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 \( \phi \) 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 \( \delta \) 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 \( \epsilon > 0 \) we have

\[
\sum_{p < N} \frac{1}{ap + k \text{ prime}} < (8 + \epsilon)H(a, k)N(\log N)^{-2}
\]

for \( N > N_0 \), where

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

and where \( N_0 \) depends only on \( \epsilon \).

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 \( \sum_{n=1}^{\infty} d_n n^{-s} \) is absolutely convergent. Then if

\[
\sum_{m=1}^{\infty} c_m m^{-s} = \sum_{m=1}^{\infty} m^{-s} \sum_{n=1}^{\infty} d_n n^{-s} \quad (\text{Re } s > 1),
\]

we have

\[
\lim_{x \to \infty} x^{-1} \sum_{m \leq x} c_m = \sum_{n=1}^{\infty} d_n n^{-1}.
\]

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 \( q > N' \).

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

\[
G(N, k, t) < 4(1 + \epsilon)t(1 + t)N(\log N)^{-1}
\]

for sufficiently large \( N \).

Received by the editors August 11, 1978.

PROOF. Fix $\epsilon > 0$. Let $p$ be a prime such that $k < p < N$. Suppose $q > N^r$ is a prime dividing $p - k$. Then $p - k = aq$ with $(a, k) = 1$ and $a < N^{1-r}$.

Clearly $a$ and $k$ are of opposite parity. Thus

$$G(N, k, t) < \sum_{k < p < N}^{(p - k)/a \text{ prime}} \sum_{a < N^{1-r}}^{' 1} \sum_{a < N^{1-r}}^{' q < (N-k)/a} 1$$

(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 $a < N^{1-r}$, we have

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

(3)

for $N > M$, 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

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

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

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

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

Then we have

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

where

$$D = \prod_{p > 2} \left( 1 + \frac{1}{p(p - 2)} \right)^{-1}.$$  (6)

Thus

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

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

First assume that $k$ is even. Then, for $\Re s > 1$,

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

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

The product converges absolutely for \( \Re s > 0 \).

Now assume that \( k \) is odd. Then, for \( \Re s > 1 \),
\[ \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \left( \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots \right) \prod_{p|k, p > 2} \left\{ 1 + f(p) \left( \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots \right) \right\} \]
\[ = \zeta(s) g(s), \]

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

In either case, we can conclude from Lemma 2 that
\[ \lim_{x \to \infty} x^{-1} \sum_{n \leq x} f(n) = g(1) = B(k) \frac{\phi(k)}{k} \prod_{p|k, p > 2} \left( 1 + \frac{1}{p(p - 2)} \right), \]
where \( B(k) \) equals 1 or \( \frac{1}{2} \) according as \( k \) is even or odd.

Let
\[ C(x) = \sum_{n \leq x} f(n) = g(1)x + o(x). \]

We have
\[ \sum_{n \leq x} f(n) = \frac{C(x)}{x} + \int_1^x \frac{C(u)}{u^2} \, du \]
\[ = O(1) + g(1) \log x + o(\log x). \quad (7) \]

Combining (6) and (7) we see that
\[ \sum_{a \leq x} \frac{H(a, k)a^{-1}}{n} \sim Df(k) B(k) \frac{\phi(k)}{k} \prod_{p|k, p > 2} \left( 1 + \frac{1}{p(p - 2)} \right) \log x \]
\[ = \frac{1}{2} \log x. \quad (8) \]

Combining (5) and (8) we see that, for large \( N \),
\[ G(N, k, t) < 4(1 + \epsilon) t(1 + t) N \log N \]

since \( (1 - r)/r^2 = t(1 + t) \). \( \Box \)

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

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 \( N' \), where \( r = (1 + t)^{-1} \). Then
\[ \pi(N) = \pi(k) + G(N, k, t) + P(N, k, t). \quad (9) \]
Lemma 4. For any $t < (\sqrt{2} - 1)/2$ and any
\[ \epsilon < \epsilon(t) = (1 - 4t(1 + t))/(2 + 5t + 4t^2) \]
we have
\[ P((\log N)^{r+1}, k, t) > \epsilon(\log N)^{r+1}(\log \log N)^{-1}, \]
provided $N$ is sufficiently large.

Proof. Choose $t < (\sqrt{2} - 1)/2$ and $\epsilon < \epsilon(t)$. By the Prime-Number Theorem we have
\[ \pi((\log N)^{r+1}) - \pi(k) > \frac{1 - \epsilon}{t + 1} (\log N)^{r+1}(\log \log N)^{-1} \quad (10) \]
for large $N$. By Lemma 3 we have
\[ G((\log N)^{r+1}, k, t) < 4(1 + \epsilon)t(\log N)^{r+1}(\log \log N)^{-1} \quad (11) \]
for large $N$.

Combining (9), (10), and (11) we see that
\[ P((\log N)^{r+1}, k, t) \]
\[ > \frac{(1 - \epsilon)(t + 1)^{-1} - 4(1 + \epsilon)t}{(log N)^{r+1}(log \log N)^{-1}} \quad (12) \]
for large $N$. Since $t < (\sqrt{2} - 1)/2$, we have $(t + 1)^{-1} - 4t > 0$. It is easy to check that if $\epsilon < \epsilon(t)$, then
\[ (1 - \epsilon)(t + 1)^{-1} - 4(1 + \epsilon)t > \epsilon. \quad (13) \]
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 $P((\log N)^{r+1}, k, t)$.

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

Proof. Let $t < (\sqrt{2} - 1)/2$ and assume without loss of generality that $\epsilon < \epsilon(t) < 1$. Let $u = \epsilon/2$, and let
\[ c = c(t, N) = \log N((t + 1)\log \log N)^{-1}. \]
Let $d = \lceil c \rceil$. Suppose $q$ is square-free and has $d$ prime factors that are counted by $P((\log N)^{r+1}, k, t)$. Then $q < (\log N)^{r(t+1)} = N$. The number of such $q$ is the binomial coefficient $B = \binom{P}{d}$, where $P = P((\log N)^{r+1}, k, t)$. By Lemma 4 we have
\[ P > \epsilon(\log N)^{r+1}(\log \log N)^{-1}. \]
Since
\[ \binom{m}{n} > \left( \frac{m}{n} \right)^n \quad \text{for } m > n > 1, \]
we have

\[ B > \left( \frac{\log N}{d} \right)^d > (\varepsilon(t + 1)(\log N))^{d}. \]  

(14)

For large \( N \) we have

\[ \frac{(1 - u)\log N}{(t + 1)\log \log N} < d < \frac{(1 + u)\log N}{(t + 1)\log \log N} \]  

(15)

and

\[ \log \log N > \frac{(1 + u)(-\log \varepsilon)}{tu}. \]  

(16)

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

\[ e^d > \exp((1 + u)\log \varepsilon \log N((t + 1)\log \log N)^{-1}) \]

\[ > \exp(-tu(1 + t)^{-1}\log N) = N^{-u(1-r)}. \]  

(17)

Also,

\[ (\log N)^{td} > \exp(t(1 - u)\log N((t + 1)\log \log N)^{-1}\log \log N) \]

\[ = \exp(t(t + 1)^{-1}(1 - u)\log N) = N^{(1-u)(1-r)}. \]  

(18)

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

\[ Q(N, k, t) > B > N^{(1-u)(1-r)-u(1-r)} = N^{(1-e)(1-r)}. \]  

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 \( M(N) < N^\varepsilon \) for sufficiently large \( N \).

Proof. This is easily proved. The proof may be found in Erdös [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 \( m^\delta \) 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 \( q < N \) 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 \( W < M(N) < N^u \) for large \( N \). By the pigeon-hole principle there is an \( m < N \) such that, for at least
\[ N^{(1-u)(1-r)-u} \geq N^{(1-r) - \varepsilon} \geq m^{(1-r) - \varepsilon} \]
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 \( m < N \), more than \( m^3 \) square-free integers \( q \) such that \( m = f(q) \). The theorem follows.

\[ \square \]

\textbf{References}


\textbf{Department of Mathematics, California State College, Stanislaus, Turlock, California 95380}