THE DIOPHANTINE EQUATION $x^2 + D = p^n$

RONALD ALTER AND K. K. KUBOTA
THE DIOPHANTINE EQUATION $x^2 + D = p^n$

RONALD ALTER AND K. K. KUBOTA

Let $D \equiv 3 \pmod{4}$ be a positive square free integer greater than 3 which is not a multiple of the odd prime $p$. If $d$ is the order of a prime ideal divisor of $(p)$ in the class group of the quadratic field $Q(\sqrt{-D})$, then in order for the diophantine equation $x^2 + D = p^n$ to have a solution in integers, it is necessary and sufficient that $(-D/p) = 1$ and that either (i) $4p^d - D$ be a square and $3p^d - D = \pm 2$ or (ii) $p^d - D$ be a square. Conditions which guarantee the uniqueness of the solution are given. A linear recurrence is used in the proof.

It is the purpose of this paper to examine the solvability in positive rational integers $x$ and $n$ of the equation

$$(1) \quad x^2 + D = p^n,$$

where $D \equiv 3 \pmod{4}$ is a positive square free integer.

Apéry [2] showed that if $p \nmid D$, equation (1) can have at most two solutions. Special cases of this equation have been considered by others. E. L. Cohen has shown in his thesis [3] that even when $D$ is not square free, equation (1) has no solutions if $p = (D + 1)/4$, where $D \geq 19$ satisfies $D \equiv 3 \pmod{8}$. The authors [1] have completed this result by showing that the equation

$$x^2 + 11 = 3^n$$

has the unique solution $(x, n) = (4, 3)$. The present paper generalizes these results by proving necessary and sufficient conditions for the solvability of equation (1) and by showing, at least in certain cases, that the solution is unique. Since the case $D = 3$ is treated in Cohen [3] it will not be discussed here, thus it shall be assumed throughout that $D > 3$. In particular, it will be shown that when $D$ is square free and $D \equiv 3$ modulo 8, then the equation has at most one solution. The proof is similar to parts of Skolem, Chowla, and Lewis's treatment [5] of Ramanujan's equation $x^2 + 7 = 2^n$. (For a more thorough discussion of this last equation the reader is referred to Hasse [4].)

First note that one can reduce to the case where $(D, p) = 1$. In fact, suppose $D = D'p^r$ where $(D', p) = 1$. There are no solutions when $n < r$. Indeed, if $(x, n)$ were such a solution, then $p^n | x^2$ and so

$$x^2/p^n + D'p^{r-n} = 1$$
which contradicts $D' > 0$. If $n \geq r$, let $k = \lceil r/2 \rceil$ so that $p^{2k} \mid x^2$ and

$$
(2) \quad (x/p^k)^2 + D'p^{r-2k} = p^{n-2k}.
$$

When $r$ is even, $r = 2k$ and so the solutions are in one-to-one correspondence with those of $y^2 + D' = p^m$ which was to be established. When $r$ is odd, equation (2) implies that there are no solutions with $n - 2k > 1$. In fact, if there were, then $p \mid (x/p^k)$ and so

$$
p^2 \mid D'p^{r-2k} = D'p
$$

which is absurd. Since $r - 2k = 1 > 0$, there are no solutions with $n - 2k = 0$. If there is a solution, then it follows that $n - 2k = 1$. But then equation (2) reads $(x/p^k)^2 + D'p = p$ and therefore $D' = 1$ and $x = 0$. Hence $D = p^{2k+1}$ and there is only the trivial solution $(x, n) = (0, 2k + 1)$.

Henceforth it will be assumed that $(D, p) = 1$. If $(x, n)$ is a solution to equation (1), then this equation can be factored as

$$
(3) \quad (x + \sqrt{-D})(x - \sqrt{-D}) = p^n
$$
in the ring of integers $\mathcal{O}$ of the quadratic field $\mathbb{Q}(\sqrt{-D})$. Any prime ideal of this ring which contains both

$$
x + \sqrt{-D} \quad \text{and} \quad x - \sqrt{-D}
$$
must also contain $2x$, $2\sqrt{-D}$, $p^n$ and so also $p$, $\sqrt{-D}$, and $-D$. Since $(D, p) = 1$, we have a contradiction and so

$$
(x + \sqrt{-D}) \quad \text{and} \quad (x - \sqrt{-D})
$$
are relatively prime ideals. Clearly neither is the whole ring. Now, if $(p)$ were prime in $\mathcal{O}$, then

$$
(x + \sqrt{-D})(x - \sqrt{-D}) = (p)^n
$$
contradicts unique factorization of ideals in $\mathcal{O}$. From the theory of quadratic fields it follows that $(-D/p) = 1$ and $(p) = \mathfrak{y}\mathfrak{y}'$ where $\mathfrak{y}$ and $\mathfrak{y}'$ are distinct conjugate prime ideals.

Equation (3) leads to the equation of ideals:

$$
(x + \sqrt{-D})(x - \sqrt{-D}) = \mathfrak{y}_n^s\mathfrak{y}'^s.
$$

Since the factors on the left are relatively prime, we have either $(x + \sqrt{-D}) = \mathfrak{y}_n^s$ or $\mathfrak{y}'^s$. Fixing the notation so the first is true, it follows that $\mathfrak{y}_n^s$ is a principal ideal and so $n = dm$ for some $m$ where $d$ is the order of $\mathfrak{y}$ in the class group of $\mathcal{O}$. By definition, $\mathfrak{y}_n^d$ is principal, say
(4) \[ y^d = \left(\frac{a + b\sqrt{-D}}{2}\right) \]

where \(a\) and \(b\) are integers with \(b \geq 0\). Thus

\[ (x + \sqrt{-D}) = y^{m^d} = \left(\frac{a + b\sqrt{-D}}{2}\right)^m. \]

Since the only units of \(\mathcal{O}\) are \(\pm 1\), it follows that

(5) \[ x + \sqrt{-D} = \pm \left(\frac{a + b\sqrt{-D}}{2}\right)^m. \]

It is easy to verify that the \(d_k = (2/\sqrt{D}) \text{Im} ((a + b\sqrt{-D})/2)^k\) satisfy the linear recurrence:

(6) \[ d_{k+2} = ad_{k+1} - p^d \cdot d_k \]

with \(d_0 = 0\) and \(d_1 = b\). An easy induction on \(s\) using equation (6) shows that the \(d_k\) satisfy

(7) \[ d_1 d_{k+s} = d_{k+1} d_s - p^d d_k d_{s-1}. \]

From equation (6), it follows that \(d_1 | d_r\) for all \(r > 0\) and a simple induction on \(r\) involving equation (7) shows that \(d_k | d_{kr}\) for all \(k, r \geq 1\). Now equation (5) together with the definition of the \(d_k\) imply that \(d_m = \pm 2\). Since \(b = d_1 | d_m, b\) is either 1 or 2.

It has been shown that a necessary condition for the solvability of equation (1) in the case \((D, p) = 1\) is that \((-D/p) = 1\) and that \(b = 1\) or 2. In each of the cases \(b = 1\) and \(b = 2\), we will now try to prove uniqueness of the solutions.

Suppose first that \(b = 1\). Since \((a + b\sqrt{-D})/2 = (a + \sqrt{-D})/2\) is an integer, \(a\) must be odd. By equation (7),

\[ d_{s+3} = d_s d_s - p^d d_s d_{s-1} \]
\[ = (a^s - 2ap^s)d_s - p^d(a^s - p^s)d_{s-1} \]
\[ \equiv d_s \pmod{2}. \]

Clearly \(d_1 = 1\) and \(d_2 = a\) are odd and \(d_3 = a^2 - p^s\) is even. Recalling that \(d_m = \pm 2\), it follows that \(3 | m\) and thus \(d_3 = \pm 2\) since \(d_3 | d_m\).

Note that since \(p^d = (a^2 + D)/4, d_2 = a^2 - p^d = \pm 2\) is equivalent to \(3p^d - D = \pm 2\). In the case of \(b = 1\), this last condition is therefore necessary and sufficient for solvability of equation (1).

Still supposing that \(b = 1\), a technique from [5] can be used to show that \(d_{3k} \neq \pm 2\) for any \(k > 1\). Let \(\xi = ((a + \sqrt{-D})/2)^k = e + fi\) and \(\xi^* = e - fi\) be the complex conjugate of \(\xi\). By definition
\[ \frac{\xi^2 - \xi'^2}{\sqrt{-D}} = \frac{(\xi - \xi')(\xi^2 + \xi\xi' + \xi'^2)}{\sqrt{-D}} = \pm 2. \]

Now \( |\xi - \xi'| \geq 1 \) and \( |\xi^2 + \xi\xi' + \xi'^2| \geq 1 \) since these are integers in \( \mathcal{O} \). So \( |\xi - \xi'| \leq 2\sqrt{D} \) and \( |\xi^2 + \xi\xi' + \xi'^2| \leq 2\sqrt{D} \). The first inequality says \( |f| \leq \sqrt{D} \) and the second says that \( |3e^2 - f^2| \leq 2\sqrt{D} \). Hence

\[
e^2 \leq \frac{2\sqrt{D} + f^2}{3} \leq \frac{2\sqrt{D} + D}{3},
\]

and so

\[
p^{2k} = \xi^k \xi' = e^2 + f^2 \leq \frac{4}{3} D + \frac{2}{3} \sqrt{D}.
\]

Now \( D = 3p^d + 2 \leq 3p^d + 2 \) and so

\[
p^{2k} \leq \frac{4}{3} (3p^d + 2) + \frac{2}{3} \sqrt{3p^d + 2} \leq 5p^d + 3.
\]

It follows that \( k = 2 \). But if \( k = 2 \), by equation (7), \( d_0 = d_3 (a^3 - 3p^d a) = \pm 2a(a^2 - 3p^d) \). If \( d_0 = \pm 2 \), we would have \( a = \pm 1 \) and \( 1 - 3p^d = \pm 1 \) which is absurd.

Note that the condition that \( D \) be square free was necessary only to assure that \( \mathcal{O}^d \) could be expressed as in equation (4). But if \( p = (D + 1)/2 = (1 + \sqrt{-D})/2 \cdot (1 - \sqrt{-D})/2 \), then we have equation (4) satisfied with \( a = b = d = 1 \). In order for this to have a solution, we need \( \pm 2 = d_3 = a^2 - p^d = 1 - p \). So \( p = 3 \) and the solution is unique. Thus previously mentioned results of E. L. Cohen [3] and the authors [1] are reproved.

Now suppose \( b = 2 \). Since \( (a + b\sqrt{-D})/2 = a/2 + \sqrt{-D} \) is an integer which is not a multiple of 2, \( a \equiv 0 \pmod{4} \). All of the \( d_k \) are even; so we may consider the sequence \( a_k = d_k/2 \) which clearly satisfies the same linear recurrence relation as do the \( d_k \). The uniqueness proof depends on the following simple congruences.

**Lemma.**

(i) If \( 2^r \mid a \) and \( 2^k \mid n \) with \( k \geq 1 \), then

\[
a_n \equiv 0 \pmod{2^{k+r-1}}.
\]

(ii) If \( 2^r \mid a \) and \( 2^k \mid n - 1 \) with \( k \geq 1 \), then

\[
a_n \equiv (-1)^{(n-1)/2}p^{(n-1)/2}a_{2^k} \pmod{2^{k+2r-2}}.
\]

**Proof.**

(i) Since \( a_n \) is a multiple of \( a_{2^k} \), it suffices to prove part (i) for \( n = 2^k \). When \( k = 1 \), \( a_2 = a \equiv 0 \pmod{2^2} \). Now
THE DIOPHANTINE EQUATION \( x^a - D = v \)

by equation (7). Since \( p^d \) is odd and

\[ a_{2k+1} = a_{2k+2k} = a_{2k} \left( a_{2k+1} - p^d a_{2k-1} \right) \]

by equation (6), the result for \( n = 2^{k+1} \) follows by induction from
that for \( n = 2^k \). The first assertion is proved.

(ii) First suppose \( k = 1 \) so that \( n = 4s + 3 \). \( a_5 = a_2 - p^d \equiv -p^d \)
(mod \( 2^{2r} \)). By equation (7),

\[ a_{4k+7} = a_{4k+3} a_5 - p^d a_4 a_{4k+2} \cdot \]

Since \( a_5 = a^4 - 3p^d a^2 + p^d \) and \( a^4 = a^5 - 2p^d \), we have \( a_{4k+7} \equiv p^d a_{4k+3} \)
(mod \( 2^{2r} \)) as desired.

In general, suppose \( n = 2m + 1 \) where \( 2^k \| n - 1 \). Then \( 2^{k-1} \| m \)
and so by the induction hypothesis, \( a_{m+1} = (a/2)^{m/2} p^{md/2} \) (mod \( 2^{k+2r-2} \)) and so \( (a_{m+1})^2 \equiv (-1)^m p^{md} \) (mod \( 2^{k+2r-2} \)). By part (i) of the lemma,
\( a_m \equiv 0 \) (mod \( 2^{k+1-r-1} \)), and so \( a_{2m} \equiv 0 \) (mod \( 2^{k+2r-i} \)) which implies a
fortiori that \( a_{2m}^2 \equiv 0 \) (mod \( 2^{k+2r-2} \)) since \( k \geq 2 \). By equation (7),

\[ a_{2m+1} = a_{m+1} - p^d a_m^2 \equiv (-1)^m p^{md} \) (mod \( 2^{k+2r-2} \))
as desired. This completes the proof of the lemma.

COROLLARY. If \( n \geq 3 \) is odd, \( 2^r \| a, 2^k \| n - 1, p \equiv 2^t - 1 \)
(mod \( 2^{t+1} \), and \( 2r - 2 \geq t \), then \( a_n \equiv 1 + 2^{t-1} \) (mod \( 2^{k+t} \)). In particular, \( a_n \not\equiv \pm 1 \) for \( n > 1 \) if \( 2(r - 1) \geq t \).

Proof. This follows from part (ii) of the lemma and the fact that if \( p \equiv 2^t - 1 \) (mod \( 2^{t+1} \), \( f \) is odd, and \( s \geq 1 \), then

\[ p^{2s} \equiv 1 + 2^{t+s} \) (mod \( 2^{t+s+1} \)).

To complete the argument, we need only find the values of \( p \)
and \( D \) which are not covered by the corollary. If \( 2r - 2 < t \), then
\( 2r \leq t + 1 \). Since \( (p) = 2^{2s} \), equation (4) implies that \( p^d = (a/2)^2 + D \).
On the other hand, \( 2^r \| a \) implies \( (a/2)^2 \equiv 2^{2r-2} \) (mod \( 2^{2r+1} \)). From these
results and the fact that \( p \equiv 2^t - 1 \) (mod \( 2^{t+1} \), one concludes that
\( D \equiv 2^t - 2^{2r-2} - 1 \) (mod \( 2^{2r} \)). Thus the exceptional cases occur when

\[ \begin{align*}
\begin{cases}
p \equiv 2^t - 1 \ (\text{mod } 2^{t+1}) \\
D \equiv 2^t - 2^{2(r-1)} - 1 \text{ (mod } 2^{2r}) \quad \text{for } r \leq \frac{t+1}{2}.
\end{cases}
\end{align*}
\]

For example, this formula yields the following exceptional cases
for \( t = 2, 3, 4, 5 \).
\[ p \equiv 3 \pmod{8} \quad \text{none} \]
\[ p \equiv 7 \pmod{16} \quad D \equiv 3 \pmod{16} \]
\[ p \equiv 15 \pmod{32} \quad D \equiv 11 \pmod{16} \]
\[ p \equiv 31 \pmod{64} \quad D \equiv 11 \pmod{16} \text{ or } D \equiv 15 \pmod{64} \]

Since \( b = 1, 2 \) mean respectively that \( 4p^d - D, p^d - D \) are squares, the results may be summarized as follows.

**Theorem.** Let \( D \equiv 3 \pmod{4} \) be a positive square free integer \( \neq 3 \), \( p \) be an odd prime which does not divide \( D \), and \( d \) be the order of a prime ideal divisor of \( (p) \) in the class group of the quadratic field \( \mathbb{Q}(\sqrt{-D}) \). In order for
\[ x^2 + D = p^n, \quad x \geq 0, \quad n \geq 0 \]
to have a solution in integers, it is necessary and sufficient that \((-D/P) = 1\) and that one of the following mutually exclusive conditions hold:

(i) \( 4p^d - D \) is a square and \( 3p^d - D = \pm 2 \),

(ii) \( p^d - D \) is a square.

In case (i), \( n = 3d \) is the unique solution. In case (ii), \( n = d \) is a solution and this solution is unique except possibly in the exceptional cases, given in equation (8), where there are at most two solutions.

**References**


Received January 18, 1972.

University of Kentucky
Allan Francis Abrahamse, **Uniform integrability of derivatives on σ-lattices** ........................................... 1

Ronald Alter and K. K. Kubota, **The diophantine equation** \( x^2 + D = p^n \) ........ 11

Grahame Bennett, **Some inclusion theorems for sequence spaces** ......................... 17

William Cutler, **On extending isotopies** ................................................................. 31

Robert Jay Daverman, **Factored codimension one cells in Euclidean n-space** ........... 37

Patrick Barry Eberlein and Barrett O’Neill, **Visibility manifolds** ......................... 45

M. Edelstein, **Concerning dentability** ................................................................. 111

Edward Graham Evans, Jr., **Krull-Schmidt and cancellation over local rings** .......... 115

C. D. Feustel, **A generalization of Kneser’s conjecture** ....................................... 123

Avner Friedman, **Uniqueness for the Cauchy problem for degenerate parabolic equations** ................................................................. 131

David Golber, **The cohomological description of a torus action** ............................ 149

Alain Goullet de Rugy, **Un théorème du genre “Andô-Edwards” pour les Fréchet ordonnés normaux** ................................................................. 155

Louise Hay, **The class of recursively enumerable subsets of a recursively enumerable set** ................................................................. 167

John Paul Helm, Albert Ronald da Silva Meyer and Paul Ruel Young, **On orders of translations and enumerations** ........................................... 185

Julien O. Hennefeld, **A decomposition for** \( B(X)^\ast \) **and unique Hahn-Banach extensions** ................................................................. 197

Gordon G. Johnson, **Moment sequences in Hilbert space** ...................................... 201

Thomas Rollin Kramer, **A note on countably subparacompact spaces** .................... 209

Yves A. Lequain, **Differential simplicity and extensions of a derivation** ................... 215

Peter Lorimer, **A property of the groups** \( \text{Aut PU}(3, q^2) \) ............................... 225

Yasou Matsugu, **The Levi problem for a product manifold** .................................. 231

John M.F. O’Connell, **Real parts of uniform algebras** ......................................... 235

William Lindall Paschke, **A factorable Banach algebra without bounded approximate unit** ................................................................. 249

Ronald Joel Rudman, **On the fundamental unit of a purely cubic field** ..................... 253

Tsun Wu Ting, **Torsional rigidities in the elastic-plastic torsion of simply connected cylindrical bars** ................................................................. 257

Philip C. Tonne, **Matrix representations for linear transformations on analytic sequences** ................................................................. 269

Jung-Hsien Tsai, **On E-compact spaces and generalizations of perfect mappings** ........ 275

Alfons Van Daele, **The upper envelope of invariant functionals majorized by an invariant weight** ................................................................. 283

Giulio Varsi, **The multidimensional content of the frustum of the simplex** ............ 303