كلية العلوم
Faculté des Sciences

جامعة محمد الأول بوجدة
UNIVERSITÉ MOHAMMED PREMIER OUJDA

Université Polytechnique
HAUTS-DE-FRANCE

Faculty of Sciences
Mohammed First University - Oujda
Laboratory ACSA

ICANTA'5 – 2026

5th International Congress on Algebra, Number Theory and Their Applications

Book of Abstracts

May 20 - 23, 2026

Scan to visit the official website

Royaume du Maroc
Académie Hassan II des Sciences et Techniques

Centre National pour la Recherche Scientifique et Technique

EHEI Oujda
RECONNUE PAR L'ÉTAT

Faculty of Sciences
Mohammed First University - Oujda
Laboratory ACSA

ICANTA'5 – 2026

5th International Congress on Algebra, Number Theory and Their Applications

In Honor of Professors A. AZIZI, M. C. ISMAILI, and M. ZIANE

The organizers of the 5th International Congress on Algebra, Number Theory and Their Applications (ICANTA'5) are honored to dedicate this edition to Professors A. AZIZI, M. C. ISMAILI, and M. ZIANE, in recognition of their outstanding contributions to mathematics, research, and higher education. Through their dedication to teaching, scientific excellence, and mentorship, they have inspired generations of students and researchers and have left a lasting mark on the mathematical community. We express our deepest gratitude and warmly wish them a happy and fulfilling retirement.

Introduction

The 5th International Congress on Algebra, Number Theory and Their Applications (ICANTA'5) is an international congress devoted to recent developments in algebra, number theory, cryptography, artificial intelligence, and their applications. This fifth edition is organized by the Laboratory of Arithmetic, Scientific Calculations and Applications (ACSA) at the Faculty of Sciences of Mohammed First University, in collaboration with the Laboratory Ceramaths of Polytechnic University Hauts-de-France. The congress will take place in the Faculty of Sciences, Oujda, Morocco, from May 20 to 23, 2026.

ICANTA'5 provides an international platform for researchers, academics, and young scientists from around the world to exchange ideas and present recent advances in various areas of pure and applied mathematics. The congress aims to promote scientific interaction between specialists working in algebra, arithmetic geometry, analytic and algebraic number theory, Iwasawa theory, Galois representations, coding theory, cryptography, artificial intelligence, and related areas. By bringing together senior experts and young researchers, ICANTA'5 fosters the exchange of ideas, the development of collaborations, and the presentation of recent results and open problems in number theory.

Foremost, this congress is an excellent occasion to pay a heartfelt tribute to Professors A. AZIZI, M. C. ISMAILI, and M. ZIANE. Through their inspiring research, dedication to students, and invaluable role in advancing our discipline, they have influenced generations of researchers and left a lasting mark on our faculty and the wider scientific community. This gathering offers a privileged opportunity to celebrate their remarkable careers and to extend, with deep gratitude and admiration, our warmest wishes as they embark on a well deserved retirement.

This Book of Abstracts gathers the summaries of the contributions presented during the congress. The abstracts are organized into two main sections. The first section is devoted to the keynote speakers and contains the abstracts of the plenary speakers. The second section contains the abstracts of contributed presentations, which are classified according to the main scientific themes of the congress: algebra, number theory, and cryptography-artificial intelligence. This organization reflects both the diversity of the scientific program and the interdisciplinary nature of the congress.

The Organizing Committee would like to express its sincere gratitude to all invited speakers, participants, contributors, members of the scientific committee, institutional partners, and sponsors whose support and commitment contributed to the success of this congress.

We warmly welcome all participants to Oujda and hope that ICANTA'5 will provide an inspiring scientific atmosphere, encourage fruitful collaborations, and contribute to new advances in mathematics and its applications.

The Organizing Committee
ICANTA'5 2026

Contents

Committees

General Chairs:

- Prof. B. Sodaïgui — Université Polytechnique Hauts-de-France, Valenciennes, France
- Prof. M. Taous — Faculty of Sciences (UMP), Oujda, Morocco
- Prof. A. Zekhnini — Faculty of Sciences (UMP), Oujda, Morocco

Organizing Committee:

- B. Aboun (FSO, Morocco)
- M. Benabdellah (FSJESO, Oujda)
- Z. Bouazouai (ESEFO, Morocco)
- M. Bouchlagham (FSO, Oujda)
- Z. Boughadi (ESEFO, Morocco)
- Y. Douzi (FSO, Morocco)
- M. Eddaou (FSJESO, Morocco)
- H. Elaaji (FSO, Morocco)
- I. Jerrari (FSO, Morocco)
- Z. Mellah (FSO, Morocco)
- E. Mermri (FSO, Morocco)
- H. Meziane (FSO, Morocco)
- N. Ouerdi (FSO, Morocco)
- M. Rahmani (FS, Oujda)
- N. Rahmani (FS, Oujda)
- T. Serraj (FSO, Morocco)
- N. Snanou (FSO, Morocco)
- MM. Talbi (CRMEFO, Morocco)
- M. Talbi (CRMEFO, Morocco)
- M. Ziane (FSO, Morocco)

Reading & Scientific Committee:

- J. Assim (FSM, Morocco)
- A. Azizi (FSO, Morocco)
- M. Azizi (ESTO, Morocco)
- A. Bayad (Évry, France)
- H. Ben-Azza (ENSAM, Morocco)
- M. Charkani (Fès, Morocco)
- M. P. Chaudhary (ISRWO, India)
- M. Chems-Eddin (FSDM, Morocco)
- A. Derhem (Morocco)
- Y. Douzi (FSO, Morocco)
- M. C. Ismaili (FSO, Morocco)
- I. Jerrari (FSO, Morocco)
- C. Levesque (Québec, Canada)
- T. Komatsu (Hangzhou, China)
- N. Mahdou (FSTF, Morocco)
- A. Mouhib (FPT, Morocco)
- A. Movahhedi (Limoges, France)
- A. Nitaj (Caen, France)
- N. Ouerdi (FSO, Morocco)
- T. Serraj (FSO, Morocco)
- E. Souidi (FSR, Morocco)
- MM. Talbi (CRMEFO, Morocco)
- M. Talbi (CRMEFO, Morocco)
- M. Waldschmidt (Paris, France)

Junior Organizing Committee:

- H. Al Kaddouri (FSO, Morocco)
- A. Al Urtassi (FS, Meknès)
- S. Batla (FS, Oujda)
- K. Benamer (FSO, Morocco)
- H. Boubker (FS, Oujda)
- E. Boufaraa (FS, Oujda)
- A. Ben Amar (FS, Oujda)
- S. Challi (FS, Oujda)
- A. El Attrassi (FS, Oujda)
- S. EL Halfa (FS, Oujda)
- N. E. Rahmani (FS, Oujda)
- A. Serji (FS, Oujda)
- Z. Slimani (FSO, Morocco)

Plenary Speakers

- Pr. M. Azizi, (Oujda, Morocco)
- Pr. A. Bayad, (Évry, France)
- Pr. H. Ben-Azza (Meknès, Morocco)
- Pr. Ph. Cassou-Noguès (Bordeaux, France)
- Pr. Pi. Cassou-Noguès (Bordeaux, France)
- Pr. M. P. Chaudhary (ISRWO, India)
- Pr. A. Chazad Movahhedi (Limoges, France)
- Pr. B. Deschamps (Le Mans, France)
- Pr. L. El Fadil (Fès, Morocco)
- Pr. C. Greither (Munich, Germany)
- Pr. A. Kacha (Kénitra, Morocco)
- Pr. Y. Kishi (Aichi, Japan).
- Pr. C. Levesque (Québec, Canada).
- Pr. N. Mahdou (Fès, Morocco).
- Pr. K. Mazhouda (Monastir, Tunisia).
- Pr. A. Nitaj (Caen, France)
- Pr. H. Oukhaba (Besançon, France)
- Pr. O. Ruatta (Limoges, France)
- Pr. B. Sodaïgui (Valenciennes, France)
- Pr. E. Souidi (Rabat, Morocco).
- Pr. M. Waldschmidt (Paris, France)

Lecturers Abstracts

This section contains the list of lecturers abstracts presented during the ICANTA'5 conference.

Each abstract includes the speaker's name, affiliation, and a summary of their presentation in the field of number theory and its applications.

A Zero-Trust AI-based Approach to Data security and privacy in EHR Systems

Mostafa AZIZI
Lab. MATSI, Department of Mathematics, ESTO, UMP, Oujda, Morocco
azizi.mos@ump.ac.ma

Keywords: EHR, AI Models, ZTA, Cybersecurity, AAA, Data Protection, Regulation Compliance Monitoring.

Abstract. This talk introduces a unified security framework, recommended for protecting Electronic Health Record (EHR) systems against cyberthreats and illegal access. In this context, we focus on the convergence of three critical approaches: adopting Zero Trust Architecture (ZTA), using AI, and observing regulatory compliance. The foundational principle is "Never trust, always verify", which is convenient to the healthcare fragmented ecosystem with local and remote workers, IoT devices, and third-party vendors. The proposed paradigm requires integrating AI-driven security mechanisms to dynamically enforce ZTA core principles. ML and DL models are leveraged for continuous behavioral analytics, providing real-time risk assessment by monitoring deviations from normal user/device operations to detect and automatically mitigate potential threats and credential misuse. This proactive approach supports the principle of least privilege access by dynamically adjusting permissions based, not only on the identity of the user, but also on the context of the access request. We aim to achieve immutable data security with a demonstrable compliance to the regulation in force like US HIPAA, EU GDPR, or Moroccan 09-08 Law. The system must ensure data integrity by utilizing tamper-proof audit trails (potentially leveraging blockchain or secure logging) to establish an unchangeable record of every data access, modification, and security event. This auditability is crucial for satisfying the accountability and breach notification requirements of considered regulations. Furthermore, compliance should be considered earlier with respect to the privacy-by-design approach. AI tools employed must align with the minimum necessary standard, often using techniques like federated learning or synthetic data during model training to minimize exposure of Protected Health Information (PHI). This integrated framework targets also to transform regulatory restrictions into verifiable technical controls, ensuring that EHR systems remain secure, trusted, and resilient against both external attacks and internal vulnerabilities (using Pseudonymization, Anonymization, and PRE-based delegation).

References

[1] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology (NIST). Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207

[2] Jia, Y., McDermid, J., Lawton, T., Habli, I. (2021). The role of explainability in assuring safety of machine learning in healthcare. arXiv. https://arxiv.org/abs/2109.00520

[3] Idrissi, I., Boukabous, M., Azizi, M., et al. (2021) Toward a deep learning-based intrusion detection system for IoT against botnet attacks. IAES International Journal of Artificial Intelligence v. 10, n. 1, pp. 110-120. ISSN 2252-8938. http://doi.org/10.11591/ijai.v10.i1.pp110-120.

[4] CISA (2022). Zero Trust Maturity Model. Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

[5] Al-Hammuri, K., Gebali, F., Kanan, A. (2023). ZTCloudGuard: Zero trust context-aware access management framework to avoid misuse cases in the era of generative AI and cloud-based health information ecosystem [Preprint]. arXiv. https://arxiv.org/abs/2312.02993

[6] Waheed, N., Rehman, A. U., Nehra, A., et al. (2023). FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain [Preprint]. arXiv. https://arxiv.org/pdf/2304.07668

[7] Edo, O.C., Ang, D., Billakota, P. et al. (2024). A zero trust architecture for health information systems. Health Technol. 14, 189-199. https://doi.org/10.1007/s12553-023-00809-4

[8] Zakhmi K, Ushmani A, Ranjan Mohanty M, et al. (2025) S. Evolving Zero Trust Architectures for AI-Driven Cyber Threats in Healthcare and Other High-Risk Data Environments: A Systematic Review. Cureus. 2025 Jun 5;17(6):e85446. doi: 10.7759/cureus.85446.

Eisenstein Series and Partitions functions

Abdelmejid Bayad
Université Paris-Saclay, Laboratoire de Mathématiques et Modélisation d'Évry, Évry, France
bayadabdelmejid@yahoo.fr

Abstract. In this talk, we investigate modular forms of fixed level and weight, focusing on Dedekind eta-quotients of prescribed level. Since every modular form can be decomposed into an Eisenstein series and a cusp form, a central problem is to determine this decomposition explicitly. This question has been studied in various settings, notably in the context of eta-quotients and Ramanujan-type congruences. Our approach yields modular equations and applications to partition congruences. In particular, the theory of Atkin operators provides a systematic way to derive further Ramanujan-type congruences, in the spirit of the classical work of Atkin and later developments by Author and others. This talk is based on the author's paper:

References

[1] Sofiane Abdelhamid Atmani, Abdelmejid Bayad, Daeyeoul Kim, *Eisenstein series and partition functions.* Math. Methods Appl. Sci. 48 (2025), no. 14, 13355-13367.

[2] Sofiane Atmani, Abdelmejid Bayad, Mohand Ouamar Hernane, *Congruences for Fourier coefficients of eta-quotients modulo powers of 5, 7, 11, 13, and 17,* Math. Methods Appl. Sci. 46 (2023), no. 5, 5001-5028.

Conception de Blockchaines Multidimensionnelles

Hussain Ben-azza
Ensam-Meknès, Laboratoire LIMSIS, UMI, Meknès, Maroc
h.benazza@umi.ac.ma

Résumé. D'abord, Nous rappelons les bases du protocole du Bitcoin qui consiste en une chaine linéaire de blocs [1]. Ensuite, Nous présentons D-BTC (Domino Bitcoin) comme exemple, qui aussi utilise la notion de preuve de travail. Le protocole D-BTC, pendant son évolution, contraint la blockchaine d'être une région finie simplement connexe du réseau $\mathbb{Z}^2$. Nous présentons quelques performances du protocole D-BTC : débit, résistance aux attaques, comparaisons avec d'autres blockchaines. Enfin, nous explorons des extensions possibles s'appuyant sur des notions de la théorie des groupes.
Mots-clés: Blockchaine; Domino; Hachage consistant; Frontière; Collision; Sécurité; Débit.

Références

[1] S. Nakamoto, Bitcoin : A Peer-to-Peer Electronic Cash System, 2008. [Online]. https://bitcoin.org/bitcoin.pdf

[2] M. Delorme and J. Mazoyer. Cellular Automata : A Parallel Model, Kluwer Academic Publishers, 1999.

[3] E. Grädel. Domino Games and Complexity, SIAM Journal on Computing, vol. 19, no. 5, 1990.

[4] A. Vince, An Extremal Graph Problem on a Grid and an Isoperimetric Problem for Polyominoes, *Electron. J. Combin.*, vol. 31, no. 2, 2024.

[5] P. de la Harpe. Topics in Geometric Group Theory, University of Chicago Press, 2000.

Torsors and Trace forms

Cassou-Nogues Philippe
Institute of Mathematics of Bordeaux, Bordeaux, France
Philippe.Cassou-nogues@math.u-bordeaux.fr

Abstract. Let K be a field of characteristic different from 2, let G be a finite group and L/K a G-Galois extension. We consider *trace form*. This is the G-quadratic form $q_L : L \to K$ defined by

$$q_L(x) = \mathrm{Tr}_{L/K}(x^2).$$

When the degree of L/K is odd, Bayer and Lenstra have proved that q_L is isometric to the unit form $< 1, \cdots, 1 >$. Our aim is to study what can be said of the form q_L for extensions of even degree.

One can attach to a quadratic form on a field, cohomological invariants which play an important role in the classification of such forms. Given a finite group scheme $\mathcal{G}$, and a $\mathcal{G}$-form, we show how to twist this form by a $\mathcal{G}$-torsor and give comparison formulas between the Hasse-Witt invariants of the form and its twist. As an application, we fully describe the trace form of any Galois extension of a global field, when the Galois group is 2-reduced. As a consequence, we obtain infinite families of Galois extensions L/K of even degree having a trace form q_L isomorphic to the unit form. Tannakian categories can provide interesting situations where to apply these formulas in higher dimension. This is a joint work with T. Chinburg, B. Morin and M.J Taylor.

Decorated trees and numerical semigroups

Pierrette CASSOU-NOGUES
IMB, Université de Bordeaux, France
piecassou@gmail.com

Abstract. The link between the two subjects is classical if we think about semigroups associated to singularities of algebraic plane curves and their trees. In this talk we want to enlarge the classes of objects that can be involved in the relation between the two topics.

On Contributions of Srinivasa Ramanujan : The Man Who Knew Infinity

M. P. CHAUDHARY
International Scientific Research and Welfare Organization, New Delhi, India
Mission Promote Research, Mumbai, India
Netaji Subhas University of Technology, New Delhi, India
dr.m.p.chaudhary@gmail.com

Abstract. In this talk we shall go through most wonderful contributions of Indian mathematician Srinivasa Ramanujan to the mathematical world. Also know about the rich legacy of scientific contributions by Indian Scholars towards Sciences.

Around the normal basis

Bruno DESCHAMPS
Département de Mathématiques, Université du Maine, Mans, France
Bruno.Deschamps@univ-lemans.fr

Abstract. In classical Galois theory, *the normal basis theorem* is a well-known result that plays a fundamental role in the theory. It states that *every finite Galois extension admits a normal basis*. This result is understood within the framework of commutative theory. In joint work with Victor Voisin, we have investigated the existence of normal bases in the case of Galois extensions of skew fields. In this setting, things turn out to be incredibly more complex and open onto a truly fascinating ocean of arithmetic properties. In this talk, we will present the subtleties of this problem in the noncommutative case and explore some navigable paths across this ocean.

Newton Polygon and extension of valuations

Lhoussain EL FADIL
Mathematics Department, Sciences Faculty, Sidi Mohamed Ben Abdellah University, Fez, Morocco
name@university.edu
Joint work with : S. BOUCHAIB

Keywords : Extension of Valuations ; Augmented Valuations ; High Order Newton Polygon Techniques.

Abstract. Let (K, v) be a rank one valued field and $L = K(\theta)$ a simple extension of K generated by θ, a root of a monic irreducible polynomial $F(x) \in R_v[x]$, where R_v is the valuation ring of (K, v). The goal of this paper is to describe all valuations of L extending v. So what our results generalize that given in [6, 7]. For every valuation ω of L extending v, the residue degree and ramification index are given. Some illustrating computation examples will be given too.

References

[1] R. Brown, *Roots of generalized Schönemann polynomials in Henselian extension fields*, Indian J. Pure Appl. Math. **39**(5) (2008), 403–410

[2] D. Cohen, A. Movahhedi and A. Salinier, *Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika, **47** (2000), 173–196

[3] G. Dumas, *'Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels'*, J. Math. Pures Appl. **6** (1906), 191–258.

[4] G. Eisenstein, *Über die Irreduztibilität und einige andere Eigenschaften der Gleichungen, von welcher die Theilung der ganzen Lemniscate abhängt*, J. reine angew. Math. **39** (1850), 160–179.

[5] L. El Fadil, *On the irreducible factors of a polynomial*, (arxiv preprint 2020)

[6] L. El Fadil, *On Newton polygon's techniques and factorization of polynomial over henselian valued fields*, J. of Alg. and Appl. **19**(10)(2020), doi: S0219498820501881

[7] A. Deajim, L. El Fadil, and A. Najim, *On a Dedekind Theorem and monogenity*, arxiv preprint: arxiv.org/abs/2106.06535

[8] O. Endler, *Valuation Theory*, Springer-Verlag, Berlin, 1972.

[9] A. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, Berlin, 2005.

[10] K. Hensel, *Untersuchung der Fundamentalgleichung einer Gattung reine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante*, J. Reine Angew. Math. **113**(1894), 61–83.

[11] J. Guardia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (1) (2012), 361–416.

[12] A. Jakhar, *On the factors of a polynomial*, Bull. Lond. Math. Soc. **52** (2020), 158–160

[13] A. Jakhar and S. Kotyada, *On the irreducible factors of a polynomial II*, J. of Algebra, (2020), doi: j.jalgebra.2020.02.045

[14] B. Jhorar, S. K. Khanduja, *Reformulation of Hensel's Lemma and extension of a theorem of Ore*, Manuscripta Math. **151** (2016), 223–241.

[15] M. R. Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly **109** (2002), 452–458.

[16] E. Nart, *Key polynomials over valued fields*, Publ. Mat. 64 (2020), 3–42.

[17] S. H. Weintraub, *A family of tests for irreducibility of polynomials*, Proc. Amer. Math. Soc. **144** (2016), 3331–3332.

[18] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[19] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann., 99 (1928), 84–117

Extensions Hopf-Galoisiennes de dimension infinie, et la correspondance de Hopf-Galois

Cornelius GREITHER
INF, Universität der Bundeswehr München, Germany
cornelius.greather@unibw.de

Keywords: Hopf algebras; field extensions; duality 14L15; 12F05

Résumé.

Cet exposé a pour but final de présenter quelques résultats nouveaux en théorie de Hopf-Galois, sans supposer une familiarité avec le sujet. Au début on rappelera les notions et résultats de base de la théorie de Hopf-Galois. On part d'une extension L/K de corps et une algèbre H de Hopf sur K, qui opère sur L; L et H étant de dimension finie sur K. Il y a quelques axiomes: L avec une application $\alpha : H \to \mathrm{End}_K(L)$ doit donner une structure qu'on appelle "module-algèbre sur H", et une certaine application $c_{H,L}(\alpha)$ déduite de α doit être bijective. Il existe une caractérization équivalente qui utilise une structure "comodule-algèbre" $L \to L \otimes H^*$; ici H^* dénote l'algèbre de Hopf duale à H. La "correspondance de Hopf-Galois" est une application défini sur le réseau des sous-algèbres de Hopf dans H, et ayant pour cible le réseau des extensions intermédiaires de L/K. Cette application est toujours injective, mais rarement surjective. Si H est un anneau de groupe, on retrouve toute la théorie de Galois classique, où la correspondance est toujours bijective.

Puis on regarde une généralisation où L/K peut avoir dimension quelconque. Ici H doit être muni d'une topologie, dite pro-artinienne. Si l'on adopte le point de vue dual (comodules), l'algèbre duale H^* n'a pas besoin de topologie. La situation duale permet une traduction dans un langage fort élémentaire, celui des ensembles et groupes avec une action de Γ, le groupe de Galois absolu de K. Les sous-corps L_0 qui proviennent d'une sous-algèbre de Hopf peuvent être caractérisées par la bijectivité d'une variante $c_{H_0;L_0,L}(\alpha)$ du morphisme $c_{H,L}(\alpha)$. Ce fait, qui a l'air tellement simple, a été découvert dans un travail récent de Bui, Vercruysse et Wiese. Nous présentons la traduction de ce fait sur le côté comodules (ce qui semble être nouveau, et encore plus simple), et finalement le transfert dans le langage des Γ-ensembles et Γ-groupes. Cet exposé s'appuie très fortement sur le travail qu'on vient de mentionner, et beaucoup de résultats bien connus et moins récents.

Références

[1] H.-Ph. Bui, J. Vercruysse, G. Wiese, *Correspondence theorems for infinite Hopf-Galois extensions*, Doc. Math. **31** (2026), 263-310.

On the algebraic independence of three p-adic continued fractions

Ali KACHA
(Work jointed with **Sarra Ahallal** and **Mohamed Begare**)
Mathematics department, Ibn Tofail University, Kenitra, Morocco
ali.kacha@uit.ac.ma

Keywords: p-adic continued fraction; rational approximation; algebraic independence.
MSC: 11J61; 13J70;11J81

Abstract. In this paper, we establish sufficient conditions on the elements of the p-adic continued fractions A and B which guarantee that the p-adic numbers A, B and A^B are algebraically independent over $\mathbb{Q}$. These elements have partial quotients that increase rapidly. We note that these results extend some work of Bundschuh. Furthermore, we give some numerical examples which illustrated the theoretical results.

Motivation. We improve some previous of results of algebraic independence of some p-adic continued fractions.

Main result.

Theorem 0.1. *Let $A \in (1 + p\mathbb{Z}_p), B \in (p\mathbb{Z}_p)$ and (α) be a real number > 2.*
If

$$| a_n |_p \geq | b_n |_p > | a_{n-1} |_p^{\alpha} \quad \text{for all} \quad n \geq 2,$$

then the p-adic continued fractions A, B and A^B are algebraically independent over $\mathbb{Q}$.

References

[1] Ahallal, S., Kacha A.: *Transcendental Continued Fraction*, Commun. Math. (30), no 1, 251-259, (2022).

[2] Ahallal, S., Kacha A.: *Transcendence of some p-adic continued fractions* ,Res. Number Theory, vol. 12, article 7, (2026).

[3] S. Ahallal and A. Kacha, *On algebraic independence of some continued fractions*, Bol. Soc. Paran. Mat. (3s.) v. 42, (2024), pp. 1-6.

[4] Bundschuh P.*Transcendental Continued Fractions*, J. Number Theory 18, 91-98, (1984).

[5] Durand A. *Indépendance algébrique de nombres complexes et critère de transcendance*, Composito math., no 35, 259-267, (1977).

[6] Lianxiang W.: *p-adic continued fraction* (II), Scientia Sinica Ser. A, 28, no 10, 1018-1028, (1985).

[7] Liouville J. *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnels algébriques*, C. R. Acad. Sci. Mat. Paris 18, 883-885, 910-911, (1844).

[8] Longhi, I., Murru, N., Saettone, F. M.*Heighs and transcendence of p-adic continued fractions*, (Accepted/In press) Ann. Mat. Pura Appl. https//do.org/10.1007/s10231-024-01476-6, (2025).

[9] Okano, T. *A note on the transcendental continued fractions* , Tokyo J. Math., Vol 10, no. 1, 151-156, (1987).

[10] Ooto, T. *Transcendental p-adic continued fractions*, Math. Z. 287, no. 3-4, 1053-1064, (2017).

A family of imaginary quadratic fields with class number divisible by 5

Yasuhiro KISHI
Department of Mathematics, Aichi University of Education, Aichi, Japan
ykishi@auecc.aichi-edu.ac.jp

Keywords: imaginary quadratic fields; class number; Fibonacci numbers. **MSC:** 11R29; 11R11

Abstract. The construction of explicit infinite families of imaginary quadratic fields whose class numbers are divisible by a given integer n is a classical and significant problem in algebraic number theory. For the case $n = 5$, several researchers have constructed such families by various methods. This research builds upon a recent study [1] concerning the family of imaginary quadratic fields $\mathbb{Q}(\sqrt{-D_s})$ where $5D_s = F_{10s+5}$, with F_n the n-th Fibonacci number. This is a joint work with Kwang-Seob Kim.

Motivation. While the previous study [1] established the divisibility by 5 for most cases, the specific case $s \equiv 0 \pmod{20}$ remained unresolved. This work aims to bridge this gap and provide a complete proof that covers every positive integer s without exception.

Main result. The main result of this study is the complete removal of the previously necessary restriction $s \not\equiv 0 \pmod{20}$. To state this result, we define a quintic polynomial $g_s(X)$ with integer coefficients as follows:

$$g_s(X) := X^5 - 10X^3 - 20X^2 + 5(20F_{10s+5}^2 - 3)X + 40F_{10s+5}^2(1 + (-1)^{s+1}L_{10s+5}) - 4.$$

Theorem 0.2. *For a positive integer s, the polynomial $g_s(X)$ is irreducible over $\mathbb{Q}$, and the splitting field of $g_s(X)$ is unramified cyclic quintic extension of $\mathbb{Q}(\sqrt{-D_s})$. Hence $\mathbb{Q}(\sqrt{-D_s})$ has class number divisible by 5.*

Methods / Applications. The method involves analyzing both the polynomials $g_s(X)$ themselves and their splitting fields. To ensure the irreducibility of these polynomials and to handle the case $s \equiv 0 \pmod{20}$, we utilize the arithmetic of ring class fields of specific orders. By further applying Sase's ramification criterion, an unramified cyclic quintic extension is exhibited within a dihedral extension of degree 10 over $\mathbb{Q}$. This characterization provides an interesting example of the connection between linear recurrence sequences and the structure of class groups.

References

[1] S. Jin and K.-S. Kim, *A new family of imaginary quadratic fields with class number divisible by* 5, Ramanujan J. **66** (2025), Paper No. 53.

Un plan projectif fini d'ordre n existe si et seulement si n est une puissance d'un premier

Claude Levesque
Département de Mathématiques et de Statistique, Université Laval, Québec, Canada
claude.levesque@mat.ulaval.ca

Abstract. Le but est de prouver la conjecture suivante: si un plan projectif fini d'ordre n existe, alors n est une puissance d'un nombre premier. Pour atteindre ce but, nous prouvons que la matrice canonique d'incidence d'un plan projectif fini d'ordre n contient un ensemble de $n-1$ matrices dérangements $n \times n$ qui forme avec l'identité I_n un groupe d'ordre n.

Ces $n-1$ carrés latins ont aussi une propriété dite de *digraphe*. Il semble que ceci nous permet de prouver par contradiction que n est une puissance d'un nombre premier.

Trivial ring extension of commutative rings, a survey

Najib MAHDOU
Department of Mathematics, FST University S.M. Ben Abdellah, Fez, Morocco
mahdou@hotmail.com

Keywords: Trivial ring extension, coherence, Ideal theory.

Abstract. Let A be a ring and M an A-module. The following ring construction, known as the *trivial extension* of A by M (also called the idealization of M), is denoted by $A \ltimes M$. It is the ring whose additive structure is that of the external direct sum $A \oplus M$, with multiplication defined by

$$(r_1, m_1)(r_2, m_2) := (r_1 r_2, r_1 m_2 + r_2 m_1)$$

for all $r_1, r_2 \in A$ and all $m_1, m_2 \in M$. This construction is sometimes referred to using different terminology or notations, such as the idealization $A(+)M$. While the exact origin of this construction is unclear, its first systematic study appears in Nagata's book [11]. The purpose of idealization is to embed M into a commutative ring R such that the structure of M as an A-module is preserved as an ideal of R.

The trivial ring extension is useful for:

1. Reducing results concerning submodules to the ideal case,
2. Generalizing results from rings to modules, and
3. Constructing examples of commutative rings with zero-divisors.

This Talk is a survey about the trivial ring extension of R by M.

References

[1] D. D. Anderson and M. Winders, Idealization of a module, J. Comm. Algebra, 1(1) (2009), 3–56.

[2] C. Bakkari, S. Kabbaj, and N. Mahdou, Trivial extensions defined by Prüfer conditions, J. Pure Appl. Algebra, 214(1) (2010), 53–60.

[3] F. Couchot, Gaussian trivial ring extensions and fqp-rings, Comm. Algebra, 43(7) (2015), 2863–2874.

[4] S. Glaz, Commutative Coherent Rings, Lecture Notes in Mathematics, Vol. 1371, Springer-Verlag, 1989.

[5] J. A. Huckaba, Commutative Rings with Zero Divisors, Marcel Dekker, New York, 1988.

[6] S. Kabbaj and N. Mahdou, Trivial extensions defined by coherent-like conditions, Comm. Algebra, 32(1) (2004), 3937–3953.

[7] S. Kabbaj and N. Mahdou, Trivial extensions of local rings and a conjecture of Costa, Lecture Notes in Pure and Appl. Math. Dekker, 231 (2003), 301–311.

[8] H. Kim, N. Mahdou, and E. H. Oubouhou, On the S-Krull dimension of a commutative ring, J. Algebra Appl., (2026), (20 pages).

[9] N. Mahdou, On Costa's conjecture, Comm. Algebra, 29(7) (2001), 2775–2785.

[10] N. Mahdou, Sufficient condition to resolve Costa's first conjecture, Comm. Algebra, 38(3) (2010), 1066–1074.

[11] M. Nagata, Local Rings, Wiley-Interscience, New York, 1962.

Superzeta functions and τ - li coefficients in the Selberg class

Kamel MAZHOUDA
(Joint work with K. Bllaca, J. Khmiri and B. Sodaïgui)
Université de Sousse et Université de Limoges, Tunisia
kamel.mazhouda@fsm.rnu.tn

Keywords: Li coefficients; superzeta functions **MSC:** 11M06, 11M41, 30D10, 30E05

Abstract. In this talk, we define superzeta functions of the first and second kind for the Selberg class, study their special values and relate them to the τ-Li coefficients.

References

[1] K. Bllaca, J. Khmiri, K. Mazhouda and B. Sodaïgui, *Superzeta functions and τ - li coefficients in the Selberg class*, Funct. Approx. Comment. Math. Advance Publication 1-21 (2026). DOI: 10.7169/facm/240906-20-10.

p-rationality and Leopoldt's conjecture

Abbas Chazad MOVAHHEDI
Laboratoire XLIM-Mathématiques Université de Limoges, France
abbas.movahhedi@unilim.fr

Abstract. Leopoldt's conjecture is known to be true for any number field which is abelian over the field $\mathbf{Q}$ of rational numbers or over any imaginary quadratic field. On the other hand, p-rationality allows to provide infinitely many highly nonabelain number fields satisfying Leopoldt's conjecture at the prime p. We will make some remarks concerning Leopoldt's conjecture for nonabelian number fields.

The Mathematics of Lattice Based Post-Quantum Cryptography

Abderrahmane NITAJ
Département de Mathématiques, Université de Caen, Campus II, Caen, France
abderrahmane.nitaj(at)unicaen.fr

Abstract. In 2022, the National Institute of Standards and Technology (NIST), selected four post-quantum cryptography schemes. Three of them are based on lattice theory, namely ML-KEM, based on CRYSTALS-Kyber, ML-DSA, based on CRYSTALS-Dilithium, and Falcon. Their security relies on the hardness of various problems in lattice theory such as the shortest vector problem (SVP), and the closest vector problem (CVP). This talk will present the mathematics of the three selected post-quantum schemes based on lattice hard problems.

References

[1] ML-KEM: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[2] ML-DSA: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

Autour des fonctions zeta des courbes sur les corps finis

Hassan Oukhaba
Université de Franche-Comte, laboratoire de mathématique, Besançon, France
hassan.oukhaba@umlp.fr

Résumé.

Les fonctions zêta des courbes sur les corps finis sont des fonctions rationnelles jouant presque le rôle de séries génératrices donnant le nombre de solutions dans les corps finis contenants le corps sur lequel sont définies les équations de la courbe. Je présenterai leur principales propriétés. J'exposerai aussi le cas des schémas de type fini sur un corps fini. Ces fonctions Zêta ont été étudiées par de nombreux mathématiciens dont André Weil qui a émit ses fameuses conjectures sur celles-ci. Ces conjectures ont été l'une des raisons du développement de la géométrie algébrique. Les conjectures ont depuis été démontrées principalement par Alexander Groethendick et Pierre Deligne.

Euclidian codes and their decoding

Olivier RUATTA
CANARI-INRIA Bordeaux and Institut Mathématiques de Bordeaux
XLIM-MATHIS Université de Limoges and CNRS
olivier.ruatta@unilim.fr

Abstract. In this talk, we will give an overview of a wide class of codes arising mainly from number-theoretic constructions: Euclidean codes. The first codes of this family are the Chinese remainder codes built over the ring of integers [S63]. Redundancy is created by exploiting a gap between the size of the encoded integer and the reconstruction capacity of the Chinese remainder theorem lifting. The first generalization of this construction is the polynomial Chinese remainder codes, which has been very successful because it includes Reed-Solomon codes as special cases. Later, Lenstra [L86] introduced and studied number field codes, showing their optimality. We discuss a unified setting to describe all these codes and show how to classify them according to the possibility and method of decoding. This allows us give some new constructions and deduce decoding algorithms for a special metric. In general, they are not linear codes in the classical sense, but polynomial codes (both commutative and tamely non-commutative) are linear and give rise to a unified decoding framework. We show that decoding algorithms all come from solving a rational reconstruction problem known as the "key equation".

This work is issue to several other independant works with several authors.

Partially joint works with: Philippe Gaborit, Camille Garnier, Ilaria Zappatore, Maxime Bombar, Mercedes Haiech, Kayode Epiphane Nouetowa.

References

[1] Stone, J. J., *Multiple-burst error correction with Chinese remainder theorem*, Journal of The Society for Industrial and Applied Mathematics; 1963.

[2] Lenstra H. W., *Codes from algebraic number fields*, 1986.

[3] Guruswami, V.; *Constructions of codes from number fields*, IEEE Transactions on Information Theory, 49(594603); 2003.

Steinitz classes of nonabelian Galois extensions and p-ary cyclic Hamming codes

Bouchaïb SODAÏGUI
Université Polytechnique Hauts-de-France, Ceramaths, FR CNRS 2037, F-59313 Valenciennes, France
bouchaib.sodaigui@uphf.fr

Abstract. Let k be a number field and $Cl(k)$ its class group. Let Γ be a finite group. Let $R_t(k,\Gamma)$ be the subset of $Cl(k)$ consisting of those classes which are realizable as Steinitz classes of tamely ramified Galois extensions of k with Galois group isomorphic to Γ. Let p be a prime number. Suppose that $\Gamma = V \rtimes_\rho C$, where V is an $\mathbb{F}_p$-vector space of dimension $r \geq 2$, C a cyclic group of order $(p^r-1)/(p-1)$ with $\gcd(r, p-1) = 1$, and ρ a faithful and irreducible $\mathbb{F}_p$-representation of C in V; an example of such a group is the alternating group A_4. We prove that $R_t(k,\Gamma)$ is a subgroup of $Cl(k)$ using an explicit description and properties of a p-ary cyclic Hamming code.

Post-Quantum Cryptography for IoT: Challenges and Practical Solutions

El Mamoun SOUIDI
Department of Mathematics, Sciences Faculty, Mohammed V University, Rabat, Morocco.
emsouidi@fsr.ac.ma

Abstract. The probable emergence of the quantum computer, after the development of Shor's algorithms (for integer factorization and discrete logarithms) and L. Grover (for quadratic-speed search), poses a significant threat to existing cryptographic schemes such as RSA and ECC, which underpin widely used Internet protocols including TLS, IPSec, SSH, and HTTPS.

At the same time, IoT devices are subject to severe resource constraints: (i) limited computational power; (ii) very restricted memory capacity; (iii) stringent energy limitations; and (iv) operation in bandwidth-constrained network environments.

The post-quantum cryptographic algorithms currently being standardized by the National Institute of Standards and Technology (NIST) were not originally designed to operate efficiently under such constraints. Accordingly, this talk highlights some advances in adapting, optimizing, and enabling the practical deployment of these PQC algorithms in real-world IoT settings, while preserving a strong security level against both quantum and classical adversaries.

Convexity of the fundamental domain of a binary form: the cyclotomic case

Michel WALDSCHMIDT
Mathematics Department, Institut Mathématique de Jussieu, Sorbonne University, Paris, FRANCE
name@university.edu

Abstract. Let $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$, $m \geqslant 1$, denote the sequence of binary cyclotomic forms, so that $\Phi_m(T,1) \in \mathbb{Z}[T]$, $m \geqslant 1$, is the sequence of cyclotomic polynomials. For $m \geqslant 3$, the fundamental domain

$$\{(x,y) \in \mathbb{R}^2 \ \mid \ \Phi_m(x,y) \leqslant 1\}$$

of Φ_m is a bounded subset of $\mathbb{R}^2$. In a forthcoming joint work with Étienne Fouvry we answer the question:
For which values of m is this domain convex?

Speakers and Abstracts

This section contains the list of contributed talks and abstracts presented during the ICANTA'5 conference, which are organized according to their respective fields: number theory, algebra, or cryptography.

Each abstract includes the speaker's name, affiliation, and a summary of their presentation in the field of number theory and its applications.

Number Theory Abstracts

Infinite 2-class field towers of real quadratic fields with 2-class rank 2

Brahim AABOUN
Joint work with: **Pr. Abdelkader Zekhnini**
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
aabounb@gmail.com

Keywords: Quadratic number fields; 2-class group; 2-class field tower **MSC:** 11R29; 11B32; 11B37

Abstract. Let k be a real quadratic field whose discriminant is not a sum of two integral squares. In this presentation, we provide the list of all real quadratic field with 2-class group of rank 2 and have 4-rank 1 or 2, and possible infinite 2-class field tower. Then, we study the infiniteness of these towers by applying the Golod-Shafarevich inequality.

Motivation. The problem of the infinite 2-class field tower remains an open conjecture, with only a limited number of specific cases having been resolved to date.

Main result.

Theorem 0.3. *Let k be a real quadratic field whose discriminant is not a sum of two integral squares. For all such fields where the 2-class group has rank 2 and 4-rank 1 or 2, we establish the condition for the 2-class field tower to be infinite.*

References

[1] B. Aaboun and A. Zekhnini, *O*n the Hilbert 2-class fields of some real quadratic number fields and applications, Rend. Circ. Mat. Palermo, II. Ser **73**, (2024).

[2] A. Azizi, M. Rezzougui, M. Taous et A. Zekhnini, *O*n the Hilbert 2-class field of some quadratic number fields, Int. J. Number Theory. Vol **15**, No. 04 (2019), 807-824.

[3] A. Azizi, M. Rezzougui et A. Zekhnini, *C*yclicity of the 2-class group of the first Hilbert 2-class field of some number fields, Commun. Math. **32** (1) (2024), 157-173.

[4] A. Ben Amar, B. Aaboun et A. Zekhnini, *O*n the 2-class group of the first Hilbert class field of some real quadratic number fields, Rend. Circ. Mat. Palermo, II. Ser **74**, (2025).

[5] E.S. Golod and I.R. Shafarevich, *O*n the class field tower. Izv. Akad. auk SSSR Ser. Math.**28**, 261-272 (1964) (in Russian); English translation in AMS Transl. 48.

[6] A. Mouhib, *A* positive proportion of some quadratic number fields with infinite Hilbert 2-class field tower . Ramanujan J **40** (2016), 405-412.

[7] R. Schoof, *I*nfinite class field towers of quadratic fields. J. Reine Angew. Math. **372** (1986), 209-220

The 2-Primary Part of the Class Group of Real Pure Quartic Fields

Ayoub AL UARTASSI
University Polytechnique Hauts-de-France, Valenciennes
University Moulay Ismaïl, Meknès, Maroc
ayoub.aluartassi@uphf.fr

Keywords: Class group; 2-rank of the class group; Pure quartic number fields ; Hilbert symbols ; Steinitz class.
MSC: 11R16, 11R29, 11R37, 11R33

Abstract. Let $K = \mathbb{Q}(\sqrt[4]{p_1q^2p_2^3})$ be a real pure quartic field, where p_1, p_2 and q are odd prime numbers such that $p_1 \equiv p_2 \equiv 3 \pmod 4$, $p_1p_2 \equiv 5 \pmod 8$, $\left(\frac{p_1}{p_2}\right) = 1$, and $\left(\frac{p_1p_2}{q}\right) = -1$. In this case, the 2-rank of the class group Cl_K is equal to 2. In this talk, we explicitly describe the structure of the 2-primary part of Cl_K in all cases where it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, by means of Steinitz classes of quadratic extensions of K unramified at all places. This study also paves the way for the investigation of the capitulation problem in a non-Galois number field over $\mathbb{Q}$.

References

[1] A. Al Uartassi, B. Sodaïgui, M. Taous, *Classes de Steinitz d'extensions galoisiennes non ramifiées*, Acta Arith. **219** (2025), no. 1, 53–80.

[2] A. Al Uartassi, B. Sodaïgui, M. Taous, *On the* 2*-class group of real pure quartic fields*, submitted.

[3] A. Al Uartassi, M. Taous, *The* 2*-Primary Part of the Class Group of Real Pure Quartic Fields*, to appear in Palestine J. Math.

A note on capitulation problem for some imaginary cyclic number fields

Abdelghani ASSARRAR
Department of Mathematics, Polydisciplinary Faculty of Taza, Taza, Morocco
abdelghani.assarrar@usmba.ac.ma

Keywords: class group, $\mathbb{Z}_2$-extension, capitulation problem, unit group.
MSC: 11R23;11R29;11R32;11R37

Abstract. In this paper, we give a new explicit infinite family of imaginary cyclic number fields K, such that the 2-class group of K capitulates in an unramified quadratic extention over K.

Main result.

Theorem 0.4. *Let $F = \mathbb{Q}(\sqrt{-pq_1q_2})$ be a imaginary quadratic number field where p, q_1 and q_2 are distinct odd prime numbers, such that $p \equiv 5 \pmod 8$, $q_1 \equiv q_2 \equiv -1 \pmod 8$, and $(p/q') = -1$. Put $v_2(q_1+1) = m_1+2$ and $v_2(q_2+1) = m_2+2$, for each positive integer n, introduce the field M_n the proper subextension of $F_{n+1}/\mathbb{Q}_n$ other than $\mathbb{Q}_{n+1}$ and F_n. Then for $m_1 < m_2$ and for large n, we have:*

1. $C_{2,M_n} \simeq (\mathbb{Z}/2\mathbb{Z})^{2^{m_1}+1}$
2. C_{2,M_n} *capitulates in* $M_n(\sqrt{pq_1q_2})$

References

[1] A. Azizi and A. Mouhib, *Capitulation des 2-classes d'idéaux de certains corps biquadratiques dont le corps de genres diffère du 2-corps de classe de Hilbert*, Pacific J. Math. **218** (2005), 107-121.

[2] A. Assarrar ans A. Mouhib, *On the unramified Abelian Iwasawa module of some number fields*, The Ramanujan Journal (2025) 68:17.

[3] K. Iwasawa, *A note on capitulation problem for number fields*, Proc. Japan Acad. Ser. A. Math. Sci.65, (1989), 59–61.

Transcendance et indépendance algébrique de certaines familles de nombres réels et approximations de fonctions spéciales

Mohamed BEGUARE

Université Ibn Tofail, Kénitra, Maroc
mohamed.beguare@uit.ac.ma

Mots-clés : Transcendance ; indépendance algébrique ; approximation diophantienne ; fonctions spéciales ; formes linéaires en logarithmes.
MSC : 11J81 ; 11J82 ; 11J86 ; 41A25

Abstract. Dans ce travail, nous étudions des propriétés de transcendance et d'indépendance algébrique pour certaines familles de nombres réels associées à des fonctions spéciales. Ces questions s'inscrivent dans le cadre de la théorie de la transcendance et de l'approximation diophantienne.

Nous établissons des critères de transcendance pour des valeurs particulières de fonctions spéciales à l'aide de méthodes d'approximation rationnelle et d'estimations exponentielles fines. En particulier, nous obtenons des conditions suffisantes assurant la transcendance de certaines valeurs remarquables.

Nous démontrons également des résultats d'indépendance algébrique pour des familles de nombres réels en utilisant des techniques issues de la théorie de Baker et des formes linéaires en logarithmes, ce qui permet d'exclure l'existence de relations algébriques non triviales.

À titre d'illustration, nous appliquons ces résultats à l'étude de certaines fonctions classiques telles que la fonction exponentielle et des fonctions spéciales associées, en obtenant des bornes explicites pour la qualité des approximations et leur vitesse de convergence.

Ces résultats contribuent à approfondir les liens entre transcendance, indépendance algébrique et approximation des fonctions spéciales.

References

[1] Ahallal, S., Kacha A.: *Transcendence of some p-adic continued fractions* ,Res. Number Theory, vol. 12, article 7, (2026).

[2] S. Ahallal and A. Kacha, *On algebraic independence of some continued fractions*, Bol. Soc. Paran. Mat. (3s.) v. 42, (2024), pp. 1-6.

[3] Bundschuh P.*Transcendental Continued Fractions*, J. Number Theory 18, 91-98, (1984).

[4] Durand A. *Indépendance algébrique de nombres complexes et critère de transcendance*, Composito math., no 35, 259-267, (1977).

[5] Lianxiang W.: *p-adic continued fraction* (II), Scientia Sinica Ser. A, 28, no 10, 1018-1028, (1985).

[6] Longhi, I., Murru, N., Saettone, F. M.*Heighs and transcendence of p-adic continued fractions*, (Accepted/In press) Ann. Mat. Pura Appl. https//do.org/10.1007/s10231-024-01476-6, (2025).

[7] Okano, T. *A note on the transcendental continued fractions* , Tokyo J. Math., Vol 10, no. 1, 151-156, (1987).

On the cyclotomic $\mathbb{Z}_2$-extension of some real quadratic number fields

Aziz BEN AMAR
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
benamaraziz137@gmail.com
Join work with: Abdelkader Zekhnini

Keywords: algebra; number theory; applications

Abstract. Let k be a real quadratic number field and k_∞ its cyclotomic $\mathbb{Z}_2$-extension. Denote by $A(k_n)$ the 2-class group of the n^{th} layer k_n of k_∞/k, where $k_0 = k$. In this paper, we are interested in determining all fields k such that $\text{rank}(A(k_0)) = 2$, k_1/k is ramified and $A(k_0) \simeq A(k_1)$. Under these conditions, we deduce infinite families for which the Iwasawa module $X(k_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, $m \geq 2$. In particular, the Greenberg's conjecture on the vanishing of the Iwasawa λ-invariant is satisfied for new families of infinitely many real quadratic number fields. This extends some results in the literature.

References

[1] A. Azizi, *Sur la capitulation des* 2*-classes d'idéaux de* $k = \mathbb{Q}(\sqrt{2pq}, i)$*, où* $p \equiv -q \equiv 1 \pmod 4$. Acta Arith. 94, 383-399 (2000)

[2] A. Azizi et A. Mouhib, Capitulation des 2-classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, où d est un entier naturel sans facteurs carrés, Acta Arith. 109 (2003), 27-63

[3] A. Azizi, M. Rezzougui et A. Zekhnini, On the maximal unramified pro-2-extension of certain cyclotomic $\mathbb{Z}_2$-extensions, Period. Math. Hung. 83, (2021), 54 – 66.

[4] J. Ávila, *Iwasawa module of the cyclotomic* $\mathbb{Z}_2$*-extension of certain real quadratic fields.* Ramanujan. J. 67, 6 (2025). https://doi.org/10.1007/s11139-025-01055-0.

[5] E. Benjamin and C. Snyder, Real quadratic fields with 2-class group of type (2, 2), Math. Scand. 76 (1995), 161-178.

[6] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2) **109** (1979), no. 2, 377-395.

[7] T. Fukuda, Remarks on $\mathbb{Z}_p$-extension of number fields, Proc. Japan Acad. Ser. A 70, (1994) 264-266.

[8] R. Greenberg, *On the Iwasawa invariants of totally real number fields,* Amer. J. Math. 98 (1976) 263-284.

[9] H. Laxmi, A. Saikia, $\mathbb{Z}_2$*-extension of real quadratic fields with* $\mathbb{Z}/2\mathbb{Z}$ *as*2*-class group at each layer.* Ramanujan J 64, 1285-1301 (2024). https://doi.org/10.1007/s11139-024-00869-8.

[10] Y. Mizusawa, *On the Iwasawa Invariants of* $\mathbb{Z}_2$*-Extensions of Certain Real Quadratic Fields,* Tokyo Journal of Mathematics Vol. 27 No. 1, 2004.

[11] Y. Mizusawa, *On the maximal unramified pro-*2*-extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields II,* Acta Arith. 119 (2005), 93-107.

[12] A. Mouhib, *The structure of the unramified abelian Iwasawa module of some number fields,* Pacific Journal of Mathematics, 323 (2023), 173-184.

[13] A. Mouhib and A. Movaheddi, *Cyclicity of the unramified Iwasawa module,* Manuscripta Mathematica, 135 (2011), 91-106.

[14] K. Iwasawa, On Γ-extensions of algebraic number fields. Bull. Am. Math. Soc. 65, 183-226 (1959).

[15] M. Rezzougui, *Sur les pro-*2*-extensions maximales non ramifiées sur les* $\mathbb{Z}_2$*-extensions cyclotomiques de certains corps de nombres,* Thèse. Université Mohamed I. Oujda, (2021).

Families of Sextic Number Fields with Prescribed Indices

Hamid BOUAOUINA
Université Polytechnique Hauts-de-France, Ceramaths, Valenciennes,
France
Hamid.Bouaouina@uphf.fr

Keywords: Dedekind's Theorem, Ore's Theorem, Prime ideals factorization, Newton polygon, Index of a number field, Monogenicity. **MSC:** 11R04

Abstract. For each prime number $p \in \{2, 3, 5\}$, we establish sufficient conditions for a sextic number field to have a prescribed p-adic valuation of its index, and we illustrate our results with explicit computational examples.

Motivation. We establish conditions for sextic number fields to have a prescribed p-adic valuation of their index for possible primes.

Main result.

Theorem 0.5. *Let $K = \mathbb{Q}(\alpha)$ be a sextic number field, where α is a root of the monic irreducible polynomial*

$$F(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x].$$

Suppose that for every $i = 0, \ldots, 5$, $v_2(a_i) \geq 1$. Then each of the following conditions guarantees that $v_2(i(K)) = 1$:

1. $a_3 \equiv 2 \pmod 4$, $a_2 \equiv 0 \pmod 4$, $v_2(a_0) < 2v_2(a_1) - v_2(a_2)$, $v_2(a_0) > 3v_2(a_2) - 2$, *and* $v_2(a_0) \not\equiv v_2(a_2) \pmod 2$.
2. $a_4 \equiv 2 \pmod 4$, $a_3 \equiv 0 \pmod 4$, $a_2 \equiv 4 \pmod 8$, $a_1 \equiv 0 \pmod 8$, *and* $v_2(a_0) = 2v_2(a_1) - 2$.

Methods / Applications. Newton polygon techniques applied to prime ideals factorization, which is rather technical but very efficient to apply.

References

[1] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh. Königl. Ges. Wiss. Göttingen **23** (1878), 1–23.

[2] H. T. Engstrom, *On the common index divisor of an algebraic number field*, Trans. Amer. Math. Soc. **32** (1930), 223–237.

[3] J. Guàrdia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

A family of real biquadratic fields with Euclidean ideal class

Hamza BOUBKER
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
hamza.boubker.d23@ump.ac.ma
Joint work with: Pr. Mohammed TAOUS

Keywords: algebra; number theory; applications **MSC:** 11A05, 11R29, 11R45

Abstract. In algebraic number theory, the study of Euclidean structures in number fields has been a central topic. In 1979, H. W. Lenstra introduced the notion of *Euclidean ideal classes* as a generalization of Euclidean domains to capture number fields with cyclic class groups. He proved that any number field possessing a Euclidean ideal class has a cyclic class group.

The converse problem has since been widely studied, particularly for real biquadratic fields of class number two. In this work, we investigate a new family of real biquadratic fields whose class number is a power of 2, and show that they admit a non-principal Euclidean ideal class.

Motivation. Understanding which number fields admit a Euclidean class remains a central problem related to the structure of class groups.

Main result. Let q, p_1, and p_2 be distinct prime numbers such that $p_1 \equiv p_2 \equiv -q \equiv 1 \pmod 4$ and $\left(\frac{q}{p_1}\right) \neq \left(\frac{2}{p_1}\right)$, $\left(\frac{q}{p_2}\right) \neq \left(\frac{2}{p_2}\right)$, where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

Theorem 0.6. *Let $K = \mathbb{Q}(\sqrt{2q}, \sqrt{p_1 p_2})$ be a real biquadratic field, where q, p_1, and p_2 are as above. If the class number of K is a power of 2, then K has a non-principal Euclidean ideal class.*

Methods / Applications. The proof relies on the 2-rank formula for class groups together with growth results due to Graves on Euclidean ideal classes. These results provide new examples supporting the converse of Lenstra's theorem.

References

[1] A. Azizi, and A. Mouhib. *Le 2-rang du groupe de classes de certains corps biquadratiques et applications.* International Journal of Mathematics 15.02 (2004): 169-182.

[2] J. Chattopadhyay and S. Muthukrishnan, *Biquadratic fields having a non-principal Euclidean ideal class*, J. Number Theory 204 (2019), 99-112.

[3] H. Graves, *Growth results and Euclidean ideals*. Journal of Number Theory, 2013, vol. 133, no 8, 2756-2769.

[4] H.W. Lenstra, *Euclidean ideal classes*, Astérisque 61 (1979) 121-131.

The reduced ideals of an imaginary cyclic quartic field

El Kamla BOUFARRA
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
b.80kamilia@gmail.com

Keywords: algebra; number theory; applications

Abstract. Let K be an algebraic number field of degree 4. The field K is said to be a cyclic quartic field if K can be written in the form

$$K = \mathbb{Q}\left(\sqrt{A\left(D + B\sqrt{D}\right)}\right),$$

where A, B, C, D are integers satisfying the following conditions: A is an odd squarefree integer, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$ and $gcd(A, D) = 1$. These conditions ensure that the extension is well-defined and avoids trivial or degenerate cases.

If $A > 0$, then K is a totally real cyclic quartic field, whereas if $A < 0$, then K is a totally imaginary cyclic quartic field.

In this paper, we focus on the totally imaginary case and investigate the structure of reduced ideals in such fields, providing explicit descriptions and criteria that facilitate their computation and classification.

Motivation. The study of reduced ideals in imaginary cyclic quartic fields is motivated by the desire to make the arithmetic of these fields explicit, computable, and structurally understandable, both from a theoretical and computational perspective.

References

[1] A. Azizi, J. Benamara, M. C. Ismaili and M. Talbi, *The reduced ideals of a special order in a pure cubic number field,* Archivum Mathematicum, Vol. 56 No. 3, (2020), 171-182.

[2] J. Benamara, *Idéaux Réduits d'un Corps Cubique Pur et Applications,* Thèse Soutenue le 27/07/2021.

[3] J. Payan, *Idéaux Réduits d'un Corps de nombres,* Séminaire de Grenoble, tome 1, 1971-1972.

Cyclicity of the 2-decomposed unramified Iwasawa module

Karim BOULAJHAF[1] **and Ali MOUHIB**[2]
Department of mathematics and informatics, University Mohammed Ben Abdellah Fes-Polydisciplinary Faculty of Taza, Taza, morocco
karim.boulajhaf@usmba.ac.ma

Keywords: Iwasawa theory, 2-rank, Real quadratic fields. **MSC:** 11R23; 11R37

Abstract. Let k be a real quadratic number field, and k_∞ its cyclotomic $\mathbb{Z}_2$-extension. We study the cyclicity of the Galois group X'_∞ over k_∞ of the maximal abelian unramified 2-extension, in which all 2-adic primes of k_∞ split completely. As consequence, we determinate the complete list of real quadratic number fields for which X'_∞ is cyclic.
When X'_∞ is cyclic non-trivial, we give a new infinite family of real quadratic fields, for which Greenberg's conjecture is valid.

Motivation. In this presentation, we study the cyclicity of the Galois group X'_∞ over k_∞ of the maximal abelian unramified 2-extension, in which all 2-adic primes of k_∞ split completely.

Main result. Main theorem is the following

Theorem 0.7. *Real quadratic number fields $k = \mathbb{Q}(\sqrt{m})$ for which X'_∞ is cyclic non-trivial are given by:*
(1) $\mathbb{Q}(\sqrt{\ell})$ *or* $\mathbb{Q}(\sqrt{2\ell})$ *with* $\ell \equiv 1 \pmod{16}$ *and* $\left(\frac{2}{\ell}\right)_4 = (-1)^{\frac{\ell-1}{8}} = 1$ *such that the 2-class group of* $\mathbb{Q}(\sqrt{2\ell+\sqrt{2}\ell})$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$;
(2) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv 5 \pmod 8$ *and* $\ell_2 \equiv 1 \pmod 8$ *such that* $\left(\frac{2}{\ell_2}\right)_4 \neq (-1)^{\frac{\ell_2-1}{8}}$;
(3) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv 9 \pmod{16}$ *and* $\ell_2 \equiv 1 \pmod 8$ *such that* $\left(\frac{2}{\ell_1}\right)_4 \neq (-1)^{\frac{\ell_1-1}{8}}$ *and* $\left(\frac{2}{\ell_2}\right)_4 \neq 1$;
(4) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv 1 \pmod{16}$ *and* $\ell_2 \equiv 9 \pmod{16}$ *such that* $\left(\frac{2}{\ell_1}\right)_4 \neq (-1)^{\frac{\ell_1-1}{8}}$ *and* $\left(\frac{2}{\ell_2}\right)_4 = (-1)^{\frac{\ell_2-1}{8}}$;
(5) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv \ell_2 \equiv -1 \pmod 8$, $\ell_1 \not\equiv -1 \pmod{16}$ *and* $\ell_2 \not\equiv -1 \pmod{16}$;
(6) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv -1 \pmod 8$, $\ell_2 \equiv 9 \pmod{16}$;
(7) $\mathbb{Q}(\sqrt{\ell_1\ell_2})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2})$ *with* $\ell_1 \equiv 3 \pmod 8$, $\ell_2 \equiv 1 \pmod 8$ *such that* $\left(\frac{2}{\ell_2}\right)_4 \neq 1$;
(8) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3})$ *with* $\ell_1 \equiv \ell_2 \equiv 5 \pmod 8$ *and* $\ell_3 \equiv 1 \pmod 8$ *such that* $\left(\frac{2}{\ell_3}\right)_4 \neq (-1)^{\frac{\ell_3-1}{8}}$;
(9) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3})$ *with* $\ell_1 \equiv \ell_2 \equiv 3 \pmod 8$ *and* $\ell_3 \equiv 1 \pmod 8$ *such that* $\left(\frac{2}{\ell_3}\right)_4 \neq 1$;
(10) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3})$ *with* $\ell_1 \equiv \ell_2 \equiv 3 \pmod 8$ *and* $\ell_3 \equiv 5 \pmod 8$;

(11) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3})$ *with* $\ell_1 \equiv \ell_2 \equiv 3\ (mod\ 8)$ *and* $\ell_3 \equiv -1\ (mod\ 8)$*;*
(12) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3})$ *with* $\ell_1 \equiv 3\ (mod\ 4)$ *and* $\ell_2 \equiv \ell_3 \equiv 5\ (mod\ 8)$*;*
(13) $\mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3\ell_4})$ *or* $\mathbb{Q}(\sqrt{2\ell_1\ell_2\ell_3\ell_4})$ *with* $\ell_1 \equiv \ell_2 \equiv 3\ (mod\ 8)$ *and* $\ell_3 \equiv \ell_4 \equiv 5\ (mod\ 8)$
where ℓ*,* ℓ_1*,* ℓ_2*,* ℓ_3 *and* ℓ_4 *denote distinct odd prime numbers.*

Methods / Applications. Iwasawa theory and Genus theory.

References

[1] A. Azizi and A. Mouhib, *Sur le rang du* 2*-groupe de classes de* $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ *ou* $m = 2$ *ou* $p \equiv 1(mod 4)$, Trans. Am. Math. Soc, vol. 353. (2001), 2741–2752.

[2] T. Fukuda, *Remarks on* $\mathbb{Z}_p$*-extensions of number fields*, Pro. Jpn. Acad. Ser. A, vol. 70. (1994), 264–266.

[3] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Am. J. Math, vol. 98. (1) (1976), 263–284.

On real biquadratic number fields for which the rank of the 2-Iwasawa module equals 3

Presented by: Ikrame DAQAQ
Joint Work with: M. M. Chems-Eddin
Mathematical Sciences and Applications Laboratory , Faculty of Science Dhar El Mahraz, Fez, Morocco
ikramedq@gmail.com

Keywords: Biquadratic Fields; Cyclotomic $\mathbb{Z}_2$-Extension; Iwasawa Module **MSC:** 11R18; 11R29; 11R11; 11R27

Abstract. Let k be a number field and $A(k)$ be its 2-class group. Let k_∞ be a $\mathbb{Z}_2$-extension of k, that is, an infinite extension of k such that the Galois group $\mathrm{Gal}(k_\infty/k)$ is topologically isomorphic to $\mathbb{Z}_2$, the ring of 2-adic numbers. For each $n \geq 1$, let k_n denotes the nth layer of the $\mathbb{Z}_2$-extension of k, i.e., the subfield of k_∞ of degree 2^n over k.

Let $\mathbb{Q}_{2,n}$ be the field $\mathbb{Q}\left(2\cos\left(2\pi/2^{n+2}\right)\right)$ and let $k_n = k\mathbb{Q}_{2,n}$, for all $n \geq 1$. For $k_\infty = \bigcup_{n\geq 1} k_n$, the extension k_∞/k is a $\mathbb{Z}_2$-extension of k called the cyclotomic $\mathbb{Z}_2$-extension of k. The inverse limit $A(k_\infty) = \varprojlim A(k_n)$, with respect to the norm maps, is called the 2-Iwasawa module of k_∞/k (for more details, see [5, Chapter 13]).

Recently 2-Iwasawa module of real biquadratic number fields was the subject of an extensive study in the papers [2–4], in which the authors investigated real biquadratic number fields k such that the rank of $A_\infty(k)$ is less than or equal to 2.

Our purpose in this work is to extend the earlier studies by investigating real biquadratic number fields for which the rank of the 2-Iwasawa module is equal to 3.

Acknowledgements. I would like to express my sincere gratitude to my supervisor for his continuous guidance, valuable advice, and support throughout this work.

I am also very grateful to the organizers of this conference for their efforts in creating a well-organized and enriching event, and for the opportunity to present this work.

References

[1] A. Azizi, A. Mouhib, *Le 2-rang du groupe de classes de certains corps biquadratiques et applications*, Int. J. Math., **15** (2004), 169–182.

[2] M. M. Chems-Eddin, *Conjecture and Iwasawa module of real biquadratic fields I*, J. Number Theory, **281** (2026), 224–266.

[3] M. M. Chems-Eddin, H. El Mamry, *Greenberg's conjecture and Iwasawa module of real biquadratic fields II*, arXiv:2601.07067 (2026).

[4] M. M. Chems-Eddin, H. El Mamry, *On the existence of the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension with prescribed metacyclic Galois group*, Ramanujan J., 2026 (to appear).

[5] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

On the Zeros of the Riemann Zeta Function with Two Ordinate Shifts

Ali EBADI
Department of Mathematics, University of New South Wales, Sydney , Australia
ali.ebadi@unsw.edu.au

Keywords: algebra; number theory; applications

Abstract. We prove that for any fixed real numbers $y_1, y_2 \neq 0$ and constant $C > 0$, there exists a threshold $T_* = T_*(y_1, y_2, C) > 0$ such that for all $T \geq T_*$, the interval $[T, T(1+\epsilon)]$, with $\epsilon = \exp\left(-C\sqrt{\log T}\right)$, contains at least one γ satisfying

$$\zeta\left(\frac{1}{2}+i\gamma\right) = 0, \quad \zeta\left(\frac{1}{2}+i(\gamma+y_1)\right) \neq 0, \quad \text{and} \quad \zeta\left(\frac{1}{2}+i(\gamma+y_2)\right) \neq 0.$$

This extends earlier work by Banks (for a single shift y) to two distinct shifts y_1, y_2. Our argument is based on the behavior of ζ and L functions in zero-free regions via Perron's formula.

Main result.

Theorem 0.8. *See https://arxiv.org/abs/2601.15610*

References

[1] Wintner. Aurel, *On the asymptotic distribution of the remainder term of the prime-number theorem.* American Journal of Mathematics 57, no. 3 (1935): 534-538.

[2] Ingham, A. E. *On two conjectures in the theory of numbers.* American Journal of Mathematics 64 (1942): 313-319.

[3] Odlyzko, A. M., and H. J. J. te Riele. *Disproof of the Mertens conjecture.* Journal für die reine und angewandte Mathematik 357 (1985): 138-160.

[4] Titchmarsh, E. C., and D. R. Heath-Brown. *The Theory of the Riemann Zeta-Function.* Oxford University Press, 1986.

[5] Banks, William D. *Shifting the ordinates of zeros of the Riemann zeta function.* Forum Mathematicum (to appear).

[6] Conrey, J. B., D. W. Farmer, and M. R. Zirnbauer. *Autocorrelation of ratios of L-functions.* Communications in Number Theory and Physics 2 (2008): 593-636.

[7] Conrey, J. B., and N. C. Snaith. *Applications of the L-functions ratios conjectures.*Proceedings of the London Mathematical Society (3), 94 (2007): 594-646.

[8] Gonek, S. M. *Mean values of the Riemann zeta-function and its derivatives.* Inventiones mathematicae 75 (1984): 123-141.

[9] Apostol, Tom M. *Introduction to Analytic Number Theory.* Springer Science & Business Media, 1998.

[10] Montgomery, Hugh L., and Robert C. Vaughan. *Multiplicative Number Theory I: Classical Theory.* No. 97. Cambridge University Press, 2007.

[11] Voronoï, Georges. *Sur une fonction transcendante et ses applications à la sommation de quelques séries.* In Annales scientifiques de l'École Normale Supérieure, vol. 21, pp. 207-267. 1904.

Explicit Formula for Polynomial Bessel Series

Abdellah EL ATTRASSI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
abdellah.elattrassi.24@ump.ac.ma
Joint work with **Pr: Mohammed Taous** and **Pr: Kamel Mazhouda**

Keywords: explicit formula; Bessel series; Mellin transform; Weil functional **MSC:** 11M36; 42A38

Abstract. Explicit formulas play a central role in analytic number theory by relating spectral data (zeros of L-functions) to arithmetic objects such as prime numbers. Classically, these formulas are expressed in terms of Dirichlet series and Fourier transforms. In this work, we present a generalization of Weil's explicit formula to a polynomial Bessel fundamental class of functions, following the framework introduced by Jorgenson and Lang.

The novelty of this result lies in two aspects:

- the replacement of exponential kernels by Bessel kernels,
- the extension of admissible test functions from bounded variation to φ-bounded variation.

Motivation. Explicit formulas establish a deep duality between zeros of analytic functions and arithmetic data. The aim is to extend this duality to a broader class of functions constructed via Bessel series, which naturally arise in spectral theory and geometric analysis.

Polynomial Bessel series. We consider functions of the form

$$B(s) = \sum_j P_j(s) K_{\alpha_j}\big(s, \log q_j^{1/2}\big),$$

where K_α denotes the modified Bessel function and P_j are polynomials satisfying suitable growth conditions.

Main result. Let $(B, \widetilde{B}, R)$ be a triple in the polynomial Bessel fundamental class satisfying the functional equation

$$B(s) + R(s) + \widetilde{B}(\sigma_0 - s) = 0.$$

Theorem 0.9 (Explicit formula)**.** *Let F be a test function satisfying suitable regularity, φ-variation and decay conditions. Then the following explicit formula holds:*

$$S_{B,a}(f) + S_{R,a}(f) - W_R(F) = \sum_j \sum_{k=0}^{n_j} c_{j,k} (\log q_j^{1/2})^{\alpha_j} \int_0^\infty F_{\sigma_0/2}^{(k-\alpha_j)} \left(-\log q_j^{1/2} \left(u + \frac{1}{u}\right)\right) u^{\alpha_j} \frac{du}{u}$$

$$+ \sum_j \sum_{k=0}^{\tilde{n}_j} \tilde{c}_{j,k} (\log \tilde{q}_j^{1/2})^{\tilde{\alpha}_j} \int_0^\infty F_{\sigma_0/2}^{(k-\tilde{\alpha}_j)} \left(-\log \tilde{q}_j^{1/2} \left(u + \frac{1}{u}\right)\right) u^{\tilde{\alpha}_j} \frac{du}{u}.$$

Interpretation. This formula expresses a duality between:

- spectral data (poles of B),
- arithmetic data (parameters q_j),
- and an analytic correction term (Weil functional).

It can be viewed as a generalization of the classical explicit formula, where exponential terms q^{-s} are replaced by Bessel kernels.

Special case. When $\alpha = \frac{1}{2}$, the Bessel function reduces to an exponential term, and the formula recovers the classical Dirichlet series case.

Methods. The proof relies on:

- contour integration and residue theorem,
- Mellin transform techniques,
- Fourier inversion for functions of bounded variation,
- asymptotic estimates for regularized harmonic series.

Conclusion. This work extends the scope of explicit formulas and provides a unified framework connecting Dirichlet series, Bessel series, and spectral theory.

References

[1] J. Jorgenson and S. Lang, *Basic analysis of regularized series and products*, Springer Lecture Notes, 1993.

[2] J. Jorgenson and S. Lang, *Extension of analytic number theory from Dirichlet series to Bessel series*, Math. Ann.

[3] A. Weil, *Sur les formules explicites*, 1952.

[4] M. Avdispahić and L. Smajlović, *Explicit formulas and φ-variation*, Math. Balkanica.

Complexes quadratiques dans la catégorie dérivée et cohomologie de Weil-étale

Saad EL BOUKHARI
Laboratory of Mathematics of Besançon, University Marie et Louis Pasteur, Besançon, France
saadelboukhari1234@gmail.com

Keywords: algebra; number theory; **MSC:**

Abstract. Le but de cette communication est de présenter quelques aspects de la théorie des complexes quadratiques dans la catégorie dérivée, ainsi que leur rôle dans certaines constructions cohomologiques en arithmétique. Nous aborderons en particulier le cadre de la cohomologie de Weil-étale en caractéristique positive, qui fournit une source naturelle d'exemples et d'applications.

L'exposé sera de nature essentiellement introductive et laissera une large place aux idées générales, en vue d'illustrer l'intérêt de ces méthodes dans l'étude cohomologique des corps globaux.

An upper bound for the Lang-Trotter conjecture for a pair of elliptic curves

Mohammed Amin Amri
LAGA, Département de mathématiques, Université Ibn Tofail, Kénitra, Maroc
mohammedamin.amri@uit.ac.ma

EL-Kaouni Yassin
LAGA, Département de mathématiques, Université Ibn Tofail, Kénitra, Maroc
yassine.el kaouni@ens paris saclay.fr

Keywords: Elliptic curves; Galois representations; Lang-Trotter conjectures

Abstract. Let E_1 and E_2 be non-CM elliptic curves defined over $\mathbb{Q}$, and let $t_1, t_2 \in \mathbb{Z}$ be fixed integers. In analogy to the well-know Lang-Trotter conjecture for a single elliptic curve, it is natural to investigate the asymptotic behavior of the counting function

$$\pi_{E_1,E_2;t_1,t_2}(x) = \#\{p \leq x : \ p \nmid N_1N_2, \ a_p(E_1) = t_1, \ a_p(E_2) = t_2\},$$

where $a_p(E_i)$ denotes the trace of Frobenius of E_i at p. In this talk, we give conditional upper bounds (upon GRH) for $\pi_{E_1,E_2;t_1,t_2}(x)$.

Real quadratic fields with cyclic 2-class group of the Hilbert 2-class field and $Cl_2(k) \simeq (2^m, 2^n)$ with $m, n \geq 2$

Adel EL MAHI
Joint work with: **Abdelkader Zekhnini and Brahim AABOUN**
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
mnledf@gmail.com

Keywords: Quadratic number fields; 2-class group; 2-class field tower **MSC:** 11R11; 11R29; 11R37

Abstract. Let k be a real quadratic field whose discriminant is not a sum of two integral squares, and let $Cl_2(k)$ be its 2-class group. Let $k_2^{(1)}$ (resp. $k_2^{(2)}$) denote the first (resp. second) Hilbert 2-class field of k. In this presentation, we identify all cases where the Galois group $G = \mathrm{Gal}(k_2^{(2)}/k)$ is non-metacyclic. Furthermore, we investigate the cyclicity of the derived subgroup $G' = \mathrm{Gal}(k_2^{(2)}/k_2^{(1)}) \simeq Cl_2(k_2^{(1)})$, assuming that $Cl_2(k) \simeq G/G' \simeq \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ with $m, n \geq 2$.

Motivation. The finiteness of the 2-class field tower remains an open problem.

References

[1] B. Aaboun and A. Zekhnini, *O*n the Hilbert 2-class fields of some real quadratic number fields and applications, Rend. Circ. Mat. Palermo, II. Ser **73**, (2024).

[2] A. Azizi, M. Rezzougui, M. Taous et A. Zekhnini, *O*n the Hilbert 2-class field of some quadratic number fields, Int. J. Number Theory. Vol **15**, No. 04 (2019), 807-824.

[3] A. Azizi, M. Rezzougui et A. Zekhnini, *C*yclicity of the 2-class group of the first Hilbert 2-class field of some number fields, Commun. Math. **32** (1) (2024), 157-173.

[4] A. Ben Amar, B. Aaboun et A. Zekhnini, *O*n the 2-class group of the first Hilbert class field of some real quadratic number fields, Rend. Circ. Mat. Palermo, II. Ser **74**, (2025).

[5] E. Benjamin, *S*ome real quadratic number fields with their Hilbert 2-class field having cyclic 2-class group, J. Number Theory, **173** (2017), 529-546.

[6] E. Benjamin and C. Snyder, *O*n the rank of the 2-class group of the Hilbert 2-class field of some quadratic fields, Quart. J. Math. 69 (4) (2018), 1163–1193.

[7] L. Redei, H. Reichardt, *D*ie Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. Reine Angew. Math.* **170** (1933) 69–74.

[8] A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.* **39** (1934), 95-111.

From Iwasawa Theory to Galois Realizations: Greenberg's Conjecture and the Inverse Galois Problem

Hamza EL MAMRY
University Sidi Mohamed Ben Abdellah, faculty of sciences Dher El mehraz, Department of mathematics, Fes, , Morocco
Hamza.elmamry@usmba.ac.ma

Joint Work with : Pr. Mohamed Mahmoud Chems-Eddin

Keywords: Iwasawa Theory ; greenberg's conjecture; units **MSC:** 11R23; 11R29;

Abstract. For an integer $m \geq 2$, we aim to investigate the realizability of types of metacyclic-nonmodular groups, whose abelianization is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, as the Galois group of the maximal unramified 2-extension (resp. pro-2-extension) of certain number fields of 2-power degree (resp. cyclotomic $\mathbb{Z}_2$-extensions). Furthermore, we show up some new techniques for studying Greenberg's conjecture for some number fields. In particular, the reader can find results concerning the real quadratic fields $F = \mathbb{Q}(\sqrt{\eta qrs})$, the real biquadratic fields $K = \mathbb{Q}(\sqrt{\eta q}, \sqrt{rs})$, with $\eta \in \{1, 2\}$, and the Fröhlich multiquadratic fields of the form $\mathbb{F} = \mathbb{Q}(\sqrt{q}, \sqrt{r}, \sqrt{s})$, where q, r and s are odd primes numbers.

References

[1] Chems-Eddin, M. M., El Mamry, H. : Greenberg's conjecture and Inverse Galois problem: metacyclic-nonmodular group of type 1 whose abelianization is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, $m \geq 2$, 2025 (accepter in Ramanujan Journal), .

[2] B. Aaboun and A. Zekhnini, On the metacyclic 2-groups whose abelianizations are of type $(2, 2^n)$, $n \geq 2$ and applications, Res. Number Theory 9, 55 (2023).

Total capitulation of some family of pure metacyclic fields

Fouad ELMOUHIB
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
fouad.cd@gmail.com

Keywords: pure metacyclic fields, 5-class groups, 5-groups. **MSC:** 20D15, 11R29, 11R20, 11R37.

Abstract. Let p be a prime number such that $p \equiv -1\ (mod\ 25)$ and ζ_5 be a primitive 5^{th} root of unity. Then $k = \mathbb{Q}(\sqrt[5]{p}, \zeta_5)$ is a pure metacyclic field of absolute degree 20. The purpose of this contribution is to underpin the problem of capitulation of the 5-class group $C_{k,5}$ of k whenever it is of type $(5, 5)$. More precisely we show that there is a total capitulation of $C_{k,5}$ in all unramified extensions of k.

Motivation. Solving the problem of capitulation of class group.

Main result.

Theorem 0.10. *Let p be a prime number such that $p \equiv -1\ (mod\ 25)$ and ζ_5 be a primitive 5^{th} root of unity. Then $k = \mathbb{Q}(\sqrt[5]{p}, \zeta_5)$ is a pure metacyclic field of absolute degree 20. Suppose that the 5-class group $C_{k,5}$ of k is of type $(5, 5)$, then there is a total capitulation of $C_{k,5}$ in all unramified cyclic quintic extensions of k.*

References

[1] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz*, Abh. Math. Sem. Univ. Hamburg 7 (1929), 46-51.

[2] N.Blackburn, *On prime-power groups with two generators*, Proc. Camb. Phil. Soc. 53 (1958), 327-337.

[3] N.Blackburn, *On a special class of p-groups*, Acta Math. 100 (1958), 45-92.

[4] Y. Berkovich, *Groups of prime power order*, Volume 1, de Gruyter, Expositions in Mathematics, 46, 2008.

[5] F.Elmouhib, M.Talbi, and A.Azizi, *5-rank of ambiguous class groups of quintic Kummer extensions*, Proc Math Sci 132, 12 (2022). https://doi.org/10.1007/s12044-022-00660-z

[6] *Ph. Furtwängler*: Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper., Abh Math. Sem. Univ. Hamburg 7 (1930), 14-36.

[7] *D.Hilbert*: Über die Theorie der relativ-Abelschen Zahlköper, Acta Math. 26 (1902), 99-132.

[8] M.Kulkarni, D.Majumdar, B.Sury, *l-class groups of cyclic extension of prime degree l*, J. Ramanujan Math. Soc. 30, No.4 (2015), 413-454.

[9] K. Iimura, *A criterion for the class number of a pure quintic field to be divisible by 5*, J. Reine Angew. Math. 292 (1977) 201-210,

[10] D.C.Mayer, *Transfers of metabelian p-groups*, Monatsh. Math. 166 (2012), no. 3-4, 467-495.

[11] D.C.Mayer, *The second p-class group of a number field*, Int. J. Number Theory 8 (2012), no. 2, 471-505.

[12] D.C. Mayer, *The distribution of second p-class groups on coclass graphs*, J. Théorie Nombres Bordeaux 25 (2013), no. 2, 401-456.

[13] R.J.Miech, *Metabelian p-groups of maximal class*, Trans. Amer. Math. Soc. 152 (1970), 331-373.

[14] B.Nebelung, *Klassiffication metabesher 3-gruppen mit Faktorkommutatogruppe von typ* $(3, 3)$ *und anwendung auf das Kapitulationsproblem*, Thèse de doctorat (1989), Kolon.

[15] C. Parry, *Class number relations in pure quintic fields*, Symposia Mathematica. 15 (1975), 475-485.

[16] The PARI Group, PARI/GP, Version 2.4.9, Bordeaux, 2017, http://pari.math.u-bordeaux.fr.

Three-variable functions to construct interleaved sequences over $\mathbb{F}_3$

Oumar FALL
Department of mathematics and Computer Sciences, UCAD, Dakar, Sénégal
oumar3.fall@ucad.edu.sn

Cheikh DIOP

Chérif Bachir DEME

Sémou DIOUF

Keywords: Interleaved sequence; Linear complexity; M-sequences **MSC:** 11B50; 11B85; 11Y16

Abstract. Let s be an m-sequence of period N over $\mathbb{F}_3$, and let m be an integer such that $2 \leq m \leq N-1$. We introduce the mapping

$$\begin{array}{rcl} f_m : \mathbb{Z}_N \times \mathbb{Z}_{m+1}^* \times \left(\mathbb{Z}_{m+2}^* \setminus \{1\}\right) & \longrightarrow & \mathbb{Z}_{Nm^2}, \\ (i,j,k) & \longmapsto & m^2 i + mj + k \pmod{M}. \end{array}$$

where $M = Nm^2$. This mapping provides a structured indexing scheme for constructing interleaved sequences.

Motivation. Interleaved sequences derived from m-sequences play a fundamental role in sequence design, particularly in applications to cryptography and communications. However, most existing constructions are limited to binary fields. In this paper, we provide some of the properties of the function f_m and we use it to construct an interleaved sequence of period $N * m^2$.

Main Result. Let s be an m-sequence of period N over $\mathbb{F}_3$, with $2 \leq m \leq N-1$. Define the mapping

$$f_m : \mathbb{Z}_N \times \mathbb{Z}_{m+1}^* \times \left(\mathbb{Z}_{m+2}^* \setminus \{1\}\right) \longrightarrow \mathbb{Z}_{Nm^2}, \quad (i,j,k) \mapsto mi + mj + k \pmod{M},$$

where $M = Nm^2$. This mapping is bijective and induces a well-defined interleaving structure over $\mathbb{F}_3$.

Consequently, using f_m, one can explicitly construct families of interleaved sequences of period Nm^2, thereby generalizing previous constructions over $\mathbb{F}_2$. This leads to the following theorem.

Theorem 0.11. *Let $u(s)$ be an interleaved sequence of period M over $\mathbb{F}_3$. Then*

$$u(s) = \left(u_{f_m(0,1,2)}, \ldots, u_{f_m(0,1,m+1)}, u_{f_m(0,2,2)}, \ldots, u_{f_m(0,2,m+1)}, \ldots, u_{f_m(0,m,m+1)}, \ldots, u_{f_m(N-1,m,m+1)} \right),$$

where f_m is the bijective function defined by

$$\begin{array}{rcl} f_m : \mathbb{Z}_N \times \mathbb{Z}_{m+1}^* \times (\mathbb{Z}_{m+2}^* \setminus \{1\}) & \longrightarrow & \mathbb{Z}_M, \\ (i,j,k) & \longmapsto & mi + mj + k \pmod{M}. \end{array} \tag{1}$$

Methods. Our approach combines algebraic techniques over finite fields with combinatorial analysis of index mappings.

Applications. The proposed construction provides a natural generalization of known binary constructions and may be useful in sequence design for cryptographic and communication systems.

References

[1] Cherif Bachir DEME, Mame Abdou DIAW, Oumar FALL, Oumar DIANKHA *Two-variable function to design interleaved sequences on* $\mathbb{F}_2$, Ad. Appl. Discrete Math., no. (2) **29** (2022), 187–203.

[2] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications., Cambridge Press, **20**, 1983.

On monogenity of certain pure number fields defined by $x^{2^u \cdot 3^v \cdot 7^t} - m$

Mohamed FARIS
Faculty of Sciences Dhar El Mahraz, P.O. Box 1796 Atlas-Fez, Sidi Mohamed Ben Abdellah University, Fez– Morocco
name@university.edu
Joint article with: Lhoussain El Fadil.

Keywords: Power integral basis, Theorem of Ore, prime ideal factorization, Newton polygons, index divisors. **MSC:** 11R04, 11R16, 11R21

Abstract. Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^u \cdot 3^v \cdot 7^t} - m$, with $m \neq \pm 1$ a square free rational integer, u, v and t three positive integers. In this paper, we study the monogenity of K. We prove that if $m \not\equiv 1 \mod 4$, $m \not\equiv \pm 1 \mod 9$, and $m \notin \{\pm 1, \pm 18, , \pm 19\} \mod 49$, then K is monogenic. But if $m \equiv 1 \mod 4$ or $m \equiv 1 \mod 9$ or $m \equiv -1 \mod 9$ and $u = 2$ or $m \equiv 1 \mod 49$ or $m \equiv -1 \mod 49$ and $u = 3$, then K is not monogenic.

Motivation. Monogenity of number fields is a classical problem of algebraic number theory, going back to Dedekind, Hasse, and Hensel (see for instance [5, 29]). An especially delicate and intensively studied problem, mainly by Gaál, Nakahara, Pohst, and their collaborators, is the monogenity of pure fields generated by a complex root α of an irreducible polynomial $x^n - m$ (see for instance [2, 20–22, 33]). The goal of this paper is to study the monogenity of pure number fields of degree $2^u \cdot 3^v \cdot 7^t$; generated by a complex root of an irreducible polynomial $x^{2^u \cdot 3^v \cdot 7^t} - m \in \mathbb{Z}[x]$, with $m \neq \pm 1$ a square free integer, u, v, and t three natural integers. The cases $uvt = 0$ have been studied in [3, 16, 27]. Also the case $u = 2$ and $t = v = 1$ was studied by the authors in [13].

Main result. Let K be a number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^u \cdot 3^v \cdot 7^t} - m$, with $m \neq \pm 1$ a square free rational integer, u, v, and t three positive integers.

Theorem 0.12. *The ring $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $m \not\equiv 1 \mod 4$, $m \not\equiv \pm 1 \mod 9$, and $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \mod 49$.*

Remark that based on Theorem 0.12, if $m \equiv 1 \mod 4$ or $m \equiv \pm 1 \mod 9$ or $\overline{m} \in \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \mod 49$, then $\mathbb{Z}[\alpha]$ is not integrally closed. But in this case, Theorem 0.12 cannot decide on the monogenity of K. The following theorem gives a partial answer. It gives a complete answer except for cases $\overline{m} \in \{-\overline{1}, \pm\overline{18}, \pm\overline{19}\} \mod 49$.

Theorem 0.13. *(1) If $m \equiv 1 \mod 4$, then 2 divides $i(K)$.*

(2) If $m \equiv 1 \mod 9$, then 3 divides $i(K)$.

(3) If $m \equiv -1 \mod 9$ and $u = 2$, then 3 divides $i(K)$.

(4) If $m \equiv 1 \mod 49$*, then* 7 *divides* $i(K)$.

(5) If $m \equiv -1 \mod 49$ *and* $u = 3$*, then* 7 *divides* $i(K)$.
In particular, if one of these conditions holds, then K *is not monogenic.*

Theorem 0.14. *Let* $F(x) = x^{2^u \cdot 3^v \cdot 7^t} - a^u$*, with* $a \neq \pm 1$ *a square free integer and* $u < 2^u \cdot 3^v \cdot 7^t$ *a positive integer which is coprime to* 42*. Then* $F(x)$ *is irreducible over* $\mathbb{Q}$*. Let* K *be the pure number field generated by a root* α *of* $F(x)$*. Then we have the following results:*

1. *If* $a \not\equiv 1 \mod 4$*,* $a \not\equiv \pm 1 \mod 9$*, and* $\overline{a} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \mod 49$*, then* K *is monogenic.*
2. *If one of the following conditions holds:*
   - *(a)* $a \equiv 1 \mod 4$,
   - *(b)* $a \equiv \pm 1 \mod 9$,
   - *(c)* $a \equiv -1 \mod 9$ *and* $u = 2$,
   - *(d)* $a \equiv 1 \mod 49$,
   - *(e)* $a \equiv -1 \mod 49$ *and* $u = 3$,

   then K *is not monogenic.*

Remark 0.15. *Our results generalize the results given in* [13]*, where previously we studied the monogenity of pure number fields of degree* 84*.*

Methods/Applications. Our proofs are based on Newton's polygon techniques and on the index divisors of K as introduced by Hensel as follows: The index of a field K is defined by $i(K) = gcd\{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}$. A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If $\mathbb{Z}_K$ has a power integral basis, then $i(K) = 1$. Therefore a field having a prime common index divisor is not monogenic.

References

[1] S. Ahmad, T. Nakahara, and S. M. Husnine, *Power integral bases for certain pure sextic fields*, Int. J. of Number Theory v:10, No 8 (2014) 2257–2265.

[2] S. Ahmad, T. Nakahara, and A. Hameed, *On certain pure sextic fields related to a problem of Hasse*, Int. J. Alg. and Comput. 26(3) (2016) 577–583

[3] H. Ben Yakou and L. El Fadil, *on power integral bases for certain pure number fields defined by* $x^{p^r} - m$, Int. J. Number theory, 2021, doi:10.1142/S1793042121500858

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg (1993)

[5] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen **23** (1878) 1–23

[6] L. El Fadil, *On Power integral bases for certain pure sextic fields*, Boletim da Sociedade Paranaense de Matematica **40(3s)** (2022) 1–7

[7] L. El Fadil, *On Power integral bases for certain pure sextic fields*J, J. Number Theory, 228 (2021) 375–389

[8] L. El Fadil, *On Power integral bases for certain pure number fields* , Publ. Math. Debrecen **100(1-2)** (2022) 219–231

[9] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{24} - m$, Stud. Sci. Math. Hung. **57**(3) (2020) 397–407

[10] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{18} - m$, Comm. Math. Uni. of Carolina 63(1) (2022)

[11] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{2\cdot 3^k} - m$, Acta Arithmetica **201(3)** (2021) 269–280

[12] L. El Fadil, On power integral bases of certain pure number fields defined by $x^{3^r 7^s} - m$, Colloquium Mathematicum, available online March 11, 2022, doi:10.4064/cm8574-6-2021

[13] L. El Fadil, M. Faris, On power integral bases of certain pure number fields defined by $x^{84} - m$, Revista de la Unión Matemática Argentina (2022), doi.org/10.33044/revuma.2836

[14] L. El Fadil,*On Newton polygon's techniques and factorization of polynomial over Henselian valued fields*, J. of Algebra and its Appl. (2020), doi: S0219498820501881

[15] L. El Fadil, J. Montes and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. 11(4) (2012) 1250073

[16] L. El Fadil and A. Najim, *On Power integral bases for certain pure number fields defined by* $x^{2^u \cdot 3^v} - m$ (To appear in ASM)

[17] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. **32(2)** (1930) 223–237.

[18] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26 (1984) 27–41

[19] L. El Fadil and I. Gaál, *On integral bases and monogeneity of pure octic number fields with non-square free parameters*, (To appear in Glasnik Mat.)

[20] I. Gaál, *Power integral bases in algebraic number fields*, Ann. Univ. Sci. Budapest. Sect. Comp. 18 (1999) 61–87

[21] I. Gaál, Diophantine equations and power integral bases, Theory and algorithm, Second edition, Boston, Birkhäuser, 2019

[22] I. Gaál, P. Olajos, and M. Pohst, *Power integral bases in orders of composite fields*, Exp. Math. 11(1) (2002) 87–90.

[23] I. Gaál and L. Remete, *Binomial Thue equations and power integral bases in pure quartic fields*, JP Journal of Algebra Number Theory Appl. 32(1) (2014) 49–61

[24] I. Gaál and L. Remete, *Power integral bases and monogenity of pure fields*, J. of Number Theory 173 (2017) 129–146

[25] J. Guardia, J. Montes and E. Nart,*Newton polygons of higher order in algebraic number theory*, J. trans. of ams **364**(1) (2012) 361–416

[26] A.Hameed and T.Nakahara, *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. R épub. Soc. Roum. 58(106) No. 4(2015) 419–433

[27] A. Hameed, T. Nakahara, S. M. Husnine, On existence of canonical number system in certain classes of pure algebraic number fields, J. Prime Res. Math. 7(2011) 19–24.

[28] H. Smith, The monogenity of radical extension, *Acta Arithmitica*, **198**(2021), 313–327.

[29] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math., 113:128–160, 1894. ISSN 0075-4102. doi: 10.1515/crll.1894.113.128.

[30] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra **146**(2) (1992) 318–334

[31] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[32] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Korper*, Math. Ann., 99 (1928), 84–117

[33] A. Pethö and M. Pohst, *On the indices of multiquadratic number fields*, Acta Arith. 153(4) (2012) 393–414

Stickelberger Elements via Adelic Eisenstein Classes

Alexandros GALANAKIS
Faculty of Computer Science, University of the Bundeswehr München (UniBw M), Munich, Germany
alexandros.galanakis@unibw.de

Keywords: Stickelberger elements; special values of L-functions; Eisenstein classes; totally real fields; adelic spaces.
MSC: 11R42; 11R80; 11R37

Abstract. This talk presents the main results of our joint work with M. Spiess (see [1]). Stickelberger elements attached to finite abelian extensions of totally real fields encode deep arithmetic information and are closely related to special values of abelian L-functions. While classical results establish rationality and integrality properties of these values at non-positive integers, finer divisibility phenomena remain subtle.

We develop an adelic and cohomological approach to the study of Stickelberger elements. More precisely, we construct adelic Eisenstein classes using equivariant sheaf cohomology on adelic spaces endowed with a coarse Grothendieck topology, called the lattice topology, and show that smoothed Stickelberger elements can be computed as cap products of these classes with canonical homology classes defined via global reciprocity. This framework yields refined divisibility results and explicit annihilation statements in the group ring.

Motivation. Stickelberger elements at non-positive integers are central objects in algebraic number theory, governing annihilation phenomena for class groups and encoding special values of partial zeta functions. Although their rationality and integrality properties are well understood, finer divisibility phenomena remain subtle.

Eisenstein classes provide a conceptual and functorial explanation of special value formulas, especially in equivariant cohomological settings. Our goal was to refine such equivariant constructions in an adelic framework, thereby obtaining stronger structural information about Stickelberger elements and their local behaviour.

Main result. Let F be a totally real field and K/F a finite abelian extension with Galois group G. Let S be a finite set of non-archimedean places of F containing all places ramified in K. For $\sigma \in G$, the associated partial zeta function $\zeta_S(\sigma, s)$ admits a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$. The Stickelberger element is defined by

$$\Theta_S(K/F, s) = \sum_{\sigma \in G} \zeta_S(\sigma, s)[\sigma^{-1}] \ \in \ \mathbb{C}[G].$$

By the theorem of Siegel and Klingen one has

$$\Theta_S(K/F, -k) \in \mathbb{Q}[G], \qquad \text{for } k \geq 0.$$

To obtain integrality one considers the T-smoothed Stickelberger element

$$\Theta_{S,T}(K/F, s) = \prod_{\mathfrak{q} \in T} \left(1 - \mathrm{N}(\mathfrak{q})^{1-s}[\sigma_{\mathfrak{q}}^{-1}]\right) \cdot \Theta_S(K/F, s),$$

where T is a finite set of places disjoint from S. Under mild hypotheses on T one has

$$\Theta_{S,T}(K/F,-k) \in \mathbb{Z}[G].$$

For $v \in S \cup S_\infty$ let $G_v \subseteq G$ denote the decomposition group at v and, if v is non-archimedean, let $I_v \subseteq G_v$ be the inertia subgroup with Frobenius element $\sigma_v \in G_v/I_v$. For $k \geq 0$ we define an ideal $\mathcal{I}_v^{(k)} \subseteq \mathbb{Z}[G]$ by

$$\mathcal{I}_v^{(k)} = \begin{cases} \ker\big(\mathbb{Z}[G] \to \mathbb{Z}[G/I_v]/\big([\sigma_v^{-1}] - \mathrm{N}(v)^k\big)\big), & v \nmid \infty, \\ ([\sigma_v] + (-1)^{k+1})\mathbb{Z}[G], & v \mid \infty. \end{cases}$$

Our main result (see [1, Thm. 1.1]) is:

Theorem 0.16. *Let $k \geq 0$ and fix $\mathfrak{p} \in S$. Assume T is chosen so that the natural restriction map on cyclotomic Galois cohomology is injective. Then*

$$\Theta_{S,T}(K/F,-k) \in \prod_{v \in S \cup S_\infty,\ v \neq \mathfrak{p}} \mathcal{I}_v^{(k)}.$$

Methods / Applications. The basic idea is to compute Stickelberger elements cohomologically. More precisely, we show that the smoothed Stickelberger elements arise as cap products between adelic Eisenstein classes and certain canonical homology classes defined via global reciprocity.

The adelic Eisenstein classes are constructed using equivariant sheaf cohomology on adelic spaces endowed with the lattice topology, a coarser notion of topology that allows for meaningful cohomological constructions in the adelic setting. To obtain refined divisibility results, we reinterpret the reciprocity homology class as a hyperhomology class, which permits a systematic local enrichment while preserving compatibility with the cap-product formalism.

Beyond divisibility results, this cohomological description of Stickelberger elements provides a natural framework for further arithmetic constructions. In particular, it can be applied to the construction of Gross–Stark units, as outlined in the author's thesis (see [2, Chapter 7]), revealing a conceptual bridge between adelic Eisenstein cohomology and the explicit class field theoretic constructions predicted by the Gross–Stark conjecture.

References

[1] A. Galanakis and M. Spieß, *Adelic Eisenstein classes and divisibility properties of Stickelberger elements*, arXiv:2402.11583 (2024).

[2] A. Galanakis, *Stickelberger Elements and Gross-Stark Units via Adelic Eisenstein Classes*, Ph.D. thesis, Universität Bielefeld, 2024.
Available at: https://pub.uni-bielefeld.de/record/2992977.

On the Arithmetic Statistics of Real Pure Quartic Fields by 2-Class Group Structure

Mbarek HAYNOU
Department of Mathematics, Faculty of Sciences and Technology, Errachidia, Morocco
m.haynou@edu.umi.ac.ma
Mohammed Taous
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
taousm@hotmail.com

Keywords: Class groups; pure quartic fields; 2-rank; Cohen-Lenstra heuristics; density of number fields
MSC: 11R11; 11R29; 11R45

Abstract. Let $K = \mathbb{Q}(\sqrt[4]{pd^2})$ be a real pure quartic number field and $k = \mathbb{Q}(\sqrt{p})$ its unique real quadratic subfield, where p is an odd prime and d is a squarefree positive integer, coprime to p, having exactly t distinct prime factors.

In this presentation, we study the asymptotic distribution of the 2-class group of K when ordered by the norm of the relative discriminant $N_{k/\mathbb{Q}}(\Delta_{K/k})$. We determine the natural densities of fields for which $Cl_2(K)$ is trivial or cyclic.

Motivation. The Cohen–Lenstra heuristics predict probabilistic distributions for class groups of number fields, but the presence of the "bad" prime 2 in quartic extensions introduces additional complexities that remain poorly understood. This work provides a complete probabilistic description of the 2-class group structure in a family of real pure quartic fields $K = \mathbb{Q}(\sqrt[4]{pd^2})$, offering a concrete testing ground for these heuristics.

Main result.

Theorem 0.17. *The density of fields with trivial* 2*-class group is*

$$d_{s,t,0} = \begin{cases} \dfrac{178}{220}, & \text{if } (s,t) = (0,0), \\ 0, & \text{otherwise.} \end{cases}$$

The density of fields with cyclic 2*-class group is*

$$d_{s,t,1} = \begin{cases} \dfrac{41}{220}, & \text{if } (s,t) = (0,0), \\ \dfrac{194}{220}, & \text{if } (s,t) = (1,0), \\ \dfrac{64}{220}, & \text{if } (s,t) = (0,1), \\ 0, & \text{otherwise.} \end{cases}$$

Methods / Applications. Our approach combines class field theory-specifically the classification of the ambiguous class group of K/k-with analytic number theory, including Landau's theorem on integers with a fixed number of prime factors, Naslund's theorem on integers with prescribed exponent patterns, and Dirichlet's theorem on primes in arithmetic progressions. The resulting densities are explicit rational numbers that can be approximated numerically using PARI/GP, providing independent verification of our asymptotic formulas. These results also serve as a benchmark for comparing observed distributions with the predictions of the Cohen–Martinet heuristics in the presence of the "bad" prime 2.

Acknowledgements. The authors thank the organizers of ICANTA'5 (May 20–23, 2026, Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco) for their hospitality and support.

References

[1] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, in: *Number Theory Noordwijkerhout 1983*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 33–62.

[2] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76.

[3] H. Cohen and J. Martinet, *Heuristics on class groups: some good primes are not too good*, Math. Comp. **63** (1994), 329–334.

[4] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. **26** (1984), 27–41.

[5] F. Gerth III, *Densities for certain ℓ-ranks in cyclic fields of degree ℓ^n*, Compositio Math. **60** (1986), 295–322.

[6] F. Gerth III, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. **99** (1987), 1–8.

[7] M. Haynou, B. Sodaïgui and M. Taous, *The 2-rank of real pure quartic number fields*, Rocky Mountain J. Math. **53** (2023), 27–48.

[8] M. Haynou and M. Taous, *On the density for some types of 2-class group of pure quartic number fields $K = \mathbb{Q}(\sqrt[4]{2d^2})$*, preprint.

[9] E. Landau, *Sur quelques problèmes relatifs à la distribution des nombres premiers*, Bull. Soc. Math. France **28** (1900), 25–38.

[10] E. Naslund, *Integers with a predetermined prime factorization*, arXiv:1203.2363 (2012).

[11] The PARI Group, *PARI/GP version 2.13.0*, Université de Bordeaux, 2020, http://pari.math.u-bordeaux.fr.

On a Variant of Pillai's Problem with Tribonacci Numbers and S-Units

Abdelghani LARHLID
Mohamed Ben Abdellah University, Polydisciplinary Faculty of Taza, Laboratory of Mathematics and Data Science (LMSD)
Fez, Morocco
abdelghani.larhlid@usmba.ac.ma

Keywords: Diophantine equations, Pillai's problem, Recurrence sequence. **MSC:** 11B39; 11D61; 11D45; 11Y50.

Abstract. Let $\{T_n\}_{n\geq 0}$ denote the sequence of Tribonacci numbers. In this paper, we investigate the exponential Diophantine equation

$$T_n - 5^x 7^y = c,$$

where $n, x, y \in \mathbb{Z}_{\geq 0}$ and c is an integer. This problem is related to variants of Pillai's equation and to the study of exponential Diophantine equations involving linear recurrence sequences and S-units.

We consider separately the cases $c = 0$ and $c \in \mathbb{N}$, and determine all integers c for which the above equation admits at least three solutions. Our approach relies on lower bounds for linear forms in logarithms, reduction arguments, and properties of linear recurrence sequences. The methods used in each case are substantially different.

References

[1] M. Ddamulira, F. Luca and M. Rakotomalala, On a problem of Pillai with Fibonacci numbers and powers of 2. Proc. Math. Sci., 127(3): 411–421 (2017).

[2] S. Guzmán Sánchez and F. Luca, Linear combinations of factorials and S-units in a binary recurrence sequence. Ann. Math. Québec, 38(2): 169–188 (2014).

[3] Y. Bugeaud and M. Laurent, Minoration effective de la distance p-adique entre puissances de nombres algébriques. J. Number Theory, 61(2): 311–342 (1996),

[4] N. P. Smart, The algorithmic resolution of Diophantine equations: a computational cookbook. Cambridge Univ. Press, Vol. 41 (1998),

[5] M. R. Murty and J. Esmonde, Problems in Algebraic Number Theory. Springer, Vol. 190 (2005),

[6] H. Batte and F. Luca, Solutions to a Pillai-type equation involving Tribonacci numbers and S-units. Mediterr. J. Math. **21** (2024), no. 5, 159,

[7] H. Batte, *Lucas numbers that are palindromic concatenations of two distinct repdigits*, arXiv:2401.05361 (2023).

[8] V. Ziegler, *On a variant of Pillai's problem involving S-units and Fibonacci numbers*, Bol. Soc. Mat. Mex. **28** (2022), no. 3, 57.

[9] V. Ziegler, *On a variant of Pillai's problem with binary recurrences and S-units*, Int. J. Number Theory **19** (2023), no. 7, 1473–1511.

[10] M. Ddamulira, *On a problem of Pillai with Fibonacci numbers and powers of* 3, Bol. Soc. Mat. Mex. **26** (2020), no. 2, 263–277.

A Gras-Type Approach to the Equivariant Tamagawa Number Conjecture through Rubin-Stark Units

Youness MAZIGH
Moulay Ismail University
Faculty of Sciences, Meknès
y.mazigh@umi.ac.ma

Joint work with : Jilali ASSIM & Saad EL BOUKHARI

Abstract. We formulate a Gras-type equality in arbitrary rank r, expressed in terms of Rubin–Stark units in finite abelian extensions of number fields, and show that it is equivalent to the corresponding component of the equivariant Tamagawa Number Conjecture (eTNC). In the case $r = 0$, this equality specializes to a form of the Brumer–Stark conjecture, while for $r = 1$ it yields refinements of certain index formulae involving elliptic units.

References

[1] **Buckingham P.,** *The equivalence of Rubin's conjecture and the ETNC/LRN for certain biquadratic extensions.* Glasgow Math. J., 56 : 335–353, (2014).

[2] **Burns D., Kurihara M. and Sano T.,** *On Iwasawa theory, zeta elements for* $\mathbb{G}_m$*, and the equivariant Tamagawa number conjecture*. Algebra and Number Theory, 11(7), 1527-1571, (2017).

[3] **Burns D., Daoud A., Sano T. and Seo S.,** *On Euler systems for the multiplicative group over general number fields.* Publ. Mat. 67(1): 89-126, (2023).

[4] **Burns D., Sano T., and Tsoi K-W.,** *On higher special elements of p-adic representations.* Int. Math. Res. Not. IMRN, (20): 15337–15411, (2021).

[5] **Dasgupta S., and Kakde M.,** *On the Brumer–Stark conjecture*. Ann. of Math. (2), 197(1), (2023), 289–388.

[6] **El Boukhari S., and Mazigh Y.,** *Rubin–Stark units and the class number* Res. Number Theory, 10(1) : Paper No. 14, (2024).

[7] **Johnston, H. and Nickel, A.,** *An unconditional proof of the abelian equivariant Iwasawa main conjecture and applications.* Amer. J. Math., (2025).

[8] **Ritter J. and Weiss A.,** *Toward equivariant Iwasawa theory.* II. Indag. Math. (N.S.), 15(4) : 549-572, (2004).

Multiplicités et cycles d'intersection en géométrie arithmétique

Najib OULED AZAIEZ
University of Sfax
najib.ouledazaiez@fss.usf.tn

Abstract. Soient X, Y, Z des sous-schémas projectifs sur un anneau noethérien. L'idéal diagonal décompose l'intersection de leurs cônes affines en chaînes de premiers, d'où une formule de réduction pour la multiplicité de Samuel et l'associativité du produit d'intersection. Ces constructions contrôlent diviseurs résultants et séries de torsion. Sur un anneau taillé, la hauteur du joint vérifie Bézout.

A new family of Brown-Myers type elliptic curves: Mordell-Weil rank and 2-Selmer group

[1]**Pankaj PATEL, Debopam Chakraborty**
[1]Department of Mathematics, BITS-Pilani, Hyderabad Campus, Hyderabad, INDIA
[1]p20200452@hyderabad.bits-pilani.ac.in

Keywords: Elliptic curves; Mordell–Weil rank; Selmer group

Abstract. In this talk, we introduce a parametric family of elliptic curves over $\mathbb{Q}$ of the form

$$E_m : y^2 = x^3 + (2m^2 + 2m + 2)x^2 + (m^4 + 2m^3 + 3m^2 + 2m + 1)x + m^2(m + 1)^2,$$

where we choose m from the intersecting set of all twin primes and the set of all Sophie-Germain primes, both conjecturally of infinite order.
We analyze the structure of the 2-Selmer group $\mathrm{Sel}_2(E_m)$ under suitable arithmetic conditions on m and the structure of the Shaferavich-Tate group and establish an upper bound for the Mordell–Weil rank $r(E_m)$. If $m^2 - 1$ is squarefree, our main result explicitly computes the 2-Selmer group of E_m in the terms of factors of $m^2 - 1$. Our results extend several earlier works that focused primarily on the Mordell–Weil ranks of special families of elliptic curves. In contrast, we simultaneously study both the rank and the 2-Selmer group, providing a more refined arithmetic description of this family, similar to our work for a different type of Brown-Myers curve in [9].

Motivation. The computation of Mordell–Weil ranks of elliptic curves is a central problem in number theory with deep connections to classical Diophantine equations. A notable example is the congruent number elliptic curve

$$E : y^2 = x^3 - n^2x,$$

whose rank determines whether n can be realized as the area of a rational right-angled triangle, or equivalently, whether there exists an arithmetic progression of three perfect squares with common difference n (cf. [4]).

Brown and Myers [2] studied the curve $E : y^2 = x^3 - x + m^2$ and showed that it has trivial torsion and Mordell–Weil rank at least two. Subsequent works by various authors (cf. [1, 3, 5, 6]) explored related families of elliptic curves over $\mathbb{Q}$. Moreover, Tadić investigated analogous questions over function fields in a series of papers [7, 8].

Motivated by these developments, we consider a more general family of elliptic curves

$$E : y^2 = x(x - n_1)(x - n_2) + t^2,$$

and analyze both its Mordell–Weil rank and its 2-Selmer group.

Theorem 0.18. *Let*

$$E_m : y^2 = x^3 + (2m^2 + 2m + 2)x^2 + (m^4 + 2m^3 + 3m^2 + 2m + 1)x + m^2(m + 1)^2.$$

where m is an even integer such that m is a prime and $m + 2$ is also a prime.

Then

$$E_m(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \textit{and} \quad r(E_m) \geq 1.$$

Applications. Our method provides a systematic way to construct families of elliptic curves with provably high rank.

It is widely conjectured that most elliptic curves over $\mathbb{Q}$ have Mordell–Weil rank 0 or 1, making curves of higher rank relatively rare. In this context, our results are significant: we explicitly produce an infinite family of elliptic curves with rank at least 2, and in certain cases at least 3.

This contributes to the growing body of examples of high-rank elliptic curves and highlights the interplay between Selmer groups and Mordell–Weil ranks.

References

[1] A. Antoniewicz, *On a family of elliptic curves*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego, **1285** (2005), 21–32.

[2] E. Brown and B. T. Myers, *Elliptic curves from Mordell to Diophantus and back*, Amer. Math. Monthly, **109** (2002), 639–649.

[3] K. Chakraborty and R. Sharma, *On a family of elliptic curves of rank at least* 2, Czech. Math. J., **72** (2022), 681–693.

[4] K. Conrad, *The congruent number problem*, Harvard College Math. Review, **2** (2008), 58–74.

[5] Y. Fujita and T. Nara, *The Mordell–Weil bases for the elliptic curve* $y^2 = x^3 - m^2x + n^2$, Publ. Math., **92** (2018), 79–99.

[6] A. Juyal and S. D. Kumar, *On the family* $y^2 = x^3 - m^2x + p^2$, Proc. Math. Sci., **128** (2018), 1–11.

[7] P. Tadić, *The rank of certain subfamilies of elliptic curves* $Y^2 = X^3 - X + T^2$, Ann. Math. Inform., **40** (2012), 145–153.

[8] P. Tadić, *On the family* $Y^2 = X^3 - T^2X + 1$, Glasnik Mat., **47** (2012), 81–93.

[9] P. Patel, D. Chakraborty, and J. Chattopadhyay, *On the Mordell–Weil Rank and* 2*-Selmer Group of a Family of Elliptic Curves*, Ramanujan J, **69**(2026), 46.

Capitulation des 2-classes d'idéaux de type $(2, 2^m)$ et applications

Mohammed REZZOUGUI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
morez2100@hotmail.fr

Keywords: Iwasawa theory; Galois theory; Class field theory; Class group, metacyclic p-group.
MSC: Primary 20D15; 11R23; Secondary 11R29; 11R32; 11R37.

Résumé. Dans ce papier, nous donnons une condition nécessaire et suffisante pour qu'un 2-groupe métabélien fini G dont l'abélianisé est de type $(2, 2^m)$, avec $m \geq 2$, soit métacyclique. Cette condition repose sur le rang du sous-groupe maximal de G qui contient les trois sous-groupes normaux d'indice 4 dans G. Ensuite nous appliquons ce résultat pour étudier la structure du groupe de Galois de la pro-2-extension maximale non ramifiée de la $\mathbb{Z}_2$-extension cyclotomique de certains corps de nombres.

Abstract. In this paper, we state a necessary and sufficient criteria for a finite metabelian 2-group G whose abelianized is of type $(2, 2^m)$, with $m \geq 2$, to be metacyclic. This criteria is based on the rank of the maximum subgroup of G which contains the three normal subgroups of G of index 4. Then, we apply this result to study the structure of the Galois group of the maximal unramified pro-2-extension of the cyclotomic $\mathbb{Z}_2$-extension of certain number fields.

References

[1] A. Azizi et A. Mouhib, *Sur le rang du* 2*-groupe de classes de* $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ *où* $m = 2$ *ou un premier* $p \equiv 1 \bmod 4$, Trans. Amer. Math. Soc. 353, No 7 (2001), 2741–2752.

[2] A. Azizi and A. Mouhib, *Capitulation des* 2*-classes d'idéaux de certains corps biquadratiques dont le corps de genres diffère du* 2*-corps de classes de Hilbert,* Pacific Journal of Mathematics Vol. 218, No 1 (2005), 17–36.

[3] A. Azizi, M. Rezzougui, M. Taous and A. Zekhnini, *On the Hilbert* 2*-class field of some quadratic number fields,* Int. J. Number Theory. Vol. 15, No. 04, (2019), 807–824

[4] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian* 2*-class field tower,* J. Number Theory **73** (1998), 182–194.

[5] N. Blackburn, *Generalizations of certain elementary theorems on p-groups,* Proc. London Math. Soc. (3) 11 (1961) 1–22.

[6] N. Blackburn, *On Prime Power Groups With Two Generators,* Proc. Cambridge Phil. Soc. **54** (1958), 327–337.

[7] T. Fukuda, *Remarks on* $\mathbb{Z}_p$*-extension of number fields,* Proc. Japan Acad. Ser. A **70** (1994) 264–266.

[8] T. Fukuda and K. Komatsu, *On the Iwasawa* λ*-Invariant of the cyclotomic* $\mathbb{Z}_2$*-extension of a real quadratic fields,* Tokyo J. Math. **28**, No. 1 (2005) 259–264.

[9] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l,* Ann.Inst.Fourier, Grenoble **23**, fasc. 3 (1973).

[10] R. Greenberg, *On the Iwasawa invariants of totally real number fields,* Amer. J. Math. **98** (1976) 263–284.

[11] M. Hall, *The theory of groups,* (Macmillan, New York, 1959.)

[12] F. P. Heider, B. Schmithals, *Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen,* J. reine angew. Math. **366** (1982) 1–25.

[13] G.A. Miller, H.C. Moreno, *Non-abelian groups in which every subgroup is abelian,* Trans. AMS 4 . **4** (1903) 398–404.

[14] K. Miyake, *Algebraic Investigations oh Hilbert's Theorem* 94*, the Principal Ideal theorem and Capitulation Problem*, Expos. Math. **7** (1989), 289–346.

[15] Y. Mizusawa, *On the maximal unramified pro-*2*-extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields,* J. Number Theory, **105**, (2004), 203–211.

[16] Y. Mizusawa, *On the maximal unramified pro-*2*-extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields II,* Acta Arith. **119**.1 (2005) 93–107

[17] A. Mouhib, *Sur la* 2*-extension maximale non ramifiée de la* $\mathbb{Z}_2$*-extension cyclotomique de certains corps quadratiques,* An. St. Univ. Ovidius Constanta, **22**(1), (2014), 207–214.

[18] M. Ozaki and H.Taya, *On the Iwasawa* λ_2*-invariants of certain families of real quadratic fields.* Manuscripta Math. **94** (1997), no. 4, 437–444.

[19] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper,* J. Reine Angew. Math. **171** (1935) 55–60.

[20] L. Rédei, *Das schiefe Product in der Gruppentheorie,* Comment. Math. Helv. **20** (1947) 225–267.

Ciclicity of the Iwasawa module of certain biquadratic number fields

Abdellah SBAI
joint work with: **Idriss Jerrari**
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
abdellah.sbai@ump.ac.ma

Keywords: algebra; number theory; applications

Abstract.

We characterize all fields of the form $\mathbb{K} := \mathbb{Q}(\sqrt{pr}, \sqrt{pq})$ and $\mathbb{L} := \mathbb{Q}(\sqrt{pr}, \sqrt{pq}, \sqrt{2})$ whose 2-class groups are cyclic, where $p \equiv 5 \pmod 8$, $q \equiv 3 \pmod 4$ and $r \equiv 3 \pmod 8$ are pairwise different primes. This characterization answers a fundamental question in class field theory, by providing a precise understanding of class group structures in real multiquadratic extensions. Furthermore, as an application we study the structure of Iwasawa module of $\mathbb{K}$ in order to examine the validity of Greenberg's conjecture.

References

[1] Mouhib, A. Movahhedi, A.: Cyclicity of the unramified Iwasawa module. Manuscripta Math. **135**, 91—106 (2011)

[2] Sbai, A., Jerrari, I., Azizi, A.: On units of real triquadratic fields and the second 2-class group of certain cyclotomic $\mathbb{Z}_2$-extensions. Ramanujan J. **67**, 25 (2025). https://doi.org/10.1007/s11139-025-01065-y

[3] Sbai, A., Jerrari, I., Azizi, A.: Unit group of some triquadratic number fields and Greenberg's conjecture. Rend. Circ. Mat. Palermo, II. Ser **74**, 115 (2025). https://doi.org/10.1007/s12215-025-01224-6

Algebraic Points on the Mulholland-Siksek Curve

El Hadji SOW
Département de Mathématiques, Faculté des Sciences et Techniques, Université de Labé, Labé, République de Guinée
elhadji.sow@univ-labe.edu.gn

Keywords: Plane curves; Degree of algebraic point; Rational point; Jacobian
MSC: 14H50; 14H40; 11D68; 12F05

Abstract. In this paper, we determine the set of algebraic points of degree at most 4 over $\mathbb{Q}$ on the hyperelliptic curve

$$X_{a,b} : w^2 = a(v^5 - b^5),$$

for $(a, b) \in \{(3, 1), (1, 3)\}$.
his extends prior works of Mulholland and Siksek, who described the set of $\mathbb{Q}$-rational on these curves in [5] and [6], respectively.

Motivation. This paper extends these results by characterizing all algebraic points of degree at most 4 over $\mathbb{Q}$.

Main result. Our main theorem provides a complete classification:

Theorem 0.19. *The set of algebraic points of degree at most* 4 *over* $\mathbb{Q}$ *on* $X_{a,b}$ *is given by:*

1. *The set of quadratic points on* $X_{a,b}$ *is given by*

$$\mathcal{S} = \left\{(\alpha, \pm\sqrt{a(\alpha^5 - b^5)}),\ \alpha \in \mathbb{Q}\right\}.$$

2. *The set of cubic points on* $X_{a,b}$ *is empty.*

3. *The set of quartic points on* $X_{a,b}$ *is given by* $C_1 \cup C_2$*, where*

$$C_1 = \left\{\left(v, \pm\sqrt{a(v^5 - b^5)}\right) \mid v \in \mathbb{Q},\ [\mathbb{Q}(v) : \mathbb{Q}] = 2\right\},$$

$$C_2 = \left\{ \begin{array}{l} (v, (v-b)\,[\lambda_1 + \lambda_2(v+b)]) \mid \lambda_1, \lambda_2 \in \mathbb{Q} \text{ and } v \text{ root of} \\ A(v) = av^4 + Av^3 + Bv^2 + Cv + D \end{array} \right\}.$$

Methods / Applications. To address this challenge, we employ fundamental tools from algebraic geometry:

- *Linear systems of divisors*: These provide the geometric framework for analyzing functions on the curve. A divisor is a formal sum of points, and its associated linear system consists of all linearly equivalent divisors. The dimension of Riemann-Roch spaces $\mathcal{L}(D)$ constrains possible coordinates of algebraic points.

- *Abel-Jacobi theorem*: This establishes a profound connection between the curve and its Jacobian variety, mapping degree-zero divisors to points on the Jacobian. For a genus g curve, the Jacobian $J(C)$ is a g-dimensional abelian variety.

- *Mordell-Weil group*: The group $J(C)(\mathbb{Q})$ of rational points on the Jacobian is finitely generated by the Mordell-Weil theorem:

$$J(C)(\mathbb{Q}) \simeq J(C)(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

  where the torsion subgroup is finite and r denotes the rank. This structure is crucial for lifting algebraic points to Jacobian points over appropriate number fields.

References

[1] The LMFDB Collaboration, The L-functions and Modular Forms Database. $https://www.lmfdb.org/Genus2Curve/Q/$ [Online; accessed 8 November 2021].

[2] E. L. Garcia, Diophantine Geometry, Course notes from the CIMPA school "Functional Equations: Theory, Practice and Interactions" held in Hanoi from 12-23 April 2021.

[3] P. A. Griffiths, Introduction to algebraic curves , Translations of mathematical monographs volume 76. American Mathematical Society, Providence (1989).

[4] M. Hindry, J. H. Silverman, Diophantine Geometry, An Introduction, Graduate Texts in Mathematics, January 1, 2000.

[5] J. TH. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantineequations. ProQuest LLC. Ann Arbor, MI; 2006.

[6] S. Siksek, Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, 2013, No. 4, page 765.

[7] G. H. Hardy, *On some expressions connected with the distribution of primes*, Proc. London Math. Soc. (2) **15** (1916), 107–121.

[8] K. Rosen, *Elementary Number Theory and Its Applications*, 5th ed., Addison Wesley, 2002.

On the capitulation of the 2-ideal classes of the field $\mathbb{K} = \mathbb{Q}(\sqrt{pq_1q_2\varepsilon_0\sqrt{\ell}})$

Mohammed TAMIMI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
med.tamimi@gmail.com

A. ZEKHNINI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
zekha1@yahoo.fr

A. AZIZI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
abdelmalekazizi@yahoo.fr

Keywords: Capitulation; 2-class group; Hilbert 2-class field; Genus field. **MSC:** 11R16; 11R29; 11R11.

Abstract. Let $\mathbb{K} = \mathbb{Q}(\sqrt{pq_1q_2\varepsilon_0\sqrt{\ell}})$ be a real cyclic quartic number field, where $\ell = 2$ or $\ell \equiv 1 \pmod 4$ is a prime, $p \equiv -q_1 \equiv -q_2 \equiv 1 \pmod 4$ are primes, and ε_0 is the fundamental unit of its quadratic subfield $k = \mathbb{Q}(\sqrt{\ell})$.

The capitulation problem studies how ideal classes become principal in field extensions, revealing key information on class groups. In this work, we examine the capitulation of the 2-class group of $\mathbb{K}$, when it is of type $(2, 2)$, in the quadratic subfields of its first Hilbert 2-class field. We determine the genus field of $\mathbb{K}$ and study the class numbers of unramified extensions.

As a main result, the Galois group of the second Hilbert 2-class field $\mathbb{K}_2^{(2)}$ is described, with cases where it is dihedral, semi-dihedral, quaternionic, or abelian of order 8. These findings provide partial resolutions of the capitulation problem and insights for further research in algebraic number theory.

Motivation. The capitulation problem is a central and challenging topic in algebraic number theory. It studies how ideal classes become principal under field extensions, providing key insights into the structure of class groups.

Main result. We investigate the capitulation of the 2-class group of $\mathbb{K}$, when it is of type $(2, 2)$, in the quadratic subfields of the first Hilbert 2-class field. We determine the genus field of $\mathbb{K}$ and study the class numbers of its unramified extensions within the Hilbert class field. In particular, we describe the structure of the Galois group of the second Hilbert 2-class field $\mathbb{K}_2^{(2)}$, identifying cases where it is dihedral, semi-dihedral, quaternionic, or abelian of order 8. As result we have the theorem

Theorem 0.20. *Let $\mathbb{K}_2^{(2)}$ denote the second Hilbert 2-class field of $\mathbb{K}$, i.e., the Hilbert 2-class field of the first Hilbert 2-class field $\mathbb{K}_2^{(1)}$. Then the Galois group $\mathrm{Gal}(\mathbb{K}_2^{(2)}/\mathbb{K})$ is:*

1. *dihedral, semi-dihedral, or quaternion of order 2^m, with $m > 3$, if*

- $\left(\frac{\ell}{q_3}\right) = \left(\frac{q_1}{q_3}\right) = 1$,
- *or* $\left(\frac{\ell}{q_3}\right) = -\left(\frac{q_1}{q_2q_3}\right) = -1$;

2. *abelian or quaternion of order* 8 *if*

- $\left(\frac{\ell}{q_3}\right) = -\left(\frac{q_1}{q_3}\right) = 1$,
- *or* $\left(\frac{\ell}{q_3}\right) = \left(\frac{q_1}{q_2q_3}\right) = -1$.

Methods / Applications. This work contributes to the understanding of the capitulation phenomenon by examining specific cases and applying relevant theoretical tools. Even a partial study provides useful insights and may guide further research in this area.

Acknowledgements. I express my sincere gratitude to my thesis supervisor, Mr. A. ZEKHNINI, for his guidance, support, and encouragement. I also thank Mr. A. AZIZI for proposing this thesis topic and for his continuous advice and support.

References

[1] A. Azizi, M. Tamimi, and A. Zekhnini, *The* 2*-rank of the class group of some real cyclic quartic number fields,* Proc. Math. Sci. 131(7), (2021).

[2] A. Azizi, M. Tamimi, and A. Zekhnini, *The* 2*-rank of the class group of some real cyclic quartic number fields* II, Turk. J. Math. 45(3), (2021), 1241-1269.

[3] A. Azizi, M. Tamimi and A. Zekhnini, *On the* 2*-class number of some real cyclic quartic number fields I*, Bol. Soc. Mat. Mex. 30, 19 (2024). https://doi.org/10.1007/s405900-23-00589-x.

[4] A. Azizi, M. Tamimi and A. Zekhnini, *On the 2-class number of some real cyclic quartic number fields II,* in New frontiers in number theory and applications, Trends in mathematics Series 2024.

[5] M. Ishida, *The genus fields of algebraic number fields,* Lecture notes in mathematics 555, Springer-Verlag (1976).

[6] H. Kisilevsky, *Number fields with class number congruent to* 4 *mod* 8 *and Hilbert's theorem* 94*,* J. Number. Theor. **8** (1976), 271-279.

[7] P. Kaplan, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques,* J. Reine angew. Math. **283/284 (1976)**, 313-363.

[8] F. Lemmermeyer, *Kuroda's class number formula,* Acta Arith. **66** (3) **(1994)**, 245-260.

A Family of MDS Codes from Galois Number Fields with Complete Splitting Primes

Youssef ZAIM
Sidi Mohammed Ben Abdellah University, ENS, Fez,Morocco
youssef.zaim@usmba.ac.ma
Joint work with : Khalid ABDELMOUMEN
Sidi Mohammed Ben Abdellah University, ENS, Fez, Morocco
khalid.abdelmoumen@usmba.ac.ma

Keywords: Algebraic codes, algebraic number fields, asymptotically good codes, Chinese Remainder codes, class field tower.

Abstract. In this paper, we present a new construction of generalized CRT error-correcting codes based on a Galois number field K, with an alphabet set of size p, a rational prime splitting completely in K. These codes resemble generalized Reed–Solomon codes over function fields. A key feature is the ease of controlling their parameters, allowing us to estimate the minimum distance prior to construction. Furthermore, under certain conditions, this construction yields Maximum Distance Separable (MDS) codes. We illustrate the construction with an explicit example using the cyclotomic field $\mathbb{Q}(\zeta_{11})$. We also provide a sufficient condition for the existence of asymptotically good codes from an infinite tower of Hilbert class fields, along with an explicit example over an imaginary quadratic number field with small root discriminant.

References

[1] P. Samuel, *Theorie algebrique des nombres*, Hermann 1971

[2] L. C. Washington, *Introduction to Cyclotomic Fields*, Second Edition, Graduate Texts in Mathematics, Springer, 1997.

[3] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, (2004).

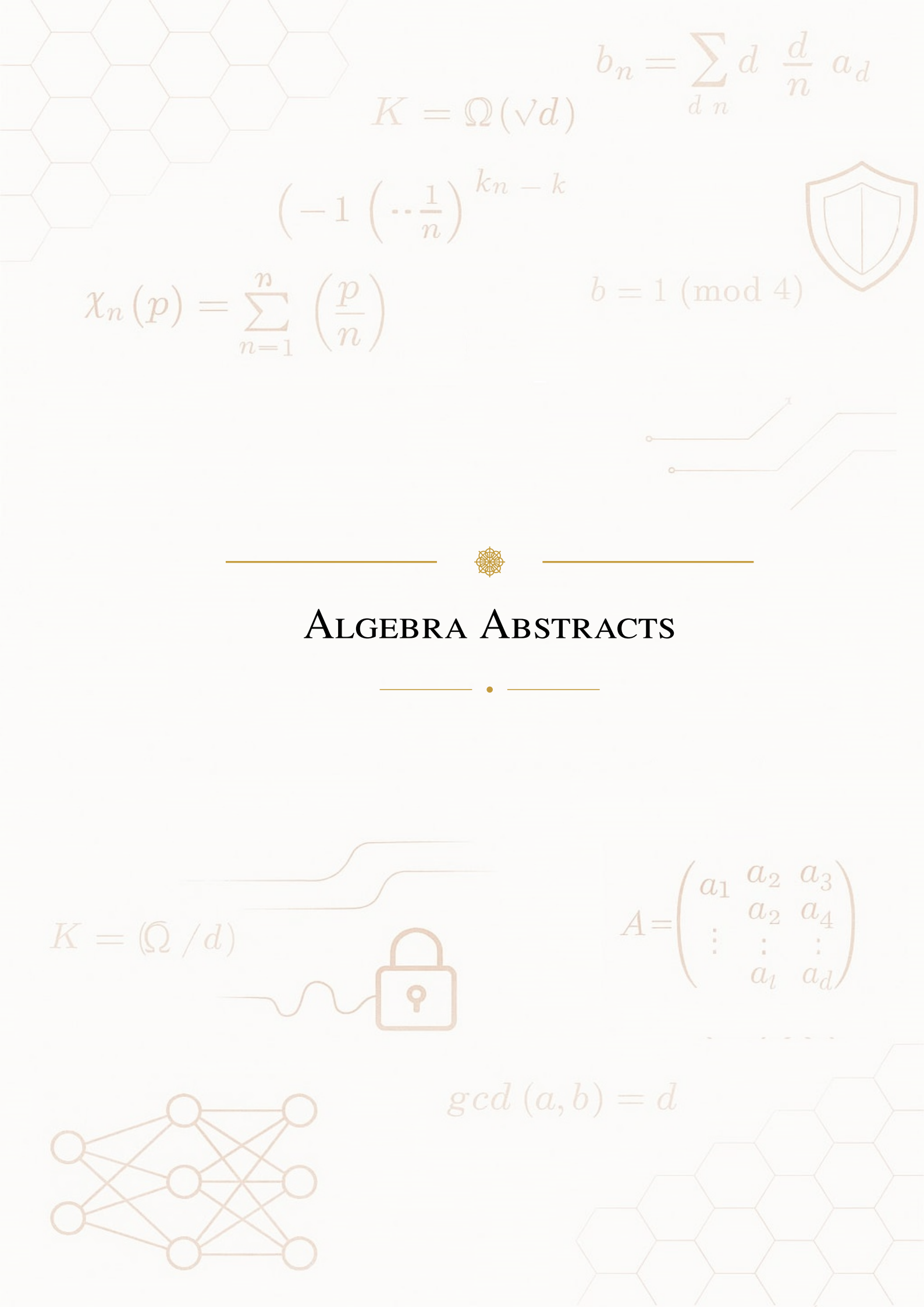
[4] V. Guruswami, *Constructions of Codes from Number Fields*, MIT Laboratory for Computer Science, 200 Technology Square, Cambridge, MA 02139, November 2000.

[5] H. W. Lenstra. *Codes from Algebraic Number Fields*. In: M. Hazewinkel, J.K. Lenstra, L.G.L.T. Meertens (eds), Mathematics and computer science II, Fundamental contributions in the Netherlands since 1945, CWI Monograph 4, pp. 95-104, North-Holland, Amsterdam, 1986.

[6] S. Roman. *Coding and Information Theory*. Hermann, Springer-Verlag, New York, 1992.

[7] F. Hajir and C. Maire, *Tamely Ramified Towers and Discriminant Bounds for Number Fields*, Compositio Mathematica, Vol. 128, pp. 35-53, Kluwer Academic Publishers, 2001.

[8] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées S-décomposées*, J. Théorie des Nombres de Bordeaux, Vol. 8, No. 1, pp. 47-73, 1996.



Algebra Abstracts

On S-pure ideals and $S - F$ rings

Adam AIT EL MEKKI
Department of Mathematics, Faculty of Science and Technology, University Sidi Mohammed Ben Abdellah, Fez, Morocco
adam.aitelmekki@usmba.ac.ma

Najib Mahdou
Department of Mathematics, Faculty of Science and Technology, University Sidi Mohammed Ben Abdellah, Fez, Morocco
mahdou@hotmail.com

Keywords: commutative algebra; homological algebra

Abstract. Let R be a commutative ring with nonzero identity and M be an R-module. In this paper, we develop more properties of S-pure ideals. Then we define S-F rings and we study their transfer to various contexts of commutative ring extensions such as the amalgamated algebra along an ideal and trivial ring extensions.

Motivation. F-rings were introduced by W. V. Vasconcelos in 1974. A commutative ring R is called an F-ring if and only if every pure ideal of R is generated by an idempotent element. Notable examples of F-rings include local rings, integral domains, and perfect rings. The primary objective of this paper is to adapt the concept of F-rings to S-pure ideals in commutative rings.

Main result.

Theorem 0.21. *Let R be a commutative ring, S a multiplicatively closed subset and I an ideal of R such that $I \cap S = \emptyset$. The following are statements are equivalent:*

1. *I is a S-pure ideal,*
2. *S^{-1} is a pure ideal,*
3. *For every $x \in R$ there existes $s \in S$ such that: $(sx) \cap I = sxI$*
4. *R/I is S-flat over R.*

Theorem 0.22. *Let R be a commutative ring, S a multiplicatively closed subset. The following statements are equivalent:*

1. *R is a S-F-ring,*
2. *Every S-pure ideal is generated by a S-idempotent,*
3. *Every cyclic S-flat module is projective.*

Methods In this paper we use standard techniques from commutative algebra and homological algebra.

Acknowledgements. The author gratefully acknowledges the financial support of the CNRST through the PhD-Associate Scholarship (PASS) Program, under which this research was conducted.

References

[1] E. Yildiz, B. A. Ersoy, and Ü. Tekir, *S*-versions and *S*-generalizations of idempotents, pure ideals and Stone type theorems, Bull. Korean Math. Soc. (1) **61** (2024), 83-92. Proc. London Math. Soc. (2) **15** (1916), 107–121.

[2] W.V. Vasconcelos, Finiteness in Projective Ideals, J. Algebra, **25** (1973), 269-278.

J-prime ideals of a commutative rings

Mohammed ASSALAMI
Laboratory of Modelling and Mathematical Structures. Department of Mathematics, Faculty of Science and Technology of Fez, Box 2202, University S.M. Ben Abdellah Fez, Morocco.
assalami.mohammed.phd@gmail.com
Joint Work with Suat Koç, Najib Mahdou and Ünsal Tekir

Keywords: J-prime ideal; prime ideal; J-ideal; n-ideal; r-ideal; amalgamation; trivial ring extension.
MSC: 13C15, 13B25, 13E99, 13A15

Abstract. Let R be a commutative ring with identity, and $J(R)$ denote the Jacobson radical of R. This paper introduces J-prime ideals, generalizing prime ideals, n-ideals, and J-ideals. A proper ideal I of R is a J-prime ideal if for every $a, b \in R, ab \in I$ implies $a \in I + J(R)$ or $b \in I$. We characterize rings in which every proper ideal is J-prime, showing that a ring has the property that every proper ideal is J-prime if and only if it is a quasilocal ring. Also, we show that (0) is a J-prime ideal if and only if the ring is présimplifiable. Furthermore, we examine J-prime ideal characteristics in various ring constructions, such as homomorphic image of rings, quotient rings, cartesian product rings, polynomial rings, power series rings, trivial ring extension and amalgamation rings.

References

[1] K. Adarbeh and M. Adarbeh, *Amalgamations of potent, semipotent, and semisimple rings*, Jordan J. Math. Stat. **16** (2023), 585–597.

[2] D. Anastasya and S. Wahyuni, *Presimplifiable and weakly presimplifiable rings*, Barekeng J. Math. Appl. **17** (2023), 1893–1900.

[3] D. D. Anderson and M. Bataineh, *Generalizations of prime ideals*, Commun. Algebra **36** (2008), 686–696.

[4] D. D. Anderson and M. Winders, *Idealization of a module*, J. Commut. Algebra **1** (2009), 3–56.

[5] M. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Series in Mathematics, Westview Press, Boulder, 2016.

[6] A. Badawi, Ü. Tekir and E. Yetkin, *On 2-absorbing primary ideals in commutative rings*, Bull. Korean Math. Soc. **51** (2014), 1163–1173.

[7] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Amalgamated algebras along an ideal*, Commutative Algebra and its Applications, Walter de Gruyter, Berlin, 2009, pp. 155–172.

[8] M. D'Anna, C. A. Finocchiaro and M. Fontana, *Properties of chains of prime ideals in an amalgamated algebra along an ideal*, J. Pure Appl. Algebra **214** (2010), 1633–1641.

[9] M. D'Anna and M. Fontana, *The amalgamated duplication of a ring along a multiplicative-canonical ideal*, Ark. Mat. **45** (2007), 241–252.

[10] M. Ebrahimpour and R. Nekooei, *On generalizations of prime ideals*, Commun. Algebra **40** (2012), 1268–1279.

C1–C3 Backbone for Zero-Divisor Graphs over $\mathbb{Z}/n\mathbb{Z}$: Graph Structure from Prime Factorization

Khaireddin ASSILA
ENSA Tétouan, Abdelmalek Essaâdi University, Morocco
khaireddin.assila@etu.uae.ac.ma

Keywords: zero-divisor graph; connectivity; diameter ≤ 3; Chinese Remainder Theorem; spectral radius; coloring.
MSC: 05C25, 05C50, 13A15, 13E15

Abstract.

We revisit zero-divisor graphs $\Gamma(R)$ with a focus on the arithmetic ring $R = \mathbb{Z}/n\mathbb{Z}$, showing how the classical three-item backbone C1–C3 already explains the main graph-theoretic features directly from the number-theoretic data of n.

C1 (Definition & connectivity). Vertices are the nonzero zero-divisors, with $x \sim y$ if and only if $xy \equiv 0 \pmod{n}$. The graph is connected in general, a classical fact that we recall with a short argument based on annihilators.

C2 (Diameter bound ≤ 3). Using the same annihilator routing, one shows that $\operatorname{diam}\Gamma(R) \leq 3$. For pedagogical examples, we verify this on small moduli and highlight typical 2- or 3-step paths.

C3 (CRT/product structure from the prime factorization of n). Writing

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

gives

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

by the Chinese Remainder Theorem. Adjacency factorizes across components, so the structure of $\Gamma(\mathbb{Z}/n\mathbb{Z})$ is dictated by the pairs (p_i, α_i):

- **Prime square:** $n = p^2$. All nonzero multiples of p form a clique, hence

  $$\Gamma(\mathbb{Z}/p^2\mathbb{Z}) \cong K_{p-1}.$$

  This yields $\omega = \chi = p - 1$ and spectral radius $p - 2$.

- **Square-free product:** $n = pq$ with distinct primes. Zero-divisors split into multiples of p and multiples of q, giving

  $$\Gamma(\mathbb{Z}/pq\mathbb{Z}) \cong K_{p-1,q-1}.$$

  Then $\chi = 2$ and the spectral radius is

  $$\sqrt{(p-1)(q-1)}.$$

More generally, an equitable partition induced by CRT blocks provides a small quotient matrix B whose eigenvalues bound (and often determine) the spectral radius, and guide quick estimates for independence number and coloring.

The entire analysis is elementary: graph parameters are read off from the prime factorization (via CRT), together with a simple spectral certificate from B. We conclude with a short catalogue for typical moduli (prime powers versus square-free n), illustrating how algebraic number-theoretic structure feeds standard graph invariants in algebraic graph theory.

References

[1] D. F. Anderson, P. S. Livingston, *The Zero-Divisor Graph of a Commutative Ring*, J. Algebra 217 (1999), 434–447. https://doi.org/10.1006/jabr.1998.7840

[2] I. Beck, *Coloring of a Commutative Ring*, J. Algebra 116 (1988), 208–226. https://doi.org/10.1016/0021-8693(88)90202-5

[3] C. Godsil, G. Royle, *Algebraic Graph Theory*, Springer (2001). https://doi.org/10.1017/CBO9780511801518

[4] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, Springer (2011). https://doi.org/10.1007/978-1-4020-9706-4

[5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer (1990). https://doi.org/10.1007/978-1-4684-6564-0

Homotopy Coherence in Enriched and Equivariant Settings

Safaa BELCAID
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
belcaidsafaa111@gmail.com

Keywords: homotopy theory; enriched categories; equivariant homotopy; higher structures

Abstract. Many algebraic and categorical structures arising in topology are not strictly associative or functorial, but instead satisfy their axioms only up to coherent homotopies. The systematic study of this phenomenon leads to the theory of homotopy coherent structures and higher categorical frameworks.

In this contribution, we investigate homotopy coherence in enriched and equivariant contexts. We focus on categories enriched over homotopical settings such as topological spaces or simplicial sets, where composition is associative only up to higher homotopies satisfying coherence conditions. We further examine how these ideas extend naturally to equivariant homotopy theory, where a group G acts on spaces and algebraic structures.

Motivation. Classical categorical structures are often too rigid to model phenomena arising in topology and homological algebra. Homotopy coherence provides a flexible framework where algebraic laws hold up to higher compatible homotopies, capturing deeper geometric information.

Main result. We establish a structural comparison between strict and homotopy coherent enriched categories in an equivariant setting, clarifying how equivariant homotopy information can be encoded via coherent diagrams indexed by orbit categories.

Theorem 0.23. *Let G be a discrete group and let $\mathcal{C}$ be a category enriched in a homotopical monoidal model category. Under suitable cofibrancy and completeness assumptions, the homotopy theory of G-equivariant enriched categories is equivalent to the homotopy theory of homotopy coherent diagrams indexed by the orbit category $\mathcal{O}_G$.*

This perspective connects enriched homotopy coherence with the classical fixed-point approach in equivariant homotopy theory and provides conceptual clarification of coherence phenomena in equivariant contexts.

Methods / Applications. Our approach combines techniques from model category theory, enriched category theory, and equivariant homotopy theory. Applications include the interpretation of G-actions on higher algebraic structures, the study of equivariant operads, and structural insights into homotopy coherent monoidal and braided G-categories.

Acknowledgements. Je remercie sincèrement mon encadrant **hicham yamoul** pour son accompagnement, son aide précieuse et sa disponibilité constante en toutes circonstances.

References

[1] J. M. Boardman and R. M. Vogt, *Homotopy Invariant Algebraic Structures on Topological Spaces*, Springer Lecture Notes in Mathematics, Vol. 347, 1973.

[2] A. D. Elmendorf, Systems of fixed point sets, *Trans. Amer. Math. Soc.* **277** (1983), 275–284.

[3] J. Lurie, *Higher Topos Theory*, Annals of Mathematics Studies 170, Princeton University Press, 2009.

[4] J. M. Boardman and R. M. Vogt, *Homotopy Invariant Algebraic Structures on Topological Spaces*, Lecture Notes in Mathematics, Vol. 347, Springer, 1973.

[5] A. D. Elmendorf, Systems of fixed point sets, *Trans. Amer. Math. Soc.* **277** (1983), 275–284.

[6] P. G. Goerss and J. F. Jardine, *Simplicial Homotopy Theory*, Progress in Mathematics, Vol. 174, Birkhäuser, 1999.

[7] W. G. Dwyer and D. M. Kan, Simplicial localizations of categories, *J. Pure Appl. Algebra* **17** (1980), 267–284.

[8] C. Berger and I. Moerdijk, On the homotopy theory of operads and monoids, *Algebr. Geom. Topol.* **3** (2003), 1089–1122.

[9] J. P. May, *Equivariant Homotopy and Cohomology Theory*, CBMS Regional Conference Series in Mathematics, Vol. 91, AMS, 1996.

[10] M. A. Mandell, J. P. May, S. Schwede and B. Shipley, Model categories of diagram spectra, *Proc. London Math. Soc.* **82** (2001), 441–512.

[11] E. Riehl, *Categorical Homotopy Theory*, Cambridge University Press, 2014.

[12] E. Riehl and D. Verity, Homotopy coherent adjunctions and the formal theory of monads, *Adv. Math.* **286** (2016), 802–888.

[13] J. Lurie, *Higher Topos Theory*, Annals of Mathematics Studies 170, Princeton University Press, 2009.

Cotorsion Dimension of the Trivial Ring Extension

Samir BOUTGHOUCHOUT
Department of Mathematics, Faculty of Science and Technology of Fez,
Box 2202, University Sidi Mohammed Ben Abdellah Fez, Morocco
samir.boutghouchout@usmba.ac.ma

Hwankoo Kim
Division of Computer Engineering, Hoseo University,
Republic of Korea
hkkim@hoseo.edu

Najib Mahdou
Department of Mathematics, Faculty of Science and Technology of Fez,
Box 2202, University S.M. Ben Abdellah Fez, Morocco
mahdou@hotmail.com

Keywords: cotorsion dimension; trivial ring extension; idealization; projective module; perfect ring; homological dimension **MSC:** 13C15; 13B25; 13E99; 13A15; 13D05

Abstract. Cotorsion dimension is a homological invariant that measures how far a module is from being cotorsion, and it is tightly connected to classical ring-theoretic properties: a ring is perfect exactly when its global cotorsion dimension is zero, and the inequality $\operatorname{cot.D}(R) \leq 1$ characterizes rings where every flat module has projective dimension at most one. In this work we investigate the behaviour of this invariant under the construction of trivial ring extensions (idealizations). Our main result establishes that for any ring R and any projective R-module P, the global cotorsion dimension is invariant under the idealization $S = R \ltimes P$:

Theorem 0.24. *Let R be a commutative ring and let P be a projective R-module. Then for the trivial ring extension $S = R \ltimes P$ one has*

$$\operatorname{cot.D}(S) = \operatorname{cot.D}(R).$$

The proof combines change-of-rings isomorphisms arising from the adjoint triple $- \otimes_R S \dashv \mathrm{Res} \dashv \mathrm{Hom}_R(S, -)$ with a careful analysis of flat S-modules via a canonical short exact sequence

$$0 \longrightarrow P \otimes_S F \longrightarrow F \longrightarrow F/PF \longrightarrow 0,$$

where F is a flat S-module. These tools yield two-sided comparison inequalities between the cotorsion dimensions over R and over S, ultimately giving the equality.

Consequences and applications. The invariance theorem has several immediate corollaries:

- *Stability of n-perfectness:* for any $n \geq 0$, $\operatorname{cot.D}(R) \leq n$ if and only if $\operatorname{cot.D}(S) \leq n$; in particular R is perfect precisely when S is perfect.
- *Local–global compatibility:* since localization commutes with idealization, $\operatorname{cot.D}(S) = \sup_{\mathfrak{p} \in \operatorname{Spec} R} \operatorname{cot.D}(R_{\mathfrak{p}})$.

- *Functorial transfer:* along the adjoint triple, cotorsion modules are preserved by restriction of scalars and by the coinduction functor $\mathrm{Hom}_R(S,-)$, and cotorsion (pre)envelopes and (pre)covers transfer between Mod $-R$ and Mod $-S$.

The theorem also provides a systematic way to construct families of rings with prescribed cotorsion dimension. We illustrate the breadth of the result with concrete examples: idealizations over fields, over $\mathbb{Z}$ with $n\mathbb{Z}$, over polynomial rings, iterated idealizations, and non-Noetherian perfect rings obtained by idealizing with large projective modules.

Methods and significance. The proof relies on elementary homological algebra and avoids heavy spectral sequence arguments, thanks to the projectivity of P which makes S a projective (hence flat) R-module. The techniques are flexible and extend to a broader class of ring extensions, opening the door to further studies of cotorsion dimension in non-commutative settings and in the context of derived categories.

Acknowledgements. H. Kim was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (2021R11A3047469).

References

[1] D. Bennis and N. Mahdou, *Gorenstein global dimensions and cotorsion dimension of rings*, Comm. Algebra **37** (2009), no. 5, 1709–1718.

[2] D. Bennis and N. Mahdou, *On n-perfect rings and cotorsion dimension*, J. Algebra Appl. **8** (2009), no. 2, 181–190.

[3] R. M. Fossum, P. A. Griffith and I. Reiten, *Trivial extensions of abelian categories*, Springer-Verlag, Berlin, 1975.

[4] L. X. Mao and N. Q. Ding, *The cotorsion dimension of modules and rings*, in: E. E. Enochs (ed.), *Abelian Groups, Rings, Modules, and Homological Algebra*, Lecture Notes in Pure and Applied Mathematics **249**, Chapman & Hall/CRC, 2006, 217–233.

Rings whose strongly Hopfian modules are Noetherian

Mankagna Albert DIOMPY
Department of Mathematics and Computer Science, University of Cheikh Anta Diop, Dakar Sénégal
albertdiompy@yahoo.fr

Ousseynou Bousso
Department of Mathematics and Computer Science, University of Cheikh Anta Diop, Dakar Sénégal
ousseynou1.bousso@ucad.edu.sn

Keywords: Hopfian; Strongly Hopfian; Noetherian; V-rings; SSI-rings; SF-Rings; polynomial extensions.
MSC: 13C60; 16D40; 16D10; 16P40

Abstract.

Motivation. Noetherian modules are always strongly Hopfian, but the converse is not true in general: the Prüfer group $M = \mathbb{Z}_{p^\infty}$ is strongly Hopfian but not Noetherian. We are therefore interested in rings for which every strongly Hopfian module is Noetherian; these rings are called SF-rings.

Main result.

Theorem 0.25. *Let R be a commutative ring and M an R-module. Then the following conditions are equivalent:*

1. *R is an SF-ring;*
2. *R is a Köthe ring;*
3. *R is an artinian principal ideal ring.*

Theorem 0.26. *Let R be a commutative ring satisfying the v.p. property. Then the following statements are equivalent:*

1. *R is an SF-ring;*
2. *R is a semisimple ring.*

Theorem 0.27. *Let R be a commutative von Neumann regular ring. Then the following statements are equivalent:*

1. *R is an SF-ring;*
2. *R is a QII-ring;*
3. *R is an SSI-ring;*
4. *R is a V-ring;*
5. *R is a strictly WV-ring.*

Theorem 0.28. *Let R be a commutative ring and M an R-module. Then R is an SF-ring if and only if $R[X_1, \ldots, X_n]$ is an SF-ring for all $n \geq 1$.*

Methods / Applications. We use module and ring theory techniques to study strongly Hopfian and Noetherian modules, providing constructions and counterexamples. The results characterize SF-rings, which can help understand the relation between Hopfian and Noetherian properties and guide further research in module theory. Moreover, these results open new avenues in commutative algebra, algebraic geometry, and post-quantum cryptography, particularly in module-based cryptographic constructions.

Acknowledgements. The authors would like to express their sincere thanks of all members of ICANTA'5 commitee.

References

[1] P. Aydogdu, A. C. Ozcan, *Semi co-Hopfian and Semi Hopfian Modules*, East-West J. Math., 10(1) (2008), 57–72.

[2] R. Wisbauer, *Foundations of Modules and Ring Theory*, Gordon and Breach Science Publishers, 1991.

[3] A. M. Dehkordi, *Rings Whose Cyclic Modules are Pure-Injective or Pure-Projective*, Journal of Algebra, 128–142 (2016).

[4] Some Results on *Locally Noetherian Modules and Locally Artinian Modules*, KYUNGPOOK Math. J., 58 (2018), 1–8.

[5] M. A. Diompy, R. D. Diouf, O. Bousso, *A Characterization of Commutative Rings in which every Semi Co-Hopfian Module is Artinian*, Commun. Combin., Cryptogr. and Computer Sci., 1 (2024), 19–22.

[6] M. A. Diompy, O. Bousso, A. El Moussaouy, *A Characterization of Rings in which every Semi-Hopfian Module is Noetherian*, Communications on Applied Nonlinear Analysis, Vol. 32, No. 4s (2025), ISSN: 1074-133X.

On rings satisfying the S-ascending chain condition on divisibility

Imane EL KHAIR
Department of Mathematics, Faculty of Science and Technology, Fez, Morocco
imane.elkhair1@usmba.ac.ma

Keywords: S-ACC_d-rings, ACC_d-rings, S-ACC-condtion, ACC-condition

Abstract. Let R be a commutative ring with identity and S be a multiplicative set of R. In this paper, we introduce and study the notion of S-ACC_d-rings as generalizations of the notions of ACC_d-rings. We say that R satisfies S-divisibility on ascending chains of ideals of R, if for every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots,$$

there exist $s \in S$ and $k \in \mathbb{N}$ such that for each $i \geq k$, we have $sI_i \subseteq x_i I_{i+1} \subseteq I_i$, for some $x_i \in R$. Several properties and characterizations of S-ACC_d-rings are given. Moreover, we study the transfer of the above properties to some constructions of rings such as trivial ring extensions.

Motivation. The generalization of the concept of ACC_d-rings.

Main result.

Theorem 0.29. *Let R be a ring satisfying the S-ACC_d condition. Then the following assertions hold:*

1. *If the set of S-finitely generated ideals in an ascending chain is infinite, then there exists an integer K such that for all $n \geq K$, the ideals I_n are S-finitely generated.*
2. *If the set of S-principal ideals in an ascending chain is infinite, then there exists an integer K such that for all $n \geq K$, the ideals I_n are S-principal.*

References

[1] I. EL Khair, H. Kim, and N. Mahdou, *Commutative rings in which every ideal is S-2-absorbing*, Rendiconti del Circolo Matematico di Palermo, (2024).

[2] A. Hamed, and S. Hizem, *Modules Satisfying the S-Noetherian Property and S-ACCR*. Communications in Algebra, **44**, (2016), 1941–1951.

[3] H. Kim, S. Mahdou and O. Es-Safi, *On rings and modules satisfying the ascending chain condition on divisibility*, Proc. Jangjeon Math. Soc., **28** 343, (2025).

Sur les polynômes tordus à valeurs entières

Mohammed FADEL
Département de Mathématiques, Faculté des Sciences, Université Mohammed Premier, Oujda, Maroc
medfadel597@gmail.com
Travail en commun avec: **Abdelkader Zekhnini**

Keywords: Polynômes à valeurs entières; Polynômes tordus; Extension de Ore. **MSC:** 16S36; 13F20; 11C99.

Abstract. Soit D un anneau intègre commutatif de corps de fractions K. Soient σ un automorphisme de K et δ une σ-dérivation c'est-à-dire δ vérifie $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$, pour tout a, b dans K. L'anneau de Ore ou l'anneau des polynômes tordus associé à σ et δ, noté par $K[X;\sigma,\delta]$, est constitué par les polynômes à coefficients dans K avec l'addition usuelle et la multiplication définie par

$$X.a = \sigma(a)X + \delta(a), \forall a \in K.$$

Quand $\delta = 0$, on le note simplement $K[X;\sigma]$. De plus, quand $\sigma = id$ et $\delta = 0$, on trouve l'anneau des polynômes usual $K[X]$.

L'étude des polynômes à valeurs entière $\mathrm{Int}(D) = \{P \in K[X] \mid P(D) \subset D\}$ a attiré beaucoup d'attention et il a été largement développée dans le cas commutatif. Nicholas J. Werner dans [3] a étendu cette théorie au cadre des polynômes tordus $K[X;\sigma]$ en introduisant l'ensemble des polynômes tordus à valeurs entière sur D: $\mathrm{Int}(D;\sigma) = \{P \in K[X;\sigma] \mid P(D) \subset D\}$ et en étudiant certaines de ses propriétés algébriques.

Dans ce travail, nous étendons l'étude au cas de l'anneau de polynômes tordus $K[X;\sigma,\delta]$ en considérant l'ensemble des polynômes tordus à valeurs entières dans le cas général

$$\mathrm{Int}(D;\sigma,\delta) = \{\, f \in K[X;\sigma,\delta] \mid f(a) \in D,\ \forall a \in D \,\}.$$

L'objectif est d'étudier la structure de ces polynômes dans le cadre non commutatif, ainsi que les conditions sous lesquelles cet ensemble forme un anneau, en mettant en évidence l'influence de σ et δ.

References

[1] A. Behajaina, *A note on integer-valued skew polynomials,* Journal of Algebra and Its Applications Vol. 22, No. 08, 2350171 (2023). https://doi.org/10.1142/S0219498823501712.

[2] Oystein Ore, *Theory of Non-Commutative Polynomials,* Annals of Mathematics Vol. 34, No. 3 (1933), pp. 480-508 (29 pages), https://doi.org/10.2307/1968173.

[3] Nicholas J. Werner, *Integer-valued skew polynomials,* Journal of Algebra and Its Applications (2021) 2150114 (20 pages). DOI: 10.1142/S0219498821501140.

Connection between two derivations and symmetric elements in prime rings with involution

Hiba FIHI and Abdellah MaMOUNI
Department of Mathematics, Faculty of Sciences, University Moulay Ismaïl, Meknes; Morocco
hiba.fihi@usmba.ac.ma
a.mamouni.fste@gmail.com

Keywords: algebra; number theory; applications **MSC:** 6N60; 16W10; 16W25

Abstract. This article examines the connection between two derivations and the center of a prime ring A with an involution $*$ of second kind that fulfills particular algebraic identities for symmetric elements and a fixed symmetric element.

Motivation. In [1] O. Ait Zemzami, K. Ouarghi and A. Mamouni investigated commutativity conditions involving derivations on prime rings and showed that certain elements defined through these conditions must be central or lead to a classification of the derivations. In particular, they proved that if a prime ring A admits a derivation d satisfying $[d(v), d(w)] - [v, w] \in Z(A)$ for all $v \in A$ and w is a fixed element in A, then w is central, and moreover, if A is a noncommutative prime ring and d is a derivation of A such that $d(v \circ w) - d(v) \circ w \in Z(A)$ for all $v \in A$, then $w^2 \in A$.

Motivated by the previous results, our purpose in this paper is to examine what happens in case we have two derivations that meet specific algebraic identities for symmetric elements and a fixed symmetric element.

Main result.

Theorem 0.30. *Let $(A, *)$ be a 2-torsion free prime ring with involution, let d_1 and d_2 be two derivations of A and b be a fixed nonzero element of A. If*

$$[d_1(s), d_2(b)] + [s, b] \in Z(A), \quad for \quad all \quad s \in S(A),$$

then $b \in Z(A)$.

Theorem 0.31. *Let $(A, *)$ be a 2-torsion free prime ring with involution, let d_1 be a nonzero derivation and d_2 a derivation of A and b be a fixed nonzero element of A. If*

$$[d_1(s), d_2(b)] - [d_2(b), s] - [b, d_1(s)] \in Z(A), \quad for \quad all \quad s \in S(A),$$

then $b \in Z(A)$. In particular, when $d_1 = 0$, it follows that $d_2(b) \in Z(A)$.

Theorem 0.32. *Let $(A, *)$ be a 2-torsion free prime ring with involution, let d_1 and d_2 be two derivations of A and b be a fixed nonzero element of A. If*

$$d_1(s) \circ d_2(b) - s \circ b \in Z(A), \quad for \quad all \quad s \in S(A),$$

then A is commutative.

Methods / Applications. In the proofs of our theorems, we use the following results:

- ([1], Lemma 2.1) Let A be a prime ring. If $ab \in Z(A)$ and $a \in Z(A)$, then $a = 0$ or $b \in Z(A)$.
- ([5], Theorem 1) Let $\delta \neq 0$ be a derivation of the prime ring A with $char(A) \neq 2$ and let $b \in A$ be such that $[b, \delta(A)] \subseteq Z(A)$, then $b \in Z(A)$.
- ([7], Lemma 3) Let A be a prime ring, and δ a derivation of A such that $[\delta(v), v] = 0$ for all $v \in A$, then A is commutative, or δ is zero.
- ([3], Lemma 2) Let A be a 2-torsion free prime ring. If $[[v, a], b] \in Z(A)$ for all $v \in A$, then $a \in Z(A)$ or $b \in Z(A)$.

References

[1] O. Ait Zemzami, K. Ouarghi and A. Mamouni, *Commuting-like elements in prime rings with derivations*, Rend. Circ. Mat. Palermo, II. **71** (2022), 665–676.

[2] H. El Mir, A. Mamouni, and L. Oukhtite, *Commutativity with algebraic identities involving prime ideals*, Commun. Korean Math. Soc. **35** (2020), 723–731.

[3] H. Fihi, A. Mamouni and K. Ouarghi, *Derivations acting on symmetric elements with central values*, In: Ashraf, M., Al Jaraden, J., Oukhtite, L., El Kinani, E.H. (eds) Algebra and Differential Equations with Applications. SICMA 2023. Springer Proceedings in Mathematics & Statistics, vol 508. Springer, Singapore.

[4] M. A. Idrissi, L. Oukhtite and N. Muthana, *Center-like subsets in rings with derivations or endomorphisms*, Comm. Alg. **45** (2019), 3794–3799.

[5] P. H. Lee and T. K. Lee, *On derivations of prime rings*. Chinese J. Math. **9** (1981), 107–110.

[6] M. R. Mozumder, N. A. Dar, and A. Abbasi, *Study of commutativity theorems in rings with involution*, Palest. J. Math. **11** (2022), 394–401.

[7] E. C. Posner, *Derivations in prime rings*, Proc. Amer. Math. Soc. **8** (1957), 1093–1100.

Graded Divided Domains

Nassima GUENNACH
Department of Mathematics, Faculty of Science and Technology, Fez, Morocco
nassima.guennach@usmba.ac.ma

Keywords: graded rings; graded divided domains; graded divided ideals **MSC:** 13A02; 13F05; 13A15

Abstract.

This work introduces and studies graded divided domains, extending the classical notion of divided domains to integral domains graded by a torsionless monoid. We first introduce a graded analogue of divided ideals and examine their fundamental properties, which naturally lead to the definition of graded divided domains. Let $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ be a commutative graded integral domain, where Γ is a torsionless monoid. A proper graded ideal I of R is called graded divided if it is comparable with every graded principal ideal of R. We then define R to be a graded divided domain if every graded prime ideal of R is graded divided.

We investigate structural properties of these notions and establish several equivalent characterizations of graded divided domains, highlighting essential differences with the classical ungraded case. In particular, we prove the following result.

Theorem 0.33. *Let $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ be a graded integral domain. The following statements are equivalent:*

1. *R is a graded divided domain;*
2. *For all graded ideals I and J of R, the ideals $\sqrt{J}$ and I are comparable;*
3. *For all homogeneous elements a and b of R, the ideals $\sqrt{bR}$ and aR are comparable;*
4. *For all homogeneous elements a and b of R, either $a \mid b$ or $b \mid a^n$ for some positive integer n.*

References

[1] A. Badawi, *On divided commutative rings*, Commun. Algebra, **27**(3) (1999), 1465–1474.

[2] D. E. Dobbs, *Divided rings and going-down*, Pacific J. Math., **67**(2) (1976), 353–363.

[3] D. E. Dobbs, *On flat divided prime ideals*, Factorization in Integral Domains, Lecture Notes Pure Appl. Math., Marcel Dekker, **189** (1997), 305–315.

Group structure of elliptic curve over the ring $\mathbb{F}_q[x]/(x^{m+n} - x^m)$.

Ahmed LAHLOU
MaSD Laboratory, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, Morocco.
ahmed.lahlou@usmba.ac.ma
Joint work with: **Abdelhakim Chillali and Ali Mouhib**

Keywords: group structure, elliptic curves. **MSC:** 11T71, 13B25, 14H52

Abstract. Let $\mathbb{F}_q[x]$ be the ring of polynomials with coefficients in the finite field $\mathbb{F}_q$, where $p = \text{char}(\mathbb{F}_q)$ is an odd prime number. Let m be a positive integer and n an odd prime number. In this paper, we study the group structure of the elliptic curve $E_{a,b}$ over $\mathbb{F}_q[x]/(x^{m+n} - x^m)$ defined by Weierstrass projective equation

$$E_{a,b} : Y^2Z = X^3 + aXZ^2 + bZ^3.$$

References

[1] M. Sala and D. Taufer, *Group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$*, Journal of Mathematical Cryptology, **18**(1), 20230025 (2024). DOI: 10.1515/jmc-2023-0025.

[2] A. Chillali and L. El Fadil, *Elliptic Curve over a Local Finite Ring R_n*, in: C. S. Ryoo (Ed.), *Number Theory and Its Applications*, IntechOpen, 2020, pp. 83–102. DOI: 10.5772/intechopen.93476.

[3] R. Invernizzi and D. Taufer, *Multiplication Polynomials for Elliptic Curves over Finite Local Rings*, in: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation (ISSAC '23)*, ACM, New York, NY, USA, 2023, pp. 352–360. DOI: 10.1145/3597066.3597068.

Solving Linear Systems via Spline Quasi-Interpolation

Soumia NGADI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
soumia.ngadi.d24@ump.ac.ma

Mohamed LAMNII and Amal BOUAICHA
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
m_lamnii1@yahoo.fr
amal.bouaicha@ump.ac.ma

Keywords: Linear systems; Spline quasi-interpolation; Discrete B-splines.

Abstract. We propose a method for solving linear systems of equations using spline-based quasi-interpolants. The approach combines two complementary strategies: discrete splines, which reduce the problem size and avoid full matrix inversion; and continuous splines, which enhance solution accuracy through an optimized selection of interpolation nodes. This hybrid strategy achieves a practical balance between computational efficiency and numerical precision.

Motivation. Solving big linear systems can be slow and unstable. We propose a faster and more stable approach: instead of solving the full system, we approximate the solution with a few localized spline functions, and solve only a reduced problem.

Main result.

Theorem 0.34. *Let $A \in \mathbb{R}^{n\times n}$, $b \in \mathbb{R}^n$, and let $B = [B_1 \ \cdots \ B_m] \in \mathbb{R}^{n\times m}$ with $m < n$ and* $\operatorname{rank}(B) = m$. *Define the subspace $\mathcal{V}_m = \operatorname{span}\{B_1, \ldots, B_m\}$. Then the least-squares approximation $X^\star \in \mathcal{V}_m$ to the solution of $AX = b$ is given by*

$$X^\star = Bc^\star, \quad \text{where } c^\star \text{ solves } (AB)^\top (AB)\, c = (AB)^\top b.$$

No inversion of A is required.

Methods. Let us consider the linear system

$$AX = b, \qquad A \in \mathbb{R}^{n\times n},\ b \in \mathbb{R}^n, \tag{2}$$

where the unknown $X \in \mathbb{R}^n$ is to be approximated.

We introduce a reduced basis of m discrete B-splines $\{B_j\}_{j=1}^m \subset \mathbb{R}^n$, with $m < n$, each supported on a small index interval (local support). The solution is sought in the subspace spanned by this basis:

$$X \approx S(c) := \sum_{j=1}^{m} c_j B_j = B\,c, \tag{3}$$

where $B = [B_1 \ \cdots \ B_m] \in \mathbb{R}^{n\times m}$ and $c \in \mathbb{R}^m$ denotes the vector of coefficients.

Substituting into the original equation yields the reduced system:

$$AB\,c \approx b. \tag{4}$$

Define the reduced matrix $\tilde{A} := AB \in \mathbb{R}^{n\times m}$. We solve the least-squares problem

$$\min_{c\in\mathbb{R}^m} \|\tilde{A}c - b\|_2^2. \tag{5}$$

If $\tilde{A}$ has full column rank, the unique minimizer is given explicitly by

$$c^\star = (\tilde{A}^\top \tilde{A})^{-1}\tilde{A}^\top b. \tag{6}$$

The approximate solution to the original system is then reconstructed as

$$X^\star := B\,c^\star. \tag{7}$$

Remark. This approach avoids direct inversion of A. Its computational cost scales with m and benefits from the locality of the B-splines, enabling efficient matrix–vector products and natural sparsity.

References

[1] C. Bracco, C. Giannelli, and A. Sestini, *Adaptive scattered data fitting by extension of local approximations to hierarchical splines*, Comput. Aided Geom. Design 52 (2017), 90–105.

[2] S. Zhang, C. Zhu, and Q. Gao, *High accuracy B-spline quasi-interpolants and applications in numerical analysis*, Applicable Anal. 102 (2023), no. 7, 2035–2054.

[3] M. Arioli and I. S. Duff, *Preconditioning linear least-squares problems by identifying a basis matrix*, SIAM J. Sci. Comput. 37 (2015), no. 5, S544–S561.

[4] L. Brugnano, D. Giordano, F. Iavernaro, and G. Rubino, *An entropy-based approach for a robust least squares spline approximation*, J. Comput. Appl. Math. 443 (2024), 115773.

[5] Y. Zhou and D. Huybrechs, *Efficient least squares approximation and collocation methods using radial basis functions*, J. Comput. Appl. Math. 447 (2024), 115870.

On the Enumeration of Subgroup Chains in the Direct Product $\mathbb{Z}_{p^n} \times A_4$: A Generating Function Approach

Mike Ekpen OGIUGO
Department of Mathematics, Yaba College of Technology, Lagos, Nigeria
mike.ogiugo@yabatech.edu.ng

Keywords: algebra; number theory ; fuzzy algebra; combinatorics **MSC:** 20B30; 20B35; 20N25; 20E15

Abstract. The enumeration of subgroup chains represents a fundamental problem in combinatorial group theory, closely linked to the study of fuzzy subgroups. This problem can be reformulated as a combinatorial question on the subgroup lattice of a group G: determining the number of chains of subgroups that terminate in G (see [1], [2]). In this paper, the characterisation of subgroup chains in the direct product $\mathbb{Z}_{p^n} \times A_4$, where p is prime and $n \geq 1$, is studied using an enumerative approach based on representatives of isomorphism classes of subgroups and their orders. This group serves as a natural model combining cyclic p-group structure with non-abelian symmetry. This method yields first-degree linear non-homogeneous recurrence relations with constant coefficients, which are solved via the generating function method. The explicit closed-form formulas are derived, expressed as polynomial functions in p and n, for the number of subgroup chains terminating in $\mathbb{Z}_{p^n} \times A_4$. This result contributes to the systematic study of subgroup lattices in classical group theory.

References

[1] M. E. Ogiugo, A. Sehgal, S. A. Adebisi & M. EniOluwafe, *The Number of Chains of Subgroups in the Lattice of Subgroups of the group* $Z_m \times A_n, n \leq 6, m \leq 3$, International J. Math. Combin., (4) (2022), 32–40.

[2] A. C. Volf, *Counting fuzzy subgroups and chains of subgroups*, Fuzzy Systems and Artificial Intelligence (10) (2004), 191–200

The $\mathcal{F}_\kappa(I)$-limit on the ring of continuous functions

Ayoub OUDIKA[1] **Hassan MOUADI**[2] **Driss KARIM**[1]
[1]Faculty of Sciences and Technology of Mohammedia, Hassan II University, Casablanca, Morocco
[2]Polydisciplinary Faculty of Taroudant, Ibnou Zohr University, Agadir, Morocco
ayouboudika.ao16@gmail.com

Keywords: Ultrafilters; infinite cardinals; $\mathcal{F}$-limit; $\mathcal{F}$-limit topology; rings of continuous functions
MSC: 13A15; 13C05; 54C40

Abstract. We extend the notion of the $\mathcal{F}$-limit, introduced in [4], to an arbitrary infinite index set I and to a family $\mathcal{F}_\kappa(I)$ of subsets of I, which is not necessarily an ultrafilter on I. This construction generalizes ultrafilter limits and provides a broader framework for describing convergence phenomena on prime spectra.

We prove that this generalized limit induces a topology on $\mathrm{Spec}(R)$, called the $\mathcal{F}_\kappa(I)$-*limit topology*. We study its fundamental properties and compare it with classical topologies such as the Zariski and constructible topologies. In particular, we show that, under suitable conditions on $\mathcal{F}_\kappa(I)$, the resulting space remains spectral.

We then specialize our study to the ring of continuous functions $C(X,\mathbb{R})$, where X is a topological space. We investigate how the $\mathcal{F}_\kappa(I)$-limit topology interacts with the algebraic and topological structure of $C(X,\mathbb{R})$, especially when X is compact Hausdorff.

Motivation. Limit constructions on $\mathrm{Spec}(R)$ provide refined tools for understanding the convergence of prime ideals beyond the classical Zariski framework. Extending these constructions to families more general than ultrafilters leads to new topological structures and deeper connections between topology and commutative algebra.

Main result.

Theorem 0.35. *Let X be a compact Hausdorff space and let $\mathcal{F}_\kappa(I)$ be a family of subsets of an infinite set I satisfying suitable stability conditions. Then the $\mathcal{F}_\kappa(I)$-limit topology on* $\mathrm{Spec}(C(X,\mathbb{R}))$ *is finer than the Zariski topology. Moreover,* $\mathrm{Spec}(C(X,\mathbb{R}))$*, endowed with this topology, is a countably compact space.*

Methods / Applications. Our approach combines techniques from ultrafilter theory, spectral topology, and the theory of rings of continuous functions. These results contribute to the understanding of generalized limit topologies and open the way to further applications in algebraic topology and non-classical convergence structures.

References

[1] H. Mouadi, D. Karim, *Some Topology on Zero-Dimensional Subrings of Product of Rings*, Filomat 34:14, 2020.
[2] L. Gillman, M. Jerison, *Rings of Continuous Functions*, Softcover reprint of the hardcover, 1960.
[3] R. Engelking, *General Topology*, Sigma Series in Pure Mathematics, 1989.
[4] S. Garcia-Ferreira, L. M. Ruza-Montilla, *The $\mathcal{F}$-limit of a sequence of prime ideals*, Communications in Algebra, 2011.
[5] W. W. Comfort, S. Negrepontis, *The Theory of Ultrafilters*, Springer-Verlag, 1974.

A Yang–Petro Type Theorem for Real Division Algebras with Left Unit

Diabang André SOULEYE
Department of Mathematics, UFR SET, University of Iba Der Thiam, Thies, Sénégal
andre.diabang@univ-thies.sn

Mballo Ama Sékou
Department of Mathematics, UFR SET, University of Iba Der Thiam, Thies, Sénégal
amasekou.mballo@univ-thies.sn

Papa Cheikhou Diop
Department of Mathematics, UFR SET, University of Iba Der Thiam, Thies Sénégal
cheikh.diop@univ-thies.sn

Keywords: real division algebra, left unit, associator identity, four-dimensional algebra, isotope.
MSC: 17A30, 17A35, 17A36.

Abstract. In this article, we study finite-dimensional real division algebras with a left unit satisfying associator identities of the form $(x^p, y^q, x^p) = 0$, where $p, q \in \{1, 2\}$. We consider in particular the identities $(x, y^2, x) = 0$, $(x^2, y, x^2) = 0$, and $(x^2, y^2, x^2) = 0$. We recall that the identity $(x, y^2, x) = 0$ is related to flexibility and, in this setting, yields the existence of a 2-dimensional subalgebra. Our main result, in the spirit of the Yang–Petro theorem, states that every algebra of dimension greater than 2 satisfying $(x^2, y, x^2) = 0$ contains a 2-dimensional subalgebra isomorphic either to $\mathbb{C}$ or to ${}^*\mathbb{C}$. We apply this result to the 4-dimensional case, obtaining structural restrictions in the complex case and an explicit family of examples in the split case. Finally, we examine the identity $(x^2, y^2, x^2) = 0$ through its full polarization and show that it also leads to the existence of a 2-dimensional subalgebra.

Motivation. The motivation for this work is to determine whether the Yang–Petro theorem extends to finite-dimensional real division algebras with left unit satisfying weak associator identities. We prove that, in the situations studied here, such algebras still admit two-dimensional subalgebras.

Main result. Our main result shows that the Yang–Petro phenomenon extends to the setting of finite-dimensional real division algebras with left unit satisfying certain weak associator identities. More precisely, every such algebra satisfying $(x^2, y, x^2) = 0$ contains a 2-dimensional subalgebra isomorphic either to $\mathbb{C}$ or to ${}^*\mathbb{C}$. In the case of the identity $(x, y^2, x) = 0$, one also obtains the existence of a 2-dimensional subalgebra isomorphic to $\mathbb{C}$. Finally, under the additional assumption that the algebra contains a central element, the same phenomenon holds for algebras satisfying $(x^2, y^2, x^2) = 0$, which then contain a 2-dimensional subalgebra isomorphic to $\mathbb{C}$.

Theorem 0.36. *Let A be a finite-dimensional left unital real division algebra with left unit e. Then the following assertions are equivalent:*

(1) A satisfies $(x, y, x) = 0$ for all $x, y \in A$;

(2) A satisfies $(x, y^2, x) = 0 \qquad$ *for all* $x, y \in A$.

Theorem 0.37. *Let A be a finite-dimensional left unital real division algebra with left unit e, satisfying* $(x^2, y, x^2) = 0 \qquad$ *for all* $x, y \in A$.

Assume $\dim R(A) > 1$. *Then there exists* $u \in A \setminus \mathbb{R}e$ *such that the subalgebra generated by u, denoted by* $A(u)$*, is isomorphic either to* $\mathbb{C}$ *or to a split two-dimensional algebra* $*\mathbb{C}$.

If moreover $\dim R(A) = 4$, *then for every* $v \in A \setminus A(u)$, *the set* $\{e, u, v, uv\}$ *is a basis of A.*

Theorem 0.38. *Let A be a four-dimensional left unital real division algebra with left unit e, satisfying*

$$(x^2, y, x^2) = 0 \qquad \text{for all } x, y \in A.$$

Then there exists $u \in A$ *such that* $A(u)$ *is isomorphic either to* $\mathbb{C}$ *or to* $*\mathbb{C}$*, but not both.*

Moreover:

(1) if $A(u) \cong \mathbb{C}$, *then* $\dim R(A_e) \in \{2, 4\}$;

(2) if $A(u) \cong *\mathbb{C}$, *then* $\dim R(A_e) = 1$.

Theorem 0.39. *Let A be a finite-dimensional real division algebra with left unit e satisfying*

$$(x^2, y^2, x^2) = 0 \qquad \text{for all } x, y \in A.$$

If A contains a non-scalar central element, then A contains a 2-dimensional subalgebra isomorphic to $\mathbb{C}$.

Methods / Applications. Our approach relies mainly on polarization and linearization techniques for associator identities, together with structural arguments specific to finite-dimensional real division algebras with left unit. We also make use of the study of central elements and the subalgebras they generate. These methods lead to Yang–Petro type results, provide criteria for the existence of 2-dimensional subalgebras, and yield applications to the structural analysis of 4-dimensional algebras.

Acknowledgements. Acknowledgements. The authors would like to express their sincere thanks to all the members of the ICANTA'5 committee.

References

[1] A. A. Albert, *Non-associative Algebras. I. Fundamental concepts and isotopy. Annals of Mathematics. 43 (1942), 685-707.*,

[2] C. T. Yang *Division algebras and fibrations of spheres by great spheres, J. Dimerential Geometry, 16 (1981), 577-593. https://doi.org/10.4310/jdg/1214436369*

[3] F. G. Frobenius, *Über lineare Substitutionen und bilineare Formen*, J. Reine Angew. Math.

[4] B. Kandé et al., *Unital Real Division Algebras Satisfying* $(x^2, y^2, x^2) = 0$. International Journal of Algebra, Vol. 15, 2021, no. 1, 11 - 15.

Cryptography, Cyber Security and Artificial Intelligence Abstracts

A Survey of Machine Learning and Deep Learning Approaches for DDoS Attack Detection in Vehicular Networks.

Anass AL JARROUDI[1], Omar CHAIEB[1], Nabil KANNOUF[2], Mohammed BENABDELLAH[1]

[1]Laboratory of ACSA, UMP, Oujda, Morocco
[2]Laboratory of LSA, UAE, Tetouan, Morocco

anass.aljarroudi.d24@ump.ac.ma
omar.chaieb.men@gmail.com
nabil.kannouf@gmail.com
med_benabdellah@yahoo.fr

Keywords: Cybersecurity; VANETs; DDoS Attack Detection **MSC:** 68M10; 68M12; 68T05

Abstract. Vehicular Ad-hoc Networks (VANETs) have an important role in Intelligent Transportation System where they make a communication possible between Vehicle to another Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P) and Vehicle to Everything (V2X), these connections allow cooperative vehicles to exchange their information such as Basic Safety Message (BSM) that contains the mobility data (Position, speed, acceleration), road trajectory of the vehicle and road traffic situation (Existence of accidents or traffic jams) using wireless communication technologies helping to improve the efficiency of the traffic flow through congestion avoidance, intersection control, accident avoidance, emergency management and emission control. All these advantages disappear when VANETs are attacked, especially because they are considered important targets due to the changing nature of vehicle movement, their decentralized operation, and their open wireless environment. There is extensive research on detecting of different attacks like Sybil, spoofing, message falsification, routing attacks, however, we find a significant research gap regarding DDoS attack detection in VANETs, especially because this attack is considered one of the most dangerous attacks due to its effect on the network availability and the performance of VANET components such as flood roadside units with fake requests, overload the on-board units and disrupt the controller in SDN-VANET which affect the system response time and prevents safety information that are urgent from arriving in time to their destination such as vehicle crash alerts and emergency warning. This survey gives an in-depth overview of recent research on DDoS attacks in VANET environments and the SDN-VANET variant. After reviewing previous studies that rely on traditional technique in detecting of DDoS attack that are based on fixed rules or known attack's signatures which produce poor results, we decided to focus in this paper on studying the approaches related to supervised machine learning, deep learning, hybrid models, and also papers that incorporate feature engineering, hyperparameter optimization and dimensionality minimization since these are what boost the efficiency of the approach in the detection of this type of attack.

Motivation. Safety is important for passengers in an autonomous environment by securing operation of the Intelligent Transportation Systems (ITS). Safe operation of selected ITS services

depends on availability and timely communication between vehicles using the Vehicular Ad Hoc Network (VANET). For example, Basic Safety Messages (BSMs) must be transmitted using reliable and timely communication in order for the ITS to respond in a timely manner and operate efficiently.

While many attended to the VANET security, they failed to offer an effective detection of DDoS attacks targeting its performance. Others focused on a different type of attack and used different datasets, evaluation frameworks, and metrics. However, DDoS attacks have a direct impact on the availability of the network, compromising the underlying benefits of ITS and potentially endangering vehicle security and safety.

Main Contribution. This survey gives an overview of the different techniques to detect DDoS attacks in VANET, dividing them according to which strategy fits them best, namely: hybrid/ensemble machine learning models, optimized classical machine learning models, deep learning models, and adaptive or distributed detection approaches. In this survey, the impact of feature selection and optimization on the performance of the models is highlighted, in addition to the datasets and tools that are commonly used. Then, the existing challenges and gaps are identified so that future researchers can focus on them to develop a more reliable and effective DDoS attack detection system.

Review Methodology and Scope. A broad survey is done on DDoS attack detection methods in VANET and SDN-VANET settings. Most of these techniques employ machine learning and deep learning models. This survey also covers different dataset generation tools and datasets, along with feature selection techniques and evaluation metrics. A thorough identification of the various DDoS detection methods detailed within this survey enables developers of DDoS detection systems to identify areas where further development of these systems would make them more successful in detecting present-day and complex DDoS attacks.

References

[1] A. Verma, R. Saha, G. Kumar, M. Conti, and J. Rodrigues, *VAIDANSHH: Adaptive DDoS detection for heterogeneous hosts in vehicular environments*, Vehicular Communications **48** (2024), 100787. doi:10.1016/j.vehcom.2024.100787.

[2] A. Verma, R. Saha, G. Kumar, and M. Conti, *PETRAK: A solution against DDoS attacks in vehicular networks*, Computer Communications **221** (2024). doi:10.1016/j.comcom.2024.04.025.

[3] M. A. Setitra and M. Fan, *Detection of DDoS attacks in SDN-based VANET using optimized TabNet*, Computer Standards & Interfaces **90** (2024), 103845.

Object Detection for Weed Recognition in Precision Agriculture: A Systematic Review of Methods, Datasets and Embedded Approaches

Hanae AL KADDOURI[1], Abdelmalek ELMEHDI[1], Youssef DOUZI[2]
[1]Smart Information, Communication, and Technology, Mohammed First University, Oujda, Morocco
[2]Arithmetic, Calcul Scientific and Applications Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco
hanae.alkaddouri@ump.ac.ma

Keywords: Weed Detection; Object Detection; Deep Learning; YOLO; Precision Agriculture

Abstract. Weed infestation is a leading cause of global crop yield loss, traditionally managed through manual labor or broad-spectrum herbicide application, methods that are costly, labor-intensive, and ecologically harmful. The emergence of precision agriculture, powered by advances in computer vision and Deep Learning (DL), opens new avenues for site-specific automated weed control. This paper presents a comprehensive systematic review of object detection approaches applied to weed recognition in agricultural settings, covering the period 2016–2024. We examine the evolution from classical Machine Learning methods (SVM, HOG, Random Forests) toward modern DL architectures, with particular emphasis on one-stage detectors (YOLO family, SSD, EfficientDet) and two-stage approaches (Faster R-CNN). We analyze fourteen publicly available benchmark datasets (DeepWeeds, CropAndWeed, PlantDoc, WeedMap, among others), comparing their scale, annotation granularity, and transfer learning suitability. Special attention is given to deploying models on embedded platforms (Jetson Nano, Raspberry Pi) via INT8 quantization and network pruning. Open challenges include domain gap between controlled and field conditions, class imbalance, and the scarcity of geographically diverse training data, display:

Motivation. The integration of DL into precision agriculture represents a paradigm shift in crop protection, offering the potential to dramatically reduce chemical inputs while improving selectivity and timeliness of interventions. Despite rapid advances in object detection, a unified analysis of architectures, datasets, and deployment constraints specific to the agricultural domain remains lacking.

Main result. Our review reveals that one-stage detectors, particularly the YOLO family, consistently dominate the precision-speed trade-off across agricultural benchmarks, while two-stage approaches remain competitive for high-accuracy, low-latency-tolerant scenarios. Dataset diversity and annotation quality emerge as the primary bottlenecks limiting generalization across crop types, growth stages, and geographic regions.

Applications. Following PRISMA guidelines, we systematically reviewed 87 peer-reviewed studies (2016–2025) across IEEE Xplore, Scopus, and Web of Science. Papers are analyzed along three axes: detection architecture, dataset characteristics, and deployment context. Findings

contribute to the broader field of intelligent agricultural systems and provide actionable guidance for researchers designing vision-based plant protection solutions.

References

[1] M. S. Islam et al., *WeedVision: Multi-Stage Growth and Classification of Weeds using DETR and RetinaNet for Precision Agriculture*, DOI:10.48550/arXiv.2502.14890

[2] V. Pandiyaraju et al., *A Hybrid CNN-ViT-GNN Framework with GAN-Based Augmentation for Intelligent Weed Detection*, DOI:10.48550/arXiv.2511.15535

[3] M. Saltık et al., *Comparative Analysis of YOLOv9, YOLOv10 and RT-DETR for Real-Time Weed Detection*, DOI:10.1007/978-3-031-91835-3

[4] K. Hu. et al., *Deep Learning Techniques for In-Crop Weed Recognition in Large-Scale Grain Production Systems: A Review*, https://doi.org/10.1007/s11119-023-10073-1

[5] U. Bhandari et al., *Precision Weed Detection Using UAVs and Deep Learning: Models, Paradigms, and Challenges*, https://doi.org/10.1016/j.atech.2025.101656

[6] A. Allmendinger. et al., *Assessing the Capability of YOLO- and Transformer-Based Object Detectors for Real-Time Weed Detection*, Precision Agriculture, 2025. https://doi.org/10.1007/s11119-025-10246-0

[7] N. Rai et al., *Agricultural Weed Identification via Optimized Deep Learning on Edge Computing*, Computers and Electronics in Agriculture, 2024. https://doi.org/10.1016/j.compag.2023.108442.

[8] S. Shinde et al., *Real-Time Weed Detection Using YOLOv9c Integrated Mobile App*, Springer, 2025. https://doi.org/10.1007/978-981-96-8043-6

[9] J. Silva et al., *Deep Learning for Weed Detection and Segmentation from UAV Images*, Remote Sensing, 2024. https://doi.org/10.3390/rs16234394

[10] N.Y. Murad et al., *Weed Detection Using Deep Learning: A Systematic Literature Review*, Sensors, 2023. https://doi.org/10.3390/s23073670

[11] W. Hu et al., *Review of Deep Learning-Based Weed Identification in Crop Fields*, International Journal of Agricultural and Biological Engineering, 2023. DOI: 10.25165/j.ijabe.20231604.8364

[12] Z. Khan et al., *Object Detection in Agriculture: A Comprehensive Review*, Agriculture, 2025. https://doi.org/10.3390/agriculture15131351

A Comparative Analysis of Machine Learning and Deep Learning Approaches for Intrusion Detection in IoT/IIoT Networks: Datasets, Feature Selection, and Explainability

Yassine ATMANI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
atmani.yassine20@gmail.com

Omar CHAIEB
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
omar.chaieb.men@gmail.com

Mohammed BENABDELLAH
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
med_benabdellah@yahoo.fr

Keywords: intrusion detection system; Internet of Things; explainable artificial intelligence; machine learning; deep learning; feature selection; PRISMA

Abstract. The fast development of the Internet of Things and the Industrial Internet of Things has significantly increased the attack surface of current networks, where heterogeneous and resource-constrained devices work in ever-changing traffic conditions. Intrusion Detection Systems are an important security measure that is usually installed at gateways, edge nodes, or cloud platforms in order to track traffic and detect anomalies or known attack patterns. Although recent machine learning and deep learning techniques have such positive results are reported to be over 99% detection accuracies on benchmark datasets are commonly acquired in controlled experimental conditions and provide black box models that do not transparency is a severe constraint in safety-critical IoT/IIoT implementations where explainability and responsibility is necessary.

This paper provides a methodological literature review based on PRISMA to evaluate ML-based and DL-based network IDS that are specifically created to operate in the IoT and IIoT settings. A total of 54 records were found in IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar, out of which 15 studies were included following a strict multi-stage screening process based on relevance, recency (2020–2025), peer-review status, and methodological soundness. The review profile of the research in the field of IDS studies is analyzed through various complementary lenses: the taxonomy of detection methods (signature-based, anomaly-based, and hybrid), the ML/DL methodologies that are used (such as random forests, SVMs, CNNs, LSTMs, autoencoders, and federated learning structures). It also reviews popular benchmark datasets such as KDD99, NSL-KDD, CICIDS2017, ToN-IoT, Bot-IoT, WUSTL-IIoT and CIC-IoT-2022 and critically evaluates their real-world applicability in terms of modeling real-world IoT traffic. We also discuss the key approaches to feature selection common in the literature, between filter-based and wrapper-based methods and bio-inspired optimization methods, and also how much (or how rarely) Explainable Artificial Intelligence (XAI) methods, including SHAP, LIME, and Grad-CAM, have been applied to IDS frameworks.

We find that there are a number of gaps. To begin with, most of the suggested IDS models are trained and tested on old or artificial data that is not sufficiently representative of the diversity and dynamism of real-world IoT/IIoT networks. Second, extreme imbalance in classes especially those that are rare and high-impact like U2R and R2L is not adequately tackled, which inflates the overall accuracy but hides the poor recall of key threat classes. Third, cross-dataset generalization is rarely tested: models trained on one benchmark (e.g., CICIDS2017) are hardly tested on other (e.g., ToN-IoT or Bot-IoT), which restricts the ability to be confident in the operational strength of the models. Fourth and most importantly, XAI methods are virtually nonexistent in the reviewed literature, which makes the decision making process opaque and thus impedes the adoption of XAI methods by analysts. On the basis of these results, we can point out open research directions in more realistic, statistically rigorous, and interpretable IDS solutions. Specifically, we support the idea of explainability being incorporated into the feature selection pipeline instead of being an after-hoc feature to generate models, which are accurate, transparent, and auditable at the same time. This research is expected to help sustain a human-AI co-operative security paradigm where intrusion notifications are not only accurate but also interpretable and actionable by security analysts.

References

[1] T. A. Ahanger et al., *Machine learning-inspired intrusion detection system for IoT*, Comput. Electr. Eng., vol. 123, 110265, 2025.

[2] S. A. Bakhsh et al., *Enhancing IoT network security through deep learning-powered IDS*, Internet Things, vol. 24, 100936, 2023.

[3] J. Malik et al., *Hybrid deep learning based threat intelligence framework for Industrial IoT systems*, J. Ind. Inf. Integr., vol. 45, 100846, 2025.

[4] A. Orman, *Cyberattack Detection Systems in IIoT Networks in Big Data Environments*, Appl. Sci., vol. 15(6), 3121, 2025.

[5] N. Ben Henda et al., *Attack Detection in IoT Network Using SVM and Improved Feature Selection*, J. Netw. Syst. Manag., vol. 32(4), 92, 2024.

[6] J. M. Peterson et al., *A Review and Analysis of the Bot-IoT Dataset*, IEEE Int. Conf. SOSE, pp. 20–27, 2021.

[7] S. K. Birthriya et al., *Detection and prevention of spear phishing attacks: A comprehensive survey*, Comput. Secur., vol. 151, 104317, 2025.

[8] F. Thabit et al., *Enhanced IDS for IoT networks through ML: an examination utilizing the AWID dataset*, Cogent Eng., vol. 11(1), 2378603, 2024.

[9] M. M. Rahman et al., *A survey on intrusion detection system in IoT networks*, Cyber Secur. Appl., vol. 3, 100082, 2025.

[10] B. Olanrewaju-George and B. Pranggono, *Federated learning-based IDS for IoT using unsupervised and supervised DL models*, Cyber Secur. Appl., vol. 3, 100068, 2025.

[11] S. Saif et al., *A comprehensive analysis of ML-based IDS: evaluating datasets and algorithms for IoT*, J. Cyber Secur. Technol., pp. 1–27, 2024.

[12] E. Elmahfoud et al., *ML Algorithms for Intrusion Detection in IoT Prediction and Performance Analysis*, Procedia Comput. Sci., vol. 236, pp. 460–467, 2024.

[13] A. Bensaoud and J. Kalita, *Optimized detection of cyber-attacks on IoT networks via hybrid DL models*, Ad Hoc Netw., vol. 170, 103770, 2025.

[14] V. Sivagaminathan et al., *IDS for wireless sensor networks using computational intelligence techniques*, Cybersecurity, vol. 6(1), 27, 2023.

[15] L. Thomas and A. B. K., *An Efficient IoT Based IDS Using Optimization Kernel ELM*, Int. J. Comput. Netw. Inf. Secur., vol. 17(2), pp. 72–87, 2025.

Lightweight Anchor-Free Detection of UI Form Components for Real-Time Desktop RPA: A Domain-Specific Deep Learning Approach

Meryem BAHRAOUI
Computer Science Department, Oujda, Morocco
meryem.bahraoui.m24@ump.ac.ma
Noura Ouerdi
LARI Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco
n.ouerdi@ump.ac.ma

Keywords: GUI element detection; UI form components; RPA; YOLOX-S; OpenCV; OCR; desktop automation; natural language instructions.

Abstract. Detecting UI form components in desktop application screenshots is a domain-specific object detection problem that differs fundamentally from general-purpose detection tasks. Form components exhibit high intra-class visual variance, strong inter-class similarity, and densely packed layouts — characteristics that make classical computer vision approaches insufficient for reliable automation. Existing deep learning solutions are predominantly trained on mobile GUI datasets, leaving the desktop RPA setting largely understudied, while no large-scale annotated dataset exists for this domain. This paper investigates whether a lightweight anchor-free detector, trained on a small purpose-built dataset, can overcome the limitations of classical approaches and achieve reliable real-time detection of UI form components within a complete end-to-end RPA pipeline driven by natural language instructions, without relying on DOM access or accessibility APIs.

Motivation. Vision-based RPA systems that operate without DOM access must rely entirely on visual inference to identify and interact with form components. Classical computer vision methods, while requiring no training, generalize poorly across the visual diversity of real-world desktop forms, degrading on complex layouts and visually ambiguous elements [1]. This gap motivates the design of a compact, domain-specific deep learning model capable of generalizing from a modest annotated dataset, while remaining compatible with real-time deployment constraints and integration into a fully operational natural language-driven RPA workflow.

Main result. We demonstrate that a lightweight anchor-free detector, fine-tuned on a small domain-specific dataset, consistently outperforms classical computer vision baselines on complex and visually diverse desktop form layouts, while meeting real-time inference constraints on standard desktop hardware without any access to the application's internal structure.

Methods / Applications.

- **Baseline:** We first establish a classical detection baseline using **OpenCV**, combining Canny edge detection and adaptive thresholding in OCR-guided label search zones, and systematically characterize its failure modes on complex desktop forms [1, 2].

- **Proposed approach:** We construct a **custom annotated dataset** of real desktop application screenshots covering six form component classes and fine-tune **YOLOX-S** [8], an anchor-free single-stage detector, selecting the Small variant for its favorable accuracy–speed trade-off under real-time constraints [3, 4].
- **Potential Impact:** Both approaches are integrated into a shared downstream pipeline combining OCR-based text extraction, fuzzy label matching, and spatial resolution, enabling natural language instructions to be compiled into executable automation scenarios for desktop RPA [5, 6, 7].

Acknowledgements. The author would like to express sincere gratitude to Professor **Noura Ouerdi** for her valuable guidance, continuous support, and insightful advice throughout the development of this research project. Special thanks are also extended to the **Faculty of Sciences at Mohammed First University (UMP)**, Oujda, for providing the academic environment and resources necessary to conduct this study.

References

[1] J. Chen, M. Xie, Z. Xing, C. Chen, X. Xu, L. Zhu, and G. Li, *Object Detection for Graphical User Interface: Old Fashioned or Deep Learning or a Combination?*, Proc. ESEC/FSE, ACM (2020), 1202–1214.

[2] M. Xie, S. Feng, Z. Xing, J. Chen, and C. Chen, *UIED: A Hybrid Tool for GUI Element Detection*, Proc. ESEC/FSE, ACM (2020), 1655–1659.

[3] S. Daneshvar and S. Wang, *GUI Element Detection Using SOTA YOLO Deep Learning Models*, arXiv:2408.03507 (2024).

[4] Z. Gao, *Improving GUI Element Detection with a Refined YOLO11-Based Approach*, Proc. EITCE 2025, ACM (2025).

[5] Y. Lu, J. Yang, Y. Shen, and A. Awadallah, *OmniParser for Pure Vision Based GUI Agent*, arXiv:2408.00203 (2024).

[6] M. Dicu and C. Chira, *Evaluating Deep Learning Models for Cross-Platform UI Component Detection*, Procedia Computer Science, 270 (2025), 2977–2986.

[7] R. Alghamdi, A. Ahmad, and F. Alsaadi, *Deep Learning-Based UI Design Analysis: Object Detection and Image Retrieval Using YOLOv8*, IJACSA, 16(4) (2025).

[8] Z. Ge, S. Liu, F. Wang, Z. Li, and J. Sun, *YOLOX: Exceeding YOLO Series in 2021*, arXiv:2107.08430 (2021).

Developing an AI-powered system for analyzing audio quality

Khadija BENAMAR[1], **Youssef DOUZI**[1], **Abderrahim ZANNOU**[2], **Hanae AL Kaddouri**[3]
[1] Laboratory of Arithmetic, Scientific Computing and Applications, Mohammed First University, Oujda, Morocco
[2] ERCI2A, FSTH, Abdelmalik Essadi University, Tetouan, Morocco
[3] Smart Information Communication and Technology Laboratory, Mohammed First University, Oujda, Morocco
khadija.benamar@ump.ac.ma

Abstract: In today's competitive business market, call centers play a key role in maintaining customer relationships and ensuring service quality. However, traditional call center workflow often involves manual, time-consuming processes to analyze customer interactions, leading to limited insights and missed opportunities. One of the richest and most underexplored sources of information in this context is voice recordings. Beyond spoken words, audio captures tone, emotion, hesitation, and intent, these are elements that are critical to understanding customer needs, therefore can drive innovative customer service strategies and improve agent performance. The proposed architecture integrates OpenAI Whisper for automatic speech recognition, MFCC-based speaker clustering for diarization, and Google Gemini for semantic and sentiment analysis to automate and enhance the evaluation of customer calls. By transforming audio data into actionable insights, the system aims to improve decision-making, enhance customer satisfaction through deeper understanding, and optimize agent training. The implementation of such a platform not only improves workflow efficiency but also allows businesses to unlock the full potential of their data by integrating it into a familiar and responsive information system. This alignment between data and digital infrastructure provides a strong foundation for continuous improvement, strategic planning, and sustainable growth.

Keywords: Speech Analytics; Audio Analysis; Sentiment Analysis; LLMs; Speaker Diarization

References

[1] H. Wu and M. Zhang, *Hierarchical cross-modal attention and dual audio pathways*, Sc. Reports (Nature), 2025.

[2] T. Rahman et al., *Comparative analysis of audio feature extraction tools*, Electronics, 9(3), 2025.

[3] L. Nguyen et al., *Sentiment analysis in the age of generative AI*, Journal of Big Data, 2024.

[4] R. Almeida and M. Costa, *Sentiment analysis using ML vs LLMs*, Machines, 2024.

[5] R. Sharma and N. Singh, *Optimized hybrid deep learning for sentiment*, Journal of Cloud Computing, 2025.

[6] A. Singh et al., *Advancing audio sentiment with diarization pipelines*, International Journal of Electrical and Electronics Engineering, 2025.

[7] A. Radford, J. W. Kim, T. Xu, G. Brockman, C. McLeavey, and I. Sutskever, *Robust speech recognition via large-scale weak supervision*, arXiv preprint arXiv:2212.04356, 2022.

[8] Z. Song, J. Zhuo, Y. Yang, Z. Ma, S. Zhang, and X. Chen, *LoRA-Whisper: Parameter-efficient and extensible multilingual ASR*, Interspeech, 2024.

[9] X. Liu et al., *Exploration of Whisper fine-tuning strategies for low-resource ASR*, EURASIP Journal on Audio, Speech, and Music Processing, 2024.

[10] C. Graham and N. Roll, *Evaluating OpenAI's Whisper ASR: Performance across diverse English accents*, JASA Express Letters, 2023.

Problèmes des Collisions dans les Blockchaines à Deux Dimensions

Salim BLOUNDI
Département de Mathématiques et Informatique, Ensam-Meknès, UMI, Meknès, Maroc
sbloundi@gmail.com

Saber Darmoun
Département de Mathématiques et Informatique, ENS, USMBA, Fès, Maroc
saber.darmoun@usmba.ac.ma

Khalid Abdelmoumen
Département de Mathématiques et Informatique, ENS, USMBA, Fès, Maroc
khalid.abdelmoumen@usmba.ac.ma

Hussain Ben-azza
Département de Génie Industriel et Productique, Ensam-Meknès, UMI, Meknès, Maroc
h.benazza@umi.ac.ma

Résumé. Pour augmenter le débit dans le cadre des blockchaines (style Bitcoin [1]), et aussi sans sacrifier la sécurité, nous proposons une approche géométrique sur les réseaux comme $\mathbb{Z}^2$. Le protocole D-BTC (Domino Bitcoin) organise les blocs (appelés B-domino), d'une blockchaine à deux dimensions L, comme un sous-ensemble simplement connexe du réseau $\mathbb{Z}^2$. La *frontière*

$$\partial L = \left\{ p \notin L \ : \ \exists\, q \in L,\ \|p - q\|_1 = 1 \ \text{ et } \ L \cup \{p\} \text{ simplement connexe} \right\}$$

satisfait, par l'inégalité isopérimétrique discrète, à $|\partial L| \geq O(\sqrt{n})$ pour les réseaux, où $n = |L|$. Cette croissance en $O(\sqrt{n})$ permet à $\Theta(\sqrt{n})$ mineurs de travailler en parallèle – contre 1 seul dans Bitcoin [1].

Avec M mineurs travaillant en parallèle, chacun doit sélectionner une position dans ∂L et effectuer une preuve de travail [6]. Sans coordination, deux mineurs peuvent choisir la même position, générant un travail gaspillé analogue au problème des anniversaires. Ce problème est distinct du consensus classique [7] car les mineurs n'ont pas besoin de s'accorder sur une valeur unique, mais de se répartir sur plusieurs positions valides.

Ce travail présente une analyse comparative entre deux méthodes : par hachage consistant, une stratégie déterministe de coordination des mineurs inspirée du *"consistent hashing"* [2] ; et une méthode appelée minage par affinité probabiliste, un cadre stochastique adaptatif fondé sur un noyau spatial Gaussien et une décroissance temporelle exponentielle. Les deux approches, construites sur le protocole D-BTC, visent le même objectif (réduire les collisions sur la frontière de la blockchaine 2D) mais diffèrent radicalement dans leur paradigme.

Nous montrons que les deux méthodes sont complémentaires – Le hachage consistant réduit le *coût* des collisions, alors que la méthode par affinité probabiliste réduit leur *fréquence* via la séparation géométrique des distributions – et proposons un plan d'intégration vers une blockchaine robuste.

Mots-clés: Blockchaine; Affinité probabiliste; Hachage consistant; Frontière; Collision; Sécurité; Débit, Bitcoin.

Références

[1] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available : https://bitcoin.org/bitcoin.pdf

[2] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, "Consistent Hashing and Random Trees : Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web," in *Proc. 29th Annual ACM STOC*, pp. 654–663, 1997.

[3] D. G. Thaler and C. V. Ravishankar, "Using Name-Based Mappings to Increase Hit Rates," *IEEE/ACM Trans. Networking*, vol. 6, no. 1, pp. 1–14, 1998.

[4] G. Grimmett, *Percolation*, 2nd ed., Grundlehren der math. Wissenschaften, vol. 321. Springer-Verlag, Berlin, 1999.

[5] A. Vince, "An Extremal Graph Problem on a Grid and an Isoperimetric Problem for Polyominoes," *Electron. J. Combin.*, vol. 31, no. 2, 2024.

[6] C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," in *Advances in Cryptology – CRYPTO '92*, LNCS vol. 740, pp. 139–147, Springer, 1992.

[7] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

A Real-Time Web-Based Platform for Human Activity Recognition Integrating WiFi CSI and Vision-Based Deep Learning

Hicham BOUDLAL
National School of Applied Sciences, Mohammed First University, Oujda, Morocco
hicham.boudlal5@gmail.com

Keywords: Human Activity Recognition, WiFi CSI, Deep Learning, Real-Time Monitoring, Dashboard Visualization, MATLAB-Python Integration, Smart Environments, Web-Based Platform

Abstract. Human Activity Recognition (HAR) is critical for healthcare, security, and smart environments, where continuous real-time monitoring is essential. This study presents a novel web-based platform that combines WiFi Channel State Information (CSI) analysis with vision-based deep learning to enable real-time, multi-modal human activity monitoring. The system employs MATLAB for CSI preprocessing, denoising, and feature extraction, while Python implements YOLOv8-based posture detection and MediaPipe skeleton extraction for precise visual tracking. A robust backend framework enables real-time communication with an interactive dashboard, providing synchronized visualization of CSI heatmaps, temporal signals, annotated images, skeletal representations, and immediate alerts via notifications and email. Experimental evaluation demonstrates the platform's high efficiency, accuracy, and low latency, enabling the monitoring of multiple activities in dynamic indoor environments. The results highlight the advantages of combining wireless sensing, computer vision, and web-based visualization within a modular, extensible architecture, offering a practical, scalable solution for healthcare, security, and ambient intelligence applications. Furthermore, this platform lays the groundwork for future integration with AI-based predictive analytics for proactive activity recognition and intervention.

References

[1] M. H. Arshad, M. Bilal, and A. Gani, "Human Activity Recognition: Review, Taxonomy and Open Challenges," *Sensors*, vol. 22, no. 17, p. 6463, Aug. 2022, doi: 10.3390/s22176463.

[2] N. Gupta, S. K. Gupta, R. K. Pathak, V. Jain, P. Rashidi, and J. S. Suri, "Human activity recognition in artificial intelligence framework: a narrative review," *Artif. Intell. Rev.*, vol. 55, no. 6, pp. 4755–4808, Aug. 2022, doi: 10.1007/s10462-021-10116-x.

[3] Z. Hussain, M. Sheng, and W. E. Zhang, "Different Approaches for Human Activity Recognition: A Survey," *J. Netw. Comput. Appl.*, vol. 167, p. 102738, Oct. 2020, doi: 10.1016/j.jnca.2020.102738.

[4] H. Jiang, C. Cai, X. Ma, Y. Yang, and J. Liu, "Smart Home Based on WiFi Sensing: A Survey," *IEEE Access*, vol. 6, pp. 13317–13325, 2018, doi: 10.1109/ACCESS.2018.2812887.

[5] H. Boudlal, M. Serrhini, and A. Tahiri, "A novel approach for simultaneous human activity recognition and pose estimation via skeleton-based leveraging WiFi CSI with YOLOv8 and MediaPipe frameworks," *Signal Image Video Process.*, Feb. 2024, doi: 10.1007/s11760-024-03031-5.

Recent Advances in Constructing Signatures from the Syndrome Decoding Problem

Sana CHALLI, **Taoufik Serraj** and **Moulay Chrif Ismaili**
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
sana.challi@ump.ac.ma

Abstract. After the initial call from the National Institute of Standards and Technology (NIST) for quantum-safe algorithms in 2016, NIST subsequently initiated another standardization effort, this time aiming for additional quantum-safe signatures from various areas, since the current selected ones rely mainly on lattices problems. The code-based signature schemes submitted in the first round can be categorized into two categories: (i) hash-and-sign schemes and (ii) zero-knowledge proof of knowledge (PoK) + Fiat-Shamir transform. The use of the hash-and-sign paradigm enjoys a very small signature size but suffers from a large public key size due to the hidden structure of the code, while schemes from the second category enjoy small public keys but quite large signatures compared to other schemes that rely on non-coding theory assumptions. In this (ongoing) work, we survey some schemes from these two categories that are mainly based on the Syndrome Decoding Problem (SDP) and its variants. Furthermore, we explore how the recent polynomial representation for SDP has significantly reduced the size of the signature.

References

[1] C. Aguilar Melchor, S. Bettaieb, L. Bidoux, T. Feneuil, P. Gaborit, N. Gama, S. Gueron, J. Howe, A. Hülsing, D. Joseph, A. Joux, M. Kulkarni, E. Persichetti, T. H. Randrianarisoa, M. Rivain, D. Yue, *Syndrome decoding in the head*, Submission to the NIST Post-Quantum Cryptography Standardization Process, Algorithm Specifications and Supporting Documentation, 2025.

[2] M. Baldi, M. Battaglioni, F. Chiaraluce, A. L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, *A new path to code-based signatures via identification schemes with restricted errors*, arXiv:2008.06403, 2020.

[3] M. Baldi, A. Barenghi, S. Bitzer, P. Karl, F. Manganiello, A. Pavoni, G. Pelosi, P. Santini, J. Schupp, F. Slaughter, et al., *Codes and Restricted Objects Signature Scheme*, Submission to the NIST Post-Quantum Cryptography Standardization Process, Algorithm Specifications and Supporting Documentation, 2025.

[4] G. Banegas, K. Carrier, A. Chailloux, A. Couvreur, T. Debris-Alazard, P. Gaborit, P. Karpman, J. Loyer, R. Niederhagen, N. Sendrier, B. Smith, J.-P. Tillich, *Wave: Round 1 Submission*, 2023.

[5] M. Battagliola, L. Mattiuz, A. Meneghetti, *VOLE-in-the-Head Signatures Based on the Linear Code Equivalence Problem*, Cryptology ePrint Archive, 2025.

[6] S. Bitzer, M. Battagliola, A. Wachter-Zeh, V. Weger, *TCitH- and VOLEitH-based Signatures from Restricted Decoding*, arXiv:2510.11224, 2026.

[7] R. Bricout, A. Chailloux, T. Debris-Alazard, M. Lequesne, *Ternary syndrome decoding with large weight*, in: Selected Areas in Cryptography — SAC 2019, 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers, pp. 437–466, Springer, Cham, 2020.

Revisited Partial Key Exposure Attack against RSA

Brahim CHNIOUNE
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
brahim.chnioune24@ump.ac.ma

Keywords: RSA ; Coppersmith's method ; LLL reduction algorithm ; Factorization ; Partial key exposure attack **MSC:** 94A60; 11T71

Abstract. Given an RSA modulus N, an encryption exponent e, and consider the corresponding secret exponent d. This paper presents a refined partial key exposure attack on RSA, combining Coppersmith's method with lattice-based reduction techniques. Assuming that a number of least significant bits of d are exposed, we recover the full secret exponent by solving the associated key equation $ed - k(p-1)(q-1) = 1$. The proposed method improves the bounds of existing partial exposure attacks in scenarios where d is small and a specific number of its least significant bits are known, thereby enabling full RSA primes recovery in polynomial time.

Motivation. More recently, Takayasu and Kunihiro proposed an attack on RSA based on unraveled linearization techniques, exploiting partial leakage of the secret exponent. Their method applies in scenarios where the decryption exponent d is small and a portion of its least significant bits (LSBs) is revealed. By leveraging this additional information, their attack enlarges the range of vulnerable private exponents to $d < N^{0.368}$.

In this work, we revisit the findings of Takayasu and Kunihiro by examining settings in which an adversary possesses partial, structured information about the decryption exponent d. .

Main result.

Theorem 0.40. *Let (N, e) denote an RSA public key with $N = pq$, where the primes satisfy $q < p < 2q$, and let $e = N^{\alpha}$. Consider a known positive integer $K = N^{\alpha_0}$. Suppose there exists an integer pair (k, d) such that $ed - k\varphi(N) = 1$, where $\varphi(N) = (p-1)(q-1)$, and assume that $d = Kd_1 + d_0$ for unknown d_1 and known d_0. Then the modulus N can be factored in polynomial time provided that $\alpha + \alpha_0 > \frac{1}{2}$ and $d < N^{\varrho}$, for some ϱ satisfying*

$$\varrho < \frac{7}{6} + \alpha_0 - \frac{1}{3}\sqrt{6\alpha + 6\alpha_0 + 1}.$$

Methods / Applications. Lattice Basis Reduction, Coppersmith technique.

Acknowledgements. The authors would like to thank the ACSA Laboratory at Université Mohammed Premier for the support provided during this research. We also express our gratitude to our colleagues for their insightful comments on the algebraic cryptanalysis of RSA-like schemes..

References

[1] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science **1592**, pp. 1–11,Springer, Berlin, Heidelberg, (1999).

[2] Boneh, D., Durfee, G., and Frankel, Y.. An attack on RSA given a small fraction of the private key bits. In Advances in Cryptology—ASIACRYPT'98: International Conference on the Theory and Application of Cryptology and Information Security Beijing, China, October 18–22, 1998 Proceedings (pp. 25-34). Springer Berlin Heidelberg (1998).

[3] Blomer, J., May, A.: New partial key exposure attacks on RSA. In Annual International Cryptology Conference (pp. 27-43). Berlin, Heidelberg: Springer Berlin Heidelberg (2003).

[4] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology,**10**(4), 233–260, (1997).

[5] Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In: IMA International Conference on Cryptography and Coding, LNCS 1355, pp. 131–142, Springer, Berlin, Heidelberg (1997).

[6] HPC-MARWAN, National Center for Scientific and Technical Research (CNRST), Rabat, Morocco. https://hpc.marwan.ma/index.php/en/.

[7] Jochemsz, E., May, A.: A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, In: ASIACRYPT 2006, LNCS 4284, pp. 267–282, Springer-Verlag (2006).

[8] Kocher, P. C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16 (pp. 104-113). Springer Berlin Heidelberg (1996).

[9] Kocher, P., Jaffe, J., and Jun, B. Differential power analysis. In Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19 (pp. 388-397). Springer Berlin Heidelberg (1999).

[10] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, **261**, pp. 513–534, (1982).

[11] May, A.: New RSA Vulnerabilities Using Lattice Reduction Methods. PhD thesis, University of Paderborn (2003).

[12] Nitaj, A.: Another generalization of Wiener's attack on RSA, In: Vaudenay, S. (Ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174–190. Springer, Heidelberg (2008)

[13] Rahmani, M., Nitaj, A., Ziane, M.: Further cryptanalysis of some variants of the RSA cryptosystem. Journal of Applied Mathematics and Computing, **71**(2), pp. 1911-1941, (2025).

A contribution to RSA security

Oumar DÈME
Electrical Engineering Department, École Supérieure Polytechnique (ESP) Cheikh Anta Diop University
BP: 15915 Dakar-Fann Senegal
deme.oumar@esp.sn

Keywords: algebra; number theory; applications

Abstract. Today, for confidentiality reasons, messages written in plain text between individuals or institutions are most often encrypted. Encryption techniques are accompanied by intensive research whose results will secure the encrypted messages that is, put them in the best possible position to protect them from attacks. Our work aims to contribute to the security of the cryptosystem RSA. For this reason, we have established a theorem whose application to certain RSA data gives the following result: Let $\phi(n)$ be the Euler indicator and (e, n) be a public key of RSA. If $\phi(n)^{-1} \mod e \leq \frac{e}{2}$ then any message block encrypted with (e, n) can be decrypted by a key strictly smaller than the private key RSA defined by $d = e^{-1} \mod \phi(n)$. However, the existence of keys smaller than the d key of RSA for decrypting messages increases the chances of success for a hacker in action. Therefore there is insecurity in using e and $\phi(n)$ which verify $\phi(n)^{-1} \mod (e) \leq \frac{e}{2}$. Let us note $CS(e, \phi(n))$, the inequality $\phi(n)^{-1} \mod (e) \leq \frac{e}{2}$. Our result can then be used to improve the security of the use of RSA at least two ways:

- verify that the pair $(e, \phi(n))$ currently in use for encryption and decryption according to RSA verifies or not the condition $CS(e, \phi(n))$. If yes, change the keys that are associated with them.
- ensure that the pair $(e, \phi(n))$ intended for generating new public and private keys for RSA do not verify the condition $CS(e, \phi(n))$.

Keywords: encryption, insecurity, RSA, private key, smaller keys.

A Systematic Review of Real-Time Multi-Human Tracking: From Correlation Filters to Transformers

Chaymae DKHISSI, Khadija LAAROUSSI
LARI Laboratory, Computer Science Department, Faculty of Sciences, Mohammed First University, Oujda Morocco
chaymae.dkhissi.m24@ump.ac.ma, kh.laaroussi@ump.ac.ma

Keywords: Multi-human tracking; Real-time tracking; Discriminative Correlation Filters (DCF); Siamese networks; Transformer-based tracking; Systematic literature review

Abstract. Multi-human tracking is a fundamental task in computer vision with applications in intelligent surveillance, robotics, and human–computer interaction. Its goal is to preserve the identities of multiple individuals across video frames despite challenges such as occlusion, illumination changes, and crowded scenes. Over time, several paradigms have been developed to address these issues. Discriminative Correlation Filters (DCF) offered high efficiency but limited robustness in complex environments. Siamese networks improved tracking through deep similarity learning, enabling more reliable person re-identification, while Transformer-based models recently advanced the field by capturing long-range and spatial–temporal dependencies. This paper presents a systematic review of recent state-of-the-art multi-human tracking methods. It provides a comparative analysis of three major paradigms—DCF-based, Siamese-based, and Transformer-based approaches—highlighting their main characteristics, strengths, limitations, and performance trade-offs. Current challenges and emerging trends are also discussed to provide a clearer overview of recent developments in real-time multi-human tracking.

Motivation. Although multi-human tracking has advanced significantly, the rapid emergence of diverse tracking paradigms has made comparative understanding increasingly challenging, particularly with respect to accuracy, robustness, and real-time performance.

Main results. The analysis indicates that DCF-based methods remain highly efficient but are generally sensitive to occlusion and background interference. Siamese-based approaches provide strong discriminative capabilities, although their adaptability over long tracking sequences may remain limited. Transformer-based models offer high accuracy and robustness by exploiting global contextual information, but they often involve significant computational cost. Overall, the review highlights the main trade-offs among these paradigms and points to emerging trends toward hybrid and context-aware tracking frameworks.

Methods / Applications. The study is based on a systematic analysis of recent literature, including a comparative examination of results reported on commonly used benchmarks. The findings provide insights into the suitability of different tracking paradigms for real-world applications such as video surveillance, autonomous systems, and smart city monitoring.

References

[1] Manzoor, S., An, Y. C., In, G. G., Zhang, Y., Kim, S., & Kuc, T. Y. (2023). SPT: Single pedestrian tracking framework with re-identification-based learning using the Siamese model. *Sensors, 23*(10), 4906. https://www.mdpi.com/1424-8220/23/10/4906

[2] Chen, P., Wang, L., Guo, L., Liu, X., Zhang, X., Jiao, L., & Liu, F. (2024). Satellite videos object tracking based on enhanced correlation filter with motion prediction network. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 17*, 12123–12137. https://doi.org/10.1109/JSTARS.2024.3421951

[3] Sun, D., Pan, Y., Lu, A., Li, C., & Luo, B. (2024). Transformer RGBT tracking with spatio-temporal multimodal tokens. *arXiv preprint arXiv:2401.01674*. https://arxiv.org/abs/2401.01674

On the Resilience of ASCON to Deep Learning–Based Side-Channel Analysis

Soufiane EL HALFA
LMA, Department of Mathematics, Faculty of Sciences, Mohammed Premier University, Oujda, Morocco
soufiane.elhalfa@gmail.com

Taoufik SERRAJ
Department of Mathematics, Faculty of Sciences, Mohammed Premier University, Oujda, Morocco
t.serraj@ump.ac.ma

Keywords: ASCON; Deep Learning (DL); Lightweight Cryptography (LWC); Side Channel Attacks (SCA) **MSC:** 94A60; 68T05

Abstract. In 2023, the National Institute of Standards and Technology (NIST) selected Ascon as the basis of its lightweight cryptography standard after a multi-round public evaluation process. Ascon is designed to provide efficient and secure cryptographic primitives for resource-constrained environments. Its standardized suite includes algorithms for Authenticated Encryption with Associated Data (AEAD), hashing, and eXtendable Output Functions (XOF). Based on a lightweight permutation-based design, Ascon offers a favorable trade-off between security, performance, and implementation cost, making it well suited for IoT devices [1].

Side-Channel Attacks (SCAs) are implementation attacks that exploit unintended information leakage arising during the execution of cryptographic operations. Unlike conventional cryptanalysis, which targets mathematical weaknesses in cryptographic constructions, SCAs infer secret data through the observation and analysis of side-channel information such as power consumption, execution timing, electromagnetic radiation, memory-access patterns, or acoustic signals [2].

In recent years, deep-learning-based side-channel analysis (DLSCA) has become a major research topic. By learning complex leakage features directly from measured traces, neural networks can significantly improve attack efficiency and may exploit weaknesses in imperfectly protected implementations, including poorly tuned masking or hiding countermeasures [3]. In this paper, we investigate the side-channel vulnerabilities of the new standardized Ascon family under deep-learning-based attacks, and we discuss methods for evaluating and improving implementation security in this context.

References

[1] Turan, M. S., McKay, K., Chang, D., Kang, J., & Kelsey, J. (2024). *Ascon-based lightweight cryptography standards for constrained devices.* In NIST Special Publication (SP) NIST SP 800–232 ipd. National Institute of Standards and Technology.

[2] Kaur, J., Cintas Canto, A., Mozaffari Kermani, M., & Azarderakhsh, R. (2025). *A survey on the implementations, attacks, and countermeasures of the nist lightweight cryptography standard: Ascon.* ACM Computing Surveys, 58(1), 1-16.

[3] Rezaeezade, A., Basurto-Becerra, A., Weissbart, L., & Perin, G. (2024, March). *One for all, all for ascon: Ensemble-based deep learning side-channel analysis.* In International Conference on Applied Cryptography and Network Security (pp. 139-157). Cham: Springer Nature Switzerland.

Trustworthy AI for Electronic Health Records: A Critical Review of Federated Learning, Explainability, and Cybersecurity Risks

Hajiba IFRAH
ENSAO, Mohammed Premier University, Oujda, Morocco
ifrah.hajiba@ump.ac.ma

Keywords: electronic health records; trustworthy AI; federated learning; explainable AI; cybersecurity; privacy preservation.

Abstract. The accelerated digitization of medical care has transformed electronic medical records into vital resources for training artificial intelligence (AI) systems capable of predicting the progression of diseases, aiding in medical decision-making, and accurately assessing the risks faced by patients. However, traditional centralized learning architectures pose serious issues: the confidentiality of sensitive data is at risk, compliance with stringent data protection regulations (such as GDPR and HIPAA) is complicated, and advanced AI models, often labeled as "black boxes," lack interpretability and transparency. In clinical practice, where patient safety is paramount, this lack of clarity leads to resistance from the medical community. In this critical review, we will examine the promising intersection of three key areas: federated learning, explainable artificial intelligence (XAI), and cybersecurity. We will investigate the potential of federated learning as a paradigm that enables collaborative training of predictive models without the need to export or directly exchange raw data. However, this approach is not without its challenges, which we will further explore. We will identify various vulnerabilities, ranging from the risks of malicious model poisoning to inference threats, as well as the difficulties posed by data heterogeneity across different institutions. Moreover, we will evaluate the role of explainable artificial intelligence techniques in boosting clinical confidence, facilitating human validation, and enhancing transparency in decisions derived from electronic health record (EHR)-based models. While post-hoc explanations and feature attribution methods have gained popularity, their integration into distributed and privacy-respecting medical learning frameworks remains limited, primarily due to concerns over data privacy, implementation complexity, and the need for standardized evaluation metrics, which hinder the effective application of these techniques in real-world clinical settings. This article argues that explainability should not be considered an optional enhancement but rather as a fundamental necessity for the safe and responsible deployment of healthcare AI. This review aims to pave the way for the development of more reliable, explainable, and resilient medical AI systems capable of meeting the increasing demands of digital health environments.

Motivation. The integration of artificial intelligence (AI) into clinical workflows cannot be reduced to a mere race for predictive performance. For the medical community to truly embrace these technologies, deployed systems must meet three fundamental requirements: proven robustness against variation and bias, sufficient transparency for external audits, and a robust guarantee of confidentiality for medical information. In this context, Trustworthy emerges as the

central organizing principle of IA applied to digital health data [1]. This analysis underscores the urgent need to move beyond the traditional separation between explainability [2], confidentiality, and cybersecurity, often considered distinct areas of study. We argue that classifying an AI system used for electronic health records as reliable requires an integrative architecture where these three dimensions are functionally interdependent.

Scope of the review. This paper reviews recent work on federated learning in healthcare, explainable AI for clinical decision support, and cybersecurity threats affecting distributed medical AI. The goal is to provide an integrated perspective rather than isolated discussions of each topic.

Main contribution. This review makes the following contributions:
1. it provides a critical synthesis of federated learning approaches for EHR-based analytics;
2. it examines the role and limitations of explainable AI in clinical environments;
3. it analyzes major cybersecurity and privacy threats affecting distributed medical AI systems;
4. it proposes future research directions toward trustworthy AI for digital health.

Methods / Applications. The paper follows a thematic review approach, organizing the literature around privacy-preserving collaboration, explainability, and cyber resilience. The resulting synthesis is relevant for researchers in artificial intelligence, cybersecurity, health informatics, and digital medicine, as well as for healthcare institutions seeking secure deployment strategies for data-driven clinical systems.

References

[1] J. Amann, A. Blasimme, E. Vayena, D. Frey, and V. I. Madai, *Explainability for artificial intelligence in healthcare: a multidisciplinary perspective,* BMC Medical Informatics and Decision Making, vol. 20, no. 1, pp. 1-9, 2020.

[2] D. Gunning and D. A. Aha, *DARPA's Explainable Artificial Intelligence (XAI) Program,* AI Magazine, vol. 40, no. 2, pp. 44-58, 2019.

A Cross-Tier Review of Attacks and Targeted Security Solutions in Medical WBANs

Khaoula Itro, Nabila Azdad, Mohammed Amine Kasmi
LARI Laboratory, Faculty of Sciences (FSO), Mohammed First University (UMP), Oujda, Morocco
khaoula.itro@ump.ac.ma

Keywords: Wireless Body Area Networks; medical WBANs; security ; attack; lightweight protection

Abstract. Wireless Body Area Networks (WBANs) are increasingly used in healthcare monitoring due to their ability to support continuous and real-time acquisition of physiological data through wearable and implantable devices. Despite their medical relevance, these systems remain exposed to multiple security threats affecting confidentiality, integrity, authentication, privacy, and service continuity. The problem becomes more critical in medical environments because WBAN devices are constrained in terms of energy, memory, computation, and communication delay. Recent literature also shows that WBAN security is addressed through fragmented directions involving lightweight authentication, anomaly detection, secure data collection, and AI-assisted eHealth protection.

Motivation. A significant part of the recent literature studies WBAN security through isolated perspectives. However, there is still a need for a structured review that classifies attacks according to the architectural layers of medical WBANs and links them to the security solutions specifically targeted in the literature.

Main contribution. This review provides a cross-tier perspective on security in medical WBANs by classifying attacks according to the sensor, gateway or edge, and backend layers. It also maps the main security solutions reported in the literature, including lightweight authentication, anomaly detection, secure data collection, and AI-assisted protection.

Methods / Applications. This paper presents a focused review of recent advances in medical WBAN security and identifies the association between attack location, security objectives, and the corresponding security solutions reported in the literature. This perspective is particularly relevant to applications such as remote patient monitoring, intelligent medical sensing, and resource-constrained healthcare environments.

References

References

[1] Jian, W., Tabassum, A., & Li, J. P. (2024). *Systematic survey on data security in wireless body area networks in IoT healthcare system*. Frontiers in Medicine, 11, 1422911.

[2] Attir, A., Naït-Abdesselam, F., & Faraoun, K. M. (2023). *Lightweight anonymous and mutual authentication scheme for wireless body area networks*. Computer Networks, 224, 109625.

[3] Islam, M. M., & Shamshuzzoha, M. (2025). *Securing wireless body area networks data transmission with machine learning: A cross-tier framework for anomaly detection and intrusion prevention*. Computational and Structural Biotechnology Reports, 2, 100031.

[4] Subramani, J., Azees, M., Rajasekaran, A. S., Aljaedi, A., Bassfar, Z., & Jamal, S. S. (2024). *Blockchain-enabled secure data collection scheme for fog-based WBAN*. IEEE Access, 12, 38287–38297.

[5] Humayun, M., Alsirhani, A., Alserhani, F., Shaheen, M., & Alwakid, G. (2024). *Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency*. Journal of Cloud Computing, 13, 37.

Interpretable Artificial Intelligence Models for Predicting Irrigation Water Suitability

Ouafae KAIBI [1*], **My Hachem AOURAGH** [1], **Abdelhadi EL OUALI**[1],**Ali ESSAHLAOUI** [1],**Abdellah El-HMAIDI** [1]

[1] Department of Geology, Faculty of Sciences, Meknes, Morocco
Moulay Ismail University

***Corresponding Author** E-mail: kaibi.w77@gmail.com

Keywords: Interpretable AI; ML; SHAP; Irrigation water suitability **MSC:** 68T05; 62J02

Abstract. This study investigates the use of supervised machine learning models for predicting irrigation water index based on physicochemical parameters. Several regression algorithms were evaluated, including linear regression, support vector regression, random forests, and gradient boosting. Among them, the XGBoost model achieved the highest predictive performance ($R^2 = 0.95$). To ensure model transparency, SHapley Additive exPlanations (SHAP) were employed to quantify the contribution of each input variable to the final prediction. The proposed framework demonstrates that high predictive accuracy can be achieved while maintaining interpretability, which is essential for reliable decision support.

Motivation. Classical irrigation water quality indices rely on fixed thresholds and may fail to capture complex nonlinear relationships between variables. Machine learning models provide flexible approximation capabilities, but their black-box nature often limits practical adoption. The objective of this work is to develop a regression framework that combines predictive strength with interpretable feature attribution.

Main result. The gradient boosting model (XGBoost) outperformed other evaluated methods in terms of predictive accuracy and robustness. SHAP analysis revealed that sodium and salinity-related indicators were the most influential features in determining irrigation suitability, providing clear and quantifiable insight into model behavior.

Methods / Applications. The models were trained using supervised learning with k-fold cross-validation to ensure stability and generalization. Gradient boosting constructs predictions through an ensemble of regression trees optimized via empirical risk minimization. Model interpretability was achieved through SHAP-based additive explanations, allowing consistent and locally accurate attribution of feature importance. The proposed approach can be generalized to other regression problems requiring both accuracy and transparency.

References

[1] L. Breiman, Random Forests, Machine Learning, 45(1), 5–32, 2001.

[2] T. Chen and C. Guestrin, XGBoost: A Scalable Tree Boosting System, Proc. 22nd ACM SIGKDD, 2016.

[3] H. Drucker, C. J. C. Burges, L. Kaufman, A. Smola, and V. Vapnik, Support Vector Regression Machines, Advances in Neural Information Processing Systems, 1997.

[4] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, Springer, 2009.

[5] S. M. Lundberg and S.-I. Lee, A Unified Approach to Interpreting Model Predictions, NeurIPS, 2017.

[6] L. S. Shapley, A Value for n-Person Games, Contributions to the Theory of Games, 1953.

A Novel CRT Legendre S-box Construction for Lightweight Encryption

Chaymae KADDOURI, El Wardani DADI and Ahmed BOUJRAF
LSA Laboratory, Abdelmalek Essaadi University, ENSAH, Al-Hoceima, Morocco
chaymae.kaddouri1@etu.uae.ac.ma

Keywords: Lightweight cryptography; S-box construction; Chinese Remainder Theorem (CRT); Legendre symbol; Nonlinearity; Differential uniformity; IoT security; Affine transformation.

Abstract. Substitution boxes (S-boxes) represent one of the fundamental nonlinear components in modern symmetric cryptographic systems. The design of lightweight and secure S-boxes has become important with the development of Internet of Things (IoT). In this paper, a novel lightweight key-dependent S-box construction method based on number theory is proposed. The proposed approach combines the Chinese Remainder Theorem (CRT), Legendre-symbol-based nonlinear perturbation, and affine transformation to generate highly nonlinear substitution mappings with low computational complexity. The construction relies on two parallel modular nonlinear functions defined over distinct prime fields. The generated outputs are fused using the CRT mechanism, producing a compact and dynamic substitution structure. To further improve the cryptographic strength, a lightweight affine transformation is applied to enhance diffusion and confusion properties. Unlike conventional S-box constructions based on finite-field inversion or chaotic systems, the proposed method utilizes modular arithmetic and quadratic residue properties, making it more suitable for lightweight cryptographic environments. The security analysis demonstrates that the proposed S-box achieves strong cryptographic characteristics, including high nonlinearity, low differential uniformity, good avalanche behavior, and satisfactory resistance against linear and differential cryptanalysis. In addition, the implementation analysis indicates that the proposed design requires low memory usage and reduced computational overhead, making it appropriate for constrained hardware platforms. The obtained results show that the proposed CRTLegendre S-box provides an efficient balance between security and lightweight implementation requirements for next-generation embedded security applications.

Motivation. The rapid growth of IoT and embedded systems has increased the demand for lightweight cryptographic components capable of providing strong security with low computational and hardware complexity. This challenge motivates the design of a novel number-theory-based S-box that combines efficiency, low memory consumption, and strong resistance against cryptographic attacks.

Main result. Proposition.

Let p_1 and p_2 be two distinct odd prime numbers, and let k be a secret key parameter. For each input $x \in \{0, 1, \ldots, 2^n - 1\}$, define two modular nonlinear functions:

$$f_1(x, k) = x^2 + a_1 x + b_1 + \chi_{p_1}(x + k) \pmod{p_1}$$

$$f_2(x,k) = x^3 + a_2x + b_2 + \chi_{p_2}(x+k) \pmod{p_2}$$

where χ_{p_i} denotes the Legendre symbol modulo p_i, and a_i, b_i are constant parameters.

The two outputs $f_1(x,k)$ and $f_2(x,k)$ are then combined using the Chinese Remainder Theorem:

$$Y = \mathrm{CRT}(f_1(x,k), f_2(x,k))$$

Finally, the value Y is reduced to n bits and transformed using an affine mapping:

$$S_k(x) = A(Y \bmod 2^n) \oplus c$$

where A is an invertible binary matrix and c is a constant vector.

Therefore, the function S_k defines a key-dependent lightweight S-box. The use of two prime modular spaces increases confusion, the Legendre symbol introduces nonlinear perturbation, the CRT combines both modular outputs into a single structure, and the affine transformation improves diffusion. If the selected parameters produce a bijective mapping, then S_k can be considered a suitable candidate for lightweight symmetric cryptographic applications.

Theorem 0.41. *Let p_1 and p_2 be two distinct odd prime numbers, and let $f_1(x,k)$ and $f_2(x,k)$ be two nonlinear modular mappings defined by*

$$f_1(x,k) = x^2 + a_1x + b_1 + \chi_{p_1}(x+k) \pmod{p_1}$$

and

$$f_2(x,k) = x^3 + a_2x + b_2 + \chi_{p_2}(x+k) \pmod{p_2}$$

where χ_{p_i} denotes the Legendre symbol modulo p_i, and a_i, b_i, k are fixed parameters. Assume that:

1. *the mappings f_1 and f_2 are nonconstant over their respective prime fields,*
2. *the CRT combination*

$$Y = \mathrm{CRT}(f_1(x,k), f_2(x,k))$$

produces distinct outputs for distinct inputs,

3. *the affine transformation*

$$S_k(x) = A(Y \bmod 2^n) \oplus c$$

uses an invertible binary matrix A.

Then the resulting mapping S_k is bijective and defines a valid key-dependent lightweight S-box.

Furthermore, the nonlinear perturbation introduced by the Legendre symbol together with the dual-prime CRT fusion increases the algebraic complexity and confusion properties of the generated substitution box, thereby improving its resistance against linear and differential cryptanalysis.

Methods / Applications. The proposed construction combines several number-theoretic techniques, including modular polynomial mappings, Legendre-symbol nonlinear perturbation, Chinese Remainder Theorem (CRT) fusion, and affine transformation, to generate a lightweight key-dependent S-box with strong cryptographic properties. The proposed approach has potential applications in lightweight block ciphers, IoT security, wireless sensor networks, RFID systems, and embedded cryptographic devices, where low computational complexity and high security are both required.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer, 2002.

[3] A. Biryukov and L. Perrin, "On Lightweight S-boxes and Their Cryptographic Properties," *IACR Cryptology ePrint Archive*, pp. 1–20, 2017.

[4] A. Winterhof and A. Shparlinski, "On the Use of the Legendre Symbol in Symmetric Cryptography," *Lecture Notes in Computer Science*, Springer, vol. 3574, pp. 324–339, 2005.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, 1990.

[6] M. Hell, T. Johansson, and W. Meier, "Grain: A Stream Cipher for Constrained Environments," *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 86–93, 2007.

[7] A. Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a Pervasive World," PhD Thesis, Ruhr University Bochum, Germany, 2009.

[8] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer, 1993.

[9] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," *Advances in Cryptology – EUROCRYPT*, Lecture Notes in Computer Science, vol. 765, pp. 386–397, 1994.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

MECGDSA and Hash-MECDSA: Novel Multi-Curve Signature Schemes for Efficient and Secure Blockchain Applications

Samir Kourtite
Département de Mathématiques, Faculté des Sciences, Université Mohammed Premier, Oujda, Morocco
samirkourtite@gmail.com
Joint work with: M. Ziane

Keywords: Blockchain Security; Multi-Curve Cryptography; Digital Signatures; MECGDSA; Hash-MECDSA; Elliptic Curve Cryptography (ECC).

Abstract. Cryptocurrencies, digital assets designed as mediums of exchange, rely on strong cryptography to secure transactions and verify asset transfers within blockchain systems, predominantly using the Elliptic Curve Digital Signature Algorithm (ECDSA). While ECDSA ensures robust security, its single-curve approach and computational overhead limit efficiency in multi-party settings. This paper proposes two advanced multi-elliptic curve digital signature schemes: MECGDSA and Hash-MECDSA. MECGDSA enhances signing efficiency by eliminating modular inverses, leveraging multiple elliptic curves tailored to performance needs. Hash-MECDSA introduces hash-based aggregation to produce compact signatures, improving security and scalability across t curves. Security analysis demonstrates that both schemes resist forgery under the random oracle model, while computational evaluation reveals MECGDSA reduces signing time and Hash-MECDSA minimizes signature size compared to existing multi-curve schemes like MECDSA. For optimal security and efficiency in blockchain systems, we recommend integrating these schemes with two or more elliptic curves. These enhancements offer a versatile framework for next-generation cryptographic applications.

References

[1] Miller, V.S.: Use of Elliptic Curves in Cryptography. In: Advances in Cryptology - CRYPTO '85, pp. 417–426. Springer, Heidelberg (1985)

[2] Koblitz, N.: Elliptic Curve Cryptosystems. Mathematics of Computation **48**(177), 203–209 (1987)

[3] NIST: Digital Signature Standard (DSS). FIPS PUB 186-4, National Institute of Standards and Technology (2013). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[4] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper (2008)

[5] Leng, J., Zhou, M., Zhao, J.L., Huang, Y., Bian, Y.: Blockchain Security: A Survey of Techniques and Research Directions. IEEE Transactions on Services Computing **15**(4), 2490–2510 (2020)

[6] Pointcheval, D., Stern, J.: Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology **13**(3), 361–396 (2000)

[7] Hankerson, D., Vanstone, S., Menezes, A.: Guide to Elliptic Curve Cryptography. Springer, New York (2004)

[8] Bi, Wei., Jia, X., Zheng, M.: A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain. arXiv preprint arXiv:1808.02988 (2018)

[9] Liu, S.G., Chen, W.Q., Liu, J.L.: An Efficient Double Parameter Elliptic Curve Digital Signature Algorithm for Blockchain. IEEE Access **9**, 77058–77066 (2021)

[10] Schnorr, C.P.: Efficient Signature Generation by Smart Cards. Journal of Cryptology **4**(3), 161–174 (1991)

[11] Gennaro, R., Goldfeder, S.: Fast Multiparty Threshold ECDSA with Fast Trustless Setup. In: Proc. ACM SIGSAC Conference on Computer and Communications Security, pp. 1179–1194 (2018)

[12] BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.1. Federal Office for Information Security (2018). https://www.bsi.bund.de

[13] Bernstein, D.J.: Curve25519: New Diffie-Hellman Speed Records. Public Key Cryptography - PKC 2006, pp. 207–228. Springer (2006)

[14] Pornin, T.: Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). RFC 6979, IETF (2013)

[15] Bernstein, D.J., Lange, T., Niederhagen, R.: Dual EC: A Standardized Back Door. In: The New Codebreakers, pp. 256–281. Springer (2016)

An Efficient Polynomial Multiplication Method over polynomial ring R

El Hassane LAAJI
SupMTI and UMP Oujda, Morocco
e.laaji@ump.ac.ma

Abdelmalek AZIZI
SupMTI and UMP Oujda, Morocco
a.azizi@ump.ac.ma

Keywords: Post-quantum cryptography, Polynomial multiplication, Lattice-based cryptography

Abstract. In this work, we propose an optimized approach for binary polynomial multiplication when multiplying polynomials defined over different rings. Let $X \in R_q = \mathbb{Z}_q[x]/(x^N + 1)$ and $Y \in R_2 = \mathbb{Z}_2[x]/(x^N + 1)$, and consider the computation of $Z = X \cdot Y \pmod 2$. We observe that only the parity of the coefficients of X influences the result modulo 2.

Based on this observation, we transform X into a binary polynomial V by extracting the least significant bit of each coefficient:

$$V_i = X_i \ \& \ 1, \quad \text{for } i = 0, \ldots, N.$$

The multiplication is then performed in the binary ring:

$$W = V \cdot Y \pmod 2.$$

Since both V and Y belong to R_2, the computation relies solely on lightweight bitwise operations (XOR and AND), eliminating the need for arithmetic over $\mathbb{Z}_q$. Consequently, $Z = W$, yielding the same result as the original computation with reduced complexity. Table 1 presents the experimental results of the proposed method, which significantly reduces computational cost, achieving performance gains of up to 40–50 % depending on the parameter set.

Method / Params (N, q)	**(256,2049)**	**(512,4097)**	**(1024,12289)**	**(2048,65537)**
Convolution	0.23 ms	0.89 ms	3.80 ms	18.40 ms
BitsMultiply	0.14 ms	0.47 ms	2.20 ms	8.90 ms
Reduction cost	40%	47%	42%	51%

Table 1: Performance comparison between classical convolution and the proposed *BitsMultiply* method

Since this method is recent and has not yet been implemented in existing cryptosystems, its security implications remain to be fully explored. This work is presented as a preliminary contribution, and we welcome feedback, critique, and collaboration from the cryptographic community, especially for implementation and comparative security analysis with classical convolution-based approaches. **Note:** Experiments were conducted on a PC with an Intel i7-2630QM, 8 GB RAM, using Java on Windows 7.

References

[1] EL H. Laaji, A. Azizi, "New Efficient and Robust NTRU post-quantum key Exchange-NTRUrobust", Journal of Theoretical and Applied Technology, Mohammed First University, Morocco, 2020.

[2] G. Alagic et al., "Status Report NISTIR 8240 on the First Round of the NIST Post-Quantum Cryptography Standardization Process," NIST, USA, 2019.

[3] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*. Springer, 1998, pp. 267–288.

[4] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Springer, 2002.

A Structural Theory of the Equivalent Local Sequence Problem and Its Cryptographic Implications

Zhour OUMAZOUZ
FST Mohammedia, Hassan II University, Morocco
oumazouzzhour@gmail.com

Abstract. The Equivalent Local Sequence Problem (ELSP) consists in recovering a sequence of local complementations between two locally equivalent graphs. While local equivalence can be decided in polynomial time, the complexity of this inversion problem depends on the structural properties of the graph family.

We analyze ELSP through the framework of group actions and algebraic graph theory. In structured settings, such as undirected graphs and directed Paley graphs, the problem admits polynomial-time solutions. In the former case, tractability follows from algebraic representations related to isotropic systems, whereas in the latter it arises from a commutative action reducing the problem to linear algebra over $\mathbb{F}_2$.

We introduce a structural classification based on commutativity, stabilizers, orbit size, and algebraic symmetry. This reveals a clear distinction between tractable families and general directed graphs, where non-commutativity and the lack of a global algebraic description suggest higher computational complexity.

We also highlight implications for graph-based cryptography: structured families are unsuitable for hardness assumptions, while non-commutative graph families provide more promising directions.

Keywords: local complementation; Paley graphs; group actions; ELSP; graph-based cryptography
MSC: 05C25; 05C50; 11T06; 94A60

References

[1] A. Bouchet, *Isotropic systems*, European Journal of Combinatorics **8** (1987), no. 3, 231–244.

[2] A. Bouchet, *Recognizing locally equivalent graphs*, Discrete Mathematics **114** (1993), no. 1–3, 75–86.

[3] A. Bouchet, *Maps and delta-matroids*, Discrete Mathematics **78** (1989), 59–71.

[4] R. Arratia, B. Bollobás, and G. B. Sorkin, *The interlace polynomial of a graph*, Journal of Combinatorial Theory, Series B **92** (2004), no. 2, 199–233.

[5] M. Van den Nest, J. Dehaene, and B. De Moor, *Graphical description of the action of local Clifford transformations on graph states*, Physical Review A **69** (2004), 022316.

[6] R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics **12** (1933), 311–320.

[7] C. Godsil and G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, vol. 207, Springer, 2001.

[8] Z. Oumazouz, *Novel public-key cryptosystem based on the problem of performing a sequence of local complementations on Paley graphs*, Int. J. of Math. and Comp. Sci. **17** (2022), no. 3, 1451–1461.

[9] Z. Oumazouz, *A proposed public-key cryptosystem constructed using Paley graphs*, International Journal of Mathematics and Computer Science **20** (2025), no. 2, 465–468.

[10] Z. Oumazouz, *On the classification of graphs induced by sequences of local complementations of Paley graphs*, Journal of Combinatorial Mathematics and Combinatorial Computing **126** (2025), 29–72.

[11] Z. Oumazouz, *An algebraic resolution of the Equivalent Local Sequence Problem via group actions in directed Paley graphs*, Journal of Combinatorial Mathematics and Combinatorial Computing **130** (2026), 165–185.

[12] Z. Oumazouz, *A constructive resolution of the Equivalent Local Sequence Problem via isotropic systems and normal matrices with applications to Paley undirected graphs*, J. of Comb. Math. and Comb. Comp., to appear.

An Improved Attack on Some Algebraic RSA Variants

Mohammed RAHMANI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
mohammed.rahmani@ump.ac.ma

Keywords: LLL algorithm, Lattice basis reduction, Coppersmith's method **MSC:** 94A60; 11T71

Abstract. At NordSec 2023, Cotan and Teşeleanu introduced a variant of the RSA cryptosystem in which the modulus $N = pq$ is formed from primes of equal bit-length, and the exponents e and d satisfy

$$ed - 1 \equiv 0 \pmod{(p^n - 1)(q^n - 1)}.$$

In this work, we propose a new cryptanalytic attack on this construction in the case where the difference between the primes is sufficiently small. Our approach relies on Coppersmith's method combined with lattice basis reduction techniques, enabling the recovery of the prime factors in polynomial time. In addition, we derive improved bounds for small private exponent attacks when the primes share a portion of their most significant bits.

Motivation. The optimal bound for small secret exponent attacks against such schemes is given by $d < N^{0.292n}$ for all integers $n \geq 1$, as established in [5]. However, this bound is difficult to achieve in practical settings. In this work, we show that when the primes share a sufficient portion of their least significant bits, it is possible to recover the secret exponent even when $d > N^{0.292n}$.

Main result.

Theorem 0.42. *Let $N = pq$ be an RSA modulus, where p and q are primes of equal bit-length satisfying $|p - q| < N^{\sigma}$ for some $\sigma \leq \frac{1}{2}$. Suppose there exist positive integers k and d such that*

$$ed - 1 = k\,\phi_n(N), \quad \text{where} \quad \phi_n(N) = (p^n - 1)(q^n - 1),$$

with $e = N^{\theta}$ and $d = N^{\delta}$. If

$$\theta \leq \frac{n-1}{\sigma}, \qquad \delta < n - \sqrt{\theta\sigma n},$$

then the prime factors of N can be recovered in polynomial time.

Methods / Applications. LLL algorithm, Groebner basis computation

References

[1] Rivest, R., Shamir, A., Adleman, L.: *A Method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, **21**(2), pp. 120–126, 1978.

[2] Boneh, D., Durfee, G.: *Cryptanalysis of RSA with private key d less than $N^{0.292}$*, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science 1592,

[3] Cotan, P., Teşeleanu, G.: *Small private key attack against a family of RSA-like cryptosystems*. In: Nordic Conference on Secure IT Systems 2023. Lecture Notes in Computer Science, pp. 57–72, 2023.

[4] Coppersmith, D.: *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*. Journal of Cryptology, 10(4), 233–260, 1997.

[5] Teşeleanu, G.: *A lattice attack against a family of RSA-like cryptosystems*, Cryptology ePrint Archive, (2024).

More on algebraic partial exposure exploitation on HAWK

Nour-eddine RAHMANI
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
nour-eddine.rahmani@ump.ac.ma

Taoufik SERRAJ
Department of Mathematics, Faculty of Sciences, Mohammed I University, Oujda, Morocco
t.serraj@ump.ac.ma

Keywords: algebra; number theory; applications, Cryptography; Post-quantum;
MSC: 11R52; 11Y16; 94A60

Abstract. We investigate the resilience of the HAWK post-quantum signature scheme against partial information leakage. HAWK, built on the module variant of the Lattice Isomorphism Problem, relies on secret vectors closely tied to the private basis during signing. We show that revealing a single algebraic coefficient of a secret vector is sufficient to recover the full signing key in polynomial time relative to the degree of the underlying cyclotomic field. Our key-recovery method exploits algebraic relationships between the secret basis, the public Gram matrix, and the preimage vector, translating leaked information into congruence constraints that are solved via structured lattice decoding using Kannan's embedding and lattice reduction. These results emphasize the critical need to secure HAWK's signing procedure against side-channel attacks and inform the design of leakage-resistant lattice-based signatures.

Motivation. The HAWK signature scheme [1] is a post-quantum signature construction based on the module variant of the Lattice Isomorphism Problem. Understanding the impact of partial leakage in lattice-based signature schemes is essential for evaluating their resistance against side-channel attacks. In HAWK, the signing procedure involves secret vectors whose algebraic structure is closely tied to the private basis. This raises the question of how much information about these vectors must leak before the entire signing key becomes recoverable.

Main result. We formalize the key-recovery mechanism obtained from partial leakage.

Theorem 0.43. *Let B be the secret signing key of the HAWK signature scheme and let x denote a secret vector involved in the signing procedure. If one algebraic coefficient of x is revealed, then the full signing key B can be recovered in polynomial time in the degree of the underlying cyclotomic number field.*

Methods / Applications. The recovery method relies on algebraic relations between the secret basis and the public Gram matrix $Q = B^\star B$ and $w = B^{-1}x$, which lead to a system of congruence constraints linking the leaked coefficient to the remaining secret components. The resulting reconstruction problem is then reduced to a structured lattice decoding instance solved using Kannan's embedding technique together with lattice reduction. Our analysis highlights the importance of protecting the signing procedure of HAWK against side-channel leakage.

References

[1] L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. van Woerden, *Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple*, in: Advances in Cryptology – ASIACRYPT 2022, Lecture Notes in Computer Science, vol. 13794, Springer, 2022, pp. 65–94.

[2] N.-E. Rahmani, T. Serraj, and M. C. Ismaili, *An Algebraic Key-Exposure Attack on the Digital Signature HAWK*, Gulf Journal of Mathematics, vol. 19, no. 2, 2025, pp. 384–397. doi:10.56947/gjom.v19i2.2778.

[3] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen **261** (1982), 515–534.

[4] R. Kannan, *Minkowski's Convex Body Theorem and Integer Programming*, Mathematics of Operations Research **12** (1987), 415–440.

An AI-Based Agent for Real-Time Detection of Random Fault Attacks on Elliptic Curve Cryptosystems

Nour el houda RAHMANI , Taoufik SERRAJ
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
nourelhouda.rahmani.m23@ump.ac.ma

Keywords: elliptic curve cryptography; random fault attack; BrainpoolP256r1; machine learning; side-channel attack; **MSC:** 94A60; 68T01

Abstract.

Fault analysis attacks (FAAs) are a significant category of side-channel attacks in which an attacker attempts to obtain secret information such as cryptographic keys by physically compromising a device. In the case of elliptic curve cryptography, the basic principle of the side-channel attack, which is based on the work of Biehl et al. [2] and further developed by Serraj *et al.* [5, 6], is based on the following basic principle: if a random fault is injected into the coordinates of a point on an elliptic curve, it is possible to effectively change the curve. In other words, a parameter of the elliptic curve (b) is replaced by another value (b'). The device is made to unknowingly calculate on a different and weaker curve. Since this parameter is not actually required for any of the main computation steps, the device will continue to operate normally without any signs of an attack. The attack will remain undetected while the device is being compromised by performing the required operations on a different curve. If the new curve is such that it is easier to analyze, it is possible for an attacker to take advantage of this weakness and obtain secret information efficiently. In this work, we propose a simulation framework and develop a machine learning-based agent to detect such random fault attacks in real time on elliptic curve cryptosystems.

Motivation. Existing formal security models for key-exchange protocols—BPR [1], Dolev–Yao [3], and eCK—do not account for physical attacks, leaving a critical gap in the analysis of protocols such as PACE. Serraj *et al.* [6] proved, using the Canfield–Erdős–Pomerance theorem on smooth numbers, that for the standard curves P-256, BrainpoolP256r1, FRP256v1, and Fp-256, the probability that a randomly faulted curve E' has a 2^{224}-smooth order exceeds 85%, confirming that FAAs are a realistic and high-probability threat in practice. No prior work has addressed this vulnerability by means of a machine-learning detection agent capable of real-time response.

Main results. We present a simulation framework and a trained machine-learning agent targeting the BrainpoolP256r1 curve (RFC 5639 [4]). A dataset of $N = 3{,}000$ labelled ECC operations is generated by simulating random faults $b \mapsto b'$ and evaluating the nine security conditions of RFC 5639 :

- N' prime, cofactor $c = 1$ (optimal resistance to subgroup attacks);
- trace $t = p + 1 - N' \neq 1$ (absence of additive transfer / anomalous curves);

- embedding degree k satisfying $(q-1)/k < 100$ (MOV resistance);
- b' a non-square in $\mathbb{F}_p$ (absence of special points, RFC 5639);
- $N' < p$ (overflow prevention); $p \equiv 3 \pmod 4$ (point compression).

Our simulation on BrainpoolP256r1 yields the following result.

Four classifiers are trained on observable features of the faulted operation (deviation $|b' - b|/p$, quadratic residuosity of b' modulo p, bit-difference count, and arithmetic residues), without direct access to the security conditions or the label-generating function. The best supervised model (Random Forest, 300 estimators) achieves:

$$\text{Accuracy} = 91.3\%, \quad F_1 = 0.903, \quad \text{AUC} = 0.918, \quad \text{CV}_{F_1} = 0.876 \pm 0.019.$$

Acknowledgements. This work was conducted with the support of the CNRST under the "PhD-Associate Scholarship – PASS" program.

References

[1] Bellare, M., Pointcheval, D., & Rogaway, P. (2000, May). Authenticated key exchange secure against dictionary attacks. In International conference on the theory and applications of cryptographic techniques (pp. 139-155). Berlin, Heidelberg: Springer Berlin Heidelberg.

[2] Biehl, I., Meyer, B., & Müller, V. (2000, August). Differential fault attacks on elliptic curve cryptosystems. In Annual international cryptology conference (pp. 131-146). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Dolev, D., & Yao, A. (2003). On the security of public key protocols. IEEE Transactions on information theory, 29(2), 198-208.

[4] Lochter, M., & Merkle, J. (2010). Elliptic curve cryptography (ECC) brainpool standard curves and curve generation (No. rfc5639).

[5] Serraj, T., Azizi, A., & Ismaili, M. C. (2014, November). How can we succeed the fault attack on PACE protocol. In 2014 5th Workshop on Codes, Cryptography and Communication Systems (WCCCS) (pp. 59-63). IEEE.

[6] Serraj, T., Ismaili, M. C., & Azizi, A. (2017, April). On the security of some elliptic curve standards in the presence of random fault analysis attacks. In 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS) (pp. 1-5). IEEE.

A Bootstrap Analysis of Feature Selection Methods for Malware Detection

Ayoub SEGHROUCHNI
LARI Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco
ayoub.seghrouchni@ump.ac.ma

Noura Ouerdi
LARI Laboratory, Faculty of Sciences, Mohammed First University, Oujda, Morocco
n.ouerdi@ump.ac.ma

Keywords: Malware detection; feature reduction; machine learning; bootstrapping; Kuncheva index.
MSC: 68T05; 68M25; 62F40; 62H30.

Abstract. Machine-learning-based malware detection operates on high-dimensional feature spaces, necessitating feature reduction techniques such as filters (e.g., ANOVA, Chi-square, Mutual Information) or wrappers (e.g., Recursive Feature Elimination [RFE]). While the literature frequently proposes "optimal" feature subsets based solely on predictive accuracy, it rarely questions whether these subsets are mathematically reproducible. An unstable feature selector renders the published subset an artifact of a specific data split rather than a generalized representation of true malware behavior. Using bootstrap resampling on EMBER 2018, we measure the Kuncheva stability index of four classical selection methods and find that two of them produce essentially noise: at $k = 50$, RFE retains only 4 of its selected 50 features consistently across resamples (Kuncheva index KI = 0.408), while ANOVA retains 46 of 50 (KI = 0.959). The choice of selection method has a far larger reproducibility footprint than the literature acknowledges.

Motivation. Feature-selection reproducibility is critical for operational deployment in cybersecurity. If an algorithm yields a completely different set of features when the training data shifts slightly, the resulting pipeline is mathematically fragile and highly susceptible to concept drift. This stability-accuracy trade-off remains systematically ignored in the malware detection domain.

Methods / Applications. We bootstrap-resample 30 stratified training sets from EMBER 2018 ($\sim$ 600 000 labeled Windows PE samples, 2,381 features) and apply each of four reduction methods (ANOVA F-test, Chi-square, Mutual Information, and RFE) at three reduction sizes $k \in \{50, 100, 200\}$. For each method we record the 30 selected subsets and compute the Kuncheva stability index, the per-feature selection frequency, and the size of the reproducible core (features selected in every bootstrap). Downstream classification (Random Forest and XGBoost) is also evaluated on the reduced features to compare stability against detection quality on the same axis.

Main result. The results are clear: ANOVA and Chi-square achieve KI > 0.92 at every k; their reproducible cores cover 74% to 92% of the selected subset. Mutual Information sits in the middle (KI = 0.78 at $k = 50$, rising with k). RFE is the least reproducible: at aggressive reduction ($k = 50$) only 8% of its selection is reproducible, and the standard deviation of pairwise Kuncheva similarity (0.117) is three times larger than that of any filter method. Crucially, RFE's

instability does *not* buy classification advantage: its F_1 on the held-out test set is no higher than ANOVA's at any k. Stability is therefore a free criterion to optimize alongside accuracy, and recommending RFE on the basis of accuracy alone, as much of the literature does, ignores a substantial reproducibility cost.

References

[1] M. Sibtain et al., *Lightweight and Robust Android Ransomware Detection Using Behavioral Analysis and Feature Reduction*, Comput. Mater. Contin., **84**(3) (2025). https://doi.org/10.32604/cmc.2025.066198

[2] L. I. Kuncheva, *A stability index for feature selection*, Proc. 25th IASTED Int. Multi-Conf. on Artificial Intelligence and Applications (2007), 390–395.

[3] S. Nogueira, K. Sechidis, and G. Brown, *On the stability of feature selection algorithms*, Journal of Machine Learning Research **18**(174) (2018), 1–54.

[4] H. S. Anderson and P. Roth, *EMBER: An open dataset for training static PE malware machine learning models*, arXiv:1804.04637 (2018).

[5] M. E. Farfoura, I. Mashal, A. Alkhatib, and R. M. Batyha, *A Low Complexity ML-Based Methods for Malware Classification*, CMC-Computers, Materials & Continua, **80**(3) (2024), 4833–4851. https://doi.org/10.32604/cmc.2024.054849

[6] Y. Pristyanto, A. F. Nugraha, B. Wulansari, M. Sulistiyono, and A. Sunyoto, *Enhancement of Machine Learning Models Using Intersection Filtering Model Based on Recursive Feature Elimination on Specified Android Malware Classification*, Int. J. Intell. Eng. Syst., **18**(3) (2025). https://doi.org/10.22266/ijies2025.0430.56

[7] Y. W. Tye, U. K. Yusof, and S. Tulpar, *Ensemble of Filter and Embedded Feature Selection Techniques for Malware Classification using High-dimensional Jar Extension Dataset*, Proc. of the 12th Int. Conf. on Software and Computer Applications (ICSCA) (2023). https://doi.org/10.1145/3587828.3587849

[8] T.-H. Lai, Y.-J. Tsai, and C.-L. Liu, *Improving the Performance of Static Malware Classification Using Deep Learning Models and Feature Reduction Strategies*, Mathematics, **13**(23), 3753 (2025). https://doi.org/10.3390/math13233753

[9] V. Rocha, L. Tschiedel, and D. Kreutz, *Generalizing Feature Selection in Android Malware Detection: The SigAPI AutoCraft Approach*, Journal of the Brazilian Computer Society, **32**(1) (2026). https://doi.org/10.5753/jbcs.2026.6043

[10] D. Z. Syeda and M. N. Asghar, *Dynamic Malware Classification and API Categorisation of Windows Portable Executable Files Using Machine Learning*, Applied Sciences, **14**(3), 1015 (2024). https://doi.org/10.3390/app14031015

[11] E. S. Alomari, Z. A. Alyasseri, and N. S. Sani, *Malware Detection Using Deep Learning and Correlation-Based Feature Selection*, Symmetry, **15**(1), 123 (2023). https://doi.org/10.3390/sym15010123

Modern Cryptography and Artificial Intelligence: the Past, the Present, and the Future

Taoufik SERRAJ
LMA, Department of mathematics, Faculty of Sciences, Mohammed Premier University, Oujda, Morocco
t.serraj@ump.ac.ma

Keywords: Cryptography; Artificial Intelligence; Quantum Computing

Abstract. Artificial intelligence (AI) and cryptography maintain a co-evolutionary relationship characterized by both offensive and defensive interactions. On one hand, AI enhances attack capabilities by facilitating cryptanalysis, encrypted traffic detection, side-channel exploitation, and the modeling of hardware security primitives such as Physically Unclonable Functions (PUFs). On the other hand, AI contributes to the improvement of cryptographic systems through protocol optimization, adaptive key management, and learning-assisted random generation. Conversely, cryptography provides a fundamental framework for trustworthy and privacy-preserving AI. Techniques such as homomorphic encryption, secure multiparty computation, and zero-knowledge proofs enable training and inference over protected data without exposing sensitive information. Cryptography also supports the integrity, authenticity, and protection of machine learning models. In the medium term, this bilateral relationship is expected to evolve into a tripartite interaction incorporating quantum computing. The convergence of AI, post-quantum cryptography, and quantum computation may redefine future paradigms of security, performance, and digital trust.

References

[1] Nitaj, A., & Rachidi, T. (2023). *Applications of neural network-based AI in cryptography.* Cryptography, 7(3), 39.

[2] Malhou, M., Perret, L., & Lauter, K. (2025, August). *AI for Code-based Cryptography.* In International Conference on Selected Areas in Cryptography (pp. 489-518). Cham: Springer Nature Switzerland.

[3] Panoff, M., Yu, H., Shan, H., & Jin, Y. (2022). *A review and comparison of AI-enhanced side channel analysis.* ACM Journal on Emerging Technologies in Computing Systems (JETC), 18(3), 1-20.

[4] Pulido-Gaytan, L. B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., & Radchenko, G. (2020, September). *A survey on privacy-preserving machine learning with fully homomorphic encryption.* In Latin American High Performance Computing Conference (pp. 115-129). Cham: Springer International Publishing.

[5] Radanliev, P. (2024). *Artificial intelligence and quantum cryptography.* Journal of analytical science and technology, 15(1), 4.

[6] Pineda, V. G., Valencia-Arias, A., Giraldo, F. E. L., & Zapata-Ochoa, E. A. (2025). *Integrating artificial intelligence and quantum computing: A systematic literature review of features and applications.* International Journal of Cognitive Computing in Engineering.

A Bibliometric analysis of Artificial Intelligence and Machine Learning Applications in Chronic Diseases

Zakaria SLIMANI[1], Hanae AL KADDOURI[2], Youssef DOUZI[1]
[1] Arithmetic, Calcul Scientific and Applications Laboratory.
[2] Smart Information Communication and Technology Laboratory.
Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
zakaria.slimani@ump.ac.ma

Keywords: Artificial Intelligence; Machine Learning; Chronic Disease

Abstract. Artificial Intelligence (AI) and Machine Learning (ML) represent a tremendous potential in several domains, medicine being one of them. On the other hand, chronic diseases represent one of the major public health challenges, accounting for a significant share of global morbidity, mortality, and healthcare costs. Therefore, the application of AI and ML is necessary to develop more efficient systems and improved treatment strategies for chronic diseases, which will directly improve patient health outcomes. This study presents a comprehensive bibliometric analysis of research published on the use of AI and ML for the optimization of chronic disease treatment protocols, based on data extracted from the Scopus database. It encompasses the analysis of document abstracts, titles, and keywords. Several bibliometric approaches were employed to examine the evolution of its application from 2016 to 2025, including keyword co-occurrence analysis and citation mapping. The analysis covers publication trends, geographical distribution of research contributions, most productive institutions and journals, and leading authors in the field. To conduct this study, VOSviewer (1) and draw.io (2) were utilized for in-depth document analysis through visualization and flowchart construction. Results reveal a significant increase in publications since 2020, with the United States, China, and European countries leading in scientific output. Key research clusters were identified around diabetes, cardiovascular diseases, and cancer, with deep learning and ensemble methods being the most frequently applied ML approaches. This bibliometric overview provides a structured foundation for understanding the current state of research and highlights promising directions for future investigation in the optimization of chronic disease management through AI-driven solutions.

References

[1] N. J. van Eck and L. Waltman, *Software survey: VOSviewer, a computer program for bibliometric mapping*, Scientometrics **84**(2) (2010), 523–538. https://doi.org/10.1007/s11192-009-0146-3

[2] Draw.io, *The open-source diagramming tool.* Available at: (https://app.diagrams.net)

[3] Y. Pan, X. Li, J. Wei, Y. Peng, Z. Hu, Y. Xiong, et al., *Application of artificial intelligence in the health management of chronic disease: bibliometric analysis*, Frontiers in Medicine **11** (2025), 1506641. https://doi.org/10.3389/fmed.2024.1506641

[4] N. H. Alhumaidi, D. Dermawan, H. F. Kamaruzaman and N. Alotaiq, *The use of machine learning for analyzing real-world data in disease prediction and management: systematic review*, JMIR Medical Informatics **13** (2025), e68898. https://doi.org/10.2196/68898

[5] E. Afrifa-Yamoah, E. Adua, E. Peprah-Yamoah, E. O. Anto, V. Opoku-Yamoah, E. Acheampong, M. J. Macartney and R. Hashmi, *Pathways to chronic disease detection and prediction: mapping the potential of machine learning to the pathophysiological processes while navigating ethical challenges*, Chronic Diseases and Translational Medicine **11**(1) (2024), 1–21. https://doi.org/10.1002/cdt3.137

[6] L. I. Weil, L. R. Zwerwer, H. Chu, M. Verhoeff, P. P. T. Jeurissen and B. C. van Munster, *Enhancing healthcare for patients with multiple chronic conditions using machine learning and medical specialist data: a scoping review*, Health and Technology **15**(1) (2025). https://doi.org/10.1007/s12553-025-01026-x

[7] K. Liu, L. Li, Y. Ma, J. Jiang, Z. Liu and Z. Ye, *Machine learning models for blood glucose level prediction in patients with diabetes mellitus: systematic review and network meta-analysis*, JMIR Medical Informatics **11** (2023), e47833. https://doi.org/10.2196/47833

[8] S. Subramani, N. Varshney, M. V. Anand, M. E. Soudagar, L. A. Al-keridis, T. K. Upadhyay, N. Alshammari, M. Saeed, K. Subramanian, K. Anbarasu and R. Rohini, *Cardiovascular diseases prediction by machine learning incorporation with deep learning*, Frontiers in Medicine **10** (2023), 1150933. https://doi.org/10.3389/fmed.2023.1150933

[9] Y. Q. Cai, D. X. Gong, L. Y. Tang, Y. Cai, H. J. Li, T. C. Jing, M. Gong, W. Hu, Z. W. Zhang, X. Zhang and G. W. Zhang, *Pitfalls in developing machine learning models for predicting cardiovascular diseases: challenges and solutions*, Journal of Medical Internet Research **26** (2024), e47645. https://doi.org/10.2196/47645

[10] Y. Lin, Z. Lin, J. Lin, H. Lin and Y. Yan, *A bibliometric analysis of the advance of artificial intelligence in medicine*, Frontiers in Medicine **12** (2025), 1504428. *https://doi.org/10.3389/fmed.2025.1504428*

McEliece Key based on Quasi-Centrosymmetric Srivastava Codes,

Ousmane NDIAYE, Massamba Sow,Cheikh Thiécoumba GUEYE
Department of Mathematics and Computer Science ,Cheikh Anta Diop University, Dakar, Senegal
{ousmane3.ndiaye,massamba2.sow,cheikht.gueye}@ucad.edu.sn

Keywords: Post-quantum cryptography, McEliece cryptosystem, Code-based cryptography, Generalized Srivastava codes, Quasi-centrosymmetric symmetry, Key size reduction, Structural attacks, Folding attack, Error-correcting codes, Public-key cryptography **MSC:** 94A60; 94B05; 94B15

Abstract. The rapid progress of quantum computing threatens classical public-key cryptosystem such as RSA and elliptic-curve cryptography through Shor's algorithm. Post-quantum cryptography aims to design secure alternatives resistant to both classical and quantum attacks. Among the main post-quantum families, code based cryptography remains one of the most mature and trusted approaches, with the McEliece cryptosystem being a prominent example.
In this paper, we introduce a quasi-centrosymmetric construction of generalized Srivastava codes. Based on this construction, we design a McEliece-type key encapsulation mechanism achieving a significant reduction in public-key size while preserving resistance against the best known information set decoding and structural attacks on code based cryptosystem.

Motivation. Balancing key size reduction with a high level of security by using centrosymmetric group (order-2 symmetric) in generalized Srivastava codes instead of dyadic and cyclic symmetric

Main result.

Theorem 0.44. *Let $q = 2^m$, $n = n_0 t$, t even number and three sequences $w = (w_0, \ldots, w_{t-1}) \in \mathbb{F}_q^t$, $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$ a $n+t$ distinct elements and $z = (z_0, \ldots, z_{n-1}) \in (\mathbb{F}_q^*)^n$ such that α,w and z satisfy:*

$$\begin{cases} z_{(b+1)t-j-1} = z_{bt+j} \\ \alpha_{(b+1)t-j-1} = \alpha_b + \alpha_{bt+j} \\ w_{t-i-1} = \alpha_b + w_i \end{cases} \qquad 0 \le i, j \le \frac{t}{2} - 1, \quad \alpha_b \in \mathbb{F}_q$$

for $b = 0$ to $n_0 - 1$. Let $\tilde{H}_0 \in \mathbb{F}_q^{t \times n}$ be:

$$\tilde{H}_0 = \begin{pmatrix} \frac{1}{\alpha_0 - w_0} & \cdots & \frac{1}{\alpha_{n-1} - w_0} \\ \vdots & \ddots & \vdots \\ \frac{1}{\alpha_0 - w_{t-1}} & \cdots & \frac{1}{\alpha_{n-1} - w_{t-1}} \end{pmatrix}.$$

Then the matrix

$$\tilde{H} = \begin{bmatrix} \tilde{H}_0 \\ \tilde{H}_1 \\ \vdots \\ \tilde{H}_{s-1} \end{bmatrix} \cdot Diag(z_0, \ldots, z_{n-1})$$

defines a parity-check matix of a (s, n_0)*-quasi-centrosymmetric code* $GS(\alpha, \omega, z)$.

Methods / Applications. Construction of generalized Srivastava codes with quasi-centrosymmetric (order-2) symmetry to reduce key size while limiting exploitable structure. Applications include post-quantum secure communications with improved key size/security trade-offs.

References

[1] A. Becker, A. Joux, A. May et A. Meurer, *Decoding random binary linear codes in* $2^{n/20}$*: How* $1 + 1 = 0$ *improves information set decoding*, In: Advances in Cryptology - EUROCRYPT 2012, Springer, pages 520–536, 2012.

[2] L. Both et A. May, *Decoding linear codes with high error rate and its impact for LPN security*, In: T. Lange et R. Steinwandt (eds), Post-Quantum Cryptography, LNCS, Springer, pages 25–46, 2018.

[3] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc et J.-P. Tillich, *Folding alternant and Goppa codes with non-trivial automorphism groups*, IEEE Transactions on Information Theory, 62(1):184–198, 2016.

[4] A. May et I. Ozerov, *On computing nearest neighbors with applications to decoding of binary linear codes*, In: Advances in Cryptology - EUROCRYPT 2015, Part I, Springer, pages 203–228, 2015.

[5] R. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, The Deep Space Network Progress Report, DSN PR 42–44, pages 114–116, 1978.

[6] O. Ndiaye, *Moderate classical McEliece keys from quasi-centrosymmetric Goppa codes*, In: S. El Hajji et al. (eds), Codes, Cryptology and Information Security, Springer Nature Switzerland, pages 77–90, 2023.

[7] J. Stern, *A method for finding codewords of small weight*, In: G. Cohen et J. Wolfmann (eds), Coding Theory and Applications, Springer Berlin Heidelberg, pages 106–113, 1989.

[8] G. Banegas, P. S. L. M. Barreto, B. O. Boidje, P.-L. Cayrel, G. N. Dione, K. Gaj, C. T. Gueye, R. Haeussler, J. B. Klamti et O. Ndiaye, *DAGS: Key encapsulation using dyadic GS codes*, Journal of Mathematical Cryptology, 12(4):221–239, 2018.

[9] O. Ndiaye, *Moderate classical McEliece keys from quasi-centrosymmetric Goppa codes*, In: S. El Hajji, S. Mesnager et E. M. Souidi (eds), Codes, Cryptology and Information Security, Springer Nature Switzerland, pages 77–90, 2023.

[10] T. P. Berger, *Cyclic alternant codes induced by an automorphism of a GRS code*, In: R. Mullin et G. Mullen (eds), Finite Fields: Theory, Applications and Algorithms, volume 225, American Mathematical Society, pages 143–154, 1999.

[11] T. P. Berger, *On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes, and extended Goppa codes*, Finite Fields and Their Applications, 6(3):255–281, 2000.

[12] N. Courtois, M. Finiasz et N. Sendrier, *How to achieve a McEliece-based digital signature scheme*, In: C. Boyd (ed), Asiacrypt 2001, LNCS vol. 2248, Springer-Verlag, pages 157–174, 2001.

[13] A. Dür, *The automorphism groups of Reed-Solomon codes*, Journal of Combinatorial Theory, Series A, 44(1):69–82, 1987.

Detection and prevention of jailbreaking attacks in conversational artificial intelligence systems

Maryame ZIYANI
Computer science Department, Oujda, Morocco
maryiame.ziyani.m24@ump.ac.ma
Noura Ouerdi
LARI Laboratory,Faculty of Sciences,Mohammed First University, Oujda, Morocco
n.ouerdi@ump.ac.ma

Keywords: Jailbreaking, LLM, Multidimensional Taxonomy, BERT, RoBERTa, Adversarial Training, AI Security.

Abstract. Despite rigorous ethical alignment mechanisms, Large Language Models (LLMs) remain vulnerable to jailbreaking attacks, which manipulate input instructions to bypass safeguards and generate harmful content. This work proposes a new security approach based on a five-axis multidimensional taxonomy, enabling each attack to be characterized simultaneously according to its technical layer, bypass mechanism, input vector, potential impact, and detectability level. Unlike the linear or binary classifications found in the current literature, this multi-axis decomposition allows us to isolate critical vulnerabilities within the lexical, semantic, and logical layers. Based on this theoretical framework, we develop a hybrid, multi-layered defense system: it combines classifiers based on BERT and RoBERTa architectures to identify surface anomalies (manipulated tokens, encodings) and semantic coherence analysis via representation shifting to detect narrative diversions and nested scenarios. Finally, we introduce a prevention strategy using adversarial training with a combined dataset—merging real prompts and optimized variants—to enhance the system's overall robustness. Our approach demonstrates that a granular defense mechanism, directly tailored to the multidimensional nature of threats, outperforms conventional security filters in terms of effectiveness.

Motivation. This research area is characterized by a **rapid technological revolution**, where new attack vectors and bypass strategies are discovered almost daily in online communities [5]. Engaging with this problematic is essential to stay at the **cutting edge of AI innovation** and to develop proactive defenses before these threats impact high-stakes domains like **healthcare and finance** [3, 4]. Our objective is to move beyond reactive filtering and provide a granular, multi-layered taxonomy and detection system that can keep pace with this ongoing "cyber arms race."

Main result. We formalize the detection capability of our hybrid system $\mathcal{D}$ in relation to the proposed multidimensional taxonomy $\mathcal{T}$ [2]. We demonstrate that combining structural analysis with semantic consistency checks provides a complete defense for the targeted layers.

Methods / Applications.

- **Techniques:** We utilize **BERT and RoBERTa** for lexical anomaly detection [5] and a **T5-small** model for Main Intent Extraction (MIE) [7]. **Adversarial training** is applied to the base model using a combined dataset (**JailbreakHub** and AdvBench) to ensure long-term resilience [1, 6].
- **Potential Impact:** This framework provides a scalable, "plug-and-play" solution to secure LLM deployments in **medicine and finance**, preventing the leakage of Personally Identifiable Information (PII) without requiring costly model retraining [5, 8].

Acknowledgements. The author would like to express sincere gratitude to Professor **Noura Ouerdi** for her valuable guidance, continuous support, and insightful advice throughout the development of this research project. Special thanks are also extended to the **Faculty of Sciences at Mohammed First University (UMP)**, Oujda, for providing the academic environment and resources necessary to conduct this study on LLM security.

References

[1] M. Al Kuwaiti and H. Ismail, *Adversarial Attacks on Large Language Models: A Survey*, Abu Dhabi University, 2024.

[2] X. Shen et al., *"Do Anything Now": Characterizing and Evaluating In-The-Wild Jailbreak Prompts*, Proc. ACM CCS '24, 2024.

[3] S. Liu, X. Cheng et al., *Defending LLMs against jailbreak attacks through representation offset detection*, Inf. Process. Manag., 63, 2026.

[4] S. Yi, Y. Liu et al., *Jailbreak Attacks and Defenses Against Large Language Models: A Survey*, Tsinghua University, 2024.

[5] B. C. Das, M. H. Amini et al., *Security and Privacy Challenges of Large Language Models: A Survey*, ACM Comput. Surv., 2025.

.

With our sincere appreciation
to all participants, speakers, and partners

ICANTA'5

Pure mathematics, powerful connections, endless applications.

Oujda, Morocco • May 20–23, 2026

www.icanta5.ump.ma