ALL INTEGRAL SOLUTIONS OF $ax^2+bxy+cy^2=w_1 w_2 \cdots w_n$*

BY L. E. DICKSON

1. *Literature.* This Diophantine equation (or cases of it) has been treated in two papers by the writer and two by Professor Wahlin, all published in this BULLETIN†. Three of these papers were based on the theory of algebraic ideals. The writer's paper of 1923 employed an elementary method to find all integral solutions of $x^2-my^2=zw$. The present paper is elementary and is a sequel to the latter paper.

2. *Reduction to the Case $n=2$.* Let q denote a quadratic form in x and y. The problem to solve $q=zw$ shall be called the homogeneous problem. To it will be reduced the problem to solve $q=w_1 \cdots w_n$. Write $z=w_1 \cdots w_{n-1}$. By our solution below of the homogeneous problem $q=zw_n$, x, y, z, w_n are products of an arbitrary integer h by certain functions X, Y, Z, W of certain parameters, only two of which, say ξ and η, occur in the quadratic expression $Q(\xi, \eta)$ for Z. Since $w_1 \cdots w_{n-1}=hZ$, evidently $w_i=h_iW_i$ $(i=1, \cdots, n-1)$, where the h_i are integers whose product is h. Hence $q=w_1 \cdots w_n$ is reduced to the solution of $Q(\xi, \eta)=W_1 \cdots W_{n-1}$, which is of the form of our initial equation with n replaced by $n-1$. The resulting values of ξ and η in terms of new parameters are to be inserted in the functions X, Y, and W.

3. *Simplification of the Homogeneous Problem.* The greatest common divisor ω of the coefficients of $q(x, y)$ must

---

* Presented to the Society, September 8, 1926.

† Vol. 27 (1920–1), p. 361; vol. 29 (1923), p. 464; vol. 30 (1924), p. 140; vol. 31 (1925), p. 430.

divide zw. Hence we may write $z=\rho Z$, $w=\sigma W$, where $\rho\sigma=\omega$. Cancellation of ω gives

$$(1) \qquad Q \equiv Ax^2 + Bxy + Cy^2 = ZW,$$

where the greatest common divisor of A, B, C is unity. By Dirichlet's theorem, Q represents an infinitude of primes. Let a be one such odd prime and let $A\kappa^2+B\kappa\lambda+C\lambda^2=a$. Evidently κ and λ are relatively prime. Hence there exist integers μ and ν for which $\kappa\nu-\lambda\mu=1$. Then

$$(2) \qquad x = \kappa X + \mu Y, \qquad y = \lambda X + \nu Y$$

is of determinant unity and transforms Q into a form in which the coefficient of X^2 is a. Thus (1) becomes

$$(3) \qquad aX^2 + 2bXY + cY^2 = ZW.$$

We shall exhibit sets of functions X, Y, Z, W which give all solutions of (3). Insertion in (2) yields like functions giving all solutions of (1).

After removing a common factor, we may assume that the greatest common divisor of X, Y, Z, W is unity. We may write

$$X = dX_1, \quad Y = dY_1, \quad Z = \delta Z', \quad d = \delta D,$$

where X_1 and Y_1 are relatively prime, and likewise Z' and D. Then δ is prime to W, and

$$d^2(aX_1^2 + 2bX_1Y_1 + cY_1^2) = \delta Z'W.$$

Hence δD^2 divides $Z'W$, so that δ divides Z', and D^2 divides W. Write $Z'=\delta Z_1$, $W=D^2W_1$. Hence

$$(4) \qquad aX_1^2 + 2bX_1Y_1 + cY_1^2 = Z_1W_1,$$

$$(5) \qquad X = \delta DX_1, \quad Y = \delta DY_1, \quad Z = \delta^2 Z_1, \quad W = D^2W_1.$$

4. *Method of Solving* (4). Multiply (4) by a and write

$$(6) \qquad m = b^2 - ac, \quad \xi = aX_1 + bY_1, \quad u = aW_1.$$

We get $\xi^2 - mY_1^2 = Z_1 u$. By the writer's paper in this BULLETIN (vol. 29 (1923), p. 464), we have

$$\xi = hx,\ Y_1 = hy,\ Z_1 = hz,\ u = hw, \tag{7}$$

$$z = el^2 + 2flq + gq^2,\ w = en^2 - 2fnr + gr^2, \tag{8}$$

$$x = k(eln + fnq - flr - gqr),\ y = lr + nq, \tag{9}$$

where $k^2 = 1$ and h, l, q, n, r are arbitrary integers, while e, f, g take the finite sets of integral values for which the resulting forms z in (8) include one and only one form from each class of equivalent quadratic forms of discriminant $4m$, whence

$$f^2 - eg = m. \tag{10}$$

Since h divides ξ and Y_1, it divides aX_1. But X_1 and Y_1 are relatively prime. Hence h divides the prime a. Thus $h = \pm 1$ or $\pm a$.

5. *Solutions of* (4) *with* $h = \pm a$. By (5)–(7), we have

$$X = \pm \delta D(x - by),\ Y = \pm \delta Day,\ Z = \pm \delta^2 az,\ W = \pm D^2 w.$$

But if we multiply l and q in (8) and (9) by δ, and n and r by D, we see that z is multiplied by δ^2, w by D^2, and both x and y by δD. Hence the suppression of the factors δD, δ^2, D^2 is equivalent to a change of parameters l, q, n, r. Also the factor ± 1 may be combined with the common factor initially removed from X, Y, Z, W. Hence every solution of (3) with $h = \pm a$ is given by

$$X = s(x - by),\ P = say,\ Z = saz,\ W = sw, \tag{11}$$

where s is an arbitrary integer and x, y, z, w are defined by (8) and (9).

6. *Solutions of* (4) *with* $h = \pm 1$. As in § 5, we may take $h = +1$. Then (6) and (7) give

$$aX_1 + bY_1 = x,\quad Y_1 = y,\quad Z_1 = z,\quad aW_1 = w. \tag{12}$$

The first step is to obtain an integral form of the quotient of w by a. We may replace w in (8) by an equivalent form whose first coefficient is not divisible by a. This is evident unless $e \equiv 0$, $g \equiv 0 \pmod{a}$. Then if f is not divisible by a, we replace r by $r+n$. The case in which also $f \equiv 0 \pmod{a}$ may be excluded* on the ground that m then has the square factor a^2.

Let therefore e be not divisible by the odd prime a. Determine integers E and ϵ so that

$$eE = 1 + \epsilon a. \tag{13}$$

Write $t = en - fr$. By (10), $ew \equiv 0 \pmod{a}$ if and only if $t^2 \equiv mr^2$, and hence by (6) if and only if $t \equiv \pm br \pmod{a}$. Then by (13),

$$n = E(f \pm b)r + av, \tag{14}$$

where v is an integer. Elimination of n from (8_2) gives

$$w = a^2vB + aE(f \pm b)Br - a(f \mp b)vr + Sr^2,$$

where

$$B = \epsilon(f \pm b)r + ev, \qquad S = g - E(f^2 - b^2).$$

By the two values of m in (6) and (10), and by (13),

$$E(f^2 - b^2) = E(eg - ac) = g - aT,\ T = Ec - \epsilon g,\ S = aT. \tag{15}$$

Since all terms of w are now divisible by a, we get †

$$W_1 = aev^2 + 2[a\epsilon(f \pm b) \pm b]vr + [T + E\epsilon(f \pm b)^2]r^2. \tag{16}$$

In the first two equations (12), we insert the value (14) of n. Thus we find

$$Y_1 = qav + [l + qE(f \pm b)]r. \tag{17}$$

---

* Or we may treat this case very simply by noting that the coefficients of w and x in (8) and (9) are now all divisible by a, while b is divisible by a by (6) and (10), whence (12) determine X_1 and W_1 integrally.

† The discriminant of this quadratic form in v and r is found to be $4m$.

If $k=\pm 1$ in (9), where the sign is the same as in (14), we find that $x-bY_1$ becomes divisible by a when we apply (13) and (15), whence

$$(18)\qquad \pm X_1 = (el + fq \mp bq)v + [\epsilon l(f \pm b) - qT]r.$$

But if $k=\mp 1$, we get

$$(19)\qquad \begin{aligned} \mp X_1 &= (el + fq \pm bq)v + l\epsilon(f \pm b)r + rP/a,\\ P &= Eq(f \pm b)^2 - gq \pm 2lb. \end{aligned}$$

If $b=\beta a$, (6) shows that m is a multiple Ma of a. Then (10) and (13) give $EMa=Ef^2-g(1+\epsilon a)$, whence

$$(20)\qquad P/a = Eq(\beta^2 a \pm 2f\beta + M) \pm 2l\beta + qg\epsilon.$$

Finally, let b be not divisible by the odd prime a. Then rP is divisible by a either when $r=Ra$ or when the congruence $P\equiv 0 \pmod{a}$ is satisfied by choice of l as a linear function of q and a new parameter L. This value of l or the value Ra of r is to be inserted in (16), (17), (19), and $Z_1=z$ of (8).

If we multiply v and r (or R) by D, and q and l (or L) by δ, we see that Z_1 is multiplied by δ^2, W_1 by D^2 and both X_1 and Y_1 by δD. Hence the suppression of the factors δD, δ^2, and D^2 from (5) is equivalent to a change of parameters v, r, etc. Hence every solution of (3) with $h^2=1$ is obtained by multiplying an arbitrary integer by (16), (17), z of (8), and (18) or (19) with P or l or r replaced by the expressions just obtained.

THE UNIVERSITY OF CHICAGO