Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 11, No. 2, May 1979
Printed in Belgium

On the Density of Odd Integers of the Form $(p-1)2^{-n}$ and Related Questions[1]

P. ERDÖS

Mathematical Institute of the Hungarian Academy of Sciences
1053 Budapest, Reáltanoda utca 13–15, Hungary

AND

A. M. ODLYZKO

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by H. Zassenhaus

Received April 15, 1978

It is shown that odd integers k such that $k \cdot 2^n + 1$ is prime for some positive integer n have a positive lower density. More generally, for any primes $p_1, ..., p_r$, the integers k such that k is relatively prime to each of $p_1, ..., p_r$, and such that $k \cdot p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} + 1$ is prime for some $n_1, ..., n_r$, also have a positive lower density.

1. INTRODUCTION

The purpose of this note is to prove the following result, which answers a question raised by P. T. Bateman.

THEOREM 1. *There exists a positive, effectively computable constant c_1 such that if $N(x)$ is the number of odd positive integers $k \leqslant x$ such that $k \cdot 2^n + 1$ is prime for some positive integer n, then*

$$N(x) \geqslant c_1 x \qquad \textit{for} \quad x \geqslant 1.$$

On the other hand, Sierpiński [9] (see also [10, p. 414; 11, pp. 10, 64]) has shown that there exist infinitely many odd k such that $k \cdot 2^n + 1$ is not prime for any n. His proof used covering congruences [3]; that is, he showed that there is a finite set of primes $q_1, ..., q_s$ such that if k belongs to a particular arithmetic progression modulo $2q_1 \cdots q_s$, then for every n, $k \cdot 2^n + 1$ is divisible by at least one of $q_1, ..., q_s$. In particular, this also shows that for a positive constant c_2,

$$N(x) \leqslant (\tfrac{1}{2} - c_2)x$$

[1] Dedicated to the Memory of Paul Turán.

0022-314X/79/020257–07$02.00/0

if x is large enough. It seems natural to conjecture that

$$N(x) \sim c_3 x \quad \text{as} \quad x \to \infty. \tag{1}$$

but we cannot prove this. We also do not see any way to ascertain whether all those odd k which are not representable as $(p-1) \cdot 2^{-n}$ actually fail to be of this form because of a covering congruence.

The smallest odd k such that $k \cdot 2^n + 1$ is composite for all n is not known at present. However, it is known [6, 7, 8], that for all odd $k \leqslant 381$, there is an n such that $k \cdot 2^n + 1$ is prime, while $383 \cdot 2^n + 1$ is composite for all $n < 2313$. The smallest k for which $k \cdot 2^n + 1$ is known to be composite for all n seems to be $k = 78557$ [8]; here $k \cdot 2^n + 1$ is always divisible by 3, 5, 7, 13, 19, 37 or 73.

In some cases the smallest n for which $k \cdot 2^n + 1$ is prime is quite large. For example, $47 \cdot 2^n + 1$ is prime for $n = 583$ but composite for all $n \leqslant 582$ [7]. The proof of our result shows that odd integers $k \leqslant x$ for which some $k \cdot 2^n + 1 \leqslant x^{1+\epsilon}$ is prime are a positive proportion (depending on ϵ) of all $k \leqslant x$, no matter how small an $\epsilon > 0$ we take.

Theorem 1 is a special case of the following more general result.

THEOREM 2. *Let $p_1, \ldots, p_r$ be any primes. Then there exist positive, effectively computable constants $c_4 = c_4(p_1, \ldots, p_r)$ and $c_5 = c_5(p_1, \ldots, p_r)$ such that if $N(p_1, \ldots, p_r; x)$ is the number of positive integers $k \leqslant x$ such that $(k, p_1 p_2 p \cdots p_r) = 1$ and $k \cdot \prod p_i^{n_i} + 1$ is prime for some $n_1, \ldots, n_r$, then*

$$N(p_1, \ldots, p_r; x) \geqslant c_4 x \qquad \text{for} \quad x \geqslant c_5.$$

Just as was the case with Theorem 1, we conjecture that $N(p_1, \ldots, p_r; x)$ is asymptotic to a constant times x. If $r \geqslant 2$, however, the situation could conceivably be quite different from that of Theorem 1 in that all integers k which are relatively prime to $p_1 \cdots p_r$ with $p_1 = 2$ could conceivably be representable as $k = (p-1)\, p_1^{-n_1} \cdots p_r^{-n_r}$. The simplest case of this question is $r = 2$, $p_1 = 2$, $p_2 = 3$. In this case all integers $k \leqslant 50{,}000$ for which $(k, 6) = 1$ have the property that $k \cdot 2^a \cdot 3^b + 1$ is prime for some nonnegative integers a, b with $a + b \leqslant 9$.

Before embarking on the proof of Theorem 2, let us note that the same method can be used for investigating k such that $k \cdot \prod p_i^{n_i} - 1$ is prime, as well as many similar sequences.

2. PROOF OF THEOREM 2

The proof of our main result relies on the modern zero-density theorem used in proving Linnik's estimate for the least prime in an arithmetic progression and on the upper bound sieve. First we introduce some notation. The constants $c_4, c_5, \ldots$, as well as those implied by the $\ll$ and 0-notation will denote effectively computable constants which depend only on $p_1, \ldots, p_r$. We will use $\mathbf{a} = (a_1, \ldots, a_r)$ to denote r-tuples of nonnegative integers, and we will write

$$P(\mathbf{a}) = \prod_{j=1}^{r} p_j^{a_j}.$$

We will write $\mathbf{1} = (1, \ldots, 1)$, so that $\mathbf{a} + \mathbf{1} = (a_1 + 1, \ldots, a_r + 1)$. As usual, $\pi(x; m, b)$ denotes the number of primes $p \leqslant x$ such that $p \equiv b(\bmod m)$.

We now state our first auxiliary result, which will be proved in the last section.

LEMMA 1. *There exist positive constants c_6 and c_7 such that if* $(b, p_1 \cdots p_r) = 1$, *then*

$$\pi(x; P(\mathbf{a}), b) \geqslant \frac{c_6 x}{P(\mathbf{a}) \log x} \qquad \textit{for} \quad x \geqslant P(\mathbf{a})^{c_7}.$$

We now choose an integer $N = N(x)$ such that

$$p_j^{N+1} \leqslant x^{1/(rc_7)}, \qquad 1 \leqslant j \leqslant r.$$

We then have $N \sim c_8 \log x$ as $x \to \infty$. We define

$$A(x) = \{(a_1, \ldots, a_r) \colon 0 \leqslant a_j \leqslant N, \qquad \text{for} \quad 1 \leqslant j \leqslant r\}.$$

For $(k, p_1 \cdots p_r) = 1$, we let $R(k, x)$ denote the number of primes q such that $q = k \cdot P(\mathbf{a}) + 1$ for some $\mathbf{a} \in A(x)$. Note that such a prime q necessarily satisfies $q \leqslant x^{1+1/c_7}$. If $\sum'$ denotes summation over only those k for which $(k, p_1 \cdots p_r) = 1$, then we obtain

$$\sum_{k \leqslant x}{}' R(k, x) \geqslant \sum_{\mathbf{a} \in A(x)} \pi(xP(\mathbf{a}), P(\mathbf{a} + \mathbf{1}), P(\mathbf{a}) + 1).$$

But by Lemma 1 and the choice of N, the right side above is (for x large enough)

$$\geqslant \frac{c_9 x}{\log x} \sum_{\mathbf{a} \in A(x)}{}' 1 \geqslant c_{10} x (\log x)^{r-1}. \tag{2}$$

Thus $R(k, x)$ is large on the average. We wish to show that it is non-zero often.

If $M(x)$ is the number of $k \leqslant x$ such that $(k, p_1 \cdots p_r) = 1$, and $R(k, x) > 0$, then by the Cauchy-Schwarz inequality

$$\Big(\sum_{k \leqslant x}{}' R(k, x)\Big)^2 \leqslant M(x) \sum_{k \leqslant x}{}' R^2(k, x). \tag{3}$$

We now apply our next auxiliary result, which will also be proved in the next section.

LEMMA 2. *There exists a constant c_{11} such that*

$$\sum_{k\leqslant x}{}' R^2(k, x) \leqslant c_{11}x(\log x)^{2r-2}.$$

To conclude the proof of our theorem we now need only combine (2), (3), and Lemma 2.

3. PROOFS OF THE AUXILIARY RESULTS

Proof of Lemma 1. This result follows from recent proofs of Linnik's theorem about the least prime in an arithmetic progression, such as that in [1, Section 6]. The main result we need is that the exceptional zero β_1 of [1, Section 6] does not occur for any modulus of the form $P(\mathbf{a})$. If the exceptional zero β_1 exists, it comes from a Dirichlet L-function $L(s, \chi)$ with a real character χ. But the nontrivial zeros of $L(s, \chi)$ are the same as those of $L(s, \chi^*)$, where χ^* is the primitive character that induces χ. However, there are only a finite number of primitive real characters modulo the $P(\mathbf{a})$, since $p_1, ..., p_r$ are fixed [2, Section 5]. Hence if we take the constant c_1 in [1, p. 39] to be small enough, the exceptional zero β_1, even if it exists, will not come from any character modulo $P(\mathbf{a})$ for any $\mathbf{a}$, and the proof of our lemma will follow from the arguments used in [1, Section 6].

Proof of Lemma 2. For k relatively prime to $p_1 \cdots p_r$, let

$$r(k, \mathbf{a}) = \begin{cases} 1 & k \cdot P(\mathbf{a}) + 1 = \text{prime}, \\ 0 & \text{otherwise}. \end{cases}$$

Then

$$R(k, x) = \sum_{\mathbf{a}\in A(x)} r(k, \mathbf{a}),$$

and

$$R^2(k, x) \leqslant \sum_{\mathbf{a}\in A(x)} r(k, \mathbf{a}) + \sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}}} r(k, \mathbf{a})\, r(k, \mathbf{b}). \tag{4}$$

Let $\mathbf{a}, \mathbf{b} \in A(x)$, $\mathbf{a} \neq \mathbf{b}$. Then by the upper bound sieve method [4, Theorem 5.7], [5, Theorem 4.2],

$$\begin{aligned}\sum_{k\leqslant x}{}' r(k, \mathbf{a})\, r(k, \mathbf{b}) \\ &\leqslant \#\{n\colon 1 \leqslant n \leqslant x,\ P(\mathbf{a})\, n + 1 \text{ and } P(\mathbf{b})\, n + 1 \text{ both prime}\} \\ &\ll \frac{x}{\log^2 x} \prod_{q\mid(P(\mathbf{a})-P(\mathbf{b}))} \left(1 + \frac{1}{q}\right),\end{aligned}$$

where q is restricted to primes different from $p_1, \dots, p_r$. Hence

$$\sideset{}{'}\sum_{k\leqslant x} \sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}}} r(k,\mathbf{a})\,r(k,\mathbf{b}) \ll \frac{x}{\log^2 x} \sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}}} \prod_{q\mid(P(\mathbf{a})-P(\mathbf{b}))}\left(1+\frac{1}{q}\right)$$

$$= \frac{x}{\log^2 x}\sideset{}{^*}\sum_{m}\frac{1}{m} \sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}\\ m\mid(P(\mathbf{a})-P(\mathbf{b}))}} 1, \qquad (5)$$

where $\sum^*$ means that we are summing over those m that are relatively prime to $p_1 \cdots p_r$ and are square-free. We wish to show that

$$\sideset{}{^*}\sum_{m}\frac{1}{m} \sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}\\ m\mid(P(\mathbf{a})-P(\mathbf{b}))}} 1 \ll N^{2r}. \qquad (6)$$

Certainly if $m=1$, the inner sum is $\leqslant (N+1)^{2r} \ll N^{2r}$. Consider $m \geqslant 2$. Let $Q(m)$ denote the largest prime divisor of m, and let $e(Q(m))$ denote the multiplicative order of p_1 modulo $Q(m)$. If $m \mid (P(\mathbf{a}) - P(\mathbf{b}))$, then certainly $P(\mathbf{a}) \equiv P(\mathbf{b}) \pmod{Q(m)}$. We wish to show that $P(\mathbf{a}) \equiv P(\mathbf{b}) \pmod{q}$ does not occur very often for a prime q. Now if $a_2, a_3, \dots, a_r$ and $b_1, b_2, \dots, b_r$ are fixed, then $P(\mathbf{a}) \equiv P(\mathbf{b}) \pmod{q}$ holds only for one in every $e(q)$ values of a_1. Hence for $m>1$,

$$\sum_{\substack{\mathbf{a},\mathbf{b}\in A(x)\\ \mathbf{a}\neq\mathbf{b}\\ P(\mathbf{a})\equiv P(\mathbf{b})(\mathrm{mod}\, m)}} 1 \leqslant (N+1)^{2r-1}\left(\frac{N+1}{e(Q(m))}+1\right).$$

Therefore the quantity on the left side of (5) is

$$\ll N^{2r} + N^{2r}\sum_{1<m<x^{1/c_7}}\frac{1}{me(Q(m))} + N^{2r-1}\sum_{1<m<x^{1/c_7}}\frac{1}{m}$$

$$\ll N^{2r} + N^{2r}\sum_{1<m<x^{1/c_7}}\frac{1}{me(Q(m))}.$$

We now need to prove that the sum on the right side above is $\ll 1$. But

$$\sum_{1<m<x^{1/c_7}}\frac{1}{me(Q(m))} \leqslant \sum_{q<x^{1/c_7}}\frac{1}{qe(q)}\prod_{q'<q}\left(1+\frac{1}{q'}\right)$$

$$\ll \sum_{q}\frac{\log q}{qe(q)}.$$

Evidently we need to show that $e(q)$ is not small too often. But if $e(q_1) = \cdots = e(q_t) = n$, then $2^t \leqslant q_1 \cdots q_t \leqslant p_1{}^n - 1$, and so $t \ll n$. Therefore there are at most $c_{12}n$ values of q with $e(q) = n$. Hence the last sum above is bounded above by a similar sum in which the first c_{12} primes q have $e(q) = 1$, the next $2c_{12}$ primes have $e(q) = 2$, and so on. Therefore

$$\sum_q \frac{\log q}{qe(q)} \ll \sum \frac{\log^{3/2} q}{q^{3/2}} \ll 1,$$

which proves (6).

To complete the proof of the lemma it thus remains only to show that the first sum on the right side of (4) does not contribute much. But by the upper bound sieve,

$$\begin{aligned}\sum_{k\leqslant x}{}' \sum_{\mathbf{a}\in A(x)} r(k, \mathbf{a}) &\leqslant \sum_{\mathbf{a}\in A(x)} |\{n \leqslant x\colon n \cdot P(\mathbf{a}) + 1 \text{ is prime}\}| \\ &\ll \sum_{\mathbf{a}\in A(x)} \frac{x}{\log x} \ll \frac{x}{\log x} N^r. \qquad (7)\end{aligned}$$

If we now combine (4)–(7), we obtain

$$\begin{aligned}\sum_{k\leqslant x}{}' R^2(k, x) &\ll \frac{x}{\log x} N^r + \frac{x}{\log^2 x} N^{2r} \\ &\ll x(\log x)^{2r-2}. \qquad \text{Q.E.D.}\end{aligned}$$

Remark. The last part of the proof of Lemma 2 can also be handled by using Romanoff's result [5] that

$$\sum_{m=1}^{\infty}{}' \frac{1}{ml(m)} < \infty,$$

where $l(m)$ denotes the multiplicative order of b modulo m, and we sum over m with $(m, b) = 1$. Our proof of the lemma yields, in fact, still another proof of Romanoff's result.

References

1. E. Bombieri, Le grand crible dans la théorie analytique des nombres, Astérisque **18** (1974).
2. H. Davenport, "Multiplicative Number Theory," Markham, Chicago, 1967.
3. P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil Math.* **2** (1950), 113–123.
4. H. Halberstam and H.-E. Richert, "Sieve Methods," Academic Press, London/New York, 1974.
5. K. Prachar, "Primzahlverteilung," Springer–Verlag, Berlin/New York, 1957.
6. R. M. Robinson, A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers, *Proc. Amer. Math. Soc.* **9** (1958), 673–681.

7. J. L. Selfridge, Solution to problem 4995, *Amer. Math. Monthly* **70** (1963), 101.

8. J. L. Selfridge, private communication.

9. W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, *Elem. Math.* **15** (1960), 73–74; Corrigendum **17** (1962), 85.

10. W. Sierpiński, "Elementary Theory of Numbers," Polish Scientific Publishers, Warsaw, 1964.

11. W. Sierpiński, "250 Problems in Elementary Number Theory," Elsevier, New York, 1970.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium