Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Klasse

der

Bayerischen Akademie der Wissenschaften zu München

Jahrgang 1948

München 1949
Verlag der Bayerischen Akademie der Wissenschaften
In Kommission beim Biederstein Verlag München

Über die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$.

Von **Rudolf Steuerwald** in München.

Vorgelegt von Herrn O. Perron am 9. Januar 1948.

Satz 1. Es seien $a > 1$ und k natürliche Zahlen; ferner sei

$$b_1 = a - 1, \qquad b_2 = a + 1, \qquad b_3 = a^2 - 1,$$

$$f_1(a, k) = \frac{a^k - 1}{a - 1}, \quad f_2(a, k) = \frac{a^k + 1}{a + 1}, \quad f_3(a, k) = \frac{a^{2k} - 1}{a^2 - 1}.$$

Dann gilt für $j = 1, 2, 3$:

Aus

(1) $$a^{k-1} \equiv 1 \pmod{k}, \qquad (2) \quad (k, b_j) = 1$$

und

(3) $$m = f_j(a, k)$$

folgt

(4) $$a^{m-1} \equiv 1 \pmod{m} \text{ und } \qquad (5) \quad (m, b_j) = 1.$$[1]

Beweis: Zunächst folgt aus (1)

(6) $$(k, a) = 1;$$

dann aus (2) und (6)

(7) $$k \equiv 1 \pmod{2}.$$

Aus (3) erhält man

(8)
$$\begin{cases} \text{für } j = 1: m - 1 = \dfrac{a\,(a^{k-1} - 1)}{a - 1}, \\ \text{für } j = 2: m - 1 = \dfrac{a\,(a^{k-1} - 1)}{a + 1}, \\ \text{für } j = 3: m - 1 = \dfrac{a^2\,(a^{k-1} - 1)\,(a^{k-1} + 1)}{(a - 1)\,(a + 1)}. \end{cases}$$

In jedem Falle schließt man aus (1), (2), (7) und (8)

(9) $$m - 1 \equiv 0 \pmod{2k}.$$

Aus (3) und (9) endlich folgt (4).

[1] Die Ganzzahligkeit von $f_1(a, k)$ und $f_3(a, k)$ ist evident; daß auch $m = f_2(a, k)$ ganz sein muß, wird im Laufe des Beweises aus (7) ersichtlich.

Zu (5) gelangt man durch Vergleich von (2) mit der jeweils aus (3) folgenden Kongruenz

$$m \equiv k \pmod{b_j}. \tag{10}$$

Damit ist Satz 1 vollständig bewiesen.

Wählt man jetzt a fest und läßt k alle nicht in $a(a-1)(a+1)$ enthaltenen Primzahlen durchlaufen, so erhält man unendlich viele verschiedene zusammengesetzte Zahlen

$$m = f_3(a, k) = \frac{a^k - 1}{a-1} \cdot \frac{a^k + 1}{a+1}.$$

Also gilt der (für $a = 1$ triviale)

Satz 2. Zu jeder natürlichen Zahl a gibt es unendlich viele zusammengesetzte natürliche Zahlen n, für welche die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$ besteht.

Zusatz bei der Korrektur:

Satz 1 verallgemeinert, Satz 2 wiederholt ein Ergebnis von M. Cipolla (vgl. Dickson, History I, S. 94).