**Scuola Superiore di Catania**

Corso specialistico

a.a. 2019-2020

# Introductory Algebraic Number Theory and Applications

This course is intended as an introduction to Algebraic number theory and its applications. Algebraic Number theory is an area of mathematics that recently found important applications in cryptography and in the area of cryptocurrencies. The class is divided in three main parts. The first two parts provide the necessary mathematical background to understand the applications that will be discussed in part three. Three hours will be devoted to the final exam.

## 1. Basics

Integral Extensions. Dedekind Domains. Invertible Ideals. Rings of Algebraic Integers. Integral bases. Quadratic Forms over quadratic fields and their composition.

## 2. Orders and Class groups.

Orders in quadratic fields. Class group. Class number. Factorizations of integer primes in imaginary quadratic fields.

## 3. Applications to Cryptography.

Computation in class groups. Computation of the discrete logarithm and of the class number; Class group of a non maximal order. Cryptanalysis of NICE encryption. Castagnos-Laguillaumie cryptosystem. More advanced constructions.