MATH. SCAND. 5 (1957), 21–26

NOTE ON SIMULTANEOUS QUADRATIC CONGRUENCES

L. J. MORDELL

Let p be an odd prime and let

$$f(x) = a_1 x_1^2 + \ldots + a_n x_n^2 + a_0 ,$$

where the a's are integers and $a_1 a_2 \ldots a_n \not\equiv 0 \pmod p$. It is well known (cf. [1, p. 491]) that the number N_1 of solutions of

$$f(x) \equiv 0 \pmod p \tag{1}$$

can be expressed in a simple form. Since all the congruences throughout this paper are taken mod p, we shall omit mod p hereafter. Then with the usual Legendre symbol, we have the results:

$$\begin{cases} \underline{n \text{ even:}} & \\ N_1 = p^{n-1} - p^{\frac{1}{2}n-1}\left(\dfrac{(-1)^{\frac{1}{2}n} a_1 a_2 \ldots a_n}{p}\right), & a_0 \not\equiv 0 , \\ N_1 = p^{n-1} + (p-1)p^{\frac{1}{2}n-1}\left(\dfrac{(-1)^{\frac{1}{2}n} a_1 a_2 \ldots a_n}{p}\right), & a_0 \equiv 0 . \end{cases} \tag{2}$$

$$\begin{cases} \underline{n \text{ odd:}} & \\ N_1 = p^{n-1} + p^{\frac{1}{2}(n-1)}\left(\dfrac{(-1)^{\frac{1}{2}(n+1)} a_0 a_1 \ldots a_n}{p}\right), & a_0 \not\equiv 0 , \\ N_1 = p^{n-1}, & a_0 \equiv 0 . \end{cases} \tag{3}$$

In particular, when p is large, we have various estimates

$$N_1 = p^{n-1} + O(p^{\frac{1}{2}n-\delta}), \qquad \delta = 1, 0, \tfrac{1}{2}, \tfrac{1}{2}n \tag{4}$$

uniformly in the constants a. These results, however, can be found without a knowledge of the exact results.

Let us now consider the number N of solutions of the $m < n$ simultaneous congruences in the n variables $x_1, x_2, \ldots, x_n$

$$f_r(x) = a_{r1} x_1^2 + \ldots + a_{rn} x_n^2 + a_{r0} \equiv 0, \qquad r = 1, 2, \ldots, m . \tag{5}$$

Received April 3, 1957.

We cannot expect to find exact formulae for N comparable in simplicity with (2) and (3). Surprisingly enough when all the $a_{r0} \equiv 0$, and $m=2$ and n is odd, the result expresses itself in a form (27) similar to (2) when $a_0 \equiv 0$. The exact results for N are not without interest and in some general cases lead to results of the types (4). They are not best possible for $m > 2$, but I give a conjecture for the best possible result. The results will be more interesting and less complicated if we impose the restriction that when all the $a_{r0} \equiv 0$, the congruences (5) are linearly independent in respect of every set of m variables taken from the n variables $x_1, x_2, \ldots, x_n$. But when the a_{r0} are not all $\equiv 0$, we assume that the congruences (5) are linearly independent in respect of every set of m variables taken from the $n+1$ variables $x_1, x_2, \ldots, x_n, 1$.

We shall see that the value of N can be expressed in terms of sums S_l, $l=0, 1, \ldots, m-1$, now defined. Write

$$B_r = b_{1r}t_1 + \ldots + b_{m-l,r}t_{m-l}, \qquad r = 0, 1, \ldots, n-l,$$

where the b's are easily expressed in terms of the a's.

Then

$$S_l = \sum_t \left(\frac{B_0 B_1 \ldots B_{n-l}}{p}\right), \tag{6}$$

where the summation is taken over a complete set of residues for each of the $m-l$ variables t. The estimation of sums such as S_l seems to be very difficult except when $n-l$ is even. Then $S_l=0$ as is seen on replacing $t_1, \ldots, t_{m-l}$ by $tt_1, \ldots tt_{m-l}$ where t is a quadratic nonresidue of p. When $n-l$ is odd and $m-1<n$ when all the $a_{n0} \equiv 0$, I suggest the best possible result

$$S_l = O\left(p^{\frac{1}{2}(m-l+1)}\right). \tag{7}$$

This is true when $m-l=2$ as follows from a deep result by Weil in the theory of algebraic function fields cf. [2]. Thus

$$S_l = \sum_t \prod_{r=0}^{n-l} \left(\frac{b_{1r}t_1 + b_{2r}t_2}{p}\right). \tag{8}$$

When $t_2 \not\equiv 0$, put $t_1 = tt_2$. Then

$$S_l = (p-1) \sum_t \prod_{r=0}^{n-l} \left(\frac{b_{1r}t + b_{2r}}{p}\right) + (p-1) \prod_{r=0}^{n-l} \left(\frac{b_{1r}}{p}\right), \tag{9}$$

and Weil's result shows that in general, the first sum is $O(p^{\frac{1}{2}})$.

A crude estimate for S_l in (6) is obtained by taking $m-l-1$ of the variables t arbitrarily. Then on noting Weil's result in (9)

$$(7') \qquad S_l = O(p^{m-l-\frac{1}{2}}),$$

we find the following results.

Suppose first that n is even. If all the $a_{r0} \equiv 0$,

$$(10) \qquad N = p^{n-m} + O\big(p^{\frac{1}{2}(n-1)} \mid p^{\frac{1}{2}(n-m+1)}\big), \qquad n \geqq 2m,$$

where the stroke separates the crude estimate on the left from the conjectured estimate on the right. If not all the $a_{r0} \equiv 0$,

$$(11) \qquad N = p^{n-m} + O\big(p^{\frac{1}{2}(n-3)} \mid p^{\frac{1}{2}(n-m)}\big), \qquad n \geqq 2m-2.$$

Next let n be odd. When all the $a_{r0} \equiv 0$,

$$(12) \qquad N = p^{n-m} + O\big(p^{\frac{1}{2}n-1} \mid p^{\frac{1}{2}(n-m+1)}\big), \qquad n \geqq 2m-1.$$

When not all the $a_{r0} \equiv 0$,

$$(13) \qquad N = p^{n-m} + O\big(p^{\frac{1}{2}n-1} \mid p^{\frac{1}{2}(n-m)}\big), \qquad n \geqq 2m-1.$$

When n does not satisfy the inequalities in (10) etc., I can find only the crude result

$$(14) \qquad N = p^{n-m} + O\big(p^{n-m-\frac{1}{2}}\big),$$

which, however, is best possible when $m = n-2$ or $n-1$, except when all the $a_{r0} \equiv 0$.

The results for $m = 2$ are given in (25) and (26).

We consider first the case when all the $a_{r0} \equiv 0$. We may suppose then that $m < n-1$ since if $m = n-1$, the congruences give the ratios of $x_1^2 : x_2^2 : \ldots$. Write $e(x) = e^{2\pi i x/p}$. Then the number of solutions of the congruences (5) is given by the formula

$$(15) \qquad p^m N = \sum_{t,\,x} e\big(t_1 f_1(x) + \ldots + t_m f_m(x)\big),$$

summed over a complete set of residues for each of $t_1, \ldots, t_m$ and $x_1, \ldots, x_n$. For clearly the general term of the sum in (15) is zero or p^m according as x is not or is a solution of (5). Hence

$$(16) \qquad p^m N = \sum_{t,\,x} e\big(A_1 x_1^2 + \ldots + A_n x_n^2\big),$$

where

$$(17) \qquad A_r = a_{1r} t_1 + \ldots + a_{mr} t_m, \qquad r = 1, 2, \ldots, n.$$

When all the t's $\equiv 0$, the corresponding terms on the right hand side give p^n. To evaluate the other terms, we require the well known Gauss' sum

$$\sum_x e(ax^2) = \begin{cases} \varepsilon\left(\dfrac{a}{p}\right)p^{\frac{1}{2}}, & a \not\equiv 0, \text{ where } \varepsilon = i^{\frac{1}{4}(p-1)^2} \\ p, & a \equiv 0\,. \end{cases}$$

Suppose now the t's are such that only λ (where $0 \leqq \lambda < m$) of the $A_1, \ldots, A_n$ are $\equiv 0$. Since any m A's are linearly independent, this is allowable and not all the t's are $\equiv 0$. Suppose then that $A_1', A_2', \ldots, A_\lambda'$ are all $\equiv 0$. Summing for the x's, the sums in $x_1, \ldots, x_\lambda$ each give p, and so we have

$$(18)\qquad p^m N = p^n + \sum_{\lambda=0}^{m-1}\left[\varepsilon^{n-\lambda}p^{\frac{1}{2}(n+\lambda)}\sum_t\left(\frac{A_{\lambda+1}' \ldots A_n'}{p}\right)\right],$$

where the sum in the t's involve $m-\lambda$ independent variables t' obtained by eliminating $t_1', t_2', \ldots, t_\lambda'$ by using $A_1' \equiv 0, \ldots A_\lambda' \equiv 0$. The summation in λ is also to include every selection of λ forms from the A's.

The general term in the t summation in (18) is zero when $n-\lambda$ is odd as is evident on writing $tt_1, tt_2, \ldots$ for $t_1, t_2, \ldots$, where t is a nonquadratic residue of p. We suppose then that $n-\lambda$ is even. Then since from (7), (7′), the crude and the conjectured estimates for the t summations are $O(p^{m-\lambda-\frac{1}{2}})$, $O(p^{\frac{1}{2}(m-\lambda+1)})$, respectively, we have

$$p^m N = p^n + \sum_{\lambda=0}^{m-1} O\left(p^{m+\frac{1}{2}(n-\lambda-1)} \mid p^{\frac{1}{2}(m+n+1)}\right).$$

Suppose first that n is even. Then the dominant term here arises from $\lambda = 0$, and we have

$$(19)\qquad N = p^{n-m} + O\left(p^{\frac{1}{2}(n-1)} \mid p^{\frac{1}{2}(n-m+1)}\right).$$

Next, let n be odd. The dominant term now arises from $\lambda = 1$, and so we have

$$(20)\qquad N = p^{n-m} + O\left(p^{\frac{1}{2}(n-2)} \mid p^{\frac{1}{2}(n-m+1)}\right).$$

Suppose next that not all the $a_{r0} \equiv 0$. We deduce the result from the number of solutions N' of the system in $n+1$ variables

$$(21)\qquad a_{r1}x_1^2 + \ldots + a_{rn}x_n^2 + a_{r0}x_0^2 \equiv 0, \qquad r = 1, 2, \ldots, m\,.$$

Denote by N'' the number of solutions with $x_0 \equiv 0$. Then

$$(22)\qquad N' = N'' + (p-1)N$$

on writing x_1x_0 etc. for x_1 when $x_0 \not\equiv 0$. Then, if n is even, we have from (20), (21)

$$(p-1)N = p^{n+1-m} + O\left(p^{\frac{1}{2}(n-1)} \mid p^{\frac{1}{2}(n-m+2)}\right) - p^{n-m} + O\left(p^{\frac{1}{2}(n-1)} \mid p^{\frac{1}{2}(n-m+1)}\right),$$

and so

$$(23) \qquad N = p^{n-m} + O\left(p^{\frac{1}{2}(n-3)} \mid p^{\frac{1}{2}(n-m)}\right), \qquad n \geqq 2m-2,\ n \text{ even}.$$

Next let n be odd. Then

$$(p-1)N = p^{n+1-m} + O\left(p^{\frac{1}{2}n} \mid p^{\frac{1}{2}(n-m+2)}\right) + O\left(p^{\frac{1}{2}(n-2)} \mid p^{\frac{1}{2}(n-m+1)}\right) - p^{n-m},$$

and so

$$(24) \qquad N = p^{n-m} + O\left(p^{\frac{1}{2}(n-2)} \mid p^{\frac{1}{2}(n-m)}\right), \quad n \geqq 2m-1,\ n \text{ odd}.$$

When $m=2$, we find the precise result from (18) and (22) on taking $\lambda = 0, 1$ and noting the terms that vanish.

If n is even,

$$(p-1)N = p^{n-1} + \varepsilon^n p^{\frac{1}{2}(n-2)}(p-1)\sum_{s=0}^{n}\prod_{r \neq s}\left(\frac{a_{1s}a_{2r}-a_{2s}a_{1r}}{p}\right) - \\ - p^{n-2} - \varepsilon^n p^{\frac{1}{2}(n-4)}\sum_{t_1, t_2}\left(\frac{A_1A_2 \ldots A_n}{p}\right),$$

or

$$(25) \qquad N = p^{n-2} + \varepsilon^n p^{\frac{1}{2}(n-2)}\sum_{s=0}^{n}\prod_{r \neq s}\left(\frac{a_{1s}a_{2r}-a_{2s}a_{1r}}{p}\right) - \\ - \varepsilon^n p^{\frac{1}{2}(n-4)}(p-1)^{-1}\sum_{t_1, t_2}\left(\frac{A_1A_2 \ldots A_n}{p}\right).$$

We can of course get rid of the factor $(p-1)^{-1}$ by using (9).

If n is odd,

$$(p-1)N = p^{n-1} + \varepsilon^{n+1}p^{\frac{1}{2}(n-3)}\sum_{t_1, t_2}\left(\frac{A_0A_1 \ldots A_n}{p}\right) - p^{n-2} - \\ - \varepsilon^{n-1}p^{\frac{1}{2}(n-3)}(p-1)\sum_{s=1}^{n}\prod_{r \neq s}\left(\frac{a_{1s}a_{2r}-a_{2s}a_{1r}}{p}\right)$$

or

$$(26) \quad N = p^{n-2} - \varepsilon^{n-1}p^{\frac{1}{2}(n-3)}\sum_{s=1}^{n}\prod_{r \neq s}\left(\frac{a_{1s}a_{2r}-a_{2s}a_{1r}}{p}\right) + \\ + \varepsilon^{n+1}p^{\frac{1}{2}(n-3)}(p-1)^{-1}\sum_{t_1, t_2}\left(\frac{A_0A_1 \ldots A_n}{p}\right).$$

When $a_{10} \equiv 0$, $a_{20} \equiv 0$, (18) gives

$$(27)\quad \begin{cases} \underline{n \text{ even:}} \\ N = p^{n-2} + \varepsilon^n p^{\frac{1}{2}(n-4)} \sum_{t_1, t_2} \left(\dfrac{A_1 \ldots A_n}{p}\right), \\ \underline{n \text{ odd:}} \\ N = p^{n-2} + \varepsilon^{n-1} p^{\frac{1}{2}(n-3)} (p-1) \sum_{s=1}^{n} \prod_{r \neq s} \left(\dfrac{a_{1s}a_{2r} - a_{2s}a_{1r}}{p}\right). \end{cases}$$

The results found were subject to restrictions on the value of n, for example $n \geqq 2m$. It does not seem easy to find good results when these restrictions are removed. I can find for (5) only

$$(28)\qquad N = p^{n-m} + O(p^{n-m-\frac{1}{2}}),$$

obtained by allowing $n-m-1$ of the variables to take arbitrary values. For then, on solving with respect to the m variables $x_1, x_2, \ldots, x_m$, we have, say, the system

$$x_r^2 \equiv a_r x^2 + b_r, \qquad r = 1, 2, \ldots m.$$

The number of solutions of this is given by

$$\begin{aligned} N' &= \sum_x \prod_{r=1}^{m} \left(1 + \left(\frac{a_r x^2 + b_r}{p}\right)\right) \\ &= \sum_x \prod_{r=1}^{m} \left(1 + \left(\frac{a_r x + b_r}{p}\right)\right)\left(1 + \left(\frac{x}{p}\right)\right) = p + \sum_g \sum_x \left(\frac{g(x)}{p}\right), \end{aligned}$$

say, where $g = g(x)$ is the product of at most $m+1$ linear factors. By Weil's result, if $(g(x)/p)$ is independent of x,

$$N' = p + O(p^{\frac{1}{2}}).$$

Otherwise, $N' = O(p)$, and a condition is imposed on the (x). In either case, (28) follows.

REFERENCES

1. P. Bachmann, *Die Arithmetik der quadratischen Formen*, Erste Abtheilung, Leipzig, 1898.
2. A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci. U.S.A. 27 (1941), 345–347.

ST. JOHN'S COLLEGE, CAMBRIDGE, ENGLAND
AND
UNIVERSITY COLLEGE, ACHIMOTA, GOLD COAST