RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

P. J. MC CARTHY

The number of restricted solutions of some systems of linear congruences

Rendiconti del Seminario Matematico della Università di Padova, tome 54 (1975), p. 59-68

<http://www.numdam.org/item?id=RSMUP_1975__54__59_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 54 (1975)

The Number of Restricted Solutions of Some Systems of Linear Congruences.

P. J. MC CARTHY (*)

We shall determine the number of solutions of a system of linear congruences

$$n_i \equiv x_{i1} + \ldots + x_{is} (\mathrm{mod}\, r)\,, \qquad i = 1, \ldots, t, \tag{1}$$

when the solutions are required to satisfy certain conditions. Two solutions, $\{x_{ij}\}$ and $\{x'_{ij}\}$, are counted as the same when and only when $x_{ij} \equiv x'_{ij} (\mathrm{mod}\, r)$ for $i = 1, \ldots, t$ and $j = 1, \ldots, s$.

For each r, and for $j = 1, \ldots, s$, let $T_j(r)$ be a nonempty set of t-tuples of integers from the set $\{1, \ldots, r\}$. We shall use the notation $\langle \ldots \rangle$ for a t-tuple since we wish to reserve the notation $(\ldots)$ for greatest common divisor. Let $M(n_1, \ldots, n_t, r, s)$ be the number of solutions of (1) with $\langle x_{1j}, \ldots, x_{tj} \rangle \in T_j(r)$ for $j = 1, \ldots, s$. Under a certain hypothesis this number can be evaluated using only elementary properties of the complex exponential function.

A function $f(n, r)$ of an integer variable n and a positive integer variable r is called an even function $(\mathrm{mod}\, r)$ if $f(n, r) = f((n, r), r)$ for all n and r. A function $g(n_1, \ldots, n_t, r)$ of t integer variables $n_1, \ldots, n_t$ and a positive integer variable r is called a totally even function $(\mathrm{mod}\, r)$ if there is an even function $(\mathrm{mod}\, r)$, say $f(n, r)$, such that $g(n_1, \ldots, n_t, r) = f((n_1, \ldots, n_1), r)$ for all $n_1, \ldots, n_t$, and r. Even functions and totally even functions $(\mathrm{mod}\, r)$ were introduced and studied by Cohen, the former in [3] and several other papers and the latter in [6].

(*) Indirizzo dell'A.: Department of Mathematics, University of Kansas, Lawrence, KS 66045, U.S.A.

For $j = 1, \ldots, s$ let

$$g_j(n_1, \ldots, n_t, r) = \sum_{\langle x_1, \ldots, x_t \rangle \in T_j(r)} e(n_1 x_1 + \ldots + n_t x_t, r),$$

where $e(n, r) = \exp(2\pi i n/r)$.

THEOREM 1. If $g_j(n_1, \ldots, n_t, r)$ is a totally even function (mod r) for $j = 1, \ldots, s$, then

$$M(n_1, \ldots, n_t, r, s) = \frac{1}{r^t} \sum_{d|r} \left\{ \prod_{j=1}^{s} g_j(r/d, r) \right\} c(n_1, \ldots, n_t, d),$$

where $g_j(n, r) = g_j(n, \ldots, n, r)$ and

$$c(n_1, \ldots, n_t, r) = \sum_{(y_1, \ldots, y_t, r) = 1} e(n_1 y_1 + \ldots + n_t y_t, r).$$

PROOF. Set $M = M(n_1, \ldots, n_t, r, s)$. Then

$$M = \sum_1 \ldots \sum_t \prod_{j=1}^{s} h_j(x_{1j}, \ldots, x_{tj}),$$

where $\sum_i$ is the summation over all solutions of the ith congruence of (1), and for $j = 1, \ldots, s$,

$$h_j(x_{1j}, \ldots, x_{tj}) = \begin{cases} 1 & \text{if } \langle x_{1j}, \ldots, x_{tj} \rangle \in T_j(r) \\ 0 & \text{otherwise.} \end{cases}$$

Since

$$h_j(x_{1j}, \ldots, x_{tj}) = \frac{1}{r^t} \sum^{(j)} \prod_{i=1}^{t} \sum_{q_{ij}=1}^{r} e\big((x_{ij} - y_{ij}) q_{ij}, r\big),$$

where $\sum^{(j)}$ is summation over all $\langle y_{1j}, \ldots, y_{tj} \rangle \in T_j(r)$, we have

$$\begin{aligned} M &= \frac{1}{r^{ts}} \sum_1 \ldots \sum_t \prod_{j=1}^{s} \sum^{(j)} \prod_{i=1}^{t} \sum_{q_{ij}=1}^{r} e\big((x_{ij} - y_{ij}) q_{ij}, r\big) \\ &= \frac{1}{r^{ts}} \sum\nolimits' \sum_1 \ldots \sum_t \prod_{j=1}^{s} \sum^{(j)} \prod_{i=1}^{t} e(x_{ij} q_{ij}, r) e(-y_{ij} q_{ij}, r) \\ &= \frac{1}{r^{ts}} \sum\nolimits' \sum_1 \ldots \sum_t \prod_{j=1}^{s} \left\{ g_j(-q_{1j}, \ldots, -q_{tj}, r) \prod_{i=1}^{t} e(x_{ij} q_{ij}, r) \right\}, \end{aligned}$$

where $\sum'$ is summation over all ts-tuples of integers from the set $\{1, \ldots, r\}$. Since $g_j(n_1, \ldots, n_t, r)$ is a totally even function (mod r), the minus signs can be removed from the arguments of this function. Hence,

$$M = \frac{1}{r^{ts}} \sum{}' \left\{ \prod_{j=1}^{s} g_j(q_{1j}, \ldots, q_{tj}, r) \right\} \prod_{i=1}^{t} \sum_{i} \prod_{j=1}^{s} e(x_{ij} q_{ij}, r) .$$

By [2, Lemma 3],

$$\sum_{i} \prod_{j=1}^{s} e(x_{ij} q_{ij}, r) = \begin{cases} r^{s-1} e(n_i q_i, r) & \text{if } q_{i1} = \ldots = q_{it} = q_i \\ 0 & \text{otherwise} . \end{cases}$$

Thus,

$$M = \frac{1}{r^t} \sum{}'' \left\{ \prod_{j=1}^{s} g_j(q_1, \ldots, q_t, r) \right\} \prod_{i=1}^{t} e(n_i q_i, r) ,$$

where $\sum''$ is summation over all t-tuples $\langle q_1, \ldots, q_t \rangle$ of integers from the set $\{1, \ldots, r\}$.

Let d run over all divisors of r, and for each d let $\langle u_1, \ldots, u_t \rangle$ run over all t-tuples of integers from the set $\{1, \ldots, r/d\}$ such that $(u_1, \ldots, u_t, r/d) = 1$. Then $\langle u_1 d, \ldots, u_t d \rangle$ runs over all t-tuples of integers from the set $\{1, \ldots, r\}$. (See [6, p. 356] and the reference given there, and Proposition 2 below.) Thus,

$$M = \frac{1}{r^t} \sum_{d \mid r} \sum_{(u_1, \ldots, u_t, r/d) = 1} \left\{ \prod_{j=1}^{s} g_j(u_1 d, \ldots, u_t d, r) \right\} e(n_1 u_1 + \ldots + n_t u_t, r/d) .$$

Since $g_j(n_1, \ldots, n_t, r)$ is a totally even function (mod r), $g_j(u_1 d, \ldots, u_t d, r) = g_j(d, r)$. Therefore,

$$\begin{aligned} M &= \frac{1}{r^t} \sum_{d \mid r} \left\{ \prod_{j=1}^{s} g_j(d, r) \right\} \sum_{(u_1, \ldots, u_t, r/d) = 1} e(n_1 u_1 + \ldots + n_t u_t, r/d) \\ &= \frac{1}{r^t} \sum_{d \mid r} \left\{ \prod_{j=1}^{s} g_j(d, r) \right\} c(n_1, \ldots, n_t, r/d) , \end{aligned}$$

which is the same as the formula in the statement of the theorem.

There is a general method for obtaining sets $T_j(r)$ such that the hypothesis of Theorem 1 is satisfied. For each r, let $D(r)$ be a nonempty

set of divisors of r, and let

$$T(r) = \{\langle x_1, \ldots, x_t\rangle : 1 \leqslant x_j \leqslant r \text{ for } j = 1, \ldots, t \text{ and } (x_1, \ldots, x_t, r) \in D(r)\} .$$

We shall show that

$$g(n_1, \ldots, n_t, r) = \sum_{\langle x_1, \ldots, x_t\rangle \in T(r)} e(n_1 x_1 + \ldots + n_t x_t, r)$$

is a totally even function (mod r).

PROPOSITION 1. [6] $c(n_1, \ldots, n_t, r)$ is a totally even function (mod r). In fact,

$$c(n_1, \ldots, n_t, r) = \sum_{d \mid (n_1, \ldots, n_t, r)} d^t \mu(r/d) .$$

PROPOSITION 2. Let d run over the divisors of r in $D(r)$, and for each d let $\langle u_1, \ldots, u_t\rangle$ run over all t-tuples of integers from the set $\{1, \ldots, r/d\}$ such that $(u_1, \ldots, u_t, r/d) = 1$. Then $\langle u_1 d, \ldots, u_t d\rangle$ runs over $T(r)$.

PROOF. Clearly, every element of $T(r)$ has the stated form, and all such t-tuples are in $T(r)$. It remains only to show that the t-tuples formed in this way are distinct. Let $d, d' \in D(r)$ and $(u_1, \ldots, u_t, r/d) = 1 = (u_1', \ldots, u_t', r/d)$. If $u_i d = u_i' d'$ for $i = 1, \ldots, t$, then $d = (u_1 d, \ldots, u_t d, r) = (u_1' d', \ldots, u_t' d', r) = d'$ and $u_i = u_i'$ for $i = 1, \ldots, t$.

PROPOSITION 3. $g(n_1, \ldots, n_t, r) = \sum_{d \in D(r)} c(n_1, \ldots, n_t, r/d)$.

PROOF. We have by Proposition 2,

$$g(n_1, \ldots, n_t, r) = \sum_{d \in D(r)} \sum_{(u_1, \ldots, u_t, r/d) = 1} e(n_1 u_1 + \ldots + n_t u_t, r/d) .$$

Following Cohen [6] we shall denote $c(n_1, \ldots, n_t, r)$ by $c^{(t)}(n, r)$ when $n_1 = \ldots = n_t = n$.

EXAMPLE 1. Let $N(n_1, \ldots, n_t, r, s)$ be the number of solutions of (1) with $(x_{1j}, \ldots, x_{tj}, r) = 1$ for $j = 1, \ldots, s$. Then,

$$N(n_1, \ldots, n_t, r, s) = \frac{1}{r^t} \sum_{d \mid r} c^{(t)}(r/d, r)^s c(n_1, \ldots, n_t, d) .$$

This result is due to Cohen [6, Theorem 8]: in [6] Cohen confined himself to the case $t = 2$, but his methods and results extend immediately to the case of and arbitrary number of congruences. The number $N(n, r, s)$ was evaluated by Ramanathan [8], Cohen [3], and others.

EXAMPLE 2. For $j = 1, \ldots, s$ let $D_j(r)$ be the set of all divisors of r which are k-free. If $Q_k(n_1, \ldots, n_t, r, s)$ is the number of solution of (1) with $(x_{1j}, \ldots, x_{tj}, r)_k = 1$, where $(x_{1j}, \ldots, x_{tj}, r)_k$ is the largest k-th power common divisor of $x_{1j}, \ldots, x_{tj}$, and r, then

$$Q_k(n_1, \ldots, n_t, r, s) = \frac{1}{r^t} \sum_{d|r} G_k(r/d, r)^s c(n_1, \ldots, n_t, d) ,$$

where

$$G_k(n, r) = \sum_{\substack{d|r \\ (d,r)_k = 1}} c^{(t)}(n, r/d) .$$

We have $N(n_1, \ldots, n_t, r, s) = Q_1(n_1, \ldots, n_t, r, s)$. The number $Q_k(n, r^k, s)$ was evaluated by Cohen [4, Theorem 12] and expressed in terms of the extended Ramanujan sum which he introduced in [1].

EXAMPLE 3. Let k and q be integers such that $k \geqslant 2$ and $0 < q < k$. Let $S_{k,q}$ be the set of all integers n such that if p^h is the highest power of a prime p dividing n, then $h \equiv 0, 1, \ldots,$ or $q-1 \pmod k$. For $j = 1, \ldots, s$ let $D_j(r)$ be the set of all divisors of r contained in $S_{k,q}$, and let $P_{k,q}(n_1, \ldots, n_t, r, s)$ be the number of solutions of (1) with $(x_{1j}, \ldots, x_{tj}, r) \in S_{k,q}$ for $j = 1, \ldots, s$. Then

$$P_{k,q}(n_1, \ldots, n_t, r, s) = \frac{1}{r^t} \sum_{d|r} H_{k,q}(r/d, r)^s c(n_1, \ldots, n_t, d) .$$

where

$$H_{k,q}(n, r) = \sum_{\substack{d|r \\ d \in S_{k,q}}} c^{(t)}(n, r/d) .$$

When $t = 1$, this result is due to Subba Rao and Harris [9, Theorem 7]: Lemma 2 of [9] is a special case of our Theorem 1.

The next example involves unitary divisors of an integer, and the reader is referred to [5] and [7] for many details regarding unitary divisors and associated arithmetical functions.

A divisor d of r is called a unitary divisor if $(d, r/d) = 1$. We de-

note by $(x, r)_*$ the largest divisor of x which is a unitary divisor of r, and we set $(x_1, \ldots, x_t, r)_* = \big((x_1, \ldots, x_t), r\big)_*$. For each r let $D(r)$ be a set of unitary divisors of r, and

$$T(r) = \{\langle x_1, \ldots, x_t\rangle : 1 \leqslant x_i \leqslant r \text{ for } i = 1, \ldots, t \text{ and } (x_1, \ldots, x_t, r)_* \in D(r)\}.$$

It turns out that the corresponding function $g(n_1, \ldots, n_t, r)$ is, in this case also, a totally even function (mod r).

Set

$$c^*(n_1, \ldots, n_t, r) = \sum_{(y_1, \ldots, y_t, r)_* = 1} e(n_1 y_1 + \ldots + n_t y_t, r)\,,$$

this is the unitary analogue of the function $c(n_1, \ldots, n_t, r)$. When $t = 1$ it is the unitary analogue of the Ramanujan sum introduced by Cohen in [5]. Let $\gamma(r)$ be the core of r, i.e., $\gamma(1) = 1$, and if $r > 1$ then $\gamma(r)$ is the product of the distinct primes which divide r. Let d run over the divisors of r such that $\gamma(d) = \gamma(r)$, and for each d let $\langle y_1, \ldots, y_t\rangle$ run over the t-tuples of integers from the set $\{1, \ldots, d\}$ such that $(y_1, \ldots, y_t, d) = 1$. Then, $\langle y_1 r/d, \ldots, y_t r/d\rangle$ runs over the t-tuples $\langle x_1, \ldots, x_t\rangle$ of integers from the set $\{1, \ldots, r\}$ such that $(x_1, \ldots, x_t, r)_* = 1$. From this it follows that

$$c^*(n_1, \ldots, n_t, r) = \sum_{\substack{d \mid r \\ \gamma(d) = \gamma(r)}} c(n_1, \ldots, n_t, d)\,.$$

Therefore, $c^*(n_1, \ldots, n_t, r)$ is a totally even function (mod r). If we denote $c^*(n_1, \ldots, n_t, r)$ by $c^{*(t)}(n, r)$ when $n_1 = \ldots = n_t = n$, then

$$c^{*(t)}(n, r) = \sum_{\substack{d \mid r \\ \gamma(d) = \gamma(r)}} c^{(t)}(n, r)\,.$$

Proposition 4. Let d run over the divisors of r in $D(r)$, and for each d let $\langle u_1, \ldots, u_t\rangle$ run over all t-tuples of integers from the set $\{1, \ldots, r/d\}$ such that $(u_1, \ldots, u_t, r/d)_* = 1$. Then $\langle u_1 d, \ldots, u_t d\rangle$ runs over $T(r)$.

The proof of this proposition is similar to that of Proposition 2. From it we obtain the following result from which we conclude that $g(n_1, \ldots, n_t, r)$ is, indeed, a totally even function (mod r).

PROPOSITION 5. With $D(r)$ and $T(r)$ as in the preceeding discussion

$$g(n_1, \ldots, n_t, r) = \sum_{d \in D(r)} c^*(n_1, \ldots, n_t, r/d) .$$

EXAMPLE 4. If $N^*(n_1, \ldots, n_t, r, s)$ is the number of solutions of (1) with $(x_{1j}, \ldots, x_{tj}, r)_* = 1$ for $j = 1, \ldots, s$ then

$$N^*(n_1, \ldots, n_t, r, s) = \frac{1}{r^t} \sum_{d|r} c^{*(t)}(r/d, r)^s c(n_1, \ldots, n_t, d) .$$

When $t = 1$, this number was evaluated by Cohen [7, Theorem 6.1]: his formula is different in form from ours, and each can be obtained from the other by using the relation between $c^*(n, r)$ and $c(n, r)$ [7, Theorem 3.1].

In our examples the restrictions are the same for all values of j. Of course, they could be chosen differently for different values of j: for example, we could obtain immediately a generalization of [7, Theorem 6.3].

Next we go in another direction and obtain a very general result of the type obtained by Sugunamma in [10]. For $i = 1, \ldots, s$, let t_i be a positive integer and for each r let $T_i(r)$ be a nonempty set of t_i-tuples of integers from the set $\{1, \ldots, r\}$. Further, let $g_i(n_1, \ldots, n_{t_i}, r)$ be defined as before. Let $L(n, r, t_1, \ldots, t_s)$ be the number of solutions of

$$n \equiv \sum_{j=1}^{t_1} x_{1j} + \ldots + \sum_{j=1}^{t_s} x_{sj} \pmod r \tag{2}$$

with $\langle x_{i1}, \ldots, x_{it_i} \rangle \in T_i(r)$ for $i = 1, \ldots, s$.

THEOREM 2. If $g_i(n_1, \ldots, n_{t_i}, r)$ is a totally even function (mod r) for $i = 1, \ldots, s$ then

$$L(n, r, t_1, \ldots, t_s) = \frac{1}{r} \sum_{d|r} \left\{ \prod_{i=1}^{s} g_i(r/d, r) \right\} c(n, d) ,$$

where $g_i(n, r) = g_i(n, \ldots, n, r)$.

PROOF. Let $L = L(n, r, t_1, \ldots, t_s)$. Then

$$L = \sum{}' \prod_{i=1}^{s} h_i(x_{i1}, \ldots, x_{it_i}) ,$$

where $\sum'$ is summation over all solutions of (2), and

$$h_i(x_{i1}, \ldots, x_{it_i}) = \frac{1}{r^{t_i}} \sum^{(i)} \prod_{j=1}^{t_i} \sum_{q_{ij}=1}^{r} e\big((x_{ij} - y_{ij})q_{ij}, r\big)\big),$$

where $\sum^{(i)}$ is summation over all $\langle y_{i1}, \ldots, y_{it_i}\rangle \in T_i(r)$. Let $t = t_1 + \ldots + t_s$. Then

$$L = \frac{1}{r^t} \sum' \prod_{i=1}^{s} \sum^{(i)} \prod_{j=1}^{t_i} \sum_{q_{ij}=1}^{r} e\big((x_{ij} - y_{ij})q_{ij}, r\big)$$

$$= \frac{1}{r^t} \sum'' \sum' \prod_{i=1}^{s} \sum^{(i)} \prod_{j=1}^{t_i} e(x_{ij}q_{ij}, r)e(-y_{ij}q_{ij}, r),$$

where $\sum''$ is summation over all t-tuples of integers from the set $\{1, \ldots, r\}$ Thus,

$$L = \frac{1}{r^t} \sum'' \sum' \prod_{i=1}^{s} \Big\{ g_i(q_{i1}, \ldots, q_{it_i}, r) \prod_{j=1}^{t_i} e(x_{ij}x_{ij}q_{ij}, r) \Big\}$$

$$= \frac{1}{r^t} \sum'' \Big\{ \prod_{i=1}^{s} g_i(q_{i1}, \ldots, q_{it_i}, r) \Big\} \sum' \prod_{i=1}^{s} \prod_{j=1}^{t_i} e(x_{ij}q_{ij}, r).$$

By [2, Lemma 3] the summation on the right is equal to $r^{t-1}e(nq, r)$ if $q_{ij} = q$ for all i and j, and is equal to zero otherwise. Hence,

$$L = \frac{1}{r} \sum_{q=1}^{r} \Big\{ \prod_{i=1}^{s} g_i(q, r) \Big\} e(nq, r).$$

If we proceed as in the final steps of the proof of Theorem 1 we will obtain the formula of Theorem 2.

EXAMPLE 5. If $N'(n, r, t_1, \ldots, t_s)$ is the number of solutions of (2) with $(x_{i1}, \ldots, x_{it_i}, r) = 1$ for $i = 1, \ldots, s$, then

$$N'(n, r, t_1, \ldots, t_s) = \frac{1}{r} \sum_{d|r} \Big\{ \prod_{i=1}^{s} c^{(t_i)}(r/d, r) \Big\} c(n, d).$$

EXAMPLE 6. If $Q_k'(n, r, t_1, \ldots, t_s)$ is the number of solutions of (2) with $(x_{i1}, \ldots, x_{it_i}, r)_k = 1$ for $i = 1, \ldots, s$, then

$$Q_k'(n, r, t_1, \ldots, t_s) = \frac{1}{r} \sum_{d|r} \left\{ \prod_{i=1}^{s} G_i^{(t_i)}(r/d, r) \right\} c(n, d) ,$$

where

$$G_i^{(t_i)}(n, r) = \sum_{\substack{d|r \\ (d,r)_k = 1}} c^{(t_i)}(n, r/d) .$$

Sugunamma evaluated $Q_k'(n, r^k, t, \ldots, t)$ [10, Theorem 5]: his formula is in terms of the extended Ramanujan sum $c_k(n, r)$.

Of course, there is a unitary analogue of Example 5. Also, we can mix the restrictions, and we shall give one example of a result of this kind.

EXAMPLE 7. Let $R(n, r, s, t)$ be the number of solutions of

$$n \equiv x_1 + \ldots + x_s + y_1 + \ldots + y_t \pmod{r}$$

with $(x_1, \ldots, x_s, r)_* = 1$ and $(y_1, \ldots, y_t, r) = 1$. Then

$$R(n, r, s, t) = \frac{1}{r} \sum_{d|r} c^{*(s)}(r/d, r) c^{(t)}(r/d, r) c(n, d) .$$

Finally, it is clear that by the same kind of arguments we could give a single result which contains both Theorem 1 and Theorem 2. In the light of these theorems, it is easy to predict what the formula in such a result would be.

BIBLIOGRAPHY

[1] E. COHEN, *An extension of Ramanujan's sum*, Duke Math. J., **16** (1949), pp. 85-90.

[2] E. COHEN, *Rings of arithmetic functions*, Duke Math. J., **19** (1952), pp. 115-129.

[3] E. COHEN, *A class of arithmetical functions*, Proc. Nat. Acad. Sci. U.S.A., **41** (1955), pp. 939-944.

[4] E. COHEN, *An extension of Ramanujan's sum, III, Connection with totient functions*, Duke Math. J., **23** (1956), pp. 623-630.

[5] E. COHEN, *Arithmetical functions associated with the unitary divisors of an integer*, Math. Zeit., **74** (1960), pp. 66-80.

[6] E. COHEN, *A class of arithmetical functions in several variables with applications to congruences*, Trans. Amer. Math. Soc., **96** (1960), pp. 355-381.

[7] E. COHEN, *Unitary functions* (mod r), *I*, Duke Math. J., **28** (1961), pp. 475-486.

[8] K. G. RAMANATHAN, *Some applications of Ramanujan's trigonometric sum* $C_m(n)$, Proc. Indian Acad. Sci. (A) **20** (1944), pp. 62-69.

[9] M. V. SUBBA RAO - V. C. HARRIS, *A new generalization of Ramanujan's sum*, J. London Math. Soc., **41** (1966), pp. 595-604.

[10] M. SUGUNAMMA, *Eckford Cohen's generalizations of Ramanujan's trigonometrical sum* $C(n, r)$, Duke Math. J., **27** (1960), pp. 323-330.

Manoscritto pervenuto in redazione l'8 agosto 1974.