NOTE ON THE LINEAR SYMMETRIC CONGRUENCE IN n VARIABLES

L. J. MORDELL

Introduction. Let $f = f(x_1, x_2, \ldots, x_n)$ be a polynomial in $n > 2$ variables with integer coefficients, and let p be a large prime. Very little appears to be known about estimates for the number N of solutions of the congruence

$$f \equiv 0 \pmod{p} \tag{1}$$

for general f. For the special case when

$$f = a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n} + a, \tag{1'}$$

I showed [**1**, p. 207] in 1932, that when $a_1 a_2 \ldots a_n a \not\equiv 0 \pmod{p}$,

$$N = p^{n-1} + O(p^{\frac{1}{2}(n-1)})$$

where the constants implied in O are independent of the a's. Particular cases of (1') have been discussed by many writers even as far back as Gauss, and (1') has been the subject of numerous papers in recent years. But no other instances of (1) seem to have been considered and so it may be of interest to study the case when f is the general linear symmetric function of the x's, say

$$f = a_0 + a_1 \sum x_1 + a_2 \sum x_1 x_2 + \ldots + a_n x_1 x_2 \ldots x_n \equiv 0. \tag{2}$$

I have been led to the conjectured

THEOREM. *When $f \equiv 0$ is not derived from $x_1 x_2 \ldots x_n \equiv a$ by a linear substitution $x_r' \equiv (Ax_r + B)/(Cx_r + D)$ $(r = 1, 2, \ldots, n)$, nor from any of*

$$a x_1 x_2 \ldots x_n + b \sum x_1 x_2 \ldots x_{n-1} \equiv 0,$$

$$\sum x_1 x_2 \ldots x_{n-2} \equiv 0, \qquad \sum x_1 x_2 \ldots x_{n-3} \equiv 0, \qquad \ldots, \sum x_1 x_2 \equiv 0,$$

by a linear substitution $x_r' \equiv Ax_r + B$ $(r = 1, 2, \ldots, n)$, then N, the number of solutions of (2), satisfies

$$N = p^{n-1} + O(p^{\frac{1}{2}(n-1)}), \tag{3}$$

where the constant implied in O is independent of the a's.

The proofs for $n = 2, 3$ are trivial. For $n = 4$, the result lies deep since it is practically equivalent to Hasse's result [**2**, p. 145] that the number of solutions of the congruence

$$y^2 \equiv ax^4 + bx^3 + cx^2 + dx + e \tag{4}$$

Received December 30, 1952.

is $p + O(p^{\frac{1}{2}})$ provided that the quartic is not congruent to a multiple of the square of a quadratic.

I know of no really worth while results for $n > 4$.

Take the cases in turn.

$n = 2$:

(5) $$f = a_0 + a_1(x_1 + x_2) + a_2x_1x_2 \equiv 0.$$

It may be supposed that a_1 and a_2 are not both congruent to zero. Then obviously if $a_2 \equiv 0$, $N = p$. If $a_2 \not\equiv 0$, two cases arise according as f is decomposable or indecomposable. In the first case $a_1^2 - a_0a_2 \equiv 0$, and f becomes $(a_1 + a_2x_1)\cdot(a_1 + a_2x_2) \equiv 0$, and there are $2p - 1$ solutions. In the second $a_1^2 - a_0a_2 \not\equiv 0$, and there are $p - 1$ solutions since x_1 may have any of the $p - 1$ values for which $a_2x_1 + a_1 \not\equiv 0$, and then x_2 is uniquely determined.

$n = 3$:

(6) $$f = a_0 + a_1(x_1 + x_2) + a_2x_1x_2 + x_3(a_1 + a_2(x_1 + x_2) + a_3x_1x_2.$$

Let N' be the number of solutions in x_1, x_2 of

(7) $$a_1 + a_2(x_1 + x_2) + a_3x_1x_2 \equiv 0.$$

Suppose first that this is reducible. Then $a_3 \not\equiv 0$ and we can put $a_1 \equiv t^2a_3$, $a_2 \equiv ta_3$, and $N' = 2p - 1$. But then

$$f = a_0 - a_3t^3 + a_3(x_1 + t)(x_2 + t)(x_3 + t),$$

and this is one of the excluded cases. Clearly $N = (p - 1)^2$ if $a_0 - a_3t^3 \not\equiv 0$, but $N = 3p^2 - 3p + 1$ if $a_0 - a_3t^3 \equiv 0$.

Suppose then (7) is not reducible. Now $N' = p - 1$ or p, according as $a_3 \not\equiv 0$ or $a_3 \equiv 0$. For each of the remaining $p^2 - N'$ sets for x_1, x_2 there is a unique value for x_3. For the N' sets, there will be solutions for x_3, and then p solutions for x_3, if and only if

(8) $$\begin{aligned} a_1 + a_2(x_1 + x_2) + a_3x_1x_2 &\equiv 0, \\ a_0 + a_1(x_1 + x_2) + a_2x_1x_2 &\equiv 0. \end{aligned}$$

Suppose first that these congruences are essentially the same, say

$$\frac{a_1}{a_0} \equiv \frac{a_2}{a_1} \equiv \frac{a_3}{a_2} \equiv t.$$

Then $f \equiv a_0(1 + tx_1)(1 + tx_2)(1 + tx_3)$, and this is an excluded case. If we had had $a_0 \equiv a_1 \equiv a_2 \equiv 0$, then $f \equiv a_3x_1x_2x_3$, an excluded case.

Apart from these cases, (8) determine $x_1 + x_2$ and x_1x_2 uniquely and so there are $O(1)$ values for x_1 and x_2. Hence

$$N = p^2 - p + \epsilon + O(p) = p^2 + O(p), \qquad \epsilon = 0, 1.$$

The work shows that there is no exception to the general result (3) except in the case $a(x_1 + t)(x_2 + t)(x_3 + t) \equiv 0$.

https://doi.org/10.4153/CJM-1953-048-0 Published online by Cambridge University Press

$n = 4$:

Here $f = g + hx_4$, where

$$g = a_0 + a_1(x_1 + x_2 + x_3) + a_2(x_2x_3 + x_3x_1 + x_1x_2) + a_3x_1x_2x_3,$$
$$h = a_1 + a_2(x_1 + x_2 + x_3) + a_3(x_2x_3 + x_3x_1 + x_1x_2) + a_4x_1x_2x_3. \tag{9}$$

The number N' of sets x_1, x_2, x_3 for which $h \equiv 0$ is $p^2 + O(p)$ except when $a_3 \equiv ta_4$, $a_2 \equiv t^2a_4$, $a_1 \equiv t^3a_4$, $a_4 \not\equiv 0$, and then f takes the excluded form

$$a_0 - a_4t^4 + a_4(x_1 + t)(x_2 + t)(x_3 + t)(x_4 + t).$$

Hence for $p^3 - p^2 - O(p)$ sets of values for x_1, x_2, x_3, there is a unique value for x_4. When $h \equiv 0$, we have solutions for x_4, in fact p solutions, if and only if x_1, x_2, x_3 satisfy both $g \equiv 0$, $h \equiv 0$, say for M solutions x_1, x_2, x_3. Then

$$N = p^3 - p^2 - O(p) + pM = p^3 + O(p^{3/2}),$$

as it will be shown that $M = p + O(p^{\frac{1}{2}})$.

Some of the exceptional cases arising are dealt with by the

LEMMA. *The functions g, h in* (9) *yield an identical congruence in x_1, x_2, x_3 of the form*

$$h + g\lambda \equiv \mu(x_1 + k)(x_2 + k)(x_3 + k) \tag{10}$$

for constants λ, μ, k, only in some of the exceptional cases.

For (10) gives

$$a_4 + \lambda a_3 \equiv \mu, \quad a_3 + \lambda a_2 \equiv \mu k,$$
$$a_2 + \lambda a_1 \equiv \mu k^2, \quad a_1 + \lambda a_0 \equiv \mu k^3.$$

Then

$$ka_4 - a_3 + \lambda(ka_3 - a_2) \equiv 0,$$
$$ka_3 - a_2 + \lambda(ka_2 - a_1) \equiv 0,$$
$$ka_2 - a_1 + \lambda(ka_1 - a_0) \equiv 0.$$

Put $f' = f(x_1, x_2, x_3, -k)$. Then

$$f' = g - kh = (a_3 - ka_4)\,x_1\,x_2\,x_3 + (a_2 - ka_3)(x_2\,x_3 + x_3\,x_1 + x_1\,x_2) + \ldots$$
$$= (ka_1 - a_0)(\lambda x_1 - 1)(\lambda x_2 - 1)(\lambda x_3 - 1).$$

Hence f can be written as

$$f = (x_4 + k)\,j + (ka_1 - a_0)(\lambda x_1 - 1)(\lambda x_2 - 1)(\lambda x_3 - 1),$$

where j is linear in each of x_1, x_2, x_3; and this expression for f must be symmetrical in x_1, x_2, x_3, x_4. Now $\lambda \equiv 0$ leads to an excluded form for f since if $k = 0$, $j = ax_1\,x_2\,x_3$. When $\lambda \not\equiv 0$, on replacing x_1 by $(x_1 + 1)/\lambda$ etc., f can be written as, say, $f = (x_4 + k')\,j' + ax_1\,x_2\,x_3$. Put

$$j' = a'x_1x_2x_3 + b'\sum_{1,2,3} x_2x_3 + c'\sum_{1,2,3} x_1 + d'.$$

https://doi.org/10.4153/CJM-1953-048-0 Published online by Cambridge University Press

Then

$$f = a'x_1x_2x_3x_4 + (a'k' + a)\,x_1x_2x_3 + b'(x_2x_3x_4 + x_3x_1x_4 + x_1x_2x_4) + c'(x_1x_4 + x_2x_4 + x_3x_4) + b'k'(x_2x_3 + x_3x_1 + x_1x_2) + c'k'(x_1 + x_2 + x_3) + d'x_4 + k'd'.$$

Since f is symmetrical in the x's, we have $b' = a'k' + a$, $c' = b'k'$, $d' = c'k'$, and so

$$f = a'x_1x_2x_3x_4 + b'\sum x_1x_2x_3 + b'k'\sum x_1x_2 + b'k'^2\sum x_1 + b'k'^3.$$

If $k' \equiv 0$, we have $f = a'x_1x_2x_3x_4 + b'\sum x_1x_2x_3$.

If $k' \not\equiv 0$, on multiplying f by k', we can clearly write f as

$$k'f = -ax_1x_2x_3x_4 + b'(x_1 + k')(x_2 + k')(x_3 + k')(x_4 + k').$$

Both these are exceptional cases. This concludes the proof of the lemma.

We now find the number M of solutions of $g \equiv 0$, $h \equiv 0$. Suppose first $a_4 \not\equiv 0$. Then if in f we replace x_1 by $x_1 - a_3/a_4$, etc., we may suppose $a_3 \equiv 0$, and so (9) takes for $h \equiv 0$ and $g \equiv 0$, the shape

$$\begin{aligned} x_1x_2x_3 &\equiv A\sum x_1 + B, \\ E\sum x_1x_2 &\equiv C\sum x_1 + D. \end{aligned} \tag{11}$$

If $E \equiv 0$, these can be written as

$$\sum x_1 \equiv F, \qquad x_1x_2x_3 \equiv G,$$

where, by the lemma, $G \not\equiv 0$. Then

$$x_1x_2(F - x_1 - x_2) \equiv G.$$

This cannot be a reducible congruence; and writing $x_1 = X + Y, x_2 = X - Y$, the number of solutions is as in Hasse's result on (3). Hence we can suppose $E = 1$, and so, with $x_1 - c$ for x_1, etc., the two congruences (11) can be written as

$$\begin{aligned} x_1x_2x_3 &\equiv A\sum x_1 + B, \\ \sum x_1x_2 &\equiv D. \end{aligned} \tag{12}$$

Then

$$\begin{aligned} x_3(x_1x_2 - A) &\equiv A(x_1 + x_2) + B, \\ x_3(x_1 + x_2) &\equiv D - x_1x_2, \end{aligned}$$

and so

$$(A(x_1 + x_2) + B)(x_1 + x_2) + (x_1x_2 - A)(x_1x_2 - D) \equiv 0. \tag{13}$$

If (13) is reducible, $x_1 + x_2$ must be expressible linearly in terms of x_1x_2, and so $-As^2 - Bs + \frac{1}{4}(A - D)^2$ must be congruent to a perfect square in s, and so $B^2 + A(A - D)^2 \equiv 0$. Hence

$$A \equiv -A_1^2, \quad B \equiv A_1^3 + DA_1,$$

say. Then (12) becomes

$$x_1x_2x_3 \equiv -A_1^2\sum x_1 + A_1^3 + DA_1,$$
$$\sum x_1x_2 \equiv D.$$

By addition, $(x_1 - A_1)(x_2 - A_1)(x_3 - A_1) \equiv 0$, and this has been noted in the lemma and is dealt with in (14) below.

Write (13) as

$$(x_2^2 + A)\,x_1^2 + (2Ax_2 + B - (A + D)\,x_2)\,x_1 + Ax_2^2 + Bx_2 + AD \equiv 0.$$

Hence $2(x_2^2 + A)\,x_1 + 2Ax_2 + B - (A + D)\,x_2 = Y$, where $Y^2 \equiv R$ and R is a quartic in x_2. This quartic cannot be a perfect square since (13) is irreducible, and so the number of solutions is given by Hasse's result and (3) holds.

Suppose next $a_4 \equiv 0$. If $a_3 \not\equiv 0$, on replacing x_1 by $x_1 + k$, etc., we may suppose $a_2 = 0$ in f. Then (9) becomes

$$g = a_0 + a_1(x_1 + x_2 + x_3) + a_3\,x_1\,x_2\,x_3 \equiv 0,$$
$$h = a_1 + a_3(x_2\,x_3 + x_3\,x_1 + x_1\,x_2) \equiv 0. \tag{14}$$

These are the same as (12) and so we have the same estimate as when $a_4 \not\equiv 0$, except possibly when $g\lambda + h$ is reducible. This occurs only when $a_1 \equiv t^2a_3$ and $a_0 \equiv 0$. Then

$$g + th \equiv a_3(x_1 + t)(x_2 + t)(x_3 + t),$$
$$g - th \equiv a_3(x_1 - t)(x_2 - t)(x_3 - t),$$

and so the solutions of (14) are given by $x_1 \equiv \pm t$, $x_2 \equiv \mp t$, x_3 arbitrary etc. Then $f = 0$ becomes

$$\sum x_1x_2x_3 + t^2\sum x_1 \equiv 0.$$

When $t \equiv 0$, this is $\sum x_1\,x_2\,x_3 \equiv 0$. When $t \not\equiv 0$, on replacing x_1 by tx_1, etc., this becomes

$$\sum x_1 + \sum x_1x_2x_3 \equiv 0.$$

Suppose finally that $a_3 \equiv a_4 \equiv 0$ so that (9) becomes

$$a_0 + a_1\sum x_1 + a_2\sum x_1x_2 \equiv 0,$$
$$a_1 + a_2\sum x_1 \equiv 0. \tag{15}$$

If $a_2 \equiv 0$, f becomes $a_0 + a_1(x_1 + x_2 + x_3 + x_4) \equiv 0$, and has p^3 solutions.

If $a_2 \not\equiv 0$, on replacing x_1 by $x_1 + c$, etc., in (15), we have

$$x_1 + x_2 + x_3 + A \equiv 0, \quad x_2\,x_3 + x_3x_1 + x_1\,x_2 + B \equiv 0,$$

say, or

$$x_1\,x_2 + (x_1 + x_2)(-A - x_1 - x_2) + B \equiv 0.$$

Unless $A \equiv B \equiv 0$, this congruence is irreducible and has $p + O(1)$ solutions.

When $A \equiv B \equiv 0$, (15) is tantamount to $a_1 \equiv a_0 \equiv 0$, and $f = 0$ becomes

$$x_4(x_1 + x_2 + x_3) + x_2\,x_3 + x_3\,x_1 + x_1\,x_2 \equiv 0.$$

This is an excluded case which has $p^2(p-1)+p\,M'$ solutions, where M' is the number of solutions of

$$x_1+x_2+x_3\equiv 0,\quad x_2x_3+x_3x_1+x_1x_2\equiv 0$$

and so of

$$x_2^2+x_2x_3+x_3^2\equiv 0.$$

References

1. L. J. Mordell, *The number of solutions of some congruences in two variables*, Math. Z., *37* (1933), 193–209.
2. H. Hasse, *Vorlesungen über Zahlentheorie* (Berlin, 1950), 145.

St. John's College, Cambridge