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/
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

<table>
<thead>
<tr>
<th>day</th>
<th>9-10:15am</th>
<th>10:45-12am</th>
<th>2-3:15pm</th>
<th>3:45-5</th>
<th>5:15-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>july 2</td>
<td></td>
<td></td>
<td>MFR</td>
<td>ELG</td>
<td>discussion</td>
</tr>
<tr>
<td>july 3</td>
<td>TE</td>
<td>ELG</td>
<td>MFR</td>
<td>exercices (MFR)</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 4</td>
<td>TE</td>
<td>CM</td>
<td>ELG</td>
<td>exercices</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 5</td>
<td>MC</td>
<td>CM</td>
<td>MFR</td>
<td>exercices</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 6</td>
<td>TE</td>
<td>CM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>july 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>july 8</td>
<td>MFR</td>
<td>CM</td>
<td>SL</td>
<td>exercices (TE)</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 9</td>
<td>MC</td>
<td>MG</td>
<td>ELG</td>
<td>SL</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 10</td>
<td>TE</td>
<td>MG</td>
<td>SL</td>
<td>exercices</td>
<td>YR lectures</td>
</tr>
<tr>
<td>july 11</td>
<td>MC</td>
<td>MG</td>
<td>exercices (TE)</td>
<td>projects</td>
<td>projects</td>
</tr>
<tr>
<td>july 12</td>
<td>MC</td>
<td>MG</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Abstracts

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 \( \mathbb{F}_q \)-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 \( \mathbb{F}_q \)-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 \( \ell \)-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.
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.

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 $> 1$.

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.
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.

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, Sénégal
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 $f_i \in R[X_n^\pm]$, nous déterminons de manière dynamique une base de Gröbner pour $I = \langle f_i \rangle_{i=1,\ldots,s} \in R[X_n^\pm]$ 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 2x2 de déterminant égal a 1.
Abstract. Il s’agit, étant donnée une matrice 2x2, 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.
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 Ousmane Mamadou Sada, University Cheikh Anta Diop, Dakar Fann, Senegal
BA Boumanga Abdoulaye, University of Thiès, Senegal
BANG MBIANG Narcisse, University of Dschang, Cameroon
CHEMS-EDDIN Mohamed Mahmoud, University Mohammed I, Oujda, Morocco
COSTE Michel, University Rennes 1, France
DJIÑTELBE Nestor, University Assane SECK, Ziguinchor, Sénégal
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
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 LENG Aferm Adrien, Ecole Normale Supérieure, Libreville, Gabon
MOHAMMED FAGEER KHAKIFA Ibrahim, Sudan University, Khartoum, Sudan
NDONG’A OWINO Julia, Jaramogi University of Science and technology, Bondo, Kenya
NKOTTO NKUNG ASSONG Sèdric, University of Kassel, Germany
NZAGANYA Nzaganya Edilson, University of Dar es salaam, Tanzania
OGUNFOLU Bamidele, University of Abidan, Nigeria
OKANZA-PÉA Mélodie, University Marien Ngouabi, Brazzaville, 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
SONKOUUE Jacques, University Yaoundé 1, Cameroon
TAMEKUE WOUNNDJA Cyprien, University of Dangbo, Benin
YOUDEGO Jocelyne, University of Ngaoundere, Cameroon
YOUUMBI Norbert, St-Francis University, Poretto PA, USA

<table>
<thead>
<tr>
<th>Sponsors</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIMPA</td>
<td><a href="https://www.cimpa.info/">https://www.cimpa.info/</a></td>
</tr>
<tr>
<td>AIMS-Cameroon</td>
<td><a href="https://aims-cameroon.org">https://aims-cameroon.org</a></td>
</tr>
<tr>
<td>PREMA</td>
<td><a href="http://www.prema-a.org/">http://www.prema-a.org/</a></td>
</tr>
<tr>
<td>IMU</td>
<td><a href="https://www.mathunion.org/">https://www.mathunion.org/</a></td>
</tr>
<tr>
<td>ANR FLAIR Project</td>
<td><a href="http://anrflair.math.cnrs.fr/">http://anrflair.math.cnrs.fr/</a></td>
</tr>
<tr>
<td>RNTA</td>
<td><a href="http://www.rnta.eu/">http://www.rnta.eu/</a></td>
</tr>
</tbody>
</table>

June 29, 2019