56

Seien m, n beliebige natürliche Zahlen und $p \geq 2$ eine Primzahl. Es ist zu beweisen, dass $m^p - n^p$ zu p teilerfremd oder durch p^2 teilbar ist.

Lösung:

Illustration

p	$m^p - n^p$	$ggT(m^p - n^p, p) = 1$	$p^2 \mid m^p - n^p$
3	$5^3 - 3^3 = 98$	$ggT(98,3) = 1$	nein
4	$5^4 - 4^4 = 369$	$ggT(369,4) = 1$	nein
2	$6^2 - 2^2 = 32$	$ggT(32,2) = 2$	$4 \mid 32$
4	$8^4 - 4^4 = 3840$	$ggT(3840,4) = 4$	$16 \mid 3840$
4	$10^4 - 4^4 = 9744$	$ggT(9744,4) = 4$	$16 \mid 9744$

1. Fall: $p \mid m$ oder $p \mid n$

Es wird angenommen $p \mid m^p - n^p$. Zu zeigen ist, dass $p^2 \mid m^p - n^p$ gilt.

Aus $p \mid m$ folgt, es existiert ein d mit $p \cdot d = m \Rightarrow (p \cdot d)^p = p^p \cdot d^p = p \cdot p^{p-1} \cdot d^p = m^p$.

Aus der Annahme $p \mid m^p - n^p$ folgt, es existiert ein t mit $p \cdot t = m^p - n^p$.

Also gilt wegen $p \mid p \cdot t$ und wegen $p \mid p \cdot p^{p-1} \cdot d^p$

$p \mid m^p - n^p$ und $p \mid m^p$.

Es gilt die Teilbarkeitsregel $a \mid b \wedge a \mid c \Rightarrow a \mid b - c$ wobei $b > c$.

Da $m^p > m^p - n^p$ und $p \mid m^p \wedge p \mid m^p - n^p \Rightarrow p \mid m^p - (m^p - n^p) = p \mid m^p - m^p + n^p = p \mid n^p \Rightarrow p \mid n$.

Es gilt $p \mid m \Rightarrow p^p \mid m^p$ und $p \mid n \Rightarrow p^p \mid n^p$.

Außerdem gilt $p^p \mid m^p \wedge p^p \mid n^p \Rightarrow p^p \mid m^p - n^p \Rightarrow p^2 \mid m^p - n^p$.

Das heißt $m^p - n^p$ ist durch p^2 teilbar.

2. Fall: $p \neg\mid m$ oder $p \neg\mid n$

Aus $p \neg\mid m \Rightarrow p \neg\mid m^p$ und aus $p \neg\mid n \Rightarrow p \neg\mid n^p$.

Da $m^p > n^p$ und $p \neg\mid m^p \wedge p \neg\mid n^p \Rightarrow p \neg\mid m^p - n^p$, und das heißt $m^p - n^p$ ist zu p teilerfremd bzw. $ggT(m^p - n^p, p) = 1$.

Insgesamt gilt also, dass $m^p - n^p$ zu p teilerfremd oder durch p^2 teilbar ist.
Was zu beweisen war.