SYSTEMS OF DIOPHANTINE EQUATIONS

A. A. AUCOIN

We first define the concept of equivalent solutions. Suppose $x_k = \alpha_k$, $y_{ij} = \beta_{ij}$ is an integral solution of the system

$$(1) \qquad f_i(x_1, \cdots, x_p) = g_i(y_{i1}, \cdots, y_{iq}) \qquad (i = 1, \cdots, n),$$

where f_i and g_i are homogeneous polynomials with integral coefficients, f_i being of degree n and g_i being of degree m. If there are no integers $s > 1$, α_k', β_{ij}' such that $\alpha_k = s^\lambda \alpha_k'$, $\beta_{ij} = s^\mu \beta_{ij}'$, where λ, μ are positive integers such that $\lambda n = \mu m$, then $x_k = \alpha_k$, $y_{ij} = \beta_{ij}$ is defined to be a primitive solution of (1). If $x_k = \alpha_k$, $y_{ij} = \beta_{ij}$ is a primitive solution of (1), then $x_k = t^\lambda \alpha_k$, $y_{ij} = t^\mu \beta_{ij}$ (derived from the primitive solution), where $t \neq 0$ is an integer, λ, μ are any positive integers such that $\lambda n = \mu m$, is also a solution. Two solutions are said to be equivalent if they may be derived from the same primitive solution.

Our first theorem concerns the solution of the system[1]

$$(2) \qquad \prod_{j=1}^{n} \sum_{k=1}^{q} a_{ijk} x_k = f_i(y_i) \qquad (i = 1, \cdots, n),$$

where $f_i(y_i) = f_i(y_{i1}, \cdots, y_{iq})$ are homogeneous polynomials of degree m, with integral coefficients, and m and n are relatively prime. We make the following preliminary definitions. a_{ijk} are integers, λ, μ are positive integers such that $n\lambda = m\mu + 1$. $p_k^{(h)}$ are integers such that $\sum_{k=1}^{q} a_{ijk} p_k^{(h)} = 0$ $(h = 1, \cdots, n-1; j = 1, \cdots, n-1; i = 1, \cdots, n)$, $A_i = A_i(\alpha) = \prod_{j=1}^{n-1} \sum_{k=1}^{q} a_{ijk} \alpha_k$, $p_{ih} = \sum_{k=1}^{q} a_{ink} p_k^{(h)}$, $p_{in} = p_{in}(\alpha) = \sum_{k=1}^{q} a_{ink} \alpha_k$, $A = A(\alpha) = \prod_{i=1}^{n} A_i$, $\bar{A}_i = A/A_i$, $P = P(\alpha) = |p_{ij}|$ is a determinant of order n, P_{ij} is the cofactor of p_{ij} in P, the α's and β's being arbitrary integers.

THEOREM 1. *Every integral solution x_k, y_{ir} of* (2) *for which $P(x) \neq 0$ and $A(x) \neq 0$ is equivalent to a solution given by*

$$(3) \qquad \begin{aligned} x_k &= \sum_{h=1}^{n-1} p_k^{(h)} s_h t^{\lambda-1} + \alpha_k t^\lambda \qquad (k = 1, \cdots, q), \\ y_{ir} &= PAt^\mu \beta_{ir} \qquad (i = 1, \cdots, n; r = 1, \cdots, g), \end{aligned}$$

Presented to the Society, October 27, 1951; received by the editors July 17, 1950 and, in revised form, April 21, 1951.

[1] Single equations of this type have been solved by two different methods. See A. A. Aucoin and W. V. Parker, *Diophantine equations whose members are homogeneous*, Bull. Amer. Math. Soc. vol. 45 (1939) pp. 330–331. See also A. A. Aucoin, *Diophantine equations of degree n*, Bull. Amer. Math. Soc. vol. 46 (1940) pp. 336–337.

where

$$(4)\qquad \begin{aligned} s_h &= P^{m-1}A^{m-1}\sum_{i=1}^{n}\overline{A}_i f_i(\beta_i)P_{ih} \qquad (h = 1, \cdots, n-1),\\ t &= P^{m-1}A^{m-1}\sum_{i=1}^{n}\overline{A}_i f_i(\beta_i)P_{in}. \end{aligned}$$

PROOF. If we let x_k have the values given by (3), the left-hand member of (2) becomes

$$\prod_{j=1}^{n-1}\sum_{k=1}^{q} a_{ijk}\left[\sum_{h=1}^{n-1} p_k^{(h)} s_h t^{\lambda-1} + \alpha_k t^{\lambda}\right]\sum_{k=1}^{q} a_{ink}\left[\sum_{h=1}^{n-1} p_k^{(h)} s_h t^{\lambda-1} + \alpha_k t^{\lambda}\right]$$

$$= \prod_{j=1}^{n-1}\left[t^{\lambda-1}\sum_{h=1}^{n-1} s_h \sum_{k=1}^{q} a_{ijk}p_k^{(h)} + t^{\lambda}\sum_{k=1}^{q} a_{ijk}\alpha_k\right]$$

$$\cdot t^{\lambda-1}\left[\sum_{h=1}^{n-1} s_h \sum_{k=1}^{q} a_{ink}p_k^{(h)} + t\sum_{k=1}^{q} a_{ink}\alpha_k\right]$$

$$= t^{n\lambda-1}\prod_{j=1}^{n-1}\sum_{k=1}^{q} a_{ijk}\alpha_k\left[\sum_{h=1}^{n-1} s_h p_{ih} + t p_{in}\right]$$

$$= t^{n\lambda-1}A_i\left[\sum_{h=1}^{n-1} s_h p_{ih} + t p_{in}\right].$$

Thus, if x_k, y_{ir} have the values given by (3), (2) becomes, after the multiplication of each equation by the corresponding $\overline{A}_i$,

$$t^{n\lambda-1}A\left[\sum_{h=1}^{n-1} s_h p_{ih} + t p_{in}\right] = P^m A^m \overline{A}_i t^{m\mu} f_i(\beta_i) \qquad (i = 1, \cdots, n).$$

This system is identically satisfied in the α's and β's if s_h and t are given by (4).

Suppose now that $x_k = \rho_k$, $y_{ir} = \nu_{ir}$ is any solution of (2). Then $\prod_{j=1}^{n}\sum_{k=1}^{q} a_{ijk}\rho_k = f_i(\nu_i)$ $(i = 1, \cdots, n)$. If we choose $\alpha_k = \rho_k$, $\beta_{ir} = \nu_{ir}$, we have

$$\begin{aligned} \overline{A}_i f_i(\beta_i) &= \overline{A}_i f_i(\nu_i)\\ &= \overline{A}_i \prod_{j=1}^{n}\sum_{k=1}^{q} a_{ijk}\rho_k\\ &= \overline{A}_i \prod_{j=1}^{n-1}\sum_{k=1}^{q} a_{ijk}\rho_k \sum_{k=1}^{q} a_{ink}\rho_k\\ &= \overline{A}_i A_i p_{in} = A p_{in} \end{aligned}$$

from which it follows that $s_h=0$ $(h=1, \cdots, n-1)$. Also

$$t = P^{m-1}A^{m-1}\sum_{i=1}^{n} Ap_{in}P_{in} = P^m A^m.$$

Hence (3) becomes $x_k=\rho_k P^{m\lambda}A^{m\lambda}$, $y_{ir}=\nu_{ir}P^{m\mu+1}A^{m\mu+1}$ from which the theorem follows.

In the particular example

$$(\ 25x- 5y-10z+ 5w)(29x+2y- 5z+10w)(x+ y+ z+ w)=p^2,$$
$$(\ 19x+17y+10z+15w)(\ 4x+7y+ 5z+ 5w)(x+2y+2z+2w)=q^2,$$
$$(-29x- 2y+ 5z-10w)(32x-9y-15z+ 5w)(x+3y-2z+2w)=r^2,$$

the integers $p_k^{(h)}$ are $(1, -2, 3, -1)$ and $(1, 3, -1, -4)$ and will make the first two factors of each equation on the left vanish.

The next system consists of two equations. Let $f_1(x)=f_1(x_1, \cdots, x_p)$, $f_2(x)=f_2(x_1, \cdots, x_q)$ be homogeneous polynomials of degree n with integral coefficients. Suppose that integers $x_i=a_i$ exist such that all the partial derivatives of f_1, as well as those of f_2, of all orders less than $n-1$ vanish for $x_i=a$. Let $g_1(u)=g_1(u_1, \cdots, u_k)$, $g_2(v)=g_2(v_1, \cdots, v_h)$ be homogeneous polynomials[2] with integral coefficients of degree m where m and n are relatively prime. λ and μ have the same meaning as in Theorem 1.

THEOREM 2. *Every integral solution of the system*[3]

$$f_1(x) = g_1(u), \qquad f_2(x) = g_2(v) \tag{5}$$

which does not satisfy

$$A(x)f_2(x) - B(x)f_1(x) = 0 \tag{6}$$

is equivalent to one given by

$$x_i = a_i s t^{\lambda-1} + \alpha_i t^{\lambda}, \quad u_j = \beta_j R(\alpha)t^{\mu}, \quad v_j = \gamma_j R(\alpha)t^{\mu}, \tag{7}$$

where

$$\begin{aligned} A(\alpha) &= \sum_{j=1}^{p} a_j \frac{\partial f_1}{\partial \alpha_j}, \qquad B(\alpha) = \sum_{j=1}^{q} a_j \frac{\partial f_2}{\partial \alpha_j}, \\ R(\alpha) &= A(\alpha)f_2(\alpha) - B(\alpha)f_1(\alpha), \\ s &= [R(\alpha)]^{m-1}[g_1(\beta)f_2(\alpha) - g_2(\gamma)f_1(\alpha)], \\ t &= [R(\alpha)]^{m-1}[A(\alpha)g_2(\gamma) - B(\alpha)g_1(\beta)], \end{aligned} \tag{8}$$

[2] We may assume that g_1 and g_2 are functions of the same variables. It is necessary that both g_1 and g_2 do not vanish identically.

[3] For single equations of this type see A. A. Aucoin, op. cit. pp. 334–335.

the α's, β's, *and* γ's *being arbitrary integers.*

PROOF. By Taylor's formula, if we let $x_i = a_i s t^{\lambda-1} + \alpha_i t^\lambda$,

$$f_1(x) = st^{n\lambda-1} \sum_{j=1}^{p} a_j \frac{\partial f_1}{\partial \alpha_j} + t^{n\lambda} f_1(\alpha),$$

$$f_2(x) = st^{n\lambda-1} \sum_{j=1}^{q} a_j \frac{\partial f_2}{\partial \alpha_j} + t^{n\lambda} f_2(\alpha).$$

Hence if x_i, u_j, v_j have the values given by (7), (5) becomes

$$t^{n\lambda-1}[A(\alpha)s + f_1(\alpha)t] = [R(\alpha)]^m t^{m\mu} g_1(\beta),$$

$$t^{n\lambda-1}[B(\alpha)s + f_2(\alpha)t] = [R(\alpha)]^m t^{m\mu} g_2(\gamma),$$

which is identically satisfied in the α's, β's, and γ's if s and t are given by (8).

Suppose that $x_i = \rho_i$, $u_j = \delta_j$, $v_j = \nu_j$ is any given solution of (5). Then $f_1(\rho) = g_1(\delta)$, $f_2(\rho) = g_2(\nu)$. If we choose $\alpha_i = \rho_i$, $\beta_j = \delta_j$, $\gamma_j = \nu_j$, then $s = 0$, $t = [R(\rho)]^m$, and the solution becomes $x_i = \rho_i [R(\rho)]^{m\lambda}$, $u_j = \delta_j [R(\rho)]^{m\mu+1}$, $v_j = \nu_j [R(\rho)]^{m\mu+1}$, which is equivalent to the given solution provided $R(\rho) \neq 0$, that is, provided $x_i = \rho_i$ does not satisfy (6).

One function which satisfies the conditions placed upon f_1 and f_2 is the determinant of order n, $D(x) = |a_{ij} x_{ij}|$ where the a's are integers and not all the a's in any row or column are zero. If there is one element x_{pq} which occurs only once in $D(x)$, we may make the choice $x_{pq} = 1$, $x_{ij} = 0$ otherwise, and then all the partial derivatives of all orders less than $n-1$ vanish. It is not necessary, in some cases, that there be a unique element x_{pq}. If $a_{ij} = 1$, for example, $D(x)$ may be the circulant. In this case the choice $x_{ij} = 1$ is made.

Another function which satisfies the conditions imposed upon f_1 and f_2 is the function $P(x) = \prod_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_j$, where all the a's are integral and the determinant $|a_{ij}|$ does not vanish. For this function we may choose x_j so that $n-1$ of the linear factors vanish and for this choice all the partial derivatives of $P(x)$ of all orders less than $n-1$ vanish.

As an example consider the equations

$$x^3 - x^2 z - xy^2 + y^2 z = u^2,$$

$$x^3 - x^2 y - xz^2 + yz^2 = v^2.$$

The partial derivatives of the first order of the functions on the left vanish for $x = y = z = 1$. We get, then, as solution $x = s + \alpha t$, $y = s + \beta t$, $z = s + \gamma t$, $u = D\lambda t$, $v = D\mu t$, where

$$D = 2(\alpha - \beta)^2(\alpha - \gamma)^2(\gamma - \beta),$$
$$s = D(\alpha - \beta)(\alpha - \gamma)[(\alpha + \gamma)\lambda^2 - (\alpha + \beta)\mu^2],$$
$$t = 2D(\alpha - \beta)(\alpha - \gamma)(\mu^2 - \lambda^2).$$

If we choose $\alpha = 3$, $\beta = 2$, $\gamma = 1$, $\lambda = -1$, $\mu = 2$, we get as solution $x = -32$, $y = 64$, $z = 160$, $u = -768$, $v = 1536$. It will be noted that x, y, z have the factor 4^2 while u and v have the factor 4^3. Hence this solution is equivalent to the primitive solution $x = -2$, $y = 4$, $z = 10$, $u = -12$, $v = 24$.

The third theorem treats a system for which there is no typical problem. The method will be illustrated by a particular system.

THEOREM 3. *Every solution of the system*

$$f_1(x_i, y_i, z_i) = g_1(x_i, y_i, z_i), \quad f_2(x_i, y_i, z_i) = g_2(x_i, y_i, z_i), \tag{9}$$

for which the members do not vanish, where f_1, f_2, g_1, g_2 *are homogeneous polynomials in each of the sets of variables,* f_1, f_2, g_1, g_2 *being of degrees* (4, 6, 2); (2, 2, 3); (7, 1, 1); (1, 4, 2) *respectively in the variables* x_i, y_i, z_i, *is equivalent* (*in a sense to be defined*) *to a solution given by*

$$x_i = \alpha_i u^7 v^{16} w^{19}, \quad y_i = \beta_i u^4 v^9 w^{11}, \quad z_i = \gamma_i u^2 v w, \tag{10}$$

where

$$u = f_1 f_2 g_1^2 g_2^2, \quad v = f_1 g_2, \quad w = f_2 g_1, \tag{11}$$

the α's, β's, *and* γ's *being arbitrary integers.*

PROOF. If we let x_i, y_i, z_i have the values given by (10), then (9) becomes

$$u^{56}v^{120}w^{144}f_1 = u^{55}v^{122}w^{145}g_1,$$
$$u^{28}v^{53}w^{63}f_2 = u^{27}v^{54}w^{65}g_2,$$

and this system is satisfied identically in the α's, β's, and γ's if u, v, w are given by (11).

We now extend the concept of equivalent solutions. If $x_i = \alpha_i$, $y_i = \beta_i$, $z_i = \gamma_i$ is any solution of the system (9) and there are no integers α_i', β_i', γ_i' and no positive integers s, a, b, and c such that $\alpha_i = s^a\alpha_i'$, $\beta_i = s^b\beta_i'$, $\gamma_i = s^c\gamma_i'$ where

$$\begin{aligned} 4a + 6b + 2c &= 7a + b + c, \\ 2a + 2b + 3c &= a + 4b + 2c, \end{aligned} \tag{12}$$

then $x_i = \alpha_i$, $y_i = \beta_i$, $z_i = \gamma_i$ is defined to be a primitive solution of (9). If $x_i = \alpha_i$, $y_i = \beta_i$, $z_i = \gamma_i$ is a primitive solution of (9), then $x_i = \alpha_i t^a$, $y_i = \beta_i t^b$, $z_i = \gamma_i t^c$ (derived from the primitive solution) where t is a nonzero integer and a, b, c are positive integers which satisfy (12), is also a solution. Two solutions are said to be equivalent if they may be derived from the same primitive solution.

Suppose now that $x_i = \lambda_i$, $y_i = \mu_i$, $z_i = \nu_i$ is any solution of (9). If we choose $\alpha_i = \lambda_i$, $\beta_i = \mu_i$, $\gamma_i = \nu_i$ we have that $x_i = \lambda_i(f_1f_2)^{56}$, $y_i = \mu_i(f_1f_2)^{32}$, $z_i = \nu_i(f_1f_2)^8$, which is equivalent to the given solution.

THE UNIVERSITY OF HOUSTON