ON THE DIOPHANTINE EQUATION \( x^2 + p^{2k+1} = 4y^n \)

S. AKHTAR ARIF and AMAL S. AL-ALI

Received 12 June 2001

It has been proved that if \( p \) is an odd prime, \( y > 1, k \geq 0, n \) is an integer greater than or equal to 4, \( (n, 3h) = 1 \) where \( h \) is the class number of the field \( \mathbb{Q}(\sqrt{-p}) \), then the equation \( x^2 + p^{2k+1} = 4y^n \) has exactly five families of solution in the positive integers \( x, y \). It is further proved that when \( n = 3 \) and \( p = 3a^2 \pm 4 \), then it has a unique solution \( k = 0, y = a^2 \pm 1 \).

2000 Mathematics Subject Classification: 11D61.

1. Introduction. The purpose of this note is to compute positive integral solutions of the equation \( x^2 + p^{2k+1} = 4y^n \), where \( p \) is an odd prime and \( n \) is any integer greater than or equal to 3. The special case when \( p = 3 \) and \( k = 0 \) was treated by Nagell [7] and Ljunggren [3] who proved that this equation has the only solutions \( y = 1 \) and \( y = 7 \) with \( n = 3 \). Later on, Ljungren [4, 5], Persson [8], and Stolt [9] studied the general equation \( x^2 + D = 4y^n \) and proved that it has a solution under certain necessary conditions on \( D \). Le [2] and Mignotte [6] proved that the equation \( D_1x^2 + D_2^m = 4y^n \) has a finite number of solutions under certain conditions on \( m \) and \( n \) but did not compute these solutions. We will prove the following theorem.

**Theorem 1.1.** The Diophantine equation

\[
x^2 + p^{2k+1} = 4y^n, \quad y > 1,
\]

where \( p \) is an odd prime, \( k \geq 0, n \) is an integer greater than or equal to 4, \( (n, 3h) = 1 \), where \( h \) is the class number of the field \( \mathbb{Q}(\sqrt{-p}) \) has exactly five families of solutions given in Table 1.1.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( n )</th>
<th>( k )</th>
<th>( x )</th>
<th>( y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>5</td>
<td>5M</td>
<td>( 11 \cdot 7^{5M} )</td>
<td>( 2 \cdot 7^{2M} )</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
<td>13M</td>
<td>( 181 \cdot 7^{13M} )</td>
<td>( 2 \cdot 7^{2M} )</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>( 7M + 1 )</td>
<td>( 13 \cdot 7^{7M} )</td>
<td>( 2 \cdot 7^{2M} )</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>5M</td>
<td>( 31 \cdot 11^{5M} )</td>
<td>( 3 \cdot 11^{2M} )</td>
</tr>
<tr>
<td>19</td>
<td>7</td>
<td>( 7M )</td>
<td>( 559 \cdot 19^{7M} )</td>
<td>( 5 \cdot 19^{2M} )</td>
</tr>
</tbody>
</table>

We start by the usual method of factorizing in the field \( \mathbb{Q}(\sqrt{-p}) \), then we use a recent result of Bilu et al. [1], about primitive divisors of a Lucas number.

We start by giving some important definitions.
**Definition 1.2.** A Lucas pair is a pair \((\alpha, \beta)\) of algebraic integers, such that \(\alpha + \beta\) and \(\alpha \beta\) are nonzero coprime rational integers and \(\alpha / \beta\) is not a root of unity. Given a Lucas pair \((\alpha, \beta)\), we define the corresponding sequence of Lucas numbers by 
\[ u_n(\alpha, \beta) = (\alpha^n - \beta^n) / (\alpha - \beta) \] (where \(n = 0, 1, 2, \ldots\)).

A prime number \(p\) is a primitive divisor of \(u_n(\alpha, \beta)\) if \(p\) divides \(u_n\), but does not divide \((\alpha - \beta)^2 u_1 u_2 \cdots u_{n-1}\).

The following result has been proved in [1].

**Lemma 1.3.** For \(n > 30\), the \(n\)th term of any Lucas sequence has a primitive divisor.

Also in [1], for \(5 \leq n \leq 30\), all values of the pairs \((\alpha, \beta)\) have been listed for which the \(n\)th term of the Lucas sequence \(u_n(\alpha, \beta)\) has no primitive divisors.

We first consider the case when \((p, x) = 1\) and prove the following theorem.

**Theorem 1.4.** Equation (1.1), where \(n\) and \(p\) satisfy the conditions of Theorem 1.1, has no solution in the positive integers \(x\) when \((p, x) = 1\) except when \(p = 7, 11, \text{ or } 19\).

**Proof.** First suppose that \(n\) is an odd integer. Without loss of generality, we can suppose that \(n\) is an odd prime. Factorizing (1.1), we obtain

\[
\left( \frac{x + p^k \sqrt{-p}}{2} \right) \cdot \left( \frac{x-p^k \sqrt{-p}}{2} \right) = y^n.
\]

(1.2)

We can easily verify that the two numbers on the left-hand side are relatively prime integers in \(Q(\sqrt{-p})\). So that

\[
\frac{x + p^k \sqrt{-p}}{2} = \left( \frac{a + b \sqrt{-p}}{2} \right)^n,
\]

(1.3)

where \(a\) and \(b\) are rational integers such that \(a \equiv b \pmod{2}\) and \(4y = a^2 + pb^2\), where \((a, pb) = 1\).

Let

\[
\alpha = \frac{a + b \sqrt{-p}}{2}, \quad \bar{\alpha} = \frac{a - b \sqrt{-p}}{2}.
\]

(1.4)

Then from (1.3), we get

\[
\frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}} = \frac{p^k}{b}.
\]

(1.5)

By equating imaginary parts in (1.3), we can easily conclude from (1.5) that

\[
\frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}} = \begin{cases} 
\pm 1 & \text{if } (p, n) = 1, \\
\pm p & \text{if } n \mid p.
\end{cases}
\]

(1.6)

It can be verified that \((\alpha, \bar{\alpha})\) is a Lucas pair as defined earlier and the only positive prime divisor of the corresponding \(n\)th Lucas number

\[
u_n = \frac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}}
\]

(1.7)
is \( p \) which is not a primitive divisor because it divides \((\alpha - \bar{\alpha})^2 = pb^2\). So the Lucas number defined in (1.7) has no primitive divisors. Using Lemma 1.3 and [1, Table 2], we deduce that (1.1) has no solutions when \( n > 13 \). When \( 5 \leq n \leq 13 \), again using [1, Table 2], we find all values of \( \alpha \) for which the Lucas number \( u_n(\alpha, \beta) \) has no primitive divisors. We consider each value of \( n \) separately.

When \( n = 13 \), then \( \alpha = (1 + \sqrt{-7})/2 \) which correspondingly gives \( k = 0, a = 1, b = 1, p = 7 \) and consequently, \( y = (a^2 + pb^2)/4 = 2, x = 181 \) is the only solution of the equation \( x^2 + p^{2k+1} = 4y^{13} \).

When \( n = 11 \), there is no \( \alpha \) for which \( u_{11}(\alpha, \bar{\alpha}) \) has no primitive divisors and so no solution of (1.1).

When \( n = 7 \), the values of \( \alpha \) for which \( u_7(\alpha, \bar{\alpha}) \) has no primitive divisors, are \( \alpha = (1 + \sqrt{-7})/2, (1 + \sqrt{-19})/2 \) which give \( y = 2 \) as a solution of \( x^2 + 7^3 = 4y^7 \) (\( x = 13 \)) and \( y = 5 \) as a solution of \( x^2 + 19 = 4y^7 \) (\( x = 559 \)). Similarly, for \( n = 5 \), we get \( y = 2 \) as a solution of \( x^2 + 7 = 4y^5 \) (\( x = 11 \)) and \( y = 3 \) as a solution of \( x^2 + 11 = 4y^5 \) (\( x = 31 \)).

Now we will prove that there is no solution for (1.1) when \( n \) is even. It suffices to consider that \( n = 4 \).

Factorizing \( x^2 + p^{2k+1} = 4y^4 \), we get
\[
(2y^2 + x) \cdot (2y^2 - x) = p^{2k+1}.
\] (1.8)

Since \((p, x) = (p, y) = 1\), then
\[
2y^2 + x = p^{2k+1}, \quad 2y^2 - x = 1
\] (1.9)
which gives \( 4y^2 = p^{2k+1} + 1 \). This can easily be checked to have no solution with \( y > 1 \).

**Proof of Theorem 1.1.** Suppose that \( p \mid x \). Let \( x = p^\lambda x_1, \ y = p^\mu y_1 \), where \((x_1, p) = (y_1, p) = 1 \) and \( \lambda, \mu \geq 1 \). Substituting in (1.1), we get
\[
p^{2\lambda} \cdot x_1^2 + p^{2k+1} = 4p^{n\mu} \cdot y_1^n.
\] (1.10)

We have the following three cases.

**Case 1.** If \( 2\lambda = \min(2\lambda, 2k+1, n\mu) \), then
\[
x_1^2 + p^{2k-2\lambda+1} = 4p^{n\mu-2\lambda} \cdot y_1^n.
\] (1.11)

This equation is impossible modulo \( p \) unless \( n\mu - 2\lambda = 0 \), and then we get \( x_1^2 + p^{2(k-\lambda)+1} = 4y_1^n \), where \((x_1, p) = (y_1, p) = 1 \). According to Theorem 1.4, this equation has no solution for all \( n \geq 4 \) except when \( n = 13, 7, 5, k = \lambda \), and \( n = 7, k = \lambda + 1 \).

Accordingly, when \( n = 13 \), we have \( 13\mu = 2\lambda \), then \( \lambda = 13\mu, \mu = 2M \) and so the solutions of (1.1) are \( p = 7, x = 181 \cdot 7^{13\mu}, \ y = 2 \cdot 7^{2M} \). Similarly, considering \( n = 5, 7 \), we get exactly the families of solutions given in the statement of Theorem 1.1.

**Case 2.** If \( 2k+1 = \min(2\lambda, 2k+1, n\mu) \), then
\[
p^{2\lambda-2k-1} \cdot x_1^2 + 1 = 4p^{n\mu-2k-1} \cdot y_1^n.
\] (1.12)

This equation is known to have no solution [7].
Case 3. If \( n \mu = \min(2\lambda, 2k + 1, n\mu) \), then
\[
p^{2\lambda - n\mu} \cdot x_1^2 + p^{2k+1-n\mu} = 4y_1^n. \tag{1.13}
\]
This equation is possible only if \( 2\lambda - n\mu = 0 \) or \( 2k + 1 - n\mu = 0 \). If \( 2\lambda - n\mu = 0 \), we get \( x_1^2 + p^{2(k-\lambda)+1} = 4y_1^n \), which is an equation of the same form as considered in Case 1.

If \( 2k + 1 - n\mu = 0 \), we get \( p(p^{\lambda-k-1} \cdot x_1)^2 + 1 = 4y_1^n \), which is known to have no solution [6]. This completes the proof of Theorem 1.1.

Note 1.5. When \( n = 3 \), factorizing (1.1), we get
\[
\frac{x + 3^k \sqrt{-3}}{2} = \varepsilon \left( \frac{a + b \sqrt{-3}}{2} \right)^3, \tag{1.14}
\]
\[
\frac{x + p^k \sqrt{-p}}{2} = \left( \frac{a + b \sqrt{-p}}{2} \right)^3, \quad p \neq 3, \tag{1.15}
\]
where \( \varepsilon = \omega \) or \( \omega^2 \) and \( \omega \) is a cube root of unity. From (1.14), we easily deduce that \( k = 0 \) and \( y = 1 \) and 7 are the only solutions as proved in [3]. We treat (1.15) by the same way as before by taking \( \alpha = (a + b \sqrt{-p})/2 \) and \( \bar{\alpha} = (a - b \sqrt{-p})/2 \), so we get \( (\alpha^3 - \bar{\alpha^3})/(\alpha - \bar{\alpha}) = \pm 1 \). It can be easily proved that \((\alpha, \bar{\alpha})\) is a Lucas pair as defined above. Using [1, Table 2], we find the following two values of \( \alpha \) for which the Lucas number \( u_3(\alpha, \bar{\alpha}) \) has no primitive divisors:
\[
\alpha = \begin{cases} 
  \frac{m + \sqrt{4 - 3m^2}}{2}, & m > 1, \\
  \frac{m + \sqrt{4 \cdot 3^k - 3m^2}}{2}, & m \not\equiv 0 \pmod{3},
\end{cases} \tag{1.16}
\]
where \((k, m) \neq (1, 2)\).

The first value of \( \alpha \) gives \( b = 1, k = 0 \) and consequently, \( p = 3a^2 \pm 4, y = a^2 \pm 1 \), and \( x = a(2a^2 \pm 3) \) is the solution of (1.1) with \( n = 3 \). No solution is found for the second value of \( \alpha \) since \( p \neq 3 \). Hence, we have the following theorem.

Theorem 1.6. The Diophantine equation
\[
x^2 + p^{2k+1} = 4y^3, \quad (p, x) = 1 \tag{1.17}
\]
has the only solutions \( k = 0 \) and \( y = 1 \) and 7 when \( p = 3 \). When \( p \) is a prime greater than 3, such that \((3, h) = 1\), where \( h \) is the class number of the field \( Q(\sqrt{-p}) \), then it has solutions only if \( p = 3a^2 \pm 4 \), and then the solution is \( k = 0, y = a^2 \pm 1, \) and \( x = a(2a^2 \pm 3) \).

References

ON THE DIOPHANTINE EQUATION $x^2 + p^{2k+1} = 4y^n$


S. AKHTAR ARIF: DEPARTMENT OF MATHEMATICS, GIRLS COLLEGE OF EDUCATION, P.O. BOX 22171, RIYADH 11495, SAUDI ARABIA
E-mail address: sarif5@hotmail.com

AMAL S. AL-ALI: DEPARTMENT OF MATHEMATICS, GIRLS COLLEGE OF EDUCATION, P.O. BOX 56778, RIYADH 11564, SAUDI ARABIA
E-mail address: amal1422h@yahoo.com