INTEGRAL SOLUTIONS OF $x^2 - my^2 = zw$ *

BY L. E. DICKSON

1. *Statement of the Theorem.* In this BULLETIN (vol. 27 (1920–1), p. 361) I stated that all integral solutions of the equation

$$x^2 - my^2 = zw$$

are obtained by multiplying the right members of

$$(1) \quad z = el^2 + 2flq + gq^2, \qquad w = en^2 - 2fnr + gr^2,$$

$$(2) \quad x = \pm (eln + fnq - flr - gqr), \qquad y = lr + nq,$$

by the same arbitrary integer, where e, f, g take only those sets of integral values (finite in number) for which the first form (1) is a reduced quadratic form having the same discriminant $4m$ as $x^2 - my^2$, so that

$$(3) \qquad f^2 - eg = m.$$

In other words, we employ a single form $el^2 + \cdots$ from each class of quadratic forms of discriminant $4m$. The number of such classes is therefore the number of sets of formulas (1), (2) giving all integral solutions of $x^2 - my^2 = zw$. If we permit the interchange of z and w, we need retain only a single sign in (2). For, if we replace l, q, n, r by $n, -r, -l, q$, respectively, we find that z and w are interchanged, y is unaltered, and x is replaced by $-x$.

In the paper cited, I was led to the above theorem by the theory of ideals, and I gave a proof when there is a single class of quadratic forms.† I stated that a simpler proof of the general theorem follows by composition. I have since found the following still simpler proof.

2. *A Simplification.* Since we may lay aside a common factor of x, y, z, w, consider $X^2 - mY^2 = ZW$, where X, Y, Z, W

*Presented to the Society, December 1, 1923.

† A complete proof of the general theorem by means of ideals has been found recently by G. E. Wahlin.

are integers without a common factor greater than 1. We may write

$$X = dx, \qquad Y = dy, \qquad d = \delta D, \qquad Z = \delta z_1,$$

where x and y are relatively prime, and likewise D and z_1, while δ is prime to W. Then $d^2(x^2 - my^2) = \delta z_1 W$, so that $z_1 W$ is divisible by δD^2. Hence $z_1 = \delta z$, $W = D^2 w$. We have been led back to our initial equation $x^2 - my^2 = zw$ with the simplification that x and y are now relatively prime.

3. *Argument.* If a prime divided both y and w, it would divide x^2 and hence also x, contrary to the last result. Since $y = l$ and $w = g$ are therefore relatively prime, there exist integers f and q such that $x = fl + qg$. Inserting these values of x, y and w in $x^2 - my^2 = zw$, we get

$$zg = (f^2 - m)l^2 + 2fglq + g^2q^2. \tag{4}$$

Since g is prime to l, we have (3), where e is an integer. Cancellation of g gives (1_1).

Let the substitution, with integral coefficients,

$$l = rl_1 + nq_1, \qquad q = sl_1 + tq_1, \qquad rt - ns = 1,$$

replace the first form (1) by a reduced form

$$F(l_1, q_1) = e_1l_1^2 + 2f_1l_1q_1 + g_1q_1^2.$$

The latter is therefore replaced by the former by the inverse substitution

$$l_1 = tl - nq, \qquad q_1 = -sl + rq.$$

Taking $l = 0$ for the moment, we see that the coefficient $g = w$ of q^2 in (1_1) is

$$F(-n, r) = e_1n^2 - 2f_1nr + g_1r^2.$$

Moreover, we have $y = l = rl_1 + nq_1$. Dropping the subscripts, we have the expressions for z, w, y in (1), (2). While the expression (2) for x may be derived from $x^2 - my^2 = zw$ by direct computation, it may be obtained more simply as follows. We have

$$gz = (fl + qg)^2 - ml^2, \qquad gw = (gr - fn)^2 - mn^2, \tag{5}$$

the first being another form of (4). The product of their linear factors is

(6) $$(fl + qg + l\sqrt{m})(gr - fn + n\sqrt{m}) = -g(\pm x - y\sqrt{m}),$$

in view of (2). Taking the product of (6) by the identity derived from it by changing the sign before $\sqrt{m}$, and removing the factor g^2, we get $zw = x^2 - my^2$. Hence x has the values in (2). This proves that conversely (1) and (2) are solutions for all values of l, q, n, r.

4. *Conclusion.* It follows that every set of integral solutions of $x^2 - my^2 = zw$ (with x and y relatively prime) is obtained by multiplying the second members of (1), (2) by the same arbitrary integer. The restriction in parenthesis may be discarded. For, by §2, the general solution of $X^2 - mY^2 = ZW$ in integers is given by

$$X = \delta Dx, \qquad Y = \delta Dy, \qquad Z = \delta^2 z, \qquad W = D^2 w.$$

Let us write

$$L = \delta l, \qquad Q = \delta q, \qquad N = Dn, \qquad R = Dr.$$

Then the values of Z, W, X, Y are derived from (1), (2) by replacing l, q, n, r by L, Q, N, R, respectively.

5. *A Companion Theorem.* The above proof applies without essential change to the solutions of the equation

(7) $$x^2 + xy + \tfrac{1}{4}(1 - m)y^2 = zw, \qquad m \equiv 1 \pmod 4,$$

and hence leads to the companion theorem of the former paper.

6. *Generalization.* As a generalization, consider

(8) $$ax^2 + 2bxy + cy^2 = zw.$$

Multiply by a and write $m = b^2 - ac$, $\xi = ax + by$. Then

(9) $$\xi^2 - my^2 = z \cdot aw.$$

Hence z, aw, ξ, y are given by the products of the right members of (1), (2) by the same arbitrary integer. The second form (1) will be divisible by a prime factor p of a if and only if n and r satisfy two linear homogeneous congruences modulo p (which may coincide); they serve to express n and r in one or two ways as linear homogeneous functions of new parameters

N and R. The initial form (1_2) becomes one or two new quadratic forms in N and R. We proceed similarly with a prime factor of a/p, etc. Finally, we obtain formulas for x from $ax = \xi - by$. We conclude that all integral solutions of (8) are products of the same arbitrary integer by the numbers obtained from a finite number of sets of four expressions each quadratic in four arbitrary parameters. The explicit formulas will be discussed on another occasion.

THE UNIVERSITY OF CHICAGO

ON THE REALITY OF THE ZEROS OF A λ-DETERMINANT *

BY R. G. D. RICHARDSON

Some of the best-known theorems of algebra are centered around the zeros of the polynomial in λ,

$$(1) \qquad \begin{vmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{vmatrix} .$$

In the classical case of the determinant connected with the equations of secular variations, where the elements a_{ij} are real and the determinant $|a_{ij}|$ formed from (1) by omitting the λ's is symmetric ($a_{ij} = a_{ji}$), these zeros turn out to be real. This theorem concerning the reality of the zeros has been extended † to the case where a_{ij} and a_{ji} are conjugate complex ($a_{ij} = \bar{a}_{ji}$). It is proposed in this note to extend it to a still more general case which has arisen in some investigations concerning pairs of bilinear forms just completed by the author. This generalization consists in allowing the coefficients of the λ's to be n^2 in number instead of n as in (1), of allowing them to be various and complex instead of all unity, and of bordering the determinant by m rows and m columns. The

* Presented to the Society October 27, 1923.

† Cf. Kowalewski, *Einführung in die Determinantentheorie*, p. 130.