POPULAR VALUES OF EULER'S FUNCTION

CARL POMERANCE

§1. *Introduction.* For each natural number m, let $N(m)$ denote the number of integers n with $\phi(n) = m$, where ϕ denotes Euler's function. There are many interesting problems connected with the function $N(m)$, such as the conjecture of Carmichael that $N(m)$ is never 1 (see [**9**], for example) and the study of the distribution of the m for which $N(m) > 0$ (see Erdős and Hall [**5**]). In this note we shall be concerned with the maximal order of $N(m)$.

In [**3**], Erdős showed that there is a positive constant c such that

$$N(m) > m^c \quad \text{for infinitely many } m. \tag{1}$$

Erdős did not explicitly compute a value of $c > 0$ for which (1) is true, but such a computation could be carried out in Erdős's proof without too much trouble. Let C be the least upper bound of the set of c for which (1) holds. Wooldridge [**11**] has recently used estimates from Selberg's upper bound sieve to show that

$$C \geqslant 3-2\sqrt{2} > 0{\cdot}17157.$$

In this note we use certain improvements on average in the Brun–Titchmarsh theorem due to Hooley [**8**] together with Bombieri's theorem to show that

$$C \geqslant 1-625/512e \approx 0{\cdot}55092. \tag{2}$$

Recently, Iwaniec has made some further improvements on the Brun–Titchmarsh theorem (H. Iwaniec, "On the Brun–Titchmarsh theorem", to appear—Theorems 6 and 10) that allow us to obtain the slight improvement that

$$C > 0{\cdot}55655. \tag{3}$$

In particular, $N(m) > m^{5/9}$ for infinitely many m. We do not present here a proof of (3). Such a proof is obtained by following our proof of (2) using the new improvements on Brun–Titchmarsh. Erdős [**4**] has conjectured that $C = 1$.

In a private communication, Erdős informed me that Davenport and Heilbronn corresponded about the function

$$F_2(x) = \sum_{m \leqslant x} N(m)^2.$$

They were able to show $F_2(x)/x \to \infty$. They conjectured that there is some $c > 0$ such that

$$F_2(x) \gg x^{1+c}. \tag{4}$$

[MATHEMATIKA, 27 (1980), 84–89]

From our work we may choose in (4) any $c < 1-625/256e$. Using the method that improves (2) to (3), we have $F_2(x) \gg x^{10/9}$. Erdős conjectures that (4) holds for every $c < 1$.

In §2 we show that

$$N(m) \leqslant m \exp\left(-(1+o(1)) \log m \operatorname{logloglog} m/\operatorname{loglog} m\right). \tag{5}$$

We also give a heuristic argument that (5) is best possible in that there is an infinite set of m for which equality holds.

Let

$$F_1(x) = \sum_{m \leqslant x} N(m).$$

Bateman [1] has shown that

$$F_1(x) = c_0 x + O\left(x \cdot \exp\{-c_1(\log x \cdot \operatorname{loglog} x)^{1/2}\}\right)$$

where $c_0 = \zeta(2)\zeta(3)/\zeta(6)$ and $c_1 < 1/\sqrt{2}$ is arbitrary. Our conjecture that (5) is best possible implies

$$F_1(x) - c_0 x = \Omega\left(x \cdot \exp\{-(1+\varepsilon) \log x \cdot \operatorname{logloglog} x/\operatorname{loglog} x\}\right)$$

for every $\varepsilon > 0$, while (3) implies

$$F_1(x) - c_0 x = \Omega(x^{5/9}).$$

I take pleasure in acknowledging the helpful comments of Harold Diamond and Paul Erdős. I also wish to thank Paul Bateman for informing me of [11]. I am also grateful to H. Iwaniec for letting me see his manuscript.

§2. *An upper bound for $N(m)$ and a conjectured lower bound.* Let

$$L(x) = \log x \operatorname{logloglog} x/\operatorname{loglog} x.$$

A reading of the proof of Lemma 2 in [10], which is an improvement of Lemma 2 in Erdős [4], shows that actually the following result is proved.

THEOREM A. *Let $A(y)$ denote the number of square-free integers $n \leqslant y$ such that for every prime factor p of n, $p-1$ divides m. Then*

$$A(y) \leqslant y/e^{(1+o(1))L(y)},$$

uniformly for all m, as $y \to \infty$.

We now show that Theorem A implies (5). First note that there is an absolute constant α such that if $\phi(n) = m$, then $n < \alpha m \operatorname{loglog} m$ (*cf.* Hardy and Wright [7], Theorem 328). Let $N^*(m)$ denote the number of square-free n with $\phi(n) = m$. Then Theorem A implies

$$N^*(m) \leqslant A(\alpha m \operatorname{loglog} m) \leqslant m/e^{(1+o(1))L(m)} \tag{6}$$

This inequality is most of the battle in the proof of (5). We now make some crude estimates that allow us to pass from $N^*(m)$ to $N(m)$.

If $\phi(n) = m$, write $n = uv$ where u is square-full, v is square-free, and $(u, v) = 1$. Thus $\phi(v) \mid m$ and $u < \alpha(m/\phi(v))$ loglog m. The number of square-full numbers below x is $O(\sqrt{x})$. Thus

$$N(m) \ll \sum_{d \mid m} ((m/d) \operatorname{loglog} m)^{1/2} N^*(d). \tag{7}$$

Using the estimate (6) if $d > \log m$ and the trivial estimate $N^*(d) \ll d \operatorname{loglog} d$ if $d \leqslant \log m$, we have for all $d \mid m$,

$$d^{-1/2} N^*(d) \leqslant m^{1/2}/e^{(1+o(1))L(m)}.$$

Thus (7) implies

$$N(m) \ll d(m) \cdot m/e^{(1+o(1))L(m)} \ll m/e^{(1+o(1))L(m)},$$

where we use the maximal order of the divisor function (due to Wigert):

$$d(m) \leqslant 2^{(1+o(1)) \log m/\operatorname{loglog} m}.$$

We now give a heuristic argument that (5) is best possible. Let $\Psi(x, y)$ denote the number of integers $n \leqslant x$ free of prime factors exceeding y and let $\Pi(x, y)$ denote the number of primes $p \leqslant x$ such that $p-1$ is free of prime factors exceeding y. It is reasonable to guess that

$$\frac{1}{x} \Psi(x, y) \sim \frac{1}{\pi(x)} \Pi(x, y)$$

if $x \geqslant y$ and $y \to \infty$. In a forthcoming joint paper with Canfield and Erdős, we shall show

$$\frac{1}{x} \Psi\Big(x, \exp((\log x)^{1/2})\Big) = \exp\Big(-(1+o(1))2^{-1}(\log x)^{1/2} \operatorname{loglog} x\Big).$$

We now show that the conjecture that (5) is best possible follows from the conjecture

$$\frac{1}{\pi(x)} \Pi\Big(x, \exp((\log x)^{1/2})\Big) = \exp\Big(-(1+o(1))2^{-1}(\log x)^{1/2} \operatorname{loglog} x\Big). \tag{8}$$

Indeed, from (8), we have

$$M = \Pi\Big(\exp((\operatorname{loglog} z)^2),\ \log z\Big)$$

$$= \exp\Big((\operatorname{loglog} z)^2 - (1+o(1)) \operatorname{loglog} z \cdot \operatorname{logloglog} z\Big).$$

Thus if B is the number of square-free numbers composed of exactly $u = [\log z/(\log\log z)^2]$ of the primes counted by M, we have

$$B = \binom{M}{u} \geqslant \left(\frac{M}{u}\right)^u = z/e^{(1+o(1))L(z)}.$$

But every number n counted by B satisfies

(i) $n \leqslant z$,

(ii) every prime factor of $\phi(n)$ is at most $\log z$.

Thus ϕ maps the set of integers counted by B to a set of cardinality at most $\Psi(z, \log z)$. Thus there is a number $m \leqslant z$ such that

$$N(m) \geqslant \frac{B}{\Psi(z, \log z)} \geqslant z/e^{(1+o(1))L(z)},$$

where we use the result of Erdős (*cf.* de Bruijn [**2**]) that

$$\Psi(z, \log z) = 4^{(1+o(1))\log z/\log\log z}.$$

Thus the conjecture (8) implies that (5) is best possible.

§3. *The proof of* (2). If $0 < u \leqslant 1$, recall that $\Pi(x, x^u)$ denotes the number of primes $p \leqslant x$ such that $p-1$ is free of prime factors exceeding x^u.

THEOREM B (Erdős [**3**]). *Suppose that there is an* $\varepsilon > 0$ *such that* $\Pi(x, x^u) > \varepsilon\pi(x)$ *for all large* x. *Let* $m_1 < m_2 < \ldots$ *be the values of* m *where* $N(m) > m^{1-u}$. *Then there are infinitely many* m_i *and, in fact,* $\log m_{i+1}/\log m_i \to 1$.

Erdős did not state his theorem as strongly as we have, but his proof, with a few simple changes, does give Theorem B. In particular, one would argue from the Brun–Titchmarsh theorem that there is a $u' < u$ with $\Pi(x, x^{u'}) > \frac{1}{2}\varepsilon\pi(x)$ for all large x. Then following Erdős's argument for u', we have Theorem B.

What Theorem B does is allow us to take "ϕ" out of the problem: to get our results we need only study the function $\Pi(x, x^u)$. In fact, both our assertion (2) and our choice of c in (4) follow directly from Theorem B and the following.

THEOREM 1. *For each* $u > 625/512e$, *there is an* $\varepsilon > 0$ *such that* $\Pi(x, x^u) > \varepsilon\pi(x)$ *for all large* x.

To prove Theorem 1, we shall first prove

THEOREM 2. $\Pi(x, x^{1/2}) \geqslant \big(1 - 4\log(5/4) + o(1)\big)\pi(x)$.

Proof. Let q denote a variable prime. By $\pi(x, q, 1)$ we mean the number of primes $p \leqslant x$ with $q \mid (p-1)$. Let

$$H(t) = \sum_{x^{1/2} < q \leqslant t} \pi(x, q, 1)\log q.$$

Using partial summation we have

$$\pi(x)-\Pi(x, x^{1/2}) = \sum_{x^{1/2} < q \leqslant x} \pi(x, q, 1)$$

$$= \frac{H(x)}{\log x} + \int_{x^{1/2}}^{x} \frac{H(t)}{t \log^2 t}\, dt .$$

Now Goldfeld [6] has shown that Bombieri's theorem implies $H(x) \sim x/2$. Also Hooley [8] has shown that

$$H(t) \leqslant (4+o(1))x \log (tx^{-1/2})/\log x , \qquad x^{1/2} < t < x . \tag{9}$$

We use (9) for $x^{1/2} < t \leqslant x^{5/8}$. Beyond $x^{5/8}$, we use the trivial estimate $H(t) \leqslant H(x)$. Thus

$$\pi(x)-\Pi(x, x^{1/2}) \leqslant (\tfrac{1}{2}+o(1))\frac{x}{\log x} + \frac{(4+o(1))x}{\log x} \int_{x^{1/2}}^{x^{5/8}} \frac{\log (tx^{-1/2})}{t \log^2 t}\, dt$$

$$+(\tfrac{1}{2}+o(1))x \int_{x^{5/8}}^{x} \frac{dt}{t \log^2 t}$$

$$= (4 \log (\tfrac{5}{4})+o(1))\frac{x}{\log x},$$

which gives our result.

Proof of Theorem 1. Let $1/2 > u > 625/512e$. We have

$$\Pi(x, x^u) = \Pi(x, x^{1/2})-(\Pi(x, x^{1/2})-\Pi(x, x^u))$$

$$\geqslant (1-4 \log (5/4)+o(1))\pi(x)- \sum_{x^u < q \leqslant x^{1/2}} \pi(x, q, 1), \tag{10}$$

by Theorem 2 (again q represents primes). We now use Bombieri's theorem and the Brun–Titchmarsh theorem to estimate the sum in (10).

From Bombieri's theorem, there is a constant B such that

$$\sum_{x^u < q \leqslant x^{1/2}/\log^B x} \pi(x, q, 1) = \pi(x) \sum_{x^u < q \leqslant x^{1/2}/\log^B x} (q-1)^{-1} + O(x/\log^2 x) .$$

$$= \pi(x) \log \frac{1}{2u} + O(x \operatorname{loglog} x/\log^2 x) . \tag{11}$$

From the Brun–Titchmarsh theorem, we have

$$\sum_{x^{1/2}/\log^B x < q \leqslant x^{1/2}} \pi(x, q, 1) \ll \pi(x) \sum q^{-1} \ll x \operatorname{loglog} x/\log^2 x . \tag{12}$$

From (10), (11), (12) we have

$$\Pi(x, x^u) \geqslant \big(1-4\log(5/4)+\log(2u)+o(1)\big)\pi(x). \tag{13}$$

Let $\varepsilon = \frac{1}{2}(1-4\log(5/4)+\log(2u))$. Since $u > 625/512e$, we have $\varepsilon > 0$. From (13) we then have $\Pi(x, x^u) > \varepsilon\pi(x)$ for all large x.

Remark. Using the new results of Iwaniec, mentioned in the introduction, we have

$$\Pi(x, x^{1/2}) \geqslant 0{\cdot}120025\pi(x)$$

for all large x. Using this in the proof of Theorem 1 yields $\Pi(x, x^u) \gg \pi(x)$ for all $u \geqslant 0{\cdot}44345$.

References

1. P. T. Bateman. "The distribution of values of the Euler function", *Acta Arith.*, 21 (1972), 329–345.
2. N. G. de Bruijn. "On the number of positive integers $\leqslant x$ and free of prime factors $> y$, II", *Nederl. Akad. Wetensch. Proc. Ser.* A, 69 = *Indag. Math.*, 38 (1966), 239–247.
3. P. Erdős. "On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's ϕ-function", *Quart. J. Math.* (*Oxford Ser.*), 6 (1935), 205–213.
4. P. Erdős. "On pseudoprimes and Carmichael numbers", *Publ. Math. Debrecen*, 4 (1956), 201–206.
5. P. Erdős and R. R. Hall. "Distinct values of Euler's ϕ-function", *Mathematika*, 23 (1976), 1–3.
6. M. Goldfeld. "On the number of primes p for which $p+a$ has a large prime factor", *Mathematika*, 16 (1969), 23–27.
7. G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers* (Fourth Ed., Oxford University Press, London, 1960).
8. C. Hooley. "On the greatest prime factor of $p+a$", *Mathematika*, 20 (1973), 135–143.
9. C. Pomerance. "On Carmichael's conjecture", *Proc. Amer. Math. Soc.*, 43 (1974), 297–298.
10. C. Pomerance, J. L. Selfridge and S. S. Wagstaff. "The pseudoprimes to $25 \cdot 10^9$", *Math. Comp.*, to appear.
11. K. R. Wooldridge. "Values taken many times by Euler's phi-function", *Proc. Amer. Math. Soc.*, 76 (1979), 229–234.

Department of Mathematics,
University of Georgia,
Athens, Georgia 30602.

10A20: *NUMBER THEORY; Elementary number theory; Number theoretic functions.*

Received on the 20th of November, 1979.