A THEOREM OF ERDÖS.

By S. Chowla.

(From the Government College, Lahore.)

Received November 21, 1936.

1. Erdös has proved the beautiful result (*Quart. Jour. of Maths.*, Oxford, Sept. 1936) that the no. of solutions of $n = (p-1)(q-1)$ is unbounded, where p, q denote primes. The object of this note is to correct an error in the argument arising from Erdös's citation of a result of Titchmarsh, which was never really proved. The correct form of the result runs as follows :

Let $\pi(x\,;\,k,\,l)$ denote the no. of primes $\equiv l \pmod{k}$ not exceeding x. Then for all $k \leq \exp(\sqrt{\log x})$, *except possibly for all multiples of a certain number* k_0, we have

$$\pi(x\,;\,k,\,l) = \frac{1}{\phi(k)} \int_2^x \frac{du}{\log u} + O[x \exp(-c\sqrt{\log x})].$$

Here the constant implied in " O " is independent of both x and k. (Titchmarsh, *Rendi. Circ. Mat. Palermo*, 57, 1933, 1—2.)

2. Let p_1 be sufficiently large, $A = p_1\, p_2 \cdots p_\lambda$ (a product of λ consecutive primes, choose λ so that

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

(since, by Bertrand's postulate, $p_{\lambda+1} < 2p_\lambda < A$) and $m = [e^{p_1}] + 1$. We evidently have $\exp(\sqrt{\log m}) > A$. Hence we can apply Titchmarsh's theorem above (which we shall refer to as T.) with $x = m$ and $k \leqslant A$ where k/A. Let k_0 (if it exists) be equal to

$$p_{m_1}\, p_{m_2} \cdots p_{m_r}$$

where the numbers m_s $(1 \leqslant s \leqslant r)$ are all different and each $m_s \leqslant \lambda$. Two cases arise

(a) $$r > \frac{\lambda}{2} + 1.$$

Then T. applies to all combinations of products of the $(r-1)$ different primes

$$p_{m_1},\, p_{m_2},\, \cdots,\, p_{m_{r-1}}$$

In this case we define

$$A' = \prod_{s=1}^{r-1} p_{m_s}$$

and observe that T. " *applies* " to all divisors of A′ *in the sense that* none of the divisors of A′ is a multiple of k_0, i.e., *none of the divisors of* A′ *is "exceptional" in the sense of* T.

(β) $r \leqslant \frac{\lambda}{2} + 1$. Then $\left(\frac{A}{k_0}, k_0\right) = 1$ so that if we take $A' = \frac{A}{k_0}$ in this case, we observe that in this case none of the divisors of A′ is "exceptional" in the sense of T.

In both cases, (α) or (β), our definition of A′ ensures that the number of divisors of A′ is at least

$$2^{\frac{1}{2}\lambda - 1}$$

for A′ is a product of at least $\left(\frac{\lambda}{2} - 1\right)$ different primes. Further, since $(A', k_0) = 1$ in one case while $A' < k_0$ in the other, *no divisor of* A′ *is an " exception " when* T. *is applied with* x = m, k ⩽ A′, k/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 no. of solutions of

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

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

First we estimate S_B.

In virtue of what has been said before, T. applies and hence the no. of solutions of $p - 1 \equiv 0(B)$ with $p \leqslant m$, is greater than $\frac{1}{2} \frac{m}{\phi(B) \log m}$.

Similarly the no. of primes $q \leqq m$ for which

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

is greater than

$$\frac{m}{2\phi(C) \log m} - \sum_{p_i/B} \pi(m\,;\, p_i C, 1)$$

But since $p_i C \leqslant A' \leqslant A < m^{\epsilon}$ it follows from Brun's method that

$$\pi(m\,;\, p_i C, 1) < \frac{c_1\, m}{\phi(p_i C) \log m}$$

(c's denoting absolute constants)

Hence

$$\sum_{p_i/B} \pi(m\,;\, p_i C. 1) < \sum_{p_i/B} \frac{c_1\, m}{\phi(p_i C) \log m}$$

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

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 no. of primes q such that

$$q - 1 \equiv 0(\mathrm{C}), \quad (q - 1, \mathrm{B}) = 1$$

is greater than $\dfrac{m}{4\phi(\mathrm{C}) \log m}$

Hence

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

We evidently have

$$\mathrm{S}' \geqslant \sum_{\mathrm{B}/\mathrm{A}'} \mathrm{S_B} > \frac{2^{\frac{\lambda}{2} - 1} m^2}{8\mathrm{A}' (\log m)^2}$$

But the integers of the form $(p - 1)(q - 1)$ with $p, q \leqslant m$ 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) $$\frac{2^{\frac{\lambda}{2} - 1}}{8 \log^2 m} = \frac{2^{\frac{\lambda}{2}}}{16 (\log m)^2} \text{ solutions.}$$

But

$$\lambda > \frac{\log \mathrm{A}}{3 \log \log \mathrm{A}}$$

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

$$\{4 (\log \mathrm{A})^2, (\log \mathrm{A})^3\}$$

is greater than A (this fact follows from the Prime Number Theorem).

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

$$\frac{2^{\frac{\lambda}{2}}}{16 (\log m)^2} > \frac{2^{\frac{\log \mathrm{A}}{6 \log \log \mathrm{A}}}}{16.64. (\log \mathrm{A})^4} > \exp\,[(\log m)^{\frac{1}{2} - \epsilon}]$$

where $\epsilon > 0$ is arbitrary.

Hence for $f(n)$, the no. of solutions of $n = (p - 1)(q - 1)$ we have,

$$\log f(n) = \Omega\{(\log n)^{\frac{1}{2} - \epsilon}\}$$

where $\epsilon > 0$ is arbitrary, the theorem of Erdös.

3. It is known that if the " extended Riemann hypothesis " is true then, if $(l, k) = 1$, $x \geqslant k^3$,

$$\lim_{k \to \infty} \frac{\pi(x\,;\, k, l)}{x/\phi(k) \log x} = 1.$$

Using this fact and $m = \mathrm{A}^3$, $\mathrm{A}' = \mathrm{A}$ in the above argument, we find that if the " extended Riemann hypothesis " is true, then $f(n) \geq \exp\left(\dfrac{c \log n}{\log \log n}\right)$ for some absolute constant $c > 0$, is true for infinitely many n.