Sonderabdruck aus
ARCHIV DER MATHEMATIK
Vol. XXVII, 1976 BIRKHÄUSER VERLAG, BASEL UND STUTTGART Fasc. 2

Bemerkungen zu einer Aufgabe in den Elementen

Professor H.-J. KANOLD zum sechzigsten Geburtstag gewidmet

Von

P. ERDÖS

G. Jaeschke stellte folgende Aufgabe in den Elementen der Mathematik (**26**, 43, Aufgabe 618 (1971); gelöst durch P. Bundschuh): Es sei $l_2(p)$ die kleinste Zahl mit $2^{l_2(p)} \equiv 1 \pmod{p}$. $E(r)$ sei die Anzahl der Primzahlen mit $l_2(p) = r$. Es gilt

$$E(r) \leqq \frac{r \log 2}{\log r}.$$

$A(x, \delta)$ sei die Anzahl der Primzahlen $\leqq x$ mit $l_2(p) > p^{\delta}$. Dann gilt

$$A(x, \delta) = (1 + o(1)) \frac{x}{\log x} \quad \text{für} \quad \delta < \frac{1}{2}$$

und

$$A\left(x, \frac{1}{2}\right) \geqq (1 - \log 2 + o(1)) \frac{x}{\log x}.$$

Ich werde die Resultate ein wenig verschärfen, indem ich

$$E(r) \leqq \left(\frac{1}{2} + o(1)\right) \frac{r \log 2}{\log r} \tag{1}$$

und

$$A\left(x, \frac{1}{2}\right) = (1 + o(1)) \frac{x}{\log x} \tag{2}$$

zeigen werde. Ich bin überzeugt, daß $E(r) = o(r^{\varepsilon})$ für jedes $\varepsilon > 0$ gilt; es ist nicht bekannt, ob $E(r)$ unbeschränkt ist; auch ist nicht bekannt, ob $E(r)$ für unendlich viele r gleich 1 ist. Das berühmte Problem der Mersenneschen Primzahlen besagt, daß $E(p) = 1$ für unendlich viele p, also daß $2^p - 1$ für unendlich viele p Primzahl ist. Dies ist bekanntlich eines der schwersten ungelösten Probleme.

Es scheint auch ganz sicher zu sein, daß für jedes $c < 1$ gilt

$$A(x, c) = o\left(\frac{x}{\log x}\right).$$

Eine berühmte Vermutung von Artin besagt, daß die Anzahl der Primzahlen $p<x$, für welche 2 primitive Wurzel ist, $(c+o(1))\dfrac{x}{\log x}$ ist für eine absolute Konstante c. Es sei $f(x)\to\infty$ beliebig; sicherlich gilt wohl

$$A\left(x,\frac{x}{f(x)}\right)=o\left(\frac{x}{\log x}\right).$$

Ein bekannter Satz von Romanoff besagt, daß

$$\sum\frac{1}{n\,l_2(n)}<\infty$$

ist, wo $l_2(n)$ für ungerades n der Exponent von 2 mod n ist und sonst $l_2(n)=\infty$ ist. Turán und ich gaben einen viel einfacheren Beweis. Vielleicht der einfachste Beweis erscheint bei P. Erdös, On some problems of Bellman and Romanoff, J. Chinese Math. Soc. (N.S.) **1**, 409—421 (1951). Ich zeigte auch (Israel J. Math. **9**, 43—48 (1971))

$$\sum_{d\mid 2^n-1}\frac{1}{d}<c\log\log n\,.$$

Es sei

$$f(x)=\max_{n\leqq x}\sum_{d\mid n}\frac{1}{d}\,,\qquad F(x)=\max_{n\leqq x}\sum_{d\mid 2^n-1}\frac{1}{d}\,;$$

vielleicht gilt sogar $F(x)-f(x)<c$. Es ist nicht schwer zu zeigen, daß

$$\max_{n\leqq x}\sum_{d\mid n(n+1)}\frac{1}{d}-f(x)<c$$

gilt, aber ($v(n)$ ist die Anzahl der verschiedenen Primfaktoren von n)

$$\max_{n\leqq x}v(n)/\max_{n\leqq x}v(n(n+1))\to 1$$

und

$$\max_{n\leqq x}v(n(n+1))-\max_{n\leqq x}v(n)\to\infty$$

kann ich nicht beweisen.

Der Beweis von (1) ist leicht.

Wenn $l_2(p)=r$ ist, so ist $p\equiv 1\ (\mathrm{mod}\ r)$, und wenn $p_1,\dots,p_k$ die Primzahlen mit $l_2(p_i)=r$ sind, so gilt $p_1\cdots p_k<2^r$ $(p_1<\cdots<p_k)$ und $p_i>i\,r$. Also ist

$$k!\,r^k<2^r\,,$$

und daraus folgt mit der Stirlingschen Formel

$$k^k\,r^k\,e^{-k}<2^r\,. \tag{3}$$

Aus (3) folgt nun (1) leicht. Wäre

$$k>\left(\frac{1}{2}+\varepsilon\right)\frac{r\log 2}{\log r}\,,$$

so kann (3) nicht wahr sein. Aus (3) würde nämlich

$$\frac{k\,r}{e} < 2^{r/k},$$

also

$$\frac{r^2 \log 2}{2e \log r} < r^{1/(1/2+\varepsilon)}$$

folgen, was für $r > r_0(\varepsilon)$ falsch ist. Damit ist (1) bewiesen. Es wäre interessant (1) zu verschärfen, aber ich konnte nicht einmal $\frac{1}{2}$ durch eine kleinere Konstante ersetzen.

Der Beweis von (2) ist viel schwerer. Wir zeigen, daß die Anzahl der Primzahlen $p \leqq x$ mit

(4) $$l_2(p) \leqq x^{1/2}$$

$o\left(\frac{x}{\log x}\right)$ ist. Es genügt natürlich zu zeigen, daß die Anzahl dieser Primzahlen für jedes η und $x > x_0(\eta)$ kleiner als $\frac{\eta x}{\log x}$ ist. Um dies einzusehen, teilen wir die Primzahlen, die (4) befriedigen, in zwei Klassen.

In der ersten Klasse sind die Primzahlen $p \leqq x$ mit $l_2(p) < \varepsilon\, x^{1/2}$, $\varepsilon = \varepsilon(\eta)$. Aus (1) folgt, daß die Anzahl der Primzahlen der ersten Klasse kleiner als

(5) $$\sum_{r < \varepsilon x^{1/2}} \left(\frac{1}{2} + o(1)\right) \frac{r \log 2}{\log r} < \frac{2\varepsilon^2 x}{\log x} < \frac{\eta}{2} \frac{x}{\log x}$$

ist für $x > x_0$ und $\eta = \eta(\varepsilon)$.

In der zweiten Klasse sind die Primzahlen $p \leqq x$ mit

(6) $$\varepsilon\, x^{1/2} < l_2(p) \leqq x^{1/2}.$$

Für die Primzahlen p, die (6) befriedigen, gilt

(7) $$p - 1 = uv, \quad u = l_2(p), \quad \varepsilon\, x^{1/2} \leqq u \leqq x^{1/2}.$$

Wir werden nun zeigen, daß die Anzahl der Primzahlen $p \leqq x$, die (7) befriedigen, $o\left(\frac{x}{\log x}\right)$ ist, und daraus folgt natürlich (2). Der Beweis benutzt die Brunsche Siebmethode und Methoden meiner Arbeiten [1] und [2]. Der Beweis wird etwas skizzenhaft dargestellt; ich verweise den interessierten Leser auf [1] und [2].

Wir teilen die Primzahlen, die (7) befriedigen, in zwei Klassen. In der ersten Klasse sind die Zahlen mit $v < \varepsilon\, x^{1/2}$. In diesem Falle ist $uv < \varepsilon x$, also $p \leqq \varepsilon x$; daher ist die Anzahl dieser Primzahlen $< \frac{2\varepsilon x}{\log x}$.

Für die Zahlen der zweiten Klasse gilt

$$\varepsilon\, x^{1/2} \leqq v < x^{1/2}/\varepsilon.$$

Die obere Grenze gilt wegen $uv < x$.

Die Zahlen der zweiten Klasse teilen wir wieder in zwei Klassen. In der ersten Unterklasse haben sowohl u als auch v mehr als $\frac{2}{3}\log\log x$ Primfaktoren (mehrfache mehrfach gezählt). Für diese Zahlen hat aber $p-1$ mindestens $\frac{4}{3}\log\log x$ Primfaktoren. Bekanntlich ist aber für fast alle Primzahlen die Anzahl der Primfaktoren $f(p-1) = (1+o(1))\log\log p$ ([2]); daher ist die Anzahl der Zahlen der ersten Unterklasse $o\left(\frac{x}{\log x}\right)$.

Ohne Beschränkung der Allgemeinheit können wir nun voraussetzen, daß für die Zahlen der zweiten Unterklasse $f(v) \leqq \frac{2}{3}\log\log x$ gilt. Nach einem bekannten Satz von Hardy und Ramanujan ist die Anzahl dieser Zahlen v $o(x^{1/2})$ $\left(\text{es ist } o\left(\frac{x^{1/2}}{(\log x)^c}\right)\right.$ $\left.\text{für ein genügend kleines } c\right)$. Die Anzahl der Zahlen $u < x/v$, für welche $uv+1$ eine Primzahl ist, ist aus der Brunschen Siebmethode kleiner als

$$c_1 \frac{x}{v} \prod_{\substack{p \nmid v \\ p<x}} \left(1-\frac{1}{p}\right) < \frac{c_2 x \prod_{p|v}(1+1/(p-1))}{v\log x} < \frac{c_3 x\log\log x}{v\log x} < \frac{c_3 x^{1/2}\log\log x}{\varepsilon\log x},$$

wegen

$$\prod_{p|v}\left(1+\frac{1}{p-1}\right) < c\log\log v < c\log\log x.$$

Daher ist die Anzahl der Zahlen der zweiten Unterklasse kleiner als

$$\frac{c_3 x^{1/2}\log\log x}{\varepsilon\log x}\, o\left(\frac{x^{1/2}}{(\log x)^c}\right) = o\left(\frac{x}{\log x}\right),$$

womit alles bewiesen ist.

Wie es oft in der Zahlentheorie vorkommt, haben wir mit ziemlich viel Mühe ein recht schwaches Resultat erhalten; vielleicht liegt die Schuld nicht an mir, sondern das Problem ist eben recht schwer.

Mit mehr Mühe und den Methoden von [3] kann ich zeigen, daß, wenn $\varepsilon_p \to 0$ beliebig langsam, die Anzahl der Primzahlen $p < x$ mit

$$l_2(p) < p^{1/2+\varepsilon_p}$$

dann $o\left(\frac{x}{\log x}\right)$ ist. Ich kann dies nicht zu $p^{1/2+c}$ verschärfen. Ich kann mit den Methoden von [1] und [2] auch zeigen, daß, wenn $y/x \to \infty$, die Anzahl der Primzahlen $p < y$, für die $p-1$ einen Teiler in $(x, 2x)$ hat, dann $o\left(\frac{y}{\log y}\right)$ ist.

Es sei $A_g(x,\delta)$ die Anzahl der ganzen Zahlen $n \leqq x$ mit $l_2(n) < x^{\delta}$. Ich kann nur zeigen, daß für jedes $\varepsilon > 0$ ein δ_ε mit $A_g(x,\delta_\varepsilon) < \varepsilon x$ existiert und für ein weiteres δ_ε' gilt $A_g(x, 1-\delta_\varepsilon') < (1-\varepsilon)x$. Weiter sei $E_g(x,r)$ die Anzahl der Teiler $d \leqq x$ von $2^r - 1$, und $E_g'(x,r)$ sei die Anzahl der Zahlen $n < x$ mit $l_2(n) = r$.

$E_g(x, r) = o(x)$ für $r = o(x^\varepsilon)$ ist unschwer, wahrscheinlich gilt dies aber auch für $r < x^c$ für jedes feste c. Es wäre recht interessant,

$$\max_r E_g'(x, r) = f(x)$$

von oben und unten möglichst gut abzuschätzen. Ist $f(x) = o(x^\varepsilon)$? Für welche Werte von r ist $E_g'(x, r) = f(x)$? Offenbar kann man hier noch viele weitere Fragen stellen, aber dies wollen wir dem Leser überlassen.

Literaturverzeichnis

[1] P. Erdös, Note on sequences of integers no one of which is divisible by any other. J. London Math. Soc. **10**, 126—128 (1935).
[2] P. Erdös, On the normal number of prime factors of $p - 1$ and some related problems concerning Euler's φ-function. Quart. J. Math. **6**, 205—213 (1935).
[3] P. Erdös, A generalization of a theorem of Besicovitch. J. London Math. Soc. **11**, 92—98 (1936).

Eingegangen am 27. 12. 1974

Anschrift des Autors:

P. Erdös
Budapest XII
Nemetvölgi I u 72c
Ungarn