BIBLIOGRAPHY FOR THE COURSE MATHEMATICS AND QUANTUM COMPUTING

In order of apparition, the main references for this course are:

(1) Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein: *Introduction to algorithms*, MIT Press.

(2) N. David Mermin: *Quantum Computer Science, An Introduction*, Cambridge University Press.

(3) Wolfgang Scherer: *Mathematics of Quantum computing, An Introduction*, Springer.

(4) Arnaud Bodin: *Quantum, un peu de mathématiques pour l'informatique quantique* (in French), available at https://exo7math.github.io/quantum-exo7/livre-quantum.pdf.

(5) Peter W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994. ArXiv preprint available at https://arxiv.org/abs/quant-ph/9508027.

(6) Oded Regev: *An efficient quantum factoring algorithm*, arXiv preprint https://arxiv.org/abs/2308.06572, 2023.

(7) Cédric Pilatte: *Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms*, arXiv preprint https://arxiv.org/abs/2404.16450, 2024.

The book (1) covers the necessary material on modular arithmetic and the RSA cryptosystem, while (2) is a very complete introduction to quantum computer science from which I took most of my inspiration. This course also borrows some ideas of presentation from unpublished notes that I took during a course taught in 2019 at the University of Bordeaux, by Jean-Marc Couveignes and Xavier Caruso (the quantum part of the course was mostly based on Mermin's book). I also took inspiration from some parts of (3) and (4), notably for some of the exercises. I especially recommand the book (4), which is freely available online and contains very detailed examples of calculations. The reading of Shor's original paper (5) is also very instructive.

The more recent preprints (6) and (7) are the references for the last section on the course on a multidimensional variant of Shor's algorithm and the proof of its correctness.