Restricted linear congruences

Khodakhast Bibak [*] Bruce M. Kapron [*] Venkatesh Srinivasan [*†]
Roberto Tauraso [‡] László Tóth [§]

August 29, 2016

Abstract

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 $\gcd(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$ 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 $a_i = t_i = 1$ $(1 \leq i \leq k)$. 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 $(a_1, \ldots, a_k) = t_i = 1$ $(1 \leq i \leq k)$. The problem is very well-motivated and has found intriguing applications in several areas of mathematics, computer science, and physics, and there is promise for more applications/implications in these or other directions.

Keywords: Restricted linear congruence; Ramanujan sum; discrete Fourier transform

2010 Mathematics Subject Classification: 11D79, 11P83, 11L03, 11A25, 42A16

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

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}. \tag{1.1}$$

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:

[*]Department of Computer Science, University of Victoria, Victoria, BC, Canada V8W 3P6. Email: {kbibak,bmkapron,srinivas}@uvic.ca

[†]Centre for Quantum Technologies, National University of Singapore, Singapore 117543.

[‡]Dipartimento di Matematica, Università di Roma "Tor Vergata", 00133 Roma, Italy. Email: tauraso@mat.uniroma2.it

[§]Department of Mathematics, University of Pécs, 7624 Pécs, Hungary. Email: ltoth@gamma.ttk.pte.hu

Proposition 1.1. *Let $a_1, \ldots, a_k, b, n \in \mathbb{Z}$, $n \geq 1$. The linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$ 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

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

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

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

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].

The special case of $k = 2$ was treated, independently, by Alder [1], Deaconescu [11], and Sander [32]. For $k = 2$ the function $N_n(2, b)$ coincides with Nagell's totient function ([27]) defined to be the number of integers $x \pmod{n}$ such that $(x, n) = (b - x, n) = 1$. From (1.2) one easily gets

$$N_n(2,b) = n \prod_{p \,|\, n, p \,|\, b} \left(1 - \frac{1}{p}\right) \prod_{p \,|\, n, p \nmid b} \left(1 - \frac{2}{p}\right). \tag{1.4}$$

From (1.4) it is clear that $N_n(2, 0) = \varphi(n)$ and

$$N_n(2,1) = n \prod_{p \,|\, n} \left(1 - \frac{2}{p}\right). \tag{1.5}$$

Interestingly, the function $N_n(2, 1)$ was applied by D. N. Lehmer [20] in studying certain magic squares. It is also worth mentioning that the case of $k = 2$ is related to a long-standing conjecture due to D. H. Lehmer from 1932 (see [11, 12]), and also has interesting applications to Cayley graphs (see [32, 33]).

The problem in the case of k variables can be interpreted as a 'restricted partition problem modulo n' ([28]), or an equation in the ring $\mathbb{Z}_n$, where the solutions are its units ([11, 32, 33]).

More generally, it has connections to studying rings generated by their units, in particular in finding the number of representations of an element of a finite commutative ring, say R, as the sum of k units in R; see [17] and the references therein. The results of Ramanathan [30, Th. 5 and 6] are similar to (1.2) and (1.3), but in another context. See also McCarthy [22, Ch. 3] and Spilker [35] for further results with these and different restrictions on linear congruences.

The general case of the restricted linear congruence

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}, \quad (x_i, n) = t_i \ (1 \le i \le k), \tag{1.6}$$

was considered by Sburlati [34]. A formula for the number of solutions of (1.6) was deduced in [34, Eq. (4), (5)] with some assumptions on the prime factors of n with respect to the values a_i, t_i $(1 \le i \le k)$ and with an incomplete proof. The special cases of $k = 2$ with $t_1 = t_2 = 1$, and $a_i = 1$ $(1 \le i \le k)$ of (1.6) were considered, respectively, by Sander and Sander [33], and Sun and Yang [36]. Cohen [10, Th. 4, 5] derived two explicit formulas for the number of solutions of (1.6) with $t_i = 1$, $a_i \mid n$, a_i prime $(1 \le i \le k)$. Jacobson and Williams [16] gave a nice explicit formula for the number of such solutions when $(a_1, \ldots, a_k) = t_i = 1$ $(1 \le i \le k)$. Also, the special case of $b = 0$, $a_i = 1$, $t_i = \frac{n}{m_i}$, $m_i \mid n$ $(1 \le i \le k)$ is related to the *orbicyclic* (multivariate arithmetic) function ([21]), which has very interesting combinatorial and topological applications, in particular in counting non-isomorphic maps on orientable surfaces (see [3, 21, 23, 24, 37, 40]). The problem is also related to Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces; see Remark 3.14.

The above general case of the restricted linear congruence (1.6) can be considered as relevant to the generalized knapsack problem (see Remark 3.12). The *knapsack problem* is of significant interest in cryptography, computational complexity, and several other areas. Micciancio [25] proposed a generalization of this problem to arbitrary rings, and studied its average-case complexity. This *generalized knapsack problem*, proposed by Micciancio [25], is described as follows: for any ring R and subset $S \subset R$, given elements $a_1, \ldots, a_k \in R$ and a target element $b \in R$, find $\langle x_1, \ldots, x_k \rangle \in S^k$ such that $\sum_{i=1}^{k} a_i \cdot x_i = b$, where all operations are performed in the ring.

In the one variable case, Alomair et al. [2], motivated by applications in designing an authenticated encryption scheme, gave a necessary and sufficient condition (with a long proof) for the congruence $ax \equiv b \pmod{n}$, with the restriction $(x, n) = 1$, to have a solution. Later, Grošek and Porubský [15] gave a short proof for this result, and also obtained a formula for the number of such solutions. In Theorem 3.1 (see Section 3) we deal with this problem in a more general form as a building block for the case of k variables $(k \ge 1)$.

In Section 3, we obtain an explicit formula for the number of solutions of the restricted linear congruence (1.6) for arbitrary integers $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \ge 1)$. Two major ingredients in our proofs are Ramanujan sums and the discrete Fourier transform (DFT) of arithmetic functions, of which properties are reviewed in Section 2. Bibak et al. [6] applied this explicit formula in constructing an almost-universal hash function family and gave some applications to authentication and secrecy codes.

2 Preliminaries

Throughout the paper we use $(a_1, \ldots, a_k)$ to denote the greatest common divisor (gcd) of $a_1, \ldots, a_k \in \mathbb{Z}$, and write $\langle a_1, \ldots, a_k \rangle$ for an ordered k-tuple of integers. Also, for $a \in \mathbb{Z} \setminus \{0\}$ and a prime p we use the notation $p^r \parallel a$ if $p^r \mid a$ and $p^{r+1} \nmid a$.

2.1 Ramanujan sums

Let $e(x) = \exp(2\pi i x)$ be the complex exponential with period 1, which satisfies for any $m, n \in \mathbb{Z}$ with $n \geq 1$,

$$\sum_{j=1}^{n} e\left(\frac{jm}{n}\right) = \begin{cases} n, & \text{if } n \mid m, \\ 0, & \text{if } n \nmid m. \end{cases} \tag{2.1}$$

For integers m and n with $n \geq 1$ the quantity

$$c_n(m) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\left(\frac{jm}{n}\right) \tag{2.2}$$

is called a *Ramanujan sum*. It is the sum of the m-th powers of the primitive n-th roots of unity, and is also denoted by $c(m, n)$ in the literature.

Even though the Ramanujan sum $c_n(m)$ is defined as a sum of some complex numbers, it is integer-valued (see Theorem 2.1 below). From (2.2) it is clear that $c_n(-m) = c_n(m)$. Clearly, $c_n(0) = \varphi(n)$, where $\varphi(n)$ is *Euler's totient function*. Also, by Theorem 2.1 or Theorem 2.3 (see below), $c_n(1) = \mu(n)$, where $\mu(n)$ is the *Möbius function* defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \text{ is not square-free}, \\ (-1)^{\kappa}, & \text{if } n \text{ is the product of } \kappa \text{ distinct primes}. \end{cases} \tag{2.3}$$

The following theorem, attributed to Kluyver [18], gives an explicit formula for $c_n(m)$:

Theorem 2.1. *For integers m and n, with $n \geq 1$,*

$$c_n(m) = \sum_{d \mid (m,n)} \mu\left(\frac{n}{d}\right) d. \tag{2.4}$$

Thus, $c_n(m)$ can be easily computed provided n can be factored efficiently. By applying the Möbius inversion formula, Theorem 2.1 yields the following property: For $m, n \geq 1$,

$$\sum_{d \mid n} c_d(m) = \begin{cases} n, & \text{if } n \mid m, \\ 0, & \text{if } n \nmid m. \end{cases} \tag{2.5}$$

The case $m = 1$ of (2.5) gives the *characteristic property* of the Möbius function:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases} \tag{2.6}$$

Note that Theorem 2.1 has several other important consequences:

Corollary 2.2. *Ramanujan sums enjoy the following properties:*

(i) For fixed $m \in \mathbb{Z}$ the function $n \mapsto c_n(m)$ is multiplicative, that is, if $(n_1, n_2) = 1$, then $c_{n_1 n_2}(m) = c_{n_1}(m) c_{n_2}(m)$. (Note that the function $m \mapsto c_n(m)$ is multiplicative for a fixed n if and only if $\mu(n) = 1$.) Furthermore, for every prime power p^r $(r \geq 1)$,

$$c_{p^r}(m) = \begin{cases} p^r - p^{r-1}, & \text{if } p^r \mid m, \\ -p^{r-1}, & \text{if } p^{r-1} \parallel m, \\ 0, & \text{if } p^{r-1} \nmid m. \end{cases} \tag{2.7}$$

(ii) $c_n(m)$ is integer-valued.

(iii) $c_n(m)$ is an even function of $m \pmod n$, that is, $c_n(m) = c_n((m, n))$, for every m, n.

The *von Sterneck number* ([39]) is defined by

$$\Phi(m, n) = \frac{\varphi(n)}{\varphi\left(\frac{n}{(m,n)}\right)} \mu\left(\frac{n}{(m, n)}\right). \tag{2.8}$$

A crucial fact in studying Ramanujan sums and their applications is that they coincide with the von Sterneck number. This result is known as *von Sterneck's formula* and is attributed to Kluyver [18]:

Theorem 2.3. *For integers m and n, with $n \geq 1$, we have*

$$\Phi(m, n) = c_n(m). \tag{2.9}$$

Ramanujan sums satisfy several important *orthogonality properties*. One of them is the following identity:

Theorem 2.4. ([9]) *If $n \geq 1$, $d_1 \mid n$, and $d_2 \mid n$, then we have*

$$\sum_{d \mid n} c_{d_1}\left(\frac{n}{d}\right) c_d\left(\frac{n}{d_2}\right) = \begin{cases} n, & \text{if } d_1 = d_2, \\ 0, & \text{if } d_1 \neq d_2. \end{cases} \tag{2.10}$$

We close this subsection by mentioning that, very recently, Fowler et al. [14] showed that many properties of Ramanujan sums can be deduced (with very short proofs!) using the theory of *supercharacters* (from group theory), recently developed by Diaconis-Isaacs and André.

2.2 The discrete Fourier transform

A function $f : \mathbb{Z} \to \mathbb{C}$ is called *periodic* with period n (also called *n-periodic* or *periodic modulo n*) if $f(m + n) = f(m)$, for every $m \in \mathbb{Z}$. In this case f is determined by the finite vector $(f(1), \ldots, f(n))$. From (2.2) it is clear that $c_n(m)$ is a periodic function of m with period n.

We define the *discrete Fourier transform* (DFT) of an n-periodic function f as the function $\widehat{f} = \mathcal{F}(f)$, given by

$$\widehat{f}(b) = \sum_{j=1}^{n} f(j) e\left(\frac{-bj}{n}\right) \quad (b \in \mathbb{Z}). \tag{2.11}$$

The standard representation of f is obtained from the Fourier representation $\widehat{f}$ by

$$f(b) = \frac{1}{n} \sum_{j=1}^{n} \widehat{f}(j) e\left(\frac{bj}{n}\right) \quad (b \in \mathbb{Z}), \tag{2.12}$$

which is the *inverse discrete Fourier transform* (IDFT); see, e.g., [26, p. 109].

The *Cauchy convolution* of the n-periodic functions f_1 and f_2 is the n-periodic function $f_1 \otimes f_2$ defined by

$$(f_1 \otimes f_2)(m) = \sum_{\substack{1 \le x_1, x_2 \le n \\ x_1 + x_2 \equiv m \pmod{n}}} f_1(x_1) f_2(x_2) = \sum_{x=1}^{n} f_1(x) f_2(m-x) \quad (m \in \mathbb{Z}).$$

It is well known that

$$\widehat{f_1 \otimes f_2} = \widehat{f_1}\,\widehat{f_2},$$

with pointwise multiplication. More generally, if $f_1, \ldots, f_k$ are n-periodic functions, then

$$\mathcal{F}(f_1 \otimes \cdots \otimes f_k) = \mathcal{F}(f_1) \cdots \mathcal{F}(f_k). \tag{2.13}$$

For $t \mid n$, let $\varrho_{n,t}$ be the n-periodic function defined for every $m \in \mathbb{Z}$ by

$$\varrho_{n,t}(m) = \begin{cases} 1, & \text{if } (m,n) = t, \\ 0, & \text{if } (m,n) \neq t. \end{cases}$$

We will need the next two results. The first one is a direct consequence of the definitions.

Theorem 2.5. *For every $t \mid n$,*

$$\widehat{\varrho_{n,t}}(m) = c_{\frac{n}{t}}(m) \quad (m \in \mathbb{Z}),$$

in particular, the Ramanujan sum $m \mapsto c_n(m)$ is the DFT of the function $m \mapsto \varrho_{n,1}(m)$.

As already mentioned in Corollary 2.2(iii), a function $f : \mathbb{Z} \to \mathbb{C}$ is called n-even, or even (mod n), if $f(m) = f((m,n))$, for every $m \in \mathbb{Z}$. Clearly, if a function f is n-even, then it is n-periodic. The Ramanujan sum $m \mapsto c_n(m)$ is an example of an n-even function.

Theorem 2.6. ([38, Prop. 2]) *If f is an n-even function, then*

$$\widehat{f}(m) = \sum_{d \,|\, n} f(d) c_{\frac{n}{d}}(m) \quad (m \in \mathbb{Z}).$$

Proof. Group the terms of (2.11) according to the values $d = (m,n)$, taking into account the definition of the n-even functions. □

3 Linear congruences with $(x_i, n) = t_i$ $(1 \le i \le k)$

In this section, using properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions, we derive an explicit formula for the number of solutions of the restricted linear congruence (1.6) for arbitrary integers $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \ge 1)$.

Let us start with the case that we have only one variable; this is a building block for the case of k variables $(k \ge 1)$. The following theorem generalizes the main result of [15], one of the main results of [2], and also a key lemma in [28] (Lemma 1).

Theorem 3.1. *Let a, b, $n \ge 1$ and $t \ge 1$ be given integers. The congruence $ax \equiv b \pmod{n}$ has solution(s) x with $(x, n) = t$ if and only if $t \mid (b, n)$ and $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right)$. Furthermore, if these conditions are satisfied, then there are exactly*

$$\frac{\varphi\left(\frac{n}{t}\right)}{\varphi\left(\frac{n}{td}\right)} = d \prod_{\substack{p \mid d \\ p \nmid \frac{n}{td}}} \left(1 - \frac{1}{p}\right) \tag{3.1}$$

solutions, where p ranges over the primes and $d = \left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right)$.

Proof. Assume that there is a solution x satisfying $ax \equiv b \pmod{n}$ and $(x, n) = t$. Then $(ax, n) = (b, n) = td$, for some d. Thus, $t \mid (b, n)$ and $\left(\frac{ax}{t}, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right) = d$. But since $\left(\frac{x}{t}, \frac{n}{t}\right) = 1$, we have $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right) = d$.

Now, let $t \mid (b, n)$ and $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right) = d$. Let us denote $A = \frac{a}{d}$, $B = \frac{b}{dt}$, $N = \frac{n}{dt}$. Then $(A, N) = (B, N) = 1$. Since $(A, N) = 1$, the congruence $Ay \equiv B \pmod{N}$ has a unique solution $y_0 = A^{-1}B$ modulo N and $(Ay_0, N) = (B, N)$, that is $(y_0, N) = 1$. It follows that $a(ty_0) \equiv b \pmod{n}$, which shows that $x_0 = ty_0$ is a solution of $ax \equiv b \pmod{n}$.

If x is such that $ax \equiv b \pmod{n}$ and $(x, n) = t$, then $x = ty$ and $Ay \equiv B \pmod{N}$. Hence, all solutions of the congruence $ax \equiv b \pmod{n}$ with $(x, n) = t$ have the form $x = t(y_0 + kN)$, where $0 \le k \le d-1$ and $\left(y_0 + kN, \frac{n}{t}\right) = 1$. Since $(y_0, N) = 1$, the latter condition is equivalent to $(y_0 + kN, d) = 1$. The number S of such solutions, using the characteristic property (2.6) of the Möbius function, is

$$\begin{aligned} S &= \sum_{\substack{0 \le k \le d-1 \\ (y_0 + kN, d) = 1}} 1 \\ &= \sum_{0 \le k \le d-1} \sum_{\delta \mid (y_0 + kN, d)} \mu(\delta) \\ &= \sum_{\delta \mid d} \mu(\delta) \sum_{\substack{0 \le k \le d-1 \\ \delta \mid y_0 + kN}} 1 = \sum_{\delta \mid d} \mu(\delta) \sum_{\substack{0 \le k \le d-1 \\ kN \equiv -y_0 \pmod{\delta}}} 1. \end{aligned}$$

Here, if $v = (N, \delta) > 1$, then $v \nmid y_0$ since $(y_0, N) = 1$. Thus, the congruence $kN \equiv -y_0 \pmod{\delta}$ has no solution in k and the inner sum is zero. If $(N, \delta) = 1$, then the same congruence has one solution in $k \pmod{\delta}$ and it has $\frac{d}{\delta}$ solutions $(\bmod d)$. Therefore,

$$S = \sum_{\substack{\delta \mid d \\ (\delta, N) = 1}} \mu(\delta) \frac{d}{\delta} = d \prod_{\substack{p \mid d \\ p \nmid N}} \left(1 - \frac{1}{p}\right) = \frac{\varphi(Nd)}{\varphi(N)} = \frac{\varphi\left(\frac{n}{t}\right)}{\varphi\left(\frac{n}{td}\right)}.$$

The proof is now complete. □

Remark 3.2. *In [2] the authors only prove the first part of Theorem 3.1 in the case of* $t = 1$*, and apply the result in checking the integrity of their authenticated encryption scheme ([2]). Their main result, [2, Th. 5.11], is obtained via a very long argument; however, formula* (3.1) *alone gives a one-line proof for [2, Th. 5.11] that we omit here.*

Corollary 3.3. *The congruence* $ax \equiv b \pmod{n}$ *has exactly one solution* x *with* $(x, n) = t$ *if and only if one of the following two cases holds:*
(i) $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right) = 1$*, where* $t \mid (b, n)$*;*
(ii) $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right) = 2$*, where* $t \mid b$*,* $n = 2^r u$*,* $r \geq 1$*,* $u \geq 1$ *odd,* $t = 2^{r-1}v$*,* $v \mid u$*.*

Proof. Let $d = \left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right)$. If $d = 1$, then (3.1) shows that there is one solution. Now for $d > 1$ it is enough to consider the case when $d = p^j$ $(j \geq 1)$ is a prime power. Let $p^r \parallel n$, $p^s \parallel t$ with $0 \leq j + s \leq r$. Then, by (3.1), there is one solution if $p^j \left(1 - \frac{1}{p}\right) = 1$ provided that $p \nmid p^{r-s-j}$. This holds only in the case $p = 2$, $j = 1$, $s + j = r$. This gives $d = 2$ together with the conditions formulated in (ii). □

We remark that Corollary 3.3, in the case of $t = 1$, was obtained in [15, Cor. 4].

Now we deal with the case of k variables $(k \geq 1)$. Assume $a_1, \ldots, a_k, b$ are fixed and let $N_n(t_1, \ldots, t_k)$ denote the number of incongruent solutions of (1.6). We note the following multiplicativity property: If $n, m \geq 1$, $(n, m) = 1$, then

$$N_{nm}(t_1, \ldots, t_k) = N_n(u_1, \ldots, u_k) N_m(v_1, \ldots, v_k), \tag{3.2}$$

with unique u_i, v_i such that $t_i = u_i v_i$, $u_i \mid n$, $v_i \mid m$ $(1 \leq i \leq k)$. This can be easily shown by the Chinese remainder theorem. Therefore, it would be enough to obtain $N_n(t_1, \ldots, t_k)$ in the case $n = p^r$, a prime power. However, we prefer to derive the next compact results, which are valid for an arbitrary positive integer n.

In the case that $a_i = 1$ $(1 \leq i \leq k)$, we prove the following result:

Theorem 3.4. *Let* b*,* $n \geq 1$*,* $t_i \mid n$ $(1 \leq i \leq k)$ *be given integers. The number of solutions of the linear congruence* $x_1 + \cdots + x_k \equiv b \pmod{n}$*, with* $(x_i, n) = t_i$ $(1 \leq i \leq k)$*, is*

$$N_n(b; t_1, \ldots, t_k) = \frac{1}{n} \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} c_{\frac{n}{t_i}}\left(\frac{n}{d}\right) \geq 0. \tag{3.3}$$

Proof. Apply the properties of the DFT. Observe that

$$(\varrho_{n,t_1} \otimes \cdots \otimes \varrho_{n,t_k})(b) = \sum_{\substack{1 \leq x_1, \ldots, x_k \leq n \\ x_1 + \ldots + x_k \equiv b \pmod{n} \\ (x_i, n) = t_i,\ 1 \leq i \leq k}} 1$$

is exactly the number $N_n(b; t_1, \ldots, t_k)$ of solutions of the given restricted congruence.

Therefore, by (2.13) and Theorem 2.5,

$$\widehat{N_n}(b; t_1, \ldots, t_k) = c_{\frac{n}{t_1}}(b) \cdots c_{\frac{n}{t_k}}(b),$$

where the variable for the DFT is b ($n, t_1, \ldots, t_k$ being parameters). Now the IDFT formula (2.12) gives

$$N_n(b; t_1, \ldots, t_k) = \frac{1}{n} \sum_{j=1}^{n} c_{\frac{n}{t_1}}(j) \cdots c_{\frac{n}{t_k}}(j) e\left(\frac{bj}{n}\right).$$

By Corollary 2.2(iii) and the associativity of gcd one has for every i ($1 \le i \le k$),

$$c_{\frac{n}{t_i}}((j,n)) = c_{\frac{n}{t_i}}\left(\left((j,n), \frac{n}{t_i}\right)\right) = c_{\frac{n}{t_i}}\left(\left(j, \left(n, \frac{n}{t_i}\right)\right)\right) = c_{\frac{n}{t_i}}\left(\left(j, \frac{n}{t_i}\right)\right) = c_{\frac{n}{t_i}}(j). \quad (3.4)$$

The properties (3.4) show that $m \mapsto c_{\frac{n}{t_1}}(m) \cdots c_{\frac{n}{t_k}}(m)$ is an n-even function. Now by applying Theorem 2.6 we obtain (3.3). □

Remark 3.5. *Note that a slight modification of the proof of [37, Prop. 21] furnishes an alternate proof for Theorem 3.4. Sun and Yang [36] obtained a different formula (with a longer proof) for the number of solutions of the linear congruence in Theorem 3.4, but we need the equivalent formula* (3.3) *for the purposes of this paper (see also [5] for another equivalent formula). We also remark that the special case of $b = 0$, $t_i = \frac{n}{m_i}$, $m_i \mid n$ $(1 \le i \le k)$ gives the function*

$$E(m_1, \ldots, m_k) = \frac{1}{n} \sum_{d \mid n} \varphi(d) \prod_{i=1}^{k} c_{m_i}\left(\frac{n}{d}\right),$$

which was shown in [37, Prop. 9] to be equivalent to the orbicyclic (multivariate arithmetic) function defined in [21] by

$$E(m_1, \ldots, m_k) := \frac{1}{n} \sum_{q=1}^{n} \prod_{i=1}^{k} c_{m_i}(q).$$

The orbicyclic function, $E(m_1, \ldots, m_k)$, has very interesting combinatorial and topological applications, in particular, in counting non-isomorphic maps on orientable surfaces, and was investigated in [3, 21, 23, 37]. See also [24, 40].

Now, using Theorem 3.1 and Theorem 3.4, we obtain the following general formula for the number of solutions of the restricted linear congruence (1.6).

Theorem 3.6. *Let $a_i, t_i, b, n \in \mathbb{Z}$, $n \ge 1$, $t_i \mid n$ $(1 \le i \le k)$. The number of solutions of the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \le i \le k)$, is*

$$N_n(b; a_1, t_1, \ldots, a_k, t_k) = \frac{1}{n} \left(\prod_{i=1}^{k} \frac{\varphi\left(\frac{n}{t_i}\right)}{\varphi\left(\frac{n}{t_i d_i}\right)} \right) \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} c_{\frac{n}{t_i d_i}}\left(\frac{n}{d}\right) \quad (3.5)$$

$$= \frac{1}{n} \left(\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \right) \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} \frac{\mu\left(\frac{d}{(a_i t_i, d)}\right)}{\varphi\left(\frac{d}{(a_i t_i, d)}\right)}, \quad (3.6)$$

where $d_i = (a_i, \frac{n}{t_i})$ $(1 \le i \le k)$.

Proof. Assume that the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod n$ has a solution $\langle x_1, \ldots, x_k\rangle \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i$ $(1 \le i \le k)$. Let $a_ix_i \equiv y_i \pmod n$ $(1 \le i \le k)$. Then $(a_ix_i, n) = (y_i, n) = t_id_i$, for some d_i $(1 \le i \le k)$. Thus, $(\frac{a_ix_i}{t_i}, \frac{n}{t_i}) = (\frac{y_i}{t_i}, \frac{n}{t_i}) = d_i$. But since $(\frac{x_i}{t_i}, \frac{n}{t_i}) = 1$, we have $d_i = (a_i, \frac{n}{t_i}) = (\frac{y_i}{t_i}, \frac{n}{t_i})$.

By Theorem 3.4, the number of solutions of the linear congruence $y_1 + \cdots + y_k \equiv b \pmod n$, with $(y_i, n) = t_id_i$ $(1 \le i \le k)$, is

$$\frac{1}{n}\sum_{d\,|\,n} c_d(b)\prod_{i=1}^{k} c_{\frac{n}{t_id_i}}\Big(\frac{n}{d}\Big)\,. \tag{3.7}$$

Now, given the solutions $\langle y_1, \ldots, y_k\rangle$ of the latter congruence, we need to find the number of solutions of $a_ix_i \equiv y_i \pmod n$, with $(x_i, n) = t_i$ $(1 \le i \le k)$. Since $(a_i, \frac{n}{t_i}) = (\frac{y_i}{t_i}, \frac{n}{t_i}) = d_i$, by Theorem 3.1, the latter congruence has exactly

$$\frac{\varphi(\frac{n}{t_i})}{\varphi(\frac{n}{t_id_i})} \tag{3.8}$$

solutions. Combining (3.7) and (3.8) we get the formula (3.5).

Furthermore, applying von Sterneck's formula, (2.9), we deduce

$$c_{\frac{n}{t_id_i}}\Big(\frac{n}{d}\Big) = \frac{\varphi(\frac{n}{t_id_i})\mu(w_i)}{\varphi(w_i)}, \tag{3.9}$$

where, denoting by $[a, b]$ the least common multiple (lcm) of the integers a and b,

$$w_i = \frac{\frac{n}{t_id_i}}{(\frac{n}{t_id_i}, \frac{n}{d})} = \frac{\frac{n}{t_id_i}}{\frac{n}{[t_id_i, d]}} = \frac{[t_id_i, d]}{t_id_i} = \frac{d}{(t_id_i, d)} = \frac{d}{((a_it_i, n), d)} = \frac{d}{(a_it_i, d)}.$$

By inserting (3.9) into (3.5) we get (3.6). □

Remark 3.7. *For fixed* a_i, t_i $(1 \le i \le k)$ *and fixed* n*, the function*

$$b \mapsto N_n(b; a_1, t_1, \ldots, a_k, t_k)$$

is an even function (*mod* n)*. This follows from the formula* (3.5)*, showing that*

$$N_n(b; a_1, t_1, \ldots, a_k, t_k)$$

is a linear combination of the functions $b \mapsto c_d(b)$ $(d \mid n)$*, which are all even* (*mod* n) *by* (2.4)*. See also* (3.4)*.*

Remark 3.8. *In the case of* $k = 1$*, by comparing Theorem 3.1 with formula* (3.5) *and by denoting* $t_1d_1 = s$*, we obtain, as a byproduct, the following identity, which is similar to* (2.10) (*and can also be proved directly*)*: If* $b, n \in \mathbb{Z}$*,* $n \ge 1$*, and* $s \mid n$*, then*

$$\sum_{d\,|\,n} c_d(b)c_{\frac{n}{s}}\Big(\frac{n}{d}\Big) = \begin{cases} n, & \text{if } (b, n) = s, \\ 0, & \text{if } (b, n) \ne s. \end{cases} \tag{3.10}$$

If in (1.6) one has $a_i = 0$ for every $1 \le i \le k$, then clearly there are solutions $\langle x_1, \dots, x_k \rangle$ if and only if $b \equiv 0 \pmod{n}$ and $t_i \mid n$ $(1 \le i \le k)$, and in this case there are $\varphi(n/t_1) \cdots \varphi(n/t_k)$ solutions.

Consider the restricted linear congruence (1.6) and assume that there is an i_0 such that $a_{i_0} \neq 0$. For every prime divisor p of n let r_p be the exponent of p in the prime factorization of n and let m_p denote the smallest $j \ge 1$ such that there is some i with $p^j \nmid a_i t_i$. There exists a finite m_p for every p, since for a sufficiently large j one has $p^j \nmid a_{i_0} t_{i_0}$. Furthermore, let

$$e_p = \#\{i : 1 \le i \le k, p^{m_p} \nmid a_i t_i\}.$$

By definition, e_p is at most the number of i such that $a_i \neq 0$.

Theorem 3.9. *Let $a_i, t_i, b, n \in \mathbb{Z}$, $n \ge 1$, $t_i \mid n$ $(1 \le i \le k)$ and assume that $a_i \neq 0$ for at least one i. Consider the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \le i \le k)$. If there is a prime $p \mid n$ such that $m_p \le r_p$ and $p^{m_p - 1} \nmid b$ or $m_p \ge r_p + 1$ and $p^{r_p} \nmid b$, then the linear congruence has no solution. Otherwise, the number of solutions is*

$$\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ m_p \le r_p \\ p^{m_p} \mid b}} p^{m_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \prod_{\substack{p \mid n \\ m_p \le r_p \\ p^{m_p - 1} \parallel b}} p^{m_p - r_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right), \tag{3.11}$$

where the last two products are over the prime factors p of n with the given additional properties. Note that the last product is empty and equal to 1 if $b = 0$.

Proof. For a prime power $n = p^{r_p}$ $(r_p \ge 1)$ the inner sum of (3.6) is

$$W := \sum_{d \mid p^{r_p}} c_d(b) \prod_{i=1}^{k} \frac{\mu\left(\frac{d}{(a_i t_i, d)}\right)}{\varphi\left(\frac{d}{(a_i t_i, d)}\right)} = \sum_{j=0}^{r_p} c_{p^j}(b) \prod_{i=1}^{k} \frac{\mu\left(\frac{p^j}{(a_i t_i, p^j)}\right)}{\varphi\left(\frac{p^j}{(a_i t_i, p^j)}\right)}.$$

Assume that $m_p \le r_p$. Then $p^{m_p - 1} \mid a_i t_i$ for every i and $p^{m_p} \nmid a_i t_i$ for at least one i. Therefore, $(a_i t_i, p^j) = p^j$ if $0 \le j \le m_p - 1$. Also, $(a_i t_i, p^{m_p}) = p^{m_p - 1}$ if $p^{m_p} \nmid a_i t_i$, and this holds for e_p distinct values of i. We obtain

$$W = \sum_{j=0}^{m_p - 1} c_{p^j}(b) + c_{p^{m_p}}(b) \frac{(-1)^{e_p}}{(p-1)^{e_p}},$$

the other terms are zero. We deduce by using (2.5) and (2.7) that

$$W = \begin{cases} p^{m_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right), & \text{if } p^{m_p} \mid b, \\ p^{m_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right), & \text{if } p^{m_p - 1} \parallel b, \\ 0, & \text{if } p^{m_p - 1} \nmid b. \end{cases} \tag{3.12}$$

Now assume that $m_p \geq r_p + 1$. Then $p^{r_p} \mid a_i t_i$ for every i and $(a_i t_i, p^j) = p^j$ for every j with $0 \leq j \leq r_p$. Hence, by using (2.5),

$$W = \sum_{j=1}^{r_p} c_{p^j}(b) = \begin{cases} p^{r_p}, & \text{if } p^{r_p} \mid b, \\ 0, & \text{if } p^{r_p} \nmid b. \end{cases}$$

Inserting into (3.6) and by using the multiplicativity property (3.2) we deduce that there is no solution in the specified cases. Otherwise, the number of solutions is given by

$$\prod_{p \mid n} p^{-r_p} \prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ m_p \geq r_p+1 \\ p^{r_p} \mid b}} p^{r_p} \prod_{\substack{p \mid n \\ m_p \leq r_p \\ p^{m_p} \mid b}} p^{m_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right)$$

$$\times \prod_{\substack{p \mid n \\ m_p \leq r_p \\ p^{m_p - 1} \parallel b}} p^{m_p - r_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right),$$

where the multiplicativity property is also applied to the product of the φ factors. This gives (3.11). □

Corollary 3.10. *The restricted congruence given in Theorem 3.9 has no solutions if and only if one of the following cases holds:*

(i) there is a prime $p \mid n$ with $m_p \leq r_p$ and $p^{m_p - 1} \nmid b$;

(ii) there is a prime $p \mid n$ with $m_p \geq r_p + 1$ and $p^{r_p} \nmid b$;

(iii) there is a prime $p \mid n$ with $m_p \leq r_p$, $e_p = 1$ and $p^{m_p} \mid b$;

(iv) n is even, $m_2 \leq r_2$, e_2 is odd and $2^{m_2} \mid b$;

(v) n is even, $m_2 \leq r_2$, e_2 is even and $2^{m_2 - 1} \parallel b$.

Proof. Use the first part of Theorem 3.9 and examine the conditions under which the factors of the products in (3.11) vanish. □

Example 3.11.

1) Consider $2x_1 + x_2 + 2x_3 \equiv 12 \pmod{24}$, with $(x_1, 24) = 3$, $(x_2, 24) = 2$, $(x_3, 24) = 4$.
Here $24 = 2^3 \cdot 3$,
$2 \mid a_1 t_1 = 6$, $2 \mid a_2 t_2 = 2$, $2 \mid a_3 t_3 = 8$,
$2^2 \nmid a_1 t_1 = 6$, $2^2 \nmid a_2 t_2 = 2$, $2^2 \mid a_3 t_3 = 8$, hence $e_2 = 2$ and $m_2 = 2$, also $2^2 \mid b = 12$,
$3 \mid a_1 t_1 = 6$, $3 \nmid a_2 t_2 = 2$, $3 \nmid a_3 t_3 = 8$, hence $e_3 = 2$, $m_3 = 1$, also $3^1 \mid b = 12$.
The number of solutions is

$$N = \varphi(24/3)\varphi(24/2)\varphi(24/4) 2^{2-3-1} \left(1 - \frac{(-1)^{2-1}}{(2-1)^{2-1}}\right) 3^{1-1-1} \left(1 - \frac{(-1)^{2-1}}{(3-1)^{2-1}}\right) = 8.$$

2) Now let $2x_1 + x_2 + 2x_3 \equiv 4 \pmod{24}$, with $(x_1, 24) = 3$, $(x_2, 24) = 2$, $(x_3, 24) = 4$, where only b is changed.

Here $2^2 \mid b = 4$, $3^{1-1} \parallel b = 4$.

The number of solutions is

$$N = \varphi(24/3)\varphi(24/2)\varphi(24/4)2^{2-3-1}\left(1 - \frac{(-1)^{2-1}}{(2-1)^{2-1}}\right)3^{1-1-1}\left(1 - \frac{(-1)^2}{(3-1)^2}\right) = 4.$$

3) Let $2x_1 + x_2 + 2x_3 \equiv 5 \pmod{24}$, with $(x_1, 24) = 3$, $(x_2, 24) = 2$, $(x_3, 24) = 4$, again only b is changed.

Here $2^{2-1} \nmid b = 5$, hence, there are no solutions by Corollary 3.10(i). (Well, this is obvious, since all terms have to be even, but 5 is odd.)

4) Let $2x_1 + x_2 + 2x_3 \equiv 10 \pmod{24}$, with $(x_1, 24) = 3$, $(x_2, 24) = 2$, $(x_3, 24) = 4$, again only b is changed.

Here $2^{2-1} \parallel b = 10$, hence, there is no solution by Corollary 3.10(v).

We believe that Theorem 3.9 and Corollary 3.10 are strong tools and may lead to interesting applications/implications. For example, we can connect the restricted linear congruences to the generalized knapsack problem. In fact, Corollary 3.10 helps us to deal with this problem in a quite natural case:

Remark 3.12. *The generalized knapsack problem with $R = \mathbb{Z}_n$ and $S = \mathbb{Z}_n^*$ has no solutions if and only if one of the cases of Corollary 3.10 holds.*

Remark 3.13. *In [6], we applied Theorem 3.9 in constructing an almost-universal hash function family using which we gave a generalization of the authentication code with secrecy presented in [2].*

Remark 3.14. *Very recently, Bibak et al. [3] using Theorem 3.9 as the main ingredient proved an explicit and practical formula for the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group (see also [23]). This problem has important applications in combinatorics, geometry, string theory, and quantum field theory (QFT). As a consequence, they obtained an 'equivalent' form of Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces (see also [21]).*

Remark 3.15. *If $k = 1$ then $e_p = 1$ for every prime $p \mid n$, and it is easy to see that from Theorem 3.9 and Corollary 3.10 we reobtain Theorem 3.1.*

The following formula is a special case of Theorem 3.9 and was obtained by Sburlati [34] with an incomplete proof.

Corollary 3.16. *Assume that for every prime $p \mid n$ one has $m_p = 1$, that is $p \nmid a_i t_i$ for at least one $i \in \{1, \ldots, k\}$. Then the number of solutions of the restricted linear congruence* (1.6) *is*

$$\frac{1}{n}\prod_{i=1}^{k}\varphi\left(\frac{n}{t_i}\right)\prod_{p\,|\,n,\,p\,|\,b}\left(1 - \frac{(-1)^{e_p-1}}{(p-1)^{e_p-1}}\right)\prod_{p\,|\,n,\,p\nmid b}\left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right). \tag{3.13}$$

4 Concluding remarks

As we already mentioned, the problem of counting the number of solutions of the linear congruence $a_1x_1+\cdots+a_kx_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \leq i \leq k)$, is very well-motivated and has found intriguing applications in number theory, combinatorics, geometry, computer science, cryptography, string theory, and quantum field theory. In this paper, we obtained an explicit formula for the number of solutions of this linear congruence in its most general form, that is, for arbitrary integers $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$. As a consequence, we derived necessary and sufficient conditions under which the above restricted linear congruence has no solutions. As this problem has appeared in several areas in mathematics, computer science and physics, we believe that our formulas might lead to more applications/implications in these or other directions.

Acknowledgements

During the preparation of this work the first author was supported by a Fellowship from the University of Victoria (UVic Fellowship).

References

[1] H. L. Alder, A generalization of the Euler φ-function, *Amer. Math. Monthly* **65** (1958), 690–692.

[2] B. Alomair, A. Clark, and R. Poovendran, The power of primes: security of authentication based on a universal hash-function family, *J. Math. Cryptol.* **4** (2010), 121–148.

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

[4] K. Bibak, B. M. Kapron, and V. Srinivasan, MMH* with arbitrary modulus is always almost-universal, *Inform. Process. Lett.* **116** (2016), 481–483.

[5] K. Bibak, B. M. Kapron, and V. Srinivasan, On a restricted linear congruence, *Int. J. Number Theory* **12** (2016), DOI: 10.1142/S179304211650130X.

[6] K. Bibak, B. M. Kapron, V. Srinivasan, and L. Tóth, On an almost-universal hash function family with applications to authentication and secrecy codes, arXiv: 1507.02331.

[7] A. Brauer, Lösung der Aufgabe 30, Jber. Deutsch. Math.–Verein **35** (1926), 92–94.

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

[9] E. Cohen, An extension of Ramanujan's sums. II. Additive properties, *Duke Math. J.* **22** (1955), 543–550.

[10] E. Cohen, Representations of even functions (mod r). III. Special topics, *Duke Math. J.* **26** (1959), 491–500.

[11] M. Deaconescu, Adding units mod n, *Elem. Math.* **55** (2000), 123–127.

[12] M. Deaconescu, On the equation $m-1 = a\varphi(m)$, *Integers: Electron. J. Combin. Number Theory* **6** (2006), #A06.

[13] J. D. Dixon, A finite analogue of the Goldbach problem, *Canad. Math. Bull.* **3** (1960), 121–126.

[14] C. F. Fowler, S. R. Garcia, and G. Karaali, Ramanujan sums as supercharacters, *Ramanujan J.* **35** (2014), 205–241.

[15] O. Grošek and Š. Porubský, Coprime solutions to $ax \equiv b \pmod{n}$, *J. Math. Cryptol.* **7** (2013), 217–224.

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

[17] D. Kiani and M. Mollahajiaghaei, On the addition of units and non-units in finite commutative rings, *Rocky Mountain J. Math.* **45** (2015), 1887–1896.

[18] J. C. Kluyver, Some formulae concerning the integers less than n and prime to n, In *Proc. R. Neth. Acad. Arts Sci. (KNAW)* **9** (1906), 408–414.

[19] D. N. Lehmer, Certain theorems in the theory of quadratic residues, *Amer. Math. Monthly* **20** (1913), 151–157.

[20] D. N. Lehmer, On the congruences connected with certain magic squares, *Trans. Amer. Math. Soc.* **31** (1929), 529–551.

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

[22] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer-Verlag, (1986).

[23] A. Mednykh and R. Nedela, Enumeration of unrooted maps of a given genus, *J. Combin. Theory Ser. B* **96** (2006), 706–729.

[24] A. Mednykh and R. Nedela, Enumeration of unrooted hypermaps of a given genus, *Discrete Math.* **310** (2010), 518–526.

[25] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions, *Comput. Complexity* **16** (2007), 365–411.

[26] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory*, Cambridge University Press, (2006).

[27] T. Nagell, Verallgemeinerung eines Satzes von Schemmel, *Skr. Norske Vid.-Akad. Oslo, Math. Class, I* **13** (1923), 23–25.

[28] C. A. Nicol and 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.

[29] H. Rademacher, Aufgabe 30, Jber. Deutsch. Math.–Verein **34** (1925), 158.

[30] K. G. Ramanathan, Some applications of Ramanujan's trigonometrical sum $c_m(n)$, Proc. Indian Acad. Sci (A) **20** (1944), 62–69.

[31] D. Rearick, A linear congruence with side conditions, *Amer. Math. Monthly* **70** (1963), 837–840.

[32] J. W. Sander, On the addition of units and nonunits mod m, *J. Number Theory* **129** (2009), 2260–2266.

[33] J. W. Sander and T. Sander, Adding generators in cyclic groups, *J. Number Theory* **133** (2013), 705–718.

[34] G. Sburlati, Counting the number of solutions of linear congruences, *Rocky Mountain J. Math.* **33** (2003), 1487–1497.

[35] J. Spilker, Eine einheitliche Methode zur Behandlung einer linearen Kongruenz mit Nebenbedingungen, *Elem. Math.* **51** (1996), 107–116.

[36] C.-F. Sun and Q.-H. Yang, On the sumset of atoms in cyclic groups, *Int. J. Number Theory* **10** (2014), 1355–1363.

[37] L. Tóth, Some remarks on a paper of V. A. Liskovets, *Integers* **12** (2012), 97–111.

[38] L. Tóth and P. Haukkanen, The discrete Fourier transform of r-even functions, *Acta Univ. Sapientiae, Math.* **3** (2011), 5–25.

[39] R. D. von Sterneck, Ein Analogon zur additiven Zahlentheorie, *Sitzber, Akad. Wiss. Wien, Math. Naturw. Klasse* **111** (Abt. IIa) (1902), 1567–1601.

[40] T. R. Walsh, Counting maps on doughnuts, *Theoret. Comput. Sci.* **502** (2013), 4–15.