$\mathbb{Z}/n\mathbb{Z}$ & Unit 20221011

Quotient Group: $\mathbb{Z}/n\mathbb{Z}$

- $(\mathbb{Z},+)$ and Subgroup $n\mathbb{Z}$.
  - We'll study the quotient group $\mathbb{Z}/n\mathbb{Z},\ (n\geq 2)$.

Notations

- Elements in $\mathbb{Z}/n\mathbb{Z}$ are of form $k+n\mathbb{Z}$.
  - Denote $\bar{k}=k+n\mathbb{Z}$.
  - $\overline{k_1}=\overline{k_2} \iff (-k_1)+k_2\in n\mathbb{Z} \iff n \text{ devides } k_2-k_1$
  - $(aN=bN \iff a^{-1}b\in N)$
- So $\mathbb{Z}/n\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\dots,\overline{k-1}\}$
  - The composition is $\bar{a}+\bar{b}=\overline{a+b}$
  - $((a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b)+n\mathbb{Z})$
- We also say "a is congruent to b modulo n", denoted by $a\equiv b \pmod n$ if $\bar{a}=\bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$.

Multiplication

- We can also define another composition, called multiplication on $\mathbb{Z}/n\mathbb{Z}$:
  - $\bar{k}\cdot\bar{l}=\overline{kl}$
- We need to verify this multiplication is "Well-Defined":
  - i.e. $\overline{k_1}=\overline{k_2},\ \overline{l_1}=\overline{l_2} \quad\Rightarrow\quad \overline{k_1}\cdot\overline{k_2}=\overline{l_1}\cdot\overline{l_2}. \quad (\overline{k_1l_1}=\overline{k_2l_2})$

$$
\begin{aligned}
\overline{k_1} = \overline{k_2} &\quad\Rightarrow\quad k_2 - k_1 = an \text{ for some } a \in \mathbb{Z} \\
\overline{l_1} = \overline{l_2} &\quad\Rightarrow\quad l_2 - l_1 = bn \text{ for some } b \in \mathbb{Z}
\end{aligned}
$$

- $$
\begin{aligned}
k_2 l_2 - k_1 l_1 &= (k_1 + an)(l_1 + bn) - k_1 l_1 \\
&= k_1 l_1 + a l_1 n + b k_1 n + abn^2 - k_1 l_1 \\
&= (a l_1 + b k_1 + abn)n
\end{aligned}
$$
- So $\overline{k_1 l_1} = \overline{k_2 l_2}$

- Question: Is $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ withe the multiplication a group?
  - Associativity: $(\bar{a}\bar{b})\bar{c} = \overline{ab} \cdot \bar{c} = \overline{abc} =$
  - Identity:
  - Inverse:
- Conclusion: $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is NOT a group

Q. Is $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ with the multiplication a group?

- Associativity: $(\bar{a}\bar{b})\bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a} \cdot \overline{bc} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$
- Identity: $\bar{1}$ since $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}$ $\forall \bar{a}$.
- Inverse: There're elements having no inverse.
  For example. $\bar{0} \cdot \bar{a} = \bar{1} \Rightarrow \bar{0} = \bar{1}$. so $\bar{0}^{-1}$ doesn't exist.

Conclusion: $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is NOT a group.

Unit

Definition

$\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is called a unit if it has multiplicative inverse.

i.e. ($\exists \bar{b} \in \mathbb{Z}/n\mathbb{Z}, \bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = \bar{1}$)

Def. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is called a unit if it has multiplicative inverse (i.e., $\exists \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{a}.\bar{b} = \bar{b}.\bar{a} = \bar{1}$)

Prop. If $\bar{a}, \bar{c}$ are both units of $\mathbb{Z}/n\mathbb{Z}$, then $\bar{a}.\bar{c}$ is also a unit of $\mathbb{Z}/n\mathbb{Z}$

Pf. $\exists \bar{b}, \bar{d} \in \mathbb{Z}/n\mathbb{Z}$. $\bar{a}\bar{b} = \bar{b}\bar{a} = \bar{1}$, $\bar{c}\bar{d} = \bar{d}\bar{c} = \bar{1}$

Then $\overline{ac}.\overline{bd} = \overline{(ac)(bd)} = \overline{(ab)(cd)} = \overline{ab}.\overline{cd} = \bar{1}.\bar{1} = \bar{1}$.

similarly $\overline{bd}.\overline{ac} = \bar{1}$.

$\bar{b}.\bar{d}$ is the inverse of $\bar{a}\bar{c}$, so $\bar{a}.\bar{c}$ is a unit.

- Group of Units

Def. The set of units of $\mathbb{Z}/n\mathbb{Z}$ with multiplication forms a group, called the "group of units", denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$

e.g. $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$. $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$.

$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$. $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$ $\quad \bar{2}.\bar{2} = \bar{4} = \bar{1}$

$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ $\quad \bar{3}.\bar{3} = \bar{9} = \bar{1}$

- Theorem

Theorem. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. The following are equivalent:

(i). $\bar{a}$ is a unit.

(ii). $\gcd(a, n) = 1$. i.e., a & n are relatively prime

(iii). $\bar{a}$ is a generator for $\mathbb{Z}/n\mathbb{Z}$.

(iv). $f_{\bar{a}}: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f_{\bar{a}}(\bar{x}) = \overline{ax}$ is an automorphism.

Pf. we will prove: (i) $\Rightarrow$ (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i)

(i) $\Rightarrow$ (iv) Given $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

$$f_{\bar{a}}(\bar{x}+\bar{y}) = \bar{a}\cdot(\bar{x}+\bar{y}) = \bar{a}\cdot\overline{x+y} = \overline{a(x+y)} = \overline{ax+ay} = \overline{ax}+\overline{ay}$$
$$= f_{\bar{a}}(\bar{x}) + f_{\bar{a}}(\bar{y})$$

So $f_{\bar{a}}$ is a homomorphism

$\bar{a}$ is a unit. denote its multiplicative inverse by $\bar{b}$.

The $f_{\bar{a}}\cdot f_{\bar{b}}(\bar{x}) = \bar{a}(\bar{b}.\bar{x}) = \overline{ab}.\bar{x} = \bar{x}$
$f_{\bar{b}}\cdot f_{\bar{a}}(\bar{x}) = \bar{b}(\bar{a}.\bar{x}) = \overline{ba}.\bar{x} = \bar{x}$ $\Big\} \Rightarrow$ $f_{\bar{b}}$ is the inverse function of $f_{\bar{a}}$.

(iv) $\Rightarrow$ (iii). $f_{\bar{a}}$ is an automorphism. In particular, it's surjective

For any $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$. $\exists\, \bar{x} \in \mathbb{Z}/n\mathbb{Z}$ $\bar{k} = f_{\bar{a}}(\bar{x}) = \overline{ax}$

we can take x to be positive, then

$$\bar{k} = \overline{ax} = \overline{\underbrace{a+\cdots+a}_{x \text{ copies}}} = \underbrace{\bar{a}+\cdots+\bar{a}}_{x \text{ copies}}$$

So $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$.

(iii) $\Rightarrow$ (ii) If $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$. Then $\bar{1} = \underbrace{\bar{a}+\bar{a}+\cdots+\bar{a}}_{l \text{ copies.}} = \overline{al}$

so $\exists\, k \in \mathbb{Z}$, $1 - al = kn$

$\Rightarrow kn + la = 1 \Rightarrow \gcd(a,n) = 1$.

(ii) $\Rightarrow$ (i) If $\gcd(a,n)=1$. $\exists\, k, l \in \mathbb{Z}$, $ka + ln = 1$.

$\Rightarrow ka - 1 \in n\mathbb{Z} \Rightarrow \bar{a}.\bar{k} = \bar{1}$

The Euler's Phi Function

Def. The Euler's Phi Function $\phi(n) = \#\{k \in \mathbb{N} \mid 1 \leq k \leq n, \gcd(k,n)=1\}$

e.g. $\phi(1)=1$. $\phi(2)=1$ $\phi(3)=2$. $\phi(4)=2$.

$\phi(3)=2 \downarrow \{1, 2, \cancel{3}\}$ $\phi(4)=2 \downarrow \{1, \cancel{2}, 3, \cancel{4}\}$

since $\bar{0} = \bar{n} \in \mathbb{Z}/n\mathbb{Z}$. $\phi(n)$ gives us the number of elements among $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ that are units. (we just proved $\gcd(a,n)=1 \Leftrightarrow \bar{a}$ is a unit). i.e., $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$

Fermat's Little Theorem

Fermat's Little Theorem.

$n \geq 2$, $\gcd(a,n)=1$. Then $a^{\phi(n)} \equiv 1 \pmod n$

Pf. $\gcd(a,n)=1 \Rightarrow \bar{a}$ is a unit. i.e. $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

$|\bar{a}| \mid |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$. $\bar{a}^{\phi(n)} = \bar{1}$. $\Rightarrow \overline{a^{\phi(n)}} = \bar{1}$

(implied by the Lagrange Theorem) $\Rightarrow a^{\phi(n)} \equiv 1 \pmod n$

Cor. p is a prime, p doesn't divide a. then $a^{p-1} \equiv 1 \pmod p$.

Pf. p prime. $\phi(p) = p-1$ $\{1, 2, \ldots, p-1, \cancel{p}\}$

$p \nmid a$, p prime $\Rightarrow \gcd(a,p)=1$. so $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

By Fermat's Little Theorem. $\bar{a}^{p-1} = \bar{a}^{\phi(p)} = \bar{1}$

Theorem. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Pf. If $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

For any $\bar{k}$. (we can assume $k>0$).

$$f(\bar{k}) = f(\underbrace{\overline{1+1+\cdots+1}}_{k \text{ copies}}) = f(\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{k \text{ copies}}) = \underbrace{f(\bar{1})+f(\bar{1})+\cdots+f(\bar{1})}_{k \text{ copies}}$$

Denote $\bar{a} = f(\bar{1})$

$$= \underbrace{\bar{a}+\cdots+\bar{a}}_{k \text{ copies}}$$

$$= \overline{\underbrace{a+\cdots+a}_{k \text{ copies}}} = \bar{a}.\bar{k}$$

$\Rightarrow f(\bar{k}) = \bar{a}.\bar{k}$

so all the automorphisms $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow f(\bar{k}) = \bar{a}.\bar{k}$ $\quad = \overline{\underbrace{a+\cdots+a}_{k \text{ copies}}} = \bar{a}.\bar{k}$

so all the automorphisms $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

have to be of the form $f(\bar{k}) = \bar{a}.\bar{k}$.

And we'll proved this kind of map is an automorphism iff $\bar{a}$ is a unit.

We see $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{ f_{\bar{a}} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \mid \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \}$.

Define $F: (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

$$\bar{a} \longmapsto f_{\bar{a}}.$$

It's clear that F is a bijection by the discussion above.

It's also a homomorphism:

$\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z}$. $F(\bar{a}\cdot\bar{b})(\bar{k}) = f_{\bar{a}\bar{b}}(\bar{k}) = (\bar{a}\cdot\bar{b})(\bar{k}) = \bar{a}(\bar{b}\cdot\bar{k})$

$$= f_{\bar{a}}(f_{\bar{b}}(\bar{k}))$$

so $\underline{F(\bar{a}\cdot\bar{b}) = F(a)\cdot F(\bar{b})}$.

$$= f_{\bar{a}}\circ f_{\bar{b}}(\bar{k})$$

$$= F(\bar{a})\cdot F(\bar{b})(\bar{k})$$

F is an isomorphism, $(\mathbb{Z}/n\mathbb{Z})^{\times} \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.