JOURNAL OF NUMBER THEORY 12, 218–223 (1980)

A Note on the Least Prime in an Arithmetic Progression

CARL POMERANCE

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

Communicated by H. L. Montgomery

Received January 5, 1978; revised July 1, 1978

Let k, l denote positive integers with $(k, l) = 1$. Denote by $p(k, l)$ the least prime $p \equiv l \pmod{k}$. Let $P(k)$ be the maximum value of $p(k, l)$ for all l. We show $\liminf P(k)/(\varphi(k) \log k) \geqslant e^{\gamma} = 1.78107\ldots$ where γ is Euler's constant and φ is Euler's function. We also show $P(k)/(\varphi(k) \log k) \to \infty$ for almost all k.

1. INTRODUCTION

Let k, l denote positive integers with $(k, l) = 1$. Denote by $p(k, l)$ the least prime $p \equiv l \pmod{k}$. Let $P(k)$ be the maximum value of $p(k, l)$ for all l. Linnik [12] has shown there is a constant c with $P(k) \ll k^c$ and Graham [6] has shown we may take $c \leqslant 20$. Furthermore Chowla [1] has observed that if the Generalized Riemann Hypothesis holds, then $P(k) \ll k^{2+\epsilon}$ for every $\epsilon > 0$. Chowla conjectured $P(k) \ll k^{1+\epsilon}$ for every $\epsilon > 0$.

In this note we shall take up the subject of lower bounds for $P(k)$. Since $P(k)$ is at least as big as the $\varphi(k)$th prime (φ is Euler's function) and since $\log k \sim \log \varphi(k)$ as $k \to \infty$, the Prime Number Theorem gives

$$\alpha := \liminf_{k \to \infty} P(k)/(\varphi(k) \log k) \geqslant 1.$$

We prove $\alpha \geqslant e^{\gamma} = 1.78107 \cdots$, where γ is Euler's constant.

It is known that $P(k)/(\varphi(k) \log k)$ is unbounded. In fact, Prachar [13] and Schinzel [16] have shown there is an absolute constant c such that for each l there are infinitely many k with

$$p'(k, l) > ck \log k \cdot \log_2 k \cdot \log_4 k/(\log_3 k)^2$$

where $\log_2 k := \log\log k$, etc., and $p'(k, l)$ is the first prime $q > k$ with $q \equiv l \pmod{k}$. Wagstaff [19] has recently achieved a similar result for prime k.

By a slight modification of the argument Hensley and Richards [7] use to prove their key lemma 2 it follows that $P(k)/(\varphi(k) \log k)$ tends to infinity when k is restricted to prime values. In this note we show $P(k)/(\varphi(k) \log k)$

0022-314X/80/020218-06$02.00/0

tends to infinity for almost all k. More precisely, we show there is a set of integers Q with density 0 such that if $k \notin Q$, then

$$P(k) \geqslant (e^{\gamma} + o(1))\varphi(k) \log k \cdot \log_2 k \cdot \log_4 k/(\log_3 k)^2$$

The possible exceptional set Q is explicitly identified as those integers k with more than $\exp(\log_2 k/\log_3 k)$ distinct prime factors.

It is reasonable to conjecture that $P(k)/(\varphi(k) \log k)$ tends to infinity for all k. We cannot show this—the hardest values of k to treat seem to be the product of the first r primes for various r.

2. The Results

Let m be a positive integer. Jacobsthal [10] has defined $g(m)$ as the least integer such that every set of $g(m)$ consecutive integers contains one number relatively prime to m. It has been remarked by Erdös [5] and Hooley [8] that from Brun's method there is a constant c_0 such that

$$g(m) \ll (\log m)^{c_0}. \tag{1}$$

We note that by a recent result of Iwaniec [9], we may take $c_0 = 2$.

THEOREM 1. *Suppose k, m are integers, with $0 < m \leqslant k/(1 + g(k))$ and $(m, k) = 1$. Then $P(k) > (g(m) - 1)k$.*

Proof. There is an integer a such that each of

$$a + 1, \quad a + 2, \ldots, \quad a + g(m) - 1$$

has a prime factor in common with m. Then each of

$$b: = ka - jm + k, \quad ka - jm + 2k, \ldots, \quad ka - jm + (g(m) - 1)k$$

has a prime factor in common with m, for any choice of j. We wish to choose j so that $(b, k) = 1$ and $m < b \leqslant k$. To accomplish the first task we need only choose j relatively prime to k. To accomplish the second task we must choose j in a certain interval of length $k/m - 1 \geqslant g(k)$. Thus we can always accomplish both tasks. With j so chosen we have

$$p(k, b) \geqslant ka - jm + g(m)k = b + (g(m) - 1)k.$$

Hence $P(k) > (g(m) - 1)k$.

THEOREM 2. *For all k we have*

$$P(k) \gg (e^{\gamma} + o(1))\varphi(k) \log k.$$

Proof. Let $\epsilon > 0$ be arbitrarily small, but fixed. Let m be the product of the first $[(1 - \epsilon) \log k/\log_2 k]$ primes which do not divide k. Hence $(m, k) = 1$. Since m is about $k^{1-\epsilon}$, it follows from (1) that for $k > k_0(\epsilon)$, $m \leqslant k/(1 + g(k))$. Hence from Theorem 1, we have for $k > k_0(\epsilon)$, $P(k) > (g(m) - 1)k$. From a result of Erdös [5], we have for $k > k_1(\epsilon)$,

$$g(m) > (1 - \epsilon)(m/\varphi(m))\nu(m),$$

where $\nu(m)$ is the number of distinct prime factors of m. Hence for $k > k_2(\epsilon)$ we have

$$\begin{aligned} P(k) &> (g(m) - 1)k \\ &> \frac{(1 - \epsilon)m}{\varphi(m)} \cdot \frac{(1 - 2\epsilon)\log k}{\log_2 k} \cdot k \\ &> \frac{(1 - 3\epsilon)\, km}{\varphi(km)\log_2(km)} \cdot \varphi(k)\log k \\ &> (1 - 4\epsilon)\, e^{\gamma}\varphi(k)\log k, \end{aligned}$$

where the last inequality follows from Mertens' theorem.

THEOREM 3. *Let Q be the set of integers k with more than* $\exp(\log_2 k/\log_3 k)$ *distinct prime factors. Then for all $k \notin Q$ we have*

$$P(k) \geqslant (e^{\gamma} + o(1))\varphi(k)\log k \cdot \log_2 k \cdot \log_4 k/(\log_3 k)^2. \tag{2}$$

Proof. Let $\epsilon > 0$ be small and fixed and let $k \notin Q$. Let m be the product of the primes below $(1 - \epsilon)\log k$ which do not divide k. From Theorem 1 we have for $k > k_0(\epsilon)$ that $P(k) > (g(m) - 1)k$, so that our result will follow if we prove for all $k > k_1(\epsilon)$ that

$$g(m) > (1 - 3\epsilon)\, e^{\gamma}(\varphi(k)/k)\log k \cdot \log_2 k \cdot \log_4 k/(\log_3 k)^2. \tag{3}$$

To prove (3) we slightly alter the proof of a theorem of Schönhage [18] as amended by Rankin [14]. We divide the primes in m into 3 classes:

$$0 < p^{(1)} \leqslant y < p^{(2)} \leqslant z < p^{(3)} \leqslant x,$$

where $x = (1 - \epsilon)\log k$, $y = \exp((1 - \epsilon)\log x \cdot \log_3 x/\log_2 x)$, and $z = x/\log_2 x$. Let

$$u = (1 - 2\epsilon)\, e^{\gamma}(\varphi(k)/k)\, x \log x \cdot \log_3 x/(\log_2 x)^2.$$

To prove (3) we must show the primes $p^{(1)}$, $p^{(2)}$, $p^{(3)}$ can "sieve out" the interval $[1, u]$. More precisely, we must demonstrate the existence of integers

a_p where p runs over the prime factors of m, such that each $n \in [1, u]$ satisfies $n \equiv a_p \pmod{p}$ for one of the p.

We begin by casting out all multiples of the primes $p^{(2)}$ from $[1, u]$. Let R be the residual set. The only members of R not dealt with in the analogous residual set in the Rankin–Schönhage proof are among those $n \in [1, u]$ divisible by a prime $q \in (y, z]$ which is not a $p^{(2)}$. Such a prime q is necessarily a factor of k, and by our choice of k, there are at most $\exp(\log_2 k/\log_3 k)$ such q. Hence the number of such $n \in [1, u]$ is at most

$$(u/y) \cdot \exp(\log_2 k/\log_3 k) = o(u/\log x).$$

Hence, as with Rankin-Schönhage, the number of members of R is at most $(1 + o(1))u \log_2 x/\log x$.

We next use the primes $p^{(1)}$ in such a manner as to sieve out as much as possible from R. This procedure multiplies the cardinality of R by a factor of at most

$$\Big(\prod_{p \leqslant y} (1 - 1/p)\Big)\Big(\prod_{\substack{p \leqslant y \\ p \mid k}} (1 - 1/p)^{-1}\Big) \leqslant \frac{1 + o(1)}{e^{\gamma} \log y} \cdot \frac{k}{\varphi(k)},$$

so that the residual set S has cardinality at most

$$\begin{aligned} &\frac{1 + o(1)}{e^{\gamma} \log y} \cdot \frac{k}{\varphi(k)} \cdot \frac{(1 + o(1))u \log_2 x}{\log x} \\ &\quad = \frac{(1 + o(1))(1 - 2\epsilon)}{1 - \epsilon} \cdot \frac{x}{\log x} \\ &\quad \leqslant (1 - \epsilon)x/\log x. \end{aligned}$$

Now the number of primes $p^{(3)}$ is $(1 + o(1))x/\log x$ (again using $k \notin Q$), so we may completely sieve out the set S using the primes in class $p^{(3)}$ for just one member each of S. This completes the verification of (3) and thus completes the proof of the theorem.

Remark. The fact that Q has density 0 can be seen at once from the fact that the "normal" number of prime factors of an integer k is $\log_2 k$. We can say a bit more—by an easy argument it can be shown that for every $\epsilon > 0$ and every n,

$$x^{1-\epsilon} \ll Q(x) \ll x/(\log x)^n,$$

where $Q(x)$ is the number of members of Q up to x. One might wonder if by somewhat sacrificing the strength of (2) one could significantly prove an exceptional set Q' to be sparser. We have not been able to do this. More explicitly, we cannot show there is a $c > 0$ and a set of integers Q' with $Q'(x) \ll x^{1-c}$ and $P(k)/(\varphi(k) \log k) \to \infty$ for $k \notin Q'$.

3. Further Comments

There is a conjecture of Kanold [11] (also independently made by Schinzel and Sierpiński [17]) that for every $d > 1$, $P(d) < d^2$. Kanold observes that $P(d) < d^2$ follows from the hypothesis: if m is the product of the primes $p < d$ with $p \nmid d$, then $g(m) < d$. It follows from our work that Kanold's hypothesis is false for all sufficiently large d. In fact if we let $k = d^{[(1+\epsilon)d/\log d]}$, then $k \notin Q$ and it follows from (3) that for $d > d_0(\epsilon)$,

$$\begin{aligned} g(m) &> (1 - 3\epsilon)\, e^{\gamma}(\varphi(d)/d) \cdot d \log d \cdot \log_3 d/(\log_2 d)^2 \\ &> (1 - 4\epsilon) d \log d \cdot \log_3 d/(\log_2 d)^3 > d. \end{aligned}$$

Of course, the falsity of Kanold's hypothesis for all large d does not rule out the conjecture $P(d) < d^2$, which we believe to be true.

If $0 < s \leqslant 1$, $0 < t$, let $f(s, t)$ denote the lower density of the set $F(s, t)$ of k for which at least $s\varphi(k)$ distinct $p(k, l)$ satisfy $p(k, l) \leqslant t\varphi(k) \log k$. In [3], Erdös shows that for every $t > 0$ there is an $s > 0$ such that for all sufficiently large k, $k \in F(s, t)$. A corollary then is: for every $t > 0$,

$$s(t) = \sup\{s : f(s, t) = 1\} > 0.$$

Moreover, it follows from the Prime Number Theorem that $s(t) \leqslant t$ for all t. From Erdös' proof in [3] we have $s(t) \sim t$ as $t \to 0$. In the same paper Erdös shows that there is a $t_0 > 1$ and an $s_0 < 1$ with infinitely many $k \notin F(s_0, t_0)$. A careful reading of the proof shows that this infinite set of k has in fact positive lower density. It thus follows that there is a $t_0 > 1$ with $s(t_0) < 1$. Of course, from our Theorem 3 we have $f(1, t) = 0$ for all t. We conjecture that $s(t) \to 1$ as $t \to \infty$. An argument of Elliott and Halberstam [2] almost gives this—from their proof $f(s, t) \to 1$ as $(s, t) \to (1, \infty)$.

A problem of B. M. Recaman [15] is to show there are only finitely many primes p for which the first p primes form a complete residue system modulo p. We generalize this problem as follows: show there are only finitely many positive integers k such that the first $\varphi(k)$ primes which do not divide k form a reduced residue system modulo k. Our Theorem 2 solves this problem. Still open is the effective determination of all the k's with this special property. We conjecture the largest such k is 30. An upper bound for such k is, in principle, effectively computable, since all of the estimates used in Theorem 2 can be made effective.

Acknowledgment

I would like to warmly thank Paul Erdös for suggesting to me the problem of computing lower bounds for $P(k)$.

REFERENCES

1. S. CHOWLA, *J. Indian Math. Soc.* **1**(2) (1934), 1–3.
2. P. D. T. A. ELLIOTT AND H. HALBERSTAM, The least prime in an arithmetic progression, *in* "Studies in Pure Mathematics," (Presented to Richard Rado), pp. 59–61, Academic Press, London/New York, 1971.
3. P. ERDÖS, On some applications of Brun's method, *Acta Sci. Math. (Szeged)* **13** (1949–50), 57–63.
4. P. ERDÖS, Some problems and results in elementary number theory, *Publ. Math. Debrecen* **2** (1951), 103–109.
5. P. ERDÖS, On the integers relatively prime to n and on a number-theoretic function considered by Jacobstahl, *Math. Scand.* **10** (1962), 163–170.
6. S. GRAHAM, On Linnik's constant, *Acta Arith.*, in press.
7. D. HENSLEY AND I. RICHARDS, Primes in intervals, *Acta Arith.* **25** (1974), 375–391.
8. C. HOOLEY, On the difference of consecutive numbers prime to n, *Acta Arith.* **8** (1963), 343–347.
9. H. IWANIEC, On the problem of Jacobsthal, *Demonstratio Math.* **11** (1978), 225–231.
10. E. JACOBSTHAL, Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist, I-III, *Norske Vid. Selsk. Forh. (Trondheim)* **33** (1960), 117–139.
11. H.-J. KANOLD, Über Primzahlen in arithmetischen Folgen, *Math. Ann.* **156** (1964), 393–395; II, *Math. Ann.* **157** (1965), 358–362.
12. U. V. LINNIK, On the least prime in an arithmetic progression. II. The Deuring–Heilbronn phenomenon, *Rec. Math.* [*Mat. Sb.*] *N.S.* **15** (57) (1944), 347–368.
13. K. PRACHAR, Über die kleinste Primzahl einer arithmetischen Reihe, *J. Reine Angew. Math.* **206** (1961), 3–4.
14. R. A. RANKIN, The difference between consecutive prime numbers V, *Proc. Edinburgh Math. Soc.* **13** (2) (1962/63), 331–332.
15. B. M. RECAMAN, Problem 672, *J. Recreational Math.* **10** (1978), 283.
16. A. SCHINZEL, Remark on the paper of K. Prachar "Über die kleinste Primzahl einer arithmetischen Reihe," *J. Reine Angew. Math.* **210** (1962), 121–122.
17. A. SCHINZEL AND W. SIERPIŃSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; erratum **5** (1959), 259.
18. A. SCHÖNHAGE, Eine Bemerkung zur Konstruktion grosser Primzahllücken, *Arch. Math.* **14** (1963), 29–30.
19. S. S. WAGSTAFF, JR., The least prime in an arithmetic progression with prime difference, *J. Reine Angew. Math.* **301** (1978), 114–115.
20. S. S. WAGSTAFF, JR., Greatest of the least primes in arithmetic progressions having a given modulus, *Math. Comp.* **33** (1979), 1073–1080.