MATHEMATICS OF COMPUTATION
Volume 74, Number 250, Pages 1025–1031
S 0025-5718(04)01674-6
Article electronically published on July 20, 2004

FIVE CONSECUTIVE POSITIVE ODD NUMBERS, NONE OF WHICH CAN BE EXPRESSED AS A SUM OF TWO PRIME POWERS

YONG-GAO CHEN

ABSTRACT. In this paper, we prove that there is an arithmetic progression of positive odd numbers for each term M of which none of five consecutive odd numbers $M, M-2, M-4, M-6$ and $M-8$ can be expressed in the form $2^n \pm p^\alpha$, where p is a prime and n, α are nonnegative integers.

INTRODUCTION

By calculation, we find that almost all positive odd numbers can be expressed in the form $2^n + p$, where n is a positive integer and p is prime. For example, $5 = 2 + 3$, $7 = 2 + 5$, $9 = 2 + 7$, $11 = 2^2 + 7$, $13 = 2 + 11$, $15 = 2 + 13$, $17 = 2^2 + 13$, etc. The first counterexample is 127. In 1934, Romanoff [11] proved that the set of positive odd numbers which can be expressed in the form $2^n + p$ has positive asymptotic density in the set of all positive odd numbers, where n is a nonnegative integer and p is prime. For a positive integer n and an integer a, let $a \pmod{n} = \{a + nk : k \in \mathbf{Z}\}$. $\{a_i \pmod{m_i}\}_{i=1}^k$ is called *a covering system* if every integer b satisfies $b \equiv a_i \pmod{m_i}$ for at least one value of i. By employing a covering system, P. Erdős [8] proved that there is an infinite arithmetic progression of positive odd numbers each of which has no representation of the form $2^n + p$. Cohn and Selfridge [7] proved that there exist infinitely many odd numbers which are neither the sum nor the difference of two prime powers. In [3] Chen proved the following result: the set of positive integers which have no representation of the form $2^n \pm p^a q^b$, where p, q are distinct odd primes and n, a, b are nonnegative integers, has positive lower asymptotic density in the set of all positive odd integers. That is, the lower asymptotic density of the set 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 [5] Chen showed that the set of positive odd integers k such that $k - 2^n$ has at least three distinct prime factors for all positive integers n contains an infinite arithmetic progression. For further related information see Chen [4], [6], Guy [9, A19, B21, F13], Jaeschke [10], and Stanton and Williams [12]. The following question is a natural one: *Are there two consecutive positive odd numbers neither of which can be expressed as a sum of two prime powers?*

Received by the editor January 2, 2003 and, in revised form, October 2, 2003.
2000 *Mathematics Subject Classification.* Primary 11A07, 11B25.
Key words and phrases. Covering systems, odd numbers, sums of prime powers.
Supported by the National Natural Science Foundation of China, Grant No. 10171046 and the Teaching and Research Award Program for Outstanding Young Teachers in Nanjing Normal University.

©2004 American Mathematical Society

In this paper, we show that the answer to the question is affirmative. In fact, we go much further.

Theorem 1. *Let $k_1, \dots, k_s$ be integers, let $\{a_{ij} \,(\mathrm{mod}\, m_{ij})\}_{j=1}^{t_i} (1 \le i \le s)$ be s covering systems with $0 \le a_{ij} < m_{ij}$, and let p_{ij} be primes with m_{ij} the order of $2 \,(\mathrm{mod}\, p_{ij})$ $(1 \le j \le t_i, 1 \le i \le s)$ such that if $p_{ij} = p_{uv}$, then*

$$2^{a_{ij}} - k_i \equiv 2^{a_{uv}} - k_u \,(\mathrm{mod}\, p_{ij}).$$

Then there exists an arithmetic progression of positive odd numbers for each term M of which none of $M + k_i$ $(1 \le i \le s)$ can be expressed in the form $2^n \pm p^\alpha$, where p is a prime and n, α are nonnegative integers.

Theorem 2. *There exists an arithmetic progression of positive odd numbers for each term M of which none of five consecutive odd numbers $M, M-2, M-4, M-6$ and $M-8$ can be expressed in the form $2^n \pm p^\alpha$, where p is a prime and n, α are nonnegative integers.*

Remark. By the proofs of Theorems 1 and 2, there is an integer $M \le 2^{2^{253000}}$ such that none of five consecutive odd numbers $M, M-2, M-4, M-6$ and $M-8$ can be expressed in the form $2^n \pm p^\alpha$. Currently, we cannot give an explicit value of M.

2. Proofs

Lemma 1. *Let p be an odd prime and let T be a positive integer. Then $2^{p^T} - 1$ has at least T distinct prime factors.*

Proof. Let q_i $(i = 1, 2, \dots, T)$ be primes with

$$q_i \Big| \frac{2^{p^i} - 1}{2^{p^{i-1}} - 1}.$$

Then $q_1, q_2, \dots, q_T$ are distinct primes. This completes the proof of Lemma 1. □

Lemma 2. *Let p be an odd prime and let m be the order of $2 \,(\mathrm{mod}\, p)$. If*

$$2^m = 1 + p^l d, \quad p \nmid d,$$

and $p^u | 2^n - 1$ for two integers $n \ge 0$ and $u > 0$, then $n = mp^{u-l} v$ for some integer v.

Proof. By using induction on r, we can prove that

$$2^{mp^r} = 1 + p^{l+r} d_r, \quad p \nmid d_r, \quad r = 0, 1, \dots.$$

By $p | 2^n - 1$ and m being the order of $2 \,(\mathrm{mod}\, p)$, we have $m | n$. Let $n = mp^h v'$, $p \nmid v'$. Then

$$2^n = 2^{mp^h v'} = 1 + p^{l+h} d'_h, \quad p \nmid d'_h.$$

Since $p^u | 2^n - 1$, we have $u \le l + h$. Hence $h \ge u - l$. Let $v = v' p^{h-u+l}$. This completes the proof of Lemma 2. □

Lemma 3. *Let $p_1, \dots, p_t$ be primes such that each prime repeats at most s times. Then there exist t distinct primes $q_1, \dots, q_t$ such that*

$$q_i | 2^{p_i^{t+s}} - 1, \quad q_i \ne p_j, \quad \textit{for all } i, j.$$

Proof. For each prime p, by Lemma 1 we may take a set $S(p)$ of primes with $|S(p)| = t + s$ such that

$$q|2^{p^{t+s}} - 1.$$

Since there are at most s indexes i with $p_i = p$, we may appoint a prime $q_i \in S(p) \setminus \{p_1, \dots, p_t\}$ for each i with $p_i = p$ such that if $p_i = p_j = p$, then $q_i \neq q_j$. If $p_i \neq p_j$, then, by $q_i \in S(p_i)$ and $q_j \in S(p_j)$ we have

$$q_i|2^{p_i^{t+s}} - 1, \quad q_j|2^{p_j^{t+s}} - 1.$$

Hence $q_i \neq q_j$. Thus, these q_i are distinct such that

$$q_i|2^{p_i^{t+s}} - 1, \quad q_i \neq p_j, \quad \text{for all } i, j.$$

This completes the proof of Lemma 3. □

Proof of Theorem 1. If $p_{iu} = p_{iv}$, then, by m_{iu} and m_{iv} being the orders of $2 \,(\operatorname{mod} p_{iu})$ and $2 \,(\operatorname{mod} p_{iv})$, respectively, we have $m_{iu} = m_{iv}$. By

$$2^{a_{iu}} - k_i \equiv 2^{a_{iv}} - k_i \,(\operatorname{mod} p_{iu})$$

and m_{iu} of the order of $2 \,(\operatorname{mod} p_{iu})$, we have

$$a_{iv} \equiv a_{iu} \,(\operatorname{mod} m_{iu}).$$

Hence $a_{iu} \,(\operatorname{mod} m_{iu}) = a_{iv} \,(\operatorname{mod} m_{iv})$. Thus, without loss of generality, we may assume that for each i, primes $p_{i1}, \dots, p_{it_i}$ are distinct. Let $T = s + t_1 + \cdots + t_s$. By Lemma 3, for each p_{ij}, we may appoint a prime q_{ij} such that all primes q_{ij} $(1 \le j \le t_i, 1 \le i \le s)$ are distinct,

$$q_{ij} \,|\, 2^{p_{ij}^T} - 1, \qquad 1 \le j \le t_i, 1 \le i \le s,$$

and $q_{ij} \neq p_{uv}$ for all $1 \le j \le t_i, 1 \le i \le s, 1 \le v \le t_u, 1 \le u \le s$. Let r_{ij} be integers such that $0 \le r_{ij} < p_{ij}$ and

$$r_{ij} \equiv 2^{a_{ij}} - k_i \,(\operatorname{mod} p_{ij}), \quad 1 \le j \le t_i, 1 \le i \le s. \tag{1}$$

Let

$$2^{m_{ij}} = 1 + p_{ij}^{l_{ij}} t_{ij}, \quad p \nmid t_{ij}, \quad 1 \le j \le t_i, \ 1 \le i \le s,$$

and $l = \max_{i,j} l_{ij}$. If there exists a nonnegative integer $b \equiv a_{ij} \,(\operatorname{mod} m_{ij})$ with

$$p_{ij}^{l+T}|2^b - k_i - r_{ij}, \tag{2}$$

then let b_{ij} be the least one of such b. If there are no such b, then let $b_{ij} = a_{ij}$. Let m be a positive integer with

$$2^m \ge \max_{i,j} p_{ij}^{l+T} + \max_i |k_i| + 1.$$

Take an integer M with

$$\begin{aligned} &M \equiv r_{ij} \,(\operatorname{mod} p_{ij}^{l+T}), \\ &M \equiv 2^{b_{ij}} - k_i \,(\operatorname{mod} q_{ij}), \quad 1 \le j \le t_j, 1 \le i \le s, \\ &M \equiv 1 + 2^m + 2^{m+1} \,(\operatorname{mod} 2^{m+2}). \end{aligned} \tag{3}$$

If $p_{ij} = p_{uv}$, then $r_{ij} = r_{uv}$ by the condition. Again, q_{ij} are distinct and each q_{ij} is different from any p_{uv}. So such an M exists by the Chinese Remainder Theorem. Now we prove that none of $M + k_i$ $(1 \le i \le s)$ can be expressed in the form $2^n \pm p^\alpha$, where p is a prime and n, α are nonnegative integers. In order to prove this, it is enough to show that for each i and any nonnegative integer n, $M + k_i - 2^n$ has at least two distinct positive prime factors. Since $\{a_{ij} \pmod{m_{ij}}\}_{j=1}^{t_i}$ is a covering system, there exists a j with

$$n \equiv a_{ij} \pmod{m_{ij}}.$$

By (1), (3) and $2^{m_{ij}} \equiv 1 \pmod{p_{ij}}$, we have

$$M + k_i - 2^n \equiv r_{ij} + k_i - 2^{a_{ij}} \equiv 0 \pmod{p_{ij}}.$$

Let

$$M + k_i - 2^n = p_{ij}^{\alpha_{ij}} K_{ij}, \quad p_{ij} \nmid K_{ij},\ \alpha_{ij} \ge 1.$$

If $\alpha_{ij} < l + T$, then by

$$\begin{aligned} |M + k_i - 2^n| &= |1 + 2^m + 2^{m+1} + 2^{m+2}u + k_i - 2^n| \\ &\ge |1 + 2^m + 2^{m+1} + 2^{m+2}u - 2^n| - |k_i| \\ &\ge 2^m - 1 - |k_i| \ge p_{ij}^{l+T}, \end{aligned}$$

we have $|K_{ij}| > 1$. In this case, $M + k_i - 2^n$ has at least two distinct prime factors. If $\alpha_{ij} \ge l + T$, then $n \equiv a_{ij} \pmod{m_{ij}}$ and

$$r_{ij} + k_i - 2^n \equiv M + k_i - 2^n \equiv 0 \pmod{p_{ij}^{l+T}}.$$

Hence $n \equiv b_{ij} \pmod{m_{ij}}$ and by (2),

$$2^{b_{ij}}(1 - 2^{n-b_{ij}}) \equiv 2^{b_{ij}} - k_i + k_i - 2^n \equiv r_{ij} + k_i - 2^n \equiv 0 \pmod{p_{ij}^{l+T}}.$$

Thus

$$p_{ij}^{l+T} | 2^{n-b_{ij}} - 1.$$

By Lemma 2 we have $n - b_{ij} = m_{ij} p_{ij}^T v_{ij}$ for some integer v_{ij}. By

$$q_{ij} \mid 2^{p_{ij}^T} - 1,$$

we have

$$q_{ij} | 2^{n-b_{ij}} - 1.$$

That is,

$$q_{ij} | 2^n - 2^{b_{ij}}.$$

Hence

$$M + k_i - 2^n \equiv 2^{b_{ij}} - k_i + k_i - 2^n \equiv 2^{b_{ij}} - 2^n \equiv 0 \pmod{q_{ij}}.$$

Thus $q_{ij} | K_{ij}$ and then $M + k_i - 2^n$ has at least two distinct prime factors. This completes the proof of Theorem 1. $\square$

Proof of Theorem 2. Let $k_1 = 0$, $k_2 = -2$, $k_3 = -4$, $k_4 = -6$ and $k_5 = -8$. Take

$$\begin{aligned}
\{a_{1j} \,(\mathrm{mod}\, m_{1j})\}_{j=1}^{8} = \{&0 \,(\mathrm{mod}\, 2), & 3 \,(\mathrm{mod}\, 4),\ &5 \,(\mathrm{mod}\, 8),\\
&9 \,(\mathrm{mod}\, 16), & 17 \,(\mathrm{mod}\, 32),\ &33 \,(\mathrm{mod}\, 64),\\
&1 \,(\mathrm{mod}\, 128), & 65 \,(\mathrm{mod}\, 128)\},&\\
\{a_{2j} \,(\mathrm{mod}\, m_{2j})\}_{j=1}^{7} = \{&1 \,(\mathrm{mod}\, 2), & 0 \,(\mathrm{mod}\, 4),\ &6 \,(\mathrm{mod}\, 8),\\
&10 \,(\mathrm{mod}\, 16), & 18 \,(\mathrm{mod}\, 32),\ &34 \,(\mathrm{mod}\, 64),\\
&2 \,(\mathrm{mod}\, 64)\},&&\\
\{a_{3j} \,(\mathrm{mod}\, m_{3j})\}_{j=1}^{26} = \{&0 \,(\mathrm{mod}\, 3), & 2 \,(\mathrm{mod}\, 4),\ &3 \,(\mathrm{mod}\, 5),\\
&1 \,(\mathrm{mod}\, 10), & 4 \,(\mathrm{mod}\, 12),\ &2 \,(\mathrm{mod}\, 15),\\
&1 \,(\mathrm{mod}\, 18), & 7 \,(\mathrm{mod}\, 20),\ &8 \,(\mathrm{mod}\, 24),\\
&19 \,(\mathrm{mod}\, 25), & 24 \,(\mathrm{mod}\, 25),\ &11 \,(\mathrm{mod}\, 36),\\
&23 \,(\mathrm{mod}\, 36), & 25 \,(\mathrm{mod}\, 40),\ &25 \,(\mathrm{mod}\, 45),\\
&40 \,(\mathrm{mod}\, 45), & 20 \,(\mathrm{mod}\, 48),\ &44 \,(\mathrm{mod}\, 48),\\
&9 \,(\mathrm{mod}\, 50), & 39 \,(\mathrm{mod}\, 50),\ &37 \,(\mathrm{mod}\, 60),\\
&35 \,(\mathrm{mod}\, 72), & 4 \,(\mathrm{mod}\, 75),\ &5 \,(\mathrm{mod}\, 120),\\
&29 \,(\mathrm{mod}\, 150), & 215 \,(\mathrm{mod}\, 360)\},&\\
\{a_{4j} \,(\mathrm{mod}\, m_{4j})\}_{j=1}^{9} = \{&0 \,(\mathrm{mod}\, 2), & 1 \,(\mathrm{mod}\, 4),\ &7 \,(\mathrm{mod}\, 8),\\
&11 \,(\mathrm{mod}\, 16), & 19 \,(\mathrm{mod}\, 32),\ &35 \,(\mathrm{mod}\, 64),\\
&67 \,(\mathrm{mod}\, 128), & 3 \,(\mathrm{mod}\, 256),\ &131 \,(\mathrm{mod}\, 256)\}\\
\{a_{5j} \,(\mathrm{mod}\, m_{5j})\}_{j=1}^{13} = \{&1 \,(\mathrm{mod}\, 2), & 2 \,(\mathrm{mod}\, 3),\ &2 \,(\mathrm{mod}\, 5),\\
&4 \,(\mathrm{mod}\, 9), & 6 \,(\mathrm{mod}\, 10),\ &6 \,(\mathrm{mod}\, 12),\\
&10 \,(\mathrm{mod}\, 18), & 0 \,(\mathrm{mod}\, 20),\ &24 \,(\mathrm{mod}\, 30),\\
&34 \,(\mathrm{mod}\, 36), & 48 \,(\mathrm{mod}\, 60),\ &34 \,(\mathrm{mod}\, 90)\\
&88 \,(\mathrm{mod}\, 180)\}.&&
\end{aligned}$$

Noting that $\{a_j \,(\mathrm{mod}\, m_j)\}_{j=1}^{k}$ is a covering system if and only if for every integer n with $0 \le n <$ l.c.m. $\{m_1, \dots, m_k\}$ there exists a j with $n \equiv a_j \,(\mathrm{mod}\, m_j)$, we can verify that $\{a_{1j} \,(\mathrm{mod}\, m_{1j})\}_{j=1}^{8}$, $\{a_{2j} \,(\mathrm{mod}\, m_{2j})\}_{j=1}^{7}$, $\{a_{3j} \,(\mathrm{mod}\, m_{3j})\}_{j=1}^{26}$, $\{a_{4j} \,(\mathrm{mod}\, m_{4j})\}_{j=1}^{9}$ and $\{a_{5j} \,(\mathrm{mod}\, m_{5j})\}_{j=1}^{13}$ are all covering systems. Now, for every $a_{ij} \,(\mathrm{mod}\, m_{ij})$ we appoint a prime p_{ij} such that m_{ij} is the order of $2 \,(\mathrm{mod}\, p_{ij})$ and if $p_{ij} = p_{uv}$, then

$$2^{a_{ij}} - k_i \equiv 2^{a_{uv}} - k_u \,(\mathrm{mod}\, p_{ij}). \tag{4}$$

Case 1. Let $p_{11} = p_{21} = p_{41} = p_{51} = 3$. Then

$$2^0 - 0 \equiv 2^1 - (-2) \equiv 2^0 - (-6) \equiv 2^1 - (-8) \,(\mathrm{mod}\, 3).$$

Case 2. Let $p_{12} = p_{22} = p_{32} = p_{42} = 5$. Then

$$2^3 - 0 \equiv 2^0 - (-2) \equiv 2^2 - (-4) \equiv 2^1 - (-6) \,(\mathrm{mod}\, 5).$$

Case 3. Let

$$p_{13} = p_{23} = p_{43} = 17, \quad p_{14} = p_{24} = p_{44} = 257,$$
$$p_{15} = p_{25} = p_{45} = 65537, \quad p_{16} = p_{26} = p_{46} = 641, \quad p_{27} = 6700417.$$

Note that both Fermat numbers F_6 and F_7 are composite, let $p_{18} = p_{47}$, p_{17} be two distinct prime divisors of $2^{64}+1$, and let p_{48}, p_{49} be two distinct prime divisors of $2^{128}+1$. Then (4) follows from the following fact:

$$2^{2^k+1} - 0 \equiv 2^{2^k+2} - (-2) \equiv 2^{2^k+3} - (-6) \pmod{2^{2^k}+1}.$$

Case 4. Let

$$p_{31} = p_{52} = 7, \quad p_{33} = p_{53} = 31,$$
$$p_{34} = p_{55} = 11, \quad p_{35} = p_{56} = 13,$$
$$p_{37} = p_{57} = 19, \quad p_{38} = p_{58} = 41,$$
$$p_{3(12)} = p_{5(10)} = 109, \quad p_{3(13)} = 37.$$

Then

$$2^0 - (-4) \equiv 2^2 - (-8) \pmod 7, \quad 2^3 - (-4) \equiv 2^2 - (-8) \pmod{31},$$
$$2^1 - (-4) \equiv 2^6 - (-8) \pmod{11}, \quad 2^4 - (-4) \equiv 2^6 - (-8) \pmod{13},$$
$$2^1 - (-4) \equiv 2^{10} - (-8) \pmod{19}, \quad 2^7 - (-4) \equiv 2^0 - (-8) \pmod{41},$$
$$2^{11} - (-4) \equiv 2^{34} - (-8) \pmod{109}.$$

Case 5. Each of 25, 45, 48, 50, 60 is the order of 2 modulus two distinct primes. These primes are 601, 1801; 631, 23311; 97, 673; 251, 4051; 61, 1321, respectively. If $m > 1$ and $m \neq 6$, then there exists at least one prime p with m the order of $2 \pmod p$ (see [1], [2], [13]). Thus we may appoint a prime p_{ij} for each of the remaining $a_{ij} \pmod{m_{ij}}$. Now, Theorem 2 follows from Theorem 1. □

Acknowledgment

I am grateful to the referee for his/her suggestion.

References

[1] A. S. Bang, Taltheoretiske Undersøgelser, *Tidsskrift for Mat.* (5), 4(1886), 70-80, 130-137.
[2] G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. Math.* 5(1904), 173-180.
[3] 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. MR 2000j:11006
[4] Y. G. Chen, On integers of the form $k2^n + 1$, *Proc. Amer. Math. Soc.* 129(2001), 355-361. MR 2003a:11004
[5] Y. G. Chen, On integers of the forms $k - 2^n$ and $k2^n + 1$, *J. Number Theory* 89(2001), 121-125. MR 2002b:11020
[6] Y. G. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, *J. Number Theory* 98(2003), 310-319. MR 2003m:11004
[7] F. Cohen and J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. Comput.* 29(1975), 79-81. MR 51:12758
[8] P. Erdős, On integers of the form $2^r + p$ and some related problems, *Summa Brasil. Math.* 2(1950), 113-123. MR 13:437i
[9] R. K. Guy, "Unsolved problems in number theory," 2nd ed., Springer, New York, 1994. MR 96e:11002
[10] G. Jaeschke, On the smallest k such that all $k \cdot 2^N + 1$ are composite, *Math. Comput.* 40(1983), 381-384; corrigendum, *Math. Comput.* 45(1985) 637. MR 84k:10006; MR 87b:11009

[11] N. P. Romanoff, Über einige Sätze der additiven Zahlentheorie, *Math. Ann.* 57(1934), 668-678.
[12] R. G. Stanton and H. C. Williams, Further results on covering of the integer $1 + k2^n$ by primes, in "Combinatorial Math. VIII," Lecture Notes in Math. 884, Springer-Verlag, Berlin/New York, 1980, 107-114. MR 84j:10009
[13] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* 3(1892), 265-284.

Department of Mathematics, Nanjing Normal University, Nanjing 210097, Peoples Republic of China
E-mail address: ygchen@pine.njnu.edu.cn