Basic algorithms in number theory and cryptography

- Denote by $\Phi(N)$ as the Euler's totient function (# primes less than N)
- Denote by $\mathbb{Z}_n = \{0, 1 \ldots, N-1\}$ and Z_N^* as the multiplicative group of $\mathbb{Z}_N$
- Denote by QR_N as the set of quadratic residues in $\mathbb{Z}_N^*$

$$QR_N = \{a | a = x^2 \bmod M \text{ dor some } x \in \mathbb{Z}_N^*\} \tag{1}$$

Facts:

1. $QR_N \leq Z_N^*$
2. $\forall p > 2$ prime, $x \to x^2 \bmod p$ is a 2 to 1 function over $\mathbb{Z}_p^*$
3. $|QR_p| = |Z_p^*|/2 = (p-1)/2$, for all prime $p > 2$.
4. For primes $p, q > 2$, let $N = pq$. Then $x \to x^2$ is a 4 to 1 function over $\mathbb{Z}_p^*$.
5. **(Fermat's little theorem)** p prime, then for all $a \in \mathbb{Z}_p^*$,

$$a^{p-1} = 1 \bmod p \tag{2}$$

Test whether a number N is prime

- **Guess**: if N is not a prime, then "for many" $a \in \mathbb{Z}_N^*$, $a^{N-1} \neq 1 \bmod N$
  - **Not true!** --> Carmichael numbers

Miller-Rabin prime test

- Let $N - 1 = t \cdot 2^h$ and t is odd
- Define $L'_N = \{a \in \mathbb{Z}_N^* | \}$

A-K-S primality test (2002) deterministic

Algorithms of Factoring

Fermat's algorithm

- Try to find non trivial (a,b) such that

$$a^2 = b^2 \bmod N \Rightarrow (a+b)(a-b) = 0 \bmod N \tag{3}$$

Lan's algorithm

- $O(\exp(k^{1/2}(\log k)^{1/2})$ where k is the bit length of the smallest prime factors of N

Number field sieve

- $O(\exp(n^{1/3}(\log n)^{2/3}))$ where n is the hyperparameter of the size of primes chosen
- Fastest classical algorithm

Smooth Numbers

- A number is B smooth if all its primes factors $\leq B$
- Denote the set of all integers up to x that are y smooth as $S(x,y)$ and $\Psi(x,y) = |S(x,y)|$.
- Rankin 1938:

$$\Psi(N, \log(N)^A) = N^{1-1/A+O(1/\log\log N)} \tag{4}$$

- Canfield, Erdos, Pomerance 1983:

$$\Psi(N, y) = N/u^{u+o(u)} \quad \mathrm{for} u \leq y^{1-\epsilon} \tag{5}$$