SOME ASYMPTOTIC FORMULAS IN NUMBER THEORY

BY

P. ERDÖS, *University of Syracuse.*

[Received 15 October, 1948.]

Szele[1] recently proved that the necessary and sufficient condition that there should be only one abstract group of order m is that $(m, \phi(m)) = 1$. In the present note we are going to investigate how many such integers there are up to n. In fact we prove the following

THEOREM. *Denote by $A(n)$ the number of integers $m < n$ for which $(m, \phi(m)) = 1$. Then*

$$A(n) = (1+o(1))\frac{ne^{-\gamma}}{\log\log\log n},$$

where γ is Euler's constant.

Throughout this paper p, q, r and s will denote primes, the c's denote absolute constants, $\epsilon > 0$ is a number which can be chosen arbitrarily small.

Clearly $(m, \phi(m)) = 1$ if and only if m is squarefree and m is not divisible by $p.\ q$, where $q \equiv 1 \pmod p$.

Denote by $A_p(n)$ the number of integers $m \leqslant n$ for which $(m, \phi(m)) = 1$ and the smallest prime factor of m is p. Clearly

$$A(n) = \sum_{p \leqslant n} A_p(n) = \Sigma_1 + \Sigma_2 + \Sigma_3, \tag{1}$$

where in Σ_1, $\quad p < (\log\log n)^{1-\epsilon}$,

in Σ_2, $\quad (\log\log n)^{1-} \leqslant p \leqslant (\log\log n)^{1+\epsilon}$

and in Σ_3, $\quad (\log\log n)^{1+\epsilon} < p$.

First we prove three lemmas.

LEMMA I. *Let $p < (\log\log n)^{1-\epsilon}$. Then*

$$\sum{}' \frac{1}{q} > c_1 \frac{\log\log n}{p} > (\log\log n)^{\epsilon/2},$$

where the dash indicates that the summation is extended over the $q \equiv 1 \pmod p$ which satisfy $q < n^{1/(\log\log n)^2}$.

1. *Comment. Math. Helv.*, 20 (1947), p. 265-7.

A result of Page[1] states that if $\pi(x, 1, k)$ denotes the number of primes $q \equiv 1 \pmod{k}$, then

$$\pi(x, 1, k) = (1+o(1)) \frac{x}{\phi(k) \log x}$$

uniformly for $k < \log x$. Thus if $x > \log n > e^p$, we have

$$\pi(x, 1, p) > \frac{1}{2} \frac{x}{p \log x}. \tag{2}$$

From (2) we obtain

$$\sum{}' \frac{1}{q} > \sum \frac{1}{4\, pl \log l} > c_1 \frac{\log \log n}{p},$$

where $\log n < l < n^{1/(\log \log n)^3}$ which proves the lemma.

LEMMA II. *Let p be any prime. Then*

$$\sum{}' \frac{1}{q} < c_2 \left(\frac{\log p + \log \log n}{p} \right),$$

where the dash indicates that $q \equiv 1 \pmod{p}$, $q \leqslant n$.

We have

$$\sum{}' \frac{1}{q} < \sum_{a=1}^{p} \frac{1}{1+ap} + \sum{}'' \frac{1}{q} < c_2 \frac{\log p}{p} + \sum{}'' \frac{1}{q}, \tag{3}$$

where in Σ'', $q \equiv 1 \pmod{p}$, $p^2 < q \leqslant n$. By a result of Titchmarsh[2] the number of primes $q \equiv l \pmod{p}$, $q \leqslant x$ is for $x > p^2$ less than

$$\frac{c_3\, x}{p \log x}.$$

Thus a simple argument shows that

$$\sum{}'' \frac{1}{q} < \frac{c_3}{p} \sum \frac{1}{x \log x} < \frac{c_2}{p} \log \log n. \tag{4}$$

Lemma II follows from (3) and (4).

LEMMA III. *Let $x \leqslant (\log \log n)^{1+\varepsilon}$ $(x \to \infty)$. Denote by $B_x(n)$ the number of integers $m \leqslant n$ not divisible by any prime $p \leqslant x$. Then uniformly in x*

1. *Proc. London Math. Soc.*, (2) (39) (1935), p. 136 equation (36).

2. *Rend. di Palermo*, 57 (1933), p. 478-9.

$$B_x(n) = (1+o(1))\, c^{-\gamma} \frac{n}{\log \log x}.$$

By the sieve of Eratosthenes we have

$$B_x(n) = n - \sum_{p \leqslant x} \left[\frac{n}{p}\right] + \sum \left[\frac{n}{p_1 p_2}\right] - \dots$$

$$= \prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) + O(2^x) = (1+o(1)) \frac{n e^{\gamma}}{\log \log x}.$$

From Lemma III we immediately obtain the following

COR. *Let $p \leqslant (\log \log n)^{1+\varepsilon}$. Denote by $C_p(n)$ the number of integers $m \leqslant n$ for which the least prime factor of m is p. Then*

$$C_p(n) = B_p\left(\frac{n}{p}\right) < c_3 \frac{n e^{-\gamma}}{p \log \log p}.$$

Now we can prove our theorem. First we estimate Σ_1. Let $p < (\log \log n)^{1-\varepsilon}$. $A_p(n)$ is clearly greater than the number of integers $m \leqslant n$ not divisible by any $q \equiv 1 \pmod p$ satisfying $q < n^{1/(\log \log n)2}$. By Brun's method[1] we thus obtain from Lemma I that

$$A_p(n) < c_4\, n\, \Pi' \left(1 - \frac{1}{q}\right) < c_5\, n\, e^{-(\log \log)^{\varepsilon/2}} = o\left(\frac{n}{(\log \log n)^2}\right),$$

where the dash indicates $q \equiv 1 \pmod p$, $q < n^{1/(\log \log n)^2}$. Thus

$$\sum_1 < \log \log n \max_{p \leqslant (\log \log n)^{1-\varepsilon}} A_p(n) = o\left(\frac{n}{\log \log n}\right). \qquad (5)$$

Now we estimate Σ_2. We have by the corollary to Lemma III that

$$\sum_2 < \sum' c_p(n) < c_6 \frac{n e^{-\gamma}}{\log \log \log n} \sum' \frac{1}{p} < c_7 \frac{\epsilon n}{\log \log \log n}, \qquad (6)$$

where the dash indicates that

$$(\log \log n)^{1-\varepsilon} \leqslant p \leqslant (\log \log n)^{1+\varepsilon}.$$

1. P. Erdös, *Proc. Cambridge Phil. Soc.*, 33 (1937), p. 8 Lemma 2. In this case one does not need the full strength of the method and the simpler arguments in Landau, *Zahlentheorie*, Vol. 1, will suffice.

Finally we estimate Σ_3. Put $x=(\log\log n)^{1+\varepsilon}$. Clearly by our remark at the beginning of the proof, i.e. $(m, \phi(m))=1$ if and only if m is squarefree, and is not divisible by any $p.q$ with $q\equiv 1 \pmod p$ we have

$$B_x(n) > \Sigma_3 > B_x(n) - \sum_{r>x}\frac{n}{r^2} - \sum{}'\frac{n}{s_1 s_2},$$

where the dash indicates that $s_1 > x$ and $s_2 \equiv 1 \pmod{s_1}$. By Lemmas II and III

$$(1+o(1))\frac{e^{-\gamma}n}{(1+\varepsilon)\log\log\log n} >$$

$$\Sigma_3 > (1+o(1))\frac{e^{-\gamma}n}{(1+\varepsilon)\log\log\log n)} - \frac{n}{x} - \sum_{s>x}\frac{\log s+\log\log n}{s^2}$$

$$> (1+o(1))\frac{e^{-\gamma}n}{(1+\varepsilon)\log\log\log n} - \frac{n}{x} - c_8\frac{\log x}{x} - \frac{\log\log n}{x}$$

$$= (1+o(1))\frac{e^{-\gamma}n}{(1+\varepsilon)\log\log\log n}. \quad (7)$$

Since ϵ can be chosen arbitrarily small, we obtain the theorem from (5), (6) and (7).

By more complicated methods we can prove the following result: Denote by $v(x)$ the number of prime factors of x. Then the number of integers $m \leqslant n$ for which $v\{m, \phi(m)\}$ does not satisfy

$$(1-\varepsilon)\log\log\log\log m < v\{(m, \phi(m))\} < (1+\varepsilon)\log\log\log\log m \text{ is } o(n).$$

An analogous but much harder problem was raised by Pillai[1]: Find an asymptotic formula for the number of integers $m \leqslant n$ which have no factor of the form $p(a.p+1)$. I can prove by much more complicated methods that the asymptotic formula for the number of these integers is

$$\frac{e^{-\gamma}}{\log 2}\frac{n}{\log\log n}.$$

I hope to return to this at another occasion.

1. *The Journal of Indian Math. Soc.*, 18 (1929-1930), p. 51-9.