# 1 Fri 8/28

## Diophantine Equation

Solving Diophantine equations: integer solutions to $ax + by = c$ for $a, b, c \in \mathbb{Z}$. Steps:

(1) Solve for $ax + by = \gcd(x, y)$ by using the Euclid's algorithm and back substitution.

(2) If $\gcd(x, y) \mid c$ then we can find solutions. Otherwise no integer solution.

**Theorem 1**

$\mathcal{S} = \{ax + by \mid a, b \in \mathbb{Z}\}$ is the set of all multiples of $\gcd(x, y)$. (The $\mathbb{Z}$-combination of $x$ and $y$ can only produce multiples of $\gcd(x, y)$.

**Proof**

Since $x, y$ are both multiples of $\gcd(x, y)$, the $\mathbb{Z}$-combination of them must also be the multiple of $\gcd(x, y)$. For the other direction, see (3). □

(3) Suppose the solution for $ax + by = \gcd(x, y)$ is $a_0x + b_0y = \gcd(x, y)$. Also suppose that $\gcd(x, y) \mid c$ and $c/\gcd(x, y) = k$. Then

$$(ka_0)x + (kb_0)y = k\gcd(x, y) = c,$$

a particular solution to $ax + by = c$.

(4) Euclid's lemma:

**Lemma 1.1**

Suppose $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

**Proof**

Since $\gcd(a, b) = 1$, then there exist $x, y$ such that $ax + by = 1$. Then

$$cax + cby = c.$$

Since $a \mid cax$ and $a \mid cby$ (from $a \mid bc$) it follows that $a \mid c$. □

Therefore the set of complete solution is

$$\mathcal{S} = \left\{ \left( (ka_0) + \frac{ny}{\gcd(x,y)}, (kb_0) - \frac{nx}{\gcd(x,y)} \right) \right\}$$

**Proof**

Let $\mathcal{S}'$ be the set of solutions. To show $\mathcal{S}' = \mathcal{S}$ we need to show $\mathcal{S} \subset \mathcal{S}'$ and $\mathcal{S} \supset \mathcal{S}'$.

Showing $\mathcal{S} \subset \mathcal{S}'$ :

$$\left( (ka_0) + \frac{ny}{\gcd(x,y)} \right) x + \left( (kb_0) - \frac{nx}{\gcd(x,y)} \right) y = (ka_0)x + (kb_0)y = c.$$

Now we show $\mathcal{S}' \supset \mathcal{S}$: let $(ka, kb)$ be a solution, therefore $kax + kby = c$. Subtracting it from $(ka_0)x + (kb_0)y = c$, we have

$$k(a - a_0)x = k(b_0 - b)y \quad \text{or} \quad (a - a_0)\frac{x}{\gcd(x,y)} = (b_0 - b)\frac{y}{\gcd(x,y)}.$$

Since $x/\gcd(x,y)$ $y/\gcd(x,y)$ are co-prime (!!), by Euclid's lemma we know

$$(a - a_0) = n\left(\frac{y}{\gcd(x,y)}\right) \text{ and } (b_0 - b) = n\left(\frac{x}{\gcd(x,y)}\right) \text{ for some } n \in \mathbb{Z}.$$

Therefore $\mathcal{S} = \mathcal{S}'$. □

## 2 Mon 8/31 Congruences

(1) We declare 2 numbers to be congruent $\pmod n$ if $a - b$ is some multiple of $n$.

**Lemma 2.1**

If $a \equiv b \pmod n$ then $a, b$ have the same remainder when divided by $n$.

**Proof**

by division algorithm, $a = nq_1 + r_1$ and $b = nq_2 + r_2$ for some $r_1, r_2, a_1, a_2$ with $r_1, r_2 \in [0, n)$. WLOG assume $r_1 \geqslant r_2$.

Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$.

We claim $r_1 - r_2$ is the remainder when you divide $a - b$ by $n$. To see this, notice that since $r_1 < n$ and $r_1 \geqslant r_2$, we have $0 \leqslant r_1 - r_2 < n$.

Since we have assumed that $a \equiv b \pmod{n}$, it follows that $a - b$ has remainder 0 when divided by $n$. Therefore $r_1 - r_2 = 0$, i.e., $r_1 - r_2$. □

(2) Imagine that we were coloring the number line by coloring all the numbers with same remainder the same color. If we color the number line by remainders of 4, then we partition $\mathbb{Z}$ into four disjoint subsets:

$$\mathbb{Z} = \{x \in \mathbb{Z} \mid x = 4k\} \underbrace{\sqcup}_{\text{disjoint union}} \{x \in \mathbb{Z} \mid x = 4k+1\} \sqcup \{x \in \mathbb{Z} \mid x = 4k+2\} \sqcup \{x \in \mathbb{Z} \mid x = 4k+3\}$$

(3) From now on, we label elements leaving the same remainder $r$ as $[r]$ (or $[r]_n$).

(4) If $a \equiv b \pmod{n}$ we can write $[a]_n = [b]_n$ or simply $[a] = [b]$.

(5) $\equiv$ is a relation. More specifically, an **equivalence relation**. Assuming $\pmod{n}$ :

   (1) Reflexive: $a \equiv a \forall a \in \mathbb{Z}$.

   (2) Symmetric: if $a \equiv b$ then $b \equiv a$.

   (3) Transitive: if $a \equiv b$ and $b \equiv c$ then $a \equiv c$.

   Relations like $>, \geqslant$ are not equivalence relations.

(6) **Summary**: partition of $\mathbb{Z}$ by congruence.

**Problem breakout room problem**

(1) Show that $\gcd(n, n+1) = 1$

(2) Show that $\gcd(2a - 3b, 4a - 5b) | b$

(3) Show that $\gcd(a, b) = 1 \implies \gcd(a + b, ab) = 1$

(4) Show that $4 \mid$ product of 4 consecutive integers.

(5) Generalize (4) to $n$.

## 3 Wed 9/2 On problems

**Solution**

(1) If $x \mid \gcd(n, n+1)$ then $x \mid n$ and $x \mid n+1$. It follows that $x \mid (n+1)-1 \implies x \mid 1$. Therefore $x = 1$ is the only divisor of $\gcd(n, n+1)$. Hence $\gcd(n, n+1) = 1$.

(2) It follows that if $x = \gcd(2a-3b, 4a-5b)$, then $x \mid 2a-3b$ and $x \mid 4a-5b$ then $x \mid 2(2a-3b)-(4a-5b) \implies x \mid -b \implies x \mid b$. Hence proven.

(3) Suppose some prime $p$ satisfy $p \mid ab$ and $p|a+b$. Then either $p \mid a$ or $p \mid b$. WLOG assume $p \mid a$. Now look at $a+b$. Since $p \mid a+b$ and $p \mid a$, it follows that $p \mid (a+b)-a \implies p \mid b$. Then this contradicts $\gcd(a,b)$ being 1. Hence there does not exist any $p$ satisfying $p \mid ab$ and $p \mid a+b$. Therefore $\gcd(a+b, ab) = 1$.

(4) One of the four consecutive numbers has to be a multiple of 4. Suppose we have $n, n+1, n+2, n+3$ and none of them is a multiple of 4. By pigeonhole principle, since all other possible remainders are $1, 2$, and 3, two of these numbers have to have the same remainder. However they cannot, because their difference is greater than 0 but less than 4. Therefore one of these four numbers *must* be a multiple of 4. Therefore their product is a multiple of 4.

(5) Likewise, one of the $n$ consecutive numbers has to be a multiple of $n$. Therefore their product has to be a multiple of $n$.

(6) For the proof that $p \mid ab \implies p \mid a \vee p \mid b$ : Suppose $p \mid ab$ but $\gcd(a,p) = \gcd(b,p) = 1$. Then by Euclid's algorithm and Bezout's identity we have integers $x, y, z, w$ such that

$$xp + ya = 1 \text{ and } zp + wb = 1$$

Multiplying the two equations we have

$$(xp+ya)(zp+wb) = 1 \implies xpzp + xpwb + yazp + yawb = 1 \implies p(xpz + xwb + yaz) + ab(yw) = 1$$

from which we conclude that $\gcd(p, ab) = 1$. Therefore $p \nmid ab$. Contradiction.

# 4 Fri 9/4

Addition, subtraction, multiplication, and scaling also work in modulo $n$.

**Example 4.1**

$$\begin{cases} 13 \equiv 9 \pmod 4 \\ 4 \equiv 16 \pmod 4 \end{cases} \implies \begin{cases} (13+4) \equiv (9+16) \pmod 4 \\ (13 \cdot 4) \equiv (9 \cdot 16) \pmod 4 \\ 13k \equiv 9k \pmod 4 \text{ for all } k \in \mathbb{Z} \end{cases}$$

Suppose we are in $\mathbb{Z}/4\mathbb{Z}$ (mod 4 world) in which $\mathbb{Z}$ is partitioned into $[0], [1], [2], [3]$. Then if $x_1, x_2 \in [x], y_1, y_2 \in [y]$, we have

$$\begin{cases} x_1 \equiv x_2 \equiv x \pmod 4 \\ y_1 \equiv y_2 \equiv x \pmod 4 \end{cases} \implies (x_1 + y_1) \equiv (x_2 + y_2) \equiv x + y \pmod 4$$

And now we can construct the addition for $\mathbb{Z}/4\mathbb{Z}$ :

| + (mod 4) | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

and multiplication table for $\mathbb{Z}/4\mathbb{Z}$ :

| × (mod 4) | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [0] |
| [3] | [0] | [3] | [2] | [1] |

Multiplication: $[3^n] = [(-1)^n]$ in $\mathbb{Z}/4\mathbb{Z}$. Therefore it can either be 1 or $-1$, depending on whether the exponent is even or odd.

Now for division: we begin by trying to solve the equation $ax \equiv b \pmod n$. Let's solve $3x \equiv 1 \pmod 4$, namely $[3][x] = [1]$ in $\mathbb{Z}/4\mathbb{Z}$. From the multiplication table we see that $x = [3]$, or $x \equiv 3 \pmod 4$, is the only possible solution.

On the other hand, $2x \equiv 1 \pmod 4$ or $[2][x] = [1]$ in $\mathbb{Z}/4\mathbb{Z}$ has no solution. Therefore $[1]/[3]$ is meaningful in $\mathbb{Z}/4\mathbb{Z}$ but $[1]/[2]$ isn't.

**Problem 2**

When can we solve $ax = b \pmod{n}$, i.e., when does $[b]/[a]$ make sense in $\mathbb{Z}/n\mathbb{Z}$?

**Solution**

I claim that this does not have a solution when $\gcd(a, n) \nmid b$.

# 5 Wed 9/9 Solving Linear Congruences

**Example 5.1**

Solve the linear congruence $3x \equiv 5 \pmod{7}$.

**Solution**

By brute force since $|\mathbb{Z}/7\mathbb{Z}| = 7$ isn't very large: $3 \cdot 4 = 12 \equiv 5 \pmod{5}$.

Better way: there exists $y$ such that $3x + 7y = 5$. All that remains is applying Euclid's algorithm. First solve $3x + 7y = \gcd(3, 7) = 1$ then multiply the solution by 5 and we get what we want. Add multiples of 7 to $x$ when needed (e.g. to make sure $0 \leqslant x \leqslant 6$).

**Problem 3**

Solve $3x \equiv 5 \pmod{18}$.

**Solution**

If this linear congruence had a solution the there exists integer $y$ satisfying $3x+18y = 5$. Since $\gcd(3, 18) \nmid 5$ this congruence has no solution.

Back to the question: when does $ax \equiv b \pmod{k}$ has a unique solution?

To have a solution, we first need to meet the requirement that $\gcd(a, k) \mid b$.

Now for the uniqueness. Suppose $ax_0 \equiv ax_1 \equiv b \pmod{k}$ with $x_0 \geqslant x_1$, then $ax_0 - ax_1 \equiv 0 \pmod{k}$. This means that $k \mid a(x_0 - x_1)$. Since $(k-1) \geqslant x_0 - x_1 \geqslant 0$, it follows that if $\gcd(a,k) = 1$ then the only solution to $k \mid a(x_0 - x_1)$ is when $x_0 = x_1$ and $k \mid 0$ (because if $k \mid a(x_0 - x_1)$ and $\gcd(a,k) = 1$ then by Euclid's lemma $k \mid (x_0 - x_1)$, the only possibility to which is if $x_0 = x_1$). Since 1 divides any integer, the first requirement is no longer necessary. Therefore, we have the following theorem:

**Theorem 2**

The linear congruence $ax \equiv b \pmod{k}$ has a unique solution if and only if $\gcd(a,k) = 1$.

## 6 Fri 9/11 Chinese Remainder Theorem

**Problem 4**

An abstract example first (an example follows): suppose $x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, x \equiv a_3 \pmod{n_3}$ and $n_1, n_2, n_3$ are *pairwise* coprime. Find $x$.

**Solution**

If we define

$$\begin{cases} N_1 = \dfrac{n_1 n_2 n_3}{n_1} = n_2 n_3 \\ N_2 = \dfrac{n_1 n_2 n_3}{n_2} = n_1 n_3 \\ N_3 = \dfrac{n_1 n_2 n_3}{n_3} = n_1 n_2 \end{cases} \quad \text{then we have to solve} \begin{cases} N_1 x_1 \equiv 1 \pmod{n_1} \\ N_2 x_2 \equiv 1 \pmod{n_2} \\ N_3 x_3 \equiv 1 \pmod{n_3} \end{cases}$$

Then we have

$$\begin{cases} a_1 N_1 x_1 \equiv a_1 \pmod{n_1} \\ a_2 N_2 x_2 \equiv a_2 \pmod{n_2} \\ a_3 N_3 x_3 \equiv a_3 \pmod{n_3} \end{cases} \implies x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \pm k \cdot \operatorname{lcm}(n_1 n_2, n_3)$$

**Example 6.1**

Solve the system of linear congruences

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

**Solution**

First verify that $3, 5, 7$ are *pairwise* coprime. Then

$$\begin{cases} N_1 = 5 \cdot 7 = 35 \\ N_2 = 3 \cdot 7 = 21 \\ N_3 = 3 \cdot 5 = 15 \end{cases}$$

and we want to find multiples of the $N$'s $(N_1x_1, N_2x_2, N_3x_3)$ satisfying

$$\begin{cases} 35x_1 \equiv 1 \pmod 3 \\ 21x_2 \equiv 1 \pmod 5 \\ 15x_3 \equiv 1 \pmod 7 \end{cases} \implies \begin{cases} 35 \cdot 2 = [2] \cdot [2] = [1] \text{ in } \mathbb{Z}/3\mathbb{Z} \\ 21 \cdot 1 = [1] \cdot [1] = [1] \text{ in } \mathbb{Z}/5\mathbb{Z} \\ 15 \cdot 1 = [1] \cdot [1] = [1] \text{ in } \mathbb{Z}/7\mathbb{Z} \end{cases} \implies \begin{cases} x_1 = 2 \\ x_2 = 1 \\ x_3 = 1 \end{cases}$$

So one solution to the system is $x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = 2(70) + 3(21) + 2(15) = 233$, and the complete solution is $\{x \in \mathbb{Z} \mid x \equiv 233 \pmod{\operatorname{lcm}(2,3,5)}\} \implies \{x \in \mathbb{Z} \mid x \equiv 23 \pmod{30}\}$.

**Remark**

In a system of two linear congruences, for example $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$ :

$$\begin{cases} N_1 = 5 \\ N_2 = 3 \end{cases} \implies \text{solve} \begin{cases} N_1x_1 = 5x_1 \equiv 1 \pmod 3 \\ N_2x_2 = 3x_2 \equiv 1 \pmod 5 \end{cases} \implies x = a_1N_1x_1 + a_2N_2x_2 = 2(5)x_1 + 3(3)x_2 = 38.$$

Whereas the old method uses Euclid's algorithm and solves $3u + 5v = \gcd(3,5) = 1$. Reducing this equation modulo 3 gives $5v \equiv 1 \pmod 3$ and reducing this equation modulo 5 gives $3u \equiv 1 \pmod 5$. In this case $v$ and $u$ are precisely $x_1$ and $x_2$. Why does this work?

**Proof**

Suppose $x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$. Then we have

$$\begin{cases} x \equiv a_1 \pmod{a_1} \\ x \equiv a_2 \pmod{a_2} \\ x \equiv a_3 \pmod{a_3} \end{cases} \text{and} \begin{cases} N_1 = n_2n_3 \\ N_2 = n_1n_3 \\ N_3 = n_1n_2 \end{cases} \text{and } N_ix_i \equiv 1 \pmod{n_i}.$$

If we reduce the equation modulo $n_1$ we have $x \equiv aN_1x_1 + 0 + 0 \pmod{n_1}$ since $n_1 \mid N_2$ and $n_1 \mid N_3$. Likewise for the other two $n$'s. □

## 7 Wed 9/16

**Theorem 3**

If $ca \equiv cb \pmod N$ then $a \equiv b \pmod{(N/\gcd(c,N))}$.

**Proof**

Let $d = \gcd(c,N)$. Then $c = c'd$ and $N = N'd$ for some $c', N' \in \mathbb{Z}$. Since $d$ is the GCD, we know $\gcd(c',N') = 1$.

Now we are given $ca \equiv cb \pmod N$ which implies $N \mid ca - cb$. Hence $N'd \mid c'd(a-b)$. Cancelling $d$ gives $N' \mid c'(a-b)$. Since $N'$ and $c'$ are coprime, by Euclid's lemma we have $N' \mid a - b$. QED. □

---

**Definition 4**

The addition ⊕ and multiplication ⊗ in $\mathbb{Z}/n\mathbb{Z}$ can be interpreted as functions from $\{0,1,\ldots,n\} \times \{0,1,\ldots,n\}$ onto $\{0,1,\ldots,n\}$, namely $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Addition ⊕ is defined by $(i,j) \mapsto i + j \pmod n$ and multiplication ⊗ is defined by $(i,j) \mapsto ij \pmod n$.

**Remark**

(1) Addition and multiplication are commutative.

(2) Addition has identity $[0]$ and multiplication has identity $[1]$.

(3) In addition, $[x]$ has additive inverse $[-x] = [n-x]$.

(4) An element $[x]$ may or may not have multiplicative inverse. No multiplicative inverse if $\gcd(x,n) \neq 1$.

(5) Addition and multiplication are associative.

## 8 Fri 9/18

**Definition 5**

A **group** $(G,\cdot)$ is a set $G$ with a binary (closed) operation $\cdot : G \times G \to G$ such that

(1) Associativity: $\cdot$ is associative: $g \cdot (h \cdot i) = (g \cdot h) \cdot i$,

(2) Identity: there exists an identity $e \in G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$.

(3) Inverse: given any $g \in G$, there exists $g'$ such that $g \cdot g' = g' \cdot g = e$.

**Example 8.1**

Some basic examples of groups and non-groups:

(1) $(\mathbb{Z},+)$ is a group with $e = 0$ and inverse $-x$.

(2) Though $(\mathbb{Z}_{\text{odd}},+)$ satisfies all three operations, it makes no sense to treat this as a group because $+$ is not a binary operation on the set of odd numbers.

(3) $(\mathbb{Z}_{\text{even}},+)$ is a group.

(4) $(\mathbb{Z}^+,+)$ is not a group because it has no inverse.

(5) $(\mathbb{Z},\times)$ is not a group because almost all elements don't have inverse.

(6) $(\mathbb{Q} \setminus \{0\},\times)$ is a group.

(7) $(\mathbb{Z}/n\mathbb{Z},\oplus)$ with $\oplus$ defined by addition mod $n$, is a group: $[0]$ as inverse and $[n-x]$ being inverse..

(8) More abstract examples of groups:

(I) Transformation of $\mathbb{R}^2$ : set of all rotations (about origin) with composition as the binary operation. Intuitive to verify. We can define a mapping $\mathbb{R} \to \mathbb{Z}/[0,360)$ by

$$\text{Rotation of } \theta \text{ degrees} \mapsto \theta \quad \text{“(mod 360 )”}$$

and if we restrict the degrees to integers then we can define $f$ : set of rotations → $\mathbb{Z}/360\mathbb{Z}$

$$a \oplus b \mapsto a + b \pmod{360}$$

(II) $(\mathcal{S}, \text{composition})$ where $\mathcal{S}$ is the set of all bijective functions from $\{1, 2, \ldots, n\}$ onto $\{1, 2, \ldots, n\}$. This is a *symmetric group*.

(III) A non-commutative group: $(\{A \in M_2(\mathbb{R}) \mid \det A \neq 0\}, \text{matrix multiplication})$.

**Proposition 6**

The identity of a group is unique. Suppose $e, e'$ are two identities, then

$$e \cdot e' = \begin{cases} e, \text{ treating } e' \text{ as the identity} \\ e', \text{ treating } e \text{ as the identity} \end{cases} \implies e = e'.$$

**Proposition 7**

Given $a \in G$, there is a unique inverse of $a$. This is why we are able to denote the inverse of $a$ as $a^{-1}$.

**Theorem 8: Cancellation Law**

If $a \cdot b = a \cdot c$ for $a, b, c \in G$, then $b = c$. Likewise $b \cdot a = c \cdot a \implies b = c$.

**Proof**

Since $a \in G$, there exists $a^{-1}$. Then

$$a \cdot b = a \cdot c \implies a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c \implies e \cdot b = e \cdot c \implies b = c,$$

and

$$b \cdot a = c \cdot a \implies b \cdot a \cdot a^{-1} = c \cdot a \cdot a^{-1} \implies b \cdot e = c \cdot e \implies b = c.$$

□

**Definition 9**

A group is called **finite** if there is a finite number of elements, for example $(\mathbb{Z}/n\mathbb{Z}, \oplus \pmod{n})$. The **order** of a group $G$, the number of elements, is denoted as $|G|$.

**Definition 10**

An element $g \in G$ has **order** (of element) $n$ if

$$\underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ times}} = e.$$

The order of $g$ is denoted as $o(g)$. In this case $o(g) = n$. If no such $n$ exists then $o(g) = \infty$.

**Theorem 11**

Each element of a finite group has finite order.

**Proof**

Pick $g \in G$ and let $G$ be a finite set. Consider the set

$$\{g, g^2, g^3, \dots\}.$$

Clearly each element in this set is also an element of $G$, and this set is infinite. On the other hand, $|G|$ is finite, so there exist $i, j \in \mathbb{N}$ with $i < j$ such that $g^i = g^j$. Therefore

$$\underbrace{g \cdot g \cdot \dots \cdot g}_{i \text{ times}} = (\underbrace{g \cdot g \cdot \dots \cdot g}_{i \text{ times}})(\underbrace{g \cdot g \cdot \dots \cdot g}_{(j-i) \text{ times}}) = \underbrace{g \cdot g \cdot \dots \cdot g}_{j \text{ times}} \implies g^{j-i} = e$$

Hence $g$ has a finite order, either $j - i$ or a divisor of $j - i$. □

**Theorem 12: Lagrange's Theorem**

Let $G$ be a finite group. Then $o(g)$ divides $|G|$ for all $g \in G$. [Will be proved next class.]

# 9 Mon 9/21

Recall from last time:

(1) Definition of a group; associativity, identity, and inverse.

(2) The inverse of an element is unique; the inverse of identity is identity.

(3) Orders of groups and elements.

**Example 9.1**

Consider the group $(\mathbb{Z}/5\mathbb{Z}, +)$. We have $o(2) = 5$ because $[2] + [2] + [2] + [2] + [2] = [0]$ and no fewer $[2]$'s can make this possible.

**Remark**

$o(e) = 1$, and the converse is also true: if $o(g) = 1$, then $g = e$.

**Theorem 13: Lagrange's Theorem with (partial) proof**

From last time: let $G$ be a finite group. Then $o(g)$ divides $|G|$ for all $g \in G$.

**Example 9.2**

Let $G = (\mathbb{Z}/5\mathbb{Z}, +)$. Then we have $o(0) = 1$ and the order of everything else is 5, indeed a divisor of $|G| = 5$. More generally, all groups of order 5 have the same structure; they are **isomorphic**.

**Proof**

First we know that, $o(g) \geqslant 1$ is finite for all $g \in G$.

If $g = e$, then $o(g) = 1$ and $1 \mid |G|$ is immediate.

Now we will look at non-identity elements.Pick $g \in G$ such that $o(g) = k$. We know that $e = g^k$ and that $g, g^2, g^3, \ldots, g^{k-1}$ includes every element of $G$. Define

$$G_1 = \{g, g^2, g^3, \ldots, g^{k-1}, g^k = e\}$$

We claim that $|G_1| = k$ because if $g^i = g^j$ for some $i \neq j$ with $0 \leqslant i < j \leqslant k-1$, then we have $e = g^{j-i}$ and $j - i < k$.

But this contradicts our assumption that $o(g) = k$.

If $G_1 = G$, this tells us $o(G) = k$ and $o(g) \mid o(G)$ and we are done.

If not, pick $g_2 \in G \setminus G_1$. Now define

$$G_2 = \{g_2 g, g_2 g^2, g_2 g^3, \dots, g_2 g^{k-1}, g_2 g^k = g_2 e\}$$

We know immediately that $|G_2| = k$, because $g_2 g^i = g_2 g^j$ then $g^{j-i}$ is again $e$.

Note that $G_1$ and $G_2$ are disjoint. Suppose not and $g_2 g^i = g^j$ with $0 \leqslant i, j \leqslant k-1$, then

$$g_2 g^i (g^{-1})^i = g^j (g^{-1})^i \implies g_2 = g^{j-i}$$

which implies $g_2 \in G_1$, contradicting our construction of $g_2 \in G \setminus G_1$.

We can keep doing this until we exhaust $G$. Then it follows that each subgroup $G_i$ is of order $k$. Therefore $|G_i|$ divides $|G|$ and $o(g) \mid |G|$.

[To be continued.] □

# 10 Wed 9/23: Worksheet 3

**Problem WS 3.3**

Let $G$ be a group and $g$, an element in $G$ of order 12. What is the order of $g^3$; what about $g^8$?

**Solution**

Since $o(g) = 12$, we know $g^{12} = e$. Therefore $(g^3)^4 = g^{12} = e$. Since 4 is the smallest integer $n$ satisfying $(g^3)^n = (g^{12})^k$ for some $k$, we conclude that $o(g^3) = 4$. Likewise $o(g^8) = 3$ since $(g^8)^3 = g^{24} = e^2 = e$. Likewise, 3 is the smallest integer $n$ satisfying $12 \mid 8n$.

**Remark**

Given a group $G$, for $g \in G$ with $o(g) = a$, then

$$o(g^k) = \frac{a}{\gcd(a,k)}$$

since we are basically trying to find the smallest positive integer $x$ satisfying $a \mid kx$: the order of $g^k$ is the smallest integer satisfying $(g^k)^x$ such that it is $e = g^a$ raised to some power.

**Problem WS3.1**

Let $G$ be a group and $g$ an element in $G$ of order $n$. Let $m$ be a positive integer with $g^m = e$. Show that $n$ divides $m$.

**Solution**

By the division algorithm, we may write $m = qn + r$ where $q, r$ are integers with $0 \leqslant r < n$. Then $g^m = g^{qm+r} = (g^m)^q \cdot g^r = e^q \cdot g^q = g^q$. Since $q < m$, $g^q = e$ only if $q = 0$, we conclude that $n \mid m$.

**Problem WS3.2**

Let $G$ be a group and $g \in G$ such that $g^9 = e$ and $g^{16} = e$. Show $g = e$.

**Solution**

Use cancellation and we get $g^{16-9} = g^7 = e$. Keep doing this (basically the Euclid's algorithm but with exponentials) until we get $g^1 = e$.

**Problem WS3.4**

Show that if $m$ is not prime, then $\{1, 2, \ldots, m-1\}$ is not a group under multiplication mod $m$. Fix this by deleting some elements.

**Solution**

**Definition 14**

Any integer $p \geqslant 2$ is a **prime** if the only divisors of $p$ are $\pm 1, \pm p$.

**Lemma 10.1**

Let $p$ be a prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.

**Proof**

Suppose for a prime $p$ we have $p \mid ab$. If $p\ mida$ we are done. If not we know $\gcd(a, p) = 1$. By Euclid's lemma we know $p \mid b$. □

Recall that $ax \equiv b \pmod{m}$ has a solution only when $\gcd(a, m) \mid b$. Therefore there is no solution to $ax \equiv 1 \pmod{m}$ when $\gcd(a, m) = 1$. Note that $[a]$ has a multiplicative inverse if and only if there exists $x$ such that $ax \equiv 1 \pmod{n}$. Hence if $\gcd(a, m) \neq 1$ and $a \in \{1, 2, \ldots, m-1\}$ there is no multiplicative inverse for $[a]$. On the other hand, since $m$ is not prime, we know such $a$ exists, for example, its smallest divisor besides 1. Hence this is not a group.

To fix this, consider the multiplicative group of $\{x \mid \gcd(x, m) = 1 \text{ and } 1 \leqslant x < m\}$. Each element in this group is coprime with $m$ so the multiplicative inverse always exists, and of course we still have the identity 1.

**Theorem 15**

If $p$ is a prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ is a group with $p - 1$ elements: $\{1, 2, \ldots, p - 1\}$.

**Theorem 16**

The order of $(\mathbb{Z}/m\mathbb{Z})^*$ is $\varphi(m)$ where $\varphi$ is Euler's totient function:

$$\varphi(n) = |\{x \mid \gcd(x, n) = 1 \text{ and } 1 \leqslant x \leqslant n - 1\}|.$$

## 11 Fri 9/25

**Proposition 17**

If $p$ is a prime, then $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p - 1\}$ is a group under multiplication mod $p$. On the other hand, if $m$ is not a prime, then $\{1, 2, \ldots, m - 1\}$ is not a group under multiplication mod $m$, but we can fix this by defining the group as

$$(\mathbb{Z}/m\mathbb{Z})^* = \{x \mid 1 \leqslant x \leqslant m - 1 \text{ and } \gcd(x, m) = 1\}.$$

Furthermore, this definition implies the definition of $(\mathbb{Z}/p\mathbb{Z})^*$. See next page.

### Proof of this proposition

(1) Associativity: obvious from multiplication.

(2) Identity: $1 \in (\mathbb{Z}/m\mathbb{Z})^*$ since $\gcd(1.m) = 1$ and $a \cdot 1 = 1 \cdot a = a$.

(3) Closure: take $x, y \in G$. By definition we know $0 \leqslant x, y \leqslant m-1$ and both are coprime to $m$. Suppose $\gcd(x, m) = \gcd(y.m) = 1$, then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{cases} ax + bm = 1 \\ cy + dm = 1 \end{cases} \implies (ax + bm)(cy + dm) = (ac)(xy) + (\sim)m = 1$$

which implies $\gcd(xy, m) = 1$, and we are done proving closure.

(4) Inverse: given $a \in (\mathbb{Z}/m\mathbb{Z})^*$, find $b \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $ab = 1$. This is nothing different from solving $ax \equiv 1 \pmod m$ while also making sure $\gcd(x, m) = 1$. Since $\gcd(a, m) = 1$ (from the fact that $a$ is in the group), we can solve $ax + my = 1$ for some $x, m$. Then the first congruence relation is already met. Now look again at the equation. $ax + my$ can also be seen as a $\mathbb{Z}$-combination of $x$ and $m$. Hence $\gcd(x, m) = 1$. Hence $[a]^{-1} = [x]$ and we have found an inverse.

Hence $(\mathbb{Z}/m\mathbb{Z})^*$ is a group under multiplication mod $m$. □

### Continuing on the Proof of Lagrange's Thm

□

### Example 11.1

$G = (\mathbb{Z}/11\mathbb{Z})^* = \{1, 2, \ldots, 10\}$. Then $|G| = 10$ and $i^{10} \equiv 1 \pmod{11}$ for all $i \in G$.
In general, we have the following:

### Theorem 18: Fermat's Little Theorem

Let $p$ be a prime. Then $a^{p-1} \equiv 1 \pmod p$ for all $1 \leqslant a \leqslant p - 1$.

**Proof**

Let $(\mathbb{Z}/p\mathbb{Z})^*$ be a group under multiplication mod $p$. Then this group has order $p-1$. Hence if $g \in (\mathbb{Z}/p\mathbb{Z})^*$ then $o(g) \mid p-1$ and $g^{p-1} = e$. □

**Theorem 19: Euler's Theorem, 1736**

Suppose $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ such that $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Note that this is an extension of Fermat's Little Theorem, and the proof is highly analogous.