THE SOLUTION OF A DIOPHANTINE EQUATION

CHARLES P. BENNER

Solutions of the diophantine equation[1]

$$\prod_{i=1}^{4} \sum_{j=1}^{3} a_{ij}x_j = f(y_1, \cdots, y_a)$$

have been given. We generalize the equation by solving the equation

$$\prod_{i=1}^{2^n} \sum_{j=1}^{2^n-1} a_{ij}x_j = f(y), \tag{1}$$

in which we suppose that $f(y) = f(y_1, \cdots, y_a)$ is a homogeneous polynomial, with integral coefficients, of degree m, where m is of the form $2^p(2q+1)$, q being a non-negative integer, p is one of the integers $0, 1, \cdots, n-1$, and thus $m \not\equiv 0 \pmod{2^n}$. We suppose further that the rank of the matrix of the forms $\sum_{j=1}^{2^n-1} a_{ij}x_j$ $(i = 1, \cdots, 2^n)$ is 2^n-1 and thus we may choose the notation such that A, the determinant of the first 2^n-1 forms, does not vanish. Let A_{ij} be the cofactor of a_{ij} in A.

THEOREM. *Every integral solution x_j, y_k of* (1) *for which the left-hand member does not vanish is equivalent* (*in a sense to be defined*) *to a solution given by*

$$\begin{aligned} x_j &= A^{m-1}s^qt^q\left[t\sum_{r=1}^{2^{n-1}} \alpha_r A_{rj} + s\sum_{r=2^{n-1}+1}^{2^n-1} \alpha_r A_{rj}\right] \quad (j = 1, \cdots, 2^n-1), \\ y_k &= A^{2^n}s^{2^{n-1-p}}t^{2^{n-1-p}}\beta_k, \end{aligned} \tag{2}$$

where s and t are given by

$$\begin{aligned} s &= \left[\prod_{i=1}^{2^n-1} \alpha_i\right] \sum_{j=1}^{2^n-1} \sum_{r=1}^{2^{n-1}} a_{2^n j}\alpha_r A_{rj}, \\ t &= Af(\beta) - \left[\prod_{i=1}^{2^n-1} \alpha_i\right] \sum_{j=1}^{2^n-1} \sum_{r=2^{n-1}+1}^{2^n-1} a_{2^n j}\alpha_r A_{rj}, \end{aligned} \tag{3}$$

the α's and β's being arbitrary integers.

PROOF. If we set

Received by the editors September 27, 1950 and, in revised form, April 20, 1951.

[1] A. A. Aucoin, *Solution of a quartic diophantine equation*, Boletin Matematico vol. 14 (1941) pp. 36–39.

$$
(4)\qquad
\begin{aligned}
&\sum_{j=1}^{2^n-1} a_{ij}x_j = A^m\alpha_i s^q t^{q+1} && (i = 1, \cdots, 2^{n-1}),\\
&\sum_{j=1}^{2^n-1} a_{ij}x_j = A^m\alpha_i s^{q+1} t^q && (i = 2^{n-1}+1, \cdots, 2^n-1),
\end{aligned}
$$

and solve the system of equations for x_j, we have

$$x_j = A^{m-1}s^q t^q\left[t\sum_{r=1}^{2^{n-1}} \alpha_r A_{rj} + s\sum_{r=2^{n-1}+1}^{2^n-1} \alpha_r A_{rj}\right] \qquad (j = 1, \cdots, 2^n-1),$$

and hence

$$
(5)\qquad
\begin{aligned}
\sum_{j=1}^{2^n-1} a_{2^n j}x_j = A^{m-1}s^q t^q\Bigg[t\sum_{j=1}^{2^n-1}\sum_{r=1}^{2^{n-1}} a_{2^n j}\alpha_r A_{rj}&\\
+ s\sum_{i=1}^{2^n-1}\sum_{r=2^{n-1}+1}^{2^n-1} a_{2^n j}\alpha_r A_{rj}\Bigg]&.
\end{aligned}
$$

If

$$(6)\qquad y_k = A^{2^n}s^{2^{n-1-p}}t^{2^{n-1-p}}\beta_k,$$

then from (4), (5), and (6) equation (1) becomes

$$
(7)\qquad
\begin{aligned}
A^{2^{n+p}(2q+1)-1}s^{2^{n-1}(2q+1)-1}t^{2^{n-1}(2q+1)}(Pt+Qs)\prod_{i=1}^{2^n-1}\alpha_i&\\
= A^{2^{n+p}(2q+1)}s^{2^{n-1}(2q+1)}t^{2^{n-1}(2q+1)}f(\beta)&,
\end{aligned}
$$

where

$$
(8)\qquad
\begin{aligned}
P &= \sum_{j=1}^{2^n-1}\sum_{r=1}^{2^{n-1}} a_{2^n j}\alpha_r A_{rj},\\
Q &= \sum_{j=1}^{2^n-1}\sum_{r=2^{n-1}+1}^{2^n-1} a_{2^n j}\alpha_r A_{rj}.
\end{aligned}
$$

Now (7) is satisfied identically in the α's and β's if s and t are given by (3). Hence a solution of (1) is given by (2) if the left-hand member does not vanish. The solution x_j, y_k is integral if the parameters are integral.

We now define the concept of equivalent solutions. Suppose that $x_j=\rho_j$, $y_k=\gamma_k$ is a solution of the equation

$$f(x_1, \cdots, x_a) = g(y_1, \cdots, y_b),$$

where f and g are homogeneous polynomials with integral coefficients, of degrees n and m respectively. If there are no integers $s>1$, ρ_j', γ_k'

such that $\rho_j = \rho_j' s^\lambda$, $\gamma_k = \gamma_k' s^\mu$, where λ and μ are positive integers such that $\lambda n = \mu m$, then $x_j = \rho_j$, $y_k = \gamma_k$ is defined to be a primitive solution of the given equation. If $x_j = \rho_j$, $y_k = \gamma_k$ is a primitive solution of the given equation and if λ and μ are positive integers such that $\lambda n = \mu m$, then $x_j = \rho_j t^\lambda$, $y_k = \gamma_k t^\mu$, where t is a nonzero integer, is also a solution and is said to be *derived* from this primitive solution. Two solutions are said to be equivalent if they may be derived from the same primitive solution.

It remains to be shown that given any solution of (1) which does not cause the left-hand member to vanish, we may choose the parameters in (2) so as to obtain a solution equivalent to the given one. Suppose that $x_j = \rho_j$, $y_k = \gamma_k$ is any such solution of (1). If we choose $\alpha_i = \sum_{j=1}^{2^n-1} a_{ij}\rho_j$ and $\beta_k = \gamma_k$ then from (1) and (3) we have

$$\begin{aligned} s - t &= \left[\prod_{i=1}^{2^n-1} \sum_{j=1}^{2^n-1} a_{ij}\rho_j \right] \sum_{j=1}^{2^n-1} \sum_{r=1}^{2^n-1} \sum_{h=1}^{2^n-1} a_{2^n j} a_{rh} A_{rj} \rho_h \\ &\quad - A \left[\prod_{i=1}^{2^n} \sum_{j=1}^{2^n-1} a_{ij}\rho_j \right] \\ &= \left[\prod_{i=1}^{2^n-1} \sum_{j=1}^{2^n-1} a_{ij}\rho_j \right] \left[\sum_{j=1}^{2^n-1} a_{2^n j} \sum_{h=1}^{2^n-1} \rho_h \sum_{r=1}^{2^n-1} a_{rh} A_{rj} - A \sum_{j=1}^{2^n-1} a_{2^n j}\rho_j \right] \\ &= \left[\prod_{i=1}^{2^n-1} \sum_{j=1}^{2^n-1} a_{ij}\rho_j \right] \left[A \sum_{j=1}^{2^n-1} a_{2^n j}\rho_j - A \sum_{j=1}^{2^n-1} a_{2^n j}\rho_j \right] = 0 \end{aligned}$$

and therefore $s = t$. Thus (2) becomes

$$x_j = A^{2^p(2q+1)} s^{2q+1} \rho_j, \qquad y_k = A^{2^n} s^{2^n - p} \gamma_k$$

which is equivalent to the solution $x_j = \rho_j$, $y_k = \gamma_k$. Hence we may choose the parameters so as to get a solution equivalent to the given solution $x_j = \rho_j$, $y_k = \gamma_k$, provided that the left member of (1) is not zero.

We may also find integers, not all zero, which will cause the left-hand member of (1) to vanish and these together with $y_k = 0$ will afford additional solutions of (1).

UNIVERSITY OF HOUSTON