Introduction to Cryptography February 20, 2018

Lecture 11: Number Theory

Instructor: Vipul Goyal *Scribe: Ariela Immordino*

1 Introduction

This lecture will go over the relevant background from number theory and hardness assumptions that will allow us to construct a One-Way-Function and eventually a One-Way-Permutation.

Preliminary Notation:

- $\mathbb{N}$ = the set of natural numbers
- $\mathbb{Z}$ = the set of integers
- $\mathbb{R}$ = the set of real numbers

2 Modular Arithmetic

Definition 1 *For any $N \in \mathbb{N}$, Z_N denotes the integers from 0 to $N-1$ (i.e. the integers mod N). Equivalently $Z_N = \{x \in \mathbb{N} : 0 \leq x < N\}$.*

For any $x \in \mathbb{N}$, the value of $x \mod N$ is r where r satisfies the following equation: $x \cdot \lfloor \frac{x}{N} \rfloor + r = N$. In other words, r is the remainder when you divide x by N.

We can do both addition and multiplication in the modular universe:

- Addition: $(a+b) \mod N = ((a \mod N) + (b \mod N)) \mod N$
- Multiplication: $(a \cdot b) \mod N = ((a \mod N) \cdot (b \mod N)) \mod N$

3 Greatest Common Divisor (GCD)

Definition 2 *For $a, b \in \mathbb{Z}$, GCD(a, b) is defined to be the greatest common divisor of a and b.*

Remark 1 *If $a, b \in \mathbb{Z}$ are relatively prime then $GCD(a, b) = 1$.*

Theorem 1 *For all $a, b \in \mathbb{N}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = GCD(a, b)$.*

Proof. The **Extended Euclidean Algorithm (EEA)** shows how to compute x and y given a and b in poly-time. ■

Lemma 2 *If $a, b \in \mathbb{N}$ are relatively prime with $a < b$, then $\exists c \in \mathbb{N}$ such that $a \cdot c = 1 \mod b$.* ***In other words, c is the inverse of $a \mod b$.***

Proof. (of Lemma 2) By EEA, we can compute $x, y \in \mathbb{Z}$ such that $ax + by = GCD(a, b)$. Since a and b are relatively prime, $GCD(a, b) = 1$.

$$\begin{aligned} ax + by &= 1 \\ \Rightarrow ax &= 1 - by \\ \Rightarrow ax \mod b &= (1 - by) \mod b \\ \Rightarrow ax &= (1 \mod b) + (-by \mod b) \\ \Rightarrow ax &= 1 \mod b \end{aligned}$$

Therefore, x is the inverse of $a \mod b$ ∎

4 Euler's Phi Function

Definition 3 *For any $N \in \mathbb{N}$, Z_N^* denotes the integers that are relatively prime to N and less than N. Equivalently $Z_N^* = \{x \in \mathbb{N} : x < N \text{ and } GCD(x, N) = 1\}$.*

Definition 4 ***Euler's Phi Function*** *(sometimes called Euler's Totient Function) is defined as follows: $\phi(N) = |Z_N^*|$*

Examples:

- $Z_4^* = \{1, 3\}$ and $\phi(4) = 2$
- $Z_9^* = \{1, 2, 4, 5, 7, 8\}$ and $\phi(9) = 6$
- $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and $\phi(11) = 10$
- for any prime p: $Z_p^* = \{1, 2, ..., p\}$ and $\phi(p) = p - 1$

Theorem 3 ***Fundamental Theorem of Arithmetic****: Every integer N can be represented as follows: $N = \prod_i p_i^{e_i}$ where $p_1 < p_2 < ... < p_k$, $\forall i.e_i > 0$ and p_i is prime. This representation is unique. $\prod_i p_i^{e_i}$ is called the prime factorization of N.*

Lemma 4 *For $N = \prod_i p_i^{e_i}$ where $p_1 < p_2 < ... < p_k$ and $\forall i.e_i > 0$ and p_i is prime.*

$$\phi(N) = N \cdot \prod_i (1 - \frac{1}{p_i})$$

Proof. By the Fundamental Theorem of Arithmetic, we know that $N = \prod_i^k p_i^{e_i}$. we will prove this using the Inclusion/Exclusion Principle[1]:

Let $A_i = \{x \in \mathbb{N} : 0 < x \leq N \text{ and } p_i \text{ divides } x\}$ for $1 \leq i \leq k$.

$$\phi(N) = |\bigcap_{i=1}^{k} \bar{A}_i| = N - |\bigcup_{i=1}^{k} A_i|$$

[1] $|\bigcup_i^n A_i| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$ (where $[n] = \{1, 2, ..., n\}$)

By the inclusion exclusion theorem:

$$\phi(N) = N - \sum_{\emptyset \neq I \subseteq [k]} (-1)^{|I|+1} |A_I| \qquad (\text{where } A_I = \bigcap_{i \in I} A_i)$$

We know that the $|A_I| = \frac{N}{\prod_{i \in I} p_i}$ since this is the amount of numbers between 1 and N that are divisible by all the p_i for $i \in I$. This gives us:

$$\phi(N) = N - \sum_{\emptyset \neq I \subseteq [k]} (-1)^{|I|+1} \frac{N}{\prod_{i \in I} p_i} = N(1 - \sum_{\emptyset \neq I \subseteq [k]} (-1)^{|I|+1} \frac{1}{\prod_{i \in I} p_i}) = N \prod_{i \in [k]} (1 - \frac{1}{p_i})$$

The last equality is by the following identity and letting $x_i = \frac{1}{p_i}$:

$$1 - \sum x_i + \sum x_i x_j - \sum x_i x_j x_k + ... + (-1)^n x_1 x_2 \cdots x_n = \prod_{i=1}^{n} (1 - x_i)$$

(Side Note: There are simpler proofs that use that ϕ is multiplicative and that $\phi(p^k) = p^k(1 - \frac{1}{p})$. One such proof can be found *here*.)

■

Remark 2 *We can verify that* $\phi(p) = p(1 - \frac{1}{p}) = p - 1$.

Remark 3 *If* $N = pq$ *where* p, q *are prime and* $p \neq q$ *then* $\phi(N) = N(1 - \frac{1}{p})(1 - \frac{1}{q}) = (p-1)(q-1)$. *(We shall see later that this is used in RSA.)*

Theorem 5 ***Fermat's Little Theorem****: If* p *is prime, for any* $a \in Z_p^*$,

$$a^{p-1} \mod p = 1$$

Theorem 6 ***Euler's Generalization****: For any* N*, for any* $a \in Z_N^*$,

$$a^{\phi(N)} \mod N = 1$$

5 Introduction to Groups

We have already seen some groups, namely Z_N with addition $\mod N$ and Z_N^* with multiplication $\mod N$, but now we will formally define what a group is. Later we will see that calculating certain things is assumed to be hard which we will take advantage of to construct a One-Way-Function.

Definition 5 *A* ***group*** *consists of a set* G *and a group operation* $\odot : G \times G \rightarrow G$ *and is formally referred to as* $(G, \odot)$*. It must satisfy the following properties:*

1. *Closure:* $\forall a, b \in G$, *if* $c = a \odot b$ *then* $c \in G$
2. *Identity: there must exist an* $e \in G$ *such that* $\forall a \in G$, $a \odot e = e \odot a = a$
3. *Associativity:* $\forall a, b, c \in G$, $(a \odot b) \odot c = a \odot (b \odot c)$

4. *Inverse: $\forall a \in G$, $\exists b \in G$ such that $a \odot b = b \odot a = e$ where e is the identity element*

Definition 6 *An* ***Abelian Group*** $(G, \odot)$ *is a group with the additional requirement that the group operation is commutative. Formally $\forall a, b \in G$ it must hold that $a \odot b = b \odot a$.*

Proposition 1 *Z_N is a group where the group operation is addition modulo N (it is assumed that this is the group operation unless stated otherwise).*

Proposition 2 *Z_N^* is a group where the group operation is multiplication modulo N (it is assumed that this is the group operation unless stated otherwise).*

Proof.

1. Closure: If $a, b \in Z_N^*$ then we will show that $(a \cdot b) \mod N \in Z_N^*$. Since both a and b are relatively prime to N, it must be the case that $(a \cdot b)$ is also relatively prime to N. Using the identity that $GCD(a \cdot b, N) = GCD((a \cdot b) \mod N, N)$ we conclude that $(a \cdot b) \mod N \in Z_N^*$.

2. Identity: We claim that 1 is the identity element. We can confirm that for any $x \in Z_N^*$ that $1 \cdot x = x \cdot 1 = x \mod N$

3. Associativity: Follows from the fact that multiplication modulo N is associative.

4. Inverses: Consider $x \in Z_N^*$. Since x and N are relatively prime, we can use EEA to find a c such that $xc = 1 \mod N$. We now just need to prove that c must also be relatively prime to N which lets us conclude that $(c \mod N) \in Z_N^*$.

   Suppose it isn't, then $\mathrm{GCD}(c, N) = d > 1$ which means that $N = N' \cdot d$ and $c = c' \cdot d$ where $c', N' \in \mathbb{N}$.

$$
\begin{aligned}
1 &= x \cdot c \mod N \\
\Rightarrow \frac{N}{d} &= (x \cdot c) \cdot \frac{N}{d} \mod N \\
&= \frac{N}{d} \cdot x \cdot c'd \mod N \\
&= N \cdot x \cdot c' \mod N \\
&= 0 \mod N \\
\Rightarrow 1 &= 0 \mod N
\end{aligned}
$$

   This is a contradiction since $1 \leq \frac{N}{d} < N$.

■

Remark 4 *In cryptography the group that is nearly always used is Z_N^*.*

Definition 7 *A* ***generator*** *$g \in G$ must be such that $\{g, g^2, g^3, ...\} = G$. Where for $n \in \mathbb{N}$, $x \in G$, $x^n = \underbrace{x \odot x \odot .. \odot x}_{n \text{ times}}$*

Definition 8 *The* ***order*** *of a group $(G, \odot)$ is equal to $|G|$.*

Theorem 7 *If the order of a group G is n then $\forall a \in G$, $a^n = e$. (This is similar to Euler's Generalization but for an arbitrary group. It is actually a corollary of Lagrange's Theorem.)*

6 Multiplicative Groups of Prime Order

We will now continue discussing and proving results about groups but with the focus of eventually constructing a One-Way Function.

Definition 9 *A **Prime Order Group** is a group where the order is a prime.*

We will see later that the most important groups in cryptography are multiplicative groups of prime order. Unfortunately the group $(Z_p^*, \cdot)$ has order $|Z_p^*| = p - 1$ so we will have to look elsewhere.

Theorem 8 ***Constructing Multiplicative Groups of Prime Order**: Let p be a prime such that $p = 2q + 1$ where q is also a prime. The group $G_q = \{x^2 : x \in Z_p^*\}$ with multiplication modulo p is a group of order p.*

Definition 10 *We will use G_q to denote a multiplicative group of order q where q is prime.*

Remark 5 *Primes that are of the form $2q + 1$ where q is also a prime are called **safe primes** in cryptography and are more generally known as Sophie-German primes.*

Theorem 9 *Every non-identity element of G_q is a generator.*

Proof. Suppose not. Then there exists a $g \in G_q$ such that $g^i = 1 \mod p$ for some $0 < i < q$. Let i be the smallest such exponent that satisfies that requirement.

By Theorem 7, we know that $g^q = 1 \mod p$. Consider the following the some $k \in \mathbb{N}$ such that $ki \leq q$:

$$\begin{aligned} g^q &= 1 \mod p \\ \Rightarrow g^{q-ki} \cdot g^{ki} &= 1 \mod p \\ \Rightarrow g^{q-ki} &= 1 \mod p \qquad\qquad [\text{since } g^{ki} = (g^i)^k = 1^k = 1 \mod p] \end{aligned}$$

Now consider the largest such $k \in \mathbb{N}$ such that $ki \leq q$. This means that $0 \leq q - ki < i$. If $q - ki = 0$ then q is a multiple of k which contradicts that q is prime. If $0 < q - ki$ since it is also less than i and $g^{q-ki} = 1 \mod p$, this contradicts that i was the smallest exponent for which that was true. ■

7 Discrete Log Problem and Assumption

Definition 11 *The **Discrete Log Problem** is defined for a group $(G, \odot)$. Given $g \in G$ where g is a generator for G and an $x \in G$, return the exponent $e \in \mathbb{N}$ where $0 \leq e < |G|$ where $g^e = x$. Then e is called the discrete log of x with respect to the generator g.*

Assumption 1 ***Discrete Log Assumption (DLA)**: Given G_q and a generator $g \in G_q$, then for every PPT A*

$$\boldsymbol{Pr}[x \xleftarrow{\$} Z_q : A(g^x) = x] \leq \nu(\log q)$$

(where $\nu(\cdot)$ is a negligible function)

Remark 6 *The DLA is believed to be true only for certain multiplicative prime order groups as there are attacks for primes of certain forms.*

8 Constructing a 1-1 One-Way Function

Theorem 10 *Let $f_g : Z_q \rightarrow G_q$ be defined as follows: $f_g(x) = g^x$. This f_g is a 1-1 One-Way Function.*

Proof. *Claim 1:* f_g is a 1-1 function.
Consider $x_1, x_2 \in Z_q$ such that $x_1 \neq x_2$ (WLOG $x_1 > x_2$). It must be the case that $f_g(x_1) = g^{x_1} \neq g^{x_2} = f_g(x_2)$ because g is a generator.
Suppose not. Then $g^{x_1} = g^{x_2} \Rightarrow g^{x_1 - x_2} = 1$. Since g is a generator, $x_1 - x_2$ is either 0 or a multiple of q. The first contradicts that x_1 and x_2 are not equal and the second contradicts that they were taken from the set Z_q.
Claim 2: f_g is a OWF.
Suppose not. There is a PPT A such that

$$\mathbf{Pr}[x \xleftarrow{\$} Z_q, A(f_g(x)) = x' : f(x') = f(x)] \geq \frac{1}{poly(\log q)}$$

Since we know that f_g is 1-1, we can simplify this probability to:

$$\mathbf{Pr}[x \xleftarrow{\$} Z_q : A(f_g(x)) = x] \geq \frac{1}{poly(\log q)}$$

Using the definition of f_g we get that that probability is equivalent to:

$$\mathbf{Pr}[x \xleftarrow{\$} Z_q : A(g^x) = x] \geq \frac{1}{poly(\log q)}$$

The existence of this PPT A contradicts the DLA. ■

Remark 7 *f_g is not a One-Way Permutation because $|Z_q| \neq |G_q|$.*