A CLASS OF SOLUBLE DIOPHANTINE EQUATIONS

By Morgan Ward

Department of Mathematics, California Institute, Pasadena

Communicated by E. T. Bell, November 21, 1950

1°. Let R be a commutative ring with a unit element, $F(x)$ a homogeneous polynomial of degree n in t indeterminates $x_1, x_2, \ldots, x_t$ with coefficients in R. Let I denote the subring of the coefficients of $F(x)$ in R; that is, the smallest ring containing all of them. We consider the existence of solutions of the diophantine equation

$$F(x) = z^m \tag{1}$$

in R or in I. Here z is an indeterminate and m is a given positive integer.

If $y_1, y_2, \ldots, y_t$ are t new indeterminates and if there exist $t + 1$ polynomials $Q(y)$; $P_i(y)$, $(i = 1, \ldots, t)$, with coefficients in R (or in I) such that

$$F(P(y)) = Q(y)^m \tag{2}$$

identically in the y, (1) will be said to have a t-parameter family of solutions in R (or in I).

2°. Theorem. *If m is prime to the degree n of $F(x)$, then the diophantine equation (1) always has a t-parameter family of solutions $\mathfrak{M}$ both in R and in I.*

For assume that m is prime to n. If m is less than n, write r for m. Then integers k and l exist uniquely determined by n and r such that

$$kn + 1 = lr, \qquad 0 < k < r, \qquad 0 < l < n.$$

Define polynomials $P(y)$; $Q(y)$ by

$$P_i(y) = y_iF(y)^k, \qquad (i = 1, \ldots, t); \qquad Q(y) = F(y)^l.$$

Then the coefficients of the $P(y)$ and $Q(y)$ lie in I. Since $F(x)$ was assumed to be homogeneous of degree n, (2) holds identically in the y with m equal to r.

If m is greater than n, divide m by n and let the quotient be q and the remainder r. Then if m is prime to n,

$$m = qn + r, \qquad 0 < r < n, \qquad r \text{ prime to } n.$$

With k, l, $P(y)$ and $Q(y)$ as before, let

$$y_i^* = y_iF(y)^k \qquad (i = 1, \ldots, t).$$

Then $F(y^*) = Q(y)^r$. Hence if

$$P_i^*(y) = y_i^*Q(y)^q \qquad (i = 1, \ldots, t)$$
$$Q^*(y) = Q(y),$$

then $F(P^*(y)) = Q^*(y)^m$ identically in the y. Since the polynomials $P^*(y)$ and $Q^*(y)$ have their coefficients in I, the proof is complete.

3°. The most interesting case of this theorem is when I is the ring of ordinary integers. For example the diophantine equation

$$x^n + y^n = z^m$$

has a two parameter family of integral solutions for every m prime to n; the diophantine equation

$$x^4 + y^4 + z^4 = z^m$$

has a three-parameter family of integral solutions for every odd m, and so on. Many other special cases occur in the literature.[1]

4°. The family $\mathfrak{M}$ of solutions of (1) in R consists of vectors $[\xi;\ \eta] = [\xi_1, \xi_2, \ldots, \xi_t;\ \eta]$ of the form

$$\begin{aligned} \xi &= P(\alpha), \quad \eta = Q(\alpha) \qquad m < n, \\ \xi &= P^*(\alpha), \quad \eta = Q^*(\alpha) \qquad m > n. \end{aligned}$$

Here α stands for t arbitrarily chosen elements $\alpha_1, \ldots, \alpha_t$ of R or of I. If the α are such that $F(\alpha) = 0$, we obtain the trivial zero solution of (1) and this is evidently the only solution of the family $\mathfrak{M}$ with $\eta = 0$ if R has zero radical. In any event the solutions of (1) in R with $z = 0$ are entirely independent of the choice of m.

5°. If R is a field, it is easy to show that every solution $[\kappa, \lambda]$ of (1) in R with $\lambda \neq 0$ is of the form

$$\kappa_i = \theta^a \xi_i \ (i = 1, 2, \ldots, t);\ \lambda = \theta^b \eta.$$

Here $[\xi;\ \eta]$ belongs to the family $\mathfrak{M}$, a and b are positive integers depending only on m and n, while θ is a field element depending only on λ. Thus in this case, $\mathfrak{M}$ gives essentially all solutions of (1) with $z \neq 0$.

6°. The situation is quite different for the solutions $\mathfrak{M}$ in I if I is a domain of integrity. $\mathfrak{M}$ by no means exhausts the possible solutions of (1) in I; in fact the components ξ, η of any $\mathfrak{M}$ solution will usually have common factors in I. For example, if I is the ring of integers, the diophantine equation

$$x_1^2 x_2 + x_1 x_2^2 = z^m$$

has a two-parameter family of integral solutions $[\xi_1, \xi_2, \eta]$ for every odd prime m other than three. But the existence of a single integral solution with ξ_1, ξ_2 co-prime [other than the trivial solutions (1, 0; 1), (0, 1; 1)] would disprove Fermat's last theorem.

[1] Dickson, *History of the Theory of Numbers*, Vol. 1.