EECS 475: Introduction to Cryptography Notes

Noah Peters

March 27, 2023

Abstract

Lecture notes for EECS 475 at the University of Michigan. LaTeXtemplate by Pingbang Hu.

Contents

4 Introduction **2**

4.1 Modular Arithmetic and Euclid's Algorithm 2

4.2 Group Theoretic View of Numbers 3

4.3 Fast Exponentiation 5

A Additional Proofs **7**

A.1 Proof of **??** 7

Chapter 4

Introduction

Lecture 19: Number Theory

20 Mar. 10:30

4.1 Modular Arithmetic and Euclid's Algorithm

We define the set of integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, and natural numbers, $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

Theorem 4.1.1 (Product of primes)**.** Every integer $N > 1$ can be written *uniquely* as a product of (power of) primes.

Lemma 4.1.1 (Division with remainder)**.** Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+$. $\exists$ unique integers q, r such that $a = q.b + r$ where $0 \leq r < b$, and they can be efficiently computed in *polynomial time* relative to the *bit length*: i.e. $\log_2 a + \log_2 b + O(1)$

With the ability to perform division in polynomial time, we are able to find the **greatest common divisor** of two integers a, b:

Definition 4.1.1 (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}^+$. Then, there exists $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = a.x + b.y$. Further, $\gcd(a, b)$ is the *smallest* positive integer that can be written this way.

We claim there is an efficient algorithm, the **Extended Euclidean Algorithm**, that computes not only $\gcd(a, b)$, but also the x, y coefficients above:

Algorithm 4.1: Extended Euclidean Algorithm

Data: $a, b \in \mathbb{Z}$ where $a \geq b > 0$
if $b | a$ **then**
  return $x = 0, y = 1$
else
  write $a = q.b + r$ where $0 < r < b$
$x', y' \leftarrow$ **ExtEuclid**(b, r)
return $x = y', y = x' - y'.q$

Verification of Extended Euclidean Algorithm. Assuming the recursive call is successful (by induction, we can), we will get back x', y' that are the gcd of b and r:

$$b.x' + r.y' = \gcd(b, r) = \gcd(a, b)$$
$$b.x' + (a - q.b).y' = a.y' + b(x' - q.y')$$

We note that $y' = x$ and $x' - q.y' = y$ and so we are done. ■

We claim that the Extended Euclidean Algorithm makes $\mathrm{O}(n)$ recursive calls.

4.2 Group Theoretic View of Numbers

Definition 4.2.1. Let $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$, indicating the set of all possible remainders of division by N, further: $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N : \gcd(x, N) = 1\}$.

Remark. For example, $\mathbb{Z}_6^* = \{1, 5\}$. Alternatively, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, showing how $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, where p is any prime number.

Lecture 20: Group Theory

We continue our review of modular arithmetic. Modular addition, subtraction, and multiplication are all closed in modular arithmetic. We have the property $a = b \mod N \Leftrightarrow N | a - b$ and further, if $a = a' \mod N$ and $b = b' \mod N$, we have: 22 Mar. 10:30

- $a + b = a' + b' \mod N$
- $a - b = a' - b' \mod N$
- $a.b = a'.b' \mod N$

However, division is not always possible:

$$3 \cdot 2 = 15 \cdot 2 \mod 24 \not\Rightarrow 3 = 15 \mod 24$$

Definition 4.2.2 (Invertability). An integer b is **invertible** if $\exists c$ where $b \cdot c = 1 \mod N$.

Lemma 4.2.1. If $b \geq 1, N > 1$, b is invertible mod $N \Leftrightarrow \gcd(b, N) = 1$.

Proof. Let $b \cdot c = 1 \mod N$.

$$\begin{aligned} &\Rightarrow b.c - 1 = N.q \\ &\Rightarrow b.c - N.q = 1. \end{aligned}$$

Thus, $\gcd(b, N) = 1$ since gcd is the smallest positive integer that is expressible in this way. ■

Using the Extended Euclidean Algorithm, we can compute inverse mod N efficiently.

Definition 4.2.3 (Group). $(G, \circ)$, where $\circ : G \times G \to G$ and $\circ(g, h)$ is denoted as $g \circ h$, is a **group** if it satisfies the properties of:

- identity: $\exists e \in G$ such that $\forall g \in G : e \circ g = g \circ e = g$
- invertability: $\forall g \in G, \exists g^{-1}$ (or $-g$) such that $g \circ g^{-1} = e$
- associativity: $\forall g_1, g_2, g_3 \in G : (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$
- (abelian groups): $\forall g, h \in G, g \circ h = h \circ g$ (i.e commutativity)

Example. For $(\mathbb{Z}_N, + \mod N)$ we have:

- identity: $a + 0 \equiv 0 + a \equiv a \mod N$
- invertability: $a + (-a) \equiv 0 \mod N$
- associativity: $a + (b + c) = (a + b) + c \mod N$

Example. For $(\mathbb{Z}_N^*, . \mod N)$ we have:

- identity: $a.1 \equiv 1.a \equiv a \mod N$
- invertability: $a.(a^{-1}) \equiv 1 \mod N$
- associativity: $a.(b.c) = (a.b).c \mod N$

The size of a group, called the **group order**, is denoted as $|G|$. For example, $(\mathbb{Z}_N, +)$ has order N, and $\mathbb{Z}_p^*, .$ has order $p-1$

Theorem 4.2.1. For a group, G, where $m = |G|$, we have that $\forall g \in G$: $g^m = 1$ (where $g^m = (((g \circ g) \circ g) \circ g) \ldots)$.

Proof. For simplicity, assume G is abelian and suppose $G = \{g_1, g_2, \ldots, g_m$ and let $g \in G$ be arbitrary. Note that

$$g \circ g_i = g \circ g_j \Rightarrow g_i = g_j$$

and so the set $\{g \circ g_i : i \in \{1, m\}\}$ covers all elements of G exactly once. Therefore:

$$g_1 \circ - g_m = g^m(g_1 \circ \ldots \circ g_m) \Rightarrow 1 = g^m.$$

■

Corollary 4.2.1 (Fermat's Little Theorem)**.** $\forall$ prime p, $\gcd(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \mod p$

Theorem 4.2.2 (Euler's Theorem)**.** For $\Phi(N) = \big|\{a|1 \leq a \leq N, \gcd(a, N) = 1\}\big|$, $|\mathbb{Z}_N^*| = \Phi(N)$ we have:

$$\text{if } \gcd(g, N) = 1 \Rightarrow g^{\Phi(N)} \equiv 1 \mod N$$

Corollary 4.2.2. For $m = |G| > 1, e \in \mathbb{Z}, \gcd(e, m) = 1$, define $d = e^{-1} \mod m$ and function $f_e \colon G \to G$ as $f_e(g) = g^e$. Then, f_e is a bijection whose inverse is f_d.

Definition 4.2.4 (Cyclic Groups)**.** A group, G, is considered **cyclic** if $\exists g \in G$ such that $G = \{1 = g^0, g^1, g^2, \ldots, g^{m-1}\}$. If this is the case, we say that g generates G.

Example. For $\mathbb{Z}_7^* = \{1, \ldots, 6\}$:

$$\text{powers of 3: } \{3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5\}$$

$$\text{powers of 2: } \{2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, \ldots\}$$

and so 3 is a generator of $\mathbb{Z}_7^*$, but 2 is not.

If there is no $g \in G$ that generates G, then G is not cyclic. Furthermore, when g does not generate G, it generates a **subgroup**:

Definition 4.2.5. $G' \subseteq G$, is a subgroup if $(G', \circ)$ is a group.

Theorem 4.2.3 (Lagrange's Theorem)**.** If $G' \subseteq G$ is a subgroup, then $|G'|$ divides $|G|$.

4.3 Fast Exponentiation

Suppose we have an element g and we want to compute g^M. Instead of naively multiplying g M times, we can observe that if $M = 2^m$:

$$g^M = g^{2^m} = g^{2^{m-1}} \cdot g^{2^{m-1}} = (g^{2^{m-1}})^2.$$

So for any M we can rewrite it as

$$M = \sum_{i=0}^{l} m_i.2^i,$$

allowing us to calculate g^m:

$$g^m = \prod_{i=0}^{l} g^{2^i},$$

where each g^{2^i} can be calculated using the above trick. This results in $O(l^2)$ multiplications altogether if $|M| = l$.

Corollary 4.3.1. Fast exponentiation allows us to compute inverses efficiently because $g^{-1} = g^{|G|-1}$ since $g^{|G|} = 1$.

We've shown we can compute g^m efficiently given g and m. But, can we efficiently compute m from g^m? It's unknown, but conjectured to be extremely difficult to do so.

Appendix

Appendix A

Additional Proofs

A.1 Proof of ??

We can now prove **??**.

Proof of ??. See here. ■