Zbl 081.27006

Erdős, Pál

Some remarks on a paper of McCarthy. (In English)

Can. Math. Bull. 1, 71-73 (1958).; remarks and corrections ibid. 3, 127-129 (1960).

Über die von *D. H. Lehmer* (Zbl 064.27902) weitgehend untersuchte Verteilung der Totative gibt der Verf. in Verallgemeinerung der von *J. McCarthy* (Zbl 078.03404) gefundenen folgende Sätze, wobei er die Abkürzung "$T(n,k)$ gilt" für "die Totative von n sind nach k gleich verteilt" anwendet, ($\varphi(x)$ ist die bekannte Eulersche Funktion, Anzahl der Totative nach n).

(1) Ist die natürliche Zahl $k = ab$ Produkt zweier teilerfremder natürlicher Zahlen $a > 1$, $b > 1$, so gibt es unendlich viele $n = p, q$ (p, q voneinander verschiedene Primzahlen), so daß $T(n,k)$ gilt, ohne daß n Ausnahmezahl bezüglich k ist (über Ausnahmezahl vgl. McCarthy, loc. cit.).

(2) Ist $k > 1$ keine Primzahl, nicht das Doppelte einer ungeraden Primzahl, so gibt es natürliche Zahlen $n = pq$ (wie vorhin) mit $\varphi(n) = 0 \bmod k$, wo $T(n,k)$ nicht gilt. Bei beiden Sätzen wendet Verf. den Primzahlsatz für arithmetische Reihen an. Den Beweis von (2) gründet Verf. auf einen angeblich leicht zu beweisenden Hilfssatz, der aber für b als Primzahl $\equiv 1 \bmod 3$ oder als das Doppelte einer Primzahl $= 5 \bmod b$ nicht gilt. Hier kann folgendes Lemma eintreten: k erfülle die Bedingungen von Satz (2), sei weiter $\neq 30$.

(A) Ist k nicht quadratfrei, $k = qb$ mit $(a,b) > 1$, so gibt es mindestens ein Totativ X nach k mit $X \equiv 1 \bmod a$, $X \equiv 1 \bmod b$, $X > k/2$, $X^2 \not\equiv -1 \bmod k$.

(B) Ist k quadratfrei, so gibt es eine Zerlegung $k = ab$, $a > 2$, $b > 2$ mit mindesten einem zugehörigen Paar von Totativen X, Y, wo $X \equiv 1 \bmod a$, $Y \equiv 1 \bmod b$, $X + Y > k$, $XY \not\equiv -1 \bmod k$ ist. Setzt man statt der — mit Druckfehlern behafteten — Formel (6), S. 74 des Verf. die Forderung $p \equiv X \bmod k$, $q \equiv Y \bmod k$, wo bei (A) die Zahl $Y = X$ zu setzen ist, so kommt man unschwer zum Satz (2) des Verf. Er scheint die Sonderrolle von $k = 30$ übersehen zu haben. Hier genügt das Beispiel $n = 77$, $\varphi(77) \equiv 0 \bmod 30$, $T(77, 30)$ gilt nicht.

Corrections and remarks:

Eine ober referierte Arbeit des Verf. wird in einigen Punkten verbessert und ergänzt. Die Beweisführung des Verf. läßt sich teilweise wie folgt verkürzen. Benützt werden die Bezeichnungen des Verf. (Vgl. auch obiges Referat).

Statt seines Lemmas beweisen wir zunächst in ganz kurzen Strichen das etwas eingeschränktere: Ist $k \neq p$ und $k \neq 2p$, wo die Primzahl p ungerade sei, gibt es zwei Totative u und v nach k mit $(u-1)(v-1) \equiv 0 \mod k, u+v > k$, wenn außerdem k nicht quadratfrei oder ungerade ist. Ist k nicht quadratfrei (gerade oder ungerade), so ist zu den Ausführungen des Verf. nichts hinzuzufügen. Ist k quadratfrei, also ungerade, so setzen wir $k = ab$ mit a als der kleinsten in k enthaltenen Primzahl, also $a < b$, $(a,b) = (a-1,b) = 1$, weiter $u = k - a + 1$. Ist $b \not\equiv 1 \mod a$, so setzen wir $v = k - b + 1$ für $b \equiv 1 \mod a$ hingegen $v = k - 2b + 1$. Man gelangt dann genau im Wege des Verf. zum Existenzbeweis unendlich vieler Zahlen n mit $\varphi(n) \equiv 0 \mod k$ $\{\varphi(n)$ die bekannte Eulersche

Funktion, Anzahl der Totative von $n\}$, $T(n,k)$ { Gleichverteilung der Totative von n nach k } findet nicht statt.
Ist endlich k quadratfrei gerade, $k = 2k'$, so beweist man zunächst auf dem schon beschrittenen Wege die Existenz unendlich vieler n mit $\varphi(n) \equiv 0 \mod k'$. $T(n,k')$ ist unrichtig. Dann ist auch $\varphi(n) \equiv 0 \mod k$, $T(n,k)$ ist unrichtig, da daraus $T(n,k')$ folgte.

L.Holzer

Classification:
11A25 Arithmetic functions, etc.

Keywords:
totients