ON SOME SPECIAL SYSTEMS OF EQUATIONS

H. H. CORSON

1. Let F be an arbitrary field. Let S be a system of equations which, when solved for two of its variables, takes the following form:

$$(1)\qquad \begin{aligned} x_1^{k_1} &= f(x_3, \cdots, x_n), \\ x_2^{k_2} &= g(x_3, \cdots, x_n), \end{aligned}$$

where f and g are arbitrary functions of the indicated variables. Consider also the equation

$$(2)\qquad y^{k_1k_2} = f^{sk_2}(y_3, \cdots, y_n)g^{rk_1}(y_3, \cdots, y_n).$$

THEOREM 1. *If* $(k_1, k_2)=1$ *and* $rk_1+sk_2=1$, *then the distinct solutions of* (1) *in* F *with* $x_1x_2\neq 0$ *may be put in one-to-one correspondence with the distinct solutions of* (2) *in* F *with* $y\neq 0$. *Moreover, these solutions of* (1), $x_1x_2\neq 0$, *may be determined from the solutions of* (2), $y\neq 0$, *and conversely, by means of transformations* (3) *and* (4) *below.*

Proof. Assuming for the rest of this section that $x_1x_2\neq 0$, $y\neq 0$, we put

$$(3)\qquad \begin{aligned} x_1 &= y^{k_2}\left\{\frac{f(y_3, \cdots, y_n)}{g(y_3, \cdots, y_n)}\right\}^r, \\ x_2 &= y^{k_1}\left\{\frac{g(y_3, \cdots, y_n)}{f(y_3, \cdots, y_n)}\right\}^s, \\ x_i &= y_i \qquad (i=3, \cdots, n) \end{aligned}$$

and notice that if $(y, y_3, \cdots, y_n)$ is a solution of (2) then (3) determines a solution of (1). Now let

$$(4)\qquad \begin{aligned} y &= x_1^s x_2^r, \\ y_i &= x_i \qquad (i=3, \cdots, n). \end{aligned}$$

It may be verified directly that if $(x_1, x_2, \cdots, x_n)$ is a solution of (1) then (4) determines a solution of (2). Further, given a solution $(x_1, x_2, \cdots, x_n)$ of (1) and a solution $(y, y_3, \cdots, y_n)$ of (2) with $x_i=y_i$ $(i=3, \cdots, n)$, then (3) implies (4) and conversely—which may be verified with the use of the relation $rk_1+sk_2=1$.

Received August 8, 1955.

We note that Theorem 1 may be extended by induction to apply to a system like (1) with an arbitrary number of equations, with $z_1^{k_1}$, $z_2^{k_2}, \cdots, z_m^{km}$ as left members, and with arbitrary functions of $z_{m+1}, \cdots$, z_n as right members if $(k_i, k_j)=1$, $i\neq j$. The argument is the same in going from n to $n+1$ equations, and transformations corresponding to (3) and (4) may be constructed.

Use will also be made of the fact that Theorem 1 is still valid if $x_3, \cdots, x_n$ are restricted to values in A, a subset of F, as long as $y_3, \cdots, y_n$ are similarly restricted.

2. **Let F now be** a finite field $GF(q)$, $q=p^t$. Assume f and g to be homogeneous polynomials of degrees m_1 and m_2 respectively, where $(m_1, k_1)=1$ and $(m_2, k_2)=1$. The solutions of (2) can be determined by the following method used by Hua and Vandiver [1] and Morgan Ward [2].

As $(k_1k_2, sk_2m_1+rk_1m_2)=1$, there are integers a, b, and c such that $ak_1k_2+b(sk_2m_1+rk_1m_2)+c(q-1)=1$ with $(a,q-1)=1$. First assuming that $y\neq 0$, set

$$
\begin{aligned}
&y=\lambda^a \\
&y_i=\lambda^{-b}z_i \qquad (i=3, \cdots, n)\,.
\end{aligned}
\tag{5}
$$

Equation (2) then assumes the following form:

$$
\lambda=f^{sk_2}(z_3, \cdots, z_n)g^{rk_1}(z_3, \cdots, z_n)\,. \tag{6}
$$

Thus every choice of $z_3, \cdots, z_n$ such that $f\neq 0$, $g\neq 0$ determines a solution of (2).

Now consider the system (1). Determine as above integers u, v, and w such that $uk_2+vm_2+w(q-1)=1$, $(u, q-1)=1$. Assuming $x_2\neq 0$, set

$$
\begin{aligned}
&x_2=\gamma^u \\
&x_i=\gamma^{-v}t_i \qquad (i=3, \cdots, n)\,.
\end{aligned}
\tag{7}
$$

It is readily seen that all values of $t_3, \cdots, t_n$ such that $f(t_3, \cdots, t_n)=0$ determine solutions of the system (1) whether $g(t_3, \cdots, t_n)=0$ or not.

The same argument is valid if g is assumed zero, which proves the following.

THEOREM 2. *If f and g are homogeneous polynomials of degrees m_1 and m_2 respectively, $(m_1, k_1)=1$ and $(m_2, k_2)=1$, then the total number of solutions of the system* (1) *in $GF(q)$ is q^{n-2}*

A similar application of Theorem 1 is the following. First let S be

$$
\begin{aligned}
x_1^{k_1} &= a_3 x_3^{em_3} + a_4 x_4^{em_4} + \cdots + a_n x^{em_n} \\
x_2^{k_2} &= b_3 x_3^{dm_3} + b_4 x_4^{dm_4} + \cdots + b_n x_n^{dm_n}
\end{aligned}
\tag{8}
$$

where $(k_1, k_2)=1$. Also if M is the least common multiple of $m_3, \cdots, m_n$, assume $(eM, k_1)=1$ and $(dM, k_2)=1$. In place of (5) we employ the following transformation in (2), following Carlitz [3]:

$$
\begin{aligned}
y &= \lambda^a \\
y_i &= \lambda^{-bM/m_i} z_i \qquad (i=3, \cdots, n),
\end{aligned}
\tag{9}
$$

where $ak_1k_2 + bM(sk_2e + rk_1d) + c(q-1) = 1$, $(a, q-1)=1$. Exactly as above follows the next theorem.

THEOREM 3. *The total number of solutions of* (8) *subject to the conditions stated above is* q^{n-2}.

Also [3] suggests the following generalization of Theorem 2. Let $f_3(x_3), f_4(x_4), \cdots, f_n(x_n)$ and $g_3(x_3), g_4(x_4), \cdots, g_n(x_n)$ be homogeneous polynomials of degrees $em_3, em_4, \cdots, em_n$ and $dm_3, dm_4, \cdots, dm_n$ respectively, where now $(x_i)=(x_{i1}, x_{i2}, \cdots, x_{is_1})$ $(i=3, \cdots, n)$. Thus by the same argument follows the next theorem.

THEOREM 4. *Replacing in* (8) $x_i^{em_i}$ *by* $f_i(x_i)$ *and* $x_i^{dm_i}$ *by* $g_i(x_i)$, $(i=3, \cdots, n)$, *then the total number of solutions of the resulting system is* $q^{s_3+\cdots+s_n}$.

3. Now let F be the rational field and let f and g in (1) be polynominals with integral coefficients. If $x_3, \cdots, x_n$ are restricted to be integers, then x_1 and x_2 in any solution must be integers.

In the equation $rk_1 + sk_2 = 1$ we may assume that $r>0$, $s<0$. In place of system (1) write

$$
\begin{aligned}
x_1'^{k_1} &= \frac{1}{x_1^{k_1}} = \frac{1}{f(x_3, \cdots, x_n)} = f'(x_3, \cdots, x_n) \\
x_2^{k_2} &= g(x_3, \cdots, x_n)\,.
\end{aligned}
\tag{10}
$$

we assume as in Theorem 2 that f and g are homogeneous of degrees m_1 and m_2 respectively, $(m_1, k_1)=1$ and $(m_2, k_2)=1$. Let a, b and c satisfy $ak_1k_2 + b(rk_1m_2 - sk_2m_1) + c(q-1) = 1$, $(a, q-1)=1$; then (5) determines a family of solutions in integers of

$$
y^{k_1k_2} = f'^{sk_2}(y_3, \cdots, y_n) g^{rk_1}(y_3, \cdots, y_n), \tag{11}
$$

$y \neq 0$. By Theorem 1, (3) determines a family of solutions of (10) with

$x_3, \cdots, x_n$ integers, and by the remark at the first of this section, a family of solutions of equations (1) with $x_1, x_2, \cdots, x_n$ integers, $x_1x_2 \neq 0$. The cases where f or g is zero may be treated as in § 2, which proves the following.

THEOREM 5. *If f and g are homogeneous polynomials with integral coefficients of degrees m_1 and m_2 respectively, $(m_1, k_1)=1$ and $(m_2, k_2)=1$ then a family of solutions in integers may be found for equations* (1) *by the method above.*

See [2] for remarks on the solution of equation (11) under the above hypotheses. Note especially the above method does not in general give all solutions.

I should like to thank Professor L. Carlitz for his very helpful interest in this material.

REFERENCES

1. L. Carlitz, *The number of solutions of certain types of equations in a finite field.* Pacific J. Math. **5** (1955), 177-181.

2. L. K. Hua and H. S. Vandiver, *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 481-487.

3. Morgan Ward, *A class of soluble diophantine equations*, Proc. Nat. Acad. Sci. U.S.A. **37** (1951), 113-114.

DUKE UNIVERSITY