Journal of Number Theory 171 (2017) 128–144

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Restricted linear congruences

Khodakhast Bibak [a,*], Bruce M. Kapron [a], Venkatesh Srinivasan [a,b], Roberto Tauraso [c], László Tóth [d]

[a] *Department of Computer Science, University of Victoria, Victoria, BC, Canada, V8W 3P6*
[b] *Centre for Quantum Technologies, National University of Singapore, Singapore, 117543*
[c] *Dipartimento di Matematica, Università di Roma "Tor Vergata", 00133 Roma, Italy*
[d] *Department of Mathematics, University of Pécs, 7624 Pécs, Hungary*

A R T I C L E   I N F O

Article history:
Received 26 March 2016
Accepted 1 July 2016
Available online 6 September 2016
Communicated by D. Goss

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

Keywords:
Restricted linear congruence
Ramanujan sum
Discrete Fourier transform

A B S T R A C T

In this paper, using properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions, we give an explicit formula for the number of solutions of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with $\gcd(x_i, n) = t_i$ ($1 \le i \le k$), where $a_1, t_1, \ldots, a_k, t_k, b, n$ ($n \ge 1$) are arbitrary integers. As a consequence, we derive necessary and sufficient conditions under which the above restricted linear congruence has no solutions. The number of solutions of this kind of congruence was first considered by Rademacher in 1925 and Brauer in 1926, in the special case of $a_i = t_i = 1$ ($1 \le i \le k$). Since then, this problem has been studied, in several other special cases, in many papers; in particular, Jacobson and Williams [*Duke Math. J.* 39 (1972) 521–527] gave a nice explicit formula for the number of such solutions when $(a_1, \ldots, a_k) = t_i = 1$ ($1 \le i \le k$). The problem is very well-motivated and has found intriguing applications in several areas of mathematics, computer science, and physics, and

* Corresponding author.
E-mail addresses: kbibak@uvic.ca (K. Bibak), bmkapron@uvic.ca (B.M. Kapron), srinivas@uvic.ca (V. Srinivasan), tauraso@mat.uniroma2.it (R. Tauraso), ltoth@gamma.ttk.pte.hu (L. Tóth).

http://dx.doi.org/10.1016/j.jnt.2016.07.018

there is promise for more applications/implications in these or other directions.

1. Introduction

Let $a_1, \ldots, a_k, b, n \in \mathbb{Z}$, $n \geq 1$. A linear congruence in k unknowns $x_1, \ldots, x_k$ is of the form

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

By a solution of (1.1) we mean an ordered k-tuple of integers modulo n, denoted by $\langle x_1, \ldots, x_k \rangle$, that satisfies (1.1). Let $(u_1, \ldots, u_m)$ denote the greatest common divisor (gcd) of $u_1, \ldots, u_m \in \mathbb{Z}$. The following result, proved by D. N. Lehmer [19], gives the number of solutions of the above linear congruence:

Proposition 1.1. *Let $a_1, \ldots, a_k, b, n \in \mathbb{Z}$, $n \geq 1$. The linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$ has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ if and only if $\ell \mid b$, where $\ell = (a_1, \ldots, a_k, n)$. Furthermore, if this condition is satisfied, then there are ℓn^{k-1} solutions.*

Interestingly, this classical result of D. N. Lehmer has been recently used [4] in introducing GMMH* which is a generalization of the well-known $\triangle$-universal hash function family, MMH*.

The solutions of the above congruence may be subject to certain conditions, such as $\gcd(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of n. The number of solutions of this kind of congruence, we call it *restricted linear congruence*, was investigated in special cases by several authors. It was shown by Rademacher [29] in 1925 and Brauer [7] in 1926 that the number $N_n(k, b)$ of solutions of the congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$ with the restrictions $(x_i, n) = 1$ $(1 \leq i \leq k)$ is

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

where $\varphi(n)$ is Euler's totient function and the products are taken over all prime divisors p of n. This result was rediscovered later by Dixon [13] and Rearick [31]. The equivalent formula

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

involving the Ramanujan sums $c_n(m)$ (see Section 2.1) was obtained by Nicol and Vandiver [28, Th. VII] and reproved by Cohen [8, Th. 6].