Ungelöste Probleme der Zahlentheorie

Teil 10: Die abc-Vermutung

Satz 1 (ABC-Satz für Polynome):

Vor.: $A, B, C \in \mathbb{C}[T]$, $ggT(A,B,C) = 1$ (d.h. const.),
A, B, C nicht alle konstant (d.h. $\deg(ABC) \geq 1$).

Beh.: $A + B = C \Rightarrow \max\{\deg A, \deg B, \deg C\} < n(ABC)$,
wo $n(ABC)$ die Anzahl der verschiedenen Nullst. von ABC bezeichnet.

Beweis: über Aufspalten von A, B, C in Linearfaktoren

in $A = a \prod_{j \leq m(A)} (X - \alpha_j)^{a_j}$, $B = b \prod_{k \leq m(B)} (X - \beta_k)^{b_k}$, $C = c \prod_{\ell \leq m(C)} (X - \gamma_\ell)^{c_\ell}$,

also $(\log A)' = \sum_{j \leq m(A)} \frac{a_j}{X - \alpha_j}$, analog für B und C.

Sei $F := \frac{A}{C}$, $G := \frac{B}{C}$, also $F + G - 1 = 0 \Rightarrow F' = -G'$

und $\frac{A}{B} = \frac{F}{G} = -\frac{G'/G}{F'/F}$.

Haben $\frac{F'}{F} = (\log F)' = (\log A)' - (\log C)'$, ebenso für $\frac{G'}{G}$.

Also:
$$\frac{A}{B} = -\frac{\left(\sum \frac{b_k}{X-\beta_k} - \sum \frac{c_\ell}{X-\gamma_\ell}\right) \cdot \mathcal{N}}{\left(\sum \frac{a_\ell}{X-\alpha_\ell} - \sum \frac{c_\ell}{X-\gamma_\ell}\right) \cdot \mathcal{N}} =: \frac{\mathcal{A}}{\mathcal{B}},$$

mit $\mathcal{N} := \prod_j (X - \alpha_j) \prod_k (X - \beta_k) \prod_\ell (X - \gamma_\ell)$, $\deg \mathcal{N} = n(ABC)$.

Nun sind $\mathcal{A}, \mathcal{B}$ Polynome, beide vom Grad $< n(ABC)$.

Da A, B teilerfremde Polynome mit $\frac{A}{B} = -\frac{\mathcal{A}}{\mathcal{B}}$, ist auch deren Grad jeweils $< n(ABC)$. □

Korollar 2 (Satz von Fermat für Polynome):

Vor.: $n \geq 3$, $X, Y, Z \in \mathbb{C}[T]$, $X^n + Y^n = Z^n$.

Beh.: Das Tripel (X, Y, Z) ist polynomielles Vielfaches einer Lösung $(x, y, z) \in \mathbb{C}^3$ von $x^n + y^n = z^n$, d.h. (X, Y, Z) ist unechte Lösung.

Bew.: Sonst sei $ggT(X, Y, Z) = 1$ (const.), aber nicht alle X, Y, Z konstant, sei $A := X^n$, $B := Y^n$, $C := Z^n$, also $A + B = C$.
Die Nullst. von $ABC = (XYZ)^n$ sind die von XYZ.
Sei $\mathbb{C} \ni X$ das Polynom mit höchstem Grad.

$$n \deg X = \deg A < n(ABC) = n(XYZ) \leq \deg XYZ \leq 3 \deg X,$$

so dass $n < 3$ folgt, $\lightning$. $\square$

Übersetzen nun den ABC-Satz in eine $\mathbb{Z}$-Version:

Linearfaktoren $\hookrightarrow$ Primteiler
Grad $\hookrightarrow$ Absolutbetrag

Somit würde $n(ABC)$ dem Radikal $R(abc) := \prod_{p | abc} p$ entsprechen.

Die Beh. im ABC-Satz würde dann $\max\{|a|, |b|, |c|\} < R(abc)$ $\circledast'$ lauten. Diese kann so nicht stimmen!

Bsp.: Sei $a = 3^{2^n}$, $b = -1$, dann ist $a + b = 3^{2^n} - 1 = c$.

Haben: $2^n \mid 3^{2^n} - 1$ (Ind.: $n = 0$ ✓, $n \rightsquigarrow n+1$: $3^{2^{n+1}} - 1 = \underbrace{(3^{2^n} - 1)}_{\text{Vielf. v. } 2^n} \cdot \underbrace{(3^{2^n} + 1)}_{\text{gerade}} \equiv 0 \pmod{2^{n+1}}$ ✓)

Also: $R(abc) \leq 3 \cdot 2 \cdot \frac{c}{2^n} < 6 \cdot \frac{3^{2^n}}{2^n}$,

(3 ↑ Faktor in a; 2 ↑ inc; $\frac{c}{2^n}$ ↖ Rest!. Faktoren inc)

aber: $a = 3^{2^n} > \frac{6 \cdot 3^{2^n}}{2^n}$ für $n \geq n_0$.

Also: $\circledast'$ gilt nicht.

$\rightsquigarrow$ Müssen $\circledast'$ modifizieren wie folgt.

abc-Vermutung: $\forall \varepsilon > 0 \; \exists C(\varepsilon) > 0$: $a,b,c \in \mathbb{Z}$, $ggT(a,b,c) = 1$, $a+b=c$
$\Rightarrow \max\{|a|,|b|,|c|\} \leq C(\varepsilon)\, R(abc)^{1+\varepsilon}$. $\circledast$

Explizit (nach Baker): $a,b,c > 0$, $a+b=c \Rightarrow c = O\Big(N \sum_{\substack{n \leq N \\ p \mid n \Rightarrow p \mid abc}} 1\Big)$, $N := R(abc)$.

1. Kor. [abc]: Fermats großer Satz (= Satz von Fermat-Wiles-Taylor): $\exists n_0 \; \forall n \geq n_0$: $x^n + y^n = z^n$ hat keine nichttriviale Lösung $(x,y,z) \in \mathbb{Z}^3$.

Bew.: Sonst sei $(x,y,z) \in \mathbb{Z}^3$ nichttriv. mit $x^n + y^n = z^n$, $ggT(x,y,z) = 1$.
Dann: $a = |x|^n$, $b = |y|^n$, $c = |z|^n$ $\overset{abc}{\rightsquigarrow}$ $\max\{|x|^n, |y|^n, |z|^n\} \leq C(\varepsilon)\, R(xyz)^{1+\varepsilon}$ $\circledast$
$\leq C(\varepsilon) \cdot |xyz|^{1+\varepsilon}$, also $|xyz|^n \leq C(\varepsilon)^3 |xyz|^{3+3\varepsilon}$,
also $(n-3-3\varepsilon) \log |xyz| \leq 3 \log C(\varepsilon)$. Da $|xyz| \geq 2$,
folgt $n < \lceil 3 \frac{\log C(\varepsilon)}{\log 2} + 3 + 3\varepsilon \rceil =: n_0(\varepsilon)$. Nun setze $n_0 := \min_{\varepsilon > 0} n_0(\varepsilon)$ für den $\lightning$. $\square$

2. Kor. [abc]: Fermat-Catalan-Vermutung: $\exists m_0 \; \forall m \geq m_0$: $x^p + y^q = z^r$
mit $x,y,z \in \mathbb{N}$, $ggT(x,y,z) = 1$, $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ $(p,q,r \in \mathbb{N})$ hat nur endl. viele Lsgn. in (x,y,z).

Bew.: Betr. Lsg. $a = x^p$, $b = y^q$, $c = z^r$ $\overset{abc}{\rightsquigarrow}$ $z^r = \max\{x^p, y^q, z^r\} \overset{\circledast}{\leq} C(\varepsilon)\, R(xyz)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{1+\varepsilon}$.
Haben: $xyz = (x^p)^{\frac{1}{p}} (y^q)^{\frac{1}{q}} (z^r)^{\frac{1}{r}} \leq (z^r)^{\frac{1}{p}+\frac{1}{q}+\frac{1}{r}} \leq z^{\frac{41}{42} r}$, also $z^r \leq C(\varepsilon)\, z^{\frac{41}{42} + (1+\varepsilon)}$.
Mit $\varepsilon := \frac{1}{83}$ folgt $z \leq C \cdot \left(\frac{1}{83}\right)^{83}$. $\square$

Catalan-Vermutung: $x^p - y^q = 1$ $(p,q,x,y \in \mathbb{N})$ hat einzige Lsg. $3^2 - 2^3 = 1$ [Mihăilescu 2004] (bewiesen).

Bem.: Aus abc folgt auch die Fermat-Version für die Gl. $Ax^p + By^q = Cz^r$.

Bestes bewiesenes
abc-Ergebnis bislang: [Stewart & Yu '91]:
$\max\{|a|,|b|,|c|\} \leq \exp\left(C \cdot R(abc)^{\frac{1}{3}+\varepsilon}\right)$, C effektiv berechenbar.

Verallgemeinerte abc-Vermutung (auf n Summanden):
$\forall n \geq 3\ \forall \varepsilon > 0\ \exists C_n(\varepsilon)$: $x_1 + \dots + x_n = 0$ mit $ggT(x_1, \dots, x_n) = 1$,
wobei keine Untersumme von $x_1 + \dots + x_n$ verschwindet
$\Rightarrow \max\{|x_1|, \dots, |x_n|\} \leq C_n(\varepsilon) \cdot R(x_1 \cdots x_n)^{2n-5+\varepsilon}$.

[Elkies 1991]: abc $\Rightarrow$ Satz von Faltings
(ehem. Mordellsche Vermutung).

Es gibt folgenden bemerkenswerten Zusammenhang zw. abc und Siegel-Nullstellen
[Granville & Stark 2000]: Glm. abc-Vermutung für Zahlkörper
$\Rightarrow$ ex. keine Siegel-Nst. für L-Funktionen zu
Charakteren $\left(\frac{-d}{\cdot}\right)$, $-d < 0$.

Glm. abc-Vermutung für Zahlkörper:
$\forall \varepsilon > 0$: ist $a + b = c$ mit a, b, c algebraisch, etwa im Zahlkörper K, so gilt:
$$H(a,b,c) = O_\varepsilon\left(\Delta_K \cdot R(abc)\right)^{1+\varepsilon},$$
wo $H(a,b,c) := \prod_{v \text{ normalisierte Bewertungen von } K} \max\{|a|_v, |b|_v, |c|_v\}$ die Höhe bezeichnet,
und $\Delta_K := |\mathrm{disc}_{\mathbb{Q}} K|^{\frac{1}{[K:\mathbb{Q}]}}$.

Ein weiterer wichtiger Aspekt der abc-Vermutung ist ihre Relevanz für diophantische Approximationen, insb. der Zusammenhang mit dem Satz von Roth, den wir nächstes Mal beleuchten.
Bei diophantischen Approximationen geht es u.a. um die Approximierbarkeit reeller Zahlen durch rationale.