PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 76, Number 2, September 1979

VALUES TAKEN MANY TIMES BY EULER'S PHI-FUNCTION

KENT WOOLDRIDGE

ABSTRACT. Let b_m denote the number of integers n such that $\phi(n) = m$, where ϕ is Euler's function. Erdős has proved that there is a $\delta > 0$ such that $b_m > m^\delta$ for infinitely many m. In this paper we show that we may take δ to be any number less than $3 - 2\sqrt{2}$.

We begin with a lemma that is a simple case of Theorem 3.12 in [2].

LEMMA 1. *Let a and k be relatively prime positive integers of opposite parity. Then for any $\varepsilon > 0$ we have*

$$\sum_{\substack{p<N \\ ap+k \text{ prime}}} 1 < (8+\varepsilon)H(a,k)N(\log N)^{-2}$$

for $N > N_0$, where

$$H(a,k) = \prod_{p>2}\left(1-(p-1)^{-2}\right)\prod_{\substack{p|ak \\ p>2}}(p-1)(p-2)^{-1}$$

and where N_0 depends only on ε.

Next we need a well-known lemma, whose proof may be found in [3].

LEMMA 2. *Let $d_1, d_2, \ldots$ be a sequence of complex numbers such that $\sum_{n=1}^\infty d_n n^{-1}$ is absolutely convergent. Then if*

$$\sum_{m=1}^\infty c_m m^{-s} = \sum_{m=1}^\infty m^{-s}\sum_{n=1}^\infty d_n n^{-s} \qquad (\operatorname{Re} s > 1),$$

we have

$$\lim_{x\to\infty} x^{-1}\sum_{m<x} c_m = \sum_{n=1}^\infty d_n n^{-1}.$$

Let k be a fixed positive integer. Let t be a positive number and let $r = 1/(1+t)$. Let $G(N,k,t)$ denote the number of primes p greater than k and not exceeding N for which $p-k$ has a prime divisor q such that $q > N^r$.

LEMMA 3. *For any $\varepsilon > 0$ and any positive $t < (\sqrt{2}-1)/2$ we have*

$$G(N,k,t) < 4(1+\varepsilon)t(1+t)N(\log N)^{-1} \tag{1}$$

for sufficiently large N.

Received by the editors August 11, 1978.
AMS (MOS) subject classifications (1970). Primary 10A20.

PROOF. Fix $\varepsilon > 0$. Let p be a prime such that $k < p \leqslant N$. Suppose $q \geqslant N^r$ is a prime dividing $p - k$. Then $p - k = aq$ with $(a, k) = 1$ and $a \leqslant N^{1-r}$. Clearly a and k are of opposite parity. Thus

$$G(N, k, t) \leqslant \sum_{\substack{k<p\leqslant N \\ (p-k)/a \text{ prime}}} \sum_{a\leqslant N^{1-r}}{}' 1 = \sum_{a\leqslant N^{1-r}}{}' \sum_{\substack{q\leqslant (N-k)/a \\ aq+k \text{ prime}}} 1 \tag{2}$$

where the prime indicates that the sum is over integers a such that a and k are of opposite parity and $(a, k) = 1$.

We shall show that, for $a \leqslant N^{1-r}$, we have

$$(N - k)\left(\log \frac{N - k}{a}\right)^{-2} \leqslant N(r \log N)^{-2} \tag{3}$$

for $N \geqslant M$, where M is independent of a. Since the left-hand side of (3) increases with a, the assertion (3) is true if it holds with a replaced by N^{1-r}. The resulting inequality is easily shown to be equivalent to

$$-r^2k(\log N)^2 \leqslant 2rN \log N \log(1 - kN^{-1}) + N(\log(1 - kN^{-1}))^2. \tag{4}$$

Note that $x \log(1 - kx^{-1}) \to -k$ as $x \to \infty$. This implies that the right-hand side of (4) is $O(\log N)$. The assertion (3) follows.

If we use Lemma 1 together with (2) and (3) we have

$$G(N, k, t) \leqslant 8(1 + \varepsilon)N(r \log N)^{-2} \sum_{a\leqslant N^{1-r}}{}' H(a, k)a^{-1}. \tag{5}$$

Define the multiplicative function f by $f(2) = 1$, $f(p) = 1 + (p - 2)^{-1}$ for $p > 2$, and

$$f(n) = \prod_{p|n} f(p) = \prod_{\substack{p|n \\ p>2}} \left(1 + \frac{1}{p - 2}\right).$$

Then we have

$$H(a, k) = Df(k)f(a),$$

where

$$D = \prod_{p>2} \left(1 + \frac{1}{p(p - 2)}\right)^{-1}.$$

Thus

$$\sum_{a\leqslant x}{}' H(a, k)a^{-1} = Df(k) \sum_{a\leqslant x}{}' f(a)a^{-1}. \tag{6}$$

We will use Lemma 2 and a partial summation to estimate the last sum.

First assume that k is even. Then, for $\operatorname{Re} s \geqslant 1$,

$$\sum_{n=1}^{\infty}{}' f(n)\frac{1}{ns} = \prod_{p\nmid k} \left\{1 + f(p)\left(\frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)\right\} = \zeta(s)g(s),$$

where

$$g(s) = \prod_{p|k}\left(1 - \frac{1}{p^s}\right)\prod_{p\nmid k}\left(1 + \frac{1}{p^s(p-2)}\right).$$

The product converges absolutely for Re $s > 0$.

Now assume that k is odd. Then, for Re $s \geqslant 1$,

$$\sum_{n=1}^{\infty}{}' f(n)\frac{1}{n^s} = \left(\frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots\right)\prod_{\substack{p\nmid k\\ p>2}}\left\{1 + f(p)\left(\frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)\right\}$$

$$= \zeta(s)g(s),$$

where

$$g(s) = \frac{1}{2^s}\prod_{p|k}\left(1 - \frac{1}{p^s}\right)\prod_{\substack{p\nmid k\\ p>2}}\left(1 + \frac{1}{p^s(p-2)}\right).$$

In either case, we can conclude from Lemma 2 that

$$\lim_{x\to\infty} x^{-1}\sum_{n<x}{}' f(n) = g(1) = B(k)\frac{\phi(k)}{k}\prod_{\substack{p\nmid k\\ p>2}}\left(1 + \frac{1}{p(p-2)}\right),$$

where $B(k)$ equals 1 or $\frac{1}{2}$ according as k is even or odd.

Let

$$C(x) = \sum_{n<x}{}' f(n) = g(1)x + o(x).$$

We have

$$\sum_{n<x}{}'\frac{f(n)}{n} = \frac{C(x)}{x} + \int_1^x \frac{C(u)}{u^2}\,du$$

$$= O(1) + g(1)\log x + o(\log x). \tag{7}$$

Combining (6) and (7) we see that

$$\sum_{a<x}{}' H(a,k)a^{-1} \sim Df(k)B(k)\frac{\phi(k)}{k}\prod_{\substack{p\nmid k\\ p>2}}\left(1 + \frac{1}{p(p-2)}\right)\log x$$

$$= \frac{1}{2}\log x. \tag{8}$$

Combining (5) and (8) we see that, for large N,

$$G(N,k,t) \leqslant 4(1+\varepsilon)t(1+t)N(\log N)^{-1},$$

since $(1-r)/r^2 = t(1+t)$. □

Note that the Prime-Number Theorem implies that Lemma 3 is trivial if $t \geqslant (\sqrt{2}-1)/2$.

Let $P(N,k,t)$ denote the number of primes in the interval $(k, N]$ such that $p - k$ is composed of primes less than N^r, where $r = (1+t)^{-1}$. Then

$$\pi(N) = \pi(k) + G(N,k,t) + P(N,k,t). \tag{9}$$

LEMMA 4. *For any* $t < (\sqrt{2} - 1)/2$ *and any*

$$\varepsilon < \varepsilon(t) = (1 - 4t(1 + t))/(2 + 5t + 4t^2)$$

we have

$$P\big((\log N)^{t+1}, k, t\big) > \varepsilon(\log N)^{t+1}(\log\log N)^{-1},$$

provided N is sufficiently large.

PROOF. Choose $t < (\sqrt{2} - 1)/2$ and $\varepsilon < \varepsilon(t)$. By the Prime-Number Theorem we have

$$\pi\big((\log N)^{t+1}\big) - \pi(k) > \frac{1-\varepsilon}{t+1}(\log N)^{t+1}(\log\log N)^{-1} \tag{10}$$

for large N. By Lemma 3 we have

$$G\big((\log N)^{t+1}, k, t\big) < 4(1 + \varepsilon)t(\log N)^{t+1}(\log\log N)^{-1} \tag{11}$$

for large N.

Combining (9), (10), and (11) we see that

$$\begin{aligned} &P\big((\log N)^{t+1}, k, t\big) \\ &\quad > \big\{(1-\varepsilon)(t+1)^{-1} - 4(1+\varepsilon)t\big\}(\log N)^{t+1}(\log\log N)^{-1} \end{aligned} \tag{12}$$

for large N. Since $t < (\sqrt{2} - 1)/2$, we have $(t + 1)^{-1} - 4t > 0$. It is easy to check that if $\varepsilon < \varepsilon(t)$, then

$$(1-\varepsilon)(t+1)^{-1} - 4(1+\varepsilon)t > \varepsilon. \tag{13}$$

If we combine (12) and (13) we have the result. □

Let $Q(N, k, t)$ denote the number of square-free integers not exceeding N that are composed of the primes counted by $P((\log N)^{t+1}, k, t)$.

LEMMA 5. *For any* $t < (\sqrt{2} - 1)/2$ *and any* ε *we have* $Q(N, k, t) > N^{(1-\varepsilon)(1-r)}$ *for large N, where* $r = (t + 1)^{-1}$.

PROOF. Let $t < (\sqrt{2} - 1)/2$ and assume without loss of generality that $\varepsilon < \varepsilon(t) < 1$. Let $u = \varepsilon/2$, and let

$$c = c(t, N) = \log N((t + 1)\log\log N)^{-1}.$$

Let $d = [c]$. Suppose q is square-free and has d prime factors that are counted by $P((\log N)^{t+1}, k, t)$. Then $q < (\log N)^{c(t+1)} = N$. The number of such q is the binomial coefficient $B = \binom{P}{d}$, where $P = P((\log N)^{t+1}, k, t)$. By Lemma 4 we have

$$P > \varepsilon(\log N)^{t+1}(\log\log N)^{-1}.$$

Since

$$\binom{m}{n} > \left(\frac{m}{n}\right)^n \quad \text{for } m > n > 1,$$

we have

$$B > \left(\frac{P}{d}\right)^d \geqslant \left(\varepsilon(t+1)(\log N)^t\right)^d. \tag{14}$$

For large N we have

$$\frac{(1-u)\log N}{(t+1)\log\log N} \leqslant d \leqslant \frac{(1+u)\log N}{(t+1)\log\log N} \tag{15}$$

and

$$\log\log N \geqslant \frac{(1+u)(-\log\varepsilon)}{tu}. \tag{16}$$

Now, using (15) and (16), we have

$$\begin{aligned}\varepsilon^d &> \exp\left((1+u)\log\varepsilon\log N((t+1)\log\log N)^{-1}\right)\\ &> \exp\left(-tu(1+t)^{-1}\log N\right) = N^{-u(1-r)}. \end{aligned}\tag{17}$$

Also,

$$\begin{aligned}(\log N)^{td} &\geqslant \exp\left(t(1-u)\log N((t+1)\log\log N)^{-1}\log\log N\right)\\ &= \exp\left(t(t+1)^{-1}(1-u)\log N\right) = N^{(1-u)(1-r)}. \end{aligned}\tag{18}$$

Using (14), (17), and (18), we see that

$$Q(N,k,t) > B > N^{(1-u)(1-r)-u(1-r)} = N^{(1-\varepsilon)(1-r)}. \quad \square$$

LEMMA 6. *Let $M(N)$ denote the number of integers not exceeding N that are composed of primes less than* $\log N$. *Then for any $\varepsilon > 0$ we have $M(N) \leqslant N^\varepsilon$ for sufficiently large N.*

PROOF. This is easily proved. The proof may be found in Erdős [1].

Let f be a multiplicative arithmetic function with $f(p) = p - k$ for prime p greater than k. We need not consider the values of f at higher prime powers or at primes not exceeding k.

THEOREM. *Let f be as above. If $\delta < 3 - 2\sqrt{2}$, then there are infinitely many m such that, for more than m^δ square-free integers q, we have $m = f(q)$.*

PROOF. If $t < (\sqrt{2} - 1)/2$ and $\varepsilon < \varepsilon(t)$ there are, by Lemma 10, at least $\varepsilon(\log N)^{t+1}(\log N)^{-1}$ primes in the interval $(k, (\log N)^{t+1}]$ such that $p - k$ is composed of primes less than $\log N$. Let $u = \varepsilon/2$ and let $r = (t+1)^{-1}$. By Lemma 5 the are at least $N^{(1-u)(1-r)}$ square-free integers $q \leqslant N$ that are composed of these primes. Let W be the number of values of $f(q)$ for these square-free integers. Since

$$f(q) = \prod_{p|q}(p-k)$$

we see that $f(q)$ is divisible only by primes less than $\log N$ for each of these q. By Lemma 6 we have $W \leqslant M(N) \leqslant N^u$ for large N. By the pigeon-hole principle there is an $m \leqslant N$ such that, for at least

$$N^{(1-u)(1-r)-u} \geqslant N^{(1-r)-\varepsilon} \geqslant m^{(1-r)-\varepsilon}$$

of these q, we have $m = f(q)$. If $\delta < 3 - 2\sqrt{2}$ we can choose $t < (\sqrt{2} - 1)/2$ and $\varepsilon < \varepsilon(t)$ so that $(1 - r) - \varepsilon = t(1 + t)^{-1} - \varepsilon > \delta$, since

$$\frac{(\sqrt{2} - 1)/2}{1 + (\sqrt{2} - 1)/2} = 3 - 2\sqrt{2}\,.$$

Thus for $\delta < 3 - 2\sqrt{2}$ and N sufficiently large, we have, for some $m \leqslant N$, more than m^{δ} square-free integers q such that $m = f(q)$. The theorem follows. □

References

1. P. Erdős, *On the normal number of prime factors of* $p - 1$ *and some related problems concerning Euler's* ϕ*-function*, Quart. J. Math. Oxford Ser. **6** (1935), 205–213.

2. H. Halberstam and H. E. Richert, *Sieve methods*, Academic Press, New York, 1974.

3. D. G. Kendall and R. A. Rankin, *On the number of Abelian groups of a given order*, Quart. J. Math. Oxford Ser. **18** (1947), 197–208.

Department of Mathematics, California State College, Stanislaus, Turlock, California 95380