Giordano Santilli
PhD Student in Mathematics

An Investigation on Integer Factorization applied to Public Key Cryptography

Abstract:
Public key cryptography allows two or more users to communicate in a secure way on an insecure channel, using two different keys: a public key, which has the function to encrypt the messages, and a private key, employed in the decryption of the ciphertext. Because of the importance of these keys, their generation is a sensible issue and it is often based on an underlying mathematical problem, which is considered hard to be solved. Among these difficult problems, the Integer Factorization Problem (IFP) is one of the most famous: given a composite integer number, recovering its factors is commonly believed to be hard (worst-case complexity).

In this talk, after a brief explanation of the developments on integer factorization and a description of the General Number Field Sieve (GNFS), I will present different strategies to face this well-known problem of Number Theory. First, I will show an attempt to improve GNFS, considering two linearly disjoint quadratic fields Q(θ₁) and Q(θ₂) and studying the relation between first-degree prime ideals in Z[θ₁] and Z[θ₂] and those in Z[θ], where Q(θ) is the quartic extension that contains both Q(θ₁) and Q(θ₂). Secondly, I will characterize the elements used in GNFS through some systems having integer solutions, that can be found using Groebner Bases.

Supervisor: Massimiliano Sala