UNIVERSITÄT
BAYREUTH

Harmlose Gleichungen — Schwierige Lösung

Michael Stoll
Universität Bayreuth

STAUNT! — Rostock, 10. September 2008

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

„Hilberts Zehntes Problem“:

Satz (Davis, Putnam, Robinson 1961; Matiyasevich 1970)

Die Existenz von ganzzahligen Lösungen einer Polynomgleichung

$$F(x_1, \ldots, x_n) = 0$$

ist unentscheidbar.

Für Gleichungen in zwei Variablen könnte es aber besser aussehen!

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

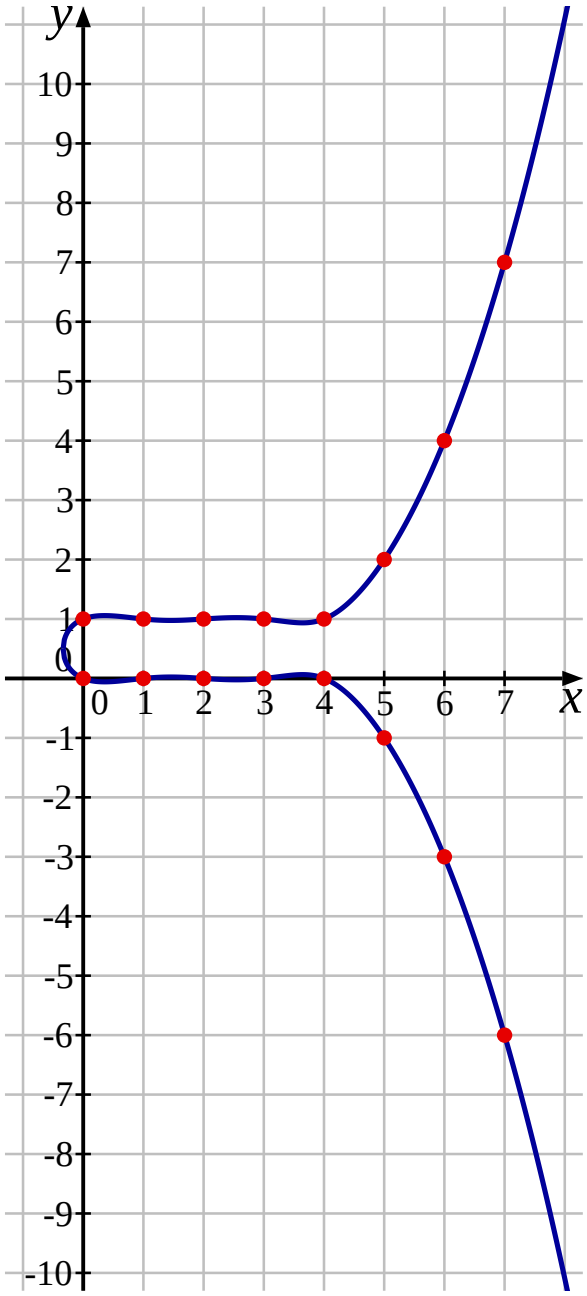
Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$\Longrightarrow$ $|x| < 10^{10^{10^{10^{600}}}}$ für Lösungen (x, y) unserer Gleichung.

Viele Verbesserungen bis heute

$\Longrightarrow$ $|x| < 10^{10^{600}}$ für Lösungen (x, y) unserer Gleichung.



Etwas Geometrie

Unsere Gleichung beschreibt
eine ebene algebraische Kurve C;
wir wollen die Menge $C(\mathbb{Z})$
der ganzzahligen Punkte bestimmen.

Wir können C in eine abelsche Fläche J
einbetten.

Satz (Weil 1928)
$J(\mathbb{Z}) = J(\mathbb{Q})$ ist eine
endlich erzeugte abelsche Gruppe.

Hier:
$J(\mathbb{Z}) \cong \mathbb{Z}^6$ kann explizit bestimmt werden.

Die Höhe

Wir haben also eine Einbettung

$$\alpha : C(\mathbb{Z}) \longrightarrow J(\mathbb{Z}) = G \cong \mathbb{Z}^6 \,.$$

Es gibt eine positive definite quadratische Form („kanonische Höhe“)

$$\widehat{h} : G \longrightarrow \mathbb{R}_{\geq 0} \,,$$

so dass

$$\widehat{h}\Big(\alpha(x,y)\Big) \approx \log |x| \,.$$

Damit verkleinert sich unser Suchraum von $10^{10^{600}}$ auf 10^{1800} !

Mehr Information

Um die sehr „dünne“ Menge $\alpha\Big(C(\mathbb{Z})\Big) \subset G$ zu finden,
sieben wir aus, indem wir notwendige Bedingungen verwenden:

Sei p eine Primzahl.
Dann haben wir folgendes kommutative Diagramm:

$$\begin{array}{ccc} C(\mathbb{Z}) & \xrightarrow{\ \alpha\ } & G \\ \Big\downarrow{\scriptstyle r_p} & & \Big\downarrow{\scriptstyle r_p} \\ C(\mathbb{F}_p) & \xrightarrow{\ \alpha_p\ } & J(\mathbb{F}_p) \end{array}$$

Wir erhalten $\alpha\Big(C(\mathbb{Z})\Big) \subset r_p^{-1}\Big(\alpha_p\Big(C(\mathbb{F}_p)\Big)\Big) = W_p + \Lambda_p$

mit $\Lambda_p = \ker\Big(G \xrightarrow{r_p} J(\mathbb{F}_p)\Big)$.

Beachte: $\#W_p \leq \#C(\mathbb{F}_p) \approx p\,,$ $\Big(G : \Lambda_p\Big) \leq \#J(\mathbb{F}_p) \approx p^2\,.$

Viele Primzahlen

Sei S eine endliche Menge von Primzahlen,
so dass jede Nebenklasse von

$$\Lambda = \bigcap_{p \in S} \Lambda_p$$

die „Kugel“ $B = \{g \in G : \hat{h}(g) < 10^{600}\}$
in höchstens einem Punkt trifft.

Sei $\bigcap_{p \in S}(W_p + \Lambda_p) = W + \Lambda$.

Dann haben wir

$$\alpha\Big(C(\mathbb{Z})\Big) \subset (W + \Lambda) \cap B \subset W$$

Wenn $W = \alpha\Big(C(\mathbb{Z})_{\text{bekannt}}\Big)$, dann sind wir fertig.

Die Rechnung

- Spezielle Behandlung kleiner Primzahlen,
  sorgfältige Wahl von S
- Wichtig: effiziente Implementierung
  (kombinatorische Explosion!)
- Rechnung braucht mehrere Stunden
  und mehr als 1 GB Speicherplatz
- Am Ende erhalten wir das gewünschte Ergebnis!

Satz (Bugeaud, Mignotte, Siksek, Stoll, Tengely)

Sind $x, y \in \mathbb{Z}$ mit

$$\binom{y}{2} = \binom{x}{5},$$

dann gilt

$$x \in \{0, 1, 2, 3, 4, 5, 6, 7, 15, 19\}.$$