ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 13, Number 1, Winter 1983

DIOPHANTINE CHAINS

JAMES C. OWINGS, JR.

ABSTRACT. We solve a large class of quadratic binary Diophantine equations without resort to the theory of quadratic number fields. Examples are given of equations amenable to our approach, including some which are intractable by classical methods. A corollary is drawn concerning the size of smallest possible solutions to certain quadratic forms.

In most treatments of Diophantine equations, the determination of all integral solutions to the quadratic binary equation

$$(*) \qquad ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with integral coefficients is reduced to the solution of a Pellian equation $x^2 - Dy^2 = K$, where $D = b^2 - 4ac$. To solve the latter one must find the fundamental unit of the real quadratic field $Q(\sqrt{D})$. This is a laborious process, to be avoided if possible. In [4] we presented an alternative approach, first suggested by W. H. Mills [2], which applies whenever $a \neq 0$, $b \neq 0$, $c \neq 0$, a divides b and d, and c divides b and e. In this paper we improve and simplify the methods of [4] and show how they may also be used in many cases when (*) does not immediately satisfy the divisibility conditions. There are still many equations we cannot solve (e.g., $x^2 - 13y^2 = 1$, whose smallest solution is $x = 649$, $y = 180$), and we do not hold much hope that the method can ever be made completely general. However, it does apply to most examples we have seen considered in number theory texts and, in these cases, effects a substantial savings in computation. It has the added attraction of being completely elementary; in particular, no knowledge of the theory of quadratic number fields is required.

If the pair (x, y) satisfies (*), then so do the pairs (x', y) and (x, y') where $ax' = -ax - by - d$ and $cy' = -cy - bx - e$. The divisibility conditions are needed to ensure that x' and y' will be integers whenever x and y are. Thus, each integral solution (x, y) generates an endless (but possibly cyclic) chain $\cdots x''y'xyx'y'' \cdots$ and in [4] we showed that the number of such

AMS classification number: 10B05
Received by the editors on April 20, 1980.

chains is always finite. If the discriminant D $(= b^2 - 4ac)$ is zero or negative, or positive but a perfect square, then (*) has only finitely many solutions, as may be seen by completing the square, and these may easily be determined. Therefore, we shall only be concerned with equations of positive nonsquare discriminant, although this is not an assumption in the following theorem.

THEOREM. *Suppose a divides b and d, c divides b and e, $a > 0$, $b \neq 0$, and either* (1) $c > 0$ *and* $a + b + c < 0$ *or* (2) $c < 0$. *Define the following finite sets of integers:*

$$X = \{x \mid ax^2 + dx + f \leqq 0\},$$
$$Y = \{y \mid cy^2 + ey + f \leqq 0\} \text{ in case (1)},$$
$$Y = \{y \mid cy^2 + ey + f \geqq 0\} \text{ in case (2), and}$$
$$W = \{w \mid (a + b + c)w^2 + (d + e)w + f \geqq 0\} \text{ in case (1)}.$$

In case (1), *let* $X' = X \cup W$, $Y' = W$ *or let* $X' = W$, $Y' = Y \cup W$. *In case* (2), *let* $X' = X$, $Y' = Y$. *Then* X', Y' *are finite sets of integers such that every chain of integral solutions to* (*) *contains some member of* X' *as an* x*-value or some member of* Y' *as a* y*-value.*

In case (1), this is an improvement of Thorem 1 of [4]. Case (2) is identical to Theorem 3(b) of [4], but for completeness we repeat the proof. The vastly more complicated Theorem 3(a) turns out to be unnecessary in applications, as we demonstrate below.

PROOF (of the theorem). The following equations follow directly from the defining relations $ax' = -ax - by - d$, $cy' = -cy - bx - e$, and equation (*).

(1) $a(xx') = cy^2 + ey + f,$
(2) $c(yy') = ax^2 + dx + f,$
(3) $a(x - y)(y - x') = -((a + b + c)y^2 + (d + e)y + f),$
(4) $c(y - x)(x - y') = -((a + b + c)x^2 + (d + e)x + f),$
(5) $a(x'' - x') = b(y - y').$

Case (1). Suppose, for example, that $X' = X \cup W$, $Y' = W$ and that C is a chain having no member of X' as an x-value and no member of Y' as a y-value. Then no member of C belongs to W, which, by equations (3) and (4), means that C is monotone; i.e., either strictly increasing or strictly decreasing. But since $X \subseteqq X'$, we also know from (2) that every y-value in C has the same sign, clearly a contradiction.

Case (2). Here $X' = X$ and $Y' = Y$. Suppose C does not satisfy the conclusion of the theorem. Since $c < 0$, equation (2) tells us that consecutive y-values of C have opposite signs. So, if we delete every other x-value

from C, the x-values remaining form a sequence which, by equation (5), is strictly monotone. But, by (1), all x-values have the same sign, again a contradiction.

We now show that the above theorem can always be used when the divisibility conditions hold, even if neither of its two cases holds directly. So suppose a and c are both positive. In the first place, if there are to be any solutions at all, gcd (a, c) must divide f, so that we may assume gcd$(a, c) = 1$. Also we may suppose b is negative, since otherwise we substitute $-y$ for y. Therefore, since a and c both divide b, $b \leqq -ac$. If $a, c \geqq 2$, then $a + b + c \leqq a - ac + c = a(1 - c) + c \leqq 2(1 - c) + c = 2 - c \leqq 0$. We cannot have $a = c = 2$, else gcd $(a, c) = 2$. So either $a > 2$ or $c > 2$, which means one of the two inequalities above is strict, yielding $a + b + c < 0$. Thus $a = 1$ or $c = 1$; by symmetry, we may assume $a = 1$. Let $b = -kc$. Then $a + b + c \geqq 0$ means $1 - kc + c \geqq 0$, implying that $k = 1$ or $c = 1$. If $c = 1, a + b + c \geqq 0$ becomes $b \geqq -2$, which implies that $D = b^2 - 4ac = b^2 - 4 \leqq 0$. As mentioned before, we are only concerned with equations of positive discriminant. If $k = 1$ and $c \leqq 4$, we again get $b^2 - 4ac = c(c - 4) \leqq 0$. Finally, if $k = 1$ and $c > 4$, we make the substitution $x = u + v$, $y = v$. Our equation becomes $(u + v)^2 - c(u + v)v + cv^2 + d(u + v) + ev + f = u^2 + (2 - c)uv + v^2 + du + (d + e)v + f = 0$. where $1 + (2 - c) + 1 = 4 - c < 0$, so that case (1) of the theorem now applies.

A linear transformation $x = Pu + Qv, y = Ru + Sv$ such that x and y are integers if and only if u and v are integers is called *unimodular*. By Cramer's Theorem, an equivalent statement is $PS - QR = \pm 1$. If one has an equation not satisfying the divisibility conditions, a discreetly chosen unimodular transformation may convert it to one that does. For example, suppose our equation is $ax^2 + bxy + cy^2 = m$ and that we have at our disposal a solution (P, R) of $ax^2 + bxy + cy^2 = 1$ (in standard terminology, this means the given quadratic form *represents* 1). Then P and R must be relatively prime; choose integers Q and S with $PS - QR = 1$. If we make the substitution above our equation becomes $u^2 + (2aPQ + b(PS + QR) + 2cRS)uv + (aQ^2 + bQS + cS^2)v^2 = m$, since $aP^2 + bPR + cR^2 = 1$. The hope is that $aQ^2 + bQS + cS^2$ is small enough to divide the coefficient of uv (it cannot be zero if $b^2 - 4ac$ is not a perfect square). Or if one has a Pellian equation $x^2 - Dy^2 = K$ and knows that $A^2 - DC^2 = 1$, where $C \neq 0$, he can make the substitution $x = u + Av$, $y = Cv$, yielding $u^2 + 2Auv + v^2 = K$. In this case, the transformation is not unimodular, but this is not an essential problem, since u and v will be expressible as fractions with denominator AC, so one solves the equation $u^2 + 2Auv + v^2 = K(AC)^2$ instead. If D is not a perfect square, and we have been assuming that it is not, then it is known

that $x^2 - Dy^2 = 1$ has infinitely many solutions [3, p. 197], but this is really no solace, as they may be hard to find. In theory, at least, the divisibility conditions can always be attained. Achieving them is often serendipitous, but if the coefficients are small, one has a reasonable chance, as in several of the examples below.

EXAMPLE 1. $u^2 - 3v^2 = -17$. Let $u = x, v = x - y$. The equation becomes $2x^2 - 6xy + 3y^2 = 17$. Case (1) of the theorem applies. $W = \varnothing$, so we can take $X' = X = \{x | 2x^2 - 17 \leqq 0\} = \{0, \pm 1, \pm 2\}$, $Y' = \varnothing$. Setting $x = 0, \pm 1, \pm 2$ we get successively $3y^2 = 17, y^2 \pm 2y = 5, y^2 \pm 4y = 3$, none of which have integral solutions. So $u^2 - 3v^2 = -17$ cannot be solved in integers.

EXAMPLE 2. [1, p. 246] $u^2 + 3uv - 5v^2 = 65$. Let $u = x + y, v = y$. We get $x^2 + 5xy - y^2 = 65$. Case (2) of the theorem applies with $X' = X = \{x | x^2 - 65 \leqq 0\} = \{x | \, |x| \leqq 8\}$, $Y' = Y = \{y | -y^2 - 65 \geqq 0\} = \varnothing$. In order for $x^2 - 5xy - y^2 = 65$ to be solvable in y, $(-5x)^2 - 4(-1)(x^2 - 65) = 29x^2 - 260$ must be a perfect square, which means $x = \pm 3$ or ± 6. If $x = \pm 3$, $y = \pm 7$ or ± 8; if $x = \pm 6$, $y = \pm 1$ or ± 29. Using the formulas $x' = -x - 5y$, $y' = -y + 5x$ we generate the chains

$$\cdots \underline{1023} \quad -197 \quad \underline{-38} \quad 7 \quad \underline{3} \quad 8 \quad \underline{-43} \quad -223 \quad \underline{1158} \cdots$$

$$\cdots \underline{291} \quad -56 \quad \underline{-11} \quad 1 \quad \underline{6} \quad 29 \quad \underline{-151} \quad -784 \quad \underline{4071} \cdots$$

in which all x-values are underlined, along with the negatives of these chains. Going back to u and v we get the following list of all solutions to the original equation: $v = 1, u = -10$ or 7; $v = 7$, $u = -31$ or 10; $v = 8$, $u = -35$ or 11; ...; $v = -784$, $u = -935$ or 3287; ...; and their negatives.

A similar example [1, p. 330] is $u^2 + uv - 7v^2 = 35$. Upon setting $u = x + 2y$, $v = y$ this becomes $x^2 + 5xy - y^2 = 35$, so that $X' = \{x | \, |x| \leqq 6\}$ and $Y' = \varnothing$. Here $29x^2 - 140$ must be a perfect square, leading to the values $x = \pm 3, \pm 4$. From these we go back to the solutions $(u, v) = (6, 1), (7, 2), (29, 13), (42, 19)$ from which all other solutions may be generated.

EXAMPLE 3. $x^2 - 97xy + y^2 + 53x - 29y + f = 0, f = 61, 71$.

(a) $f = 61$. Case 1 of the theorem applies.

$$X = \{x | x^2 + 53x + 61 \leqq 0\} = \{-2, -3, \ldots, -51\},$$

$$Y = \{y | y^2 - 29y + 61 \leqq 0\} = \{0, 1, 2, \ldots, 27\},$$

$$W = \{w | -95w^2 + 24w + 61 \geqq 0\} = \{0\}, \text{ so}$$

we let $X' = W = \{0\}$, $Y' = Y \cup W = \{0, 1, 2, \ldots, 27\}$. $x = 0$ is impossible; so every chain of solutions has some member of Y as a y-value. Solving for x by the quadratic formula, we get

$$2x = 97y - 53 \pm \sqrt{9405y^2 - 10166y + 2565}.$$

So $9405y^2 - 10166y + 2565$ must be a perfect square. Trying successively $y = 0, 1, 2, \ldots, 27$ we find there are no solutions. Classically, one sets $9405y^2 - 10166y + 2565 = v^2$, multiplies through by 4(9405), completes the square on y, and sets $u = 2(9405)y - 10166$. This yields $u^2 - 4(9405)v^2 = (10166)^2 - 4(9405)(2565)$, i.e., $u^2 - 37620v^2 = 6852256$. One now has the unpleasant task of showing that this equation has no solution, or at least no solution which will make y an integer. In a private communication, Daniel Shanks showed that this equation is unsolvable.

(b) $f = 71$. X and Y are the same as in (a), W is now $\{0, 1\}$. So we let $X' = \{0, 1\}$, $Y' = \{0, 1, 2, \ldots, 27\}$. As before, $x = 0$ is impossible; however, we do have the solution $x = 1$, $y = 1$. Solving for x we find that now $9405y^2 - 10166y + 2525$ must be a square. Testing $y = 0, 1, 2, \ldots, 27$ we get $y = 1$ as the only possibility. Therefore, all solutions lie in the single chain $\cdots$ 125 $\underline{1}$ 1 $\overline{86}$ 8370 $\cdots$ generated by (1, 1) and the relations $y' = -y + 97x + 29$, $x' = -x + 97y - 53$. To determine these solutions classically one must solve the Pell equation $u^2 - 4(9405)v^2 = 1$, not an easy task in itself, and then enumerate by hand all solutions to $u^2 - 4(9405)v^2 = (10166)^2 - 4(9405)(2525) = 8357056$ satisfying certain bounds (see [3, p. 205, Theorem 108]).

By constructing an appropriate list of squares, one can, using the above techniques, easily determine the range of $x^2 - 97xy + y^2 + 53x - 29y$ between given bounds. For instance, the only possible values of f, $0 < f \leqq 100$, are 28, 52, 54, 71, and 78. We know of no reasonable way of doing this by classical methods, as each value of f must be dealt with separately. In theory the entire range can be characterized, as in [1, p. 328, Example 3], but it is difficult to apply those methods to the present example.

We close with an easy corollary, one of several that may be drawn from our theorem.

COROLLARY. *Suppose $a > 0$, $b \neq 0$, a divides b, c divides b, and either $c > 0$ and $a \pm b + c < 0$ or $c < 0$. Let m be an integer. Then $ax^2 + bxy + cy^2 = m$ is solvable in integers x, y if and only if there exists a solution (x, y) with $|x| \leqq \sqrt{|m|}$ or $|y| \leqq \sqrt{|m|}$. If m is positive, this can be improved to $|x| \leqq \sqrt{|m/a|}$ or $|y| \leqq \sqrt{|m/c|}$.*

REFERENCES

1. W. Adams, and L. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, N.J., 1976.

2. W.H. Mills, *A method for solving certain Diophantine equations*, Proc. Amer. Math. Soc. **5** (1954), 473–475.

3. Trygve Nagell, *Introduction to Number Theory*, Chelsea, New York, 1964.

4. J.C. Owings, Jr., *An elementary approach to Diophantine equations of the second degree*, Duke Math. Jour. **37** (1970), 261–273.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742