Bull. Austral. Math. Soc. **78** (2008), 431–436
doi:10.1017/S0004972708000804

ON THE DENSITY OF INTEGERS OF THE FORM $(p-1)2^{-n}$ IN ARITHMETIC PROGRESSIONS

XUE-GONG SUN and JIN-HUI FANG ✉

(Received 18 February 2008)

Abstract

Erdős and Odlyzko proved that odd integers k such that $k2^n + 1$ is prime for some positive integer n have a positive lower density. In this paper, we characterize all arithmetic progressions in which natural numbers that can be expressed in the form $(p-1)2^{-n}$ (where p is a prime number) have a positive proportion. We also prove that an arithmetic progression consisting of odd numbers can be obtained from a covering system if and only if those integers in such a progression which can be expressed in the form $(p-1)2^{-n}$ have an asymptotic density of zero.

2000 *Mathematics subject classification*: 11A07, 11B25, 11P32.

Keywords and phrases: asymptotic density, covering systems, arithmetic progressions.

1. Introduction

Let k, n be integers and let p be a prime. Natural numbers of the special form $k2^n + 1$ have long attracted much interest. In 1960, Sierpiński [11] proved that there are infinitely many positive odd integers k such that $k2^n + 1$ is composite for all positive integers n. In 1979, Erdős and Odlyzko [8] established that the lower asymptotic density of odd integers k such that $k2^n + 1$ is prime for some positive integer n is positive. In 1962, J. L. Selfridge discovered (unpublished) that for any positive integer n, the number $78557 \cdot 2^n + 1$ is divisible by one of the primes 3, 5, 7, 13, 19, 37 or 73. It is still an open question whether 78557 is the least positive odd number k for which $k2^n + 1$ $(n = 1, 2, \ldots)$ are all composite. In [2], Chen proved that the set of positive odd integers k such that $k2^n + 1$ possesses at least three distinct prime factors for all positive integers n has a positive lower asymptotic density. In [3], Chen further showed that the set of positive odd integers k such that $k2^n + 1$ has at least three distinct prime factors for all positive integers n contains an infinite arithmetic progression. For other related results, we refer the reader to the works of Chen [1–6], Chen and Sun [7], Guy [9], and Luca and Stănică [10].

This work was supported by the National Natural Science Foundation of China Grant Nos. 10771103 and 10801075.

In [8], Erdős and Odlyzko proposed the question: do all odd integers k which are not representable as $(p-1)2^{-n}$ actually fail to be of this form because of a covering system? In the present paper, we answer this question in the case of an arithmetic progression. We also consider the following problem.

PROBLEM 1. Is it possible to characterize all arithmetic progressions in which the natural numbers that can be expressed in the form $(p-1)2^{-n}$ constitute a positive proportion?

For integers m and a, let $a \pmod{m} = \{a + mk : k \in \mathbb{Z}\}$. A system of congruences $\{a_i \pmod{m_i}\}_{i=1}^{t}$ is called a covering system if every integer b satisfies $b \equiv a_i \pmod{m_i}$ for at least one value of i.

REMARK. Let $\{a_i \pmod{m_i}\}_{i=1}^{t}$ be a covering system such that there exist distinct primes $p_1, p_2, \ldots, p_t$ with

$$p_i | 2^{m_i} - 1 \quad (1 \le i \le t).$$

By the Chinese remainder theorem, there exists an arithmetic progression $x \equiv x_0 \pmod{p_1 p_2 \cdots p_t}$ satisfying

$$x 2^{a_i} + 1 \equiv 0 \pmod{p_i} \quad (1 \le i \le t).$$

Now we consider any positive integer M with $M \equiv x_0 \pmod{p_1 p_2 \cdots p_t}$.

Assume that M can be expressed in the form $(p-1)2^{-n}$; then there exists at least one index i with $n \equiv a_i \pmod{m_i}$.

Thus

$$M 2^n + 1 \equiv M 2^{a_i} + 1 \equiv 0 \pmod{p_i}.$$

So $p = p_i$ and $M = (p_i - 1)2^{-n}$.

This implies that the asymptotic density of integers in $x_0 \pmod{p_1 p_2 \cdots p_t}$ which can be expressed in the form $(p-1)2^{-n}$ is zero.

The above discussion naturally leads us to consider the inverse problem.

PROBLEM 2. Can any arithmetic progression of odd numbers in which the asymptotic density of integers that can be expressed in the form $(p-1)2^{-n}$ is zero be obtained from a covering system?

For a positive integer m, let $m = 2^r m'$, $2 \nmid m'$. Denote by $e(m)$ the multiplicative order of $2 \pmod{m'}$; in other words, $e(m)$ is the smallest positive integer l such that $2^l \equiv 1 \pmod{m'}$.

In this paper, we solve the above two problems completely, and prove the following main results.

https://doi.org/10.1017/S0004972708000804 Published online by Cambridge University Press

THEOREM. *Let m and s be integers with $2\nmid s$ and $2|m$.*

(a) *If there exists an integer n_0 with $1 \le n_0 \le e(m)$ such that $(2^{n_0}s+1, m') = 1$, then the lower density of natural numbers in the arithmetic progression $\{s+mk\}_{k=1}^{\infty}$ which can be expressed as $(p-1)2^{-n}$ is positive.*

(b) *If there is no integer with $1 \le n \le e(m)$ such that $(2^n s+1, m') = 1$, then the density of natural numbers in the arithmetic progression $\{s+mk\}_{k=1}^{\infty}$ which can be expressed as $(p-1)2^{-n}$ is zero, and such an arithmetic progression can be obtained from a covering system.*

COROLLARY. *An arithmetic progression of odd numbers can be obtained from a covering system if and only if the asymptotic density of integers in such a progression which can be expressed in the form $(p-1)2^{-n}$ is zero.*

2. Proofs

In this paper, $\pi(x; m, a)$ denotes the number of primes $p \le x$ which satisfy $p \equiv a \pmod m$. Before proving the theorem, we need the following lemmas.

LEMMA 3 [8, Lemma 1]. *Given positive integers n and b with $(b, n) = 1$, there exist positive constants c_1 and c_2 depending only on the prime factors of n such that*

$$\pi(x, n, b) \ge \frac{c_1 x}{n \log x} \quad \text{for } x \ge n^{c_2}.$$

Take

$$c_3 = \frac{1}{2c_2 \log 2}.$$

Then, for $x > \max\{e^{1/c_3}, m^{2c_2}\}$,

$$c_3 \log x > 1 \quad \text{and} \quad m^{c_2} < x^{1/2}.$$

Hence

$$(2^{c_3 \log x} m)^{c_2} = (x^{c_3 \log 2} m)^{c_2} = x^{c_2 c_3 \log 2} m^{c_2} < x.$$

Define

$$r(k, n) = \begin{cases} 1 & \text{if } k2^n + 1 \text{ is prime,} \\ 0 & \text{otherwise} \end{cases}$$

and

$$R(k, x) = \sum_{n \le c_3 \log x} r(k, n).$$

LEMMA 4. *Let m and s be integers with $2\nmid s$ and $2|m$. If there exists an integer n_0 with $1 \le n_0 \le e(m)$ and $(2^{n_0}s+1, m') = 1$, then there is a positive constant c_6 such that*

$$\sum_{\substack{k \le x \\ k \equiv s \ (\mathrm{mod}\ m)}} R(k, x) \ge c_6 x.$$

https://doi.org/10.1017/S0004972708000804 Published online by Cambridge University Press

PROOF.

$$\begin{aligned}
&\sum_{\substack{k\le x\\ k\equiv s\ (\mathrm{mod}\ m)}} R(k,x)\\
&= \sum_{\substack{k\le x\\ k\equiv s\ (\mathrm{mod}\ m)}} \sum_{n\le c_3\log x} r(k,n)\\
&= \sum_{n\le c_3\log x} \sum_{\substack{k\le x\\ k\equiv s\ (\mathrm{mod}\ m)}} r(k,n)\\
&= \sum_{n\le c_3\log x} \#\{q : q = k2^n+1,\ q \text{ is a prime},\ k\equiv s\ (\mathrm{mod}\ m),\ k\le x\}\\
&= \sum_{n\le c_3\log x} \pi(x2^n+1;\ 2^n m,\ 2^n s+1)\\
&\ge \sum_{n_0+e(m)l\le c_3\log x} \pi(x2^{n_0+e(m)l}+1;\ 2^{n_0+e(m)l}m,\ 2^{n_0+e(m)l}s+1).
\end{aligned}$$

Combining the facts that

$$(2^{c_3\log x}m)^{c_2} < x \quad \text{and} \quad n_0+e(m)l \le c_3\log x,$$

we obtain

$$x2^{n_0+e(m)l}+1 \ge (2^{n_0+e(m)l}m)^{c_2}.$$

From Lemma 3, it follows that

$$\begin{aligned}
&\sum_{n_0+e(m)l\le c_3\log x} \pi(x2^{n_0+e(m)l}+1;\ 2^{n_0+e(m)l}m,\ 2^{n_0+e(m)l}s+1)\\
&\ge c_1 \sum_{n_0+e(m)l\le c_3\log x} \frac{x2^{n_0+e(m)l}+1}{2^{n_0+e(m)l}m\log(x2^{n_0+e(m)l}+1)}\\
&\ge c_4x \sum_{n_0+e(m)l\le c_3\log x} \frac{1}{\log(x2^{n_0+e(m)l}+1)}\\
&\ge c_5x \sum_{n_0+e(m)l\le c_3\log x} \frac{1}{\log x}\\
&\ge c_6x.
\end{aligned}$$

This completes the proof of Lemma 4. □

LEMMA 5 [8, Lemma 2]. *There exists a positive constant c_7 such that*

$$\sum_{k\le x} R^2(k,x) \le c_7x.$$

https://doi.org/10.1017/S0004972708000804 Published online by Cambridge University Press

PROOF OF THE THEOREM, PART (a). By the Cauchy–Schwarz inequality,

$$\Big(\sum_{\substack{k\le x\\ k\equiv s \ (\mathrm{mod}\ m)}} R(k,x)\Big)^2$$
$$\le \#\{k : 1\le k\le x,\ k\equiv s\ (\mathrm{mod}\ m),\ R(k,x)\ge 1\}\sum_{\substack{k\le x\\ k\equiv s \ (\mathrm{mod}\ m)}} R^2(k,x)$$
$$\le \#\{k : 1\le k\le x,\ k\equiv s\ (\mathrm{mod}\ m),\ R(k,x)\ge 1\}\sum_{k\le x} R^2(k,x).$$

Then, by Lemmas 4 and 5,

$$\#\{k : 1\le k\le x,\ k\equiv s\ (\mathrm{mod}\ m),\ R(k,x)\ge 1\}\ge c_8x.$$

This completes the proof of statement (a) in the theorem. □

PROOF OF THE THEOREM, PART (b). Let $p_1, p_2, \ldots, p_t$ be all the distinct odd prime factors of m such that, for each $1\le i\le t$, there exists a nonnegative integer a_i with $2^{a_i}s+1\equiv 0\ (\mathrm{mod}\ p_i)$. Let m_i be the multiplicative order of $2\ (\mathrm{mod}\ p_i)$. We shall prove that $\{a_i\ (\mathrm{mod}\ m_i)\}_{i=1}^t$ is a covering system.

For arbitrary positive integer a, let l be an integer with $1\le l\le e(m)$ such that $l\equiv a\ (\mathrm{mod}\ e(m))$.

By the assumption, there is no l' with $1\le l'\le e(m)$ such that $(2^{l'}s+1, m')=1$, so

$$(2^ls+1, m')>1.$$

Since $l\equiv a\ (\mathrm{mod}\ e(m))$, it follows that

$$2^ls+1\equiv 2^as+1\ (\mathrm{mod}\ m'),$$

and then $(2^as+1, m')>1$. Hence there exists some i such that $p_i|2^as+1$.

Noting that $2^{a_i}s+1\equiv 0\ (\mathrm{mod}\ p_i)$, we obtain

$$2^as+1\equiv 2^{a_i}s+1\ (\mathrm{mod}\ p_i),$$

so

$$a\equiv a_i\ (\mathrm{mod}\ m_i).$$

Thus we have proved that $\{a_i\ (\mathrm{mod}\ m_i)\}_{i=1}^t$ is a covering system. From the above discussion, we can show that the arithmetic progression $\{s+mk\}_{k=1}^\infty$ may be obtained from a covering system $\{a_i\ (\mathrm{mod}\ m_i)\}_{i=1}^t$. By the remark in Section 1, we know that the density of integers in such an arithmetic progression which can be expressed in the form $(p-1)2^{-n}$ is zero. This completes the proof of statement (b) in the theorem. □

Acknowledgements

We sincerely thank our tutor Yong-Gao Chen for his useful suggestions and valuable help. We are also grateful to the referee for his/her helpful comments.

https://doi.org/10.1017/S0004972708000804 Published online by Cambridge University Press

References

[1] Y. G. Chen, 'On integers of the form $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$', *Proc. Amer. Math. Soc.* **128** (2000), 1613–1616.

[2] ———, 'On integers of the form $k2^n + 1$', *Proc. Amer. Math. Soc.* **129** (2001), 355–361.

[3] ———, 'On integers of the forms $k - 2^n$ and $k2^n + 1$', *J. Number Theory* **89** (2001), 121–125.

[4] ———, 'On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$', *J. Number Theory* **98** (2003), 310–319.

[5] ———, 'On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$', *J. Number Theory* **125** (2007), 14–25.

[6] ———, 'Five consecutive positive odd numbers, none of which can be expressed as a sum of two prime powers', *Math. Comp.* **74** (2005), 1025–1031.

[7] Y. G. Chen and X. G. Sun, 'On Romanoff's constant', *J. Number Theory* **106** (2004), 275–284.

[8] P. Erdős and A. M. Odlyzko, 'On the density of odd integers of the form $(p - 1)2^{-n}$ and related questions', *J. Number Theory* **11** (1979), 257–263.

[9] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn (Springer, New York, 2004).

[10] F. Luca and P. Stănică, 'Fibonacci numbers that are not sums of two prime powers', *Proc. Amer. Math. Soc.* **133** (2005), 1887–1890.

[11] W. Sierpiński, 'Sur un problème concernant les nombres $k2^n + 1$', *Elem. Math.* **15** (1960), 73–74; Corrigendum **17** (1962), 85.

XUE-GONG SUN, Department of Mathematics, Nanjing Normal University,
Nanjing 210097, People's Republic of China
and
Department of Mathematics and Science, Huai Hai Institute of Technology,
Lian Yun Gang 222005, Jiangsu, People's Republic of China
e-mail: fangjinhui1114@163.com

JIN-HUI FANG, Department of Mathematics, Nanjing Normal University,
Nanjing 210097, People's Republic of China

https://doi.org/10.1017/S0004972708000804 Published online by Cambridge University Press