Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the number of solutions of a restricted linear congruence

K. Vishnu Namboothiri [a,b,*]

[a] *Department of Mathematics, Government Polytechnic College, Vennikulam, Pathanamthitta, Kerala 689 544, India*
[b] *Department of Collegiate Education, Government of Kerala, India*

ARTICLE INFO

Article history:
Received 21 August 2017
Received in revised form 29 October 2017
Accepted 8 January 2018
Available online xxxx
Communicated by S.J. Miller

MSC:
11P83
11L03
11A25
42A16

Keywords:
Restricted linear congruence
Generalized gcd
Generalized Ramanujan sum
Discrete Fourier transforms

ABSTRACT

Consider the linear congruence equation

$$a_1^s x_1 + \ldots + a_k^s x_k \equiv b \,(\mathrm{mod}\ n^s) \text{ where } a_i, b \in \mathbb{Z}, s \in \mathbb{N}.$$

Denote by $(a,b)_s$ the largest $l^s \in \mathbb{N}$ which divides a and b simultaneously. Given $t_i | n$, we seek solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}^k$ for this linear congruence with the restrictions $(x_i, n^s)_s = t_i^s$. Bibak et al. [2] considered the above linear congruence with $s = 1$ and gave a formula for the number of solutions in terms of the Ramanujan sums. In this paper, we derive a formula for the number of solutions of the above congruence for arbitrary $s \in \mathbb{N}$ which involves the generalized Ramanujan sums defined by E. Cohen [5].

* Correspondence to: Department of Mathematics, Government Polytechnic College, Vennikulam, Pathanamthitta, Kerala 689 544, India.
E-mail address: kvnamboothiri@gmail.com.

https://doi.org/10.1016/j.jnt.2018.01.013
0022-314X/

1. Introduction

Let $a_i, b \in \mathbb{Z}$ for $i = 1, \dots k$ and $n, s \in \mathbb{N}$. Consider the linear congruence equation

$$a_1^s x_1 + \dots + a_k^s x_k \equiv b \,(\text{mod } n^s). \tag{1}$$

Such equations were considered by many authors who attempted to find either their solutions or the number of solutions. For the case $s = 1$, such an attempt was made by D.N. Lehmer [9] who proved that

Theorem 1.1. *Let $a_1, \dots, a_k, b, n \in \mathbb{Z}, n \geq 1$. The linear congruence equation*

$$a_1 x_1 + \dots + a_k x_k \equiv b \,(mod\ n)$$

has a solution $\langle x_1, \dots, x_n \rangle \in \mathbb{Z}_n^k$ if and only if $l|b$ where l is the gcd of $a_1, \dots, a_k, n$. Furthermore, if this condition is satisfied, then there are ln^{k-1} solutions.

Later the focus was shifted to solving the above type of congruence equations with some extra restrictions on the solutions x_i. One such restriction is requiring that the solutions should satisfy $gcd(x_i, n) = t_i \,(1 \leq i \leq k)$ where t_i are given positive divisors of n. A linear congruence with such restrictions is called to be a restricted linear congruence. These kind of restricted congruences were tried to solve by many authors some of which were special cases of the problem we are going to solve here. With $a_i = s = 1$ and restrictions $(x_i, n) = 1$, Rademacher [17] and Brauer [4] independently gave a formula for the number of solutions $N_n(k, b)$ of the congruence. An equivalent formula involving the Ramanujan sums was proved by Nicol and Vandiver [16], and E. Cohen [6]. The number of solutions given by them is

$$N_n(k, b) = \frac{1}{n} \sum_{d|n} c_d(b) \left(c_n \left(\frac{n}{d} \right) \right)^k \tag{2}$$

where $c_r(n)$ denote the usual Ramanujan sum.

The restricted congruence (1) (with $s = 1$) and their solutions has found interesting applications in various fields including number theory, cryptography, combinatorics, computer science etc. Liskovets defined a multivariate arithmetic function in [10]. The special case of our restricted congruence problem with $b = 0$ and $a_i = s = 1$ is related to this multivariate function. This function has many combinatorial as well as topological applications. In computer science, the restricted congruence problem has applications in studying universal hashing (see Bibak et al. [3]).

In [1] Bibak et al. considered the linear congruence (1) taking $a_i = s = 1$ and the restrictions $(x_i, n) = t_i$ where t_i are given positive divisors of n. This was later generalized for an arbitrary s with still requiring $a_i = 1$ by K V Namboothiri in [15]. It was proved there that

Please cite this article in press as: K.V. Namboothiri, On the number of solutions of a restricted linear congruence, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.01.013