A FORMULA FOR THE NUMBER OF SOLUTIONS OF A RESTRICTED LINEAR CONGRUENCE

K. Vishnu Namboothiri, Alappuzha

Received December 25, 2018. Published online January 15, 2020.
Communicated by Clemens Fuchs

Abstract. Consider the linear congruence equation $x_1 + \ldots + x_k \equiv b \pmod{n^s}$ for $b \in \mathbb{Z}$, $n, s \in \mathbb{N}$. Let $(a, b)_s$ denote the generalized gcd of a and b which is the largest l^s with $l \in \mathbb{N}$ dividing a and b simultaneously. Let $d_1, \ldots, d_{\tau(n)}$ be all positive divisors of n. For each $d_j \mid n$, define $\mathcal{C}_{j,s}(n) = \{1 \leqslant x \leqslant n^s \colon (x, n^s)_s = d_j^s\}$. K. Bibak et al. (2016) gave a formula using Ramanujan sums for the number of solutions of the above congruence equation with some gcd restrictions on x_i. We generalize their result with generalized gcd restrictions on x_i and prove that for the above linear congruence, the number of solutions is

$$\frac{1}{n^s} \sum_{d \mid n} c_{d,s}(b) \prod_{j=1}^{\tau(n)} \Big(c_{n/d_j,s}\Big(\frac{n^s}{d^s}\Big)\Big)^{g_j}$$

where $g_j = |\{x_1, \ldots, x_k\} \cap \mathcal{C}_{j,s}(n)|$ for $j = 1, \ldots, \tau(n)$ and $c_{d,s}$ denotes the generalized Ramanujan sum defined by E. Cohen (1955).

Keywords: restricted linear congruence; generalized gcd; generalized Ramanujan sum; finite Fourier transform

MSC 2020: 11D79, 11P83, 11L03, 11A25, 42A16

1. Introduction

The history of attempts to find general solutions of linear congruences is very old. For the general linear congruence equation

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

Lehmer (see [9]) proved the following theorem.

DOI: 10.21136/MB.2020.0171-18

© The author(s) 2020. This is an open access article under the CC BY-NC-ND licence

Theorem 1.1. *Let $a_1, \ldots, a_k, b, n \in \mathbb{Z}$, $n \geqslant 1$. The linear congruence equation* (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 is the gcd of $a_1, \ldots, a_k, n$. Furthermore, if this condition is satisfied, then there are ln^{k-1} solutions.*

The above type of congruence equations is called a restricted linear congruence, if we put some restrictions on the solution set, like $(x_i, n) = t_i$, where t_i are given positive divisors of n. Many authors have attempted to solve this kind of restricted congruences with various conditions. With $a_i = 1$ and restriction $(x_i, n) = 1$, Rademacher (see [15]) and Brauer (see [16]) independently gave a formula for the number of solutions $N_n(k, b)$ of the congruence (1.1). Their formula is

$$N_n(k,b) = \frac{\varphi(n)^k}{n} \prod_{p \mid n, p \mid b} \Big(1 - \frac{(-1)^{k-1}}{(p-1)^{k-1}}\Big) \prod_{p \mid n, p \nmid b} \Big(1 - \frac{(-1)^k}{(p-1)^k}\Big), \tag{1.2}$$

where φ is the Euler totient function and p are all the prime divisors of n. An equivalent formula involving the Ramanujan sums was proved by Nicol and Vandiver (see [14]) initially and Cohen (see [7]) later. They proved that

$$N_n(k,b) = \frac{1}{n} \sum_{d \mid n} c_d(b) \Big(c_n\Big(\frac{n}{d}\Big)\Big)^k, \tag{1.3}$$

where $c_d(b)$ denotes the usual Ramanujan sum.

The restricted congruence (1.1) and its solutions have found interesting applications in various fields like number theory, cryptography, combinatorics and computer science. The special case of the problem with $b = 0$ and $a_i = 1$ is related to the multivariate arithmetic function defined by Liskovets (see [10]) which has many combinatorial as well as topological applications. The problem has also found use in studying universal hashing (see Bibak et al. [4]) which has applications in computer science.

In [2], Bibak et al. considered the linear congruence (1.1) with $a_i = 1$ and the restrictions $(x_i, n) = t_i$ where t_i are given positive divisors of n. They proved the following theorem.

Theorem 1.2. *Let $b, n \in \mathbb{Z}$, $n \geqslant 1$, and $d_1, \ldots, d_{\tau(n)}$ be the positive divisors of n. For $1 \leqslant j \leqslant \tau(n)$, put $\mathcal{C}_j = \{1 \leqslant x \leqslant n \colon (x, n) = d_j\}$. The number of solutions of the linear congruence $x_1 + \ldots + x_k \equiv b \pmod{n}$ with $g_j = |\{x_1, \ldots, x_k\} \cap \mathcal{C}_j|$ is*[1]

$$\frac{1}{n} \sum_{d \mid n} c_d(b) \prod_{j=1}^{\tau(n)} \Big(c_{n/d_j}\Big(\frac{n}{d}\Big)\Big)^{g_j}. \tag{1.4}$$

[1] The formula appearing in Theorem 1.1 of Bibak et al. (see [2]) seems to contain mistyped d in the place of n/d in the second Ramanujan sum.

This result has been proved in some special cases by many authors, for example in [7], [8], [14], [17]. Bibak et al. themselves gave an alternate proof for the above result in [3]. The author himself generalized this result in [13] giving a formula for the number of solutions of the congruence equation $a_1^s x_1 + \ldots + a_k^s x_k \equiv b \pmod{n^s}$ with the restrictions modified to $(x_i, n^s)_s = d_i^s$ where d_i are the positive divisors of n and n^s is the modulus. We here give an alternate formula for the number of solutions of the congruence using techniques of finite Fourier transform of arithmetic functions and properties of Ramanujan sums following [2] closely. At this point, we would like to mention the quadratic congruence $a_1 x_1^2 + \ldots + a_k x_k^2 \equiv b \pmod{n}$, the solutions of which were attempted to be counted by Tóth in [18] using techniques involving the Jordan totient function and Ramanujan sums. We expect our result and proof, which use properties of generalized Ramanujan sums, to make some impact on attempts to solve such nonlinear congruences and to demonstrate the diverse ways in which generalizations of Ramanujan sums can work.

2. Notations and basic results

For $a, b \in \mathbb{Z}$ with at least one of them nonzero, the generalized gcd of these numbers $(a, b)_s$ is defined to be the largest l^s with $l \in \mathbb{N}$ dividing a and b simultaneously. Therefore $(a, b)_1 = (a, b)$, the usual gcd of two integers, $\tau(n)$ denotes the number of positive divisors of an integer n.

For a positive integer r, an arithmetic function f is said to be periodic with period r (or r-periodic) if $f(m+r) = f(m)$ for every $m \in \mathbb{Z}$. By $e(x)$, we denote the complex exponential funcion $\exp(2\pi i x)$ which has period 1.

Let $c_r(n)$ denote the Ramanujan sum which is defined to be the sum of nth powers of primitive rth roots of unity. That is,

$$c_r(n) = \sum_{j=1,(j,r)=1}^{r} e\Big(\frac{jn}{r}\Big). \tag{2.1}$$

For a positive integer s, Cohen (see [5]) generalized the Ramanujan sum defining $c_{r,s}$ by

$$c_{r,s}(n) = \sum_{j=1,(j,r^s)_s=1}^{r^s} e\Big(\frac{nj}{r^s}\Big). \tag{2.2}$$

Note that for $s = 1$, this definition gives the usual Ramanujan sum defined in

equation (2.1). In the same paper, Cohen also gave the formula

$$c_{r,s}(n) = \sum_{d|r,d^s|n} \mu\Big(\frac{r}{d}\Big) d^s, \tag{2.3}$$

where μ is the Moebius function.

We now have an easy, but very useful lemma.

Lemma 2.1. *As a function of a, $(a,b)_s$ is b-periodic.*

P r o o f. Note that $(a,b)_s$ is the largest l^s with $l \in \mathbb{N}$ that divides a and b simultaneously. So $a = l^s a_1$ and $b = l^s b_1$ with a_1 and b_1 sharing no common sth power. Now $l^s \mid a+b$ and $l^s \mid b$. If $(a+b,b)_s = l^s l_1^s$ for some $l_1 \in \mathbb{N}$, then $l_1^s \mid a+b$ and $l_1^s \mid b$ so that $l_1^s \mid a$ as well. Therefore $(a,b)_s = l^s l_1^s$ and so $l_1 = 1$. Then $(a+b,b)_s = l^s$. □

Let r, s be positive integers. A function f that satisfies $f(m) = f((m,r^s)_s)$ is called an (r,s)-*even function*. This concept was introduced by McCarthy in [11] and many of its properties were studied there. The above lemma says that an (r,s)-even function is r^s-periodic.

The following statement appeared as Lemma (2) in [6]. Note that our notation $c_{r,s}(n)$ is exactly the same as the notation $c_s(n,r)$ given by Cohen in [6].

Lemma 2.2. *If $(n,r^s)_s = l^s$, then $c_{r,s}(n) = c_{r,s}(l^s)$.*

The above two lemmas combined together tell that $c_{r,s}(n)$ is r^s-periodic. It also follows that $c_{r,s}(-n) = c_{r,s}(n)$.

We now have one more lemma. Since we could not find a proof for this anywhere, we prove it using some elementary arguments.

Lemma 2.3. *Let $e \mid n$. Then $c_{e,s}$ is (n,s)-even. That is, $c_{e,s}(m) = c_{e,s}((m,n^s)_s)$.*

P r o o f. We use two facts;

(1) $c_{e,s}$ is (e,s)-even.

(2) $((m,n^s)_s, e^s)_s = l^s$ if and only if l^s is the largest sth power dividing $(m,n^s)_s$ and e^s, that is if and only if l^s is the largest sth power dividing m, n^s and e^s. Therefore l^s is the largest sth power dividing m and e^s, and so $(m,e^s)_s = l^s$. The conclusion is that $((m,n^s)_s, e^s)_s = (m,e^s)_s$.

Combining these two facts, we get

$$c_{e,s}((m,n^s)_s) = c_{e,s}(((m,n^s)_s, e^s)_s) = c_{e,s}((m,e^s)_s) = c_{e,s}(m).$$

□

For an r-periodic arithmetic function $f(n)$, its *finite Fourier transform* is defined as the function

$$\hat{f}(b) = \frac{1}{r}\sum_{n=1}^{r} f(n)e\Big(\frac{-bn}{r}\Big). \tag{2.4}$$

A *Fourier representation of* f is given by

$$f(n) = \sum_{b=1}^{r} \hat{f}(b)e\Big(\frac{bn}{r}\Big). \tag{2.5}$$

See, for example, [12], page 109 or [1], Chapter 8 for a detailed study on finite Fourier transforms.

We are now ready to state and prove our main result.

3. The main theorem

Theorem 3.1. *Let $b, n \in \mathbb{Z}$, $n \geqslant 1$, and $d_1 \ldots, d_{\tau(n)}$ be the positive divisors of n. For $1 \leqslant j \leqslant \tau(n)$, define $\mathcal{C}_{j,s}(n) = \{1 \leqslant x \leqslant n^s \colon (x, n^s)_s = d_j^s\}$. The number of solutions (with all permutations of a solution considered to be the same) of the linear congruence*

$$x_1 + \ldots + x_k \equiv b \pmod{n^s} \tag{3.1}$$

with given numbers $g_j = |\{x_1, \ldots, x_k\} \cap \mathcal{C}_{j,s}(n)|$, $1 \leqslant j \leqslant \tau(n)$ is

$$\frac{1}{n^s}\sum_{d|n} c_{d,s}(b) \prod_{j=1}^{\tau(n)} \Big(c_{n/d_j,s}\Big(\frac{n^s}{d^s}\Big)\Big)^{g_j}. \tag{3.2}$$

P r o o f. As we have already mentioned, the proof uses the basic properties of finite Fourier transforms of r^s-periodic functions, the properties of generalized Ramanujan sums, and some combinatorial arguments. We follow the same approach used by Bibak et al. in [2].

Let $\hat{f}(b)$ denote the number of solutions of the linear congruence (3.1). Therefore $\hat{f}(b)$ is the number of possible ways of writing b as a sum modulo n^s using g_j elements in $\mathcal{C}_{j,s}$ where j varies from 1 to $\tau(n)$. Note that if b is replaced with $b + n^s$ in this equation, it remains the same. So $\hat{f}(b) = \hat{f}(b + n^s)$ and therefore $\hat{f}$ is n^s-periodic. Let us consider the following product of exponential sums:

$$\prod_{j=1}^{\tau(n)} \Big(\sum_{x\in\mathcal{C}_{j,s}} e\Big(\frac{mx}{n^s}\Big)\Big)^{g_j}.$$

To understand this product of sums better, put $\alpha = e(m)$. Then the product becomes

$$\prod_{j=1}^{\tau(n)} \Big(\sum_{x \in \mathcal{C}_{j,s}} \alpha^{x/n^s} \Big)^{g_j}.$$

Expanding this product of sums, we get terms like $\alpha^{1/n^s}, \alpha^{2/n^s}, \ldots, \alpha^{(n^s-1)/n^s}$. Some of these powers need not occur as it depends on whether the sum of terms in $\mathcal{C}_{j,s}$ can be equal to that power. For example, α^{5/n^s} does not exist if the elements in various $\mathcal{C}_{j,s}$ cannot add up together to give 5 modulo n^s. Now, how many times does each α^{b/n^s} exist? As many times as is the number of possible solutions of the linear congruence with g_j entries from $\mathcal{C}_{j,s}$. But this is precisely our $\hat{f}(b)$. So we get

$$\sum_{b=1}^{n^s} \hat{f}(b) e\Big(\frac{bm}{n^s}\Big) = \prod_{j=1}^{\tau(n)} \Big(\sum_{x \in \mathcal{C}_{j,s}} e\Big(\frac{mx}{n^s}\Big) \Big)^{g_j}.$$

We now calculate the inner sum in this product,

$$\sum_{x \in \mathcal{C}_{j,s}} e\Big(\frac{mx}{n^s}\Big) = \sum_{\substack{1 \leqslant x \leqslant n^s, \\ (x,n^s)_s = d_j^s}} e\Big(\frac{mx}{n^s}\Big) = \sum_{\substack{1 \leqslant y \leqslant n^s/d_j^s, \\ (y, n^s/d_j^s)_s = 1}} e\Big(\frac{my}{n^s/d_j^s}\Big) = c_{n/d_j,s}(m),$$

which gives

$$\sum_{b=1}^{n^s} \hat{f}(b) e\Big(\frac{bm}{n^s}\Big) = \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(m))^{g_j}.$$

Use the fact that $\hat{f}(b)$ is n^s-periodic. By the finite Fourier transform theory, we get

$$\hat{f}(b) = \frac{1}{n^s} \sum_{m=1}^{n^s} \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(m))^{g_j} e\Big(\frac{-bm}{n^s}\Big)$$

now collect the terms with same generalized gcd

$$= \frac{1}{n^s} \sum_{d|n} \sum_{\substack{1 \leqslant m \leqslant n^s, \\ (m,n^s)_s = d^s}} \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(m))^{g_j} e\Big(\frac{-bm}{n^s}\Big)$$

$$= \frac{1}{n^s} \sum_{d|n} \sum_{\substack{1 \leqslant m' \leqslant n^s/d^s, \\ (m', n^s/d^s)_s = 1}} \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(m'd^s))^{g_j} e\Big(\frac{-bm'd^s}{n^s}\Big)$$

$$= \frac{1}{n^s} \sum_{d|n} \sum_{\substack{1 \leqslant m' \leqslant n^s/d^s, \\ (m', n^s/d^s)_s = 1}} e\Big(\frac{-bm'}{n^s/d^s}\Big) \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}((m'd^s, n^s)_s))^{g_j}$$

$$= \frac{1}{n^s} \sum_{d|n} \sum_{\substack{1 \leqslant m' \leqslant n^s/d^s, \\ (m', n^s/d^s)_s = 1}} e\Big(\frac{-bm'}{n^s/d^s}\Big) \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(d^s))^{g_j}$$

$$= \frac{1}{n^s} \sum_{d|n} c_{n/d,s}(b) \prod_{j=1}^{\tau(n)} (c_{n/d_j,s}(d^s))^{g_j} = \frac{1}{n^s} \sum_{d|n} c_{d,s}(b) \prod_{j=1}^{\tau(n)} \Big(c_{n/d_j,s}\Big(\frac{n^s}{d^s}\Big)\Big)^{g_j}.$$

□

We give a small example to demonstrate the result: Consider the linear congruence $x_1 + x_2 \equiv 5 \pmod{16}$. Here $n^s = 4^2$, $b = 5$, $k = 2$, $\{d_j^2\} = \{1, 4, 16\}$ and so

$$\begin{aligned}
\mathcal{C}_{1,2} &= \{1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15\}, \\
\mathcal{C}_{2,2} &= \{4, 8, 12\}, \\
\mathcal{C}_{3,2} &= \{16\}.
\end{aligned}$$

Suppose that we want to find solutions with the restrictions $(x_1, 16)_2 = 1$ and $(x_2, 16)_2 = 4$. In this case $g_1 = 1$, $g_2 = 1$, $g_3 = 0$. By simple observation, we get the number of solutions to be 3, which are $\langle 1, 4\rangle$, $\langle 9, 12\rangle$, $\langle 13, 8\rangle$. Now according to our formula, the computation is the following:

$$\begin{aligned}
&\sum_{d|4} c_{d,2}(5) \prod_{j=1}^{3} c_{4/d_j,2}\Big(\frac{16}{d^2}\Big)^{g_j} \\
&\quad = c_{1,2}(5) \cdot \prod_{j=1}^{3} c_{4/d_j,2}\Big(\frac{16}{1^2}\Big)^{g_j} + c_{2,2}(5) \cdot \prod_{j=1}^{3} c_{4/d_j,2}\Big(\frac{16}{2^2}\Big)^{g_j} \\
&\qquad + c_{4,2}(5) \cdot \prod_{j=1}^{3} c_{4/d_j,2}\Big(\frac{16}{4^2}\Big)^{g_j} \\
&\quad = c_{1,2}(5) \cdot (c_{4,2}(16) \cdot c_{2,2}(16) c_{1,2}(16)) + c_{2,2}(5) \cdot (c_{4,2}(4) \cdot c_{2,2}(4) c_{1,2}(4)) \\
&\qquad + c_{4,2}(5) \cdot (c_{4,2}(1) \cdot c_{2,2}(1) c_{1,2}(1)) \\
&\quad = 1 \cdot 12 \cdot 3 \cdot 1 + (-1) \cdot (-4) \cdot 3 \cdot 1 + 0 \cdot 0 \cdot (-1) \cdot 1 = 48,
\end{aligned}$$

which on division by 16 gives 3 as the number of solutions. We have used identity (2.3) to evaluate $c_{r,s}$ at various values.

Though it appears that computing the number of solutions using the above formula is more tedious than performing the direct calculations, we feel that such a closed formula may be useful for many other purposes. For example, the same formula derived by Bibak et al. in [2] with $s = 1$ was used to design an almost-universal hash function family in [4] which had applications in authentication schemes.

References

[1] *T. M. Apostol*: Introduction to Analytic Number Theory. Undergraduate Texts in Mathematics. Springer, New York, 1976. zbl MR doi

[2] *K. Bibak, B. M. Kapron, V. Srinivasan*: On a restricted linear congruence. Int. J. Number Theory *12* (2016), 2167–2171. zbl MR doi

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

[4] *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. (2018), 357–375. zbl MR doi

[5] *E. Cohen*: An extension of Ramanujan's sum. Duke Math. J. *16* (1949), 85–90. zbl MR doi

[6] *E. Cohen*: An extension of Ramanujan's sum. II. Additive properties. Duke Math. J. *22* (1955), 543–550. zbl MR doi

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

[8] *J. D. Dixon*: A finite analogue of the Goldbach problem. Can. Math. Bull. *3* (1960), 121–126. zbl MR doi

[9] *D. N. Lehmer*: Certain theorems in the theory of quadratic residues. Am. Math. Monthly *20* (1913), 151–157. zbl MR doi

[10] *V. A. Liskovets*: A multivariate arithmetic function of combinatorial and topological significance. Integers *10* (2010), 155–177. zbl MR doi

[11] *P. J. McCarthy*: The generation of arithmetical identities. J. Reine Angew. Math. *203* (1960), 55–63. zbl MR doi

[12] *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

[13] *K. V. Namboothiri*: On the number of solutions of a restricted linear congruence. J. Number Theory *188* (2018), 324–334. zbl MR doi

[14] *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

[15] *H. Rademacher*: Aufgabe 30. Jahresber. Dtsch. Math.-Ver. *34* (1925), page 158. (In German.)

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

[17] *J. W. Sander, T. Sander*: Adding generators in cyclic groups. J. Number Theory *133* (2013), 705–718. zbl MR doi

[18] *L. Tóth*: Counting solutions of quadratic congruences in several variables revisited. J. Integer Seq. *17* (2014), Article 14.11.6, 23 pages. zbl MR

Author's address: *K. Vishnu Namboothiri*, Department of Mathematics, Government College, Ambalapuzha, Alappuzha 688 561, Kerala, India, and Department of Collegiate Education, Government of Kerala, 6th Floor, Vikas Bhavan, Palayam, Thiruvananthapuram 695 033, Kerala, India, e-mail: `kvnamboothiri@gmail.com`.