# ON THE DIOPHANTINE EQUATION $A x^{2}+2^{2 m}=y^{n}$ 

## FADWA S. ABU MURIEFAH

(Received 6 May 1999 and in revised form 20 February 2000)


#### Abstract

Let $h$ denote the class number of the quadratic field $\mathbb{Q}(\sqrt{-A})$ for a square free odd integer $A>1$, and suppose that $n>2$ is an odd integer with $(n, h)=1$ and $m>1$. In this paper, it is proved that the equation of the title has no solution in positive integers $x$ and $y$ if $n$ has any prime factor congruent to 1 modulo 4 . If $n$ has no such factor it is proved that there exists at most one solution with $x$ and $y$ odd. The case $n=3$ is solved completely. A result of E. Brown for $A=3$ is improved and generalized to the case where $A$ is a prime $\not \equiv 7(\bmod 8)$.


2000 Mathematics Subject Classification. Primary 11D41.

1. Introduction. Let $A, m, n$ denote positive integers where $n$ is odd $>1$ and $A$ square free odd integer. Let $K=\mathbb{Q}(\sqrt{-A})$, where $\mathbb{Q}$ is the field of rational numbers, let further $h$ denote the number of classes of ideals in $K$ and suppose $(h, n)=1$. In this paper, we consider the Diophantine equation $A x^{2}=2^{2 m}=y^{n}$, where $x$ and $y$ are integers. The case $A=1$ was studied in [1] so we will assume that $A>1$. The first result regarding this equation is due to Nagell [5] who proved that when $m=0,1$, this equation has no solutions in integers $x$ and $y$ under the above assumptions about $A$ and $n$ so we will suppose that $m>0$. Since $n$ is odd, there is no loss of generality in considering only odd primes $p$ and $x, y$ positive integers, so we will assume this in what follows.

We start by proving the main result of this paper.
Theorem 1.1. Let $A>1$ be a square free odd integer, $p$ an odd prime with $(h, p)=1$ and $m \geq 1$. Then the Diophantine equation

$$
\begin{equation*}
A x^{2}+2^{2 m}=y^{p} \tag{1.1}
\end{equation*}
$$

has no solution with $x$ odd in any of the following cases:
(i) if $A=3$;
(ii) if $p \equiv 1(\bmod 4)$;
(iii) if $A \equiv 3(\bmod 4)$ and $p>3$.

For $p=3$, such a solution exists if and only if A is the square-free part of either $(1 / 3)(1+$ $\left.2^{m+3}\right)$ with $m$ even or of $(1 / 3)\left(2^{2 m}-1\right)$, although in these cases, there might be other solutions if $3 \mid h$.

Proof. We factorize (1.1) in the field $K$,

$$
\begin{equation*}
\left(2^{m}+x \sqrt{-A}\right)\left(2^{m}-x \sqrt{-A}\right)=y^{p} . \tag{1.2}
\end{equation*}
$$

Now the principal ideal $\left\lfloor 2^{m}+x \sqrt{-A}\right\rfloor$ and its conjugate ideal are coprime, so $\left\lfloor 2^{m}+\right.$ $x \sqrt{-A}\rfloor=\pi^{p}$ for some ideal $\pi$ in $K$. It follows that $\pi^{p}$ is a principal ideal and since (h,p) $=1$, therefore $\pi$ is a principal ideal, say $\pi=[\xi]$ for some element $\xi$ in $K$. So we get the equation

$$
\begin{equation*}
\left\lfloor 2^{m}+x \sqrt{-A}\right\rfloor=[\xi]^{p} \tag{1.3}
\end{equation*}
$$

and, consequently,

$$
\begin{equation*}
\left(2^{m}+x \sqrt{-A}\right)=\varepsilon \xi^{p} \tag{1.4}
\end{equation*}
$$

for some unit $\varepsilon$ in $K$. Therefore we have the following three cases:

$$
\begin{align*}
& x \sqrt{-3}+2^{m}=\left(\frac{1 \pm \sqrt{-3}}{2}\right)\left(\frac{a+b \sqrt{-3}}{2}\right)^{3}, \quad a \equiv b(\bmod 2) \\
& x \sqrt{-A}+2^{m}=\left(\frac{a+b \sqrt{-A}}{2}\right)^{p}, \quad a \equiv b \equiv 1(\bmod 2)  \tag{1.5}\\
& x \sqrt{-A}+2^{m}=(a+b \sqrt{-A})^{p}
\end{align*}
$$

for some rational integers $a$ and $b$.
Equating the imaginary parts in the first case we get

$$
\begin{equation*}
16 x= \pm\left(a^{3}-9 a b^{2}\right)+\left(3 a^{2} b-3 b^{3}\right) \tag{1.6}
\end{equation*}
$$

and we can absorb the lower sign into $a$. Then

$$
\begin{equation*}
16 x=(a+b)^{3}-12 a b^{2}-4 b^{3} \tag{1.7}
\end{equation*}
$$

Since $a$ and $b$ have the same parity, we write $2 c=a+b$, and obtain

$$
\begin{equation*}
2 x=c^{3}-3 c b^{2}+b^{3} \tag{1.8}
\end{equation*}
$$

Equation (1.8) is impossible, since the right-hand side is odd unless both $b$ and $c$ are even, and then this side is divisible by 8 if they are which is not possible since $x$ is odd. So this case does not arise.

The second case arises only if $A \equiv 3(\bmod 4)$, and we will prove that in this case $p=3$ and $A \neq 3$.

Observe that $((a+b \sqrt{-A}) / 2)^{p} \in Z[\sqrt{-A}]$ only if $A \equiv 3(\bmod 8)$ and $p=3$ and then equating the real parts in this case, we get

$$
\begin{equation*}
2^{m+3}=a\left(a^{2}-3 A b^{2}\right) \tag{1.9}
\end{equation*}
$$

Since $a$ is odd we get $a= \pm 1$ and then

$$
\begin{equation*}
\pm 2^{m+3}=1-3 A b^{2} \tag{1.10}
\end{equation*}
$$

Now $A>1$, so only the negative sign holds and then

$$
\begin{equation*}
A b^{2}=\frac{1+2^{m+3}}{3} \tag{1.11}
\end{equation*}
$$

Considering this equation modulo 3 we deduce that $m$ should be even. If $A=3$, then we get

$$
\begin{equation*}
-2^{m+3}=(1-3 b)(1+3 b) \tag{1.12}
\end{equation*}
$$

So

$$
\begin{equation*}
2^{t}=1+3 b, \quad-2^{k}=1-3 b \tag{1.13}
\end{equation*}
$$

where $t+k=m+3$. By adding these two equations we get $t=2, k=1$, which is impossible since $m \geq 1$.

Finally the third case can occur for all $A$, and we will prove that there is no solution when either $p \equiv 1(\bmod 4)$ or $A \equiv 3(\bmod 4)$.

Since $x$ is odd it follows that $y=a^{2}+A b^{2}$ is odd, so $a$ and $b$ have opposite parity. On equating the real parts we get

$$
\begin{equation*}
2^{m}=a \sum_{r=0}^{(p-1) / 2}\binom{p}{2 r} a^{p-2 r-1}\left(-A b^{2}\right)^{r} \tag{1.14}
\end{equation*}
$$

Here $\sum$ is odd, since the first and the last terms have opposite parity and the rest are all even. So $a= \pm 2^{m}, b$ is odd and from (1.14) we get

$$
\begin{equation*}
\pm 1=\sum_{r=0}^{(p-1) / 2}\binom{p}{2 r} 2^{m(p-2 r-1)}\left(-A b^{2}\right)^{r} \tag{1.15}
\end{equation*}
$$

Then $\pm 1 \equiv 2^{m(p-1)}(\bmod p)$ and so the lower sign is impossible. That is,

$$
\begin{equation*}
1=\sum_{r=0}^{(p-1) / 2}\binom{p}{2 r} 2^{m(p-2 r-1)}\left(-A b^{2}\right)^{r} \tag{1.16}
\end{equation*}
$$

and $a=2^{m}$. So $y=2^{2 m}+A b^{2}$.
Now suppose that $p \equiv 1(\bmod 4)$, say $p=1+2^{k} u$, where $(u, 2)=1$ and $k \geq 2$. Since both $b$ and $A$ are odd,

$$
\begin{equation*}
b^{p-1}=\left(b^{u}\right)^{2^{k}} \equiv 1\left(\bmod 2^{k+2}\right), \quad(-A)^{(p-1) / 2}=\left(A^{u}\right)^{2^{k-1}} \equiv 1\left(\bmod 2^{k+1}\right) \tag{1.17}
\end{equation*}
$$

Then from (1.16) we get

$$
\begin{align*}
1 & \equiv\binom{p}{3} 2^{2 m}\left(-A b^{2}\right)^{(p-3) / 2}+p b^{p-1}(-A)^{(p-1) / 2}\left(\bmod 2^{k+1}\right)  \tag{1.18}\\
& \equiv \frac{p(p-2)}{3} \cdot 2^{k+2 m-1} u\left(-A b^{2}\right)^{(p-1) / 3}+p\left(\bmod 2^{k+1}\right)
\end{align*}
$$

since $m \geq 1$, therefore $k+2 m-1 \geq k+1$, so from (1.18) we get $3 \equiv 3 p\left(\bmod 2^{k+1}\right)$. Hence $p \equiv 1\left(\bmod 2^{k+1}\right)$ which is not possible. We conclude that there is no solution when $p \equiv 1(\bmod 4)$. If $A \equiv 3(\bmod 4)$, then considering (1.16) modulo 4 we get $p \equiv 1(\bmod 4)$ hence there is no solution when $A \equiv 3(\bmod 4)$.

Now let $p=3$ in (1.16) then

$$
\begin{equation*}
1=2^{2 m}-3 A b^{2} \tag{1.19}
\end{equation*}
$$

or $A b^{2}=\left(2^{2 m}-1\right) / 3$. This completes the proof.

Remark 1.2. From Theorem 1.1, we note that to solve (1.1) it is sufficient to consider (1.16) where $b$ is odd, $p \equiv 3(\bmod 4)$, and $A \equiv 1(\bmod 4)$. If there is a solution then $y=2^{2 m}+A b^{2}$.

Now we prove the following theorem which gives us the number of solutions of our equation.

Theorem 1.3. For a given $A$, if (1.1) has a solution in $x$ odd where $(h, p)=1$, then it is unique.

Proof. If $A \equiv 3(\bmod 4)$, we have proved that there is a solution only if $p=3$, and we have found this unique solution. If $A \equiv 1(\bmod 4)$, then from the last proof it is sufficient to consider (1.16), where $b$ is odd and $p \equiv 3(\bmod 4)$. Suppose $b_{1}>b>0$ is another solution, then from (1.16) we obtain

$$
\begin{equation*}
1=\sum_{r=0}^{(p-1) / 2}\binom{p}{2 r} 2^{m(p-2 r-1)}\left(-A b_{1}^{2}\right)^{r} . \tag{1.20}
\end{equation*}
$$

Subtracting (1.20) from (1.16) and dividing by $b_{1}^{2}-b^{2}$, we get

$$
\begin{align*}
0 & =\sum_{r=0}^{(p-1) / 2}\binom{p}{2 r} \frac{b_{1}^{2 r}-b^{2 r}}{b_{1}^{2}-b^{2}} \cdot 2^{m(p-2 r-1)}(-A)^{r}  \tag{1.21}\\
& \equiv p \cdot \frac{b_{1}^{p-1}-b^{p-1}}{b_{1}^{2}-b^{2}}(\bmod 2) .
\end{align*}
$$

Since $p \equiv 3(\bmod 4)$, the number $\left(b_{1}^{p-1}-b^{p-1}\right) /\left(b_{1}^{2}-b^{2}\right)$ is odd, so (1.21) is impossible and the solution is unique as required.

Now we prove that to solve (1.1) it is sufficient to consider only $x$ odd. First we need the following lemma.

Lemma 1.4 [4]. The Diophantine equations

$$
\begin{equation*}
A x^{2}+1=2 y^{n}, \quad A \equiv 1(\bmod 4), \quad A x^{2}+1=4 y^{n}, \quad A \equiv 3(\bmod 4), \tag{1.22}
\end{equation*}
$$

have no solutions in positive integers with $y>1, n>2,2 \nmid n y$ and $(n, h)=1$.
Theorem 1.5. If $A=3$, equation (1.1) has a solution with $x$ even only if $m \equiv$ $-1(\bmod p)$, and this solution is given by $x=2^{m}$; for all other $A \equiv 7(\bmod 8)$ with $(h, p)=1$ there exists a solution with $x$ even of the form $x=2^{u} X$ with $X$ odd, if and only if there is a solution of the equation $A X^{2}+2^{2(m-u)}=Y^{p}$.

Proof. If $x$ is even then $y$ is even, so let $x=2^{u} X, y=2^{v} \cdot Y$, where $u>0, v>0$, $(2, X)=(2, Y)=1$. Then (1.1) becomes

$$
\begin{equation*}
A\left(2^{u} X\right)^{2}+2^{2 m}=2^{v p} Y^{p} \tag{1.23}
\end{equation*}
$$

We have three cases:
(1) $p v>2 u=2 m$. Then cancelling $2^{2 m}$ in (1.23) we get

$$
\begin{equation*}
A X^{2}+1=2^{v p-2 m} Y^{p} \tag{1.24}
\end{equation*}
$$

where $X$ is odd. Now $A \not \equiv 7(\bmod 8)$, so $v p-2 m=1$ or 2 .

If $A \equiv 1(\bmod 4)$ then $v p-2 m=1$ and so $A X^{2}+1=2 Y^{p}$. This equation has no solution from Lemma 1.4. If $A \equiv 3(\bmod 8)$, then $v p-2 m=2$, so $A X^{2}+1=4 Y^{p}$, and again from Lemma 1.4 this equation has no solution in integers with $Y>1$. Let $Y=1$, then $A X^{2}+1=4 Y^{p}$ implies that $A=3, X=1$ and hence $x=2^{m}$, also $v p=2 m+2$ implies that $m \equiv-1(\bmod p)$,
(2) $2 u>2 m=v p$. Then cancelling $2^{2 m}$ in (1.23) we get $A\left(2^{u-m} X\right)^{2}+1=Y^{p}$. This equation has no solution [5, Theorem 25].
(3) $2 m>2 u=p v$. Then

$$
\begin{equation*}
A X^{2}+2^{2(m-u)}=Y^{p} \tag{1.25}
\end{equation*}
$$

and this is (1.1) with $x$ odd and smaller $m$.
Remark 1.6. From the proof of the last theorem we deduce that to solve (1.1) in even integers when $A \neq 3$ and $A \not \equiv 7(\bmod 8)$, it is sufficient to consider the equation

$$
\begin{equation*}
A X^{2}+2^{2(m-u)}=Y^{p} \tag{1.26}
\end{equation*}
$$

where $x=2^{u} X, y=2^{v} \cdot Y, m>u>0, v>0,(2, X)=(2, Y)=1$, and $2 u=p v$.
Summarizing the above we give the following theorem.
Theorem 1.7. The Diophantine equation (1.1) where $A \not \equiv 7(\bmod 8)$ and $(h, p)=1$ has no integer solution if $p \equiv 1(\bmod 4)$. In particular, the equation $p x^{2}+2^{2 m}=y^{p}$ has no solution for all $p>3$ and $p \not \equiv 7(\bmod 8)$.
Proof. If $x$ is odd, then from Theorem 1.1, equation (1.1) has no solution when $p \equiv 1(\bmod 4)$. Now let $x$ be even then from Theorem 1.5 it is sufficient to consider the equation

$$
\begin{equation*}
A X^{2}+2^{2(m-u)}=Y^{p}, \tag{1.27}
\end{equation*}
$$

where $X$ is odd and $0<u<m$. Since $p \equiv 1(\bmod 4)$ then again Theorem 1.1 implies that there is no solution.
Now the class number of the field $\mathbb{Q}(\sqrt{-p})$ is less than $p$, so as above the equation $p x^{2}+2^{2 m}=y^{p}$ has no solution if $p \equiv 1(\bmod 4)$. Let $p \equiv 3(\bmod 4)$, since $p>3$, therefore the equation has no solution in odd integers from Theorem 1.1(iii). If $x$ is even then we have

$$
\begin{equation*}
p X^{2}+2^{2(m-u)}=Y^{p} \tag{1.28}
\end{equation*}
$$

where $X$ is odd. Equation (1.28) has no solution in odd integers from the first part.

Brown [2, Theorem 3] considered the Diophantine equation (1.1) when $A=3$, but he did not solve it completely. In the following we give the complete solution.
Theorem 1.8. The Diophantine equation $3 x^{2}+2^{2 m}=y^{p}$ has a solution only if $m \equiv-1(\bmod p)$, and this solution is given by $x=2^{m}, y=2^{(2 m+2) / p}$.
Proof. Now $A=3$ and the field $\mathbb{Q}(\sqrt{-3})$ is a unique prime factorization domain, so from Theorem 1.1 this equation has no solution for all $p$ if $x$ is odd. If $x$ is even then from Theorem 1.5 we have $x=2^{m}, y=2^{(2 m+2) / p}$. Also the equation

$$
\begin{equation*}
3 X^{2}+2^{2(m-u)}=Y^{p} \tag{1.29}
\end{equation*}
$$

where $X$ is odd, has no solution from the first part of this proof.

Combining the two last theorems we can generalize Brown's result [2] for any odd prime $p$ as follows.

Theorem 1.9. The Diophantine equation $p x^{2}+2^{2 m}=y^{p}$, where $p \not \equiv 7(\bmod 8)$, has a solution only if $p=3$ and $m \equiv 2(\bmod 3)$ and this solution is given by $x=2^{m}$, $y=2^{(2 m+2) / 3}$.

Considering (1.16) modulo 8 it is easy to prove the following.
Corollary 1.10. For a given $A$, in (1.16) where $m \geq 2$, if $A \equiv 1(\bmod 8)$ then $p \equiv 7(\bmod 8)$ and if $A \equiv 5(\bmod 8)$ then $p \equiv 3(\bmod 8)$.

As a special case we consider $A=q$ an odd prime and prove the following theorem.
Theorem 1.11. The Diophantine equation $q x^{2}+2^{2 m}=y^{3}$, where $q \equiv 1(\bmod 4)$ is a prime integer and $(3, h)=1$, has a solution only if $q=5$ and $m=2+3 M$, and the unique solution is given by $x=43 \cdot 2^{3 M}$ and $y=21 \cdot 2^{2 M}$.

Proof. First suppose that $x$ is odd, since $q \equiv 1(\bmod 4)$ and $p=3$, therefore it is sufficient to consider (1.16), then $y=2^{2 m}+q b^{2}$ and

$$
\begin{equation*}
3 q b^{2}=2^{2 m}-1=\left(2^{m}-1\right)\left(2^{m}+1\right) . \tag{1.30}
\end{equation*}
$$

From [5] it is sufficient to consider $m \geq 2$ and from Corollary 1.10 we have $q \equiv 5(\bmod 8)$. Now $\left(2^{m}-1,2^{m}+1\right)=1$, let $b=c d$, where $(c, d)=1$ and both $c$ and $d$ are odd, then from (1.30) we have only the following possibilities:
(1) $2^{m}-1=3 q c^{2}, 2^{m}+1=d^{2}$, subtracting these two equations, we get $2=d^{2}-3 q c^{2}$ which is not possible modulo 3 .
(2) $2^{m}-1=3 c^{2}, 2^{m}+1=q d^{2}$, considering the first equation modulo 8 , we get $m=2$ and hence $q=5$. Therefore $y=2^{2 m}+q b^{2}=2^{4}+5(1)=21$ and so $x=43$.
(3) $2^{m}-1=d^{2}, 2^{m}+1=3 q c^{2}$, again considering the first equation modulo 8 , we get $m=1$ and then $q=1$ which is not our case.
(4) $2^{m}-1=q c^{2}, 2^{m}+1=3 d^{2}$, considering the first equation modulo 8 , we get a contradiction.

Now suppose that $x$ is even, then we have only the following equation:

$$
\begin{equation*}
q X^{2}+2^{2(m-u)}=Y^{3} \tag{1.31}
\end{equation*}
$$

where $x=2^{u} X, y=2^{v} \cdot Y, m>u>0, v>0,(2, X)=(2, Y)=1$, and $2 u=3 v$. From the first part of this proof, equation (1.31) has a unique solution given by $q=5$, $m-u=2, X=43$, and $Y=21$. Since $2 u=3 v$ we get $3 \mid u$, let $u=3 M$ then $m=2+3 M$ and $v=2 M$. Hence $x=43 \cdot 2^{3 M}$ and $y=21 \cdot 2^{2 M}$.

We are unable to solve (1.1) completely when $A \equiv 1(\bmod 4)$ but we are able to solve it for many particular values of $A$ for all $p$ as we will show in the following example. But before this we give a corollary which will help us.

Corollary 1.12. If $m$ is odd then the Diophantine equation (1.1) has no solution in $x$ odd when $5 \mid A$.

Proof. Since $m$ is odd, therefore from the proof of Theorem 1.1, it is sufficient to consider (1.16), where $p \equiv 3(\bmod 4)$. If $5 \mid A$ in $(1.16)$, then we get $1 \equiv 2^{m(p-1)}(\bmod 5)$ which implies that $4 \mid m(p-1)$ and this is not possible.

EXAMPLE 1.13. Consider the Diophantine equation $5 x^{2}+2^{10}=y^{p}$.
Here $m=5, A=5, h=2$, so from Corollary 1.12, this equation has no solution in $x$ odd for all $p$. If $x$ is even then it is sufficient to consider the equation

$$
\begin{equation*}
5 X^{2}+2^{2(5-u)}=Y^{p} \tag{1.32}
\end{equation*}
$$

where $x=2^{u} X, y=2^{v} \cdot Y, 5>u>0, v>0,(2, X)=(2, Y)=1$, and $2 u=p v$. Since $p$ is an odd prime, the only possibility is $u=3, p=3$, and (1.32) becomes $5 X^{2}+2^{4}=Y^{3}$, which has a unique solution from Theorem 1.11, given by $X=43$ and $Y=21$, so the given equation has a unique solution, $x=8.43, y=4.21$, and $p=3$.

By using the method similar to [3, Lemma 3] we can prove the following lemma.
Lemma 1.14. If $q$ is any odd prime which divides the integer $b$ defined in (1.16), then

$$
\begin{equation*}
2^{m(q-1)} \equiv 1\left(\bmod q^{2}\right) \tag{1.33}
\end{equation*}
$$

Considering (1.16) modulo 3 we are able to prove the following theorem.
Theorem 1.15. If $3 \mid b$ in (1.16), then $m=3^{k} \cdot m^{\prime}$, where $k \geq 1,\left(3, m^{\prime}\right)=1$ and either
(1) $3 \nmid A$ and then there is no solution if $k$ even, or
(2) $3 \mid A$ and then there is no solution if $k$ odd.

Proof. Let $3 \mid b$ then from Lemma $1.14,2^{2 m} \equiv 1(\bmod 9)$ which implies that $3 \mid m$. Let $m=3^{k} \cdot m^{\prime}$, where $\left(3, m^{\prime}\right)=1, k \geq 1$. Since $p \equiv 3(\bmod 4)$, put $p-1=2 \cdot 3^{t} \cdot p^{\prime}$, where $\left(2, p^{\prime}\right)=\left(3, p^{\prime}\right)=1, t \geq 0$ and put $b=3^{s} \cdot b^{\prime}$, where $\left(3, b^{\prime}\right)=1, s \geq 1$. Rewrite (1.16) as

$$
\begin{equation*}
1-2^{m(p-1)}=\sum_{r=1}^{(p-1) / 2}\binom{p}{2 r} 2^{m(p-2 r-1)}\left(-A b^{2}\right)^{r} \tag{1.34}
\end{equation*}
$$

The general term in the right-hand side is

$$
\begin{equation*}
\binom{p}{2 r} 2^{m(p-2 r-1)}\left(-A b^{2}\right)^{r}=\binom{p-2}{2 r-2} 2^{m(p-2 r-1)} \times \frac{p b^{2 r-2}}{r(2 r-1)} \cdot b^{2}(-A)^{r} . \tag{1.35}
\end{equation*}
$$

Since $3^{2 r-2} \geq r(2 r-1)$ for $r \geq 1$, this right-hand side is divisible at least by $3^{2 S+t}$ if ( $3, A$ ) $=1$, so from (1.34) we get

$$
\begin{equation*}
2^{m(p-1)} \equiv 1\left(\bmod 3^{2 s+t}\right) \tag{1.36}
\end{equation*}
$$

Since 2 is a primitive root of $3^{2 s+t}$, therefore $\phi\left(3^{2 s+t}\right) \mid m(p-1)$ which implies that $3^{2 s+t-1} \mid 2 \cdot 3^{k} m^{\prime} \cdot 3^{t} p^{\prime}$, hence $3^{2 s-k-1} \mid m^{\prime} p^{\prime}$. But $\left(3, m^{\prime}\right)=\left(3, p^{\prime}\right)=1$, so $2 s-k-1=0$ which implies that $k$ is odd.

Now if $3 \mid A$, then the right-hand side in (1.34) is divisible at least by $3^{2 s+t+1}$ and as above we get $k=2 s$, implying $k$ even.

We are unable to solve (1.1) completely when $p=7$, but as a special case we prove the following theorem.

Theorem 1.16. The Diophantine equation (1.1), where $(7, h)=1$, has no solution in $x$ odd when $p=7, A \equiv 1(\bmod 12)$, and $m=3^{2 k} \cdot m^{\prime}$, where $k \geq 1,\left(3, m^{\prime}\right)=1$.

Proof. Here $p=7$, so from Theorem 1.1(iii) we get $A \equiv 1(\bmod 4)$. Put $p=7$ in (1.16), then

$$
\begin{equation*}
1=2^{6 m}-21 A b^{2} 2^{4 m}+35 A^{2} b^{4} 2^{2 m}-7 A^{3} b^{6} . \tag{1.37}
\end{equation*}
$$

If $3 \mid b$ in (1.37) then from Theorem 1.15(1), this equation has no solution. So $(3, b)=1$, and then considering (1.37) modulo 3 we get

$$
\begin{equation*}
2 A^{2}-A^{3} \equiv 0(\bmod 3) \tag{1.38}
\end{equation*}
$$

which is not true since $A \equiv 1(\bmod 3)$.
Theorem 1.17. If $(3, m)=1$, then the Diophantine equation (1.1), where $(p, h)=1$ has no solution in $x$ odd when $A \equiv 1(\bmod 24)$.

Proof. The case $m=1$, the Diophantine equation (1.1) has no solution [5]. Let $m \geq 2$, since $A \equiv 1(\bmod 8)$ then from Corollary $1.10, p=7+8 H$. Since $(3, m)=1$, then from Theorem $1.15,(3, b)=1$ so $b^{2} \equiv 1(\bmod 3)$. Considering (1.16) modulo 3, where $A \equiv 1(\bmod 3)$ we get

$$
\begin{equation*}
1 \equiv \sum_{r=0}^{(p-1) / 2}\binom{p}{2 r}(-1)^{r}(\bmod 3) \equiv \frac{(1+i)^{p}+(1-i)^{p}}{2}(\bmod 3) . \tag{1.39}
\end{equation*}
$$

But $(1 \pm i)^{8} \equiv 1(\bmod 3)$, so (1.39) implies that

$$
\begin{align*}
1 & \equiv \frac{\left\{(1+i)^{8(1+H)}(1-i)+(1-i)^{8(1+H)}(1+i)\right\}}{2(1+i)(1-i)}(\bmod 3) \\
& \equiv 4^{1+H} \times \frac{1}{2}(\bmod 3)  \tag{1.40}\\
& \equiv 2(\bmod 3)
\end{align*}
$$

which is a contradiction.
Example 1.18. Consider the Diophantine equation $73 x^{2}+2^{14}=y^{p}$.
Here $m=7, A=73, h=4$ so from Theorem 1.17, this equation has no solution in $x$ odd. If $x$ is even then it is sufficient to consider the equation

$$
\begin{equation*}
73 X^{2}+2^{2(7-u)}=Y^{p} \tag{1.41}
\end{equation*}
$$

where $x=2^{u} X, y=2^{v} \cdot Y, 7>u>0, v>0,(2, X)=(2, Y)=1$, and $2 u=p v$. If $(7-u, 3)=1$, then (1.41) has no solution from Theorem 1.17. If $3 \mid 7-u$ then $u=1$ or 4 , which is not possible since $2 u=p v$. So the given equation has no solution in integers.

Acknowledgement. The author would like to thank the referee for his valuable suggestions.

## REFERENCES

[1] S. A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^{2}+2^{k}=y^{n}$, Int. J. Math. Math. Sci. 20 (1997), no. 2, 299-304. MR 98b:11032. Zbl 881.11038.
[2] E. Brown, Diophantine equations of the form $a x^{2}+D b^{2}=y^{p}$, J. Reine Angew. Math. 291 (1977), 118-127. MR 55\#12631. Zbl 338.10018.
[3] J. H. E. Cohn, The Diophantine equation $x^{2}+C=y^{n}$, Acta Arith. 65 (1993), no. 4, 367-381. MR 94k:11037. Zbl 795.11016.
[4] W. Ljunggren, Über die Gleichungen $1+D x^{2}=2 y^{n}$ und $1+D x^{2}=4 y^{n}$, Norske Vid. Selsk. Forh. (Trondhjem) 15 (1943), no. 30, 115-118 (German). MR 8,442g. Zbl 028.34604.
[5] T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, Nova Acta Soc. Sci. Upsal. (4) 16 (1954), no. 2, 38 pp. MR 17,13b. Zbl 057.28304.

Fadwa S. Abu Muriefah: Girls College of Education, Science Sections (Mathematics), Sitten Street, Al Malaz, P.O. Box 27104, Riyadh, Saudi Arabia

E-mail address: abumuriefah@yahoo.com

