ACTA ARITHMETICA
135.1 (2008)

# Fermat numbers and integers of the form $a^k + a^l + p^\alpha$

by

Yong-Gao Chen (Nanjing), Rui Feng (Nanjing)
and Nicolas Templier (Montpellier)

**1. Introduction.** In 1849, A. de Polignac [20] conjectured that every odd number larger than 3 can be written as the sum of an odd prime and a power of 2. He found a counterexample 959 soon. In 1934, N. P. Romanoff [22] proved that the set of positive odd integers which can be expressed in the form $2^n + p$ has positive lower asymptotic density, where $n$ is a nonnegative integer and $p$ a prime. In 1950, J. G. van der Corput [11] proved that the counterexamples to de Polignac's conjecture form a set of positive lower density. Using a covering system, P. Erdős [15] proved that there is an infinite arithmetic progression of positive odd integers each of which has no representation of the form $2^n + p$. Recall that $\{a_i \pmod{m_i}\}_{i=1}^k$ is called a *covering system* if every integer is congruent to $a_i \pmod{m_i}$ for at least one value of $i$. For further related results see Chen [3–8], Guy [16], Cohen and Selfridge [10].

Refining the argument of Erdős, R. Crocker [12] proved that there are infinitely many positive odd integers not representable as the sum of a prime and two positive powers of two. P. Z. Yuan [25] proved that there are infinitely many positive odd integers not representable as the sum of a prime power and two positive powers of two. Before this Z. W. Sun and M. H. Le [23] handled the integers of the form $c(2^a + 2^b) + p^\alpha$ for many values of the constant $c$. Another natural problem arises if one replaces the powers of two by powers of other integers. This is what we discuss in this article.

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

*Key words and phrases*: Fermat numbers, generalized Fermat numbers, Erdős problems, Zsigmondy's theorem, covering systems.

Research of Y. G. Chen supported by the National Natural Science Foundation of China, Grant No 10771103 and 10471064.

This work was partially completed when the third author studied at École Normale Supérieure.

All these articles are closely connected to Fermat numbers $F_n = 2^{2^n} + 1$. Currently $F_0, F_1, F_2, F_3, F_4$ are the only known Fermat primes. We do not know whether there are infinitely many Fermat primes and whether there are infinitely many Fermat composite numbers. On the other hand, we cannot exhibit an odd number of reasonable size which cannot be represented as the sum of a prime power and two powers of two (with nonnegative exponents). For example we have checked there are no such numbers between 3 and $10^7$. One of our results implies that if the number of odd numbers less than $x$ which cannot be represented as the sum of a prime power and two powers of two is $o(\sqrt{x})$, then there are infinitely many Fermat primes (Theorem 3′). If the number of odd numbers less than $x$ which cannot be represented as the sum of a prime power and two powers of two is $O(x^{1/4})$, then all sufficiently large Fermat numbers are primes (Theorem 3). So it is of interest to estimate the number of odd numbers less than $x$ which cannot be represented as the sum of a prime power and positive powers of two. Erdős (see Guy [16, A19]) suggested that there may be $cx$ of them less than $x$, but can $> x^{\varepsilon}$ be proved? For related results on Fermat numbers, one may refer to [16, A3] and [2, 13, 14, 24].

For any integer $a \geq 2$ let $\mathcal{N}_a$ be the set of all positive integers $M$ with $(M, a) = 1$ and $(M-2, a-1) = 1$ such that $M$ cannot be written as the sum of a prime power and two powers of $a$. The following theorems are proved.

Theorem 1. *Let $a$ be an odd positive integer which is not a power of 2 minus 1. Then $|\mathcal{N}_a \cap [1, x]| \geq c_1 \log x$ and the set $\mathcal{N}_a \cap [1, x]$ contains an arithmetic progression of length $c_2 \log x/(\log\log x)^3$, where $c_1, c_2$ are two computable positive constants depending only on $a$.*

Theorem 2. *If $a$ is an even positive integer and there exists an integer $m \geq 10$ such that $a^{2^m} + 1$ is composite, then $|\mathcal{N}_a \cap [1,\, x]| \geq c \log\log x$ for all sufficiently large $x$, where $c$ is a computable positive constant depending only on $a$ (and $m$).*

Theorem 3. *Let $a$ be an even positive integer. If $|\mathcal{N}_a \cap [1, x]| = O(x^{1/4})$, then for every sufficiently large integer $m$, the integer $a^{2^m} + 1$ is a prime.*

Theorem 4. *Let $a$ be an odd positive integer which is not a power of 2 minus 1. If $|\mathcal{N}_a \cap [1, x]| = O(x^{1/4} \log x)$, then for every sufficiently large integer $m$, the integer $\frac{1}{2}(a^{2^m} + 1)$ is a prime.*

Theorem 3′. *Let $a$ be an even positive integer. If $|\mathcal{N}_a \cap [1, x]| = o(\sqrt{x})$, then there are infinitely many positive integers $m$ such that $a^{2^m} + 1$ are prime.*

Theorem 4′. *Let $a$ be an odd positive integer which is not a power of 2 minus 1. If $|\mathcal{N}_a \cap [1, x]| = o(\sqrt{x \log x})$, then there are infinitely many positive integers $m$ such that $\frac{1}{2}(a^{2^m} + 1)$ are prime.*

Remark 1. We demand $(M, a) = 1$ because many odd numbers $M$ with $(M, a) \neq 1$ are not of the form $M = a^k + a^l + p^\alpha$ $(k, l > 0)$ for trivial reasons: $p$ would then divide $a$, and the set of integers $a^k + a^l + p^\alpha$ with $p \mid a$ has asymptotic density 0. For a similar reason we demand $(M - 2, a - 1) = 1$ because else $M = a^k + a^l + p^\alpha$ would imply $p \mid a - 1$. Except these two, there are no other trivial observations.

One might look for a stronger theorem by requiring $M$ to lie in an arbitrary arithmetic progression. If one tries to solve this question with the same methods, one can see that it is closely related to a conjecture of Erdős: there are covering systems with distinct and arbitrary large moduli.

Question 1. *Given an integer* $a \geq 2$ *and an arithmetic progression*, *are there integers* $M$ *in the progression with* $(M, a) = 1$ *and* $(M - 2, a - 1) = 1$ *such that* $M$ *cannot be written as the sum of a prime power and two powers of* $a$*?*

Remark 2. In the previous articles, the theorems and proofs were stated with positive exponents, and it was implicit that one could improve them to nonnegative exponents.

Remark 3. The only known method to prove upper bounds is by sieving. Romanoff's method applies to $a > 2$ without major change and gives $|\mathcal{N}_a \cap [1, x]| \leq cx$ for some effectively computable constant $c$ (see [22, 15, 17, 9, 18]). An improvement to $|\mathcal{N}_2 \cap [1, x]| \leq cx$, where $c$ is a constant less than $1/4$, would be already deep since it would imply Linnik's approximation to Goldbach problem with four powers of two (see [18, Prop. 1]), while currently it is solved unconditionally (resp. under GRH) with eight powers (resp. seven powers) in [19].

Remark 4. One can think that the larger $a$ is, the fewer integers of the form $a^k + a^l + p^\alpha$ there will be. Still, one cannot deduce the theorem from the apparently harder case $a = 2$. Moreover, all the examples constructed so far involve arithmetic properties of the numbers $a^n - 1$, which quite vary with $a$. In particular, when $a$ is a power of 2 minus 1 these congruence methods might fail. We are not convinced at all that Theorem 1 will hold in this case, and we ask the following question.

Question 2. *Is it possible to write any odd integer greater than* 10 *and prime to* 3 *as the sum of two powers of* 3 *and a prime power?*

Remark 5. On the other hand, the condition that $a^{2^m} + 1$ is composite for some $m \geq 10$ seems superfluous, and although we do not know how yet, we believe it should be possible to remove it by a refinement of the method.

## 2. Proofs.

First of all, we construct a suitable covering system. All the moduli are distinct and no power of two appears as a modulus. Let us recall that a conjecture of Erdős states that we cannot find a covering system with all moduli odd, distinct and greater than one.

Lemma 1.

$$\begin{array}{lll}
0 \pmod{3}, & 1 \pmod{2\cdot 3}, & 4 \pmod{2^2\cdot 3}, \\
1 \pmod{7}, & 0 \pmod{2\cdot 7}, & 13 \pmod{3\cdot 7}, \\
22 \pmod{2^3\cdot 3}, & 2 \pmod{2^2\cdot 7}, & 18 \pmod{2^3\cdot 7}, \\
40 \pmod{2\cdot 3\cdot 7}, & 10 \pmod{2^2\cdot 3\cdot 7}, & 2 \pmod{3^2}, \\
5 \pmod{2\cdot 3^2}, & 0 \pmod{5}, & 8 \pmod{2\cdot 5}, \\
11 \pmod{3\cdot 5}, & 44 \pmod{3^2\cdot 5}, & 2 \pmod{2\cdot 3\cdot 5}, \\
53 \pmod{2\cdot 3^2\cdot 5}, & 14 \pmod{2^2\cdot 3\cdot 5}, & 4 \pmod{2^2\cdot 5}, \\
17 \pmod{2^2\cdot 3^2\cdot 5}, & 35 \pmod{2^2\cdot 3^2} &
\end{array}$$

*is a covering system. We label it by* $\{a_i \pmod{m_i}\}_{i=1}^{23}$.

Remark. We can compare this covering system with the one used in [12, 25] (see below). We allow the use of $6 = m_2$ as modulus because the second exception in Zsigmondy's theorem below does not occur since $a$ is not 2.

We omit the proof of Lemma 1 which is a direct check once the system is given.

Lemma 2. *Let $m$ be a positive integer. There exists a polynomial $P_m(x)$ of degree $m$ whose coefficients depend only on $m$ such that for any fixed $m$ integers $a_1, \ldots, a_m \geq 2$, and any arithmetic progression of length $L$, the number of integers in the arithmetic progression which are of the form*

$$a_1^{\alpha_1} + \cdots + a_m^{\alpha_m},$$

*where $\alpha_1, \ldots, \alpha_m$ are nonnegative integers, is less than $P_m(\log L)$.*

*Proof.* We shall proceed by induction on $m$.

The case $m = 1$ is trivial. Assume that the conclusion holds for $m$. Given an arithmetic progression of length $L$ with common difference $R$ and initial term $A$, let us count the integers of the form $x = a_1^{\alpha_1} + \cdots + a_{m+1}^{\alpha_{m+1}}$ in the progression.

We may assume that $a_{m+1}^{\alpha_{m+1}}$ is the largest among the $a_i^{\alpha_i}$, by multiplying the bound by $m+1$. There is at most one integer $0 \leq x < R$ in the progression, so we may assume $A \geq R$, by adding 1 to the bound. Now, we have $A/(m+1) < a_{m+1}^{\alpha_{m+1}} \leq A + (L-1)R$, so that $\alpha_{m+1}$ lies in a set of cardinality at most $2\log((m+1)(1+(L-1)R/A))+1$, which is smaller than $2\log(m+1) + 2\log L + 1$. By multiplying the bound by this factor, we may assume that $a_{m+1}^{\alpha_{m+1}}$ is fixed. So $x - a_{m+1}^{\alpha_{m+1}}$ lies in an arithmetic progression of length less than $L$ and is of the form $a_1^{\alpha_1}+\cdots+a_m^{\alpha_m}$. We apply the induction hypothesis, which concludes the proof of Lemma 2.

Remark. The key issue in this lemma is that the upper bound $P_m(\log L)$ does not depend on the common difference $R$ of the progression.

Example 1. We can take $P_3(x)=48x^3+216x^2+318x+157$.

Let us recall the main fact concerning the arithmetic property of the sequence $a^n-1$.

Definition. A prime factor $p$ of $a^n-1$ is called *primitive* if $p \nmid a^j-1$ for all $0<j<n$.

Zsigmondy's Theorem (see [1, 21] for a proof). *Let $a$ and $n$ be integers greater than* 1. *Then there exists a primitive prime factor of $a^n-1$, except exactly in the following cases*: (i) $n=2$, $a=2^\beta-1$, *where* $\beta\ge 2$; (ii) $n=6$, $a=2$.

We fix for each $p_i$ a primitive prime factor of $a^{m_i}-1$ for each $1\le i\le 23$, where $\{a_i \pmod{m_i}\}_{i=1}^{23}$ is the covering system from Lemma 1. This is possible by Zsigmondy's theorem when $a>2$. Because the $m_i$ are all distinct, the $p_i$ are all distinct. When $a=2$ we replace the covering system by the one in [12], that is,

$$\begin{array}{llll}
0 \pmod{3}, & 0 \pmod{5}, & 1 \pmod{9}, & 1 \pmod{10}, \\
8 \pmod{12}, & 8 \pmod{15}, & 4 \pmod{18}, & 7 \pmod{20}, \\
5 \pmod{24}, & 29 \pmod{30}, & 2 \pmod{36}, & 14 \pmod{36}, \\
17 \pmod{40}, & 34 \pmod{45}, & 43 \pmod{45}, & 13 \pmod{48}, \\
37 \pmod{48}, & 16 \pmod{60}, & 19 \pmod{60}, & 26 \pmod{72}, \\
62 \pmod{72}, & 52 \pmod{90}, & 37 \pmod{120}, & 49 \pmod{144}, \\
121 \pmod{144}, & 103 \pmod{180}, & 106 \pmod{180}, & 229 \pmod{360}.
\end{array}$$

Similarly, we fix $p_i$ for each distinct modulus $m_i$. For nondistinct $m_i$, we take primes 37 and 109 for modulus 36; 631 and 23311 for modulus 45; 97 and 673 for modulus 48; 61 and 1321 for modulus 60; 433 and 38737 for modulus 72; 577 and 487824887233 for modulus 144; 29247661 and 54001 for modulus 180. Thus the $p_i$ are also all distinct. Let $T_2=28$ and $T_a=23$ $(a>2)$.

*Proofs of Theorems 1 and 2.* When $a$ is odd, let

$$\gamma_k=\frac{1}{2}\,(a^{2^k}+1),\quad k\ge 1,$$

and let $\gamma_0$ be an odd prime factor of $a+1$, which exists by assumption. When $a$ is even, let

$$\gamma_k=a^{2^k}+1,\qquad k\ne m,$$

and let $\gamma_m$ be the least odd prime factor of $a^{2^m}+1$.

The $p_i$ and the $\gamma_k$ are coprime because there is no power of 2 in the moduli $m_i$ of the covering system. It is clear that $p_i \nmid 2a(a-1)$, $(\gamma_k, 2a(a-1)) = 1$ and $(\gamma_k, \gamma_l) = 1$ for all $k \neq l$.

For each $n \geq 1$, we consider positive integers $M_n$ that satisfy the following congruences:

(1) $M_n \equiv 0 \pmod{\gamma_k}$ for $0 \leq k \leq n-1$;
(2) $M_n \equiv 2 \cdot a^{a_i} \pmod{p_i}$ for $1 \leq i \leq T_a$;
(3) $M_n \equiv 1 \pmod{2a(a-1)}$ if $a$ is odd;
(4) $M_n \equiv b \pmod 8$, where $b \in \{3, 7\}$, $b \not\equiv 1 + a \pmod 8$ if $a$ is even;
(5) $M_n \equiv 1 \pmod{a'(a-1)}$, where $a'$ is the odd part of $a$, if $a$ is even.

By (3–5) we have $(M_n, a) = 1$ and $(M_n - 2, a - 1) = 1$. Suppose that $M_n < a^{2^n}$ and $M_n = a^k + a^l + p^\alpha$, where $k,\ l,\ \alpha$ are nonnegative integers and $p$ is a prime.

Case 1: $M_n = 2 \cdot a^l + p^\alpha$ for some nonnegative integers $l, \alpha$ and a prime $p$. By Lemma 1 there exists an integer $i$ with $l \equiv a_i \pmod{m_i}$. By (2) we have $M_n - 2 \cdot a^l \equiv 2 \cdot a^{a_i} - 2 \cdot a^l \equiv 0 \pmod{p_i}$. Hence

$$p = p_i, \quad \alpha > 0.$$

Case 2: $M_n = a^k + a^l + p^\alpha$, where $k,\ l,\ \alpha$ are nonnegative integers with $k \neq l$ and $p$ is a prime. We want to prove $p = \gamma_0,\ \gamma_1$. We may assume that $k > l$. Let $r \geq 0$ be the integer with

$$2^r \parallel k - l.$$

This implies that

$$\gamma_r \mid a^k + a^l.$$

Because $M_n < a^{2^n}$, we have $r \leq n-1$. Hence (1) implies

$$\gamma_r \mid M_n.$$

Thus $\gamma_r \mid p^\alpha$, that is,

$$\gamma_r = p^\beta, \qquad \beta, \alpha > 0.$$

Now we claim that

$$p \equiv 1 \pmod{2^{r+1}}.$$

In fact, since $a^{2^r} \equiv -1 \pmod p$, the order of $a \pmod p$ is exactly $2^{r+1}$, so that the claim is a consequence of Fermat's little theorem. Now if $r \geq 2$, then $k \equiv l \pmod 4$. If $2 \nmid a$, then $a^k + a^l \equiv 2 \pmod 4$ and $M_n = a^k + a^l + p^\alpha \equiv 3 \pmod 4$, which contradicts (3). If $2 \mid a$, then $a^k + a^l \equiv 0, 1, a, a^2 \pmod 8$ and $M_n = a^k + a^l + p^\alpha \equiv 1, 2, a+1, a^2+1 \pmod 8$, which contradicts (4). Therefore we must have $r = 0, 1$.

Combining Cases 1 and 2 shows that if $M_n < a^{2^n}$ and $M_n \in \mathcal{N}_a$, then

(6) $$M_n \in \{a^k + a^l + \gamma_0^\alpha, a^k + a^l + \gamma_1^\alpha\} \cup \{2a^k + p_i^\alpha \mid i = 1, 2, \ldots, T_a\}.$$

Case I: Assume that $a$ is odd. By the Chinese Remainder Theorem, conditions (1–3) are equivalent to a single congruence modulo some integer $R$. Because the dependence on $n$ appears only in condition (1), we have

$$R \ll \prod_{j=0}^{n-1} \gamma_j \ll \prod_{j=0}^{n-1} \frac{a^{2^j}+1}{2} \ll 2^{-n}(a^{2^n}-1).$$

Here and in the following the implied constants depend only on $a$. The integers $M_n$ with $0 < M_n < a^{2^n}$ form an arithmetic progression $\mathcal{T}$ of length $\gg 2^n$. By (6) and Lemma 2 the number of integers in $\mathcal{T}$ which are of the form $a^k + a^l + p^\alpha$, where $k,\ l,\ \alpha$ are nonnegative integers and $p$ is a prime, is less than $25P_3(\log|\mathcal{T}|)$.

For every sufficiently large $x$, let $n$ be the integer with

$$a^{2^n} \le x < a^{2^{n+1}}.$$

Then $|\mathcal{T}| \gg 2^n \gg \log x$ and the number of integers in $\mathcal{T} \cap \mathcal{N}_a$ is more than

$$|\mathcal{T}| - 25P_3(\log|\mathcal{T}|) \gg \log x.$$

Moreover, it is clear that—up to a multiplicative constant—there are more than

$$\frac{|\mathcal{T}|}{25P_3(\log|\mathcal{T}|)} \gg \frac{\log x}{(\log\log x)^3}$$

consecutive terms in $\mathcal{T}$ that belong to $\mathcal{N}_a$. This completes the proof of Theorem 1.

Remark. The use of Lemma 2 avoids the introduction of additional congruences. An explicit (but more involved) construction of an infinite set of integers in $\mathcal{N}_a$ is found in Chapter 3.2 of Rui Feng's master thesis.

Case II: Assume that $a$ is even. We assume that $a > 2$ (when $a = 2$, Theorem 2 is a consequence of [25, Lemma 2.4]; a slight modification of the argument given below would also work). By the Chinese Remainder Theorem, conditions (1, 2, 4, 5) are equivalent to a single congruence modulo

$$R = 8a'(a-1)\prod_{i=1}^{23} p_i \cdot \prod_{j=0}^{n-1} \gamma_j.$$

Since each $p_i$ is a primitive prime factor of $a^{m_i} - 1$ and each $m_i$ divides one of $2^3 \cdot 3 \cdot 7$ and $2^2 \cdot 3^2 \cdot 5$, we have

$$\prod_{i=1}^{23} p_i \le (a^{2^3\cdot 3\cdot 7} - 1)(a^{2^2\cdot 3^2\cdot 5} - 1) \le a^{2^3\cdot 3\cdot 7 + 2^2\cdot 3^2\cdot 5} = a^{348}.$$

Since $m \ge 10$ and $a^{2^m}+1$ is composite, we have $(a^{2^m}+1)/\gamma_m > a^{2^9}$. Hence, for $n \geq m+1$ we have

$$\prod_{j=0}^{n-1} \gamma_j < a^{-2^9} \prod_{j=0}^{n-1} (a^{2^j}+1) = a^{-2^9}\, \frac{a^{2^n}-1}{a-1}.$$

Thus

$$R < a^{-161}(a^{2^n}-1).$$

The integers $M_n$ with $0 < M_n < a^{2^n}$ form an arithmetic progression $\mathcal{T}$ of length at least $a^{161}$. We choose an arithmetic progression $\mathcal{T}_1$ by taking $2^{25}$ consecutive terms in $\mathcal{T}$. By (6) and Example 1 the number of integers in $\mathcal{T}_1$ which are of the form $a^k+a^l+p^\alpha$, where $k$, $l$, $\alpha$ are nonnegative integers and $p$ is a prime, is less than

$$25(48 \cdot 20^3 + 216 \cdot 20^2 + 318 \cdot 20 + 157) < 2^{25}.$$

So there exist integers $M_n$ in $\mathcal{T}_1 \cap \mathcal{N}_a$. For each $n > m$ we have $M_n < a^{2^n} < a^{2^n}+1 = \gamma_n < M_{n+1}$. For every sufficiently large $x$, let $n$ be the integer with

$$a^{2^n} \leq x < a^{2^{n+1}}.$$

Then $M_n \leq x$ and

$$|\mathcal{N}_a \cap [1,x]| \geq n-m \gg \log\log x.$$

Similarly we have

$$|\mathcal{N}_2 \cap [1,x]| \geq n-m \gg \log\log x.$$

This completes the proof of Theorem 2.

*Proofs of Theorems 3 and 4.* For each integer $k \geq 1$, we let $\gamma_k$ be the least odd prime factor of $a^{2^k}+1$. Existence of such factors can be deduced from the fact that $a^{2^k}+1 \not\equiv 0,4 \pmod 8$. Recall that $a$ is different from $2^\beta-1$ by assumption, so that we may choose an odd prime factor $\gamma_0 \mid a+1$. As before, the primes $p_i$ and $\gamma_k$ are distinct. It is also clear that $p_i \nmid 2a(a-1)$ and $\gamma_k \nmid 2a(a-1)$.

Now we follow the proofs of Theorems 1 and 2.

By the Chinese Remainder Theorem conditions (1–5) are equivalent to a single congruence modulo some integer $R_n$. Because the dependence on $n$ appears only in condition (1), we have

$$R_n \asymp \prod_{j=0}^{n-1} \gamma_j. \tag{7}$$

Case 1: Assume that $a$ is even and $a^{2^k}+1$ is composite for infinitely many $k$. Now we choose two integers $n > m+1$, with $m$ arbitrarily large, such that $a^{2^m}+1$ and $a^{2^{n-1}}+1$ are both composite. Then

$$R_n \ll a^{-2^{m-1}} \cdot a^{-2^{n-2}} \cdot \prod_{j=0}^{n-1} (a^{2^j}+1) \ll a^{-2^{m-1}} x_n^{3/4},$$

where $x_n = a^{2^n}-1$. The integers $M_n$ with $0 < M_n \le x_n$ form an arithmetic progression $\mathcal{T}$ of length $\gg a^{2^{m-1}} x_n^{1/4}$. By Lemma 2 the number of integers in $\mathcal{T} \cap \mathcal{N}_a$ is more than

$$|\mathcal{T}| - 30P_3(\log|\mathcal{T}|) \gg a^{2^{m-1}} x_n^{1/4}.$$

This contradicts $|\mathcal{N}_a \cap [1,x]| = O(x^{1/4})$ for large $x$, and completes the proof of Theorem 3.

Case 2: Assume that $a$ is odd and $(a^{2^k}+1)/2$ is composite for infinitely many $k$. As before choose $n > m+1$ such that $(a^{2^m}+1)/2$ and $(a^{2^{n-1}}+1)/2$ are both composite. Similarly we find that the integers $M_n$ with $0 < M_n \le x_n = a^{2^n}-1$ form an arithmetic progression $\mathcal{T}$ of length

$$\gg a^{2^{m-1}} 2^n x_n^{1/4} \gg a^{2^{m-1}} x_n^{1/4} \log x_n.$$

By Lemma 2 the number of integers in $\mathcal{T} \cap \mathcal{N}_a$ is more than

$$|\mathcal{T}| - 25P_3(\log|\mathcal{T}|) \gg a^{2^{m-1}} x_n^{1/4} \log x_n.$$

This contradicts $|\mathcal{N}_a \cap [1,x]| = O(x^{1/4}\log x)$ for large $x$, and completes the proof of Theorem 4.

*Proof of Theorem 3′.* We follow the proof of Theorem 3. Suppose that $a^{2^m}+1$ are composite for all integers $m \ge K$. Then

$$\gamma_m \le a^{-2^{m-1}}(a^{2^m}+1),$$

and by (7) we have

$$R_n \ll \prod_{m=K}^{n-1} a^{-2^{m-1}} \cdot \prod_{m=0}^{n-1} (a^{2^j}+1) \ll a^{2^{n-1}}.$$

The integers $M_n$ with $0 < M_n \le a^{2^n}-1$ form an arithmetic progression $\mathcal{T}$ of length $\gg a^{2^{n-1}}$. By Lemma 2 the number of integers in $\mathcal{T} \cap \mathcal{N}_a$ is more than

$$|\mathcal{T}| - 30P_3(\log|\mathcal{T}|) \gg a^{2^{n-1}},$$

which contradicts $|\mathcal{N}_a \cap [1,x]| = o(\sqrt{x})$. This completes the proof of Theorem 3′.

*Proof of Theorem 4′.* We follow the proof of Theorem 4. Suppose that $\frac{1}{2}(a^{2^m}+1)$ is composite for all integers $m \ge K$. Then

$$\gamma_m \le 2^{-1/2} a^{-2^{m-1}} (a^{2^m}+1). \tag{8}$$

By (7) and (8) we have

$$R_n \ll 2^{-n/2} \prod_{m=K}^{n-1} a^{-2^{m-1}} \cdot \prod_{m=0}^{n-1} (a^{2^j} + 1) \ll 2^{-n/2} a^{2^{n-1}}.$$

The integers $M_n$ with $0 < M_n \le a^{2^n} - 1$ form an arithmetic progression $\mathcal{T}$ of length $\gg 2^{n/2} a^{2^{n-1}}$. By Lemma 2 the number of integers in $\mathcal{T} \cap \mathcal{N}_a$ is more than

$$|\mathcal{T}| - 25P_3(\log |\mathcal{T}|) \gg 2^{n/2}\sqrt{a^{2^n} - 1},$$

which is in contradiction with $|\mathcal{N}_a \cap [1, x]| = o(\sqrt{x \log x})$. This completes the proof of Theorem 4′.

## References

[1] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. 5 (1904), 173–180.

[2] A. Björn and H. Riesel, *Factors of generalized Fermat prime numbers*, Math. Comp. 67 (1998), 441–446.

[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.

[4] —, *On integers of the form* $k2^n + 1$, ibid. 129 (2001), 355–361.

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

[6] —, *On integers of the form* $k^r - 2^n$ *and* $k^r 2^n + 1$, ibid. 98 (2003), 310–319.

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

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

[9] Y. G. Chen and X. G. Sun, *On Romanoff's constant*, ibid. 106 (2004), 275–285.

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

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

[12] R. Crocker, *On the sum of a prime and two powers of two*, Pacific J. Math. 36 (1971), 103–107.

[13] H. Dubner and Y. Gallot, *Distribution of generalized Fermat prime numbers*, Math. Comp. 71 (2002), 825–832.

[14] H. Dubner and W. Keller, *Factors of generalized Fermat numbers*, Math. Comp. 64 (1995), 397–405.

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

[16] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.

[17] M. B. Nathanson, *Additive Number Theory*, Grad. Texts in Math. 164, Springer, New York, 1996.

[18] J. Pintz, *A note on Romanov's constant*, Acta Math. Hungar. 112 (2006), 1–14.

[19] J. Pintz and I. Z. Ruzsa, *On Linnik's approximation to Goldbach's problem. I*, Acta Arith. 109 (2003), 169–194.

[20] A. de Polignac, *Six propositions arithmologiques déduites de crible d'Eratosthène,* Nouv. Ann. Math. 8 (1849), 423–429.

[21] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. 125 (1997), 1913–1919.

[22] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. 109 (1934), 668–678.

[23] 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.

[24] J. Young, *Large primes and Fermat factors*, Math. Comp. 67 (1998), 1735–1738.

[25] P. Z. Yuan, *Integers not of the form* $c(2^a + 2^b) + p^\alpha$, Acta Arith. 115 (2004), 23–28.

Department of Mathematics
Nanjing Normal University
Nanjing 210097, China
E-mail: ygchen@njnu.edu.cn
rui.templier@gmail.com

Département de mathématiques
Université Montpellier II
Place Eugène Bataillon 34095, Montpellier, France
E-mail: nicolas.templier@normalesup.org

*Received on 20.6.2007*
*and in revised form on 1.9.2008* (5465)