REDUCIBLE DIOPHANTINE SYSTEMS

BY E. T. BELL

1. *Reducibility.* The algorithm of reciprocal arrays, developed in a previous paper,* can be applied to obtain the complete solutions in integers of a larger class of diophantine equations. In this note the application to equations reducible to Type VI of the previous paper is described; the most general Type VII can be treated similarly. Details, particularly in the examples in §3, which follow immediately from the theory of reciprocal arrays, which was fully discussed, are omitted. By *solution* is meant *all sets of rational integers satisfying a given diophantine system.*

A point which was inadvertently omitted from the paper on arrays must first be supplied. Let, for the moment,

$$(1) \qquad X_1, \cdots, X_n; Y_1, \cdots, Y_m; \cdots; W_1, \cdots, W_s$$

be $n+m+\cdots+s$ independent variables, finite in number; let $a, b, \cdots, c$ be arbitrary constant integers $\neq 0$, and let the $a_i, b_j, \cdots, c_k$ be arbitrary constant integers >0. To find the solution of

$$(2) \qquad aX_1^{a_1} \cdots X_n^{a_n} = bY_1^{b_1} \cdots Y_m^{b_m} = \cdots = cW_1^{c_1} \cdots W_s^{c_s},$$

when $|ab \cdots c|$ *is greater than unity* (omitted from the previous paper), we treat $a, b, \cdots, c$ first as independent variables, and solve for them along with the X's, Y's, $\cdots$, W's. In those solutions in which no $X, Y, \cdots, W$ takes the value zero, $a, b, \cdots, c$ will thus be given as products of powers of the parameters.† Thus each of the constant integers $a, b, \cdots, c$ is exhibited as a power product of a certain type, say

$$a = \alpha_1^{p_1} \cdots \alpha_r^{p_r}, \; b = \beta_1^{q_1} \cdots \beta_t^{q_t}, \cdots, c = \gamma_1^{h_1} \cdots \gamma_u^{h_u},$$

where the Greek letters are certain of the parameters. Hence

* E. T. Bell, *Reciprocal arrays and diophantine analysis*, American Journal of Mathematics, vol. 55, January, 1933, pp. 50–66; M. Ward, *A type of multiplicative diophantine system*, ibid., pp. 67–77.

† A *parameter* here is a variable ranging over integer values, zero excluded.

these parameters in the solution are constrained to take only a finite number of distinct sets of constant values, since $a, b, \cdots, c$ are constants.* Each such set defines a class of solutions. If $N(n; d_1, \cdots, d_g)$ is the total number of decompositions of n in the form $n = \xi_1^{d_1} \cdots \xi_g^{d_g}$, the number of classes in the solution of (2) is

$$N(a; p_1, \cdots, p_r)N(b; q_1, \cdots, q_t) \cdots N(c; h_1, \cdots, h_u).$$

We shall now define reducibility as applied to diophantine systems. Let

$$(3) \qquad x_1, \cdots, x_n; y_1, \cdots, y_m; \cdots; w_1, \cdots, w_s$$

be $n+m+\cdots+s$ independent variables. If a diophantine system in the independent variables (3) is equivalent to the system (2), where now the variables (1) are linear homogeneous functions of the variables (3) with integer coefficients (there is no gain in generality in rational coefficients), of the following kind,

(4) the X's are functions of the x's alone, the Y's of the y's alone, $\cdots$, the W's of the w's alone,

(5) the respective determinants of the X's, Y's, $\cdots$, W's are $A, B, \cdots, C$, and $AB \cdots C \neq 0$,

we shall say that the diophantine system is *reducible.*

THEOREM. *The solution of a reducible diophantine system is given by an application of reciprocal arrays followed, if* $|AB \cdots C| > 1$, *by a simple enumeration of cases according to congruences moduli* $A, B, \cdots, C$, *and the solution by classical methods of certain linear homogeneous diophantine equations with given constant coefficients.*

Consider first the sets of integers contributed to the solution when none of the $X, Y, \cdots, W$ is zero. Then, since $AB \cdots C \neq 0$, the solution of the system (2), in which the variables are as in (1), enables us to solve algebraically for the variables (3). This expresses the variables (3) of the original system as sums of

* It can be shown that resolutions of $a, b, \cdots, c$ in the above type exist. For example, if $a = 11$, the resolution $a = \alpha_1^2 \alpha_2^3$ can not occur, but $a = \alpha_1^2 \alpha_2^3 \alpha_3$ may, and $|\alpha_1| = |\alpha_2| = 1$, $\alpha_3 = 11$ are the only possibilities.

power-products of parameters with rational coefficients; the coefficients of the x's, y's, $\cdots$, w's have the respective common denominators $A, B, \cdots, C$. That an infinity of sets of integers $x_i, y_j, \cdots, w_k$ satisfying the original system exist is evident, since each parameter may be replaced by $AB \cdots C$ times itself. The finding of all such sets, and hence the first stage of the solution, becomes a straight-forward exercise in linear congruences, moduli $A, B, \cdots, C$, on replacing the several powers of parameters by their possible forms to the given moduli. This further separates the sets in the solution into classes. Since $A, B, \cdots, C$ are constants, all the classes can be found in a finite number of steps, explicitly.

The sets contributed when some of the $X, Y, \cdots, W$ are zero are found by solving sets of linear homogeneous equations. Thus, for example, singling out the X's, if $n=1$, then $x_1=0$, and at least one of each of the Y's, $\cdots$, W's must vanish, while the rest may take any arbitrary integer values. Suppose $n>1$. Then, since $A \neq 0$, not all the X's can vanish. Suppose we require precisely n_1 of the X's to vanish, $0<n_1<n$. Applying the classical theory of linear homogeneous equations, we can determine the integer solutions of the set obtained from the n_1 vanishing X's. By (2), at least one of each of the Y's, $\cdots$, W's must now vanish, and these may be treated in the same way as the X's. The variables (3) being independent, any set obtained from the X's may be combined with any from each of the Y's, $\cdots$, W's, to give the total contribution to the solution.

2. *Equivalence.* A simple but powerful device applies the idea of reducibility to numerous interesting types of diophantine systems. Refer to (3). Let $F, G, \cdots, H$ be polynomials in the x's, y's, $\cdots$, w's, respectively, with integer coefficients (there is no gain in generality with rational coefficients, and likewise for $p', q', \cdots, r'$), and suppose that constant integers $p', q', \cdots, r'$ different from zero exist such that, *indentically*,

$$\begin{aligned} p'F(x_1, \cdots, x_n) &= pX_1^{a_1} \cdots X_n^{a_n}, \\ q'G(y_1, \cdots, y_m) &= qY_1^{b_1} \cdots Y_m^{b_m}, \\ \cdots & \qquad \cdots \\ r'H(z_1, \cdots, z_s) &= rW_1^{c_1} \cdots W_s^{c_s}, \end{aligned}$$

where the capital letters denote the linear forms previously defined. Then we shall say that

$$p'F(x_1, \cdots, x_n) = q'G(y_1, \cdots, y_m) = \cdots = r'H(w_1, \cdots, w_s)$$

is *equivalent* to (2), or to any system reducible to (2). The following theorem is an immeditate consequence of the definitions.

THEOREM. *The solution of any diophantine system equivalent to a reducible system is obtainable by the algorithm of reciprocal arrays, linear congruences, and the solution of linear equations.*

3. *Examples.* Before attempting any application of the method, it is well to calculate, or at least estimate, the total number of parameters necessary and sufficient for the solution first. This number may be called the *order* of the system. It was calculated in each of the following examples. For certain quite general systems of the type (2), with the variables (1), the order has been determined by Ward in the paper cited.*

The equation

$$(x + y + z)^3 + u^3 + v^3 + w^3 = (u + v + w)^3 + x^3 + y^3 + z^3$$

illustrates §2; it is reducible, being equivalent to

$$(x + y)(y + z)(z + x) = (u + v)(v + w)(w + u).$$

The solution falls into two sets.

(i) f, g, h, k are arbitrary integers. The first set is obtained by combining any one of the following sets of values for x, y, z with any one for u, v, w:

x	y	z	u	v	w
f	$-f$	g	h	$-h$	k
f	g	$-f$	h	k	$-h$
g	f	$-f$	k	h	$-h$

(ii) $\phi_1, \cdots, \phi_9$ are parameters (as defined in §1);

$$a \equiv \phi_1\phi_4\phi_7, \quad b \equiv \phi_2\phi_5\phi_8, \quad c \equiv \phi_3\phi_6\phi_9,$$

* To see the desirability of first calculating the order, consider the system, given as an example by Ward, for one of his formulas,

$$X_1^9 = Y_1^5 = Z_1^4Z_2^4 = W_1W_2W_3W_4.$$

Although the number of algebraically independent variables of the system is only 5, the order is 46217626.

$$p \equiv \phi_1\phi_5\phi_9, \quad q \equiv \phi_2\phi_6\phi_7, \quad r \equiv \phi_3\phi_4\phi_8,$$
$$1 = (\phi_4\phi_7, \phi_5\phi_9) = (\phi_5\phi_8, \phi_6\phi_7) = (\phi_6\phi_9, \phi_4\phi_8),$$

where (i, j) denotes the G.C.D. of the integers i, j. Then

$$x = (a - b + c)/2, \qquad u = (p - q + r)/2,$$
$$y = (a + b - c)/2, \qquad v = (p + q - r)/2,$$
$$z = (-a + b + c)/2, \qquad w = (-p + q + r)/2,$$

where $\phi_1, \cdots, \phi_9$ satisfy in turn the following parity conditions, imposed to select all integers from the above rational forms of $x, \cdots, w$:

(iii) at least one parameter occurring in each of the triads a, b, c, p, q, r is even;

(iv) all 3 parameters in any one of the triads a, b, c, p, q, r are even, and the remaining 6 parameters are odd;

(v) any one of the 9 parameters is even and the remaining 8 odd.

Another completely solvable equation based on the same identity as the preceding is

$$(x + y + z)^3 = x^3 + y^3 + z^3 + w_1^{a_1} w_2^{a_2} \cdots w_s^{a_s},$$

where $a_1, \cdots, a_s$ are arbitrary constant integers >0. For, this equation is equivalent to

$$3(x + y)(y + z)(z + x) = w_1^{a_1} w_2^{a_2} \cdots w_s^{a_s},$$

which we solve by the algorithm of arrays for $x+y$, $y+z$, $z+x$, $w_1, \cdots, w_s$. From this solution x, y, z are obtained as in the preceding example.

The direct solution by the same method of

$$x^2 + y^n = z^2$$

is laborious if $n>4$; Ward's additive dual of the multiplicative method of arrays enables us to write down the rest of the solution in addition to the trivial part $y=0$, $x=\pm z$, almost by inspection. Since the equation is reducible to $y^n = uv$, with $x=(u-v)/2$, $z=(u+v)/2$, we find

$$y = \phi_1\phi_2 \cdots \phi_{n+1},$$
$$x = (\phi_1^n\phi_2^{n-1}\phi_3^{n-2} \cdots \phi_{n-1}^2\phi_n - \phi_2\phi_3^2 \cdots \phi_{n-1}^{n-2}\phi_n^{n-1}\phi_{n+1}^n)/2,$$
$$z = (\phi_1^n\phi_2^{n-1}\phi_3^{n-2} \cdots \phi_{n-1}^2\phi_n + \phi_2\phi_3^2 \cdots \phi_{n-1}^{n-2}\phi_n^{n-1}\phi_{n+1}^n)/2,$$

where the ϕ's are parameters. The parity restrictions on the parameters are obvious. The additive method does not (as yet) provide G.C.D. conditions on the parameters. However, if only formulas giving the solution are required, without regard to possible avoidable duplications as the parameters independently range over all integers $\neq 0$, the G.C.D. conditions can be ignored.

Numerous interesting equations which in one respect generalize the preceding examples arise from Boutin's identity,*

$$\sum \pm (\pm x_1 \pm x_2 \pm \cdots \pm x_n)^n = n!\, 2^n x_1 \cdots x_n,$$

where the sum refers to the 2^n possible combinations of signs within the parentheses, and the outer sign is the product of the inner. For example, taking $n=4$, we write down the solution of

$$\begin{aligned}&(x_1 + y_1 + z_1 + u_1)^4 + (x_2 - y_2 - z_2 - u_2)^4\\ &+ (x_1 - y_1 - z_1 + u_1)^4 + (x_2 + y_2 + z_2 - u_2)^4\\ &+ (x_1 - y_1 + z_1 - u_1)^4 + (x_2 + y_2 - z_2 + u_2)^4\\ &+ (x_1 + y_1 - z_1 - u_1)^4 + (x_2 - y_2 + z_2 + u_2)^4\end{aligned}$$

= the like with the suffixes 1, 2 interchanged, from the equivalent

$$x_1 y_1 z_1 u_1 = x_2 y_2 u_2 z_2 .$$

Disregarding the trivial part in which at least one of x_i, y_i, z_i, u_i, $(i=1, 2)$, is zero, we get the rest of the solution immediately by writing down the pair of reciprocal arrays corresponding to the last equation. Thus

$$x_1 = \phi_1\phi_5\phi_9\phi_{13},\ y_1 = \phi_2\phi_6\phi_{10}\phi_{14},\ z_1 = \phi_3\phi_7\phi_{11}\phi_{15},\ u_1 = \phi_4\phi_8\phi_{12}\phi_{16},$$

$$x_2 = \phi_1\phi_6\phi_{11}\phi_{16},\ y_2 = \phi_2\phi_7\phi_{12}\phi_{13},\ z_2 = \phi_3\phi_8\phi_9\phi_{14},\ u_2 = \phi_4\phi_5\phi_{10}\phi_{15},$$

where the ϕ's are parameters, and the G.C.D. conditions are

$$(x_1, x_2) = \phi_1,\ (y_1, y_2) = \phi_2,\ (z_1, z_2) = \phi_3,\ (u_1, u_2) = \phi_4 .$$

For use with cubic equations the solution of $x^3 = yzw$ is frequently required, so we state it, leaving the proof as an exercise in arrays. Neglecting the trivial part of the solution in which $x=0$, we get for the rest, in which $x \neq 0$,

* Quoted by Dickson, *History of the Theory of Numbers*, vol. 2, p. 723. The identity, however, is due to Cauchy, who stated and proved it in a paper which has been overlooked by historians of Waring's problem.

$x = mabcfghpqr,\ y = mgh(af)^2p^3,\ z = mca(bg)^2q^3,\ w = mbf(ch)^2r^3,$

where the parameters $m, \cdots, r$ may be restricted by the G.C.D. conditions

$$1 = (a, f) = (b, g) = (c, h),$$
$$1 = (afp, bcqr) = (bgq, hfrp) = (chr, agpq).$$

The most immediate application of this is to the solution of $x^3+f(y, z, w)=0$, where $f(y, z, w)$ is any ternary cubic factorable into 3 linear, homogeneous factors whose determinant is ± 1. The solution can be written down from the above.

CALIFORNIA INSTITUTE OF TECHNOLOGY

A NOTE ON THE FOUR-POINT PROPERTY

BY L. M. BLUMENTHAL

1. *Introduction.* It has been pointed out by Menger that a metric space may be defined as a semi-metric space each three points of which is congruent to three points of a euclidean plane.

In a recent article, W. A. Wilson has considered a metric space that has the property that any n points of the space can be imbedded in a euclidean $(n-1)$-dimensional space.* Such a space is said to have the n-point property. An investigation of such spaces led Wilson to two important theorems. He shows (1) that if a convex, externally convex, and complete space has the four-point property, then the space has the n-point property for every integer n, and (2) that a convex, externally convex, complete, and separable space which has the four-point property is congruent with some euclidean space or with Hilbert space. It follows from the first theorem that pseudo-euclidean sets do not exist in a space satisfying the hypotheses of the theorem. This fact is of importance in connection with the problem of determining surfaces in which pseudo-euclidean n-tuples can be imbedded, for n greater than four. The second theorem, obtained by applying the first one to a well known theorem of

* W. A. Wilson, *A relation between metric and euclidean spaces*, American Journal of Mathematics, vol. 54 (1932), pp. 505–517.