PACIFIC JOURNAL OF MATHEMATICS
Vol. 124, No. 1, 1986

ON THE SOLVABILITY OF THE DIOPHANTINE EQUATION $dV^2 - 2eVW - dW^2 = 1$

KENNETH HARDY AND KENNETH S. WILLIAMS

This paper treats the diophantine equation $dV^2 - 2eVW - dW^2 = 1$, where d and e are positive integers, by methods using the arithmetic of the ring of the gaussian integers.

1. Introduction. We denote the integral binary quadratic form $ax^2 + 2bxy + cy^2$ by (a, b, c), and its determinant $b^2 - ac$ by m. We consider only forms which are properly primitive, that is for which $\mathrm{GCD}(a, 2b, c) = 1$, and indefinite, that is for which $m > 0$. Two forms (a, b, c) and (A, B, C) of determinant m are said to be equivalent if there exist integers p, q, r, s with $ps - qr = 1$ such that

$$a(px + qy)^2 + 2b(px + qy)(rx + sy) + c(rx + sy)^2 = Ax^2 + 2Bxy + Cy^2.$$

If (a, b, c) and (A, B, C) are equivalent we write $(a, b, c) \sim (A, B, C)$. The relation $\sim$ is an equivalence relationship and the equivalence class containing (a, b, c) is denoted by $[a, b, c]$. Composition of these classes is defined by $[a, b, a'c] * [a', b, ac] = [aa', b, c]$. The set of equivalence classes of forms of determinant m under composition is a finite abelian group. The identity element of this group is the principal class $[1, 0, -m]$ and the inverse of the class $[a, b, c]$ is given by $[a, b, c]^{-1} = [a, -b, c]$.

If m is of the form $m = d^2 + e^2$, where d and e are positive integers such that $\mathrm{GCD}(d, 2e) = 1$, the form $(d, -e, -d)$ has determinant m and the class $[d, -e, -d]$ is such that $[d, -e, -d]^2 = [d^2, -e, -1] = [-1, 0, m]$ [**3**, Proposition 1]. If the equation $x^2 - my^2 = -1$ is insolvable in integers x and y then $[-1, 0, m] \neq [1, 0, -m]$ [**3**, p. 599] and so $[d, -e, -d] \neq [1, 0, -m]$, showing that the equation $dV^2 - 2eVW - dW^2 = 1$ is insolvable in integers V and W. On the other hand, if the equation $x^2 - my^2 = -1$ is solvable [**3**, p. 599], then $[-1, 0, m] = [1, 0, -m]$, so that $[d, -e, -d]^2 = [1, 0, -m]$, in which case it may be possible that $[d, -e, -d] = [1, 0, -m]$. Kaplan [**4**, Chapitre VIII] has shown that among all the representations of m in the form $m = d^2 + e^2$, $\mathrm{GCD}(d, 2e) = 1$, there is exactly one such pair (d, e) for which $[d, -e, -d] = [1, 0, -m]$ holds, in which case $dV^2 - 2eVW - dW^2 = 1$ is solvable in integers V and W.

In this paper we give a complete treatment of the solvability of the diophantine equation

$$dV^2 - 2eVW - dW^2 = 1, \tag{1.1}$$

where d and e are positive integers. Our method uses the arithmetic of the ring of gaussian integers rather than the theory of binary quadratic forms.

The equation (1.1) is clearly insolvable if d is even or if d and e have a common factor > 1. Hence we may assume that d and e are positive coprime integers with d odd. We note that d odd implies that $m = d^2 + e^2$ satisfies $m \equiv 1 \pmod 4$ or $m \equiv 2 \pmod 8$. In §2 we show that if $m = d^2 + e^2$ is a square then the equation (1.1) is insolvable (Theorem 1). When m is nonsquare two cases arise according as the pellian equation

$$x^2 - my^2 = -1 \tag{1.2}$$

is solvable or not. In §3 we show that the insolvability of (1.2) implies insolvability of (1.1) (Theorem 2). Assuming the solvability of (1.2), we give in §4 a necessary and sufficient condition for (1.1) to be solvable in terms of the minimal solution (x_0, y_0) of (1.2), that is the solution in positive integers x and y with y least (Theorem 3). In §5 we show that among all the pairs of positive coprime integers (d, e) with d odd satisfying $d^2 + e^2 = m$, where m is a fixed nonsquare positive integer for which (1.2) is solvable, there is exactly one pair for which (1.1) is solvable (Theorem 4). In the remainder of §5 it is shown how this unique pair can be obtained as the solution of a linear congruence (Theorem 5). In §6 we show how one solution of (1.1) can be used to give all the solutions. The paper is concluded in §7 with some numerical examples.

2. m square. We begin by treating the case when $m = d^2 + e^2$ is a square and prove the following theorem.

THEOREM 1. *If d and e are positive coprime integers with d odd such that $m = d^2 + e^2 = n^2$ $(n > 0)$, then the diophantine equation* (1.1) *is insolvable.*

Proof. We suppose that (1.1) is solvable in integers V and W. Multiplyng (1.1) by d and completing the square, we obtain

$$(dV - eW)^2 - n^2W^2 = d. \tag{2.1}$$

Factoring (2.1) we see that there exists a divisor t of d such that

$$dV - (e + n)W = t, \qquad dV - (e - n)W = d/t. \tag{2.2}$$

Eliminating V in (2.2), we obtain

$$2nW = \frac{d}{t} - t. \tag{2.3}$$

If $W = 0$, from (1.1) we obtain $dV^2 = 1$, so that $d = 1$. Hence $1 + e^2 = n^2$, which implies $e = 0$, contrary to assumption. Thus we have $|W| \geq 1$ and $t^2 \neq d$, and so from (2.3) we obtain

$$2n \leq \left| \frac{d}{t} - t \right|. \tag{2.4}$$

If $\sqrt{d} < t \leq d$ then (2.4) implies

$$2n \leq t - \frac{d}{t} < t \leq d < n.$$

which is impossible.

If $0 < t < \sqrt{d}$ then (2.4) implies

$$2n \leq \frac{d}{t} - t < \frac{d}{t} \leq d < n,$$

which is impossible.

If $-\sqrt{d} < t < 0$ then (2.4) implies

$$2n \leq t - \frac{d}{t} < -\frac{d}{t} \leq d < n,$$

which is impossible.

If $-d \leq t < -\sqrt{d}$ then (2.4) implies

$$2n \leq \frac{d}{t} - t < -t \leq d < n,$$

which is impossible.

This completes the proof of Theorem 1.

3. m nonsquare and $x^2 - my^2 = -1$ insolvable. In the case $m = d^2 + e^2$ nonsquare and such that (1.2) is insolvable, we prove the following result.

THEOREM 2. *If d and e are positive coprime integers with d odd such that $m = d^2 + e^2$ is a nonsquare for which the pellian equation* (1.2) *is insolvable, then the diophantine equation* (1.1) *is insolvable.*

Proof. Suppose that (1.1) is solvable in integers V and W. We define integers x and y by

$$x = eV^2 + 2dVW - eW^2, \qquad y = V^2 + W^2. \tag{3.1}$$

Then, from the identity

$$(dV^2 - 2eVW - dW^2)^2 + (eV^2 + 2dVW - eW^2)^2 = (d^2 + e^2)(V^2 + W^2)^2, \tag{3.2}$$

we obtain $1 + x^2 = my^2$, contradicting the insolvability of (1.2).

This completes the proof of Theorem 2.

4. m nonsquare and $x^2 - my^2 = -1$ solvable. We define the *normalized* greatest common divisor $\mathrm{NGCD}(\alpha, \beta)$ of two nonzero gaussian integers α and β to be the unique associate $a + bi$, among the four associated GCD's of α and β, which satisfies

$$\begin{cases} a \text{ odd}, a > 0, & \text{if } 1 + i \nmid a + bi, \\ a > 0, b \geq 0, & \text{if } 1 + i \mid a + bi. \end{cases} \tag{4.1}$$

We prove the following theorem.

THEOREM 3. *Let d and e be positive coprime integers with d odd such that $m = d^2 + e^2$ is a nonsquare for which* (1.2) *is solvable. Let (x_0, y_0) be the minimal solution of* (1.2), *that is the solution in positive integers with y_0 least. Then* (1.1) *is solvable if and only if*

$$\begin{cases} d + ei = \mathrm{NGCD}(x_0 + i, m) \text{ or } \mathrm{NGCD}(x_0 - i, m), \\ \qquad\qquad \text{when } m \equiv 1 \pmod 4, \\ d + ei = \mathrm{NGCD}(x_0 + i, m), \\ \qquad\qquad \text{when } m \equiv 2 \pmod 8 \text{ and } x_0 \equiv -de \pmod 4, \\ d + ei = \mathrm{NGCD}(x_0 - i, m), \\ \qquad\qquad \text{when } m \equiv 2 \pmod 8 \text{ and } x_0 \equiv de \pmod 4. \end{cases} \tag{4.2}$$

Proof. We begin by showing that if (4.2) holds then (1.1) is solvable. We may suppose without loss of generality that $d + ei$ divides $x_0 + i$, written $d + ei \mid x_0 + i$, as the case $d + ei \mid x_0 - i$ is similar. From the equation $x_0^2 - my_0^2 = -1$ we obtain

$$\left(\frac{x_0 + i}{d + ei}\right)\left(\frac{x_0 - i}{d - ei}\right) = y_0^2, \tag{4.3}$$

where the gaussian integers $(x_0 + i)/(d + ei)$ and $(x_0 - i)/(d - ei)$ are coprime. Hence for some unit ε $(= \pm 1, \pm i)$ and integers V and W we have (as $y_0 > 0$)

$$\frac{x_0 + i}{d + ei} = \varepsilon(V + Wi)^2, \quad y_0 = V^2 + W^2. \tag{4.4}$$

Clearly as $-1 = i^2$ we may suppose that $\varepsilon = 1$ or i by replacing V and W by $-W$ and V respectively if necessary.

We first treat the case $m \equiv 1 \pmod 4$. In this case we have

$$d \equiv y_0 \equiv 1 \pmod 2, \quad e \equiv x_0 \equiv 0 \pmod 2.$$

From $y_0 = V^2 + W^2$ we see that V and W are of opposite parity, so that $(V + Wi)^2 \equiv 1 \pmod 2$. Taking $x_0 + i = \varepsilon(d + ei)(V + Wi)^2$ modulo 2 we obtain $i \equiv \varepsilon \pmod 2$, so that $\varepsilon = i$, giving

$$x_0 + i = i(d + ei)(V + Wi)^2. \tag{4.5}$$

Equating coefficients of i on both sides of (4.5) we obtain

$$1 = dV^2 - 2eVW - dW^2,$$

showing that (1.1) is solvable.

Next we consider the remaining case when $m \equiv 2 \pmod 8$. In this case we have

$$d \equiv e \equiv x_0 \equiv y_0 \equiv 1 \pmod 2.$$

From $y_0 = V^2 + W^2$ we see that V and W are of opposite parity and so

$$(V + Wi)^2 \equiv V^2 - W^2 \equiv 2V^2 - 1 \equiv 2V - 1 \pmod 4.$$

Taking $x_0 + i = \varepsilon(d + ei)(V + Wi)^2$ modulo 4 we obtain

$$x_0 + i \equiv \varepsilon(d + ei)(2V - 1) \pmod 4.$$

Squaring this congruence we deduce that

$$2x_0 i \equiv \varepsilon^2 2dei \pmod 8,$$

so that

$$x_0 \equiv \varepsilon^2 de \pmod 4.$$

Hence we have

$$\begin{cases} \varepsilon = 1 & \text{if } x_0 \equiv de \pmod 4, \\ \varepsilon = i, & \text{if } x_0 \equiv -de \pmod 4. \end{cases} \tag{4.6}$$

As we have assumed that $d + ei \mid x_0 + i$, from (4.2), we see that $x_0 \equiv -de \pmod 4$, and so by (4.6) we deduce that $\varepsilon = i$. Thus

$$x_0 + i = i(d + ei)(V + Wi)^2$$

and equating coefficients of i we obtain

$$1 = dV^2 - 2eVW - dW^2.$$

Conversely we now show that if (1.1) is solvable then $d + ei$ satisfies (4.2). Let (V, W) be a solution in integers of (1.1).

Define integers x and y by

$$x = -eV^2 - 2dVW + eW^2, \qquad y = V^2 + W^2. \tag{4.7}$$

Then we have

$$x + i = (-eV^2 - 2dVW + eW^2) + (dV^2 - 2eVW - dW^2)i$$

so that

$$x + i = i(d + ei)(V + Wi)^2, \tag{4.8}$$

giving

$$x^2 + 1 = (d^2 + e^2)(V^2 + W^2)^2 = my^2,$$

so that (x, y) is a solution of (1.2).

Next we calculate the GCD of $x + i$ and m. From (4.8) we have

$$\mathrm{GCD}(x + i, m) = (d + ei)\mathrm{GCD}\big((V + Wi)^2, d - ei\big).$$

Now we show that $\mathrm{GCD}((V + Wi)^2, d - ei) = 1$, otherwise there exists a gaussian prime π such that

$$\pi \mid V + Wi, \quad \pi \mid d - ei,$$

in which case, from (4.7), we have

$$x \equiv 2W^2(e + di) \equiv 0 \pmod{\pi}, \qquad y \equiv 0 \pmod{\pi},$$

contradicting that $\mathrm{GCD}(x, y) = 1$ as (x, y) is a solution of (1.2). Thus, as d and e are positive with d odd, we have

$$\mathrm{NGCD}(x + i, m) = d + ei, \tag{4.9}$$

in accordance with (4.1).

Further, we note that in the case $m \equiv 2 \pmod 8$, we can deduce from (4.8) that

$$x \equiv -de \pmod 4 \tag{4.10}$$

exactly as we proved $x_0 \equiv -de \pmod 4$ above.

Now, as (x, y) is a solution of (1.2), we have by the theory of the pellian equation

$$x + y\sqrt{m} = \begin{cases} \left(x_0 + y_0\sqrt{m}\right)^{2k+1}, & \text{if } x > 0, \\ -\left(x_0 - y_0\sqrt{m}\right)^{2k+1}, & \text{if } x < 0, \end{cases} \tag{4.11}$$

for some non negative integer k. From (4.11) we obtain

$$x = \begin{cases} x_0^{2k+1} + \binom{2k+1}{2} x_0^{2k-1} y_0^2 m + \cdots, & \text{if } x > 0, \\ -x_0^{2k-1} - \binom{2k+1}{2} x_0^{2k-1} y_0^2 m - \cdots, & \text{if } x < 0, \end{cases} \tag{4.12}$$

where the higher terms are all divisible by m^2. Hence as $x_0^2 \equiv -1 \pmod{m}$ we have

$$x \equiv \begin{cases} (-1)^k x_0 \pmod{m}, & \text{if } x > 0, \\ (-1)^{k+1} x_0 \pmod{m}, & \text{if } x < 0. \end{cases} \tag{4.13}$$

In the case $m \equiv 2 \pmod 8$, we will also need $x \pmod 4$. As x_0 and y_0 are both odd, (4.12) gives

$$x \equiv \begin{cases} x_0 + 2\binom{2k+1}{2} x_0 \pmod 4, & x > 0, \\ -x_0 - 2\binom{2k+1}{2} x_0 \pmod 4, & x < 0, \end{cases}$$

that is

$$x \equiv \begin{cases} x_0(-1)^k \pmod 4, & \text{if } x > 0, \\ x_0(-1)^{k+1} \pmod 4, & \text{if } x < 0, \end{cases} \tag{4.14}$$

because

$$\binom{2k+1}{2} = k(2k+1) \equiv k \equiv \frac{1}{2}\left((-1)^k - 1\right) \pmod 2.$$

The proof will now be completed by considering three cases.

If $m \equiv 1 \pmod 4$ we have by (4.9) and (4.13)

$$\begin{aligned} d + ei &= \mathrm{NGCD}(x + i, m) = \mathrm{NGCD}(\pm x_0 + i, m) \\ &= \mathrm{NGCD}(x_0 \pm i, m) \end{aligned}$$

as required.

If $m \equiv 2 \pmod 8$ and $x_0 \equiv -de \pmod 4$ then by (4.10) we have $x \equiv x_0 \pmod 4$ and so by (4.14) we obtain

$$\begin{cases} k \equiv 0 \pmod 2, & \text{if } x > 0, \\ k \equiv 1 \pmod 2, & \text{if } x < 0, \end{cases}$$

and thus by (4.13) we have

$$x \equiv x_0 \pmod m,$$

and so appealing to (4.9) we get

$$d + ei = \mathrm{NGCD}(x + i, m) = \mathrm{NGCD}(x_0 + i, m),$$

as required.

If $m \equiv 2 \pmod 8$ and $x_0 \equiv de \pmod 4$ then by (4.10) we have $x \equiv -x_0 \pmod 4$ and so by (4.14) we obtain

$$\begin{cases} k \equiv 1 \pmod 2, & \text{if } x > 0, \\ k \equiv 0 \pmod 2, & \text{if } x < 0, \end{cases}$$

which gives by (4.13)

$$x \equiv -x_0 \pmod m,$$

so that appealing to (4.9) we get

$$\begin{aligned} d + ei &= \mathrm{NGCD}(x + i, m) = \mathrm{NGCD}(-x_0 + i, m) \\ &= \mathrm{NGCD}(x_0 - i, m), \end{aligned}$$

as required.

This completes the proof of Theorem 3.

5. Uniqueness. Up to this point our focus has been on a given pair of positive integers d and e, with d odd, in terms of which the integer m is defined by $m = d^2 + e^2$. We will now shift the emphasis by assuming that the positive integer m is given and considering all its decompositions as the sum of two squares.

In view of Theorems 1 and 2, in order for (1.1) to be solvable, it suffices to consider only those positive nonsquare integers m for which (1.2) is solvable. In this case every odd prime divisor of m is congruent to 1 modulo 4 and m contains at most one factor of 2. Thus m is expressible in the form $d^2 + e^2$ with d and e positive coprime integers and d odd. We now use Theorem 3 to show that among such pairs of integers (d, e), there is exactly one pair for which (1.1) is solvable.

THEOREM 4. *Let m be a nonsquare positive integer for which* (1.2) *is solvable. Then among all the pairs of positive coprime integers (d, e) satisfying $m = d^2 + e^2$ with d odd there is exactly one pair $(d, e) = (D, E)$ such that* (1.1) *is solvable.*

Proof. We begin by showing that there is at least one decomposition of m in the form $d^2 + e^2$ for which (1.1) is solvable. Recalling that

(x_0, y_0) denotes the minimal solution of (1.2) and setting $r + si = \mathrm{NGCD}(x_0 + i, m)$ we define positive integers D and E as follows:

if $m \equiv 1 \pmod 4$, we let

$$D + Ei = \begin{cases} r + si & \text{if } s > 0, \\ r - si, & \text{if } s < 0; \end{cases} \tag{5.1}$$

if $m \equiv 2 \pmod 8$,

$$D + Ei = \begin{cases} r + si, & \text{if } rs \equiv -x_0 \pmod 4, \\ s + ri, & \text{if } rs \equiv x_0 \pmod 4. \end{cases} \tag{5.2}$$

Clearly we have D odd and $\mathrm{GCD}(D, E) = 1$.

Next we show that $D^2 + E^2 = m$. From the definition of D and E we see that $D + Ei \mid x_0 + i$ or $D + Ei \mid x_0 - i$. Without loss of generality we may suppose that $D + Ei \mid x_0 + i$. From the equation $x_0^2 - my_0^2 = -1$, we see that

$$\left(\frac{x_0 + i}{D + Ei}\right)(x_0 - i) = \frac{m}{D + Ei} \cdot y_0^2, \tag{5.3}$$

where the gaussian integers $(x_0 + i)/(D + Ei)$ and $m/(D + Ei)$ are coprime. The equation (5.3) shows that $m/(D + Ei) \mid x_0 - i$. But $m/(D + Ei) \mid m$ so we must have

$$\frac{m}{D + Ei} \mid \mathrm{GCD}(x_0 - i, m) = D - Ei,$$

and so

$$m \mid D^2 + E^2. \tag{5.4}$$

On the other hand, as $D + Ei \mid m$, taking conjugates we obtain $D - Ei \mid m$. Hence we have

$$\mathrm{LCM}(D + Ei, D - Ei) \mid m,$$

that is

$$\frac{D^2 + E^2}{\mathrm{GCD}(D + Ei, D - Ei)} \mid m. \tag{5.5}$$

Next we note that

$$\begin{aligned} \mathrm{GCD}(D + Ei, D - Ei) &= \mathrm{GCD}(x_0 + i, x_0 - i, m) \\ &= \mathrm{GCD}(x_0 + i, 2i, m), \end{aligned}$$

so that

$$\mathrm{GCD}(D + Ei, D - Ei) = \begin{cases} 1, & \text{if } m \equiv 1 \pmod 4, \\ 1 + i, & \text{if } m \equiv 2 \pmod 8. \end{cases} \tag{5.6}$$

From (5.5) and (5.6) we see that

$$D^2 + E^2 \mid m, \quad \text{if } m \equiv 1 \pmod 4, \tag{5.7}$$

and

$$\frac{D^2 + E^2}{1 + i} \mid m, \quad \text{if } m \equiv 2 \pmod 8. \tag{5.8}$$

From (5.8) we deduce that $(D^2 + E^2)/2 \mid m$, and as $(D^2 + E^2)/2$ is odd, this gives $(D^2 + E^2)/2 \mid m/2$, that is

$$D^2 + E^2 \mid m, \quad \text{if } m \equiv 2 \pmod 8. \tag{5.9}$$

Then the result $m = D^2 + E^2$ now follows from (5.4), (5.7) and (5.9).

Thus $m = D^2 + E^2$ is a decomposition of m as a sum of two squares which satisfies (4.2). Hence, by Theorem 3, the equation $DV^2 - 2EVW - DW^2 = 1$ is solvable.

Finally, it is clear that $m = D^2 + E^2$ is the only decomposition of m for which (1.1) is solvable, for if there were another such decomposition, say $m = d^2 + e^2$, then we would have, by Theorem 3, $d + ei = D + Ei$, giving $d = D$, $e = E$, completing the proof.

COROLLARY. *If* $p \equiv 1 \pmod 4$ *is a prime then the diophantine equation*

$$aV^2 - 2bVW - aW^2 = 1$$

is solvable, where a and b are the unique positive integers with

$$p = a^2 + b^2, \qquad a \equiv 1 \pmod 2.$$

In the next theorem we go on to show how the pair (D, E) can be constructed.

THEOREM 5. *Let m be a nonsquare positive integer such that* (1.2) *is solvable with minimal solution* (x_0, y_0). *Then there exists a unique pair of coprime integers* $(d, e) \neq (0, 0)$ *satisfying*

$$\begin{cases} d - x_0 e \equiv 0 \pmod m, \\ |d| < \sqrt{m}\,, \ |e| < \sqrt{m}\,, \\ d \text{ odd}, \ d > 0, & \text{if } m \equiv 1 \pmod 4, \\ d > 0, \ e > 0, & \text{if } m \equiv 2 \pmod 8. \end{cases} \tag{5.10}$$

Then the unique pair (D, E) specified in Theorem 4 for which the equation (1.1) is solvable is given by

$$(D, E) = \begin{cases} (d, e), & \text{if } m \equiv 1 \pmod 4, \ e > 0, \\ (d, -e), & \text{if } m \equiv 1 \pmod 4, \ e < 0, \\ (d, e), & \text{if } m \equiv 2 \pmod 8, \ x_0 \equiv -de \pmod 4, \\ (e, d), & \text{if } m \equiv 2 \pmod 8, \ x_0 \equiv de \pmod 4. \end{cases} \tag{5.11}$$

Proof. The following result was proved by Aubrey [**1**] (see also [**2**]) in 1913: if a, b and m are integers satisfying

$$m > 0, \quad \mathrm{GCD}(a, m) = 1, \quad b/\sqrt{m} \text{ not an integer},$$

then there exist integers x and y not both zero such that

$$ax - by \equiv 0 \pmod{m}$$

and

$$|x| < \sqrt{m}, \quad |y| < \sqrt{m}.$$

Taking $a = 1$ and $b = x_0$, we see that there are integers d and e (not both zero) such that

$$d - x_0 e \equiv 0 \pmod{m}, \qquad |d| < \sqrt{m}, |e| < \sqrt{m}. \tag{5.12}$$

It is clear that $d^2 + e^2 = m$ as $0 < d^2 + e^2 < 2m$ and $d^2 + e^2 \equiv x_0^2 e^2 + e^2 \equiv -e^2 + e^2 \equiv 0 \pmod{m}$.

Next we show that $\mathrm{GCD}(d, e) = 1$. Let $g = \mathrm{GCD}(d, e)$, and set $d = gd_1$, $e = ge_1$. From $d^2 + e^2 = m$ we obtain $d_1^2 + e_1^2 = m_1$, where $m_1 = m/g^2$. From (5.12) there exists an integer k such that $d - x_0 e = km$ and hence $d_1 = x_0 e_1 + kgm_1$. Thus, from $(x_0 e_1 + kgm_1)^2 + e_1^2 = m_1$ we use $x_0^2 + 1 = my_0^2$ to deduce that

$$g\left(gy_0^2 e_1^2 + 2kx_0 e_1 + k^2 g m_1\right) = 1,$$

proving that $g = 1$.

Next we show that if (d_1, e_1) is another solution of (5.12) with d_1 and e_1 not both zero, then

$$(d_1, e_1) = \pm(d, e), \pm(e, -d). \tag{5.13}$$

From $d - x_0 e \equiv d_1 - x_0 e_1 \equiv 0 \pmod{m}$, we see that

$$de_1 - d_1 e \equiv 0 \pmod{m}$$

and

$$dd_1 + ee_1 \equiv 0 \pmod{m}.$$

In view of

$$\left(\frac{dd_1 + ee_1}{m}\right)^2 + \left(\frac{de_1 - d_1 e}{m}\right)^2 = \frac{\left(d^2 + e^2\right)\left(d_1^2 + e_1^2\right)}{m^2} = 1,$$

we must have

$$dd_1 + ee_1 = \pm m, \quad de_1 - d_1 e = 0,$$

or

$$dd_1 + ee_1 = 0, \quad de_1 - d_1 e = \pm m$$

from which (5.13) follows. Thus there is a unique solution of (5.12) satisfying

$$\begin{cases} d \text{ odd}, d > 0 & \text{if } m \equiv 1 \pmod 4, \\ d > 0, e > 0, & \text{if } m \equiv 2 \pmod 8. \end{cases}$$

Finally we show that (D, E) defined by (5.11) satisfies (4.2) and so is the unique pair specified in Theorem 4. It suffices to treat the case

$$m \equiv 2 \pmod 8, \quad x_0 \equiv de \pmod 4,$$

as the others are similar. We must show that $e + di = \text{NGCD}(x_0 - i, m)$ in this case.

As $d - x_0 e \equiv 0 \pmod m$, we have $x_0 d + e \equiv 0 \pmod m$, and so

$$\frac{x_0 - i}{e + di} = \left(\frac{x_0 e - d}{m}\right) - i\left(\frac{x_0 d + e}{m}\right)$$

is a gaussian integer. Thus $e + di \mid x_0 - i$ and, as $e + di \mid m$, we have

$$e + di \mid \text{GCD}(x_0 - i, m) \tag{5.14}$$

Next we show that $\text{GCD}(x_0 - i, m) \mid e + di$. To do this let π denote any prime factor of $\text{GCD}(x_0 - i, m)$. Then, as $\pi \mid m$, we see from $d - x_0 e \equiv 0 \pmod m$ that $d \equiv x_0 e \pmod \pi$. But $x_0 \equiv i \pmod \pi$, so $d \equiv ie \pmod \pi$, giving $e + di \equiv 0 \pmod \pi$. Thus we have

$$\text{GCD}(x_0 - i, m) \mid e + di. \tag{5.15}$$

From (5.14) and (5.15) we see that $e + di$ is a GCD of $x_0 - i$ and m. However d and e are positive integers so that $\text{NGCD}(x_0 - i, m) = e + di$, which completes the proof.

6. Complete set of solutions of (1.1). In this section d and e are positive integers for which (1.1) is solvable. We let (V_0, W_0) be a particular solution of (1.1) and show how all solutions (V, W) of (1.1) may be obtained in terms of V_0, W_0 and the minimal solution (x_0, y_0) of (1.2).

Let (V, W) be any solution of (1.1) and set

$$\alpha = \frac{(dV - eW) + W\sqrt{m}}{(dV_0 - eW_0) + W_0\sqrt{m}}.$$

The norm of α is

$$\frac{(dV - eW)^2 - mW^2}{(dV_0 - eW_0)^2 - mW_0^2} = \frac{d(dV^2 - 2eVW - dW^2)}{d(dV_0^2 - 2eV_0W_0 - dW_0^2)} = 1.$$

Moreover α is of the form $A + B\sqrt{m}$, where A and B are integers given by

$$A = dVV_0 - e(VW_0 + WV_0) - dWW_0,$$
$$B = -VW_0 + WV_0.$$

Hence, by the theory of the pellian equation, we have

$$\alpha = \pm\left(x_0 + y_0\sqrt{m}\right)^{2k},$$

where k is an integer. Thus we have shown the existence of an integer k such that

$$(6.1)\ (dV - eW) + W\sqrt{m} = \pm\left(x_0 + y_0\sqrt{m}\right)^{2k}\left((dV_0 - eW_0) + W_0\sqrt{m}\right).$$

Conversely let V and W be defined by (6.1) for some integer k. Taking norms of both sides of (6.1), we see that (V, W) satisfies (1.1). It remains to show that V and W are both integers.

Define integers T and U by

$$T + U\sqrt{m} = \pm\left(x_0 + y_0\sqrt{m}\right)^{2k}.$$

Then equating coefficients in (6.1) we obtain

$$dV - eW = T(dV_0 - eW_0) + mUW_0,$$
$$W = TW_0 + U(dV_0 - eW_0).$$

Clearly W is an integer. Solving for V we obtain (using $d^2 + e^2 = m$)

$$V = (T + eU)V_0 + dUW_0$$

so that V is also an integer.

It now follows that all solutions of (1.1) may be obtained from (6.1) in terms of the particular solutions (V_0, W_0) and (x_0, y_0).

7. Numerical examples. If $d = 11$ and $e = 8$ then $m = 185 = 11^2 + 8^2 \equiv 1 \pmod 4$ is nonsquare and such that (1.2) has minimal solution $x_0 = 68$, $y_0 = 5$. In this case $\mathrm{NGCD}(68 + i, 185) = 11 - 8i$, while $\mathrm{NGCD}(68 - i, 185) = 11 + 8i$, so that Theorem 3 applies to show (1.1) is solvable ($(V, W) = (2, 1)$ is a solution.) We note that $185 = 13^2 + 4^2$ so that (1.1) is insolvable for $d = 13$ and $e = 4$ by Theorem 4.

In case $m = 130 = 3^2 + 11^2 = 7^2 + 9^2$ we have $m \equiv 2 \pmod 8$, nonsquare, and such that (1.2) has minimal solution $x_0 = 57$, $y_0 = 5$. Now $\mathrm{NGCD}(57 + i, 130) = 9 + 7i$ and as $57 \equiv -9.7 \pmod 4$ we see by Theorems 3 and 4 that (1.1) is solvable only in the case when $d = 9$ and $e = 7$ ($(V, W) = (-1, 2)$ is a solution).

To illustrate the use of Theorem 5, take $m = 845$. Then $m \equiv 1 \pmod 4$ is nonsquare and $x_0 = 12238$, $y_0 = 421$ is the required minimal solution of (1.2). The candidates for the unique pair (d, e) satisfying (5.10) must be solutions of $m = d^2 + e^2$, that is, $(d, e) = (13, \pm 26), (19, \pm 22), (29, \pm 2)$. The only pair satisfying $d - x_0 e \equiv 0 \pmod m$ is $(d, e) = (29, -2)$, so that $(D, E) = (29, 2)$ is the unique pair for which (1.1) is solvable ($(V, W) = (15,14)$ is a solution).

References

[1] L. Aubry, *Un théorème d'arithmétique*, Mathesis (4), **3** (1913).

[2] A. Brauer and R. L. Reynolds, *On a theorem of Aubry-Thue*, Canad. J. Math., **3** (1951), 367–374.

[3] Pierre Kaplan, *Divisibilité par 8 du nombre des classes de corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan, **25** (1973), 596–608.

[4] _____, *Cours d'arithmétique*, Université de Nancy I.

Received April 21, 1985 and in revised form August 19, 1985. First author's research supported by Natural Sciences and Engineering Research Council Canada Grant A-8049. Second author's research suported by Natural Sciences and Engineering Research Council Canada Grant A-7233.

CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA K1S 5B6