PACIFIC JOURNAL OF MATHEMATICS
Vol. 46, No. 1, 1973

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

$$x^2 + D = p^n , \tag{1}$$

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 $D \geqq 19$ 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 $p^n \mid x^2$ and so

$$x^2/p^n + D'p^{r-n} = 1$$

which contradicts $D' > 0$. If $n \geqq r$, let $k = [r/2]$ so that $p^{2k} \mid x^2$ and

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

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

$$(x + \sqrt{-D})(x - \sqrt{-D}) = p^n \tag{3}$$

in the ring of integers $\mathcal{O}$ of the quadratic field $Q(\sqrt{-D})$. 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 $(p) = \mathfrak{P}\mathfrak{P}'$ where $\mathfrak{P}$ and $\mathfrak{P}'$ are distinct conjugate prime ideals.

Equation (3) leads to the equation of ideals:

$$(x + \sqrt{-D})(x - \sqrt{-D}) = \mathfrak{P}^n\mathfrak{P}'^n.$$

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

$$(4) \qquad \mathfrak{P}^d = \left(\frac{a + b\sqrt{-D}}{2}\right)$$

where a and b are integers with $b \geqq 0$. Thus

$$(x + \sqrt{-D}) = \mathfrak{P}^{md} = \left(\frac{a + b\sqrt{-D}}{2}\right)^m .$$

Since the only units of $\mathcal{O}$ are ± 1, it follows that

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

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

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

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

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

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

$$\begin{aligned} d_{s+3} &= d_4 d_s - p^d d_3 d_{s-1} \\ &= (a^3 - 2ap^d)d_s - p^d(a^2 - p^d)d_{s-1} \\ &\equiv d_s \pmod 2 . \end{aligned}$$

Clearly $d_1 = 1$ and $d_2 = a$ are odd and $d_3 = a^2 - p^d$ is even. Recalling that $d_m = \pm 2$, it follows that $3 \mid m$ and thus $d_3 = \pm 2$ since $d_3 \mid d_m$. Note that since $p^d = (a^2 + D)/4$, $d_3 = a^2 - p^d = \pm 2$ 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 ξ. By definition

$$d_{3k} = \frac{\xi^3 - \xi'^3}{\sqrt{-D}} = \frac{(\xi - \xi')(\xi^2 + \xi\xi' + \xi'^2)}{\sqrt{-D}} = \pm 2 .$$

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

$$e^2 \leqq \frac{2\sqrt{D} + f^2}{3} \leqq \frac{2\sqrt{D} + D}{3} ,$$

and so

$$p^{dk} = \xi\xi' = e^2 + f^2 \leqq \frac{4}{3} D + \frac{2}{3}\sqrt{D} .$$

Now $D = 3p^d \mp 2 \leqq 3p^d + 2$ and so

$$p^{dk} \leqq \frac{4}{3}(3p^d + 2) + \frac{2}{3}\sqrt{3p^d + 2} \leqq 5p^d + 3 .$$

It follows that $k = 2$. But if $k = 2$, by equation (7), $d_6 = d_3(a^3 - 3p^d a) = \pm 2a(a^2 - 3p^d)$. If $d_6 = \pm 2$, 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 $\mathfrak{P}^d$ could be expressed as in equation (4). But if $p = (D + 1)/4 = (1 + \sqrt{-D})/2 \cdot (1 - \sqrt{-D})/2$, 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* $2^r \| a$ *and* $2^k \| n$ *with* $k \geqq 1$, *then*

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

(ii) *If* $2^r \| a$ *and* $2^k \| n - 1$ *with* $k \geqq 1$, *then*

$$a_n \equiv (-1)^{(n-1)/2} p^{(n-1)d/2} \pmod{2^{k+2r-2}} .$$

Proof. (i) Since a_n is a multiple of a_{2k}, it suffices to prove part (i) for $n = 2^k$. When $k = 1$, $a_2 = a \equiv 0 \pmod{2^r}$. Now

$$a_{2k+1} = a_{2k+2k} = a_{2k}(a_{2k+1} - p^d a_{2k-1})$$

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

$$a_{2k+1} = aa_{2k} - p^d a_{2k-1} \equiv a_{2k-1} \pmod 2$$

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 $n = 4s + 3$. $a_3 = a_2 - p^d \equiv -p^d \pmod{2^{2r}}$. By equation (7),

$$a_{4k+7} = a_{4k+3}a_5 - p^d a_4 a_{4k+2} .$$

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

In general, suppose $n = 2m + 1$ where $2^k \| n - 1$. Then $2^{k-1} \| m$ and so by the induction hypothesis, $a_{m+1} \equiv (-1)^{m/2}p^{md/2} \pmod{2^{k-1+2r-2}}$ and so $(a_{m+1})^2 \equiv (-1)^m p^{md} \pmod{2^{k+2r-2}}$. By part (i) of the lemma, $a_m \equiv 0 \pmod{2^{k-1+r-1}}$, and so $a_m^2 \equiv 0 \pmod{2^{2k+2r-4}}$ which implies a fortiori that $a_m^2 \equiv 0 \,(2^{k+2r-2})$ since $k \geqq 2$. By equation (7),

$$a_{2m+1} = a_{m+1}^2 - p^d a_m^2 \equiv (-1)^m p^{md} \pmod{2^{k+2r-2}}$$

as desired. This completes the proof of the lemma.

COROLLARY. *If* $n \geqq 3$ *is odd,* $2^r \| a$, $2^k \| n - 1$, $p \equiv 2^t - 1 \pmod{2^{t+1}}$, *and* $2r - 2 \geqq t$, *then* $a_n \equiv 1 + 2^{k+t-1} \pmod{2^{k+t}}$. *In particular,* $a_n \neq \pm 1$ *for* $n > 1$ *if* $2(r - 1) \geqq t$.

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

$$p^{2^s f} \equiv 2^{t+s} + 1 \pmod{2^{t+s+1}} .$$

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 $2r \leqq t + 1$. Since $(p) = \mathfrak{P}\mathfrak{P}'$, equation (4) implies that $p^d = (a/2)^2 + D$. On the other hand, $2^r \| a$ implies $(a/2)^2 \equiv 2^{2r-2} \pmod{2^{2r+1}}$. From these results and the fact that $p \equiv 2^t - 1 \pmod{2^{t+1}}$, one concludes that $D \equiv 2^t - 2^{2r-2} - 1 \pmod{2^{2r}}$. Thus the exceptional cases occur when

$$(8) \quad \begin{cases} p \equiv 2^t - 1 \pmod{2^{t+1}} \\ \text{and} \\ D \equiv 2^t - 2^{2(r-1)} - 1 \pmod{2^{2r}} \quad \text{for } r \leqq \dfrac{t+1}{2} . \end{cases}$$

For example, this formula yields the following exceptional cases for $t = 2, 3, 4, 5$.

$p \equiv 3 \pmod 8$	none
$p \equiv 7 \pmod{16}$	$D \equiv 3 \pmod{16}$
$p \equiv 15 \pmod{32}$	$D \equiv 11 \pmod{16}$
$p \equiv 31 \pmod{64}$	$D \equiv 11 \pmod{16}$ 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 $Q(\sqrt{-D})$. In order for*

$$x^2 + D = p^n,\ x \geqq 0,\ n \geqq 0$$

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

1. R. Alter and K. K. Kubota, *The diophantine equation $x^2 + 11 = 3^n$, and a related sequence*, J. Number Theory, (to appear).

2. R. Apéry, *Sur une équation diophantienne*, Comptes Rendus Paris (Sér. Math., Phys., Astr.), **251** (1960), 1263-1264.

3. E. L. Cohen, *Sur certaines équations diophantiennes quadratiques*, Comptes Rendus Paris (Sér. math., Phys., Astr.), **274** (1972), 139-140.

4. H. Hasse, *Über eine diophantische Gleichungen von Ramanujan-Nagell und ihre Verallgemeinerung*, Nag. Math. J., **27** (1966), 77-102.

5. T. H. Skolem, S. Chowla, and D. J. Lewis, *The diophantine equation $2^{n+2} - 7 = x^2$ and related problems*, Proc. Amer. Math. Soc., **10** (1959), 663-669.

Received January 18, 1972.

UNIVERSITY OF KENTUCKY