# EIN ZAHLENTHEORETISCHER SATZ

Von P. ERDÖS UND P. TURAN (Budapest)

(Auszug aus einem Briefe an N. P. Romanoff).

...In Ihrer Arbeit [1]) steht folgender Satz:
Es sei $l(k)$ die kleinste positive ganze Zahl, für die $a^{l(k)} \equiv 1 \pmod{k}$, dann konvergiert die Reihe $\sum\limits_{\substack{k=1 \\ (a,\,k)=1}}^{\infty} \frac{\mu(k)^2}{k l(k)}$.

Es ist uns gelungen allgemein die Konvergenz der Reihe

$$\sum_{k=1}^{\infty} \frac{1}{k\,l(k)},$$

wo $\varepsilon > 0$, folgendermassen zu beweisen:

$l(k)$ sei die kleinste ganze Zahl, für welche $a^{l(k)} \equiv 1$ $(mod\, k)$, wo $a$ eine fixe ganze Zahl ist. Dann ist $\sum\limits_{\substack{k=1 \\ (a,\,k)=1}}^{\infty} \frac{1}{k\,l(k)^{\varepsilon}}$ konvergent.

Wir teilen die Zahlen in zwei Gruppen. Für die Zahlen der ersten Gruppe sei $l(k) \geqslant (\log k)^{\frac{2}{\varepsilon}}$, für die der zweiten Gruppe hingegen $l(k) < (\log k)^{\frac{2}{\varepsilon}}$. Für die $k$ der ersten Gruppe ist $\sum\limits_{\substack{k=1 \\ (a,\,k)=1}}^{\infty}{}' \frac{1}{k\,l(k)^{\varepsilon}} \leqslant \sum\limits_{k=1}^{\infty} \frac{1}{k \log^2 k}$ konvergent, sodass wir uns nur mit dem zweiten Teil beschäftigen müssen. Wir beweisen, dass $\sum \frac{1}{k}$, ausgedehnt, auf diese $k$, konvergent ist. Wir beweisen dies, indem wir zeigen, dass die Anzahl der in die zweite Gruppe gehörigen $k \leqslant n$ für jedes $n$ von der Grössenordnung $O\left(\frac{n}{\log^2 n}\right)$ ist, woraus sich die Konvergenz des $\sum'' \frac{1}{k}$ unmittelbar ergibt. Es sei nun $n$ eine beliebige, aber fixe,

[1]) „Über einige Sätze der additiven Zahlentheorie" Mathematische Annalen 109, 1934, S. 668–678.

Zahl; wir vergrössern die Anzahl der Zahlen der zweiten Gruppe, wenn wir jene $k$ Zahlen ($k < n$) in Betracht ziehen, für die $l(k) < (\log n)^{\frac{2}{\varepsilon}}$. Als Anzahl dieser Zahlen erhalten wir $O\left(\frac{n}{(\log n)^2}\right)$.

Nach Definition sind diese $k$ Zahlen unter den Teilern der Zahlen $(a-1), (a^2-1), \ldots, a^{\left[(\log n)^{\frac{2}{\varepsilon}}\right]}-1$; also vergrössern wir die Anzahl der obigen Zahlen k, wenn wir diejenigen Zahlen bis $n$ nehmen, die aus den verschiedenen Primfaktoren der Zahlen $(a-1), (a^2-1), \ldots, (a^{\left[(\log n)^{\frac{2}{\varepsilon}}\right]}-1)$ zusammengesetzt sind. Es ist klar, dass die Anzahl der verschiedenen Primfaktoren der Zahl $k$ kleiner ist als $C_1 \log k$, also enthält ein Glied der obigen Zahlenreihe höchstens $O(\log^{\frac{2}{\varepsilon}} n)$ verschiedene Primfaktoren; infolgedessen ist die Anzahl der verschiedenen Primfaktoren $O(\log^{\frac{4}{\varepsilon}} n)$.

Nun beweisen wir folgenden Satz. Wie wir auch $[\log^{\frac{4}{\varepsilon}} n]$ Primzahlen angeben, ist die Anzahl derjenigen Zahlen, die nur aus diesen Primzahlen zusammengesetzt sind $O\left(\frac{n}{\log^2 n}\right)$. Unter diesen Zahlen gibt es nämlich solche, bei denen 1. die Anzahl der verschiedenen Primfaktoren $\geqq \sqrt{\log n}$ ist und 2. bei denen die Zahl der verschiedenen Primfaktoren $< \sqrt{\log n}$ ist. Die Anzahl der Teiler der Zahlen, der ersten Gruppe ist offensichlich $> 2^{\sqrt{\log n}}$; oder wenn wir mit $d(n)$ die Anzahl der Teiler von $n$ bezeichnen, $O(n \log n) = \sum_{1}^{n} d(n) > R(n)\, 2^{\sqrt{\log n}}$ und daraus $R(n) = O\left(\frac{n \log n}{\sqrt{\log n}}\right) = O\left(\frac{n}{\log^2 n}\right)$.

Für die Zahlen der zweiten Gruppe ist die Anzahl der verschiedenen Primfaktoren $< \sqrt{\log n}$. Ein Primfaktor kann höchstens mit dem Exponent $[2 \log n]$ vorkommen, denn $2^{2 \log n} > n$. Also müssen wir aus $\left[(\log n)^{\frac{4}{\varepsilon}+1}\right]$ Primzahlen und Primzahlpotenzen die Kombinationen $1, 2; \ldots \left[\sqrt{\log n}\right]$—ter Ordnung bilden, und auf diese Weise erhalten wir alle Zahlen der zweiten Gruppe. Die Anzahl dieser Zahlen ist offenbar $O\left(e^{\log\log n \left(\frac{4}{\varepsilon}+1\right)\sqrt{\log n}}\right) = O\left(\frac{n}{\log^2 n}\right)$ q. e. d.

Es wäre vielleicht interessan, $\sum_{\substack{k=1 \\ (a, k)=1}}^{n} l(k)$ abzuschätzen. Es scheint wahrscheinlich, dass die obige Summe $O(n^2)$ ist. Der Beweis scheint aber sehr schwer zu sein.

---

## Об одной теореме из теории чисел

П. Эрдеш и П. Туран (Будапешт)

(из письма к Н. П. Романову).

В настоящей заметке доказывается следующее предложение: ряд $\sum_{k=1}^{\infty} \frac{1}{k\, l(k)^{\varepsilon}}$, где $l(k)$ означает наименьшее из чисел $m$, удовлетворяющих сравнению $a^m \equiv 1 \pmod{k}$, сходится при всяком $\varepsilon > 0$.

Это предложение является обобщением аналогичной теоремы, доказанной Н. Романовым в его указанной выше работе.

---