Algebra, Arithmetic and Applications

Institut de Mathématiques et de Sciences Physiques

Porto-Novo, Bénin

June 12-24, 2022

Coordinators

Christian Maire, University of Franche-Comté, France
Japhet Odjoumani, Abomey-Calavi University and IMSP, Bénin

Scientific Committee

Armana Cécile, University of Franche-Comté, France
Ezome Tony, University of Masuku Franceville, Gabon
Elisa Lorenzo Garcia, University of Neuchâtel, Switzerland
Anne Quéguiner-Mathieu (chair), University Paris 13, France
Alain Togbé, Purdue University Northwest, USA

---

http://www.imsp-uac.org
http://www.rnta.eu/Benin2022/

Schedule

	9-10	10:20-11:20	11:30-12:30	2pm -3pm	3:15-4:15	4:30-5:30
June 13	Welcome Session	CM	MW	CA	CM	discussions I
June 14	CM	AT	CA	MW	exercices	YRL
June 15	CM	AT	CA	DB	ELG	discussions II
June 16	DB	AT	CA	ELG	exercices	YRL
June 17	DB	AT	CA	AQM	TE	open questions
June 18	DB	AT	ELG	–	–	
June 19						
June 20	AQM	FL	FP	MW	TE	YRL
June 21	AQM	FL	FP	ELG	exercices	open questions
June 22	AQM	FL	FP	ELG	TE	discussions
June 23	AQM	FL	FP	TE	TE	YRL
June 24	FP	MW	exercices	exercices	exercices	

Introduction to Algebraic Groups

AQM: Anne Quéguiner Mathieu – *Linear Algebraic Groups*

DB: Demba Barry – *Quadratic and Hermitian Forms and Algebras with involution*

CM: Christian Maire – *Central Simple Algebras and Brauer Group*

Analytic Number Theory and Diophantine Approximation

MW: Michel Waldschmidt – *Diophantine Approximation*

AT: Alain Togé – *Arithmetic Functions I*

LF: Florian Luca – *Arithmetic Functions II*

Geometry of Elliptic Curves

CA: Cécile Armana – *Modular Forms and Elliptic Curves*

FP: Francesco Pappalardi – *Introduction to Elliptic Curves*

Geometry methods in Information Theory

ELG: Elisa Lorenzo Garcia – *Curves over Finite Fields*

TE: Tony Ezome – *Some Mathematics Underlying Public key Cryptography*

YRL: Young Researchers Lectures.

Discussions I by Vlady, Japhet, Cécile and Tony. *Presentation of our partners.*

Discussions II by Elisa, Cécile and Tony. *Women in mathematics.*

Abstracts

Introduction to Algebraic Groups

Demba BARRY
Quadratic and hermitian forms and algebras with involution
Involution on a central simple algebra. Relation with hermitian forms. Relation with quadratic forms, skew-symmetric bilinear forms and hermitian forms in the split case. Different types of involutions. Isotropic and hyperbolic involutions. Associated groups, notably group of isometries, including the orthogonal group, and the corresponding adjoint groups. Functorial point of view.

Christian MAIRE
Central simple algebras and Brauer group
Different characterizations of central simple algebras; degree and index. Splitting fields and Galois splitting fields. Reduced norm and trace. Invertible elements and reduced norm 1 elements in a central simple algebra. Brauer equivalence and Brauer group. Brauer group of local fields; Brauer group of a number field.

Anne QUEGUINER-MATHIEU
Linear algebraic groups
Definition, and examples (borrowed from parts I and II). The root system of an algebraic group. Classification of linear algebraic groups. André Weil's theorem, describing groups of classical type in terms of some algebra with involution.

Analytic Number Theory and Diophantine Approximation

Alain TOGBE
Arithmetic functions I
Arithmetic functions and Dirichlet multiplication. Averages of arithmetical functions. Some elementary theorems on the distribution of prime. DirichletâĂŹs theorem on primes in arithmetic progressions Periodic arithmetic functions.

Florian LUCA
Arithmetic functions II
Average orders of arithmetic functions, maximal orders, normal orders, the Turan-Kubilius Theorem Introduction to probabilistic number theory, density of sets of integers. Smooth numbers, Applications: there are fewer pseudoprimes than primes. Sieves. Brun pure sieve. Applications to twin primes. Results about primes in arithmetic progressions (Brun-Titchmarsch and Bombieri-Vinogradov). Carmichael numbers. Proof that there are infinitely many Carmichael numbers.

Michel WALDSCHMIDT
Approximation diophantienne
Approximation d'un nombre réel par des nombres rationnels; Fractions continues; Application à l'équation de Brahmagupta-Pell-Fermat. Approximation d'un nombre algébrique par des nombres rationnels; Théorème de Thue-Siegel- Roth, théorème du sous-espace de Schmidt; Application aux équations diophantiennes. Introduction à la géométrie paramétrique des nombres. Application aux exposants d'approximation simultanÃle.

Geometry of Elliptic Curves

Cécile ARMANA
Modular forms and elliptic curves
Elliptic curves over the complex numbers. Modular group, modular functions and modular forms. The space of modular forms for $SL_2(\mathbb{Z})$. Hecke theory. If time allows: overview of elliptic curves associated to weight-2 cusp forms, Eichler-Shimura theory.

Francesco PAPPALARDI
Introduction aux courbes elliptiques
Examples of elliptic curves, drawing elliptic curves, the set of rational points of an elliptic curve, intersection between a line and an elliptic curve, the point at infinity of an elliptic curve, singular points, the group law, Weierstrass equations and their classification, elliptic curves over finite fields and their properties, the Hasse bound, the structure of the group of points over finite fields.

Geometry methods in Information Theory

Tony EZOME
Some Mathematics Underlying Public key Cryptography
Basics on Cryptology (Cryptography, Cryptanalysis). Pairings and Cryptology. Code Based Cryptography. Isogeny Based Cryptography.

Elisa LORENZO GARCIA
Curves over Finite Fields
Algebraic curves: concepts and definitions. The Riemann Hypothesis over Finite Fields. Applications: codes and cryptography. Maximal curves. Frobenius distributions.

Participants

ADEDJI Kouessi Norbert, IMSP, Bénin
adedjnorb1988@gmail.com

ADEGBINDIN Chefiath, IMSP, Bénin
adegbindinchefiath@gmail.com

ADJAKIDJE Roméo Jésugnon, IMSP, Bénin
romeo.adjakidje@imsp-uac.org

ARMANA Cécile, Université de Franche-Comté, France
cecile.armana@univ-fcomte.fr

CAMARA Mustapha, University Assane Seck of Ziguinchor, Sénégal
m.camara5367@zig.univ.sn

BARRY Demba, University of Bamako, Mali
barry.demba@gmail.com

BELLO Abdel Kadir, IMSP, Bénin
abdel.bello@imsp-uac.org

BIDOUAN Romziath, IMSP, Bénin
romziath.bidouan@imsp-uac.org

CAKPO K. Jocelyn, IMSP, Bénin
cakpojocelyn@gmail.com

DOSSAVI-YOYO Appolinaire, IMSP, Bénin
appolinairedossaviyovo@yahoo.fr

DOSSOU-YOVO Virgile, IMSP, Bénin
dosvirs20@gmail.com

ETCHIO Gisèle, Université d'Abomey Calavi, Bénin
etchiogisele95@gmail.com

EZOME Tony, Université des Sciences et Techniques de Masuku, Franceville, Gabon
tony.ezome@gmail.com

FAYE Mariame Ndao, University Gaston Berger, Sénégal
fayemariamandao@gmail.com

GUEGUELIGUE Joy, IMSP, Bénin
papajoy2016@gmail.com

GUEYE Alioune, University Gaston Berger, Sénégal
gueye.alioune2@ugb.edu.sn

IBARA NGIZA MFUMU Roslan, Université Marien Ngouabi, Brazzaville, Congo
roslancello7@gmail.com

KASSA Kourété Koutré, UAC, Bénin
kassapascal5@gmail.com

LORENZO GARCIA Elisa, University of Neuchâtel, Switzerland
elisa.lorenzo@unine.ch

KOUDJO Ferdinand Hountondji, IMSP, Bénin
ferdinand.koudjo@imsp-uac.org

KOUGNANKOU Yéntidié, IMSP, Bénin
benikougnana@gmail.com

LUCA Florian, The university of the Witwatersrand, South Africa
florian.luca@wits.ac.za

MAIRE Christian, Université de Franche-Comté, France
christian.maire@univ-fcomte.fr

MIAYOKA Brice, Université Marien Ngouabi, Brazzaville, Congo
bricemiayoka@gmail.com

NANSOKO Souleymane, IMSP, Bénin
souleymane.nansoko@imsp-uac.org

ODJOUMANI Japhet, Université d'Abomey-Calavi et IMSP, Bénin
odjoumanij@yahoo.fr

OGUNFOLU Olusola, University of Ibadan, Nigeria
ogunfolu.olusola@dlc.ui.edu.ng

ORO DJIBRIL Nabil, UAC, Bénin
66073833orodjibrilnabil@gmail.com

OWOLABI Sonagnon Julien, IMSP, Bénin
julien.owolabi@imsp-uac.org

PAPPALARDI Francesco, University Roma 3,Italy,
pappa@mat.uniroma3.it

PEKA MINGA Sarielle, Université de Maroua, Cameroun
pmssarie@gmail.com

PONCHO-KOTEY Ephraim Nii Amon, University of Ghana, Ghana
Ephraim.poncho@aims.ac.rw

QUEGUINER-MATHIEU Anne, Université Paris 13, France
queguin@math.univ-paris13.fr

RAVELOMANANA Vlady, University Paris Sorbonne, France
vlad@irif.fr

SANKARA Karim, Université Nazi Boni, Burkina Faso
sankara86@yahoo.fr

SEFFAH Safia, Université Houari Boumedienne, Algérie
safiaseffah58@gmail.com

SOWANOU Martine, Université d'Abomey Calavi, Bénin
martinesowanou12@gmail.com

TAKOUDA Toï Lucien, IMSP, Bénin
toilucien@gmail.com

TASSIGUE Wabout Timothé, Université d'Abomey Calavi et IMSP, Bénin
tassiguewabou@gmail.com

TCHAMMOU Euloge, IMSP, Bénin
tchammoue@yahoo.fr

TOGBÉ Alain, Purdue University Northwest, USA et IMSP, Bénin
atogbe@pnw.edu

TOUGMA Charles Wend-Waoga, Thomas Universiy, Burkina Faso
tougmacharles@yahoo.fr

WALDSCHMIDT Michel, Universiy Paris Sorbonne, France
miw@math.jussieu.fr

Young Researchers Lectures

ADEDJI Kouessi Norbert, IMSP, Bénin

On the solutions of the Diophantine equation $F_n \pm \frac{a(10^m-1)}{9} = k!$.

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$, for all $n \geq 0$. In this talk, we find all positive integer solutions (m, n, a, k) of the Diophantine equation $F_n \pm \frac{a(10^m-1)}{9} = k!$ with $1 \leq a \leq 9$. This is joint work with F. Luca and A. Togbé.

CAMARA Mustapha, University Assane Seck of Ziguinchor, Sénégal

Points algébriques de petits degrés sur les courbes hyperelliptiques $C_{n^2} : y^2 = x^5 + n^2$.

On s'intéresse à la détermination de l'ensemble des points algébriques de degré au plus 3 *sur $\mathbb{Q}$ pour les courbes hyperelliptiques C_{n^2} d'équations affines*

$$C_{n^2} : y^2 = x^5 + n^2,$$

avec $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 1250, 1296, 5000\}$.

DOSSOU-YOVO Virgile, IMSP, Bénin

Wiener's attack on RSA.

Let $N = pq$ be an RSA modulus and e be a public exponent. Let $\varphi(N) = (p-1)(q-1)$ be the Euler's totient function.The Wiener's attack on RSA consists in determining the private key d in the equation $ed - k\varphi(N) = 1$ when $d < \frac{1}{3}N^{\frac{1}{4}}$, using the public key (e, N) and the continued fractions.

GUEYE Alioune, University Gaston Berger, Sénégal

Concidence between k-Fibonacci numbers and products of two Fermat numbers.

We find all k-Fibonacci numbers which are products of two Fermat numbers.

IBARA Roslan, Université Marien Ngouabi, Brazzaville, Congo

Sur le groupe des classes de la clôture normale de $\mathbb{Q}(\sqrt[p]{n})$.

En théorie des nombres, le groupe de classes d'un corps de nombres K permet de mesurer la non principalité de l'anneau des entiers de K. C'est un groupe fini dont le nombre d'éléments est appelé le nombre de classes de K. En 1971, *Taira Honda prouve que le*

nombre de classes de $\mathbb{Q}(\zeta_3, \sqrt[3]{n})$ *est égal à* h^2 *ou* $3h^2$ *avec* h *le nombre de classes de* $\mathbb{Q}(\sqrt[3]{n})$*. Vers* 2016*, L.C. Washington propose une précision sur le résultat de Honda pour certaines valeurs de* n*.*
En 2020*, René Schoof prouve l'énoncé de Washington dans un contexte plus général avec une étude de la structure galoisienne du groupe de classes de la clôture normale de* $\mathbb{Q}(\sqrt[p]{n})$ *pour* p *premier impair.*
Dans cet exposé, on présentera le résultat de René Schoof.

MIAYOKA Brice, Université Marien Ngouabi, Brazzaville, Congo

Rational points on algebraic curves.

Let C *be an algebraic curve of genus* g *defined over the rational field, in this lecture we describe the calculation of rational points on the curve* C*.*

NANSOKO Souleymane, IMSP, Bénin

Balancing numbers as sum of same power of consecutive balancing numbers.

In this paper, we find all the balancing numbers which are sum of same power of consecutive balancing numbers. For this, we find all the solutions of the Diophantine equation $B_n^x + B_{n+1}^x + \cdots + B_{n+k-1}^x = B_m$ *in positive integers* (m, n, k, x)*, where* B_i *is the* i^{th} *term of the balancing sequence.*

OGUNFOLU Olusola, University of Ibadan, Nigeria

Counting the number of distinct fuzzy subgroups of some presentation groups.

We determine the number of subgroups of a presentation group. We identify the form, order of elements of the group and draw the subgroups lattice. We used certain equivalence relation to find the number of fuzzy subgroups of the presentation groups with generators. We also find an explicit formulae for the number of subgroups and determine chains of subgroups that end in the group wish established the number of fuzzy subgroups.

PONCHO-KOTEY Ephraim Nii Amon, University of Ghana, Ghana

The Game of Set-The hidden mathematics.

The Game of set is a card game where by there is a race to collect 3 *cards with some matching properties. In some cases it is difficult to find a match and some may claim there is no match. What are the conditions to have a "set"? We will analyse this question using an algebraic and geometric approach.*

SANKARA Karim, Université Nazi Boni, Burkina Faso

Hilbert's class field tower - Ozaki's Theorem.

In this talk, we will first of all give short words about ramified extensions of a number field k. Since a Hilbert class field is the maximal unramified abelian extension for all finite prime number of a number field k, we will describe the process of construction of unramified extension of a number field k in order to show what we call Hilbert's class field tower. We will end our presentation by an interested result about every finite p-group G and the p-Hilbert class field tower of some number field k proved by M. Ozaki.

SEFFAH Safia, Université Houari Boumedienne, Algérie

Repdigits as Product of Two k-Fibonacci Numbers or Two k-Lucas Numbers.

For an integer $k \geq 2$. Let $F_n^{(k)}, L_n^{(k)}$ be the k- Fibonacci and the k-Lucas sequences, respectively. For these sequences the first k terms are $0, \ldots, 0, 1$ and $0, \ldots, 0, 2, 1$, respectively, and each term afterwards is the sum of the preceding k terms. In this paper, we will show that $F_n^{(k)} F_m^{(k)}$ (resp. $L_n^{(k)} L_m^{(k)}$) can represent a repdigit.

TCHAMMOU Euloge, IMSP, Bénin

On some systems of simultaneous Pellian equations.

A system of simultaneous Pellian equations is a system of Diophantine equations of the form

$$ax^2 - by^2 = \delta_1, \quad cy^2 - dz^2 = \delta_2, \tag{1}$$

where $a, b, c, d, \delta_1, \delta_2$ are nonzero integers, and $\gcd(ab, \delta_1) = \gcd(cd, \delta_2) = 1$. It is well-known that if $d\delta_1 \neq b\delta_2$, then the system (1) has at most finitely many solutions in positive integers.
In this presentation, we consider and study the following system of simultaneous Pellian equations

$$\begin{cases} x^2 - (a^2b^2 \pm a)y^2 &= 1 \\ y^2 - pz^2 &= 4b^2, \end{cases} \tag{2}$$

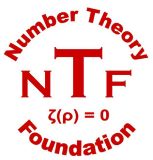
where $a \geq 2$ and $b \geq 1$ are positive integers and p is an odd prime, as well as the system

$$x^2 - (a^{2k}b^{2l} + 1)y^2 = 1 \quad \text{and} \quad y^2 - pz^2 = -1, \tag{3}$$

where a, b, k and l are positive integers such that $a \geq 2, b \geq 2$ and p is an odd prime number. Our proof uses the theory of continued fractions and is mainly based on an elementary method related to the results that we will recall or prove firstly.

Sponsors

IMSP	http://www.imsp-uac.org
CIMPA	https://www.cimpa.info/
IMU	https://www.mathunion.org/
ICTP	https://www.ictp.it/
Compositio Foundation	https://compositio.nl/#
Number Theory Foundation	https://numbertheoryfoundation.org/
Projet FLAIR, ANR	http://anrflair.math.cnrs.fr/
Université de Franche-Comté	http://www.univ-fcomte.fr/
IMJ Paris Sorbonne	https://www.imj-prg.fr/
LAGA University Paris 13	https://www.math.univ-paris13.fr/laga/
Neuchâtel University	https://www.unine.ch/
RNTA	http://www.rnta.eu/




June 9, 2022