BULLETIN DE L'ACADÉMIE
POLONAISE DES SCIENCES
Série des sciences math., astr.
et phys. — Vol. X, No. 12, 1962

MATHEMATICS
(THEORY OF NUMBERS)

Some Remarks on the Functions φ and σ

by

P. ERDŐS

Presented by W. SIERPIŃSKI on October 9, 1962

In a previous psper [I] I proved answering a question of Miss Jankowska that there exist infinitely many pairs of squarefree integers a and b satisfying

$$(a, b) = 1, \quad \varphi(a) = \varphi(b), \quad \sigma(a) = \sigma(b), \quad \nu(a) = \nu(b)$$

($\nu(n)$ denotes the number of distinct prime factors of n).

I also proved her second conjecture, namely that for every k there are k squarefree integers $a_1, \ldots, a_k$ satisfying

$$(1) \qquad \varphi(a_i) = \varphi(a_j), \quad \sigma(a_i) = \sigma(a_j), \quad \nu(a_i) = \nu(a_j), \quad 1 \leqslant i < j \leqslant k.$$

I further asked if for every k there exist integers which besides (1) also satisfy $(a_i, a_j) = 1$, $1 \leqslant i < j \leqslant k$. I cannot at present decide this but 1 can prove the following weaker

THEOREM. *For every k there are squarefree integers $a_1, \ldots, a_k$ satisfying*

$$(2) \qquad (a_i, a_j) = 1, \quad \varphi(a_i) = \varphi(a_j), \quad \nu(a_i) = \nu(a_j), \quad 1 \leqslant i < j \leqslant k.$$

The same result holds if we replace $\varphi(n)$ by $\sigma(n)$.

The novel feature of our proof will be that we use the following purely combinatorial theorem of Rado and myself ([2], theor. III).

Let $1 \leqslant a$ and b be positive integers and let

$$(3) \qquad c = b!\, a^{b+1}\left(1 - \frac{1}{2!\, a} - \frac{2}{3!\, a^2} - \cdots - \frac{b-1}{b!\, a^{b-1}}\right).$$

Then, if we have given any $c+1$ sets each having at most b elements we can always find $a+1$ of them having pairwise the same intersection.

From (3) we immediately deduce that if we have given $b!\, a^{b+1}$ sets each having at most b elements we can always find $a+1$ of them having pairwise the same intersection. We will use the theorem in this form, In our paper [2] we show that (3) is best possible for $a = 2$, $b = 2$, but it is no longer best possible for $a = 3$, $b = 2$. We thought it probable that in (3) $b!$ can be replaced by c_1^b for some absolute constant c_1. If this could be done, we could easily show by the methods of [1] and the present paper that (1) is solvable for every k with the added condition $(a_i, a_j) = 1$, $1 \leqq i < j \leqq k$. So far we were not successful in improving (3).

Denote by $d_p(n)$ the number of divisors of n of the form $p - 1$. There is an absolute constant c_2 and an infinite sequence $n_1 < n_2 < \ldots$ for which (cf [3])

$$(4) \qquad d_p(n_k) > n_k^{c_2/(\log\log n_k)^2}.$$

Denote by $q_1, \ldots, q_{t_k}$ the primes q_i for which $q_i - 1 \mid n_k$.

By (4) we have

$$t_k > n_k^{c_2/(\log\log n_k)^2}.$$

Put

$$w = \left[\frac{10(\log\log n_k)^2}{c_2}\right] + 1$$

and denote by

$$(5) \qquad s_1, \ldots, s_{l_k}, \quad l_k = \binom{t_k}{w} > \left(\frac{t_k}{w}\right)^w > \frac{n_k^{10}}{w^w} > n_k^5$$

the squarefree integers composed of the q_i and having w prime factors. Clearly ($\exp z = e^z$)

$$(6) \qquad \varphi(s_i) < s_i < n_k^w < \exp\left(\frac{20\log n_k(\log\log n_k)^2}{c_2}\right) = E.$$

From $q_i - 1 \mid n$ we obtain that the $\varphi(s_i)$ are all composed of the prime factors of n_k. From the prime number theorem (or a more elementary theorem) we obtain

$$(7) \qquad v(n_k) < 2\log n_k/\log\log n_k$$

and let $r_1, \ldots, r_u$, $u = v(n_k) < \dfrac{2\log n_k}{\log\log n_k}$ be the distinct prime factors of n_k. The number of distinct integers of the form $\varphi(s_i)$ is by (6) not greater than the number of integers not exceeding E composed of the r_i, $1 \leqq i \leqq u$. Clearly each r_i must occur with an exponent not greater than

$$(8) \qquad \frac{20\log n_k(\log\log n_k)^2}{c_2\log 2} = \frac{\log E}{\log 2} = t$$

(since $2^t = E$).

Therefore, the number of integers $\leqq E$ composed of the r's is less than $(1+t)^u$. By (7) and (8) for sufficiently large n_k

$$(1+t)^u < (\log n_k)^{2u} < n_k^4.$$

Thus, finally, the number of distinct integers of the form $\varphi(s_i)$ is less than n_k^4. But then, by (5), there are at least n_k of the s_i say

$$s_{i_1}, \dots, s_{i_z}, \quad z \geqslant n_k \quad \text{for which} \quad \varphi(s_{i_1}) = \dots = \varphi(s_{i_z}).$$

Now we apply the theorem of Rado and myself. We consider the primes q_i as elements and the s_{i_j}, $1 \leqslant j \leqslant z$ as sets having w elements. By (3) there are more than

$$\left(\frac{n_k}{w!}\right)^{1/(w+1)} > n_k^{c_2/20(\log\log n_k)^2} \tag{9}$$

integers s_{i_j} having pairwise the same common factor. We obtain (9) by putting in (3) $c = n_k$, $b = w$, $a = n_k^{c_2/20(\log\log n_k)^2}$. Dividing away with this common factor we finally obtain more than $n_k^{c_2/20(\log\log n_k)^2}$ integers $\leqslant E$ (by (6) the s_i are $\leqslant E$) which are pairwise relatively prime and for which the value of the φ function coincides. This completes the proof of our Theorem.

We clearly obtain the following stronger result:

For infinitely many m there are more than

$$m^{c_3/(\log\log m)^2}$$

pairwise relatively prime integers $i_1, \dots, i_l$ ***for which*** $\varphi(i_t) = m$, $1 \leqslant t \leqslant l$.

I pointed out in [1] that $m^{c_3/(\log\log m)^2}$ can certainly not be replaced here by $m^{c_4/\log\log m}$ if c_4 is sufficiently large, thus our result is fairly sharp.

MATHEMATICS DEPARTMENT, UNIVERSITY COLLEGE, LONDON

REFERENCES

[1] P. Erdös, Solution *of two problems of Jankowska*, Bull. Acad. Polon. Sci., Sér. sci. math., astr. et phys., 6 (1958), 545—547.

[2] P. Erdös and R. Rado, *Intersection theorems for systems of sets,* Jour. London Math. Soc., 35 (1960), 85—90.

[3] K. Prachar, *Über die Anzahl der Teiler einer natürlichen* Zahl, *welche die Form* $p-1$ *haben*, Monatsh. für Math., 59 (1955), 91—103.