Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics

AIMS-Cameroon, Limbé

July 2 - 13, 2019

Organizing Committee

Christian Maire, University of Franche-Comté, France, christian.maire@univ-fcomte.fr
Aminatou Pecha, University of Maroua, Cameroon, aminap2001@yahoo.fr

Scientific Committee

Michel Coste, University Rennes 1, France
Marco Garuti, Universita Degli Studi Di Padova, Italy
Christian Maire, University of Franche-Comté, France
Marie-Françoise Roy, University Rennes 1, France

http://www.prema-a.org/cimpa-school-limbe/

The CIMPA-School "Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics" took place at AIMS-Cameroon, Limbé, from july 2 to july 13, 2019.
This mathematical meeting brought together

- 50 participants: 7 lecturers, one participant from CIMPA staff, 18 participants from Cameroon, 22 participants from other African regions (outside of Cameroon), a french and a USA participant.
- 20 nationalities namely participants coming from: Algeria, Burkina Faso, Cameroon, République du Congo, République Démocratique du Congo, Gabon, Ghana, Kenya, Madagascar, Mali, Niger, Nigeria, Rwanda, Senegal, Sudan, Tanzania, but also, France, Italy, Spain and USA.
- 11 females and 39 males.

The *Congress of African Women in Mathematics Association* (AWMA) is an associated Regional Workshop of this School for Central Africa; indeed African Women Mathematicians met at AIMS-Cameroon two days after, with the opportunity to attend the School.

Scientific content
This School has offered an intensive teaching session to graduate students and young researchers from Africa. The topics developed were in Algebraic Geometry and Number Theory. The following six courses have been selected:

- *Advanced topics in semi-algebraic geometry and modelization in robot kinematics*, by Michel Coste,
- *Counting points on algebraic varieties*, by Tony Ezome,
- *Basic algebraic number theory and class field theory*, by Elisa Lorenzo Garcia,
- *Fundamental groups in Algebraic and Arithmetic Geometry*, by Marco Garuti.
- *Tate module and Abelian varieties*, by Christian Maire,
- *Quantitative and algorithmic recent results in real algebraic geometry*, by Marie-Françoise Roy,

These fundamental courses describe all theoretical elements needed for the applications in cryptography and robot kinematics which have been developed at the end of the School. Beyond lectures, we have also planned:

- sessions devoted to solving exercises,
- sessions with computers with Sage, by Samuel Lelievre,
- a list of mini-projects has been proposed at the beginning of the School, in relation with some courses; at the end of the meeting, students have made short presentations of their work,
- lectures given by young researchers on their works.

Files of the exercices and mini-projects topics are attached at the end of the report.

Host institution and local context in mathematics
African Institute for Mathematical Science (AIMS, https://aims-cameroon.org) is an innovative, pan-African centre for Post Graduate education, research and outreach

which has achieved global recognition since opening in South Africa in 2003. AIMS-Cameroon is part of the network of AIMS centers and offers a one year Master's degree in mathematical science to African graduates every year since 2013. It is located in Limbé, in the South West Region of Cameroon. Professor Mama Foupouagnigni is the President of AIMS-Cameroon and Professor Marco Garuti, from Universita Degli Studi Di Padova in Italy, is the Academic Director.

On the other hand, Algebraic Geometry and Number Theory in sub-Saharan Africa got a fresh start in 2011, when some African young researchers went back in their native countries after their PhD defenses. Since then between 2011 and 2013 there have been PhD defenses from students working locally in Africa.
This is in this context that, on January 16th 2012, the *Pole of Research in Mathematics and their Applications in Information Security* (PRMAIS, HTTPS://WWW.PREMA-A.ORG/) was created. It is hosted in *Université des Sciences et Techniques de Masuku in Franceville (Gabon)*, and it is funded by Simons Foundation. PRMAIS consists of three components: PRMAIS-Senegal, PRMAIS-Cameroon, PRMAIS-Madagascar; and since 1st May 2018, a new network PREMA with researchers from Tunisia, Nigeria, Niger, Burkina Faso and Mali. PRMAIS aims to develop fundamental mathematical topics from Algebraic Geometry and Number Theory in African universities. Applications of these theoretical studies in cryptography, coding theory and robot kinematics are also developed. PREMA members have important collaborations with researchers all over the world.

Prior work related to the School

Since 2015, PRMAIS has organized or supported many mathematical meetings in Africa, at least two events every year. Let us just mention the events of the last two years.

- On 13 January 2017, *Les Journées Algébriques du Gabon*, in Ecole Normale Supérieure, Libreville (Gabon).
- From 10 to 23 May 2017 in Thiès (Senegal), an African Mathematical School in *Mathematics for Post-Quantum Cryptography and Signal Processing.*
- From 2 to 14 April 2018 in Franceville (Gabon), an African Mathematical School in the theme *Mathematics for asymmetric cryptography and robot kinematics.*
- From 18 to 22 February 2019, *Les Journées Algébriques du Gabon*, in Ecole Normale Supérieure, Libreville.

The stay

The participants from abroad arrived in Douala airport the week-end before the School. Some of them had to stay one night or two nights in Douala, in order to take some shuttle organized by AIMS-Cameroon (Limbé is at two-hours drive from Douala).

The School officialy started on tuesday 2nd of july with the presentation of AIMS-Cameroon by Marco Garuti, of PREMA by Tony Ezome and of CIMPA by Vlady Ravelomanana.

The lectures of the School have been given in the main classroom of AIMS-Cameroon since the dates chosen correspond to a vacation period in AIMS-Cameroon. The classroom was equipped with a video projector and large green board.

During the School, AIMS-Cameroon provided with its facilities to all participants (internet connection, financial staff, cleaning services, etc.), including accomodation for about 48 students and for the lecturers. Meals have been taken in the main building.
At the end of the School, participants have been the possibility to fill up a questionnaire concerning the School. The evaluaton show that the atmosphere, scientific content and activities proposed during the School (courses, exercises, mini-projects, lectures by young researchers) have been very appreciated. However the participants suggested that the totality of lecturers give documents on line for their courses. The lack of water in rooms during several days was reported and criticized.

Funding

The School has received financial support from

CIMPA	https://www.cimpa.info/
AIMS-Cameroon	https://aims-cameroon.org
PREMA	http://www.prema-a.org/
IRMAR Univ. Rennes 1	https://irmar.univ-rennes1.fr
IMU	https://www.mathunion.org/
OpenDreamKit Horizon 2020	https://opendreamkit.org/
ANR FLAIR Project	http://anrflair.math.cnrs.fr/
RNTA	http://www.rnta.eu/

Schedule

day	9-10:15am	10:45-12am	2-3:15pm	3:45-5	5:15-6
july 2			MFR	ELG	discussion
july 3	TE	ELG	MFR	exercices (MFR)	YR lectures
july 4	TE	CM	ELG	exercices (ELG)	YR lectures
july 5	MC	CM	MFR	exercices (ELG)	YR lectures
july 6	TE	CM			
july 7					
july 8	MFR	CM	SL	exercices (TE)	YR lectures
july 9	MC	MG	ELG	SL	YR lectures
july 10	TE	MG	SL	exercices	YR lectures
july 11	MC	MG	exercices (TE)	projects	projects
july 12	MC	MG			

MFR: Marie-Françoise Roy
Quantitative and algorithmic recent results in real algebraic geometry

MC: Michel Coste
Advanced topics in semi-algebraic geometry and modelization in Robot Kinematics

ELG: Elisa Lorenzo Garcia
Basic algebraic number theory and class field theory

SL: Samuel Lelievre
Introduction to SAGE

CM: Christian Maire
Tate Module and Abelian Varieties

TE: Tony Ezome
Point counting on algebraic varieties and applications in cryptography

MG: Marco Garuti
Fundamental groups in Algebraic and Arithmetic Geometry

YR: young researchers

Abstracts of courses

Michel Coste, University Rennes 1, France, michel.coste@univ-rennes1.fr

Advanced topics in semi-algebraic geometry and modelization in Robot Kinematics

The course will give a short introduction to Robot Kinematics and show examples of applications of algebraic and semialgebraic geometry in this field. I shall discuss direct and inverse kinematics and singularities, especially for parallel robots. I shall also discuss mechanisms having several operating modes, with possibly different degrees of freedom. I shall explain methods to translate problems of robot kinematics into systems of polynomial equations, including the model of the group of rigid motions given by the Study quadric, using dual quaternions. The effective methods of algebraic and semialgebraic geometry can then be applied (elimination, decomposition into primary components, cylindrical algebraic decomposition...). Problems to study with the help of computer algebra systems will be given to the students.

Tony Ezome, University of Masuku Franceville, Gabon, latonyo2000@yahoo.fr

Point counting on algebraic varieties and applications in cryptography.

Given an algebraic variety V over a finite field $\mathbb{F}_q$, we know that the $\mathbb{F}_{q^k}$-rational points on V form a finite set. What arises naturally in our mind is the construction of a process which computes the number of $\mathbb{F}_{q^k}$-rational points in V. This is one of the most important and very recurrent questions in cryptography, particularly when V is a (hyper-)elliptic curve C or a Jacobian variety J_C. That led to many points counting algorithms. This course aims to describe the more important methods. We will start with the naive algorithm (enumeration of points) which is a quite general method, and then we will describe the Baby Step Giant Step algorithm for elliptic curves. We will explain how are related the Frobenius endomorphism of a curve C, the number of rational points on C, the number of rational points on the Jacobian J_C, and Weil conjectures. We will also describe the Schoof ℓ-adic algorithm and the main steps in SEA algorithm. We will end by giving a technique for selecting a hyperelliptic curve C (and the underlying finite field) suitable for implementing a discrete logarithm cryptosystem in the Jacobian variety J_C.

Elisa Lorenzo Garcia, University Rennes 1, France, elisa.lorenzogarcia@univ-rennes1.fr

Basic algebraic number theory and class field theory

We will start by studying the structure of the decomposition of prime ideals in number fields and by discussing the definitions of norm, trace and discriminant. From there we will move to the basics of Class Field Theory: we will define the Artin symbol and we will state the Reciprocity Law. We will end by showing the applications of the Class Field Theory to the Theory of the Complex Multiplication. All the course will be illustrated with several examples which will help to the understanding of these deep theories.

Marco Garuti, Universita Degli Studi Di Padova, Italy, and AIMS-Cameroon, marco@aims-cameroon.org

Fundamental groups in Algebraic and Arithmetic Geometry

The course is a survey on the theory of Fundamental Groups in Algebraic and Arithmetic Geometry. Starting from Grothendieck's theory developed in SGA 1, we will review his Anabelian philosophy and its applications to the search for points on varieties.

Christian Maire, University of Franche-Comté, France, christian.maire@univ-fcomte.fr

Tate modules and abelian varieties

In this course, we will introduce the key concepts (and some basic tools) of Galois representations of Tate modules of Abelian varieties (elliptic curves and more generally Jacobian varieties). We will first spend time on elliptic curves to introduce in detail some notions in order to well understand their Tate module: locus of ramification, Frobenius and characteristic polynomial, mod p representation, L-function, image of the representation, modularity, etc. After that, we will explain how these properties extend to the case of genus > 1.

Marie-Françoise Roy, University Rennes 1, France, marie-francoise.roy@univ-rennes1.fr

Quantitative and algorithmic recent results in real algebraic geometry

Important theoretical results in real algebraic geometry such as the algebraic proofs of the fundamental theorem of algebra (valid for a real closed field), the curve selection lemma, the finiteness theorem (i.e a closed semi-algebraic set has closed description) have been recently studied from a quantitative and algorithmic point of view. Several methods are used: the cylindrical decomposition and the critical point method. In both cases, algebraic results about sub-resultants play a role. Important theoretical results in real algebraic geometry have been recently studied from a quantitative and algorithmic point of view. Several methods are used: the cylindrical decomposition and the critical point method. In both cases, algebraic results about sub-resultants play a role. The course treated the following topics

- *real root counting,*
- *quantifier elimination,*
- *semi-algebraic sets and cylindrical decomposition,*
- *connected components and critical point method.*

Lectures given by young researchers

ADEYEMO Hammed Praise, University of Ibadan, Nigeria

Stanley Symmetric Functions of Springer Permutations.

Abstract. In this talk, I will give a construction of Stanley symmetric functions indexed by Springer permutations and establish their connection with that of Grassmannian permutations. This will be done in type A.

BA Boumanga Abdoulaye, University of Thiès, Senegal

Cryptographie et sécurité de l'information sur le Web

Abstract. Dans cet exposé nous allons d'abord pouvoir appréhender le fonctionnement de l'infrastructure Web et ensuite comprendre comment la cryptographie est mise en oeuvre sur le Web pour assurer la sécurité de l'information, tout en précisant leurs enjeux majeurs pour un gouvernement ou une organisation.

BANG Narcisse, University of Daschang, Cameroon

Efficient computation of the Miller Loop and the Final exponentiation in Pairing-Based Cryptography

Abstract. In this talk, we show how one can efficiently computes pairings which are very useful in Cryptography.

DJINTELBE Nestor, University Assane SECK, Ziguinchor, Senegal

Compactifications of the space of rigid motions.

Abstract. We present different compactifications of the space of rigid motions and their applications in some problems of robot kinematics.

FOTUE-TABUE Alexandre,

MacWilliams' identity

Abstract. In this talk, we revisit the MacWilliams' identity, which is a relation between the weight enumerator of a linear code and the weight enumerator of its dual code.

FOUAZOU LONTOUO Perez, University of Dschang, Cameroon

Analogues Vélu's formulas for Hessian curve

Abstract. We give an analog of the Vélu's formulas for the Hessian model of an elliptic curve.

KOUMLA KANG-RANG Keth, Abdou Moumouni University of Niamey, Niger.

Généralisation de la théorie des bases de Gröbner dynamiques aux polynômes de Laurent à coefficients sur des anneaux de Dedekind

Abstract. Si R *est un anneau de Dedekind et* $f_i \in \mathrm{R}[X_n^{\pm}]$*, nous déterminons de manière dynamique une base de Gröbner pour* $I = \langle f_i \rangle_{i=1,\cdots,s} \in \mathrm{R}[X_n^{\pm}]$ *et ses syzygies modules.*

MOUSSA Seydou, University Dan Dicko Dankoulodo de Maradi, Niger

Rationalité de l'ensemble des configurations singulières d'une plate-forme de Gough-Stewart

Abstract. Dans cet exposé, nous montrons que l'ensemble des configurations singulières d'une plate-forme de Gough-Stewart admet une paramétrisation rationnelle.

NZAGANYA Nzaganya Edilson, University of Dar es salaam, Tanzania

Topology of a Projective hypersurfaces

Abstract. We compute the Euler characteristics of projective hypersurfaces by using the Griffiths residues and by using Chern classes.

NDONG'A OWINO Julia, Jaramogi University of Science and technology, Bondo, Kenya

Completeness of compact operators whose norms are eigenvalues

PONCHO-KOTEY Ephraim Nii Amon, AIMS Rwanda, Kigali, Rwanda

Counting of Rational Points On an Elliptic Curve

SALISSOU DANGO Mamane Djamilou, University Abdou Moumouni, Niamey, Niger

Factorisation des matrices 2×2 de déterminant égal a 1.

Abstract. Il s'agit, étant donnée une matrice 2×2*, de déterminant* 1*, de pouvoir l'écrire sous la forme d'un produit de matrices élémentaires. Nous regarderons le cas des matrices constantes, polynômiales multivariées et à coefficients dans un anneau de polynômes de Laurent.*

YOUEGO Jocelyne, University of Ngaoundere, Cameroon

Isogeny of supersingular elliptic curves in cryptography.

Abstract. In this talk, we present isogeny of elliptic curves and how they can be used to construct cryptographic primitives.

Participants

ADEYEMO Hammed Praise, University of Ibadan, Nigeria
AMANI FARAJA Deborah, AIMS-Cameroon
ANDRIAMANDRATOMANANA Njaka Harilala, University of Padova, Italy
AZEBAZE GUIMAGANG Laurian, University Yaoundé 1, Cameroon
BA Boumanga Abdoulaye, University of Thiès, Senegal
BANG MBIANG Narcisse, University of Dschang, Cameroon
COSTE Michel, University Rennes 1, France
DJINTELBE Nestor, University Assane SECK, Ziguinchor, Senegal
EZOME Tony, University of Masuku, Franceville, Gabon
FOBASSO TCHINDA Arnaud Girès, University of Yaounde 1, Cameroon
FOMBOH Mary, University of Buea, Cameroon
FOTUE TABUE Alexandre, University Yaoundé 1, Cameroon
FOUAZOU LONTOUO Perez, University of Dschang, Cameroon
FOUOTSA Emmanuel, University of Bamenda, Cameroon
FOUOTSA TAKO Boris, University of Roma 3, Italy
GARUTI Marco, Universita Degli Studi Di Padova, Italy
HANWA Anne, University of Ngaoundéré, Cameroon
HASSAN Hoyam, University of Khartoum, Sudan
IBARA NGIZA MFUMU Roslan, University Marien Ngouabi, Brazaville, Congo
KAMWA DJOMOU Franck Rivel, University of Dschang, Cameroon
KEM-MEKA Peguy, AIMS-Cameroon
LELIEVRE Samuel, University Paris-Sud, France
LEPEYI-LEBOUMA Junior, Ecole Normale Supérieure, Libreville, Gabon
LORENZO GARCIA Elisa, University Rennes 1, France
MAIGA Abdoulaye, AIMS-Senegal, Dakar, Senegal
MAIRE Christian, University of Franche-Comté, France
MANTIKA Gilbert, University of Maroua, Cameroon
MEMIAGHE LENGA Fermi Adrien, Ecole Normale Supérieure, Libreville, Gabon
MOHAMMED FAGEER KHAKIFA Ibrahim, Sudan University, Khartoum, Sudan
MONNEAU Régis, Ecole des Ponts, ParisTech, France
NDONG'A OWINO Julia, Jaramogi University of Science and technology, Bondo, Kenya
NGO BABEM Annette, AIMS-Cameroon, Cameroon
NKOTTO NKUNG ASSONG Sedric, University of Kassel, Germany
NZAGANYA Nzaganya Edilson, University of Dar es salaam, Tanzania
OKANZA-PEA Mélodie, University Marien Ngouabi, Brazaville, Congo
OULD MOHAMED Rezki, University Houari Boumediene, Alger, Algeria
PECHA Amina, University of Maroua, Cameroon

PONCHO-KOTEY Ephraim Nii Amon, AIMS Rwanda, Kigali, Rwanda
RAVELOMANANA Vlady, CIMPA and University Paris Diderot, France
ROY Marie-Françoise, University Rennes 1, France
SAINHERY Phrador, University of Padova, Italy
SALIOU Douboula, University of Maroua, Cameroon
SALISSOU DANGO Mamane Djamilou, University Abdou Moumouni, Niamey, Niger
SALL Mohamadou, Senegal
SANKARA Karim, University Nazi Boni, Burkina Faso
SETH-KOUMLA Kang-Rang, University Abdou Moumouni, Niamey, Niger
SEYDOU Moussa, University Dan Dicko Dankoulodo de Maradi, Niger
SONKOUE Jacques, University Yaoundé 1, Cameroon
YOUEGO Jocelyne, University of Ngaoundere, Cameroon
YOUMBI Norbert, St-Francis University, Poretto PA, USA

July 22, 2019