Louis Joel Mordell

Incomplete exponential sums and incomplete residue systems for congruences

Czechoslovak Mathematical Journal, Vol. 14 (1964), No. 2, 235–242

Persistent URL: `http://dml.cz/dmlcz/100615`

Чехословацкий математический журнал, т. 14 (89) 1964, Прага

INCOMPLETE EXPONENTIAL SUMS AND INCOMPLETE RESIDUE SYSTEMS FOR CONGRUENCES

L. J. MORDELL, Cambridge und Arizona University

(Received June 16, 1962)

An estimate for the sum (1) in terms of the sum (2) and an estimate for the number of solutions of the system (3) in terms of the number of solutions of the system (4) are established.

Let p be a prime, $\xi = (\xi_1, \ldots, \xi_n)$ be n integer variables and let $f(\xi), f_1(\xi), \ldots, f_m(\xi)$ be $m + 1$ polynomials in the ξ with integer coefficients. Let $l = (l_1, \ldots, l_n)$ be n given integers with $0 \leqq l_1 < p, \ldots, 0 \leqq l_n < p$, say $0 \leqq (l) < p$. We consider here two related problems.

The first is to find an estimate for the exponential sum

$$S_n' = \sum_{\xi} e(f(\xi_1, \ldots, \xi_n)), \quad 0 \leqq \xi_1 < l_1, \ldots, 0 \leqq \xi_n < l_n, \tag{1}$$

say $0 \leqq (\xi) < (l)$, where $e(x) = \exp(2\pi i x/p)$, in terms of the complete exponential sum,

$$S_n = \sum_{x} e(f(x_1, \ldots, x_n)), \quad 0 \leqq (x) < p. \tag{2}$$

The second problem is to find an estimate for the number of solutions $N'_{n,m}$ of the m simultaneous congruences mod p

$$f_1(\xi) \equiv 0, \ldots, f_m(\xi) \equiv 0, \quad 0 \leqq (\xi) < (l) \tag{3}$$

in terms of the number $N_{n,m}$ of solutions of

$$f_1(x) \equiv 0, \ldots, f_m(x) \equiv 0, \quad 0 \leqq (x) < p. \tag{4}$$

Hereafter, all variables and summations expressed in terms of latin characters take the values $0, 1, \ldots, p - 1$. The ξ variables ξ_1 etc., take the values $0, 1, \ldots, l_1 - 1$, etc.

Both of these problems are of some interest and importance in number theory. Not much reference to them is found in books on number theory. Simple instances are given in VINOGRADOV's book on "Elementary number theory", and also by L. K. HUA [1]. Other results are found in scattered papers [2]. It may be useful to give an expository and unified account of these topics and to make the proofs a little more obvious and to find some general results.

A result for the first problem is well known when $n = 1$. We present the proof in a slightly different form. This extends also at once to the case of general n, and the same idea serves for the second problem.

Suppose then $n = 1$, $\xi = \xi_1$, and so

$$S_1' = \sum_{\xi} e(f(\xi)), \quad 0 \leqq \xi < l .$$

Clearly

$$pS_1' = \sum_{x,t,\xi} e(f(x) + t(x - \xi)) . \tag{5}$$

For the sum in t is zero unless $x = \xi$ when it gives a factor p.

We now sum for ξ. The term with $t = 0$ contributes $l \sum_x e(f(x)) = lS_1$. When $t \neq 0$, on summing for ξ, we have $\sum_{\xi} e(-t\xi) = (1 - e(-tl))/(1 - e(-t))$, so that

$$pS_1' = lS_1 + \sum_{x,t>0} e(f(x) + tx)\,(1 - e(-tl))/(1 - e(-t)) . \tag{6}$$

Suppose now that we have an estimate independent of t given by

$$\Big|\sum_x e(f(x) + tx)\Big| \leqq E . \tag{7}$$

Then $|pS_1' - lS_1| \leqq E \sum_{t>0} (\sin \pi t/p)^{-1} \leqq Ep \log p$, as is well known. Hence

$$S_1' = lp^{-1}S_1 + \Theta E \log p \quad \text{where} \quad |\Theta| < 1 ,$$

a well known result.

We next consider the case of general n and so $\xi = (\xi_1, \ldots, \xi_n)$, $l = (l_1, \ldots, l_n)$, $x = (x_1, \ldots, x_n)$ and $\xi_1 < l_1$, etc. We write

$$S_n' = \sum_{\xi} e(f(\xi)) , \quad S_n = \sum_x e(f(x)) . \tag{8}$$

We suppose there exist estimates $E_n^{(0)}, E_n^{(1)}, \ldots, E_n^{(n)}$ independent of the t's such that

$$\Big|\sum_x e(f(x) + t \,.\, x)\Big| \leqq E_n^{(r)} , \tag{9}$$

where the t part is a vector product, i.e. $t \,.\, x = \sum_{j=1}^{n} t_j x_j$, and the r refers to the number of t which are not zero. Thus $E_n^{(0)} = |S_n|$. In general, the estimates $E_n^{(r)}$ can be replaced by an estimate E_n independent of the r, but sometimes it is more useful to retain the $E_n^{(r)}$. Then the value of $E_n^{(r)}$ will depend upon which r of the t are not zero, and the r summation will then include all the choices of the t being zero.

We prove that

$$S_n' = l_1 \ldots l_n p^{-n} S_n + \Theta_n^{(n)} E_n^{(n)} (\log p)^n + R_n , \quad |\Theta_n^{(n)}| < 1 , \tag{10}$$

where with the convention about the r summation no confusion will arise if we write

$$(11) \qquad R_n = \sum_{r=1}^{n-1} \Theta_n^{(r)} l_{r+1} \dots l_n p^{r-n} E_n^{(r)} (\log p)^r , \quad |\Theta_n^{(r)}| < 1 .$$

The proof is similar to that for $n = 1$. Thus

$$(12) \qquad p^n S_n' = \sum_{\xi, t, x} e(f(x) + t \, . \, (x - \xi)) .$$

Clearly the t summation gives zero unless $x = \xi$ when we get $p^n S_n'$. When all the t are zero in (12), we have a contribution $l_1 l_2 \dots l_n S_n$. Suppose next r of the t are not zero. For convenience in writing, suppose these are $t_1, \dots, t_r$ and so $t_{r+1}, \dots, t_n$ are all zero. The ξ summation gives a contribution

$$l_{r+1} \dots l_n \sum_{t,x} e(f(x) + t \, . \, x) \frac{1 - e(-l_1 t_1)}{1 - e(-t_1)} \dots \frac{1 - e(-l_r t_r)}{1 - e(-t_r)} .$$

This has modulus less than

$$l_{r+1} \dots l_n \sum_t E_n^{(r)} (\sin \pi t_1 / p \dots \sin \pi t_r / p)^{-1} < l_{r+1} \dots l_n E_n^{(r)} p^r (\log p)^r .$$

Summing this for r, and denoting by $\Theta_n^{(r)}$ numbers such that $|\Theta_n^{(r)}| < 1$, and noting our convention about the r summation, we have the value of R_n given in (11).

We come to the second problem. Denote by $N_{n,m}'$ the number of solutions of the congruences

$$(13) \qquad f_j(\xi) \equiv 0 , \quad 0 \leqq (\xi) < (l) \quad (j = 1, \dots, m) ,$$

and by $N_{n,m}$ the number of solutions of the congruences

$$(14) \qquad f_j(x) \equiv 0 , \quad 0 \leqq (x) < p \quad (j = 1, \dots, m) .$$

If we put $u \, . \, f(x) = u_1 f_1(x) + \dots + u_m f_m(x)$, we have

$$(15) \qquad p^{n+m} N_{n,m}' = \sum_{u,t,x,\xi} e(u \, . \, f(x) + t \, . \, (x - \xi)) ,$$

since the sum in t, u is zero unless $x = \xi$, $f_j(\xi) \equiv 0$ $(j = 1, \dots, m)$. We shall require some estimates for exponential sums independent of the t, u. Suppose that

$$(16) \qquad \Big|\sum_{x,u} e(u \, . \, f(x) + t \, . \, x)\Big| \leqq E_n^{(r)} ,$$

where the r refers to the number of t which are not zero. Sometimes the estimate $E_n^{(r)}$ can be replaced by an estimate E_n independent of the r, but as is seen later, it may be more useful to retain the $E_n^{(r)}$. We note as before that the value of $E_n^{(r)}$ will depend upon the selection of r of the t which are not zero, and that the r summation includes all selections.

We prove that

$$N'_{n,m} = l_1 \dots l_n p^{-n} N_{n,m} + \Theta_n E_n^{(n)} (\log p)^n + R_n\,, \tag{17}$$

where

$$R_n = \sum_{r=1}^{n-1} \Theta_n^{(r)} l_{r+1} \dots l_n p^{r-n-m} (\log p)^r E_n^{(r)} \tag{18}$$

with the convention for the r summation and the Θ have moduli <1.

When all the t are zero in (15), we have a contribution $p^m l_1 \dots l_n N_{n,m}$. Suppose next r of the t are not zero, say $t_1, \dots, t_r$. Then just as in (12), we have a contribution $\Theta_n^{(r)} l_{r+1} \dots l_n E_n^{(r)} p^r (\log p)^r$, and so (17) and (18) follow.

The estimate (17) depends upon finding useful estimates for the $E_n^{(r)}$. Crude estimates for the x summation are easily found but then the u summation introduces a factor p. More precise results can be found when a simple closed expression for the x summation can be found in terms of u. This occurs when $m = 1$ and $f(x)$ is the general quadratic polynomial in the x. For simplicity, we consider the two cases:

$$f(x) = a_1 x_1^2 + \dots + a_n x_n^2 + a\,, \quad a_1 \dots a_n \not\equiv 0\,. \tag{19}$$

$$f(x) = a_1 x_1^2 + \dots + a_s x_s^2 + a_{s+1} x_{s+1} + \dots + a_n x_n + a\,, \quad a_1 a_2 \dots a_n \not\equiv 0\,. \tag{20}$$

In the first case, the general exponential sum (16) becomes, say,

$$E = \sum_{x,u} e(u(a_1 x_1^2 + \dots + a_n x_n^2 + a) + t_1 x_1 + \dots + t_n x_n)\,. \tag{21}$$

Suppose first that all the t are zero. Then there is a contribution $E' = p l_1 \dots l_n N_{n,1}$, where $N_{n,1}$ is the number of solutions of the congruence

$$a_1 x_1^2 + \dots + a_n x_n^2 + a \equiv 0\,.$$

Then

$$\begin{aligned} pN_{n,1} &= \sum_{u,x} e(u(a_1 x_1^2 + \dots + a_n x_n^2 + a)) = \\ &= p^n + \sum_{u=1,x=0}^{p-1} e(u(a_1 x_1^2 + \dots + a_n x_n^2 + a)) = \\ &= p^n + i^{n((p-1)/2)^2} \left(\frac{a_1 \dots a_n}{p}\right) p^{n/2} \sum_{u=1}^{p-1} \left(\frac{u}{p}\right)^n e(au)\,, \end{aligned}$$

and so is easily evaluated. As the result is well known, it will suffice to quote it for $p \not\equiv 2$.

Suppose first n is even.

If $a \not\equiv 0$, $N_{n,1} = p^{n-1} - \left(\frac{(-1)^{n/2} a_1 \dots a_n}{p}\right) p^{(n-2)/2}$.

If $a \equiv 0$, $N_{n,1} = p^{n-1} - (p-1)\left(\frac{(-1)^{n/2} a_1 \dots a_n}{p}\right) p^{(n-2)/2}$.

Suppose next n is odd.

$$\text{If } a \not\equiv 0,\ N_{n,1} = p^{n-1} + \left(\frac{(-1)^{(n+1)/2}\, a a_1 \dots a_n}{p}\right) p^{(n-1)/2}.$$

$$\text{If } a \equiv 0,\ N_{n,1} = p^{n-1}.$$

Suppose next that all the t are not zero. Then the sum in (21) with $u = 0$ is zero and so we may suppose herafter that $u \not\equiv 0$.

The sums in the x are Gaussian sums and so we now have a contribution

$$(22)\quad E' = i^{n((p-1)/2)^2} p^{n/2} \left(\frac{a_1 a_2 \dots a_n}{p}\right) \sum_u{}' \left(\frac{u^n}{p}\right) e\left(au - \frac{t_1^2}{4a_1 u} - \dots - \frac{t_n^2}{4a_n u}\right),$$

where $1/4a_1 u = u'$ with $4a_1 u u' \equiv 1$ etc.

We must now consider the sums

$$K_{c,d}^{(n)} = \sum_u{}' \left(\frac{u}{p}\right)^n e(cu + d/u)$$

where $1/u = u'$ and $uu' \equiv 1$. When n is even, these are the well known Kloosterman sums. If $cd \equiv 0$, $K_{c,d}^{(n)} = -1$ unless $c \equiv d \equiv 0$ when $K_{c,d}^{(n)} = p - 1$. If $cd \not\equiv 0$, we have Weil's estimate

$$|K_{c,d}^{(0)}| \leqq 2\sqrt{p},$$

and this can also be used unless $c \equiv d \equiv 0$.

When n is odd, Salié ([4], p. 102) has proved that $K_{c,d}^{(1)}$ can be expressed in finite terms. For our purpose, it suffices to state that $|K_{c,d}^{(1)}| < 2\sqrt{p}$. Hence in (17), (18) we can take $E_n^{(r)} = O(p^{(n+1)/2})$.

We consider now the second case of the quadratic form given by (20). The exponential sum (16) becomes

$$(23)\qquad E = \sum_{x,u} e(g(x, u)),$$

where

(24)

$$g(x, u) = u(a_1 x_1^2 + \dots + a_s x_s^2 + a_{s+1} x_{s+1} + \dots + a_n x_n + a) + t_1 x_1 + \dots + t_n x_n.$$

When all the t are zero, we have a contribution p^n to E since

$$a_1 x_1^2 + \dots + a_s x_s^2 + a_{s+1} x_{s+1} + \dots + a_n x_n + a \equiv 0$$

has p^{n-1} solutions.

Suppose next that all the t are not zero. Then the contribution to E when $u = 0$ is zero and so we may suppose that u does not take the value zero. The sums in $x_1, \dots, x_s$ are Gaussian sums and so this gives

$$E' = i^{s((p-1)/2)^2} p^{s/2} \left(\frac{a_1 \dots a_s}{p}\right) \sum_{x,u} \left(\frac{u}{p}\right)^s e(h(x, u)),$$

where

$$h(x, u) = x_{s+1}(a_{s+1}u + t_{s+1}) + \dots + x_n(a_n u + t_n) + au - \frac{t_1^2}{4a_1 u} - \dots - \frac{t_s^2}{4a_s u} .$$

The sums for $x_{s+1}, \dots, x_n$ are zero unless

$$a_{s+1}u + t_{s+1} = 0, \dots, a_n u + t_n = 0 .$$

This gives at most one value of u. Hence

$$|E'| \leqq p^{s/2} . p^{n-s} = p^{n-s/2} . \tag{25}$$

This can be used in (17) and (18) for all the $E_n^{(r)}$.

The particular case when $n = 2$ was dealt [2] with in a slightly more general form.

We consider finally the case of m simultaneous congruences in n variables,

$$f_j(\xi) \equiv 0 , \quad 0 \leqq (\xi) < (l) , \quad j = 1, \dots, m .$$

We have already seen that the number $N'_{n,m}$ of solutions is given by

$$N'_{n,m} = l_1 \dots l_n p^{-n} N_{n,m} + \Theta_n^{(n)} (\log p)^n E_n^{(n)} + R_n , \tag{26}$$

where

$$R_n = \sum_{r=1}^{n-1} \Theta_n^{(r)} l_{r+1} \dots l_n p^{r-n-m} (\log p)^r E_n^{(r)} \tag{27}$$

with the convention about the r summation. The number $N_{n,m}$ is given by

$$p^m N_{n,m} = \sum_{x,u} e(\sum_{s=1}^{m} u_s f_s(x)) . \tag{28}$$

The terms with all the $u \equiv 0$ contribute p^n to the sum and so we suppose herafter that all the u are not $\equiv 0$. In some instances, it may be desirable to consider the various cases arising when some of the u are $\equiv 0$. This is not so when all the $f(x)$ are quadratic forms such as

$$f_s(x) = a_{s,1} x_1^2 + \dots + a_{s,n} x_n^2 + a_s . \tag{29}$$

I have given some results for such congruences. It may be useful, however, to give a self contained resume with more detail for the case $m = 2$ when the results are fairly simple. The summation (28) becomes

$$S = \sum_{u,x} e(h(x, u)) , \tag{30}$$

where

$$h(x, u) = \sum_{s=1}^{n} (\sum_{t=1}^{m} (u_t a_{ts}) x_s^2 + \sum_{t=1}^{m} u_t a_t) . \tag{31}$$

Suppose first that the u are such that no x^2 has a coefficient $\equiv 0$. The sums in the x are Gauss's sums and so there is a contribution S' to (30) given by

$$(32)\ S' = i^{n((p-1)/2)^2} p^{n/2} \sum_u \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + \dots + u_m a_{ms}}{p}\right) e(u_1 a_1 + \dots + u_m a_m) .$$

Suppose next that r of the x^2 have coefficients $\equiv 0$. The summation in these x gives p^r. Then on replacing r of the u in terms of the remaining $n - r$ of the u, we have a sum similar to that in (32). In general, it is not easy to find precise estimates for (32) even when Weil's results are used.

The special case $m = 2$, $a_1 = a_2 = 0$ is worthy of attention. Then (32) becomes

$$S' = i^{n((p-1)2)^2} p^{n/2} \sum_u \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p}\right).$$

The contribution to the series when $u_2 \equiv 0$ is

$$\sum_{u_1} \left(\frac{u_1^n}{p}\right)\left(\frac{a_{11} \dots a_{1n}}{p}\right) = 0 \quad \text{if } n \text{ is odd},$$

$$= (p-1)\left(\frac{a_{11} \dots a_{1n}}{p}\right) \quad \text{if } n \text{ is even.}$$

When $u_2 \not\equiv 0$, we put $u_1 = uu_2$. The contribution to S' is

$$i^{n((p-1)/2)^2} p^{n/2} \sum_{u,u_2} \left(\frac{u_2}{p}\right)^n \prod_{s=1}^{n} \left(\frac{ua_{1s} + a_{2s}}{p}\right) = 0 \quad \text{if } n \text{ is odd},$$

$$= O((p-1)\, p^{(n+3)/2}) \quad \text{if } n \text{ is even},$$

since the number of solutions of

$$v^2 \equiv \prod_{s=1}^{n} \left(\frac{ua_{1s} + a_{2s}}{p}\right)$$

is $p + O(\sqrt{p})$ by Weil's theorem.

We consider next the case in (31) when some of the x^2 have a coefficient $\equiv 0$. We suppose for simplicity that this occurs for only one coefficient, and so the a must satisfy the condition $a_{1,\lambda}/a_{2,\lambda} \not\equiv a_{1,\mu}/a_{2,\mu}$ for all $\lambda \neq \mu$, $1 \leqq \lambda, \mu \leqq n$. It suffices to examine the case when x_1^2 has a coefficient $\equiv 0$. Then $u_1 a_{11} + u_2 a_{21} \equiv 0$, and the contribution to (31) takes the form

$$S'' = i^{(n-1)((p-1)/2)^2} p^{(n+1)/2} \sum_u \prod_{s=2}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p}\right).$$

Put $u_1 = ta_{21}$, $u_2 = -ta_{11}$. Then

$$S'' = i^{(n-1)((p-1)/2)^2} p^{(n+1)/2} \sum_t \left(\frac{t}{p}\right)^{n-1} \prod_{s=2}^{n} \left(\frac{a_{21} a_{1s} - a_{11} a_{2s}}{p}\right) =$$

$$= 0 \text{ if } n \text{ is even}, \quad = O(p^{(n+3)/2}) \text{ if } n \text{ is odd.}$$

Then from (28) we have

$$p^2 N_{n,2} = p^n + O(p^{(n+3)/2}) .$$

Hence $N_{n,2} = p^{n-2} + O(p^{(n-1)/2})$ and this is contained in the result given in my paper.

This work has been supported in part by the National Science Foundation, Washington, D. C.

References

[1] *L. K. Hua:* Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie. Enz. der math. Wiss., Leipzig 1959.

[2] *L. J. Mordell:* The number of solutions in incomplete residue sets of quadratic congruences. Archiv der Math. *VIII* (1957), 153—157.

[3] *L. J. Mordell:* Note on simultaneous quadratic congruences. Mathematica Scandinavica *5* (1957), 21—26.

[4] *H. Salié:* Über die Kloostermanschen Summen. Math. Zeitschrift *34* (1932), 91—109.

Резюме

НЕПОЛНЫЕ ПОКАЗАТЕЛЬНЫЕ СУММЫ И НЕПОЛНЫЕ СИСТЕМЫ ВЫЧЕТОВ ДЛЯ СРАВНЕНИЙ

Л. Й. МОРДЕЛ (L. J. Mordell), Кембридж

Пусть p — простое число, $x_1, \ldots, x_n$, $\xi_1, \ldots, \xi_n$ — целые переменные, $f, f_1, \ldots$ $\ldots, f_m$ — полиномы с целыми коэффициентами и $l_1, \ldots, l_n$ — целые числа такие, что $0 \leqq l_1 < p, \ldots, 0 \leqq l_n < p$. Положим $e(x) = \exp(2\pi i\, x/p)$. В работе приведена оценка суммы

$$\sum e(f(\xi_1, \ldots, \xi_n)) \quad (0 \leqq \xi_1 < l_1, \ldots, 0 \leqq \xi_n < l_n)$$

при помощи суммы

$$\sum e(f(x_1, \ldots, x_n)) \quad (0 \leqq x_1 < p, \ldots, 0 \leqq x_n < p)$$

и оценка числа решений системы сравнений mod p

$$f_1(\xi_1, \ldots, \xi_n) \equiv 0, \ldots, f_m(\xi_1, \ldots, \xi_n) \equiv 0 \quad (0 \leqq \xi_1 < l_1, \ldots, 0 \leqq \xi_n < l_n)$$

при помощи числа решений системы сравнений

$$f_1(x_1, \ldots, x_n) \equiv 0, \ldots, f_m(x_1, \ldots, x_n) \equiv 0 \quad (0 \leqq x_1 < p, \ldots, 0 \leqq x_n < p) .$$

Особенно изучается случай, когда f_j — квадратические полиномы.