Def: Ein <u>abc-Tripel</u> besteht aus drei Zahlen $a,b,c \in \mathbb{N}$ sodass

$$(a,b,c)=1 \qquad \underline{\text{und}} \qquad a+b=c$$

Ein <u>abc-Treffer</u> ist ein abc-Tripel mit

$$c > \prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p$$

Proposition 2.12: Es gibt unendlich viele abc-Treffer

Beweis: Sei $a=1$, $b=3^{2^k}-1$ und $c=3^{2^k}$

Dann gilt $\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p = 3 \prod_{\substack{p \in \mathbb{P} \\ p \mid b}} p$

$$\begin{aligned} b &= 3^{2^k}-1 \\ &= (3^{2^{k-1}}+1)(3^{2^{k-1}}-1) \\ &\vdots \\ &= (3^{2^{k-1}}+1)(3^{2^{k-2}}+1)\cdots(3^{2^0}+1)(3^{2^0}-1) \end{aligned}$$

gerade, gerade, 4, gerade

$$\Rightarrow 2^{k+2} \mid b$$

$$\Rightarrow \prod_{\substack{p \in \mathbb{P} \\ p \mid b}} p \leq \frac{b}{2^{k+1}}$$

$$\Rightarrow \prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \leq 3\frac{b}{2^{k+1}} < 3\frac{c}{2^{k+1}} < c \qquad \text{für alle } k \in \mathbb{N}^+ \qquad \square$$

Bemerkung: Der Fehlbetrag $\frac{2^{k+1}}{3}$ wird groß

aber klein in Vergleich zu c.

Die abc-Vermutung (Masser, Oesterlé)

$\forall \varepsilon > 0 \quad \exists\, C(\varepsilon)$ sodass für alle abc-Tripel gilt

$$c \leq C(\varepsilon) \Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \Big)^{1+\varepsilon}$$

Äquivalent dazu wäre:

$\forall \varepsilon > 0$ existieren nur endlich viele abc-Tripel

mit $c > \Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \Big)^{1+\varepsilon}$

Bemerkung: $c > \Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \Big)^{1+\varepsilon} \iff \ln(c) > (1+\varepsilon) \ln\Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \Big)$

$$\iff q(a,b,c) := \frac{\ln(c)}{\ln\Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} p \Big)} > 1+\varepsilon$$

Vermutung: $\forall \varepsilon > 0$ existieren nur endlich viele abc-Tripel

mit $q(a,b,c) > 1+\varepsilon$.

Der größte bekannte Wert für $q(a,b,c)$:

Sei $a = 2$, $b = 109 \cdot 3^{10}$, $c = 23^5$

$$\prod_{\substack{p \in \mathbb{P} \\ p \mid abc}} = 2 \cdot 3 \cdot 23 \cdot 109$$

Dann ist $q(a,b,c) \approx 1{,}6299$

Bemerkung: Die abc-Vermutung hat viele Verbindungen mit anderen Vermutungen und Sätzen aus der Zahlentheorie

z.B. großer Fermatsche Satz für großes n.

Satz 2.13: Aus der abc-Vermutung folgt:

$\exists\, n_0 \in \mathbb{N}$ sodass

$x^n + y^n = z^n$

keine Lösungen $x, y, z \in \mathbb{N}^+$ hat für $n \geq n_0$

Beweis: Sei $x, y, z \in \mathbb{N}^+$ teilerfremd und sodass $x^n + y^n = z^n$

Sei $\varepsilon > 0$

Aus der abc-Vermutung folgt

$$z^n \leq C(\varepsilon) \Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid x^n y^n z^n}} p \Big)^{1+\varepsilon}$$

$$= C(\varepsilon) \Big(\prod_{\substack{p \in \mathbb{P} \\ p \mid xyz}} p \Big)^{1+\varepsilon}$$

$$\leq C(\varepsilon) \left(z^3 \right)^{1+\varepsilon}$$

$$= C(\varepsilon)\, z^{3+3\varepsilon}$$

$$\Rightarrow z^{n-3-3\varepsilon} \leq C(\varepsilon)$$

$$(n-3-3\varepsilon) \ln(z) \leq \ln(C(\varepsilon))$$

$$\ln(z) \leq \frac{\ln(C(\varepsilon))}{n-3-3\varepsilon} < \ln(2) \quad \text{für } n > \frac{\ln(C(\varepsilon))}{\ln(2)} + 3 + 3\varepsilon$$

$$\Rightarrow \quad z < 2$$

$$\Rightarrow \quad z = 1$$

$$\Rightarrow \quad x \text{ oder } y = 0 \qquad \lightning \qquad \square$$

Bemerkung: Mit der Annahme, dass keine abc-Tripel mit $q(a,b,c) \geq 2$ existieren würde folgen:

Die Fermatgleichung mit $n > 6$ hat keine nicht-triviale Lösung.

Mochizuki hat in August 2012 behauptet, die abc-Vermutung bewiesen zu haben

- 4 Paper
- 500 Seiten
- neue Theorie entwickelt

Diese Behauptung ist noch nicht bestätigt

Zur abc-Vermutung gibt es einen analogen Satz für Polynome, den wir beweisen werden.

Wir müssen dafür einige Definitionen für Polynome erweitern

z.B. Teile

Primzahlen

$\leq$

⋮

Kapitel 3: Ringe

Def: Ein **Ring** ist eine Menge R mit zwei binären Operationen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ sodass folgende Eigenschaften erfüllt sind:

1. $a+b = b+a$ $\quad \forall a,b \in R$ — Kommutativität von $+$
2. $a+(b+c) = (a+b)+c$ $\quad \forall a,b,c \in R$ — Assoziativität
3. $\exists\, n \in R$ sodass $a+n = n+a = a$ $\quad \forall a \in R$ — Additive Identität
   (wir bezeichnen dieses n mit 0)
4. $\forall a \in R$ $\exists\, b \in R$ sodass $a+b = b+a = 0$ — Additive Inverse
   (wir bezeichnen dieses b mit $-a$)
5. $a \cdot b = b \cdot a$ $\quad \forall a,b \in R$ — Kommutativität von $\cdot$
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\quad \forall a,b,c \in R$ — Assoziativität
7. $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ $\quad \forall a,b,c \in R$ — Distributivität

Bemerkung: Vorsicht! Manchmal wird ein Ring anders definiert (insbesondere wird 5 oft ausgelassen, und 7 dann für Multiplikation links und rechts gegeben).

2–4 besagen, dass $(R,+)$ eine Gruppe ist.
Mit 1 ist sie sogar eine abelsche Gruppe.

Def: Ein Ring mit 1 ist ein Ring mit der zusätzlichen Eigenschaft

8. $\exists\, m \in R$ sodass $m \cdot a = a \cdot m = a$ $\quad \forall a \in R$
   (wir bezeichnen dieses m mit 1)

Beispiele: Ring mit 1: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Ring ohne 1: $2\mathbb{Z}$ (gerade Zahlen)

nicht-kommutativer Ring (ohne Eigenschaft 5): $n \times n$ Matrizen $(n>1)$

Def: Sei $(R, +, \cdot)$ ein Ring mit 1 und $a, b \in R$, $a \neq 0$.

a teilt b $\Leftrightarrow \exists\, c \in R$ sodass $a \cdot c = b$

a heisst eine Einheit $\Leftrightarrow a \mid 1$

Seien $p, q \in R$ keine Einheiten und $p, q \neq 0$

p heisst prim falls $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$ $\quad \forall a, b \in R$

q heisst irreduzibel falls $ab = q \Rightarrow a$ oder b ist eine Einheit.

Beispiel: Im Ring $\mathbb{Z}$ sind die Einheiten ± 1

und die Primelemente $\pm p$ $\quad (p \in \mathbb{P})$

= irreduzible Elemente

Lemma 3.1: Sei $(R, +, \cdot)$ ein Ring mit 1 und ~~$a \in R$~~ ohne Nullteiler und $a \in R$

a ist prim $\Rightarrow a$ ist irreduzibel

aber die Rückrichtung gilt nicht unbedingt

Beweis: Übungsaufgabe