BRIEF REVIEW OF MODULAR ARITHMETIC, GROUPS, AND FIELDS

1. Modular Arithmetic

Definition 1.1. Given an integer m called the *modulus*, we say for $a, b \in \mathbb{Z}$ that $a \equiv b \pmod{m}$ (a is *congruent* to b modulo m) if $m \mid a - b$.

Example 1.1. $5 \equiv 2 \pmod{3}$, $29 \equiv 5 \pmod{8}$, $-3 \equiv -7 \pmod{4}$

Consider $a = mq + r$, where r is the remainder when dividing a by m. Then $a \equiv r \pmod{m}$, i.e., computing modulo m means taking the remainder when dividing by m.

The following three statements are equivalent:

(1) $a \equiv b \pmod{m}$,
(2) there exists $k \in \mathbb{Z}$ with $a = b + km$,
(3) when divided by m, both a and b leave the same remainder.

Note. $a \equiv 0 \pmod{m}$ means that $m \mid a$.

Note. When performing modular arithmetic on a computer, it is usually convienient to work with least positive remainders. In other words, represent $a \bmod m$ by the unique integer $r \in \{0, 1, \ldots, m-1\}$ such that $a \equiv r \pmod{m}$. In most programming languages, the % operator returns a negative remainder if one of the operands is negative; you need to make it positive yourself.

```
a = -5 % 3     // a = -2
if (a < 0)
  a += 3       // a = 1
```

Congruence modulo m satisfies the following properties:

(1) $a \equiv a \pmod{m}$ (reflexive)
(2) $a \equiv b \pmod{m} \longrightarrow b \equiv a \pmod{m}$ (symmetric)
(3) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (transitive property)
(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Rules for performing arithmetic modulo m :

(1) Constants can be reduced modulo m (use least positive remainders).
(2) You can add or subtract anything from both sides of an equation.
(3) You can multiply anything to both sides of an equation.
(4) You can divide both sides by r if $\gcd(r, m) = 1$. If $d = \gcd(r, m) \neq 1$, you can do the same but the result is correct modular m/d.
(5) To change $-k \pmod{m}$ to its positive equivalent, add enough m's to $-k$ until it is positive.
(6) (Cancellation laws) If $a + k \equiv b + k \pmod{m}$, then $a \equiv b \pmod{m}$. If $ak \equiv bk \pmod{m}$, then $a \equiv b \pmod{m/\gcd(m, k)}$.

Example 1.2. Solve $6x + 5 \equiv -7 \pmod{4}$.

We have

$$\begin{aligned}
6x + 5 &\equiv -7 \pmod{4} && \\
2x + 1 &\equiv 1 \pmod{4} && \text{(reduce constants modulo 4)} \\
2x &\equiv 0 \pmod{4} && \text{(subtract 1 from both sides)} \\
x &\equiv 0 \pmod{2} && \text{(divide both sides by 2 — note soln is mod2)} .
\end{aligned}$$

1.1. **Inversion.** Division (except for the cancellation law) in not defined for modular arithmetic per se. However, the essence of division is captured by the notion of *multiplicative inverses*. For example, in the real numbers $\mathbb{R}$, the multiplicative inverse of $x \in \mathbb{R}$ is defined to be the real number x^{-1} such that $xx^{-1} = x^{-1}x = 1$. Division in $\mathbb{R}$ can be viewed as multiplication by inverses, for example, x/y is the same as xy^{-1}.

Multiplicative inverses modulo m are defined analogously.

Definition 1.2. A multiplicative inverse of a modulo m is any integer a^{-1} such that $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$.

Any integer x which satisfies the linear congruence

$$ax \equiv 1 \pmod{m}$$

is an inverse of a modulo m. Note that this linear congruence is soluble if and only if $\gcd(a, m) = 1$, i.e., a has a multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$. Also, if it is soluble, then there are infinitely many solutions; if a^{-1} is an inverse of a, then $a^{-1} + km$ is also an inverse for any $k \in \mathbb{Z}$.

Example 1.3. $7^{-1} \equiv 15 \pmod{26}$, since

$$7 \cdot 15 \equiv 15 \cdot 7 \equiv 105 \equiv 1 \pmod{26} \ .$$

$7^{-1} \pmod{26}$ exists because $\gcd(7, 26) = 1$. $41 = 15 + 26$, $67 = 15 + 2 \cdot 26$, and $-63 = 15 - 3 \cdot 26$ are also inverses. Indeed, $15 + 26k$, $k \in \mathbb{Z}$, are all inverses of 7, since

$$7(15 + 26k) \equiv (15 + 26k)7 \equiv 105 + 26(7k) \equiv 1 \pmod{26} \ .$$

Example 1.4. Compute $D = \left(\begin{smallmatrix} 7 & 9 \\ 3 & 12 \end{smallmatrix}\right)^{-1} \pmod{26}$.

We will use the fact that if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2}$, then

$$A^{-1} = \frac{1}{|A|}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \ .$$

In our case, $A = \left(\begin{smallmatrix} 7 & 9 \\ 3 & 12 \end{smallmatrix}\right)$, $|A| = 57$, and

$$A^{-1} = \frac{1}{57}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix} \ .$$

To verify that this is indeed an inverse (over $\mathbb{R}^{2\times 2}$) we compute

$$A^{-1}A = \frac{1}{57}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} = \frac{1}{57}\begin{pmatrix} 57 & 0 \\ 0 & 57 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ .$$

To compute $A^{-1} \pmod{26}$, we first need to compute $57^{-1} \pmod{26}$. Since $\gcd(57, 26) = 1$, we know it exists, i.e., the linear congruence

$$57x \equiv 5x \equiv 1 \pmod{26} \tag{1}$$

has a solution. To compute 57^{-1}, we can either solve (1) using the extended Euclidean algorithm (which we'll cover later), or, since the modulus 26 is so small, simply find it by trial and error. We compute $57^{-1} \equiv 5^{-1} \equiv 21 \pmod{26}$.

Once we have $57^{-1} \pmod{26}$, the rest of the computation proceeds as follows:

$$\begin{aligned} A^{-1} &\equiv 57^{-1}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix} \pmod{26} \\ &\equiv 21\begin{pmatrix} 12 & 17 \\ 23 & 7 \end{pmatrix} \pmod{26} \\ &\equiv \begin{pmatrix} 252 & 357 \\ 483 & 147 \end{pmatrix} \pmod{26} \\ &\equiv \begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix} \pmod{26} \ . \end{aligned}$$

Verify:

$$A^{-1}A = \begin{pmatrix} 261 & 286 \\ 234 & 261 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26} \ .$$

1.2. **Congruence Classes.** Let $m > 0$ be a modulus. Congruence modulo m is an equivalence relation, partitioning the integers into m distint equivalence classes. Define $[r]$ to be the set of all $a \in \mathbb{Z}$ such that $a \equiv r \pmod{m}$. We call $[r]$ a residue (or equivalence) class modulo m, and we put $\mathbb{Z}_m$ to be the set of all residue classes modulo m. Then $|\mathbb{Z}_m| = m$ and

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

i.e., $[0] = [m] = [2m] = \ldots$

Suppose $a = qm + r$ and $\gcd(r, m) = 1$. Then $\gcd(a, m) = 1$, and we see that if $a \in [r]$ and $\gcd(r, m) = 1$, then $\gcd(a, m) = 1$. Define

$$\mathbb{Z}_m^* = \{[r] \in \mathbb{Z}_m \mid \gcd(r, m) = 1\} \ .$$

We call $\mathbb{Z}_m^*$ a reduced set of residues modulo m.

Define the operation $*$ on $\mathbb{Z}_m^*$ as

$$[r] * [s] = [rs], \quad [r], [s] \in \mathbb{Z}_m^* \ .$$

Given $[r] \in \mathbb{Z}_m^*$, there exists $[s] \in \mathbb{Z}_m^*$ such that $[r] * [s] = [1]$, i.e., $[s]$ is an inverse of $[r]$ in $\mathbb{Z}_m^*$. To find s, solve $rs \equiv 1 \pmod{m}$.

2. Group Theory

Definition 2.1. Let G be any set with an operation $*$ defined on G with the following properties:

(1) if $a, b \in G$, then $a * b \in G$ (closure),
(2) if $a, b, c \in G$, then $(a * b) * c = a * (b * c) = a * b * c$ (associativity),
(3) there exists $e \in G$ such that $\forall a \in G$ we have $e * a = a * e = a$ (e is called an identity element),
(4) $\forall a \in G$, there exists an element a^{-1} such that $a^{-1} * a = a * a^{-1} = e$ (existence of inverses)

G is said to form a *group* under the operation $*$.

If $\forall a, b \in G$ $a * b = b * a$, then G is said to be a *commutative* or *abelian* group.

If G is a group and $|G|$ is infinite, we say that G is an infinite group. For example:

- $\mathbb{Z}$ under $+$
- $\mathbb{Q}$ under $\times$
- $\mathbb{R}^{n \times n}$ under matrix multiplication (not abelian)
- set of points on $y^2 = x^3 + ax + b$ over $\mathbb{Q}$

If $|G|$ is finite and $|G| = k$, we say that G is a group of order k. For example:

- $\mathbb{Z}_m$ under $+$
- $\mathbb{Z}_m^*$ under $\times$
- set of points on $y^2 = x^3 + ax + b$ modulo p prime

We now write ab for $a * b$. Let $a \in G$ (a group). Define $a^n = aaa \ldots a$ (n a's) for $n \in \mathbb{Z}^+$ and $a^0 = e$.

Theorem 2.1. $(a^n)^{-1} = (a^{-1})^n$.

Define $a^{-n} = (a^{-1})^n$, $n \in \mathbb{Z}^+$. We have $a^n a^m = a^{n+m}$, $n, m \in \mathbb{Z}$.

Definition 2.2. If $a \in G$ and k is the least positive integer such that $a^k = e$, then k is the *order* of a in G.

Theorem 2.2. *For any finite group, there always exists a finite order for each $a \in G$.*

Proof. Let G be a finite group and let $a \in G$. Consider the sequence

$$\{a, a^2, a^3, \ldots, a^m, \ldots, a^n, \ldots, a^\infty\} \ .$$

Since we can put $n > |G|$, we must have two elements in the sequence being the same, i.e., $a^m = a^n$ for some n, m with $n > m$ and

$$e = a^m(a^m)^{-1} = a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \ .$$

□

Definition 2.3. If G is a group and $H \subseteq G$, then H is called a *subgroup* of G if H is also a group under the same operation of G.

Theorem 2.3 (Lagrange)**.** *If G is a finite group and H is a subgroup of G, then $|H| \mid |G|$.*

Let G be a finite group and let $a \in G$. Consider $H = \{e, a, a^2, \ldots, a^{k-1}\}$, where k is the order of a. H is a subgroup of $G \longrightarrow k \mid |G|$.

The trivial subgroups of a group G are G and $\{e\}$.

Definition 2.4. A group like $H = \{e, a, a^2, \ldots, a^{k-1}\}$ is called a *cyclic group* if there exists some $g \in H$ such that for every $a \in H$, $a = g^i$ $(i \in \mathbb{Z})$. We denote this group by $< g >$.

3. Field Theory

Definition 3.1. Let F be any set with operations $+$ and $\times$ defined on F satisfying the following properties:

(1) F is an abelian group with respect to $+$
(2) $F - \{0\}$ (0 is the additive identity) is an abelian group with respect to $\times$
(3) $+$ and $\times$ are distributive in R, i.e.,

$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc \quad \forall a, b, c \in R \ .$$

F is said to form a *field* under $+$ and $\times$.

Example 3.1. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields — $\mathbb{Z}$ is not a field.

$\mathbb{Z}_p$ is a field under (modular) addition and multiplication if p is prime. This field is denoted by $\mathbb{F}_p$ or $GF(p)$ (Galois field).

Let $\mathbb{F}$ be any field. Then $\{0, 1\} \subseteq \mathbb{F}$ where 0 denotes the additive identity element and 1 denotes the multiplicative identity. Denote for $a \in \mathbb{Z}^+$:

$$\dot{a} = \sum_{i=1}^{a} 1 \in \mathbb{F} \ .$$

There are two possible cases:

(1) $\dot{a} \neq 0$ for any $a \in \mathbb{Z}^+$,
(2) there exists a minimal $m \in \mathbb{Z}^+$ such that $\dot{m} = 0$.

Definition 3.2. A field having Property 1 is said to be a field of characteristic 0. A field having Property 2 is said to be a field of characteristic m.

Example 3.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields of characteristic 0 and $\mathbb{F}_p$ is a field of characteristic p.

Definition 3.3. Let $\mathbb{F}_1$ and $\mathbb{F}_2$ be fields and suppose we have a mapping $\Theta : \mathbb{F}_1 \mapsto \mathbb{F}_2$ such that:

(1) Θ is onto,
(2) Θ is one-to-one,
(3) $\Theta(x + y) = \Theta(x) + \Theta(y)$,
(4) $\Theta(xy) = \Theta(x)\Theta(y)$

We say that $\mathbb{F}_1$ and $\mathbb{F}_2$ are *isomorphic*.

Theorem 3.1. *Any field of characteristic* 0 *has a subfield isomorphic to* $\mathbb{Q}$.

Corollary 3.2. *If* $\mathbb{F}$ *is a field of characteristic* 0, *then* $\mathbb{F}$ *is an infinite field.*

Notice that any finite field must have non-zero characteristic.

Theorem 3.3. *Let* $\mathbb{F}$ *be any field of characteristic* m. *Then* m *must be prime.*

Theorem 3.4. *Any field of characteristic* p *contains a subfield isomorphic to* $\mathbb{F}_p$.

Theorem 3.5. *If* $\mathbb{F}$ *is a finite field of characteristic* p, *then* $|F| = p^n$ *for some* $n \in \mathbb{Z}^+$.

Theorem 3.6. *If* $\mathbb{F}_1$ *and* $\mathbb{F}_2$ *are finite fields and* $|\mathbb{F}_1| = |\mathbb{F}_2|$, *then* $\mathbb{F}_1 \cong \mathbb{F}_2$.

The finite field with p^n elements is denoted by $\mathbb{F}_{p^n}$ or $\mathbb{F}_q$, where $q = p^n$. Although all finite fields of the same order are isomorphic, there may be several different *representations*, some of which may be more attractive computationally than others.

3.1. **Finite Fields.** Finite fields of order p and 2^n are important in cryptography. For example:

- a number of public-key systems are set in the multiplicative group of $\mathbb{F}_p$ (denoted by $\mathbb{F}_p^*$),
- elliptic curves in cryptography are typically defined over $\mathbb{F}_p$ or $\mathbb{F}_{2^n}$,
- Rijndael uses arithmetic in $\mathbb{F}_{2^8}$ for its non-linear substitutions.

Arithmetic in $\mathbb{F}_p$ is simply integer arithmetic modulo p. Unfortunately, performing integer arithmetic modulo p^n does not yield a field (why?). In general, to construct a finite field of order p^n :

- Find a polynomial $m(x)$ over $\mathbb{F}_p$ which is irreducible and of degree n.
- The residue classes of polynomials in $\mathbb{F}_p[x]$ (polynomials with coefficients in $\mathbb{F}_p$) modulo $m(x)$ form a finite field under polynomial addition and polynomial multiplication.

Thus:

- The elements of $\mathbb{F}_{p^n}$ can be represented by polynomials with coefficients in $\mathbb{F}_p$ of degree $< n$.
- Addition is addition of polynomials (coefficient arithmetic modulo p).
- Multiplication is multiplication of polynomials modulo $m(x)$ (coefficient arithmetic modulo p).

Example 3.3. Rijndael uses arithmetic in $\mathbb{F}_{2^8}$ with $m(x) = x^8 + x^4 + x^3 + x + 1$. Notice that an element $f \in \mathbb{F}_{2^8}$ has the form

$$f = a_7x^7 + a_6x^6 + \cdots + a_1x + a_0, \quad a_i \in \mathbb{F}_2$$

and thus every 8-bit byte can be identified with a unique field element.

Let $f = x^6 + x^4 + x^2 + x + 1$ and $g = x^7 + x + 1$. Then

$$\begin{aligned} f + g &= (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) \\ &= x^7 + x^6 + x^4 + x^2 \\ fg &= (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod m(x) \\ &= x^7 + x^6 + 1 \end{aligned}$$

Notice that addition in $\mathbb{F}_{2^n}$ is simply bitwise XOR. To compute the multiplicative inverse of $f(x) \in \mathbb{F}_{2^n}$, compute $g(x)$ such that $f(x)g(x) \equiv 1 \pmod{m(x)}$, using the Extended Euclidean Algorithm for polynomials.