Chinese Remainder Theorem

Example: Find $[13]^{-1}$ in $\mathbb{Z}_{42}$

$[13x]=[1]$ in $\mathbb{Z}_{42}$

$13x \equiv 1 \pmod{42}$

$13x + 42y = 1$ EEA: $(\underbrace{13}_{x}, -4)$ is one soln.

$x \equiv 13 \pmod{42}$

$[x] \equiv [13]$ So $[13]^{-1} = [13]$ in $\mathbb{Z}_{42}$

Chinese Remainder Theorem

Suppose $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ such that $\gcd(m_1, m_2) = 1$.

Consider $\begin{cases} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \end{cases}$

Find all possible int n for which both are true.

Example $\begin{cases} n \equiv 2 \pmod{3} & ① \\ n \equiv 1 \pmod{4} & ② \end{cases}$

$n = 5$ is one soln

$n = -7, 17, 29, 41,$

$n \equiv 5 \pmod{12}$

① $\Rightarrow n = 2 + 3x$ for some $x \in \mathbb{Z}$ ③

Sub into ②. $2 + 3x \equiv 1 \pmod{4}$

$3x \equiv -1 \pmod{4}$

$x \equiv 1 \pmod{4}$

So $x = 1 + 4y$ for some $y \in \mathbb{Z}$

Sub into ③: $n = 2 + 3(1+4y) = 5 + 12y \Rightarrow n \equiv 5 \pmod{12}$

$S = \{n \in \mathbb{Z} \mid ① ②\}$ $T = \{n \in \mathbb{Z} \mid n \equiv 5 \pmod{12}\}$

We proved that $S \subseteq T$.

To prove $T \subseteq S$: Assume $n \equiv 5 \pmod{12}$, check ①, ② are satisfied.

CRT: If $\gcd(m_1, m_2) = 1$, then for any $a_1, a_2 \in \mathbb{Z}$, there exists an int soln to:

$$\begin{cases} n \equiv a_1 \pmod{m_1} & ① \\ n \equiv a_2 \pmod{m_2} & ② \end{cases}$$

If n_0 is one int soln, then the complete soln is $n \equiv n_0 \pmod{m_1 \cdot m_2}$

Build a solution: $① \Rightarrow n = a_1 + m_1 x$ for some $x \in \mathbb{Z}$.

Plug into ②: $a_1 + m_1 x \equiv a_2 \pmod{m_2}$

$$m_1 x \equiv (a_2 - a_1) \pmod{m_2}$$

Let $m_1' \in \mathbb{Z}$ such that

$[m_1'] = [m_1]^{-1}$ in $\mathbb{Z}_{m_2}$. This exists since $\gcd(m_1, m_2) = 1$.

$$m_1' m_1 x \equiv m_1' (a_2 - a_1) \pmod{m_2}$$
$$x \equiv m_1' (a_2 - a_1) \pmod{m_2}$$

Pick $x = m_1'(a_2 - a_1)$ So $n = a_1 + m_1 (m_1'(a_2 - a_1))$

Proposition (from A6): If $\gcd(m,n)=1$, then $a \equiv b \pmod{mn}$ if and only if $a \equiv b \pmod m$ and $a \equiv b \pmod n$.

Proof of CRT: Let $m_1' \in \mathbb{Z}$ such that $[m_1'] = [m_1]^{-1}$ in $\mathbb{Z}_{m_2}$. This inverse exists since $\gcd(m_1, m_2) = 1$.

Let $n = a_1 + m_1 m_1' (a_2 - a_1)$. Since $m_1 \equiv 0 \pmod{m_1}$,
$n \equiv a_1 + 0 \equiv a_1 \pmod{m_1}$. Since $m_1 m_1' \equiv 1 \pmod{m_2}$,
$n \equiv a_1 + 1 \cdot (a_2 - a_1) \equiv a_2 \pmod{m_2}$.
So an int soln exists.

Let $S = \{n \in \mathbb{Z} \mid ① ② \text{ hold}\}$, $T = \{n \in \mathbb{Z} \mid n \equiv n_0 \pmod{m_1 m_2}\}$

Suppose $n \in S$. So $n \equiv a_1 \pmod{m_1}$, $n \equiv a_2 \pmod{m_2}$

But $n_0 \in S$ So $n_0 \equiv a_1 \pmod{m_1}$, $n_0 \equiv a_2 \pmod{m_2}$

By transitivity, $n \equiv n_0 \pmod{m_1}$ and $n \equiv n_0 \pmod{m_2}$

By prop above, $n \equiv n_0 \pmod{m_1 m_2}$, so $n \in T$. So $S \subseteq T$.

Suppose $n \in T$. So $n \equiv n_0 \pmod{m_1 m_2}$. So $n = n_0 + m_1 m_2 x$.
So $n \equiv n_0 \pmod{m_1} \equiv a_1 \pmod{m_1}$. And
$n \equiv n_0 \pmod{m_2} \equiv a_2 \pmod{m_2}$.

So $n \in S \Rightarrow S = T$ $\square$.