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

By P. ERDŐS (*Manchester*)

[Received 11 June 1936]

IN a previous paper* I proved that for an infinity of n the number of solutions of the equation

$$n = (p-1)(q-1)(r-1) \quad (p, q, r \text{ primes})$$

is greater than $(\log n)^{c_1}$. The proof was elementary and was based on the fact that the normal number of prime factors of $(p-1)$ is $\log\log n$.† But then I was unable to prove even that the number of solutions of $n = (p-1)(q-1)$ is unbounded. In this paper I shall prove that, for an infinity of n, the number of solutions of the equation $n = (p-1)(q-1)$ is greater than $\exp\{\sqrt{(\log n)}-\epsilon\}$.

The proof will be shorter than that of (I), but it will not be elementary, and will be very similar to the argument used in my paper 'On the representation of an integer as the sum of k kth powers'.‡

Let p_1 be sufficiently large, $A = p_1 p_2 \dots p_\lambda$ $(p_1, p_2, \dots, p_\lambda$ consecutive primes),

$$(\log A)^2 < p_1 \leqslant (\log A p_{\lambda+1})^2 < 4(\log A)^2, \tag{1}$$

(since by Tschebischeff's theorem $p_{\lambda+1} < 2p_\lambda < A$), and $m = [e^{p_1}]+1$. We evidently have $\exp\sqrt{(\log m)} > A$.

We estimate the number of solutions S of the congruence

$$(p-1)(q-1) \equiv 0 \pmod{A}$$

with

$$p, q \leqslant m.$$

We write $A = BC$ and denote by S_B the number of solutions of

$$(p-1)(q-1) \equiv 0 \pmod{A}, \quad p-1 \equiv 0 \pmod{B}, \quad q-1 \equiv 0 \pmod{C}$$

with

$$(q-1,\, B) = 1, \qquad p, q \leqslant m.$$

First we estimate S_B.

* See above, pp. 16–19. I shall refer to this paper as (I).

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

‡ P. Erdős, *J. of London Math. Soc.* 11 (1936), 133–6.

From a result of Titchmarsh's* it follows that, if $y < A$, with the possible exception of a single y, the number of primes p such that

$$p \equiv 1 \pmod y, \qquad p \leqslant m$$

is greater than $\frac{1}{2}m/\{\phi(y)\log m\}$.

Hence, with the possible exception of a single B

$$[B \leqslant A < \exp\sqrt{(\log m)}],$$

the number of primes not exceeding m for which $p-1 \equiv 0 \pmod B$ is greater than $\frac{1}{2}m/\{\phi(B)\log m\}$. Similarly, with the possible exception of a single C, the number of primes q not exceeding m for which

$$q-1 \equiv 0 \pmod C \text{ and } (q-1, B) = 1$$

is greater than $$\frac{m}{2\phi(C)\log m} - \sum_{p_i|B} \pi(m, p_i C, 1),$$

where $\pi(m, p_i C, 1)$ denotes the number of primes not exceeding m and congruent to unity to modulus $p_i C$. But, since $p_i C < A < m^\epsilon$, it follows from Brun's method that

$$\pi(m, p_i C, 1) < \frac{c_1 m}{\phi(p_i C)\log m} \quad (c\text{'s denoting absolute constants}).$$

Hence $$\sum_{p_i|B} \pi(m, p_i C, 1) < \sum_{p_i|B} \frac{c_1 m}{\phi(p_i C)\log m}$$

$$< \frac{c_1 \lambda m}{\phi(C)\log m(p_1-1)} < \frac{c_2 \lambda m}{\phi(C)(\log A)^2 \log m},$$

but, from (1), $(\log A)^{2\lambda} < A$ and so $\lambda < \log A$. Thus

$$\sum_{p_i|B} \pi(m, p_i C, 1) < \frac{c_2 m}{\phi(C)\log A \log m} < \frac{m}{4\phi(C)\log m}.$$

Hence the number of primes q less than m and such that

$$q-1 \equiv 0 \pmod C, \qquad (q-1, B) = 1$$

* E. C. Titchmarsh, *Rendi. Circ. Mat. Palermo*, 54 (1930), 414–29. The result states (p. 424) that, if k is any integer not exceeding $\exp\sqrt{(\log x)}$ one value of k possibly excluded, and l is a fixed number prime to k, then the number of primes not exceeding x and prime to l to modulus k equals

$$\frac{1}{\phi(k)} \int_2^x \frac{du}{\log u} + Ox\exp[-c\sqrt{(\log x)}].$$

is, with one possible exception, greater than

$$\frac{m}{\phi(C)4\log m}.$$

Hence, with the possible exception of two B's,

$$S_B > \frac{m^2}{8\phi(A)(\log m)^2}.$$

We evidently have $$S > \sum_{B|A} S_B,$$

since the same $q-1$ cannot occur for different B's.

Hence $$S > \frac{(2^\lambda - 2)m^2}{8\phi(A)(\log m)^2} > \frac{2^\lambda m^2}{16A(\log m)^2}.$$

But the integers of the form $(p-1)(q-1)$ with p, q less than m are evidently less than m^2. Hence we may find n ($< m^2$) a multiple of A for which the equation $n = (p-1)(q-1)$ has more than $2^\lambda/16(\log m)^2$ solutions.

But $$\lambda > \frac{\log A}{3\operatorname{loglog} A};$$

for all prime factors of A are less than $(\log A)^3$ since, by (1), $p_1 < 4(\log A)^2$, and the product of primes in the interval

$$(4(\log A)^2, (\log A)^3)$$

is greater than A. This fact follows from the prime-number theorem but may be deduced by elementary methods too.

Thus, since $\log m < 2p_1 < 8(\log A)^2$, we finally have

$$\frac{2^\lambda}{16(\log m)^2} > \frac{2^{\frac{\log A}{3\operatorname{loglog} A}}}{16.64(\log A)^4} > \exp\left(\frac{c_3 \log A}{\operatorname{loglog} A}\right) > \exp\{\sqrt{(\log m)}-\epsilon\}.$$

Hence the result.

By a quite different elementary method I obtained the following result. Let C be sufficiently large and $p_1 < p_2 < \ldots < p_x < n$ any set of primes such that

$$x > \frac{Cn \operatorname{loglog} n}{(\log n)^2},$$

then the products $(p_i - 1)(p_r - 1)$ cannot be all different.