*…cujus rei demonstrationem mirabilem sane detexi.*
*Hanc marginis exiguitas non caperet.*
Pierre de Fermat, *Observation 2. FO.I.291*

---

linear, homogen $ax + by = 0$ $d = (a, b)$

$\left( \frac{a}{d} \mid y \wedge \frac{b}{d} \mid x \right) \Rightarrow x = x_k = k\frac{b}{d} \wedge y = y_k = -k\frac{a}{d}$ $(k \in \mathbb{Z})$

linear, inhomogen $ax + by = c$ lösbar $\Leftrightarrow d \mid c$

$$x = x_s + x_k \wedge y = y_s + y_k$$

*Ermitteln von* $(x_s, y_s)$ : $(x_s, y_s)$ *spezielle Lösung*

(a) Rechnen in $\mathbb{Z}^*_{a/d}$ oder $\mathbb{Z}^*_{b/d}$ *(Indextafel)*

(b) euklidischer Algorithmus *(Kettenbruchentwicklung)*

---

Pythagoräische Tripel $x^2 + y^2 = z^2$ $(k = (x, y, z))$

$(a, b) = 1$ $k^2(a^2 + b^2) = k^2c^2$ *oBdA.* $a \equiv 0$,

$a^2 = c^2 - b^2 = (c + a)(c - a)$ $b \equiv c \equiv 1 \bmod 2$

$a^2 = 4\frac{(c+a)}{2}\frac{(c-a)}{2} = 4r^2s^2$ $((r, s) = 1)$

*daher:* $(\Leftrightarrow)$ $x = k \cdot 2rs,\ y = k \cdot (r^2 - s^2),\ z = k \cdot (r^2 + s^2)$

**Fermatsche Gleichung** $x^n + y^n = z^n$ „Großer Fermatscher Satz“

*(Fermatsche Vermutung)* für $n \geq 3$ nur trivial lösbar

für einige $n$ *(prim)*: Fermat, Euler, … *Fermat's Last Theorem*

*vollständig:* Andrew Wiles 1993, Taylor-Wiles 1994

---

*(Fermat: la descente infini)* $x^4 + y^4 = z^2$ in $\mathbb{N} \setminus \{0\}$ nicht lösbar

lösbar $\Rightarrow x_1^4 + y_1^4 = z_1^2$ mit $z_1 < z$ Widerspruch! ■

*obdA.* $(x, y, z) = 1$ *oBdA.* $x \equiv 0,\ y \equiv z \equiv 1 \bmod 2$

$\Rightarrow$ $x^2 = 2rs \wedge y^2 = r^2 - s^2$ $r \equiv 1, s \equiv 0 \bmod 2$

*also* $x^2 = 2 \cdot 2\frac{s}{2}r = 2(2p^2)q^2$ $(r, s) = (p, q) = 1$

$(r^2 = s^2 + y^2 \Rightarrow)$ $(q^2)^2 = (2p^2)^2 + b^2$ $\Rightarrow 2p^2 = 2m^2n^2$

*und mit:* $q^2 = (m^2)^2 + (n^2)^2$ ■

---

allgemein $P(x_1, x_2, \cdots, x_n) = 0$ (Polynom über $\mathbb{Z}$)

*(10. Hilbert-Problem 1900)* *(Matiyasevich 1970)*

Lösbarkeit ist *(algorithmisch)* nicht entscheidbar,

*d.h.* es gibt kein endliches Verfahren *(Computerprogramm)*,

das für **alle** diophantischen Gleichungen anwendbar ist.

(*Selbst wenn:* Die Anzahl der Lösungen ist *(höchstens)* endlich.)