Ungelöste Probleme der Zahlentheorie

Teil 11: Der Satz von Roth, Transzendenz und die abc-Vermutung

Ein klassischer Satz ist der Approximationssatz von Dirichlet, der sich mit dem Schubfachprinzip beweisen lässt:

$\forall \alpha \in \mathbb{R}, X>1 \quad \exists m,n \in \mathbb{Z}, (m,n)=1, 1 \le n \le X: \left|\alpha - \frac{m}{n}\right| < \frac{1}{nX} \left(\le \frac{1}{n^2}\right).$

Für $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ hat $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}$ also ∞ viele Lösungen, für $\alpha \in \mathbb{Q}$ hingegen nur endl. viele $\left[\frac{1}{n^2} > \left|\frac{a}{b} - \frac{m}{n}\right| \ge \frac{1}{bn} \Rightarrow n < b\right]$

Damit werden also rationale Zahlen charakterisiert.

Sei $A := \{\alpha \in \mathbb{C};\ \exists f \in \mathbb{Z}[X]\setminus 0 : f(\alpha)=0\}$ die Menge der algebraischen Zahlen. Für $\alpha \in (A \cap \mathbb{R}) \setminus \mathbb{Q}$ gibt es also unendl. viele $\frac{m}{n} \in \mathbb{Q}$ mit $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}$.

Nach dem Satz von Liouville gilt für $\alpha \in A \cap \mathbb{R}$ mit $\deg \alpha =: d > 1$:

$\exists c = c(\alpha) > 0 \ \forall \frac{m}{n} \in \mathbb{Q}, n>0: \left|\alpha - \frac{m}{n}\right| > \frac{c}{n^d}.$

Daher lassen sich reell algebraische Zahlen nicht besser approximieren als mit dem Exponenten d in dieser Ungl. Daher sind Zahlen wie $\alpha := \underbrace{\text{cfrac}}_{=\text{Kettenbruch}}(1, 10^{1!}, 10^{2!}, 10^{3!}, \dots)$ transzendent, d.h. nicht algebraisch.

In der Theorie der transzendenten Zahlen gibt es bis heute viele offene Fragen. So ist die Menge der algebraischen Zahlen in $\mathbb{R}$ abzählbar, d.h. "fast" alle reellen Zahlen sind transzendent. Dennoch ist es von konkreten reellen Zahlen nur schwer möglich, ihre Transzendenz nachzuweisen. Die Transzendenz von e und π nach Hermite/Lindemann u.a. wird heute zusammengefasst als Satz von Lindemann-Weierstraß: Sind $\alpha_1, \dots, \alpha_n$ verschieden und algebraisch, sowie $\beta_1, \dots, \beta_n \neq 0$ algebraisch, so ist $\beta_1 e^{\alpha_1} + \dots + \beta_n e^{\alpha_n} \neq 0$.

Dies zeigt die Transzendenz von e, und aus $e^{i\pi} + 1 = 0$ folgt die von π.

Eine Menge reeller Zahlen $\alpha_1, \dots, \alpha_n$ heißt algebraisch unabhängig, wenn es kein Polynom $P \in \mathbb{Q}[X_1, \dots, X_n]\setminus 0$ gibt mit $P(\alpha_1, \dots, \alpha_n) = 0$.

Eine der wichtigsten ungelösten Probleme in der Theorie der transzendenten Zahlen ist Schanuels Vermutung: Sind $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ linear unabh. über $\mathbb{Q}$, so gibt es unter den $2n$ Zahlen $\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n}$ mindestens n, die algebraisch unabhängig über $\mathbb{Q}$ sind. (Dies verallgemeinert den Satz von Lindemann/Weierstraß)

Wir behandeln nun der Satz von Roth, insb. im Zusammenhang mit der abc-Vermutung.

Der Satz von Roth besagt, dass der Exponent 2 bei der Dirichlet-Approximation optimal ist für alle irrationalen reellen algebraischen Zahlen:

Satz von Roth (1955, Fields-Medaille): Sei $\alpha \in (\mathbb{A} \cap \mathbb{R}) \setminus \mathbb{Q}$. Dann gilt:
$\forall \varepsilon > 0 \; \exists C_{\alpha,\varepsilon} > 0 : \left|\alpha - \frac{m}{n}\right| \geq \frac{C_{\alpha,\varepsilon}}{n^{2+\varepsilon}}$ für alle $\frac{m}{n} \in \mathbb{Q}$.

M.a.W.: $\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^{2+\varepsilon}}$ hat nur endl. viele Lösungen für $\frac{m}{n} \in \mathbb{Q}$.

Vermutung von S. Lang: $\forall \alpha \in \mathbb{A} \cap \mathbb{R}$, $\deg \alpha \geq 3$: $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 (\log q)^{\kappa}}$, $\kappa > 1$ beel.,
hat nur endlich viele Lösungen. (das präzisiert "ε")

Wir zeigen als erstes eine Anwendung des Satzes von Roth, nämlich dass bestimmte Thue-Gleichungen nur endlich viele Lsgn. über $\mathbb{Z}$ haben.

Wir haben:

Ramanujans taxicab-Zahl $1729 = 1^3 + 12^3 = 9^3 + 10^3$ ist auf genau 2 Arten darstellbar als Summe zweier Kuben.

Bew.: Da $(X+Y) \cdot (X^2 - XY + Y^2) = X^3 + Y^3 \overset{!}{=} 1729 = 7 \cdot 13 \cdot 19$,
erhalten wir alle (endl. vielen) Faktorisierungen $1729 = A \cdot B$
durch Lösen von $A = X + Y$ und $B = X^2 - XY + Y^2$.

Die Substitution $Y = A - X$ führt auf $X^2 - AX + \frac{1}{3}(A^2 - B) = 0$.

$$\text{l.S.} = X^2 - AX + \tfrac{1}{3}\left(A^2 - X^2 + X(A-X) - (A-X)^2\right)$$
$$= X^2 - AX - \tfrac{1}{3}X^2 + \tfrac{1}{3}AX - \tfrac{1}{3}X^2 + \tfrac{2}{3}AX - \tfrac{1}{3}X^2 = 0$$

Somit reicht es zu checken, wann $\frac{1}{6}\left(3A \pm \sqrt{12B - 3A^2}\right) \in \mathbb{Z}$ ist.
Dies geht nur mit den Paaren $A = 13, B = 133$ und $A = 19, B = 91$, die zu obigen beiden Lösungen führen. □

[Ebenso kann man noch checken, dass die $m < 1729$ höchstens eine Darstellung als Summe zweier Kuben zulassen.]

Wir zeigen nun allgemeiner als Anwendung des Satzes von Roth:

Satz von Thue: Sind $a, b, m \in \mathbb{Z} \setminus \{0\}$, so hat $aX^3 + bX^3 = m$ nur endlich viele Lösungen in $\mathbb{Z}$.

Beweis: Ist $x, y \in \mathbb{Z}$ ein Lösungspaar, so ist $X = ax$, $Y = y$ eine Lösung von $X^3 + a^2 b Y^3 = a^2 m$, also zeigen wir den Satz ⚠ mit $a = 1$.
Ebenso kann y durch $-y$, und b durch $-b$ ersetzt werden. Daher betr. ⚠ $X^3 - bY^3 = m$, $m, b \in \mathbb{N}$. Betr. die Faktorisierung $X^3 - bY^3 = (X - \alpha Y)\cdot(X^2 + \alpha XY + \alpha^2 Y^2)$, $\alpha := \sqrt[3]{b}$.

- Ist b ein Kubus, so ist $\alpha \in \mathbb{N}$ und wir können wie oben vorgehen.
- Andernfalls hat $x - \alpha y$ kleinen Absolutbetrag, da $x^2 + \alpha xy + \alpha y^2 = \left(x + \frac{1}{2}\alpha y\right)^2 + \frac{3}{4}(\alpha y)^2 \geq \frac{3}{4}\alpha^2 y^2$,

so dass folgt: $m = x^3 - by^3 = |x - \alpha y| \cdot |x^2 + \alpha xy + \alpha^2 y^2| \geq \frac{3}{4}\alpha^2 y^2 |x - \alpha y|$.
Dies zeigt:

$$\left|\alpha - \frac{x}{y}\right| \leq \frac{4m}{3\alpha^2 y^3}.$$

Wegen dem Satz von Roth ist die l.S. aber durch $\frac{c}{y^{2+\varepsilon}}$ nach unten beschr., wo $c = c(\alpha) > 0$. Es folgt

$$y < \left(\frac{4m}{3\alpha^2 c}\right)^{\frac{1}{1-\varepsilon}},$$

so dass die Ungl. $\left|\alpha - \frac{x}{y}\right| \leq \frac{4m}{3\alpha^2 y^3}$ also nur endl. viele Lsgn. $\frac{x}{y}$ haben kann.

□

Bem.: Zur Zeit von Thue war der Satz von Roth noch unbewiesen.
Thue benutzte eine schwächere Abschätzung, mit der dieser Beweis noch klappt, und welche nur für algebraische reelle Zahlen vom Grad 3 gültig war.

Wir behandeln als nächstes den Zusammenhang des Satzes von Roth mit der abc-Vermutung.
Dazu formulieren wir den Satz von Roth um zu folgender Version:

Roth-Variante ⊕:
Sei $F(x,y) \in \mathbb{Z}[x,y]$ eine binäre homogene Form ohne mehrfachen Faktor.
Dann ist: $\forall \varepsilon > 0 \; \exists C(\varepsilon) > 0 \; \forall (m,n) = 1: \; |F(m,n)| \geq C(\varepsilon) \cdot n^{\deg(F)-2-\varepsilon}$.

Beh.: Roth $\Leftrightarrow$ Version ⊕.

Beweis: „$\Rightarrow$": Sei F gegeben wie in ⊕. Dann ist für $(m,n)=1$, $d := \deg F$:

$$|F(m,n)| = n^d \left|F\left(\tfrac{m}{n},1\right)\right| = n^d \cdot c \cdot \prod_{\substack{\alpha \\ F(\alpha,1)=0}} \left|\alpha - \tfrac{m}{n}\right| \geq C(\varepsilon) \cdot n^{d-2-\varepsilon}.$$

(Zerlegung: $F(t,1) = c \cdot \prod_{\alpha} (t-\alpha)$; Roth auf einen Faktor, für die anderen ist $|\alpha' - \tfrac{m}{n}| \simeq |\alpha' - \alpha|$ abh. von F)

„$\Leftarrow$": Sei α geg. mit Mipo $f(t)$ und dessen Homogenisierung sei $F(x,y)$.
$\left[f(t) = \sum_{i=0}^{d} a_i t^i \Rightarrow F(x,y) = \sum_{i=0}^{d} a_i x^i y^{d-i} \right]$.

Mipo = Minimalpolynom

Dann: $n^{d-2-\varepsilon} \overset{\oplus}{\leq} C(\varepsilon) \cdot |F(m,n)| = C(\varepsilon) \cdot n^d \cdot c \prod_{\substack{\alpha \\ F(\alpha,1)=0}} \left|\alpha - \tfrac{m}{n}\right|$, mit $\tfrac{m}{n}$ nahe α

folgt $\left|\alpha - \tfrac{m}{n}\right| \geq C_{F,\varepsilon} \, n^{-2-\varepsilon}$ für $C_{F,\varepsilon} > 0$,
also Roth. □

Eine Verschärfung von ⊕ stellt die folgende Vermutung ⊛ dar:
Ist F wie in ⊕ geg., so ist $\prod_{p \mid F(m,n)} p = R(F(m,n)) \geq C(\varepsilon) \cdot \max\{|m|,|n|\}^{\deg(F)-2-\varepsilon}$.

Beh.: Vermutung $\circledast \Rightarrow$ abc-Vermutung

Bew.: Sei $a+b=c$. Wähle $F(x,y) = xy(x+y)$ in $\circledast$, $\deg F = 3$.

Dann:

$$R(abc) = \prod_{p \mid abc} p = \prod_{p \mid F(a,b)} p \overset{\circledast}{\geq} C(\varepsilon) \underbrace{\max\{|a|,|b|\}}_{\geq |c|/2}^{3-2-\varepsilon},$$

also ist

$$\left(\prod_{p \mid abc} p\right)^{\frac{1}{1-\varepsilon}} \geq \tilde{C}(\varepsilon) \cdot \max\{|a|,|b|,|c|\}. \text{ Mit } \frac{1}{1-\varepsilon} = 1+\varepsilon' \text{ folgt die abc-Beh. } \square$$

Bem.: Es gilt auch umgekehrt: abc $\Rightarrow$ Vermutung $\circledast$, obwohl $\circledast$ stärker scheint, dies wird mittels arithmetischer Geometrie gezeigt.

[Bombieri 1994]

Somit: abc $\Leftrightarrow \circledast \Rightarrow$ Roth

Bem. [Langevin, 1996]: abc $\Rightarrow \left|\alpha - \frac{m}{n}\right| > \frac{C(\varepsilon)}{R(mn)\, n^{\varepsilon}}$ für alle $\frac{m}{n} \in \mathbb{Q}$,

was stärker ist als der Satz von Roth.

[van Frankenhuysen, 1999] zeigte, dass eine Verfeinerung des Satzes von Roth sowohl die Mordellsche Vermutung als auch die abc-Vermutung impliziert

Mehr zur abc-Vermutung auf

www.math.unicaen.fr/~mitaj/abc.html