

Drei-Quadrate-Satz von Gauß

Satz. Eine natürliche Zahl n ist genau dann als Summe dreier Quadratzahlen darstellbar,

$$n = x_1^2 + x_2^2 + x_3^2, \quad x_\nu \in \mathbb{Z},$$

wenn sich n darstellen lässt als

$$n = 4^k m \quad \text{mit } 4 \nmid m \quad \text{und} \quad m \not\equiv 7 \pmod{8}.$$

Satz von Aubry

Satz. Sei $n \in \mathbb{N}_1$. Genau dann besitzt die Gleichung

$$n = x_1^2 + x_2^2 + x_3^2$$

eine ganzzahlige Lösung $(x_1, x_2, x_3) \in \mathbb{Z}^3$, wenn die Gleichung

$$nt^2 = x_1^2 + x_2^2 + x_3^2$$

eine nicht-triviale Lösung $(t, x_1, x_2, x_3) \in \mathbb{Z}^4$ besitzt.

Beweis-Idee für Drei-Quadrate-Satz

Es genügt, den Satz für quadratfreies n zu beweisen.

Man bestimmt eine zu n teilerfremde ganze Zahl $q \geq 1$, die Summe von 2 Quadraten ist, so dass die Legendre-Gleichung

$$nx^2 - qy^2 = z^2 \quad (\star)$$

nicht-trivial lösbar ist.

Erinnerung: $(\star)$ genau dann nicht-trivial lösbar, wenn

- (i) n ist Quadrat modulo q ,
- (ii) $-q$ ist Quadrat modulo n .

Beweis-Idee für Drei-Quadrate-Satz

Fortsetzung

Ist $q = u^2 + v^2$, so erhält man aus $(\star)$

$$nx^2 = (u^2 + v^2)y^2 + z^2 = (uy)^2 + (vy)^2 + z^2$$

und Anwendung des Satzes von Aubry liefert den Drei-Quadrate-Satz.

Im Fall $n \equiv 1, 2 \pmod{4}$ kann man q als Primzahl $p \equiv 1 \pmod{4}$ wählen, im Fall $n \equiv 3 \pmod{8}$ kann man $q = 2p$ mit einer Primzahl $p \equiv 1 \pmod{4}$ wählen.

Beweis-Idee für Drei-Quadrate-Satz

Fortsetzung 2

Genauer:

- Fall $n \equiv 1 \pmod{4}$. Man wählt eine Primzahl p mit
$$p \equiv 2n - 1 \pmod{4n}.$$
- Fall $n \equiv 2 \pmod{4}$. Man wählt eine Primzahl p mit
$$p \equiv n - 1 \pmod{4n}.$$
- Fall $n \equiv 3 \pmod{8}$. Man wählt eine Primzahl p mit
$$p \equiv n - 2 \pmod{4n}$$
und setzt $q := 2p$.

Dabei wird der Dirichletsche Primzahlsatz benutzt.

Beweis-Idee für Drei-Quadrate-Satz

Fortsetzung 3

Um zu zeigen, dass für die so gewählten p, q jeweils die Legendre-Gleichung

$$nx^2 - qy^2 = z^2 \quad (\star)$$

nicht-trivial lösbar ist, wird wesentlich das Quadratische Reziprozitätsgesetz und seine Ergänzungssätze benutzt.