$$

$$3^m \equiv 3 \mod 8 \quad \Leftrightarrow \; m \text{ ungerade},$$

$$2^n \equiv 0 \mod 8 \quad \text{für } 3 \leq n.$$

Wir unterscheiden nun die Fälle:

1. Gilt $3^m+1 = 2^n$, sind lediglich die beiden Paare $(1,2)$ und $(3,4)$ möglich. Für $n \geq 3$ hätte man nämlich $2^n \equiv 0 \mod 8$, es gibt aber keine Potenzen von 3 mit Rest 7 mod 8.

2. Ist $2^n + 1 = 3^m$ und $3^m \equiv 3 \mod 8$, bleibt nur die Lösung $(2,3)$, da nur $2^1 \equiv 2 \mod 8$.

3. Im Fall $2^n+1 = 3^m$ und $3^m \equiv 1 \mod 8$ muss m gerade sein. Für $m = 2k$ ergibt sich

$$(3^{2k} - 1) = (3^k - 1)(3^k + 1) = 2^n$$

Das Produkt zweier Zahlen mit Differenz 2 müsste also eine Potenz von 2 sein. Dies ist nur für 2 und 4 möglich. Wir erhalten also die Lösung $(8, 9)$. Dies ist auch die einzige Lösung, die in Catalans Gleichung zugelassen ist, da in den anderen Fällen Potenzen kleiner 2 auftreten. □

3 Victor A. Lebesgue: $x^p = y^2 + 1$

Bereits 6 Jahre nachdem Catalan seine Vermutung äußerte, gelang es Victor A. Lebesgue, sie für den Spezialfall $q = 2$ zu verifizieren.

Satz 1 (V.A. Lebesgue (1850))**.** *Für jedes $p \geq 2$ hat die Gleichung*

$$x^p = y^2 + 1$$

keine ganzzahlige Lösung außer den trivialen $y = 0$ und $x = 1$ für ungerades p bzw. $y = 0$ und $x = \pm 1$ für gerades p.

Für eine nichttriviale Lösung ergibt sich zunächst:

p ist ungerade.

Beweis:

Für gerades p hätte man nämlich:

$$(x^{\frac{p}{2}} - y)(x^{\frac{p}{2}} + y) = 1$$

und damit

$$(x^{\frac{p}{2}} - y) = (x^{\frac{p}{2}} + y) = \pm 1.$$

Subtraktion liefert aber $y = 0$. Wir erhalten also den bekannten trivialen Fall. □

$\boxed{y \text{ ist gerade.}}$

Beweis:

Wir nehmen an, y wäre ungerade, also $y^2 \equiv 1 \mod 4$. Für x ergäbe sich dann

$$x^p \equiv 2 \mod 4.$$

Für ungerades x wäre x^p aber ebenfalls ungerade. Für gerades x wäre x^p hingegen durch 4 teilbar. Die Annahme, dass y ungerade ist, muss also falsch sein.

□

Wir rechnen nun in den Gaußschen Zahlen $\mathbb{Z}[i]$. Dabei ist

$$\mathbb{Z}[i] = \{u + i\,v \mid u, v \in \mathbb{Z}\}.$$

Die Addition und die Multiplikation sind wie in den komplexen Zahlen definiert. Mit diesen Verknüpfungen ist $\mathbb{Z}[i]$ ein Hauptidealring. In $\mathbb{Z}[i]$ ergibt sich $x^p = y^2 + 1 = (1 + i\,y)\,(1 - i\,y)$. Mit geradem y gilt:

$\boxed{1 + i\,y \text{ und } 1 - i\,y \text{ sind teilerfremd in } \mathbb{Z}[i].}$

Beweis:

Wir nehmen an, $z \in \mathbb{Z}[i]$ ist Teiler von $1 + i\,y$ und $1 - i\,y$. Dann teilt z auch 2 und, da y gerade ist, auch $i\,y$. Man hat also $z|i\,y$ und $z|1 + i\,y$. Daraus ergibt sich aber $z|1$. Ein Teiler von $1 + i\,y$ und $1 - i\,y$ ist also eine Einheit in $\mathbb{Z}[i]$.

□

Damit lässt sich nun zeigen, dass $1 + i\,y$ in $\mathbb{Z}[i]$ eine p-te Potenz ist. Es gilt also:

$\boxed{1 + i\,y = a^p \text{ für ein } a \in \mathbb{Z}[i].}$

Beweis:

Da $\mathbb{Z}[i]$ ein Hauptidealring ist, existiert die Primfaktorzerlegung. Sei

$$1 + i\,y = \varepsilon_a \prod a_j,\ 1 - i\,y = \varepsilon_b \prod b_j,\ x = \varepsilon_x \prod x_j$$

mit Einheiten $\varepsilon_a, \varepsilon_b, \varepsilon_x$. Aus $x^p = y^2 + 1 = (1 + i\,y)(1 - i\,y)$ wird also

$$\varepsilon_a \prod a_j \varepsilon_b \prod b_j = \left(\varepsilon_x \prod x_j\right)^p = \varepsilon_x^p \prod x_j^p.$$

Da $1 + i\,y$ und $1 - i\,y$ teilerfremd sind, können wir die Teiler von x disjunkt in Teiler von $1 + i\,y$ und $1 - i\,y$ sortieren. Wir nehmen an, dass $x_1, ..., x_l$ die Teiler von $1 + i\,y$ sind. Jedes x_i taucht offenbar p-mal in der Primfaktorzerlegung auf. Betrachten wir nun die Einheit ε_a. Da p ungerade ist, lässt sich jede der vier Einheiten von $\mathbb{Z}[i]$ als p-te Potenz darstellen, denn

$$1 = 1^p, \qquad -1 = (-1)^p,$$

$$i = i^p \text{ für } p \equiv 1 \mod 4 \quad \text{und} \quad i = (-i)^p \text{ für } p \equiv 3 \mod 4$$

$$-i = (-i)^p \text{ für } p \equiv 1 \mod 4 \quad \text{und} \quad -i = i^p \text{ für } p \equiv 3 \mod 4$$

Es gibt also eine Einheit ε mit $\varepsilon^p = \varepsilon_a$. Wir setzen

$$a = \varepsilon \prod_{j=1}^{l} x_j.$$

□

Für ein a mit $a^p = 1 + i\,y$ gilt nun:

a hat ungeraden Realteil und geraden Imaginärteil.

Beweis:

Wir bemerken zunächst, dass der Realteil von a^p ungerade und der Imaginärteil

gerade ist. Daraus lässt sich schließen, dass auch a diese Struktur haben muss. Zur Abkürzung sagen wir zu einer Gaußschen Zahl $q + i\,r$, sie ist vom Typ

$$(q \mod 2, r \mod 2).$$

Die obige Behauptung lautet dann gerade, dass a^p vom Typ $(1,0)$ a vom Typ $(1,0)$ impliziert, sofern p ungerade ist. Man beachte dazu die Multiplikationsregeln in $\mathbb{Z}[i]$:

$$(q + i\,r)(s + i\,t) = qs - rt + i\,(qt + rs),\ (q + i\,r)^2 = q^2 - r^2 + i\,(2qr).$$

Der Typ $(1,0)$ ist offenbar multiplikativ abgeschlossen. Wir betrachten nun die anderen Fälle.

- Wäre a vom Typ $(0,0)$, so auch alle Potenzen von a. Außerdem ist das Produkt einer beliebigen Gaußschen Zahl mit einer Zahl von diesem Typ wieder von diesem Typ.
- Wäre a vom Typ $(1,1)$, dann wäre a^2 vom Typ $(0,0)$. Wegen obiger Überlegung sind dann alle weiteren Potenzen von a vom Typ $(0,0)$.
- Wäre a vom Typ $(0,1)$, wäre a^2 und damit alle geraden Potenzen von a vom Typ $(1,0)$. Wir interessieren uns aber lediglich für die ungeraden Potenzen. Da das Produkt einer Zahl vom Typ $(0,1)$ und einer vom Typ $(1,0)$ vom Typ $(0,1)$ ist, können wir auch diesen Fall ausschließen.

a ist also tatsächlich vom Typ $(1,0)$.

□

Es gilt nun weiterhin:

$\boxed{a = 1 + i\,u \text{ für ein } u \in 2\mathbb{Z}.}$

Beweis:

Da $a^p = 1 + i\,y$ ist, gilt

$$2 = a^p + \overline{a}^p = (a + \overline{a}) \left(\sum_{j=1}^{p} (-1)^{j+1} a^{p-j} \overline{a}^{j-1} \right).$$

Offenbar ist jeder der Summanden im rechten Faktor vom Typ $(1, 0)$. Da es sich um eine ungerade Anzahl von Summanden handelt, ist auch die Summe von diesem Typ. Das bedeutet aber, dass 2 diesen Faktor nicht teilt. Wir erhalten:

$$a + \overline{a} = \pm 2, \text{ also } a = \pm(1 + i\,u) \text{ für ein } u \in 2\mathbb{Z}.$$

Für $a = -(1 + i\,u)$ ergäbe sich aber aus $a^p + \overline{a}^p = 2$:

$$\sum_{j=1}^{l} \binom{p}{2j} (iu)^{2j} = -2 \text{ mit } p = 2l + 1.$$

In jedem Summanden auf der linken Seite taucht der Faktor 2 mindestens quadratisch auf. Die Gleichung kann also unmöglich erfüllt sein. Es bleibt lediglich die Möglichkeit $a = 1 + i\,u$.

□

Im letzten Schritt zeigen wir nun, dass auch dieser Fall wieder auf die bereits bekannte triviale Lösung $y = 0$ für das Ausgangsproblem führt. Es gilt nämlich:

$\boxed{u = 0.}$

Beweis:

Um $u \neq 0$ auszuschließen, setzen wir wie oben $a = 1 + i\,u$ in die Gleichung $a^p + \overline{a}^p = 2$ ein und erhalten:

$$\sum_{j=1}^{l} \binom{p}{2j} (i\,u)^{2j} = 0 \text{ mit } p = 2l + 1.$$

Wenn wir nun $u \neq 0$ annehmen, können wir die Gleichung durch $(i\,u)^2$ dividieren und erhalten:

$$\sum_{j=1}^{l} \binom{p}{2j} (i\,u)^{2j-2} = 0.$$

Diese Gleichung kann aber unmöglich erfüllt sein, was allerdings etwas schwieriger einzusehen ist. Die Tatsache basiert auf folgender Ungleichung:

$$\operatorname{ord}_2\left(\binom{p}{2}\right) < \operatorname{ord}_2\left(\binom{p}{k}u^{k-2}\right) \text{ für } k \geq 4 \text{ gerade, } u \in 2\mathbb{Z} \setminus \{0\},\ p \geq 3.$$

Dies bedeutet, dass 2 in der Primfaktorzerlegung von jedem Summanden ab dem zweiten häufiger vorkommt als in der Primfaktorzerlegung des ersten Summanden. Die Summe kann also nicht Null ergeben. Um die Ungleichung zu verifizieren, betrachten wir für $p \geq 3$ die Identität

$$\binom{p}{k}(i\,u)^{k-2} = \binom{p}{2}\binom{p-2}{k-2}\frac{2(i\,u)^{k-2}}{k(k-1)}.$$

Für gerades u und gerades k gilt

$$\operatorname{ord}_2\left(2u^{k-2}\right) \geq k-1 > \log_2(k) \geq \operatorname{ord}_2(k) = \operatorname{ord}_2(k(k-1)),$$

also

$$\operatorname{ord}_2\left(\binom{p}{k}u^{k-2}\right) \geq \operatorname{ord}_2\left(\binom{p}{2}\right) + \operatorname{ord}_2\left(\frac{2u^{k-2}}{k(k-1)}\right) > \operatorname{ord}_2\left(\binom{p}{2}\right).$$

Die Annahme $u \neq 0$ führt daher zu einem Widerspruch.

□

Für $u = 0$ hat man aber $a = 1$ und somit $1 + i\,y = 1$, also $y = 0$. Damit ist der Satz von V. A. Lebesgue bewiesen. Die Gleichung $x^p = y^2 + 1$ hat nur die trivialen ganzzahligen Lösungen.

Literatur

[1] René Schoof. *Catalan's Conjecture.* Springer, Berlin, 2008.

[2] Shai Simonson. *The Mathematics of Levi ben Gershon, the Ralbag.* Dpt. of Math and Comp. Sc., Stonehill College, North Easton, MA, 2000.