Trends in Mathematics

Jordi Guàrdia
Nicuşor Minculete
Diana Savin
Montserrat Vela
Abdelkader Zekhnini
Editors

New Frontiers in Number Theory and Applications

Birkhäuser

Trends in Mathematics

Trends in Mathematics is a series devoted to the publication of volumes arising from conferences and lecture series focusing on a particular topic from any area of mathematics. Its aim is to make current developments available to the community as rapidly as possible without compromise to quality and to archive these for reference.

Proposals for volumes can be submitted using the Online Book Project Submission Form at our website www.birkhauser-science.com.

Material submitted for publication must be screened and prepared as follows:

All contributions should undergo a reviewing process similar to that carried out by journals and be checked for correct use of language which, as a rule, is English. Articles without proofs, or which do not contain any significantly new results, should be rejected. High quality survey papers, however, are welcome.

We expect the organizers to deliver manuscripts in a form that is essentially ready for direct reproduction. Any version of TEX is acceptable, but the entire collection of files must be in one particular dialect of TEX and unified according to simple instructions available from Birkhäuser.

Furthermore, in order to guarantee the timely appearance of the proceedings it is essential that the final version of the entire material be submitted no later than one year after the conference.

Jordi Guàrdia • Nicuşor Minculete • Diana Savin •
Montserrat Vela • Abdelkader Zekhnini
Editors

New Frontiers in Number Theory and Applications

Birkhäuser

Editors
Jordi Guàrdia
Department of Mathematics
Universitat Politècnica de Catalunya
Barcelona, Catalunya, Spain

Diana Savin
Department of Mathematics and Computer Science
Transilvania University of Braşov
Braşov, Romania

Abdelkader Zekhnini
Department of Mathematics
Mohammed Premier University
Oujda, Morocco

Nicuşor Minculete
Department of Mathematics and Computer Science
Transilvania University of Braşov
Braşov, Romania

Montserrat Vela
Department of Mathematics
Universitat Politècnica de Catalunya
Barcelona, Catalunya, Spain

ISSN 2297-0215 ISSN 2297-024X (electronic)
Trends in Mathematics
ISBN 978-3-031-51958-1 ISBN 978-3-031-51959-8 (eBook)
https://doi.org/10.1007/978-3-031-51959-8

This book is published under the imprint Birkhäuser, www.birkhauser-science.com by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

The genesis of this book goes back to numerous collaborations among the editors: various subsets of us have co-authored research papers, co-organized workshops and conferences, and have met either personally or virtually, in number theory meetings. Beyond just our scientific connections, there's a personal rapport among us that serves as the foundation for this exciting new collaboration, aimed to expand our joint research interests.

The book combines papers with new results, articles of a more expository character, articles with new proofs of known results, and some articles of mixed nature.

Beyond its scientific content, this book also underscores the global nature of contemporary research: the authors come from nine different countries all over the world.

From class field theory to analytic theory, almost all subjects in Number Theory are the focus of some of the chapters in the book. The ordering of the chapters reflects the mathematical proximity of their contents. A brief description of every chapter and its authors follows this preface.

The editors wish to thank all the authors for their contributions, and a list of anonymous referees whose insightful comments and suggestions enriched the book's content. Also, the third editor thanks professor Mirela Ştefănescu for her useful comments about the format of this book.

Barcelona, Catalunya, Spain — Jordi Guàrdia
Braşov, Romania — Nicuşor Minculete
Braşov, Romania — Diana Savin
Barcelona, Catalunya, Spain — Montserrat Vela
Oujda, Morocco — Abdelkader Zekhnini

Contents

About the Chapters of This Book and Their Authors

Abdelmalek Azizi, Jamal Benamara and El Hassane Laaji have contributed in this book an interesting chapter that illustrates the applications of algebra and number theory in cryptography. The title of their chapter is "Survey Number Theoretic Transform Algorithm over a Polynomial Ring and Its Application". The authors study the multiplication performance over the polynomial rings of the form $R_q = \mathbb{Z}_q[X]/(X^n + 1)$. The Number Theoretic Transform (NTT) can reduce the multiplication complexity in R_q from $O(n^2)$ to $O(n \log n)$. Compared to convolution multiplication, it increases the speed performance by a factor of up to $\times 3$. The NTT algorithm is used to increase the speed performance of the cryptographic functions of some Lattice-Based Cryptosystems like NTRU, NewHope (Ring-LWE), Keyber, and Falcon (Signature scheme), which are proposed to be standardized by NIST (National Institute of Standards and Technology) as post-quantum cryptosystems capable of resisting quantum computer attacks.

Abdelmalek Azizi is one of the creators of the number theory school in Morocco. Jamal Benamara and El Hassane Laaji are specialists in number theory and cryptography.

Abdelmalek Azizi, Jamal Benamara and El Hassane Laaji are working at Mohamed Premier University, Sciences Faculty, Mathematics Department, Oujda.

Abdelmalek Azizi, Mohamed Mahmoud Chems-Eddin, Abdelkader Zekhnini are specialists in algebraic number theory; currently their field of interest is class field theory. Abdelkader Zekhnini is working at Mohamed Premier University, Sciences Faculty, Mathematics Department, Oujda, Morocco, and Mohamed Mahmoud Chems-Eddin is working at Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mahraz, Department of Mathematics, Fez, Morocco. Last years, they published high-level articles which operate in class field theory. They contribute in this book with the chapter entitled *On the Hilbert* 2*-class field towers of the layers of some cyclotomic* $\mathbb{Z}_2$*-extensions* . The authors study the structure of the Galois groups of second Hilbert 2-class fields of the layers of the cyclotomic $\mathbb{Z}_2$-extensions of some special Dirichlet fields.

Dorin Andrica and Ovidiu Bagdasar have authored the chapter "Some Remarks on the Coefficients of Cyclotomic Polynomials". This work studies some

properties of these important polynomials which have applications in various areas of mathematics. In particular, the authors present some recent advances regarding the practical calculation of the coefficients of these polynomials, based on a recursive formula involving Ramanujan sums.

Dorin Andrica is Emeritus Professor at the Faculty of Mathematics and Computer Science, Babeş-Bolyai University, Cluj-Napoca, Romania. He is the author of some books on number theory published by Springer, including *Quadratic Diophantine Equations* in 2015.

Ovidiu Bagdasar is Associate Professor at the University of Derby, United Kingdom. He holds a PhD in applied mathematics from University of Nottingham and another PhD in pure mathematics from Babeş-Bolyai University, Cluj-Napoca, Romania. He has co-authored with Dorin Andrica the book *Recurrent Sequences: Key Results, Applications, and Problems* published by Springer in 2020.

Cristina Ballantine and George Beck have contributed in this book with the chapter entitled "Partitions Enumerated by Self-similar Sequences". In enumerative combinatorics, we often count the number of elements in sets of discrete structures built up recursively. This chapter is part of the study of the inverse problem: given a sequence of positive integers defined recursively, find sets whose cardinality is given by the sequence. More specifically, the authors start with familiar classical recursive sequences, modify them to be self-similar, and survey sets of integer partitions counted by such sequences. Cristina Ballantine received her PhD from the University of Toronto with a thesis on automorphic forms and hypergraphs. She is a professor at the College of the Holy Cross in Massachusetts. Her current research is in number theory and combinatorics with an emphasis on partition theory. George Beck received a BSc (Honours Math) from McGill University and an MA in math from the University of British Columbia. He has worked as a technical writer, director, and editor at Wolfram Research for the last 30 years. His mathematical interests are in combinatorics and geometry.

Fouad Elmouhib, Mohamed Talbi, Abdelmalek Azizi are specialists in algebraic number theory. They have contributed in this book with the chapter entitled "On the Exact Divisibility by 5 of the Class Number of Some Pure Metacyclic Fields". Let $\Gamma = \mathbb{Q}(\sqrt[5]{n})$ be a pure quintic field, where n is a natural number 5^{th} power-free. Let $k = \mathbb{Q}(\sqrt[5]{n}, \zeta_5)$, with ζ_5 is a primitive 5^{th} root of unity, be the normal closure of Γ, and a pure metacyclic field of degree 20 over $\mathbb{Q}$. When n takes some particular forms, the authors show that Γ admits a trivial 5-class group and 5 divides exactly the class number of k.

Fouad Elmouhib is working at Mohamed Premier University, Sciences Faculty, Mathematics Department, Oujda and Mohamed Talbi is working at Regional Center of Professions of Education and Training, Oujda, Morocco.

Lhoussain El Fadil is working at Sidi Mohamed Ben Abdellah University, Fez—Morocco. He has contributed two chapters on number theory in this book. First chapter is entitled *On Monogenity of Certain Number Fields Defined by a Trinomial* $x^{p^r} + ax + b$. Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible trinomial $F(x) = x^{p^r} + ax + b \in \mathbb{Z}[x]$ for some positive prime integer p and a positive integer r. The goal of this paper is to give

some sufficient conditions on $F(x)$, which guarantee that p is a common index divisor of K, and so that K is not monogenic. For $p = 2$ and $r = 3$, let K be an octic number field generated by a complex root of a monic irreducible trinomial $F(x) = x^8 + ax + b \in \mathbb{Z}[x]$. He characterizes when $\mathbb{Z}[\alpha]$ is integrally closed. He also gives necessary and sufficient conditions on $F(x)$, which determine all prime index divisors of K.

Second chapter is entitled "Irreducible Factors of a Polynomial and Extensions of Valuations". Let (K, v) be a valued field, R_v its valuation ring, M_v its maximal ideal, $\mathbb{F}_v$ its residue field, and $L = K(\alpha)$ a finite simple field extension of K, generated by a root α of a monic irreducible polynomial $F \in R_v[X]$. The main goal of this chapter is to describe all valuations of L extending v, together the ramification index and the residue degree are calculated for every extension. In particular, if the author assumes that the polynomial $\overline{F}$ factors as a product of r distinct powers of monic irreducible polynomials over $\mathbb{F}_v$, then the author gives necessary conditions on F in order to have exactly r valuations of L extending v. Some applications will be given too.

Alexandru Gica is currently working at University of Bucharest. He is teaching, since 1993, Elementary Number Theory, Analytic Number Theory and Algebraic Number Theory, at the University of Bucharest. He defended his PhD thesis ("Analytical Methods in Number Theory") in 2001, under the supervision of Toma Albu (and under the guidance of Laurenţiu Panaitopol). His main area of research is Algebraic Number Theory. When writing the current chapter (*Lengths and Class Numbers*), he tried to give a comprehensive survey of his research which followed the ideas from his PhD thesis. The thread of the paper is the interplay between lengths and class numbers.

Nurten Gürses, Gülsüm Yeliz Saçli, Salim Yüce are specialists in geometry, algebra and number theory. They are currently working at the Yildiz Technical University, Faculty of Arts and Sciences, Department of Mathematics, Istanbul, Türkiye. They have contributed in this book a chapter entitled *On Extended k-order Fibonacci and Lucas Numbers via $\mathcal{DGC}$ Numbers* . The dual-generalized complex numbers ($\mathcal{DGC}$) are one of the hypercomplex numbers and constructed by the doubling procedure of the dual numbers and the generalized complex numbers. This work introduces direct extended version of k-order Fibonacci/Lucas numbers by bringing together $\mathcal{DGC}$ numbers and generalized k-order Fibonacci/Lucas numbers. As a similar approach, two parameters $\mathcal{DGC}$ extension of Fibonacci numbers, namely the (s, r)-$\mathcal{DGC}$ Fibonacci numbers, are also discussed via same method. The special identities and several properties are examined. Moreover, these extended versions give dual-complex, hyper-dual and dual-hyperbolic extended k-order Fibonacci/Lucas numbers for the specific conditions. Also, considering specific choices of the value k, the important results are discussed and the classifications are given.

Eszter Gyimesi, Gábor Nyul, Gabriella Rácz are currently working at the University of Debrecen, Institute of Mathematics from Debrecen, Hungary. Gábor Nyul is an expert in combinatorics and number theory. Eszter Gyimesi and Gabriella Rácz are specialists in combinatorics. They have contributed in this book a chapter

entitled "Generalizations of Stirling-like and Bell-like Numbers" about the results of their research group. Stirling and Bell numbers are fundamental objects of enumerative combinatorics, they count, among others, partitions of a finite set. The authors give a survey on recent results concerning generalizations of these numbers: when certain elements are not allowed to be in the same block; when there are restrictions on the cardinality of the blocks; the Whitney–Dowling type variant arising from abstract algebra; ordered modifications where the blocks or the partition is ordered. In addition to their results published in previous papers, some new theorems and proofs are also presented.

Sorina Ionică is working at University of Picardie Jules Verne, Amiens, France. She is a specialist in the area of algorithmic number theory and its applications to cryptography. She has contributed in this book with the chapter entitled "The Complex Multiplication Method for Genus 3 Curves". The author considers the problem of constructing genus 3 hyperelliptic curves defined over the complex field with the property that their Jacobians are simple and admit complex multiplication (CM). In genus 1 and 2, a natural answer comes from the theory of complex multiplication of Shimura and Taniyama, since all simple principally polarized abelian varieties (p.p.a.v.) of dimension 1 and 2 are isomorphic to Jacobians of hyperelliptic curves. In genus 3, the situation is more complicated and thus more interesting. Up to isomorphism, every p.p.a.v. of dimension 3 is the Jacobian of a complete smooth projective curve of genus 3. Moreover, this curve is isomorphic either to a hyperelliptic or a plane quartic curve. However, the moduli space of p.p.a.v. in dimension 3 has dimension 6 and the subspace of Jacobians of hyperelliptic curves has codimension 1. Therefore, given a random sextic CM field, she expects that the set of p.p.a.v. with CM by the maximal order of that field will not contain any hyperelliptic Jacobians. The author reviews progress made in recent years on the construction of Jacobians of hyperelliptic curves with CM in genus 3.

David Leep received his PhD in Mathematics from the University of Michigan in 1980 and is currently a Professor of Mathematics at the University of Kentucky. He conducts research in areas ranging from the algebraic theory of quadratic forms, homogeneous forms in many variables, Galois theory, and varieties over finite fields and p-adic fields. In his chapter ("An Optimal Version of Warning's Theorem over the Field of Two Elements") in this volume, Leep finds optimal lower bounds for the number of zeros of a system of polynomials with coefficients in the field of two elements in terms of the degree and the number of variables of the system, and thereby finding an improved statement for the two-element field of a result that is often called Warning's second theorem.

Daniel C. Mayer is professor and project leader at Karl-Franzens University Graz, Austria. His expertise comprises algebraic number theory and p-group theory, and his contribution to this book is a chapter with the title "New Perspectives of the Power-Commutator Structure: Coclass Trees of CF-Groups and Related BCF-Groups". This chapter completely identifies the non-metabelian Schur sigma-automorphism groups of 3-class field towers of imaginary quadratic fields with non-elementary 3-class group and moderate rank distribution (§7, Theorem 9, Corollary 1).

Mircea Merca is working at Polytechnic University of Bucharest. His research fields are the theory of partitions, number theory, combinatorics, special functions and algorithms. He contributes in this book with the chapter entitled "The Euler-Riemann Zeta Function with Even Arguments in Terms of Binomial Coefficients". He investigates new methods for computing the Euler-Riemann zeta functions with even arguments. He provides formulas for $\zeta(4n)$, $\zeta(6n)$, $\zeta(8n)$, $\zeta(10n)$ and $\zeta(12n)$ as sums over all the unrestricted integer partitions of the positive integer n. This method uses only (large) integer arithmetic, is simpler to program and provides significant improvements in computing the values of $\zeta(4n)$, $\zeta(6n)$, $\zeta(8n)$, $\zeta(10n)$ or $\zeta(12n)$ as sums over integer partitions.

Nicuşor Minculete and **Diana Savin** are currently working at Transilvania University of Braşov, Romania. Nicuşor Minculete is a specialist in analytic and elementary number theory, especially in the study of inequalities (involving positive integers) in number theory. Diana Savin is a specialist in algebraic number theory, especially ramification theory in algebraic numbers number fields. They have contributed in this book with the chapter entitled "Some Properties of a Type of Entropy of an Ideal and the Divergence of Two Ideals". In a previous article they generalized the notion of entropy for certain ideals in rings of algebraic integers. In this chapter the authors obtain some results related to the entropy of a positive integer number and the divergence of two numbers and also some results about the entropy of some types of ideals and the divergence of two ideals. In the last section of their chapter, the authors find some inequalities, involving the entropy H of an exponential divisor of a positive integer, respectively the entropy H of an exponential divisor of an ideal.

Sever Angel Popescu is a specialist in algebraic number theory, particularly in valuation theory and Galois theory. He obtained a PhD degree in 1986 with dr. doc. Nicolae Popescu from the Institute of Mathematics of the Romanian Academy. He has more than 45 papers, published in known mathematical journals. He was also professor of Advanced Mathematics at the Technical University of Civil Engineering Bucharest, and published some advanced mathematical books for engineers and physicists, including in Springer Verlag Publishing House. His chapter in the present book, "A Simple and Self-contained Proof for the Lindemann-Weierstrass Theorem" is a self-contained and easy to understand exposition of the famous classical results of Lindemann and Weierstrass in transcendental number theory.

Mohammed Tamimi and Abdelkader Zekhnini have contributed in this book by a chapter entitled "On the 2-class number of some real cyclic quartic number fields II". Let $\mathbb{K} = \mathbb{Q}(\sqrt{n\epsilon_0\sqrt{\ell}})$ be a real cyclic quartic number field, with $\ell \equiv 5 \pmod 8$ a prime positive integer, n a positive square-free integer relatively prime to ℓ and ϵ_0 the fundamental unit of the real quadratic subfield $k = \mathbb{Q}(\sqrt{\ell})$. In this chapter, the authors are interested in studying the powers of 2 dividing the class number of the 2-class group of rank 2 of some fields $\mathbb{K}$.

Mohammed Tamimi is working at Mohamed Premier University, Sciences Faculty, Mathematics Departement, Oujda, Morocco.

László Tóth is a Professor and Head of Department at the University of Pécs, Hungary. He obtained the PhD degree in Mathematics at the Babeş-Bolyai University of Cluj, Romania in 1996, as well as at the University of Debrecen, Hungary in 2003. He received the title Doctor of the Hungarian Academy of Sciences in 2020. He has published more than one hundred scientific papers in Number Theory, Combinatorics and Group Theory. He is editor and referee for several mathematical journals, and Editor-in-Chief of the journal *Mathematica Pannonica*. His contribution to the present book is the chapter entitled *Counting subgroups of the groups* $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$*: a survey* . This chapter gives an overview of exact and asymptotic formulas on the number of cyclic subgroups and total number of subgroups of the groups in the title, where $k \geq 2$ and $n_1, \ldots, n_k$ are arbitrary positive integers. Some new results are also pointed out.

George C. Ţurcaş is currently affiliated with the Faculty of Mathematics and Computer Science at Babeş-Bolyai University in Cluj-Napoca, Romania. He specializes in Algebraic Number Theory, with a particular emphasis on elliptic curves. George earned his PhD from the University of Warwick, where he was mentored by Samir Siksek. He has contributed in this book with the chapter entitled "On the p-isogenies of elliptic curves with multiplicative reduction over quadratic fields" to this book. In his work, George presents sufficient conditions for the absence of p-isogenies in infinite families of elliptic curves defined over quadratic fields and showcases a Diophantine application using the "modular method" for one of these results. The chapter further explores some computational facets of bielliptic modular curves.

Montserrat Vela is currently working at the University Politècnica de Catalunya-Barcelona Tech. Her research is presently centered on Hopf-Galois theory, working together with T. Crespo and A. Rio. They have described the Hopf Galois character of all separable extensions of degree less than or equal to 6 according to the Galois group of the Galois closure and the intermediate extensions. She contributes in this book with the chapter entitled "The Hopf-Galois Structures of the 3 and 6-Division Points of the Lemniscate Curve", where she determines all Hopf Galois structures of the number field generated by the coordinates of a real three (or six) division point of the lemniscate.

About the Editors

Jordi Guàrdia is an associate professor in the Math Department at Universitat Politècnica de Catalunya-Barcelona Tech. His research has been focused in arithmetic geometry and computational number theory. Jointly with J. Montes and E. Nart, he has been involved in the development of Montes algorithm and its theoretical and computational applications, including the Magma package "+Ideals". They are now working in higher rank valuation theory and the interaction between number theory and singularities theory. He is one of the founders of the biannual conference "Jornadas de Teoria de Números", and is an active member of the "Seminari de Teoria de Nombres de Barcelona".

Nicuşor Minculete is an associate professor and vice dean at the Faculty of Mathematics and Computer Science, Transilvania University of Braşov, Romania. Nicuşor Minculete earned a degree in Mathematics at University of Bucharest (1994) and a PhD in Mathematics at Institute of Mathematics of the Romanian Academy (2012). His research interests include mathematical inequalities and its applications; number theory; Euclidean geometry. He is a Member of the Editorial Board at the following journals: *European Journal of Mathematics and Applications*, *International Journal of Geometry*, *Bulletin of the Transilvania University of Brasov*, *General Mathematics*, *Octogon Mathematical Magazine*. He has published 100 research papers.

Diana Savin is an associate professor at the Faculty of Mathematics and Computer Science, Transilvania University of Braşov, Romania. Diana Savin graduated from the Faculty of Mathematics and Computer Science of the University of Bucharest in 1996. She obtained the PhD degree in Mathematics at Ovidius University of Constanţa, Romania, in 2004, with a thesis about Diophantine equations. Diana Savin works in number theory. Her research directions are algebraic number theory (especially ramification theory in algebraic numbers number fields), associative algebras, computational number theory and combinatorics. She wrote several research articles on these areas. Alone or jointly with V. Acciaro, M. Taous and A.

Zekhnini, she has been studying quaternion algebras over some algebraic number fields, using ramification theory in algebraic number fields.

Montserrat Vela is an associate professor of the Math Department at Universitat Politècnica de Catalunya-Barcelona Tech. She has worked mainly in the inverse problem in Galois theory. Nowadays, her research is focused on Hopf-Galois theory, having published some relevant papers jointly with T. Crespo and A. Rio. She is an active member of the "Seminari de Teoria de Nombres de Barcelona".

Abdelkader Zekhnini is an associate professor at the Mohammed Premier University, Sciences Faculty, Department of Mathematics, Oujda, Morocco. He obtained the PhD degree in Mathematics in 2014, at the same university with a thesis on capitulation theory and Hilbert class field towers. Before, he was a mathematics teacher in high schools. Abdelkader Zekhnini works in many directions of number theory as algebraic number theory (especially capitulation theory), Hilbert class field towers, Iwasawa theory, commutative algebra (Integer valued polynomials, Pòlya fields) and associative algebras. He wrote several research papers on these areas, over 40, published in Web of Science indexed journals.

Survey number theoretic transform algorithm over a polynomial ring and its application

Abdelmalek Azizi, Jamal Benamara, and El Hassane Laaji

1 Introduction

The Number Theoretic Transform (NTT) is an efficient method for multiplying two polynomials of high degree with integer coefficients. It serves as a generalization of the Discrete Fourier Transform (DFT) but works over a quotient ring rather than a field of complex numbers [10]. NTT and DFT share similar computation speedup property as some related works, such as the paper titled "Complexity of Computations with Matrices and Polynomials" by Victor Pan, which presents a new algorithm for efficiently computing the DFT of polynomials and matrices [12].

There are several algorithms available to compute polynomial multiplication, including the schoolbook algorithm [9], Karatsuba algorithm [8], Toom-Cook algorithm [5], and others.

NTT finds numerous applications in computer arithmetic and the cryptographic domain, reducing the time complexity of polynomial multiplication from $O(n^2)$ to $O(n \log n)$ [4]. When compared to convolution multiplication, it increases speed performance by a factor of up to $\times 3$.

The NTT algorithm is employed to accelerate the cryptographic functions of various schemes based on lattices. For example, the work of Alkim et al. [1] on New-Hope," a cryptosystem whose security relies on lattice problems and is constructed on Ring Learning With Error (Ring-LWE), utilizes the NTT algorithm combined with the Montgomery algorithm to speed up modular multiplication [11]. This cryptosystem was proposed for the NIST post-quantum standardization project and has already been used and implemented in a new release of Google Chrome, namely "Chrome Canary." Similarly, the work of Azizi et al. [2] on "NTRUrobust,"

A. Azizi · J. Benamara · E. H. Laaji (✉)
Mohammed First University Morocco, Oujda, Morocco
e-mail: e.laaji@ump.ac.ma

J. Guàrdia et al. (eds.), *New Frontiers in Number Theory and Applications*, Trends in Mathematics, https://doi.org/10.1007/978-3-031-51959-8_1

a post-quantum cryptosystem whose security is based on lattice problems and NTRU assumptions, uses the NTT algorithm combined with the "Fast-Modular Multiplication Algorithm" (FMMA) [3].

In this work, wa are interested in describing and analyzing the NTT algorithm over the polynomial rings of the form $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.

2 Preliminary

Let $n \geq 2$ be a nonzero positive integer. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes q of the form $1 + kn$, where k is also a nonzero positive integer. For a such prime q, we know that $\mathbb{F}_q = \mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ is a finite field of cardinal q, and the multiplicative group $\mathbb{Z}_q^*$ of integers modulo q is a cyclic group of order $\varphi(q) = q - 1 = kn$, where φ is the Euler's totient function, hence it must have one generator τ which is a primitive $(q-1)$-th root of unity modulo q, therefore, If we put $\omega \equiv \tau^k \pmod{q}$, then we have

$$w^n = \tau^{nk} = \tau^{q-1} = \tau^{\varphi(q)} \equiv 1 \pmod{q}$$

and since $\omega^i \neq 1$ for all $1 \leq i < n$, then ω is a primitive nth root of unity that is required in computing Number Theoretic Transform (NTT).

Let $f(X) \in \mathbb{Z}_q[X]$ be a nonzero polynomial of degree d, then the polynomial ring $\mathbb{Z}_q[X]$ in the variable X, with coefficients belonging to $\mathbb{Z}_q$ modulo $f(X)$, i.e. the ring $R_q = \mathbb{Z}_q[X]/f(X)$ contains exactly q^d elements (see [7]).

Any vector $a \in \mathbb{Z}_q^n$ can be viewed as an element g of R_q such that $g(X) = \sum_{i=0}^{n-1} a_i X^i$.

Evaluating the polynomial $g(X) \pmod{f(X)}$ at ω^j for $0 \leq j \leq n-1$, we get $b_j = g(\omega^j)$.

The NTT is an extension of the DFT, is defined over the field $\mathbb{Z}_q$ by using the primitive nth root of unity ω

$$\begin{array}{rccc} \text{NTT}: & \mathbb{Z}_q^n & \longmapsto & \mathbb{Z}_q^n \\ & a = (a_0, \ldots, a_{n-1}) & \longmapsto & b = (b_0, \ldots, b_{n-1}) \end{array}$$

where $b_i = \sum_{j=0}^{n-1} a_j \omega^{ij}$. Since $gcd(n, q) = 1$, then we can compute $n^{-1} \pmod{q}$ and the inverse of NTT is given as following:

$$a_k = n^{-1} \sum_{i=0}^{n-1} b_i \omega^{-ki} \pmod{q}.$$

3 Number Theoretic Transform Algorithm (NTT)

The number-theoretic transform (NTT) is indeed a generalization of the Discrete Fourier Transform (DFT) as mentioned in [10]. While the DFT is defined in the complex number group, the NTT is carried out in the positive integer group and finite fields.

In the context of polynomials, the NTT provides an efficient method for multiplication in the ring of the form $R_q = \mathbb{Z}_q[X]/(X^n + 1)$, where n is a power of two and q is a prime number. This type of polynomial ring arises in various mathematical and computational contexts, particularly in the realm of computer arithmetic and cryptography.

One of the key advantages of using NTT is that it significantly reduces the time complexity of polynomial multiplication from the inefficient $O(n^2)$ to a much more efficient $O(n \log n)$. This improvement in time complexity can have a substantial impact on the performance of algorithms and systems that rely on polynomial multiplication, making NTT particularly valuable in various applications.

Due to its efficiency, NTT has found widespread applications in computer arithmetic and the cryptographic domain. Its ability to speed up polynomial multiplication makes it a crucial component in many algorithms and protocols that require efficient polynomial operations.

In summary, the Number Theoretic Transform (NTT) is a powerful mathematical tool that provides an efficient way to multiply polynomials in certain rings, such as $R_q = \mathbb{Z}_q[X]/(X^n + 1)$. Its applications range from computer arithmetic to cryptographic schemes, where it helps improve performance and reduce time complexity.

Let $\mathcal{R}$ be an unit ring and let n be a positive integer. We say that an element $\omega \in \mathcal{R}$ is a principal nth root of unity if the two following assertions are verified:

$$\omega^n = 1 \tag{1}$$

$$\sum_{j=0}^{n-1} \omega^{jk} = 0 \quad for \quad 1 \leq k < n. \tag{2}$$

When the second assertion is replaced by the following assertion:

$$\omega^k \neq 1 \quad for \quad 1 \leq k < n \tag{3}$$

we say that ω is a primitive nth root of unity.

Note that, the two notion coincide when $\mathcal{R}$ is an integral domain. Indeed, if we put $\alpha = \omega^k$ for $1 \leq k < n$, then $\alpha^n = 1$ which means that $(\alpha - 1)\sum_{j=0}^{n-1} \alpha^j = 0$, and since $\alpha - 1 \neq 0$ we get $\sum_{j=0}^{n-1} \alpha^j = \sum_{j=0}^{n-1} \omega^{jk} = 0$.

The discrete Fourier transform (DFT) over $\mathcal{R}$ is the linear function, mapping the element $a = (a_0, \ldots, a_{n-1}) \in \mathcal{R}^n$ to an other element $b = (b_0, \ldots, b_{n-1}) \in \mathcal{R}^n$ such that

$$b_i = \sum_{j=0}^{n-1} a_j \omega^{ij}, \tag{4}$$

where ω is a principal nth root of unity.

We can describe this function by matrix multiplication $b = Ma$, where $M = (\omega^{jk})_{0 \leq j,k \leq n-1}$ is an $n \times n$ matrices over $\mathcal{R}$.

The ω^{-1} is also a principal nth root of unity because $\omega^{-n} = 1$ and we have

$$\sum_{j=0}^{n-1} \omega^{-jk} = \sum_{j=0}^{n-1} \omega^{nk} \omega^{-jk} = \sum_{i=0}^{n-1} \omega^{(n-j)k} = \sum_{i=0}^{n-1} \omega^{ik} = 0$$

which guarantees the assertion (2) above.

If the inverse of n exist in $\mathcal{R}$ (i.e $n^{-1} \in \mathcal{R}$), then $n^{-1}\omega^{-jk} \in \mathcal{R}$ for all $0 \leq j, k \leq n-1$, hence the inverse of M also exist and it is given as::

$$M^{-1} = n^{-1}(\omega^{-jk})_{0 \leq j,k \leq n-1}$$

and the inverse of DFT is given by the following formula:

$$c_k = n^{-1} \sum_{i=0}^{n-1} b_i \omega^{-ki} \tag{5}$$

Indeed,

$$\begin{aligned} n^{-1} \sum_{i=0}^{n-1} b_i \omega^{-ki} &= n^{-1} \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} a_j \omega^{ij}) \omega^{-ki} \\ &= n^{-1} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_j \omega^{i(j-k)} \end{aligned}$$

$$= n^{-1} \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} \omega^{i(j-k)}$$

for $j \neq k$ by (2) we get $\sum_{i=0}^{n-1} \omega^{i(j-k)} = 0$ and for $j = k$, $\sum_{i=0}^{n-1} \omega^{i(j-k)} = n$, hence

$$n^{-1} \sum_{i=0}^{n-1} b_i \omega^{-ki} = a_j.$$

If we identify the n-tuple $(a_0, \ldots, a_{n-1}) \in \mathcal{R}^n$ with the polynomial $A(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in \mathcal{R}[x]$ we write $b_j = A(\omega^j)$ and the inverse is $a_k = n^{-1} A(\omega^{-k})$.

In the following, we construct a special ring $\mathcal{R}$ where we will specializing the DFT for getting The Number Theoretic Transform.

It is well known by the Dirichlet's theorem on arithmetic progressions, that for any two positive coprime integers m and n there are infinitely many primes q of the form $m + kn$, where k is also a positive integer, especially there are infinitely many primes q of the form $kn + 1$. For a such prime q, we know that $\mathbb{F}_q = \mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ is a finite field of cardinal q, and the multiplicative group $\mathbb{Z}_q^*$ of integers modulo q is a cyclic group of order $\varphi(q) = q - 1 = kn$, where φ is the Euler's totient function, hence he must have one generator g which is a primitive $(q-1)$th root of unity modulo q.

If we put $\omega \equiv g^k \pmod{q}$, then we have

$$w^n = g^{nk} = g^{q-1} = g^{\varphi(q)} \equiv 1 \pmod{q}$$

and since $\omega^i \neq 1$ for all $1 \leq i < n$, then ω is a primitive nth root of unity that is required in computing NTT.

Now, let $f(x) \in \mathbb{Z}_q[x]$ be a nonzero polynomial of degree d, then ring $R_q = \mathbb{Z}_q[x]/f(x)$ contains exactly q^d elements.

The NTT is the DFT over the field $\mathbb{Z}_q$ using the primitive nth root of unity ω

$$\begin{array}{rccc} \text{DFT}: & \mathbb{Z}_q^n & \longmapsto & \mathbb{Z}_q^n \\ & a = (a_0, \ldots, a_{n-1}) & \longmapsto & b = (b_0, \ldots, b_{n-1}) \end{array}$$

where $b_i = \sum_{j=0}^{n-1} a_j \omega^{ij}$. The vector $a \in \mathbb{Z}_q^n$ can be viewed as an element g of R_q such that $g(x) = \sum_{i=0}^{n-1} a_i x^i$.

Evaluating the polynomial $g(x) \pmod{f(x)}$ at ω^j for $0 \leq j \leq n-1$, we get $b_j = g(\omega^j)$.

Since $gcd(n, q) = 1$, then we can compute $n^{-1} \pmod{q}$ and the inverse of DFT is given as following:

$$n^{-1} \sum_{i=0}^{n-1} b_i \omega^{-ki} \pmod{q}.$$

4 NTT Algorithm Application

We chose $n = 2^s$ for some $s \in \mathbb{N}^*$, $f(X) = X^n + 1$ and we us NTT-algorithm in the quotient rin $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.

4.1 Transforming a Polynomial from Normal Form to NTT Form

Transforming a polynomial from normal form to Number-Theoretic Transform (NTT) form involves converting its coefficients into a special representation suitable for efficient polynomial multiplication and convolution operations in the ring of integers modulo q (Rq).

The NTT form allows for faster polynomial operations, which is particularly useful in certain applications like cryptography and signal processing.

For a polynomial $f = \sum_{i=0}^{n-1} f_i X^i \in R_q$, the NTT function is defined by

$$NTT(f) = fNtt = \sum_{i=0}^{n-1} fNtt_i X^i. \tag{6}$$

$$with \quad fNtt_i = \sum_{j=0}^{n-1} \gamma^j f_j \omega^{ij} \pmod{q}. \tag{7}$$

where $\gamma = \omega^{1/2}$.

4.2 Transforming a Polynomial from NTT Form to Normal Form

The inverse of NTT function to return to normal form is computed by the below formula:

$$invNTT(fNtt) = f = \sum_{i=0}^{n-1} f_i X^i, \tag{8}$$

$$with \quad f_i = n^{-1}\gamma^{-i} \sum_{j=0}^{n-1} fNtt_j \omega^{-ij} \pmod{q}. \tag{9}$$

So the NTT algorithm can perform the multiplication of two polynomials $h = f * g \in R_q$ by:

- Transforming them to NTT form ($\hat{f}$ and $\hat{g}$);
- Computing the product in NTT form by the point-wise multiplication noted by ($\circ$), $\hat{h} = \hat{f} \circ \hat{g} \pmod{q}$ (that means $\hat{h}_i = \hat{f}_i * \hat{g}_i \pmod{q}$);
- And finally transforming the $hNTT$ polynomial from NTT form to normal form by the inverse of NTT function: $h = invNTT(\hat{h})$.

Consequently, an important reduction cost of multiplication can be achieved by pre-computing and storing the powers values related to these parameters: ω and $\gamma^2 = \omega$, in bit-reversed ordering [10].

4.3 Pre-computation

In practice, For C++ implementation of NTT algorithm, based on the Cooley-Tukey [1, 10] method, we should computing and storing the following arrays in C++ file ($precomp.h$) [6]: $Bitrev$, $GAMA$, $OMEGA$, and $invOMEGA$ in reversible order of bits, and $invGAMA$ in normal order as above:

1. $Bitrev$: Saving the values from 1 to $(n-1)$ in reversible bits;
2. $GAMMA$: saving the powers of $\gamma^{bitrev[i]}$ in reversible bits;
3. $OMEGA$: saving the powers of $\omega^{bitrev[i]}$ in-reversible bits:
4. $invOMEGA$: saving the powers of $\omega^{-bitrev[i]}$ in reversible bits:
5. $InvGAMMA$: saving the powers of $n^{-1}\gamma^{-i}$ in normal order.

The reader can see the developed functions on C++, for computing those arrays coefficients[6].

Computing Bit-Reversible Array

Before pre-computing arrays cited above, we must pre-compute also a bi-reversal array that contains the bit reversible of an integer $i \in [0, n-1]$, used by NTT algorithm. The reader can see the algorithm for computing the bit reversible of an integer[6].

Computing OMEGA Array

Defining the nth primitive root of unity ω and computing the coefficients $\omega^i * S$ and store them in the $OMEGA$ array , say: $OMEGA[i] = \omega^* S$; the algorithm is as follow:

1. $for(i = 0; i < n; i++)\{$
2. $OMEGA[i] = \omega^{birev[i]} * S \pmod q\}$.

Computing invOMEGA Array

Defining the inverse of nth primitive root of unity $\omega^{-1} = invomega$ and computing the coefficients of $invOMEGA$ array, say: $invOMEGA[i] = invomega^{birev[i]} * S$; the algorithm is as follow:

1. $for(i = 0; i < n; i++)\{$
2. $invOMEGA[i] = invomega^{birev[i]} * S \pmod q\}$.

Computing GAMMA Array

Defining the nth primitive root of unity γ and computing the coefficients of $GAMMA$ array, say: $GAMMA[i] = \gamma^{birev[i]} * S$; the algorithm is as follow:

1. $for(i = 0; i < n; i++)\{$
2. $GAMMA[i] = \gamma^{birev[i]} * S \pmod q\}$.

Computing invGAMMA Array

Defining the nth primitive root of unity $invgamma$ and computing the coefficients of $invGAMMA$ array, say: $invGAMMA[i] = invgamma^i * S$; the algorithm is as follow:

1. $for(i = 0; i < n; i++)\{$
2. $invGAMMA[i] = invgamma^i * S \pmod q\}$.

4.4 Optimised NTT Algorithm

The optimized algorithm can reduce the complexity of the multiplication on the ring R_q from $O(n^2)$ to $O(nlog(n))$.

Input:a polynomial $A \in R_q$, dimension n, and q.
$for(i = 0; i < 10; i+ = 2;)do : \quad d = (1 << i);$
$for(st = 0; start < d; st + +)do : move = 0;$
$for(j = st; j < n - 1; j+ = 2 * d)do :$
$A[j] = (A[j] + A[j + d]);$
$A[j + d] = (recomp[move + +] * (A[j] - A[j - d]))\ (\text{mod } q);$
end for;
end for;
odd level
$d <<= 1;$
$for(st = 0; st < d; st + +)do : move = 0;$
$for(j = st; j < n - 1; j+ = 2 * d)do :$
$A[j] = (A[j] + A[j + d]);$
$A[j + d] = (recomp[move + +] * (A[j] - A[j - d]))\ (\text{mod } q);$
end for;
end for;
end for.
Output: The transformed polynomial A .

Comment
This function $CoolyNTT(.)$, will be called by the $NTT(.)$ and $invNTT(.)$ functions, which we will describe respectively in the algorithms 2 and 3 below. The precomputed array $recomp$ in line 6 and 14, takes the values of $Gama$ or $invGama$ (as described before) according to our need the polynomial f in its normal form or in NTT form $\hat{f}$.

Input: a polynomial f in normal form, $OMEGA$, et $GAMMA$;
$bitrev\_vector(f);$
$for(i = 0; i < n; i + +;)do :$
$f[i] = (f[i] * OMEGA[i])\ (\text{mod } q);$
end for;
$\hat{f} \leftarrow CoolyNTT(f, GAMMA);$
Output: a polynomial in NTT form $\hat{f}$;

Comment
In line 2, the function $bitrev\_vector(f)$, computes the polynomial coefficients of f in reversible order , according to the size of the dimension n in bits; and in