Scientific Report on the CIMPA Research School
Arithmétique algorithmique et cryptographie

May 7 – 18, 2018

University of Kinshasa, Democratic Republic of Congo

The school took place in the Faculté des Sciences of the University of Kinshasa, Kinshasa, from May 7 to May 18, 2018. It gathered about 50 participants:

- 7 mathematicians from several countries (France, Italy, Ivory Coast, Madagascar, USA) who gave 40 hours of lectures on selected topics as well as exercise sessions,
- 8 young participants from neighbouring countries (Benin, Cameroon, Congo-Brazzaville, Ivory Coast, South Africa), master students or PhD students, in number theory or cryptography,
- about 40 regular local participants from the University of Kinshasa and other universities in DRC, mathematicians or computer scientists, students or researchers, interested in the topics of this school.

According to local and external attendees, this school was a great success. It succeeded particularly well in gathering people from different mathematical backgrounds with interests in computational aspects of number theory and cryptography. Attendance remained high until the end of the school. Participants took a very active part by asking questions during lectures or solving exercises during tutorial sessions. As few participants were at ease with English, all courses were ultimately given in French.

One of the highlights of the school was an introduction and several tutorial sessions devoted to SageMath, in connection with the content of the lectures. Before the school, this software was essentially unknown to most participants, and only a few of them have had experience with a mathematical software. We took the time to set up SageMath on personal computers of participants and we devoted 6 hours to learning and using it in different number-theoretic contexts. SageMath was a perfect choice for this school since some attendees with a background in computer science were already acquainted with Python, the language on which it is based. The versatility of SageMath has raised a lot of interest. Several participants have expressed their wish to continue using it in the future for their research or teaching.

The website of the school:

`https://indico.math.cnrs.fr/e/cimpakinshasa2018/`

contains teaching material related to the school and made available to the participants.

We believe this school will have a mid and long-term impact on number theory in the Democratic Republic of Congo and surrounding countries. The local organizers are already planning future developments, in form of invitation of lecturers for intensive courses on similar topic for a longer period.

We would like to thank the International Mathematical Union for its generosity, which contributed to the undeniable success of this school.

The organizers,

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

Rebecca Walo Omana,
Full Professor, University of Kinshasa, D. R. of Congo, rebecca.walo@unikin.ac.cd

Appendix 1: List of courses and speakers

- *Applications de la théorie élémentaire des nombres à la cryptographie* – Alain Togbé (Purdue University Northwest, USA)
- *Fonctions génératrices et applications* – Fanja Rakotondrajao (University of Antananarivo, Madagascar)
- *Les courbes elliptiques et leur arithmétique* – Francesco Pappalardi (University Roma 3, Italy) and Cécile Armana (University of Franche-Comté, France)
- *Théorie algébrique des nombres et corps finis, en lien avec la théorie des codes* – Michel Waldschmidt (University Paris 6, France) and Antoine Kitombole (University of Kinshasa, DRC)
- *Décompositions polynomiales et quelques algorithmes de factorisation sur les corps finis* – François Tanoé (University Félix-Houphouët-Boigny, Ivory Coast)
- *Une introduction aux cryptosystèmes basés sur les courbes elliptiques et à leur sécurité* – Sorina Ionica (University of Picardie, France)

In addition, 4 hours were devoted to exercise sessions and 6 hours to tutorial sessions on SageMath.

Appendix 2: Timetable

See next page.

École CIMPA Kinshasa 2018 - emploi du temps (version du 19/05/2018)

Cours 1 : *Applications de la théorie élémentaire des nombres à la cryptographie* (A. Togbé) - 6 heures
Cours 2 : *Fonctions génératrices et applications* (F. Rakotondrajao) - 6 heures
Cours 3 : *Les courbes elliptiques et leur arithmétique* (F. Pappalardi et C. Armana) - 6+3 heures
Cours 4 : *Algebraic number theory and Finite fields in connection with coding theory* (M. Waldschmidt et A. Kitombole) - 8+1 heures
Cours 5 : *Décompositions polynomiales et quelques algorithmes de factorisation sur les corps finis* (F. Tanoé) - 6 heures
Cours 6 : *An introduction to curve-based cryptosystems and their security* (S. Ionica) - 6 heures
TD et TP Sage : 9 heures *(répartis entre les différents cours)*

	Lundi 7 mai	**Mardi 8 mai**	**Mercredi 9 mai**	**Jeudi 10 mai**	**Vendredi 11 mai**
9h00-9h50	Cours 1 (Togbé)	Cours 1 (Togbé)	TD (Togbé)	Cours 1 (Togbé)	Cours 2 (Rakotondrajao)
9h50-10h00	*Pause*	*Pause*	*Pause*	*Pause*	*Pause*
10h00-10h50	Cours 2 (Rakotondrajao)	Cours 2 (Rakotondrajao)	Cérémonie d'ouverture	Cours 2 (Rakotondrajao)	Cours 3 (Armana)
10h50-11h10	*Pause café*	*Pause café*	*Pause café*	*Pause café*	*Pause café*
11h10-12h00	Cours 3 (Pappalardi)	Cours 3 (Pappalardi)	TD (Pappalardi) Présentation de SageMath (Armana)	Cours 3 (Pappalardi)	Cours 4 (Waldschmidt)
12h00-14h00	*Pause déjeuner*	*Pause déjeuner*	*Cocktail et pause déjeuner*	*Pause déjeuner*	*Photo de groupe et pause déjeuner*
14h00-14h50	Cours 1 (Togbé)	Cours 1 (Togbé)	*Excursion*	Cours 1 (Togbé)	Cours 6 (Ionica)
14h50-15h10	*Pause café*	*Pause café*		*Pause café*	*Pause café*
15h10-16h00	Cours 2 (Rakotondrajao)	Cours 2 (Rakotondrajao)		Cours 3 (Pappalardi)	TP (Armana / Ionica)
16h00-16h10	*Pause*	*Pause*		*Pause*	*Pause*
16h10-17h00	Cours 3 (Pappalardi)	Cours 3 (Pappalardi)		TD (Rakotondrajao)	Cours 4 (Waldschmidt)

	Lundi 14 mai	**Mardi 15 mai**	**Mercredi 16 mai**	**Jeudi 17 mai**	**Vendredi 18 mai**
9h00-9h50	Cours 3 (Armana)	Cours 5 (Tanoé)	Cours 5 (Tanoé)	Cours 4 (Waldschmidt)	TP (Armana)
9h50-10h00	*Pause*	*Pause*	*Pause*	*Pause*	*Pause café*
10h00-10h50	Cours 5 (Tanoé)	Cours 4 (Waldschmidt)	Cours 4 (Waldschmidt)	Cours 4 (Kitombole)	TP (Armana)
10h50-11h10	*Pause café*	*Pause café*	*Pause café*	*Pause café*	*Pause café*
11h10-12h00	Cours 6 (Ionica)	Cours 6 (Ionica)	Cours 6 (Ionica)	Cours 4 (Waldschmidt)	Cérémonie de clôture
12h00-14h00	*Pause déjeuner*	*Pause déjeuner*	*Pause déjeuner*	*Pause déjeuner*	*Pause déjeuner*
14h00-14h50	Cours 4 (Waldschmidt)	Cours 5 (Tanoé)	Cours 5 (Tanoé)	TD (Waldschmidt)	*Libre*
14h50-15h10	*Pause*	*Pause*	*Pause*	*Pause*	
15h10-16h00	Cours 5 (Tanoé)	Cours 4 (Waldschmidt)	Cours 6 (Ionica)	Cours 3 (Armana)	
16h00-16h10	*Pause*	*Pause*	*Pause*	*Pause*	
16h10-17h00	Cours 6 (Ionica)	TP (Armana / Ionica)	TP (Armana / Ionica)	*Libre*	

Appendix 3: List of participants

CIMPA participants (7)

1. Ms. Chèfiath ADEGBINDIN (Institut de Mathématiques et de Sciences Physiques, Porto-Novo, Bénin, doctorante), adegbindinchefiath@gmail.com
2. Mr Gilda Rech BANSIMBA (Université Marien Ngouabi, Brazzaville, République du Congo, doctorant), bansimbagilda@gmail.com
3. Mr. Franklin ELION (Université Marien Ngouabi, Brazzaville, République du Congo, doctorant), elionfranck@gmail.com
4. Mr. Perez Broon FOUAZOU LONTOUO (Université de Dschang, Cameroun, doctorant), fouazouperez@gmail.com
5. Mr. Boris FOUOTSA TAKO (Université de Yaoundé I, Yaoundé, Cameroun, doctorant), fouotsab@yahoo.fr
6. Mr. Peter KIDOUDOU (Université Marien Ngouabi, Brazzaville, République du Congo, doctorant), peter.kidoudou@umng.cg
7. Mr. Bagnantissoun Euloge TCHAMMOU (Université Félix Houphouët Boigny, Abidjan, Côte d'Ivoire, doctorant), tchammoue@yahoo.fr

Other non local participants (1)

1. Mr. Audace Amen DOSSOU-OLORY (Stellenbosch University, Afrique du Sud, doctorant), audace@aims.ac.za

Local participants (total number 76, regular participants: around forty)

They were mainly students, teachers and researchers, in mathematics or computer science, mainly from the University of Kinshasa but from other universities and schools in D.R.C as well.

1. Mr. Bavon KASONGO MGUYA (Université de Kinshasa, RDC), bavonkas@gmail.com, chercheur
2. Mr. Joseph OLELA, lotanga.joseph.18@gmail.com
3. Mr. Albert NTUMBA (Université de Kinshasa, RDC)
4. Mr. Alex MASANGANA (Institut Supérieur d'Informatique Chaminade, Kinshasa, RDC), alexmasangana@gmail.com, étudiant gradué en informatique
5. Mr. Alphonse-Roger LULA BABOLE (Université de Kinshasa, RDC), lulababole@gmail.com, lulababole@yahoo.fr
6. Mr. Arnaud WATUSADISI (Université de Kinshasa, RDC), watusadisiarnaud@gmail.com
7. Mr. Arsène MITINGUI IZANA (Université de Kinshasa, RDC), mitinguiarsyny@hotmail.com
8. Mr. Ben PAKOKO NGUZ (Université de Kinshasa, RDC)

9. Mr. Berto NTANGU (Université de Kinshasa, RDC), bertontantgu@gmail.com, étudiant gradué en informatique
10. Mr. Bopatriciat BOLUMA MANGATA (Université de Kinshasa, RDC), boluma.mangata@gmail.com
11. Mr. Calvin MATONDO BWAYI (Université de Kinshasa, RDC), matymatondo@yahoo.fr
12. Mr. Chaco MUKADI NTUMBA (Université de Kinshasa, RDC), chaco.mukadi@gmail.com, étudiant gradué en informatique
13. Mr. Charly MASOBELE MVITA (Université de Kinshasa, RDC), charlymasobele@gmail.com, chercheur en informatique
14. Mr. Christian MAZAMBA (Université de Kinshasa, RDC), mazambachristian@gmail.com, étudiant gradué en mathématiques et informatique
15. Mr. Coen FUNDATECA, coenfundateca@gmail.com
16. Mr. David NGALAMULUME (Université de Kinshasa, RDC), davidngalamulume1@gmail.com
17. Mr. David YOMBO (Université de Kinshasa, RDC),davidyombo92@gmail.com, étudiant gradué en informatique
18. Mr. Denis MAMBA KABALA (Université de Kinshasa, RDC), denis.mamba@unikin.ac.cd, enseignant en informatique
19. Mr. Didier MAMBULU EKONGO (Université de Kinshasa, RDC)
20. Mr. Dieu Merci MATSHUDI SENGA (Université Chrétienne Cardinal Malula (UCCM ex.ISPL)), matsenga2@gmail.com, assistant en mathématiques et informatique
21. Mr. Edouard TSHONGA (Université de Kinshasa, RDC), tshongashindani@gmail.Com
22. Mr. Emmanuel MASAMBA BULU (Université de Kinshasa, RDC), emmasbulu@yahoo.fr, emmasbulu@gmail.com
23. Mr. Evariste SINDANI (Université de Kinshasa, RDC), evaristesindani@gmail.com, chercheur
24. Mr. Ferawi MABLA BOBINA (Université de Kinshasa, RDC), mablaferawi@gmail.com, assistant
25. Mr. Fiston KOWEPINDO HULUTE (Université de Kinshasa, RDC), jospin.kowepindo@unikin.ac.cd, chercheur en mathématiques et informatique
26. Mr. Fiston MUKUNDA WALASA (Université de Kinshasa, RDC), fistonmukunda@live.com
27. Mr. Flavien NGIMBI (Université de Kinshasa, RDC), flashnging@gmail.com
28. Mr. Francis LUMINGU THAMBA (Université Libre de Boma, Boma, RDC), francislumingu12@gmail.com, enseignant en informatique
29. Mr. Francis MAYALA LEMBA (Université Pédagogique Nationale, Kinshasa, RDC), mathprogr1@gmail.com, enseignant
30. Mr. François Joseph NDUMBI KABEYA (Université de Kinshasa, RDC)

31. Mr. Gilles BOKOLO TAMBA (Université de Kinshasa, RDC), rgillesb@gmail.com, assistant en mathématiques
32. Mr. Glory SEKELE, glorysekele@gmail.com
33. Mr. Gradi KAMINGU (Université de Kinshasa, RDC), gradi.l.kmingu@aims-senegal.org, candidat-assistant en mathématiques
34. Mr. Herman MATONDO MANANGA (Université de Kinshasa, RDC), hdm-mat@gmail.com, enseignant-chercheur en mathématiques
35. Mr. Hermes HERMES (Université de Kinshasa, RDC), freshlikebatch121@gmail.com, enseignant-chercheur
36. Mr. Issa RAMADHANI (Université de Kinshasa, RDC), proframad@yahoo.fr, professeur
37. Mr. Jacques MBUYI (Université de Kinshasa, RDC), kmbuyijack@gmail.com, enseignant-chercheur en mathématiques appliquées
38. Mr. Jean-Louis AKAKATSHI OSSAKO (Université de Kinshasa, RDC), jlakakat-shi@gmail.com
39. Mr. Joël BIOLA KAJEMBE (Université de Kinshasa, RDC), jkayembe2015@outlook.fr, étudiant gradué
40. Mr. Joël KABUYA ILUNGA (Université de Kinshasa, RDC), joel.kabuya@unikin.ac.cd, assistant en informatique
41. Mr. Joël KINGANGA (Université de Kinshasa, RDC), joelkinga@gmail.com, enseignant-chercheur en informatique
42. Mr. John POMA (Université de Kinshasa, RDC), pomaesendo7@gmail.com, étudiant gradué en mathématiques et informatique
43. Mr. Jojo TSHITENGE MUPUWE (Université de Kinshasa, RDC), tshitenge-jojo@gmail.com, enseignant-chercheur en informatique
44. Mr. Joseph Désiré BUKWELI KYEMBA (Université de Kinshasa, RDC)
45. Mr. Josué Claude NTANTA Mr. B. (Université de Kinshasa, RDC), laude.ntanta@unikin.ac.cd, assistant en mathématiques
46. Mr. Junior KANINGINI LUTALA (Université de Kinshasa, RDC), kaninginiju-nior@gmail.com, chercheur en informatique
47. Mr. Justin Mao MAWEJA TSHABOLA (Université de Mbujimayi, Mbujimayi, RDC), ajewam@gmail.com, enseignant-chercheur en mathématiques
48. Mr. Kasengedia MOTUMBE (Institut Supérieur des Techniques Appliquées, Kinshasa), professeur
49. Mr. Michel-Évariste TSHODI TOLEMBO (Université Notre Date de Tshumbe, RDC), micheltshodi@gmail.com
50. Mr. Ndongala Michel NKUJU, michel.nk12@gmail.com

51. Mr. Noël BILA KHONDE (Université de Kinshasa, RDC), noel.bila@unikin.ac.cd , enseignant-chercheur en informatique
52. Mr. Pamphile MUYA MUSANGU (Université de Kinshasa, RDC)
53. Mr. Parfum BUKANGA CHRISTIAN (Université de Kinshasa, RDC), akili-malie@gmail.com, enseignant-chercheur en informatique
54. Mr. Patience-Ryan TEBUA TENE (Université de Kinshasa, RDC), ryantebuas@gmail.com, étudiant en mathématiques appliquées
55. Mr. Patrick BOKUNGU EFOTO (Université de Kinshasa, RDC), bokungu-patrick1@gmail.com
56. Mr. Peter OTCHUDI EPENGE (Université de Kinshasa, RDC), peterotchudi@gmail.com, étudiant gradué en mathématiques et informatique
57. Mr. Reagan MANDIYA EMOMO (Université de Kinshasa, RDC), reagaeamomo@gmail.com
58. Mr. Reagan TSHIANGOMBA KASONSA (Université de Kinshasa, RDC)
59. Mr. Rey IRENGE BADOSANYA (Université de Kinshasa, RDC), irengerey8080@gmail.com
60. Mr. Riddy WABI NKUMU (Université de Kinshasa, RDC), riddywabi@gmail.com, étudiant gradué en mathématiques et informatique
61. Mr. Rostin MABELA (Université de Kinshasa, RDC), rostin.mabela@unikin.ac.cd, enseignant-chercheur en mathématiques
62. Mr. Saint-Jean DJUNGU (Université de Kinshasa, RDC), professeur en informatique
63. Mr. Salomon MANDI MAMBU (Université de Kinshasa, RDC), samanLEROI@gmail.com, étudiant gradué en informatique
64. Mr. Serge KUTUMBAKANA (Université Pédagogique Nationale, Kinshasa, RDC), kutumbakanamawanga@gmail.com, chercheur
65. Mr. Sion SION ISRAEL (Université de Kinshasa, RDC), sionisrael2@gmail.com
66. Mr. Tighana BASELE WENGE (Université de Kinshasa, RDC)
67. Mr. Tony TONA LAMDU (Université de Kinshasa, RDC) ,tonytoma2009@yahoo.fr, enseignant en mathématiques
68. Mr. Tresor NGOYI LANDU (Université de Kinshasa, RDC), ngoyilandu@gmail.com
69. Mr. Tshimanga TSHISWAKA (Université de Kinshasa, RDC), tshimangahenry23@gmail.com
70. Mr. Victoire SEBURIRI (Université de Kinshasa, RDC), victoireseburiri@gmail.com, étudiant gradué
71. Mr. Victor FARIALA MUCHANGA (Université de Mbujimayi, Mbujimayi, RDC), victorfariala@gmail.com, enseignant-chercheur à l'Institut supérieur des Sciences et Techniques Appliquées
72. Mr. Yves MANGONGO TINDA (Université de Kinshasa, RDC), ymangongo@aims.ac.tz, chercheur en mathématiques

73. Ms. Nana KABUJENDA KABASU (Université de Kinshasa, RDC), nanakabujenda@gmail.com, étudiante en informatique
74. Ms. Rebecca WALO OMANA (Université de Kinshasa, RDC), rebecca.walo@unikin.ac.cd, rwalo@yahoo.fr, professeur de mathématiques
75. Ms. Ruth CIBOLA NKONGOLO (Université de Kinshasa, RDC), ruthnkongolo@gmail.com, étudiante graduée en informatique
76. Ms. Véronique PHOLA MASUNDA (Université de Kinshasa, RDC), veroniquephola@gmail.com