PLAN OF THE COURSE
MATHEMATICS AND QUANTUM COMPUTING

1. Motivation: cryptosystems relying on the difficulty of arithmetic problems

1.1. Generalities on groups, order of an element, characters.

1.2. The example of $\mathbf{Z}/n\mathbf{Z}$.

1.3. The RSA scheme and factorization of integers.

1.4. Diffie–Hellman key exchange and the Discrete Logarithm Problem.

2. Introduction to quantum computing

2.1. Some notions of quantum physics.

2.2. Qubits as elements of an Hermitian space.

2.3. Operations on qubits : only unitary operators make sense!

2.4. Measuring qubits.

2.5. Deutsch-Jozsa algorithm.

3. Shor's algorithm

3.1. Overview of Shor's factoring algorithm.

3.2. Period-finding algorithm via Quantum Fourier Transform.

3.3. Implementing the gates U_f and QFT_{2^n}.

4. An overview of Regev's variant of Shor's algorithm and Pilatte's proof of correctness

4.1. Regev's variant as a multidimensional period-finding algorithm.

4.2. Analytic number theory techniques in Pilatte's proof correctness.