45

Sei m eine ungerade natürliche Zahl und n eine beliebige natürliche Zahl. Es ist zu beweisen, dass $\text{ggT}(2^m-1, 2^n+1)=1$.

Lösung: Beweis durch Widerspruch

2^ν ist für alle $\nu \in \mathbb{N}_0$ stets eine gerade Zahl, mit Ausnahme von $\nu=0$ ($2^0=1$). Daraus folgt, dass alle $2^\nu-1$ bzw. $2^\nu+1$ für $\nu \geq 1$ ungerade Zahen sein müssen, somit auch sämtliche Teiler dieser Zahlen.

Definiert man $d=\text{ggT}(2^m-1, 2^n+1)$, so folgt, dass auch d eine ungerade Zahl sein muss.

Angenommen, es gelte $d>1$.

Ist $d=\text{ggT}(2^m-1, 2^n+1)$, dann existieren Zahlen x und y, für die gilt: $d\cdot x=2^m-1$ und $d\cdot y=2^n+1$. Aus $d\cdot x=2^m-1$ folgt $d\cdot x+1=2^m$; aus $d\cdot y=2^n+1$ folgt $d\cdot y-1=2^n$.

Potenzieren ergibt:

$$d\cdot x+1=2^m \Rightarrow (d\cdot x+1)^n=(1+dx)^n=(2^m)^n=2^{m\cdot n}=2^{nm}$$

$$d\cdot y-1=2^n \Rightarrow (d\cdot y-1)^m=(-1+dy)^m=(2^n)^m=2^{n\cdot m}=2^{nm}$$

Der binomische Satz für alle natürlichen Zahlen n und alle reellen Zahlen a und b heißt

$$(a+b)^n=\sum_{\nu=0}^{n}\binom{n}{\nu}\cdot a^{n-\nu}\cdot b^\nu$$

Für $a=1, b=dx, \nu=k$ ergibt das

$$(1+dx)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot 1^{n-k}\cdot (dx)^k=\sum_{k=0}^{n}\binom{n}{k}\cdot (dx)^k=1+\sum_{k=1}^{n}\binom{n}{k}\cdot (dx)^k=1+\sum_{k=1}^{n}\binom{n}{k}\cdot d^k\cdot x^k$$

$$=1+\sum_{k=1}^{n}\binom{n}{k}\cdot d\cdot d^{k-1}\cdot x^k=1+d\cdot\sum_{k=1}^{n}\binom{n}{k}\cdot d^{k-1}\cdot x^k$$

Setzt man für $\sum_{k=1}^{n}\binom{n}{k}\cdot d^{k-1}\cdot x^k=v$, so ist $(1+dx)^n=1+d\cdot v$

Für $a=-1, b=dy, \nu=k, n=m$ ergibt das

$$(-1+dy)^m=\sum_{k=0}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot(dy)^k=\binom{m}{0}\cdot(-1)^{m-0}\cdot(dy)^0+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot(dy)^k$$

Da m eine ungerade natürliche Zahl ist, folgt daraus

$$\binom{m}{0}\cdot(-1)^{m-0}\cdot(dy)^0+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot(dy)^k=1\cdot(-1)\cdot 1+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot(dy)^k$$

$$=-1+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot(dy)^k=-1+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot d^k y^k=-1+\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot d\cdot d^{k-1}y^k$$

$$=-1+d\cdot\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot d^{k-1}y^k$$

Setzt man für $\sum_{k=1}^{m}\binom{m}{k}\cdot(-1)^{m-k}\cdot d^{k-1}y^k=w$, so ist $(-1+dy)^m=-1+d\cdot w$

Es gilt nun

$(1+dx)^n=2^{nm}=1+d\cdot v$ und $(-1+dy)^m=2^{nm}=-1+d\cdot w$.

Also $2^{nm} = 1 + d \cdot v$ und $2^{nm} = -1 + d \cdot w$.
Addiert man beide Gleichungen, so erhält man
$2^{nm} + 2^{nm} = (1 + dv) + (-1 + dw)$ also $dv + dw = 2 \cdot 2^{nm} = d \cdot (v + w) = 2 \cdot 2^{nm}$. Das heißt, d ist immer eine gerade Zahl.

Die Annahme $d > 1$ ergibt somit, dass d dann immer eine gerade Zahl ist, was im Widerspruch dazu steht, dass d eine ungerade Zahl sein muss.
Die einzige ungerade Zahl d kann also nur d = 1 sein.

Was zu beweisen war.