Final Report for the CIMPA School
Cryptography, theoretical and computational aspects of number Theory

August 15-26, 2022

AIMS Senegal, Mbour, Senegal

1 Summary

The CIMPA School *Cryptography, theoretical and computational aspects of number Theory* took place at AIMS Senegal in Mbour, from August 15 to 26, 2022. Initially scheduled in 2021, it was postponed to 2022 because of the Covid pandemic. The website of the school is:
`https://indico.math.cnrs.fr/e/cimpa2021senegal`

This CIMPA School is the last part of an intensive five-week training research program in number theory and cryptography organized at AIMS Senegal in 2021/22. The program also consisted of:

- the African Mathematical School (EMA) *Introduction to Number Theory, Cryptography and related courses*: September 6 to 17, 2021 (two weeks),
- the workshop *Women in Sage in Senegal*: September 20 to 24, 2021 (one week).

The objective of these events was to attract new PhD students in particular women, to develop and nurture scientific exchanges on algebra, number theory and cryptography in this region of Africa, in particular research collaborations and co-supervisions of students between African mathematicians and non-African mathematicians. This program has received dedicated funding from the CNRS through its *Dispositif de soutien aux collaborations avec l'Afrique subsaharienne.*

The CIMPA school gathered 44 persons among which 42 were present onsite:

- 35 young participants: 6 Bachelor students, 12 Master students, 12 PhD students, 5 Post-docs/Faculty. Among them:
    - 30% of young participants were studying in West African countries outside of Senegal: Algeria, Benin, Burkina Faso, Cameroon, Ghana, Ivory Coast, Togo. Because of the diversity of students at AIMS, two additional nationalities were represented: Nigeria and Republic Democratic of Congo.
    - 70% were studying in Senegal: 16% were Master students at AIMS Senegal, others participants were coming from universities Dakar, Saint-Louis, Bambey, Thies.
    - also 37% were women and 63% were men.
- 9 lecturers, main organizers or CIMPA representative: confirmed mathematicians or computer scientists from Canada, France, Senegal, South Africa, and USA. Among them, two were women and also the main organizers.

We selected 11 CIMPA participants and 10 of them attended the school (one from Sudan was unable to come because her visa was not ready in time). Vlady Ravelomanana was the CIMPA representative for this school.

2 Scientific content

The objective of the school was to provide participants with mathematical foundations and essential tools in number theory and cryptography. The final list of the seven courses is:

- Cécile Armana (Université de Franche-Comté, France): *Algorithmic number theory*
- Sorina Ionica (Université Picardie Jules Vernes, France) : *La cryptographie basée sur les courbes elliptiques* – online
- Claude Levesque (Université Laval, Canada): *Some aspects of algebraic number theory related with cryptography*
- Florian Luca (University of the Witwatersrand, South Africa): *Diophantine equations*
- Abderrahmane Nitaj (Université de Caen, France): *La cryptographie basée sur les réseaux* – online
- Alain Togbé (Purdue University Northwest, USA): *Elementary number theory and cryptography*
- Michel Waldschmidt (Sorbonne Université, France): *Elementary approach to elliptic curves*

A total of 49 hours of lectures was delivered, including exercise sessions. Two lecturers, unable to attend the school, gave their course and exercises online using Zoom. A list of bibliographical references and recommended readings for all the courses was given to the participants a couple of weeks before the school.

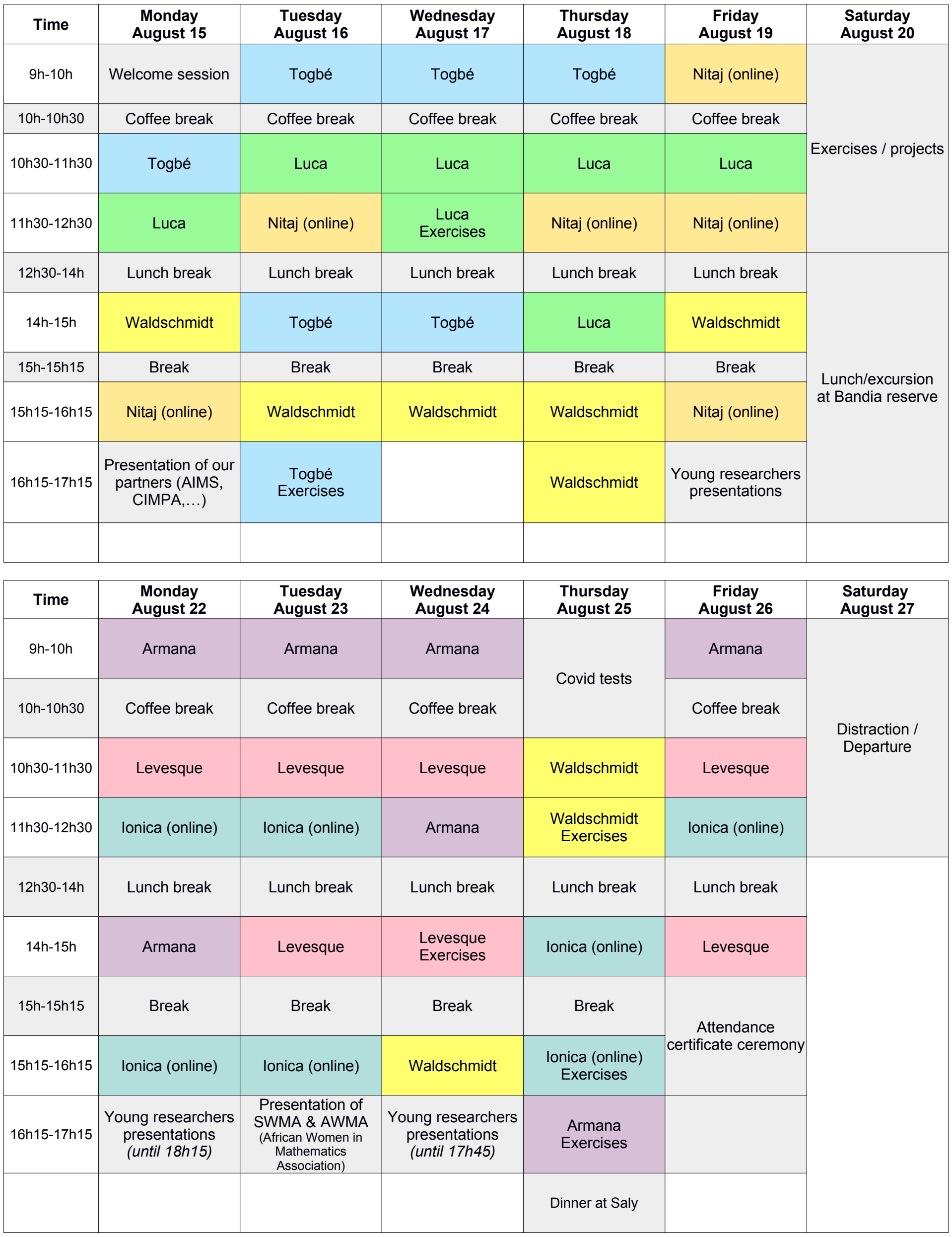
Besides the courses, we also hosted nine contributed research presentations (20 minute each) by young participants:

- Kouèssi Norbert Adedji (Institut de Mathématiques et de Sciences Physiques, Benin): *The extension of the $D(-k)$-triple $\{1, k, k+1\}$ to a quadruple*
- Virgile Dossou-Yovo (Institut de Mathématiques et de Sciences Physiques, Benin): *Improved Cryptanalysis of RSA*
- Seny Fadera (Université Gaston Berger de Saint-Louis, Senegal): *Le cryptosystème KMOV et ses variantes : Étude, Attaque et Implémentation*
- Alioune Gueye (Université Gaston Berger de Saint-Louis, Senegal): *An exponential equation involving k-Fibonacci numbers*
- Seyni Kane (Université Gaston Berger de Saint-Louis, Senegal): *Server-Supported Signatures for Mobile Devices*
- Patrick Nyadjo Fonga (AIMS Cameroon): *Finite rational sets matching by homography*
- Ephraim Poncho-Kotey (AIMS Ghana): *The Kirkman School Girls Problem*
- Safia Seffah (Université des Sciences et de la Technologie Houari-Boumediene, Algiers, Algeria): *On Fermat and Mersenne numbers expressible as product of two k-Fibonacci numbers*
- Charles Tougma (Université Thomas Sankara, Burkina Faso): *On dihedral (D_4)-Pólya fields*

The languages of the school were French and English. Courses were taught mostly in English, occasionally French. Young researchers gave their presentations mostly in French.

We also hosted presentations of our partners (CIMPA, AIMS, IMU,...), and of the Senegalese and African Women in Mathematics Associations.

Timetable of the school



Time	Monday August 15	Tuesday August 16	Wednesday August 17	Thursday August 18	Friday August 19	Saturday August 20
9h-10h	Welcome session	Togbé	Togbé	Togbé	Nitaj (online)	Exercises / projects
10h-10h30	Coffee break	Coffee break	Coffee break	Coffee break	Coffee break	
10h30-11h30	Togbé	Luca	Luca	Luca	Luca	
11h30-12h30	Luca	Nitaj (online)	Luca Exercises	Nitaj (online)	Nitaj (online)	
12h30-14h	Lunch break	Lunch break	Lunch break	Lunch break	Lunch break	Lunch/excursion at Bandia reserve
14h-15h	Waldschmidt	Togbé	Togbé	Luca	Waldschmidt	
15h-15h15	Break	Break	Break	Break	Break	
15h15-16h15	Nitaj (online)	Waldschmidt	Waldschmidt	Waldschmidt	Nitaj (online)	
16h15-17h15	Presentation of our partners (AIMS, CIMPA,…)	Togbé Exercises		Waldschmidt	Young researchers presentations	

Time	Monday August 22	Tuesday August 23	Wednesday August 24	Thursday August 25	Friday August 26	Saturday August 27
9h-10h	Armana	Armana	Armana	Covid tests	Armana	Distraction / Departure
10h-10h30	Coffee break	Coffee break	Coffee break		Coffee break	
10h30-11h30	Levesque	Levesque	Levesque	Waldschmidt	Levesque	
11h30-12h30	Ionica (online)	Ionica (online)	Armana	Waldschmidt Exercises	Ionica (online)	
12h30-14h	Lunch break	Lunch break	Lunch break	Lunch break	Lunch break	
14h-15h	Armana	Levesque	Levesque Exercises	Ionica (online)	Levesque	
15h-15h15	Break	Break	Break	Break	Attendance certificate ceremony	
15h15-16h15	Ionica (online)	Ionica (online)	Waldschmidt	Ionica (online) Exercises		
16h15-17h15	Young researchers presentations *(until 18h15)*	Presentation of SWMA & AWMA (African Women in Mathematics Association)	Young researchers presentations *(until 17h45)*	Armana Exercises		
				Dinner at Saly		

3 Organization

The school benefitted from the very good equipment at AIMS Senegal. It took place in a comfortable classroom equipped with a large interactive digital board which can be used as a blackboard, a videoprojector and an additional blackboard. Each participant had a desk with a PC provided by AIMS, equipped with Ubuntu, Zoom, Python,... (some participants also brought their own laptop). A very reliable Wifi connection was available. Two online courses took place using Zoom.

At this period – before the new academic year – we were able to benefit from the accommodation facilities at AIMS: shared rooms in the student residence, single rooms in the professor residence, with all the necessary comfort and Wifi connection and within a short walking distance to AIMS Center. This facilities were provided at a very affordable price (15€ for a student, 30€ for a professor per weekday). Even though there was no direct financial contribution from AIMS Senegal for this school, we would like to emphasize this important indirect contribution. It explains why the total budget of this school is lower than for other similar events, and we are very grateful to AIMS Senegal for having given us access to these facilities.

All meals were taken at the AIMS Center during weekdays, and at the student residence during the weekend. A lunch–excursion at the Bandia natural reserve took place on the first weekend, and a social dinner at Saly on the second week. The drivers of AIMS took care of some of our small daily trips during the school, and transportation to and from Dakar international airport.

Fortunately the situation regarding the Covid pandemic was much more favorable than last year. Vaccinated travellers did not required a Covid to enter Senegal. Out of 10 CIMPA participants, only 5 required Covid tests for their trip and the others were vaccinated (some of them have been vaccinated specially for the school). As a consequence, the organizational and financial impact of these Covid tests is moderate: about 450€ which is much less than the 1500€ we had for the EMA school.

4 Outcome

An anonymous survey conducted after the school showed that the participants were overall very satisfied. Most of them very positively mentioned the content of the courses and the dedication of the lecturers, and insisted on the importance for participants of making contact with new people with similar mathematical interests. One participant said that the school also helped identify her/his mathematical gaps. Another said s/he would have preferred all courses to be held on site (a comment that could be agreed upon). Another participant appreciated the fact that speakers and participants regularly had their meals together, which provided opportunities for extra discussions. Finally one participant thanked the school for showing that “women have the same rights on mathematics as men”.

As for the impact, we believe this school has:

- consolidated the links in number theory between Senegal and France,
- helped to promote the development of research in number theory in Senegal,

- encouraged young people from Senegal, and more generally West Africa, to pursue a PhD thesis in number theory or cryptography, especially among women,
- helped us identify promising young researchers that we will support during their thesis and early career.

We are planning some follow-up activities:

- a Research School on number theory and arithmetic geometry in Gabon (December 2022, `https://indico.math.cnrs.fr/e/algebraicdaysgabon22`),
- at the request of a faculty participant, a project of EMA/CIMPA schools in Togo is also in discussion for the following years.

We are very grateful to AIMS Senegal for hosting and supporting the school, helping immensely with the organization and managing the school's fundings, providing excellent housing and working conditions, and a very pleasant environment, and for the availability and professionalism of all its staff. We also would like to warmly thank all the institutions and organizations that have supported it and contributed to its success, in particular the CIMPA.

The organizers,

Cécile Armana,
Assistant Professor, University of Franche-Comté, France, `cecile.armana@univ-fcomte.fr`

Bernadette Faye,
Assistant Professor, University Gaston Berger at Saint-Louis, Senegal, `bernadette.fayee@gmail.com`

5 Participants

Format of the list: last name, first name, gender ([F] or [M]), status, affiliation and country of affiliation, email address.

1. Adedji Kouèssi Norbert, [M], Postdoc, Institut de Mathématiques et Sciences Physiques, Dangbo, Benin, `adedjnorb1988@gmail.com`
2. Armana Cécile, [F], Professor, Université de Franche-Comté, Besançon, France, `cecile.armana@univ-fcomte.fr`
3. Ba Ousmane Mamadou Sada, [M], PhD student, Université Cheikh Anta Diop, Dakar, Senegal, `juniorouse@live.fr`
4. Bah Elhadj Amadou, [F], Bachelor student, Université Cheikh Anta Diop, Dakar, Senegal, `elamadoubah945@gmail.com`
5. Cisse Amina, [F], Bachelor student, Université Cheikh Anta Diop, Dakar, Senegal, `cisseamina113@gmail.com`
6. Dia El Hadji Mamadou, [M], Master student, Université Gaston Berger de Saint-Louis, Senegal, `eldjimdia@gmail.com`
7. Diop Fatou, [F], Master student, Université Gaston Berger de Saint-Louis, Senegal, `fatoudiop1595@gmail.com`

8. Diop Ndeye Seye, [F], PhD student, Université Alioune Diop de Bambey, Senegal, `n.diop5348@zig.univ.sn`
9. Diouf Dior, [F], Bachelor degree, Université Cheikh Anta Diop, Dakar, Senegal, `diordiouf1996@gmail.com`
10. Dossou-Yovo Virgile Sèdjro Romuald, [M], Postdoc, Institut de Mathématiques et Sciences Physiques, Dangbo, Benin, `dosvirs20@gmail.com`
11. Edjeou Bilizimbéyé, [M], Postdoc, Université Gaston Berger de Saint-Louis, Senegal, `edjeou@bilizimbeye@ugb.edu.sn`
12. Fadera Seny, [H], Master student, Université Gaston Berger de Saint-Louis, Senegal, `faderaousseynou@gmail.com`
13. Faye Bernadette, [F], Professor, Université Gaston Berger de Saint-Louis, Senegal, `bernadette.fayee@gmail.com`
14. Faye Mariama Ndao, [F], PhD student, Université Gaston Berger de Saint-Louis, Senegal, `fayemariamandao@gmail.com`
15. Gueye Alioune, [M], PhD student, Université Gaston Berger de Saint-Louis, Senegal, `gueye.alioune2@ugb.edu.sn`
16. Hane Marie Diamy, [F], Bachelor student, Université Gaston Berger de Saint-Louis, Senegal, `hanemariediamy@gmail.com`
17. Ionica Sorina, Professor, Université Picardie Jules Verne, France, `sorina.ionica@u-picardie.fr` — **online**
18. Kagny Ibrahima, [M], Master student, Université Check Anta Diop, Dakar, Senegal, `ibrahimakgny00@gmail.com`
19. Kakanou Kossi Richmond, [M], Master student, Université Cheikh Anta Diop, Dakar, Senegal, `kakori98@gmail.com`
20. Kam Tsemo Sandra Marion, [F], Master student, AIMS Senegal, `sandra.m.k.tsemo@aims-senegal.org`
21. Kane Seyni, [M], Master student, Université Gaston Berger de Saint-Louis, Senegal, `kane.seyni@ugb.edu.sn`
22. Kaningini Lutala Netho Junior, [M], Master student, AIMS Senegal, `netho.j.k.lutala@aims-senegal.org`
23. Kemche Merline Huguette, [F], PhD student, visiting student AIMS Senegal, `kmerlineh@gmail.com`
24. Levesque Claude, [M], Professor, Université Laval, Canada, `Claude.Levesque@mat.ulaval.ca`
25. Luca Florian, [M], Professor, University of the Witwatersrand, South Africa, `Florian.Luca@wits.ac.za`
26. Mahi Affly Roce Aurélie Claude, [F], PhD Student, Université Félix Houphouët Boigny, Abidjan, Ivory Coast, `roceaffly@gmail.com`
27. Mballo Ama Sékou, [M], PhD student, Université de Thiès, Senegal, `amasekou.mballo@univ-thies.sn`

28. Mbaye Mouhamed Lamine, [M], PhD student, Université Cheikh Anta Diop, Dakar, Senegal, `lamine0093@gmail.com`
29. Nwaeme Christian Nnaemeka, [M], Master student, AIMS Senegal, `christian.n.nwaeme@aims-senegal.org`
30. Ndiongue Mohamed Lamine, [M], Master student, Université Gaston Berger de Saint-Louis, Senegal, `ndionguemohamedlamine@gmail.com`
31. Ngom Ablaye, [M], Bachelor student, Université Cheikh Anta Diop, Dakar, Senegal, `ngomstar39@gmail.com`
32. Nitaj Abderrahmane, Professor, Université de Caen Normandie, France, `abderrahmane.nitaj@unicaen.fr` — **online**
33. Nyadjo Fonga Patrick, [M], Master student, AIMS Cameroon, `patrick.fonga@aims-cameroon.org`
34. Nyamsi Senegue Gomez, [M], PhD Student, Université de Dchang, Cameroon, `nyamsigomez@gmail.com`
35. Poncho-Kotey Ephraim Nii Amon, [M], PhD student, University of Ghana, `ephraim.poncho@aims.ac.rw`
36. Ravelomanana Vlady, [M], Professor, Université Paris Cité, France, `vlad@irif.fr`
37. Seffah Safia, [F], PhD student, Université des Sciences et de la Technologie Houari-Boumediene, Algiers, Algeria, `safiaseffah58@gmail.com`
38. Sylla Khady, [F], Bachelor student, Université Cheikh Anta Diop, Dakar, Senegal, `khs.sylla2000@gmail.com`
39. Thiam Omar, [M], Master student, Université Gaston Berger de Saint-Louis, Senegal, `louis Senegal thiamomar753@gmail.com`
40. Tiebekabe Pagdame, [M], Postdoc, Université Cheikh Anta Diop, Dakar, Senegal and Togo, `tpagdame.math@gmail.com`
41. Togbe Alain, [M], Professor, Purdue University Northwest, USA, `atogbe@pnw.edu`
42. Tougma Charles Wend-Waoga, [M], Postdoc, Université Thomas Sankara, Ouagadougou, Burkina Faso, `tougmacharles@yahoo.fr`
43. Waldschmidt Michel, [M], Professor, Sorbonne Université, Paris, France, `michel.waldschmidt@imj-prg.fr`
44. Youego Joseline, [F], PhD Student, Université de Ngaoundéré, Cameroon, `joselineyouego@yahoo.fr`

6 Financial report

Grants received for the organization of this school:

CIMPA	12,000 €
CIMPA (Covid tests only)	2,000 €
CNRS (France) – SENAREX project (*)	7,938 €
Travel grants from lecturers	4,413 €
Number Theory Foundation	2,085 €
Foundation Compositio Mathematica	2,000 €
International Centre for Theoretical Physics (ICTP)	2,000 €
International Mathematical Union – CDC (IMU)	2,000 €
Total	*34,436 €*

(*) SENAREX (écoles SENégalaises en ARithmétique et mathématiques EXplicites) is a two-year project funded by CNRS as a result of the call for proposals *Dispositif de Soutien aux Collaborations avec l'Afrique subsaharienne.* Led by Cécile Armana and Bernadette Faye, it contributed to funding three mathematical schools that were held at AIMS Senegal in 2021/22: this African Mathematical School, the workshop *Women in Sage in Senegal*, and the CIMPA school in 2022.

Among the funds received for this CIMPA school, 40% were granted by the CIMPA. This is in accordance with the CIMPA guidelines (no more than 1/2 of the total budget of the school should be provided by CIMPA).

Detail of the expenses made with the CIMPA funding:

Plane tickets for 6 CIMPA participants (**)	3,773.66€
Lodging for 29 young participants (8 CIMPA participants, 21 locals)	2,523.66€
Meals for 31 young participants and lecturers (10 CIMPA participants, 21 locals) + coffee breaks and mineral water	5,548.85€
Covid tests for 5 CIMPA participants	418.17€
Total of CIMPA expenses	*12,264.34€*

(**) Names of those CIMPA participants : Affly Roce Aurélie Mahi (Ivory Coast), Patrick Nyadjo fonga (Cameroon), Senegue Gomez Nyamsi (Cameroon), Tiebekabe Pagdame (Togo), Joseline Youego (Cameroon). Other CIMPA participants had their plane tickets covered by CNRS, ICTP, IMU.

54% of the CIMPA financial support was used for travel and living expenses of CIMPA participants. Unfortunately this is less than stated in the CIMPA guidelines ("At least 2/3 of the CIMPA financial support needs to be used for travel and/or living expenses of CIMPA participants"). The reason is the last-minute cancellation of a CIMPA participant from Sudan who could not get her visa in time.

A final figure: outside of the travel grants, 20% of the school budget was used to cover expenses for some lecturers (plane tickets, lodging, meals) and the CIMPA representative (lodging, meals).

7 Descriptions of the courses

Cécile Armana (Université de Franche-Comté, France): **Algorithmic number theory**

Number theory has long been inseparable from algorithms. Finding efficient algorithms may help to understand the structure of numbers and to explore this structure, we are assisted by the algorithms we already have. In this course we will start with classical algorithms and their analysis (Horner method for evaluating polynomials, modular arithmetic, Euclidean algorithms, exponentiation by squaring,...). We will then focus on algorithms more specific to number theory (squares modulo a prime number, (pseudo)-primality tests, factorization of integers). If time allows, we will discuss advanced algorithms based on elliptic curves (Schoof's algorithm for counting points on elliptic curves over finite fields, Lenstra's factorization algorithm of integers, elliptic curve primality tests).

References:

- Victor Shoup, *A computational introduction to number theory and algebra.* Cambridge University Press, second edition (2008). File available at `https://shoup.net/ntb/ntb-v2.pdf`
- Steven Galbraith, *Mathematics of Public Key Cryptography.* Cambridge University Press (2012). Full extended text available at `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`
- Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, Second Edition. Springer (2005).
- David Bressoud, *Factorization and Primality Testing.* Undergraduate Texts in Mathematics, Springer (1989).
- Henri Cohen, *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics, Springer (1993).

Sorina Ionica (Université Picardie Jules Vernes, France) : **La cryptographie basée sur les courbes elliptiques** – online

Ce cours aborde les principaux thèmes mathématiques pour s'initier à la cryptographie basée sur les courbes elliptiques. Le cours est composé des chapitres suivants :
Chapitre 1 : Le protocole de Diffie-Hellman et le système d'ElGamal - mise en oeuvre à l'aide des courbes elliptiques
Chapitre 2 : Attaques élémentaires du problème du logarithme discret sur des courbes elliptiques
Chapitre 3 : Introduction à la cryptographie à base d'isogénies.

Références :

- Steven Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, 2012. Full extended text available at
  `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`
- Antoine Joux, *Algorithmic Cryptanalysis*, Chapman and Hall/CRC (24 juin 2009).
- Joseph Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer Verlag, 2009.
- *Handbook of elliptic and hyperelliptic curve cryptography*, Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren, Chapman and Hall/CRC, 2005.

Claude Levesque (Université Laval, Canada): **Some aspects of algebraic number theory related with cryptography**

This course will focus on binary quadratic forms. There are useful to compute the class number of real quadratic fields. There is a cryptosystem based on the class group of quadratic fields that resists attacks made with quantum computers.

Florian Luca (University of the Witwatersrand, South Africa): **Diophantine equations**

Linear equations, quadratic equations (parametrization of Pythagorean triples, Pell equations), Applications of modular arithmetic to the resolution of exponential Diophantine equations. Applications of linear forms in logarithms.

References:

- Y. Bugeaud, *Linear forms in logarithms and applications*, IRMA Lectures in Mathematics and Theoretical Physics, 28. European Mathematical Society (EMS), Zürich, 2018.
- B. M. M. de Weger, B. M. M. *Algorithms for Diophantine equations.* CWI Tract, 65. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. File available at `https://www.win.tue.nl/~bdeweger/downloads/CWI%20Tract%2065.pdf`
- F. Luca, Exponential Diophantine equations, *Notes from the International Autumn School on Computational Number Theory*, 267–309, Tutor. Sch. Workshops Math. Sci., Birkhäuser/Springer, Cham, 2019. File available at `https://link.springer.com/content/pdf/10.1007%2F978-3-030-12558-5_4.pdf`
- T. N. Shorey; R. Tijdeman, *Exponential Diophantine equations.* Cambridge Tracts in Mathematics, 87. Cambridge University Press, Cambridge, 1986.

Abderrahmane Nitaj (Université de Caen, France): **La cryptographie basée sur les réseaux** – online

Ce cours aborde les principaux thèmes mathématiques pour s'initier à la cryptographie basée sur les réseaux. Le cours est composé des chapitres suivants :
Chapitre 1: Introduction aux réseaux et aux problèmes difficiles.
Chapitre 2 : Les système NTRU et LWE.
Chapitre 3: Application des réseaux à la cryptanalyse de RSA et de NTRU.
Chaque chapitre sera mis en pratique à l'aide du système de calcul Python.

Références :

- Nguyen, Phong Q., Vallée, Brigitte: *The LLL Algorithm, Survey and Applications*, Information Security and Cryptography, Springer-Verlag Berlin Heidelberg 2010.
- Tancrède Lepoint: *Design and Implementation of Lattice-Based Cryptography*, Cryptography and Security, École Normale Supérieure de Paris - ENS Paris, 2014. Available at `https://tel.archives-ouvertes.fr/tel-01069864/document`
- Chris Peikert: *A Decade of Lattice Cryptography*, February 17, 2016. Available at `https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`
- Federico Bergami: *Lattice-Based Cryptography*, ALGANT Master's Thesis - 20 July 2016. Available at `https://www.math.u-bordeaux.fr/~ybilu/algant/documents/theses/BERGAMI.pdf`

Alain Togbé (Purdue University Northwest, USA): **Elementary number theory and cryptography**

In this course, we will introduce the basics of the elementary number theory to introduce cryptography. So we will use the theory of congruences to gently introduce cryptography. We will start from the Caesar cipher to present the public-key cryptography. We will also discuss the knapsack cryptosystem (which is based on the difficult classic problem in combinatorics known as the knapsack problem) and the discrete logarithm problem.

References:

- David M. Burton, *Elementary Number Theor*y, seventh edition, McGraw-Hill.
- J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer.

Michel Waldschmidt (Sorbonne Université, France): **Elementary approach to elliptic curves**

Examples of elliptic curves, drawing elliptic curves, the set of rational points of an elliptic curve, intersection of a line and an elliptic curve, the point at infinity of an elliptic curve, basics of projective geometry, 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, applications to cryptography.

Lecture notes:
`http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/EllipticFunctions.pdf`

References:

- J. H. Silverman, *The Arithmetic of Elliptic Curves*, Chapters III, V and VIII. (Graduate Texts in Mathematics) 2nd ed. 2009 Edition, Springer.
- K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, (Graduate Texts in Mathematics) 2nd ed. 1998, Springer.

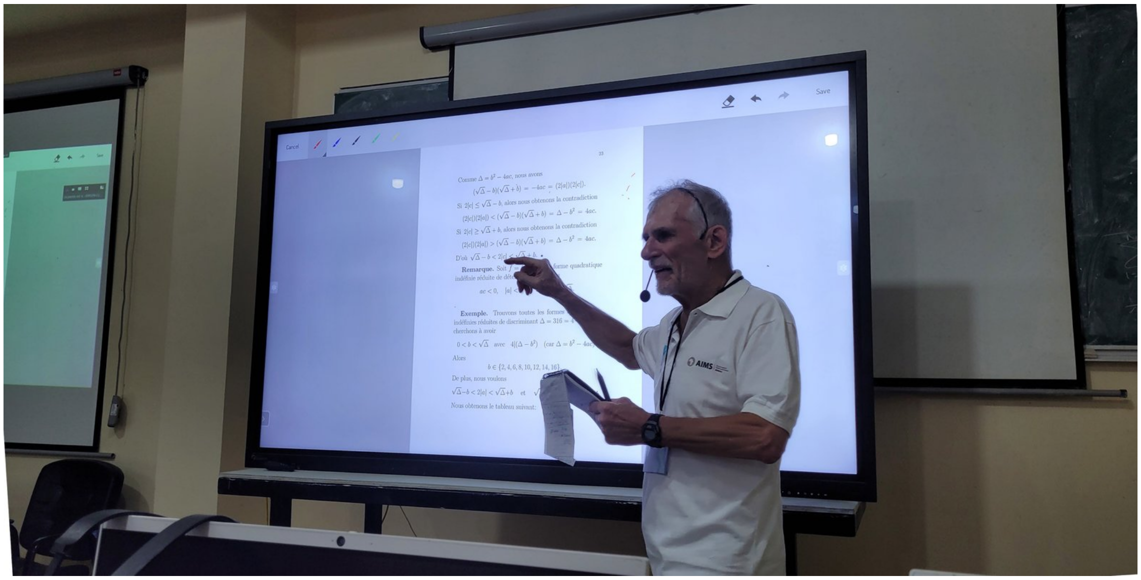
8 Pictures

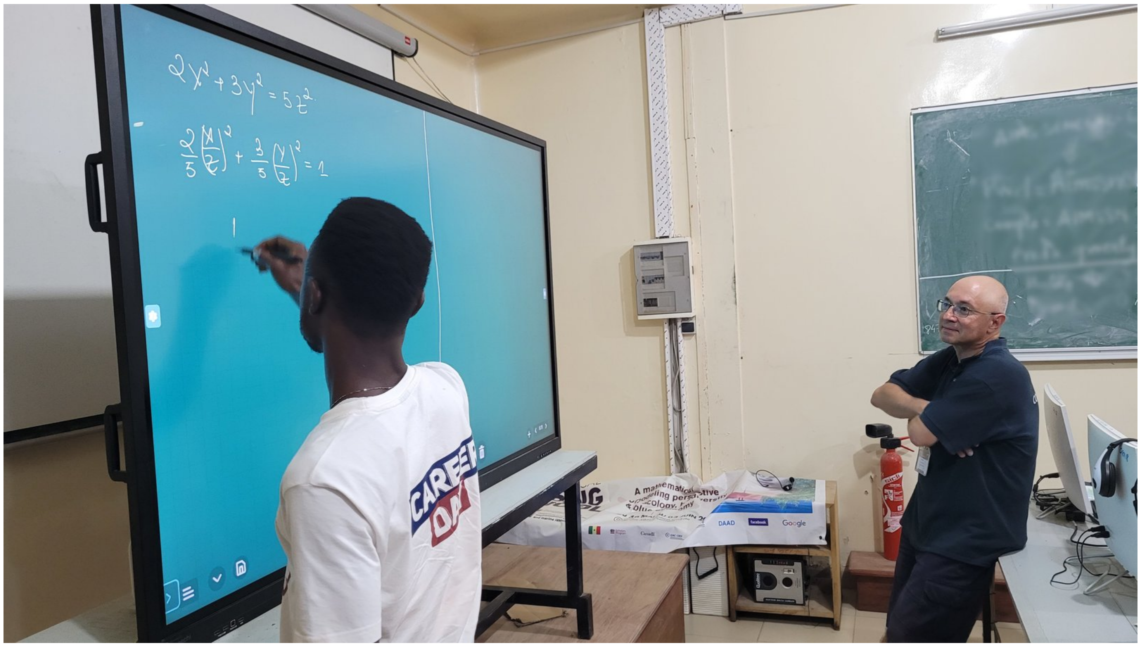
AIMS
CIMPA
AIMS
RENCONTRE ANNUELLE DES JEUNES SCIENTIFIQUES
Lieu :
AIMS Sénégal, Mbour
ICTP
PROJET ANR FLAIR

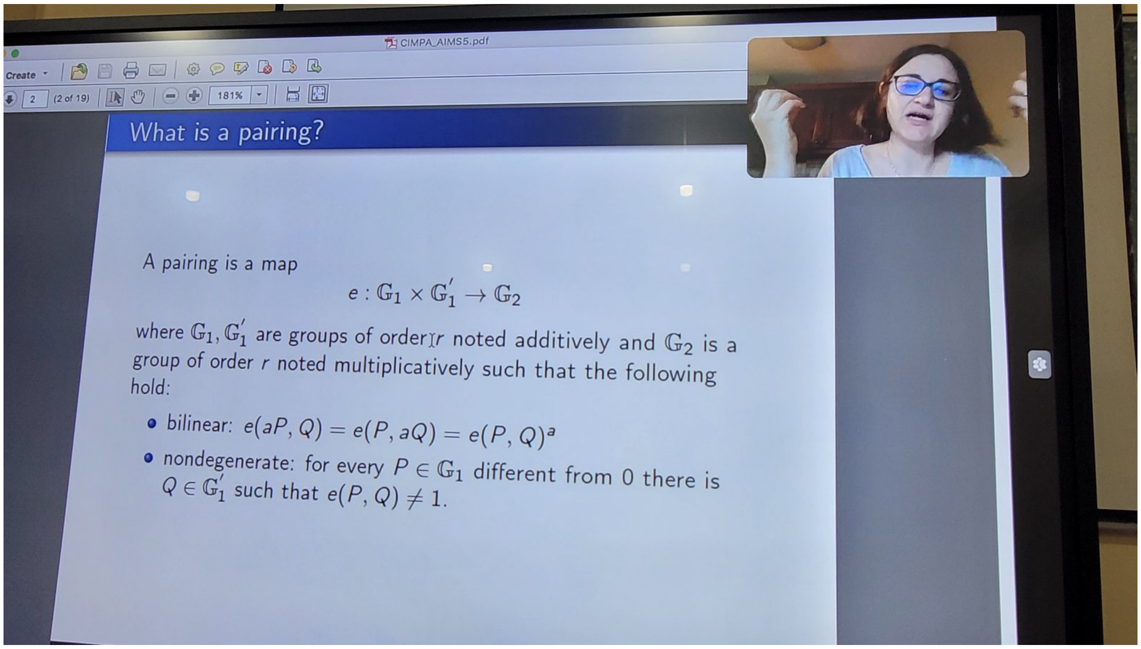
CIMPA
AIMS
African Institute for Mathematical Sciences
SENEGAL
RENCONTRE ANNUELLE DES JEUNES SCIENTIFIQUES
Introduction à la théorie des nombres, à la cryptographie et aux cours connexes.
Lieu :
AIMS Sénégal, Mbour
Promouvoir et développer la recherche en mathématiques (algèbre, théorie des nombres et cryptographie)
Attirer de nouveaux étudiants et offrir une plateforme aux jeunes chercheurs
Coopération internationale pour le progrès scientique
ICTP
The Abdus Salam International Centre for Theoretical Physics
IAEA
INTERNATIONAL MATHEMATICAL UNION
CDC
GANDA
The POSTCRYPTUM project
PROJET ANR FLAIR
UNIVERSITé DE FRANCHE-COMTé
Lm^B
mathrice

AIMS

Euclidean division of μ by λ:
μ = nλ + ν
n ∈ ℤ
0 ≤ ν < λ.
ν = μ − n
If λ ∈ ℝ, ℤλ = {aλ | a ∈ ℤ}
is a discret subgroup of ℝ.
Conversely: G ⊂ ℝ discrete, G ≠ {0}
G ∩ ℝ>0 ≠ ϕ ∃λ ∈ G ∩ ℝ>0, smallest
element > 0 in G Let μ ∈ G




$2x^2 + 3y^2 = 5z^2$
$\frac{2}{5}\left(\frac{x}{z}\right)^2 + \frac{3}{5}\left(\frac{y}{z}\right)^2 = 1$
CAREER DAY
DAAD
Google



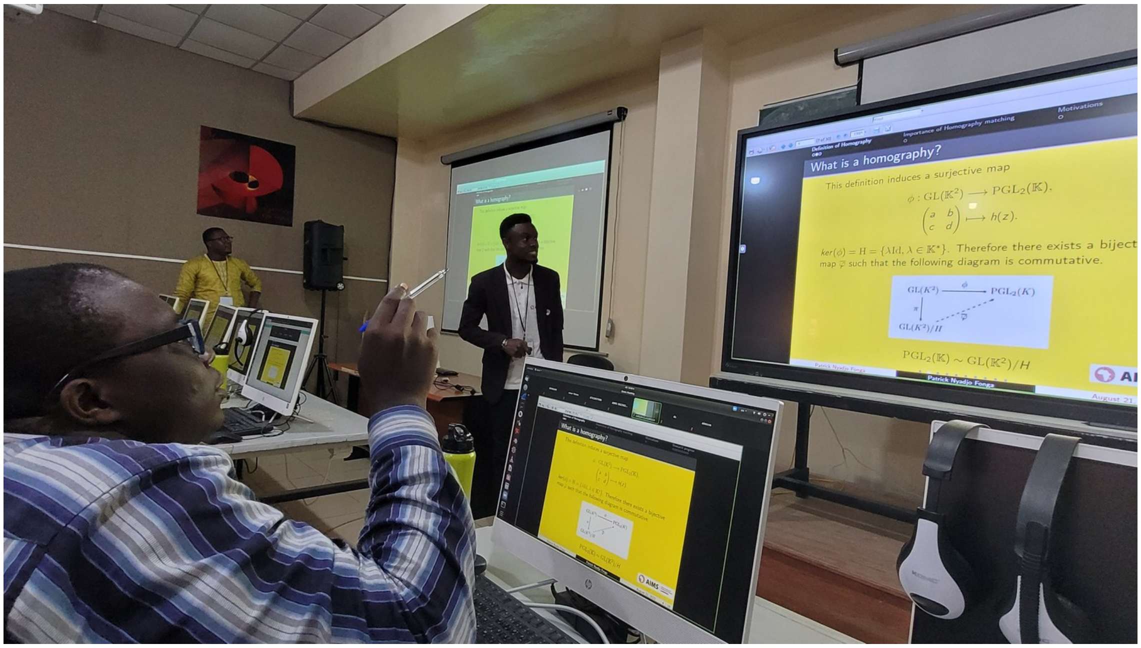
What is a pairing?

A pairing is a map

$$e : \mathbb{G}_1 \times \mathbb{G}_1' \to \mathbb{G}_2$$

where $\mathbb{G}_1, \mathbb{G}_1'$ are groups of order r noted additively and $\mathbb{G}_2$ is a group of order r noted multiplicatively such that the following hold:

- bilinear: $e(aP, Q) = e(P, aQ) = e(P, Q)^a$
- nondegenerate: for every $P \in \mathbb{G}_1$ different from 0 there is $Q \in \mathbb{G}_1'$ such that $e(P, Q) \neq 1$.

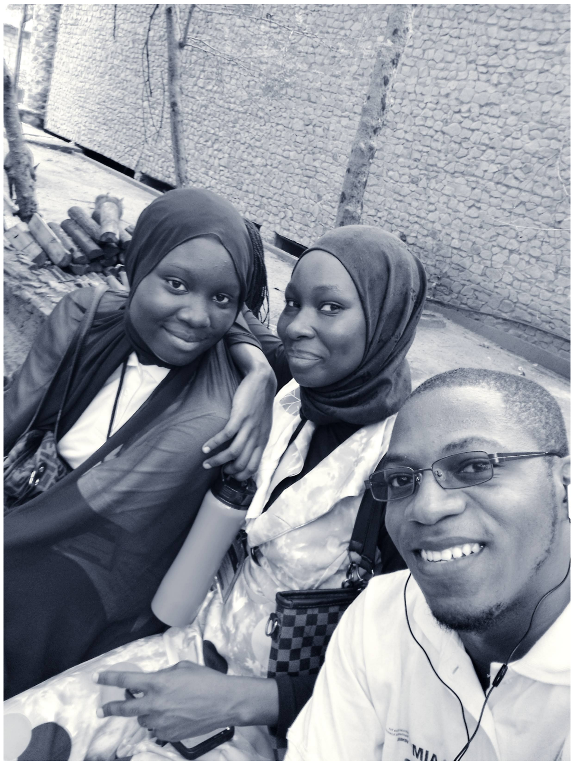

Definition of Homography
Importance of Homography matching
Motivations
What is a homography?
This definition induces a surjective map
$\phi : \mathrm{GL}(\mathbb{K}^2) \longrightarrow \mathrm{PGL}_2(\mathbb{K})$.
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto h(z)$.
$ker(\phi) = \mathrm{H} = \{\lambda \mathrm{Id}, \lambda \in \mathbb{K}^*\}$. Therefore there exists a biject
map $\overline{\varphi}$ such that the following diagram is commutative.
$\mathrm{GL}(K^2) \xrightarrow{\phi} \mathrm{PGL}_2(K)$, π, $\overline{\varphi}$, $\mathrm{GL}(K^2)/H$
$\mathrm{PGL}_2(\mathbb{K}) \sim \mathrm{GL}(\mathbb{K}^2)/H$
Patrick Nyadjo Fonga
August 21

Definition:
$0 < b < \sqrt{\Delta}$
$\Delta = b^2 - 4ac$
$\sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$
$2 | b$

IMPA
AIMS

SWMA
Association Sénégalaise des Femmes en Maths(SWMA)
Présenté par
Dr. Bernadette Faye
August 23, 2022

MILANO



Dior
MILANO
CIMPA
AIMS

PA
AIMS
African Institute for Mathematical Sciences SENEGAL
RENCONTRE
NNUELLE DES JEUN
SCIENTIFIQUES
Introduction à la
à la cryptographie
Lieu :
AIMS Sénég
Promouvoir et développer la recherche en mathématiques (algèbre, théorie des nombres et cryptographie)
Attirer de nouveaux étudiants et offrir une plateforme aux jeunes chercheurs
Coopération internationale pour le progrès scientifique
ICTP
PROJET ANR FLAIR
AIMS