Number Theoretic Methods and their Significance in Computer Science, Information Theory, Combinatorics, and Geometry

by

Khodakhast Bibak
MMath, University of Waterloo, 2013

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Computer Science

Number Theoretic Methods and their Significance in Computer Science, Information Theory, Combinatorics, and Geometry

by

Khodakhast Bibak
MMath, University of Waterloo, 2013

Supervisory Committee

Dr. Bruce M. Kapron, Co-supervisor
(Department of Computer Science, UVic)

Dr. Venkatesh Srinivasan, Co-supervisor
(Department of Computer Science, UVic)

Dr. T. Aaron Gulliver, Outside Member
(Department of Electrical and Computer Engineering, UVic)

Supervisory Committee

Dr. Bruce M. Kapron, Co-supervisor
(Department of Computer Science, UVic)

Dr. Venkatesh Srinivasan, Co-supervisor
(Department of Computer Science, UVic)

Dr. T. Aaron Gulliver, Outside Member
(Department of Electrical and Computer Engineering, UVic)

ABSTRACT

In this dissertation, I introduce some number theoretic methods and discuss their intriguing applications to a variety of problems in computer science, information theory, combinatorics, and geometry. First, 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 restricted linear congruences in their 'most general case'. As a consequence, we derive necessary and sufficient conditions under which these congruences have no solutions. The number of solutions of this kind of congruence was first considered by Rademacher in 1925 and Brauer in 1926, in a special case. Since then, this problem has been studied, in several other special cases, in many papers. 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.

Universal hash functions, discovered by Carter and Wegman in 1979, have many important applications in computer science. Applying our results we construct an almost-universal hash function family which is used to give a generalization of a recent authentication code with secrecy scheme.

As another application of our results, we prove an explicit and practical formula for the number of surface-kernel epimorphisms from a co-compact Fuchsian group to

a cyclic group. This problem has important applications in combinatorics, geometry, string theory, and quantum field theory (QFT). As a consequence, we obtain an 'equivalent' form of Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces.

We also consider the number of solutions of linear congruences with distinct coordinates, and using a graph theoretic method, generalize a result of Schönemann from 1839. Also, we give explicit formulas for the number of solutions of unweighted linear congruences with distinct coordinates. Our main tools are properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions. Then, as an application, we derive an explicit formula for the number of codewords in the Varshamov–Tenengolts code $VT_b(n)$ with Hamming weight k, that is, with exactly k 1's. The Varshamov–Tenengolts codes are an important class of codes that are capable of correcting asymmetric errors on a Z-channel. As another application, we derive Ginzburg's formula for the number of codewords in $VT_b(n)$, that is, $|VT_b(n)|$. We even go further and discuss applications to several other combinatorial problems, some of which have appeared in seemingly unrelated contexts. This provides a general framework and gives new insight into these problems which might lead to further work.

Finally, we bring a very deep result of Pierre Deligne into the area of coding theory — we connect Lee codes to Ramanujan graphs by showing that the Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs (this solves a recent conjecture). Our main tools are Deligne's bound from 1977 for estimating a particular kind of trigonometric sum and a result of Lovász from 1975 (or of Babai from 1979) which gives the eigenvalues of Cayley graphs of finite Abelian groups. Our proof techniques may motivate more work in the interactions between spectral graph theory, character theory, and coding theory, and may provide new ideas towards the long-standing Golomb–Welch conjecture.

Contents

ACKNOWLEDGEMENTS

I have been very fortunate to have Bruce Kapron and Venkatesh Srinivasan as my supervisors. I would like to express my sincere gratitude to them for their constant support, motivation, enthusiasm, and many insightful conversations. Bruce and Venkatesh gave me the freedom to work on any problem that I was interested in and always believed in me. Also, they have been sincere friends at all times.

I am very grateful to Aaron Gulliver for sitting on my committee, his interest to my work, helpful comments, and several interesting questions and discussions. Also, I am very grateful to Michael Jacobson for agreeing to be the external examiner of my dissertation.

My thanks also go to Roberto Tauraso and László Tóth for many fruitful discussions which led to some joint papers. Also, I would like to thank Valerie King and Ulrike Stege for their encouragement and interest in my work.

Igor Shparlinski has had a great impact on my academic life. Igor always supported me, encouraged me, and believed in me. My special thanks go to Igor for his constant support and unending encouragement.

I also thank the entire UVic CS Department staff for always being so helpful and friendly.

Finally, I am eternally grateful to the unbounded love and support of my parents and siblings. Last, but not least, my deepest gratitude and love belong to my wife Azadeh for being the source of encouragement and support for me all the time.

DEDICATION

To my beloved wife Azadeh

Chapter 1

Introduction

Number theory is a vast and fascinating area of mathematics which has been enriched by its formidable links to almost every area of mathematical sciences. Number theory is so fundamental that it is sometimes called "The Queen of Mathematics". In this dissertation, I introduce some number theoretic methods and discuss their intriguing applications to a variety of problems in computer science, information theory, combinatorics, and geometry.

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

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

There are many problems in mathematics, computer science, and engineering that can be modelled and/or studied using linear congruences and their variants. Examples include:

- certain hash functions (e.g., multilinear modular hashing);
- the (generalized) knapsack problem;
- certain pseudorandom number generators;
- certain partition problems;
- some problems in coding theory (e.g., the Varshamov–Tenengolts codes);
- some problems related to studying rings generated by their units;

- certain problems in geometry (e.g., Harvey's theorem);

Therefore, developing techniques for finding (the number of) solutions of linear congruences and their variants is an important problem, and most parts of this dissertation are devoted to studying such problems and their applications. 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 [77], gives the number of solutions of the above linear congruence:

Proposition. 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.

The solutions of the above congruence may be subject to certain conditions, such as $(x_i, n) = t_i$ $(1 \leq i \leq k)$, 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 first considered by Rademacher [105] in 1925 and Brauer [21] 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 [65] gave a nice explicit formula for the number of such solutions when $(a_1, \ldots, a_k) = t_i = 1$ $(1 \leq i \leq k)$. In Chapter 2, 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 restricted linear congruences in their 'most general case', that is, for *arbitrary* integers $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$. As a consequence, we derive necessary and sufficient conditions under which the above restricted linear congruence has no solutions. 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. Some of these applications are discussed in the next chapters. My papers [14, 17] are based on the results in this chapter.

Universal hashing, discovered by Carter and Wegman [26] in 1979, has many important applications in computer science. MMH* is a well-known Δ-universal hash function family. In Chapter 3, we first introduce a generalization of MMH* and investigate its universality via connecting the universal hashing problem to the number of solutions of linear congruences. We then introduce a variant of MMH*, that we

call GRDH, where we use an arbitrary integer $n > 1$ instead of prime p and let the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ satisfy the conditions $(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of n. Applying our aforementioned approach, we prove that the family GRDH is an ε-almost-Δ-universal family of hash functions for some $\varepsilon < 1$ if and only if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-almost-Δ-universal, where p is the smallest prime divisor of n. Finally, as an application of our results, we propose an authentication code with secrecy scheme. This strongly generalizes the scheme studied by Alomair et al. [4, 6]. My papers [13, 18, 19] are based on the results in this chapter.

Graphs embedded into surfaces have many important applications, in particular, in combinatorics, geometry, and physics. For example, ribbon graphs and their counting is of great interest in string theory and quantum field theory (QFT). Recently, Koch, Ramgoolam, and Wen [70] gave a refined formula for counting ribbon graphs and discussed its applications to several physics problems. An important factor in this formula is the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group. In Chapter 4, we give an explicit and practical formula for the number of such epimorphisms. As a consequence, we obtain an 'equivalent' form of Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces. Our main tool is the explicit formula for the number of solutions of restricted linear congruences that we will prove in Chapter 2. My paper [12] is based on the results in this chapter.

As mentioned, Chapter 2 considers the number of solutions of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with the restrictions $(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$ are arbitrary integers. Another restriction of potential interest is imposing the condition that all x_i are *distinct* modulo n. Unlike the first problem, there seems to be very little published on the second problem. Recently, Grynkiewicz et al. [50], using tools from additive combinatorics and group theory, proved necessary and sufficient conditions under which the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, where $a_1, \ldots, a_k, b, n$ $(n \geq 1)$ are arbitrary integers, has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with all x_i distinct modulo n; see also [1, 50] for connections to zero-sum theory. So, it would be an interesting problem to give an explicit formula for the number of such solutions. Quite surprisingly, this problem was first considered, in a special case, by Schönemann [117] almost two centuries ago(!) but his result seems to have been forgotten. Schönemann [117] proved an explicit

formula for the number of such solutions when $b = 0$, $n = p$ a prime, and $\sum_{i=1}^{k} a_i \equiv 0 \pmod{p}$ but $\sum_{i \in I} a_i \not\equiv 0 \pmod{p}$ for all $I \subsetneq \{1, \ldots, k\}$. In Chapter 5, we generalize Schönemann's theorem using Lehmer's result [77] and a result on graph enumeration recently obtained by Ardila et al. [8]. Specifically, we obtain an explicit formula for the number of solutions of the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$, with all x_i distinct modulo n, when $(\sum_{i \in I} a_i, n) = 1$ for all $I \subsetneq \{1, \ldots, k\}$, where $a_1, \ldots, a_k, b, n$ $(n \geq 1)$ are arbitrary integers. This seems to be a rather uncommon method in the area; besides, our proof technique or its modifications may be useful for dealing with other cases of this problem (or even the general case) or other relevant problems. My paper [15] is based on the results in this chapter.

In Chapter 6, we first give explicit formulas for the number of solutions of unweighted linear congruences with distinct coordinates. Our main tools are properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions. Then, as an application, we derive an explicit formula for the number of codewords in the Varshamov–Tenengolts code $VT_b(n)$ with Hamming weight k, that is, with exactly k 1's. The Varshamov–Tenengolts codes are an important class of codes that are capable of correcting asymmetric errors on a Z-channel. As another application, we derive Ginzburg's formula for the number of codewords in $VT_b(n)$, that is, $|VT_b(n)|$. We even go further and discuss applications to several other combinatorial problems, some of which have appeared in seemingly unrelated contexts. This provides a general framework and gives new insight into all of these problems which might lead to further work. The problem in the general case (that is, the number of solutions of weighted linear congruences with distinct coordinates) and its applications to coding theory and combinatorics remain unsolved. My paper [16] is based on the results in this chapter.

The long-standing Golomb–Welch conjecture [47] states that there are no perfect Lee codes for spheres of radius greater than 1 and dimension greater than 2. Resolving this conjecture has been one of the main motivations for studying perfect and quasi-perfect Lee codes. Very recently, Camarero and Martínez [25], showed that for every prime number $p > 5$ such that $p \equiv \pm 5 \pmod{12}$, the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$, where S_2 is the set of units of $\mathbb{Z}_p[i]$, induces a 2-quasi-perfect Lee code over $\mathbb{Z}_p^m$, where $m = 2\lfloor \frac{p}{4} \rfloor$. They also conjectured [25, Conj. 31] that the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is a Ramanujan graph for every prime p such that $p \equiv 3 \pmod{4}$. In Chapter 7, we solve this conjecture. Our main tools are Deligne's bound [35] from 1977 for estimating a particular kind of trigonometric sum and a re-

sult of Lovász [87] from 1975 (or of Babai [9] from 1979) which gives the eigenvalues of Cayley graphs of finite Abelian groups. Our proof techniques may motivate more work in the interactions between spectral graph theory, character theory, and coding theory, and may provide new ideas towards the Golomb–Welch conjecture. My paper [11] is based on the results in this chapter.

Chapter 2

Restricted Linear Congruences

2.1 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

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}. \tag{2.1.1}$$

By a solution of (2.1.1) we mean an ordered k-tuple of integers modulo n, denoted by $\langle x_1, \ldots, x_k \rangle$, that satisfies (2.1.1). 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 [77], gives the number of solutions of the above linear congruence:

Proposition 2.1.1. *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 ([13]) 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 [105] in 1925 and Brauer [21] 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 $(x_i, n) = 1$ $(1 \le i \le k)$ is

$$N_n(k,b) = \frac{\varphi(n)^k}{n} \prod_{p \mid n, p \mid b} \left(1 - \frac{(-1)^{k-1}}{(p-1)^{k-1}}\right) \prod_{p \mid n, p \nmid b} \left(1 - \frac{(-1)^k}{(p-1)^k}\right), \tag{2.1.2}$$

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 [37] and Rearick [108]. The equivalent formula

$$N_n(k,b) = \frac{1}{n} \sum_{d \mid n} c_d(b) \Big(c_n\left(\frac{n}{d}\right)\Big)^k, \tag{2.1.3}$$

involving the Ramanujan sums $c_n(m)$ (see Section 2.2.1) was obtained by Nicol and Vandiver [102, Th. VII] and reproved by Cohen [27, Th. 6].

The special case of $k = 2$ was treated, independently, by Alder [3], Deaconescu [33], and Sander [114]. For $k = 2$ the function $N_n(2,b)$ coincides with Nagell's totient function ([101]) defined to be the number of integers $x \pmod{n}$ such that $(x,n) = (b-x,n) = 1$. From (2.1.2) one easily gets

$$N_n(2,b) = n \prod_{p \mid n, p \mid b} \left(1 - \frac{1}{p}\right) \prod_{p \mid n, p \nmid b} \left(1 - \frac{2}{p}\right). \tag{2.1.4}$$

From (2.1.4) it is clear that $N_n(2,0) = \varphi(n)$ and

$$N_n(2,1) = n \prod_{p \mid n} \left(1 - \frac{2}{p}\right). \tag{2.1.5}$$

Interestingly, the function $N_n(2,1)$ was applied by D. N. Lehmer [78] 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 [33, 34]), and also has interesting applications to Cayley graphs (see [114, 115]).

The problem in the case of k variables can be interpreted as a 'restricted partition problem modulo n' ([102]), or an equation in the ring $\mathbb{Z}_n$, where the solutions are its units ([33, 114, 115]). 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 [67] and the references therein. The results of Ramanathan [106, Th. 5 and 6] are similar to (2.1.2) and

(2.1.3), but in another context. See also McCarthy [91, Ch. 3] and Spilker [125] for further results with these and different restrictions on linear congruences.

The general case of the restricted linear congruence

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}, \quad (x_i, n) = t_i \ (1 \le i \le k), \tag{2.1.6}$$

was considered by Sburlati [116]. A formula for the number of solutions of (2.1.6) was deduced in [116, 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 (2.1.6) were considered, respectively, by Sander and Sander [115], and Sun and Yang [129]. Cohen [29, Th. 4, 5] derived two explicit formulas for the number of solutions of (2.1.6) with $t_i = 1$, $a_i \mid n$, a_i prime $(1 \le i \le k)$. Jacobson and Williams [65] 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 ([85]), which has very interesting combinatorial and topological applications, in particular in counting non-isomorphic maps on orientable surfaces (see [12, 85, 92, 93, 131, 139]). The problem is also related to Harvey's famous theorem on the cyclic groups of automorphisms of compact Riemann surfaces; see Remark 2.3.15. We also remark that, recently, Yang and Tang [144] considered the quadratic version of this problem in the special case of $k = 2$, $a_1 = a_2 = 1$, $t_1 = t_2 = 1$, and posed some problems for more general cases.

The above general case of the restricted linear congruence (2.1.6) can be considered as relevant to the generalized knapsack problem (see Remark 2.3.13). The *knapsack problem* is of significant interest in cryptography, computational complexity, and several other areas. Micciancio [96] proposed a generalization of this problem to arbitrary rings, and studied its average-case complexity. This *generalized knapsack problem*, proposed by Micciancio [96], 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. [4], 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 [49] gave a short proof for this result,

and also obtained a formula for the number of such solutions. In Theorem 2.3.1 (see Section 6.2) 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 6.2, we obtain an explicit formula for the number of solutions of the restricted linear congruence (2.1.6) 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 discrete Fourier transform (DFT) of arithmetic functions, of which properties are reviewed in Section 7.2. Bibak et al. [19] applied this explicit formula in constructing an almost-universal hash function family and gave some applications to authentication and secrecy codes.

2.2 Preliminaries

In this section, we review Ramanujan sums, the discrete Fourier transform (DFT) of arithmetic functions, and some of their properties which are needed in this chapter. Throughout the dissertation we use $(a_1, \ldots, a_k)$ and $\operatorname{lcm}(a_1, \ldots, a_k)$ to denote, respectively, the greatest common divisor and the least common multiple of integers $a_1, \ldots, a_k$, 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 $p^r \mid\mid a$ if $p^r \mid a$ and $p^{r+1} \nmid a$. We also use $\mathbf{0}$ to denote the vector of all zeroes. The multiplicative group of integers modulo n is denoted by $\mathbb{Z}_n^*$.

2.2.1 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 $n \geq 1$,

$$\sum_{j=1}^{n} e\left(\frac{jm}{n}\right) = \begin{cases} n, & \text{if } n \mid m, \\ 0, & \text{if } n \nmid m. \end{cases} \tag{2.2.1}$$

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

$$c_n(m) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\left(\frac{jm}{n}\right) \tag{2.2.2}$$

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 2.2.1 below). From (2.2.2) 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 2.2.1 or Theorem 2.2.3 (see below), $c_n(1) = \mu(n)$, where $\mu(n)$ is the *Möbius function* defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \text{ is not square-free}, \\ (-1)^{\kappa}, & \text{if } n \text{ is the product of } \kappa \text{ distinct primes}. \end{cases} \tag{2.2.3}$$

The following theorem, attributed to Kluyver [68], gives an explicit formula for $c_n(m)$:

Theorem 2.2.1. *For integers m and n, with $n \geq 1$,*

$$c_n(m) = \sum_{d \,|\, (m,n)} \mu\Big(\frac{n}{d}\Big)\, d. \tag{2.2.4}$$

Thus, $c_n(m)$ can be easily computed provided n can be factored efficiently. By applying the Möbius inversion formula, Theorem 2.2.1 yields the following property: For $m, n \geq 1$,

$$\sum_{d \,|\, n} c_d(m) = \begin{cases} n, & \text{if } n \mid m, \\ 0, & \text{if } n \nmid m. \end{cases} \tag{2.2.5}$$

The case $m = 1$ of (2.2.5) gives the *characteristic property* of the Möbius function:

$$\sum_{d \,|\, n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases} \tag{2.2.6}$$

Note that Theorem 2.2.1 has several other important consequences:

Corollary 2.2.2. *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 $(r \geq 1)$,

$$c_{p^r}(m) = \begin{cases} p^r - p^{r-1}, & \text{if } p^r \mid m, \\ -p^{r-1}, & \text{if } p^{r-1} \parallel m, \\ 0, & \text{if } p^{r-1} \nmid m. \end{cases} \tag{2.2.7}$$

(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* ([138]) is defined by

$$\Phi(m,n) = \frac{\varphi(n)}{\varphi\left(\frac{n}{(m,n)}\right)} \mu\left(\frac{n}{(m,n)}\right). \tag{2.2.8}$$

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 [68]:

Theorem 2.2.3. *For integers m and n, with $n \geq 1$, we have*

$$\Phi(m,n) = c_n(m). \tag{2.2.9}$$

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

Theorem 2.2.4. ([28]) *If $n \geq 1$, $d_1 \mid n$, and $d_2 \mid n$, then we have*

$$\sum_{d \mid n} c_{d_1}\left(\frac{n}{d}\right) c_d\left(\frac{n}{d_2}\right) = \begin{cases} n, & \text{if } d_1 = d_2, \\ 0, & \text{if } d_1 \neq d_2. \end{cases} \tag{2.2.10}$$

We close this subsection by mentioning that, very recently, Fowler et al. [42] 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.

2.2.2 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 (2.2.2) 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

$$\widehat{f}(b) = \sum_{j=1}^{n} f(j) e\left(\frac{-bj}{n}\right) \quad (b \in \mathbb{Z}). \tag{2.2.11}$$

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

$$f(b) = \frac{1}{n} \sum_{j=1}^{n} \widehat{f}(j) e\left(\frac{bj}{n}\right) \quad (b \in \mathbb{Z}), \tag{2.2.12}$$

which is the *inverse discrete Fourier transform* (IDFT); see, e.g., [99, 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

$$\mathcal{F}(f_1 \otimes \cdots \otimes f_k) = \mathcal{F}(f_1) \cdots \mathcal{F}(f_k). \tag{2.2.13}$$

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 2.2.5. *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 2.2.2(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 2.2.6. ([133, 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 (2.2.11) according to the values $d = (m,n)$, taking into account the definition of the n-even functions. □

2.3 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 (2.1.6) 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 [49], one of the main results of [4], and also a key lemma in [102] (Lemma 1).

Theorem 2.3.1. *Let a, b, $n \ge 1$ and $t \ge 1$ 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 $\left(a, \frac{n}{t}\right) = \left(\frac{b}{t}, \frac{n}{t}\right)$. Furthermore, if these conditions are satisfied, then there are exactly*

$$\frac{\varphi\left(\frac{n}{t}\right)}{\varphi\left(\frac{n}{td}\right)} = d \prod_{\substack{p \,|\, d \\ p \nmid \frac{n}{td}}} \left(1 - \frac{1}{p}\right) \tag{2.3.1}$$

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 (2.2.6) 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 $(\mathrm{mod}\ d)$. 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 2.3.2. *In [4] the authors only prove the first part of Theorem 2.3.1 in the case of* $t = 1$*, and apply the result in checking the integrity of their authenticated encryption scheme ([4]). Their main result, [4, Th. 5.11], is obtained via a very long argument; however, formula* (2.3.1) *alone gives a one-line proof for [4, Th. 5.11] that*

we omit here.

Corollary 2.3.3. *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 (2.3.1) 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 (2.3.1), 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 2.3.3, in the case of $t = 1$, was obtained in [49, 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 (2.1.6). We note the following multiplicativity property: If $n, m \geq 1$, $(n,m) = 1$, then

$$N_{nm}(t_1, \ldots, t_k) = N_n(u_1, \ldots, u_k) N_m(v_1, \ldots, v_k), \tag{2.3.2}$$

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 2.3.4. *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*

$$N_n(b; t_1, \ldots, t_k) = \frac{1}{n} \sum_{d \mid n} c_d(b) \prod_{i=1}^{k} c_{\frac{n}{t_i}}\left(\frac{n}{d}\right) \geq 0. \tag{2.3.3}$$

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 (2.2.13) and Theorem 2.2.5,

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

where the variable for the DFT is b ($n, t_1, \ldots, t_k$ being parameters). Now the IDFT formula (2.2.12) 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 2.2.2(iii) and the associativity of gcd one has for every i ($1 \le i \le k$),

$$c_{\frac{n}{t_i}}((j,n)) = c_{\frac{n}{t_i}}\left(\left((j,n), \frac{n}{t_i}\right)\right) = c_{\frac{n}{t_i}}\left(\left(j, \left(n, \frac{n}{t_i}\right)\right)\right) = c_{\frac{n}{t_i}}\left(\left(j, \frac{n}{t_i}\right)\right) = c_{\frac{n}{t_i}}(j). \tag{2.3.4}$$

The properties (2.3.4) 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 2.2.6 we obtain (2.3.3). □

Remark 2.3.5. *Note that a slight modification of the proof of [131, Prop. 21] furnishes an alternate proof for Theorem 2.3.4. Sun and Yang [129] obtained a different formula (with a longer proof) for the number of solutions of the linear congruence in Theorem 2.3.4, but we need the equivalent formula* (2.3.3) *for the purposes of this chapter (see also [14] 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 [131, Prop. 9] to be equivalent to the orbicyclic (multivariate arithmetic) function defined in [85] 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 [12, 85, 92, 131]. See also [93, 139].

Now, using Theorem 2.3.1 and Theorem 2.3.4, we obtain the following general formula for the number of solutions of the restricted linear congruence (2.1.6).

Theorem 2.3.6. *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 $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \leq i \leq k)$, is*

$$N_n(b; a_1, t_1, \ldots, a_k, t_k) = \frac{1}{n}\left(\prod_{i=1}^{k}\frac{\varphi\left(\frac{n}{t_i}\right)}{\varphi\left(\frac{n}{t_id_i}\right)}\right)\sum_{d\,|\,n}c_d(b)\prod_{i=1}^{k}c_{\frac{n}{t_id_i}}\left(\frac{n}{d}\right) \tag{2.3.5}$$

$$= \frac{1}{n}\left(\prod_{i=1}^{k}\varphi\left(\frac{n}{t_i}\right)\right)\sum_{d\,|\,n}c_d(b)\prod_{i=1}^{k}\frac{\mu\left(\frac{d}{(a_it_i,d)}\right)}{\varphi\left(\frac{d}{(a_it_i,d)}\right)}, \tag{2.3.6}$$

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

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 $(x_i, n) = t_i$ $(1 \leq i \leq k)$. Let $a_ix_i \equiv y_i \pmod{n}$ $(1 \leq i \leq k)$. Then $(a_ix_i, n) = (y_i, n) = t_id_i$, for some d_i $(1 \leq i \leq k)$. 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 2.3.4, the number of solutions of the linear congruence $y_1+\cdots+y_k \equiv b \pmod{n}$, with $(y_i, n) = t_id_i$ $(1 \leq i \leq k)$, is

$$\frac{1}{n}\sum_{d\,|\,n}c_d(b)\prod_{i=1}^{k}c_{\frac{n}{t_id_i}}\left(\frac{n}{d}\right). \tag{2.3.7}$$

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 $(x_i, n) = t_i$ $(1 \leq i \leq k)$. Since $(a_i, \frac{n}{t_i}) = (\frac{y_i}{t_i}, \frac{n}{t_i}) = d_i$, by Theorem 2.3.1, the latter congruence has exactly

$$\frac{\varphi(\frac{n}{t_i})}{\varphi(\frac{n}{t_id_i})} \tag{2.3.8}$$

solutions. Combining (2.3.7) and (2.3.8) we get the formula (2.3.5).

Furthermore, applying von Sterneck's formula, (2.2.9), we deduce

$$c_{\frac{n}{t_id_i}}\left(\frac{n}{d}\right) = \frac{\varphi(\frac{n}{t_id_i})\mu(w_i)}{\varphi(w_i)}, \tag{2.3.9}$$

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

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

By inserting (2.3.9) into (2.3.5) we get (2.3.6). □

Remark 2.3.7. *For fixed a_i, t_i $(1 \le i \le k)$ and fixed n, the function*

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

is an even function (mod n). This follows from the formula (2.3.5)*, showing that*

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

is a linear combination of the functions $b \mapsto c_d(b)$ $(d \mid n)$, which are all even (mod n) by (2.2.4)*. See also* (2.3.4)*.*

Remark 2.3.8. *In the case of $k = 1$, by comparing Theorem 2.3.1 with formula* (2.3.5) *and by denoting $t_1 d_1 = s$, we obtain, as a byproduct, the following identity, which is similar to* (2.2.10) *(and can also be proved directly): If $b, n \in \mathbb{Z}$, $n \ge 1$, and $s \mid n$, then*

$$\sum_{d \mid n} c_d(b) c_{\frac{n}{s}}\left(\frac{n}{d}\right) = \begin{cases} n, & \text{if } (b,n) = s, \\ 0, & \text{if } (b,n) \ne s. \end{cases} \tag{2.3.10}$$

While Theorem 2.3.6 is useful from several aspects (for example, we use it in the proof of Theorem 4.3.3), for many applications (for example, the ones considered in this dissertation) we need a more explicit formula.

If in (2.1.6) 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 (2.1.6) and assume that there is an i_0 such that $a_{i_0} \ne 0$. For every prime divisor p of n let r_p be the exponent of p in the prime factorization of n and let $m_p = m_p(a_1, t_1, \dots, a_k, t_k)$ 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

$$e_p = e_p(a_1, t_1, \dots, a_k, t_k) = \#\{i : 1 \le i \le k, p^{m_p} \nmid a_i t_i\}.$$

By definition, $1 \le e_p \le$ the number of i such that $a_i \neq 0$. Note that in many situations instead of $m_p(a_1, t_1, \dots, a_k, t_k)$ we write m_p and instead of $e_p(a_1, t_1, \dots, a_k, t_k)$ we write e_p for short. However, it is important to note that both m_p and e_p always depend on $a_1, t_1, \dots, a_k, t_k, p$.

Theorem 2.3.9. *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 $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, 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*

$$\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ m_p \le r_p \\ p^{m_p} \mid b}} p^{m_p - r_p - 1}\left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \prod_{\substack{p \mid n \\ m_p \le r_p \\ p^{m_p - 1} \parallel b}} p^{m_p - r_p - 1}\left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right), \tag{2.3.11}$$

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 (2.3.6) 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 (2.2.5) and (2.2.7) that

$$W = \begin{cases} p^{m_p-1}\left(1 - \frac{(-1)^{e_p-1}}{(p-1)^{e_p-1}}\right), & \text{if } p^{m_p} \mid b, \\ p^{m_p-1}\left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right), & \text{if } p^{m_p-1} \parallel b, \\ 0, & \text{if } p^{m_p-1} \nmid b. \end{cases} \tag{2.3.12}$$

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 (2.2.5),

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

Inserting into (2.3.6) and by using the multiplicativity property (2.3.2) 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 (2.3.11). □

Interestingly, if in Theorem 2.3.9 we put $a_i = t_i = 1$ $(1 \leq i \leq k)$ then we get the following result first proved by Rademacher [105] in 1925 and Brauer [21] in 1926.

Corollary 2.3.10. *Let $b, n \in \mathbb{Z}$ and $n \geq 1$. The number of solutions of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with $(x_i, n) = 1$ $(1 \leq i \leq k)$ is*

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

Proof. Since $a_i = t_i = 1$ $(1 \leq i \leq k)$, for every prime divisor p of n we have $m_p = 1$

and $e_p = k$. So, for every prime divisor p of n we also have $m_p = 1 \leq r_p$. Clearly, the first part of Theorem 2.3.9 does not hold in this special case, that is, there is no prime $p \mid n$ such that $m_p \leq r_p$ and $p^{m_p-1} \nmid b$ or $m_p \geq r_p + 1$ and $p^{r_p} \nmid b$. Furthermore, we have

$$\prod_{p \mid n, p \mid b} p^{r_p} \prod_{p \mid n, p \nmid b} p^{r_p} = n.$$

Thus, the result follows by a simple application of the second part of Theorem 2.3.9, (2.3.11). □

Corollary 2.3.11. *The restricted congruence given in Theorem 2.3.9 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 2.3.9 and examine the conditions under which the factors of the products in (2.3.11) vanish. □

We note that, while Theorem 2.3.9 may seem a bit complicated, it is in fact easy to work with. Here we show, via several examples, how to apply Theorem 2.3.9.

Example 2.3.12.

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 $24 = 2^3 \cdot 3$,

$2 \mid a_1t_1 = 6$, $2 \mid a_2t_2 = 2$, $2 \mid a_3t_3 = 8$,

$2^2 \nmid a_1t_1 = 6$, $2^2 \nmid a_2t_2 = 2$, $2^2 \mid a_3t_3 = 8$, hence $e_2 = 2$ and $m_2 = 2$, also $2^2 \mid b = 12$,

$3 \mid a_1t_1 = 6$, $3 \nmid a_2t_2 = 2$, $3 \nmid a_3t_3 = 8$, 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 2.3.11(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 2.3.11(v).

Corollary 2.3.11 is the only result in the literature which gives *necessary and sufficient conditions* for the (non-)existence of solutions of restricted linear congruences in their most general case. We believe that Theorem 2.3.9 and Corollary 2.3.11 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 2.3.11 helps us to deal with this problem in a quite natural case:

Remark 2.3.13. *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 2.3.11 holds.*

Remark 2.3.14. *In [19], we applied Theorem 2.3.9 in constructing an almost-universal hash function family using which we gave a generalization of the authentication code with secrecy presented in [4].*

Remark 2.3.15. *Very recently, Bibak et al. [12] using Theorem 2.3.9 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 [92]). 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 [85]).*

Remark 2.3.16. *If $k = 1$ then $e_p = 1$ for every prime $p \mid n$, and it is easy to see that from Theorem 2.3.9 and Corollary 2.3.11 we reobtain Theorem 2.3.1.*

The following formula is a special case of Theorem 2.3.9 and was obtained by Sburlati [116] with an incomplete proof.

Corollary 2.3.17. *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* (2.1.6) *is*

$$\frac{1}{n}\prod_{i=1}^{k}\varphi\left(\frac{n}{t_i}\right)\prod_{p\,|\,n,\,p\,|\,b}\left(1-\frac{(-1)^{e_p-1}}{(p-1)^{e_p-1}}\right)\prod_{p\,|\,n,\,p\nmid b}\left(1-\frac{(-1)^{e_p}}{(p-1)^{e_p}}\right). \tag{2.3.13}$$

2.4 An equivalent form of Theorem 2.3.4

Now, we combine ideas from the finite Fourier transform of arithmetic functions and Ramanujan sums to present a new and short proof for an equivalent form of Theorem 2.3.4 with the hope that its idea might be applicable to other relevant problems. In fact, as problems of this kind have many applications, having generalizations and/or new proofs and/or equivalent formulas for this problem may lead to further work. This theorem generalizes the main results of [27, 37, 102, 115], one of the main results of [114], and also gives an equivalent formula for the main result of [129].

Theorem 2.4.1. *Let $b, n \in \mathbb{Z}$, $n \geq 1$, and $\mathcal{D}_1, \ldots, \mathcal{D}_{\tau(n)}$ be all positive divisors of n. For $1 \leq l \leq \tau(n)$, define $\mathcal{C}_l := \{1 \leqslant x \leqslant n \ : \ (x, n) = \mathcal{D}_l\}$. The number of solutions of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with $\kappa_l = |\{x_1, \ldots, x_k\} \cap \mathcal{C}_l|$, $1 \leq l \leq \tau(n)$, is*

$$\frac{1}{n}\sum_{d\,|\,n} c_d(b)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l}. \tag{2.4.1}$$

Proof. Suppose that $\widehat{f}_n(k, b)$ denotes the number of solutions of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with $\kappa_l = |\{x_1, \ldots, x_k\} \cap \mathcal{C}_l|$, $1 \leq l \leq \tau(n)$. One can observe that, for every $m \in \mathbb{N}$, we have

$$\sum_{b=1}^{n}\widehat{f}_n(k, b)e\left(\frac{bm}{n}\right) = \prod_{l=1}^{\tau(n)}\left(\sum_{x\in\mathcal{C}_l} e\left(\frac{mx}{n}\right)\right)^{\kappa_l}. \tag{2.4.2}$$

First, we give a short combinatorial argument to justify (2.4.2). Here the key idea is that $\widehat{f}_n(k,b)$ can be interpreted as the number of possible ways of writing b as a sum modulo n of κ_1 elements of $\mathcal{C}_1$, κ_2 elements of $\mathcal{C}_2$, ... , $\kappa_{\tau(n)}$ elements of $\mathcal{C}_{\tau(n)}$. Now, expand the right-hand side of (2.4.2). Note that each term of this expansion has $e(\frac{m}{n})$ as a factor (compare this to the left-hand side of (2.4.2)). Also note that the exponent of each term of this expansion (ignoring m) is just a sum of some elements of $\mathcal{C}_1, \ldots, \mathcal{C}_{\tau(n)}$, which equals b $(1 \le b \le n)$. In fact, recalling the above interpretation of $\widehat{f}_n(k,b)$, we can see that in this expansion there are exactly $\widehat{f}_n(k,1)$ terms of the form $e(\frac{m}{n})$, $\widehat{f}_n(k,2)$ terms of the form $e(\frac{2m}{n})$, ... , $\widehat{f}_n(k,n)$ terms of the form $e(m)$; that is, there are exactly $\widehat{f}_n(k,b)$ terms of the form $e(\frac{bm}{n})$, for $1 \le b \le n$. Therefore, we get the left-hand side of (2.4.2).

Putting $x_l' = \frac{x}{\mathcal{D}_l}$, $1 \le l \le \tau(n)$, we get

$$\sum_{x \in \mathcal{C}_l} e\left(\frac{mx}{n}\right) = \sum_{\substack{x=1 \\ (x,n)=\mathcal{D}_l}}^{n} e\left(\frac{mx}{n}\right) = \sum_{\substack{x_l'=1 \\ (x_l', n/\mathcal{D}_l)=1}}^{n/\mathcal{D}_l} e\left(\frac{mx_l'}{n/\mathcal{D}_l}\right) = c_{\frac{n}{\mathcal{D}_l}}(m).$$

Therefore,

$$\sum_{b=1}^{n} \widehat{f}_n(k,b) e\left(\frac{bm}{n}\right) = \prod_{l=1}^{\tau(n)} \left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l}.$$

Now, by (2.2.11) and (2.2.12), and since $c_{\frac{n}{\mathcal{D}_l}}(m) = c_{\frac{n}{\mathcal{D}_l}}((m,n))$, we have

$$\begin{aligned}
\widehat{f}_n(k,b) &= \frac{1}{n}\sum_{m=1}^{n} e\left(\frac{-bm}{n}\right)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l} \\
&= \frac{1}{n}\sum_{d\,|\,n}\sum_{\substack{m=1\\(m,n)=d}}^{n} e\left(\frac{-bm}{n}\right)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(m)\right)^{\kappa_l} \\
&= \frac{1}{n}\sum_{d\,|\,n}\sum_{\substack{m=1\\(m,n)=d}}^{n} e\left(\frac{-bm}{n}\right)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\
&\overset{m'=m/d}{=} \frac{1}{n}\sum_{d\,|\,n}\sum_{\substack{m'=1\\(m',n/d)=1}}^{n/d} e\left(\frac{-bm'}{n/d}\right)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\
&= \frac{1}{n}\sum_{d\,|\,n} c_{n/d}(-b)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\
&= \frac{1}{n}\sum_{d\,|\,n} c_{n/d}(b)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l} \\
&= \frac{1}{n}\sum_{d\,|\,n} c_{d}(b)\prod_{l=1}^{\tau(n)}\left(c_{\frac{n}{\mathcal{D}_l}}(d)\right)^{\kappa_l}.
\end{aligned}$$

□

2.5 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 chapter, 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.

I close this chapter by proposing some problems for future work.

Problem 2.1. It seems that restricted linear congruences can be connected to the famous *zero-sum theory*. Specifically, I think that Corollary 2.3.11 can lead to a new proof of the *Erdős–Ginzberg–Ziv Theorem with units* which was conjectured and proved by some leading number theorists (see [2]).

Problem 2.2. What can we say about *restricted quadratic congruences*, the quadratic version of restricted linear congruences? Right now, there are only some partial results (for $k = 2$) available.

Chapter 3

Applications to Universal Hashing and Authentication with Secrecy

3.1 Introduction

Universal hash functions, discovered by Carter and Wegman [26], have many applications in computer science, including cryptography and information security [20, 38, 52, 54, 57, 58, 109, 134, 140], pseudorandomness [56, 103], complexity theory [112, 122], randomized algorithms [63, 100], data structures [104, 121], and parallel computing [66, 79]. Since universality of hash functions and its variants are concepts central to this work, we begin by describing them in detail. Our description of these concepts closely follows the definitions given in [52].

3.1.1 Universal hashing and its variants

Let D and R be finite sets. Let H be a family of functions from domain D to range R. We say that H is a *universal* family of hash functions ([26]) if the probability, over a random choice of a hash function from H, that two distinct keys in D have the same hash value is at most $1/|R|$. That is, universal hashing captures the important property that distinct keys in D do not *collide* too often. Furthermore, we say that H is an *ε-almost-universal* (ε-AU) family of hash functions if the probability of collision is at most ε, for $\frac{1}{|R|} \leq \varepsilon < 1$. In other words, an ε-AU family, for sufficiently small ε, is *close* to being universal; see Definition 3.1.1 below. Universal and almost-universal hash functions have many applications in algorithm design. For example, they have been used to provide efficient solutions for the dictionary problem in which the goal

is to maintain a dynamic set that is updated using insert and delete operations using small space so that membership queries that ask if a certain element is in S can be answered quickly.

Motivated by applications to cryptography, a notion of Δ-universality was introduced in [72, 110, 128]. Suppose that R is an Abelian group. We say that H is a Δ-*universal* family of hash functions if the probability, over a random $h \in H$, that two distinct keys in D hash to values that are distance b apart for any b in R is $1/|R|$. Note that the case $b = 0$ corresponds to universality. Furthermore, we say that H is ε-*almost-*Δ-*universal* (ε-AΔU) if this probability is at most ε, $\frac{1}{|R|} \leq \varepsilon < 1$. We remark that ε-AΔU families have applications to message authentication. Informally, it is possible to design a message authentication scheme using ε-AΔU families such that two parties can exchange signed messages over an unreliable channel and the probability that an adversary can forge a valid signed message to be sent across the channel is at most ε ([52]). Also, the well-known leftover hash lemma states that (almost) universal hash functions are good randomness extractors.

Finally, in Section 6.3 on authentication codes with secrecy, we need the notion of strong universality which was introduced in [140]. We say that H is a *strongly universal* family of hash functions if the probability, over a random choice of a hash function from H, that two distinct keys x and y in D are mapped to a and b respectively is $1/|R|^2$. We say that H is ε-*almost-strongly-universal* (ε-ASU) if this probability is at most ε, $\frac{1}{|R|^2} \leq \varepsilon < \frac{1}{|R|}$.

We now provide a formal definition of the concepts introduced above as in [52]. For a set $\mathcal{X}$, we write $x \leftarrow \mathcal{X}$ to denote that x is chosen uniformly at random from $\mathcal{X}$.

Definition 3.1.1. Let H be a family of functions from a domain D to a range R. Let ε 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.

- The family 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 ε-*almost-universal* (ε-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. The family H is a Δ-*universal family of hash functions* if for any two distinct $x, y \in D$, and all $b \in R$, we have $\Pr_{h \leftarrow H}[h(x) -$

$h(y) = b] = \frac{1}{|R|}$, where ' $-$ ' denotes the group subtraction operation. Also, H is an *ε-almost-Δ-universal* (ε-AΔU) *family of hash functions* if for any two distinct $x, y \in D$, and all $b \in R$, we have $\Pr_{h \leftarrow H}[h(x) - h(y) = b] \leq \varepsilon$.

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

3.1.2 MMH*

The hash function family we study, GRDH, is a variant of a well-known family which was named MMH* (Multilinear Modular Hashing) by Halevi and Krawczyk [52]. Let p be a prime and k be a positive integer. Each hash function in the family MMH* takes as input a k-tuple, $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$. It computes the dot product of $\mathbf{m}$ with a fixed k-tuple $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$ and outputs this value modulo p.

Definition 3.1.2. Let p be a prime and k be a positive integer. The family MMH* is defined as follows:

$$\text{MMH}^* := \{g_{\mathbf{x}} \ :\ \mathbb{Z}_p^k \to \mathbb{Z}_p \mid \mathbf{x} \in \mathbb{Z}_p^k\}, \tag{3.1.1}$$

where

$$g_{\mathbf{x}}(\mathbf{m}) := \mathbf{m} \cdot \mathbf{x} \pmod p = \sum_{i=1}^{k} m_i x_i \pmod p, \tag{3.1.2}$$

for any $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$, and any $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_p^k$.

The family MMH* is widely attributed to Carter and Wegman [26], while it seems that Gilbert, MacWilliams, and Sloane [44] had already discovered it (but in the finite geometry setting). Halevi and Krawczyk [52], using the multiplicative inverse method, proved that MMH* is a Δ-universal family of hash functions. We also remark that, recently, Leiserson et al. [79] rediscovered MMH* (called it "DOTMIX compression function family") and using the same method as of Halevi and Krawczyk [52] proved that DOTMIX is Δ-universal. Then they apply this result in studying the prob-

lem of deterministic parallel random-number generation for dynamic multithreading platforms in parallel computing.

Theorem 3.1.3. ([52, 79]) *The family* MMH* *is a* Δ*-universal family of hash functions.*

3.1.3 Our contributions

Suppose that, instead of a prime p, one uses an arbitrary integer $n > 1$ in the definition of MMH*. Then we get a generalization of MMH* that we call GMMH* (Generalized Multilinear Modular Hashing). Additionally, we ask that the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ satisfy the conditions $\gcd(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of n. We call this new family GRDH (Generalized Restricted Dot Product Hashing) and refer the reader to Section 6.2 for a formal definition.

Many natural questions arise: What can we say about universality (or ε-almost-universality) of GMMH* and GRDH? What can we say about Δ-universality (or ε-almost-Δ-universality) of GMMH* and GRDH? Recently, Alomair, Clark, and Poovendran [4] presented a construction of codes with secrecy based on a universal hash function family that is a special case of GRDH. Is it possible to generalize their construction and analyse its security properties?

- In Section 3.2, we prove a generalization of Theroem 3.1.3 via connecting the universal hashing problem to the number of solutions of linear congruences.

- In Theorem 3.3.3, we prove that if $n, k > 1$ then the family GRDH is an ε-AU family of hash functions for some $\varepsilon < 1$ if and only if n is odd and $\gcd(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-AU, where p is the smallest prime divisor of n. This bound is tight.

- In Remark 3.3.4, we conclude (from the idea of the proof of Theorem 3.3.3) that if $k = 1$ then the family GRDH is an ε-AU family of hash functions for some $\varepsilon < 1$ if and only if $\gcd(x_1, n) = t_1 = 1$. Furthermore, if $\gcd(x_1, n) = t_1 = 1$ (that is, if $x_1 \in \mathbb{Z}_n^*$) then the collision probability for any two distinct messages is exactly zero.

- In Theorem 3.3.5, we show that if $n > 1$ then the family GRDH is an ε-AΔU family of hash functions for some $\varepsilon < 1$ if and only if n is odd and

$\gcd(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then GRDH is $\frac{1}{p-1}$-AΔU, where p is the smallest prime divisor of n. This bound is tight.

- In Theorem 3.4.2, we generalize the construction of authentication code with secrecy presented in [4, 6]. Using Theorem 3.3.5, we show that our construction is a $\frac{1}{(p-1)n^{k-1}}, \frac{1}{p-1}$-authentication code with secrecy for equiprobable source states on $\mathbb{Z}_n^k \setminus \{\mathbf{0}\}$, where n is odd, and p is the smallest prime divisor of n.

Our results show that if one uses a composite integer n in the definition of MMH* then even by choosing the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$ from $\mathbb{Z}_n^{*k}$, or more generally, choosing the keys $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$ from $\mathbb{Z}_n^k$ with the general conditions $\gcd(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $t_1, \ldots, t_k$ are given positive divisors of n, we cannot get any strong collision bound (unless $k = 1$ and $\gcd(x_1, n) = t_1 = 1$; in this case, as we mentioned above, the collision probability for any two distinct messages is exactly zero). Such impossibility results were not known before.

We believe that connecting the universal hashing problem to the number of solutions of (restricted) linear congruences is a novel idea and could be also of independent interest. A key ingredient in the proofs is Theorem 2.3.9 which gives an explicit formula for the number of solutions of restricted linear congruences (this theorem was proved in the Chapter 2 using properties of Ramanujan sums and of the finite Fourier transform of arithmetic functions). We believe that this is the first work that introduces applications of Ramanujan sums, finite Fourier transform, and restricted linear congruences in the study of universal hashing. We hope this approach will lead to further work.

3.2 GMMH*

Given that, in the definition of MMH*, the modulus is a prime, it is natural to ask what happens if the modulus is an arbitrary integer $n > 1$. Is the resulting family, that we call GMMH*, still Δ-universal? If not, what can we say about ε-almost-universality or ε-almost-Δ-universality of this new family? This is an interesting and natural problem, and while it has a simple solution (see, Theorem 3.2.2 below), to the best of our knowledge there are no results regarding this problem in the literature.

Definition 3.2.1. Let n and k be positive integers $(n > 1)$. The family GMMH*

is defined as follows:

$$\mathrm{GMMH}^* := \{h_{\mathbf{x}} \ : \ \mathbb{Z}_n^k \to \mathbb{Z}_n \mid \mathbf{x} \in \mathbb{Z}_n^k\}, \tag{3.2.1}$$

where

$$h_{\mathbf{x}}(\mathbf{m}) := \mathbf{m} \cdot \mathbf{x} \pmod{n} = \sum_{i=1}^{k} m_i x_i \pmod{n}, \tag{3.2.2}$$

for any $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$, and any $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$.

MMH* has important applications, however, in applications that, for some reasons, we have to work in the ring $\mathbb{Z}_n$, the family GMMH* may be used.

Now, we state and prove the following result about ε-almost-Δ-universality of GMMH*. Proposition 2.1.1, due to D. N. Lehmer [77], is the main ingredient in the proof.

Theorem 3.2.2. *Let n and k be positive integers ($n > 1$). The family* GMMH* *is* $\frac{1}{p}$-AΔU*, where p is the smallest prime divisor of n. This bound is tight.*

Proof. Suppose that n has the prime factorization $n = p_1^{r_1} \ldots p_s^{r_s}$, where $p_1 < \cdots < p_s$ are primes and $r_1, \ldots, r_s$ are positive integers. Let $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$ and $\mathbf{m}' = \langle m_1', \ldots, m_k' \rangle \in \mathbb{Z}_n^k$ be any two distinct messages. Put $\mathbf{a} = \langle a_1, \ldots, a_k \rangle = \mathbf{m} - \mathbf{m}'$. For every $b \in \mathbb{Z}_n$ we have

$$h_{\mathbf{x}}(\mathbf{m}) - h_{\mathbf{x}}(\mathbf{m}') = b \Longleftrightarrow \sum_{i=1}^{k} m_i x_i - \sum_{i=1}^{k} m_i' x_i \equiv b \pmod{n} \Longleftrightarrow \sum_{i=1}^{k} a_i x_i \equiv b \pmod{n}.$$

Note that since $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$, we have n^k ordered k-tuples $\langle x_1, \ldots, x_k \rangle$. Also, since $\mathbf{m} \neq \mathbf{m}'$, there exists some i_0 such that $a_{i_0} \neq 0$. Now, we need to find the maximum number of solutions of the above linear congruence over all choices of $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and $b \in \mathbb{Z}_n$. By Proposition 2.1.1, if $\ell = \gcd(a_1, \ldots, a_k, n) \nmid b$ then the linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv b \pmod{n}$ has no solution, and if $\ell = \gcd(a_1, \ldots, a_k, n) \mid b$ then the linear congruence has ℓn^{k-1} solutions. Thus, we need to find the maximum of $\ell = \gcd(a_1, \ldots, a_k, n)$ over all choices of $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$. Clearly,

$$\max_{\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}} \gcd(a_1, \ldots, a_k, n)$$

is achieved when $a_{i_0} = p_1^{r_1-1}p_2^{r_2}\dots p_s^{r_s} = \frac{n}{p_1}$, and $a_i = 0$ $(i \neq i_0)$. So, we get

$$\max_{\mathbf{a}=\langle a_1,\dots,a_k\rangle\in\mathbb{Z}_n^k\setminus\{\mathbf{0}\}} \gcd(a_1,\dots,a_k,n) = p_1^{r_1-1}p_2^{r_2}\dots p_s^{r_s} = \frac{n}{p_1}.$$

Therefore, for any two distinct messages $\mathbf{m}, \mathbf{m}' \in \mathbb{Z}_n^k$, and all $b \in \mathbb{Z}_n$, we have

$$\Pr_{h_{\mathbf{x}}\leftarrow\text{GMMH}^*}[h_{\mathbf{x}}(\mathbf{m}) - h_{\mathbf{x}}(\mathbf{m}') = b] \leq \max_{\mathbf{a}=\langle a_1,\dots,a_k\rangle\in\mathbb{Z}_n^k\setminus\{\mathbf{0}\}} \frac{n^{k-1}\gcd(a_1,\dots,a_k,n)}{n^k} = \frac{1}{p_1}.$$

This means that GMMH* is $\frac{1}{p_1}$-AΔU. Clearly, this bound is tight; take, for example, $a_1 = \frac{n}{p_1}$ and $a_2 = \cdots = a_k = 0$. □

Corollary 3.2.3. *If in* Theorem 3.2.2 *we let n be a prime then we obtain* Theorem 3.1.3.

Proof. When n is prime, $\gcd_{\mathbf{a}=\langle a_1,\dots,a_k\rangle\in\mathbb{Z}_n^k\setminus\{\mathbf{0}\}}(a_1,\dots,a_k,n) = 1$, so we get Δ-universality. □

We remark that if in the family GMMH* we let the keys $\mathbf{x} = \langle x_1,\dots,x_k\rangle \in \mathbb{Z}_n^k$ satisfy the general conditions $\gcd(x_i,n) = t_i$ $(1 \leq i \leq k)$, where $t_1,\dots,t_k$ are given positive divisors of n, then the resulting family, which we call GRDH, is no longer 'always' ε-AΔU; see the next section for details.

3.3 GRDH

In this section, we introduce a variant of MMH* that we call GRDH (Generalized Restricted Dot Product Hashing). Then we investigate the ε-almost-universality and ε-almost-Δ-universality of GRDH via connecting the problem to the number of solutions of restricted linear congruences.

Definition 3.3.1. Let n and k be positive integers $(n > 1)$. We define the family RDH as follows:

$$\text{RDH} := \{\Upsilon_{\mathbf{x}} \ : \ \mathbb{Z}_n^k \to \mathbb{Z}_n \ : \ \mathbf{x} \in \mathbb{Z}_n^{*k}\}, \tag{3.3.1}$$

where

$$\Upsilon_{\mathbf{x}}(\mathbf{m}) := \mathbf{m}\cdot\mathbf{x} \pmod n = \sum_{i=1}^{k} m_i x_i \pmod n, \tag{3.3.2}$$

for any $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^{*k}$, and any $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$. Suppose that $t_1, \ldots, t_k$ are given positive divisors of n. Now, if in the definition of RDH instead of having $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^{*k}$, we have, more generally, $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i$ $(1 \leq i \leq k)$, then we get a generalization of RDH that we call GRDH.

It would be interesting to investigate for which values of n, GRDH is ε-AU or ε-AΔU. We now deal with these problems. The explicit formula for the number of solutions of restricted linear congruences (Theorem 2.3.9) along with our approach for giving a generalization of Theorem 3.1.3 play key roles here.

First, we prove the following lemma which is needed in proving the main results.

Lemma 3.3.2. *Let k and n be positive integers ($n > 1$). For every prime divisor p of n let r_p be the exponent of p in the prime factorization of n. Also, suppose that $t_1, \ldots, t_k$ are given positive divisors of n. There are the following two cases:*
(i) If there exists some i_0 such that $t_{i_0} \neq 1$ then there exists $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \backslash \{\mathbf{0}\}$ such that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, t_1, \ldots, a_k, t_k) > r_p$.
(ii) If $t_i = 1$ $(1 \leq i \leq k)$ then for every $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ there exists at least one prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$.

Proof. (i) WLOG, let $t_1 \neq 1$, say, $t_1 = t$ with $t \mid n$ and $t > 1$. Take $a_1 = \frac{n}{t}$ and $a_2 = \cdots = a_k = 0$. Now, for every prime $p \mid n$ we have $p^{r_p} \mid a_i t_i$ $(1 \leq i \leq k)$. Therefore, for every prime $p \mid n$ we have $\mathfrak{m}_p(\frac{n}{t}, t, 0, t_2, \ldots, 0, t_k) > r_p$.
(ii) Let $t_i = 1$ $(1 \leq i \leq k)$ and $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ be given. Suppose that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, \ldots, a_k) > r_p$. This implies that for every prime $p \mid n$ we have $p^{r_p} \mid a_i$ $(1 \leq i \leq k)$. Therefore, we get $n \mid a_i$ $(1 \leq i \leq k)$ which is not possible because there exists some i such that $a_i \in \mathbb{Z}_n \setminus \{0\}$. □

Now, we are ready to investigate the ε-almost-universality of GRDH.

Theorem 3.3.3. *Let n and k be positive integers $(n, k > 1)$. The family* GRDH *is an ε-*AU *family of hash functions for some $\varepsilon < 1$ if and only if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then* GRDH (*which is then reduced to* RDH) *is $\frac{1}{p-1}$-*AU*, where p is the smallest prime divisor of n. This bound is tight.*

Proof. Assume the setting of the family GRDH, and that $\mathbf{t} = \langle t_1, \ldots, t_k \rangle$ is given. Let $n > 1$ and for every prime divisor p of n let r_p be the exponent of p in the prime factorization of n. Suppose that $\mathbf{m} = \langle m_1, \ldots, m_k \rangle \in \mathbb{Z}_n^k$ and $\mathbf{m}' = \langle m'_1, \ldots, m'_k \rangle \in \mathbb{Z}_n^k$

are any two distinct messages. Put $\mathbf{a} = \langle a_1, \ldots, a_k \rangle = \mathbf{m} - \mathbf{m}'$. Since $\mathbf{m} \neq \mathbf{m}'$, there exists some i such that $a_i \neq 0$. If in the family GRDH there is a collision between $\mathbf{m}$ and $\mathbf{m}'$, this means that there exists an $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with $(x_i, n) = t_i$, $t_i \mid n$ $(1 \leq i \leq k)$ such that $\Upsilon_{\mathbf{x}}(\mathbf{m}) = \Upsilon_{\mathbf{x}}(\mathbf{m}')$. Clearly,

$$\Upsilon_{\mathbf{x}}(\mathbf{m}) = \Upsilon_{\mathbf{x}}(\mathbf{m}') \Longleftrightarrow \sum_{i=1}^{k} a_i x_i \equiv 0 \pmod{n}.$$

So, we need to find the number of solutions $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of the restricted linear congruence $a_1 x_1 + \cdots + a_k x_k \equiv 0 \pmod{n}$, with $(x_i, n) = t_i$, $t_i \mid n$ $(1 \leq i \leq k)$. Here, since $b = 0$, none of the two cases stated in the first part of Theorem 2.3.9 holds. Thus, by formula (2.3.11), there are exactly

$$\prod_{i=1}^{k} \varphi\left(\frac{n}{t_i}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \tag{3.3.3}$$

choices for such $\mathbf{x} = \langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ that satisfy the aforementioned restricted linear congruence, where the last product is over the prime factors p of n with $\mathfrak{m}_p \leq r_p$, r_p is the exponent of p in the prime factorization of n, $\mathfrak{m}_p$ is the smallest $j \geq 1$ such that there is some i with $p^j \nmid a_i t_i$, and

$$e_p = \#\{i : 1 \leq i \leq k, p^{\mathfrak{m}_p} \nmid a_i t_i\}.$$

Also, since $(x_i, n) = t_i$ $(1 \leq i \leq k)$, the *total* number of choices for $\langle x_1, \ldots, x_k \rangle$ is $\prod_{i=1}^{k} \varphi(\frac{n}{t_i})$. Therefore, given any $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$, the collision probability is exactly

$$P_{\mathbf{a}}(n, \mathbf{t}) = \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right). \tag{3.3.4}$$

Now, there are two cases:

(i) If for a prime $p \mid n$ we have $\mathfrak{m}_p \leq r_p$ then, by (3.3.4), the term corresponding to this p in $P_{\mathbf{a}}(n, \mathbf{t})$ equals

$$p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \leq p^{r_p - r_p - 1} \left(1 - \frac{(-1)^{2-1}}{(p-1)^{2-1}}\right) = \frac{1}{p-1}.$$

(ii) If for a prime $p \mid n$ we have $\mathfrak{m}_p > r_p$ then, by (3.3.4), the term corresponding to this p in $P_{\mathbf{a}}(n, \mathbf{t})$ equals 1.

Let there exists some i_0 such that $t_{i_0} \neq 1$. Then, by Lemma 3.3.2(i), there exists an $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ such that for every prime $p \mid n$ we have $\mathfrak{m}_p(a_1, t_1, \ldots, a_k, t_k) > r_p$. Now, by (3.3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ is *exactly one*. Now, assume that $t_i = 1$ $(1 \leq i \leq k)$. Then, if n is even, by taking $a_1 = a_2 = \frac{n}{2}$ and $a_3 = \cdots = a_k = 0$, one can see that $\mathfrak{m}_2(\frac{n}{2}, \frac{n}{2}, 0, \ldots, 0) = r_2$ and $e_2 = 2$, and for every other prime $p \mid n$ we have $\mathfrak{m}_p(\frac{n}{2}, \frac{n}{2}, 0, \ldots, 0) > r_p$. Now, by (3.3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ is *exactly one*.

Now, suppose that n is odd and $t_i = 1$ $(1 \leq i \leq k)$. Then, by Lemma 3.3.2(ii), for every $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ there exists at least one prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$. Now, by (3.3.4) and cases (i), (ii) above, one can see that

$$\max_{\mathbf{a}=\mathbf{m}-\mathbf{m}' \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}} P_{\mathbf{a}}(n, \mathbf{t})$$

is achieved in a specific $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ for which there exists *exactly one* prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$, and furthermore, p has to be the smallest prime divisor of n that we denote by $p_{\min}$.

Consequently, if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$ then for any two distinct messages $\mathbf{m}, \mathbf{m}' \in \mathbb{Z}_n^k$, we have

$$\Pr_{\Upsilon_{\mathbf{x}} \leftarrow \mathrm{GRDH}}[\Upsilon_{\mathbf{x}}(\mathbf{m}) = \Upsilon_{\mathbf{x}}(\mathbf{m}')] \leq \max_{\mathbf{a}=\mathbf{m}-\mathbf{m}' \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}} P_{\mathbf{a}}(n, \mathbf{t}) \leq \frac{1}{p_{\min} - 1} \leq \frac{1}{2}.$$

Therefore, if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$ then GRDH (which is then reduced to RDH) is $\frac{1}{p_{\min}-1}$-AU. We also note that this bound is tight: take $a_1 = a_2 = \frac{n}{p_{\min}}$ and $a_3 = \cdots = a_k = 0$. So, we get that $\mathfrak{m}_{p_{\min}}(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) = r_{p_{\min}}$ and $e_{p_{\min}} = 2$, and for every other prime $p \mid n$ we get that $\mathfrak{m}_p(\frac{n}{p_{\min}}, \frac{n}{p_{\min}}, 0, \ldots, 0) > r_p$. Now, by (3.3.4) and case (ii) above, the collision probability for this specific $\mathbf{a}$ is *exactly* $\frac{1}{p_{\min}-1} \leq \frac{1}{2}$. □

The following remark gives a necessary and sufficient condition for the ε-almost-universality of the family GRDH in the case of $k = 1$. We omit the proof as it is simply obtained from the above argument (this special case can also be proved directly, or, from [17, Th. 3.1]).

Remark 3.3.4. *If $k = 1$ then the family* GRDH *is an ε-*AU *family of hash functions for some $\varepsilon < 1$ if and only if $(x_1, n) = t_1 = 1$. Furthermore, if $(x_1, n) = t_1 = 1$ then the collision probability for any two distinct messages is exactly zero.*

Now, we investigate the ε-almost-Δ-universality of GRDH. Note the change from $k > 1$ in Theorem 3.3.3 to $k \geq 1$ in Theorem 3.3.5. The proof idea is similar to that of Theorem 3.3.3; so, in the proof we only write the parts which need more arguments.

Theorem 3.3.5. *Let n and k be positive integers ($n > 1$). The family* GRDH *is an ε-*AΔU *family of hash functions for some $\varepsilon < 1$ if and only if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$. Furthermore, if these conditions are satisfied then* GRDH (*which is then reduced to* RDH) *is $\frac{1}{p-1}$-*AΔU*, where p is the smallest prime divisor of n. This bound is tight.*

Proof. Assume the setting of the family GRDH, and that $\mathbf{t} = \langle t_1, \ldots, t_k \rangle$ is given. Let $n > 1$ and for every prime divisor p of n let r_p be the exponent of p in the prime factorization of n. If for a given $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and a given $b \in \mathbb{Z}_n$ there is a prime $p \mid n$ such that $\mathfrak{m}_p \leq r_p$ and $p^{\mathfrak{m}_p - 1} \nmid b$, or, such that $\mathfrak{m}_p \geq r_p + 1$ and $p^{r_p} \nmid b$, then, by the first part of Theorem 2.3.9, the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ is *exactly zero*. Otherwise, given any $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and any $b \in \mathbb{Z}_n$, the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ is exactly

$$Q_{\mathbf{a},b}(n, \mathbf{t}) = \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p \\ p^{\mathfrak{m}_p} \mid b}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \prod_{\substack{p \mid n \\ \mathfrak{m}_p \leq r_p \\ p^{\mathfrak{m}_p - 1} \parallel b}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right). \tag{3.3.5}$$

Now, there are three cases:
(i) If for a prime $p \mid n$ we have $\mathfrak{m}_p \leq r_p$ and $p^{\mathfrak{m}_p - 1} \parallel b$ then, by (3.3.5), the term corresponding to this p in $Q_{\mathbf{a},b}(n, \mathbf{t})$ equals

$$p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p}}{(p-1)^{e_p}}\right) \leq p^{r_p - r_p - 1} \left(1 - \frac{(-1)^1}{(p-1)^1}\right) = \frac{1}{p-1}.$$

(ii) If for a prime $p \mid n$ we have $\mathfrak{m}_p \leq r_p$ and $p^{\mathfrak{m}_p} \mid b$ then, by (3.3.5), the term corresponding to this p in $Q_{\mathbf{a},b}(n, \mathbf{t})$ equals

$$p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \leq p^{r_p - r_p - 1} \left(1 - \frac{(-1)^{2-1}}{(p-1)^{2-1}}\right) = \frac{1}{p-1}.$$

(iii) If for a prime $p \mid n$ we have $\mathfrak{m}_p > r_p$ and $p^{r_p} \mid b$ then, by (3.3.5), the term corresponding to this p in $Q_{\mathbf{a},b}(n,\mathbf{t})$ equals 1.

If there exists some i_0 such that $t_{i_0} \neq 1$ then the argument is exactly the same as before (just take $b = 0$). Now, assume that $t_i = 1$ $(1 \leq i \leq k)$. Then, if n is even, take $a_1 = b = \frac{n}{2}$ and $a_2 = \cdots = a_k = 0$. Now, one can see that, by (3.3.5) and case (iii) above, the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ for these specific $\mathbf{a}$ and b is *exactly one*.

Now, suppose that n is odd and $t_i = 1$ $(1 \leq i \leq k)$. Then, by (3.3.5), Lemma 3.3.2(ii), and cases (i), (ii), (iii) above, one can see that

$$\max_{\substack{\mathbf{a}=\mathbf{m}-\mathbf{m}' \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\} \\ b \in \mathbb{Z}_n}} Q_{\mathbf{a},b}(n,\mathbf{t})$$

is achieved in a specific $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\}$ and a specific $b \in \mathbb{Z}_n$ for which there exists *exactly one* prime $p \mid n$ such that $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$ and $p^{\mathfrak{m}_p - 1} \mid\mid b$, or, $\mathfrak{m}_p(a_1, \ldots, a_k) \leq r_p$ and $p^{\mathfrak{m}_p} \mid b$, and also $p^{r_p} \mid b$ for every other prime $p \mid n$; furthermore, p has to be the smallest prime divisor of n that we denote by $p_{\min}$.

Consequently, if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$ then for any two distinct messages $\mathbf{m}, \mathbf{m}' \in \mathbb{Z}_n^k$, and all $b \in \mathbb{Z}_n$, we have

$$\Pr_{\Upsilon_{\mathbf{x}} \leftarrow \mathrm{GRDH}}[\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b] \leq \max_{\substack{\mathbf{a}=\mathbf{m}-\mathbf{m}' \in \mathbb{Z}_n^k \setminus \{\mathbf{0}\} \\ b \in \mathbb{Z}_n}} Q_{\mathbf{a},b}(n,\mathbf{t}) \leq \frac{1}{p_{\min} - 1} \leq \frac{1}{2}.$$

Therefore, if n is odd and $(x_i, n) = t_i = 1$ $(1 \leq i \leq k)$ then GRDH (which is then reduced to RDH) is $\frac{1}{p_{\min}-1}$-AΔU. We also note that this bound is tight: take $a_1 = b = \frac{n}{p_{\min}}$ and $a_2 = \cdots = a_k = 0$. Now, by (3.3.5) and case (iii) above, one can see that the probability that we have $\Upsilon_{\mathbf{x}}(\mathbf{m}) - \Upsilon_{\mathbf{x}}(\mathbf{m}') = b$ for these specific $\mathbf{a}$ and b is *exactly* $\frac{1}{p_{\min}-1}$. □

Remark 3.3.6. *While the proofs of Theorem 3.3.3 and Theorem 3.3.5 are simple thanks to Theorem 2.3.9, there may be simpler proofs (say, without relying on the counting arguments as we do) for these results. However, given the general statements of Theorem 3.3.3 and Theorem 3.3.5, possible simpler proofs for these results which cover the 'whole' statements may not be necessarily that shorter. Besides, we believe that our proof techniques have their own merit and these connections and techniques may motivate more work in universal hashing and related areas.*

Remark 3.3.7. *If in Theorem 3.3.5 we let $k = 1$, then we get the main result of the*

paper by Alomair et al. [4, Th. 5.11] which was obtained via a very long argument.

Remark 3.3.8. *Using Theorem 2.3.9 and the idea of the proof of Theorem 3.3.5 one can see that there are cases in which the collision probability in the family* GRDH *is exactly zero (Corollary 2.3.11 completely characterizes these cases). This can be considered an advantage of the family* GRDH *and is not the case in the family* MMH**, as the collision probability in* MMH* *is exactly* $\frac{1}{p}$ *which never vanishes.*

3.4 Applications to authentication with secrecy

As an application of the results of the preceding section, we propose an authentication code with secrecy scheme which generalizes a recent construction [4, 6]. We remark that Alomair et al. have applied their scheme in several other papers; see, e.g., [5] for an application of this approach in the authentication problem in RFID systems. So, our results may have implications in those applications, as well. We adopt the notation of [90] in specifying the syntax of these codes. In particular, we consider key-indexed families of coding rules.

An *authentication code with secrecy* (or *code* for short) is a tuple $\mathrm{C} = (\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, specified by the following sets: $\mathcal{S}$ of *source states* (or *plaintexts*), $\mathcal{M}$ of *messages* (or *ciphertexts*), $\mathcal{K}$ of *keys*, $\mathcal{E}$ of *authenticated encryption (AE) functions* and $\mathcal{D}$ of *verified decryption functions*. The sets $\mathcal{E}$ and $\mathcal{D}$ are indexed by $\mathcal{K}$. For $k \in \mathcal{K}$, $\mathcal{E}_k : \mathcal{S} \to \mathcal{M}$ is the associated authenticated encryption function and $D_k : \mathcal{M} \to \mathcal{S} \cup \{\perp\}$ is the associated verified decryption function. The encryption and decryption functions have the property that for every $m \in \mathcal{S}$, $\mathcal{D}_k(\mathcal{E}_k(m)) = m$. Moreover, for any $c \in \mathcal{M}$, if $c \neq \mathcal{E}_k(m)$ for some $m \in \mathcal{S}$, $\mathcal{D}_k(c) = \perp$.

Before presenting our construction, we first note that although it is not explicitly stated in [4, 6], the construction given there is correct only for the case of a uniform distribution on source states. This will be the case for our construction, as well. We note that this assumption, while unrealistically strong from a security perspective, is commonly used in the study of authentication codes with secrecy. Following the terminology of [61] (see also [62]), we will call such codes *authentication and secrecy codes for equiprobable source probability distributions*. Henceforth we will work under the assumption of equiprobable source states.

We now give the security definitions required for authentication and secrecy. We begin with a definition of secrecy.

Definition 3.4.1. We say that $\mathrm{C} = (\mathcal{S}, \mathcal{M}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ provides *ε-secrecy* on $\mathcal{S}' \subseteq \mathcal{S}$ if every $m \in \mathcal{S}'$ and $c \in \mathcal{M}$,

$$\Pr_{m' \leftarrow \mathcal{S}, k \leftarrow \mathcal{K}}[m' = m | \mathcal{E}_k(m') = c] \leq \varepsilon.$$

Thus, $\frac{1}{|\mathcal{S}|}$-secrecy on $\mathcal{S}$ corresponds to the standard notion of Shannon secrecy [120] (for a uniform message distribution).

With respect to authentication, we restrict attention to *substitution attacks*, also known as *spoofing attacks of order* 1. A C-*forger* is a mapping $\mathcal{F} : \mathcal{M} \to \mathcal{M}$. Note that there are no computational restrictions on $\mathcal{F}$. We say that C is *δ-secure against substitution attacks* if for every C-forger $\mathcal{F}$,

$$\Pr_{m \leftarrow \mathcal{S}, k \leftarrow \mathcal{K}, c \leftarrow \mathcal{E}_k(m)}[\mathcal{F}(c) \neq c \wedge \mathcal{D}_k(\mathcal{F}(c)) \neq \perp] \leq \delta.$$

Finally, we say that C is an *ε, δ-authentication code with secrecy for equiprobable source states* on $\mathcal{S}'$ if it is ε-secret on $\mathcal{S}'$ and δ-secure against substitution attacks.

For any $n, k \in \mathbb{N}$, we define $\mathrm{C}^{n,k}_{\mathrm{RDH}}$ as follows: $\mathcal{S} = \mathbb{Z}_n^k$, $\mathcal{K} = \mathbb{Z}_n^k \times (\mathbb{Z}_n^*)^k$, $\mathcal{M} = \mathbb{Z}_n^k \times \mathbb{Z}_n$. Thus, source states are k-tuples $\mathbf{m} = \langle m_1, \ldots, m_k \rangle$, keys are pairs $\langle \mathbf{x}, \mathbf{y} \rangle$ of k-tuples $\mathbf{x} = \langle x_1, \ldots, x_k \rangle$, $\mathbf{y} = \langle y_1, \ldots, y_k \rangle$, and ciphertexts are pairs $\langle \mathbf{c}, t \rangle$.

Note that we will sometimes write pairs using the notation $\cdot||\cdot$ rather than the usual $\langle \cdot, \cdot \rangle$, e.g., we write a key pair as $\mathbf{x}||\mathbf{y}$. Also, we may abuse terminology, and for a ciphertext $\mathbf{c}||t$, call $\mathbf{c}$ the ciphertext and t the *tag*. The authenticated encryption function $\mathcal{E}$ is defined as follows:

$$\mathcal{E}_{\mathbf{x}||\mathbf{y}}(\mathbf{m}) = \Psi_{\mathbf{x}}(\mathbf{m})||\Upsilon_{\mathbf{y}}(\mathbf{m}),$$

where Υ is the RDH hash function, and

$$\Psi_{\mathbf{x}}(\mathbf{m}) = \mathbf{m} + \mathbf{x} \pmod{n} = \langle m_1 + x_1 \pmod{n}, \ldots, m_k + x_k \pmod{n} \rangle.$$

To define $\mathcal{D}$, we first define Ψ^{-1}:

$$\Psi^{-1}_{\mathbf{x}}(\mathbf{c}) = \mathbf{c} - \mathbf{x} \pmod{n} = \langle c_1 - x_1 \pmod{n}, \ldots, c_k - x_k \pmod{n} \rangle.$$

Then

$$\mathcal{D}_{\mathbf{x}||\mathbf{y}}(\mathbf{c}||t) = \begin{cases} \Psi_{\mathbf{x}}^{-1}(\mathbf{c}) & \text{if } \Upsilon_{\mathbf{y}}(\Psi_{\mathbf{x}}^{-1}(\mathbf{c})) = t; \\ \perp & \text{otherwise.} \end{cases}$$

Now, we are ready to state and prove our main result in this section:

Theorem 3.4.2. *Let $n, k \in \mathbb{N}$, where n is odd, and p the smallest prime divisor of n. Then $\mathrm{C}_{\mathrm{RDH}}^{n,k}$ is a $\frac{1}{(p-1)n^{k-1}}, \frac{1}{p-1}$-authentication code with secrecy for equiprobable source states on $\mathbb{Z}_n^k \setminus \{\mathbf{0}\}$.*

We will establish this theorem by the following sequence of lemmas.

Lemma 3.4.3. *Let $n, k \in \mathbb{N}$, where n is odd, and p the smallest prime divisor of n. Then $\mathrm{C}_{\mathrm{RDH}}^{n,k}$ is $\frac{1}{(p-1)n^{k-1}}$-secret on $\mathbb{Z}_n^k \setminus \{\mathbf{0}\}$.*

Proof. We first note that for any $\mathbf{m}$, $\mathbf{c}$, and t,

$$\Pr_{\mathbf{m}',\mathbf{x}\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\mathbf{m}' = \mathbf{m}|\mathcal{E}_{\mathbf{x}||\mathbf{y}}(\mathbf{m}') = \mathbf{c}||t] = \Pr_{\mathbf{m}'\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\mathbf{m}' = \mathbf{m}|\Upsilon_{\mathbf{y}}(\mathbf{m}') = t].$$

This follows from the independence of $\Psi_{\mathbf{x}}(\mathbf{m}')$ and $\Upsilon_{\mathbf{y}}(\mathbf{m}')$, conditioned on $\mathbf{m}' = \mathbf{m}$, along with the fact that Ψ provides Shannon secrecy. But

$$\begin{aligned} \Pr_{\mathbf{m}'\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\mathbf{m}' = \mathbf{m}|\Upsilon_{\mathbf{y}}(\mathbf{m}') = t] &= \Pr_{\mathbf{m}'\leftarrow\mathbb{Z}_n^k,\mathbf{y}\leftarrow(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}}(\mathbf{m}') = t|\mathbf{m}' = \mathbf{m}]/n^{k-1} \\ &\leq \frac{1}{(p-1)n^{k-1}}, \end{aligned}$$

where the equality follows by Bayes' rule and the fact that for $\mathbf{m}' \leftarrow (\mathbb{Z}_n)^k$ and $\mathbf{y} \leftarrow (\mathbb{Z}_n^*)^k$, $\Upsilon_{\mathbf{y}}(\mathbf{m}')$ is uniformly distributed in $\mathbb{Z}_n$, and the inequality follows, assuming $\mathbf{m} \neq \mathbf{0}$, by Theorem 3.3.5. □

We now establish a *key hiding* property which will be needed to prove resistance to substitution attacks.

Lemma 3.4.4. *For $n, k \in \mathbb{N}$, $\mathbf{y} \in (\mathbb{Z}_n^*)^k$, $\mathbf{c} \in \mathbb{Z}_n^k$ and $t \in \mathbb{Z}_n$,*

$$\Pr_{\mathbf{x},\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}' = \mathbf{y}|\mathcal{E}_{\mathbf{x}||\mathbf{y}'}(\mathbf{m}) = \mathbf{c}||t] = \frac{1}{|(\mathbb{Z}_n^*)^k|}.$$

Proof. First note that since $\mathbf{x}$ and $\mathbf{m}$ are chosen independently of $\mathbf{y}'$, it is the case that $\Psi_{\mathbf{x}}(\mathbf{m})$ and $\mathbf{y}'$ are independent. So we just need to show that

$$\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}' = \mathbf{y}|\Upsilon_{\mathbf{y}'}(\mathbf{m}) = t] = \frac{1}{|(\mathbb{Z}_n^*)^k|}.$$

Note that

$$\begin{aligned}\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}] &= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t\wedge\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\ &= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t\wedge\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\ &= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t]\cdot\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]/\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\ &= \Pr_{\mathbf{m}\in\mathbb{Z}_n^k}[\Upsilon_{\mathbf{y}}(\mathbf{m})=t]=\frac{1}{|\mathbb{Z}_n|},\end{aligned}$$

where the last equality follows because the product of a uniformly random element of $\mathbb{Z}_n$ and a fixed element of $\mathbb{Z}_n^*$ is uniformly distributed in $\mathbb{Z}_n$, and the sum of a fixed number of uniformly random elements of $\mathbb{Z}_n$ is uniformly distributed in $\mathbb{Z}_n$. We now have

$$\begin{aligned}&\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}|\Upsilon_{\mathbf{y}'}(\mathbf{m})=t]\\ &\qquad=\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}]\cdot\frac{\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]}{\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t]}.\end{aligned}\quad(3.4.1)$$

But

$$\begin{aligned}\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t] &= \sum_{\mathbf{y}\in(\mathbb{Z}_n^*)^k}\Pr_{\mathbf{m}\in\mathbb{Z}_n^k,\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\Upsilon_{\mathbf{y}'}(\mathbf{m})=t|\mathbf{y}'=\mathbf{y}]\cdot\Pr_{\mathbf{y}'\in(\mathbb{Z}_n^*)^k}[\mathbf{y}'=\mathbf{y}]\\ &= \frac{1}{|\mathbb{Z}_n|}.\end{aligned}$$

Combining this with (3.4.1) completes the proof. □

Remark 3.4.5. This key hiding property does not hold in general. The given proof depends on the fact that $\mathbf{m}$ is uniformly distributed in $\mathbb{Z}_n^k$.

Lemma 3.4.6. *Let $n, k \in \mathbb{N}$, where n is odd, and p the smallest prime divisor of n. Then $\mathrm{C}_{\mathrm{RDH}}^{n,k}$ is $\frac{1}{p-1}$-secure against substitution attacks.*

Proof. By way of contradiction suppose that $\mathcal{F}$ produces a substitution with probability greater than $\frac{1}{p-1}$. By averaging, there must be some $\mathbf{m} \in \mathbb{Z}_n^k$ such that if $\mathcal{E}_{\mathbf{x}||\mathbf{y}}(\mathbf{m}) = \mathbf{c}||t$, for random $\mathbf{x}$ and $\mathbf{y}$, then $\mathcal{F}(\mathbf{c}||t) = \mathbf{c}'||t'$ such that $\mathbf{c}'||t' \neq \mathbf{c}||t$ and $\Upsilon_{\mathbf{y}}(\Phi_{\mathbf{x}}^{-1})(\mathbf{c}') = t'$. Let $b = t - t'$ and $\mathbf{m}' = (\Phi_{\mathbf{x}}^{-1})(\mathbf{c}')$. Note that it must be the case

that $\mathbf{m}' \neq \mathbf{m}$. By the preceding lemma, $\mathbf{y}$ and $\mathbf{m}'$ are statistically independent. So,

$$\Upsilon_{\mathbf{y}}(\mathbf{m}) - \Upsilon_{\mathbf{y}}(\mathbf{m}') = b,$$

for randomly chosen $\mathbf{y} \in (\mathbb{Z}_n^*)^k$, violating that RDH is $\frac{1}{p-1}$-AΔU by Theorem 3.3.5. □

3.4.1 Discussion

The proposed scheme, which is a generalization of the scheme proposed in [4, 6], is defined using the *encrypt-and-authenticate* paradigm (see [10, 73] and the references therein, for a detailed discussion about these generic constructions and their security analysis). Since this approach requires the decryption of a purported ciphertext before its authentication, it is susceptible to attacks if the implementation of the decryption function leaks information when given invalid ciphertexts. Surprisingly, the preferred *encrypt-then-authenticate* approach will not work in our setting because it is not key-hiding.

We now show that the assumption that messages are generated uniformly at random is necessary for our result, by showing that any authentication scheme achieving ε-security against substitution attacks for arbitrary source distributions is in fact an ε-ASU hash family.

We begin with some definitions.

Definition 3.4.7. An *authentication code* is specified by a tuple $\mathrm{M} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{M}, \mathcal{V})$ where $\mathcal{S}$ is the set of *source states*, $\mathcal{T}$ is the set of *tags*, $\mathcal{K}$ is the set of *keys*, $\mathcal{M} : \mathcal{K} \times \mathcal{S} \to \mathcal{T}$, and $\mathcal{V} : \mathcal{K} \times \mathcal{T} \to \{0,1\}$. It must be the case that for all $k \in \mathcal{K}$ and $m \in \mathcal{S}$, $\mathcal{V}_k(m||\mathcal{M}_k(m)) = 1$. A *forger* is a mapping $\mathcal{F} = \langle \mathcal{F}_1, \mathcal{F}_2 \rangle$ where $\mathcal{F}_1 : \mathcal{S} \times \mathcal{T} \to \mathcal{S}$ and $\mathcal{F}_2 : \mathcal{S} \times \mathcal{T} \to \mathcal{T}$. We say M is *$\varepsilon$-secure against substitution attacks* if for every forger $\mathcal{F}$ and distribution $\mathbf{S}$ on $\mathcal{S}$,

$$\Pr_{\substack{k \leftarrow \mathcal{K}, m \leftarrow_{\mathbf{S}} \mathcal{S} \\ t \leftarrow \mathcal{M}_k(m)}}[\mathcal{F}_1(m,t) \neq m \wedge \mathcal{V}_k(\mathcal{F}(m||t)) = 1] \leq \varepsilon.$$

Theorem 3.4.8. *Suppose* $\mathrm{M} = (\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{M}, \mathcal{V})$ *is ε-secure against substitution attacks. Then* $\{\mathcal{M}_k \mid k \in \mathcal{K}\}$ *is an* ε-ASU *hash function family.*

Proof. Suppose $\{\mathcal{M}_k \mid k \in \mathcal{K}\}$ is not an ε-ASU hash family. So there are $m' \neq m'' \in \mathcal{S}$ and $t', t'' \in \mathcal{T}$ such that $\Pr_{k \leftarrow \mathcal{K}}[\mathcal{M}_k(m'') = t'' \wedge \mathcal{M}_k(m') = t'] > \varepsilon$. Take $\mathcal{F}$ such that

$\mathcal{F}(m'||t') = m''||t''$, and let $\mathbf{S}$ be the distribution on $\mathcal{S}$ which puts all weight on m'. Then

$$\begin{aligned}
& \Pr_{\substack{k\leftarrow\mathcal{K},m\leftarrow_{\mathbf{S}}\mathcal{S}\\ t\leftarrow\mathcal{M}_k(m)}}[\mathcal{F}_1(m,t)\neq m\wedge\mathcal{V}_k(\mathcal{F}(m||t))=1] \\
= & \Pr_{\substack{k\leftarrow\mathcal{K}\\ t\leftarrow\mathcal{M}_k(m')}}[\mathcal{F}_1(m',t)\neq m'\wedge\mathcal{V}_k(\mathcal{F}(m'||t)=1] \\
= & \Pr_{\substack{k\leftarrow\mathcal{K}\\ t\leftarrow\mathcal{M}_k(m')}}[\mathcal{F}_1(m',t)\neq m'\wedge\mathcal{V}_k(\mathcal{F}(m'||t)=1|t=t']\cdot\Pr_{\substack{k\leftarrow\mathcal{K}\\ t\leftarrow\mathcal{M}_k(m')}}[t=t'] \\
= & \Pr_{k\leftarrow\mathcal{K}}[\mathcal{F}_1(m',t')\neq m'\wedge\mathcal{V}_k(\mathcal{F}(m'||t')=1\wedge\mathcal{M}_k(m')=t'] \\
= & \Pr_{k\leftarrow\mathcal{K}}[m''\neq m'\wedge\mathcal{M}_k(m'')=t''\wedge\mathcal{M}_k(m')=t'] > \varepsilon.
\end{aligned}$$

□

Problem 3.1. So far, we have mentioned an application of GRDH in cryptography. As universal hash functions have many applications in computer science, it would be an interesting question to investigate other areas where GMMH* and GRDH are of possible interest.

Chapter 4

Applications to Combinatorics and Geometry

4.1 Introduction

A *surface* is a compact oriented two-dimensional topological manifold. Roughly speaking, a surface is a space that 'locally' looks like the Euclidean plane. Informally, a graph is said to be *embedded into* (or *drawn on*) a surface if it can be drawn on the surface in such a way that its edges meet only at their endpoints. A *ribbon graph* is a finite and connected graph together with a cyclic ordering on the set of half edges incident to each vertex. One can see that ribbon graphs and embedded graphs are essentially equivalent concepts; that is, a ribbon graph can be thought as a set of disks (or vertices) attached to each other by thin stripes (or edges) glued to their boundaries. There are several other names for these graphs in the literature, for example, *fat graphs*, or *combinatorial maps*, or *unrooted maps*. For a thorough introduction to the theory of embedded graphs we refer the reader to the lovely book by Lando and Zvonkin [75].

Graphs embedded into surfaces have many important applications, in particular, in combinatorics, geometry, and physics. For example, ribbon graphs and their counting is of great interest in string theory and quantum field theory (QFT). Here we quote some of these applications and motivations from [69, 70]:

- Ribbon graphs arise in the context of MHV rules for constructing amplitudes. In the MHV rules approach to amplitudes, inspired by twistor string theory, amplitudes are constructed by gluing MHV vertices. Counting ribbon graphs

play an important role here in finding different ways of gluing the vertices which contribute to a given amplitude.

- The number of ribbon graphs is the fundamental combinatorial element in perturbative large N QFT computations, since we need to be able to enumerate the graphs and then compute corresponding Feynman integrals.

- In matrix models (more specifically, the Gaussian Hermitian and complex matrix models), which can be viewed as QFTs in zero dimensions, the correlators are related very closely to the combinatorics of ribbon graphs. There is also a two-dimensional structure (related to string worldsheets) to this combinatorics.

- There is a bijection between vacuum graphs of Quantum Electrodynamics (QED) and ribbon graphs. In fact, the number of QED/Yukawa vacuum graphs with $2v$ vertices is equal to the number of ribbon graphs with v edges. This can be proved using permutations. Note that QED is an Abelian gauge theory with the symmetry circle group $U(1)$.

Mednykh and Nedela [92] obtained a formula for the number of unrooted maps of a given genus. Recently, Koch, Ramgoolam, and Wen [70] gave a refinement of this formula to make it more suitable for applications to several physics problems, such as the ones mentioned above. In both formulas, there is an important factor, namely, the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group. A formula for the number of such epimorphisms is given in [92] but it does not seem to be very applicable, especially for large values, because one needs to find, as part of the formula, a challenging summation involving the products of some Ramanujan sums and for each index of summation one needs to calculate these products. The aim of this chapter is to give a very explicit and practical formula for the number of such epimorphisms. Our formula does not contain Ramanujan sums or other challenging parts, and is easy to work with. As a consequence, we obtain an 'equivalent' form of the famous Harvey theorem on the cyclic groups of automorphisms of compact Riemann surfaces.

In the next section, we review Fuchsian groups and Harvey's theorem. Our main result is presented in Section 6.3. A key ingredient in the proofs is Theorem 2.3.9 which gives an explicit formula for the number of solutions of restricted linear congruences (this theorem was proved in the Chapter 2 using properties of Ramanujan sums and of the finite Fourier transform of arithmetic functions).

4.2 Fuchsian groups and Harvey's theorem

A *Fuchsian group* Γ is a finitely generated non-elementary discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$, the group of orientation-preserving isometries of the hyperbolic plane $\mathbb{H}^2$. Fuchsian groups were first studied by Poincaré in 1882 in connection with the uniformization problem (later the uniformization theorem), and he called the groups Fuchsian after Lazarus Fuchs whose paper (1880) was a motivation for Poincaré to introduce this concept. By a classical result of Fricke and Klein (see, e.g., [145]), every such group Γ has a presentation in terms of the generators $\mathsf{a}_1, \mathsf{b}_1, \ldots, \mathsf{a}_g, \mathsf{b}_g$ (hyperbolic), $\mathsf{x}_1, \ldots, \mathsf{x}_k$ (elliptic), $\mathsf{y}_1, \ldots, \mathsf{y}_s$ (parabolic), and $\mathsf{z}_1, \ldots, \mathsf{z}_t$ (hyperbolic boundary elements) with the relations

$$\mathsf{x}_1^{n_1} = \cdots = \mathsf{x}_k^{n_k} = \mathsf{x}_1 \cdots \mathsf{x}_k \mathsf{y}_1 \cdots \mathsf{y}_s \mathsf{z}_1 \cdots \mathsf{z}_t [\mathsf{a}_1, \mathsf{b}_1] \cdots [\mathsf{a}_g, \mathsf{b}_g] = 1, \tag{4.2.1}$$

where $k, s, t, g \geq 0$, $n_i \geq 2$ $(1 \leq i \leq k)$, and $[a, b] = a^{-1}b^{-1}ab$. The integers $n_1, \ldots, n_k$ are called the *periods* of Γ, and g is called the *orbit genus*. The Fuchsian group Γ is determined, up to isomorphism, by the tuple $(g; n_1, \ldots, n_k; s; t)$ which is referred to as the *signature* of Γ. If $k = 0$ (i.e., there are no periods), Γ is called a Fuchsian *surface group*. If $s = t = 0$, the group is called *co-compact* (or *F-group*, or *proper*). Some authors by a Fuchsian group mean a co-compact Fuchsian group. In this chapter, we only work with co-compact Fuchsian groups.

We denote by $\mathrm{Hom}(\Gamma, G)$ (resp., $\mathrm{Epi}(\Gamma, G)$) the set of homomorphisms (resp., epimorphisms) from a Fuchsian group Γ to a finite group G. There is much interest (with many applications) in combinatorics, geometry, algebra, and physics, in counting homomorphisms and epimorphisms from a Fuchsian group to a finite group. For example, Liebeck and Shalev [83, 84] obtained good estimates for $|\mathrm{Hom}(\Gamma, G)|$, where Γ is an arbitrary Fuchsian group and G is a symmetric group or an alternating group or a finite simple group.

An epimorphism from a Fuchsian group to a finite group with kernel a Fuchsian surface group is called *surface-kernel* (or *smooth*). Harvey proved that an epimorphism ϕ from a co-compact Fuchsian group Γ to a finite group G is surface-kernel if and only if it preserves the periods of Γ, that is, for every elliptic generator x_i $(1 \leq i \leq k)$ of order n_i, the order of $\phi(\mathsf{x}_i)$ is precisely n_i. The above-mentioned equivalence appears in Harvey's influential 1966 paper [55] on the cyclic groups of automorphisms of compact Riemann surfaces. The main result of this paper is the following theorem

which gives necessary and sufficient conditions for the existence of a surface-kernel epimorphism from a co-compact Fuchsian group to a cyclic group.

Theorem 4.2.1. ([55]) *Let Γ be a co-compact Fuchsian group with signature $(g; n_1, \ldots, n_k)$, and let $\mathfrak{n} := \mathrm{lcm}(n_1, \ldots, n_k)$. There is a surface-kernel epimorphism from Γ to $\mathbb{Z}_n$ if and only if the following conditions are satisfied:*

(i) $\mathrm{lcm}(n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_k) = \mathfrak{n}$, for all i;

(ii) $\mathfrak{n} \mid n$, and if $g = 0$ then $\mathfrak{n} = n$;

(iii) $k \neq 1$, and, if $g = 0$ then $k > 2$;

(iv) if $\mathfrak{n}$ is even then the number of periods n_i such that $\mathfrak{n}/n_i$ is odd is also even.

By a result of Burnside [23], and of Greenberg [48], every finite group G acts as a group of automorphisms of a compact Riemann surface of genus at least two. The *minimum genus* problem asks to find, for a given finite group G, the minimum genus of those compact Riemann surfaces on which G acts faithfully as a group of conformal automorphisms. Harvey [55], using Theorem 4.2.1, solved the minimum genus problem when G is the cyclic group $\mathbb{Z}_n$; in fact, he gave an explicit value for the minimum genus in terms of the prime factorization of n. Then, as a corollary, he obtained a famous result of Wiman [143] on the *maximum order* for an automorphism of a compact Riemann surface of genus γ by showing that this maximum order is $2(2\gamma + 1)$.

Harvey's paper [55] played a pioneering role in studying groups of automorphisms of compact Riemann surfaces and also has found important applications in some other areas of mathematics like combinatorics. See, for example, the survey by Bujalance et al. [22] on the "research inspired by Harvey's theorem", in which the authors describe many results about the actions of several classes of groups, including cyclic, Abelian, solvable, dihedral, etc., along with the minimum genus and maximum order problems for these classes.

4.3 Counting surface-kernel epimorphisms from Γ to $\mathbb{Z}_n$

In this section, we obtain an explicit formula for the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group. First, we need a formula that connects the number of epimorphisms to the number of homomorphisms as, generally, enumerating homomorphisms is easier than enumerating epimorphisms.

The classical version of the Möbius inversion formula states that if f and g are arithmetic functions satisfying $g(n) = \sum_{d\,|\,n} f(d)$, for every integer $n \geq 1$, then

$$f(n) = \sum_{d\,|\,n} \mu\Big(\frac{n}{d}\Big)\, g(d), \tag{4.3.1}$$

for every integer $n \geq 1$. The Möbius function and Möbius inversion were studied for functions over locally finite partially ordered sets (posets) first by Weisner [141] and Hall [53], motivated by group theory problems. Later, Rota [111] extended this idea and put it in the context of combinatorics. Following the argument given in [53], we prove the following simple result.

Theorem 4.3.1. *Let Λ be a finitely generated group. Then*

$$|\mathrm{Epi}(\Lambda, \mathbb{Z}_n)| = \sum_{d\,|\,n} \mu\Big(\frac{n}{d}\Big)\, |\mathrm{Hom}(\Lambda, \mathbb{Z}_d)|, \tag{4.3.2}$$

where the summation is taken over all positive divisors d of n.

Proof. Clearly, for a finitely generated group Λ and a finite group G we have

$$|\mathrm{Hom}(\Lambda, G)| = \sum_{H \leq G} |\mathrm{Epi}(\Lambda, H)|,$$

because every homomorphism from Λ to G induces a unique epimorphism from Λ to its image in G.

Taking $G = \mathbb{Z}_n$, and since the cyclic group $\mathbb{Z}_n$ has a unique subgroup $\mathbb{Z}_d$ for every positive divisor d of n and has no other subgroups, we get

$$|\mathrm{Hom}(\Lambda, \mathbb{Z}_n)| = \sum_{d\,|\,n} |\mathrm{Epi}(\Lambda, \mathbb{Z}_d)|.$$

Now, by applying the Möbius inversion formula, (4.3.1), the theorem follows. □

We also need the following well-known result which gives equivalent defining formulas for *Jordan's totient function* $J_k(n)$ (see, e.g., [91, pp. 13-14]).

Lemma 4.3.2. *Let n, k be positive integers. Then*

$$J_k(n) = \sum_{d\,|\,n} d^k \mu\Big(\frac{n}{d}\Big) = n^k \prod_{p\,|\,n} \left(1 - \frac{1}{p^k}\right), \tag{4.3.3}$$

where the left summation is taken over all positive divisors d of n, and the right product is taken over all prime divisors p of n.

Now, using the above results, we obtain an explicit formula for the number $|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)|$ of surface-kernel epimorphisms from a co-compact Fuchsian group Γ to the cyclic group $\mathbb{Z}_n$.

Theorem 4.3.3. *Let Γ be a co-compact Fuchsian group with signature $(g; n_1, \ldots, n_k)$, and let $\mathfrak{n} := \mathrm{lcm}(n_1, \ldots, n_k)$. If $\mathfrak{n} \nmid n$ then there is no surface-kernel epimorphism from Γ to $\mathbb{Z}_n$. Otherwise, the number of surface-kernel epimorphisms from Γ to $\mathbb{Z}_n$ is*

$$|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)| = \frac{n^{2g}}{\mathfrak{n}} \prod_{i=1}^{k} \varphi(n_i) \prod_{p \,|\, \frac{n}{\mathfrak{n}}} \left(1 - \frac{1}{p^{2g}}\right) \prod_{p \,|\, \mathfrak{n}} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right), \tag{4.3.4}$$

where $e_p = \#\{i : 1 \leq i \leq k, p \nmid \mathfrak{n}/n_i\}$.

Proof. By Theorem 4.3.1, we have

$$|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)| = \sum_{d \,|\, n} \mu\Big(\frac{n}{d}\Big) \, |\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)|, \tag{4.3.5}$$

where $|\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)|$ is the number of surface-kernel homomorphisms from Γ to $\mathbb{Z}_d$. It is easy to see that for every positive divisor d of n we have $|\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)| = d^{2g} N_d$, where N_d is the number of solutions of the restricted linear congruence $x_1 + \cdots + x_k \equiv 0 \pmod{d}$, with $\gcd(x_i, d) = \frac{d}{n_i}$ $(1 \leq i \leq k)$. Suppose that $\mathfrak{D} := \{d > 0 : d \mid n \text{ and } \mathfrak{n} \mid d\}$. Clearly, if $\mathfrak{D}$ is empty then $|\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)| = 0$, for every divisor d of n, which then implies that $|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)| = 0$, by (4.3.5). Let $\mathfrak{n} \nmid n$. Then $\mathfrak{n} \nmid d$, for every divisor d of n. Thus, $\mathfrak{D}$ is empty which then implies that $|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)| = 0$, by (4.3.5). Now, let $\mathfrak{n} \mid n$. Then there exists at least one divisor d of n such that $\mathfrak{n} \mid d$. So, $\mathfrak{D}$ is non-empty. Now, for every $d \in \mathfrak{D}$, by Theorem 2.3.9, we have

$$N_d = \prod_{i=1}^{k} \varphi(n_i) \prod_{\substack{p \,|\, d \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right), \tag{4.3.6}$$

where r_p is the exponent of p in the prime factorization of d, $\mathfrak{m}_p$ is the smallest $j \geq 1$ such that there is some i with $p^j \nmid \frac{d}{n_i}$, and $e_p = \#\{i : 1 \leq i \leq k, p^{\mathfrak{m}_p} \nmid d/n_i\}$. On the

other hand, by Theorem 2.3.6, we have

$$N_d = \frac{1}{d}\sum_{d' \,|\, d} \varphi(d') \prod_{i=1}^{k} c_{n_i}\left(\frac{d}{d'}\right),$$

which, as was proved in [131, Prop. 9], equals

$$N_d = \frac{1}{d}\sum_{q=1}^{d} \prod_{i=1}^{k} c_{n_i}(q).$$

Now, since the Ramanujan sum $c_n(m)$ is a periodic function of m with period n, it is easy to see (from the above equivalent expressions) that the value of N_d will remain the same if we replace d with $\mathfrak{n}$ in (4.3.6). Consequently, we obtain the following explicit formula for the number of surface-kernel homomorphisms from Γ to $\mathbb{Z}_d$,

$$|\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)| = d^{2g} \prod_{i=1}^{k} \varphi\left(n_i\right) \prod_{\substack{p \,|\, \mathfrak{n} \\ \mathfrak{m}_p \leq r_p}} p^{\mathfrak{m}_p - r_p - 1} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right),$$

where r_p is the exponent of p in the prime factorization of $\mathfrak{n}$, $\mathfrak{m}_p$ is the smallest $j \geq 1$ such that there is some i with $p^j \nmid \frac{\mathfrak{n}}{n_i}$, and $e_p = \#\{i : 1 \leq i \leq k, p^{\mathfrak{m}_p} \nmid \mathfrak{n}/n_i\}$.

Note that since $\mathfrak{n} = \mathrm{lcm}(n_1, \ldots, n_k)$, for every prime divisor p of $\mathfrak{n}$ we have $p \nmid \frac{\mathfrak{n}}{n_i}$ for at least one i. This means that $\mathfrak{m}_p = 1$ for every prime divisor p of $\mathfrak{n}$. Also, note that

$$\prod_{p \,|\, \mathfrak{n}} p^{r_p} = \mathfrak{n}.$$

Therefore, we get

$$|\mathrm{Hom}_{\mathrm{S}}(\Gamma, \mathbb{Z}_d)| = \frac{d^{2g}}{\mathfrak{n}} \prod_{i=1}^{k} \varphi\left(n_i\right) \prod_{p \,|\, \mathfrak{n}} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right),$$

where $e_p = \#\{i : 1 \leq i \leq k, p \nmid \mathfrak{n}/n_i\}$.

Now, using (4.3.5), letting $d = v\mathfrak{n}$, and then using Lemma 4.3.2, we obtain

$$\begin{aligned}
|\mathrm{Epi_S}(\Gamma, \mathbb{Z}_n)| &= \sum_{\mathfrak{n} \,|\, d \,|\, n} \mu\Big(\frac{n}{d}\Big) \frac{d^{2g}}{\mathfrak{n}} \prod_{i=1}^{k} \varphi\left(n_i\right) \prod_{p \,|\, \mathfrak{n}} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \\
&= \sum_{v \,|\, \frac{n}{\mathfrak{n}}} \mu\left(\frac{n/\mathfrak{n}}{v}\right) v^{2g} \mathfrak{n}^{2g-1} \prod_{i=1}^{k} \varphi\left(n_i\right) \prod_{p \,|\, \mathfrak{n}} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right) \\
&= \frac{n^{2g}}{\mathfrak{n}} \prod_{i=1}^{k} \varphi\left(n_i\right) \prod_{p \,|\, \frac{n}{\mathfrak{n}}} \left(1 - \frac{1}{p^{2g}}\right) \prod_{p \,|\, \mathfrak{n}} \left(1 - \frac{(-1)^{e_p - 1}}{(p-1)^{e_p - 1}}\right),
\end{aligned}$$

where $e_p = \#\{i : 1 \leq i \leq k, p \nmid \mathfrak{n}/n_i\}$. □

Example 4.3.4.

1) Let Γ be the co-compact Fuchsian group with signature $(1; 2, 3, 4)$. Find the number of surface-kernel epimorphisms from Γ to $\mathbb{Z}_{24}$.

Here $\mathfrak{n} = \mathrm{lcm}(2, 3, 4) = 12 = 2^2 \cdot 3$. Also, $2 \mid \frac{\mathfrak{n}}{n_1} = 6$, $2 \mid \frac{\mathfrak{n}}{n_2} = 4$, $2 \nmid \frac{\mathfrak{n}}{n_3} = 3$. So, $e_2 = 1$. Therefore, by Theorem 4.3.3, we have

$$|\mathrm{Epi_S}(\Gamma, \mathbb{Z}_{24})| = 0,$$

because

$$1 - \frac{(-1)^{e_2 - 1}}{(2-1)^{e_2 - 1}} = 1 - \frac{(-1)^{1-1}}{1^{1-1}} = 0.$$

Of course, this example also follows directly from Harvey's theorem (Theorem 4.2.1).

2) Let Γ be the co-compact Fuchsian group with signature $(2; 36, 500, 125, 9)$. Find the number of surface-kernel epimorphisms from Γ to $\mathbb{Z}_{9000}$.

Here $\mathfrak{n} = \mathrm{lcm}(36, 500, 125, 9) = \mathrm{lcm}(2^2 \cdot 3^2, 2^2 \cdot 5^3, 5^3, 3^2) = 2^2 \cdot 3^2 \cdot 5^3 = 4500$. We have

$2 \nmid \frac{\mathfrak{n}}{n_1} = 5^3$, $2 \nmid \frac{\mathfrak{n}}{n_2} = 3^2$, $2 \mid \frac{\mathfrak{n}}{n_3} = 2^2 \cdot 3^2$, $2 \mid \frac{\mathfrak{n}}{n_4} = 2^2 \cdot 5^3$, so, $e_2 = 2$;
$3 \nmid \frac{\mathfrak{n}}{n_1} = 5^3$, $3 \mid \frac{\mathfrak{n}}{n_2} = 3^2$, $3 \mid \frac{\mathfrak{n}}{n_3} = 2^2 \cdot 3^2$, $3 \nmid \frac{\mathfrak{n}}{n_4} = 2^2 \cdot 5^3$, so, $e_3 = 2$;
$5 \mid \frac{\mathfrak{n}}{n_1} = 5^3$, $5 \nmid \frac{\mathfrak{n}}{n_2} = 3^2$, $5 \nmid \frac{\mathfrak{n}}{n_3} = 2^2 \cdot 3^2$, $5 \mid \frac{\mathfrak{n}}{n_4} = 2^2 \cdot 5^3$, so, $e_5 = 2$.

Now,

$$\prod_{p\,|\,4500}\left(1-\frac{(-1)^{e_p-1}}{(p-1)^{e_p-1}}\right)$$
$$=\left(1-\frac{(-1)^{2-1}}{(2-1)^{2-1}}\right)\left(1-\frac{(-1)^{2-1}}{(3-1)^{2-1}}\right)\left(1-\frac{(-1)^{2-1}}{(5-1)^{2-1}}\right)=\frac{15}{4}.$$

Therefore, by Theorem 4.3.3, we have

$$|\mathrm{Epi}_{\mathrm{S}}(\Gamma,\mathbb{Z}_{9000})|$$
$$=\frac{9000^4}{4500}\varphi\left(2^2\cdot 3^2\right)\varphi\left(2^2\cdot 5^3\right)\varphi\left(5^3\right)\varphi\left(3^2\right)\left(1-\frac{1}{2^4}\right)\times\frac{15}{4}=7381125\cdot 10^{12}.$$

3) Let Γ be the co-compact Fuchsian group with signature $(0;36,500,125,9)$. Find the number of surface-kernel epimorphisms from Γ to $\mathbb{Z}_{9000}$.

Here since $g=0$,

$$\prod_{p\,|\,\frac{n}{\mathfrak{n}}}\left(1-\frac{1}{p^{2g}}\right)=\prod_{p\,|\,2}\left(1-\frac{1}{p^0}\right)=0.$$

Therefore, by Theorem 4.3.3, we have

$$|\mathrm{Epi}_{\mathrm{S}}(\Gamma,\mathbb{Z}_{9000})|=0.$$

Of course, this example also follows directly from Harvey's theorem.

Remark 4.3.5. *In the proof of Theorem 4.3.3 we have used only a special case of Theorem 2.3.9 where $a_i=1$ $(1\le i\le k)$ and $b=0$. But there may be other generalizations/variants of these or other groups so that for counting the number of surface-kernel epimorphisms (or other relevant problems) we have to use the 'full power' of Theorem 2.3.9.*

Remark 4.3.6. *In order to get explicit values for $|\mathrm{Epi}_{\mathrm{S}}(\Gamma,\mathbb{Z}_n)|$ from Theorem 4.3.3, we only need to find the prime factorization of n, of $\mathfrak{n}$, and of the periods $n_1,\ldots,n_k$. Then we can easily compute e_p, $\varphi(n_i)$, etc. In fact, even for Harvey's theorem (Theorem 4.2.1) we need to find these prime factorizations! So, Theorem 4.3.3 has roughly the same computational cost as Harvey's theorem.*

Clearly, for a co-compact Fuchsian group with all periods equal to each other we have $e_p = \#\{i : 1 \leq i \leq k, p \nmid \mathfrak{n}/n_i\} = k$, for every prime divisor p of $\mathfrak{n}$. Therefore, we get the following simpler formula from Theorem 4.3.3.

Corollary 4.3.7. *Let Γ be a co-compact Fuchsian group with signature $(g; n_1, \ldots, n_k)$, where $n_1 = \cdots = n_k = \mathfrak{n}$. If $\mathfrak{n} \nmid n$ then there is no surface-kernel epimorphism from Γ to $\mathbb{Z}_n$. Otherwise, the number of surface-kernel epimorphisms from Γ to $\mathbb{Z}_n$ is*

$$|\mathrm{Epi}_{\mathrm{S}}(\Gamma, \mathbb{Z}_n)| = \frac{n^{2g}\varphi(\mathfrak{n})^k}{\mathfrak{n}} \prod_{p \mid \frac{n}{\mathfrak{n}}} \left(1 - \frac{1}{p^{2g}}\right) \prod_{p \mid \mathfrak{n}} \left(1 - \frac{(-1)^{k-1}}{(p-1)^{k-1}}\right). \tag{4.3.7}$$

Interestingly, using Theorem 4.3.3, we can obtain an 'equivalent' form of Harvey's theorem (Theorem 4.2.1). See also [85]. Note that conditions (i), (iii) in Corollary 4.3.8 are exactly the same as, respectively, conditions (ii), (iv) in Harvey's theorem.

Corollary 4.3.8. *Let Γ be a co-compact Fuchsian group with signature $(g; n_1, \ldots, n_k)$, and let $\mathfrak{n} := \mathrm{lcm}(n_1, \ldots, n_k)$. There is a surface-kernel epimorphism from Γ to $\mathbb{Z}_n$ if and only if the following conditions are satisfied:*

(i) $\mathfrak{n} \mid n$, and if $g = 0$ then $\mathfrak{n} = n$;

(ii) $e_p > 1$ for every prime divisor p of $\mathfrak{n}$;

(iii) if $\mathfrak{n}$ is even then e_2 is also even.

Proof. The proof simply follows by using the first part of Theorem 4.3.3 and examining the conditions under which the factors of the products in (4.3.4) do not vanish. □

4.4 A problem

It is an interesting problem to develop these counting arguments for the classes of non-cyclic groups. Such results would be very important from several aspects, for example, may lead to more extensions of Harvey's theorem and new proofs for the existing ones, and also may provide us new ways for dealing with the minimum genus and maximum order problems for these classes of groups. So, we pose the following question.

Problem 4.1. Give explicit formulas for the number of surface-kernel epimorphisms from a co-compact Fuchsian group to a non-cyclic group, say, Abelian, solvable, dihedral, etc.

Chapter 5

On Linear Congruences with Distinct Coordinates: A Graph Theoretic Method

5.1 Introduction

In Chapter 2, we considered the number of solutions of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with the restrictions $\gcd(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $a_1, t_1, \ldots, a_k, t_k, b, n$ $(n \geq 1)$ are arbitrary integers. Another restriction of potential interest is imposing the condition that all x_i are *distinct* modulo n. Unlike the first problem, there seems to be very little published on the second problem. Recently, Grynkiewicz et al. [50], using tools from additive combinatorics and group theory, proved necessary and sufficient conditions under which the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, where $a_1, \ldots, a_k, b, n$ $(n \geq 1)$ are arbitrary integers, has a solution $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with all x_i distinct modulo n; see also [1, 50] for connections to zero-sum theory. So, it would be an interesting problem to give an explicit formula for the number of such solutions. Quite surprisingly, this problem was first considered, in a special case, by Schönemann [117] almost two centuries ago(!) but his result seems to have been forgotten. Schönemann [117] proved the following result:

Theorem 5.1.1. *Let p be a prime, $a_1, \ldots, a_k$ be arbitrary integers, and $\sum_{i=1}^{k} a_i \equiv 0 \pmod{p}$ but $\sum_{i \in I} a_i \not\equiv 0 \pmod{p}$ for all $I \subsetneq \{1, \ldots, k\}$. The number $N_p(k)$ of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_p^k$ of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{p}$, with all x_i distinct modulo p, is independent of the coefficients $a_1, \ldots, a_k$ and is equal*

to

$$N_p(k) = (-1)^{k-1}(k-1)!(p-1) + (p-1)\cdots(p-k+1).$$

In this chapter, we generalize Schönemann's theorem using Proposition 2.1.1 and a result on graph enumeration recently obtained by Ardila et al. [8]. This seems to be a rather uncommon method in the area; besides, our proof technique or its modifications may be useful for dealing with other cases of this problem (or even the general case) or other relevant problems. We state and prove our main result in the next section.

5.2 Main Result

Our generalization of Schönemann's theorem is obtained via a graph theoretic method which may also be of independent interest. We need two formulas on graph enumeration (see Theorem 5.2.2 below) recently obtained by Ardila et al. [8]. These formulas are in terms of the *deformed exponential function* which is a special case of the *three variable Rogers-Ramanujan function* defined below. These functions have interesting applications in combinatorics, complex analysis, functional differential equations, and statistical mechanics (see [8, 71, 76, 86, 118, 124] and the references therein).

Definition 5.2.1. The *three variable Rogers-Ramanujan function* is

$$R(\alpha,\beta,q) = \sum_{m\geq 0} \frac{\alpha^m \beta^{\binom{m}{2}}}{(1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{m-1})}.$$

Also, the *deformed exponential function* is

$$F(\alpha,\beta) = R(\alpha,\beta,1) = \sum_{m\geq 0} \frac{\alpha^m \beta^{\binom{m}{2}}}{m!}.$$

Let $g(c,e,k)$ be the number of simple graphs with c connected components, e edges, and k vertices labeled $1,\ldots,k$, and $g'(e,k)$ be the number of simple *connected* graphs with e edges and k labeled vertices. Suppose that

$$G(t,y,z) = \sum_{c,e,k} g(c,e,k) t^c y^e \frac{z^k}{k!},$$

and

$$CG(y,z) = \sum_{e,k} g'(e,k) y^e \frac{z^k}{k!}.$$

Ardila et al. [8] proved the following theorem.

Theorem 5.2.2. *The generating functions for counting simple graphs and simple connected graphs satisfy, respectively,*

$$G(t,y,z) = F(z,1+y)^t,$$

and

$$CG(y,z) = \log F(z,1+y),$$

where F is the deformed exponential function defined above.

Now, we are ready to state and prove our main result.

Theorem 5.2.3. *Let $a_1,\ldots,a_k,b,n$ $(n \geq 1)$ be arbitrary integers, and $(\sum_{i\in I} a_i, n) = 1$ for all $I \subsetneq \{1,\ldots,k\}$. The number $N_n(b;a_1,\ldots,a_k)$ of solutions $\langle x_1,\ldots,x_k\rangle \in \mathbb{Z}_n^k$ of the linear congruence $a_1x_1+\cdots+a_kx_k \equiv b \pmod n$, with all x_i distinct modulo n, is*

$$N_n(b;a_1,\ldots,a_k)$$
$$= \begin{cases} (-1)^k(k-1)! + (n-1)\cdots(n-k+1), & \text{if } (\sum_{i=1}^k a_i, n) \nmid b; \\ (-1)^{k-1}(k-1)!\left((\sum_{i=1}^k a_i, n) - 1\right) + (n-1)\cdots(n-k+1), & \text{if } (\sum_{i=1}^k a_i, n) \mid b. \end{cases}$$

Proof. Let $\langle x_1,\ldots,x_k\rangle \in \mathbb{Z}_n^k$ be a solution of the linear congruence $a_1x_1+\cdots+a_kx_k \equiv b \pmod n$. We construct a graph $G = (V,E)$ with vertex set $V = \{1,\ldots,k\}$ and connect the vertices u and v if and only if $x_u \equiv x_v \pmod n$. By this construction, the number of solutions $\langle x_1,\ldots,x_k\rangle \in \mathbb{Z}_n^k$ of the linear congruence $a_1x_1+\cdots+a_kx_k \equiv b \pmod n$, with some x_i equal to each other modulo n, is now directly related to the number of connected components of the graph $G = (V,E)$. The reason is that when some x_i are equal to each other modulo n, then by connecting their indices (as vertices of the graph G) we get a connected component of G, and we can simplify the linear congruence by grouping the x_i which are equal to each other modulo n.

This procedure eventually gives a new linear congruence in which the coefficients are of the form $\sum_{i\in I} a_i$, where $I \subseteq \{1,\dots,k\}$, and the number of terms is equal to the number of connected components of the corresponding graph. Therefore, to find the number of solutions of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with some x_i equal to each other modulo n, we first construct the corresponding graph. If this graph has $c > 1$ connected components then since $(\sum_{i\in I} a_i, n) = 1$ for all $I \subsetneq \{1,\dots,k\}$, by Proposition 2.1.1 the number of solutions of the linear congruence with those x_i equal to each other modulo n is equal to n^{c-1}. Also, if this graph is connected, that is, $c = 1$ (which means that all x_i are equal to each other modulo n) then the linear congruence has just one term (and its coefficient is $\sum_{i=1}^{k} a_i$), and so, by Proposition 2.1.1 the number of solutions in this case, we denote it by A, is equal to $(\sum_{i=1}^{k} a_i, n)$ if $(\sum_{i=1}^{k} a_i, n) \mid b$, and is equal to zero otherwise. Let $g(c,e,k)$ be the number of simple graphs with c connected components, e edges, and k vertices labeled $1,\dots,k$, and $g'(e,k)$ be the number of simple *connected* graphs with e edges and k labeled vertices. Now, by the inclusion-exclusion principle, we have

$$\begin{aligned} N_n(b;a_1,\dots,a_k) &= \sum_{e=0}^{\binom{k}{2}} (-1)^e \left(Ag'(e,k) + \sum_{c=2}^{k} n^{c-1} g(c,e,k) \right) \\ &= A\sum_{e=0}^{\binom{k}{2}} (-1)^e g'(e,k) + \frac{1}{n}\sum_{e=0}^{\binom{k}{2}} \sum_{c=2}^{k} (-1)^e n^c g(c,e,k) \\ &= (A-1)\sum_{e=0}^{\binom{k}{2}} (-1)^e g'(e,k) + \frac{1}{n}\sum_{e=0}^{\binom{k}{2}} \sum_{c=1}^{k} (-1)^e n^c g(c,e,k). \end{aligned}$$

In order to evaluate the latter expression, we use the two formulas in Theorem 5.2.2. In fact, by Theorem 5.2.2, we have

$$\sum_{e,k} (-1)^e g'(e,k) \frac{z^k}{k!} = \log F(z,0),$$

and

$$\sum_{c,e,k} (-1)^e n^c g(c,e,k) \frac{z^k}{k!} = F(z,0)^n,$$

where F is the deformed exponential function. Note that $F(z,0) = 1 + z$. Now, we have

$$\sum_{e=0}^{\binom{k}{2}}(-1)^e g'(e,k) = \text{the coefficient of } \frac{z^k}{k!} \text{ in } \log(1+z), \text{ which is equal to } \frac{k!(-1)^{k+1}}{k},$$

and

$$\sum_{e=0}^{\binom{k}{2}}\sum_{c=1}^{k}(-1)^e n^c g(c,e,k) = \text{the coefficient of } \frac{z^k}{k!} \text{ in } (1+z)^n, \text{ which is equal to } k!\binom{n}{k}.$$

Consequently, the number $N_n(b; a_1, \ldots, a_k)$ of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with all x_i distinct modulo n, is

$$\begin{aligned} N_n(b; a_1, \ldots, a_k) &= \frac{(A-1)k!(-1)^{k+1}}{k} + \frac{k!\binom{n}{k}}{n} \\ &= \begin{cases} (-1)^k(k-1)! + (n-1)\cdots(n-k+1), & \text{if } (\sum_{i=1}^{k} a_i, n) \nmid b; \\ (-1)^{k-1}(k-1)!\left((\sum_{i=1}^{k} a_i, n) - 1\right) + (n-1)\cdots(n-k+1), & \text{if } (\sum_{i=1}^{k} a_i, n) \mid b. \end{cases} \end{aligned}$$

□

Chapter 6

Applications to the Varshamov–Tenengolts Codes and Several Other Combinatorial Problems

6.1 Introduction

A *Z-channel* (also called a *binary asymmetric channel*) is a channel with binary input and binary output where a transmitted 0 is always received correctly, but a transmitted 1 may be received as either 1 or 0. These channels have many applications, for example, some data storage systems and optical communication systems can be modelled using these channels. In 1965, Varshamov and Tenengolts [137] introduced an important class of codes, known as the Varshamov–Tenengolts codes or VT-codes, that are capable of correcting asymmetric errors on a Z-channel (see also [136]). Levenshtein [80, 81], by giving an elegant decoding algorithm, showed that these codes could also be used for correcting a single deletion or insertion (see [94, 98, 123] for three nice surveys on error-correcting codes for channels with deletion/insertion errors).

Definition 6.1.1. Let n be a positive integer and $0 \leq b \leq n$ be a fixed integer. The Varshamov–Tenengolts code $VT_b(n)$ is the set of all binary vectors $\langle y_1, \ldots, y_n \rangle$

such that

$$\sum_{i=1}^{n} iy_i \equiv b \pmod{n+1}.$$

For example, $VT_0(5) = \{00000, 10001, 01010, 11100, 00111, 11011\}$, where we have shown vectors as strings. So, $|VT_0(5)| = 6$. The *Hamming weight* of a string over an alphabet is defined as the number of non-zero symbols in the string. For example, the Hamming weight of 01010 is 2, and the number of codewords in $VT_0(5)$ with Hamming weight 2 is 2.

Varshamov in his fundamental paper "On an arithmetic function with an application in the theory of coding" ([135]) proved that the maximum number of codewords in the Varshamov–Tenengolts code $VT_b(n)$ is achieved when $b = 0$, that is, $|VT_0(n)| \geq |VT_b(n)|$ for all b. Several natural questions arise: What is the number of codewords in the Varshamov–Tenengolts code $VT_b(n)$, that is, $|VT_b(n)|$? Given a positive integer k, what is the number of codewords in $VT_b(n)$ with Hamming weight k, that is, with exactly k 1's? Ginzburg [46] in 1967 considered the first question and proved an explicit formula for $|VT_b(n)|$ (in fact, he proved an explicit formula for the size of q-ary, rather than binary, Varshamov–Tenengolts codes, where q is an arbitrary positive integer). In this chapter, we deal with both questions and obtain explicit formulas for them via a novel approach, namely, *connecting the Varshamov–Tenengolts codes to linear congruences with distinct coordinates*. Since in a Z-channel a transmitted 1 may be received as either 1 or 0, having an explicit formula for the number of codewords in $VT_b(n)$ with Hamming weight k may be useful, among other things, in detecting more errors and/or some specific errors. We even go further and show that the number of solutions of these congruences is related to several other combinatorial problems, some of which have appeared in seemingly unrelated contexts. (For example, as we will discuss in Section 6.3, Razen, Seberry, and Wehrhahn [107] considered two special cases of a function considered in this chapter and gave an application in coding theory in finding the complete weight enumerator of a code generated by a circulant matrix.) This provides a general framework and gives new insight into all these problems which might lead to further work. Let us now describe these congruences.

Consider the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, where $a_1, \ldots, a_k, b, n$ ($n \geq 1$) are arbitrary integers. What can we say about the number of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of this congruence with all x_i *distinct* modulo n? In Chapter 5, using Proposition 2.1.1 and a result on graph enumeration recently obtained by Ardila

et al. [8], we studied an special case of this problem which generalizes Schönemann's theorem. Specifically, we obtained an explicit formula for the number of solutions of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with all x_i distinct modulo n, when $(\sum_{i\in I} a_i, n) = 1$ for all $I \subsetneq \{1, \ldots, k\}$, where $a_1, \ldots, a_k, b, n$ $(n \geq 1)$ are arbitrary integers. Clearly, this result does not resolve the problem in its full generality; for example, it does not cover the important case of $a_i = 1$ $(1 \leq i \leq k)$ and this is what we consider in this chapter with an entirely different approach. Specifically, we give an explicit formula for the number $N_n(k, b)$ of such solutions when $a_i = 1$ $(1 \leq i \leq k)$, and do the same when in addition all x_i are *positive* modulo n. Our main tools in this chapter are properties of Ramanujan sums and of the discrete Fourier transform of arithmetic functions. In Section 6.2, we derive the explicit formulas, and discuss applications to the Varshamov–Tenengolts codes. In Section 6.3, we discuss applications to several other combinatorial contexts.

6.2 Solutions with distinct coordinates and applications to the Varshamov–Tenengolts codes

In this section, we obtain an explicit formula for the number of solutions $\langle x_1, \ldots, x_k\rangle \in \mathbb{Z}_n^k$ of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with all x_i distinct modulo n, and do the same when in addition all x_i are positive modulo n. We also discuss applications to the Varshamov–Tenengolts codes. First, we need some preliminary results.

Lemma 6.2.1. *Let n be a positive integer and m be a non-negative integer. We have*

$$\prod_{j=1}^{n} \left(1 - ze^{2\pi ijm/n}\right) = (1 - z^{\frac{n}{d}})^d,$$

where $d = (m, n)$.

Proof. It is well-known that (see, e.g., [126, p. 167])

$$1 - z^n = \prod_{j=1}^{n} \left(1 - ze^{2\pi ij/n}\right).$$

Now, letting $d = (m, n)$, we obtain

$$\prod_{j=1}^{n}\left(1-ze^{2\pi ijm/n}\right)=\prod_{j=1}^{n}\left(1-ze^{2\pi ij\frac{m/d}{n/d}}\right)$$
$$=\left(\prod_{j=1}^{n/d}\left(1-ze^{2\pi ij\frac{m/d}{n/d}}\right)\right)^{d}$$
$$\overset{(\frac{m}{d},\frac{n}{d})=1}{=}\left(\prod_{j=1}^{n/d}\left(1-ze^{\frac{2\pi ij}{n/d}}\right)\right)^{d}=(1-z^{\frac{n}{d}})^{d}.$$

□

Similarly, we can prove the following lemma.

Lemma 6.2.2. *Let n be a positive integer and m be a non-negative integer. We have*

$$\prod_{j=1}^{n}\left(z-e^{2\pi ijm/n}\right)=(z^{\frac{n}{d}}-1)^{d},$$

where $d=(m,n)$.

By changing z to $-z$ and using the binomial theorem, Lemma 6.2.1 gives:

Corollary 6.2.3. *Let n be a positive integer and m, k be non-negative integers. The coefficient of z^k in*

$$\prod_{j=1}^{n}\left(1+ze^{2\pi ijm/n}\right),$$

is $(-1)^{k+\frac{kd}{n}}\binom{d}{\frac{kd}{n}}$, where $d=(m,n)$.

Now, we are ready to obtain an explicit formula for the number of solutions of the linear congruence.

Theorem 6.2.4. *Let n be a positive integer and $b\in\mathbb{Z}_n$. The number $N_n(k,b)$ of solutions $\langle x_1,\ldots,x_k\rangle\in\mathbb{Z}_n^k$ of the linear congruence $x_1+\cdots+x_k\equiv b \pmod n$, with all x_i distinct modulo n, is*

$$N_n(k,b)=\frac{(-1)^k k!}{n}\sum_{d\,|\,(n,\,k)}(-1)^{\frac{k}{d}}c_d(b)\binom{\frac{n}{d}}{\frac{k}{d}}. \tag{6.2.1}$$

Proof. It is well-known that (see, e.g., [51, pp. 3-4]) the number of partitions of b into exactly k *distinct* parts each taken from the given set A, is the coefficient of $q^b z^k$ in

$$\prod_{j \in A} \left(1 + zq^j\right).$$

Now, take $A = \mathbb{Z}_n$ and $q = e^{2\pi i m/n}$, where m is a non-negative integer. Then, the number $P_n(k, b)$ of partitions of b into exactly k *distinct* parts each taken from $\mathbb{Z}_n$ (that is, the number of solutions of the above linear congruence, with all x_i distinct modulo n, if order does not matter), is the coefficient of $e^{2\pi i b m/n} z^k$ in

$$\prod_{j=1}^{n} \left(1 + ze^{2\pi i j m/n}\right).$$

This in turn implies that

$$\sum_{b=1}^{n} P_n(k, b) e^{2\pi i b m/n} = \text{the coefficient of } z^k \text{ in } \prod_{j=1}^{n} \left(1 + ze^{2\pi i j m/n}\right).$$

Let $e(x) = \exp(2\pi i x)$. Note that $N_n(k, b) = k! P_n(k, b)$. Now, using Corollary 6.2.3, we get

$$\sum_{b=1}^{n} N_n(k, b) e\left(\frac{bm}{n}\right) = (-1)^{k + \frac{kd}{n}} k! \binom{d}{\frac{kd}{n}},$$

where $d = (m, n)$. Now, by (2.2.11) and (2.2.12), we obtain

$$\begin{aligned}
N_n(k,b) &= \frac{(-1)^k k!}{n} \sum_{m=1}^{n} (-1)^{\frac{kd}{n}} e\left(\frac{-bm}{n}\right) \binom{d}{\frac{kd}{n}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} \sum_{\substack{m=1 \\ (m,\, n)=d}}^{n} (-1)^{\frac{kd}{n}} e\left(\frac{-bm}{n}\right) \binom{d}{\frac{kd}{n}} \\
&\overset{m'=m/d}{=} \frac{(-1)^k k!}{n} \sum_{d \,|\, n} \sum_{\substack{m'=1 \\ (m',\, n/d)=1}}^{n/d} (-1)^{\frac{kd}{n}} e\left(\frac{-bm'}{n/d}\right) \binom{d}{\frac{kd}{n}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} (-1)^{\frac{kd}{n}} c_{n/d}(-b) \binom{d}{\frac{kd}{n}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} (-1)^{\frac{kd}{n}} c_{n/d}(b) \binom{d}{\frac{kd}{n}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} (-1)^{\frac{k}{d}} c_d(b) \binom{\frac{n}{d}}{\frac{k}{d}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, (n,\, k)} (-1)^{\frac{k}{d}} c_d(b) \binom{\frac{n}{d}}{\frac{k}{d}}.
\end{aligned}$$

□

Corollary 6.2.5. *If n or k is odd then from (6.2.1) we obtain the following important special cases of the function $P_n(k,b) = \frac{1}{k!} N_n(k,b)$:*

$$P_n(k,0) = \frac{1}{n} \sum_{d \,|\, (n,\, k)} \varphi(d) \binom{\frac{n}{d}}{\frac{k}{d}}, \tag{6.2.2}$$

$$P_n(k,1) = \frac{1}{n} \sum_{d \,|\, (n,\, k)} \mu(d) \binom{\frac{n}{d}}{\frac{k}{d}}. \tag{6.2.3}$$

Corollary 6.2.6. *If $(n,k) = 1$ then (6.2.1) is independent of b and simplifies as*

$$N_n(k) = \frac{k!}{n} \binom{n}{k}.$$

(Of course, this can also be proved directly.) If in addition we have $n = 2k + 1$ then

$$P_n(k) = \frac{1}{k!}N_n(k) = \frac{1}{2k+1}\binom{2k+1}{k} = \frac{1}{k+1}\binom{2k}{k},$$

which is the Catalan number.

Remark 6.2.7. *Using (2.2.5), it is easy to see that (6.2.1) also works when $k = 0$.*

Now, we introduce the important function $T_n(b)$ which is the sum of $P_n(k, b)$ over k. There are several interpretations for the function $T_n(b)$, for example, $T_n(b)$ can be interpreted as the number of subsets of the set $\{1, 2, \ldots, n\}$ which sum to b modulo n.

Corollary 6.2.8. *Let $T_n(b) := \sum_{k=0}^{n} \frac{1}{k!}N_n(k, b) = \sum_{k=0}^{n} P_n(k, b)$. Then we have*

$$T_n(b) = \frac{1}{n}\sum_{\substack{d \mid n \\ d \text{ odd}}} c_d(b)2^{\frac{n}{d}}. \tag{6.2.4}$$

Proof. We have

$$\begin{aligned}
T_n(b) &= \sum_{k=0}^{n} \frac{(-1)^k}{n} \sum_{d \mid (n,\, k)} (-1)^{\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} c_d(b) \\
&= \frac{1}{n}\sum_{d \mid n} c_d(b) \sum_{\substack{k=0 \\ d \mid k}}^{n} (-1)^{k+\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} \\
&= \frac{1}{n}\sum_{\substack{d \mid n \\ d \text{ odd}}} c_d(b) \sum_{\substack{k=0 \\ d \mid k}}^{n} (-1)^{k+\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} + \frac{1}{n}\sum_{\substack{d \mid n \\ d \text{ even}}} c_d(b) \sum_{\substack{k=0 \\ d \mid k}}^{n} (-1)^{k+\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} \\
&= \frac{1}{n}\sum_{\substack{d \mid n \\ d \text{ odd}}} c_d(b)2^{\frac{n}{d}}.
\end{aligned}$$

Note that in the last equality we have used the fact that if $d \mid n$ and d is even then

$$\sum_{\substack{k=0 \\ d \mid k}}^{n} (-1)^{k+\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} = \sum_{\substack{k=0 \\ d \mid k}}^{n} (-1)^{\frac{k}{d}} \binom{\frac{n}{d}}{\frac{k}{d}} = 0.$$

□

What is the number of subsets of the set $\{1, 2, \ldots, n-1\}$ which sum to b modulo n? Using Corollary 6.2.8, we can obtain an explicit formula for the number of such subsets (see also [89]).

Corollary 6.2.9. *The number $T'_n(b)$ of subsets of the set $\{1, 2, \ldots, n-1\}$ which sum to b modulo n is*

$$T'_n(b) = \frac{1}{2}T_n(b) = \frac{1}{2n}\sum_{\substack{d \mid n \\ d \text{ odd}}} c_d(b)2^{\frac{n}{d}}. \tag{6.2.5}$$

Proof. Let A be a subset of the set $\{1, 2, \ldots, n-1\}$ which sum to b modulo n. Then A and $A \cup \{n\}$ are both subsets of the set $\{1, 2, \ldots, n\}$ and both sum to b modulo n. Therefore, $T'_n(b) = \frac{1}{2}T_n(b)$. □

Now, we connect these results to the Varshamov–Tenengolts codes $VT_b(n)$ by giving an explicit formula for the number of codewords in $VT_b(n)$, that is, $|VT_b(n)|$. Of course, this result has been already discovered by Ginzburg [46] in 1967 even in a more general form (see Remark 6.2.11 below), but we derive it via a novel approach and as a consequence of our results. Later in Corollary 6.2.14, we obtain an explicit formula for the number of codewords in $VT_b(n)$ with Hamming weight k.

Corollary 6.2.10. *The number $|VT_b(n)|$ of codewords in the Varshamov–Tenengolts code $VT_b(n)$ is*

$$|VT_b(n)| = \frac{1}{2(n+1)}\sum_{\substack{d \mid n+1 \\ d \text{ odd}}} c_d(b)2^{\frac{n+1}{d}}. \tag{6.2.6}$$

Proof. Let $\langle y_1, \ldots, y_n \rangle$ be a codeword in $VT_b(n)$. Note that $\sum_{i=1}^{n} iy_i$ is just the sum of some elements of the set $\{1, 2, \ldots, n\}$. Therefore, finding the number of codewords in $VT_b(n)$ boils down to finding the number of subsets of the set $\{1, 2, \ldots, n\}$ which sum to b modulo $n+1$. The result now follows by a direct application of Corollary 6.2.9. □

Remark 6.2.11. *Ginzburg [46] in 1967 in his important paper "A certain number-theoretic function which has an application in coding theory" proved the following explicit formula for the number $|VT_{b,q}(n)|$ of codewords in the q-ary, rather than*

binary, Varshamov–Tenengolts code $VT_{b,q}(n)$, where q is an arbitrary positive integer:

$$|VT_{b,q}(n)| = \frac{1}{q(n+1)} \sum_{\substack{d \,|\, n+1 \\ (d,q)=1}} c_d(b) q^{\frac{n+1}{d}}. \tag{6.2.7}$$

Formula (6.2.7) was later rediscovered by Stanley and Yoder [127] in 1973, and in the binary case (that is, when $q = 2$) by Sloane [123] in 2002.

Remark 6.2.12. *From (6.2.7) and Theorem 2.2.3 it is clear that the maximum number of codewords in the q-ary Varshamov–Tenengolts code $VT_{b,q}(n)$ is achieved when $b = 0$, that is,*

$$|VT_{0,q}(n)| = \frac{1}{q(n+1)} \sum_{\substack{d \,|\, n+1 \\ (d,q)=1}} \varphi(d) q^{\frac{n+1}{d}} \geq |VT_{b,q}(n)|,$$

for all b. Of course, this has been already observed by Stanley and Yoder [127].

In some applications (for example, in coding theory) we also need to consider the case that all x_i are *positive* and *distinct* modulo n. Now, we obtain an explicit formula for the number of such solutions.

Theorem 6.2.13. *Let n be a positive integer and $b \in \mathbb{Z}_n$. The number $N_n^{>0}(k,b)$ of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with all x_i positive and distinct modulo n, is*

$$N_n^{>0}(k,b) = \frac{(-1)^k k!}{n} \sum_{d \,|\, n} (-1)^{\lfloor \frac{k}{d} \rfloor} c_d(b) \binom{\frac{n}{d} - 1}{\lfloor \frac{k}{d} \rfloor}. \tag{6.2.8}$$

Proof. Clearly, $N_n^{>0}(k,b) = N_n(k,b) - N_n^0(k,b)$, where $N_n^0(k,b)$ denotes the number of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ with all x_i distinct modulo n and one of x_i is zero modulo n. Also, clearly, $N_n^0(k,b) = kN_n^{>0}(k-1,b)$. Thus,

$$N_n(k,b) = N_n^{>0}(k,b) + kN_n^{>0}(k-1,b). \tag{6.2.9}$$

Now, using Theorem 6.2.4 we have

$$\begin{aligned}
N_n(k,b) &= \frac{(-1)^k k!}{n} \sum_{d \,|\, (n,\,k)} (-1)^{\frac{k}{d}} c_d(b) \binom{\frac{n}{d}}{\frac{k}{d}} \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, (n,\,k)} (-1)^{\frac{k}{d}} c_d(b) \left(\binom{\frac{n}{d}-1}{\frac{k}{d}} + \binom{\frac{n}{d}-1}{\frac{k}{d}-1} \right) \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} c_d(b) \left((-1)^{\frac{k}{d}} \binom{\frac{n}{d}-1}{\frac{k}{d}} - (-1)^{\frac{k}{d}-1} \binom{\frac{n}{d}-1}{\frac{k}{d}-1} \right) \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} c_d(b) \left((-1)^{\lfloor \frac{k}{d} \rfloor} \binom{\frac{n}{d}-1}{\lfloor \frac{k}{d} \rfloor} - (-1)^{\lfloor \frac{k-1}{d} \rfloor} \binom{\frac{n}{d}-1}{\lfloor \frac{k-1}{d} \rfloor} \right) \\
&= \frac{(-1)^k k!}{n} \sum_{d \,|\, n} (-1)^{\lfloor \frac{k}{d} \rfloor} c_d(b) \binom{\frac{n}{d}-1}{\lfloor \frac{k}{d} \rfloor} \\
&\quad + k \frac{(-1)^{k-1}(k-1)!}{n} \sum_{d \,|\, n} (-1)^{\lfloor \frac{k-1}{d} \rfloor} c_d(b) \binom{\frac{n}{d}-1}{\lfloor \frac{k-1}{d} \rfloor}.
\end{aligned}$$

Note that in the fourth equality above we have used the fact that $\lfloor \frac{k}{d} \rfloor = \lfloor \frac{k-1}{d} \rfloor + 1$ if $d \mid k$, and $\lfloor \frac{k}{d} \rfloor = \lfloor \frac{k-1}{d} \rfloor$ if $d \nmid k$. Now, recalling (6.2.9) we obtain the desired result. □

We believe that Theorem 6.2.13 is also a strong tool and might lead to interesting applications. For example, it immediately gives an explicit formula for the number of codewords in the Varshamov–Tenengolts code $VT_b(n)$ with Hamming weight k. As we mentioned, since in a Z-channel a transmitted 1 may be received as either 1 or 0, such a result may be useful, among other things, in detecting more errors and/or some specific errors.

Corollary 6.2.14. *The number $|VT_b^{1,k}(n)|$ of codewords in the Varshamov–Tenengolts code $VT_b(n)$ with Hamming weight k is*

$$|VT_b^{1,k}(n)| = \frac{(-1)^k}{n+1} \sum_{d \,|\, n+1} (-1)^{\lfloor \frac{k}{d} \rfloor} c_d(b) \binom{\frac{n+1}{d}-1}{\lfloor \frac{k}{d} \rfloor}. \tag{6.2.10}$$

Proof. Let $\langle y_1, \ldots, y_n \rangle$ be a codeword in $VT_b(n)$ with Hamming weight k, that is, with exactly k 1's. Denote by x_j the position of the jth one. Note that $1 \le j \le k$

and $1 \leq x_1 < x_2 < \cdots < x_k \leq n$. Now, we have

$$\sum_{i=1}^{n} iy_i \equiv b \pmod{n+1} \Longleftrightarrow x_1 + \cdots + x_k \equiv b \pmod{n+1}.$$

Therefore, finding the number of codewords in $VT_b(n)$ with Hamming weight k boils down to finding the number of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_{n+1}^k$ of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n+1}$, with all x_j positive and distinct modulo $n+1$, and with disregarding the order of the coordinates. The result now follows by a direct application of Theorem 6.2.13. □

6.3 More applications and connections

Interestingly, some special cases of the functions $P_n(k, b)$, $N_n(k, b)$, $T_n(b)$, and $T'_n(b)$ that we studied in this chapter have appeared in a wide range of combinatorial problems, sometimes in seemingly unrelated contexts. Here we briefly mention some of these applications and connections:

Ordered partitions acted upon by cyclic permutations. Consider the set of all ordered partitions of a positive integer n into k parts acted upon by the cyclic permutation $(12 \ldots k)$. Razen, Seberry, and Wehrhahn [107] obtained explicit formulas for the cardinality of the resulting family of orbits and for the number of orbits in this family having exactly k elements. These formulas coincide with the expressions for $P_n(k, 0)$ and $P_n(k, 1)$, respectively, when n or k is odd (see Corollary 6.2.5). Razen et al. [107] also discussed an application in coding theory in finding the complete weight enumerator of a code generated by a circulant matrix.

Permutations with given cycle structure and descent set. Gessel and Reutenauer [43] counted permutations in the symmetric group S_n with a given cycle structure and descent set. One of their results gives an explicit formula for the number of n-cycles with descent set $\{k\}$, which coincides with the expression for $P_n(k, 1)$ when n or k is odd. Interestingly, the mapping introduced by Gessel and Reutenauer [43] has the *Burrows-Wheeler transformation* (BWT) as a special case. The BWT, introduced by Burrows and Wheeler [24], is a famous invertible data compression algorithm (see [30, 41]).

Fixed-density necklaces and Lyndon words. If n or k is odd then the expres-

sions for $P_n(k,0)$ and $P_n(k,1)$ give, respectively, the number of fixed-density binary necklaces and fixed-density binary Lyndon words of length n and density k, as described by Gilbert and Riordan [45], and Ruskey and Sawada [113].

Necklace polynomial. The function $T_n(b)$ is closely related to the polynomial

$$M(q,n) = \frac{1}{n}\sum_{d\,|\,n}\mu(d)q^{\frac{n}{d}},$$

which is called the *necklace polynomial* of degree n (it is easy to see that $M(q,n)$ is integer-valued for all $q \in \mathbb{Z}$). In fact, if n is odd then $M(2,n) = T_n(1)$. The necklace polynomials turn up in various contexts in combinatorics and algebra. For example, they appear as (see, e.g., [59, 74, 95, 126]):

- the number of *aperiodic necklaces* (also called *Lyndon words*) of length n in an alphabet of size q (this justifies the name of "necklace polynomial"). Note that the number of *necklaces* of length n in an alphabet of size q is

  $$\frac{1}{n}\sum_{d\,|\,n}\varphi(d)q^{\frac{n}{d}},$$

  which coincides with the expression for $T_n(0)$ when $q = 2$ and n is odd;

- the number of monic irreducible polynomials of degree n over the finite field $\mathbb{F}_q$, where q is a prime power;

- the *Witt formula* in the context of free Lie algebras, which gives the number of basic commutators of degree n in the free Lie algebra on q generators;

- the exponent in the *cyclotomic identity*:

  $$\frac{1}{1-qz} = \prod_{n=1}^{\infty}\left(\frac{1}{1-z^n}\right)^{M(q,\,n)},$$

  which is a consequence of the Poincaré-Birkhoff-Witt Theorem (or PBW Theorem) on the structure of the universal enveloping algebras of Lie algebras (Metropolis and Rota [95] gave a bijective proof of this identity). The cyclotomic identity is the main ingredient in the proof of the Witt formula.

Quasi-necklace polynomial. The function $T'_n(b)$ is also closely related to the polynomial

$$M'(q,n) = \frac{1}{2n}\sum_{d\,|\,n}\mu(d)q^{\frac{n}{d}},$$

that we call the *quasi-necklace polynomial* of degree n. In fact, if n is odd then $M'(2,n) = T'_n(1)$. The quasi-necklace polynomials also turn up in various contexts in combinatorics. For example, they appear as:

- the number of transitive unimodal cyclic permutations obtained by Weiss and Rogers [142] (motivated by problems related to the structure of the set of periodic orbits of one-dimensional dynamical systems) using methods related to the work of Milnor and Thurston [97]. See also [130] which gives a generating function for the number of unimodal permutations with a given cycle structure;
- the number of periodic patterns of the tent map [7];
- the exponent in a problem related to casino shelf shuffling machines [36].

6.4 A problem

It would be an interesting problem to see if the technique presented in this chapter can be modified so that it covers the problem in its full generality. So, we pose the following question.

Problem 6.1. Let $a_1,\ldots,a_k,b,n$ $(n \geq 1)$ be arbitrary integers. Give an explicit formula for the number of solutions $\langle x_1,\ldots,x_k\rangle \in \mathbb{Z}_n^k$ of the linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$ with all x_i *distinct* modulo n, and do the same when in addition all x_i are *positive* modulo n.

Such results would be interesting from several aspects. As mentioned in the previous chapters, the number of solutions of the linear congruence with the restrictions $(x_i,n) = t_i$ $(1 \leq i \leq k)$, where $t_1,\ldots,t_k$ are given positive divisors of n, has found interesting applications in number theory, combinatorics, geometry, physics, computer science, and cryptography. Therefore, having an explicit formula for the number of solutions with all x_i (positive and) distinct modulo n may also lead to interesting applications in these or other directions — as we have shown in the chapter, even

the special case of $a_i = 1$ $(1 \leq i \leq k)$ has interesting applications in coding theory and several other combinatorial contexts. The problem may also have implications in zero-sum theory; see [1, 50] for the related discussion.

6.5 Discussion

In this chapter, we study a number theory problem systematically, obtain some explicit formulas for the problem, and then give two coding theory applications. Of course, we also give several other combinatorial applications. We would like to remark that Dolecek and Anantharam [39] obtained an explicit formula for the number of codewords with Hamming weight w in a 'variant' of the Varshamov–Tenengolts code $VT_b(n)$ where the modulus is $w+1$ instead of $n+1$. Specifically for that variant, their formula counts the number of codewords with Hamming weight w, that is, the Hamming weight is dependent on the modulus. But our Corollary 6.2.14 deals exactly with the Varshamov–Tenengolts code $VT_b(n)$ (not a variant of it) and gives an explicit formula for the number of codewords in $VT_b(n)$ with Hamming weight k, where k, unlike the result of Dolecek and Anantharam, does not depend on the modulus and is *arbitrary*. So, the result of Dolecek and Anantharam is very different from Corollary 6.2.14. Of course, the expression (3.7) in their paper is exactly the same as our formula (6.2.1) that we proved in Theorem 6.2.4 for the number of solutions of the linear congruence $x_1 + \cdots + x_k \equiv b \pmod{n}$, with all x_i distinct modulo n, but they have not mentioned these congruences in their paper. So, the result of Dolecek and Anantharam does not have any relation to the results of this chapter and moreover, the nature of this chapter (which stems from number theory) is quite different. It is an interesting problem to prove such a 1-1 correspondence between their formula (3.7) and our Theorem 6.2.4. Also, note that all the ingredients used in this chapter have been known decades before the paper by Dolecek and Anantharam [39].

Chapter 7

Character Theory and Finite Fields Applied to a Problem Stemming from Coding Theory

7.1 Introduction

The long-standing Golomb–Welch conjecture [47] states that there are no perfect Lee codes for spheres of radius greater than 1 and dimension greater than 2. Resolving this conjecture has been one of the main motivations for studying perfect and quasi-perfect Lee codes. Very recently, Camarero and Martínez [25], showed that for every prime number $p > 5$ such that $p \equiv \pm 5 \pmod{12}$, the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$, where S_2 is the set of units of $\mathbb{Z}_p[i]$, induces a 2-quasi-perfect Lee code over $\mathbb{Z}_p^m$, where $m = 2\lfloor \frac{p}{4} \rfloor$. They also conjectured [25, Conj. 31] that the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is a Ramanujan graph for every prime p such that $p \equiv 3 \pmod{4}$. In this chapter, we solve this conjecture. Our main tools, which are reviewed in the next section, are Deligne's bound [35] from 1977 for estimating a particular kind of trigonometric sum and a result of Lovász [87] from 1975 (or of Babai [9] from 1979) which gives the eigenvalues of Cayley graphs of finite Abelian groups. Our proof techniques may motivate more work in the interactions between spectral graph theory, character theory, and coding theory, and may provide new ideas towards the Golomb–Welch conjecture.

Let us first recall here briefly some terminologies and concepts that we will need

in this chapter. The ring of *Gaussian integers* is defined as

$$\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}, i = \sqrt{-1}\}.$$

In other words, Gaussian integers are the lattice points in the Euclidean plane. The *norm* of a Gaussian integer $w = x + yi$ is $\mathrm{N}(w) = |w|^2 = x^2 + y^2$. The elements of $\mathbb{Z}[i]$ with norm 1 are called the *units* of $\mathbb{Z}[i]$; so, the units of $\mathbb{Z}[i]$ are just ± 1 and $\pm i$. Similarly, the ring of Gaussian integers modulo a positive integer n is defined as

$$\mathbb{Z}[i]/n\mathbb{Z}[i] \cong \mathbb{Z}_n[i] = \{a + bi : a, b \in \mathbb{Z}_n, i = \sqrt{-1}\}.$$

Note that the definition of norm (and so unit) in the ring $\mathbb{Z}_n[i]$ is the same as that of $\mathbb{Z}[i]$ except that we need to evaluate the norm modulo n. That is, the *norm* of $z = a + bi \in \mathbb{Z}_n[i]$ is $\mathrm{N}(z) = a^2 + b^2 \pmod{n}$, and $z = a + bi \in \mathbb{Z}_n[i]$ is a *unit* of $\mathbb{Z}_n[i]$ if and only if

$$a^2 + b^2 \equiv 1 \pmod{n}.$$

The following classical result gives necessary and sufficient conditions under which the ring $\mathbb{Z}_n[i]$ is a field; see, e.g., [40, Fact 3].

Proposition 7.1.1. *Let $n > 1$ be an integer. The ring $\mathbb{Z}_n[i]$ is a field if and only if n is a prime and $n \equiv 3 \pmod{4}$.*

Let Γ be a group written in additive notation. A non-empty subset $S \subseteq \Gamma$ is said to be *symmetric* if $S = -S$, where $-S = \{-x : x \in S\}$. In other words, S is symmetric if $-x \in S$ whenever $x \in S$. Now, we define Cayley graphs:

Definition 7.1.2. Let Γ be a group, written additively, and S be a finite symmetric subset of Γ which does not contain the identity element of Γ. The *Cayley graph* of Γ with respect to S, denoted by $G = \mathrm{Cay}(\Gamma, S)$, is the graph whose vertex set is Γ, and such that $u \sim v$ if and only if $v - u \in S$. Note that the Cayley graph $G = \mathrm{Cay}(\Gamma, S)$ is undirected, simple, $|S|$-regular, and vertex-transitive. Also, G is connected if and only if S generates Γ.

Roughly speaking, an expander is a highly connected sparse graph, that is, every subset of its vertices has a large set of neighbours. An important special case, namely, Ramanujan graphs are also of great interest. These graphs are actually 'optimal' expanders, from the spectral point of view. Roughly speaking, a Ramanujan graph

is a connected regular graph whose second largest eigenvalue in absolute value is 'asymptotically' the smallest possible (or, equivalently, whose spectral gap is 'asymptotically' the largest possible). Formally, a finite, connected, k-regular graph G is called a *Ramanujan graph* if every eigenvalue $\lambda \neq \pm k$ of G satisfies the bound

$$|\lambda| \leq 2\sqrt{k-1}.$$

To this date, there are only a few explicit constructions (which are useful for applications) of expanders and Ramanujan graphs, all given using several strong (and seemingly unrelated!) mathematical tools; mainly from number theory. These graphs have a great deal of seminal applications in many disciplines such as computer science, cryptography, coding theory, and even in pure mathematics! See [32, 60, 88] for detailed discussions and surveys on expanders and Ramanujan graphs, their interactions with other areas like number theory and group theory, and their many wide-ranging applications.

Now, we review some basic facts about group characters; see, e.g., [64, 119] for more details. A *character* of a group Γ is a group homomorphism from Γ to the unit circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. So, if Γ is a finite group then a character of Γ can be defined as a group homomorphism from Γ to $\mathbb{C}^*$, the multiplicative group of non-zero complex numbers. For a group Γ, the *trivial* character χ_0 is the function on Γ where $\chi_0(g) = 1$, for all $g \in \Gamma$. The characters of a finite group are linearly independent. A finite group Γ has *at most* $|\Gamma|$ characters and a finite Abelian group Γ has *exactly* $|\Gamma|$ distinct characters. For a finite Abelian group Γ with the trivial character χ_0,

$$\sum_{g\in\Gamma} \chi(g) = \begin{cases} |\Gamma|, & \text{if } \chi = \chi_0; \\ 0, & \text{if } \chi \neq \chi_0. \end{cases}$$

7.2 Proof ingredients and techniques

In this section, we prove the conjecture proposed in [25], by showing that the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is a $(p+1)$-regular Ramanujan graph. First, we mention the proof ingredients. The following proposition lists some classical facts from spectral graph theory; see, e.g., [31]. As it is common, by an eigenvalue (resp., eigenvector) of a graph we mean an eigenvalue (resp., eigenvector) of the adjacency matrix of that graph.

Proposition 7.2.1. *Let G be a simple graph (i.e., without loops or multiple edges) of order n, with the adjacency matrix $A(G)$, and with the maximum degree $\Delta(G)$. Also, let $\lambda_{\min}(G)$ and $\lambda_{\max}(G)$ denote, respectively, the smallest and the largest eigenvalues of G. The following facts hold:*

- *The graph G has n eigenvalues (including multiplicities), and since $A(G)$ is real and symmetric, all these eigenvalues are real.*
- *We have $\lambda_{\max}(G) \leq \Delta(G)$. Furthermore, if G is k-regular then $\lambda_{\max}(G) = k$, and for every eigenvalue λ of G, $|\lambda| \leq k$.*
- *If G is k-regular then the multiplicity of the eigenvalue k equals the number of connected components of G. So, if G is k-regular then G is connected if and only if the eigenvalue k has multiplicity one.*
- *The graph G is bipartite if and only if its spectrum is symmetric about 0. Also, if G is connected then G is bipartite if and only if $\lambda_{\min}(G) = -\lambda_{\max}(G)$.*

It is well-known that the spectra of Cayley graphs of finite groups can be expressed in terms of characters of the underlying group ([9, 87]). The following result determines the eigenvalues and eigenvectors of Cayley graphs of finite Abelian groups. The theorem follows from a more general result of Lovász [87] from 1975 (or of Babai [9] from 1979).

Theorem 7.2.2. *Let Γ be a finite Abelian group, $\chi : \Gamma \to \mathbb{C}^*$ be a character of Γ, and S be a symmetric subset of Γ which does not contain the identity element of Γ. Then the vector $v_\chi = (\chi(g))_{g\in\Gamma}$ is an eigenvector of the Cayley graph $G = \mathrm{Cay}(\Gamma, S)$, with the corresponding eigenvalue being*

$$\lambda_\chi = \sum_{s\in S} \chi(s).$$

In order to find the degree of the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$, we need to evaluate the number of solutions of certain quadratic congruences. The problem of counting the number of solutions of quadratic congruences in several variables has been investigated, in a general form, in [132], where a general formula is proved. Specifically, Tóth [132] considered the quadratic congruence

$$a_1x_1^2 + \cdots + a_kx_k^2 \equiv b \pmod{n}, \tag{7.2.1}$$

where $b \in \mathbb{Z}$, $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}^k$, and proved an explicit formula (see Theorem 7.2.3 below) for the number $N_k(b, n, \mathbf{a})$ of solutions $\langle x_1, \ldots, x_k \rangle \in \mathbb{Z}_n^k$ of (7.2.1), when n is odd. The formula involves a special kind of trigonometric sums, namely, quadratic Gauss sums that we now define. Let $e(x) = \exp(2\pi i x)$ be the complex exponential with period 1. For positive integers m and n with $\gcd(m, n) = 1$, the quantity

$$S(m, n) = \sum_{j=1}^{n} e\left(\frac{mj^2}{n}\right) \tag{7.2.2}$$

is called a *quadratic Gauss sum.*

Theorem 7.2.3. *Let k, b, n be integers $(k, n \geq 1)$, and $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}^k$. We have*

$$N_k(b, n, \mathbf{a}) = n^{k-1} \sum_{d \mid n} \frac{1}{d^k} \sum_{\substack{m=1 \\ (m,d)=1}}^{d} e\left(\frac{-bm}{d}\right) S(ma_1, d) \cdots S(ma_k, d).$$

Note that the Gauss sum has the Ramanujan sum as a special case. Interestingly, when k is even, n is odd, and $(a_1 \cdots a_k, n) = 1$, the number of solutions can be expressed in terms of the Ramanujan sum; see [132] for a proof:

Theorem 7.2.4. *Let $k = 2m$, where m is a positive integer, b be an integer, n be an odd positive integer, $(a_1 \cdots a_k, n) = 1$, and $\mathbf{a} = \langle a_1, \ldots, a_k \rangle \in \mathbb{Z}^k$. We have*

$$N_k(b, n, \mathbf{a}) = n^{2m-1} \sum_{d \mid n} \frac{c_d(b)}{d^m} \left(\frac{(-1)^m a_1 \cdots a_{2m}}{d}\right).$$

Putting $k = 2$, $a_1 = a_2 = 1$, $b = 1$, and $n = p^r$ (a power of a prime) in Theorem 7.2.3 (or in Theorem 7.2.4 when p is an odd prime), the following special case is obtained (see [132]):

Lemma 7.2.5. *Let p be a prime and r be a positive integer. The number $N_2(1, p^r)$*

of solutions of the quadratic congruence $x^2 + y^2 \equiv 1 \pmod{p^r}$ *is*

$$N_2(1, p^r) = \begin{cases} p^r(1 - \frac{1}{p}), & \text{if } p \equiv 1 \pmod 4,\ r \geq 1; \\ p^r(1 + \frac{1}{p}), & \text{if } p \equiv 3 \pmod 4,\ r \geq 1; \\ 2, & \text{if } p = 2,\ r = 1; \\ 2^{r+1}, & \text{if } p = 2,\ r \geq 2. \end{cases}$$

If $\mathbb{F}$ and $\mathbb{E}$ are fields and $\mathbb{F} \subseteq \mathbb{E}$, then $\mathbb{E}$ is said to be an *extension* of $\mathbb{F}$, denoted by $\mathbb{E}$ / $\mathbb{F}$. The *degree* of a field extension $\mathbb{E}$ / $\mathbb{F}$, denoted by $[\mathbb{E} : \mathbb{F}]$, is the dimension of $\mathbb{E}$ as a vector space over $\mathbb{F}$. A field extension $\mathbb{E}$ / $\mathbb{F}$ is called a *finite extension* if $[\mathbb{E} : \mathbb{F}] < \infty$. Let $\mathbb{F}_{q^n}$ be a finite extension field of the finite field $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_{q^n}$, the *field norm* of α is defined by (see, e.g., [82, Def. 2.27])

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha^{(q^n-1)/(q-1)}.$$

The elements of $\mathbb{F}_{q^n}$ with field norm 1 are called the *units* of $\mathbb{F}_{q^n}$.

Lemma 7.2.6. *Let p be a prime such that $p \equiv 3 \pmod 4$. Then for every $z \in \mathbb{Z}_p[i]$ the field norm of z coincides with the norm of z in the usual sense, that is, as the norm of a Gaussian integer modulo p.*

Proof. Let $z = a + bi \in \mathbb{Z}_p[i]$, where p is a prime and $p \equiv 3 \pmod 4$. Then, by the above definition, the field norm of z equals

$$\begin{aligned} \mathrm{N}_{\mathbb{Z}_p[i]/\mathbb{Z}_p}(a + bi) &= (a + bi)^{p+1} \\ &= (a + bi)(a + bi)^p \\ &= (a + bi)(a^p + b^p i^p) \\ &= a^{p+1} + ab^p i^p + ba^p i + b^{p+1} i^{p+1} \\ &\equiv a^2 + b^2 \pmod p, \end{aligned}$$

where we have used Fermat's little theorem and also the binomial theorem for commutative rings of characteristic p (see, e.g., [82, Th. 1.46]) which says that in a commutative ring R of prime characteristic p, we have

$$(x + y)^{p^n} = x^{p^n} + y^{p^n},$$

for every $x, y \in R$ and every positive integer n. Note that the value $a^2 + b^2 \pmod p$ is just the norm of z as a Gaussian integer modulo p. □

Deligne [35] using tools from algebraic geometry and cohomology proved the following crucial bound.

Theorem 7.2.7. *Suppose that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is the field extension of degree n of the finite field $\mathbb{F}_q$, S_n is the set of units of $\mathbb{F}_{q^n}$, and χ is a nontrivial character of the additive group of $\mathbb{F}_{q^n}$. Then*

$$\Big| \sum_{s \in S_n} \chi(s) \Big| \leq n q^{\frac{n-1}{2}}.$$

Now, we are ready to prove our main result. This problem has been mentioned as Conjecture 31 in [25].

Theorem 7.2.8. *Let p be a prime, $p \equiv 3 \pmod 4$, and S_2 be the set of units of $\mathbb{Z}_p[i]$. Then the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is a $(p+1)$-regular Ramanujan graph.*

Proof. By Proposition 7.1.1, the ring $\mathbb{Z}_n[i]$ is a field if and only if n is a prime and $n \equiv 3 \pmod 4$. Thus, for a prime p with $p \equiv 3 \pmod 4$ we have $\mathbb{Z}_p[i] \cong \mathbb{F}_{p^2}$. Also, we know that for a prime p with $p \equiv 3 \pmod 4$, $\mathbb{Z}_p[i]$ as an extension field of the finite field $\mathbb{F}_p$ has degree 2 (because $\{1, i\}$ can serve as a basis), that is, $[\mathbb{Z}_p[i] : \mathbb{F}_p] = 2$.

Note that S_2 is a symmetric subset of $\mathbb{Z}_p[i]$ and does not contain the identity element of $\mathbb{Z}_p[i]$. Since the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is of order p^2, it has p^2 real eigenvalues. Also, by Lemma 7.2.5, the number of solutions of the quadratic congruence $x^2 + y^2 \equiv 1 \pmod p$ is $p+1$, so, $|S_2| = p+1$ which means that $\mathcal{G}_p$ is $(p+1)$-regular. By Theorem 7.2.2, the eigenvalues of $\mathcal{G}_p$ are determined by

$$\lambda_\chi = \sum_{s \in S_2} \chi(s),$$

where χ runs over all characters of $\mathbb{Z}_p[i]$; note that since $\mathbb{Z}_p[i]$, as an additive group, is a finite Abelian group, it has p^2 distinct characters. The eigenvalue corresponding to the trivial character χ_0 of $\mathbb{Z}_p[i]$ equals

$$\lambda_{\chi_0} = \sum_{s \in S_2} \chi_0(s) = \sum_{s \in S_2} 1 = |S_2| = p+1.$$

Of course, as $\mathcal{G}_p$ is $(p+1)$-regular, we already knew, by Proposition 7.2.1, that $p+1$ is an eigenvalue of $\mathcal{G}_p$ (in fact, the largest one).

Note that since p is a prime and $p \equiv 3 \pmod 4$, by Lemma 7.2.6, for every $z \in \mathbb{Z}_p[i]$ the field norm of z coincides with the norm of z as a Gaussian integer modulo p, thus, the 'field norm' (and so unit) in Theorem 7.2.7 is in fact the 'norm' (and so unit) we already have. Now, by Theorem 7.2.7, the absolute values of the eigenvalues corresponding to the nontrivial characters $\chi \neq \chi_0$ of $\mathbb{Z}_p[i]$ satisfy the bound

$$|\lambda_\chi| = \Big| \sum_{s \in S_2} \chi(s) \Big| \leq 2\sqrt{p}.$$

Therefore, $\mathcal{G}_p$ is a $(p+1)$-regular Ramanujan graph. We remark that since $\mathcal{G}_p$ is $(p+1)$-regular and the eigenvalue $p+1$ has multiplicity one, by Proposition 7.2.1, $\mathcal{G}_p$ is connected. This in turn implies that S_2 generates $\mathbb{Z}_p[i]$. □

Since by the above argument, $-(p+1)$ is not an eigenvalue of $\mathcal{G}_p$, by Proposition 7.2.1, we get:

Corollary 7.2.9. *The Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$ is not bipartite. This implies that $\mathcal{G}_p$ has at least one odd cycle.*

7.3 A problem

It would be an interesting problem to consider such problems also for the case that p is a prime with $p \equiv 1 \pmod 4$. So, we pose the following question.

Problem 7.1. Let p be a prime, $p \equiv 1 \pmod 4$, and S_2 be the set of units of $\mathbb{Z}_p[i]$. What can we say about the Cayley graph $\mathcal{G}_p = \mathrm{Cay}(\mathbb{Z}_p[i], S_2)$? Can we prove that almost all such graphs are Ramanujan?

Probably the first step here would be to prove some character sum bound. Such a result would be very interesting from several aspects and most certainly would need deep tools from several areas of mathematics in particular algebraic geometry and number theory.

Bibliography

[1] D. Adams and V. Ponomarenko, Distinct solution to a linear congruence, *Involve* **3** (2010), 341–344.

[2] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin, and F. Pappalardi, Contributions to zero-sum problems, *Discrete Math.* **306** (2006), 1–10.

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

[4] 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.

[5] B. Alomair, L. Lazos, and R. Poovendran, Securing low-cost RFID systems: An unconditionally secure approach, *J. Comput. Secur.* **19** (2011), 229–257.

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

[7] K. Archer and S. Elizalde, Cyclic permutations realized by signed shifts, *J. Combin.* **5** (2014), 1–30.

[8] F. Ardila, F. Castillo, and M. Henley, The arithmetic Tutte polynomials of the classical root systems, *Int. Math. Res. Not.* **2015** (2015), 3830–3877.

[9] L. Babai, Spectra of Cayley graphs, *J. Combin. Theory Ser. B* **27** (1979), 180–189.

[10] 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.

[11] K. Bibak, B. M. Kapron, and V. Srinivasan, The Cayley graphs associated with some quasi-perfect Lee codes are Ramanujan graphs, *IEEE Trans. Inform. Theory* **62** (2016), 6355–6358.

[12] 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.

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

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

[15] K. Bibak, B. M. Kapron, and V. Srinivasan, On linear congruences with distinct coordinates: A graph theoretic method, submitted.

[16] K. Bibak, B. M. Kapron, and V. Srinivasan, Codewords in the Varshamov–Tenengolts codes with Hamming weight k and several combinatorial applications, submitted.

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

[18] K. Bibak, B. M. Kapron, V. Srinivasan, and L. Tóth, On a variant of multilinear modular hashing with applications to authentication and secrecy codes, In Proceedings of the *International Symposium on Information Theory and Its Applications — ISITA 2016*, Monterey, California, USA, Oct. 30 – Nov. 2, 2016, pp. 320–324.

[19] K. Bibak, B. M. Kapron, V. Srinivasan, and L. Tóth, On an almost-universal hash function family with applications to authentication and secrecy codes, submitted; https://eprint.iacr.org/2015/1187.

[20] 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.

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

[22] E. Bujalance, F.-J. Cirre, G. Gromadzki, A survey of research inspired by Harvey's theorem on cyclic groups of automorphisms, In *Geometry of Riemann Surfaces*, London Math. Soc. Lecture Note Ser., 368, Cambridge University Press, (2010), pp. 15–37.

[23] W. Burnside, *Theory of groups of finite order (Note K)*, Dover Publications, (1955).

[24] M. Burrows and D. J. Wheeler, A block-sorting lossless data compression algorithm, Technical Report 124, Digital Equipment Corporation, (1994).

[25] C. Camarero and C. Martínez, Quasi-perfect Lee codes of radius 2 and arbitrarily large dimension, *IEEE Trans. Inform. Theory* **62** (2016), 1183–1192.

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

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

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

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

[30] M. Crochemore, J. Désarménien, and D. Perrin, A note on the Burrows-Wheeler transformation, *Theoret. Comput. Sci.* **332** (2005), 567–572.

[31] D. Cvetkovič, M. Doob, and H. Sachs, *Spectra of Graphs: Theory and Applications*, 3rd. ed., Johann Ambrosius Barth, (1995).

[32] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory and Ramanujan Graphs*, Cambridge University Press, (2003).

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

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

[35] P. Deligne, *Cohomologie Étale, SGA* $4\frac{1}{2}$, Springer-Verlag, (1977).

[36] P. Diaconis, J. Fulman, and S. Holmes, Analysis of casino shelf shuffling machines, *Ann. Appl. Probab.* **23** (2013), 1692–1720.

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

[38] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *SIAM J. Comput.* **38** (2008), 97–139.

[39] L. Dolecek and V. Anantharam, Repetition error correcting sets: Explicit constructions and prefixing methods, *SIAM J. Discrete Math.* **23** (2010), 2120–2146.

[40] G. Dresden and W. M. Dymàček, Finding factors of factor rings over the Gaussian integers, *Amer. Math. Monthly* **112** (2005), 602–611.

[41] P. Ferragina, R. Giancarlo, G. Manzini, and M. Sciortino, Boosting textual compression in optimal linear time, *J. ACM* **52** (2005), 688–713.

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

[43] I. M. Gessel and C. Reutenauer, Counting permutations with given cycle structure and descent set, *J. Combin. Theory Ser. A* **64** (1993), 189–215.

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

[45] E. N. Gilbert and J. Riordan, Symmetry types of periodic sequences, *Illinois J. Math.* **5** (1961), 657–665.

[46] B. D. Ginzburg, A certain number-theoretic function which has an application in coding theory (Russian), *Problemy Kibernet.* **19** (1967), 249–252.

[47] S. W. Golomb and L. R. Welch, Perfect codes in the Lee metric and the packing of polyominoes, *SIAM J. Appl. Math.* 18 (1970), 302–317.

[48] L. Greenberg, Conformal transformations of Riemann surfaces, *Amer. J. Math.* **82** (1960), 749–760.

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

[50] D. J. Grynkiewicz, A. Philipp, and V. Ponomarenko, Arithmetic-progression-weighted subsequence sums, *Israel J. Math.* **193** (2013), 359–398.

[51] H. Gupta, Partitions — a survey, *J. Res. Nat. Bur. Standards – B. Math. Sci.* **74B** (1970), 1–29.

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

[53] P. Hall, The Eulerian functions of a group, *Q. J. Math.* **7** (1936), 134–151.

[54] 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.

[55] W. J. Harvey, Cyclic groups of automorphisms of a compact Riemann surface, *Q. J. Math.* **17** (1966), 86–97.

[56] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, A pseudorandom generator from any one-way function, *SIAM J. Comput.* **28** (1999), 1364–1396.

[57] M. Hayashi, General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel, *IEEE Trans. Inf. Theory* **52** (2006), 1562–1575.

[58] M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, *IEEE Trans. Inf. Theory* **57** (2011), 3989–4001.

[59] M. Hazewinkel, Witt vectors. Part 1, *Handbook of Algebra*, Vol. 6, pp. 319–472, Elsevier, (2009).

[60] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc.* 43 (2006), 439–561.

[61] M. Huber, Authentication and secrecy codes for equiprobable source probability distributions, *IEEE International Symposium on Information Theory — ISIT 2009*, 1105–1109.

[62] M. Huber, Combinatorial designs for authentication and secrecy codes, *Foundations and Trends in Communications and Information Theory*, 5(6), 581–675, (2010).

[63] R. Impagliazzo and D. Zuckerman, How to recycle random bits, *Proceedings of the 30th Annual Symposium on Foundations of Computer Science — FOCS 1989*, 248–253.

[64] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, (1994).

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

[66] H. J. Karloff, S. Suri, and S. Vassilvitskii, A model of computation for MapReduce, *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms — SODA 2010*, 938–948.

[67] 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.

[68] 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.

[69] R. d. M. Koch and S. Ramgoolam, Strings from Feynman graph counting: Without large N, *Phys. Rev. D* **85** 026007 (2012).

[70] R. d. M. Koch, S. Ramgoolam, and C. Wen, On the refined counting of graphs on surfaces, *Nuclear Phys. B* **870** (2013), 530–581.

[71] V. P. Kostov and B. Shapiro, Hardy-Petrovitch-Hutchinson's problem and partial theta function, *Duke Math. J.* **162** (2013), 825-861.

[72] H. Krawczyk, LFSR-based hashing and authentication, *14th Annual International Cryptology Conference — CRYPTO 1994*, 129–139.

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

[74] J. C. Lagarias and B. L. Weiss, Splitting behavior of S_n-polynomials, *Res. Number Theory* **1** (2015), Article: 7.

[75] S. K. Lando and A. K. Zvonkin, *Graphs on Surfaces and Their Applications (with Appendix by D. B. Zagier)*, Springer-Verlag, (2004).

[76] J. K. Langley, A certain functional-differential equation, *J. Math. Anal. Appl.* **244** (2000), 564–567.

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

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

[79] C. E. Leiserson, T. B. Schardl, and J. Sukha, Deterministic parallel random-number generation for dynamic-multithreading platforms, *Proceedings of the 17th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming — PPoPP 2012*, 193–204.

[80] V. I. Levenshtein, Binary codes capable of correcting deletions, insertions and reversals (in Russian), *Doklady Akademii Nauk SSSR* **163** (1965), 845–848. English translation in *Soviet Physics Dokl.* **10** (1966), 707–710.

[81] V. I. Levenshtein, Binary codes capable of correcting spurious insertions and deletions of ones (in Russian), *Problemy Peredachi Informatsii* **1** (1965), 12–25. English translation in *Problems of Information Transmission* **1** (1965), 8–17.

[82] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, (1997).

[83] M. W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601.

[84] M. W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, *Invent. Math.* **159** (2005), 317–367.

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

[86] Y. Liu, On some conjectures by Morris et al., about zeros of an entire function, *J. Math. Anal. Appl.* **226** (1998), 1–5.

[87] L. Lovász, Spectra of graphs with transitive groups, *Period. Math. Hungar.* **6** (1975), 191–195.

[88] A. Lubotzky, Expander graphs in pure and applied mathematics, *Bull. Amer. Math. Soc.* 49 (2012), 113–162.

[89] G. Maze, Partitions modulo n and circulant matrices, *Discrete Math.* **287** (2004), 77–84.

[90] L. McAven, R. Safavi-Naini, and M. Yung, Symmetric authentication codes with secrecy and unconditionally secure authenticated encryption, *Progress in Cryptology — INDOCRYPT 2004*, 148–161.

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

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

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

[94] H. Mercier, V. K. Bhargava, and V. Tarokh, A survey of error-correcting codes for channels with symbol synchronization errors, *IEEE Commun. Surv. Tutor.* **12** (2010), 87–96.

[95] N. Metropolis and G.-C. Rota, Witt vectors and the algebra of necklaces, *Adv. Math.* **50** (1983), 95–125.

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

[97] J. Milnor and W. Thurston, On iterated maps of the interval, *Dynamical Systems*, Lecture Notes in Mathematics, Vol. 1342, pp. 465–563, Springer, (1988).

[98] M. Mitzenmacher, A survey of results for deletion channels and related synchronization channels, *Probab. Surv.* **6** (2009), 1–33.

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

[100] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, (1995).

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

[102] 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.

[103] N. Nisan, Pseudorandom generators for space-bounded computations, *Proceedings of the 22nd Annual ACM symposium on Theory of Computing — STOC 1990*, 204–212.

[104] A. Pagh and R. Pagh, Uniform hashing in constant time and optimal space, *SIAM J. Comput.* **38** (2008), 85–96.

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

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

[107] R. Razen, J. Seberry, and K. Wehrhahn, Ordered partitions and codes generated by circulant matrices, *J. Combin. Theory Ser. A* **27** (1979), 333–341.

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

[109] R. Renner and S. Wolf, Simple and tight bounds for information reconciliation and privacy amplification, *Advances in Cryptology — ASIACRYPT 2005*, 199–216.

[110] P. Rogaway, Bucket hashing and its application to fast message authentication, *15th Annual International Cryptology Conference — CRYPTO 1995*, 29–42.

[111] G.-C. Rota, On the foundations of combinatorial theory. I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368.

[112] S. Rudich and A. Wigderson, *Computational Complexity Theory*, IAS/Park City Mathematics Series, American Mathematical Society, (2004).

[113] F. Ruskey and J. Sawada, An efficient algorithm for generating necklaces with fixed density, *SIAM J. Comput.* **29** (1999), 671–684.

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

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

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

[117] T. Schönemann, Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben, *J. Reine Angew. Math.* **1839** (1839), 231–243.

[118] A. D. Scott and A. D. Sokal, The repulsive lattice gas, the independent-set polynomial, and the Lovász local lemma, *J. Stat. Phys.* **118** (2005), 1151–1261.

[119] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, (1977).

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

[121] A. Siegel, On universal classes of extremely random constant-time hash functions, *SIAM J. Comput.* **33** (2004), 505–543.

[122] M. Sipser, A complexity theoretic approach to randomness, *Proceedings of the 15th Annual ACM symposium on Theory of Computing — STOC 1983*, 330–335.

[123] N. J. A. Sloane, On single-deletion-correcting codes, In *Codes and Designs*, Ohio State University, May 2000 (Ray-Chaudhuri Festschrift), K. T. Arasu and A. Seress (editors), Walter de Gruyter, Berlin, 2002, pp. 273–291.

[124] A. D. Sokal, The leading root of the partial theta function, *Adv. Math.* **229** (2012), 2603–2621.

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

[126] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, 2nd ed., Cambridge University Press, (2012).

[127] R. P. Stanley and M. F. Yoder, A study of Varshamov codes for asymmetric channels, Jet Propulsion Laboratory, Technical Report 32-1526, Vol. XIV (1973), 117–123.

[128] D. R. Stinson, On the connection between universal hashing, combinatorial designs and error-correcting codes, *Electronic colloquium on computational complexity (ECCC)*, 2(52), 1995.

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

[130] J.-Y. Thibon, The cycle enumerator of unimodal permutations, *Ann. Comb.* **5** (2001), 493–500.

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

[132] L. Tóth, Counting solutions of quadratic congruences in several variables revisited, *J. Integer Seq.* **17** (2014), Article 14.11.6.

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

[134] H. Tyagi and A. Vardy, Universal hashing for information-theoretic security, *Proceedings of the IEEE* **103** (2015), 1781–1795.

[135] R. R. Varshamov, On an arithmetic function with an application in the theory of coding (in Russian), *Dokl. Akad. Nauk SSSR* **161** (1965), 540–543.

[136] R. R. Varshamov, A class of codes for asymmetric channels and a problem from the additive theory of numbers, *IEEE Trans. Inform. Theory* **19** (1973), 92–95.

[137] R. R. Varshamov and G. M. Tenengolts, Codes which correct single asymmetric errors (in Russian), *Avtomatika i Telemekhanika* **26** (1965), 288–292. English translation in *Automation and Remote Control* **26** (1965), 286–290.

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

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

[140] 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.

[141] L. Weisner, Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.* **38** (1935), 474–484.

[142] A. Weiss and T. D. Rogers, The number of orientation-reversing cycles in the quadratic map, *Oscillation, Bifurcation and Chaos*, CMS Conference Proc., Vol. 8, pp. 703–711, (1987).

[143] A. Wiman, Üeber die hyperelliptischen Curven und diejenigen vom Geschlechte p = 3 welche eindeutigen Transformationen in sich zulassen, *Bihang Till. Kongl. Svenska Veienskaps-Akademiens Hadlingar, Stockholm* **21** (1895-6), 1–23.

[144] Q.-H. Yang and M. Tang, On the addition of squares of units and nonunits modulo n, *J. Number Theory* **155** (2015), 1–12.

[145] H. Zieschang, E. Vogt, and H. -D. Coldeway, *Surfaces and Planar Discontinuous Groups*, Springer-Verlag, (1980).