Algebra, Arithmetic and Applications

Institut de Mathématiques et de Sciences Physiques

Porto-Novo, Benin

June 12-24, 2022

Coordinators

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

Scientific Committee

Cécile Armana, University of Franche-Comté, France
Tony Ezome, University of Masuku Franceville, Gabon
Elisa Lorenzo García, 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/

The CIMPA-School *Algebra, Arithmetic and Applications* took place at IMSP-Benin, Dangbo, from June 12 to June 24, 2022.
This mathematical meeting brought together:

- 41 participants: 10 lecturers (3 from France, 1 from Gabon, 1 from Italy, 1 from Mali, 1 from South Africa, 1 from Switzerland, 1 from the USA) + 21 participants from Benin + 13 participants from other African regions (outside of Benin),
- 15 nationalities from Africa: Algeria, Benin, Burkina Faso, Cameroon, Republic of Congo, Gabon, Ghana, Mali, Nigeria, Senegal, South Africa.
- 11 females and 30 males.

Scientific content
This School has offered an intensive teaching session to graduate students and young researchers from Africa. The topics developed were in algebra and in number theory. The following were courses took place:

- *Introduction to algebraic groups*, by Demba Barry, Christian Maire and Anne Quéguiner-Mathieu,
- *Analytic Number Theory and Diophantine Approximation*, by Florian Luca, Alain Togbé and Michel Waldschmidt,
- *Geometry of elliptic curves*, by Cécile Armana and Francesco Pappalardi,
- *Geometry methods in Information Theory*, by Tony Ezome and Elisa Lorenzo García.

Some of these fundamental courses introduced all theoretical elements needed for the applications in Information Theory which have been developed at during the courses of Tony Ezome and Elisa Lorenzo García. Beyond lectures, there were also:

- sessions devoted to solving exercises,
- sessions devoted to open questions,
- session to promote women in mathematics,
- lectures given by young researchers on their works.

Host institution and local context in mathematics
The *Institut de Mathématiques et de Sciences Physiques* (IMSP) is a regional Institute, integrated into the University of Abomey-Calavi. It was born in 1988 and it is located in Dangbo, in the South of Benin.
It is an affiliate center of what became the Abdus Salam ICTP. Since 1994 The IMSP has been elevated to the rank of Center of Excellence by the African Mathematical Union (AMU). It is a member of the Network of Mathematical Sciences for Africa and the African Network of Scientific and Technological Institutions.
The IMSP has also received the following international recognitions:

- Emerging Regional Centre of Excellence (ERCE) label of the European Mathematical Society for the period 2016-2020.

– for the period 2014-2020, Excellent Center of Mathematics and Applications (*Centre d'Excellence d'Afrique en Sciences Mathématiques et Applications* (CEA-SMIA) https://ceasma-benin.org/) of the World Bank.

The main mission of the IMSP is to provide African societies with young scientists and to encourage South-South cooperation in the fields of research.
The IMSP has thus implemented a policy of regular exchanges with scientists from the sub-region, the continent, certain universities and research centers in European and American countries.

Professor Carlos Ogouyandjou is the current Director of IMSP and Professor Joël Tossa is the current coordinator of the CEA-SMIA.

Prior work related to the School

The School *Algebra, Arithmetic and Applications* is part of a series of events that have taken place these last years, aiming at gathering young researchers from this part of Africa:

– From December 06 to 18, 2021, a research School in number theory and applications at IMSP;
– Some CIMPA schools: Cameroon (2019), Democratic Republic of Congo (2018), Côte d'Ivoire (2017), Benin (2014);
– Since 2012, project PREMA https://www.prema-a.org and its many mathematical meetings in the Africa: Burkina-Faso, Cameroon, Gabon, Niger, Senegal, etc.

Infrastructure and stay

The IMSP is located in Dangbo, about 50 km from Cotonou International Airport.
The participants from abroad arrived in Cotonou airport the week-end before the School. Shuttles have been organized by IMSP.
Participants were accommodated at the Residence of Songhai Center (www.songhai.org), Porto Novo, 30 minutes from IMSP. Bus shuttles have been provided by the organization. During the School, lunches and coffee breaks have been served at IMSP, and dinners have been scheduled at Songhai Center.

The IMSP is a recognized research center and has all the necessary facilities for research presentations, in particular IMSP provided with its facilities to all participants (internet connection, financial staff, etc.). The classroom was equipped with a video projector and two whiteboards.

The School officially started on Monday, June 13 with speeches of Professor Tossa, Professor Ogouyandjou and Professor Avlessi, President of the University of Abomey-Calavi. The official School dinner took place on Thursday, June 23 in the presence of the director of the IMSP.

A touristic tour has been organized to visit to Ouidah and Ganvié on Sunday, June 19.

Funding
The School has received financial support from:

IMSP	http://www.imsp-uac.org
CIMPA	https://www.cimpa.info/
IMU-CDC partially supported by the Abel Board	https://www.mathunion.org/cdc
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/

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	exercises	YRL
June 15	CM	AT	CA	DB	ELG	time for introductions
June 16	DB	AT	CA	ELG	exercises	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	FP	exercises	open questions
June 22	AQM	FL	FP	ELG	TE	discussions II
June 23	AQM	FL	FP	TE	TE	YRL
June 24	ELG	MW	exercises	closing ceremony		

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 Togbé – *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 García – *Curves over Finite Fields*

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

YRL: Young Researchers Lectures.

Discussions I by Elisa and Alain. *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 $SL_2(\mathbb{Z})$.

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 GARCÍA
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, Benin
adedjnorb1988@gmail.com

ADEGBINDIN Chefiath, IMSP, Benin
adegbindinchefiath@gmail.com

ADIGBÉ Lorsechaque, IMSP, Benin
lorsechaqueadigbe@gmail.com

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

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

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

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

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

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

CAMARA Moustapha, University Assane Seck of Ziguinchor, Senegal
m.camara5367@zig.univ.sn

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

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

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

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

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

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

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

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

KOUGNANKOU Yéntidié, IMSP, Benin
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, Republic of Congo
bricemiayoka@gmail.com

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

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

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

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

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

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

PEKA MINGA Sarielle, Université de Maroua, Cameroon
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

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

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

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

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

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

TCHAMMOU Euloge, IMSP, Benin
tchammoue@yahoo.fr

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

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

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

Young Researchers Lectures

ADEDJI Kouessi Norbert, IMSP, Benin

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 Moustapha, University Assane Seck of Ziguinchor, Senegal

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, Benin

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, Senegal

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

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

MIAYOKA Brice, Université Marien Ngouabi, Brazzaville, Republic of 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, Benin

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, Algeria

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, Benin

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.

TOUGMA Charles Wend-Waoga, Université Thomas Sankara, Burkina Faso

Corps de Pólya.

Un corps de nombres K est un corps de Pólya si le module $\mathrm{Int}(\mathscr{O}_K)$ des polynômes à valeurs entières sur son anneau des entiers $\mathscr{O}_K$ admet une base régulière. Le but de cet exposé est de déterminer quand le compositum de deux corps de Pólya quadratiques est un corps de Pólya lorsque le nombre premier 2 est totalement ramifié. Nous repondrons ainsi à des questions soulevées par certains auteurs sur les corps biquadratiques.

June 25, 2022