Algebraische Zahlentheorie

Literatur

- D.A. Marcus: Number Fields
- J. Neukirch: Algebraic Number Theory
- S. Lang: "
- A. Fröhlich, M.J. Taylor: "

1. Einführung: Fermats Letzter Satz

Primitive Pythagoräische Tripel

Finde alle ganzzahligen Lsg x, y, z von $x^2 + y^2 = z^2$ mit $\gcd(x,y,z) = 1$.

- Ist (x,y,z) Lsg, so muss z ungerade sein (bekannt. Übl. mod 4)
- Betrachte die Gl in $K = \mathbb{Q}(i)$. Faktorisiere in $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i$ (Gaußsche ganze Zahlen).

$$\Rightarrow (x + yi)(x - yi) = z^2$$

- Algebra: $\mathbb{Z}[i]$ ist euklidisch $\Rightarrow$ HIR $\Rightarrow$ faktoriell

Bem. Es gilt $x + yi = u\alpha^2$ für ein $\alpha \in \mathbb{Z}[i]$ und $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Bew: Genügt z zu: Für jedes Primel $\pi \in \mathbb{Z}[i]$ gilt $\operatorname{ord}_\pi(x+iy) = \max\{a \in \mathbb{N}_0 ; \pi^a \mid x+iy\}$ ist gerade.

Falls $\operatorname{ord}_\pi(x+iy) > 0$, so gilt $\pi \mid z$ und $\operatorname{ord}_\pi(z^2) = 2\operatorname{ord}_\pi(z)$ ist gerade.

Es genügt also zz: $\pi \nmid x - iy$.

Ang $\pi \mid x - iy$.

$\overset{\pi \mid x+iy}{\Rightarrow} \pi \mid 2x$

Es gilt $\operatorname{ggT}(2x, z) = 1 \quad (x \perp z)$

[Denn $2 \nmid z$ und aus $p \mid x$ u. $p \mid z$ folgt $p \mid y$, ↯ zu $\operatorname{ggT}(x,y,z) = 1$]

$\Rightarrow \exists\, a, b \in \mathbb{Z}: 2xa + zb = 1.$

$\Rightarrow \pi \mid 1$, ↯

Die Annahme ist falsch. □

- Schreibe $x + yi = u\alpha^2$, $\alpha = m + ni$,

$= u(m^2 + 2mni - n^2) \qquad m, n \in \mathbb{Z}$

$\Rightarrow \{x, y\} = \{\pm(m^2 - n^2), \pm 2mn\}$, $z = \pm(m^2 + n^2)$

Dabei sind $(m, n) = 1$, $2 \mid mn$.

- Umgekehrt liefert jedes Paar solcher m, n ein pythagoräisches Tripel x, y, z.

Fermats letzter Satz

Sei nun $n \in \mathbb{N}$, $n > 2$.

Die Gleichung

$$x^n + y^n = z^n \qquad (*)$$

hat keine Lösung mit $x, y, z \in \mathbb{Z} \setminus \{0\}$.

- Wurde 1995 bewiesen durch A. Wiles als Folgerung der Shimura-Taniyama-Vermutung.
- Für viele n kann man auch mit elg. $\mathbb{Z}$ argumentieren.
- Fall $n=4$: Übung (*) hat keine Lsg
- $n=3, n>4$:

Genügt $n \geq 3$, dass * keine Lsg hat, falls $n=p$ ungerade Prim ist.
Dann falls $n=a \cdot b$, so ist

$$x^n + y^n = z^n$$
$$\Leftrightarrow (x^a)^b + (y^a)^b = (z^a)^b .$$

- Reicht also $x^p + y^p = z^p$ für ungerade Prim $p \geq 5$.

Angenommen $x, y, z \in \mathbb{Z} \setminus \{0\}$ wird Lsg.
Ziel: Finde Widerspruch.
OBdA: $ggT(x,y,z) = 1$.
Unterscheide 2 Fälle:
1. Fall: p ist coprim zu x, y, z.
2. Fall: p teilt (genau) eine der Zahlen x, y, z.
Wir betr. hier nur den 1. Fall.

Bem: $x^3+y^3=z^3$ hat keine Lg. vom Typ 1.

Bew: $3 \nmid x \Rightarrow x^3 \equiv \pm 1 \pmod 9$

$3 \nmid y \Rightarrow x^3+y^3 \equiv -2, 0, 2 \pmod 9 \quad \not\equiv \pm 1 \pmod 9$. □

Sei nun $p > 3$, (x,y,z) prim Typ 1 Lg von $x^p+y^p=z^p$. (**)

Bem: Sei $\omega = e^{2\pi i/p}$. Dann gilt

$$x^p+y^p = (x+y)(x+y\omega)(x+y\omega^2)\cdot\ldots\cdot(x+y\omega^{p-1}).$$

Bew: Setze $t = -\frac{x}{y}$ in

$$t^p-1 = (t-1)(t-\omega)(t-\omega^2)\cdot\ldots\cdot(t-\omega^{p-1}).$$

Damit wird (**) zur multiplikativen □
Gl.

$$(x+y)(x+y\omega)\cdot\ldots\cdot(x+y\omega^{p-1}) = z^p \qquad (***)$$

ein Ring $\mathbb{Z}[\omega] \subset \mathbb{Q}[\omega]$.

Satz: Angenommen $\mathbb{Z}[\omega]$ ist faktoriell (z.B. für $p=3,5$). Dann hat (**) keine Typ 1 Lg.

Bew: $\mathbb{Z}[\omega]$ faktoriell

$\overset{(***)}{\Rightarrow}$ $x+y\omega = u\alpha^p$ für ein $\alpha \in \mathbb{Z}[\omega]$, $u \in \mathbb{Z}[\omega]^*$.

(Übung)

$p \nmid x, p \nmid y$
$\Rightarrow$ $x \equiv y \ (p)$ (Übung)

Betrachte $x^p + (-z)^p = (-y)^p$
genauso
$\Rightarrow$ $x \equiv -z \ (p)$

$\Rightarrow$ $2x^p \equiv x^p + y^p = z^p \equiv -x^p \ (p)$

$\Rightarrow$ $p \mid 3x^p$

$p > 3, p \nmid x$
$\Rightarrow$ $\lightning$ $\square$

Problem: $\mathbb{Z}[\omega]$ ist oft nicht faktoriell
z.B. für $p = 23$.

Kann man auch in diesen Fällen etwas sagen?

- Wir haben die eindeutige Primfaktorzerlegung benutzt, um $x + y\omega = u\alpha^p$ zu zeigen.
- Geht das auch anders?
- Ja, es geht für „reguläre p" (z.B. 23)

Benutze: • $\mathbb{Z}[\omega]$ ist Dedekindring.
• In Dedekindringen hat jedes Ideal eine eindeutige Faktorisierung in Primideale

$$(x) = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_n^{v_n}$$

$\overset{(***)}{\Rightarrow}$ $(x+y\omega) = I^p$

für ein Ideal $I \subset \mathbb{Z}[\omega]$.

- Falls p reg. PZ, so kann man schließen
  $I = (\alpha)$ ist Hauptideal.
  $\Rightarrow (x+y\omega) = I^p = (\alpha)^p = (\alpha^p)$.
  $\Rightarrow x+y\omega = u\alpha^p$ mit $u \in \mathbb{Z}[\omega]^+$.
  $\overset{p \nmid x, p \nmid y}{\Rightarrow} x \equiv y \ (p)$ (wie vorher)
  $\Rightarrow \lightning$ "

Reguläre PZ:

$\mathfrak{I} := \{ \mathfrak{a} \subset \mathbb{Z}[\omega] \text{ Ideal} \}$ Menge der Ideale

Äquivalenzrelation:

$\mathfrak{a} \sim \mathfrak{b}$, falls $\alpha\mathfrak{a} = \beta\mathfrak{b}$ für geeignete $\alpha, \beta \in \mathbb{Z}[\omega]$.

Satz: Die Menge der Äquivalenzklassen $\mathfrak{I}/\sim$ ist endlich (und hat Kardinalität als ab. Gruppe)

$h := \#\mathfrak{I}/\sim$ heißt Klassenzahl von $\mathbb{Z}[\omega]$ ($h = h(p)$)

Def: Eine PZ p heißt regulär, falls $p \nmid h$.

Gruppenstruktur auf $\mathcal{I}/_{\sim}$:

$$[a] \cdot [b] := [a \cdot b]$$

- ist wohldef.
- Einselement $= [(1)] =$ Klasse des Hauptideals
- Jede Klasse $[a]$ hat Inverses.

Bem: p regulär $\Leftrightarrow$ $\mathcal{I}/_{\sim}$ enthält kein El der Ordnung p.

Folgerung: Ist p reg und I^p Hauptideal, so ist I bereits Hauptideal.

Bew:

$$[I]^p = [I^p] = [(1)]$$

$$\Rightarrow \operatorname{ord}[I] \mid p$$

$$\Rightarrow \operatorname{ord}[I] \mid \operatorname{ggT}(p, h) \overset{p \text{ reg}}{=} 1$$

$$\Rightarrow \operatorname{ord}[I] = 1$$

$$\Rightarrow [I] = [(1)]$$

$$\Rightarrow I = (\alpha) \text{ Hauptideal } \square$$

$\Rightarrow$ (**) hat keine Typ 1 Lsg.

- Ähnlich (etwas komplizierter): Für reg PZ hat (**) keine Typ 2 Zahl.

⇒ Fermats letzter Satz für reg PZ.

Bem: Es gibt so viele irreguläre PZ.
z.B. 37, 59, 67.

Frage: Gibt es so viele reg PZ?
Offen.

Betrachte:

- Zahlkörper $K/\mathbb{Q}$ ($\mathbb{Q}[\omega]$)
- Ganzheitsringe $\mathcal{O}_K/\mathbb{Z}$ ($\mathbb{Z}[\omega]$)
- Primidealzerlegung
- Einheitengruppe $\mathcal{O}_K^*$ / $\mathbb{Z}[\omega]^*$)
- Idealklassengruppe $Cl(K)$ ($\frac{\text{Ideale}}{\text{Hauptideale}}$)

⋮