CS 7880 Graduate Cryptography October 18, 2017

Lecture 12: Field Arithmetic

Lecturer: Daniel Wichs *Scribe: Yashvanth Kondi*

1 Topics Covered

- Fundamentals of field arithmetic
- Introduction to modular arithmetic
- Group theory

2 Fundamentals of Field Arithmetic

Given two integers a, b the cost of performing standard operations is as follows:

- $a + b$, $a \times b$, $\frac{a}{b}$, $a \mid b$: poly in input size.
- a^b: result of computation is exponential in input size, so trivially there exists no algorithm to perform exponentiation in poly time.
- $\mathsf{gcd}(a, b)$:
  1. if $a = b$, output b
  2. else 'divide' b by a to obtain k, r such that $a = k \cdot b + r$ where $r < b$, and output $\mathsf{gcd}(b, r)$.

  Euclid's algorithm (above) computes the greatest common divisor of a and b. As $\frac{b+r}{2b+r} \leq \frac{2}{3}$, there are at most $\log_{\frac{3}{2}}(a + b)$ iterations, keeping the overall running time polynomial in the inputs.
- $\mathsf{egcd}(a, b) = (x, y)$ such that $a \cdot x + b \cdot y = \mathsf{gcd}(a, b)$: can be computed in poly time by extending Euclid's algorithm, as described below.
  $\mathsf{egcd}(a, b)$:
  1. if $a = b$, output $(1, 0)$
  2. else 'divide' b by a to obtain k, r such that $a = k \cdot b + r$ where $r < b$, and compute $(x', y') = \mathsf{egcd}(b, r)$.
  3. Output $(y', x' - y' \cdot k)$.

3 Modular Arithmetic

The set of integers modulo N is denoted $\mathbb{Z}_N$. Given $a, b \in \mathbb{Z}_N$, computing $(a+b) \pmod N$ and $(a \cdot b) \pmod N$ is straightforward to do in poly time.

Given $a \in \mathbb{Z}_N$, the 'inverse' of a is denoted a^{-1}, and by definition $a \cdot a^{-1} = 1 \pmod N$.

Theorem 1 *An $a \in \mathbb{Z}_N$ has an inverse if and only if* $\mathsf{gcd}(a, N) = 1$.

Proof: For a given $a \in \mathbb{Z}_N$, denote its inverse x. By definition, $a \cdot x = 1 \pmod N$. This implies that $\exists y$ such that $a \cdot x = 1 + N \cdot y$. This gives proves the existence of integers (x, y) such that $a \cdot x - N \cdot y = 1$, which implies that $\mathsf{gcd}(a, N) = 1$. $\square$

Exponentiation. Given $a, b \in \mathbb{Z}_N$, computing $a^b \pmod N$ can be done in poly time via the 'repeated square' algorithm. Let the number of bits to represent an element in $\mathbb{Z}_N$ be $n = \log_2 N$. The technique is to parse b into bits $b_0 b_1 \cdots b_n$, and then make use of the observation that $b = \sum_{i \in [n]} 2^i \cdot b_i$ to simplify the computation as follows:

$$a^b = a^{\left(\sum_{i \in [n]} 2^i \cdot b_i\right)} = \prod_{i \in [n]} a^{2^i \cdot b_i}$$

The algorithm itself follows easily, as described below.
$\mathsf{exp}_N(a, b)$:

1. Parse b into bits $b_0 b_1 \cdots b_n$.
2. Set $c = 1$, and $d = a$.
3. If $b_0 = 1$, update $c = a$
4. For $i \in [2, n]$: Update $d = d^2$. If $b_i = 1$, then update $c = c \cdot d \pmod N$
5. Output c.

4 Groups

A group $(\mathbb{G}, *)$ characterized by a set of elements $\mathbb{G}$ and an operator $*$, satisfies the following properties:

1. **Closure:** $\forall a, b \in \mathbb{G}$, we have that $a * b \in \mathbb{G}$.
2. **Associativity:** $\forall a, b, c \in \mathbb{G}$, we have that $(a * b) * c = a * (b * c)$.
3. **Identity:** $\exists e \in \mathbb{G}$ such that $\forall a \in \mathbb{G}$, $a * e = e * a = a$.
4. **Inverse:** $\forall a \in \mathbb{G}$, $\exists a^{-1} \in \mathbb{G}$ such that $a * a^{-1} = a^{-1} * a = e$.

It's easy to see that $(\mathbb{Z}_N, +)$ is a group with identity element $e = 0$. However $(\mathbb{Z}_N, \times)$ is not a group (as 0 does not have an inverse for any N), and may not be a group for every N even if zero is omitted. This is because inverses exist only for $a \in \mathbb{Z}_N$ where $\mathsf{gcd}(a, N) = 1$. We instead work with group $(\mathbb{Z}_N^*, \times)$, where $\mathbb{Z}_N^* = \{a : a \in \mathbb{Z}_N,\ \mathsf{gcd}(a, N) = 1\}$.

Group order. The order $\varphi(N)$ of N is given by the size of the group $\mathbb{Z}_N^*$, ie. $\varphi(N) = |\mathbb{Z}_N^*|$. It is easy to see that for a prime p, $\varphi(p) = p - 1$.

Subgroups. If $\mathbb{H} \subseteq \mathbb{G}$, we call $H = (\mathbb{H}, *)$ a subgroup of $G = (\mathbb{G}, *)$ if $(\mathbb{H}, *)$ is also a group. This is denoted $H \subseteq G$.

Theorem 2 *Lagrange's Theorem. Let $H = (\mathbb{H}, *)$ and $G = (\mathbb{G}, *)$ be groups. If $H \subseteq G$, then $|\mathbb{H}|$ divides $|\mathbb{G}|$.*

Proof: Let $\mathbb{H} = \{h_1, h_2 \cdots h_{|\mathbb{H}|}\}$. Pick $g_1 \in \mathbb{G}$, $g_1 \notin \mathbb{H}$ and enumerate $g_1\mathbb{H} = \{g_1 \cdot h_1, g_1 \cdot h_2 \cdots g_1 \cdot h_{|\mathbb{H}|}\}$. Continue to pick $g_i \in \mathbb{G}$, $g_i \notin \mathbb{H} \cup \{g_1, g_2 \cdots g_{i-1}\}$ and generate $g_i\mathbb{H} = \{g_i \cdot h_1, g_i \cdot h_2 \cdots g_i \cdot h_{|\mathbb{H}|}\}$. Note that $g_i\mathbb{H}$ and $g_j\mathbb{H}$ are completely disjoint sets when $i \neq j$. This can be shown as follows: consider g such that $g \in g_i\mathbb{H}$ and $g \in g_j\mathbb{H}$. Therefore $g_i \cdot h_{i'} = g_j \cdot h_{j'} = g$ for some $i', j' \in [|\mathbb{H}|]$. This gives us $g_i = g_j \cdot h_{j'} \cdot h_{i'}^{-1}$. Now, any element in $g_i\mathbb{H}$ can be interpreted as $g_i \cdot h_k = g_j \cdot h_{j'} \cdot h_{i'}^{-1} \cdot h_k = g_j \cdot h_{k'}$ for some k'. This proves that if $g_i\mathbb{H}$ and $g_j\mathbb{H}$ have even one common element, then $i = j$. As all the $g_i\mathbb{H}$ sets are therefore disjoint, once we exhaust all possible $g_i \in \mathbb{G}$ we will have that $\sum_{i \in [n]} |g_i\mathbb{H}| = |\mathbb{G}|$ for some integer n. $\square$

Corollary 1 *If p is prime, then $\forall a \in \mathbb{Z}_p^*$, $a^{p-1} = 1 \pmod{p}$.*

Cyclic Groups. Let $G = (\mathbb{G}, *)$. Consider $g \in \mathbb{G}$. Denote $\langle g \rangle = \{g^0, g^1, \cdots g^{q-1}\}$ as the subgroup 'generated' by g. We say that G is cyclic if $\langle g \rangle$ is cyclic, ie. $g^q = g^0 = 1$. Note that $g^i \cdot g^j = g^{i+j \pmod{q}}$. The size q of $\langle g \rangle$ is the order of the group.

Proof: (Postponed proof of Fermat's Little Theorem, see Corollary 1).
$|\langle a \rangle| = q \mid (p-1)$, so $a^{p-1} = a^{q \cdot k} = 1 \pmod{p}$ $\square$

Also observe that $a^b \pmod{N} = a^{b \pmod{\varphi N}} \pmod{N}$, so $a^b = a^{\varphi N \cdot k + b \pmod{\varphi N}}$. Note that $\langle g \rangle$ is isomorphic to $\mathbb{Z}_q$, ie. $(\langle g \rangle, \cdot) \cong (\mathbb{Z}_q, +)$.

Theorem 3 *If p is prime, then $(\mathbb{Z}_p^*, \times)$ is a cyclic group. ie. $\exists g$ such that $\mathbb{Z}_p^* = \{1, g, g^2, \cdots g^{p-1}\}$.*