Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Uni
K. Halupczok

Z1: Die Fermatsche Vermutung

Stichworte: Algebraische ZT: Einführung anhand der Fermatschen Vermutung, pythagoräische Tripel, indische Formeln, Beitrag von Kummer zur F.V., Kummersches Lemma

---

1.1. **Einleitung:**
Wir behandeln in dieser Vorlesung die Anfangsgründe der algebraischen Zahlentheorie. Das gängige Grundlagenwissen aus der Vorlesung "Algebra" wird vorausgesetzt. Das aus einer Vorlesung "Einführung in die ZT" z.T. bekannte Wissen, wie z.B. das Zerlegungsverhalten von Gaußschen Primzahlen im Zahlring $\mathbb{Z}[i]$, soll vertieft und verallgemeinert werden, ist aber keine unmittelbare Voraussetzung, da wir hier den algebraischen Zugang verfolgen. Algebraische Methoden stehen dabei im Fokus. Wir behandeln als erstes die fermatsche Vermutung als Einstieg:

1.2. Fermat (1601-1665): „Die Gleichung $x^n + y^n = z^n$ hat für $n \geq 3$ keine ganzzahlige Lösung (x,y,z) mit $x \cdot y \cdot z \neq 0$." Heute: Satz von Taylor-Wiles / Großer Fermatscher Satz (engl. Fermat's last theorem). ~ vgl. S. Singh "Fermats letzter Satz", 2000.
Die Bemühungen, diesen Satz zu beweisen, waren stets ein Motor zur Entwicklung der algebraischen Zahlentheorie.

1.3. Es genügt, die Unlösbarkeit für $n=4$ und $n=p \geq 3$ prim zu beweisen.
⌜Ist $n = mp$ mit $p \geq 3$ prim, so ist $(x^m)^p + (y^m)^p = (z^m)^p$ zu lösen, ansonsten ist $n = 4m$, also $(x^m)^4 + (y^m)^4 = (z^m)^4$ zu lösen.⌟
$n=4$: Unlösbarkeit von Fermat bewiesen. ⌜Vgl. Einf. ZT: EZ 14.6 / "Methode des unendlichen Abstiegs"⌟
$n=3$: Unlösbarkeit von Euler bewiesen. ⌜Vgl. Satz 1.18⌟
Vollständig bewiesen: 1995 von Taylor und Wiles.
$n=2$: Die ganzzahligen Lösungen (x,y,z) von $x^2 + y^2 = z^2$ mit $x,y,z \neq 0$ heißen pythagoräische Tripel. Ein pyth. Tripel heißt primitiv, falls x,y,z keinen gemeinsamen Teiler $\neq \pm 1$ haben.
Ist (x,y,z) ein primitives pyth. Tripel, so sind je zwei seiner Komponenten teilerfremd. ⌜klar⌟

1.4. **Bestimmung sämtlicher primitiver pyth. Tripel** (x,y,z):
Betr. (*) $x^2+y^2=z^2$ mod 4, d.h. wenden den Hom. $\mathbb{Z}\to\mathbb{Z}/4$ an:
Die einzigen Quadrate mod 4 sind 0 und 1.
Somit ist genau eine der Zahlen x,y gerade. ("Modulare Brille" mod 4)

Sei also $2 \mid y$. In $\mathbb{Z}[i]=\{a+bi;\ a,b\in\mathbb{Z}\}$, dem Ring der Gaußschen Zahlen, gilt: $z^2=x^2+y^2=(x+yi)(x-yi)$,
beachte: $\mathbb{Z}[i]$ ist faktoriell. (vgl. auch Z4)
Erinn.: Integritätsbereich: kommut. nullteilerfreier Ring $R\neq 0$ mit 1. Ein ID R heißt faktoriell, falls jedes $a\neq 0$ eine (bis auf Einheiten) eind. PFZ in irred. Elemente besitzt.

1.5. Beh.: $x+yi$ und $x-yi$ sind teilerfremd in $\mathbb{Z}[i]$ (für $xy\neq 0$, $2\mid y$, (x,y,z) pr.prim.)
Bew.: Sonst: $\exists\,\pi\in\mathbb{Z}[i]$ prim: $\pi\mid(x+yi)$ und $\pi\mid(x-yi)$.
Also: $\pi\mid 2yi$, und da $\mathbb{Z}[i]^\times=\{\pm 1,\pm i\}$ (vgl. Z6), folgt $\pi\mid 2y$.
Da π prim, folgt $\pi\mid 2$ oder $\pi\mid y$, also ist in jedem Fall $\pi\mid y$, da $2\mid y$.
Da $\pi\mid z$, sind y,z nicht teilerfremd in $\mathbb{Z}[i]$.
Nach Lemma 1.6. folgt: y,z nicht teilerfremd in $\mathbb{Z}$,
$\lightning$ zu (x,y,z) primitives pyth. Tripel. □

1.6. **Lemma:** Seien $A\subseteq B$ faktorielle Integritätsbereiche,
$u,v\in A$ in A teilerfremd. Dann gilt:
(a) Ist A ein HIB (Hauptidealbereich), dann sind u,v teilerfremd in B.
(b) Ist A kein HIB, sind u,v in B i.a. nicht teilerfremd.
Bew.: (a): Sei $t\in B$, $t\mid u$, $t\mid v$, d.h. $\exists\,a,b\in B: u=at,\ v=bt$.
Da u,v in A teilerfremd und A ein HIB, ist $Au+Av=A\cdot 1=A$ ("Bezout"),
d.h. $\exists\,x,y\in A: 1=xu+yv$. Es folgt $xat=xu=1-yv=1-ybt$,
d.h. $(xa+yb)t=1$, also ist $t\in B^\times$, und somit sind u,v auch in B teilerfremd.
(b): Betr. $A:=K[XZ,YZ]$, $B:=K[X,Y,Z]$, wo K Körper, X,Y,Z Unbestimmte. Dann ist A kein HIB. Sei $u:=XZ$, $v:=YZ$. Sei $t\in A$, $t\mid u,t\mid v\Rightarrow t\in K^\times=A^\times$, d.h. u,v teilerfr. in A.
Aber in B gilt: $t:=Z$ teilt u und v, und $t\notin B^\times=K^\times$, d.h. in B sind u,v nicht teilerfremd. □

1.7. Betr. die PF z $z^2 = \pi_1^{2e_1} \cdots \pi_s^{2e_s} = (x+yi)(x-yi)$ in $\mathbb{Z}[i]$.
Folgerung: $\exists\, \alpha \in \mathbb{Z}[i],\ \varepsilon \in \mathbb{Z}[i]^\times$: $x+yi = \varepsilon \alpha^2$. [$\pi_j^2 \mid (x+yi)(x-yi)$ $\Rightarrow \pi_j^2 \mid (x+yi)$ oder $\pi_j^2 \mid (x-yi)$]
Schreiben $\alpha = u+vi$ mit $u, v \in \mathbb{Z}$.
Dann ist $\alpha^2 = (u^2-v^2) + 2uvi$, also $x+yi = \varepsilon((u^2-v^2)+2uvi)$.
Da x ungerade, ist $\varepsilon = \pm 1$ [sonst: $x = \pm 2uv$ ↯]
Es folgt für $u, v \in \mathbb{Z}$:

$$\boxed{\begin{aligned} x &= \pm(u^2-v^2) \\ y &= \pm 2uv \\ z &= \pm(u^2+v^2) \end{aligned}}$$

„indische Formeln" (**)

[$z^2 = x^2+y^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = (u^2+v^2)^2$.]

1.8. Bsp.: Primitive pyth. Tripel sind (3,4,5), (15,8,17), (5,12,13), (35,12,37), (21,20,29), (7,24,25), (63,16,65), ...

1.9. Satz: (a) Zu jedem primitiven pyth. Tripel (x,y,z) mit $2 \mid y$ gibt es $u, v \in \mathbb{Z}$ mit (**). [= ind. Formeln]
(b) Für $u, v \in \mathbb{Z} \setminus \{0\}$ mit $v \neq \pm u$ def. (**) ein pyth. Tripel.
Bew.: (a): vgl. 1.7, (b): Seien $u, v \in \mathbb{Z} \setminus \{0\}$, $v \neq \pm u$, x, y, z wie in (**).
Dann ist $x^2+y^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = (u^2+v^2)^2 = z^2$, also (x,y,z) mit $x \cdot y \cdot z \neq 0$ ein pyth. Tripel. □

1.10. Sei nun $n = p > 3$, betrachten $x^p + y^p = z^p$, p prim.
Annahme: $\exists$ Lösung $x, y, z \in \mathbb{Z} \setminus \{0\}$, dabei seien $0 \neq x, y, z$ teilerfremd.
Fall 1: $p \nmid xyz$.
Versuchen $x^p + y^p = z^p$ in Faktoren zu zerlegen.
Ansatz von Kummer (1810–1893): Arbeiten im Ring $\mathbb{Z}[\omega]$ mit $\omega = e^{\frac{2\pi i}{p}}$.
Haben: $\mathbb{Z}[\omega] = \bigoplus_{i=0}^{p-2} \mathbb{Z}\omega^i$ (vgl. 2.9). Wegen $T^p - 1 = \prod_{i=0}^{p-1} (T - \omega^i)$ ⊕ gilt

$$(1)\quad z^p = x^p + y^p = (-y)^p \cdot \left(\left(\tfrac{x}{y}\right)^p - 1\right) = (-y)^p \prod_{i=0}^{p-1} \left(-\tfrac{x}{y} - \omega^i\right) = (x+y)(x+y\omega)\cdots(x+y\omega^{p-1}).$$

1.11. Nehmen jetzt zusätzlich an: $\mathbb{Z}[\omega]$ ist faktoriell.
Bem.: Dies ist nichtig genau wenn $p \leq 19$. [Vgl. mit Z15.]

1.12. Beh.: Für $i \not\equiv j \bmod p$ sind $x+y\omega^i$ und $x+y\omega^j$ teilerfremd in $\mathbb{Z}[\omega]$. (2)
Bew.: Sei o.E. $i<j$. Annahme: $\exists$ gemeinsamer Primfaktor $\pi \in \mathbb{Z}[\omega]$.
Dann: $\pi \mid y(\omega^j - \omega^i) = y(\omega^{j-i}-1)\omega^i \Rightarrow \pi \mid y(1-\omega^{j-i})$.
(ω^i: Einheit)
Betr. nun
$$T^{p-1} + \dots + T + 1 = \prod_{\ell=1}^{p-1} (T-\omega^\ell) \text{ in } \mathbb{Q}(\omega).$$ [$\oplus$ durch $T-1$]
Somit: $\pi \mid y \prod_{\ell=1}^{p-1}(1-\omega^\ell) = yp$, d.h. $\pi \mid p$ oder $\pi \mid y$,
also ist $\pi \mid p$, da $\pi \mid z$ und y, z teilerfremd, vgl. Lemma 1.6.
Wegen $\pi \mid z$ und p, z teilerfremd ist dies ein $\lightning$. □

1.13. Folgerung: Jeder Faktor $x+y\omega^i$ in (1) ist von der Form
(3) $\quad x+y\omega^i = u\alpha^p$, $\alpha \in \mathbb{Z}[\omega]$, $u \in \mathbb{Z}[\omega]^\times$. [Vgl. 1.7]

1.14. Kummersches Lemma: Für jede Einheit $u \in \mathbb{Z}[\omega]^\times$ ist $\frac{u}{\bar{u}}$ eine Potenz von ω,
dabei bezeichnet $\bar{u}$ das konjugiert Komplexe von u. Bew.: s. Z2.

1.15. Beh.: $x \equiv y \ (p)$. (4)
Bew.: Betr. (3) mod p, d.h. in $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]p$.
Sei $\pi : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\mathbb{Z}[\omega]p$.
[Für $\mathbb{Z}[\omega] \ni \beta = b_0 + b_1\omega + \dots + b_{p-2}\omega^{p-2}$ gilt:
$\beta \in \mathbb{Z}[\omega]p \Leftrightarrow \forall i : p \mid b_i$.]
Schreiben $\alpha = a_0 + a_1\omega + \dots + a_{p-2}\omega^{p-2}$, und da die Charakteristik
von $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]p$ gleich p ist, gilt
$$\pi(\alpha^p) = (\pi\alpha)^p = \Big(\sum_{i=0}^{p-2} (\pi a_i)(\pi\omega)^i\Big)^p \overset{\text{char}=p}{=} \sum_{i=0}^{p-2} (\pi a_i)^p = \pi\Big(\underbrace{\sum_{i=0}^{p-2} a_i^p}_{=:a}\Big).$$
Mit anderen Worten: $\alpha^p \equiv a \ (p)$, mit $a \in \mathbb{Z}$.

Also folgt aus (3): $x+y\omega \equiv u a \ (p)$ für ein $a \in \mathbb{Z}$.

Betr. $\pi : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]p$

Konjugation $\downarrow$ $\quad /\!/\!/ \quad \downarrow$

$\hat{\pi} : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]p.$

Da die Konjugation das von p erzeugte Ideal auf sich abbildet, folgt: $x+y\bar{\omega} \equiv \bar{u} a \ (p)$, also $x+y\omega \equiv \frac{u}{\bar{u}}(x+y\bar{\omega}) = \frac{u}{\bar{u}}(x+y\omega^{-1}) \ (p)$.

Nach dem Kummerschen Lemma 1.14 $\exists k, 0 \le k \le p-1 : \frac{u}{\bar{u}} = \omega^k$.

Also ist $x+y\omega \equiv x\omega^k + y\omega^{k-1} \ (p)$, d.h.

$(x+y\omega) - (x\omega^k + y\omega^{k-1}) \in \mathbb{Z}[\omega]\cdot p.$

Nun ist $x\omega^k + y\omega^{k-1} = \begin{cases} x\omega^k + y\omega^{k-1}, & 0 < k < p-1, \\ x - y - y\omega - y\omega^2 - \ldots - y\omega^{p-2}, & k = 0, \\ -x - x\omega - x\omega^2 - \ldots - (x-y)\omega^{p-2}, & k = p-1. \end{cases}$

Folgerung: • $1 < k < p-1$: $p \mid x$ ↯

• $k = 1$: $p \mid (x + y\omega - x\omega - y) = (x-y)(1-\omega) \Rightarrow p \mid x-y$, d.h. (4)

• $k = p-1$: $p \mid x$ ↯ • $k = 0$: $p \mid y$ ↯ □

Wenden (4) noch an auf $(-y)^p = (-z)^p + x^p$ und erhalten $x \equiv -z \ (p)$.

Also ist $2x^p = x^p + x^p \equiv x^p + y^p = z^p \equiv -x^p \ (p)$, also $3x^p \equiv 0 \ (p)$.

Da $p > 3$, ist also $p \mid x$ ↯. Haben gezeigt:

1.16. **Satz:** Ist $p > 3$ so, dass $\mathbb{Z}[e^{2\pi i/p}]$ faktoriell ist, d.h. ist $p \le 19$, so hat $x^p + y^p = z^p$ keine ganzzahlige Lösung (x,y,z) mit $p \nmid xyz$.

1.17. **Bem.:** Behandeln hier den Fall $p \mid xyz$ nicht weiter. Ferner ist der Fall $p = 3$, $p = 3 \nmid xyz$ leicht behandelbar:

1.18. **Satz:** $x^3 + y^3 = z^3$ hat keine ganzzahlige Lsg. $(x,y,z) \in \mathbb{Z}^3$ mit $3 \nmid xyz$.

Bew.: "Modulare Brille" mod 9: Jeder Kubus lässt mod 9 den Rest $0, \pm 1$. Mit Rest $\neq 0$ (9) wäre für $3 \nmid xyz$ also $(\pm 1) + (\pm 1) \equiv \pm 1$ (9), ↯. [$(\pm 1 + 3k)^3 = \pm 1 + 3 \cdot 3k \pm 3 \cdot (3k)^2 + (3k)^3 \equiv \pm 1$ (9)] □