Elementary Algebra

bowen

December 21, 2025

Contents

1 Mod n Class

1. Finite Field and Finite Group
(a) Consider $(\mathbb{Z}/n\mathbb{Z})$,
when n is prime p, $\mathbb{Z}/p\mathbb{Z}$ forms a finite group, with characteristic p and
$|\mathbb{Z}/p\mathbb{Z}| = p$, which are $[0], ...[p-1] \in \mathbb{Z}/p\mathbb{Z}$
when n is composite, $\mathbb{Z}/n\mathbb{Z}$ forms a finite ring

(b) For $(\mathbb{Z}/n\mathbb{Z})$ field,

(i) We can consider when does $ax \equiv b \pmod{n}$ has solution?
i.e. when does a have an multiplicative inverse on mod n field.

By **Bezout's Lemma** (if $(a, n) \mid b$, then $ax + kn = b$ has integer solution),
if $(a, n) = 1$, a is invertible (a^{-1} exists), then $x \equiv a^{-1}b \pmod{n}$
We may wonder what a^{-1} is, by bezout, there exists s,t such that $as + nt = 1$, then

$$a^{-1} \equiv s \pmod{n}$$

(ii) To Understand under groups, if $(a, n) = 1$, then $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then a has multiplicative inverse.

2. Orders and Primitive Roots

(1) (Orders Modulo a Prime) Given a prime p, the order of an integer a modulo p with $p \nmid a$ is the smallest positive k such that

$$a^k \equiv 1 \pmod{p}$$

We say $ord_p(a) = k$
We might ask whether such order always exists, which is obvious that such order always exists by Fermat's Little Theorem (if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$),
and we get $ord_p(a) < p$ for free

(2) If p is prime and a is integer with $p \nmid a$, we have

$$a^n \equiv 1 \pmod{1} \iff ord_p(a) \mid n$$

An example to illustrate the power of Orders
Find natural solutions such that $n \mid 2^n - 1$

$n = 1$ is trivial, then we can claim $n > 1$
We first observe that n and $2^n - 1$ are odds
Let p be the smallest prime such that $p \mid n$, then we have

$$2^n \equiv 1 \pmod{p}$$

and $2^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem
By the theorem above, we have

$$ord_p(2) \mid n \text{ and } ord_p(2) \mid p-1$$

Since $(2, p) = 1$, $ord_p(2)$ must exists.
Since we took p to be the smallest prime that divides n, we observe that only 1 divides n and $p - 1$, hence

$$ord_p(2) = 1$$

which implies $2^1 \equiv 1 \pmod{p}$, which is impossible.

(3) (General Orders) Given $(a, n) = 1$, with $n > 0$, $ord_n(a)$ is the smallest positive k such that $a^k \equiv 1 \pmod{n}$

(4) (Primitive Roots) Given positive n. If $ord_n(g) = \phi(n)$, then g is a primitive root modulo n. (For a prime p, $\phi(p) = p - 1$)
To see when such roots exist is extremely hard
A primitive root exists modulo n iff $n = 1, 2, 4$ or if n is in the form p^k or $2p^k$ for some positive integer k and odd prime p.

(5) We say g is a primitive root a modulo p, the set $\{a^1, ..., a^{p-1}\}$ where all a^i are different mod p.

(6) (Sum of Powers Modulo n) Let p be a prime and x be a positive integer. Find all residues the sum $\sum_{i=1}^{p-1} i^x$ can give when divided by p.

Case 1: $p - 1 \mid x$, then $x = k(p-1)$ for some k, by Fermat's Little Theorem,

$$\sum_{i=1}^{p-1} i^x = \sum_{i=1}^{p-1} i^{k(p-1)} \equiv \sum_{i=1}^{p-1} i^k \pmod p = p - 1$$

Case 2: $p - 1 \nmid x$, then let g be the primitive root modulo p. We can rewrite the given sum as

$$\sum_{i=1}^{p-1} i^x = \sum_{i=1}^{p-1} g^{ix} \pmod p$$

Then by the sum of geometric seq, we have

$$\sum_{i=1}^{p-1} i^x = g^x \cdot \frac{g^{(p-1)x} - 1}{g^x - 1} = g^x \cdot \frac{g^{x^{p-1}} - 1}{g^x - 1} = g^x \cdot \frac{1 - 1}{g^x - 1} \pmod p$$

which gives 0. We remains to eliminate $g^x - 1 \equiv 0 \pmod p$, which is obvious since g is a primitive root and $p - 1 \nmid x$
Therefore the only residues are 0 and $p - 1$ divided by p.

3. Basic Groups

- Multiplicative Group (U_n)
In particular, we are interested in Multiplicative group over integer modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times = \{a : 1 \leq a \leq n \ s.t. \ (a, n) = 1\}$
By the definition, it's not hard to find out

$$|(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$$

where $\phi(n) = n \cdot \Pi_{p|n}(1 - \frac{1}{p})$ is the Euler Totient Function, which counts the number of relative primes to n.
To see why it holds, we can apply inclusion-exclusion on the set $\{1, 2, ..., n\}$.

Notice that,
(1) $|\mathbb{Z}/p\mathbb{Z}| = p - 1$
(2) If $(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$
(3) If p is prime, $k \geq 1$, then

$$\phi(p^k) = p^k \cdot (1 - \frac{1}{p})$$

- Symmetric Group (S_n)
A mapping $\pi : \{1, ..., n\} \to \{1, ..., n\}$ defined as $\pi(i) = j$
The Following are subgroups of S_n, it's clear that $|S_n| = n!$ by multiplication rule.
Notice for composition $\pi_1 o \pi_2$, we compute from right to left.

- Cyclic Group (C_n)
  C_n can be visualized as arranging n elements on the vertices of n-polygons with rotation.
  If we take n = 4 as an example,
  (1) The identity map e is indeed one of the permutation, which gives e
  (2) If we send $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1$, which gives (1234)
  (3) If we send $1 \rightarrow 3 \rightarrow 1$and $2 \rightarrow 4 \rightarrow 2$, which gives (13)(24)
  (4) If we send $1 \rightarrow 4 \rightarrow 3 \rightarrow 2$, which gives (1432)
  Hence, $C_n = \{e, (1234), (13)(24), (1432)\}$
  And not hard to find out
  $$|C_n| = n$$
- Alternating Group (A_n)
  A_n consists of even permutations in S_n, which means it collects those operations with even numebr of ()
  Observe that $|A_n| = \frac{n!}{2}$
- Dihedral Group (D_n)
  D_n denotes the group of rotation and reflection symmetries on n-side polygons.
  observe that C_n is a subgroup of D_n, where D_n has extra n reflection symmetries.
  Hence $|D_n| = 2n$, n rotation symmetries and n reflection symmetries.

2 Theorems Recap

1. **Bertrand's Postulate**: For every integer $n > 1$, there exists a prime p such that $n < p < 2n$.
We can use the distribution of primes to argue $\sum_k \frac{1}{k}$ is never an integer.

2. **Lagrange's Theorem**: If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

3. **Euler's Theorem**: If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.
"We can understand Euler's Theorem as applying Lagrange theorem to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$"

   On the $(\mathbb{Z}/n\mathbb{Z})^{\times}$ multiplicative group of n, we define the order of a modulo n as

$$ord_n(a) = \min\{k > 0 : a^k \equiv 1 \pmod{n}\}$$

   Moreover, we can consider the subgroup $< a >$ of $(\mathbb{Z}/n\mathbb{Z})^{\times}$, where $< a >$ is the cyclic group generated by a.
If we take a closer look at $< a >= \{1, a, a^2, ..., a^{ord_n(a)-1}\}$, it's clear that $| < a > | = ord_n(a)$.
i.e. sometimes $ord_n(a)$ denotes as the smallest period of the cyclic group generated by a
This motivates the induction step for 1991-USAMO-q3.

   Then by Lagrange, we have

$$ord_n(a) \,|\, |(\mathbb{Z}/n\mathbb{Z})^{\times}| = \phi(n)$$

   i.e. $\phi(n) = kn$ for some integer k
Then we have

$$a^{\phi(n)} \equiv a^{k \cdot ord_n(a)} \equiv (a^{ord_n(a)})^k \equiv 1^k \equiv 1 \pmod{n}$$

4. **Fermat's Little Theorem**:
(General Form) For integer a and prime p, $a^p \equiv a \pmod{p}$
(For p is prime and $(a, p) = 1$) $a^{p-1} \equiv 1 \pmod{p}$.

   for the particular case when $(a, p) = 1$, it gurantees that a has a multiplicative inverse on mod p field.
Hence, we can multiply a^{-1} on both sides of $\equiv$ not changing the congruence.

   which shows that Fermat's Little Theorem is an immediate consequence of Euler's Totient Theorem, since $\phi(p) = p - 1$.

5. **Chinese Remainder Theorem**: If $n_1, n_2, \ldots, n_k$ are pairwise coprime integers,
denote $n = n_1 \cdot n_2 \ldots n_k$ then the system
$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
$\ldots$
$x \equiv a_k \pmod{n_k}$
has a solution and any two solutions x_1, x_2 satisfies that

$$x_1 \equiv x_2 \pmod{n}$$

   Equivalently, we can rewrite via groups, which is if $n = \Pi_1^k n_i$ with $(n_i, n_j) = 1$ for all $i \neq j$, then

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq (\mathbb{Z}/n_1\mathbb{Z})^{\times} \times (\mathbb{Z}/n_2\mathbb{Z})^{\times} \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^{\times}$$

   If $(a, n) = 1$, we can easily observe the isomorphism which is

$$a \pmod{n} \mapsto (a \pmod{n}_1, \ldots, a \pmod{n}_k)$$

   In fact, we can try to understand Euler's Totient Theorem via CRT.
Let $n = p_1^{k_1} \cdot \cdots \cdot p_r^{k_r}$
For each i, we have $a^{\phi(p_i^{k_i})} \equiv 1 \pmod()p_i^{k_i})$, then we have a "global" Euler formula.

6. **Lifting-The-Exponent Lemma (LTE)**: For odd prime p, if $p \mid x - y$ and $p \nmid xy$, then $\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$.

   $v_p(a)$ denotes number of p occurs in the prime factorization of a.
   i.e. Largest n such that $p^n \mid a$, by convention we denote $v_p(0) = \infty$

   It's useful when we are trying to consider the following questions related to diophantines:
   (1) For which power k, we have $p^k \mid x^n - y^n$
   (2) WTS a number is not square-free or a perfect power
   (3) Find the largest or smallest solution to diophantines if exists.

   Basic Facts:
   (1) $v_p(a \cdot b) = v_p(a) + v_p(b)$
   (2) $v_p(a + b) \geq min\{v_p(a), v_p(b)\}$
   (3) $v_p(a) \leq log_p(|a|)$ for $a \neq 0$

   Motivation Problem does $11^n - 1$ divisible by 10
   We can convert the problem to what does $v_p(x^n - y^n)$ look like if $p \mid x - y$
   Observe that $x^n - y^n = (x - y) \cdot (x^{n-1} + \cdots + xy^{n-2} + y^{n-1})$
   Using the above property we obtain,

   $$v_p(x^n - y^n) = v_p(x - y) + v_p((x^{n-1} + \cdots + xy^{n-2} + y^{n-1}))$$

   But the $v_p(x - y)$ is independent of n, then we have to focus on the second term.

7. **Orbit-Stabilizer Theorem**: If a finite group G acts on a set X, then for any $x \in X$, $|G| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$.

8. **Cauchy's Theorem**: If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p.

9. **Burnside's Lemma**: If a finite group G acts on a set X, then the number of orbits is $\frac{1}{|G|}\sum_{c \in G} |X^c|$, where X^c is the set of elements fixed by c.

10. **Sylow Theorems**:
    - For a finite group G of order $p^a m$ where $p \nmid m$, there exists a Sylow p-subgroup of order p^a.
    - All Sylow p-subgroups are conjugate.
    - The number n_p of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.

11. **Wilson's Theorem**: A positive integer $p > 1$ is prime if and only if $(p - 1)! \equiv -1 \pmod{p}$.

3 Diophantines

1. Tactics

4 Order and Premitive Roots

1. Order of an integer a modulo p is the smallest integer d such that $a^d \equiv 1 \pmod{p}$ denote as $ord_p(a) = d$

2. (Fundamental Theorem of Order)

   Theorem 4.1. *If p not divides a, then*

   $$a^n \equiv 1 \pmod{p} \iff ord_p(a)|n$$