Wiederholung:

Satz 6.4 (Fermat) Die diophantische Gleichung $X^4 + Y^4 = Z^2$ hat keine nicht-trivialen ganzzahligen Lösungen

Für den Beweis verwenden wir die Methode des unendlichen Abstiegs: Angenommen es gibt eine Lösung, konstruieren wir daraus eine „kleinere" Lösung.

Setzen wir das Argument immer wieder fort, so bekommen wir immer wieder „kleinere" Lösungen, in Widerspruch zum Satz vom kleinsten Element.

Beweis: Sei (x, y, z) eine ganzzahlige Lösung mit $x, y, z \neq 0$
oBdA ist $ggT(x, y, z) = 1$ und $x, y, z > 0$.

Wie in Satz 6.3 ist (oBdA) x ungerade
y gerade
z ungerade

$y^4 = z^2 - x^4 = (z - x^2)(z + x^2)$ und $x^2 \equiv x \equiv z \bmod 2$

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

(ist $d := ggT(z - x^2, z + x^2)$, so gilt $2 | d$
und $d | (z - x^2 + z + x^2) = 2z \Rightarrow \frac{d}{2} | z$
$\Rightarrow \frac{d}{2} | (z + x^2 - z) = x^2$
$\Rightarrow \frac{d}{2} = 1$, denn $(x, z) = 1$)

Daher gibt es zwei Fälle

1. $z - x^2 = 2a^4$
   $z + x^2 = 8b^4$ $\quad a, b \in \mathbb{N}^+$, a ungerade, $(a,b) = 1$

2. $z - x^2 = 8b^4$
   $z + x^2 = 2a^4$ $\quad a, b \in \mathbb{N}^+$, a ungerade, $(a,b) = 1$

Im Fall 1 gilt $2x^2 = 8b^4 - 2a^4$

$\Rightarrow x^2 = 4b^4 - a^4$

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

$4b^4 \equiv 0 \mod 4$

$-a^4 \equiv -1 \mod 4$ (a ungerade) ↯

Im Fall 2 gilt $2z = 2a^4 + 8b^4$

$\Rightarrow z = a^4 + 4b^4$ also $0 < a < z$

$\Rightarrow (a^4 + 4b^4) - x^2 = 8b^4$

$a^4 - x^2 = 4b^4$

$(a^2 - x)(a^2 + x) = 4b^4$

Wäre $m \in \mathbb{N}^+$ ein Teiler von a und x, so gilt

$m \mid a^2 - x \Rightarrow m \mid 4b^4$

$\Rightarrow m \mid b^4$ (x ungerade $\Rightarrow$ m ungerade)

$\Rightarrow m = 1$ (da $(a,b) = 1$)

$\Rightarrow (a, x) = 1$.

$\Rightarrow ggT(a^2-x, a^2+x) = 2$ (Argument wie oben)

Also ist $a^2-x = 2c^4$, $a^2+x = 2d^4$ für $c,d \in \mathbb{N}^+$ $(c,d)=1$.

Dann ist $2a^2 = 2c^4 + 2d^4$

$$c^4 + d^4 = a^2$$

mit $ggT(a,c,d)=1$ und $0<a<z$

Argumentieren wir rekursiv, dann erhalten wir eine unendliche absteigende Folge von natürlichen Zahlen. ↯ □

$z > a > \dots$

Korollar 6.5: Die Gleichung $X^4+Y^4=Z^4$ hat keine nicht-triviale ganzzahlige Lösung

Beweis: Wäre (x,y,z) eine Lösung, so ist (x,y,z^2) eine Lösung zu $X^4+Y^4=Z^2$ □

Satz 6.6 (Wiles, 1995): Die Gleichung $X^n+Y^n=Z^n$ hat keine nicht-triviale ganzzahlige Lösung für $n \in \mathbb{N}$, $n \geq 3$.

Beweis: Ausgelassen.

Bemerkung: Sei $n = pm$ für $p \in \mathbb{P} \setminus \{2\}$, $m \in \mathbb{N}^+$

Dann gilt $x^n + y^n = z^n \iff (x^m)^p + (y^m)^p = (z^m)^p$

Oder sei $n = 4k$

Dann gilt $x^n + y^n = z^n \iff (x^k)^4 + (y^k)^4 = (z^k)^4$

Es würde also reichen, die Aussage für ungerade Primzahlen und $n = 4$ zu beweisen

(und $n = 4$ haben wir schon bewiesen)

Wir sehen einen Ansatz von Sophie Germain für ungerade Primzahlen.

Def: Eine <u>Sophie-Germain-Primzahl</u> ist eine ungerade Primzahl p sodass $2p+1 \in \mathbb{P}$.

Satz 6.7 (Sophie Germain): Sei p eine Sophie-Germain-Primzahl.

Dann hat die Gleichung $X^p + Y^p = Z^p$ keine ganzzahlige Lösung (x, y, z) mit $p \nmid xyz$

Beweis: Die Gleichung $X^p + Y^p = Z^p$ hat eine ganzzahlige Lösung (x, y, z) mit $p \nmid xyz$ genau dann, wenn

$X^p + Y^p + Z^p = 0$ eine solche Lösung hat

(da p ungerade ist, gilt $(-z)^p = -z^p$)

Angenommen es gäbe eine solche Lösung von $X^p + Y^p + Z^p = 0$, (x, y, z).

Wir dürfen annehmen, dass $ggT(x, y, z) = 1$, also sind x, y, z paarweise teilerfremd.

Es ist $-x^p = y^p + z^p = (y+z)(z^{p-1} - z^{p-2}y + z^{p-3}y^2 - \dots + y^{p-1})$

Sei r ein gemeinsamer Primteiler von $y+z$ und $(z^{p-1} - z^{p-2}y + \dots + y^{p-1})$

$$p \nmid x \Rightarrow p \nmid x^p \Rightarrow p \nmid y+z$$
$$\Rightarrow (r, p) = 1$$

$$y + z \equiv 0 \mod r$$
$$\Rightarrow y \equiv -z \mod r$$

und $z^{p-1} - z^{p-2}y + \dots + y^{p-1} \equiv 0 \mod r$

$$\Rightarrow \underbrace{z^{p-1} + z^{p-1} + \dots + z^{p-1}}_{p} \equiv 0 \mod r$$

$$p z^{p-1} \equiv 0 \mod r$$

$$\Rightarrow z^{p-1} \equiv 0 \mod r \quad (r, p) = 1$$

$\Rightarrow r \mid pz \quad (r \in \mathbb{P})$

$\Rightarrow r \mid (z+y-z) = y \quad \lightning \quad (z,y) = 1.$

$\Rightarrow ggT(y+z,\ z^{p-1} - z^{p-2}y + \dots + y^{p-1}) = 1.$

also $y+z = A^p$

$z^{p-1} - z^{p-2}y + \dots + y^{p-1} = T^p$ mit $A, T \in \mathbb{Z}$ und $(A,T) = 1$

Analog erhalten wir $x+y = B^p$

$x+z = C^p$

mit $B, C \in \mathbb{Z}$

Es ist $p = \frac{q-1}{2}$ für $q \in \mathbb{P}$ also gilt

$$x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} \equiv 0 \mod q$$

Angenommen $q \nmid xyz$

Nach dem kleinen Fermatschen Satz gilt $x^{\frac{q-1}{2}} \equiv \pm 1 \mod q$

$y^{\frac{q-1}{2}} \equiv \pm 1 \mod q$

$z^{\frac{q-1}{2}} \equiv \pm 1 \mod q$

$\Rightarrow x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} \equiv -3, -1, 1, 3 \mod q$

$\not\equiv 0 \mod q$ für $q > 3$ $\lightning$ $(q = 2p+1 \geq 7)$

Also gilt (oBdA) $q \mid x$

Es ist $B^p + C^p - A^p = (x+y) + (x+z) - (y+z) = 2x$

$\Rightarrow \quad B^p + C^p - A^p \equiv 0 \mod q$

Also gilt auch $q \mid ABC$ (gleiches Argument wie oben mit xyz)

Es gilt $q \mid x$ und $(x,y)=1$

$\Rightarrow q \nmid x+y = B^p$

$\Rightarrow q \nmid B$

ähnlich gilt $q \nmid C$

$\Rightarrow q \mid A$

Also $-y \equiv z \mod q$

$\Rightarrow T^p = z^{p-1} - z^{p-2}y + \dots + y^{p-1} \equiv p y^{p-1} \mod q$

$B^p = x+y \equiv y \mod q$

$\Rightarrow y^{p-1} \equiv (B^{p-1})^p \mod q$

Es ist $T \not\equiv 0 \mod q$ $\quad (A,T)=1$

$\Rightarrow T^p \equiv p y^{p-1} \equiv p (B^{p-1})^p \mod q$

$T^{\frac{q-1}{2}} \equiv p (B^{p-1})^{\frac{q-1}{2}} \mod q$

$\Rightarrow \pm 1 \equiv \pm p \mod q$ $\quad \lightning$ $\quad q = 2p+1$

Also gibt es keine solche Lösung (x,y,z) $\square$

Bemerkung: Mit etwas mehr Arbeit und einer allgemeineren Bedingung als $2p+1 \in \mathbb{P}$, hat Sophie Germain den großen Fermatschen Satz für alle Primexponenten < 100 beweisen können.

Frage: Gibt es unendlich viele Sophie-Germain-Primzahlen?

Unbekannt.