Czechoslovak Mathematical Journal, 74 (149) (2024), 1185–1206

LINEAR CONGRUENCES AND A CONJECTURE OF BIBAK

Chinnakonda Gnanamoorthy Karthick Babu, Ranjan Bera,
Balasubramanian Sury, Bangalore

Received April 20, 2024. Published online November 18, 2024.

Abstract. We address three questions posed by K. Bibak (2020), and generalize some results of K. Bibak, D. N. Lehmer and K. G. Ramanathan on solutions of linear congruences $\sum_{i=1}^{k} a_i x_i \equiv b \pmod{n}$. In particular, we obtain explicit expressions for the number of solutions, where x_i's are squares modulo n. In addition, we obtain expressions for the number of solutions with order restrictions $x_1 \geqslant \ldots \geqslant x_k$ or with strict order restrictions $x_1 > \ldots > x_k$ in some special cases. In these results, the expressions for the number of solutions involve Ramanujan sums and are obtained using their properties.

Keywords: system of congruence; restricted linear congruence; Ramanujan sum; discrete Fourier transform

MSC 2020: 11D79, 11P83, 11A25, 11T55, 11T24

1. Introduction and statements of main results

Let $a_1, \ldots, a_k, b$ be integers and n be a positive integer. A linear congruence in k unknowns $x_1, \ldots, x_k$ is a congruence of the form

$$a_1 x_1 + \ldots + a_k x_k \equiv b \pmod{n}. \tag{1.1}$$

More than a century ago, Lehmer in [19] proved that a linear congruence represented by (1.1) has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ if and only if $l \mid b$, where $l = (a_1, \ldots, a_k, n)$. Here and henceforth the notation $(u_1, \ldots, u_k)$ denotes the GCD of integers $u_1, \ldots, u_k$. Further, if this condition is satisfied, then there are ln^{k-1} solutions. Over the years, solutions of the linear congruence (1.1), which are subject to different types of restrictions such as GCD restrictions $(x_i, n) = t_i$ $(1 \leqslant i \leqslant k)$ for prescribed divisors $t_1, \ldots, t_k$ of n, have been extensively investigated.

DOI: 10.21136/CMJ.2024.0151-24

In a different direction, order-restricted solutions $x_1 \geqslant \ldots \geqslant x_k$ of the linear congruence represented by (1.1) seem to have been studied for cryptographic applications. In 1962, Riordan in [27] derived an explicit formula for order-restricted solutions when $a_i = 1$ for all i, $b = 0$ and $n = k$. More recently, Bibak in [1] extended Riordan's result; specifically to the case, where $a_i = 1$ for all i as before, but allowing arbitrary integers k and b. The vast literature (see [5], [8], [11], [24], [25]) on these topics bears witness to their applicability in diverse fields such as cryptography, coding theory, combinatorics, and computer science. For a comprehensive overview of these applications and further insights, one can refer to [2], [3], [5], [6], [18].

In this paper, we answer some questions posed by Bibak, and generalize some results of Bibak, Lehmer and Ramanathan (see Theorems 1.1, 1.3, 1.4 and Corollary 1.2). The expressions naturally involve Ramanujan sums.

In the last section of [1], Bibak posed the following three interesting problems. The first one asks for solutions x_i that are squares modulo n for (1.1). We solve this problem (see Theorems 1.1). We say that $(x_1, \ldots, x_k)$ is a square solution of (1.1) if x_i's are squares modulo n, for $1 \leqslant i \leqslant k$. Thus, we are looking at the set

$$\Big\{(x_1, \ldots, x_k) \in \mathbb{Z}_n^k \colon \sum_{i=1}^{k} a_i x_i \equiv b \pmod{n},\ x_i = y_i^2,\ y_i \in \mathbb{Z}_n\Big\}.$$

We point out that square solutions cannot simply be counted by enumerating the set

$$\Big\{(y_1, \ldots, y_k) \in \mathbb{Z}_n^k \colon \sum_{i=1}^{k} a_i y_i^2 \equiv b \pmod{n}\Big\}.$$

Subtleties about square solutions are explained in Section 2. A second problem posed by Bibak is to study the general case of strictly ordered solutions $x_1 > \ldots > x_k$ of (1.1) for which a special case is addressed by us in Theorem 1.3 stated below. Another problem asks for an explicit formula for the number of order-restricted solutions $x_1 \geqslant \ldots \geqslant x_k$. Theorem 1.4 below can be considered a partial answer towards that, and is a mild generalization of Bibak's result.

Theorem 1.1. *Let $S_n(b; a_1, \ldots, a_k)$ denote the number of square solutions of (1.1). Assume n is an odd positive integer, having a prime factorization $n = p_1^{l_1} \ldots p_r^{l_r}$. Then we have*

$$S_n(b; a_1, \ldots, a_k) = \frac{1}{n} \prod_{q=1}^{r} \Big(\sum_{m=1}^{p^{l_q}} e\Big(\frac{-bm}{p^{l_q}}\Big) + \sum_{\substack{K \subset \{1,\ldots,k\} \\ K \neq \phi}} \frac{1}{2^{|K|}} S_K \Big),$$

where

$$S_K = \sum_{m=1}^{p^{l_q}} e\Big(\frac{-bm}{p^{l_q}}\Big) \prod_{i\in K}\Big(\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l_q-1} \Big(C_{p^{l_q-j_i}}(a_i m) + \varepsilon_p\Big(\frac{a_i m/p^{l_q-j_i-1}}{p}\Big) \times \varrho_{j_i}(a_i m) p^{l_q-j_i-1/2}\Big)\Big), \tag{1.2}$$

$$\varrho_{j_i}(x) = \begin{cases} 1 & \text{if } (x, p^{l_q-j_i}) = p^{l_q-j_i-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

Here $C_n(b)$ denotes the Ramanujan sum as before, and the other notations appearing are $\big(\frac{\cdot}{p}\big)$, the Legendre symbol modulo p, $e(x) = \mathrm{e}^{2\mathrm{i}\pi x}$ and ε_n is the sign of the Gauss sum given by

$$\varepsilon_n = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4, \\ i & \text{if } n \equiv 3 \pmod 4. \end{cases} \tag{1.4}$$

In the special case when $n = p^l$, $(a_i, n) = 1 = (b, n)$ for all i we have the following simplified expression for S_K's in $S_n(b; a_1, \dots, a_k)$:

Corollary 1.2. *We have*

$$S_K = \Big(\sum_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{l-1} \phi(p^{l-j}) \Big)^{|K|} + \sum_{m=1}^{p-1} e\Big(\frac{-bm}{p}\Big) \Big(-p^{l-1} + \sum_{\substack{j=2\\ j\equiv 0 \pmod 2}}^{l-1} \phi(p^{l-j}) + \varepsilon_p\Big(\frac{m}{p}\Big) p^{l-1/2} \Big)^{|K|}.$$

Moreover, when $n = p^2$, $k = 2$, and $(a_i, p) = 1$, Theorem 1.1 reduces to the following formula for any $b \in \mathbb{Z}_{p^2}$:

$$S_{p^2}(b; a_1, a_2) = \begin{cases} \frac{1}{4}p(p-5)+2 & \text{if } p \equiv 1 \pmod 4,\ p \nmid b \text{ and } (\frac{b}{p}) = 1, \\ \frac{1}{4}(p(p-1)) & \text{if } p \equiv 1 \pmod 4,\ p \nmid b \text{ and } (\frac{b}{p}) = -1, \\ \frac{1}{2}p(p-1) & \text{if } p \equiv 1 \pmod 4 \text{ and } p \parallel b, \\ \frac{1}{2}p(p-1)+1 & \text{if } p \equiv 1 \pmod 4 \text{ and } p^2 \mid b, \\ \frac{1}{4}p(p+1) & \text{if } p \equiv -1 \pmod 4,\ p \nmid b \text{ and } (\frac{b}{p}) = -1, \\ \frac{1}{4}p(p-3)+2 & \text{if } p \equiv -1 \pmod 4,\ p \nmid b \text{ and } (\frac{b}{p}) = 1, \\ 0 & \text{if } p \equiv -1 \pmod 4 \text{ and } p \parallel b, \\ 1 & \text{if } p \equiv -1 \pmod 4 \text{ and } p^2 \mid b. \end{cases}$$

Note that if $k = 2$, $a_1 = a_2 = 1$, $b = 2$, $p = 3$, $n = p^2$, the corollary above gives the value $\frac{1}{4}p(p+1) = 3$, which counts all the square solutions

$$\{(1,1),(4,7),(7,4)\}$$

of $x_1 + x_2 \equiv 2 \pmod 9$.

For the number $N_n(k,a,b)$ of solutions $x_1 > x_2 > \ldots > x_k$ of $ax_1 + ax_2 + \ldots + ax_k \equiv b \pmod n$, we obtain the following expression. More precisely, we prove:

Theorem 1.3. *Let n be a positive integer and $b \in \mathbb{Z}_n$. Then for any given integer a with $f = (a,n)$ and $f \mid b$ we have*

$$N_n(k,a,b) = \frac{(-1)^k f}{n} \sum_{d \mid (n/f,k)} (-1)^{k/d} \binom{n/d}{k/d} C_d(b).$$

The special case when $a = 1$ is due to Ramanathan, see [26], Theorem 4. Of course, in the special case $(a,n) = 1$, Theorem 1.3 reduces to Ramanathan's theorem with $a^{-1}b$ in place of b, using a basic property of Ramanujan sums. Another special case of Theorem 1.3 partially answers another question (see [4], Problem) posed by Bibak, Kapron and Srinivasan; this is described at the end of this section.

Surprisingly, Bibak does not seem to be aware of Ramanathan's result. We also became aware of it only after we proved Theorem 1.3 and found that the specific case where $a_i = 1$ for all i had already been handled in this almost 80-year old paper.

The general case of order-restricted solutions $x_1 \geqslant \ldots \geqslant x_k$ of (1.1) posed by Bibak is still open, but we obtain the following partial result. Let $k = k_1 + k_2 + \ldots + k_t$ be a partition of k, and we consider (1.1), where

$$(1.5)\quad a_1 = a_2 = \ldots = a_{k_1},\ a_{k_1+1} = \ldots = a_{k_1+k_2}, \ldots a_{k_1+\ldots+k_{t-1}+1} = \ldots = a_{k_1+\ldots+k_t}$$

modulo n. Let $M_n(k_1,\ldots,k_t,a_1,\ldots,a_t,b)$ be the number of solutions of the congruence

$$\sum_{i=1}^{k} a_i x_i \equiv b \pmod n$$

satisfying $x_1 \geqslant x_2 \geqslant \ldots \geqslant x_{k_1}$, $x_{k_1+1} \geqslant \ldots \geqslant x_{k_1+k_2}$, …, $x_{k_1+\ldots+k_{t-1}+1} \geqslant \ldots \geqslant x_{k_1+\ldots+k_t}$. We prove:

Theorem 1.4. *Let $k = k_1 + \ldots + k_t$ and $a_1, \ldots, a_k$ be integers modulo n, as above. Then*

$$\begin{aligned} M_n(k_1, \ldots, k_t, a_1, \ldots, a_t, b) \\ &= \frac{1}{n} \sum_{d_1 \mid n} \cdots \sum_{d_t \mid n} \frac{d_1}{d_1 + k_1 d_1/n} \cdots \frac{d_t}{d_t + k_t d_t/n} \\ &\quad \times \binom{d_1 + k_1 d_1/n}{k_1 d_1/n} \cdots \binom{d_t + k_t d_t/n}{k_t d_t/n} \sum_{\substack{m=1 \\ (a_i m, n) = d_i \\ i=1,\ldots,t}}^{n} e\Big(\frac{-bm}{n}\Big). \end{aligned}$$

Suppose that $(a_i, n) = f$ for all i. Then we have

$$\begin{aligned} M_n(k_1, \ldots, k_t, a_1, \ldots, a_t, b) \\ &= \frac{f}{n} \sum_{d \mid (n/f, k_1, \ldots, k_t)} \frac{n^t}{(n+k_1)\ldots(n+k_t)} \binom{n + k_1/d}{k_1/d} \cdots \binom{n + k_t/d}{k_t/d} C_d(b), \end{aligned}$$

where $C_d(b)$ denotes the Ramanujan sum.

Here, some of the a_i's ($i \leqslant t$) may be equal; note, for instance, that if $a_1 = a_2$, the solutions counted by the theorem correspond to separate orderings $x_1 \geqslant \ldots \geqslant x_{k_1}$ and $x_{k_1+1} \geqslant \ldots \geqslant x_{k_1+k_2}$. The special case of the first statement when $t = 1$ and $a_i = 1$ for all i, is due to Bibak, see [1]. Moreover, when $k_1 = \ldots = k_t = 1$, the formula for $M_n(1, \ldots, 1, a_1, \ldots, a_k, b)$ simplifies to $f n^{k-1}$, which aligns with Lehmer's theorem (see [19]), as it accounts for all possible solutions of (1.1) when $a_1, \ldots, a_k$ are distinct.

Theorem 1.3 can be interpreted as a subset sum problem in the abelian group $\mathbb{Z}_n$. More generally, let A be any abelian group and let D be a finite subset of A containing n elements. For a positive integer $1 \leqslant k \leqslant n$ and an element $b \in A$, let $N_D(k, b)$ denote the number of k-element subsets $S \subseteq D$ such that $\sum_{a \in S} a = b$. In particular, when A is a finite cyclic group $\mathbb{Z}_n$, the formula for $N_D(k, b)$ is the same as the formula for $N_n(k, 1, b)$ discussed earlier. In fact, for any finite abelian group A, Li and Wan in [21] obtained an explicit formula for $N_D(k, b)$ when $D = A$. Also, an analogous problem has been investigated in the context of the finite field $\mathbb{F}_q$ of characteristic p, see [20].

The decision version of the subset sum problem over D is to determine $N_D(k, b) > 0$ for some $1 \leqslant k \leqslant n$. This problem has significant applications in coding theory and cryptography. It is a well-known NP-complete problem even when A is cyclic (finite or infinite) or the additive group of a finite field $\mathbb{F}_q$. In particular, when $A = \mathbb{Z}$, the subset sum problem forms the basis of the knapsack cryptosystem. The case $A = \mathbb{F}_q$ is related to the deep hole problem of extended Reed-Solomon codes, see [10].

1.1. Distinct solutions and Schönemann's theorem. Another interesting problem related to the linear congruences that has been considered in the literature is counting distinct solutions. This problem was first addressed in a special case by Schönemann (see [28]) almost two centuries ago. Let $D_n(b; a_1, \ldots, a_k)$ denote the number of solutions of the linear congruence $a_1x_1 + \ldots + a_kx_k \equiv b \pmod{n}$, with all x_i distinct. Schönemann in [28] proved the following result.

Theorem (Schönemann (1839))**.** *Let p be a prime, $a_1, \ldots, a_k$ be arbitrary integers, and $\sum_{i=1}^{k} a_i \equiv 0 \pmod{p}$ and $\sum_{i\in I} a_i \not\equiv 0 \pmod{p}$ for all $\phi \neq I \subsetneq \{1, \ldots, k\}$. Then the number $D_p(k, 0)$ is independent of the coefficients $a_1, \ldots, a_k$ and is equal to*

$$D_p(0; a_1, \ldots, a_k) = (-1)^{k-1}(k-1)!\,(p-1) + (p-1)\ldots(p-k+1).$$

Recently, in 2013, Grynkiewicz et al. in [14] in obtained the necessary and sufficient condition to determine $D_n(b; a_1, \ldots, a_k) > 0$. In 2019, Bibak et al. in [4] generalized Schönemann's theorem using a graph theoretic method. They proved the following result:

Theorem 1.5 ([4], Theorem 2.3)**.** *Let $a_1, \ldots, a_k, b$ be arbitrary integers and n be a positive integer, and $\left(\sum_{i\in I} a_i, n\right) = 1$ for all $\phi \neq I \subsetneq \{1, \ldots, k\}$. Then we have*

$$D_n(b; a_1, \ldots, a_k) = \begin{cases} (-1)^k(k-1)! + (n-1)\ldots(n-k+1) & \text{if } \left(\sum_{i=1}^{k} a_i, n\right) \nmid b, \\ (-1)^{k-1}(k-1)!\left(\left(\sum_{i=1}^{k} a_i, n\right) - 1\right) + (n-1)\ldots(n-k+1) & \text{if } \left(\sum_{i=1}^{k} a_i, n\right) \mid b. \end{cases}$$

Furthermore, they also asked for an explicit formula for $D_n(b; a_1, \ldots, a_k)$ without restricting the gcd of the a_i's and n, see [4], Problem 1. When $a_1 = \ldots = a_k = a$, the problem of counting solutions of strict order-restricted linear congruence is equivalent to counting the distinct solutions of the linear congruence up to permutations. As a consequence of Theorem 1.3, we have the following corollary:

Corollary 1.6. *Let n be a positive integer and $b \in \mathbb{Z}_n$. Then for any given integer a with $f = (a, n)$ and $f \mid b$, we have*

$$D_n(a, b) = D_n(b; a, \ldots, a) = \frac{k!f(-1)^k}{n} \sum_{d\mid(n/f,k)} (-1)^{k/d} \binom{n/d}{k/d} C_d(b), \tag{1.6}$$

where $C_d(b)$ denotes the Ramanujan sum.

Since all the coefficients are a, the gcd conditions mentioned in Theorem 1.5 are the same as the conditions $(a \cdot i, n) = 1$ for all $1 \leqslant i \leqslant k-1$. Thus, assuming these conditions on n implies that $f = (a, n) = 1$ and either $(k, n) = 1$ or k is the smallest prime divisor of n. Suppose k is the smallest prime divisor of n. Then by (1.6), we have

$$\begin{aligned} D_n(a,b) &= \frac{k!\,(-1)^k}{n}\left((-1)^k\binom{n}{k}C_1(b) - \binom{n/k}{1}C_k(b)\right), \\ &= \begin{cases} (-1)^k(k-1)! + (n-1)\dots(n-k+1) & \text{if } k \nmid b, \\ (-1)^{k-1}(k-1)!\,(k-1) + (n-1)\dots(n-k+1) & \text{if } k \mid b. \end{cases} \end{aligned}$$

Suppose $(k, n) = 1$. Then from (1.6) it follows that

$$D_n(b) = (n-1)\dots(n-k+1).$$

Therefore, the obtained formula (1.6) provides a proof of Theorem 1.5 in the special case when all coefficients $a_1 = \ldots = a_k = a$. Moreover, this formula also addresses the problem posed in [4] for the specific case where $a_1, \ldots, a_k$ are all equal to a.

2. Square solutions—some subtleties

We say that $(x_1, \ldots, x_k)$ is a square solution of (1.1) if x_i's are squares modulo n for $1 \leqslant i \leqslant k$. Given integers $a_1, \ldots, a_k, b$ and a positive integer n, it is an interesting problem to determine the necessary and sufficient conditions that guarantee the existence of a square solution to the congruence represented by (1.1). Thus, we are looking at the set

$$\left\{(x_1, \ldots, x_k) \in \mathbb{Z}_n^k \colon \sum_{i=1}^{k} a_i x_i \equiv b \pmod{n},\ x_i = y_i^2,\ y_i \in \mathbb{Z}_n\right\}.$$

We point out that square solutions cannot simply be counted by enumerating the set

$$\left\{(y_1, \ldots, y_k) \in \mathbb{Z}_n^k \colon \sum_{i=1}^{k} a_i y_i^2 \equiv b \pmod{n}\right\}.$$

For instance, if we consider the congruence $x_1 + x_2 \equiv 1 \pmod{27}$, there are four square solutions

$$\{(1,0), (0,1), (9,19), (19,9)\},$$

whereas in the latter set

$$\{(y_1, y_2) \colon y_1^2 + y_2^2 \equiv 1 \pmod{27}\},$$

6 elements correspond to $(1,0)$ and 12 elements correspond to $(9,19)$. Indeed, the six solutions $(1,0), (1,9), (1,18), (26,0), (26,9), (26,18)$ of $\{(y_1, y_2) \colon y_1^2 + y_2^2 \equiv 1 \pmod{27}\}$ correspond to the single solution $(1,0)$ of $\{x_1 + x_2 \equiv 1 \pmod{27} \colon x_1, x_2$

squares}. Similarly,

$$(3,10),(6,10),(12,10),(3,17),(6,17),(12,17),$$
$$(24,10),(21,10),(15,10),(24,17),(21,17),(15,17)$$

are the twelve solutions of $\{(y_1,y_2)\colon\ y_1^2+y_2^2\equiv 1 \pmod{27}\}$ corresponding to the single solution $(9,19)$. Thus, the complexity of this problem can vary significantly, depending on the specific values of a_i, b, and n. However, a necessary condition for the latter set to be nonempty also gives a necessary condition for a square solution to exist. One can easily see that when $n=p^l$, if $(b,p)=1$ and there exists a subset S of $\{a_1,\dots,a_k\}$ such that

$$s=\sum_{a_i\in S} a_i\in\mathbb{Z}_{p^l}^* \quad\text{and}\quad \Big(\frac{s}{p}\Big)=\Big(\frac{b}{p}\Big),$$

then (1.1) has a square solution $(x_1,\dots,x_k)$, namely

$$x_i=\begin{cases} s^{-1}b & \text{if } a_i\in S,\\ 0 & \text{otherwise.}\end{cases}$$

But then, due to Lemma 4.3, the above observation holds for any odd positive n. A related problem explored in the literature is the counting of representations of an integer b as a sum of squares modulo n, where b is any given integer. More generally, for given integers $a_1,\dots,a_k,b$ and positive integers $t_1,\dots,t_k$ and n counting the number of solutions of the congruence

$$a_1x_1^{t_1}+\ldots+a_kx_k^{t_k}\equiv b \pmod{n} \tag{2.1}$$

has also been studied in the literature; for example (see [9], [13], [16], [22], [30] and Section 8.6 of [17]). When n is an odd prime, t is any positive integer and $t_1=\ldots=t_k=t$, the solutions of (2.1) were first studied by Lebesgue in 1837, see [12], Chapter X. In 1932, Hull in [16] proved a formula for counting the solutions to (2.1) when t is any positive integer such that $t_1=\ldots=t_k=t$ and $a_1=\ldots=a_k=1$. Recently, Tóth in [30] investigated the solutions of (2.1) under various conditions on the a_i's, depending on the modulus n when $t_1=\ldots=t_k=2$. More recently, Li and Ouyang in [22] have provided an algorithm for computing the number of solutions of (2.1) under the additional restriction that x_i is a unit for every $i\in J\subseteq\{1,\dots,k\}$.

Along with the other results, Hull in Theorem 23 of [16] discussed a sufficient condition on k in order to (2.1) has a solution when $t\geqslant 2$ is a fixed integer, $t_1=\ldots=t_k=t$ and $a_1=\ldots=a_k=1$. Specifically for the case when $t=2$ and $n=p^l$, where p is an odd prime, the provided sufficient condition is as follows:

(1) If $(b,p)=1$, then there is a solution whenever $k\geqslant 2$.
(2) If $p\mid b$, then there is a solution whenever $k\geqslant 3$.

Notice that this sufficient condition also guarantees the existence of a square solution to the congruence represented by (1.1). This is because $x_1^2 + \ldots + x_k^2 \equiv b \pmod{n}$ is equivalent to $y_1 + \ldots + y_n \equiv b \pmod{n}$, where $y_i \equiv x_i^2 \pmod{n}$. As a result, (1.1) has a square solution whenever $k \geqslant 3$ and $a_1 = \ldots = a_k = 1$.

Furthermore, in the case of $k = 1$, the congruence (1.1) has a square solution if and only if b is a square. Also, for $k = 2$, there exist linear congruences with $a_1 = a_2 = 1$ and $(b, n) > 1$ that do not have square solutions. For example, consider the congruence $x_1 + x_2 \equiv 3 \pmod{9}$, which lacks square solutions as the squares modulo 9 are $0, 1, 4, 7$.

Unlike the case of existence, the question of counting the number of square solutions for (1.1) is not equivalent to the question of counting the number of representations as a sum of squares. This happens because the number of solutions to all solvable congruences of the form $x^2 \equiv a \pmod{n}$ may not be the same for every integer a, although it is the same for every coprime a. As a result, determining the number of representations that correspond to the same square solution is rather difficult.

For example, consider the square solutions of the congruence $x_1 + x_2 \equiv 1 \pmod{27}$, which are given by $(1, 0), (0, 1), (19, 9), (9, 19)$. In this case, the number of representations corresponding to $(1, 0)$ is 6, while the number of representations corresponding to $(19, 9)$ is 12. This discrepancy arises because the congruence $x^2 \equiv 0 \pmod{27}$ has 3 solutions, and $x^2 \equiv 9 \pmod{27}$ has 6 solutions. Hence, our aim is to count the number of square solutions for (1.1). Let $S_n(b; a_1, \ldots, a_k)$ denote the number of square solutions of (1.1). Theorem 1.1 provides a formula for $S_n(b; a_1, \ldots, a_k)$. The proof of the theorem and its corollary stated in the introduction are given in Section 4.

3. Preliminaries

3.1. Discrete Fourier transform. An arithmetic function $f\colon \mathbb{Z} \to \mathbb{C}$ is said to be periodic with period n (or n-periodic) for some $n \in \mathbb{N}$ if for every $b \in \mathbb{Z}$, $f(b + n) = f(b)$. From definition (3.1), it is clear that $C_n(b)$ is a periodic function of b with period n. For an n-periodic arithmetic function f, its discrete (finite) Fourier transform (DFT) is defined to be the function

$$\hat{f}(b) = \sum_{j=1}^{n} f(j) e\Big(\frac{-bj}{n}\Big) \quad \text{for } b \in \mathbb{Z}.$$

A Fourier representation of f is given by

$$f(b) = \frac{1}{n} \sum_{j=1}^{n} \hat{f}(j) e\left(\frac{bj}{n}\right) \quad \text{for } b \in \mathbb{Z},$$

which is the inverse discrete Fourier transform.

3.2. Gauss sums and Ramanujan sums. Let n be a positive integer. A Dirichlet character χ modulo n is an arithmetic function $\chi\colon\ \mathbb{Z} \to \mathbb{C}$ with period n which is an extension of a group homomorphism from the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ to the set of complex numbers $\mathbb{C}$ via

$$\chi(m) = \begin{cases} \chi(m \pmod n) & \text{if } (m,n) = 1, \\ 0 & \text{if } (m,n) \geqslant 1. \end{cases}$$

Indeed, the extension of the trivial homomorphism χ_0 is known as the principal character modulo n. This particular Dirichlet character, denoted as χ_0, is defined as follows:

$$\chi_0(m) = \begin{cases} 1 & \text{if } (m,n) = 1, \\ 0 & \text{if } (m,n) \geqslant 1. \end{cases}$$

The conductor of a Dirichlet character χ modulo n is the smallest divisor of n for which χ is periodic. We say that a Dirichlet character χ modulo n is primitive if the conductor of χ is n. Otherwise, we say that χ is imprimitive.

For any Dirichlet character $\chi(m)$ to the modulus n, the Gauss sum $\tau(\chi)$ is defined by

$$\tau(\chi) = \sum_{m=1}^{n} \chi(m) e\Big(\frac{m}{n}\Big),$$

where $e(x)$ denote $\mathrm{e}^{2\pi \mathrm{i} x}$. Further, the more general Gauss sum is the discrete Fourier transform of a Dirichlet character χ modulo n, namely

$$\tau_b(\chi) = \widehat{\chi}(-b) = \sum_{m=1}^{n} \chi(m) e\Big(\frac{bm}{n}\Big) \quad \text{for } b \in \mathbb{Z}.$$

For a Dirichlet character χ modulo n induced by a primitive character $\chi^\star$ modulo $n^\star$, the following lemma reduces the computation of the general Gauss sum $\tau_b(\chi)$ to the Gauss sum $\tau(\chi^\star)$.

Lemma 3.1 ([23], Theorems 9.7 and 9.12)**.** *Let χ modulo n be a nonprincipal character induced by the primitive character $\chi^\star$ modulo $n^\star$. Put $r = n/(m, n^\star)$. If $n^\star \nmid r$, then $\tau_m(\chi) = 0$, while if $n^\star \mid r$, then*

$$\tau_m(\chi) = \bar{\chi}^\star\Big(\frac{m}{(n,m)}\Big)\mu(r/n^\star)\chi^\star\Big(\frac{r}{n^\star}\Big)\frac{\varphi(n)}{\varphi(r)}\tau(\chi^\star).$$

In particular,

$$\tau_m(\chi) = \bar{\chi}(m)\mu\Big(\frac{n}{n^\star}\Big)\chi^\star\Big(\frac{n}{n^\star}\Big)\tau(\chi^\star) \quad \text{if } (m,n) = 1.$$

Furthermore, we have

$$|\tau_m(\chi^\star)| = \sqrt{n^\star}.$$

Though, we know that $|\tau(\chi)| = \sqrt{n}$ holds for any primitive character χ modulo n, the determination of the argument of the $|\tau(\chi)|$ is a difficult problem. In the case of real primitive characters, $\tau(\chi)$ were evaluated completely by Gauss.

Lemma 3.2 (Gauss)**.** *Let $n \geqslant 1$ be an odd squarefree integer and let χ be a real primitive character modulo n. Then we have*

$$\tau(\chi) = \varepsilon_n \sqrt{n},$$

where ε_n is defined as in (1.4).

When χ_0 is the principal character modulo n, the general Gauss sum $\tau_b(\chi_0)$ is called the Ramanujan sum, i.e.,

$$\tau_b(\chi_0) = C_n(b) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\Big(\frac{jb}{n}\Big). \tag{3.1}$$

Now, we list some properties of the Ramanujan sums:

(i) $C_n(b)$ is integer-valued.

(ii) For fixed $b \in \mathbb{Z}$ the function $b \to C_n(b)$ is multiplicative, i.e., if $(n_1, n_2) = 1$, then $C_{n_1 n_2}(b) = C_{n_1}(b) C_{n_2}(b)$.

(iii) The function $b \to C_n(b)$ is multiplicative for a fixed n if and only if $\mu(n) = 1$, where μ denotes the Möbius function.

(iv) $C_n(b)$ is an even function of b, that is, $C_n(b) = C_n((b, n))$ for every b, n.

(v) For integers b and $n \geqslant 1$ we have

$$C_n(b) = \frac{\varphi(n)}{\varphi(n/(b,n))} \mu\Big(\frac{n}{(b,n)}\Big).$$

3.3. Generating functions of partition with certain conditions. For a positive integer n, a partition of n is a nonincreasing sequence of positive integers $p_1, p_2, \ldots, p_k$ whose sum is n. Each p_i is called a part of the partition. Let the function $p(n)$ denote the number of partitions of the integer n. It is well-known that the generating function of the sequence $\{p(n)\}_{n=0}^{\infty}$ is

$$\begin{aligned} \sum_{n \geqslant 0} p(n) q^n &= (1 + q + q^2 + q^3 + \ldots)(1 + q + q^2 + q^3 + \ldots)(1 + q^3 + q^6 + \ldots) \ldots \\ &= \frac{1}{1-q} \cdot \frac{1}{1-q^2} \cdot \frac{1}{1-q^3} \ldots = \prod_{i=1}^{\infty} \frac{1}{1-q^i} \quad \text{for } |q| < 1. \end{aligned} \tag{3.2}$$

From a combinatorial perspective, the monomial chosen from the ith parenthesis $1 + q^i + q^{2i} + q^{3i} + \ldots$ in (3.2) represents the number of times the part i appears in

the partition. In particular, if we choose the monomial $q^{n_i i}$ from the ith parenthesis, then the value i will appear n_i times in the partition. Each selection of monomials makes one contribution to the coefficient of q^n in the expression. More precisely, each contribution must be of the form $q^{1n_1} \cdot q^{2n_2} \cdot q^{3n_3} \ldots = q^{n_1+2n_2+3n_3+\cdots}$. Thus, the coefficient of q^n is the number of ways of writing $n = n_1 + 2n_2 + 3n_3 + \ldots$, where $n_1, n_2, n_3, \ldots$ are nonnegative integers representing the total count of parts of size $1, 2, 3, \ldots$ in the partition, respectively.

Suppose $A = \{a_1, a_2, a_3, \ldots\}$ is a set of positive integers. In general, the generating function for the number of partitions of n into members of set A is

$$f_A(q) = \prod_{a_j \in A} \frac{1}{1 - q^{a_j}}.$$

Moreover, the following lemma gives the generating function of the number of partitions of n into k parts, each taken from the given set A.

Lemma 3.3 ([15])**.** *Let A be a set of positive integers. Let k be a positive integer and b be a nonnegative integer. The number of partitions of b into k parts, each taken from the set A, is the coefficient of $q^b z^k$ in*

$$\prod_{a_j \in A} \frac{1}{1 - zq^{a_j}}.$$

Furthermore, if we multiply the coefficient of $q^b z^k$ in the expression

$$\prod_{a_j \in A} (1 - zq^{a_j})$$

by $(-1)^k$, then we obtain the number of distinct partitions of b into exactly k parts, with each taken from the set A.

4. Square solutions—proof of Theorem 1

It is convenient to use the characteristic function for squares in our proofs. Using this and Hensel's lemma, we prove multiplicativity for square solutions.

Recall that an element $a \in \mathbb{Z}_n$ is a square in $\mathbb{Z}_n$ (or square modulo n) if and only if $x^2 \equiv a \pmod{n}$ has a solution. The units (elements of $\mathbb{Z}_n$ that are relatively prime to n) that are squares are called quadratic residues modulo n. We define a function $\square_n \colon \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$\square_n(b) = \begin{cases} 1 & \text{if } b \text{ is a square modulo } n, \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

The following statement is a version of Hensel's lemma.

Lemma 4.1. *Suppose $f(x) \in \mathbb{Z}[x]$ and $f(a) \equiv 0 \pmod{p^m}$ and $f'(a) \not\equiv 0 \pmod{p}$. Then there is a unique $t \in \{0, 1, \ldots, p-1\}$ such that $f(a + tp^m) \equiv 0 \pmod{p^{m+1}}$.*

We use the following observations in the next lemma.

Let $s(n)$ and $q(n)$ denote the number of squares in $\mathbb{Z}_n$ and the number of quadratic residues in $\mathbb{Z}_n$, respectively. Equivalently,

$$s(n) = \sum_{b=1}^{n} \square_n(b) \quad \text{and} \quad q(n) = \sum_{\substack{b=1 \\ (b,n)=1}}^{n} \square_n(b).$$

It is well known that $q(n)$ is a multiplicative function. Stangl in [29] showed that $s(n)$ is a multiplicative function. Furthermore, for any odd prime p, he derived the following recursion formula for $s(p^r)$:

$$s(p^r) = q(p^r) + s(p^{r-2}) \quad \text{for } r \geqslant 3 \tag{4.2}$$

and $s(p) = q(p) + 1 = \frac{1}{2}(p+1)$, $s(p^2) = q(p^2) + 1 = \frac{1}{2}(p^2 - p + 2)$. This recursion formula follows from the observation that an element b is a square in $\mathbb{Z}_{p^{r-2}}$ if and only if bp^2 is a square in $\mathbb{Z}_{p^r}$. As a consequence of this recursion formula, we have the following lemma.

Lemma 4.2. *For an odd prime p and a positive integer l we have*

$$\sum_{x=1}^{p^l} \square_{p^l}(x) e\Big(\frac{xm}{p^l}\Big) = 1 + \frac{1}{2} \sum_{\substack{j=0 \\ j \equiv 0 \pmod 2}}^{l-1} \sum_{\substack{x=1 \\ (x,p^{l-j})=1}}^{p^{l-j}} \Big(1 + \Big(\frac{x}{p}\Big)\Big) e\Big(\frac{xm}{p^{l-j}}\Big), \tag{4.3}$$

where $\big(\frac{\cdot}{p}\big)$ is the Legendre symbol mod p.

P r o o f. For any $x \in \mathbb{Z}_{p^l}$ with $(x, p^l) = 1$, we can express x as

$$x = x_{l-1}p^{l-1} + \ldots + x_1 p + x_0,$$

where $0 \leqslant x_i \leqslant p-1$ for $0 \leqslant i \leqslant l-1$ and $x_0 \neq 0$. If x_0 is a residue modulo p, then the congruence $y^2 \equiv x \pmod{p}$ has a solution. Using Lemma 4.1 with the polynomial $f(x) = y^2 - x$, we can lift this solution modulo p^l. Alternatively, we can define $\frac{1}{2}(1 + (\frac{x}{p}))$ as a characteristic function for quadratic residues modulo p^l.

We now prove (4.3) by induction on l. If $l = 1$, then (4.3) follows from the definition of the Legendre symbol. If $l = 2$, then we have $s(p^2) = q(p^2) + 1$. Therefore (4.3) follows from the above observation.

Now we assume that the claim is true if $l \leqslant m-1$. By using (4.2) and the hypothesis, we write

$$\sum_{x=1}^{p^m} \square_{p^m}(x) e\Big(\frac{xm}{p^m}\Big) = 1 + \frac{1}{2} \sum_{\substack{j=0 \\ j\equiv 0 \pmod 2}}^{m-3} \sum_{\substack{x=1 \\ (x,p^{m-2-j})=1}}^{p^{m-2-j}} \Big(1+\Big(\frac{x}{p}\Big)\Big) e\Big(\frac{xm}{p^{m-2-j}}\Big) + \sum_{\substack{x=1 \\ (x,p^m)=1}}^{p^m} \square_{p^m}(x) e\Big(\frac{xm}{p^m}\Big).$$

By using the above observation, we write

$$\begin{aligned}\sum_{x=1}^{p^m} \square_{p^m}(x) e\Big(\frac{xm}{p^m}\Big) &= 1 + \frac{1}{2} \sum_{\substack{j=0 \\ j\equiv 0 \pmod 2}}^{m-3} \sum_{\substack{x=1 \\ (x,p^{m-2-j})=1}}^{p^{m-2-j}} \Big(1+\Big(\frac{x}{p}\Big)\Big) e\Big(\frac{xm}{p^{m-2-j}}\Big) \\ &\quad + \frac{1}{2} \sum_{\substack{x=1 \\ (x,p^m)=1}}^{p^m} \Big(1+\Big(\frac{x}{p}\Big)\Big) e\Big(\frac{xm}{p^m}\Big) \\ &= 1 + \frac{1}{2} \sum_{\substack{j=0 \\ j\equiv 0 \pmod 2}}^{m-1} \sum_{\substack{x=1 \\ (x,p^{m-j})=1}}^{p^{m-j}} \Big(1+\Big(\frac{x}{p}\Big)\Big) e\Big(\frac{xm}{p^{m-j}}\Big).\end{aligned}$$

This completes the proof of Lemma 4.2. □

Recall that $S_n(b; a_1, \ldots, a_k)$ denotes the number of square solutions of (1.1). Now, we show that the function $n \to S_n(b; a_1, \ldots, a_k)$ is multiplicative for any given integers $a_1, \ldots, a_k, b$.

Lemma 4.3. *Let $a_1, \ldots, a_k, b$ be integers. Then for any n and n' relatively prime we have*

$$S_{nn'}(b; a_1, \ldots, a_k) = S_n(b; a_1, \ldots, a_k) \cdot S_{n'}(b; a_1, \ldots, a_k).$$

P r o o f. It is easy to see that every square solution of the linear congruence $a_1x_1+\ldots+a_kx_k \equiv b \pmod{nn'}$ corresponds to a square solution of $a_1x_1+\ldots+a_kx_k \equiv b \pmod n$ and a square solution of $a_1x_1 + \ldots + a_kx_k \equiv b \pmod{n'}$. Thus, we have

$$S_{nn'}(b; a_1, \ldots, a_k) \leqslant S_n(b; a_1, \ldots, a_k) \cdot S_{n'}(b; a_1, \ldots, a_k).$$

Conversely, let $(x_1, \ldots, x_k)$ and $(x'_1, \ldots, x'_k)$ be square solutions of $a_1x_1+\ldots+a_kx_k \equiv b \pmod n$ and $a_1x'_1 + \ldots + a_kx'_k \equiv b \pmod{n'}$, respectively. Since $(n, n') = 1$, it

follows from the Chinese remainder theorem that there is a unique γ_i modulo nn' for each $1 \leqslant i \leqslant k$ such that

$$\gamma_i \equiv x_i \pmod{n}, \quad \gamma_i \equiv x_i' \pmod{n'} \quad \text{for } 1 \leqslant i \leqslant k.$$

Therefore, we have

$$a_1\gamma_1 + \ldots + a_k\gamma_k - b \equiv a_1x_1 + \ldots + a_kx_k - b \equiv 0 \pmod{n},$$
$$a_1\gamma_1 + \ldots + a_k\gamma_k - b \equiv a_1x_1' + \ldots + a_kx_k' - b \equiv 0 \pmod{n'}$$

and hence, $(n, n') = 1$ implies that $a_1\gamma_1 + \ldots + a_k\gamma_k \equiv b \pmod{nn'}$. Also, for each $1 \leqslant i \leqslant k$, the congruences

$$y_i^2 \equiv \gamma_i \pmod{n} \equiv x_i \pmod{n}, \quad y_i^2 \equiv \gamma_i \pmod{n'} \equiv x_i' \pmod{n'}$$

have solutions implying that $n \mid (y_i^2 - \gamma_i)$ and $n' \mid (y_i^2 - \gamma_i)$ for each $1 \leqslant i \leqslant k$. Since n and n' are relatively prime, we obtain $y_i^2 \equiv \gamma_i \pmod{nn'}$. Therefore, $(\gamma_1, \ldots, \gamma_k)$ is a square solution of $a_1x_1 + \ldots + a_kx_k \equiv b \pmod{nn'}$. This completes the proof of Lemma 4.3. □

We need one final lemma on Gauss sums that will be used in proving Theorem 3 on square solutions.

Lemma 4.4. *Let p be an odd prime and l be a positive integer. Let χ_{p^l} be a real character modulo p^l induced by the Legendre symbol $\left(\frac{\cdot}{p}\right)$ modulo p. Then for any positive integer m we have*

$$\sum_{x=1}^{p^l} \chi_{p^l}(x) e\Big(\frac{mx}{p^l}\Big) = \begin{cases} \varepsilon_p\Big(\dfrac{m/p^{l-1}}{p}\Big) p^{l-1/2} & \text{if } (m, p^l) = p^{l-1}, \\ 0 & \text{otherwise,} \end{cases}$$

where ε_p is defined as in (1.4).

P r o o f. If $p^l \mid m$, then it is straightforward to see that the required sum vanishes. Suppose $p^l \nmid m$, then by using Lemma 3.1 with $n = p^l$, $n^\star = p$ and $r = p^l/(p^l, m)$, we obtain

$$\sum_{x=1}^{p^l} \chi_{p^l}(x) e\Big(\frac{mx}{p^l}\Big) = \begin{cases} \Big(\dfrac{m/(p^l, m)}{p}\Big) \mu\Big(\dfrac{r}{p}\Big) \Big(\dfrac{r/p}{p}\Big) \dfrac{\varphi(p^l)}{\varphi(r)} \tau\Big(\Big(\dfrac{\cdot}{p}\Big)\Big) & \text{if } (m, p) \mid r, \\ 0 & \text{if } (m, p) \nmid r. \end{cases}$$

It follows from the definition of the Legendre symbol that

$$\Big(\frac{r/p}{p}\Big) = \Big(\frac{p^{l-1}/(m, p^l)}{p}\Big) = \begin{cases} 1 & \text{if } (m, p^l) = p^{l-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the sum is possibly nonzero only when $(m,p^l)=p^{l-1}$. Suppose $(m,p^l)=p^{l-1}$, then we have

$$\sum_{x=1}^{p^l}\chi_{p^l}(x)e\Big(\frac{mx}{p^l}\Big)=\Big(\frac{m/p^{l-1}}{p}\Big)\mu(1)\Big(\frac{1}{p}\Big)\frac{\varphi(p^l)}{\varphi(p)}\tau\Big(\Big(\frac{\cdot}{p}\Big)\Big)=p^{l-1}\Big(\frac{m/p^{l-1}}{p}\Big)\tau\Big(\Big(\frac{\cdot}{p}\Big)\Big).$$

Since the Legendre symbol is a real primitive character modulo p, by using Lemma 3.2, we obtain the required estimate. □

P r o o f of Theorem 1.1. Our aim is to calculate $S_n(b;a_1,\dots,a_k)$. Since $n=p_1^{l_1}\dots p_r^{l_r}$, by applying Lemma 4.3, it is enough to calculate $S_{p_i^{l_i}}(b;a_1,\dots,a_k)$ for $1\leqslant i\leqslant r$. For any $p\in\{p_1,\dots,p_r\}$ we write

$$\begin{aligned}&S_{p^l}(b;a_1,\dots,a_k)\\&\quad=\frac{1}{p^l}\sum_{m=1}^{p^l}\Big(\sum_{x_1=1}^{p^l}\square_{p^l}(x_1)\dots\sum_{x_k=1}^{p^l}\square_{p^l}(x_k)e\Big(\frac{(a_1x_1+\dots+a_kx_k-b)m}{p^l}\Big)\Big)\\&\quad=\frac{1}{p^l}\sum_{m=1}^{p^l}e\Big(\frac{-bm}{p^l}\Big)\sum_{x_1=1}^{p^l}\square_{p^l}(x_1)e\Big(\frac{a_1x_1m}{p^l}\Big)\dots\sum_{x_k=1}^{p^l}\square_{p^l}(x_k)e\Big(\frac{a_kx_km}{p^l}\Big),\end{aligned}$$

where $\square_{p^l}$ is defined as in (4.1). Then by using Lemma 4.2, we obtain

$$\begin{aligned}&S_{p^l}(b;a_1,\dots,a_k)\\&\quad=\frac{1}{p^l}\sum_{m=1}^{p^l}e\Big(\frac{-bm}{p^l}\Big)\Big(1+\frac{1}{2}\sum_{\substack{j_1=0\\ j_1\equiv0\pmod 2}}^{l-1}\sum_{\substack{x_1=1\\(x_1,p^{l-j_1})=1}}^{p^{l-j_1}}\Big(1+\Big(\frac{x_1}{p}\Big)\Big)e\Big(\frac{a_1x_1m}{p^{l-j_1}}\Big)\Big)\\&\qquad\dots\Big(1+\frac{1}{2}\sum_{\substack{j_k=0\\ j_k\equiv0\pmod 2}}^{l-1}\sum_{\substack{x_k=1\\(x_k,p^{l-j_k})=1}}^{p^{l-j_k}}\Big(1+\Big(\frac{x_k}{p}\Big)\Big)e\Big(\frac{a_kx_km}{p^{l-j_k}}\Big)\Big)\\&\quad=\frac{1}{p^l}\sum_{m=1}^{p^l}e\Big(\frac{-bm}{p^l}\Big)J_1(m)\dots J_k(m),\end{aligned}$$

where

$$J_i(m)=1+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv0\pmod 2}}^{l-1}\sum_{\substack{x_i=1\\(x_i,p^{l-j_i})=1}}^{p^{l-j_i}}\Big(1+\Big(\frac{x_i}{p}\Big)\Big)e\Big(\frac{a_ix_im}{p^{l-j_i}}\Big)\quad\text{for } 1\leqslant i\leqslant k.$$

Now, consider

$$\begin{aligned}
&J_i(m)\\
&= 1+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1}\sum_{\substack{x_i=1\\ (x_i,p^{l-j_i})=1}}^{p^{l-j_i}} e\Big(\frac{a_i x_i m}{p^l}\Big)+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1}\sum_{\substack{x_i=1\\ (x_i,p^{l-j_i})=1}}^{p^{l-j_i}}\Big(\frac{x_i}{p}\Big)e\Big(\frac{a_i x_i m}{p^{l-j_i}}\Big)\\
&= 1+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1} C_{p^{l-j_i}}(a_i m)+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1}\sum_{\substack{x_i=1\\ (x_i,p^{l-j_i})=1}}^{p^{l-j_i}}\Big(\frac{x_i}{p}\Big)e\Big(\frac{a_i x_i m}{p^{l-j_i}}\Big),
\end{aligned}$$

where $C_{p^{l-j_i}}(a_i m)$ is a Ramanujan's sum defined as in (3.1). By using Lemma 4.4, we write

$$J_i(m)=1+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1}\Big(C_{p^{l-j_i}}(a_i m)+\varepsilon_p\Big(\frac{a_i m/p^{l-j_i-1}}{p}\Big)\varrho_{j_i}(a_i m)p^{l-j_i-1/2}\Big),$$

where $\varrho_{j_i}(x)$ is defined as in (1.3). Therefore, we have

$$\begin{aligned}
S_{p^l}(b;a_1,\dots,a_k)&=\frac{1}{p^l}\sum_{m=1}^{p^l} e\Big(\frac{-bm}{p^l}\Big)\prod_{i=1}^{k}\Big(1+\frac{1}{2}\sum_{\substack{j_i=0\\ j_i\equiv 0 \pmod 2}}^{l-1}\Big(C_{p^{l-j_i}}(a_i m)\\
&\quad+\varepsilon_p\Big(\frac{a_i m/p^{l-j_i-1}}{p}\Big)\varrho_{j_i}(a_i m)p^{l-j_i-1/2}\Big)\Big)\\
&=\frac{1}{p^l}\Big(\sum_{m=1}^{p^l} e\Big(\frac{-bm}{p^l}\Big)+\sum_{\substack{K\subset\{1,\dots,k\}\\ K\neq\phi}}\frac{1}{2^{|K|}}S_K\Big),
\end{aligned}$$

where S_K is defined as in (1.2). This completes the proof of Theorem 1.1. □

P r o o f of Corollary 1.2. Since $(a_i,n)=1$ for all i, (1.2) can be written as

$$\begin{aligned}
S_K&=\sum_{r=0}^{l}\sum_{\substack{m=1\\ (m,p^l)=p^r}}^{p^l} e\Big(\frac{-bm}{p^l}\Big)\\
&\quad\times\Big(\sum_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{l-1}\Big(C_{p^{l-j}}(m)+\varepsilon_p\Big(\frac{m/p^{l-j-1}}{p}\Big)\varrho_j(m)p^{l-j-1/2}\Big)\Big)^{|K|}\\
&=\Big(\sum_{\substack{j=0\\ j\equiv 0 \pmod 2}}^{l-1} C_{p^{l-j}}(p^l)\Big)^{|K|}+S'_K,
\end{aligned}$$

where

$$S'_k = \sum_{r=0}^{l-1} \sum_{\substack{m=1 \\ (m,p^l)=p^r}}^{p^l} e\Big(\frac{-bm}{p^l}\Big)\Big(\sum_{\substack{j=0 \\ j\equiv 0 \pmod 2}}^{l-1} \Big(C_{p^{l-j}}(m)+\varepsilon_p\Big(\frac{m/p^{l-j-1}}{p}\Big)\varrho_j(m)p^{l-j-1/2}\Big)\Big)^{|K|}.$$

As we assume $(b,n)=1$, by using the property (v) of the Ramanujan sum and Lemma 3.1, we obtain that both sums

$$\sum_{\substack{m=1 \\ (m,p^l)=p^r}}^{p^l} e\Big(\frac{-bm}{p^l}\Big) \quad \text{and} \quad \sum_{\substack{m=1 \\ (m,p^l)=p^r}}^{p^l} e\Big(\frac{-bm}{p^l}\Big)\Big(\frac{m}{p}\Big)$$

vanish for $r \leqslant l-2$. So, when we apply the binomial expansion, we notice that the inner sums of terms where $r \leqslant l-2$ vanish. Thus, using the definition of ϱ_j (see Definition 1.3) and property (v) of the Ramanujan sum, we write

$$S'_K = \sum_{m=1}^{p-1} e\Big(\frac{-bm}{p}\Big)\Big(-p^{l-1} + \sum_{\substack{j=2 \\ j\equiv 0 \pmod 2}}^{l-1} \phi(p^{l-j}) + \varepsilon_p\Big(\frac{m}{p}\Big)p^{l-1/2}\Big)^{|K|}.$$

This completes the proof of Corollary 1.2. □

5. Order restricted congruence—Proof of Theorem 3

In this section, we discuss the proof of Theorem 1.4. We shall use the following lemma.

Lemma 5.1 ([7], Lemma IV.6)**.** *Let n be a positive integer and a, m be nonnegative integers. Then we have*

$$\prod_{j=1}^{n}\Big(1 - ze\Big(\frac{jam}{n}\Big)\Big) = (1-z^{n/d})^d, \quad \text{where } d=(am,n).$$

P r o o f of Theorem 1.4. Let $k = k_1 + \ldots + k_t$ be a partition of k given as in (1.5). By using Lemma 3.3, we see that the number of partitions of b into k parts such that exactly k_1 parts taken from the set A_1, exactly k_2 parts taken from the set A_2, and so on, up to exactly k_t parts taken from the set A_t, is the coefficient of $q^b z_1^{k_1} \ldots z_t^{k_t}$ in

$$\prod_{j_1\in A_1} \frac{1}{1-z_1q^{j_1}} \times \ldots \times \prod_{j_t\in A_t} \frac{1}{1-z_tq^{j_t}}.$$

Taking $A_i = \{a_i, 2a_i, \dots, na_i\}$ for $i = 1, \dots, t$ and $q = e^{2\pi \mathrm{i} m/n}$, where m is a non-negative integer, we observe

$$\sum_{b=1}^{n} M_n(k_1, \dots, k_t, a_1, \dots, a_t, b) e\Big(\frac{bm}{n}\Big)$$

to be the coefficient of $z_1^{k_1} \dots z_t^{k_t}$ in

$$\prod_{i=1}^{t} \prod_{j_i=1}^{n} \Big(1 - z_i e\Big(\frac{j_i m}{n}\Big)\Big)^{-1}.$$

By using Lemma 5.1, we obtain

$$\sum_{b=1}^{n} M_n(k_1, \dots, k_t, a_1, \dots, a_t, b) e\Big(\frac{bm}{n}\Big) = (-1)^{(k_1 d_1 + \dots + k_t d_t)/n} \binom{-d_1}{k_1 d_1/n} \dots \binom{-d_t}{k_t d_t/n},$$

where $d_i = (a_i m, n)$ for $i = 1, \dots, t$. Now, by taking the inverse Fourier transform, we write $M_n(k_1, \dots, k_t, a_1, \dots, a_t, b)$ as

$$\begin{aligned}
&\frac{1}{n} \sum_{m=1}^{n} (-1)^{(k_1 d_1 + \dots + k_t d_t)/n} \binom{-d_1}{k_1 d_1/n} \dots \binom{-d_t}{k_t d_t/n} e\Big(\frac{-bm}{n}\Big) \\
&= \frac{1}{n} \sum_{m=1}^{n} \frac{d_1}{d_1 + k_1 d_1/n} \dots \frac{d_t}{d_t + k_t d_t/n} \binom{d_1 + k_1 d_1/n}{k_1 d_1/n} \dots \binom{d_t + k_t d_t/n}{k_t d_t/n} e\Big(\frac{-bm}{n}\Big) \\
&= \frac{1}{n} \sum_{d_1 \mid n} \dots \sum_{d_t \mid n} \frac{d_1}{d_1 + k_1 d_1/n} \dots \frac{d_t}{d_t + k_t d_t/n} \binom{d_1 + k_1 d_1/n}{k_1 d_1/n} \dots \binom{d_t + k_t d_t/n}{k_t d_t/n} \\
&\quad \times \sum_{\substack{m=1 \\ (a_i m, n) = d_i \\ i = 1, \dots, t}}^{n} e\Big(\frac{-bm}{n}\Big).
\end{aligned}$$

If we assume $(a_i, n) = f$ for $i = 1, \dots, t$, we write $d_i = (a_i m, n) = f(m, n/f) = fd$ for $i = 1, \dots, t$. Thus, we have

$$\begin{aligned}
&\frac{f}{n} \sum_{d \mid n/f} \frac{df}{df + k_1 df/n} \dots \frac{df}{df + k_t df/n} \binom{df + k_1 df/n}{k_1 df/n} \dots \binom{df + k_t df/n}{k_t df/n} C_{n/df}(-b) \\
&= \frac{f}{n} \sum_{d \mid n/f} \frac{n/d}{n/d + k_1/d} \dots \frac{n/d}{n/d + k_t/d} \binom{n/d + k_1/d}{k_1/d} \dots \binom{n/d + k_t/d}{k_t/d} C_d(b) \\
&= \frac{f}{n} \sum_{d \mid (n/f, k_1, \dots, k_t)} \frac{n^t}{(n + k_1) \dots (n + k_t)} \binom{(n + k_1)/d}{k_1/d} \dots \binom{(n + k_t)/d}{k_t/d} C_d(b).
\end{aligned}$$

This completes the proof of Theorem 1.4. □

As an illustration of the first statement, consider the congruence $2(x_1 + x_2) + 3(x_3 + x_4) \equiv 5 \bmod 6$. Theorem 1.4 gives the number of solutions to be 63, which can be seen by listing all the solutions with $x_1 \geqslant x_2$ and $x_3 \geqslant x_4$.

As an illustration of the second statement, consider the congruence $x_1 + x_2 + 3(x_3 + x_4) \equiv 1 \bmod 4$. Theorem 1.4 gives the number of solutions to be 24, which can be seen by listing all the solutions with $x_1 \geqslant x_2$ and $x_3 \geqslant x_4$.

6. Strict order restricted congruence—Proof of Theorem 2

P r o o f of Theorem 1.3. By taking $A = \{a, 2a, \dots, na\}$ and $q = \mathrm{e}^{2\pi \mathrm{i} m/n}$, where m is a nonnegative integer in Lemma 3.3, we see that

$$\sum_{b=1}^{n} (-1)^k N_n(a,b) e\Big(\frac{bm}{n}\Big)$$

equals to the coefficient of z^k in

$$\prod_{j=1}^{n} \Big(1 - ze\Big(\frac{jm}{n}\Big)\Big).$$

By using Lemma 5.1, we obtain

$$\sum_{b=1}^{n} (-1)^k N_n(a,b) e\left(\frac{bm}{n}\right) = (-1)^{kd/n} \binom{d}{kd/n},$$

where $d = (am, n)$. Now, by taking the inverse Fourier transform, we write

$$\begin{aligned}
N(a,b) &= \frac{(-1)^k}{n} \sum_{m=1}^{n} (-1)^{kd/n} \binom{d}{kd/n} e\Big(\frac{-bm}{n}\Big) \\
&= \frac{(-1)^k}{n} \sum_{d|n} \sum_{\substack{m=1 \\ (am,n)=d}}^{n} (-1)^{kd/n} \binom{d}{kd/n} e\Big(\frac{-bm}{n}\Big) \\
&= \frac{(-1)^k f}{n} \sum_{d|n/f} (-1)^{kdf/n} \binom{df}{kdf/n} \sum_{\substack{m=1 \\ (m,n/f)=d}}^{n/f} e\Big(\frac{-bm}{n}\Big) \\
&= \frac{(-1)^k f}{n} \sum_{d|n/f} (-1)^{kdf/n} \binom{df}{kdf/n} C_{n/df}(-b) \\
&= \frac{(-1)^k f}{n} \sum_{d|(n/f,k)} (-1)^{k/d} \binom{n/d}{k/d} C_d(b).
\end{aligned}$$

This completes the proof of Theorem 1.3.

Acknowledgment. The authors are grateful to the referee for her/his comments. The first two authors would like to thank the Indian Statistical Institute, Bangalore centre for providing an ideal environment to carry out this work. The second author expresses his gratitude to NBHM for financial support during the period of this work.

References

[1] *K. Bibak*: Order-restricted linear congruences. Discrete Math. *343* (2020), Article ID 111690, 4 pages. zbl MR doi

[2] *K. Bibak, B. M. Kapron, V. Srinivasan*: Counting surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group with motivations from string theory and QFT. Nucl. Phys., B *910* (2016), 712–723. zbl MR doi

[3] *K. Bibak, B. M. Kapron, V. Srinivasan*: Unweighted linear congruences with distinct coordinates and the Varshamov-Tenengolts codes. Des. Codes Cryptography *86* (2018), 1893–1904. zbl MR doi

[4] *K. Bibak, B. M. Kapron, V. Srinivasan*: A generalization of Schönemann's theorem via a graph theoretic method. Discrete Math. *342* (2019), 3057–3061. zbl MR doi

[5] *K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, L. Tóth*: Restricted linear congruences. J. Number Theory *171* (2017), 128–144. zbl MR doi

[6] *K. Bibak, B. M. Kapron, V. Srinivasan, L. Tóth*: On an almost-universal hash function family with applications to authentication and secrecy codes. Int. J. Found. Comput. Sci. *29* (2018), 357–375. zbl MR doi

[7] *K. Bibak, O. Milenkovic*: Explicit formulas for the weight enumerators of some classes of deletion correcting codes. IEEE Trans. Commun. *67* (2019), 1809–1816. doi

[8] *A. Brauer*: Lösung der Aufgabe 30. Jahresber. Dtsch. Math.-Ver. *35* (1926), 92–94. (In German.) zbl

[9] *C. Calderón, J. M. Grau, A. M. Oller-Marcén, L. Tóth*: Counting invertible sums of squares modulo n and a new generalization of Euler's totient function. Publ. Math. Debr. *87* (2015), 133–145. zbl MR doi

[10] *Q. Cheng, E. Murray*: On deciding deep holes of Reed-Solomon codes. Theory and Applications of Models of Computation. Lecture Notes in Computer Science 4484. Springer, Berlin, 2007, pp. 296–305. zbl MR doi

[11] *E. Cohen*: A class of arithmetical functions. Proc. Natl. Acad. Sci. USA *41* (1955), 939–944. zbl MR doi

[12] *L. E. Dickson*: History of the Theory of Numbers. II. Diophantine Analysis. Chelsea Publishing, New York, 1966. zbl MR

[13] *J. M. Grau, A. M. Oller-Marcén*: Fast computation of the number of solutions to $x_1^2 + \ldots + x_k^2 \equiv \lambda \pmod{n}$. J. Number Theory *200* (2019), 427–440. zbl MR doi

[14] *D. J. Grynkiewicz, A. Philipp, V. Ponomarenko*: Arithmetic-progression-weighted subsequence sums. Isr. J. Math. *193* (2013), 359–398. zbl MR doi

[15] *H. Gupta*: Partitions - a survey. J. Res. Natl. Bur. Stand., Sect. B *74* (1970), 1–29. zbl MR doi

[16] *R. Hull*: The numbers of solutions of congruences involving only kth powers. Trans. Am. Math. Soc. *34* (1932), 908–937. zbl MR doi

[17] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics 84. Springer, New York, 1990. zbl MR doi

[18] *D. Jacobson, K. S. Williams*: On the number of distinguished representations of a group element. Duke Math. J. *39* (1972), 521–527. zbl MR doi

[19] *D. N. Lehmer*: Certain theorems in the theory of quadratic residues. Am. Math. Mon. *20* (1913), 148–157. zbl MR doi

[20] *J. Li, D. Wan*: On the subset sum problem over finite fields. Finite Fields Appl. *14* (2008), 911–929. zbl MR doi
[21] *J. Li, D. Wan*: Counting subset sums of finite Abelian groups. J. Comb. Theory, Ser. A *119* (2012), 170–182. zbl MR doi
[22] *S. Li, Y. Ouyang*: Counting the solutions of $\lambda_1 x_1^{k_1} + \ldots + \lambda_t x_t^{k_t} \equiv c \bmod n$. J. Number Theory *187* (2018), 41–65. zbl MR doi
[23] *H. L. Montgomery, R. C. Vaughan*: Multiplicative Number Theory. I. Classical Theory. Cambridge Studies in Advanced Mathematics 97. Cambridge University Press, Cambridge, 2007. zbl MR doi
[24] *C. A. Nicol, H. S. Vandiver*: A von Sterneck arithmetical function and restricted partitions with respect to a modulus. Proc. Natl. Acad. Sci. USA *40* (1954), 825–835. zbl MR doi
[25] *H. Rademacher*: Über den Vektorenbereich eines konvexen ebenen Bereiches. Jahresber. Dtsch. Math.-Ver. *34* (1925), 64–79. (In German.) zbl
[26] *K. G. Ramanathan*: Some applications of Ramanujan's trigonometrical sum $C_m(n)$. Proc. Indian Acad. Sci., Sect. A *20* (1944), 62–69. zbl MR doi
[27] *J. Riordan*: Enumerations for permutations in difference form. Proc. Am. Math. Soc. *13* (1962), 107–110. zbl MR doi
[28] *T. Schönemann*: Theorie der symmetrischen Functionen der Wurzeln einer Gleichung: Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben. J. Reine Angew. Math. *19* (1839), 231–243. (In German.) zbl MR doi
[29] *W. D. Stangl*: Counting squares in $\mathbb{Z}_n$. Math. Mag. *69* (1996), 285–289. zbl MR doi
[30] *L. Tóth*: Counting solutions of quadratic congruences in several variables revisited. J. Integer Seq. *17* (2014), Article ID 14.11.6, 23 pages. zbl MR

Authors' address: Chinnakonda Gnanamoorthy Karthick Babu (corresponding author), Ranjan Bera, Balasubramanian Sury, Statistics and Mathematics Unit, Indian Statistical Institute, R.V. College Post, Bangalore-560059, India, e-mail: cgkarthick24@gmail.com, ranjan.math.rb@gmail.com, surybang@gmail.com.