Course 2-12-1, Room 1002

- https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-12-1
- 12h on Lattice-based Cryptography
- 12h on Zero-Knowledge and Searchable Encryption by Brice Minaud

Lattice-based Cryptography

Phong Nguyễn

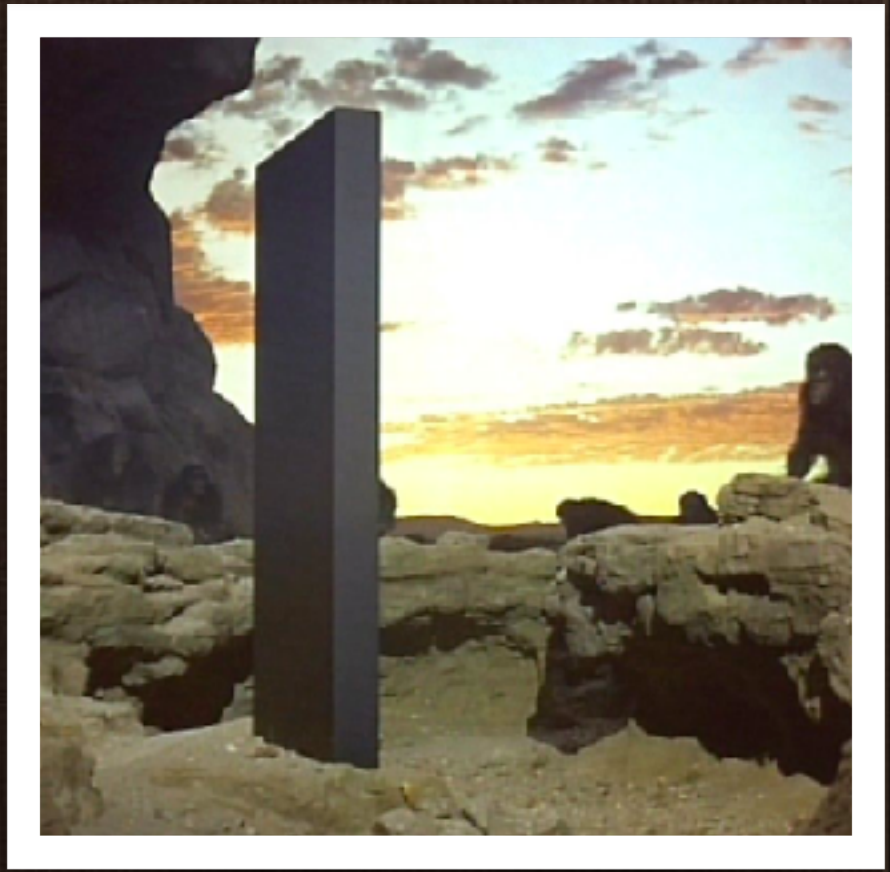
September 2022

Announcement

- Thanks to 

I offer Internship/PhD/Post-doc positions at ENS/Inria.
  - M2 internship proposals.
- Other crypto offers at ENS: B. Minaud and D. Pointcheval.  

A long time ago...



Sphere Packings

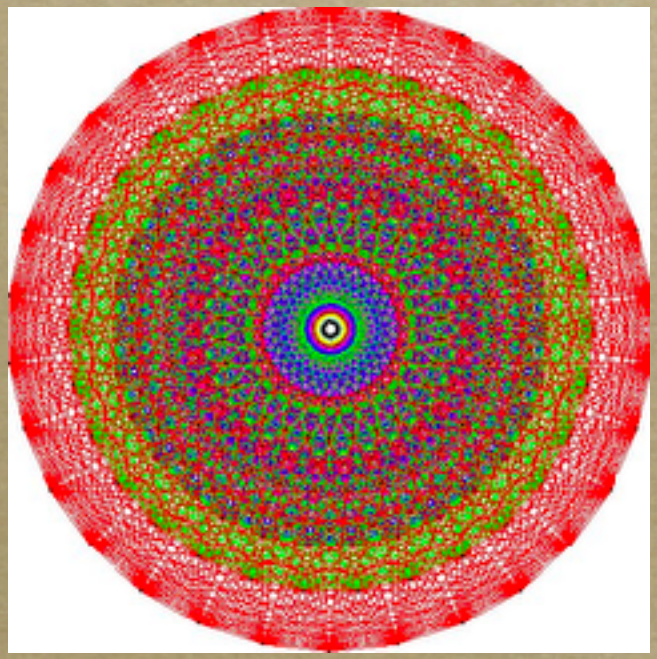
The Hexagonal Packing

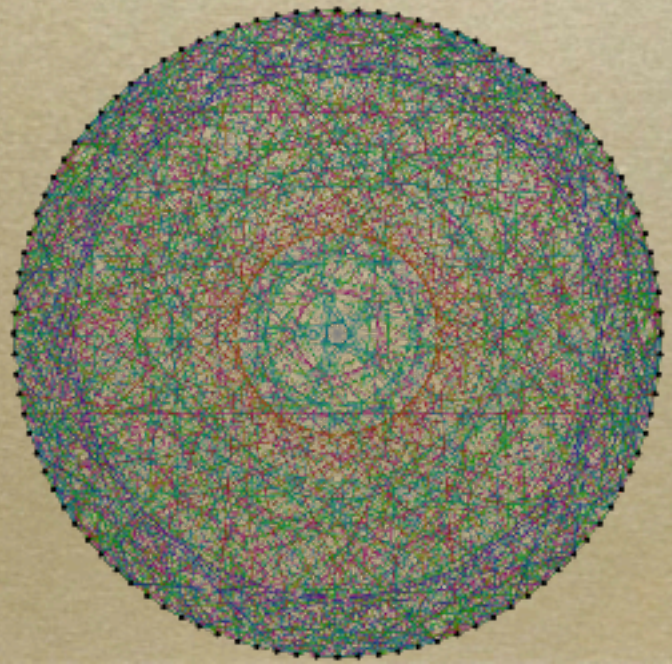
Kepler's "Conjecture"

- « proved » by Hales (1998,2005,2014).
- Perrin (Nobel 1926) used the conjecture to estimate Avogadro constant.

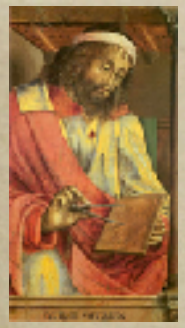
Breakthroughs

- In 2016, Viazovska et al. proved that the best sphere packings in dimensions 8 and 24 are lattice packings: E_8 and the Leech lattice.





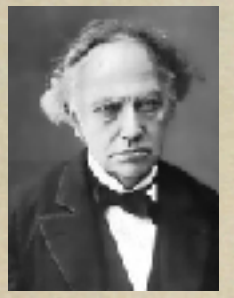
Another motivation...



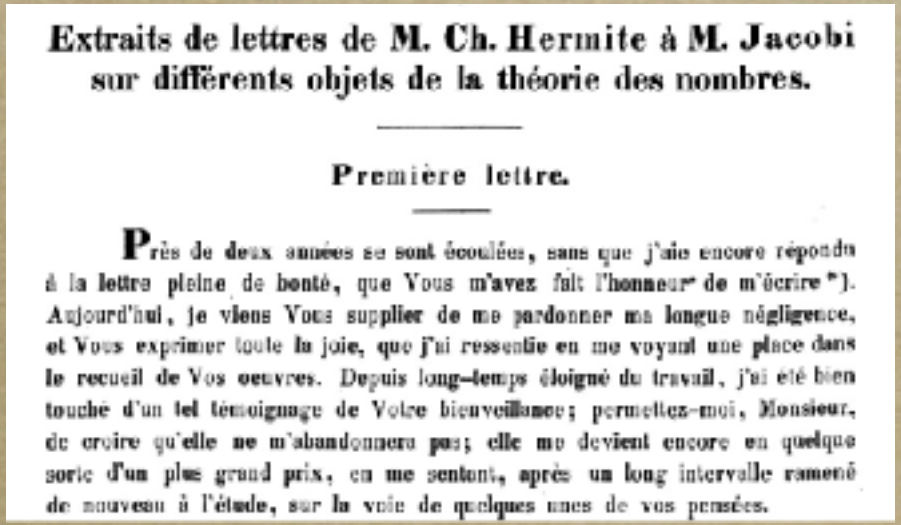
300 BC: Euclid's Algorithm

- Input: two integers $a \geq b \geq 0$.
- Output: gcd(a,b).
- While $b \neq 0$
  - a := a mod b
  - Swap(a,b)
- Return(a)

Generalizations



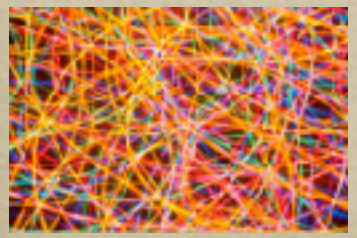
- 1773: Given (n,a,b,c), Lagrange answers if n of the form $ax^2+bxy+cy^2$
- 1850: Hermite invents an n-dimensional analogue of Lagrange's algorithm for positive definite quadratic forms.



Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres.

Première lettre.

Près de deux années se sont écoulées, sans que j'aie encore répondu à la lettre pleine de bonté, que Vous m'avez fait l'honneur de m'écrire *). Aujourd'hui, je viens Vous supplier de me pardonner ma longue négligence, et Vous exprimer toute la joie, que j'ai ressentie en me voyant une place dans le recueil de Vos oeuvres. Depuis long-temps éloigné du travail, j'ai été bien touché d'un tel témoignage de Votre bienveillance; permettez-moi, Monsieur, de croire qu'elle ne m'abandonnera pas; elle me devient encore en quelque sorte d'un plus grand prix, en me sentant, après un long intervalle ramené de nouveau à l'étude, sur la voie de quelques unes de vos pensées.



The Ubiquity of Lattices

- Applications in computer science, statistical physics, etc.
- In mathematics
  - Algebraic number theory, Algebraic geometry, Sphere packings, etc.
  - Fields medals: G. Margulis (1978), E. Lindenstrauss and S. Smirnov (2010), M. Bhargava (2014), A. Venkatesh (2018), M. Viazovska (2022).

Context

Context

- Lattices have become a buzzword in cryptography.

Fully-Homomophic Encryption

Worst-case to Average-case Reductions

Post-Quantum Cryptography

- The goal of this course is to understand the applications of lattices to algorithms, complexity and cryptography.

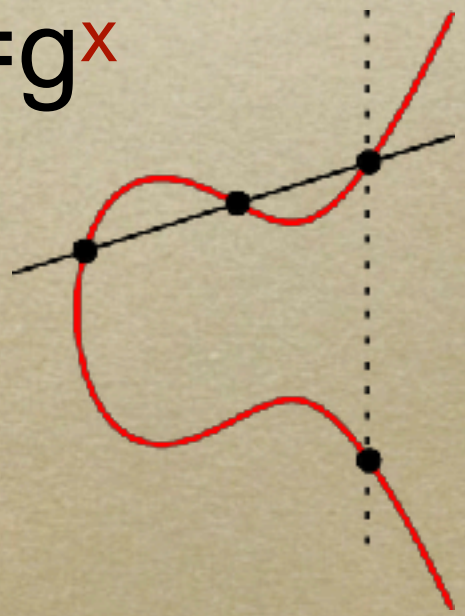
Milestones

- 1978: The Merkle-Hellman Cryptosystem
- 1982: First use of lattices in crypto: breaking Merkle-Hellman.
- 1996: Ajtai's SIS reduction and the first lattice cryptosystems (NTRU, Ajtai-Dwork, GGH...)
- 2005: Regev's LWE (Gödel Prize 2018)
- 2009: Gentry's fully-homomorphic encryption based on lattices.
- 2017-: NIST's post-quantum crypto standardization.

1994: Shor's Breakthrough

- [FOCS '94]: A quantum computer can factor and extract discrete logarithms efficiently.

$y=g^x$



$N=pq$

RSA

certicom | BlackBerry Subsidiary

The Quantum Menace

- 2006: creation of the Post-Quantum Cryptography conference.
- It was a small conference until…

The Quantum Menace

- 2014: GCHQ released a quantum attack on their own lattice-based cryptosystem.

GCHQ

- 2015: NSA announced a transition to post-quantum cryptography: cryptographic algorithms resistant to quantum computers.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

The Quantum Wave

- 2018-28:  €1billion for quantum technologies. Special funds in UK, France, Germany, Netherlands…
- 2018-23:  €1billion.
- Much more in China.

- Google, IBM, Microsoft, Intel/TUDelft, Alibaba/CAS, etc.

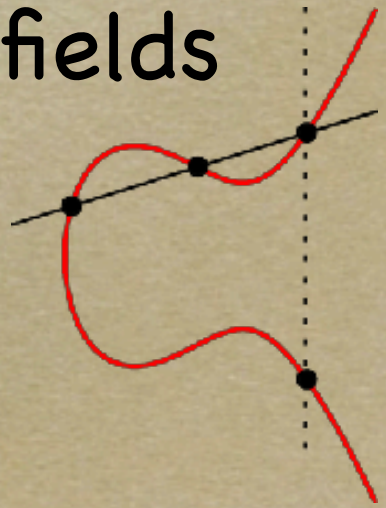
The NIST Competition

- In 2016, NIST announced a call for post-quantum standards:
  - 5 security levels
  - Public-key encryption
  - Signature

Post-Quantum Candidates

- Lattices: TLS-prototype tested several months by Chrome/Google

- Coding theory
- Multivariate polynomials over finite fields
- Elliptic curve isogenies



The NIST Competition

- 2017: 64 Round-1 candidates: 40% lattices.
- 2019: 26 Round-2 candidates: 46% (12) lattices.
- 2020: 7 Round-3 Finalists: 71% lattices (3/4 encryption and 2/3 signature).
- 2022: 4 standards: 75% (3) lattices.
  - NSA requests adoption by 2035
  - ANSSI request hybrid adoption by 2025

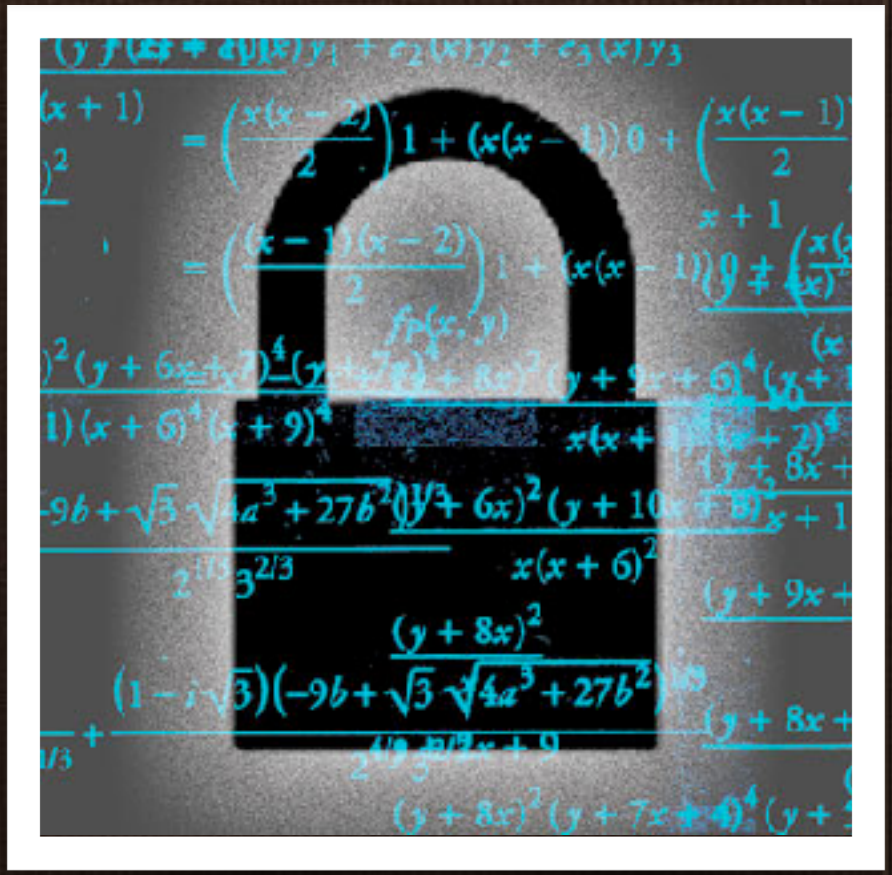
4 NIST Standards

- KEM/encryption (1):
  - Crystals-Kyber: **El Gamal** using MLWE lattices
- Signatures (3)
  - Crystals-Dilithium: **Schnorr**/Fiat-Shamir with aborts using MLWE
  - Falcon: **Rabin**/GGH-GPV using NTRU lattices
  - Sphincs+: Hash-based
- Might still be affected by patents.

This course

- Lattices in Algorithms, Complexity and Cryptography
- Lattice Analogues of:
  - RSA: Encryption with Trapdoors
  - Diffie-Hellman key exchange
  - El Gamal: Encryption without Trapdoors
  - Rabin signatures
- Attacks

Lattice-based Cryptography



Classical Public-Key Cryptography

- **RSA** cryptography uses finite (abelian) groups of hidden order, typically $G=(\mathbf{Z}/N\mathbf{Z})^\times$ where $N=pq$.
- Because the order can be recovered in subexponential time by factoring, the group must be large: 2048 bits, 4096 bits, etc.

Classical Public-Key Cryptography

- To speed things up, **Elliptic curve crypto** uses smaller groups (of known order): elliptic curves over finite fields.
  - The best ECDL classical attack runs in exponential time, thus the group can be chosen much smaller than an RSA group.
  - Although the group operations are more expensive, it is globally faster.

Lattice Cryptography

- To speed things up, l**attice crypto** instead uses larger groups with cheaper operations: an additive finite abelian group such as $\mathbf{Z}/p\mathbf{Z}$ or $(\mathbf{Z}/q\mathbf{Z})^n$.
  - Sometimes, the best attack runs in time subexponential in the group size, yet exponential in the lattice dimension.