DIOPHANTINE EQUATIONS WHOSE MEMBERS ARE HOMOGENEOUS*

A. A. AUCOIN AND W. V. PARKER

Desboves† has stated that a necessary and sufficient condition for the equation $ax^m+by^m=cz^n$ to have a solution in integers is that c be of the form as^m+bt^m. This would seem to imply‡ that the values of c are restricted whatever be the values of m and n. That this is not the case follows from our first theorem:

THEOREM 1. *If f and g are homogeneous polynomials with integral coefficients, of degrees m and n, respectively, where m and n are relatively prime, then the equation*

$$f(x_1, x_2, \cdots, x_r) = g(y_1, y_2, \cdots, y_s) \tag{1}$$

always has solutions in integers x_i and y_j; and every solution in which the members of (1) *do not vanish is equivalent (in a sense to be defined) to one of the infinitude of solutions given by*

$$x_i = \alpha_i[f(\alpha)]^{n-p}[g(\beta)]^p, \qquad y_j = \beta_j[f(\alpha)]^{m-q}[g(\beta)]^q, \tag{2}$$

where α_i and β_j are arbitrary integers, p and q are integers defined by

$$0 \leqq p \leqq n, \qquad 0 \leqq q \leqq m, \qquad mp - nq = 1, \tag{3}$$

and $f(\alpha)=f(\alpha_1, \alpha_2, \cdots, \alpha_r)$, $g(\beta)=g(\beta_1, \beta_2, \cdots, \beta_s)$.

Since m and n are relatively prime, there exist integers p and q§ such that $0\leqq p\leqq n$, $0\leqq q\leqq m$, $mp=nq+1$, and consequently $n(m-q)=m(n-p)+1$.

If in (1) we let

$$x_i = \alpha_i t^p u^{n-p}, \qquad y_j = \beta_j t^q u^{m-q}, \tag{4}$$

we have‖

---

* Presented to the Society, April 15, 1939.

† A. Desboves, *Mémoire sur la résolution en nombres entières de l'équation* $ax^m+by^m=cz^n$, Nouvelles Annales de Mathématiques, (2), vol. 18 (1879), p. 481. An examination of Desboves's proof shows that he really means that c multiplied by the nth power of an integer u must be of the form as^m+bt^m. His statement therefore appears to be a mere tautology.

‡ For other examples suggesting the same notion, see Carmichael, *Diophantine Analysis*, p. 53, example 14; p. 54, example 21; p. 73, examples 24, 25.

§ Barnard and Child, *Higher Algebra*, p. 415.

‖ Since for a homogeneous function of degree n, $f(az)=a^nf(z)$.

$$t^{mp}u^{m(n-p)}f(\alpha) = t^{nq}u^{n(m-q)}g(\beta). \tag{5}$$

If we choose $t=g(\beta)$ and $u=f(\alpha)$, (5) is satisfied identically in the α's and β's. Hence a solution of (1) expressed in terms of $r+s$ arbitrary parameters is

$$x_i = \alpha_i[f(\alpha)]^{n-p}[g(\beta)]^p, \qquad y_j = \beta_j[f(\alpha)]^{m-q}[g(\beta)]^q. \tag{6}$$

If the α's and β's are integers, then x_i and y_j as given by (6) are integers.

An integral solution $x_i=\lambda_i$, $y_j=\mu_j$ of (1) is defined to be a primitive solution if there are no integers $k>1$, λ_i', μ_j' such that $\lambda_i=k^a\lambda_i'$, $\mu_j=k^b\mu_j'$, where a and b are positive integers such that $am=bn$. If $x_i=\lambda_i$, $y_j=\mu_j$ is a primitive solution of equation (1), then $x_i=\lambda_i d^a$, $y_j=\mu_j d^b$ (derived from the primitive solution), where d is an integer different from zero* and a and b are positive integers such that $am=bn$, is also a solution in integers. Two solutions derived from the same primitive solution shall be called equivalent.

Suppose now that $x_i=\lambda_i$, $y_j=\mu_j$ is any primitive solution of (1) for which $f(\lambda)\neq 0$. If in (6) we choose $\alpha_i=\lambda_i$, $\beta_j=\mu_j$, we get the solution

$$x_i = \lambda_i[f(\lambda)]^{n-p}[g(\mu)]^p = \lambda_i[f(\lambda)]^n, \quad y_j = \mu_j[f(\lambda)]^{m-q}[g(\mu)]^q = \mu_j[f(\lambda)]^m$$

which is equivalent to the given primitive solution.

It is interesting to note that when g is a monomial, say $g=cy^n$, the solution may be written in terms of r arbitrary parameters. For in this case (6) becomes

$$x_i = c^p\alpha_i[f(\alpha)]^{n-p}\beta^{np}, \qquad y = c^q[f(\alpha)]^{m-q}\beta^{nq+1} = c^q[f(\alpha)]^{m-q}\beta^{mp},$$

which is equivalent to $x_i=c^p\alpha_i[f(\alpha)]^{n-p}$, $y=c^q[f(\alpha)]^{m-q}$. If $x_i=\lambda_i$, $y=\mu\neq 0$ is a primitive solution in this case, the choice of parameters $\alpha_i=\lambda_i$ gives the solution $x_i=c^n\lambda_i\mu^{n(n-p)}$, $y=c^m\mu^{n(m-q)}=c^m\mu\cdot\mu^{m(n-p)}$ which is equivalent to $x_i=\lambda_i$, $y=\mu$.

The method employed above may be extended to obtain solutions of certain equations in which the members are not homogeneous. The nature of this extension is expressed in the following theorem:

THEOREM 2. *The equation*

$$\sum_{h=1}^{p} a_h \prod_{i=1}^{r} x_i^{\alpha_{hi}} = \sum_{k=1}^{q} b_k \prod_{j=1}^{s} y_j^{\beta_{kj}}, \tag{7}$$

where the a's and b's are integers and each α_{hi}, β_{kj} is a nonnegative integer, always has a solution in integers if there exist nonnegative

* If $d=0$, the solution is trivial.

integers m, n, u_i, v_i, w_j, z_j, $(i=1, 2, \cdots, r; j=1, 2, \cdots, s)$, *such that*

$$\begin{aligned} &\sum_{i=1}^{r} \alpha_{hi}u_i = m, \qquad \sum_{i=1}^{r} \alpha_{hi}v_i = n+1, \qquad h = 1, 2, \cdots, p, \\ &\sum_{j=1}^{s} \beta_{kj}w_j = m+1, \quad \sum_{j=1}^{s} \beta_{kj}z_j = n, \qquad k = 1, 2, \cdots, q; \end{aligned} \tag{8}$$

and every such solution in which the members of (7) *do not vanish is equivalent* (*in a sense to be defined*) *to one of the infinitude of solutions given by*

$$x_i = \alpha_i[f(\alpha)]^{u_i}[g(\beta)]^{v_i}, \qquad y_j = \beta_j[f(\alpha)]^{w_j}[g(\beta)]^{z_j}, \tag{9}$$

where α_i, β_j *are arbitrary integers and*

$$f(\alpha) = \sum_{h=1}^{p} a_h \prod_{i=1}^{r} \alpha_i^{\alpha_{hi}}, \qquad g(\beta) = \sum_{k=1}^{q} b_k \prod_{j=1}^{s} \beta_j^{\beta_{kj}}.$$

If in (7) we let

$$x_i = \alpha_i t^{u_i} u^{v_i}, \qquad y_j = \beta_j t^{w_j} u^{z_j}, \tag{10}$$

we have

$$t^m u^{n+1} f(\alpha) = t^{m+1} u^n g(\beta), \tag{11}$$

where m, n are given by (8). If we choose $t=f(\alpha)$, $u=g(\beta)$, (11) is satisfied identically in the α's and β's. Substituting these values for t, u in (10) gives (9) as a solution of (7).

When conditions (8) are satisfied, there also exist nonnegative integers M, u_i', w_j' such that

$$\sum_{i=1}^{r} \alpha_{hi}u_i' = M, \qquad \sum_{j=1}^{s} \beta_{kj}w_j' = M, \qquad h = 1, 2, \cdots, p;\ k = 1, 2, \cdots, q. \tag{12}$$

If $x_i=\lambda_i$, $y_j=\mu_j$ is an integral solution of (7) and there are no integers u_i', w_j', $d>1$, λ_i', μ_j' such that $\lambda_i=\lambda_i' d^{u_i'}$, $\mu_j=\mu_j' d^{w_j'}$, where u_i' and w_j' satisfy (12), then we say that this solution is primitive.

If $x_i=\lambda_i$, $y_j=\mu_j$ is a primitive solution, then $x_i=\lambda_i d^{u_i'}$, $y_j=\mu_j d^{w_j'}$ (derived from the primitive solution), where $d\neq 0$ is an integer and u_i', w_j' are any nonnegative integers satisfying (12), is also an integral solution. We define two solutions to be equivalent if they are derived from the same primitive solution. With this definition, we may show that (9) gives a solution equivalent to any existing solution of (7) for which the members do not vanish.

Suppose $x_i=\lambda_i$, $y_j=\mu_j$ is any integral solution of (7) and select $\alpha_i=\lambda_i$, $\beta_j=\mu_j$ in (9); then we get

$$x_i = \lambda_i[f(\lambda)]^{u_i+v_i}, \qquad y_j = \mu_j[f(\lambda)]^{w_j+z_j}. \tag{13}$$

Since for $h=1, 2, \cdots, p$; $k=1, 2, \cdots, q$

$$\sum_{i=1}^{r} \alpha_{hi}(u_i + v_i) = \sum_{j=1}^{s} \beta_{kj}(w_j + z_j) = m + n + 1,$$

solution (13) is equivalent to $x_i=\lambda_i$, $y_j=\mu_j$.

An interesting special case of Theorem 2 is the equation

$$\sum_{i=1}^{r} a_i x_i^{p_i} = \sum_{j=1}^{s} b_j y_j^{q_j}, \tag{14}$$

where a_i, b_j are integers, p_i, q_j are positive integers, and the lowest common multiple m of the p_i's is prime to the lowest common multiple n of the q_j's. The solution in this case is

$$x_i = \alpha_i[f(\alpha)]^{m_i(np)}[g(\beta)]^{m_i p}, \qquad y_j = \beta_j[f(\alpha)]^{n_j(mq)}[g(\beta)]^{n_j q},$$

where $m_i=m/p_i$, $n_j=n/q_j$ and p, q are integers satisfying the conditions $0\leqq p\leqq n$, $0\leqq q\leqq m$, and $mp=nq+1$; and $f(\alpha)=\sum_{i=1}^{r} a_i\alpha_i^{p_i}$, $g(\beta)=\sum_{j=1}^{s} b_j\beta_j^{q_j}$.

Equation (14) may be made to satisfy the conditions of Theorem 1. If in (14) we let $x_i=\xi_i t^{m_i-1}$, $y_j=\eta_j u^{n_j-1}$, we get

$$\sum_{i=1}^{r} a_i\xi_i^{p_i} t^{m-p_i} = \sum_{j=1}^{s} b_j\eta_j^{q_j} u^{n-q_j}.$$

This is a homogeneous function of degree m equal to a homogeneous function of degree n where m and n are relatively prime; hence Theorem 1 applies.

It may be pointed out that some equations of the form of (14) which do not satisfy the hypothesis of Theorem 2 may be rearranged so that these conditions are satisfied. For example, we may solve $ax^2+by^3+cz^4=dw^3$ by writing it in the form $ax^2+cz^4=dw^3-by^3$. The same may be said of some equations of type (7).

As an illustration of Theorem 2, the equation $ax^2y+bxz+cyz^2=pu^3+qv$ has solutions $x=\alpha AB^2$, $y=\beta$, $z=\gamma AB^2$, $u=\rho AB$, $v=\sigma A^3B^3$, where $A=a\alpha^2\beta+b\alpha\gamma+c\beta\gamma^2$, $B=p\rho^3+q\sigma$. If x', y', z', u', v' is any solution of the equation, the selection $\alpha=x'$, $\beta=y'$, $\gamma=z'$, $\rho=u'$, $\sigma=v'$ for the parameters gives $x=x'A^3$, $y=y'$, $z=z'A^3$, $u=u'A^2$, $v=v'A^6$, since $A=B$, which is equivalent to the given solution.

LOUISIANA STATE UNIVERSITY