Final report on the CIMPA school on:

Explicit Number Theory

The University of the Witwatersrand Johannesburg, South Africa
January 8-19, 2018

The CIMPA research school “Explicit Number Theory" was organized by CIMPA in conjunction with The University of the Witwatersrand. It was held at The University of the Witwatersrand from the 8th to the 19th of January 2018. The website of the school with updated information is located at

http://www.rnta.eu/SA2018/

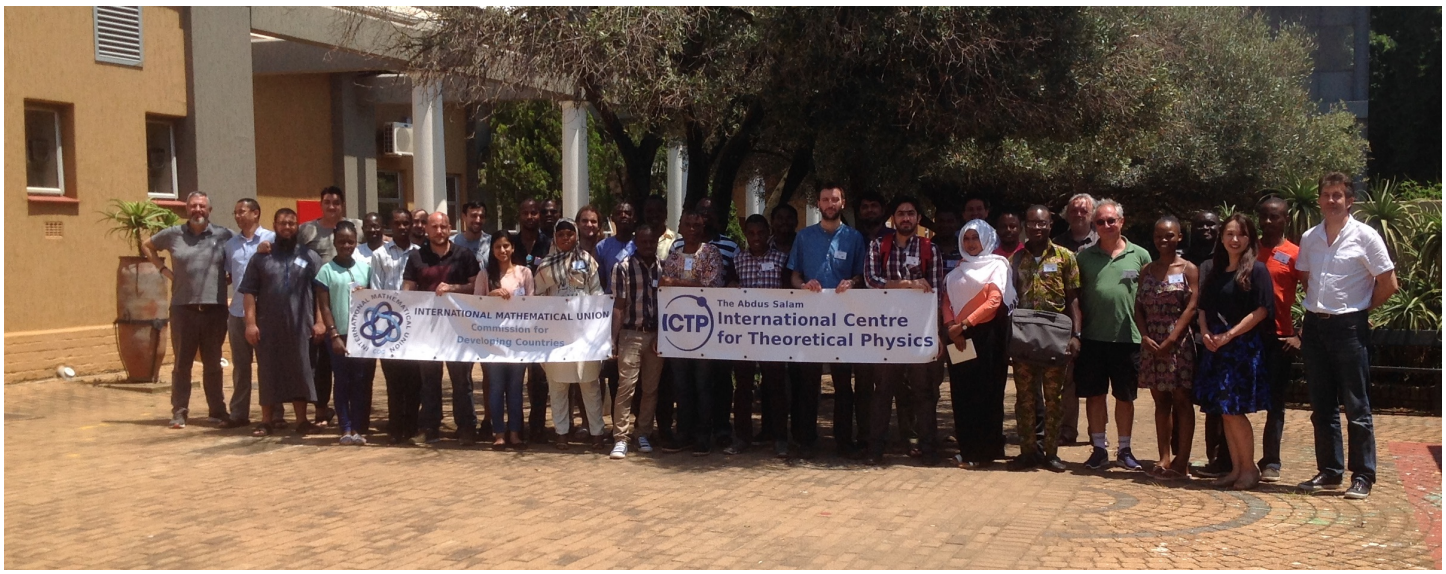
The classes were given by 7 lecturers from six different countries including two from Italy, one from Chile, France, the Netherlands, South Africa and the Unite States of America; there were 2 female lecturers which is 28.5% of the total number of lecturers.

There were 40 participants from 18 countries including 16 from South Africa and 24 from other countries: 2 from Benin, Congo, Ghana, India, and Pakistan, 1 from Algeria, Austria, Croatia, Egypt, France, Japan, Israel, Ivory Coast, Mali, Perù, Saudi Arabia, Senegal, and Sudan the last participant was the representative of CIMPA coming from France.

The school obtained supports from CIMPA, the center of excellence in Mathematical and Statistical Science of Wits University (CoE-MaSS), the commission for developing countries of the International Mathematical Union (IMU-CDC), the Number Theory Foundation (NTF), Foundation Compositio Mathematica, ALGANT consortium, the Open dreamkit project, the Italian minister of foreign affairs, the International Center for Theoretical Physics, the Société Arithmétiques de Bordeaux, the Agence National de la Recherche. Furthermore we acknowledge the generosity of Prof. Florian Luca and Prof. Loyiso Nongxa who supported the school through their personal grants.

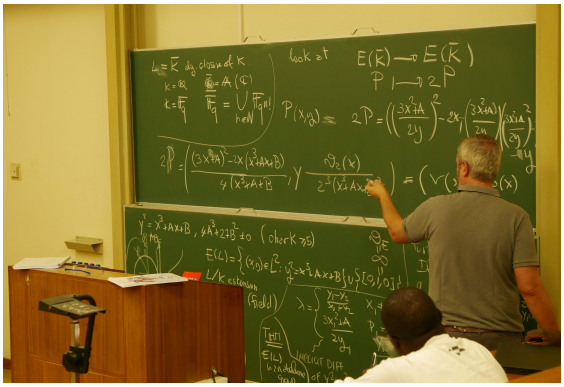
Among participants, there were 32 males (14 from South Africa and 18 from other countries) and 8 female (2 from South Africa and 6 from other countries). The female participants were 20% of total participants. The list of participants can be found at the end of this report.

The school started on January 8th, with a short opening ceremony which included speeches from the Head of the Mathematics Department, the Dean of the Faculty of Science, the scientific attaché of the French embassy and representatives for CIMPA, ICTP and the ALGANT consortium.



Most of the classes of the first week were of an introductory nature, some of the students already knew most of the stuff, but a number of them learned a lot during that week. The classes of the second week were more advanced but they were standing on the firm ground that was built in the first week. The background level of the participants was very wide but all of them learned something, depending on the participants some courses were more popular than others, but altogether it seems that all courses were at the right level for the students: all the speakers made a great effort to give clear talks, and they succeeded very well.

On the morning of the last day of the school we had two talks by guest lecturers. All the details can be found in the detailed program below.



Over the weekend an excursions took place on Saturday. We visited the Lion Park located 30km away from Johannesburg in the morning, while in the afternoon we took a hike in a nearby park.

Participants were hosted in the main campus of the University of the Witwatersrand, where also the dining hall and the lecture room were were located so they could easily do everything on foot. The lecturers were hosted in a nearby campus, but took all their meals in the same hall, Convocation hall, of the student. The atmosphere of the school was very interesting especially because there were so many different nationality present. The student interact extensively and they organised a session of talks in the afternoon of Wednesday of the second week.

Unfortunately a few accepted students were refused a visa form South African Authorities and so could not attend the school.

On the budget side we noticed a trend, spreading among a few of the various agency funding this type of schools, of requiring invoices. This makes very difficult to manage expenditures. For example on the departure day a few students did not have the cash for the train ticket. The cash was then provided by the lecturers. Furthermore, larger amount of funds remain unspent as it is difficult to get invoices matching exactly the given amounts. Moreover at least one participant could not come because it was impossible for him to pay the airline ticket in advance.

Below you find a the members of the various committee, the program of the school, and the list of participants. A detailed budget is attached on a separate document.

Scientific Committee

Yuri Bilu
Université de Bordeaux

Shabnam Akhtari,
University of Oregon

Florian Luca
The university of the Witwatersrand

Amalia Pizarro
Universidad de Valparaíso

Valerio Talamanca
Università Roma Tre

Local Committee

Florian Luca
The university of the Witwatersrand

Charlotte Brennan
The university of the Witwatersrand

Betsie Jonck
The university of the Witwatersrand

Arnold Knopfmacher
The university of the Witwatersrand

Augustine Munagi
The university of the Witwatersrand

Schedule

	Monday	Tuesday	Wednesday	Thursday	Friday
09.00-09.50 10.00-10.50	**Registration and Opening Ceremony**	**Analytic Number Theory** Luca	**Algebraic Number Theory** Talamanca	**Explicit Methods in ANT** Pizarro	**Elliptic Curves** Pappalardi/Stevenhagen
10.50-11.10			**BREAK**		
11.10-12.00	**Analytic Number Theory** Luca	**Algebraic Number theory** Talamanca	**Elliptic Curves** Pappalardi/Stevenhagen	**Analytic Number Theory** Luca	**Algebraic Number theory** Talamanca
12.10-13.00	**Algebraic Number Theory** Talamanca				
13.00-15.00			**LUNCH**		
15.00-15.50 16.00-16.50	**Elliptic Curves** Pappalardi/Stevenhagen	**Diophantine Equations** Bilu	Free Afternoon	**Diophantine Equations** Bilu	**Exercises session**

	Monday	Tuesday	Wednesday	Thursday	Friday
09.00-09.50	**Explicit Methods in ANT** Pizarro	**Elliptic Curves** Pappalardi/Stevenhagen	**Heights of algebraic numbers** Akhtari	**Elliptic curves** Pappalardi/Stevenhagen	**Explicit Methods in ANT** Pizarro
10.00-10.50					**Elliptic curves** Pappalardi/Stevenhagen
10.50-11.10			**BREAK**		
11.10-12.00	**Diophantine Equations** Bilu	**Diophantine Equations** Bilu	**Explicit Methods in ANT** Pizarro	**Heights of algebraic numbers** Akhtari	**Invited seminars**
12.10-13.00	**Heights of algebraic numbers** Akhtari				
13.00-15.00			**LUNCH**		
15.00-15.50 16.00-16.50	**Analytic Number Theory** Luca	**Heights of algebraic numbers** Akhtari	**Participants seminar**	**Free Afteroon**	

Courses

Introduction to analytic number theory Florian Luca

- Chebyshev estimates;
- Abel summation formula;
- The Moebius function;
- The prime number theorem;
- Mean values of arithmetic functions;
- The Brun pure sieve.

Introduction to algebraic number theory Valerio Talamanca

- Number fields
- Norms, traces, and discriminants
- Ring of integers
- Ideal factorization in Dedekind rings
- Decomposition and ramification
- Archimedean and non archimedean absolute values

Explicit solution of Diophantine equations Yuri Bilu

- Classical Diophantine equations in two variables, their theory, relations with Diophantine Approximation and with Algebraic Number Theory: linear equation; Pell equation; Thue equation; elliptic, hyperelliptic, superelliptic equations; general equation, Siegel's finiteness theorem;
- Baker's method, effective results
- From effective to explicit: the Las-Vegas Principle
- Continued Fractions and Baker-Davenport Lemma
- Explicit solution of simultaneous Pell equations and of Thue equations.

Explicit lower bounds for heights of algebraic numbers Shabnam Akhtari

- Heights of Algebraic Numbers
- Heights of Vectors and Polynomials
- Lehmer's Problem
- Effective Lower Bounds for Height of Algebraic Numbers
- Effective Computations in Number Fields

Explicit methods in algebraic number Theory Amalia Pizarro

- Introduction: Pell equations and special cases of Fermat last Theorem. Number fields. Ring of integers
- Integral bases and discriminant: explicit computations in quadratic and cyclotomic fields.
- Unique factorization of ideals in Dedekind domains. Explicit factorization of primes in rings of integers. Ramification.
- Ideal class group. Minkowski's bound and finiteness of the class group. Explicit computation in quadratic number fields.
- Dirichlet's Theorem. Units in real quadratic fields.

Elliptic curves over finite fields with prescribed order Francesco Pappalardi and Peter Stevenhagen

- Introduction to elliptic curves: Weierstrass Equations, the Group Law, the j-Invariant, endomorphisms, division polynomials, the Weil Pairing. Elliptic curves over finite fields, the Frobenius Endomorphism, Hasse-Weil bounds. Schoof's Algorithm for computing the group order, supersingular curves.
- Explicit construction of elliptic curves with prescribed order: Complex elliptic curves: Weierstrass parametrization multiplier ring, j-invariant. Complex multiplication. Lattices with given multiplier ring: the class polynomial. Elliptic curves with given point group: reduction mod p, twisting. Explicit construction of cryptographic curves.

Seminars

A Global History of Mathematics, Kitagawa Tomoko, Oxford University, United Kingdom
Representation of positive integers by binary cyclotomic forms Michel Waldschmidt, Sorbonne Unuversité, Paris, France

Student's Seminars

Expository talk on L-functions, by Ali Raza

Abstract: In this talk I will present overview of L-functions in which I will define Riemann zeta function, after that I will gave some explanation to its zeroes and will present Riemann hypoth- esis. I will mention Dirichlet L-function associated to Dirichlet character and will present generalized Riemann hypothesis. In the end I will discuss particular case of Dedekind zeta function.

On Schinzel-Wócik problem, by Mohamed Anwar

Abstract: The Schinzel–WÃşjcik problem consists in determming if Given $a_1, \ldots, a_r \in \mathbb{Q}^* - \{1\}$, there exist infinitely many primes p such that they have the same multiplicative order modulo p. I will mention some results about SchinzelâĂŞWÃşjcik problem and SchinzelâĂŞWÃşjcik problem on average.

On a Generalization of the Lucas Primality Test, by Faith Shadow Zottor

Abstract: This work has primality testing as its central axis. It discusses among other primality tests, the Lucas primality tests for Mersenne numbersand looks at a generalization of the Lucas functions to a polynomial of degree three(3). A discussion on a primality test based on RoettgerâĂŹs generalization of the Lucas functions is also included. The most relevant Number Theory background needed to understand the primality tests are also included.

Inducibility of Topological Trees and Related Topics, by Audace Amen Vioutou DossouOlory

Abstract:The inducibility is the maximum asymptotic density of isomorphic embeddings to a graph. The main part of our research is concerned with the inducibility of homeomorphically irreducible rooted trees with bounded degree sequence (a.k.a topological d-ary trees). Another related topic for our study is the investigation of the number of distinct leaf-induced subtrees of a topological tree. On the one hand, we shall take a look at the extremal trees with respect to this tree-parameter. On the other hand, we shall restrict ourselves to some special classes of trees and provide exact as well as asymptotic formulas for their number of nonisomorphic leaf-induced subtrees.

One Dimensional Modular Polynomial, by Abdoulaye MAIGA

Abstract: In this talk we will present the modulus space (up to isomorphism) of elliptic curves over C and the modular jâĹŠinvariant defined from it. We will show how define and compute a polynomial which parametrize pâĹŠisogenous elliptic curves (up to isomorphism) over C. This polynomial has many applications in elliptic curves cryptography (ECDLP, Isogenies Based Cryptography).

Algebraic Values of Transcendental functions, by Taboka Prince Chalebgwa

Abstract: Let $f : C \longrightarrow C$ be a transcendental analytic (or meromorphic) function. Roughly speaking, a typical question that is often asked regarding the arithmetic nature of the values of f is the following: Given an algebraic number α, is $f(\alpha)$ algebraic or transcendental? In tackling this question, one often chooses a more modest approach by first specifying certain parameters or conditions on the algebraic numbers considered, or the function f itself. More specifically, the problem I often consider is of the following sort: given some $R > 0$, $d \geq 1$ and $H \geq e$, say, can one bound the cardinality (in terms of R, d and H) of the set of all $z \in B(0, R)$ such that height $(z, f(z)) \leq H$ and $[Q(z, f(z)) : \mathbb{Q}] \leq d$? Most contemporary bounds are of the form $C\,(logH)^{\rho}$, for some effective constant $C > 0$and ρ depending on H, R and d. In this (rather short) talk, I shall give an outline of the ingredients that went into a recent result of ours regarding certain meromorphic functions with given growth conditions.

Introduction to the Theory of Beidleman near vector space , by Prudence Djagba

Abstract: In linear algebra, the theory of vector space over skewfield is generalised to a structure non-linear called near vector space. There are several notions of near vector spaces introduced by different researchers: Beidleman 1996, Andre 1974, Whaling 1987, Karzel. My PhD is concerned to the contribution to the theory of Beidleman near vector space. A pair (M, R) is called Beidleman near vector space if M is nearring module over a nearfield R, there exist$R$-submodules $M_i, i \in I$ such that each of M_i contains no proper R-subgroup and M is direct sum of $M_i, i \in I$. In this talk we present some basic properties of Beidleman near vector space and give some few results about finite dimensional Beidleman near vector space and number of subspaces of dimension k of the near vector space (R^n, R) where R is a nearfield. Finally we will introduce my future work about similarities and difference between Andre and Beidlemannear vector space (subspaces structure and linear mapping).

List of Participants

Chèfiath Awero Adegbindin, Institut de Mathematiques et de Sciences Physiques, Porto-Novo, Benin;
Nikola Adŷaga, University of Zagreb, Croatia;
Shabnam Akhtari, University of Oregon, United States of America;
Abdulaziz Mohammed Alanzi, University of Tabuk, Saudi Arabia;
Mohamed Anwar, Ain Shams University, Cairo, Egypt;
Adnan Aslam, Rachna College of Engineering and Technology, Gujranwala, Pakistan;
Gilda Rech Bansimba, L'Université Marien Ngouabi, Brazzaville, Congo;
Jean Just Bashingwa, University of the Witwatersrand, Johannesburg, South Africa;
Yuri Bilu Université de Bordeaux, France ;
Taboka Chalebgwa, Stellenbosch University, South Africa
Audace Amen V. Dossou-Olory, Stellenbosch University, South Africa;
Bernadette Faye, AIMS-Senegal, Mbour-Thies, Senegal;
Breuer Florian, Stellenbosch University, South Africa;
Abe Auguste Sezare, Gnagne Université de Félix Houphouët-Boigny, Abidjan 01, Cote d'Ivoire ;
Hoyam Hassan, University of Khartoum, Sudan;
Ankita Jindal, Indian Institute of Technology Delhi, New Delhi, India;
Florian Luca ,The university of the Witwatersrand, South Africa;
Ddamulira Mahadi, Graz University of Technology, Graz, Austria;
Abdoulaye Maiga, AIMS-Senegal, Mbour-Thies, Senegal;
Vhuhwavho Matibe, University of the Witwatersrand, Johannesburg, South Africa;
Cornelie Mitcha Malanda , L'Université Marien Ngouabi, Brazzaville, Congo;
Cele Mpendulo, University of KwaZulu- Natal, Durban, South Africa;
Augustine Munagi, University of the Witwatersrand, Johannesburg, South Africa;
Dylan Nelson, Stellenbosch University, South Africa;
Sibiya Nontobeko, University of KwaZulu- Natal, Durban, South Africa;
Benedict Vasco Normenyo, Institut de Mathematiques et de Sciences Physiques, Porto-Novo, Benin;
Darlison Nyirenda, University of the Witwatersrand, Johannesburg, South Africa;
Ayédjo T. A. Japhet Odjouman, Institut de Mathematiques et de Sciences Physiques, Porto-Novo, Benin;
Francesco Pappalardi, Università Roma Tre, Italy;
Oratilwe Penwell, Stellenbosch University, South Africa;
Jabulani Phakati, University of the Witwatersrand, Johannesburg, South Africa;
Amalia Pizarro, Universidad de Valparaíso, Chile;
Djagba Prudence, Stellenbosch University, South Africa;
Kumar Ram, Indian Institute of Technology, Jharkhand, India;
Vlad Ravelomanana, Unuversité Paris Diderot, France;
Ali Raza , Abdus Salam School of Mathematical Sciences, Lahore, Pakistan;
Salah Eddine Rihane, Université des Sciences et de la Technologie Houari Boumendien, Algeria;
Otoya Rodrigo, Universidad de Lima, Peru;
Mark Sias, University of the Witwatersrand, Johannesburg, South Africa;
Pierre Sanon Sogo, Stellenbosch University, South Africa;
Peter Stevenhagen, Universiteit Leiden, The Netherlands;
Valerio Talamanca, Università Roma Tre, Italy;
M . Mudziiri Shumba Tendai, University of KwaZulu- Natal, Durban, South Africa;
Kitagawa Tomoko, Oxford University, United Kingdom;
Michel Waldschmidt, Sorbonne Université, Paris, France;
Ezra Waxman, Tel Aviv University, Israel;
Shadow Faith Zottor, University of Ghana,, Accra, Ghana.