Restricted linear congruences and an authenticated encryption scheme

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

March 9, 2015

Abstract

In this paper, using properties of Ramanujan sums and of the finite 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 $(x_i, n) = t_i$ ($1 \leq i \leq k$), where $a_1, t_1, \ldots, a_k, t_k, b, n$ ($n \geq 1$) are arbitrary integers. Some special cases of this problem have been studied in many papers, and have found very interesting applications in number theory, combinatorics, and cryptography, among other areas. We also propose an authenticated encryption scheme, and using our explicit formula, analyze the integrity of this scheme.

Keywords: Restricted linear congruence; Ramanujan sum; finite Fourier transform; universal hashing; authenticated encryption

2010 Mathematics Subject Classification: 11D79, 11P83, 11L03, 11A25, 42A16, 94A60, 94A62

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

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}. \quad (1.1)$$

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). The following well-known result, proved by D. N. Lehmer [31], 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 $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$ has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ if and only if $\ell | b$, where $\ell = (a_1, \ldots, a_k, n)$. Furthermore, if this condition is satisfied, then there are $\ell n^{k-1}$ solutions.

The solutions of the above congruence may be subject to certain conditions, such as $(x_i, n) = t_i$, where $t_i$’s $(1 \leq i \leq k)$ are given positive integers. The number of solutions of these kinds of congruences, we call them restricted linear congruences, were investigated, in special cases, by several authors. It was shown by Rademacher [46] in 1925 and Brauer [8] 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

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

(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 [15] and Rearick [49]. The equivalent formula

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

(1.3)

involving the Ramanujan sums, $c_n(m)$, was obtained by Nicol and Vandiver [43, Th. VII] and reproved by Cohen [10, Th. 6].

The special case of $k = 2$ was treated, independently, by Alder [1], Deaconescu [12], and Sander [50]. For $k = 2$, the function $N_n(2, b)$ coincides with Nagell’s totient function $\varphi_2(n)$ defined to be the number of integers $x \pmod{n}$ such that $(x, n) = (b-x, n) = 1$. From (1.2), one easily gets

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

(1.4)

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

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

(1.5)

Interestingly, the function $N_n(2, 1)$ was applied, by D. N. Lehmer [32], 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, [12, 13]), and also has interesting applications to Cayley graphs (see, [50, 51]).

The problem in the case of $k$ variables can be considered as a ‘finite analogue of the Goldbach problem’ in the ring $\mathbb{Z}_n$ of residue classes modulo $n$ ([15]), and can also be viewed as a ‘restricted partition problem modulo $n$’ ([13]), or an equation in the ring $\mathbb{Z}_n$, where the solutions are its units ([12, 50, 51]). 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 $R$; which itself has close interaction with algebraic graph theory (see, [25] and the references therein). The results of Ramanathan [47, Th. 5 and 6] are similar to (1.2) and (1.3), but in another context. See also McCarthy [36, Ch. 3] and Spilker [55] for further results with these and different restrictions on linear congruences.

The general case of the restricted linear congruence

$$a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}, \quad (x_i, n) = t_i \quad (1 \leq i \leq k), \quad (1.6)$$

was considered by Sburlati [52]. A formula for the number of solutions of (1.6) was deduced in [52, Eq. (4), (5)] with some assumptions on the prime factors of $n$ with respect to the values $a_i, t_i \ (1 \leq i \leq k)$ and without a clear proof. The special cases of $k = 2$ with $t_1 = t_2 = 1$, and $a_i = 1 \ (1 \leq i \leq k)$, of (1.6) were considered, respectively, by Sander and Sander [51], and Sun and Yang [58]. Also, the special case of $b = 0$, $t_i = \frac{n}{m_i}, m_i | n \ (1 \leq i \leq k)$, is related to the orbicyclic (multivariate arithmetic) function ([33]), which has very interesting combinatorial and topological applications, in particular, in counting non-isomorphic maps on orientable surfaces (see, [33, 37, 38, 59, 65]).

The above general case of the restricted linear congruence, (1.6), can be considered as relevant to the generalized knapsack problem. The knapsack problem is of significant interest in cryptography, computational complexity, and several other areas. Micciancio [39] proposed a generalization of this problem to arbitrary rings, and studied the average-case complexity of it. This generalized knapsack problem, proposed by Micciancio [39], 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, Gröschek and Porubský [20] 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 ($k \geq 1$).

In Section 3 we obtain an explicit formula for the number of solutions of the restricted linear congruence (1.6) for arbitrary integers $a_1, t_1, \ldots, a_k, t_k, b, n \ (n \geq 1)$. Two major ingredients in our proofs are Ramanujan sums and the finite Fourier transform (FFT) of arithmetic functions, of which properties are reviewed in Section 2. In Section 4, we review universal hash functions, discovered by Carter and Wegman [9], and propose a generalization of this construction by allowing the keys, $x$'s, to be chosen from $\mathbb{Z}_n^*$. In Section 5, we generalize the authenticated encryption scheme proposed by Alomair et al [2] in a way which is also applicable to handle long messages; thereby obtaining a way to expand the message space. Then, using our explicit formula from Section 3, we analyze the integrity of this scheme.
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 \(p^r \mid | a\) if \(p^r \mid a\) and \(p^{r+1} \nmid a\).

2.1 Ramanujan sums

Let \(e(x) = \exp(2\pi ix)\) 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

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

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.

Ramanujan sums and some of their properties were certainly known before Ramanujan’s paper [48], as Ramanujan himself declared in [48]; nonetheless, probably the reason that these sums bear Ramanujan’s name is that “Ramanujan was the first to appreciate the importance of the sum and to use it systematically”, according to Hardy (see, [17] for a discussion about this).

Ramanujan sums have important applications in additive number theory, for example, in the context of the Hardy-Littlewood circle method, Waring’s problem, and sieve theory (see, e.g., [40] [42] [63] and the references therein). As a major result in this direction, one can mention Vinogradov’s theorem (in its proof, Ramanujan sums play a key role) stating that every sufficiently large odd integer is the sum of three primes, and so every sufficiently large even integer is the sum of four primes (see, e.g., [42] Chapter 8]. Ramanujan sums have also interesting applications in cryptography [34] [53], coding theory [18] [56], combinatorics [33] [37], graph theory [30] [35], signal processing [61] [62], physics [44] [45], and several other places.

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 [26], gives an explicit formula for \(c_n(m)\):
Theorem 2.1. For integers \( m \) and \( n \), with \( n \geq 1 \),
\[
c_n(m) = \sum_{d \mid (m,n)} \mu \left( \frac{n}{d} \right) d.
\] (2.4)

Thus, \( c_n(m) \) can be easily computed provided \( n \) can be factored efficiently. One can compare (2.4) with the formula
\[
\varphi(n) = \sum_{d \mid n} \mu \left( \frac{n}{d} \right) d.
\] (2.5)

By applying the Möbius inversion formula, Theorem 2.1 yields the following property: For \( m, n \geq 1 \),
\[
\sum_{d \mid n} c_d(m) = \begin{cases} n, & \text{if } n \mid m, \\ 0, & \text{if } n \nmid m. \end{cases}
\] (2.6)

The case \( m = 1 \) of (2.6) gives the characteristic property of the Möbius function:
\[
\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}
\] (2.7)

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 \( c_{n_1n_2}(m) = c_{n_1}(m)c_{n_2}(m) \). (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 \( p^r \) \((r \geq 1)\),
\[
c_{p^r}(m) = \begin{cases} p^r - p^{r-1}, & \text{if } p^r \mid m, \\ -p^{r-1}, & \text{if } p^{r-1} \mid m, \\ 0, & \text{if } p^{r-1} \nmid m. \end{cases}
\] (2.8)

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

(iii) \( c_n(m) \) is an even function of \( m \) \((\text{mod } n)\), that is, \( c_n(m) = c_n((m,n)) \), for every \( m, n \).

von Sterneck [64], in his work on a kind of integer partition problems modulo an integer, employed the number
\[
\Phi(m,n) = \frac{\varphi(n)}{\varphi \left( \frac{n}{(m,n)} \right)} \mu \left( \frac{n}{(m,n)} \right),
\] (2.9)

which is known as the von Sterneck number, von Sterneck’s function, or the Dedekind-von Sterneck function. The number (2.9) has many applications in number theory and combinatorics, among other places.

A crucial fact in studying Ramanujan sums and their applications is that they coincide with von Sterneck’s function.
Theorem 2.3. For integers $m$ and $n$, with $n \geq 1$, we have
\[
\Phi(m, n) = c_n(m).
\] (2.10)

The equality (2.10) is widely attributed to Hölder [23], while Kluyver [26] had already discovered it about thirty years before Hölder [23] (see, [17] for a discussion about this). There are several names for Theorem 2.3 in the literature, for example, Hölder’s theorem, the Dedekind-Hölder theorem, and von Sterneck’s formula.

Ramanujan sums satisfy several important orthogonality properties. One of them is the following identity (see [11], [17, Th. 3.11], [36, Th. 2.8]):

Theorem 2.4. If $n \geq 1$, $d_1 | n$, and $d_2 | n$, then we have
\[
\sum_{d \mid n} cd_1 \left(\frac{n}{d}\right) c_d \left(\frac{n}{d_2}\right) = \begin{cases} n, & \text{if } d_1 = d_2, \\ 0, & \text{if } d_1 \neq d_2. \end{cases}
\] (2.11)

We close this subsection by mentioning that, very recently, Fowler et al [17] 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 finite 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 $m \in \mathbb{Z}$. From (2.2), it is clear that $c_n(m)$ is a periodic function of $m$ with period $n$.

We define the finite Fourier transform (FFT) of an $n$-periodic function $f$ as the function $\hat{f} = F(f)$, given by
\[
\hat{f}(b) = \sum_{m=1}^{n} f(m) e\left(\frac{-bm}{n}\right) \quad (b \in \mathbb{Z}).
\] (2.12)

Then the inverse finite Fourier transform (IFFT), that is, the Fourier representation of $f$ is obtained as (cf., e.g., [10, p. 109])
\[
f(m) = \frac{1}{n} \sum_{b=1}^{n} \hat{f}(b) e\left(\frac{bm}{n}\right) \quad (m \in \mathbb{Z}).
\] (2.13)

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
\[
(f_1 \otimes f_2)(m) = \sum_{x_1, x_2 \, (\text{mod } n)} f_1(x_1) f_2(x_2) = \sum_{x=1}^{n} f_1(x) f_2(n - x) \quad (m \in \mathbb{Z}).
\]
It is well known that
\[ \hat{f_1 \otimes f_2} = \hat{f_1} \hat{f_2}. \]
More generally, if \( f_1, \ldots, f_k \) are \( n \)-periodic functions, then
\[ \mathcal{F}(f_1 \otimes \cdots \otimes f_k) = \mathcal{F}(f_1) \cdots \mathcal{F}(f_k). \tag{2.14} \]

For \( t \mid n \), let \( g_{n,t} \) be the \( n \)-periodic function defined for every \( m \in \mathbb{Z} \) by
\[ g_{n,t}(m) = \begin{cases} 1, & \text{if } (m, n) = t, \\ 0, & \text{if } (m, n) \neq t. \end{cases} \]

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

**Theorem 2.5.** For every \( t \mid n \),
\[ \hat{g}_{n,t}(m) = c_n^\frac{t}{n}(m) \quad (m \in \mathbb{Z}), \]
in particular, the Ramanujan sum \( m \mapsto c_n(m) \) is the FFT of the function \( m \mapsto g_{n,1}(m) \).

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.** (\cite{60}, Prop. 2) If \( f \) is an \( n \)-even function, then
\[ \hat{f}(m) = \sum_{d \mid n} f(d) c_n^\frac{m}{d}(m) \quad (m \in \mathbb{Z}). \]

**Proof.** Group the terms of \( (2.12) \) according to the values \( d = (m, n) \), taking into account the definition of the \( n \)-even functions. \( \square \)

### 3 Linear congruences with \( (x_i, n) = t_i \) \( (1 \leq i \leq k) \)

In this section, using properties of Ramanujan sums and of the finite 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 \( a_1, t_1, \ldots, a_k, t_k, b, n \) \((n \geq 1)\).

Let us start with the case that we have only one variable; this is a building block for the case of \( k \) variables \((k \geq 1)\). The following theorem generalizes the main result of \cite{20}, one of the main results of \cite{2}, and also a key lemma in \cite{43} (Lemma 1).

**Theorem 3.1.** Let \( a, b, n \geq 1 \) and \( t \geq 1 \) be given integers. The congruence \( ax \equiv b \mod n \) has solution(s) \( x \) with \( (x, n) = t \) if and only if \( t \mid (b, n) \) and \( (a, \frac{n}{t}) = (\frac{b}{t}, \frac{n}{t}) \). Furthermore, if these conditions are satisfied, then there are exactly
\[ \varphi\left(\frac{n}{t}\right) \varphi\left(\frac{n}{td}\right) = d \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \tag{3.1} \]
incongruent solutions, where \( d = (a, \frac{n}{t}) = (\frac{b}{t}, \frac{n}{t}) \).
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 \( \left( \frac{a}{t}, \frac{n}{t} \right) = 1 \), so 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 \( A = \frac{a}{t}, B = \frac{b}{t}, N = \frac{n}{t} \). Then \( (A, N) = (B, N) = 1 \). If \( x \) is such that \( ax \equiv b \pmod{n} \) and \( (x, n) = t \), then \( x = ty \) and \( Ay \equiv B \pmod{N} \). Conversely, since \( (A, N) = 1 \), the congruence \( Ay \equiv B \pmod{N} \) has a unique solution \( y_0 = A^{-1}B \pmod{N} \) 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 \( ax \equiv b \pmod{n} \).

Hence, all solutions of the congruence \( ax \equiv b \pmod{n} \) with \( (x, n) = t \) have the form \( x = t(y_0 + kN), \) where \( 0 \leq k \leq d - 1 \) and \( (y_0 + kN, \frac{n}{t}) = 1 \). 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 of the M"obius function, \([2.7]\), is

\[
S = \sum_{0 \leq k \leq d-1} \frac{1}{(y_0 + kN, d)} = \sum_{0 \leq k \leq d-1} \mu(\delta) \sum_{\delta | d} \left( 1 - \frac{\varphi(\delta)}{\varphi(d)} \right) \frac{\varphi(N\delta)}{\varphi(N)} = \frac{\varphi(N)}{\varphi(N)}.
\]

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 \( \frac{\delta}{\varphi(\delta)} \) solutions \( (mod \; d) \). Therefore,

\[
S = \sum_{\delta | d} \mu(\delta) \frac{d}{\delta} \prod_{p | d, p | N} \left( 1 - \frac{1}{p} \right) = \frac{\varphi(Nd)}{\varphi(N)} = \frac{\varphi(N)}{\varphi(N)}.
\]

The proof is now complete. \( \square \)

**Corollary 3.2.** 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) \( (a, \frac{n}{t}) = (\frac{b}{t}, \frac{n}{t}) = 1 \), where \( t \mid (b, n) \) and
(ii) \( (a, \frac{n}{t}) = (\frac{b}{t}, \frac{n}{t}) = 2 \), where \( t \mid b, \; n = 2^ru, \; r \geq 1, \; u \geq 1 \) odd, \( t = 2r^{-1}v, \; v \mid u. \)

Proof. If \( d = 1 \), then \([3.2]\) 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 \( p^s \parallel n, \; p^t \parallel t \) with \( 0 \leq j + s \leq r \). Then, by \([3.2]\), 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). \( \square \)

We remark that Corollary 3.2, in the case of \( t = 1 \), was obtained in \([21]\) Cor. 4].
Now, we deal with the case of \( k \) variables \((k \geq 1)\). We note the following multiplicativity property: Let \( N_n(t_1, \ldots, t_k) \) denote the number of incongruent solutions of (1.6) and let \( n, m \geq 1, (n, m) = 1 \). Then

\[
N_{nm}(t_1, \ldots, t_k) = N_n(u_1, \ldots, u_k)N_m(v_1, \ldots, v_k),
\]

with unique \( u_i, v_i \) such that \( t_i = u_i v_i, u_i | n, v_i | m \) \((1 \leq i \leq k)\), where \( a_1, \ldots, a_k, b \) are fixed. 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 3.3.** 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

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

Note that Sun and Yang [58] obtained a different formula (with a longer proof) for the number of solutions of the above linear congruence (in Theorem 3.3), but we need the above equivalent formula, (3.3), for the purposes of this paper. We also remark that the special case of \( b = 0, t_i = \frac{n}{m_i}, m_i \mid n \) \((1 \leq i \leq k)\), 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 ([59 Prop. 9]) to be equivalent to the *orbicyclic* (multivariate arithmetic) function ([33]) defined 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 [33, 37, 59] (see, also, [38, 65]).

In what follows, we give the proof of the formula (3.3). In fact, we offer two ‘minimal’ proofs to show that only basic properties of Ramanujan sums and of the FFT, respectively, are required. The first one is a slight modification of the proof of [59 Prop. 21].

**Proof.** First method. Put \( x'_i = \frac{x_i}{t_i} \) \((1 \leq i \leq k)\). Using (2.1), the number \( N_n(k, b, t_1, \ldots, t_k) \)
of solutions is

\[ N_n(k, b, t_1, \ldots, t_k) = \sum_{x_1=1}^{n} \cdots \sum_{x_k=1}^{n} \frac{1}{n} \sum_{j=1}^{n} e \left( \frac{j(x_1 + \cdots + x_k - b)}{n} \right) \]

\[ = \frac{1}{n} \sum_{j=1}^{n} \left( -\frac{jb}{n} \right) \prod_{i=1}^{k} \sum_{x_i=1}^{n/\tau_i} e \left( \frac{jx_i}{n/\tau_i} \right) \]

\[ = \frac{1}{n} \sum_{j=1}^{n} \left( -\frac{jb}{n} \right) \prod_{i=1}^{k} c_{\tau_i}^n(j) \]

By Corollary 2.2/(iii) and the associativity of gcd,

\[ c_{\tau_i}^n((j, n)) = c_{\tau_i}^n \left( \left( j, \frac{n}{\tau_i} \right) \right) = c_{\tau_i}^n \left( \left( j, \frac{n}{\tau_i} \right) \right) = c_{\tau_i}^n \left( j, \frac{n}{\tau_i} \right). \quad (3.4) \]

Moreover, \( c_{\tau_i}^n(-b) = c_{\tau_i}^n (b) \) (\( c_n(m) \) is integer-valued, by Corollary 2.2/(ii)). Hence,

\[ N_n(k, b, t_1, \ldots, t_k) = \frac{1}{n} \sum_{d|n} \sum_{j=1}^{n} e \left( -\frac{jb}{n} \right) \prod_{i=1}^{k} c_{\tau_i}^n(j) \]

\[ = \frac{1}{n} \sum_{d|n} \sum_{j=1}^{n} \sum_{j'=1}^{n/d} e \left( -\frac{j'b}{n/d} \right) \prod_{i=1}^{k} c_{\tau_i}^n(d) \]

\[ = \frac{1}{n} \sum_{d|n} c_{\tau_i}^n(-b) \prod_{i=1}^{k} c_{\tau_i}^n(d) \]

\[ = \frac{1}{n} \sum_{d|n} c_{\tau_i}^n(b) \prod_{i=1}^{k} c_{\tau_i}^n(d) = \frac{1}{n} \sum_{d|n} c_d(b) \prod_{i=1}^{k} c_{\tau_i}^n \left( \frac{n}{d} \right), \]

finishing the proof.
Second method. Now we apply the properties of the FFT. Observe that
\[
(\varrho_{n,t_1} \otimes \cdots \otimes \varrho_{n,t_k})(b) = \sum_{x_1, \ldots, x_k \bmod n} 1
\]
is exactly the number \(N_n(k, b, t_1, \ldots, t_k)\) of solutions of the given restricted congruence. That is,
\[
N_n(b, k, t_1, \ldots, t_k) = (\varrho_{n,t_1} \otimes \cdots \otimes \varrho_{n,t_k})(b).
\]
Therefore, by (2.14) and Theorem 2.5
\[
\widehat{N}_n(k, b, t_1, \ldots, t_k) = c_{\frac{n}{r_1}}(b) \cdots c_{\frac{n}{r_k}}(b),
\]
and the IFFT formula, (2.13), gives
\[
N_n(k, b, t_1, \ldots, t_k) = \frac{1}{n} \sum_{j=1}^{n} c_{\frac{n}{r_1}}(j) \cdots c_{\frac{n}{r_k}}(j) e^{\left(\frac{b j}{n}\right)}.
\]

The properties (3.4) show that \(m \mapsto c_{\frac{n}{r_1}}(m) \cdots c_{\frac{n}{r_k}}(m)\) is an \(n\)-even function. Now, by applying Theorem 2.6 the proof follows. \(\square\)

Now, using Theorems 3.1 and 3.3 we obtain the following general formula for the number of solutions of the restricted linear congruence (1.6).

**Theorem 3.4.** Let \(a_i, t_i, b, n \in \mathbb{Z}, n \geq 1, t_i \mid n\) \((1 \leq i \leq k)\). The number of solutions of the linear congruence \(a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}\), with \((x_i, n) = t_i\) \((1 \leq i \leq k)\), is
\[
N_n(k, b, a_1, t_1, \ldots, a_k, t_k) = \frac{1}{n} \prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}d_i\right) \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} c_{\frac{n}{r_it_i}}\left(\frac{n}{d}\right)
\]
\[
= \frac{1}{n} \left(\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right)\right) \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} \mu\left(\frac{d}{(a_it_i, d)}\right) \varphi\left(\frac{d}{(a_it_i, d)}\right),
\]
where \(d_i = \left(a_i, \frac{n}{t_i}\right)\) \((1 \leq i \leq k)\).

**Proof.** Assume that the linear congruence \(a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}\), has a solution \(x_i, x_k \in \mathbb{Z}_n^k\) with \((x_i, n) = t_i\) \((1 \leq i \leq k)\). Let \(a_i x_i \equiv y_i \pmod{n}\) \((1 \leq i \leq k)\). Then \((a_i x_i, n) = d_i\) \((1 \leq i \leq k)\). Thus, \(\left(\frac{a_i x_i}{t_i}, \frac{n}{t_i}\right) = \left(\frac{y_i}{t_i}, \frac{n}{t_i}\right) = d_i\). But since
\[
\left(\frac{x_i}{t_i}, \frac{n}{t_i}\right) = 1,
\]
we have \(d_i = \left(a_i, \frac{n}{t_i}\right) = \left(\frac{a_i}{t_i}, \frac{n}{t_i}\right)\).

By Theorem 3.3 the number of solutions of the linear congruence \(y_1 + \cdots + y_k \equiv b \pmod{n}\), with \((y_i, n) = t_id_i\) \((1 \leq i \leq k)\), is
\[
\frac{1}{n} \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} c_{\frac{n}{r_it_i}}\left(\frac{n}{d}\right).
\]
Now, given the solutions \(\langle y_1, \ldots, y_k \rangle\) of the latter congruence, we need to find the number of solutions of \(a_i x_i \equiv y_i \pmod{n}\), with \((x_i, n) = t_i (1 \leq i \leq k)\). Since \(\left( a_i, \frac{n}{t_i} \right) = \left( \frac{n}{t_i}, \frac{n}{t_i} \right) = d_i\), so by Theorem 3.1 the latter congruence has exactly

\[
\frac{\varphi \left( \frac{n}{t_i} \right)}{\varphi \left( \frac{n}{d_i} \right)} \tag{3.8}
\]
solutions. Combining (3.7) and (3.8) we get the formula (3.5).

Furthermore, applying von Sterneck’s formula, (2.10), we deduce

\[
c_{\frac{n}{t_i d_i}} \left( \frac{n}{d_i} \right) = \frac{\varphi \left( \frac{n}{t_i d_i} \right) \mu(w_i)}{\varphi(w_i)}, \tag{3.9}
\]
where, denoting by \([a, b]\) the lcm of the integers \(a\) and \(b\),

\[
w_i = \frac{n}{[t_i, d_i, n]} = \frac{n}{t_i d_i} = \frac{[t_i d_i, d]}{t_i d_i} = \frac{d}{(t_i d_i, d)} = \frac{d}{((a_i t_i, n), d)} = \frac{d}{(a_i t_i, d)}.
\]

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

\begin{proof}
\end{proof}

\textbf{Remark 3.5.} For fixed \(a_i, t_i \ (1 \leq i \leq k)\) and fixed \(n\), the function

\[
b \mapsto N_n(k, b, a_1, t_1, \ldots, a_k, t_k)
\]
is an even function \(\pmod{n}\). This follows from the formula (3.5), showing that

\[
N_n(k, b, a_1, t_1, \ldots, a_k, t_k)
\]
is a linear combination of the functions \(b \mapsto c_d(b) \ (d \mid n)\), which are all even \(\pmod{n}\) by (2.4). See also (3.4).

\textbf{Remark 3.6.} In the case of \(k = 1\), by comparing Theorem 3.1 with formula (3.5) and by denoting \(t_1 d_1 = s\), we obtain, as a byproduct, the following identity, which is similar to (2.11) (and can also be proved directly): If \(b, n \in \mathbb{Z}, n \geq 1\), and \(s \mid n\), then

\[
\sum_{d \mid n} c_d(b) c_{\frac{n}{d}} \left( \frac{n}{d} \right) = \begin{cases} n, & \text{if } (b, n) = s, \\ 0, & \text{if } (b, n) \neq s. \end{cases} \tag{3.10}
\]

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

Now, assume that there is an \(i_0\) such that \(a_{i_0} \neq 0\). For a prime \(p\) and \(j \geq 1\) let

\[
e_p^{(j)} = \#\{ i : 1 \leq i \leq k, p^j \nmid a_i t_i \} \geq 0
\]
and let

\[
m_p = m = \min\{ j : j \geq 1, e_p^{(j)} \neq 0 \} \geq 1,
\]
that is, \(p^{m-1} \mid a_i t_i\) for every \(1 \leq i \leq k\), but there is at least one \(i\) such that \(p^m \nmid a_i t_i\). There exists a finite \(m_p = m\), since for a sufficiently large \(j\) one has \(p^j \nmid a_{i_0} t_{i_0}\) and \(e_p^{(j)} \geq 1\).
Theorem 3.7. Let \(a_i, t_i, b, n \in \mathbb{Z}, \ n \geq 1, \ t_i \mid n \ (1 \leq i \leq k)\) 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 \((x_i, n) = t_i \ (1 \leq i \leq k)\). If there is a prime \(p \mid n\) such that \(p^r \mid \mid n\) with \(m_p = m \leq r\) and \(p^{m-1} \nmid b\) or with \(m_p = m \geq r + 1\) and \(p^r \nmid b\), then the linear congruence has no solution. Otherwise, the number of solutions is

\[
\prod_{i=1}^{k} \varphi \left( \frac{n}{t_i} \right) \prod_{p^j \mid |n \ \text{or} \ p^j \mid |b \ \text{and} \ m \leq r} \binom{m}{p} \left(1 - \frac{(-1)^{e_p(i)-1} \text{if } p^m \nmid b}{(p-1)^{e_p(i)}-1} \right) \prod_{p^j \mid |n \ \text{or} \ p^j \mid |b \ \text{and} \ m \leq r} \binom{m}{p} \left(1 - \frac{(-1)^{e_p(i)-1} \text{if } p^m \nmid b}{(p-1)^{e_p(i)}-1} \right), \tag{3.11}
\]

where the last product is empty and equal to 1 if \(b = 0\).

Proof. For a prime power \(n = p^r \ (r \geq 1)\) the inner sum of (3.6) is

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

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

\[
W = \sum_{j=0}^{m-1} c_{p^j}(b) + c_{p^m}(b) \frac{(-1)^{e_p(i)-1}}{(p-1)^{e_p(i)}-1},
\]

the other terms are zero. We deduce by using (2.6) and (2.8) that

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

Now assume that \(m_p = m \geq r + 1\). Then \(p^r \mid a_i t_i\) for every \(i\) and \((a_i, p^j) = p^j\) for every \(j\) with \(0 \leq j \leq r\). Hence, by using (2.6),

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

Inserting into (3.6) and by using the multiplicativity property (3.2) the proof is complete. □
Corollary 3.8. The restricted congruence given in Theorem 3.7 has no solutions if and only if one of the following cases holds:

- (i) there is a prime \( p \mid n \) with \( m \leq r \) and \( p^{m-1} \nmid b \);
- (ii) there is a prime \( p \mid n \) with \( m \geq r + 1 \) and \( p^{r} \nmid b \);
- (iii) there is a prime \( p \mid n \) with \( m \leq r \), \( e_{p}^{(m)} = 1 \) and \( p^{m} \mid b \);
- (iv) \( n \) is even, \( m_{2} = m \leq r \), \( e_{2}^{(m)} \) is odd and \( 2^{m} \mid b \);
- (v) \( n \) is even, \( m_{2} = m \leq r \), \( e_{2}^{(m)} \) is even and \( 2^{m-1} \mid b \).

Proof. Use the first part of Theorem 3.7 and examine the conditions under which the factors of the products in (3.11) vanish. \( \square \)

Example 3.9.

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 \( 24 = 2^{3} \cdot 3 \),
\[
2 \mid a_{1}t_{1} = 6, 2 \mid a_{2}t_{2} = 2, 2 \mid a_{3}t_{3} = 8, \text{so, } e_{2}^{(1)} = 0,
\]
\[
2^{2} \mid a_{1}t_{1} = 6, 2^{2} \mid a_{2}t_{2} = 2, 2^{2} \mid a_{3}t_{3} = 8, \text{so, } e_{2}^{(2)} = 2 \text{ and } m_{2} = 2, \text{ also } 2^{2} \mid b = 12
\]
\[
3 \mid a_{1}t_{1} = 6, 3 \mid a_{3}t_{3} = 8, \text{ so, } e_{3}^{(1)} = 2, m_{3} = 1, \text{ also } 3^{1} \mid b = 12.
\]

The number of solutions is
\[
N = \phi(24/3)\phi(24/2)\phi(24/4)2^{2-3-1}\left(1 - \frac{(-1)^{2-1}}{(2-1)^{2-1}}\right)3^{1-1-1}\left(1 - \frac{(-1)^{2-1}}{(3-1)^{2-1}}\right) = 8.
\]

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 \( 2^{2} \mid b = 4 \), \( 3^{1-1} \mid b = 4 \).

The number of solutions is
\[
N = \phi(24/3)\phi(24/2)\phi(24/4)2^{2-3-1}\left(1 - \frac{(-1)^{2-1}}{(2-1)^{2-1}}\right)3^{1-1-1}\left(1 - \frac{(-1)^{2}}{(3-1)^{2}}\right) = 4.
\]

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 \( 2^{2-1} \mid b = 5 \), hence, there are no solutions by Corollary 3.8/(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 \( 2^{2-1} \mid b = 10 \), hence, there are no solutions by Corollary 3.8/(v).

Remark 3.10. If \( k = 1 \), then \( e_{p}^{(m)} = 1 \) for every prime \( p \mid n \), and it is easy to see that from Theorem 3.7 and Corollary 3.8 we reobtain Theorem 3.7.

The following formula is a special case of Theorem 3.7 and was obtained by Sburlati \[52\] without a clear proof.
Corollary 3.11. Assume that for every prime $p \mid n$ one has $e_p^{(1)} = \#\{i : 1 \leq i \leq k, p \nmid a_it_i\} \geq 1$, that is $p \nmid a_it_i$ for at least one $i \in \{1, \ldots, k\}$. Then the number of solutions of the restricted linear congruence (1.6) is

$$\frac{1}{n} \prod_{i=1}^{k} \phi \left( \frac{n}{t_i} \right) \prod_{p \mid (b,n)} \left( 1 - \frac{(-1)^{e_p^{(1)} - 1}}{(p-1)^{e_p^{(1)} - 1}} \right) \prod_{p \nmid b} \left( 1 - \frac{(-1)^{e_p^{(1)}}}{(p-1)^{e_p^{(1)}}} \right).$$  \hspace{1cm} (3.13)

4 Universal hashing

Universal hash functions, discovered by Carter and Wegman [9], have many applications in computer science, for example, in cryptography, complexity theory, randomized algorithms, dictionary data structures, parallel computing, and many others. Universal hashing captures the desired property that distinct keys do not collide (that is, have the same hash value) too often. In [21] the authors have gathered the definitions of various kinds of universal hash functions from several papers:

**Definition 4.1.** Let $H$ be a family of functions from a domain $D$ to a range $R$. Let $\varepsilon$ be a constant such that $\frac{1}{|R|} \leq \varepsilon < 1$. The probabilities below, are taken over the random choice of hash function $h$ from the set $H$.

- $H$ is a universal family of hash functions if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \frac{1}{|R|}$. Also, $H$ is an $\varepsilon$-almost-universal ($\varepsilon$-AU) family of hash functions if for any two distinct $x, y \in D$, we have $\Pr_{h \leftarrow H}[h(x) = h(y)] \leq \varepsilon$.

- Suppose $R$ is an Abelian group. $H$ is a $\Delta$-universal family of hash functions if for any two distinct $x, y \in D$, and all $a \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = a] = \frac{1}{|R|}$, where ‘$-$’ denotes the group subtraction operation. Also, $H$ is an $\varepsilon$-almost-$\Delta$-universal ($\varepsilon$-AA$\Delta$U) family of hash functions if for any two distinct $x, y \in D$, and all $a \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = a] \leq \varepsilon$.

- $H$ is a strongly universal family of hash functions if for any two distinct $x, y \in D$, and all $a, b \in R$, we have $\Pr_{h \leftarrow H}[h(x) = a, h(y) = b] = \frac{1}{|R|^2}$. Also, $H$ is an $\varepsilon$-almost-strongly universal ($\varepsilon$-ASU) family of hash functions if for any two distinct $x, y \in D$, and all $a, b \in R$, we have $\Pr_{h \leftarrow H}[h(x) = a, h(y) = b] \leq \frac{\varepsilon}{|R|^2}$.

Carter and Wegman [9] constructed a special family of hash functions defined below (this family called MMH$^*$ in [21]):

**Definition 4.2.** Let $p$ be a prime and $k$ be a positive integer. The family MMH$^*$ is defined as follows:

$$\text{MMH}^* := \{g_x : \mathbb{Z}_p^k \to \mathbb{Z}_p \mid x \in \mathbb{Z}_p^k\}.$$  \hspace{1cm} (4.1)
where
\[ g_x(m) := m \cdot x \pmod p = \sum_{i=1}^{k} m_i x_i \pmod p, \] (4.2)
for any \( x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k \), and any \( m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k \).

It is well-known that MMH* is a universal family of hash functions ([9, 21]).

**Theorem 4.3.** The family MMH* is a universal family of hash functions.

Now, we introduce a generalization of the MMH* by allowing the keys, \( x \)'s, to be chosen from \( \mathbb{Z}_n^* \)

**Definition 4.4.** Let \( n \) and \( k \) be positive integers. We define the family BLF as follows:
\[ \text{BLF} := \{ \Upsilon_x : \mathbb{Z}_n^k \to \mathbb{Z}_n : x \in \mathbb{Z}_n^* \}, \] (4.3)
where
\[ \Upsilon_x(m) := m \cdot x \pmod n = \sum_{i=1}^{k} m_i x_i \pmod n, \] (4.4)
for any \( x = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^* \), and any \( m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k \).

Clearly, BLF is a multilinear map (in fact, a bilinear form). It is easy to see that BLF is not universal, or even \( \varepsilon \)-almost-universal (\( \varepsilon \)-AU), for all positive integers \( n \). But it would be an interesting question to investigate for which values of \( n \), BLF is universal, or \( \varepsilon \)-AU (see, also, [14]).

### 5 An authenticated encryption scheme based on the BLF family

In this section, we propose an authenticated encryption scheme based on the BLF family defined in Section 4. Then, using our results from Section 3, we analyze the integrity of this scheme.

We recall that two important notions in cryptography are secrecy and integrity. Encryption only provides secrecy, but in many cases (e.g., financial transactions) we need integrity (or authenticity), as well. These notions, secrecy and integrity, are orthogonal, and in particular a cryptographic scheme that offers even perfect secrecy makes no guarantees with respect to integrity. The latter property requires an additional mechanism, namely a message authentication code (or MAC), also known as a cryptographic checksum or a keyed hash function, defined formally as [24]:

**Definition 5.1.** A MAC is a tuple of algorithms \((\text{Gen}, \text{Mac}, \text{Vrfy})\):
• **Gen** is a key generation algorithm; a randomized algorithm that returns a key $k$.

• **Mac** is a tag generation algorithm; a randomized and/or stateful algorithm that takes a key $k$ and a message $m$ and returns an authentication tag $t$. This is usually written as: $t \leftarrow \text{Mac}_k(m)$.

• **Vrfy** is a verification algorithm; a deterministic algorithm that takes a key $k$, a message $m$, and an authentication tag $t$, and returns $\text{Vrfy}_k(m, t) \in \{0, 1\}$. (0 for false and 1 for true.)

We require that for every key $k$, and every $m \in \mathcal{M}$ (where, $\mathcal{M}$ is a message space), $\text{Vrfy}_k(m, \text{Mac}_k(m)) = 1$.

Note that the adversary has a goal to ‘forge’ the MAC, that is, to produce any pair $(m, t)$ such that $\text{Vrfy}_k(m, t) = 1$. Message authentication codes (MACs) were invented in 1974 by Gilbert, MacWilliams, and Sloane [19], using ideas from projective spaces over finite fields. Their system is fast, but has two drawbacks: it requires keys longer than the length of messages, and also a new key for every message.

There are three common approaches to MACs: constructing MACs based on block ciphers (such as DES), based on cryptographic hash functions (such as MD5), and based on universal hash functions. The latter, discovered by Wegman and Carter [66] (which is usually referred to as the Wegman-Carter paradigm), is one of the most widely used MAC constructions. In this scheme, the legitimate parties share a secret hash function drawn randomly from an $\varepsilon$-A△U family of hash functions, and a secret encryption key (a sequence of random one-time pads). A message is authenticated by first hashing it with the shared hash function and then encrypting the resulting hash value with the shared encryption key (shared one-time pad). Note that one-time pads are of the length of the hash value rather than of the length of the message. The resulting encrypted hash value, called an *authentication tag*, is transmitted together with the message (as a pair). Upon receiving this pair, the legitimate party recomputes and validates it.

Constructing MACs based on universal hash functions is stunning from several points of view. For example, even if an adversary who has unbounded computational power performs $q$ black-box oracle queries to both algorithms used by the MAC, then the probability to forge the MAC is at most $q\varepsilon$ (see, [28, 66]). Black et al [17] best describe the reasons that MAC constructions based on universal hashing is one of the most widely used MAC constructions and “why universal hashing?” as: “the above approach is a promising one for building a highly-secure and ultra-fast MAC. The reasoning is like this: the speed of a universal hashing MAC depends on the speed of the hashing step and the speed of the encrypting step. But if the hash function compresses messages well (i.e., its output is short) then the encryption shouldn’t take long simply because it is a short string that is being encrypted. On the other hand, since the combinatorial property of the universal hash function family is mathematically proven (making no cryptographic hardness assumptions), it needs no “over-design” or “safety margin” the way a cryptographic primitive would. Quite the opposite: the hash function family might as well be the fastest, simplest thing that one can prove universal. Equally important, the above approach makes for desirable security properties. Since the cryptographic primitive is applied only to the (much shorter) hashed image of the
message, we can select a cryptographically conservative design for this step and pay with only a minor impact on speed. And the fact that the underlying cryptographic primitive is used only on short and secret messages eliminates many avenues of attack. Under this approach security and efficiency are not conflicting requirements — quite the contrary, they go hand in hand.”

Several computationally secure MACs based on universal hash functions have been proposed following the Wegman-Carter paradigm; see, e.g., [6, 7, 16, 21, 22, 27, 57, 66] and the references therein.

Encryption schemes that are provably secure even against an adversary who has unbounded computational power are called perfectly secret. Roughly speaking, an encryption scheme is perfectly secret if the distributions over messages and ciphertexts are independent.

Formally, let $\mathcal{M}$ be the space of messages, $\mathcal{C}$ the space of ciphertexts and $\mathcal{K}$ the space of keys. An encryption scheme is a tuple of randomized functions $(\text{Gen}, \text{Enc}, \text{Dec})$, where Gen is a key generator and for any $k \in \mathcal{K}$ and $m \in \mathcal{M}$, the encryption and decryption functions Enc, Dec satisfy $\text{Dec}(k, \text{Enc}(k, m)) = m$. Let $M$ denote an arbitrary distribution on $\mathcal{M}$, and $K$ denote the distribution on $\mathcal{K}$ produced by Gen. This induces a distribution on $\mathcal{C}$, which we denote by $C$. We now give the definition of perfect secrecy developed by Shannon [54].

**Definition 5.2.** (24) An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ over a message space $\mathcal{M}$ is said to be perfectly secret if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$, we have

$$\Pr[M = m | C = c] = \Pr[M = m]. \quad (5.1)$$

This means that the ciphertext should not leak any information about the underlying plaintext. In other words, the a priori probability of a message $m \in \mathcal{M}$ is the same as the a posteriori probability of the message $m$ given the corresponding ciphertext.

There are several methods to construct authenticated encryption (AE) schemes. One of these methods is “generic composition”, in which an encryption scheme and an authentication scheme are ‘appropriately’ combined. There are three different approaches to authenticated encryption by generic composition: authenticate-then-encrypt (AtE), encrypt-then-authenticate (EtA), and encrypt-and-authenticate (E&A). SSL uses a variant of AtE, IPSec uses a variant of EtA, and Transport Layer of SSH uses a variant of E&A. See [5, 29] and the references therein, for a detailed discussion about these generic constructions and their security analysis.

Let us consider the original universal hash function family discovered by Carter and Wegman [9]. Fix $m$ and $n$, and choose a prime $p \geq m$. For all $a, b \in \mathbb{Z}_p$, define

$$h_{a,b}(x) = ((ax + b) \mod p) \mod n. \quad (5.2)$$

Carter and Wegman [9] showed that the family $H := \{h_{a,b} | a, b \in \mathbb{Z}_p, \text{ with } a \neq 0\}$ is universal. Note that in using this universal hash function family for message authentication, two keys, $a$ and $b$, and two modular operations in $\mathbb{Z}_p$, one addition and one multiplication, are needed. Also, in order to get message integrity and perfect secrecy, the message should be encrypted with a one-time pad (OTP) first, and then the encrypt-then-authenticate (EtA) approach is applied; thus, three keys and three modular operations are needed. However,
Alomair and Poovendran [4] proposed an authenticated encryption scheme which tries to reduce the key size for achieving authentication. In fact, their scheme needs only two keys, and two modular operations in $\mathbb{Z}_p$, one addition and one multiplication, but provides the same level of message integrity and also perfect secrecy. Later, Alomair et al [2] generalized this scheme by allowing operations to be performed over $\mathbb{Z}_n$ ($n \geq 1$) instead of $\mathbb{Z}_p$, and analyzed the security of this construction. Note that the latter construction does not provide perfect secrecy, in general; in fact, perfect secrecy is achieved only if messages are restricted to belong to $\mathbb{Z}_n^*$ ([2, Cor. 5.1]). See, also, [3] for an application of this approach in the authentication problem in RFID systems. In what follows, we generalize their scheme ([2]) in a way which is also applicable to handle long messages; thereby obtaining a way to expand the message space. Then, using our explicit formula from Section 3, we analyze the integrity of this scheme.

5.1 Set up

In this scheme, the legitimate parties share a secret hash function, say $\Upsilon_x$, drawn randomly from the BLF family, and a secret encryption key, say $x' = \langle x'_1, \ldots, x'_k \rangle$, chosen uniformly (and independently from $x$) from $\mathbb{Z}_n^k$. A message $m = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$ is authenticated by separately and simultaneously hashing it with the shared hash function

$$\Upsilon_x(m) \equiv \sum_{i=1}^{k} m_i x_i \pmod{n},$$

and encrypting it with the shared encryption key

$$\Psi_{x'}(m) = m + x' \pmod{n} = \langle m_1 + x'_1 \pmod{n}, \ldots, m_k + x'_k \pmod{n} \rangle.$$ (5.4)

The resulting hash value, called an authentication tag, and the encrypted message are transmitted together (as a pair). Upon receiving this pair, the legitimate party recomputes and validates it.

5.2 Message integrity

Assume that the legitimate party has received the ciphertext $\Psi_{x'}(m)$ and its corresponding authentication tag $\Upsilon'(m)$. The legitimate party first extracts the plaintext $m'$ as follows:

$$m' \equiv \Psi_{x'}(m) - x' \pmod{n}.$$ (5.5)

Now, the system checks the integrity of the extracted $m'$ by the following linear congruence:

$$\Upsilon_x(m) \equiv m' \cdot x \pmod{n}.$$ (5.6)

In fact, the extracted message, $m'$, is valid if and only if the linear congruence [5.6] holds.

Clearly, there are two cases for examining the integrity of this scheme, namely, modifying the ciphertext only, and modifying both the ciphertext and the authentication tag.
Modifying the ciphertext only

Suppose an adversary has modified the ciphertext $\Psi'_x$ to $\Psi'_x'$. Upon receiving, the system extracts (the modified ciphertext) $\Psi'_x'$, and outputs a plaintext, say $m'$, which is computed by $m' \equiv \Psi'_x - x' \pmod{n}$. Suppose $m' = m + a \pmod{n}$, for some $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$. Now, by (5.3), one can see that the extracted message, $m'$, will pass the integrity check (5.6) if and only if the linear congruence

$$a_1 x_1 + \cdots + a_k x_k \equiv 0 \pmod{n} \quad (5.7)$$

has a solution $\langle x_1, \ldots, x_k \rangle$, with $(x_i, n) = 1$ (1 ≤ $i$ ≤ $k$). Now, applying Corollary 3.8 one can determine exactly all the cases that the extracted message, $m'$, will pass the integrity check (5.6).

Modifying both the ciphertext and the authentication tag

Suppose an adversary has modified the ciphertext $\Psi'_x$ to $\Psi'_x'$. Upon receiving, the system, similar to the above, extracts (the modified ciphertext) $\Psi'_x'$, and outputs a plaintext, say $m'$, which is computed by $m' \equiv \Psi'_x - x' \pmod{n}$. Suppose $m' = m + a \pmod{n}$, for some $a = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{0\}$. Also, suppose the adversary has modified the authentication tag $\Upsilon'_x$ to $\Upsilon'_x'$. Let $\Upsilon'_x = \Upsilon'_x + b \pmod{n}$, for some $b \in \mathbb{Z}_n \setminus \{0\}$. Now, by (5.3), one can see that the extracted message, $m'$, will pass the integrity check (5.6) if and only if the linear congruence

$$a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n} \quad (5.8)$$

has a solution $\langle x_1, \ldots, x_k \rangle$, with $(x_i, n) = 1$ (1 ≤ $i$ ≤ $k$). Now, again, applying Corollary 3.8 one can determine exactly all the cases that the extracted message, $m'$, will pass the integrity check (5.6).

6 Concluding remarks

As we have mentioned, the number of solutions of some special cases of the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ (1 ≤ $i$ ≤ $k$), have found very interesting applications in number theory, combinatorics, and cryptography, among other areas. 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 $a_1, t_1, \ldots, a_k, t_k, b, n$ ($n \geq 1$), and also gave an application of our explicit formula in designing an authenticated encryption scheme. As this problem has appeared in several areas in mathematics and computer science, so we believe that our formulas will have implications in these or other applications and 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 $\phi$-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] B. Alomair, L. Lazos, and R. Poovendran, Securing low-cost RFID systems: An unconditionally secure approach, *J. Comput. Secur.* 19 (2011), 229–257.

[4] B. Alomair and R. Poovendran, Information theoretically secure encryption with almost free authentication, *J.UCS* 15 (2009), 2937–2956.

[5] M. Bellare and C. Namprempre, Authenticated encryption: relations among notions and analysis of the generic composition paradigm, *Advances in Cryptology — ASIACRYPT 2000*, LNCS 1976, 2000, 531–545.

[6] D. J. Bernstein, The Poly1305-AES message-authentication code, *Fast Software Encryption — FSE 2005*, LNCS 3557, 2005, 32–49.

[7] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, UMAC: Fast and secure message authentication, *Advances in Cryptology — CRYPTO 1999*, LNCS 1666, 1999, 216–233.

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

[9] J. L. Carter and M. N. Wegman, Universal classes of hash functions, *J. Comput. System Sci* 18 (1979), 143–154.

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

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

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

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

[14] M. Dietzfelbinger, Universal hashing and $k$-wise independent random variables via integer arithmetic without primes, *Symposium on Theoretical Aspects of Computer Science — STACS 96*, LNCS 1046, 1996, 567–580.

[15] J. D. Dixon, A finite analogue of the Goldbach problem, *Canad. Math. Bull.* 3 (1960), 121–126.
[16] M. Etzel, S. Patel, and Z. Ramzan, Square hash: fast message authentication via optimized universal hash functions, *Advances in Cryptology — CRYPTO 1999*, LNCS **1666**, 1999, 234–251.

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

[18] E. E. Gad, M. Langberg, M. Schwartz, and J. Bruck, Constant-weight gray codes for local rank modulation, *IEEE Trans. Inform. Theory* **57** (2011), 7431–7442.

[19] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, *Bell Syst. Tech. J.* **53** (1974), 405–424.

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

[21] S. Halevi and H. Krawczyk, MMH: Software message authentication in the Gbit/second rates, *Fast Software Encryption — FSE 1997*, LNCS **1267**, 1997, 172–189.

[22] H. Handschuh and B. Preneel, Key-recovery attacks on universal hash function based MAC algorithms, *Advances in Cryptology — CRYPTO 2008*, LNCS **5157**, 2008, 144–161.

[23] O. Hölder, Zur Theorie der Kreisteilungsgleichung $K_m(x) = 0$, *Prace Mat. Fiz.* **43** (1936), 13–23.

[24] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman and Hall/CRC, (2007).

[25] D. Kiani and M. Mollahajiaghaei, On the addition of units and non-units in finite commutative rings, *Rocky Mountain J. Math.*, to appear.

[26] 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.

[27] T. Kohno, J. Viega, and D. Whiting, CWC: A high-performance conventional authenticated encryption mode, *Fast Software Encryption — FSE 2004*, LNCS **3017**, 2004, 408–426.

[28] H. Krawczyk, LFSR-based hashing and authentication, *Advances in Cryptology — CRYPTO 1994*, LNCS **839**, 1994, 129–139.

[29] H. Krawczyk, The order of encryption and authentication for protecting communications (or: how secure is SSL?), *Advances in Cryptology — CRYPTO 2001*, LNCS **2139**, 2001, 310–331.

[30] T. A. Le and J. W. Sander, Integral circulant Ramanujan graphs of prime power order, *Electron. J. Combin.* **20** (2013), #P35.
[31] D. N. Lehmer, Certain theorems in the theory of quadratic residues, *Amer. Math. Monthly* **20** (1913), 151–157.

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

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

[34] H. Liu, A note on local randomness in polynomial random number and random function generators, *Appl. Math. Comput.* **186** (2007), 1360–1366.

[35] B. Mans and I. Shparlinski, Random walks, bisections and gossiping in circulant graphs, *Algorithmica* **70** (2014), 301–325.

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

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

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

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

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

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

[42] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Springer-Verlag, (1996).

[43] 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.

[44] M. Planat, M. Minarovjech, and M. Saniga, Ramanujan sums analysis of long-period sequences and $1/f$ noise, *Europhys. Lett. EPL* **85** (2009), 40005.

[45] M. Planat and H. C. Rosu, Cyclotomy and Ramanujan sums in quantum phase locking, *Phys. Lett. A* **315** (2003), 1–5.

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

[47] K. G. Ramanathan, Some applications of Ramanujan’s trigonometrical sum $c_m(n)$, *Proc. Indian Acad. Sci (A)* **20** (1944), 62–69.
[48] S. Ramanujan, On certain trigonometric sums and their applications in the theory of numbers, *Trans. Cambridge Philos. Soc.* **22** (1918), 259–276.

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

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

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

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

[53] P. Scholl and N. Smart, Improved key generation for Gentry’s fully homomorphic encryption scheme, *Cryptography and Coding*, LNCS **7089**, 2011, 10–22.

[54] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, **28** (1949), 656–715.

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

[56] R. P. Stanley and M. F. Yoder, A study of Varshamov codes for asymmetric channels, *JPL Technical Report* 32-1526 XIV (1973), 117–123.

[57] D. R. Stinson, Universal hashing and authentication codes, *Des. Codes Cryptogr.* **4** (1994), 369–380.

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

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

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

[61] P. P. Vaidyanathan, Ramanujan sums in the context of signal processing–Part I: Fundamentals, *IEEE Trans. Signal Process.* **62** (2014), 4145–4157.

[62] P. P. Vaidyanathan, Ramanujan sums in the context of signal processing–Part II: FIR representations and applications, *IEEE Trans. Signal Process.* **62** (2014), 4158–4172.

[63] R. C. Vaughan, *The Hardy-Littlewood Method*, second edition, Cambridge University Press, (1997).

[64] R. D. von Sterneck, Ein Analogon zur additiven Zahlentheorie, *Sitzber, Akad. Wiss. Wien, Math. Naturw. Klasse* **111** (Abt. IIa) (1902), 1567–1601.
[65] T. R. Walsh, Counting maps on doughnuts, *Theoret. Comput. Sci.* 502 (2013), 4–15.

[66] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, *J. Comput. System Sci* 22 (1981), 265–279.