

PARAMETRIC SOLUTIONS OF CERTAIN
DIOPHANTINE EQUATIONS*

BY T. A. PIERCE

In this note parametric solutions of certain diophantine equations are given. The method of obtaining the solutions is derived from an equation involving the determinants of certain matrices. It will be recognized that the method is a generalization of the method of Euler and Lagrange which depends on forms which repeat under multiplication. The matrices used in this paper must be such that their forms are retained under matrix multiplication and addition. When integer values are assigned to the parameters of our solutions we obtain integer solutions of the particular equation under consideration; however not all integer solutions are necessarily furnished this way.

Let A be a square matrix with elements in a given field; then

$$|A - \lambda I| = f(\lambda) = 0$$

is the characteristic equation of A . If the resultant of $f(\lambda) = 0$ and another equation $g(\lambda) = 0$ be denoted by $R(f, g)$, then it is known† that

$$|g(A)| = R(f, g).$$

If now B is the matrix which has $g(\lambda) = 0$ as its characteristic equation, then

$$|f(B)| = R(g, f)$$

and hence we have

$$(1) \quad |g(A)| = (-1)^{mn} |f(B)|,$$

where m and n are the degrees of $f(\lambda) = 0$ and $g(\lambda) = 0$, respectively. Equation (1) may be identified with diophantine equations of various types as the following examples illustrate.

Let

$$A = \begin{pmatrix} x & \alpha y & \beta z \\ \beta z & x & \alpha y \\ \alpha y & \beta z & x \end{pmatrix}, \quad B = \begin{pmatrix} u & iv \\ iv & u \end{pmatrix},$$

* Presented to the Society, December 30, 1930.

† Frobenius, *Journal für Mathematik*, vol. 84, p. 11.

where $\alpha = (a^2b)^{1/3}$ and $\beta = (ab^2)^{1/3}$, and where a and b are relatively prime integers and neither has a square factor. Then $1, \alpha,$ and β constitute the basis for integers of the pure cubic number field defined by $x^3 - a^2b = 0$, and $|A|$ is the norm of an integer in this field. Again, $|B|$ is the norm of an integer in the field $k(i)$. The characteristic function of A is

$$f(\lambda) = (x - \lambda)^3 + a^2by^3 + ab^2z^3 - 3ab(x - \lambda)yz,$$

and that of B is

$$g(\lambda) = (u - \lambda)^2 + v^2.$$

When calculating $f(B)$, we first expand and then reduce by $g(B) = 0$, since B satisfies its characteristic equation. We obtain

$$g(A) = \begin{pmatrix} X & \alpha Y & \beta Z \\ \beta Z & X & \alpha Y \\ \alpha Y & \beta Z & X \end{pmatrix}, \quad f(B) = \begin{pmatrix} U & iV \\ iV & U \end{pmatrix},$$

where

$$\begin{aligned} X &= x^2 + 2abyz - 2ux + u^2 + v^2, \\ Y &= 2xy + bz^2 - 2uy, \\ Z &= 2xz + ay^2 - 2uz, \\ U &= x^3 + a^2by^3 + ab^2z^3 - 3abxyz + (2u - 3x)(u^2 + v^2) \\ &\quad + (6xu - 3x^2 + 3abyz - 3u^2 + v^2)u, \\ V &= (6xu - 3x^2 + 3abyz - 3u^2 + v^2)v; \end{aligned}$$

and these, by (1), constitute a five-parameter solution of the equation

$$X^3 + a^2bY^3 + ab^2Z^3 - 3abXYZ = U^2 + V^2.$$

If we take

$$A = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}, \quad \text{and} \quad B = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix},$$

we find, by calculating $f(B)$ and $g(A)$ and substituting in (1), that the equation

$$(2) \quad X^2 + Y^2 = Z^2$$

has the two-parameter solution

$$X = (x - u)^2 - y^2 = m^2 - n^2$$

$$Y = 2y(x - u) = 2mn$$

$$Z = (x - u)^2 + y^2 = m^2 + n^2.$$

This is the well known fundamental solution of (2). If

$$A = \begin{pmatrix} x + (-a)^{1/2}y & , & (-b)^{1/2}(u + (-a)^{1/2}v) \\ (-b)^{1/2}(u - (-a)^{1/2}v) & , & x - (-a)^{1/2}y \end{pmatrix},$$

$$B = \begin{pmatrix} p + (-c)^{1/2}q & , & (-d)^{1/2}(r + (-c)^{1/2}s) \\ (-d)^{1/2}(r - (-c)^{1/2}s) & , & p - (-c)^{1/2}q \end{pmatrix},$$

then (1) becomes

$$(3) \quad X^2 + aY^2 + bU^2 + abV^2 = P^2 + cQ^2 + dR^2 + cdS^2$$

and this has the eight-parameter solution

$$X = 2x(p - x) + \theta, \quad P = 2p(x - p) - \theta,$$

$$Y = 2y(p - x), \quad Q = 2q(x - p),$$

$$U = 2u(p - x), \quad R = 2r(x - p),$$

$$V = 2v(p - x), \quad S = 2s(x - p),$$

where

$$\theta = x^2 + ay^2 + bu^2 + abv^2 - (p^2 + cq^2 + dr^2 + cds^2).$$

When arbitrary integral values are assigned to the parameters we obtain a sequence of numbers simultaneously representable by the quaternary forms on either side of (3).

These examples are sufficient to illustrate the nature and extent of our method. It will be noted in particular that the method applies to certain diophantine equations formed by equating the norms of integers in different fields.