ACTA ARITHMETICA
XCIX.2 (2001)

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

by

Zhi-Wei Sun (Nanjing) and Mao-Hua Le (Zhanjiang)

1. Introduction. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{P}$ denote the set of (positive) primes. In 1950 van der Corput [Co] showed that those positive odd integers not representable in the form $2^a + p$ (where $a \in \mathbb{N}$ and $p \in \mathbb{P}$) form a subset of $\mathbb{Z}^+ = \{1, 2, \ldots\}$ with positive lower asymptotic density. By means of cover of the ring $\mathbb{Z}$ of integers, P. Erdős [E] constructed a residue class of odd numbers which contains no integers of the form $2^a + p$. (See also W. Sierpiński [Si].) On the basis of the work of F. Cohen and J. L. Selfridge [CS], in 2000 Zhi-Wei Sun [Su] showed that any integer in the residue class

$$47867742232066880047611079 \pmod{6648303402501871163986252749 0}$$

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.

Lemma I of R. Crocker [Cr2] asserts that for each $n = 3, 4, \ldots$ the number $2^{2^n} - 1$ cannot be expressed as the sum of a prime and of two *distinct* positive powers of 2; this was first observed by A. Schinzel after his reading the earlier paper [Cr1]. (See p. 447 of [Si], and footnote 1 of [Cr2], where R. Crocker wrote that he had obtained the result independently.) Through computer search the referee notes that the above $2^{2^n} - 1$ cannot be replaced by $2^{2^n} + 1$ or $2^{2^n} - 3$. It seems that $2^{2^n} - 1 = 2^a + p$ has infinitely many solutions including

$$(n, a, p) = (2, 3, 7),\ (3, 6, 191),\ (4, 11, 63487),\ (5, 31, 2147483647).$$

In view of the above, it is natural to ask the following

Question 1. *Are there infinitely many positive odd integers which cannot be written as the sum of a prime power and of two distinct powers of* 2*?*

2000 *Mathematics Subject Classification*: Primary 11P32; Secondary 11D61.

The first author is supported by the Teaching and Research Award Fund for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P.R. China. The second author is supported by the NSFs of China and Guangdong Province.

In this paper we answer the question affirmatively by strengthening Schinzel's result.

In 1971 Crocker [Cr2] successfully combined the observation of Schinzel with the idea of Erdős [E] on integers not of the form 2^a+p and showed that there are infinitely many positive odd numbers which cannot be the sum of a prime and of two positive powers of 2, though the least such number greater than 8 is extremely large and one can hardly write it out explicitly.

Crocker's work in [Cr2] suggests the following

QUESTION 2. *Let c be a positive integer. Are there infinitely many positive odd integers not of the form $c(2^a+2^b)+p^\alpha$ where $a,b,\alpha\in\mathbb{N}$ and $p\in\mathbb{P}$?*

Though we are not able to answer this question for $c=1$, we can give a positive answer for any Fermat number c.

Now we state our main results.

THEOREM 1. *The only solutions of the diophantine equation*

$$2^{2^n}-1=2^a+2^b+p^\alpha \tag{1.1}$$

with

$$n,a,b,\alpha\in\mathbb{N},\quad a>b\quad\text{and}\quad p\in\mathbb{P} \tag{1.2}$$

are as follows:

$$2^{2^2}-1=2^2+2+3^2=2^3+2^2+3=2^3+2+5, \tag{1.3}$$

$$2^{2^3}-1=2^3+2^2+3^5=2^7+2+5^3. \tag{1.4}$$

REMARK 1. The referee finds that the diophantine equation

$$2^{2^n}-1+2^a+2^b=p\quad\text{ with } n,a,b\in\mathbb{N},\ a>b \text{ and } p\in\mathbb{P}$$

has a lot of solutions including

$$(n,a,b)=(3,9,1),\ (3,28,20),\ (4,22,6),\ (5,45,13),\ (6,76,12),\ (7,137,9).$$

He also notices that $2^{2^3}-1$ can be written as the sum of a prime and of three powers of 2 in many ways, e.g. $2^8-1=2^5+2^6+2^7+31$.

Theorem 1 has the following consequence.

COROLLARY 1. *For each $n=3,4,5,\ldots$ the number $2^{2^n}-5$ cannot be the sum of two prime powers except that $2^{2^3}-5=2^3+3^5$.*

Our second theorem is the following

THEOREM 2. *There are infinitely many positive odd integers not representable by $c(2^a+2^b)+p^\alpha$ where $a,b,\alpha\in\mathbb{N}$, $p\in\mathbb{P}$ and c is a Fermat number.*

In fact, the only solutions of the diophantine equation

$$2^{2^n} - 1 = c(2^a + 2^b) + p^\alpha \tag{1.5}$$

with $n \in \mathbb{N}$ *and* a, b, c, p, α *as above, are as follows*:

$$2^{2^2} - 1 = 3(2^0 + 2^0) + 3^2 = 5(2^0 + 2^0) + 5, \tag{1.6}$$

$$2^{2^2} - 1 = 3(2 + 2) + 3, \quad 2^{2^3} - 1 = 3(2 + 2) + 3^5. \tag{1.7}$$

By using congruences modulo Fermat numbers and powers of two, we reduce the proofs of Theorems 1 and 2, in Section 2, to solving some exponential diophantine equations in Section 3.

2. Two auxiliary propositions. Let F_r denote the Fermat number $2^{2^r} + 1$ for $r = 0, 1, 2, \ldots$ Then

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

are all primes, but $F_5 = 641 \cdot 6700417$ as discovered by Euler. It is well known that

$$\prod_{r=0}^{n-1} F_r = F_n - 2 = 2^{2^n} - 1 \quad \text{for } n = 1, 2, \ldots \tag{2.1}$$

(This fact can be easily proved by induction.) Thus the Fermat numbers $F_0, F_1, F_2, \ldots$ are pairwise coprime.

Let $F_r^* > 1$ be a divisor of F_r for every $r = 0, 1, 2, \ldots$ Lemma II of Crocker [Cr2] states that for $n \geq 3$ and $w \equiv 1 \pmod{16}$ if $W = w \prod_{r=0}^{n-1} F_r^* \leq 2^{2^n} - 1$ then W cannot be expressed in the form $2^a + 2^b + p$ with $a, b \in \mathbb{Z}^+$, $a \neq b$ and $p \in \mathbb{P}$. Crocker obtained this by finding a proper divisor of $W - 2^a - 2^b$.

In this section we aim to generalize Crocker's Lemma II via congruences.

PROPOSITION 1. *Let* n, w, w' *be positive integers with*

$$w \equiv 1 \pmod{16}, \quad w' \equiv 1, \pm 3 \pmod{8}, \quad W = w \prod_{r=0}^{n-1} F_r^* \leq 2^{2^n} - 1. \tag{2.2}$$

Suppose that

$$W = w'(2^a + 2^b) + p^\alpha \quad \text{where } a, b, \alpha \in \mathbb{N},\ a > b \text{ and } p \in \mathbb{P}. \tag{2.3}$$

Then $\alpha > 0$, *and one of the following* (i) *and* (ii) *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. Write $a - b = 2^k q$ where $k \in \mathbb{N}$, $q \in \mathbb{Z}^+$ and $2 \nmid q$. Obviously $2^k \leq a - b \leq a < 2^n$ and hence $k < n$. As q is odd, $F_k = 2^{2^k} + 1$ divides

$2^{2^k q}+1=2^{a-b}+1$. So

$$p^\alpha = W - w'2^b(2^{a-b}+1) \equiv 0 \pmod{F_k^*}.$$

Therefore $\alpha>0$, $p \mid F_k^*$ and $b\neq 0$.

It is known that for each $r=2,3,\ldots$ any prime divisor of F_r has the form $2^{r+2}m+1$ with $m\in\mathbb{Z}^+$. (See Theorem 5.5.1 of [A].) Thus $F_5^*, F_6^*, \ldots$ are all congruent to 1 modulo 2^{5+2}, and so are the primes $F_3^*=F_3$ and $F_4^*=F_4$. Observe that $F_0^*F_1^*F_2^* = F_0F_1F_2 = 2^8-1$. So $\prod_{r=0}^{n-1} F_r^* \equiv -1 \pmod{2^7}$ if $n>2$.

Assume $k\geq 2$. Then $p\equiv 1 \pmod{2^{k+2}}$ since $p\mid F_k$. Note that $n>k\geq 2$ and $a\geq 2^k\geq k+2$. Therefore

$$w'2^b = W - w'2^a - p^\alpha \equiv -1-0-1 = -2 \pmod{2^4},$$

hence $b=1$ and $w'\equiv -1 \pmod 8$, which contradicts (2.2).

By the above $k\in\{0,1\}$. If $b\geq 3$, then $2^n > a \geq 4$ and hence $n>2$, therefore

$$p^\alpha = W - w'(2^a+2^b) \equiv -1 \pmod 8,$$

which is impossible since $p\in\{F_0,F_1\}=\{3,5\}$. So b must be 1 or 2. In the case $k=1$, we have $p=5$ and

$$w'2^b = W - w'2^a - 5^\alpha \equiv 3-0-1 = 2 \pmod 4,$$

so $b=1$ and $a\equiv b+2\equiv 3 \pmod 4$. ∎

Remark 2. In the proof of Proposition 1, we first use congruences modulo Fermat numbers, then use congruences modulo powers of 2. This strategy enables us to bound p and b in (2.3).

Now we go further to determine possible values of a in the case $w'\in\{1,F_0,F_1,F_2,\ldots\}$.

Proposition 2. *Let $\alpha\in\mathbb{N}$ and $c\in\{1,F_0,F_1,F_2,\ldots\}$. Let n,w be positive integers with*

$$W = w\prod_{r=0}^{n-1} F_r^* \leq 2^{2^n}-1. \tag{2.4}$$

(i) *If $a,b\in\mathbb{N}$, $a>b$, $a\not\equiv b \pmod 2$, $b\in\{1,2\}$,*

$$w\equiv 1 \pmod{16} \quad \text{and} \quad W = c(2^a+2^b)+3^\alpha, \tag{2.5}$$

then $a=b+1$ and $c=1$.

(ii) *If $a\in\mathbb{N}$, $a\equiv 3 \pmod 4$,*

$$w\equiv 1 \pmod{2^7} \quad \text{and} \quad W = c(2^a+2)+5^\alpha, \tag{2.6}$$

then $a\in\{3,7\}$ and $c\in\{1,5\}$.

Proof. If $c = F_m \le W$, then $m < n$ since $W < F_n$, thus F_m^* divides both c and W.

(i) By (2.5) and the above, if $c > 1$ then $3 \mid c$ and hence $c = F_0 = 3$.

Suppose that $a \ge 4$. Then $n > 2$ and

$$2^b c + 3^\alpha = W - 2^a c \equiv -1 - 0 = -1 \pmod{2^4}.$$

Clearly powers of 3 can only be congruent to $1, 3, -7, -5$ modulo 16. If $c = 1$, then we must have $b = 2$ and $3^\alpha \equiv -5 \equiv 3^3 \pmod{16}$, hence $\alpha \equiv 3 \pmod 4$ and

$$2^a = W - 3^\alpha - 2^2 \equiv 0 - 3^3 - 4 \equiv -1 \pmod 5,$$

which contradicts $a \not\equiv b \pmod 2$. If $c = 3$, then $3 \cdot 2^b + 3^\alpha \equiv -1 \equiv 15 \pmod{16}$ and hence $3^{\alpha-1} \equiv 5 - 2^b \pmod{16}$; it follows that $\alpha \equiv 3b - 1 \pmod 4$, thus $3(2^a + 2^b) = W - 3^\alpha \equiv 0 - 3^{3b-1} \pmod 5$, which is impossible since $b \in \{1, 2\}$.

In view of the above, $a \le 3$ and thus $a - b = 1$. Observe that $3(2^a + 2^b) = 9 \cdot 2^b = 2^{b+3} + 2^b$. So $c \ne 3$ and hence $c = 1$.

(ii) If $c > 1$, then $5 \mid c$ and hence $c = 5 = F_1$.

Assume that $a \ne 3, 7$. Then $2^n > a \ge 8$ and so $n > 3$. Observe that

$$5^\alpha = W - c(2^a + 2) \equiv -1 - 2c \pmod{2^7}$$

and 5 has order 2^5 modulo 2^7. It is easy to verify that

$$5^3 \equiv -3 \pmod{2^7} \quad \text{and} \quad 5^{21} \equiv -11 \pmod{2^7}.$$

So $\alpha = 32\beta + c'$ for some $\beta \in \mathbb{N}$ where $c' = 3, 21$ according as $c = 1, 5$. Note that $257 = F_3 = F_3^*$ divides W and $5^{32} \equiv -4 \pmod{257}$. So we have

$$16^{(a+1)/4} + 4 = 2(2^a + 2) = \frac{2}{c}(W - 5^\alpha) \equiv -\frac{2}{c} \cdot 5^{c'}(-4)^\beta \pmod{257},$$

where $-\frac{2}{c}5^{c'} \equiv 7, -92 \pmod{257}$ according as $c = 1, 5$. This is actually impossible since powers of 16 can only be congruent to $\pm 1, \pm 16$ modulo 257. ∎

Remark 3. In the proof of Proposition 2, we first use congruences modulo powers of 2, then use congruences modulo Fermat numbers. This variation allows us to bound a successfully.

3. Some exponential diophantine equations. For $a, m \in \mathbb{N}$ clearly $F_m(2^a + 2^a) = 2^{\bar a} + 2^{\bar b}$ where $\bar a = 2^m + a + 1 > \bar b = a + 1$. Thus, with the help of Propositions 1 and 2, we have reduced Theorems 1 and 2 to the following

Proposition 3. *For the exponential diophantine equations*

(3.1) $\quad 2^{2^n} - 1 = 2^2 + 2 + 3^\alpha \qquad$ *with* $n, \alpha \in \mathbb{Z}^+$;

(3.2) $\quad 2^{2^n} - 1 = 2^3 + 2^2 + 3^\alpha \qquad$ *with* $n, \alpha \in \mathbb{Z}^+$;

(3.3) $2^{2^n}-1=c(2^3+2)+5^\alpha$ *with* $n,\alpha\in\mathbb{Z}^+$ *and* $c\in\{1,5\}$;

(3.4) $2^{2^n}-1=c(2^7+2)+5^\alpha$ *with* $n,\alpha\in\mathbb{Z}^+$ *and* $c\in\{1,5\}$,

the only solutions are

$$(n,\alpha)=(2,2);\ (2,1),(3,5);\ (2,1);\ (3,3)$$

respectively.

Proof. (3.1) modulo 8 yields $2\,|\,\alpha$. It is known (see, e.g., [J]) that the Ramanujan–Nagell equation

(3.5) $$x^2+7=2^y \quad \text{with } x,y\in\mathbb{Z}^+$$

only has solutions

$$(x,y)=(1,3),\ (3,4),\ (5,5),\ (11,7),\ (181,15).$$

Thus the only solution of (3.1) is $n=\alpha=2$.

By S. Uchiyama [U] the equation

(3.6) $$3^x+13^y=2^z \quad \text{with } x,y,z\in\mathbb{Z}^+$$

only has solutions $(x,y,z)=(1,1,4),(5,1,8)$. So the only solutions of (3.2) are $(n,\alpha)=(2,1),(3,5)$.

By Theorem 6 of R. Scott [Sc], if k,l are integers with $1<k<l$, $\gcd(k,l)=1$ and $(k,l)\neq(3,5),(3,13)$ then the diophantine equation

$$k^x+l^y=2^z \quad \text{with } x,y,z\in\mathbb{Z}^+$$

has at most one solution. We will use this fact below.

In the light of Scott's result, the equation

(3.7) $$5^x+11^y=2^z \quad \text{with } x,y,z\in\mathbb{Z}^+$$

only has the solution $(x,y,z)=(1,1,4)$. So the only solution of (3.3) with $c=1$ is $(n,\alpha)=(2,1)$. If $c=5$ and (3.3) holds, then

(3.8) $$5^\alpha+51=2^z \quad \text{where } z=2^n,$$

hence $5^\alpha+20\equiv 2^z \pmod{31}$, which is impossible since $5^3\equiv 2^5\equiv 1\pmod{31}$.

By Scott's result the equation

(3.9) $$5^x+131^y=2^z \quad \text{with } x,y,z\in\mathbb{Z}^+$$

only has the solution $(x,y,z)=(3,1,8)$. Thus the only solution of (3.4) with $c=1$ is $n=\alpha=3$. If $c=5$ and (3.4) holds, then

(3.10) $$5^\alpha+651=2^z \quad \text{where } z=2^n,$$

thus $5^\alpha+3\equiv 0\pmod 8$ and hence $2\nmid\alpha$, as $7\,|\,651$ we have $2^z\equiv 5^\alpha\equiv(-2)^\alpha=-2^\alpha\pmod 7$, which is absurd. ∎

Proof of Corollary 1. Let $n \geq 3$ be an integer. Since $2^{2^n} - 5$ is odd, it cannot be written as the sum of two odd prime powers. Suppose that $2^{2^n} - 5 = 2^a + p^\alpha$ for some $a, \alpha \in \mathbb{N}$ and $p \in \mathbb{P}$ with $(n, a, p, \alpha) \neq (3, 3, 3, 5)$. Then

$$2^{2^n} - 1 = 2^a + 2^2 + p^\alpha,$$

and hence $a = 2$ by Theorem 1. So

$$p^\alpha = 2^{2^n} - 1 - 2 \cdot 2^2 = (2^{2^n} + 3)(2^{2^n} - 3).$$

Thus $\alpha \neq 0$, $2 \nmid p$, and p divides $2^{2^n} + 3 - (2^{2^n} - 3) = 6$. Therefore $p = 3$, which contradicts $2^{2^n} \not\equiv 0 \pmod 3$. ∎

4. Several open problems. Does the set of positive odd integers not of the form $2^a + 2^b + p^\alpha$ (where $a, b, \alpha \in \mathbb{N}$, $a \neq b$ and $p \in \mathbb{P}$) have a positive lower asymptotic density? This question is open and seems hard.

We close the paper with two conjectures posed by the first author.

CONJECTURE 1. *There are infinitely many odd integers not of the form* $\pm 2^a \pm 2^b \pm p^\alpha$ *where* $a, b, \alpha \in \mathbb{N}$, $p \in \mathbb{P}$ *and any choice of signs can be made.*

CONJECTURE 2. *Question* 2 *in Section* 1 *always has an affirmative answer.*

Acknowledgments. The authors are indebted to the referee for his/her helpful suggestions.

References

[A] W. S. Anglin, *The Queen of Mathematics—An Introduction to Number Theory*, Kluwer, Dordrecht, 1995, 212–213.

[CS] F. Cohen and J. L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comp. 29 (1975), 79–81.

[Co] J. G. van der Corput, *On de Polignac's conjecture*, Simon Stevin 27 (1950), 99–105.

[Cr1] R. Crocker, *A theorem concerning prime numbers*, Math. Mag. 34 (1960/61), 316, 344.

[Cr2] —, *On a sum of a prime and two powers of two*, Pacific J. Math. 36 (1971), 103–107.

[E] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. 2 (1950), 113–123.

[J] W. Johnson, *The diophantine equation* $X^2 + 7 = 2^n$, Amer. Math. Monthly 94 (1987), 59–62.

[Sc] R. Scott, *On the equations* $p^x - b^y = c$ *and* $a^x + b^y = c^z$, J. Number Theory 44 (1993), 153–165.

[Si] W. Sierpiński, *Elementary Theory of Numbers*, PWN-Polish Sci. Publ., Warszawa, and North-Holland, Amsterdam, 1987, 445–448.

[Su] Z. W. Sun, *On integers not of the form* $\pm p^a \pm q^b$, Proc. Amer. Math. Soc. 128 (2000), 997–1002.

[U] S. Uchiyama, *On the diophantine equation* $2^x = 3^y + 13^z$, Math. J. Okayama Univ. 19 (1976/1977), 31–38.

Department of Mathematics
Nanjing University
Nanjing 210093
The People's Republic of China
E-mail: zwsun@nju.edu.cn

Department of Mathematics
Zhanjiang Normal College
Zhanjiang 524048
The People's Republic of China

Received on 26.7.2000
and in revised form on 3.11.2000 (3857)