Recall from Prev. lecture:

CRT (two congruences case): Let $m_1, m_2 \in \mathbb{Z}^+$ with $\gcd(m_1, m_2) = 1$. For all $b_1, b_2 \in \mathbb{Z}$ the system of congruences

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

has a unique solution modulo $m_1 m_2$.

Proof. By EEA. $1 = sm_1 + tm_2$ for some $s, t \in \mathbb{Z}$.

$$sm_1 \equiv 1 \pmod{m_2} \Longrightarrow b_2 s m_1 \equiv b_2 \pmod{m_2}$$

We also have $b_2 s m_1 \equiv 0 \pmod{m_1}$

By analogy, $b_1 t m_2 \equiv b_1 \pmod{m_1}$

$b_1 t m_2 \equiv 0 \pmod{m_2}$

Add two numbers together:

$c := b_2 s m_1 + b_1 t m_2 \equiv b_1 \pmod{m_1}$

$c := b_2 s m_1 + b_1 t m_2 \equiv b_2 \pmod{m_2}$

Uniqueness: Assume we have another solution $c' = x$.

$$\begin{matrix} c \equiv c' \equiv b_1 \pmod{m_1} \\ c \equiv c' \equiv b_2 \pmod{m_2} \end{matrix} \Rightarrow \begin{matrix} c - c' \equiv 0 \pmod{m_1} \\ c - c' \equiv 0 \pmod{m_2} \end{matrix}$$

$\Rightarrow c - c' \equiv 0 \pmod{m_1 m_2}$ (by Principle 3)

$\Rightarrow c \equiv c' \pmod{m_1 m_2}$.

Check: any $x \equiv c \pmod{m_1 m_2}$ is a solution - Ex $\boxtimes$

The proof provides an algorithm for finding the solution of the system.

Example: $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$

(1) Start with the first two congruences.

$1 = 2 \cdot 3 - 1 \cdot 5$

the solution of the first two congruences is

$x \equiv 3 \cdot 2 \cdot 3 - 2 \cdot 1 \cdot 5 \equiv 8 \pmod{15}$

(2) Add the third congruence

$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 4 \pmod{7} \end{cases}$

$1 = 1 \cdot 15 - 2 \cdot 7$ (by guessing)

Then $x \equiv 4 \cdot 1 \cdot 15 - 8 \cdot 2 \cdot 7 \equiv 60 - 112 \equiv -52 \pmod{105}$

$\equiv 53 \pmod{105}$.

Chinese Remainder Theorem (Full version):
Let $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$ be pairwise coprime, i.e. $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Then for any $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ the following system

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

has a unique solution modulo $m_1 m_2 \cdot \ldots \cdot m_k$.

Proof: is based on two congruences version of CRT.

- The first two congruences are equivalent to $x \equiv c_2 \pmod{m_1 m_2}$ for some $c_2 \in \mathbb{Z}$.
- Add 3rd congruence.
  We have $\gcd(m_1 m_2, m_3) = 1$ (why?). Then

$$\begin{cases} x \equiv c_2 \pmod{m_1 m_2} \\ x \equiv b_3 \pmod{m_3} \end{cases} \iff x \equiv c_3 \pmod{m_1 m_2 m_3}$$

- Add 4th congruence and so on. $\boxtimes$

Example: $\begin{cases} 3x \equiv 4 \pmod{10} \\ 2x \equiv 5 \pmod{27} \end{cases}$

Simplify each congruence:

$3x \equiv 4 \pmod{10} \iff x \equiv 3^{-1} \cdot 4 \pmod{10}$

$3^{-1} \equiv 7 \pmod{10}$ (since $3 \cdot 7 = 21 \equiv 1 \pmod{10}$)

$2^{-1} \equiv 14 \pmod{\cancel{10}\ 27}$

$$\begin{cases} x \equiv 3^{-1} \cdot 4 \equiv 7 \cdot 4 \equiv 8 \pmod{10} \\ x \equiv 2^{-1} \cdot 5 \equiv 14 \cdot 5 \equiv 16 \pmod{27} \end{cases}$$

Now follow the algorithm from CRT.

Apply EEA:

$27 = 2 \cdot 10 + 7$
$10 = 1 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$

27	10	7	3	1
·	·	2	1	2
0	1	$\bar{2}$	3	$\bar{8}$
1	0	1	$\bar{1}$	3

Finally, $1 = 3\cdot 27 - 8\cdot 10$.

$\cancel{x \equiv 8\cdot 3\cdot 27 - 16\cdot 8\cdot 10 =}$

$$x = 8\cdot 3\cdot 27 - 16\cdot 8\cdot 10 = 648 - 1280 = -632 \pmod{270}$$
$$= 178 \pmod{270}.$$

§8. Computing powers in modular arithmetics

Q: ~~Com~~ How to compute $2^{2016} \pmod{\underset{37\cdot 47}{\overset{\parallel}{1739}}}$?

Approach 1 (naive). We start with $2^1 = 2$, then compute $2^2, 2^3, 2^4, 2^5, \dots, 2^{2016} \pmod{1739}$. It requires 2016 multiplications.

Approach 2 (Use Euler-Fermat Theorem):

$$\varphi(1739) = 36\cdot 46 = 1656.$$

So $2^{2016} = 2^{1656}\cdot 2^{360} \pmod{1739} \equiv 2^{360} \pmod{1739}$.

Then it will require 360 multiplications.