On integers which are the sum of a power of 2 and a polynomial value

Florian Luca
Fundación Marcos Moshinsky
Instituto de Ciencias Nucleares UNAM
Circuito Exterior, C.U., Apdo. Postal 70-543
Mexico D.F. 04510, Mexico
fluca@matmor.unam.mx

Carlos Gustavo Moreira
IMPA
Estrada Dona Castorina 110
Rio de Janeiro, Brasil
gugu@impa.br

Carl Pomerance
Mathematics Department, Dartmouth College,
Hanover, NH 03755, USA
carl.pomerance@dartmouth.edu

March 11, 2013

Abstract

Here, we show that if $f(x) \in \mathbb{Z}[x]$ has degree at least 2 then the set of integers which are of the form $2^k + f(m)$ for some integers $k \geq 0$ and m is of asymptotic density 0. We also make some conjectures and prove some results about integers not of the form $|2^k \pm m^a(m-1)|$.

1 Introduction

This paper started by looking at positive integers not of the form $\pm 2^k \pm m^a(m-1)$, where a, k and m are nonnegative integers. This problem is inspired by results from [4], where it is proved that each of the three sets

$$\{n > 0 \ : \ n \text{ even}, \ n \neq 2^k + \phi(m)\},$$
$$\{n > 0 \ : \ n \text{ even}, \ n \neq 2^k - \phi(m)\},$$
$$\{n > 0 \ : \ n \text{ even}, \ n \neq \phi(m) - 2^k\}$$

is infinite. Here, $\phi(m)$ is the Euler function of m. Furthermore, it was shown in [4] that the first of the above three sets is of positive lower density. It is not known if either of the last two sets above is of positive lower density. It is also not known if the intersection of the above three sets is infinite.

The constructions from [4] of even positive integers in one of the above three sets start with positive integers $n \equiv 2 \pmod 4$. Then, at least if $k \geq 2$, any one of the equations $n = \pm 2^k \pm \phi(m)$ leads by reduction modulo 4 to the conclusion that $2 \| \phi(m)$. Thus, $m = 4$, p^{a+1}, or $2p^{a+1}$ for some odd prime p and nonnegative integer a. When $m = 4$, we get positive integers of the form $2^k \pm \phi(4) = 2^k \pm 2$, which are easy to avoid because there are very few of them. Since $\phi(p^{a+1}) = \phi(2p^{a+1})$, it follows that we may take $m = p^{a+1}$ and so look at the numbers $\pm 2^k \pm p^a(p-1)$. These are exactly the numbers we study in this paper without the additional information that p is prime.

For a fixed a, the numbers of the above form are particular instances of integers of the form $\pm 2^k \pm f(m)$, where $f(X) = X^a(X-1)$ is a polynomial of degree $a+1$. Then we realized that some of our results hold for the larger class of numbers of the form $|2^k + f(m)|$, where $f(X) \in \mathbb{Z}[X]$ is a polynomial of degree at least 2, so we shall formulate and prove those results in this degree of generality.

In this paper, we formulate the following conjecture.

Conjecture 1. *The set of integers*

$$\mathcal{A} = \{n \ : \ n = |2^k \pm m^a(m-1)| \textit{ for some integers } a \geq 1, \ k \geq 0 \textit{ and } m\}$$

is of asymptotic density zero.

The rest of the paper is organized as follows. In Section 2, we prove the analog of the Conjecture (1) above for the numbers of the form $|2^k + f(m)|$, where $f(x) \in \mathbb{Z}[x]$ has degree at least 2. In particular, this proves that Conjecture 1 holds if we fix the value of the parameter $a \geq 1$ and let only k and m be variables. In Section 3, we prove Conjecture 1 conditionally under the *abc*-conjecture. In Section 4, we prove some unconditional partial results towards Conjecture 1.

2 Integers of the form $|2^k + f(m)|$

Theorem 1. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \geq 2$. Then the set of integers*

$$\mathcal{A}_f = \{|2^k + f(m)| : k \geq 0,\ m \in \mathbb{Z}\}$$

is of asymptotic density zero. In particular, the number of members n of $\mathcal{A}_f$ with $n \leq x$ is $O_f(x^{1/d} \log x)$.

Proof. Write $f(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$. Let x be a large real number. Consider the equation

$$a_0 m^d + a_1 m^{d-1} + \cdots + a_d + 2^k = n, \tag{1}$$

in integers $k \geq 0$ and m, where $|n| \leq x$. We need to show that there are at most $O(x^{1/d} \log x)$ possibilities for n.

For each fixed value of k, the number of integers m with $|f(m) + 2^k| \leq x$ is $O(x^{1/d})$ uniformly in k. Assume that $|m| \leq x^2$. Then equation (1) implies that

$$2^k \leq |n| + |f(m)| = O(x + |m|^d) = O(x^{2d})$$

showing that $k = O(\log x)$. Hence, there are at most $O(x^{1/d} \log x)$ pairs of integers $|m| \leq x^2$ and $k \geq 0$ which can participate in an equation of the form (1).

From now on, we assume that $|m| > x^2$. We shall show there are only $O_f(1)$ solutions in this case.

Multiplying both sides of equation (1) by the fixed integer

$$a := d^d a_0^{d-1}$$

and grouping some terms, we get

$$m_1^d + a2^k = an + R(m), \tag{2}$$

where $m_1 = da_0 m + a_1$ and $R(X) \in \mathbb{Z}[X]$ is some fixed polynomial of degree at most $d-2$. Thus, $|R(m)| = O(|m|^{d-2})$. Write $k = dq + r$, where $r \in \{0, 1, \ldots, d-1\}$ and fix also the value for r. Relation (2) leads to

$$\prod_{i=1}^{d} (m_1 - \zeta_i 2^q) = O(x + |m|^{d-2}), \tag{3}$$

where $\zeta_1, \ldots, \zeta_d$ are all the roots of the polynomial $X^d + a2^r$. Observe that these roots are distinct. We divide the above equation (3) by m_1^d and by $\prod_{i=1}^{k} \zeta_i = (-1)^d a 2^r$, and using the fact that $|m_1| \gg |m|$, we infer that

$$\prod_{i=1}^{k} \left(\zeta_i^{-1} - \frac{2^q}{m_1} \right) = O\left(\frac{x + |m|^{d-2}}{|m_1|^d} \right) = O\left(\frac{x}{|m|^d} + \frac{1}{m^2} \right). \tag{4}$$

Put

$$\delta = \min\{|\zeta_i^{-1} - \zeta_j^{-1}| : 1 \le i < j \le d\}.$$

Since $m > x^2$, the right side of equation (4) tends to 0 when $x \to \infty$. Thus, $2^q/m_1$ is very close to ζ_i^{-1} for some $i = 1, \ldots, d$. Fix this value of i. Then $2^q/m_1 - \zeta_i^{-1}$ tends to 0 as x tends to infinity. Since

$$\left| \zeta_i^{-1} - \frac{2^q}{m_1} \right| < \frac{\delta}{2} \quad \text{implies} \quad \left| \zeta_j^{-1} - \frac{2^q}{m_1} \right| > \frac{\delta}{2} \quad \text{for all} \quad j \neq i \in \{1, \ldots, d\},$$

we conclude that, using $|m| > x^2$,

$$\left| \zeta_i^{-1} - \frac{2^q}{m_1} \right| = O\left(\frac{x}{|m|^d} + \frac{1}{m^2} \right) = O\left(\frac{1}{m^{1.5}} \right). \tag{5}$$

We may assume that $\zeta_i^{-1} - 2^q/m_1 \neq 0$ since otherwise, (2) implies that $an + R(m) = 0$. This implies that n is constant in the case that R is constant, and that $|m| \ll x^{1/\deg R}$ in the case that R is not constant. But $|m| > x^2$, so there are at most finitely many choices. Thus, (5) implies that we may assume

$$0 < \left| \zeta_i^{-1} - \frac{2^q}{m_1} \right| = O\left(\frac{1}{m^{1.5}} \right).$$

However, the above inequality has only finitely many integer solutions (m_1, q) by Ridout's version [6] of Roth's theorem [7]. This completes the proof. $\square$

Remark. A close analysis of the above proof shows that the statement of Theorem 1, with $x^{1/d}\log x$ replaced with $x^{1/d}(\log x)^{O(1)}$, remains true with essentially the same proof if one replaces 2^k by $\mathcal{S}$-units. These are positive integers k all whose prime factors belong to a fixed finite set of primes. We give no further details, but alert the reader also to the paper [1] where a similar result is proved in the case $d = 2$.

3 A conditional result

For a nonzero integer n we write $\gamma(n) = \prod_{p|n} p$ for its algebraic radical. The famous *abc* conjecture is the following statement.

Conjecture 2. *Let $\varepsilon > 0$ be fixed. There exists a constant $C(\varepsilon)$ depending on ε such that if a, b are coprime positive integers, then*

$$a + b \leq C(\varepsilon)\gamma(ab(a+b))^{1+\varepsilon}.$$

Our next result is conditional upon the *abc* conjecture.

Proposition 1. *The set $\mathcal{A}$ is of asymptotic density zero under the abc conjecture.*

Proof. Let x be a large positive real number and let us put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$. Let $n \in \mathcal{A}(x)$ and say $n = |2^k \pm m^a(m-1)|$. If $m = 0,\ \pm 1$, then $n = 2^k,\ 2^k \pm 2$, and the counting function of such $n \leq x$ has order $O(\log x)$. Also, unconditionally, we may assume that

$$n = |2^k - |m^a(m-1)||, \tag{6}$$

since if $n = 2^k + |m^a(m-1)|$, then $|m| \ll x^{1/2}$, $k \ll \log x$, and $a \ll \log x$, so the number of possibilities for n is $O(x^{1/2}(\log x)^2)$.

So, we assume that $|m| \geq 2$ and that (6) holds. Let $d = \gcd(2^k, m^a(m-1))$. Clearly, $d = 2^\lambda$ for some nonnegative integer λ. If $\lambda > \log\log x$, then $2^{\lfloor \log\log x \rfloor}$ divides n. The number of such $n \leq x$ is at most $x/2^{\lfloor \log\log x \rfloor} < x/\sqrt{\log x} = o(x)$ as $x \to \infty$. Assume now that $\lambda \leq \log\log x$. We apply the *abc* conjecture with some small ε to the relation

$$\frac{n}{d} = \left| 2^{k-\lambda} - \left| \frac{m^a(m-1)}{d} \right| \right|,$$

getting

$$\frac{|m|^{a+1}}{d} \le \frac{2|m|^a|m-1|}{d} \ll_\varepsilon \gamma(n2^{k-\lambda}m^a(m-1))^{1+\varepsilon}$$
$$\le (2x(|m|+1)^2)^{1+\varepsilon} \ll_\varepsilon x^{1+\varepsilon}|m|^{2+2\varepsilon},$$

which yields

$$|m|^{a-1-2\varepsilon} \ll x^{1+\varepsilon}2^\lambda \ll x^{1+\varepsilon}\log x.$$

Thus, if $a \ge 3$, then taking $\varepsilon = 1/10$, we get

$$|m| \ll x^{(1+\varepsilon)/(2-2\varepsilon)}\log x \ll x^{11/18}\log x.$$

Furthermore, since $|m| \ge 2$, we get that $2^{a-1.2} \ll x^{1.1}\log x$, implying $a \ll \log x$. Finally, since

$$2^k \ll \max\{x, |m|^{a+1}\} \le \max\{x, |m|^{3(a-1.2)}\} \ll x^{3.3}(\log x)^3,$$

we also get that $k \ll \log x$. Thus, the number of triples (a, k, m) such that $a \ge 3$ and $|2^k \pm m^a(m-1)| \le x$ is, under the *abc* conjecture, of cardinality $O(x^{11/18}(\log x)^3) = o(x)$ as $x \to \infty$.

We have left the cases $a = 1, 2$, but here we have the result unconditionally by Theorem 1. This completes the proof of Proposition 1. □

4 Unconditional partial results

Here, we prove some unconditional results about the set $\mathcal{A}$. As in the previous section, we may assume (unconditionally) that $|m| > 1$. We also shall assume that $m > 0$ (so that $m \ge 2$) by also dealing with the case of integers of the form $|2^k - m^a(m+1)|$. In fact, since there are few integers of the form $|2^k - 2^a(2 \pm 1)|$, we shall assume that $m \ge 3$. And from Theorem 1, we shall assume that $a \ge 3$.

Lemma 1. *Assume that* $0 < |2^k - m^a(m \pm 1)| \le x$ *and* $m \ge 3$. *Then* $a \ll \log x/\log m + \log m \log\log m$.

Proof. We treat only the case of the $\pm$ sign being negative since the other case is similar. If $2^k \le x^2$, then $m^a \le m^a(m-1) \le 2^k + x \le 2x^2$, therefore $a \ll \log x/\log m$. Assume next that $2^k > x^2$. Then

$$|2^{-k}m^a(m-1) - 1| \le \frac{x}{2^k} \le 2^{-k/2}.$$

We apply a linear form in logarithms à la Baker (see, for example, [5]) to the left hand side of the above inequality which is nonzero because of our hypothesis $|2^k - m^a(m-1)| > 0$. Observe that $k+1 \le a$. We get

$$|2^{-k}m^a(m-1) - 1| \ge \exp(-C(\log m)^2 \log(k+1)),$$

where C is some absolute constant. Thus,

$$2^{-k/2} \ge \exp(-C(\log m)^2 \log(k+1)),$$

yieding $k \ll (\log m)^2 \log(k+1)$. This implies that $k \ll (\log m)^2 \log\log m$. Since $k \gg a \log m$, we get that $a \ll \log m \log\log m$. The desired conclusion follows. □

Corollary 1. *The number of integers $n = |2^k - m^a(m \pm 1)| \le x$ where $a \ge 3$, $3 \le m \le x/(\log x)^2$ is $o(x)$ as $x \to \infty$.*

Proof. Again we shall deal only with the case when the $\pm$ sign is negative, the other case being similar. If $m^a(m-1) \le 3x$, then the number of choices for m is $O(x^{1/4})$, the number of choices for a is $O(\log x)$, and the number of choices for k is $O(\log x)$, so in this case the number of values of n is $O(x^{1/4}(\log x)^2)$. If $m^a(m-1) > 3x$, then for each pair m, a there are at most two values of k with $|2^k - m^a(m \pm 1)| \le x$. Assuming $m \le x/(\log x)^2$, Lemma 1 implies that $a \ll \log x \log\log x$. Thus, there are at most $O(x \log\log x/\log x)$ triples m, a, k. This completes the proof. □

So, from now on, we may assume that $m \ge x/(\log x)^2$ and $a \ge 3$.

As we have mentioned, Theorem 1 implies that for each fixed a there are few members $|2^k - m^a(m \pm 1)| \in \mathcal{A}(x)$. The next result allows us to handle all values of a to a large bound.

Theorem 2. *For each $T \ge 3$, the number of integers $|2^k - m^a(m \pm 1)| \in \mathcal{A}(x)$ with $k \ge 0$, $m \ge x/(\log x)^2$, and $3 \le a \le T$ is $O(T^2(\log T)(\log x)\log\log T)$.*

Proof. For $|2^k - m^a(m \pm 1)| \le x$, we have

$$2^k = m^a(m \pm 1) + O(x),$$

with a uniform O-constant. Thus,

$$k \log 2 = (a+1)\log m \pm \frac{1}{m} + O\left(\frac{1}{m^2}\right),$$

using $x < m^{a-1}$. Dividing by $a+1$ and exponentiating, we get

$$2^{k/(a+1)} = m\left(1 \pm \frac{1}{(a+1)m} + O\left(\frac{1}{am^2}\right)\right) = m \pm \frac{1}{a+1} + O\left(\frac{1}{am}\right),$$

and so

$$(a+1)2^{k/(a+1)} = (a+1)m \pm 1 + O\left(\frac{1}{m}\right). \qquad (7)$$

Write $k = q(a+1) + r$ for integers q, r with $0 \le r \le a$. Then (7) implies that for large x the case $r = 0$ does not occur, since the left side would be an integer divisible by $a+1$ and the right side for large x is an integer not compatible with this. So we assume that $r \in \{1, \ldots, a\}$.

We shall apply a quantitative version of the Subspace theorem due to Evertse [2]. We take $\mathbb{K} = \mathbb{Q}$ and $n = 2$. We let $V = \{\infty\} \cup \{p \ge 2 \text{ prime}\}$ be the set of all the places of $\mathbb{Q}$. The corresponding valuations are, for a rational nonzero number y, given by $|y|_\infty = |y|$ and $|y|_p = p^{-\mathrm{ord}_p(y)}$ if p is a prime, where $\mathrm{ord}_p(y)$ is the exponent of p in the factorization of y. When $\mathbf{y} = (y_1, y_2)$ and $v \in V$, we put

$$|\mathbf{y}|_v = \begin{cases} \sqrt{y_1^2 + y_2^2} & \text{if} \quad v = \infty, \\ \max\{|y_1|_v, |y_2|_v\} & \text{if} \quad v = p. \end{cases}$$

We put

$$H(\mathbf{y}) = \prod_{v \in V} |\mathbf{y}|_v.$$

All this can be found on page 226 of [2] for the particular case of $n = 2$ and $\mathbb{K} = \mathbb{Q}$. We now take $S = \{2, \infty\}$, $\mathbf{x} = (x_1, x_2)$,

$$l_{1,\infty}(x_1, x_2) = 2^{r/(a+1)}x_1 - x_2, \;\; l_{2,\infty}(\mathbf{x}) = x_1, \;\; l_{1,2}(\mathbf{x}) = x_1, \;\; l_{1,2}(\mathbf{x}) = x_2.$$

We extend the infinite valuation to $\mathbb{Q}(2^{1/(a+1)})$ in such a way that it is the absolute value. It is easy to compute that one can take $H = 2$ and $D = a+1$ as upper bounds for the heights and degrees of the number fields containing the coefficients of $l_{i,v}$ for $i = 1, 2$ and $v \in S$ as on the line 1 of page 228 of [2]. We compute the double product

$$\prod_{i=1}^{2} \prod_{v \in S} |l_{i,v}(\mathbf{x})|_v$$

for $\mathbf{x} = ((a+1)2^q, (a+1)m \pm 1)$. Using estimate (7), we get that the above double product is at most

$$|(a+1)2^{k/(a+1)} - ((a+1)m \pm 1)| \times (a+1)2^{k/(a+1)} \times 2^{-q}$$
$$\ll \frac{(a+1)2^{r/(a+1)}}{m} \ll \frac{a}{m} \ll \frac{1}{(am)^{2/3}} \ll \frac{1}{\|\mathbf{x}\|^{2/3}}, \tag{8}$$

where $\|\mathbf{x}\| = \max\{|x_1|, |x_2|\}$ and for the next-to-last inequality we used the fact that $a \ll \log m \log\log m$ (Lemma 1), therefore certainly $a \ll m^{1/5}$. Since $m \geq x/(\log x)^2$, it follows that for large x, we have

$$\prod_{i=1}^{2}\prod_{v\in S} |l_{i,v}(\mathbf{x})|_v < \frac{1}{2\|\mathbf{x}\|^{1/2}}. \tag{9}$$

It is easy to see that for our system of forms, we have that

$$\det(l_{1,v}, l_{2,v}) = \pm 1 \quad \text{for} \quad v \in S.$$

Since also $2\|\mathbf{x}\| \geq H(\mathbf{x})$ because $\mathbf{x}$ is a vector with integer components, we get right away that inequality (9) implies

$$\prod_{v\in S}\prod_{i=1}^{2} \frac{|l_{i,v}(\mathbf{x})|_v}{|\mathbf{x}|_v} < \left(\prod_{v\in S} |\det(l_{1,v}, l_{2,v})|_v\right) H(\mathbf{x})^{-2-1/2},$$

which is inequality (1.3) on page 228 in [2] with $\delta = 1/2$. Note that $(a+1)2^q$ and $(a+1)m \pm 1$ are not necessarily coprime, but $a+1$ and $(a+1)m \pm 1$ are coprime. Thus, $H(\mathbf{x}) \geq H((a+1, 1)) = a+1 \geq 3 > H$, and so we are in the situation (i) of the theorem on page 228 in [2]. That theorem then implies that $\mathbf{x}$ is in a totality of at most $2^{508}\log(4(T+1))\log\log(4(T+1))$ subspaces; that is, at most $O(\log T \log\log T)$ subspaces. This is for a fixed $a \leq T$ and $r \in \{1, \ldots, a\}$. Assume now a, r and a subspace is fixed. This means that $c_1x_1 - c_2x_2 = 0$ holds for some fixed $(c_1, c_2) \neq (0, 0)$. We may assume that $\gcd(c_1, c_2) = 1$. Thus, $(a+1)2^q/((a+1)m \pm 1) = c_2/c_1$ is fixed. This does not mean that 2^q and $(a+1)m \pm 1$ are fixed, but that for some integer d, $(a+1)2^q = c_2 d$, $(a+1)m \pm 1 = c_1 d$. Further, since $a+1$ is coprime to $c_1 d$ we have that d is a divisor of 2^q, so that $d = 2^\lambda$ for some integer $\lambda \geq 0$.

Assume that $2^k - m^a(m \pm 1) \geq 0$, the case where it is negative being similar. The relation

$$2^{q(a+1)+r} - m^a(m \pm 1) = n \quad \text{with} \quad 0 \leq n \leq x,$$

leads to

$$2^r \left(\frac{c_2 2^\lambda}{a+1}\right)^{a+1} - \left(\frac{c_1 2^\lambda \mp 1}{a+1}\right)^a \left(\frac{c_1 2^\lambda \mp 1}{a+1} \pm 1\right) = n.$$

Multiplying both sides by $(a+1)^{a+1}$, we get

$$F(2^\lambda) = n(a+1)^{a+1}, \quad \text{where} \quad 0 \le n \le x,$$

and where $F(y) \in \mathbb{Z}[y]$ is some polynomial of degree $a+1$. Let then $n_1, \ldots, n_t$ be all the integers n that arise in this fashion corresponding to $\lambda_1 < \cdots < \lambda_t$. So $F(2^{\lambda_i}) = n_i(a+1)^{a+1}$. If $t \ge 2$ and $1 \le i < t$, then

$$2^{\lambda_t} - 2^{\lambda_i} \mid F(2^{\lambda_t}) - F(2^{\lambda_i}) = (n_t - n_i)(a+1)^{a+1}, \text{ so that } 2^{\lambda_i} \mid (n_t - n_i)(a+1)^{a+1}.$$

Since $\lambda_t > 0$ and $2^{\lambda_t} \mid (a+1)m \pm 1$, it follows that $a+1$ is odd. Thus, for $i < t$, $2^{\lambda_i} \mid n_t - n_i$, so that $\lambda_i = O(\log x)$ and hence $t = O(\log x)$. This was when a, r and the subspace were fixed. Since there are $O(\log T \log\log T)$ possible subspaces whenever both $a \le T$ and $r \le a$ are fixed, we get a bound of

$$O(T^2(\log T)(\log x)\log\log T)$$

on the total number of possibilities for $n \in \mathcal{A}(x)$. This finishes the proof of the theorem. □

Corollary 2. *But for a set of cardinality $o(x)$ as $x \to \infty$, the members $|2^k - m^a(m \pm 1)|$ of $\mathcal{A}(x)$ with $m, a > 0$ have*

$$a > \frac{x^{1/2}}{\log x \log\log x}, \quad m > \exp\left(\frac{x^{1/2}}{(\log x \log\log x)^2}\right), \quad k > \frac{x}{(\log x \log\log x)^3}.$$

Proof. The inequality for a follows immediately from Theorem 1, Corollary 1, and Theorem 2 with $T = x^{1/2}/(\log x \log\log x)$. The inequality for m follows now from Lemma 1 and the inequality for a. Note that for large x, Corollary 1 implies that

$$2^k \ge m^a(m-1) - x \ge 2m^a - x > m^a,$$

so that $k > a \log m$. Thus, the third inequality in the corollary follows from the first two. □

Proposition 2. *The set of integers $|2^k - m^a(m \pm 1)| \in \mathcal{A}$ with $m, a > 0$ and either m even or both a odd and k even has asymptotic density zero.*

Proof. It follows from Corollary 2 that the members of $\mathcal{A}$ arising from a triple m, a, k with m even is $o(x)$ as $x \to \infty$. (This also follows from Theorem 1.) Thus, assume that m is odd, a is odd, and k is even. We have

$$|2^{k/2} - m^{(a-1)/2}\sqrt{m(m \pm 1)}||2^{k/2} + m^{(a-1)/2}\sqrt{m(m \pm 1)}| = O(x).$$

Thus,

$$\left| \frac{2^{k/2}}{m^{(a-1)/2}} - \sqrt{m(m \pm 1)} \right| = O\left(\frac{x}{m^{a-1}\sqrt{m(m-1)}} \right).$$

By Corollary 2 we may assume that $x/\sqrt{m(m-1)} = o(x)$ as $x \to \infty$, so that for large x we have

$$\left| \frac{2^{k/2}}{m^{(a-1)/2}} - \sqrt{m(m \pm 1)} \right| < \frac{1}{2(m^{(a-1)/2})^2}.$$

A well-known result of Legendre tells us that $2^{k/2}/m^{(a-1)/2}$ is a convergent of $\sqrt{m(m \pm 1)}$. In fact, we have $\sqrt{m(m+1)} = [m, 2, \{2m, 2\}]$, and $\sqrt{m^2 - m} = [m-1, 2, \{2m-2, 2\}]$. Furthermore, if p/q is a convergent of $\sqrt{m(m+1)}$, then $p^2 - m(m+1)q^2 = \pm 1, \ \pm m$. The second possibility is not convenient for us since $m > x$. Similarly, if p/q is a convergent of $\sqrt{m(m-1)}$, then $p^2 - m(m-1)q^2 = \pm 1, \ \pm(m-1)$, and again the second one is not convenient for us since it is too large. Thus, $2^{k/2}/m^{(a-1)/2} = p/q$ is a convergent of $\sqrt{m(m \pm 1)}$ such that $p^2 - m(m \pm 1)q^2 = \pm 1$. The numbers $2^{k/2}$ and $m^{(a-1)/2}$ are coprime, so $p = 2^{k/2}, q = m^{(a-1)/2}$, and we are talking about the member 1 of $\mathcal{A}$, which is negligible. This completes the proof. □

Remark. It is easy to see that the odd members of $\mathcal{A}$ have asymptotic density 0, since if m, a, k give rise to an odd number n, we must have $k = 0$. Are there infinitely many positive even numbers that are not members of $\mathcal{A}$? This question might be answerable by the methods of Luca [3]. (That paper discusses the conjecture of Erdős that there are infinitely many integers which are not the sum or difference of two powers.)

Acknowledgments. Part of this work was done during a visit of F. L. at IMPA in January of 2010. He thanks the people of this Institute for their hospitality and financial support. F. L. was also partially supported by a Marcos Moshinsky Fellowship and Projects PAPIIT IN104512, CONACyT 163787 and CONACyT 193539. C. P. was partially supported by NSF grant DMS-1001180.

References

[1] M. A. Bennett, F. Luca, and J. Mulholland, 'Twisted extensions of the cubic case of Fermat's last theorem', *Ann. Sci. Math. Québec* **35** (2011), 1–15.

[2] J.–H. Evertse, "An improvement of the quantitative Subspace theorem", *Compositio Math.* **101** (1996), 225–311.

[3] F. Luca, 'On integers which are differences of two powers', Mathematika **49** (2002), 231–243.

[4] F. Luca and V. J. Mejía Huguet, 'Some remarks on Sierpiński numbers and related problems', *Bol. Soc. Mat. Mexicana* **15** (2009), 11–23.

[5] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II', *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180; English translation in *Izv. Math.* **64** (2000), 1217–1269.

[6] D. Ridout, 'Rational approximations to algebraic numbers', *Mathematika* **4** (1957), 125–131.

[7] K. F. Roth, 'Rational approximations to algebraic numbers', *Mathematika* **2** (1955) 1-20; corrigendum ibid. **2** (1955), 168.