CS 127/CSCI E-127: Introduction to Cryptography

Prof. Salil Vadhan — Fall 2013

Lecture Notes 8:

Computational Number Theory

Reading.

- Katz–Lindell 2nd edition §8.0,8.1,8.2.3,8.3.0-8.3.2 OR 1st edition §7.0,7.1,7.2.3,7.3.0-7.3.2

Computational Number theory is a major source of hard problems (eg one-way functions) for cryptography.

1 Modular arithmetic: $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$

Basic definitions:

- $x \equiv y \pmod{N}$ if $N|(x-y)$. (Written $x = y \bmod N$ in Katz–Lindell.)
- $[x \bmod N] \stackrel{\text{def}}{=}$ unique $x' \in \{0, \ldots, N-1\}$ s.t. $x \equiv x' \pmod{N}$.
- $\mathbb{Z}_N \stackrel{\text{def}}{=} \{0, \ldots, N-1\}$ with arithmetic $(+,\cdot)$ modulo N.
  We cannot divide in general: $5 \cdot 8 \equiv 5 \cdot 1 \pmod{35}$.

Fact 1 (Extended Euclidean Algorithm) *For any $x, y \in \mathbb{N}$ there exists two integers a, b such that $ax + by = \gcd(x, y)$. Moreover, such a and b can be found in polynomial time.*

Definition of $\mathbb{Z}_N^*$

$$\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_N : \gcd(x, N) = 1\} = \text{elements of } \mathbb{Z}_N \text{ with multiplicative inverses}$$

By a *multiplicative inverse* for x we mean an element $y \in \mathbb{Z}_N$, denoted $y = x^{-1}$, such that $x \cdot y \equiv 1 \pmod{N}$. Given N and $x \in \mathbb{Z}_N^*$, we can compute x^{-1} in polynomial time:

Example: In $\mathbb{Z}_{35}^*$, $3^{-1} = \ldots$.

Euler phi function

$$\phi(N) \stackrel{\text{def}}{=} |Z_N^*|$$

Example:

- $\mathbb{Z}_{35}^* =$
- $\phi(35) =$

Q: how to generate random elements of $\mathbb{Z}_N^*$?

Fact 2

$$\phi(N) = N \cdot \prod_{primes\ p|N} \left(1 - \frac{1}{p}\right) \geq \frac{N}{6\log\log N}$$

2 Groups

- An *abelian group* G is a set G with binary operation $\star$ satisfying associativity, identity, inverses, and commutativity.
  Examples: $\mathbb{Z}_N$ under addition, $\mathbb{Z}_N^*$ under multiplication.
- **Fact:** In any group G, $\underbrace{x \star x \star \cdots \star x}_{|G|} = \text{id}$ for all $x \in G$.
  Examples:
- **Corollary:** $\forall x \in \mathbb{Z}_N^*,\ x^{\phi(N)} \equiv 1 \pmod{N}$.
  Example: $[2^{24} \bmod 35] =$

3 $\mathbb{Z}_p$ when p prime

- $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ (because $\phi(p) = p - 1$) and thus $\mathbb{Z}_p$ is called a *field*.
- **Fermat's Little Theorem:** For every $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$.
- A polynomial of degree d has at most d solutions mod p.
- For every prime p, there is a $g \in \mathbb{Z}_p^*$ such that $\{1 \bmod p, g \bmod p, g^2 \bmod p, g^3 \bmod p, \ldots, g^{p-2} \bmod p\} = \mathbb{Z}_p^*$. Such a g is called a *generator* of $\mathbb{Z}_p^*$.
  Example: $\mathbb{Z}_{11}^* =$
- **Fact 3** *We can generate random n-bit prime p together with a (random) generator of $\mathbb{Z}_p^*$ time* $\text{poly}(n)$.
- **Discrete logarithms:** For $x \in \mathbb{Z}_p^*$, $\log_g x \stackrel{\text{def}}{=} [\text{unique } i \in \{0, \ldots, p-2\} \text{ s.t. } g^i \equiv x \pmod{p}]$. Computing the discrete logarithm is believed to be hard, even if p and g are known.

4 Chinese Remainder Theorem

Fact 4 (Chinese Remainder Theorem) *Let $N = pq$ with $\gcd(p, q) = 1$. Then the map $x \mapsto (x \bmod p, x \bmod q)$ from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ is one-to-one and onto. In particular, for every $(y, z) \in \mathbb{Z}_p \times \mathbb{Z}_q$, there exists a unique $x \in \mathbb{Z}_N$ s.t. $x \equiv y \pmod{p}$ and $x \equiv z \pmod{q}$. Moreover, x can be found in polynomial time given (y, z, p, q).*

Proof sketch: What is the inverse map?

Example: $Z_{35} \leftrightarrow \mathbb{Z}_5 \times \mathbb{Z}_1 5$

Using the Chinese Remainder Theorem, an arithmetic question modulo N can be reduced to an arithmetic problem modulo p and modulo q, *provided we know the factorization of* N.

5 Quadratic Residues

We define $\mathrm{QR}_N \stackrel{\text{def}}{=} \{x^2 \bmod N : x \in \mathbb{Z}_N^*\}$.

Proposition 5 *When p odd prime, $|\mathrm{QR}_p| = |\mathbb{Z}_p^*|/2 = (p-1)/2$.*

Proof: Consider the map from $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$, given by $x \mapsto x^2$. A square in $\mathbb{Z}_p^*$ has at least two square roots because $a^2 \equiv (-a)^2 \mod p$ and $a \not\equiv -a \mod p$ as p is odd. A square in $\mathbb{Z}_p^*$ has at most two square roots: $\mathbb{Z}_p$ is a field so a polynomial of degree d has at most d roots modulo p. We consider the polynomial $x^2 - c \equiv 0 \pmod p$: for any c, the polynomial has at most two roots in $\mathbb{Z}_p$. The map is hence exactly 2 to 1. ■

Proposition 6 *When $N = pq$ for odd primes p, q, $|\mathrm{QR}_N| = |\mathbb{Z}_N^*|/4$ and $x \mapsto x^2$ is 4-to-1 on $\mathbb{Z}_N^*$.*

Proof: Let us prove that $s \in \mathrm{QR}_N \iff (s \mod p \in \mathrm{QR}_p)$ and $(s \mod q \in \mathrm{QR}_q)$.

The map $x \mapsto x^2$ is 4-to-1 on $\mathbb{Z}_N^*$.

$$|\mathrm{QR}_N| = |\mathbb{Z}_N^*|/4 = \frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$$

■

Example: elements of QR_{35}