QUADRATIC DIOPHANTINE EQUATIONS IN THE RATIONAL AND QUADRATIC FIELDS

BY

IVAN NIVEN

1. **Introduction and summary.** It is well known that the equation

$$lx + my + n = 0, \tag{1}$$

with rational integral coefficients, has either no solution in rational integers or an infinite number of solutions. The same result is true in quadratic fields, that is, when l, m and n are integers of a given quadratic field, and solutions are sought among the integers of the field.

We are here concerned with the number of integral solutions of the general quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \qquad a \neq 0; A = b^2 - 4ac, \tag{2}$$

with integral coefficients from the field of rational numbers or from some quadratic field. The quantity A is defined for convenient reference. We can take $a \neq 0$ without any loss of generality, by the use (if necessary) of linear transformations of determinant unity (so that the number of integral solutions is not changed).

First, suppose that the coefficients of (2) are rational integers. If A is negative, then the graph of (2) is finite in extent, and there is at most a finite number of solutions in integers. If $A \geqq 0$, the graph of (2) is a parabola, an hyperbola, or two straight lines, and we prove the following result.

THEOREM 1. *Let the coefficients of equation* (2) *be rational integers, with* $A \geqq 0$. *Then if* (2) *has one solution in integers, it has an infinite number, with the following exceptions: if* (2) *represents two essentially irrational straight lines, it has at most one integral solution; if* (2) *is an hyperbola whose asymptotes are essentially rational, then it has at most a finite number of integral solutions.*

By an *essentially rational* straight line, we mean one whose equation can be put in the form (1), with rational integral coefficients; otherwise we say that a line is *essentially irrational.*

Next, suppose that the coefficients of (2) are from a real quadratic field. It turns out in this case that we can have an infinite number of integral solutions when the curve is finite in extent. Also, the hyperbola does not divide into two cases, as it does in Theorem 1. Before stating the theorem, we recall the definition that a totally negative quadratic integer is a negative integer

Presented to the Society, September 5, 1941; received by the editors April 29, 1941.

whose conjugate is also negative. Thus $-5-2^{1/2}$ is totally negative, whereas $-5-4\ (2^{1/2})$ is negative but not totally negative.

THEOREM 2. *Let the coefficients of* (2) *be integers of a real quadratic field F. Then if* (2) *has one solution in integers of F, it has an infinite number, except in the following cases: if* (2) *represents a point, or a pair of straight lines whose coefficients are essentially outside the field F, then it has at most one integral solution in F; if* (2) *represents an ellipse (so that A is negative), and A is totally negative, then it has at most a finite number of integral solutions in F.*

Finally, suppose the coefficients of (2) are from an imaginary quadratic field. Our result is much the same, but there are interesting differences.

THEOREM 3. *Let the coefficients of* (2) *be integers of an imaginary quadratic field F. Then one solution of* (2) *in integers implies an infinite number of such solutions, with the following exceptions: if the left side of* (2) *factors into two linear expressions in x and y, with coefficients essentially outside F, then* (2) *has at most one integral solution in F; if $A \neq 0$ is the square of an integer of F, and the left side of* (2) *is not factorable into linear expressions in x and y, then* (2) *has at most a finite number of integral solutions in F.*

In proving Theorems 2 and 3, we use the Pell equation in quadratic fields,

$$\xi^2 - \gamma\eta^2 = 1. \tag{3}$$

In this connection, we prove the following theorem.

THEOREM 4. *Let γ be an integer, not zero, of a quadratic field F. Then equation* (3) *has an infinite number of integral solutions (ξ, η) in the field F if and only if γ is not the square of an integer of F when F is imaginary, and γ is not totally negative when F is real.*

That the conditions of this theorem are sufficient to insure an infinite number of solutions of (3), is proved in the next two sections. The necessity of the conditions follows from Theorems 2 and 3, as we shall see at the end of §3.

Theorems 1, 2, and 3 are sufficiently similar that the principal results can be proved by a common method; this is presented in §4. Then the theorems are completed in the last three sections. The methods employed throughout the paper are elementary.

2. **The Pell equation in quadratic fields.** If γ is a positive rational integer, not a square, it is well known that equation (3) has an infinite number of solutions in rational integers. We can obtain a similar result for quadratic fields from a classical theorem on the units of relatively cyclic fields.

Let γ now be an integer of a quadratic field F. If γ is not a perfect square in F, and not a rational integer, then the biquadratic field $K = R(\gamma^{1/2})$ is rela-

tively cyclic of prime order two over F. It is known(1) that there exists a relative unit of norm 1 in the field K over F, provided that among the four conjugate fields determined by K there are twice as many real fields as there are among the two conjugate fields determined by F. This condition is satisfied when F is an imaginary field, because the conjugate of F, being identical with F, is also imaginary; consequently, equation (3) has a non-trivial integral solution (that is, a solution with $\eta \neq 0$) in F provided γ is not a perfect square in F.

On the other hand, if F is a real quadratic field, then it is again identical with its conjugate, and we require K and its conjugates to be real. Now K and its conjugates are identical in pairs, each field being either $R(\gamma^{1/2})$ or $R(\bar{\gamma}^{1/2})$, where $\bar{\gamma}$ is the conjugate of γ in F. These are real provided that γ and $\bar{\gamma}$ are positive, or in other words, provided that γ is totally positive. Hence we can conclude that if γ is a totally positive integer of a real quadratic field F, then equation (3) has a non-trivial integral solution in F.

Having one solution of (3), we can obtain more by means of the composition formula

$$(\xi_1^2 - \gamma\eta_1^2)(\xi_2^2 - \gamma\eta_2^2) = (\xi_1\xi_2 + \gamma\eta_1\eta_2)^2 - \gamma(\xi_1\eta_2 + \xi_2\eta_1)^2.$$

This provides an infinitude of different solutions. For example, a non-trivial solution compounds with itself to give a different non-trivial solution. We have proved this lemma.

LEMMA 1. *Let γ be an integer, not a square, of any quadratic field F. Let γ be totally positive if F is real. Then equation* (3) *has an infinite number of integral solutions in F.*

3. **Real quadratic fields.** Lemma 1 is not the best possible result for real quadratic fields. We now prove:

LEMMA 2. *If γ is a positive, but not totally positive, integer of a real quadratic field F, then equation* (3) *has an infinite number of integral solutions in F.*

We prove this by a method analogous to that of Dirichlet(2) for rational and Gaussian integers. Let F be obtained by extending the rational numbers by $m^{1/2}$, m being positive, square-free, and greater than 1. Then γ has the form $a+bm^{1/2}$, where $a-bm^{1/2}$ is negative. For convenience, let δ denote the positive square root of γ. For any positive rational integer n, we let v range over the values $1, 2, \cdots, n+1$. Let u be the greatest integer less than $vm^{1/2}$, that is, $u = [vm^{1/2}]$, and we have

(1) Cf. David Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4, p. 275 (Theorem 92) and p. 279.

(2) Cf. Dickson, *History of the Theory of Numbers*, vol. 2, p. 373.

$$|u - vm^{1/2}| < 1. \tag{4}$$

Choose y and x as follows:

$$y = [\delta(u + vm^{1/2})/(2m^{1/2})], \qquad x = [\delta(u + vm^{1/2}) - ym^{1/2}] + 1.$$

These equations imply the inequalities

$$0 \leqq \delta(u + vm^{1/2}) - 2ym^{1/2} < 2m^{1/2},$$

and

$$0 < x + ym^{1/2} - \delta(u + vm^{1/2}) \leqq 1, \tag{5}$$

respectively, and these add to give the result

$$0 < x - ym^{1/2} < 1 + 2m^{1/2}. \tag{6}$$

As v ranges over the integers $1, 2, \cdots, n+1$ the expression involved in (5) takes values between 0 and 1, at least two of which differ by less than $1/n$. We subtract these to obtain

$$X + Ym^{1/2} - \delta(U + Vm^{1/2}) < \frac{1}{n}, \tag{7}$$

and the inequalities (4) and (6) imply that the rational integers X, Y, U and V satisfy

$$|U - Vm^{1/2}| < 2, \qquad |X - Ym^{1/2}| < 1 + 2m^{1/2}. \tag{8}$$

Using the fact that $|V| \leqq n$, we can write

$$\begin{aligned} |X + Ym^{1/2} + \delta(U + Vm^{1/2})| &\leqq |X + Ym^{1/2} - \delta(U + Vm^{1/2})| + 2|\delta(U + Vm^{1/2})| \\ &< \frac{1}{n} + 2\delta|U - Vm^{1/2}| + 2\delta|2Vm^{1/2}| \\ &< \frac{1}{n} + 2\delta(2 + 2nm^{1/2}). \end{aligned}$$

The multiplication of this inequality by (7) gives

$$|(X + Ym^{1/2})^2 - \delta^2(U + Vm^{1/2})^2| < 1 + 2\delta(2 + 2m^{1/2}),$$

and we set $\xi = X + Ym^{1/2}$ and $\eta = U + Vm^{1/2}$ to obtain

$$|\xi^2 - \gamma\eta^2| < 1 + 2\delta(2 + 2m^{1/2}). \tag{9}$$

We now show that this inequality is satisfied by an infinitude of pairs (ξ, η). The left side of inequality (7) is not zero, for otherwise δ would be an element of the field F. Then γ, being the square of an element of F, would be totally positive, contrary to hypothesis. Now if the number of pairs of quad-

ratic integers satisfying (9) were finite, the rational integer n could be chosen so large that none of these pairs would satisfy (7). Our method would therefore give another pair of values satisfying (7) and (9).

Having shown that (9) represents an infinite number of inequalities, we now show that $\xi^2-\gamma\eta^2$ assumes only a finite set of values. We cannot conclude this directly from inequality (9), because there are infinitely many integers of a real quadratic field which are less in absolute value than a given positive quantity. However, there is but a finite number of integers of such a field which, *together with their conjugates*, are bounded in absolute value. Since $\bar{\gamma}$ is negative, we can use (8) to obtain

$$\left|\bar{\xi}^2-\bar{\gamma}\bar{\eta}^2\right| = (X-Ym^{1/2})^2-\bar{\gamma}(U-Vm^{1/2})^2 < (1+2m^{1/2})^2-\bar{\gamma}(4).$$

Hence the infinite set of quadratic integers $\xi^2-\gamma\eta^2$ of inequality (9) ranges over a finite set of values. At least one of these values, say ρ, is equal to $\xi^2-\gamma\eta^2$ for an infinite number of pairs

$$(\xi_1, \eta_1), (\xi_2, \eta_2), \cdots . \tag{10}$$

We now show that it is possible to select from (10) an infinite subsequence

$$(\xi_{i_1}, \eta_{i_1}), (\xi_{i_2}, \eta_{i_2}), \cdots , \tag{11}$$

such that

$$\begin{aligned} \xi_{i_j}-\xi_{i_k} &\equiv 0 \pmod{\rho}, \\ \eta_{i_j}-\eta_{i_k} &\equiv 0 \pmod{\rho}. \end{aligned} \qquad (j, k = 1, 2, 3, \cdots), \tag{12}$$

Let the quantities $\xi_1, \xi_2, \cdots$ of (10) be written as

$$X_1+Y_1m^{1/2}, X_2+Y_2m^{1/2}, \cdots , \tag{13}$$

the X_i and Y_i being rational integers. Let $N(\rho)$ denote the norm of ρ. Since each X_i $(i=1, 2, \cdots)$ is congruent to some term of the complete residue system 0, 1, 2, $\cdots$, $N(\rho)-1$, modulo $N(\rho)$, it follows that an infinite number of these are congruent to one particular term of this residue system. Thus from (13) we have selected an infinite subsequence, and from the latter we can select another so that the Y_j are congruent to one another modulo $N(\rho)$. We continue this process of selecting subsequences with the terms η_i of (10), and obtain finally a sequence (11) such that congruences analogous to (12) hold modulo $N(\rho)$, and these imply (12).

We now select two different pairs from (11), say (ξ_r, η_r) and (ξ_s, η_s); let these be independent in the sense that one pair is not the negative of the other pair. They satisfy the relations

$$\xi_r^2-\gamma\eta_r^2 = \xi_s^2-\gamma\eta_s^2 = \rho, \tag{14}$$

and we multiply these equations to get

$$(\xi_r\xi_s - \gamma\eta_r\eta_s)^2 - \gamma(\xi_r\eta_s - \xi_s\eta_r)^2 = \rho^2. \tag{15}$$

But the congruences (12) imply that the integer $\xi_r\eta_s - \xi_s\eta_r$ is divisible by ρ. Consequently $\xi_r\xi_s - \gamma\eta_r\eta_s$ is divisible by ρ, and we obtain a solution of (3) by dividing (15) by ρ^2. The solution thus obtained is not trivial, that is, $\xi_r\eta_s - \xi_s\eta_r \neq 0$. For otherwise we could write $\xi_r = k\xi_s$ and $\eta_r = k\eta_s$ with $k \neq \pm 1$, and these relationships contradict (14). Noting that an infinite number of solutions of (3) can now be obtained by the method set forth at the end of §2, we have completed the proof of the lemma.

LEMMA 3. *Let γ be a negative, but not totally negative, integer of a real quadratic field F. Then equation* (3) *has infinitely many integral solutions in F.*

This is a direct consequence of Lemma 2. For, by hypothesis the integer $\bar{\gamma}$ is positive. Hence there are infinitely many solutions of

$$\xi^2 - \bar{\gamma}\eta^2 = 1.$$

The conjugates of these solutions are solutions of (3), and the lemma is proved.

LEMMA 4. *Suppose that $\gamma = \alpha^2 \neq 0$, where α is an integer of a real quadratic field F. Then equation* (3) *has an infinite number of integral solutions in F.*

As in Lemma 2, we take F to be $R(m^{1/2})$. When α is multiplied by its conjugate $\bar{\alpha}$, the result is a rational integer, the norm of α, say n. Now there are infinitely many pairs of rational integers satisfying

$$u^2 - mn^2v^2 = 1,$$

since mn^2 is not a square. Taking $\xi = u$ and $\eta = m^{1/2}\bar{\alpha}v$, we obtain infinitely many solutions of (3).

Lemmas 1, 2, 3, and 4 give all cases of Pell equations (3) in quadratic fields with an infinite number of solutions, for it is a consequence of Theorems 2 and 3 that equation (3) can have but a finite number of integral solutions for values of γ other than those stated in the above lemmas. Thus, upon proving these theorems, we shall have Theorem 4 as a consequence.

4. **The general theory.** We return our attention to equation (2), the coefficient field F being the rational numbers or some quadratic field. Solving for x we get

$$x = \frac{1}{2a}\{-by - d \pm (Ay^2 + By + C)^{1/2}\}, \tag{16}$$

where $B = 2bd - 4ae$ and $C = d^2 - 4af$.

Case 1. $B^2 - 4AC \neq 0$; A is positive and not a square when F is the field of rational numbers; A is neither zero nor totally negative when F is a real quad-

ratic field; A is not the square of an integer of F when F is an imaginary quadratic field. With these hypotheses, we show that one integral solution of (2) implies an infinite number. Let there be such a solution (x_0, y_0). Then there exists an integer t_0 such that the equation

$$t^2 = Ay^2 + By + C \tag{17}$$

is satisfied by the values t_0, y_0. We substitute these values in (17), and subtract the result from (17), to get an equation which can be written in the form

$$(t - t_0)(t + t_0) = (y - y_0)(Ay + Ay_0 + B). \tag{18}$$

We look for integral solutions of this equation. We write

$$p(y - y_0) = 2aq(t + t_0), \quad 2aq(Ay + Ay_0 + B) = p(t - t_0), \tag{19}$$

where p and q will be specified later. Eliminating t from these equations, we get

$$(p^2 - 4a^2Aq^2)y = p^2y_0 + 4a^2q^2(Ay_0 + B) + 4pqat_0. \tag{20}$$

By the hypotheses of the case under discussion, and by the lemmas of the last two sections, we can choose the integers p and q in infinitely many ways so that

$$p^2 - 4a^2Aq^2 = 1. \tag{21}$$

Thus we obtain integral values for y in (20). These, in turn, give integral values for t in (19), as can be seen by eliminating y from these equations.

We now make certain that these values of y give integral values of x in (16). Multiplying the first equation in (19) by p, and eliminating p^2 by the use of (21), we see that

$$(y - y_0) + 4a^2A(y - y_0) = 2apq(t + t_0).$$

Hence $y \equiv y_0 \pmod{2a}$, and the same argument applied to the second equation in (19) shows that $t \equiv t_0 \pmod{2a}$. These imply the congruence

$$-by - d \pm t \equiv -by_0 - d \pm t_0 \pmod{2a}.$$

Since y_0 and t_0 give the integral value x_0 in (16), this congruence shows that our method gives integral values for x, provided that the sign is chosen properly.

Finally we must demonstrate that the above procedure gives an infinitude of solutions of (16). Using (21) to eliminate p^2 from (20), we have

$$y = y_0 + 4aq\{aq(2Ay_0 + B) + pt_0\}. \tag{22}$$

First, suppose that $t_0 = 0$. Then $2Ay_0 + B \neq 0$, for otherwise we could write $y_0 = -B/2A$, and these values of t_0 and y_0, when substituted in (17), give $B^2 - 4AC = 0$, contrary to hypothesis. Also $a \neq 0$, so that the coefficient of q^2

in (22) is not zero. Consequently, each different value of q^2 gives a different value of y.

In the second place, if $t_0 \neq 0$, we show that of all the values satisfying (21), only a finite number give $y = y_0$ in (22). Values of p and q giving $y = y_0$ satisfy $aq(2Ay_0 + B) + pt_0 = 0$, and the result of eliminating p from (21) by means of this equation is

$$q^2\{(2aAy_0 + aB)^2 - 4a^2At_0^2\} = t_0^2.$$

This is satisfied by not more than two values of q.

Suppose now that equation (22) gives only a finite set of values, say $y_0, y_1, \cdots, y_r$. We select a rational prime π which does not divide any of $y_1 - y_0, y_2 - y_0, \cdots, y_r - y_0$. Let (P, Q) be such a solution of

$$P^2 - 4a^2A\pi^2Q^2 = 1$$

that the corresponding solutions $p = P$, $q = \pi Q$ of (21) do not give $y = y_0$ in (22). Then the value y thus obtained from (22), having the property that $y - y_0$ is divisible by π, is different from $y_1, y_2, \cdots, y_r$. We have shown, therefore, that (22) gives an infinite set of different values.

Case 2. $A = 0$, $B^2 - 4AC \neq 0$, so that $B \neq 0$. Again we assume one integral solution (x_0, y_0) of (16), and show that it can be used to generate an infinite number. Proceeding as we did in the first case, we get the following equation analogous to (18)

$$E(y - y_0) = (t - t_0)(t + t_0).$$

We write

$$y - y_0 = 2aq(t + t_0), \qquad t - t_0 = 2aqB,$$

where q is any integer of F. Eliminating t from these equations, we have

$$y = 4a^2q^2B + 4aqt_0 + y_0.$$

The coefficient of q^2 is not zero, and hence this formula gives an infinitude of integral values of y. As in Case 1, we have $y \equiv y_0$ and $t \equiv t_0 \pmod{2a}$, so that the values of y give integral values of x in (16).

Case 3. $B^2 - 4AC = 0$; neither A nor C is negative when F is a real field. In other words, we are now treating the case where the left side of equation (2) factors into two linear expressions, both being real when F is real. Equation (16) can be written in the form

$$2ax + by + d = \pm (A^{1/2}y + C^{1/2}).$$

If both $A^{1/2}$ and $C^{1/2}$ are in F, then these linear equations have integral coefficients from F. As was remarked at the beginning of §1, one integral solution implies an infinite number.

If $A^{1/2}$ is in F, but $C^{1/2}$ is not, then obviously there is no integral solution in F, for such a solution would enable us to write $C^{1/2}$ as an element of F.

If $C^{1/2}$ is in F, but $A^{1/2}$ is not, then any solution (x_0, y_0) must have $y_0=0$. Also, since $B=2A^{1/2}C^{1/2}$, and B is in F, it follows that $C=0$. Hence the only possible solution is $y_0=0$, $x_0=-d/2a$.

If neither $A^{1/2}$ nor $C^{1/2}$ is in F, any integral solution (x_0, y_0) must be such that $A^{1/2}y_0+C^{1/2}=0$, which fixes the value of y_0; and x_0 must therefore satisfy $2ax+by_0+d=0$, so that there cannot be more than one solution.

5. **The rational case.** We now prove Theorem 1; the coefficients of (2) are taken to be rational integers. The case in which (2) represents a pair of straight lines was treated in Case 3 in the last section. If (2) represents a parabola, then $A=0$ and $B\neq 0$. This was discussed in Case 2 in the last section. Hence we can complete the proof of Theorem 1 by treating the hyperbola. We prove this lemma.

LEMMA 5. *Let* (2) *represent an hyperbola, so that* $A>0$ *and* $B^2-4AC\neq 0$. *Then the asymptotes are essentially rational if and only if* A *is a perfect square.*

First, if the asymptotes are rational, we can write (2) in the form

$$a(x+\alpha_1 y+\beta_1)(x+\alpha_2 y+\beta_2)=\delta, \tag{23}$$

where α_1, α_2, β_1, and β_2 are rational, and the asymptotes are obtained by equating to zero the expressions in parentheses. Equating coefficients in (2) and (23), we obtain

$$b=a(\alpha_1+\alpha_2), \qquad c=a\alpha_1\alpha_2.$$

Hence we can write

$$A=b^2-4ac=a^2(\alpha_1+\alpha_2)^2-4a^2\alpha_1\alpha_2=a_2(\alpha_1-\alpha_2)^2.$$

The integer A is the square of a rational number, and consequently is the square of a rational integer.

Conversely, suppose that $A=k^2\neq 0$. In order to show that the asymptotes are rational, we exhibit them. Multiplying (2) by $4a$, we have

$$(2ax+by)^2-k^2y^2+4adx+4aey+4af=0.$$

Multiplying by k^2, and completing the squares, we obtain

$$(2akx+bky+dk)^2-(k^2y-2ae+bd)^2=T, \tag{24}$$

where T is given by

$$d^2k^2-4afk^2-(2ae-bd)^2. \tag{25}$$

The asymptotes of the hyperbola are obtained by factoring the difference of two squares on the left of (24), and equating the factors to zero. It is obvious that they are rational lines, and this completes the proof of the lemma.

We now consider Case 1 of §4 in the light of Lemma 5, and see that we have proved that an hyperbola (2), with irrational asymptotes, has either no integral solutions or an infinite number. To complete the proof of Theorem 1, we must show that an hyperbola (2), with rational asymptotes, cannot have an infinite number of integral solutions.

Let (x_0, y_0) be a point with integral coordinates lying on the hyperbola. Let equation (1), with rational integral coefficients, denote an asymptote. Then the distance from the point on the curve to the asymptote is

$$\left| \frac{lx_0 + my_0 + n}{(l^2 + m^2)^{1/2}} \right| \geqq \frac{1}{(l^2 + m^2)^{1/2}},$$

since lx_0+my_0+n is a nonzero integer. But the asymptotes approach the curve, so that the points of the hyperbola whose distances from the adjacent asymptote are greater than any given positive quantity, must lie in a finite region of the plane. Consequently, only a finite number of points with integral coordinates lie on the hyperbola.

6. **The proof of Theorem 2.** Let the coefficients of (2) be integers of a real quadratic field. If (2) represents a point, then obviously it cannot have more than one integral solution. The situation in which (2) represents a pair of straight lines was treated in Case 3 of §4; a parabola in Case 2; an hyperbola, or an ellipse with A not totally negative in Case 1. All that remains is the last statement of Theorem 2, concerning the ellipse with A totally negative; we turn to this now.

Multiplying equation (2) by $4a$, we get

$$(2ax + by)^2 - Ay^2 + 4adx + 4aey + 4af = 0.$$

We multiply by $-A$, and complete the squares to arrive at

$$-AX^2 + Y^2 = (bd - 2ae)^2 - A(d^2 - 4af), \tag{26}$$

where

$$X = 2ax + by + d, \qquad Y = Ay + bd - 2ae. \tag{27}$$

Suppose that the quadratic field with which we are dealing is $R(m^{1/2})$, where m is positive. Then the integer A, being totally negative, has the form

$$-p - qm^{1/2}, \qquad p > \left| qm^{1/2} \right| \geqq 0, \tag{28}$$

where p and q are rational integers, or perhaps the halves of odd rational integers in case $m \equiv 1 \pmod 4$. We are looking for integral values of x and y in $R(m^{1/2})$, so we suppose that $X = w + tm^{1/2}$, and $Y = u + vm^{1/2}$. Let the right side of equation (26) be $r + sm^{1/2}$. The quantities w, t, u, v, r, and s are rational integers (or perhaps the halves of odd rational integers).

Substituting these values in (26), and equating the rational terms, we have the result

$$p(w^2 + t^2m) + 2qmwt + u^2 + v^2m = r. \tag{29}$$

The inequality in (28) enables us to write

$$p(w^2 + t^2m) \geqq 2\,|\,qm^{1/2}\,|\cdot|\,wtm^{1/2}\,| = |\,2qmwt\,|,$$

so that r must not be negative if (29) is to have any solutions. Equation (29) implies that

$$u^2 + v^2m \leqq r, \qquad pw^2 + pmt^2 + 2qmwt \leqq r.$$

Clearly the first of these inequalities has only a finite number of solutions in integers (or halves of odd integers) u and v. The same is true of the second inequality in w and t, because the discriminant of the left side is

$$4q^2m^2 - 4mp^2 < 4q^2m^2 - 4m(mq^2) = 0,$$

by (28). Hence the number of integral solutions in X and Y of (26) is finite, and, by (27), the number of integral solutions of (2) is finite.

7. **Imaginary quadratic fields.** We now prove Theorem 3. The situation in which $B^2-4AC=0$, that is, in which the left side of (2) factors, was treated in Case 3 of §4. When $B^2-4AC\neq 0$, Cases 1 and 2 handle the situations with A not a perfect square, and A zero, respectively. All that remains to be proved, therefore, is that (2) cannot have an infinite number of solutions when $B^2-4AC\neq 0$ and A is a perfect square in F, say k^2. We can proceed as in §5, and obtain equations (24) and (25); T must be different from zero, since otherwise the left side of (2) would be factorable into two linear factors, contrary to hypothesis. We use the substitution

$$X = 2akx + bky + dk, \qquad Y = k^2y - 2ae + bd,$$

to write (24) in the form $X^2 - Y^2 = T$, from which we get

$$|\,X - Y\,|\cdot|\,X + Y\,| = |\,T\,|. \tag{30}$$

As in the last section, we show that there is only a finite number of solutions in X and Y, and this implies the result we want. Now the positive rational integer $|\,T\,|$ can be factored into a pair of positive rational integers in but a finite number of ways. Any integral solution of (30) must correspond to one of these factorings. For any such factoring, say $|\,T\,| = rs$, we can write $|\,X-Y\,| = r$ and $|\,X+Y\,| = s$, or vice versa. But there is only a finite number of integers of any imaginary quadratic field with absolute value equal to a given rational integer. Hence we have only a finite number of pairs $(X-Y,\ X+Y)$ satisfying (30), and each pair gives at most one integral solution $(X,\ Y)$.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.