Problem 108

Prof. Dr. Manfred Börgens

Technische Hochschule Mittelhessen

Fachbereich Mathematik, Naturwissenschaften und Datenverarbeitung

Stand 2016-05-21

$n \in \mathbf{N}, \quad m \in \mathbf{N}, \; m > 2$

$n \mid 2^n - 1$ **gilt nur für** $n = 1$

$n \mid m^n - 1$ **gilt für unendlich viele** n

Die erste Aussage muss offenbar nur ungerade n in Betracht ziehen.

Annahme: $n \mid 2^n - 1$ gilt für ein ungerades $n > 1$.

d sei der kleinste positive Exponent mit $n \mid 2^d - 1$ bzw. $2^d = 1 \; mod \; n$. Dann gilt $d \mid n$.

(Hinweis: d ist die *multiplikative Ordnung* von $2 \; mod \; n$.)

Begründung: $n = k \cdot d + r, \; 0 \leq r < d \quad \Rightarrow \quad 2^n = (2^d)^k \cdot 2^r \quad \Rightarrow \quad 2^n \; mod \; n =$

$= ((2^d \; mod \; n)^k \cdot (2^r \; mod \; n)) \; mod \; n \quad \Rightarrow \quad 1 = 2^r \; mod \; n$

Wegen $r < d$ ist $r = 0$.

Auch für den kleinsten Primfaktor p von n gilt $p \mid 2^d - 1$ bzw. $2^d = 1 \; mod \; p$.

Nach dem Kleinen Satz von Fermat gilt $2^{p-1} = 1 \; mod \; p$.

Für den kleinsten positiven Exponenten d_1 mit $2^{d_1} = 1 \; mod \; p$ gilt analog zur obigen Argumentation, dass sowohl d als auch $p - 1$ Vielfache von d_1 sind.

$d_1 > 1$ ist also ein Faktor von n, der kleiner ist als p. Dies erzeugt einen **Wid.**, da p der kleinste Primfaktor ist. Die Annahme ist also falsch.

(Quelle: https://web.archive.org/

web/20120104074313/http://www.immortaltheory.com/NumberTheory/2nmodn.htm)

Die zweite Aussage gehört zur Aufgabenstellung von Problem 108.