1 The case $x^4+y^4 = z^4$ and Sophie Germain's Theorem

Satz 1 (1.Satz von Sophie Germain)**.** *Ist p Prim und $a \in \mathbb{N}$ teilerfremd zu p, so gilt:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Definition 2. *Eine Primzahl p heisst Sophie-Germain-Primzahl (SGP), wenn sie ungerade ist und auch $q = 2p + 1$ eine Primzahl ist.*

Beispiel 3. *p=3 und q=7* $\rightarrow 3 \in SGP$
p=7 und q=15, $q \notin Prim \rightarrow 7 \notin SGP$

Theorem 4. *Sei p eine SGP. Dann gibt es keine Lösung der Gleichung*

$$x^p + y^p + z^p = 0$$

für $x, y, z \in \mathbb{Z}$ mit $p \nmid xyz$ und x, y, z paarweise teilerfremd.

Beweis. Sei $q = 2p + 1$, (x, y, z) eine nichttriviale Lösung.
Aus $x^p + y^p + z^p = 0 \Rightarrow x^p + y^p = -z^p = xy^{p-1} - x^2y^{p-2} + \cdots - x^{p-1}y + x^p + y^p - xy^{p-1} + x^2y^{p-2} + \cdots + x^{p-1}y = x(y^{p-1} - xy^{p-2} + \cdots x^{p-1}) + y(y^{p-1} - xy^{p-2} + \cdots x^{p-1}) = (x + y)\underbrace{(y^{p-1} - xy^{p-2} + \cdots x^{p-1})}_{\alpha}$ wegen $p \nmid z$ gilt $p \nmid (x + y)$.

Sei r eine Primzahl des ggT von $(x + y)$ und α. Dann gilt $r \neq p$ und $x \equiv -y \pmod{r}$, weil $p \nmid (x + y)$ und $r|(x + y)$.

Daher gilt:
$$\begin{aligned} 0 &\equiv y^{p-1} - xy^{p-2} + \cdots + x^{p-1} \pmod{r} \\ &\equiv y^{p-1} - (-y)y^{p-2} + \cdots + (-y)^{p-1} \\ &\equiv y^{p-1} + y^{p-1} + \cdots + y^{p-1} \pmod{1} \\ 0 &\equiv py^{p-1} \pmod{r} \Leftrightarrow r|py^{p-1} \text{ da } r \nmid p \\ &\Rightarrow r|y \text{ da } r|(x + y) \text{ und } r|y \text{ folgt } r|x \\ &\Rightarrow r|z \text{ WIDERSPRUCH!!!!} \end{aligned}$$

$(-y)^p = x^p + y^p$ und $(-x)^p = y^p + z^p$ analog.[1]

$q = 2p + 1 \Rightarrow q - 1 = 2p$ so $a^{q-1} = \begin{cases} 1 \pmod{q}, & q \nmid a, \\ 0 \pmod{q}, & q \nmid a, q|a. \end{cases}$ ...

Für $q > 3$ gilt: $x^p + y^p + z^p = 0 \equiv 0 \pmod{q}$

- $q|2x = x + y + x + z - y - z = a^p + b^p - c^p \equiv \pmod{q}$

- $q|x$ $a^p = x + y$ wenn $q|a^p \Rightarrow q|y$ WIDERSPRUCH!
  $\Rightarrow q|c^p$

[1] Frage: Warum $x + y = a^p$ für ein $a, t \in \mathbb{Z}$?
Lösung: Primfaktorzerlegung

- $q|(a^p + b^p) = (x + y + x + z) = (2x + y + z) \Rightarrow y + z \equiv 0 \pmod{q}$

$s^p = z^{p-1} - yz^{p-2} + \cdots + y^{p-1} | y \equiv -z \pmod{q} = py^{p-1} \pmod{q}$
$s^p \equiv \pm 1 \pmod{q}, q \nmid y.$

$py^{p-1} \equiv \pm 1 \pmod{q}$

$(-z)^p = (x + y)t^p$ und $\pm 1 \equiv y^p \equiv yt^p \pmod{q}$ mit $q \nmid y$
$q = 2p + 1 \Rightarrow p \not\equiv \pm 1 \pmod{q}$ □

By Kevin Ondo at 11. November 2011