critical line $\mathrm{Re}\, s = \frac{1}{2}$ does *not* contain an arithmetical progression. It follows that $f_{a,\beta}$ is *not* constant.

Case 4. $\sigma = \frac{1}{2}$. In this case we invoke a theorem of Putnam [2] saying that the set of zeros of $\zeta(s)$ on the critical line $\mathrm{Re}\, s = \frac{1}{2}$ does not contain an arithmetical progression. It follows that also in this case $f_{a,\beta}$ *cannot* be constant.

Case 5. $0 < \sigma < \frac{1}{2}$. Because of the functional equation for $\zeta(s)$ this case may be reduced to Case 3.

Summarizing, we have the following

THEOREM. *If a and β are positive constants and $f_{a,\beta}\colon \boldsymbol{R}\to\boldsymbol{R}$ is defined by* (3) *then $f_{a,\beta}$ is a constant function only in case $a = \beta = \dfrac{\log 2}{k}$, where k is any positive integer.*

Acknowledgement. The author wishes to thank J. Vaaler at the California Institute of Technology for drawing his attention to Putnam's paper [2].

References

[1] K. Knopp, *Theory and application of infinite series*, Blackie and Son Ltd., 1928.
[2] C. R. Putnam, *On the non-periodicity of the zeros of the Riemann zeta-function*, Amer. J. Math. 76 (1954), pp. 97–99.
[3] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Oxford 1951.
[4] *Wiskundige Opgaven*, Noordhoff N. V., Groningen, 19, I (1950), pp. 308–311.

MATHEMATICAL CENTRE
Amsterdam, Netherlands

Received on 26. 11. 1976 (897)

ACTA ARITHMETICA
XXXV (1979)

Some results in number theory, I

by

M. Ram Murty (Cambridge, Mass.) and V. Kumar Murty (Ottawa, Ont.)

Dedicated to the memory of Professor Paul Turán

Let $\varphi(n)$ denote Euler's totient function and $V(n)$ the number of distinct prime factors of n. In this paper, we shall study the quantity $V\big((n, \varphi(n))\big)$ which arises naturally in group theory. For example, letting $G(n)$ denote the number of non-isomorphic groups of order n, we have by a classical result of Burnside that $G(n) = 1$ if and only if $V(n, \varphi(n)) = 0$ (i.e. $(n, \varphi(n)) = 1$). Erdös [1] showed that the number $F_1(x)$ of $n \leqslant x$ satisfying the latter condition is

$$F_1(x) = \big(1+o(1)\big)xe^{-\gamma}/\log_3 x \tag{1}$$

where γ is Euler's constant and we write $\log_1 x = \log x$, $\log_a x = \log(\log_{a-1} x)$. More generally, we can define $F_k(x)$ to be the number of $n \leqslant x$ for which $G(n) = k$. The authors [2] have shown that for each k,

$$F_k(x) \ll x/\log_4 x.$$

The proof depended essentially on a weak form of the following result stated by Erdös in [1]: for each $\varepsilon > 0$, the number of $n \leqslant x$ that fail to satisfy

$$(1-\varepsilon)\log_4 n < V\big(n, \varphi(n)\big) < (1+\varepsilon)\log_4 n$$

is $o(x)$. (A proof of this was supplied by the authors in [2].)

It is an interesting number-theoretic problem to estimate the number $A_k(x)$ of $n \leqslant x$ for which $V\big(n, \varphi(n)\big) = k$. Our main result here is the following theorem.

THEOREM. *For each $k \geqslant 0$, we have*

$$A_k(x) = \frac{\big(1+o(1)\big)xe^{-\gamma}(\log_4 x)^k}{k!\log_3 x}. \tag{2}$$

The proof will require several lemmas and intermediate results. The first two lemmas are due to Erdös [1].

LEMMA 1. *Let p be a fixed prime. Then*
$$\sum_{s\leqslant x}{}^{*}\frac{1}{s}\ll\frac{1}{p}(\log p+\log_2 x),$$
where the asterisk indicates that the sum is over primes $s\leqslant x$, $s\equiv 1\pmod p$.

We remark here that unless otherwise stated, p, q and s will denote primes.

LEMMA 2. *Let $p<(\log_2 x)^{1-\varepsilon}$. Then the number of $pm\leqslant x$ such that m has no prime divisor $\equiv 1\pmod p$ is $o(x/(\log_2 x)^2)$, uniformly in p.*

LEMMA 3. *Let $H_k(x)$ be the number of $n\leqslant x$ of the form $n=p_1p_2\dots p_k m$, where*

(i) $p_i<(\log_2 x)^{1-\varepsilon}$, $i=1,2,\dots,k$,

(ii) *all the prime divisors of m are* $\geqslant(\log_2 x)^{1+\varepsilon}$,

(iii) $(m,\varphi(m))=1$.

Then for each fixed k,
$$H_k(x)=\frac{(1+o(1))xe^{-\gamma}(\log_4 x)^k}{k!\log_3 x}.$$

Proof. By definition,
$$H_k(x)=\sum_p\sum_m{}'1 \tag{3}$$
where the outer sum is over all $p_i<(\log_2 x)^{1-\varepsilon}$ $(1\leqslant i\leqslant k)$ and the inner sum is over $m\leqslant x/p_1\dots p_k$ satisfying (ii) and (iii). Erdös' proof of (1) shows that
$$\sum_m{}'1=\frac{(1+o(1))xe^{-\gamma}}{(p_1p_2\dots p_k)\log_3 x} \tag{4}$$
and as the product $p_1\dots p_k$ is obtained $k!$ times in the k-fold outer sum of (3), we get
$$H_k(x)=\frac{(1+o(1))xe^{-\gamma}}{k!\log_3 x}\Big(\sum_p\frac{1}{p}\Big)^k=\frac{(1+o(1))xe^{-\gamma}(\log_4 x)^k}{k!\log_3 x}$$
proving the lemma.

We are now ready to prove our theorem.

Proof of theorem. We shall give the proof for $k=1$ and then sketch the modifications needed for general k. Write
$$A_1(x)=A_1'(x)+A_1''(x) \tag{5}$$
where $A_1'(x)$ counts the contribution of squarefree n to $A_1(x)$ and $A_1''(x)$ counts the remaining n. First we estimate $A_1''(x)$. If n is not squarefree and $V(n,\varphi(n))=1$ then certainly $n=p^a m$ $(a\geqslant 2)$ with $(p,m)=1$ and $(m,\varphi(m))=1$. The number of such $n\leqslant x$ with $p>\log_2 x=y$ (say) is clearly
$$\ll\sum_{p>y}\sum_{a\geqslant 2}\frac{x}{p^a}\ll\frac{x}{y},$$
and the number of remaining non-squarefree n in $A_1(x)$ is
$$\ll\sum_{p\leqslant y}\sum_{a\geqslant 2}A_0\Big(\frac{x}{p^a}\Big)\ll\frac{x}{\log_3 x}$$
using (1). Thus, we have
$$A_1''(x)\ll x/\log_3 x. \tag{6}$$
If n is squarefree, then $V(n,\varphi(n))=1$ implies that
$$n=pm,\ (m,\varphi(m))=1 \text{ and } m \text{ has at least one prime divisor } q\equiv 1\pmod p. \tag{7}$$
Let $\varepsilon>0$ be fixed. Then, we write
$$A_1'(x)=\Sigma_1+\Sigma_2+\Sigma_3+\Sigma_4$$
where the sums are over those $n\leqslant x$ in $A_1'(x)$ of the form (7) and

in Σ_1, $p>(\log_2 x)^{1+\varepsilon}$,

in Σ_2, $(\log_2 x)^{1-\varepsilon}\leqslant p\leqslant(\log_2 x)^{1+\varepsilon}$,

in Σ_3, $p<(\log_2 x)^{1-\varepsilon}$ and at least one prime divisor of m is $<(\log_2 x)^{1-\varepsilon}$,

in Σ_4, $p<(\log_2 x)^{1-\varepsilon}$ and all the prime divisors of m are $>(\log_2 x)^{1-\varepsilon}$.

Clearly, we have by Lemma 1,
$$\Sigma_1\ll\sum_p\sum_{q<x}{}^{*}\frac{x}{pq}\ll\sum_p\frac{x}{p^2}(\log p+\log_2 x) \tag{8}$$
$$\ll\frac{x}{(\log_2 x)^{1+\varepsilon}}(\log_3 x+\log_2 x)=o(x\log_4 x/\log_3 x).$$
Also, we get from (1) that
$$\Sigma_2\ll\sum A_0\Big(\frac{x}{p}\Big)\ll\sum\frac{x}{p\log_3(x/p)}\ll x/\log_3 x, \tag{9}$$
where all the sums are over p in the range indicated for Σ_2. Now from Lemma 2, the number of $m\leqslant x$, $(m,\varphi(m))=1$ which have a prime divisor $<(\log_2 x)^{1-\varepsilon}$ is
$$o(x/(\log_2 x)^2)(\log_2 x)^{1-\varepsilon}=o(x/\log_2 x).$$
Hence,
$$\Sigma_3=o\Big(\frac{x}{\log_2 x}\sum\frac{1}{p}\Big)=o\Big(\frac{x\log_4 x}{\log_2 x}\Big) \tag{10}$$

where the sum is over $p < (\log_2 x)^{1-\varepsilon}$. For Σ_4, we write

(11) $$\Sigma_4 = \Sigma_4' + \Sigma_4''$$

where in the first sum, all the prime divisors of m are $> (\log_2 x)^{1+\varepsilon}$, and the second sum contains the remaining n of Σ_4. Thus, for the n in Σ_4'', there is a prime divisor q (say) with

(12) $$(\log_2 x)^{1-\varepsilon} < q < (\log_2 x)^{1+\varepsilon}$$

so

$$\Sigma_4'' \ll \sum_p \sum_q A_0(x/pq) \ll \frac{x}{\log_3 x} \sum_{p,q} \frac{1}{pq}$$

where the sum over q is in the range (12) and the sum over p is in the range specified for Σ_4. The sum over q is clearly $< \varepsilon$ so we get

(13) $$\Sigma_4'' < \varepsilon x \log_4 x / \log_3 x.$$

Finally, recalling the definition of $H_1(x)$ from Lemma 3, noting that our n are now squarefree, and that in the range of Σ_4 every number in (7) satisfies $V(n, \varphi(n)) = 1$, we get

$$H_1(x) \geqslant \Sigma_4' \geqslant H_1(x) - T(x)$$

where $T(x)$ is the number of $pm = n \leqslant x$ such that m has no prime divisor $\equiv 1 \pmod p$ and p is in the range specified for Σ_4. Lemmas 2 and 3 imply that

(14) $$\Sigma_4' = \frac{\big(1+o(1)\big) x e^{-\gamma} \log_4 x}{\log_3 x}$$

so that combining (5), (6), (8)–(11), (13) and (14), and noting that $\varepsilon > 0$ was arbitrary, the proof for $k = 1$ is completed.

Now we sketch the modifications needed in the above proof, for general k. As before, we write $A_k(x) = A_k'(x) + A_k''(x)$ using the notation as in (5). Recalling $y = \log_2 x$, we get

(15) $$A_k''(x) \ll \sum_{p \leqslant y} \sum_{a \geqslant 2} A_{k-1}\left(\frac{x}{p^a}\right) + \frac{x}{y} \ll \frac{x (\log_4 x)^{k-1}}{\log_3 x}$$

by induction. To estimate $A_k'(x)$, we write the $n \leqslant x$ that are counted, in the form

(16) $$n = p_1 \ldots p_k m, \quad \big(m, \varphi(m)\big) = 1 \quad \text{and} \quad \big(n, \varphi(n)\big) = p_1 \ldots p_k.$$

Then as before,

$$A_k'(x) = \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4$$

where now, the sums are over those $n \leqslant x$ of the form (16) and
- in Σ_1, some $p_i > (\log_2 x)^{1+\varepsilon}$,
- in Σ_2, some p_i satisfies $(\log_2 x)^{1-\varepsilon} < p_i < (\log_2 x)^{1+\varepsilon}$,
- in Σ_3, all $p_i < (\log_2 x)^{1-\varepsilon}$ and at least one prime divisor of m is $< (\log_2 x)^{1-\varepsilon}$,
- in Σ_4, all $p_i < (\log_2 x)^{1-\varepsilon}$ and all the prime divisors of m are $> (\log_2 x)^{1-\varepsilon}$.

For Σ_1, the estimate (8) holds as before, and also

(17) $$\Sigma_2 \ll x/\log_3 x, \quad \Sigma_3 = o\big(x (\log_4 x)^k / \log_3 x\big),$$

by simple modifications in (9) and (10). Finally, writing $\Sigma_4 = \Sigma_4' + \Sigma_4''$ in the same notation as in (11), we find again by a simple modification that

(18) $$\Sigma_4'' = o\big(x (\log_4 x)^k / \log_3 x\big)$$

and

(19) $$H_k(x) \geqslant \Sigma_4' \geqslant H_k(x) - \sum_{j=0}^{k-1} A_j(x)$$

as clearly all n counted by $H_k(x)$ satisfy $V\big(n, \varphi(n)\big) \leqslant k$. By induction,

$$\sum_{j=0}^{k-1} A_j(x) \ll x (\log_4 x)^{k-1} / \log_3 x,$$

so that by Lemma 3, we get from (19) that

(20) $$\Sigma_4' = \frac{\big(1+o(1)\big) x e^{-\gamma} (\log_4 x)^k}{k! \log_3 x}$$

and combining (15), (8), (17), (18) and (20), the proof of the theorem is complete.

Acknowledgement. We would like to thank Professor K. S. Williams for his helpful comments.

References

[1] P. Erdös, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. 12 (1948), pp. 75–78.

[2] M. Ram Murty and V. Kumar Murty, *The number of groups of a given order*, to appear.

M.I.T.
Cambridge, Massachusetts, U.S.A.
CARLETON UNIVERSITY
Ottawa, Ontario, Canada

Received on 31. 12. 1976 (906)