Wiederholung:

Satz 5.12 (Lagrange): Sei $p \in \mathbb{P} \setminus \{2\}$

$$\exists\, x, y \in \mathbb{N} \text{ sodass } x^2 + y^2 = p \iff p \equiv 1 \bmod 4$$

Beweis von Satz 5.12:

$\Rightarrow$: Sei $p = x^2 + y^2$

$$x^2 \equiv 0, 1 \bmod 4$$
$$y^2 \equiv 0, 1 \bmod 4$$
$$\Rightarrow p \equiv 0, 1, 2 \bmod 4$$

aber $p \in \mathbb{P} \setminus \{2\} \Rightarrow p$ ungerade $\Rightarrow p \equiv 1 \bmod 4$.

$\Leftarrow$: Sei $p \equiv 1 \bmod 4$

$\Rightarrow \left(\frac{-1}{p}\right) = 1$ (1. Ergänzungssatz)

$\Rightarrow \exists\, r$ sodass $r^2 \equiv -1 \bmod p$

Sei $e, f := \lfloor \sqrt{p} \rfloor + 1$

Nach Satz 5.13 existieren $0 \le x < e$, $1 \le y < f$

sodass $r \equiv \pm x y^{-1} \bmod p$

also $x, y \le \lfloor \sqrt{p} \rfloor < \sqrt{p}$ $(\sqrt{p} \notin \mathbb{Z})$

$$\Rightarrow -1 \equiv r^2 \equiv x^2 (y^{-1})^2 \bmod p$$
$$\Rightarrow -y^2 \equiv x^2 \bmod p$$
$$\Rightarrow x^2 + y^2 \equiv 0 \bmod p$$

Aber $0 < x^2 + y^2 < 2p$

$$\Rightarrow x^2 + y^2 = p.$$

□

Warum haben wir nur Primzahlen in Satz 5.12 betrachtet?

Bemerkung: $(a^2+b^2)(c^2+d^2) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$

$= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2$

$= (ac+bd)^2 + (ad-bc)^2$

d.h. wenn m und n jeweils als Summe zweier Quadratzahlen darstellbar sind, dann ist auch $m \cdot n$ als Summe zweier Quadratzahlen darstellbar.

Korollar 5.14: Sei $n \in \mathbb{N}$ sodass jeder Primteiler p von n mit $p \equiv 3 \bmod 4$ mit gerader Vielfachheit vorkommt.
Dann ist n als Summe zweier Quadratzahlen darstellbar.

Beweis: Aufgabe.

Es gilt sogar „genau dann wenn"

Satz 5.15: Sei $n \in \mathbb{N}$ und $q_1, \dots, q_k$ die Primteiler von n kongruent 3 mod 4.

n ist Summe zweier Quadratzahlen $\iff \nu_{q_i}(n)$ ist gerade $\forall 1 \le i \le k$

Beweis: Ausgelassen.

Satz 5.16 (Lagrange): Jede natürliche Zahl ist als Summe von vier Quadratzahlen darstellbar.

Für den Beweis brauchen wir folgendes Lemma

Lemma 5.17 (Euler-Identität)

Seien $x_i, y_i \in \mathbb{Z}$ für $1 \le i \le 4$

Dann gilt

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = {} & (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ & + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ & + (x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ & + (x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2\end{aligned}$$

Beweis: Aufgabe (einfach ausmultiplizieren)

Beweis von Satz 5.16:

Es ist $0 = 0^2+0^2+0^2+0^2$

$1 = 1^2+0^2+0^2+0^2$

Wegen der Euler-Identität müssen wir den Satz nur für Primzahlen beweisen,

und wegen $2 = 1^2+1^2+0^2+0^2$ auch nur für ungerade Primzahlen.

Sei also $p \in \mathbb{P} \setminus \{2\}$

- Es gibt $\frac{p+1}{2}$ Quadratzahlen mod p ($\frac{p+1}{2}$ quadratische Reste und 0)
- Und daher auch $\frac{p+1}{2}$ Restklassen der Form $-1-x^2 \bmod p$

Da es insgesamt nur p Restklassen gibt, existiert eine die beide Bedingungen erfüllt

d.h. $\exists x, y \in \mathbb{Z}$ sodass $y^2 \equiv -1-x^2 \bmod p$

$$\Rightarrow x^2+y^2+1 \equiv 0 \bmod p.$$

Wählen wir x, y mit $\frac{-p}{2} < x, y < \frac{p}{2}$, dann gilt

$$0 < x^2+y^2+1 < 3\left(\frac{p}{2}\right)^2 < p^2$$

Also gibt es ein $n \in \mathbb{N}^+$ mit $n<p$ sodass np Summe von drei (also auch Summe von vier) Quadratzahlen ist.

Sei $m \in \mathbb{N}^+$ die kleinste Zahl, sodass mp Summe von vier Quadratzahlen ist. Es gilt $1 \leq m < p$ und wir wollen beweisen, dass $m=1$.

Angenommen $m>1$ und $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ (1)

Sei $x_i \equiv y_i \bmod m$ mit $\frac{-m}{2} < y_i \leq \frac{m}{2}$ für $1 \leq i \leq 4$.

Dann gilt $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \bmod m$

$$\Rightarrow y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m.$$

Also existiert $r \in \mathbb{N}$ sodass

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = rm \qquad (2)$$

und da $\frac{m}{2} < y_i \leq \frac{m}{2}$ ist $rm \leq 4\left(\frac{m}{2}\right)^2 = m^2$

$$\Rightarrow r \leq m.$$

Wir multiplizieren (1) und (2) und erhalten

$$rpm^2 = A^2 + B^2 + C^2 + D^2$$

wobei A, B, C, D die Terme auf der rechten Seite der Euler-Identität sind.

$$A = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \mod m$$
$$\equiv mp \mod m$$
$$\equiv 0 \mod m.$$

$$B = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \equiv x_1 x_2 - x_2 x_1 + x_3 x_4 - x_4 x_3 \mod m$$
$$\equiv 0 \mod m.$$

Ähnlich sind $C, D \equiv 0 \mod m$,

$$\Rightarrow \frac{A}{m}, \frac{B}{m}, \frac{C}{m}, \frac{D}{m} \in \mathbb{Z}$$

und $rp = (A/m)^2 + (B/m)^2 + (C/m)^2 + (D/m)^2$

ist Summe von vier Quadraten

Wir müssen noch zeigen, dass $r \neq 0, m$.

Wäre $r = 0$, dann ist $y_1 = y_2 = y_3 = y_4 = 0$

$\Rightarrow x_1, x_2, x_3, x_4 \equiv 0 \mod m$

$\Rightarrow m^2 \mid mp$ (aus (i))

$\Rightarrow m \mid p$

Wäre $r = m$, dann folgt $y_1 = y_2 = y_3 = y_4 = \frac{m}{2}$

$\Rightarrow x_i = \frac{m}{2} + c_i m$ mit $c_i \in \mathbb{Z}$, $1 \leq i \leq 4$

$\Rightarrow x_i^2 = m^2/4 + c_i m^2 + c_i^2 m^2$

$\equiv \frac{m^2}{4} \mod m^2$

$\Rightarrow mp \equiv 4 (m^2/4) \mod m^2$

$\equiv 0 \mod m^2$

$\Rightarrow m \mid p$

In beiden Fällen gilt $m \mid p$

Und da $1 \leq m < p$ und $p \in \mathbb{P}$ gilt $m = 1$ $\lightning$ $\square$

Kapitel 6 : Diophantische Gleichungen

Def: Eine Diophantische Gleichung ist eine Gleichung der Gestalt

$f(X_1, \ldots, X_n) = 0$

wobei f ein Polynom mit ganzzahlige Koeffizienten ist.

z.B. $10X_1^2 + 3X_1X_2 - 5X_2 + 5 = 0$

$X^2 + Y^2 - Z^2 = 0$ (wir schreiben auch $X^2 + Y^2 = Z^2$)

$X^n + Y^n = Z^n$

$a_1X_1 + a_2X_2 + \ldots + a_nX_n = m$

aber nicht $e^X = Y$

$\frac{X}{4} + 8Y = 0$ (aber $X + 32Y = 0$ ist erlaubt
deswegen ist „ganzzahlig" nicht
restriktiver als „rational")

$\sqrt{2}X^2 - 1 = 0$

Wir suchen ganzzahlige oder rationale Lösungen
Bzw. wir wollen wissen, ob solche Lösungen existieren.

Es kann sein, dass eine diophantische Gleichung rationale Lösungen hat, aber keine ganzzahligen. z.B. $2X = 1$.

Beispiel: Die diophantische Gleichung $a_1 X_1 + \dots + a_n X_n = m$ hat eine ganzzahlige Lösung $\Leftrightarrow$ $ggT(a_1, \dots, a_n) \mid m$.