WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ 14: Höhere Potenzgleichungen

Stichworte: Fermatproblem, Fall $n=4$, abc-Vermutung, Fermat/Catalan für große Exponenten, gemischte diophantische Gleichungen, Taxizahlen, Waringsches Problem, Hardy/Littlewood

14.1. Einleitung: Die pyth. Gleichung $x^2+y^2=z^2$ und auch andere diophantische Gleichungen vom Grad 2 haben unendlich viele ganzzahlige Lösungen. Bei Gleichungen höheren Grades hat man i.a. höchstens endlich viele ganzzahlige Lösungstupel. Wir stellen einige hier vor. In vielen Fällen ist dabei die "modulare Brille" ein nützliches Werkzeug.

14.2. Def.: Die Gleichung $x^n+y^n=z^n$ mit $n\geq 3$ heißt Fermatsche Gleichung. (P. de Fermat, 1601–1655)
Zu den ganz großen Problemen der Mathematik gehörte lange Zeit die

14.3. Fermatsche Vermutung / Der große Fermatsche Satz (Fermat's last Theorem):
Für alle $n\geq 3$ hat die Fermatsche Gleichung keine nichttriviale Lösung $(x,y,z)\in\mathbb{Z}^3$.
(last Theorem: für die "letzte" noch unbewiesene Aussage Fermats)

14.4. Bem.: In den etwa 350 Jahren ihrer Geschichte haben sich fast alle namhaften Mathematiker ernsthaft um einen Beweis der Fermatschen Vermutung bemüht. Insbesondere die Entwicklung der algebraischen Zahlentheorie wurde durch die Arbeit an dieser Vermutung entscheidend vorangetrieben. Erst in der Neuzeit, etwa im Jahr 1995 gelang A. Wiles / R. Taylor der vollständige Beweis, der heute großer Fermatscher Satz / Fermat's last theorem heißt.
Vgl. auch das Buch "Fermat's last theorem" von S. Singh.

14.5. Bem.: Falls die Unlösbarkeit der Fermat-Glg. für ein $n\geq 3$ bewiesen ist, dann folgt sie wegen $x^{mn}=(x^m)^n$ auch für jedes Vielfaches von n. Daher genügt es, den Beweis der Unlösbarkeit für $n=4$ und alle Primzahlexponenten $n=p\in\mathbb{P}$, $p\geq 3$, zu führen.
Wir zeigen hier den Fall $n=4$, den bereits Fermat bewiesen hat.
Der berühmte Beweisversuch von E. Kummer für $n=p\geq 3$ prim wird in ZT I behandelt.

14.6. **Satz (Fermat):** Die Gleichung $x^4+y^4=z^4$ hat keine nichttriviale Lösung $(x,y,z)\in\mathbb{Z}^3$.

Bew.: Es genügt, die Unlösbarkeit für $(x,y,z)\in\mathbb{N}^3$ nachzuweisen.

1.) **Def. von z_0:** Es genügt, die Unlösbarkeit von $x^4+y^4=z^2$ (*) zu zeigen.

Ann.: Sei (*) in $\mathbb{N}^3$ lösbar, und sei $z_0 := \min\{z\in\mathbb{N};\ \exists x,y\in\mathbb{N}: x^4+y^4=z^2\}$.
Seien $x,y\in\mathbb{N}$ mit $x^4+y^4=z_0^2$. Es muss $(x,y)=1$ gelten, da sonst in (*) durch Kürzen zu einem kleineren z führen würde. Insb. ist $2\nmid x$ oder $2\nmid y$, also ist $z_0^2=x^4+y^4\equiv 1\ (4)$ oder $z_0^2=x^4+y^4\equiv 2\ (4)$. Der letzte Fall tritt nicht ein. (modulare Brille mod 4)
Es bleibt $z_0\equiv 1(2)$ und OE $x\equiv 0(2)$, $y\equiv 1(2)$.

2.) **Anwenden der indischen Formeln (Satz 13.4):**
Da (x^2,y^2,z_0) ein primitives pyth. Tripel ist,
ex. $u,v\in\mathbb{N}$, $u>v$, $(u,v)=1$, $u+v\equiv 1(2)$, $x^2=2uv$, $y^2=u^2-v^2$, $z_0=u^2+v^2$.
Aus $u\equiv 0\ (2)$, $v\equiv 1(2)$ folgt $y^2\equiv 3(4)$, ↯ (modulare Brille mod 4).
Also ex. $w\in\mathbb{N}$ mit $u\equiv 1(2)$, $v=2w$.

3.) **Konstruktion von z_1:** Aus 2.) ergibt sich $\left(\frac{x}{2}\right)^2=\frac{2uv}{4}=uw$, $(u,w)=1$,
also ex. $z_1\in\mathbb{N}$, $d\in\mathbb{N}$: $u=z_1^2$, $w=d^2$, $(z_1,d)=1$ und $y^2=u^2-v^2=z_1^4-4d^4$,
also ist (+) $(2d^2)^2+y^2=(z_1^2)^2$, wobei $2d^2$, y, z_1^2 p.w. teilerfremd sind.

4.) **Beweis von $z_1<z_0$:** Auf (+) wird erneut Satz 13.4 (indische Formeln) angewandt,
und es gibt $u_1,v_1\in\mathbb{N}$, $u_1>v_1$, $(u_1,v_1)=1$, $u_1+v_1\equiv 1\ (2)$,
$2d^2=2u_1v_1$, $y=u_1^2-v_1^2$, $z_1^2=u_1^2+v_1^2$.
Wegen $d^2=u_1v_1$ und $(u_1,v_1)=1$ ex. $x_1,y_1\in\mathbb{N}$: $u_1=x_1^2$, $v_1=y_1^2$, $x_1^4+y_1^4=z_1^2$.
Aber wegen $0<z_1\le z_1^2=u\le u^2<u^2+v^2=z_0$
ist somit eine kleinere Zahl als z_0 gefunden, die (*) löst, ↯. □

14.7. **Bem.:** Die hier benutzte Methode, zu einer angenommenen Lösung eine kleinere zu konstruieren, geht auf Fermat zurück und wird nach ihm "descendendo infinie" (= Methode des unendlichen Abstiegs) genannt.

- Der schwierigere Fall $n=3$ wurde von Euler gelöst, der Fall $n=5$ von Dirichlet und Legendre. Diese Fälle können nicht mit der Methode des unendlichen Abstiegs gezeigt werden, sondern benötigen eine algebraische Untersuchung (→ algebraische ZT / ZT I).
- S. Germain bewies den sog. 1. Fall der Fermatschen Vermutung ($p\nmid xyz$) für alle $n=p$, für die $2p+1$ prim.

Wir zeigen noch, dass das Fermatproblem (und Verallgemeinerungen) für alle hinreichend großen n eine Folgerung der weitreichenden, noch offenen abc-Vermutung ist.

14.8. **abc-Vermutung:** $\forall \varepsilon > 0 \; \exists C(\varepsilon) > 0 : a, b, c \in \mathbb{Z}$, $(a,b,c) = 1$, $a + b = c$
$\Rightarrow \max\{|a|, |b|, |c|\} \leq C(\varepsilon) \cdot \gamma(abc)^{1+\varepsilon}$,
wobei $\gamma(m) := \prod_{p \mid m} p$ das Radikal bzw. der quadratfreie Kern von $m \in \mathbb{Z}$ bezeichnet.

14.9. **Bem.:** Der Zusatz mit ε im Exponenten ist wesentlich, in der Form "max... $\leq C' \cdot \gamma(a,b,c)$" kann dies nicht stimmen: Mit $a = 3^{2^n}$, $b = -1$, ist $a + b = 3^{2^n} - 1 = c$, wo $2^n \mid 3^{2^n} - 1$, [laut Induktion: $n = 0$ ✓, $n \to n+1$: $3^{2^{n+1}} - 1 = (3^{2^n} - 1) \cdot (3^{2^n} + 1) \equiv 0 \; (2^{n+1})$.] gilt $\gamma(abc) \leq 3 \cdot 2 \cdot \frac{c}{2^n} < 6 \cdot \frac{3^{2^n}}{2^n}$, aber $a = 3^{2^n} > \frac{6 \cdot 3^{2^n}}{2^n}$ für $n \geq n_0$.
(Faktor in a; $< c$; restliche Faktoren in c)

14.10. **Kor. (abc):** Fermats großer Satz mit hinr. großen Exponenten:
$\exists n_0 \; \forall n \geq n_0 : x^n + y^n = z^n$ hat keine nichttriviale Lösung $(x,y,z) \in \mathbb{Z}^3$.

Bew.: Sonst sei $(x,y,z) \in \mathbb{Z}^3$ nichttriv. mit $x^n + y^n = z^n$, $(x,y,z) = 1$.
Dann: $a = |x|^n$, $b = |y|^n$, $c = |z|^n \overset{abc}{\Rightarrow} \max\{|x^n|, |y^n|, |z^n|\} \leq C(\varepsilon) \gamma(xyz)^{1+\varepsilon} \leq C(\varepsilon) |xyz|^{1+\varepsilon}$,
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 $n \leq \lceil 3 \frac{\log C(\varepsilon)}{\log 2} + 3 + 3\varepsilon \rceil =: n_0(\varepsilon)$. Nun setze $n_0 := \min_{\varepsilon > 0} n_0(\varepsilon)$ für den $\forall$. □

14.11. **Kor. (abc):** Fermat-Catalan-Gleichung:
Die Gleichung $x^p + y^q = z^r$ mit $p,q,r \in \mathbb{N}$, $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$
hat nur endlich viele Lösungen in $(x,y,z) \in \mathbb{N}^3$, $(x,y,z) = 1$.

Bew.: Betr. für eine Lösung $a = x^p$, $b = y^q$, $c = z^r$
$\overset{abc}{\Rightarrow} z^r = \max\{x^p, y^q, z^r\} \leq C(\varepsilon) \gamma(xyz)^{1+\varepsilon} \leq C'(\varepsilon) (xyz)^{1+\varepsilon}$.
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 $z^r \leq C(\varepsilon) z^{\frac{41}{42} r (1+\varepsilon)}$,
mit $\varepsilon = \frac{1}{83}$ folgt $z \leq C \cdot (\frac{1}{83})^{83}$. □

14.12. **Bem.:** • Als Catalan-Gleichung bezeichnet man $x^p - y^q = 1$ für $x,y,p,q \in \mathbb{N}$, $p,q \geq 2$. Die Catalan-Vermutung besagt, dass $3^2 - 2^3 = 1$ die einzige Lösung dieser Glg. ist. Dies wurde 2004 von Mihăilescu bewiesen (mit recht klassischen algebraischen ZT-Methoden).
• Aus der abc-Vermutung folgt auch eine entsprechende Version für die Glg. $Ax^p + By^q = Cz^r$, die noch allgemeiner als die Fermat-/Catalan-/Fermat-Catalan-Glg. ist.

Weitere spezielle diophantische Gleichungen können mit verschiedenen Methoden behandelt werden. Wir geben eine kleine Auswahl.

14.13. **Satz:** Die diophantische Gleichung $x^3+5=117y^3$ hat keine Lösung $(x,y)\in\mathbb{Z}^2$.

Bew.: Falls eine Lösung (x,y) ex., und da $9\mid 117$, muss $9\mid x^3+5$ gelten, was unmöglich ist wegen $x^3+5\equiv 4,5,6\ (9)$ [modulare Tafel mod 9; Kuben mod 9: $0,\pm 1$] □

14.14. **Satz:** Es gibt unendlich viele nat. Zahlen, die auf zweierlei Weisen die Summe von zwei Kuben sind, wie z.B. $1729=1^3+12^3=9^3+10^3$ (die kleinste solche Zahl, vgl. die berühmte Anekdote über Hardy/Ramanujan, nach der solche "Taxizahlen" genannt werden).

Filmtipp: "The man who knew infinity" / dt. "Die Poesie des Unendlichen" (Film, 2016)

Bew.: Klar nach Ramanujans Identität

$$(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3=(-5a^2+5ab+3b^2)^3+(6a^2-4ab+4b^2)^3.$$ □

14.15. **Satz:** Die einzigen Lösungen $(x,y,z)\in\mathbb{Z}^3$ von $x+y+z=x^3+y^3+z^3=3$ sind $(1,1,1)$, $(-5,4,4)$, $(4,-5,4)$, $(4,4,-5)$.

Bew.: Die Identität $(x+y+z)^3-(x^3+y^3+z^3)=3(x+y)(x+z)(y+z)$ zeigt: Sind x,y,z ganze Zahlen mit $x+y+z=3=x^3+y^3+z^3$, so gilt

$$8=(x+y)(x+z)(y+z)=(3-x)(3-y)(3-z) \qquad (\otimes)$$

so dass $8=(3-x)(3-y)(3-z)$.

Damit folgt, dass jede der drei Zahlen $3-x$, $3-y$, $3-z$ gerade, oder genau eine von ihnen gerade ist.

Im ersten Fall sind diese im Betrag $=2$ wegen $(\otimes)$, also auch $=2$, d.h. $x=y=z=1$.

Im zweiten Fall, wegen $(\otimes)$, ist eine der drei Zahlen im Betrag $=8$, die anderen im Betrag $=1$. Somit ist dann eine davon $=8$, die anderen $=-1$. Dies zeigt letztlich $x=-5, y=z=4$, oder $x=y=4, z=-5$, oder $x=4, y=-5, z=4$. Wir haben damit genau die 4 angeg. Lösungen. □

14.16. **Satz:** Die Gleichung $x^2=y^3+z^5$ hat unendlich viele Lösungen $(x,y,z)\in\mathbb{Z}^3$.

Bew.: Es genügt, für $n\in\mathbb{N}$ die Tripel $x=n^{10}(n+1)^8$, $y=n^7(n+1)^5$, $z=n^4(n+1)^3$ zu betrachten, für die die Gleichung erfüllt ist:

$$x^2=n^{20}(n+1)^{16}=n^{20}(n+1)^{15}\cdot(n+1)=n^{21}(n+1)^{15}+n^{20}(n+1)^{15}=y^3+z^5.$$ □

14.17. **Satz:** Weder die Gl.g. $3^a + 1 = 5^b + 7^c$ noch $5^a + 1 = 3^b + 7^c$ hat eine Lösung $(a,b,c) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$.

Bew.: Ist $a \neq 0$, ist keine der beiden Gleichungen modulo 3 lösbar (modulare Brille mod 3). □

14.18. **Bem.:** • Der 4-Quadratesatz von Lagrange kann als Spezialfall eines allgemeineren Problems aufgefasst werden:

Waringsches Problem: Existiert zu jedem $k \in \mathbb{N}$ ein $g(k) \in \mathbb{N}$, so dass jedes $n \in \mathbb{N}$ als Summe $\sum_{i=1}^{g(n)} x_i^k$ von $\leq g(k)$ vielen k-ten Potenzen mit $x_1, \dots, x_{g(n)} \in \mathbb{N}_0$ dargestellt werden kann? (E. Waring behauptete im Jahr 1770 ohne weiteren Kommentar $g(2)=4$, $g(3)=9$, $g(4)=19$ usw.)

• Der erste allgemeine Beweis der Existenz eines $g(k)$ für alle $k \in \mathbb{N}$ wurde 1909 von D. Hilbert gegeben. Der 4-Quadratesatz zeigt $g(2)=4$. Wieferich/Kempner zeigten 1909/12, dass $g(3)=9$, wobei nur die Zahlen 23 und 239 genau 9 Kuben zur Darstellung benötigen. Für $k \leq 7$ wurden bislang die vermuteten Werte für $g(k)$ bestätigt.

• Folgender analytische Ansatz ist im Waring-Problem gewinnbringend.

Sei $S_k(\alpha) := \sum_{m \leq n^{1/k}} \exp(2\pi i \alpha m^k)$ für $k \in \mathbb{N}$, $\alpha \in \mathbb{R}$.

Dann gilt für alle $s, n \in \mathbb{N}$, dass $R_{k,s}(n) := \#\{(x_1, \dots, x_s) \in \mathbb{N}^s ;\ x_1^k + \dots + x_s^k = n\}$

$$= \int_0^1 S_n^s(\alpha) \exp(-2\pi i \alpha n)\, d\alpha.$$

Eine genaue Analyse des $\int$ (die sogenannte Kreismethode nach Hardy/Littlewood, 1919/20) führt zur Lösung des Waringschen Problems wie folgt:

14.19. **Satz** (Hardy/Littlewood): Sei $k \geq 2$. Ist $s \geq 2^k + 1$, dann ist

$$R_{k,s}(n) \underset{\text{asymptotisch}}{\sim} \frac{\Gamma^s(1+\frac{1}{k})}{\Gamma(\frac{s}{k})} \cdot \mathfrak{S}_{k,s}(n)\, n^{s/k - 1} \quad \text{für } n \to \infty,$$

wobei Γ die Gammafunktion bezeichnet, und $\mathfrak{S}_{k,s}(n) \geq c_1(k,s) > 0$ die singuläre Reihe des Waring-Problems. [o.B.]

14.20. **Bem.:** • Somit ist für die angegebenen k, s die Darstellungsanzahl $R_{k,s}(n)$ für alle hinreichend großen n positiv.

• Man beachte die u.S. für s, die es geben muss: denn für $s=2$ und $k \geq 3$ beinhaltet das Waring-Problem genau das Fermat-Problem.