CPEG 472/672 — Applied Cryptography April 28, 2020

Handout A

Instructor: Nektarios Tsoutsos

1 Basic Divisibility

We denote a set of integers with $\mathbb{Z}$. If $a, b, q, r \in \mathbb{Z}$, the Euclidean division Theorem states that:

$$a = q \cdot b + r \text{ so that } 0 \leq r < b. \tag{1}$$

In this case, we write $a = r \bmod q$.

For $a, b, q \in \mathbb{Z}$, we say *a divides b* and write $a|b$ if there exists integer q so that $a \cdot q = b$. If $a, b, c, X, Y \in \mathbb{Z}$ so that $a|b$ and $a|c$, then $a|(Xb + Yc)$ for any X, Y. If $a, b \in \mathbb{Z}$ and $a|b$ so that $a \neq 1$ and $a \neq b$, then a is called a *non-trivial factor* of b.

Prime numbers: An integer $p > 1$ is called a *prime number* if it does not have non-trivial factors. Note, the first prime number is 2.

Modular arithmetic: If $a, b, N \in \mathbb{Z}$ we say that a, b are *congruent modulo N* if the remainder ($a \bmod N$) equals the remainder ($b \bmod N$). That is, a, b are congruent modulo N when:

$$a = q_a \cdot N + r, \quad b = q_b \cdot N + r. \tag{2}$$

If a is congruent to b modulo N, we write $a \equiv b \bmod N$.

Multiplicative inverse mod$N$**:** If $b, N \in \mathbb{Z}$, we define the multiplicative inverse of b the value b^{-1} so that $b \cdot b^{-1} = 1 \bmod N$.

2 The Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic states that every integer greater than 1 can be expressed in *exactly one way* (apart from rearrangement) as *a product of one or more primes*. This is also known as the *unique factorization theorem*.

Greatest Common Divisor (GCD): If $a, b \in \mathbb{Z}$ so that $a \geq 0$ and $b \geq 0$ but not both $a, b = 0$ at the same time, then $GCD(a, b)$ equals the largest integer c so that $c|a$ and $c|b$.

Remarks: If p is prime, $GCD(a, p)$ equals either 1 or p. If $a, b \in \mathbb{Z}$ and $GCD(a, b) = 1$, then a, b are *relatively prime* (or co-prime or mutually prime). If $a, b, c \in \mathbb{Z}$ with $GCD(a, b) = 1$ and $a|c$ as well as $b|c$, then $ab|c$. If $a, N \in \mathbb{Z}$ with $N > 1$, then a has a *modular multiplicative inverse* if and only if $GCD(a, N) = 1$. The GCD can be efficiently computed using the *Euclidean Algorithm*.

Extended Euclidean Algorithm: If $a, b \in \mathbb{Z}$ and $a, b > 0$, then there exist $X, Y \in \mathbb{Z}$ so that $GCD(a, b) = X \cdot a + Y \cdot b$. The value of X, Y and $GCD(a, b)$ can be efficiently computed using the *Extended Euclidean Algorithm*.

3 Basic Group Theory

A *Group* $\mathbb{G}$ is a set of numbers along with a mathematical operation $\diamond$ that has the following properties:

1. *Closure:* For any a, b in the group, then $a \diamond b$ is also in the group.
2. *Associativity:* For any a, b, c in the group, then $(a \diamond b) \diamond c = a \diamond (b \diamond c)$.
3. *Existence of unique identity:* The group as a unique element e so that $e \diamond a = a \diamond e = a$ for any a in the group.
4. *Existence of inverse for each element:* For any a in the group, there is always a unique element b in the group so that $a \circ b = e$.

A Group $\mathbb{G}$ is called an *Abelian* group if it also *commutative*, so that $a \diamond b = b \diamond a$. When the group operation is *additive* then $\diamond$ resembles addition $(+)$, while when the group operation is *multiplicative* then $\diamond$ resembles multiplication $(\cdot)$. In a multiplicative group, we can write $g^b = g \cdot g \cdot \ldots \cdot g$, to indicate that g is multiplied b times.
Example: The set of integers is an Abelian Group under addition. However, the set of integers is not a group under multiplication as many integers do not have a multiplicative inverse (such as integer 2).
Order of a group: The order of a Group $\mathbb{G}$, denoted as $|\mathbb{G}|$, is the number of its elements (i.e., its *cardinality*).

3.1 Finite Groups

If $\mathbb{G}$ is group and $n = |G|$ is the order of the group, we say that $\mathbb{G}$ is a *finite group* if it contains a finite number of elements. In this case, for any element $g \in \mathbb{G}$, we have $g^n = 1$.

If $\mathbb{G}$ is a finite group and $n = |G| > 1$ is the order of the group, then for any element $g \in \mathbb{G}$ and integer i, we have $g^i = g^{i \bmod n}$.
The Group $\mathbb{Z}_N$: If $N \in \mathbb{Z}$ and $N > 1$, then we define as $\mathbb{Z}_N$ the *additive* Abelian group of order N, comprising the integers $\{0, 1, \ldots, N-1\}$. The group operation is *addition modulo N*.
The Group $\mathbb{Z}_N^*$: If $N \in \mathbb{Z}$ and $N > 1$, then $\mathbb{Z}_N^*$ is an Abelian group under *multiplication modulo N* and it is defined as:

$$\mathbb{Z}_N^* = \{a, \text{ so that } 0 < a < N \text{ and } GCD(a, N) = 1\} \tag{3}$$

That is, $\mathbb{Z}_N^*$ is the group of integers less than N that *are invertible with respect to multiplication.* Invertibility is guaranteed for an integer a if and only if $GCD(a, N) = 1$. Note, not every integer less than N is invertible. In $\mathbb{Z}_N^*$ the identity element is integer 1.
Euler's totient function $\varphi()$: Every integer N is either prime or can be factorized to a set of primes and prime powers. If $N \in \mathbb{Z}$ then N is factorized as:

$$N = \prod_i p_i^{e_i}, \tag{4}$$

where p_i are distinct prime numbers raised to power $e_i > 0$, and $\prod_i$ denotes multiplication of i prime powers. Then, in the general case where we have prime powers (i.e., $e_i > 1$ for some i), Euler's totient function of N is denoted as $\varphi(N)$ and equals:

$$\varphi(N) = \prod_i p_i^{e_i - 1} \cdot (p_i - 1). \tag{5}$$

If we do not have prime powers in the factorization of N (i.e., when $e_i = 1$ for every prime p_i), then $\varphi(N)$ equals:

$$\varphi(N) = \prod_i (p_i - 1). \tag{6}$$

Example: If $N = 15 = 3 \cdot 5$ then $\varphi(N) = (3-1) \cdot (5-1) = 8$. Also, if p is a prime, $\varphi(p) = p - 1$.
The order of $\mathbb{Z}_N^*$: The order of the group $\mathbb{Z}_N^*$ is $|\mathbb{Z}_N^*| = \varphi(N)$.

3.2 Euler's Theorem

For any $N > 1 \in \mathbb{Z}$ and $a \in \mathbb{Z}_N^*$ it holds that:

$$a^{\varphi(N)} = 1 \bmod N \qquad \text{(Euler's Theorem)}. \tag{7}$$

Note, since $a \in \mathbb{Z}_N^*$, then a, N must be comprime (i.e., $GCD(a, N) = 1$).
Fermat's Little Theorem: If p is a prime integer and $a > 0 \in \mathbb{Z}_p$ then it holds that:

$$a^{p-1} = 1 \bmod p. \tag{8}$$

4 Cyclic Groups

If $\mathbb{G}$ is a finite group of order $m = |\mathbb{G}|$ and $g \in \mathbb{G}$ then $g^m = 1$. That is, any element of $\mathbb{G}$ multiplied m times, where m is the order of the group, equals 1.

If $i \in \mathbb{Z}$ with $0 < i \leq m$, and if i is the smallest integer so that $g^i = 1$, then g can generate exactly i elements of $\mathbb{G}$ (i.e., g defines a subgroup of $\mathbb{G}$). The integer i is called *the order of group element g*. Specifically, if $\mathbb{G}$ is a finite group and $g \in \mathbb{G}$ is a group element, the *order of* g is the smallest integer $i > 0 \in \mathbb{Z}$ so that $g^i = 1$. Note, the order of the group element g is not necessarily the same as the order of the group $\mathbb{G}$.

If $\mathbb{G}$ is a finite group of order $m = |\mathbb{G}|$, and $g \in \mathbb{G}$ has order i, then $i | m$.
Group Generators: If $\mathbb{G}$ is a finite group and there exists an element $g \in \mathbb{G}$ so that the order of g equals $m = |\mathbb{G}|$ (i.e., the order of g equals the order of $\mathbb{G}$), then $\mathbb{G}$ is a *cyclic group* and g is a *generator* of $\mathbb{G}$. Specifically, the set of all possible values g^a for $a \in \{0, 1, 2, \ldots, m-1\}$ is exactly the set of all m elements of $\mathbb{G}$.

If $\mathbb{G}$ is a *cyclic group* with order $m = |\mathbb{G}|$ then for each integer $d > 0$ that divides m there is exactly one subgroup of $\mathbb{G}$ of order d that has exactly $\varphi(d)$ different generators; each generator of the subgroup has order d.

If the order of $\mathbb{G}$ is a prime number p, then $\mathbb{G}$ is a *cyclic group.* In this case, every element of $\mathbb{G}$, except its identity element e, is a generator of $\mathbb{G}$.

If p is a prime number, then the group $\mathbb{Z}_p^*$ is cyclic. In this case, the order of the group is $|\mathbb{Z}_p^*| = p - 1$.