Hindernisse

Manchmal gibt es einen einfachen Grund, warum keine ganzzahlige Lösung existiert.

Reelle Hindernisse: Hat eine Gleichung keine reellen Lösungen, so hat sie auch keine ganzzahligen bzw. rationalen Lösungen.

Beispiele: $X^2+1=0$ hat keine reellen Lösungen
also auch keine ganzzahligen bzw. rationalen

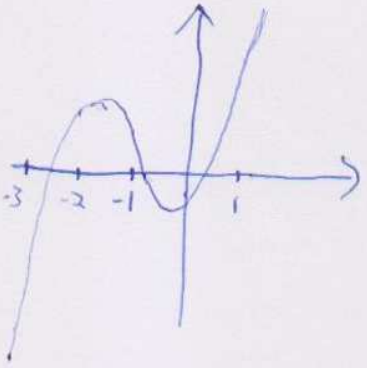
$X^2-XY+Y^2+1=0$ hat keine reellen Lösungen

denn $X^2-XY+Y^2+1=(X-\frac{1}{2}Y)^2+\frac{3}{4}Y^2+1>0$ für $X,Y\in\mathbb{R}$

Wenn alle reelle Lösungen sich in einem Bereich finden, wo es keine ganzen Zahlen gibt, existiert keine ganzzahlige Lösung.

Beispiel: $f(x)=2X^3+5X^2-1=0$

$f(-3)=-10$
$f(-2)=3$
$f(-1)=2$
$f(0)=-1$
$f(1)=6$



die drei Lösungen liegen in $(-3,-2)$, $(-1,0)$ und $(0,1)$

also gibt es keine ganzzahlige Lösung

Hindernisse modulo m: Hat eine diophantische Gleichung keine ganzzahlige Lösung modulo einer natürlichen Zahl m, so hat sie auch keine ganzzahlige Lösung.

Beispiel: $9X^2 - 2Y^2 = 13291$ hat keine ganzzahlige Lösung

denn $13291 \equiv 3 \mod 8$

$$9X^2 \equiv X^2 \equiv 0, 1, 4 \mod 8$$

$$-2Y^2 \equiv 0, -2 \mod 8$$

$$\Rightarrow 9X^2 - 2Y^2 \equiv 0, 1, 2, 4, 6, 7 \mod 8.$$

Die Nichtexistenz solcher Hindernisse ist eine einfache notwendige Bedingung für die Existenz ganzzahliger Lösungen. Allerdings ist diese Bedingung nicht hinreichend

Satz 6.1 (Lind, Reichardt): Die Gleichung $X^4 - 17 = 2Y^2$ hat Lösungen in $\mathbb{R}$ und Lösungen modulo m $\forall m \in \mathbb{N}^+$, aber keine rationalen (insbesondere keine ganzzahligen) Lösungen

Beweis: Ausgelassen (siehe Schmidt)

Proposition 6.2: Die Gleichung $Y^2 = X^3 + 7$ hat keine ganzzahlige Lösung

Beweis: Sei (x, y) eine Lösung

$$y^2 \equiv 0, 1 \mod 4$$

$$\Rightarrow x^3 \equiv y^2 - 7 \equiv 1, 2 \mod 4$$

$\Rightarrow x$ ungerade.

Es ist auch $y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$

$$= (x+2)((x-1)^2 + 3)$$

$(x-1)^2 \equiv 0 \mod 4$ (x ungerade)

$\Rightarrow (x-1)^2 + 3 \equiv 3 \mod 4$

Also hat $(x-1)^2 + 3$ einen Primfaktor p mit $p \equiv 3 \mod 4$

$\Rightarrow y^2 + 1 \equiv 0 \mod p$

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

$\Rightarrow p \equiv 1 \mod 4$ (1. Ergänzungssatz) $\lightning$ □

Bemerkung: Gleichungen der Gestalt $y^2 = x^3 + ax^2 + bx + c$ heissen <u>elliptische Kurven</u> und sind sehr wichtig in der modernen Zahlentheorie

(z.B. Beweis des großen Fermatschen Satzes von Wiles, public-key Verschlüsselung, Primzahltests, Millenniumsprobleme, ...)

Wir betrachten die diophantische Gleichung $X^n + Y^n = Z^n$

Def: Eine ganzzahlige Lösung (x,y,z) der Gleichung $X^2 + Y^2 = Z^2$ mit $x,y,z > 0$ heisst ein <u>Pythagoräisches Tripel</u>

Das Tripel ist <u>primitiv</u> wenn $ggT(x,y,z) = 1$

Satz 6.3 (Euklid): Jedes primitive Pythagoräische Tripel hat die Gestalt

$$x = b^2 - a^2$$
$$y = 2ab$$
$$z = a^2 + b^2$$

mit $a, b \in \mathbb{N}^+$, $a < b$, $(a,b) = 1$ und $a \not\equiv b \bmod 2$

(eventuell nach Vertauschen von x und y)

d.h. die primitiven Pythagoräischen Tripel entsprechen genau den Paaren $(a,b) \in \mathbb{N}^2$ mit $0 < a < b$, $(a,b) = 1$ und $a \not\equiv b \bmod 2$

Wir können also Pythagoräische Tripel leicht konstruieren.

Beweis: Da $ggT(x,y,z) = 1$ sind x,y,z nicht alle gerade

Wären x, y ungerade, dann wäre $x^2 + y^2 \equiv 2 \bmod 4$

aber $z^2 \equiv 0, 1 \bmod 4$ ↯

Also ist (oBdA) x ungerade und y gerade $\Rightarrow z$ ungerade

Es ist $z^2 - x^2 = y^2$

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

$\Rightarrow \frac{z-x}{y} = \frac{y}{z+x}$

Es ist $\frac{z-x}{y} \in \mathbb{Q}$

Sei $\frac{z-x}{y} = \frac{a}{b}$ mit $a, b \in \mathbb{N}^+$
$(a,b) = 1$

$\Rightarrow \frac{z+x}{y} = \frac{b}{a}$

$\frac{z}{y} - \frac{x}{y} = \frac{a}{b}$, $\frac{z}{y} + \frac{x}{y} = \frac{b}{a}$

$\Rightarrow \frac{z}{y} = \frac{1}{2}\left(\frac{a}{b} + \frac{b}{a}\right)$
$= \frac{a^2+b^2}{2ab}$

und $\frac{x}{y} = \frac{1}{2}\left(\frac{b}{a} - \frac{a}{b}\right)$
$= \frac{b^2-a^2}{2ab}$

Es ist $ggT(a,b) = 1$ also sind a, b nicht beide gerade.

Wären beide ungerade, dann ist $\frac{a^2+b^2}{2}$ ungerade
und ab ungerade

$\frac{z}{y} = \frac{\frac{1}{2}(a^2+b^2)}{ab} \Rightarrow 2ab = \frac{1}{2}(a^2+b^2)y$

aber $2ab$ ungerade, $\frac{1}{2}(a^2+b^2)y$ gerade $\lightning$

Also sind a, b nicht beide gerade,

also ist $ggT(a^2+b^2, 2ab) = ggT(a^2+b^2, ab) = 1$

wäre p ein gemeinsamer Primteiler von a^2+b^2 und ab,
dann gilt $p \mid a$ oder $p \mid b$
oBdA $p \mid a \Rightarrow p \mid a^2$
und $p \mid a^2+b^2 \Rightarrow p \mid b^2$
$\Rightarrow p \mid b$
$\Rightarrow (a,b) \geq p > 1$ ↯

und $ggT(b^2-a^2, 2ab) = 1$ ("ähnlich")

Es ist auch $(y,z) = (y,x) = 1$ wäre $d > 1$ ein gemeinsamer Teiler von x und y, so gilt $d^2 \mid x^2+y^2 = z^2$
$\Rightarrow d \mid z$
$\Rightarrow ggT(x,y,z) \geq d > 1$ ↯
für y und z ähnlich.

Also ist
$$x = b^2 - a^2$$
$$y = 2ab$$
$$z = a^2 + b^2$$

mit $(a,b) = 1$ und $a \not\equiv b \bmod 2$. □

Satz 6.4 (Fermat): Die diophantische Gleichung $X^4 + Y^4 = Z^2$
hat keine nicht-trivialen ganzzahligen Lösungen
($x, y, z \neq 0$)

Beweis: Nächstes Mal.