TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH
KHOA TOÁN - TIN HỌC

TRƯỜNG HÈ CIMPA "Applied Number Theory" năm 2024

Tiếp nối sự thành công của Trường hè Seams và CIMPA vào năm 2015 - 2016, mục đích của Trường hè CIMPA năm 2024 là để giới thiệu cho các sinh viên về một số vấn đề trong Lý thuyết số và ứng dụng của nó vào Lý thuyết mật mã và Lý thuyết code.

Với mục tiêu này, khoa Toán - Tin học, Trường Đại học Sư phạm TPHCM tổ chức Trường hè CIMPA với các bài giảng của các chuyên gia hàng đầu trên thế giới.

- Thời gian: 03/06/2024 - 14/06/2024.
- Địa điểm: Trường Đại học Sư phạm Thành phố Hồ Chí Minh,

280 An Dương Vương, phường 4, quận 5, Thành phố Hồ Chí Minh, Việt Nam.

I. Ban tổ chức

- **Dung Duong** (University of Wollongon)
- **Nguyen Thi Nga** (Ho Chi Minh City University of Education)
- **Thuy Pham** (Ho Chi Minh City University of Education)
- **Valerio Talamanca** (Università Roma Tre)
- **Ha Tran** (Concordia University of Edmonton)

II. Nội dung:

Trường hè CIMPA bao gồm **04** khóa học bằng tiếng Anh, thông tin chi tiết của từng khóa học như sau:

1. **Course 1: Elliptic Curves**

Giảng viên: Francesco Pappalardi and Valerio Talamanca.

Tóm tắt: Weierstrass Equations, The Group Law, Projective Space and the Point at Infinity, Cubic Equations, Quartic Equations, The j-invariant Elliptic Curves in Characteristic 2, Endomorphisms, Singular Curves, Torsion Points, Division Polynomials, The Weil Pairing, Elliptic Curves over Finite Fields, The Frobenius

Endomorphism, Supersingular Curves, Elliptic Curves over Q, The Torsion Subgroup. The Lutz-Nagell Theorem, heights on projective spaces and on elliptic curves and the Mordell-Weil Theorem. Elliptic curves over the complex numbers. Elliptic curves with complex multiplication. The main theorem of complex multiplication. Supersingular curves and maxiaml orders of quaternion algebras.

Kiến thức chuẩn bị: Đại số tuyến tính và hình học sơ cấp.

Tài liệu tham khảo:

[1] L. Washington, *Elliptic Curves Number Theory and Cryptography*.

[2] D. Husemoller, *Elliptic curves.*

[3] J. Silverman, J. Tate Rational, *Points on Elliptic Curves*.

2. **Course 2: Algorithmic Number Theory**

Giảng viên: Laura Geatti và Rene Schoof.

Tóm tắt: In this course, we will first introduce the class group and the unit group of a number field and study the structures of these groups. After that, we study algorithms to compute these for arbitrary number fields. In particular, we describe Buchmann's subexponential algorithm. In this context we introduce the ideal lattices associated to a number field and the equivalent concept of Arakelov divisors. We define the Arakelov class group and the concept of a reduced Arakelov divisor. Computing short vectors in ideal lattices is the key ingredient of Buchmann's algorithm.

In addition, special attention will be paid to algorithms to compute class groups of imaginary quadratic fields. Here the Arakelov divisors are simply 2-dimensional lattices in C. Classically the theory and the algorithms are described in terms of binary quadratic forms. This part will be used in the security analysis of isogeny-based cryptography.

Kiến thức chuẩn bị: Đại số tuyến tính và đại số sơ cấp.

Tài liệu tham khảo:

[1] Daniel A. Marcus, *Number fields*, Universitext, Springer.

[2] R. Schoof, *Algebraic Number Theory*: www.mat.uniroma2.it/ eal/moonen.pdf

3. **Course 3: Algebraic Coding Theory**

Giảng viên: Michel Waldschmidt và Frederique Elise Oggier.

Tóm tắt: Algebraic coding theory rests on arithmetic and finite fields. The first part of this course will be devoted to this background. The theory of cyclotomic polynomials is a basic tool. The second part will start with the definitions and basic properties of codes, many examples will be given, including Hamming codes, Golay codes, Bose-ChaudhuriHocquenghem codes, Reed-Solomon codes. Many exercices will be proposed.

Kiến thức chuẩn bị:

- **Arithmetic, finite fields.**

  Cyclic groups

  Residue classes modulo n

  The ring Z[X]

  Mobius inversion formula

  Gauss fields

  Cyclotomic polynomials

  Decomposition of cyclotomic polynomials over a finite field

  Trace and Norm

  Infinite Galois theory

- **Coding Theory:**

  Some historical dates

  Hamming distance

  Definitions, Examples

  Cyclic codes

  Detection, correction and minimal distance

  Hamming codes

  Generator matrix and check matrix

  Minimum distance of a code

  Golay codes

  Duality and self-duality

Sphere packing and Singleton bounds.

Maximum distance separable codes

Perfect codes

Weight enumerator

Reed-Mueller codes

Goppa codes

Generalized Hamming distance

Rank distance

Generalized rank distance.

4. **Course 4: Isogeny-based Cryptography**

Giảng viên: Benjamin Wesolowski and Mingjie Chen.

Tóm tắt: Cryptography builds its foundations on a handful of presumably hard computational problems. While classical problems would not resist an adversary equipped with a quantum computer, alternative solutions are being developed, for secure postquantum cryptography. Isogeny-based cryptography is one of these solutions, and relies on the presumed hardness of the isogeny-finding problem: given two elliptic curves, find an isogeny connecting them. In this course, we will discuss the hardness of this problem, and the cryptosystems that can be built from it. We will first discuss the underlying computational problems, and how they relate to each other: the isogeny-finding problem, the endomorphism ring problem, and the vectorisation problem. We will then discuss how to build cryptographic schemes from these problems, and analyse their security: one-way functions, key exchanges, proofs of knowledge, and signatures.

Kiến thức chuẩn bị: Đường cong Elliptic trên trường hữu hạn.

Tài liệu tham khảo:

[1] Luca De Feo, *Mathematics of Isogeny Based Cryptography Isogeny-based Cryptography School course materials*, https://isogenyschool2020.co.uk/

III. Giảng viên

• Mingjie Chen, University of Birmingham, UK.

• Laura Geatti, Universit`a di Roma Tor Vergata, Italy

• Frederique Oggier, Nanyang Technological University (NTU), Singapore

• Francesco Pappalardi, Universit`a Roma Tre, Italy

• Rene Schoof, Universita di Roma Tor Vergata, Italy

• Valerio Talamanca, Universit`a Roma Tre, Italy

• Michel Waldschmidt, Sorbonne Universite, Paris, France

• Benjamin Wesolowski, CNRS researcher (charge de recherche) at the Institut de Mathématiques de Bordeaux, France

IV. Đối tượng tham dự

Trường hè dự kiến tài trợ cho khoảng 50 sinh viên tham dự trong đó có 30 sinh viên Việt Nam và 20 sinh viên quốc tế.

Các bạn đăng kí và được CIMPA chấp nhập sẽ được hỗ trợ theo kinh phí của chương trình. Trường hè vẫn tạo điều kiện cho các bạn không đăng kí đến tham gia và học tập, tuy nhiên sẽ không có hỗ trợ.

Hạn chót đăng kí: 28 tháng 02 năm 2024.

V. Thông tin về Trường hè

- Website Trường hè: http://www.rnta.eu/HCMC2024/

- Website đăng kí: A CIMPA school in Ho Chi Minh city (rnta.eu)

Thông tin chi tiết liên hệ:

- Email: khoatoantin@hcmue.edu.vn hoặc truonglq@hcmue.edu.vn

- Điện thoại: 0375532190