ACTA ARITHMETICA
XXII (1973)

On the values of Euler's φ-function

by

P. ERDÖS (Budapest) and R. R. HALL (Heslington)

Introduction. Let M denote the set of distinct values of Euler's φ-function, that is, $m \in M$ if and only if

$$m = \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

for some positive integer n. Let $m_1, m_2, m_3, \ldots$ be the elements of M arranged in increasing sequence.

Our main object in this paper is to estimate the sum

$$V(x) = \sum_{m_i \leqslant x} 1$$

from above. Note that $V(x) \geqslant \pi(x)$, for M includes the sequence $\{p-1\}$, and it was shown by Erdös [1] that for each positive ε,

$$V(x) = O\left(\frac{x}{\log^{1-\varepsilon} x}\right).$$

We prove the following

THEOREM. *For each $B > 2\sqrt{2/\log 2}$, we have that*

$$V(x) = O\left(\pi(x) \exp\{B\sqrt{\log\log x}\}\right).$$

We have not yet found a comparable estimate from below; we remark that it may be shown that

$$V(x) = \Omega\left(\pi(x)\,(\log\log x)^t\right)$$

for every fixed t, and we hope to study this further perhaps in a later paper.

An interesting problem is to investigate the gaps in the sequence $\{m_i\}$. Since this includes the sequence $\{p-1\}$, we have that

$$m_{i+1} - m_i = O(m_i^a)$$

for every $a > 3/5$ by Montgomery's estimate [2] for the difference between consecutive primes. It is clear that our theorem gives

$$m_{i+1} - m_i = \Omega\left(\frac{\log m_i}{\exp\{B\sqrt{\log\log m_i}\}}\right)$$

for every $B > 2\sqrt{2/\log 2}$, and it is possible that in fact

$$m_{i+1} - m_i = \Omega(\log m_i),$$

although we cannot prove this. We now give the proof of our main result.

LEMMA 1. *Let $\omega(n)$ denote the number of prime factors of n counted according to multiplicity. Then the number of integers $n \leqslant x$ for which*

$$\omega(n) \geqslant \frac{2}{\log 2}\log\log x$$

is $O\{\pi(x)\log\log x\}$.

Proof. Let $\omega'(n)$ denote the number of odd prime factors of n, and $\nu(n)$ the number of distinct prime factors. Then for all y,

$$(1+y)^{\omega'(n)} = \sum_{d|n}{}' y^{\nu(d)}(1+y)^{\omega(d)-\nu(d)}$$

where $\sum'$ denotes a sum restricted to odd d. Hence for real, non-negative y,

$$\sum_{n\leqslant x}(1+y)^{\omega'(n)} \leqslant x\sum_{d\leqslant x}{}'\frac{y^{\nu(d)}}{d}(1+y)^{\omega(d)-\nu(d)} \leqslant x\prod_{3\leqslant p\leqslant x}\left(1+\frac{y}{p-1-y}\right),$$

provided $y < 2$. This does not exceed

$$x(\log x)^y\exp\left(\frac{A}{2-y}\right)$$

where A is an absolute constant. Setting $y = t-1$ we have that

$$\sum_{n\leqslant x} t^{\omega'(n)} \leqslant x(\log x)^{t-1}\exp\left(\frac{A}{3-t}\right)$$

provided $1 \leqslant t < 3$, and we deduce that for this range of values of t,

$$\sum_{\substack{n\leqslant x\\ \omega'(n)\geqslant t\log\log x}} 1 \leqslant x(\log x)^{t-1-t\log t}\exp\left(\frac{A}{3-t}\right).$$

Next, set $u = 2/\log 2 < 3$. If $\omega(n) \geqslant u\log\log x$ and $2^k \| n$, we must have $\omega'(n) \geqslant u\log\log x - k$. The number of integers $n \leqslant x$ for which

$k \geqslant \frac{1}{2}u\log\log x$ is $O(x/\log x)$ and so

$$\sum_{\substack{n\leqslant x\\ \omega(n)\geqslant u\log\log x}} 1 \leqslant \sum_{0\leqslant k\leqslant \frac{1}{2}u\log\log x}\ \sum_{\substack{m\leqslant x/2^k\\ \omega'(m)\geqslant u\log\log x-k}} 1 + O\left(\frac{x}{\log x}\right).$$

Set $k = h\log\log x$ so that h varies in the range $[0, \frac{1}{2}u]$. Certainly $1 \leqslant u-h < 3$, and so the inner sum on the right is

$$\ll \pi(x)\,(\log x)^{(u-h)-(u-h)\log(u-h)-h\log 2} \ll \pi(x)$$

since the maximum value of the exponent of $\log x$ is zero. Summing over $k \leqslant u\log\log x$ we obtain our result.

LEMMA 2. *The number of integers $n \leqslant x$ which have no prime factor exceeding*

$$x^{1/6\log\log x}$$

is

$$O\{\pi(x)\log\log x\}.$$

Proof. We divide the integers $n \leqslant x$ into two classes. If $n \leqslant \sqrt{x}$ or $\omega(n) \geqslant u\log\log x$, n belongs to the first class. Otherwise it belongs to the second class.

By Lemma 1, the number of integers in the first class is $O\{\pi(x)\log\log x\}$. If n belongs to the second class, its largest prime factor p must satisfy

$$p^{u\log\log x} > \sqrt{x}.$$

Since $u < 3$ this gives the result.

Proof of the Theorem. There exists an absolute constant c such that for all $n \geqslant 1$,

$$n/\varphi(n) \leqslant c\log\log 3\varphi(n).$$

Let $l = c\log\log 3x$, so that if $\varphi(n) \leqslant x$, then $n \leqslant xl$.

Let m be a value of φ not exceeding x. Either $\omega(m) \geqslant u\log\log x$, or $m = \varphi(n)$ where $n \leqslant xl$ and $\omega\{\varphi(n)\} < u\log\log x$. Therefore

$$V(x) \leqslant \sum_{\substack{m\leqslant x\\ \omega(m)\geqslant u\log\log x}} 1 + \sum_{\substack{n\leqslant xl\\ \omega\{\varphi(n)\}<u\log\log x}} 1.$$

The first sum is $O\{\pi(x)\log\log x\}$ by Lemma 1, and it remains to study the second. Note that $l \geqslant 1$ for $x \geqslant 1$, moreover that for $x > e^e$, which we may assume, the function

$$x^{1/6\log\log x}$$

is increasing. We may therefore restrict our attention to those n in the second sum with at least one prime factor larger than this; by Lemma 2

the number of integers $n \leqslant xl$ not counted is

$$O\left(\pi(x)\,(\log\log x)^2\right).$$

In the remaining sum, we may write $n = mp$ where

$$p > x^{1/6\log\log x}, \qquad m < lx^{1-1/6\log\log x}.$$

Then

$$V(x) \leqslant \sum_{\omega\{\varphi(m)\}<u\log\log x} \pi\left(\frac{xl}{m}\right) + O\left(\pi(x)\,(\log\log x)^2\right)$$

$$\leqslant \frac{x(\log\log x)^2}{\log x} \sum_{\omega\{\varphi(m)\}<u\log\log x} \frac{1}{m}.$$

We do not restrict the size of m in this sum, as the series is convergent, as we will show.

Consider the function

$$f(z) = \sum_{n=1}^{\infty} \frac{z^{\omega\{\varphi(n)\}}}{n}.$$

We are only concerned with real z in the range $0 \leqslant z < 1$, and we show that for these values of z the series is convergent. Incidentally, it is therefore absolutely convergent, and so $f(z)$ is well-defined, for $|z| < 1$. The behaviour of this series on the unit circle $|z| = 1$ is an interesting and complicated problem.

Since $\omega\{\varphi(n)\}$ is additive $z^{\omega\{\varphi(n)\}}$ is multiplicative and

$$f(z) = \prod_p \left(1 + \frac{z^{\omega(p-1)}}{p-z}\right) \leqslant \exp \sum_p \frac{z^{\omega(p-1)}}{p-z}$$

for $0 \leqslant z < 1$, provided the series on the right converges.

We apply the following result of Erdös [1]. For every $\varepsilon > 0$ there exists a positive $\delta = \delta(\varepsilon)$ such that the number of primes $p \leqslant x$ for which

$$|\nu(p-1) - \log\log x| \geqslant \varepsilon \log\log x$$

is

$$O\left(\frac{x}{(\log x)^{1+\delta}}\right).$$

Let k and H be positive numbers. Then

$$\sum_{\nu(p-1)\leqslant k} \frac{1}{p} \leqslant \sum_{p\leqslant H} \frac{1}{p} + \int_H^{\infty} \frac{1}{t^2} \Big(\sum_{\substack{p\leqslant t \\ \nu(p-1)\leqslant k}} 1 \Big)\, dt.$$

We select

$$H = H(k) = \exp\exp\left(\frac{k}{1-\varepsilon}\right)$$

so that in the integrand, the condition $\nu(p-1) \leqslant k$ implies that

$$\nu(p-1) \leqslant (1-\varepsilon)\log\log t.$$

The integral is therefore convergent, and we have that for $\varepsilon > 0$,

$$\sum_{\nu(p-1)\leqslant k} \frac{1}{p} \leqslant \frac{k}{1-\varepsilon} + C(\varepsilon)$$

where $C(\varepsilon)$ is independent of k. Therefore for $0 \leqslant z < 1$,

$$\sum_p \frac{z^{\nu(p-1)}}{p} = \sum_{k=0}^{\infty} z^k \sum_{\nu(p-1)=k} \frac{1}{p} = (1-z) \sum_{k=0}^{\infty} z^k \sum_{\nu(p-1)\leqslant k} \frac{1}{p}$$

$$\leqslant (1-z) \sum_{k=0}^{\infty} \left(\frac{kz^k}{1-\varepsilon} + C(\varepsilon) z^k\right) \leqslant \frac{z}{(1-\varepsilon)(1-z)} + C(\varepsilon).$$

Since $\omega(p-1) \geqslant \nu(p-1)$, this gives

$$\sum_p \frac{z^{\omega(p-1)}}{p-z} \leqslant \sum_p \frac{z^{\nu(p-1)}}{p} + \sum_p \frac{1}{p(p-1)} \leqslant \frac{z}{(1-\varepsilon)(1-z)} + C'(\varepsilon),$$

and so

$$f(z) \leqslant C''(\varepsilon) \exp\left\{\frac{z}{(1-\varepsilon)(1-z)}\right\}, \qquad \text{for} \qquad 0 \leqslant z < 1,$$

where $C'(\varepsilon)$ and $C''(\varepsilon)$ depend on ε only. We are now ready to estimate the sum

$$\sum_{\omega\{\varphi(m)\}<u\log\log x} \frac{1}{m}.$$

For $z < 1$, this does not exceed

$$f(z) z^{-u\log\log x}.$$

We may choose z optimally, and we select the value which gives

$$\left(\frac{z}{1-z}\right)^2 = (1-\varepsilon)\, u \log\log x.$$

Therefore

$$\sum_{\omega\{\varphi(m)\}<u\log\log x} \frac{1}{m} \leqslant C''(\varepsilon) \exp\left\{2\sqrt{\frac{u\log\log x}{1-\varepsilon}}\right\}$$

and so for every $B > 2\sqrt{2/\log 2}$, we have that

$$V(x) = O\{\pi(x)\exp\{B\sqrt{\log\log x}\}\}.$$

This completes the proof.

References

[1] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quart. Journ. Math. 6 (1935), pp. 205–213.

[2] H. L. Montgomery, *Zeros of L-functions*, Invent. Math. 8 (1969), pp. 346–354.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN
ACADEMY OF SCIENCES, Budapest
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, York

Received on 6. 12. 1971 (243)

ACTA ARITHMETICA
XXII (1973)

Waring's problem in GF[q, x]

by

William A. Webb (Pullman, Wash.)

I. Introduction. Throughout this paper $q = p^\gamma$, p a prime greater than k, γ a positive integer; GF(q) denotes the finite field of q elements; and GF[q, x] denotes the ring of polynomials over GF(q).

Waring's problem is that of expressing an element of an algebraic system as a fixed number of elements of that system which are kth powers. In [11] and [12] Schwarz and Tornheim deal with Waring's problem for systems including GF(q). In [10] Paley treats Waring's problem in GF[q, x], and in [2], [3], [4], [5], [6] and [7], Carlitz and Cohen consider several problems where the powers are restricted to squares.

In Paley's work, the degree of the summands is not restricted, while in the work of Carlitz and Cohen it is. This makes the problem quite different. Also, Carlitz and Cohen obtain formulas for the number of ways a polynomial in GF[q, x] may be written as a sum of squares, whereas Paley's method yields only existence.

In this paper we wish to show that $K = A_1^k + \ldots + A_s^k$ always has a solution for a fixed s and all K, where $\deg A_i^k = \deg K$. It is convenient to restrict the A_i to be primary (i.e. have leading coefficient of 1), so we will actually treat the following slightly more restrictive problem.

Let $R_s(K)$ denote the number of solutions of

$$K = \delta_1 A_1^k + \ldots + \delta_s A_s^k \tag{1}$$

where $\deg K = nk$; $\deg A_i = n$; A_i primary; $\delta_i \in \mathrm{GF}(q)$, $\delta_i \neq 0$, and δ_i a kth power in GF(q); and $\delta_1 + \ldots + \delta_s = \mathrm{signum}\, K$ (signum K = leading coefficients of K). (By [11] if $s \geqslant k$ it is possible to pick the δ_i to be kth powers and have $\delta_1 + \ldots + \delta_s = \mathrm{signum}\, K$. It is then possible to absorb the δ_i into the A_i^k to get a solution of the original problem.) We will obtain an asymptotic formula for $R_s(K)$ and in doing so show that $R_s(K) > 0$ for s of a certain magnitude.

Although there are many possible analogs of Waring's problem for GF[q, x], the above is one of the most natural and closest to Waring's problem for the rational integers. It should be noted that allowing the