Recall: The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a,m) \mid b$. When $(a,m) \mid b$, the set of all solutions is $\{x \in \mathbb{Z} : x_0 + t \cdot \frac{m}{(a,m)}, t \in \mathbb{Z}\}$ which is same as $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{(a,m)}}\}$, where x_0 is just one of the solutions.

We can find x_0 using Euclid's algorithm:

$$ax \equiv b \pmod{m} \Rightarrow ax = mk + b \Rightarrow ax - mk = b$$

Inverse in $\mathbb{Z}_n$: For an a, is there an x such that $ax \equiv 1 \pmod{n}$?

- Only when $(a,n) \mid 1$, i.e $(a,n) = 1$. x is called the inverse of a modulo n, and we write $x \equiv a^{-1} \pmod{n}$.

To solve $ax \equiv b \pmod{n}$ with $(a,n) = 1$:

$$ax \equiv b \pmod{n} \Longleftrightarrow a^{-1} \cdot a \cdot x \equiv a^{-1} \cdot b \pmod{n}$$

$$\Longleftrightarrow x \equiv a^{-1} \cdot b \pmod{n}.$$

Exercise: $(a,n) = 1 \Rightarrow (a^{-1}, n) = 1$.

Also $(a^{-1})^{-1} \equiv a \pmod{n}$.

Some Terminology: In the previous lecture we solved $9x \equiv 6 \pmod{12}$.

Answer: $\{x \in \mathbb{Z} : x = 2 + 4t,\ t \in \mathbb{Z}\}$

$= \{x \in \mathbb{Z} : x \equiv 2 \pmod 4\}$

Question: Solve $9x \equiv 6 \pmod{12}$ in $\mathbb{Z}_{12}$.

$x \equiv 2 \pmod 4$: ......, $2, 6, 10, 14, 18, 22, 26, \ldots.$

$\Rightarrow x \equiv 2, 6, 10 \pmod{12}$

Question: Solve $x \equiv 1 \pmod 3$ in $\mathbb{Z}_9$?

$x = 3k + 1$. Write $k = 3\ell + r$ with $0 \leqslant r \leqslant 2$,

$\Rightarrow x = 3 \cdot (3\ell + r) + 1 = 9\ell + 3r + 1$

$\Rightarrow x \equiv 1, 4,$ or $7 \pmod 9$.

Question: Can we solve $x \equiv 1 \pmod 6$ in $\mathbb{Z}_8$?

Is 7 in $\mathbb{Z}_8$ (i.e. $[7]_8$) a solution or not?

- $7 \equiv 1 \pmod 6 \Rightarrow$ it should be a solution
- $[7]_8 = [15]_8$ and $15 \not\equiv 1 \pmod 6 \Rightarrow$ maybe not.

So, we cannot solve $x \equiv 1 \pmod 6$ in $\mathbb{Z}_8$.

In general, when does it make sense to solve $x \equiv a \pmod{m}$ in $\mathbb{Z}_n$?

- We should have $b \equiv c \pmod{n} \Rightarrow b \equiv c \pmod{m}$,
  i.e. $n \mid b-c \Rightarrow m \mid b-c$.
  Only when $m \mid n$.

Simultaneous Linear Congruences

Easier case: Which integers x satisfy both $x \equiv 1 \pmod{2}$ and $x \equiv 1 \pmod{5}$?

- We can solve $x \equiv 1 \pmod{2}$ in $\mathbb{Z}_n$ for $2 \mid n$.
- We can solve $x \equiv 1 \pmod{5}$ in $\mathbb{Z}_n$ for $5 \mid n$.

$\Rightarrow$ We should expect a solution in $\mathbb{Z}_{10}$.

$2 \mid x-1$ and $5 \mid x-1 \iff 10 \mid x-1 \iff x \equiv 1 \pmod{10}$

What about $x \equiv 2 \pmod{4}$, $x \equiv 2 \pmod{6}$, $x \equiv 2 \pmod{15}$?

$$4 \mid x-2,\ 6 \mid x-2,\ 15 \mid x-2 \iff \underbrace{[4,6,15]}_{=60} \mid x-2$$

$\iff x \equiv 2 \pmod{60}$.

Theorem: $x \equiv a \pmod{m_1}, x \equiv a \pmod{m_2}, \ldots, x \equiv a \pmod{m_k}$ is equivalent to $x \equiv a \pmod{m}$ where $m = [m_1, m_2, \ldots, m_k]$.
(Special case: $(m_i, m_j) = 1$ for all $i \neq j$ and $m = m_1 m_2 \cdots m_k$)

- If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then working with $m_i = p_i^{\alpha_i}$ might be extremely useful.

e.g. To prove x is divisible by 120 ($x \equiv 0 \pmod{\underset{2^3 \cdot 3^1 \cdot 5^1}{\overset{\|}{120}}}$), we can show that x is divisible by all of $8, 3$, and 5.

Next, we make our problem a little bit harder.

Which integers x satisfy both $x \equiv 1 \pmod 5$ and $x \equiv 5 \pmod 7$?

We should expect to find a solution in $\mathbb{Z}_{35}$.

$5k+1$ $\quad$ $k = 7\ell + r$

$x \equiv 1 \pmod 5 \Rightarrow x \equiv 1, 6, 11, 16, 21, 26, 31 \pmod{35}$

$x \equiv 5 \pmod 7 \Rightarrow x \equiv 5, 12, 19, 26, 33, 40 \pmod{35}$

$\Rightarrow x \equiv 26 \pmod{35}$

What about $x \equiv 1 \pmod{10}$, $x \equiv 5 \pmod{14}$?

$[10, 14] = 70$

$x \equiv 1 \pmod{10} \Rightarrow x \equiv 1, 11, 21, 31, 41, 51, 61 \pmod{70}$

$x \equiv 5 \pmod{14} \Rightarrow x \equiv 5, 19, 33, 47, 61 \pmod{70}$

$\Rightarrow x \equiv 61 \pmod{70}$.

What about $x \equiv 1 \pmod{10}$, $x \equiv 4 \pmod{14}$?

$[10, 14] = 70$

$x \equiv 1 \pmod{10} \Rightarrow x \equiv 1, 11, 21, 31, 41, 51, 61 \pmod{70}$

$x \equiv 4 \pmod{14} \Rightarrow x \equiv 4, 18, 32, 46, 60 \pmod{70}$

$\Rightarrow$ No solution.

$x \equiv 1 \pmod{10} \Rightarrow x$ is odd

$x \equiv 4 \pmod{14} \Rightarrow x$ is even.

We should be careful about this kind of compatibility issues in the linear congruences. The congruences above were not compatible in $\mathbb{Z}_2$ ($2 \mid 10$ and $2 \mid 14$) and we won't have such a problem if we work with pairwise coprime moduli.

Chinese Remainder Theorem: (pairwise coprime moduli)

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $\dots$, $x \equiv a_k \pmod{m_k}$ with $(m_i, m_j) = 1$ for all $i \neq j$ has a unique solution $x \equiv a \pmod{m_1 m_2 \cdots m_k}$ in $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ for some a.

- Let's see an example with $k=2$: $x \equiv 2 \pmod{15}$ and $x \equiv 3 \pmod{7}$.

$x \equiv 3 \pmod{7} \Rightarrow x = 7k+3$. Now, we solve $7k+3 \equiv 2 \pmod{15}$

$\Rightarrow 7k \equiv -1 \pmod{15} \Rightarrow 7k \equiv 14 \pmod{15} \Rightarrow k \equiv 2 \pmod{15}$.

Write $k = 15\ell + 2$ and $x = 7k + 3 = 7\cdot(15\ell + 2) + 3$

$$= 105\ell + 17$$

So, $x \equiv 17 \pmod{105}$.

<u>Proof:</u> We'll prove by induction on k.

$k = 1$: trivial

$k = 2$: similar to the example given above.

$x \equiv a_1 \pmod{m_1} \Rightarrow x = c \cdot m_1 + a_1$.

$cm_1 + a_1 \equiv a_2 \pmod{m_2} \Rightarrow cm_1 \equiv a_2 - a_1 \pmod{m_2}$.

Since $(m_1, m_2) = 1$, there is an $m_1^{-1} \pmod{m_2}$.

Then $cm_1 \cdot m_1^{-1} \equiv (a_2 - a_1) \cdot m_1^{-1} \pmod{m_2}$

$\Rightarrow c \equiv (a_2 - a_1) \cdot m_1^{-1} \pmod{m_2} \Rightarrow c = \ell \cdot m_2 + (a_2 - a_1) \cdot m_1^{-1}$

$\Rightarrow x = (\ell \cdot m_2 + (a_2 - a_1) \cdot m_1^{-1}) \cdot m_1 + a_1$

$$= \ell \cdot m_1 m_2 + \boxed{(a_2 - a_1) \cdot m_1^{-1} \cdot m_1 + a_1} \longrightarrow a \pmod{m_1 m_2}.$$

Assume CRT is true for some k and consider it for $k+1$.

Using base case, combine the last two congruences and apply the induction hypothesis for the remaining congruences.

$(m_1, m_2, \ldots, m_{k-1}, m_k, m_{k+1}) \longrightarrow (m_1, m_2, \ldots, m_{k-1}, m_k \cdot m_{k+1})$.

What if we don't have $(m_i, m_j) = 1$?

- Split each $(\text{mod } m_i)$ into some $(\text{mod } p^\alpha)$ using prime factorisations

- For each prime, gather all congruences like $(\text{mod } p^\alpha)$. They will be either incompatible or they can be reduced to a single congruence.

highest power of p

- look at $(\text{mod } p^\alpha)$ with largest α. Other congruences might be incompatible with this one or they will be redundant.

- If everything is compatible, then solve the congruences $(\text{mod } p^\alpha)$ using CRT. If at least one of them is incompatible, then there is no solution.

We'll see some examples on wednesday.