ON THE INTEGERS WHICH ARE THE TOTIENT OF A PRODUCT OF THREE PRIMES

By PAUL ERDŐS (*Manchester*)

[Received 1 April 1935]

THROUGHOUT this paper $p, q, r, p', q', r', s, P$ are used to denote prime numbers; ϵ an arbitrarily small positive number; n all sufficiently large integers, i.e. $n > n(\epsilon)$; $N(p, m)$ the number of the primes p not exceeding m and belonging to a defined set. The C denote positive absolute constants, not always the same in each occurrence. I prove the following

THEOREM. *If $f(n)$ is the number of solutions of the equation*

$$(p-1)(q-1)(r-1) = n \tag{1}$$

in primes p, q, r no two of which are equal, then

$$\varlimsup_{n\to\infty} f(n) = \infty.$$

I believe, but cannot prove, that a similar result holds for the solution of
$$(p-1)(q-1) = n.$$

We require the following

LEMMA.* *If the primes p are such that $p-1$ has more than $(1+\epsilon)\log\log n$ or less than $(1-\epsilon)\log\log n$ different prime factors, then*

$$N(p, n) = o\left(\frac{n}{\log n}\right). \tag{2}$$

This result is included in the more general one that, if P_k denotes a prime such that P_k-1 has exactly k different prime factors, then

$$N(P_k, n)\log^2 n < Cn(C+\log\log n)^{k+3}.$$

From this is deduced exactly as in my paper quoted above that

$$\sum_{k<(1-\epsilon)\log\log n} N(P_k, n) + \sum_{k>(1+\epsilon)\log\log n} N(P_k, n) = o\left(\frac{n}{(\log n)^{1+\delta}}\right) \tag{3}$$

where $\delta = \delta(\epsilon) > 0$.

I prove from (3) that, if P denotes a prime such that $P-1$ has more than $(1+\epsilon)\log\log P$ or less than $(1-\epsilon)\log\log P$ factors, then

* P. Erdős, *Quart. J. of Math.* (Oxford), 6 (1935), 205–13.

$\sum P^{-1}$ converges. It suffices to show that

$$N(P,n) = o\left(\frac{n}{(\log n)^{1+\delta'}}\right) \tag{4}$$

where δ' is a positive constant. In (4) either $P \leqslant \sqrt{n}$, i.e. there are at most $\sqrt{n}$, values of P; or $n \geqslant P > \sqrt{n}$, and then

$$\log\log n \geqslant \log\log P > \log\log n - 1,$$

and so

$$(1+\epsilon)\log\log P > (1+\tfrac{1}{2}\epsilon)\log\log n,$$

$$(1-\epsilon)\log\log P < (1-\tfrac{1}{2}\epsilon)\log\log n.$$

Hence the P's exceeding $\sqrt{n}$ are included among the primes Q $(< n)$ for which $Q-1$ has more than $(1+\frac{1}{2}\epsilon)\log\log n$ or less than $(1-\frac{1}{2}\epsilon)\log\log n$ different prime factors. Then from (3), with $\delta' = \delta(\frac{1}{2}\epsilon)$,

$$N(P,n) \leqslant o\left(\frac{n}{(\log n)^{1+\delta'}}\right) + n^{\frac{1}{2}} = o\left(\frac{n}{(\log n)^{1+\delta'}}\right).$$

Typify by A the positive integers not exceeding n such that

$$pqr = A,$$

where no two of the primes p, q, r are equal, and $p-1$, $q-1$, $r-1$ each have more than $(1-\epsilon)\log\log n$ factors. I prove that

$$N(A,n) > C\frac{n}{\log n}. \tag{5}$$

Denote by p' (or q', r') the primes such that $p'-1$ has more than $(1-\epsilon)\log\log n$ different prime factors. Take the primes, say r', less than $n/p'q'$ for arbitrary and unequal p', q', and multiply them by $p'q'$. The integers $p'q'r'$ belong to the A's, and each A can be obtained at most six times in this way. Hence

$$6N(A,n) \geqslant \sum_{p',q'} N'\left(r', \frac{n}{p'q'}\right), \tag{6}$$

the summation being extended over all different p', q', and N' denoting the omission of p', q' among the r' in calculating N. It suffices for our object to take only those p', q' for which

$$n^{\frac{1}{8}} < p', q' < n^{\frac{1}{4}}.$$

I prove now that

$$\sum_{n^{\frac{1}{8}} < p' < n^{\frac{1}{4}}} \frac{1}{p'} > C. \tag{7}$$

For

$$\sum_{p \leqslant n} \frac{1}{p} = \log\log n + C + o(1),$$

and so
$$\sum_{n^{\frac{1}{8}}<p<n^{\frac{1}{4}}} \frac{1}{p} > C. \tag{8}$$

The primes p in this sum such that $p-1$ has less than $(1-\epsilon)\log\log n$ different prime factors occur among the primes P $(n^{\frac{1}{8}} < P < n^{\frac{1}{4}})$ which are such that $P-1$ has less than $(1-\frac{1}{2}\epsilon)\log\log P$ different prime factors. For clearly
$$(1-\epsilon)\log\log n < (1-\tfrac{1}{2}\epsilon)\log\log P,$$
since
$$\log\log n - \log 8 < \log\log P < \log\log n - \log 4.$$
Hence, since the series $\sum P^{-1}$ converges,
$$\sum_{n^{\frac{1}{8}}<P<n^{\frac{1}{4}}} P^{-1} < \epsilon, \quad \text{say},$$
for arbitrarily small positive ϵ, and n greater than some $n(\epsilon)$. Then (7) follows on omitting the P from the p in (8). On squaring (7),
$$\sum_{n^{\frac{1}{8}}<p',q'<n^{\frac{1}{4}}}^{p'\neq q'} \frac{1}{p'q'} > C, \tag{9}$$
the omission of the terms in which $p' = q'$ being allowable, since $\sum 1/p^2$ converges. On subtracting from the number of primes s less than $n/p'q'$ the number of those for which $s-1$ has less than $(1-\frac{1}{2}\epsilon)\log\log\frac{n}{p'q'}$ different prime factors, i.e. $o\left(\frac{n}{p'q'}\Big/\log\frac{n}{p'q'}\right)$ from (2), by replacing ϵ by $\frac{1}{2}\epsilon$ and n by $n/p'q'$, we have
$$N\left(r', \frac{n}{p'q'}\right) > \frac{Cn}{p'q'\log n}.$$
Hence, from (6),
$$6N(A,n) \geqslant \sum_{n^{\frac{1}{8}}<p',q'<n^{\frac{1}{4}}}^{p'\neq q'} \frac{Cn}{p'q'\log n} \geqslant \frac{Cn}{\log n},$$
by (9).

Denote now by B_1, B_2,... the different integers in the set $\phi(A)$, where A does not exceed n and ϕ denotes Euler's ϕ-function. The B's are clearly of the form
$$(p'-1)(q'-1)(r'-1).$$
I prove that
$$N(B,n) = o(n/\log n). \tag{10}$$
Define the *quadratic part* of an integer $I = p^{\alpha}q^{\beta}...$ as the product of the powers p^{α} with indices exceeding unity. Split the B's into two classes B_1, B_2 according as their quadratic part has respectively more than or not more than $\epsilon\log\log n$ different prime factors. Obviously

the integers B_1 have a divisor which is composed of prime factors, in number exactly $[\epsilon \log\log n]$ $(= j$, say), each occurring with a power exceeding unity. Hence

$$N(B_1, n) < n\left(\sum_{p,\alpha} \frac{1}{p^\alpha}\right)^j < \frac{nC^j}{j!} < n\left(\frac{C}{j}\right)^j = o\left(\frac{n}{\log n}\right),$$

where the summation extends to all primes p and all indices α exceeding unity so that the double series converges.

Each of the integers in B_2 is of the form

$$(p'-1)(q'-1)(r'-1),$$

where $p'-1$, $q'-1$, $r'-1$ each have at least $(1-\epsilon)\log\log n$ different prime factors, and so at least $(3-3\epsilon)\log\log n$ prime factors, not necessarily all different. But from the definition of B_2, $p'-1$, $q'-1$ can have as common factors at most $\epsilon \log\log n$ different primes; and similarly for $q'-1$, $r'-1$, etc. Hence each integer in B_2 has at least $(3-6\epsilon)\log\log n$ different prime factors and so at least $2^{(3-6\epsilon)\log\log n}$ divisors. But

$$\sum_{t=1}^{n} d(t) < Cn \log n,$$

and so* $\quad N(B_2, n) < Cn \log n/2^{(3-6\epsilon)\log\log n} = o\left(\frac{n}{\log n}\right),$

if we now suppose ϵ taken so small that

$$2^{3-6\epsilon} > e^2 = (2{\cdot}71...)^2.$$

Hence $\quad N(B, n) = N(B_1, n) + N(B_2, n) = o(n/\log n).$

This is (10).

Then, from (5), $N(A, n) \geqslant \frac{1}{\epsilon} N(B, n)$ for every positive constant ϵ, if $n > n(\epsilon)$. Hence at least one of the B's less than n is represented at least $1/\epsilon$ times in the form $\phi(N)$ for every $1/\epsilon$ if $n > n(\epsilon)$. This concludes the proof of the main theorem.

* It is here that the method breaks down for the solution of

$$(p-1)(q-1) = n.$$