ACTA ARITHMETICA
VIII (1963)

Note on a paper of A. Rotkiewicz

by

T. ESTERMANN (London)

In his paper *Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme* $nk+1$ (Enseignement Math. 7 (1961), pp. 277-280), A. Rotkiewicz has given a simple elementary proof of the particular case of Dirichlet's prime number theorem which states that, for every natural number k, there are infinitely many primes $p\equiv 1 \pmod{k}$. The proof can be made even simpler.

I follow Rotkiewicz in noting that it is sufficient to prove the following

THEOREM. *Let k be any integer greater than* 1. *Then there is a prime p such that*

$$p\equiv 1 \pmod{k}\,. \tag{1}$$

Proof. For any positive rational number r, let $\operatorname{num} r$ and $\operatorname{den} r$ be the numerator and the denominator of the fraction that expresses r in its lowest terms.

The following lemma is trivial:

LEMMA 1. *Let $n_1, n_1, \dots, n_l$ be natural numbers, let each of the numbers $m_1, m_2, \dots, m_l$ be either* 1 *or* -1, *and let*

$$\prod_{h=1}^{l} n_h^{m_h} = r\,.$$

Then $\operatorname{num} r \operatorname{den} r$ *is a divisor of* $n_1 n_2 \dots n_l$.

Now let

$$r=\prod_{d\mid k}(k^{k/d}-1)^{\mu(d)}\,, \tag{2}$$

where μ is Möbius's function.

LEMMA 2. *Let p be any prime divisor of* $\operatorname{num} r \operatorname{den} r$. *Then* (1) *holds.*

Proof. Let k' be the greatest square-free divisor of k. Then, by (2),

$$r=\prod_{d\mid k'}(k^{k/d}-1)^{\mu(d)}\,. \tag{3}$$

Hence, by Lemma 1,

$$\operatorname{num} r \operatorname{den} r \,\Big|\, \prod_{d\mid k'} (k^{k/d}-1),$$

which implies that p divides at least one of the factors of the last product. In other words, there is a natural number d_0 such that

(4) $$d_0 \mid k'$$

and

(5) $$p \mid k^{k/d_0}-1 .$$

By (5),

(6) $$p \nmid k .$$

Hence the order of $k \pmod p$ exists. Let us denote it by b. Then $k^m \equiv 1 \pmod p$ if and only if $b \mid m$. Hence

(7) $$b \mid p-1$$

and, by (5), $b \mid k/d_0$, which implies

(8) $$b \mid k .$$

I shall prove that

(9) $$b = k .$$

Suppose this is not so. Then, by (8), k/b is an integer greater than 1. Hence there is a prime q such that

(10) $$q \mid k/b ,$$

i.e.

(11) $$b \mid k/q .$$

Now we have

(12) $$\prod_{d\mid k'} f(d) = \prod_{d\mid k'/q} \{f(d)f(qd)\}$$

for any function f for which the left-hand side of this equation exists. Taking $f(d) = (k^{k/d}-1)^{\mu(d)}$, we obtain from (3) and (12) that

(13) $$r = \prod_{d\mid k'/q} \left(\frac{k^{k/d}-1}{k^{k/(qd)}-1}\right)^{\mu(d)} .$$

Dealing with (13) as we dealt with (3), we find that there is a natural number d_1 such that

(14) $$d_1 \mid k'/q$$

and

(15) $$p \,\Big|\, \frac{k^{k/d_1}-1}{k^{k/(qd_1)}-1} ,$$

which implies $p \mid k^{k/d_1}-1$, i.e. $k^{k/d_1} \equiv 1 \pmod p$, i.e. $b \mid k/d_1$. From this and (11) we obtain $b \mid (k/d_1, k/q)$. Now, by (14), $k/(qd_1)$ is an integer, and $(q, d_1) = 1$ (since k' is square-free). Hence $(k/d_1, k/q) = k/(qd_1)\cdot(q, d_1) = k/(qd_1)$. It follows that $b \mid k/(qd_1)$, i.e.

(16) $$k^{k/(qd_1)} \equiv 1 \pmod p .$$

Now

$$\frac{k^{k/d_1}-1}{k^{k/(qd_1)}-1} = \sum_{n=0}^{q-1} k^{nk/(qd_1)}$$

hence, by (16),

$$\frac{k^{k/d_1}-1}{k^{k/(qd_1)}-1} \equiv q \pmod p ,$$

and hence, by (15), $p \mid q$. From this and (10) it follows that $p \mid k$, which contradicts (6). This proves (9), and (1) follows from (9) and (7), so that Lemma 2 is proved.

To complete the proof of the theorem, we still have to show that there exists a prime divisor of $\operatorname{num} r \operatorname{den} r$, i.e. that

(17) $$r \neq 1 .$$

LEMMA 3. *Let $n_1, n_2, \ldots, n_l$ be distinct natural numbers, and let each of the numbers $m_1, m_2, \ldots, m_l$ be either 1 or -1. Then*

(18) $$\prod_{h=1}^{l} (1-k^{n_h})^{m_h} \neq 1 .$$

Proof. Suppose (without loss of generality) that n_1 is the least of the numbers $n_1, n_2, \ldots, n_l$. Let S be the set of those natural numbers $h \leqslant l$ for which $m_h = m_1$, and T the set of those for which $m_h = -m_1$. Then (18) is equivalent to

$$\prod_{h\in S} (1-k^{n_h}) \neq \prod_{h\in T} (1-k^{n_h}) .$$

Now $n_h \geqslant n_1+1$ $(h = 2, 3, \ldots, l)$. Hence the two sides of (19) are respectively congruent to $1-k^{n_1}$ and $1 \pmod{k^{n_1+1}}$. This proves Lemma 3.

Let $d_1, d_2, \ldots, d_l$ be the positive divisors of k'. Let $n_h = k/d_h$ and $m_h = \mu(d_h)$. Then (since l is even) it follows from (3) that r is equal to the left-hand side of (18), and we obtain (17) from Lemma 3.

UNIVERSITY COLLEGE, LONDON

Reçu par la Rédaction le 24. 10. 1962