ACTA ARITHMETICA
115.1 (2004)

Integers not of the form $c(2^a + 2^b) + p^\alpha$

by

Pingzhi Yuan (Guangzhou)

1. Introduction. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and let $\mathbb{P}$ denote the set of (positive) primes. There have been some studies on the integers not of the form $2^a + p^\alpha$ and $2^a + 2^b + p^\alpha$ (where $a, b, \alpha \in \mathbb{N}$ and $p \in \mathbb{P}$). N. P. Romanoff [7] proved that the set of positive odd numbers which can be represented in the form $2^a + p$ has positive asymptotic density in the set of all positive odd integers, while J. G. van der Corput [2] proved a similar result for the set of positive odd integers which cannot be represented in the form $2^a + p$. A step forward was made by P. Erdős [5] who used covering congruences to exhibit a residue class of odd integers not of the form $2^a + p$. Using similar methods, F. Cohen and J. L. Selfridge [1] proved that there exists an arithmetic progression of odd numbers which are neither the sum nor the difference of a power of 2 and a prime power; Z. W. Sun [9] constructed a residue class of odd integers which is not of the form $\pm 2^a \pm p^\alpha$ where $a, \alpha \in \mathbb{N}, p \in \mathbb{P}$ and any choice of signs can be made.

On the other hand, A. Schinzel observed that for $n \geq 3$, the number $2^{2^n} - 1$ is not of the form $2^a + 2^b + p$, where $a > b \in \mathbb{Z}^+$ and $p \in \mathbb{P}$ (see the footnote 1 of [4]). Combining the observation of Schinzel with the idea of Erdős [5], i.e., the idea of using covering congruences, in 1971 R. Crocker [4] showed that there are infinitely many positive odd integers not of the form $2^a + 2^b + p$ where $a, b \in \mathbb{N}$ and $p \in \mathbb{P}$. By generalizing Crocker's Lemma II via congruences and using some results on exponential diophantine equations, Z. W. Sun and M. H. Le [10] strengthened Schinzel's result by proving that for $n \geq 4$, the number $2^{2^n} - 1$ is not of the form $2^a + 2^b + p^\alpha$, where $n, a, b, \alpha \in \mathbb{N}, a > b$ and $p \in \mathbb{P}$. In 2001 Sun (see [10]) made the following conjecture.

Conjecture 1.1. *For any positive integer c, there are infinitely many positive odd integers not of the form $c(2^a + 2^b) + p^\alpha$, where $a, b, \alpha \in \mathbb{N}$ and $p \in \mathbb{P}$.*

2000 *Mathematics Subject Classification*: 11B75, 11B25, 11P32.

Sun and Le [10] showed that the conjecture holds if c is a Fermat number $2^{2^n}+1$.

On the basis of the work of Crocker [4] and Erdős [5], with Schlickewei's [8] result on S-unit equations and some results on exponential diophantine equations via congruences, in this paper we give an affirmative answer to the above conjecture. We prove

THEOREM 1.1. *For any given positive integer c, there are infinitely many positive odd integers not of the form $c(2^a+2^b)+p^\alpha$, where $a,b,\alpha\in\mathbb{N}$ and $p\in\mathbb{P}$.*

2. Preliminaries. Let $S=\{0,p_1,\dots,p_s\}$, where $p_1,\dots,p_s\in\mathbb{P}$. For $v\in S$ we denote by $|\,|_v$ the v-adic absolute value on $\mathbb{Q}$, where $v=0$ stands for the standard absolute value. An element $x\in\mathbb{Q}$ is called an *S-unit* if $\prod_{v\in S}|x|_v=1$.

LEMMA 2.1 ([8]). *Let S be a set as above. Then the number of integral solutions $(x_1,\dots,x_{n+1})$ of the equation*

$$a_1x_1+\cdots+a_{n+1}x_{n+1}=0,\qquad \gcd(x_1,\dots,x_{n+1})=1$$

where each x_i is an S-unit, and a_i $(i=1,\dots,n+1)$ are fixed rational integers such that no proper sub-sum $a_{i_1}x_{i_1}+\cdots+a_{i_m}x_{i_m}$ vanishes, is bounded by

$$(8(s+1))^{2^{26n+4}(s+1)^6}.$$

A system of residue classes $a_i \pmod{n_i}$, $1\le i\le k$, is called a *covering congruence system* of $\mathbb{Z}$ if for any given integer $n\in\mathbb{Z}$, there is at least one $i\in\{1,\dots,k\}$ such that $n\equiv a_i \pmod{n_i}$.

LEMMA 2.2. *Let $a_i \pmod{n_i}$, $0\le a_i<n_i$, $1\le i\le k$, be a covering congruence system, $p_1,\dots,p_k$ be distinct prime divisors of $2^{n_1}-1,\dots,2^{n_k}-1$ respectively, and $x\equiv 2^{a_s} \pmod{p_s}$ for every $1\le s\le k$. If $x=2^n+p^\alpha$ for some $n,\alpha\in\mathbb{N}$, then there is an $s\in\{1,\dots,k\}$ such that $n=a_s+an_s$ and $x=2^n+p_s^b$ for some $a,b\in\mathbb{N}$.*

Proof. Since $\{a_i \pmod{n_i}\}_{i=1}^k$ is a covering system, we have $n\equiv a_s \pmod{n_s}$ for some $s\in\{1,\dots,k\}$. Moreover, since $2^{n_s}\equiv 1 \pmod{p_s}$ by the definition of p_i's, we have $x=2^n+p^\alpha\equiv 2^{a_s}+p^\alpha \pmod{p_s}$. On the other hand we have $x\equiv 2^{a_s} \pmod{p_s}$ according to our assumptions. Consequently, $p=p_s$ and the lemma follows. ∎

For every nonnegative integer r, let F_r denote the Fermat number $2^{2^r}+1$. It is well known [6] that

$$\prod_{r=0}^{n-1}F_r=F_n-2=2^{2^n}-1\quad\text{for } n=1,2,\dots, \tag{1}$$

which can be easily proved by induction. This implies that the Fermat numbers $F_0, F_1, \ldots$ are pairwise coprime.

REMARK 1. As the referee pointed out, the nontrivial fact that F_{10} has a prime divisor $2^{12} \cdot 11131 + 1$, which is essential to our argument, was proved by Selfridge in the 1950's.

We have

LEMMA 2.3. *For* $n \geq 3$ *and* $w \equiv 1 \pmod{16}$, *let* $w \prod_{i=0}^{n-1} B_i \leq 2^{2^n} - 1$, *where* $B_i \mid F_i$ *and* $B_i > 1$. *Suppose* $w \prod_{i=0}^{n-1} B_i = 2^a + 2^b + p^\alpha$, *where* $a, b, \alpha \in \mathbb{N}$, $a > b$ *and* $p \in \mathbb{P}$. *Then* $\alpha > 0$, *and one of the following statements holds*:

(i) $a \not\equiv b \pmod 2$, $b \in \{1, 2\}$ *and* $p = 3$.
(ii) $a \equiv 3 \pmod 4$, $b = 1$ *and* $p = 5$.

Proof. This is a special case of Proposition 1 of [10]. ∎

As in Crocker [4], we choose the covering congruence system $a_i \pmod{n_i}$, $1 \leq i \leq 28$, to be

0(3), 0(5), 1(9), 1(10), 8(12), 8(15), 4(18), 7(20), 5(24),
29(30), 2(36), 14(36), 17(40), 34(45), 43(45), 13(48), 37(48),
16(60), 19(60), 26(72), 62(72), 52(90), 37(120), 49(144),
121(144), 103(180), 106(180), 229(360),

where $a(n)$ stands for the residue class $a \pmod n$. It can be shown to be a covering congruence system by straightforward numerical methods; the corresponding p_i of $2^{n_i} - 1, 1 \leq i \leq 28$, are chosen to be

7, 31, 73, 11, 13, 151, 19, 41, 241, 331, 37, 109, 61681, 631, 23311,
97, 673, 61, 1321, 833, 38737, 18837001, 4562284561, 577,
487824887233, 29247661, 54001, 168692292721.

Set

$$G_{10} = (2^{2^{10}} + 1)/(2^{12} \cdot 11131 + 1).$$

Let $M_n = 2^n - 1$ be the nth Mersenne number. It is well known [6] that $\gcd(M_m, M_n) = M_{\gcd(m,n)}$. With this property, one can check easily that

$$(p_i, 2^{2^n} - 1) = 1 \quad \text{for every } p_i \text{ and } n,\ 1 \leq i \leq 28,$$

and also

$$16 \prod_{i=1}^{28} p_i < G_{10}, \quad \text{say} \quad \Big(16 \prod_{i=1}^{28} p_i\Big) v < G_{10} < (v+1)\Big(16 \prod_{i=1}^{28} p_i\Big)$$

for some fixed $v \geq 1$; by simple numerical calculation and estimation, v exists and in fact seems to be very large here ($> 2^{520}$).

Consider the following simultaneous conditions:

$$t \equiv 2^{a_i} \pmod{p_i}, \quad 1 \le i \le 28, \quad t \equiv -1 \pmod{16}, \quad t \equiv 0 \pmod{9},$$
$$t \equiv 0 \pmod{(2^{2^n}-1)/G_{10}F_0}, \quad t \le 2^{2^n}-1.$$

We denote the above simultaneous system by S_n for every $n > 10$.

By the Chinese Remainder Theorem, S_n is satisfied by any integer (and only those integers) such that

$$t \equiv q_n \left(\mathrm{mod}\, \frac{2^{2^n}-1}{G_{10}} \cdot 48 \prod_{i=1}^{28} p_i \right), \quad t \le 2^{2^n}-1, \tag{2}$$

where one may assume that q_n satisfies S_n and $0 < q_n < (2^{2^n}-1)/G_{10} \cdot 16\prod_{i=1}^{28} p_i$, and so q_n is fixed for any chosen n. Clearly, there are v ($> 2^{520}$) or $v+1$ positive integers satisfying (2). We have

LEMMA 2.4. *Let t be as above. Then t is not of the form $2^a + 2^b + p^\alpha$, where $a, b, \alpha \in \mathbb{N}$ and $p \in \mathbb{P}$.*

Proof. We apply Lemma 2.3 with $B_i = F_i$ for $0 \le i \le n-1$, $i \ne 10$ and $B_{10} = F_{10}/G_{10}$. Then by the construction of t, it suffices to prove that

(i) $t \ne 2^a + p^\alpha$, $a, \alpha \in \mathbb{N}$, $p \in \mathbb{P}$;
(ii) $t \ne 2^a + 2 + 3^\alpha$, $a \equiv 0 \pmod 2$, $\alpha > 0$;
(iii) $t \ne 2^a + 4 + 3^\alpha$, $a \equiv 1 \pmod 2$, $\alpha > 0$;
(iv) $t \ne 2^a + 2 + 5^\alpha$, $a \equiv 3 \pmod 4$, $\alpha > 0$.

Since $3^\alpha \equiv 3, 9, 11, 1 \pmod{16}$ and $t \equiv -1 \pmod{16}$, it follows that $t = 2^a + 2 + 3^\alpha$, $a \equiv 0 \pmod 2$, $a > 3$ cannot hold simultaneously. Since $t \equiv 0 \pmod 9$ and $t \ne 9$, we have $t \ne 2^2 + 2 + 3^\alpha$. Thus (ii) holds.

Modulo 9, $t = 2^a + 4 + 3^\alpha$, $a \equiv 1 \pmod 2$, $\alpha > 1$ hold only when $a \equiv 5 \pmod 6$. Further if $a \equiv 5 \pmod 6$, then modulo 7, we get $2^a + 4 + 3^\alpha \equiv 36 + 3^\alpha \not\equiv 1 \equiv 2^{a_1} \pmod{p_1}$, where $a_1 = 0$, $p_1 = 7$; and so we are left with $\alpha = 1$, but $t = 2^a + 7$ is impossible since $t \equiv -1 \pmod{16}$ and $t \ne 15$. Thus (iii) holds.

Modulo 3, $t = 2^a + 2 + 5^\alpha, a \equiv 3 \pmod 4, \alpha > 0$ hold only when $\alpha \equiv 1 \pmod 2$. Further if $\alpha \equiv 1 \pmod 2$, then modulo 13, since $5^\alpha \equiv \pm 5 \pmod{13}$, if $t = 2^a + 2 + 5^\alpha \equiv 2^8 \pmod{13} \equiv 2^{a_5} \pmod{p_5}$, then $2^a \equiv 2, -1 \pmod{13}$, and so $a \equiv 1, 6 \pmod{12}$, which contradicts $a \equiv 3 \pmod 4$. Thus (iv) holds.

By Lemma 2.2 and the construction of t, we know that (i) holds only when there is an $s \in \{1, \dots, 28\}$ such that $t = 2^a + p_s^\alpha$ and $a = a_s + bn_s$ for some $b, \alpha \in \mathbb{N}$.

From $t \equiv -1 \pmod{16}$, we get $a = 1$ if $p_s \equiv 1 \pmod 4$, $a \ge 2$ and α is odd if $p_s \equiv -1 \pmod 4$, whence this is impossible for those s with $p_s \equiv 1 \pmod 4$ and $a_s \ne 1$; from $t \equiv 0 \pmod 5$, we have $2^a \pm 1 \equiv 0 \pmod 5$, and so $a \equiv 0 \pmod 2$ if $p_s \equiv \pm 1 \pmod 5$; from $t \equiv 0 \pmod 9$, we have $2^a + 1 \equiv 0$

$(\mathrm{mod}\, 3)$, and so $a \equiv 1 \pmod 2$ if $p_s \equiv 1 \pmod 3$. It is easy to check that we are left with $p_3 = 73, a_3 = 1, n_3 = 9$ and $p_1 = 7, a_1 = 0, n_1 = 3$ by the above considerations, but $t \neq 2 + 73^\alpha$ since $t \equiv -1 \pmod{16}$. Since $t \equiv 2 \pmod{11}$ and α is odd, if $t = 8 + 7^\alpha$, then $7^\alpha \equiv 5 \pmod{11}$, and it follows that $-1 = \left(\frac{7}{11}\right)^\alpha = \left(\frac{5}{11}\right) = 1$, which is impossible. Therefore (i) also holds, which implies the lemma. ∎

Remark 2. Lemma 2.4 also implies an affirmative answer to Question 1 in [10].

3. Proof of Theorem 1.1. Let $c = c_0 \cdot 2^k$ with $2 \nmid c_0$. If $c_0 \neq 1$, then $c_0(2^n - 1) = c(2^a + 2^b) + p^\alpha$ holds only if $c_0 = p^{\alpha_1}$, whence

$$2^n - 1 = 2^{a+k} + 2^{b+k} + p^{\alpha_2}, \quad p^{\alpha_1} = c_0.$$

Applying Lemma 2.1 with $s = 2$ and $n = 4$, we find that the above equation has only finitely many integral solutions (n, a, b, α_2). Therefore there are infinitely many odd integers of the form $c_0(2^n - 1)$ which are not of the form $c(2^a + 2^b) + p^\alpha$, where $a, b, \alpha \in \mathbb{N}$ and $p \in \mathbb{P}$.

Suppose $c_0 = 1$. Then $c(2^a + 2^b) + p^\alpha$ reduces to the form $2^a + 2^b + p^\alpha$, and so it suffices to treat the case of $c = 1$, which has been done in Lemma 2.4. ∎

4. More precise conjectures. Finally, I suggest the following precise conjectures which seem to be correct.

Conjecture 4.1. *The set of positive odd integers not of the form* $2^a + 2^b + p^\alpha$, *where* $a, b, \alpha \in \mathbb{N}$ *and* $p \in \mathbb{P}$, *has a positive lower asymptotic density.*

Conjecture 4.2. *The set of positive odd integers not of the form* $2^a + 2^b + p^\alpha q^\beta$, *where* $a, b, \alpha, \beta \in \mathbb{N}$ *and* $p, q \in \mathbb{P}$, *is infinite and has asymptotic density* 0.

Conjecture 4.3. *Every odd integer* n *can be represented in the form* $2^a + 2^b + p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, *where* $a, b, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{N}$ *and* $p_1, p_2, p_3 \in \mathbb{P}$.

Conjecture 4.4. *The set of positive odd integers not of the form* $\pm 2^a \pm 2^b \pm p^\alpha$, *where* $a, b, \alpha \in \mathbb{N}$ *and* $p \in \mathbb{P}$, *is infinite and has asymptotic density* 0.

Conjecture 4.5. *Every odd integer* n *can be represented in the form* $\pm 2^a \pm 2^b \pm p^\alpha q^\beta$, *where* $a, b, \alpha, \beta \in \mathbb{N}$ *and* $p, q \in \mathbb{P}$.

Acknowledgments. The work was done at Leiden University when I was a visiting scholar. I would like to thank Robert Tijdeman, Jan Hendrik Evertse and the Mathematical Institute for their hospitality. And I am grateful to the referee for his/her helpful suggestions.

References

[1] F. Cohen and J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comp. 29 (1975), 79–81.
[2] J. G. van der Corput, *On de Polignac's conjecture*, Simon Stevin 27 (1950), 99–105.
[3] R. Crocker, *A theorem concerning prime numbers*, Math. Mag. 34 (1960/1961), 316–344.
[4] —, *On a sum of a prime and two powers of two*, Pacific J. Math. 36 (1971), 103–107.
[5] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. 2 (1950), 113–123.
[6] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[7] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. 57 (1934), 668–678.
[8] H. P. Schlickewei, *An explicit upper bound for the number of solutions of* S*-unit equation*, J. Reine Angew. Math. 406 (1990), 109–120.
[9] Z. W. Sun, *On integers not of the form* $\pm p^a \pm q^b$, Proc. Amer. Math. Soc. 128 (2000), 997–1002.
[10] Z. W. Sun and M. H. Le, *Integers not of the form* $c(2^a + 2^b) + p^\alpha$, Acta Arith. 99 (2001), 183–190.

Department of Mathematics
Sun Yat-Sen University
Guangzhou 510275, P.R. China
E-mail: yuanpz@mail.csru.edu.cn
mcsypz@zsu.edu.cn

Received on 29.7.2002
and in revised form on 18.4.2004 (4339)