PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 129, Number 2, Pages 355–361
S 0002-9939(00)05916-5
Article electronically published on August 28, 2000

ON INTEGERS OF THE FORM $k2^n + 1$

YONG-GAO CHEN

(Communicated by David E. Rohrlich)

Abstract. In this paper we show 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 has positive lower asymptotic density.

1. Introduction

Integers of the form $k2^n + 1$ have received special attention. One main reason is that the potential factors of Fermat numbers have the form $k2^n + 1$. One may refer to Guy [10], A3, B21, and [1], [2], [4], [5], [8], [11], [12], [15]–[18]. In 1960 Sierpiński [17] used the congruence covering system to prove that there are infinitely many positive odd integers k such that $k2^n + 1$ is composite for all positive integers n. On the other hand, P. Erdős and A. W. Odlyzko [9] showed that the lower asymptotic density of odd integers k such that $k2^n + 1$ is prime for some positive integer n is positive.

In [6] we introduced the notation of $(2, 1)-$primitive $m-$covering systems. By constructing a $(2, 1)-$primitive $2-$covering system and using a result on linear forms in logarithms, we show that the set of positive odd integers, which have no representation of the form $2^n \pm p^\alpha q^\beta$, where p, q are distinct primes and n, α, β are nonnegative integers (hence $n \geq 1$), has positive lower asymptotic density. That is, the lower asymptotic density of positive odd integers k such that $k - 2^n$ has at least three distinct prime factors for all positive integers n is positive.

In this paper, by using the same $(2, 1)-$primitive $2-$covering system in [6] and a result on linear forms in $p-$adic logarithms, we show 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 has positive lower asymptotic density.

In [6] and Sections 1-3 of this paper, all constants are effective computable (Baker's method). In Section 4 we point out that Mahler's result, which is an analogous extension of Roth's result, also works well for [6] and the present paper, but related constants are noneffective computable (Roth's method).

We only consider integers of the form $k - 2^n$ or $k2^n + 1$. For cases $k + 2^n$ and $k2^n - 1$ we have the exact same conclusions by using the same method. Our method also works well for integers of the form $ka + b^n$ or $ka^n + b$ with some reasonable restrictions on a, b and k.

Received by the editors April 29, 1999.
2000 *Mathematics Subject Classification.* Primary 11A07, 11B25.
This research was supported by the Fok Ying Tung Education Foundation and the National Natural Science Foundation of China, Grant No 19701015.

2. Notations and the main results

All primes in [6] and this paper are positive primes. We call $\{a_i(n_i)\}_{i=1}^t$ a covering system if every integer y satisfies $y \equiv a_i (\bmod n_i)$ for at least one value of i. For the construction of covering systems one may refer to S. L. G. Choi [7]. For further related information one may see Guy [10], A19, B21 and F13. The following notations have been used in [6].

Definition 1. A positive integer d is said to be an $(a,b)-$primitive divisor of order n if $d|a^n - b^n$ and $d \nmid a^m - b^m$ for all $1 \le m < n$.

Definition 2. $\{a_i(n_i)\}_{i=1}^t$ is said to be an $m-$covering system if every integer belongs to at least m of $a_1(n_1)$, $a_2(n_2)$, $\cdots$, $a_t(n_t)$.

Definition 3. $\{a_i(n_i)\}_{i=1}^t$ is said to be a $(2,1)-$primitive $m-$covering system if $\{a_i(n_i)\}_{i=1}^t$ is an $m-$covering system and there exist distinct primes $p_1, p_2, \cdots, p_t$ such that for each i, p_i is a $(2,1)-$primitive divisor of order n_i $(1 \le i \le t)$.

For $m \ge 3$ we do not know whether there exist $(2,1)-$primitive $m-$covering systems. I believe so. For convenience, let

$$\begin{aligned} Y_r =& \{k : k > 0, 2 \nmid k,\ k - 2^n \text{ has at least } r \text{ distinct} \\ & \text{prime factors for all positive integers } n\}, \end{aligned}$$

$$\begin{aligned} G_r =& \{k : k > 0, 2 \nmid k,\ k2^n + 1 \text{ has at least } r \text{ distinct} \\ & \text{prime factors for all positive integers } n\}. \end{aligned}$$

For a subset A of the natural numbers, let

$$A(x) = \{a \in A : a \le x\},$$

$$\underline{d}(A) = \liminf_{x \to \infty} \frac{|A(x)|}{x}.$$

That is, $\underline{d}(A)$ is the lower asymptotic density of A.

In this paper the following conclusions are proved. The main theorem in [6] is included as a part of Theorem 1(ii).

Theorem 1. *Suppose that there exists a $(2,1)-$primitive $r-$covering system. Then*
(i) $\underline{d}(G_{r+1}) > 0$ *and G_r contains an infinite arithmetic progression;*
(ii) $\underline{d}(Y_{r+1}) > 0$ *and Y_r contains an infinite arithmetic progression.*

Corollary. (i) $\underline{d}(G_3) > 0$ *and G_2 contains an infinite arithmetic progression;*
(ii) $\underline{d}(Y_3) > 0$ *and Y_2 contains an infinite arithmetic progression.*

Theorem 2. *The following statements are equivalent to each other:*
(i) *there exists a $(2,1)-$primitive $r-$covering system;*
(ii) *there exist an odd integer k and a finite set $\{p_1, \cdots, p_t\}$ of distinct primes such that $k2^n + 1$ is divisible by at least r of $p_1, \cdots, p_t$ for all positive integers n;*
(iii) *there exist an odd integer k and a finite set $\{p_1, \cdots, p_t\}$ of distinct primes such that $k - 2^n$ is divisible by at least r of $p_1, \cdots, p_t$ for all positive integers n.*

3. Proofs

To prove Theorem 1, we need a result on linear forms in $p-$adic logarithms. Here we use a special case of the corollary of Theorem 1 in Yu [19] (p. 245).

Lemma 1 (Yu [19])**.** *Let $a_1, \cdots, a_r$, $b_1, \cdots, b_r$ be nonzero integers with $|a_i| + 2 \leq A$, $3|b_i| \leq B$ $(1 \leq i \leq r)$. Suppose that*

$$a_1^{b_1} \cdots a_r^{b_r} - 1 \neq 0.$$

Then

$$\mathrm{ord}_2 \left(a_1^{b_1} \cdots a_r^{b_r} - 1 \right) \leq c \log(4B),$$

where

$$c = 11145 \cdot 24^r (r+1)^{2r+4} \frac{1}{(\log 2)^{r+2}} (\log A)^r \log(2^{12} \cdot 3r(r+1) \log A).$$

Lemma 2. *Let $p_1, \cdots, p_t$ be distinct odd primes and $x \geq 3$. Then the number of positive odd integers $M \leq x$ such that there exist a positive integer n and distinct primes $q_1, \cdots, q_r \in \{p_1, \cdots, p_t\}$ with*

$$M2^n + 1 = q_1^{\beta_1} \cdots q_r^{\beta_r}, \quad \beta_i \geq 1, \quad i = 1, \cdots, r,$$

is less than $c_1(\log\log x)(\log x)^r$, where c_1 depends only on r and $p_1, \cdots, p_t$.

Proof. Given $q_1, \cdots, q_r \in \{p_1, \cdots, p_t\}$. Let $A = \max p_i + 2$. Suppose that M is a positive odd integer with $M \leq x$ and

$$M2^n + 1 = q_1^{\beta_1} \cdots q_r^{\beta_r}, \quad n \geq 1, \quad \beta_i \geq 1, \quad i = 1, \cdots, r. \tag{1}$$

By (1) and Lemma 1 we have

$$n = \mathrm{ord}_2 \left(q_1^{\beta_1} \cdots q_r^{\beta_r} - 1 \right) \leq c \log(12 \max \beta_i), \tag{2}$$

where c depends only on r and A. By (1) and (2) we have

$$\begin{aligned} 2^{\max \beta_i} &\leq q_1^{\beta_1} \cdots q_r^{\beta_r} = M2^n + 1 \leq M2^{n+1} \\ &\leq x 2^{1 + c \log(12 \max \beta_i)}. \end{aligned}$$

Hence

$$\max \beta_i < c_2 \log x. \tag{3}$$

By (2) and (3) we have

$$n \leq c_3 \log\log x.$$

Thus, for $q_1, \cdots, q_r \in \{p_1, \cdots, p_t\}$, the number of positive odd integers $M \leq x$ such that there exist a positive integer n and positive integers $\beta_1, \cdots, \beta_r$ with

$$M2^n + 1 = q_1^{\beta_1} \cdots q_r^{\beta_r}$$

is less than

$$c_3 (c_2)^r (\log\log x)(\log x)^r.$$

Lemma 2 follows by taking $c_1 = c_3 (c_2)^r C_t^r$.

Proof of Theorem 1(i). This proof is similar to the proof of the main theorem in [6]. Suppose that $\{a_i \pmod{n_i}\}_{i=1}^t$ is a $(2,1)-$primitive $r-$covering system and $p_1, \cdots, p_t$ are corresponding primes in Definition 3. Take an integer M satisfying

$$M2^{a_i} + 1 \equiv 0 \pmod{p_i}, \quad i = 1, \cdots, t, \tag{4}$$

$$M + 1 \equiv 0 \pmod 2.$$

For any positive integer n there exist $i_1, \cdots, i_r$ with $1 \le i_1 < i_2 < \cdots < i_r \le t$ and

$$n \equiv a_{i_j} \pmod{n_{i_j}}, \quad j = 1, 2, \cdots, r.$$

Then by (4) and

$$2^{n_{i_j}} \equiv 1 \pmod{p_{i_j}}, \quad j = 1, \cdots, r$$

we have

$$M2^n + 1 \equiv M2^{a_{i_j}} + 1 \equiv 0 \pmod{p_{i_j}}, \quad j = 1, \cdots, r.$$

Thus

$$M2^n + 1 = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_r}^{\alpha_{i_r}} b, \quad \alpha_{i_j} > 0 \ (j = 1, 2, \cdots, r), \ b \in \mathbf{Z}.$$

This means that $M \in G_r$. Hence, if

$$M2^n + 1 = q_1^{\beta_1} \cdots q_r^{\beta_r}, \quad \beta_i \ge 0, \quad i = 1, \cdots, r,$$

where $q_1, \cdots, q_r$ are distinct primes, then $q_i \in \{p_1, \cdots, p_t\}$ and $\beta_i \ge 1$ $(i = 1, 2, \cdots, r)$. By Lemma 2 the number of such $M \le x$ is less than

$$c_1(\log\log x)(\log x)^r.$$

It is well known that the number of positive odd integers $M \le x$ with (4) is more than

$$\frac{x}{2p_1 \cdots p_t} - 1, \quad x \ge X_3.$$

Therefore, there exist at least $\frac{x}{2p_1\cdots p_t} - 1 - 2c_1(\log\log x)(\log x)^r$ positive odd numbers $M \le x$ such that $M2^n + 1$ has at least $r + 1$ distinct prime factors for all positive integers n. It is clear that all integers with (4) constitute an infinite arithmetic progression. This completes the proof of Theorem 1(i). The proof of Theorem 1(ii) is exactly as the proof of the main theorem in [6], except add $M \in Y_r$. This completes the proof of Theorem 1.

The corollary follows from Theorem 1 and the fact that there exists a $(2,1)-$primitive $2-$covering system (see the proof of the corollary in [6]).

Proof of Theorem 2. By the proof of Theorem 1 we know that (i) implies (ii) and (iii). We now prove that (ii) implies (i). For each i, let n_i and a_i be the least positive integers such that

$$2^{n_i} \equiv 1 \pmod{p_i}, \quad k2^{a_i} + 1 \equiv 0 \pmod{p_i}. \tag{5}$$

Then, for each i, p_i is a $(2,1)-$primitive divisor of order n_i. For any positive integer n, by the assumption, there exist $j_1, \cdots, j_r$ such that

$$p_{j_i} | k2^n + 1, \quad i = 1, 2, \cdots, r. \tag{6}$$

By (5) and (6) we have

$$p_{j_i} \nmid k, \quad p_{j_i} | k(2^n - 2^{a_{j_i}}).$$

Hence

$$2^{n-a_{j_i}} \equiv 1 \pmod{p_{j_i}}, \quad i = 1, \cdots, r. \tag{7}$$

By the definition of n_{j_i} and (7) we have $n \equiv a_{j_i} \pmod{n_{j_i}}$ $(1 \le i \le r)$. Thus $\{a_i \pmod{n_i}\}_{i=1}^t$ covers each positive integer at least r times, and hence is an $r-$covering system. Therefore, (ii) implies (i). Similarly, (iii) implies (i). This completes the proof of Theorem 2.

4. Noneffective versions

In [6] and the above arguments, all constants are effective computable. In this section we use Mahler's result, which is an analogous extension of Roth's result, to prove Lemma 2 in [6] and Lemma 2 (in a weak form which is sufficient for our purpose).

Lemma 3 (Mahler [13], Ridout [14])**.** *Let θ be any nonzero algebraic number, let $p_1, \cdots, p_t$, $q_1, \cdots, q_l$ be distinct primes and let $\alpha, \beta, \gamma, c'$ be real numbers with*

$$0 \le \alpha \le 1, \quad 0 \le \beta \le 1, \quad \gamma > \alpha + \beta, \quad c' > 0.$$

Let a, b, a', b' be positive integers with

$$a = a' p_1^{\alpha_1} \cdots p_t^{\alpha_t}, \quad \alpha_i \ge 0, \quad i = 1, \cdots, t,$$

$$b = b' q_1^{\beta_1} \cdots q_l^{\beta_l}, \quad \beta_j \ge 0, \quad j = 1, \cdots, l,$$

$$1 \le a' \le c' a^{\alpha}, \quad 1 \le b' \le c' b^{\beta}.$$

Then

$$\left| \theta - \frac{b}{a} \right| > \frac{c''}{a^{\gamma}} \quad \text{if } \theta - \frac{b}{a} \ne 0,$$

where $c'' > 0$ depends only on $\theta, p_1, \cdots, p_t$, $q_1, \cdots, q_l$, α, β, γ and c'.

(I) *Proof of Lemma* 2 *in* [6]. Let $q_1, \cdots, q_r$ be distinct primes with

$$|2^n - q_1^{\alpha_1} \cdots q_r^{\alpha_r}| \le x, \quad n \ge 1, \quad \alpha_i \ge 0, \quad i = 1, \cdots, r.$$

By Lemma 3 we have

$$x \ge 2^n \left| 1 - \frac{q_1^{\alpha_1} \cdots q_r^{\alpha_r}}{2^n} \right| \ge 2^n \frac{c''}{2^{0.5n}} \quad (\theta = 1, \alpha = \beta = 0, \gamma = \frac{1}{2}).$$

So

$$n \le c^{(3)} \log x. \tag{8}$$

Hence

$$\begin{aligned} 2^{\max \alpha_i} &\le q_1^{\alpha_1} \cdots q_r^{\alpha_r} \le |q_1^{\alpha_1} \cdots q_r^{\alpha_r} - 2^n| + 2^n \\ &\le x + 2^{c^{(3)} \log x}. \end{aligned}$$

Thus

$$\max \alpha_i \le c^{(4)} \log x. \tag{9}$$

All $c^{(i)}$ depend only on $q_1, \cdots, q_r$. Lemma 2 in [6] follows from (8) and (9). $\square$

(II) *Proof of Lemma* 2 (*a weak form*). Let $q_1, \cdots, q_r$ be distinct primes and $1 \le M \le x$ with

$$M2^n + 1 = q_1^{\beta_1} \cdots q_r^{\beta_r}, \quad n \ge 1,\ \beta_i \ge 0, \quad i = 1, \cdots, r. \tag{10}$$

If $n < \log x$, then

$$2^{\max \beta_i} \le q_1^{\beta_1} \cdots q_r^{\beta_r} \le M2^{n+1} \le x2^{1+\log x}.$$

Hence

$$\max \beta_i \le c^{(5)} \log x.$$

In this case, the number of $M \le x$ satisfying (10) is less than $c^{(6)}(\log x)^{r+1}$. Now assume that $n \ge \log x$. Then

$$M^{\log 2} \le x^{\log 2} = 2^{\log x} \le 2^n.$$

That is,

$$M \le (2^n M)^{(1+\log 2)^{-1}}.$$

Thus, by Lemma 3 with $\theta = 1$, $a' = 1$, $b' = M$, $\alpha = 0$, $\beta = (1 + \log 2)^{-1}$ and $\gamma = 2/3$, we have

$$\begin{aligned} 1 &= q_1^{\beta_1} \cdots q_r^{\beta_r} \left(1 - \frac{2^n M}{q_1^{\beta_1} \cdots q_r^{\beta_r}}\right) \\ &\ge q_1^{\beta_1} \cdots q_r^{\beta_r} \frac{c^{(7)}}{(q_1^{\beta_1} \cdots q_r^{\beta_r})^{2/3}}. \end{aligned} \tag{11}$$

By (10) and (11) we have $M \le c^{(8)}$. All $c^{(i)}$ depend only on $q_1, \cdots, q_r$. This completes the proof.

References

1. R. Baillie, *New primes of the form $k \cdot 2^n + 1$,* Math. Comput. 33(1979), 1333-1336. MR **80h:**10009
2. R. Baillie, G. V. Cormack and H. C. Williams, *The problem of Sierpiński concerning $k \cdot 2^n + 1$,* Math. Comput. 37 (1981), 229-231; corrigendum, 39(1982), 308. MR **83a:**10006b
3. A. Baker, *The theory of linear forms in logarithms,* Transcendence Theory: Advances and Applications (Academic Press, London and New York, 1977). MR **58:**16543
4. W. Bosma, *Explicit primality criteria for $h \cdot 2^k \pm 1$,* Math. Comput. 61(1993), 97-109. MR **94c:**11005
5. D. A. Buell and J. Young, *Some large primes and the Sierpiński problem*, SRC Technical Report 88-004, Supercomputing Research Center, Lanham MD, 1988.
6. Y. G. Chen, *On integers of the form $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*, Proc. Amer. Math. Soc. (to appear). CMP 99:14
7. S. L. G. Choi, *Covering the set of integers by congruences classes of distinct moduli,* Math. Comput. 25(1971), 885-895. MR **45:**6744
8. G. V. Cormack and H. C. Williams, *Some very large primes of the form $k \cdot 2^n + 1$,* Math. Comput. 35(1980), 1419-1421; corrigendum, Wilfrid Keller, 38(1982), 335. MR **82k:**10011
9. 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. MR **80i:**10077
10. R. K. Guy, Unsolved problems in number theory, 2nd ed. Springer, New York, 1994. MR **96e:**11002
11. G. Jaeschke, *On the smallest k such that all $k \cdot 2^N + 1$ are composite,* Math. Comput. 40(1983), 381-384; corrigendum, 45(1985), 637. MR **87b:**11009
12. Wilfrid Keller, *Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$,* Math. Comput. 41(1983), 661-673. MR **85b:**11119

13. K. Mahler, *On the fractional parts of powers of a rational number (II),* Mathematika 4(1957), 122-124. MR **20:**33
14. D. Ridout, *Rational approximations to algebraic numbers,* Mathematika 4(1957), 125-131. MR **20:**32
15. 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. MR **20:**3097
16. J. L. Selfridge, *Solution of problem 4995,* Amer. Math. Monthly 70(1963), 101.
17. W. Sierpiński, *Sur un problème concernant les nombres $k \cdot 2^n + 1$,* Elem. Math. 15(1960), 73-74; MR 22# 7983, corrigendum, 17(1962), 85.
18. R. G. Stanton and H. C. Williams, *Further results on covering of the integer $1 + k2^n$ by primes,* Combinatorial Math. VIII, Lecture Notes in Math. 884, Springer-Verlag, Berlin, New York, 1980, 107-114.
19. Kunrui Yu, *Linear forms in $p-$adic logarithms, III,* Compositio Mathematica 91(1994), 241-276. MR **95f:**11050

Department of Mathematics, Nanjing Normal University, Nanjing 210097, People's Republic of China

E-mail address: ygchen@pine.ninu.edu.cn