5. The Chinese Remainder Theorem

Motivating example: let's solve the system $\begin{cases} 2x \equiv 5 \pmod{7} \\ 3x \equiv 4 \pmod{8} \end{cases}$

In $\mathbb{Z}_7$: $2^{-1} = 4$, so $4(2x \equiv 5) \bmod 7$

$$\Rightarrow \quad x \equiv 6 \bmod 7$$

$$\Rightarrow \quad x = 6 + 7t, \quad \text{for } t \in \mathbb{Z}.$$

Plug this into $3x \equiv 4 \pmod{8}$

$$\Rightarrow 3(6+7t) \equiv 4 \bmod 8$$

$$\Rightarrow 5t \equiv 2 \bmod 8 \qquad (\text{Note: } 5^{-1} = 5 \text{ in } \mathbb{Z}_8)$$

$$\Rightarrow 5(5t \equiv 2) \bmod 8$$

$$\Rightarrow t \equiv 2 \bmod 8$$

$$\Rightarrow t = 2 + 8s, \quad \text{for } s \in \mathbb{Z}$$

Plug $t = 2 + 8s$ back in $x = 6 + 7t$

$$= 6 + 7(2 + 8s)$$

$$= 20 + 56s \quad \Rightarrow \quad \boxed{x \equiv 20 \pmod{56}}$$

What could go wrong: Solve $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 0 \pmod{6} \end{cases}$

$x = 3 + 4t$, for $t \in \mathbb{Z}$

Reduce modulo 6: $3 + 4t \equiv 0 \bmod 6 \Rightarrow 4t \equiv -3 \pmod{6}$.

This has no solution because $\gcd(4, 6) \nmid -3$.

<u>Chinese remainder theorem</u> (number theory version): Let $n_1, \dots, n_k \in \mathbb{Z}^+$ be pairwise coprime. For any $a_1, \dots, a_k \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$ that solves the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Moreover, all solutions are congruent modulo $N = n_1 n_2 \cdots n_k$.

This is a special case of a much more general result.

<u>Groups</u>: If $H \leq G$, then $x \equiv y \pmod{H}$ if $y^{-1}x \in H$.
(or $x - y \in H$ in additive notation)

<u>Rings</u>: If $I \trianglelefteq R$, then $r \equiv s \bmod I$ if $r - s \in I$.

<u>Warm-up</u>: If $I, J \trianglelefteq R$, then $IJ = (ab \mid a \in I, b \in J)$

$$= \{a_1 b_1 + \dots + a_k b_k \mid a_i \in I, b_j \in J\} \subseteq I \cap J$$

<u>Examples</u>:

$(9)(6) = (54) \subseteq \mathbb{Z}$	product
$(9) \cap (6) = (18)$	lcm
$(9) + (6) = (3)$	gcd

<u>Remark</u>: In $\mathbb{Z}$, $\gcd(x, y) = 1$ iff $\exists\, a, b \in \mathbb{Z}$ s.t. $ax + by = 1$ (a unit), or equivalently, $(x) + (y) = \mathbb{Z}$.

<u>Def</u>: Two ideals I, J of R are co-prime if $I + J = R$.

Chinese Remainder Theorem (rings, 2 ideals). Let R have 1 and I, J be co-prime ideals. Then for any $r_1, r_2 \in R$, $\exists\, r \in R$ s.t. $r - r_1 \in I$ and $r - r_2 \in J$, i.e., r solves the system $\begin{cases} x \equiv r_1 \bmod I \\ x \equiv r_2 \bmod J. \end{cases}$

Pf: Write $1 = a + b$, $a \in I$, $b \in J$, and set $r = r_2 a + r_1 b$.

why this works:

$$r - r_1 = (r - r_1 b) + r_1(b-1) = r_2 a + r_1(b-1) = r_2 a - r_1 a = (r_2 - r_1) a \in I \quad ✓$$

$$r - r_2 = (r - r_2 a) + r_2(a-1) = r_1 b + r_2(a-1) = r_1 b - r_2 b = (r_1 - r_2) b \in J \quad ✓$$

Chinese Remainder Theorem (ring verscon): Let R be a ring with 1, and $I_1, \dots, I_n$ pairwise co-prime ideals. Then for any $r_1, \dots, r_n \in R$, $\exists\, r \in R$ s.t. $x = r$ solves the system
$$\begin{cases} x \equiv r_1 \mod I_1 \\ \vdots \\ x \equiv r_n \mod I_n. \end{cases}$$

Moreover, any 2 solutions are congruent modulo $I_1 \cap \dots \cap I_n$.

Pf: $\boxed{n=1}$ For $j = 2, \dots, n$, write $1 = a_j + b_j$, where $a_j \in I_1$, $b_j \in I_j$.

Then
$$\begin{aligned} 1 &= (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) \\ &= a_2(a_3+b_3)\cdots(a_n+b_n) + b_2(a_3+b_3)\cdots(a_n+b_n) \in I_1 + \prod_{j=2}^{n} I_j = R. \end{aligned}$$

Now apply the CRT for 2 ideals to the system
$$\begin{cases} x \equiv 1 \mod I_1 \\ x \equiv 0 \mod \prod_{j=2}^{n} I_j \end{cases}$$

Let $s_1 \in R$ be a solution.

Note that $s_1 \equiv 0 \mod I_j$ for $j = 2, \dots, n$.

Similarly, let s_k be a solution to
$$\begin{cases} x \equiv 1 \mod I_k \\ x \equiv 0 \mod \prod_{j \neq k} I_j \end{cases}$$

Now, set $r = r_1 s_1 + \dots + r_n s_n$.

Note that $r \equiv r_j \mod I_j$ ✓

Now, if $s \in R$ is another solution, then $s \equiv r_j \equiv r \mod I_j \quad \forall j = 1, \dots, n$, and so $s \equiv r \mod \bigcap_{j=1}^{n} I_j$. $\square$

Cor: Let $I_1, \dots, I_n$ be ideals of R. Then $\exists$ ring homom

$$g : R/(I_1 \cap \cdots \cap I_n) \hookrightarrow R/I_1 \times \cdots \times R/I_n.$$

Moreover, if $1 \in R$ and $I_j + I_k = R \ \forall j \neq k$, then g is an isomorphism.

Pf: Let $f : R \longrightarrow R/I_1 \times \cdots \times R/I_n$ be the canonical mapping,

$$r \longmapsto (r + I_1, \dots, r + I_n).$$

This is clearly a homom. with $\ker f = I_1 \cap \cdots \cap I_n$.

By the FIHT, $\exists !\, g$ that we seek.

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\eta"'] & & R/I_1 \times \cdots \times R/I_n \\ & R/(I_1 \cap \cdots \cap I_n) \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

- This is 1-1 because of the CRT: all solutions are congruent modulo $\bigcap_{j=1}^{n} I_j$
- If the I_j's are pairwise co-prime, then g is onto by the CRT (every system can be solved).

Example of CRT: Let $R = \mathbb{Z}$ and $I_j = (m_j)$ for $j = 1, \dots, n$ with $(m_i, m_j) = 1$ for $i \neq j$. Then $I_1 \cap \cdots \cap I_n = (m_1 m_2 \cdots m_n)$ and

$$\mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n};$$

Cor: Let $n = p_1^{d_1} \cdots p_n^{d_n}$, distinct primes p_j. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{d_1}} \times \cdots \times \mathbb{Z}_{p_n^{d_n}}.$$

Remark: If R is a Euclidean domain, then the proof of the CRT is constructive.

Specifically, use the Euclidean algorithm to write

$$c_k m_k + d_k \prod_{j \neq k} m_j = \gcd\left(m_k, \prod_{j \neq k} m_j\right) = 1 \quad \text{where } I_j = (m_j).$$

Then set $s_k = d_k \prod_{j \neq k} m_j$ and $r = r_1 s_1 + \cdots + r_n s_n$ is the sol'n.