Week 4

The chinese remainder theorem

Ex ①: I have some pebbles

into 3 piles → 1 remaining   4, 7, 10, 13, ..

into 5 piles → 2 remaining   7, 12, 17, 22

Question: how many pebbles do I have

A1: 7

A2. 22

Conjecture: $7+15n$ for any $n \in \mathbb{Z}$

Ex ②: Add another condition

in piles of 7 → 3 remaining

A1: 52

A2: $52 + 3 \cdot 7 \cdot 5 = 157$

Ex ③: Conditions

piles of 4 ⟶ 2

piles of 6 ⟶ 4   10 works

Ex ④: piles of 4 ⟶ 1   1, 5, 9, 13, ...

piles of 6 ⟶ 4   4, 10, 16, 22, ...

Chinese remainder theorem: (OG version)

Suppose $m_1, m_2, \ldots, m_N$ are pairwise relatively prime

Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_N \pmod{m_N}$$

has a unique solution modulo $m_1 m_2 \ldots m_N$

Proof For each $1 \le k \le N$, let

$$M_k = \frac{m_1 m_2 \cdots m_N}{m_k} = m_1 m_2 \ldots \underset{\uparrow \text{omit}}{\hat{m}_k} \ldots m_N$$

then $\gcd(M_k, m_k) \Rightarrow 1$ so M_k has an inverse mod m_k, call it y_k (multiplicative inverse) then $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_N M_N y_N$ is a solution (not the smallest)

to check

$$x \equiv a_1 0 y_1 + a_2 0 y_2 + \dots + a_k M_k y_k + \dots + a_N 0 y_N \pmod{m_k}$$
$$\equiv a_k (M_k y_k) \equiv a_k \cdot 1 = a_k \pmod{m_k}$$

Ex: 5

$x \equiv 15 \pmod{37}$

$x \equiv 7 \pmod{61}$

$M_1 = 61 \qquad M_2 = 37$

$M_1 = 61 \equiv 24 \pmod{37}$

$M_2 = 37 \equiv 37 \pmod{61}$

what is the inverse of 24 mod 37?

Divide: $37 = 1 \cdot 24 + 13$ $\qquad \gcd(37, 24) = \gcd(24, 13)$

$24 = 1 \cdot 13 + 11$

$13 = 1 \cdot 11 + 2$

$11 = 5 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

reverse: $1 = 11 - 5 \cdot 2$

$= 1 - 5(13 - 1 \cdot 11)$

$= 6 \cdot 11 - 5 \cdot 13$

$= 6(24 - 1 \cdot 13) - 5 \cdot 13$

$= 6 \cdot 24 - 11 \cdot 13$

$= 6 \cdot 24 - 11(37 - 1 \cdot 24)$

$= 17 \cdot 24 - 11 \cdot 37$

mod 37: $\quad 1 \equiv 17 \cdot 24 \pmod{37}$

so $y_1 = 17$

to get the remainder of 37 mod 61:

$61 = 37 + 24$

$37 = 24 + 13$

$24 = 13 + 11$

$13 = 11 + 2$

$11 = 5 \cdot 2 + 1$

$2 = 1 + 0$

$1 = 11 - 5 \cdot 2$

$1 = 11 - 5(13 - 11)$

$= 4 \cdot 11 - 5 \cdot 13$

$= -4(24 - 13) - 5 \cdot 13$

$= -4 \cdot 24 - 9 \cdot 13$

$y_2 = -28 \equiv 33 \pmod{61}$

<u>More</u> <u>modern</u>: Desired remainders

$a_1 \pmod{m_1}, \dots, a_N \pmod{m_N}$

$\Updownarrow$

$a_1 \in \mathbb{Z}/m_1\mathbb{Z} \quad \dots \quad a_N \in \mathbb{Z}/m_N\mathbb{Z} \iff (a_1, a_2, \dots, a_N) \in \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_N\mathbb{Z}$

• let $\pi_k(x) = a_k$ where $\pi_k : \mathbb{Z} \to \mathbb{Z}/m_k\mathbb{Z}$

so $\pi(x) = (a_1, a_2, \dots, a_N)$ $\pi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_N\mathbb{Z}$

then " there always exist an x"

$$\Updownarrow$$

π is surjection

and "unique up to $m_1 m_2 \cdots m_N$"

$$\Downarrow$$

$$\mathrm{Ker}(\pi) = m_1 m_2 \cdots m_N \mathbb{Z} = (m_1\mathbb{Z}) \cdots (m_N\mathbb{Z})$$

so 1st iso theorem says

$$\mathbb{Z}/m_1 m_2 \cdots m_N\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_N\mathbb{Z}$$

more generally

$$R/I_1 \cdots I_N \simeq R/I_1 \times \dots \times R/I_N$$

A bit of informal category theory

A category $\mathcal{C}$ consists of

1) Collection of objects (often visualized as dots)
2) Collection of arrows (sometimes called morphisms) between objects

$$a \xrightarrow{f} b$$

satisfying a few basic conditions (composition, associativity, unique identity arrow)

Ex 1: $X = \{1, 2, 3\}$

→ make a category $\mathcal{C}_X$

• objects are subsets of X

• arrows: $S \to T$ iff $S \subseteq T$

$$\begin{tikzcd}
 & \{1,2,3\} & \\
\{1,2\} \arrow[ur] & \{1,3\} \arrow[u] & \{2,3\} \arrow[ul] \\
\{1\} \arrow[u] \arrow[ur] & \{2\} \arrow[ul] \arrow[ur] & \{3\} \arrow[u] \arrow[ul] \\
 & \emptyset \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Ex 2 Set

• objects: sets

• arrows: functions between sets

$$\begin{tikzcd}
X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \arrow[d, shift left, "\phi"] \\
 & Z \arrow[u, shift left, "h"]
\end{tikzcd}$$

Some others:

- $\underline{\text{Grp}}$: objects: groups
  arrows: group homomorphisms
- $\underline{\text{Ab}}$ objects: abelian groups
  arrows: group homomorphisms

$\underline{\text{Ring}}$ objects: rings (w/ 1)
arrows: ring hom.

$\underline{\text{Vec}}_{\mathbb{R}}$ objects: vector space of $\mathbb{R}$
arrows: linear transformations

$\underline{\text{Ex 3}}$ (odd)

$\underline{\text{Mat}}_{\mathbb{R}}$ matrices with real entries

objects: natural numbers
arrows: $n \xrightarrow{A} m$ where A is an $n \times m$ matrix

New notion: "universal property"

$\underline{\text{Ex 4}}$ In $\mathcal{C}_X$ where $X = \{1,2,3\}$

$$\begin{tikzcd}
 & \{1,2,3\} & \\
\{1,2\} \arrow[ur] & \{1,3\} \arrow[u] & \{2,3\} \arrow[ul] \\
\{1\} \arrow[u] \arrow[ur] & \{2\} \arrow[ul] \arrow[ur] & \{3\} \arrow[u] \arrow[ul] \\
 & \emptyset \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Suppose S, T are objects in $\mathcal{C}_X$

$$\begin{tikzcd}
 & \bullet T \\
\bullet S &
\end{tikzcd}$$

Q: Is there a single object in $\mathcal{C}_X$ that captures the information of this diagram

Alternatively: is there a single object closest to this diagram?

More precisely: is there an object Z with arrows to this diagram

$$\begin{tikzcd}
Z \arrow[r, "g"] \arrow[d, "f"'] & T \\
S &
\end{tikzcd}$$

Z is closest among all such contenders

ie. if

$$\begin{tikzcd}
W \arrow[r, "\exists!\phi"] \arrow[rr, bend left, "i"] \arrow[dr, bend right, "h"'] & Z \arrow[r, "g"] \arrow[d, "f"] & T \\
& S &
\end{tikzcd}$$

then there exists a unique arrow $\phi : W \to Z$ such that $h = f \circ \phi$ and $i = g \circ \phi$

What is this magical set Z?

It's their intersection: $S \cap T$

$$\begin{tikzcd}
S \cap T \arrow[r] \arrow[d] & T \\
S &
\end{tikzcd}$$

"Dually"

$Z = S \cup T$

$$\begin{tikzcd}
& T \arrow[d, "g"] \arrow[dr, bend left] & \\
S \arrow[r, "f"] \arrow[rr, bend right] & Z \arrow[r, dashed] & W
\end{tikzcd}$$

Ex 6 In Set

$$\begin{tikzcd}
W \arrow[r, "\phi"] \arrow[rr, bend left, "i"] \arrow[dr, bend right, "h"'] & Z \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & Y \\
& X &
\end{tikzcd}$$

$$\begin{tikzcd}
Z = X \times Y \arrow[r, "(x,y) \mapsto y"] \arrow[d, "(x,y) \mapsto x"'] & Y \\
X &
\end{tikzcd}$$

$\phi(w) = (h(w), i(w))$

Similarly

$Z = X \amalg Y$ (disjoint union)

$$\begin{tikzcd}
& Y \arrow[d] \arrow[dr, bend left, "i"] & \\
X \arrow[r] \arrow[rr, bend right, "h"'] & Z \arrow[r, "\phi"] & W
\end{tikzcd}$$

ex: $A = \{a,b,c\}$ $Y = \{1,2\}$

Up a notch (in Set)

Diagram

$V = \{(x,y) : f(x) = g(y)\}$

$V = X \times_Z Y$

"fiber product"

$$\begin{tikzcd}
V \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & Y \arrow[d, "g"] \\
X \arrow[r, "f"] & Z
\end{tikzcd}$$

the other way

$$\begin{tikzcd} Z \arrow[r, "g"] \arrow[d, "f"'] & Y \arrow[d] \\ X \arrow[r] & V = X \underset{Z}{\sqcup} Y \end{tikzcd}$$

"amalgamated union"

$= X \cup Y /\sim$

where $x \sim y$ if $x = f(z)$ and $y = g(z)$

Back to Ring

"universal property of quotients"

For an ideal $I \subseteq R$ what is special about R/I

A: there is a hom. $\pi : R \to R/I$

with $I \subseteq \ker(\pi)$, i.e. $\pi(I) = 0$

This is universal

if $\phi : R \to S$ with $I \subseteq \ker(\phi)$

then

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "\phi"'] & R/I \arrow[d, dashed, "\exists ! \psi"] \\ & S \end{tikzcd}$$

Lattice isomorphism theorem

$$\begin{tikzcd}[column sep=small] & \mathbb{Z} = (1) \arrow[dl, dash] \arrow[dr, dash] & & \\ (2) \arrow[dr, dash] & & (3) \arrow[dl, dash] \arrow[dr, dash] & \\ & (6) \arrow[dr, dash] & & (9) \arrow[dl, dash] \\ & & (18) & \end{tikzcd}$$

$$\begin{tikzcd}[column sep=small] & \mathbb{Z}/(18) & & \\ (\bar{2}) \arrow[dr, dash] & & (\bar{3}) \arrow[dl, dash] \arrow[dr, dash] & \\ & (\bar{6}) \arrow[dr, dash] & & (\bar{9}) \arrow[dl, dash] \\ & & (\overline{18}) & \\ & & \shortparallel & \\ & & (0) & \end{tikzcd}$$