Recitation 1

In this recitation, we recall some mathematical background. These concepts will be used later in cryptographic constructions.

1 Modular Arithmetic

Definition 1.1. *For $n > 0$ and integers a, b we say that $a \equiv b \pmod{n}$ if n divides $a - b$. Also denoted as $n \mid a - b$.*

e.g. $7 \equiv 2 \pmod{5}$.

This relation is an equivalence relation. It is consistent with respect to addition and multiplication. That is, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denote the set of equivalence classes and the operations $+$ and $\cdot$ defined on them.

2 Groups

Definition 2.1 (Group). *A set G with an associated operation $\cdot : G \times G \to G$ is called a* group *if the following properties are satisfied:*

- Closure. *If $a, b \in G$ then the product $a \cdot b \in G$.*
- Associativity. *For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
- Identity. *There is an identity element e such that $e \cdot a = a \cdot e = a$ for all $a \in G$.*
- Inverse. *For all elements $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

In this class, most of the groups we will encounter will also be commutative*, i.e., $a \cdot b = b \cdot a$ for all $a, b \in G$.*

We start with examples:

- $(\mathbb{Z}, +)$ *Integers under addition.* The set $\{\cdots -2, -1, 0, 1, 2, \ldots\}$. Zero is the additive inverse.
- $(\mathbb{N}, +)$ *Natural numbers under addition.* No identity.
- $(\mathbb{Z}, \cdot\,)$ *Integers under multiplication.* No inverse for 2.
- $(\mathbb{Z}_n, +)$
- $\mathbb{Z}_n$ *under multiplication.* No inverse for 0.
- *Polynomials over integers of degree at most 2 under addition.*
- $\{\ldots, -4, -2, 0, 2, 4, 6 \ldots\}$ under addition.
- $\{-1, 1, 3, 5, \ldots\}$ *under addition.* No identity.
- $\mathbb{Z}_{11} \setminus \{0\}$ *under multiplication.* Works for any prime.
- Others that are groups: $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, the set of permutations on $\{0, 1, 2\}$ under function composition, vectors of integers: $\mathbb{Z}^2$.

2.1 $\mathbb{Z}_p \setminus \{0\}$ is a Group: The Extended Euclid's algorithm

Need to show that every $a \in \mathbb{Z}_p$, such that $a \neq 0$ has an inverse.

Definition 2.2 (Greatest Common Divisor (GCD)). *The* $\gcd(a, b)$ *is defined as the largest largest* $d \in \mathbb{Z}$ *such that* $d|a$ *and* $d|b$ *but* $\gcd(0, 0) = 0$.

e.g. $\gcd(10, 8) = 2$, $\gcd(3, 5) = 1$, $\gcd(10, 0) = 10$.

Definition 2.3 (Relatively prime). *Integers* a *and* b *are relatively prime if* $\gcd(a, b) = 1$.

Euclid's Algorithm for computing the GCD: For non-negative numbers a and b,

$$\gcd(a, b) = \begin{cases} a & \text{if } b = 0, \\ \gcd(b, a \bmod b) & \text{otherwise.} \end{cases}$$

Example: $\gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = \gcd(1, 0)$.

Theorem 2.4. *For* $a \not\equiv 0 \bmod p$, a^{-1} *exists and can be computed efficiently.*

Proof. We first show that it exists. Then we will describe an algorithm to compute it efficiently. Consider the set $S = \{a, 2a, 3a, \ldots (p-1)a\}$ all $\bmod p$.

First claim: $0 \notin S$. Because if $p|a * b$ then $p|a$ or $p|b$. Not possible.

Second claim: All the elements are distinct. If $ab \equiv ab' \pmod{p}$ then $p|a(b - b')$. Hence $p|a$ or $p|(b - b')$ and both are not possible as $0 < a < p$ and $0 < (b - b') < p$.

So all $p - 1$ elements in S are disjoint and non-zero. Hence by pigeonhole principle, one of them is 1. i.e., there exist b such that $ab \equiv 1 \pmod{p}$. □

The Extended Euclid's algorithm can compute $a^{-1} \bmod p$ for any $\gcd(a, p) = 1$. In the extended Euclid's algorithm, we compute not only the gcd, but also a witness x, y such that $ax + by = \gcd(a, b)$.

```
def Euclid(a, b):
  if b == 0:
    return a
  return Euclid(b, a % b)
```

```
def ExtEuclid(a, b):
  if b == 0:
    # As gcd(a,0) = a = a*1 + 0*0.
    return (a, 1, 0)
  (d, x1, y1) = ExtEuclid(b, a % b)
  # As d = b*x1 + (a%b)*y1 and
  # a = b*(a//b) + (a%b).
  return (d, y1, x1 - (a//b)*y1)
```

```
gcd(7,5)
  gcd(5,2)
    gcd(2,1)
      gcd(1,0)
      out (1,1,0)
    out (1,0,1)
  out (1,1,-2)
out (1,-2,3)
```

Figure 1: Euclid's Algorithm and Extended Euclid's Algorithm.

3 Finite Fields

We define the notion of a field.

Definition 3.1 (Field). *A tuple* $(F, +, \cdot)$ *is a field if the following properties are satisfied:*

1. $(F, +)$ *is a commutative group. That is,*
   (a) Closure. *If* $a, b \in F$ *then* $a + b \in F$.
   (b) Associativity. *For all* $a, b, c \in F$, $(a + b) + c = a + (b + c)$.
   (c) Identity. *There is an identity element* $0 \in F$ *such that* $0 + a = a + 0 = a$ *for all* $a \in F$.
   (d) Inverse. *For all elements* $a \in F$, *there exists* $-a \in F$ *such that* $a + (-a) = -a + a = 0$.
   (e) Commutativity. $a + b = b + a$ *for all* $a, b \in F$.

2. $(F \setminus \{0\}, \cdot\,)$ *is a commutative group. The identity element is called* 1.

3. Distributivity. *For all* $a, b, c \in F$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

Examples of fields include rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$. Integers $\mathbb{Z}$ are not a field because they do not have multiplicative inverses for non-zero elements.

Theorem 3.2. $(\mathbb{Z}_p, +, \cdot)$ *for any prime* p *is a field. Also denoted as* $\mathbb{F}_p$.

The proof is left as an exercise. The difficult part of showing that multiplicative inverses exist is already done.

Theorem 3.3. *Every finite field has size* p^k *for prime* p *and positive integer* k. *There exists a unique finite field of size* p^k *for all primes* p *and positive integers* k.

We will not show this. We will however describe the construction of finite fields of size 2^k. Let $f(x)$ be an irreducible polynomial of degree k over $\mathbb{F}_2$. To give some examples: $x^2+1 = (x+1)(x+1)$. While $x^2 + x + 1$ is irreducible.

Theorem 3.4. *Let* $f(x)$ *be an irreducible polynomial of degree* k *over* $\mathbb{F}_2$. *Then* $\mathbb{F}_2[x]/(f)$ *is a field where* $\mathbb{F}_2[x]$ *is the set of all polynomials over* $\mathbb{F}_2$.

Example 3.5. $\mathbb{F}_{2^2} = \{0, 1, x, x + 1\}$ with irreducible polynomial $x^2 + x + 1$. Addition is to simply add the polynomials over $\mathbb{F}_2$. And to multiply, first multiply the two polynomials and then compute the remainder modulo $f(x) = x^2 + x + 1$. e.g., $x(x + 1) = x^2 + x = 1$ after reducing mod f. And $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1 = x$.

Similarly we can construct $\mathbb{F}_{2^8}$ used in AES by using the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x + 1$.