Chinese Remainder Theorem

Suppose $\gcd(n,m) = 1$.

Then $f: \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$$(a \bmod nm) \longmapsto (a \bmod n, a \bmod m)$$

is a bijection.

Proof (Constructive)

Suppose we wish to solve

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

There exist integers s and t s.t.

$$ns + mt = 1 \qquad (*)$$

(this exists by Extended Euclidean Algorithm, since $\gcd(n,m) = 1$.)

So from $(*)$

$$ns \equiv 1 \pmod m$$
$$mt \equiv 1 \pmod n$$

Take

$$x = ans + bmt$$

Then

$$x \equiv ans \equiv a \pmod m$$
$$x \equiv bmt \equiv b \pmod n.$$

∎

Example. Find x s.t. $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$

(check: $\gcd(5,7) = 1$ ✓)

Solve $7s + 5t = 1$.

Answer: $s = 3,\ t = -4$.

or $s = -2,\ t = 3$

aside

aside. (diff: $7(5) + 5(-7) = 0$)

Let $x = 2(7 \cdot 3) + 3(5(-4)) \pmod{35}$

$= 42 - 60$

$= -18$

$= 17$

Check: ✓

$17 \equiv 2 \pmod 5$

$17 \equiv 3 \pmod 7$

Important note:

If $x \equiv a \pmod{mk}$ then $x \equiv a \pmod{m}$.

So we have maps

$$\mathbb{Z}/mk\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$a \bmod mk \longmapsto a \bmod m$$

This map is many-to-1.

"fibre" = preimage of a = "lifts" of a

- $a + (k-1)m$
- $\vdots$
- $a + 2m$
- $a + m$
- a
- $\downarrow$
- a

$\mathbb{Z}/mk\mathbb{Z}$ $\downarrow$ $\mathbb{Z}/m\mathbb{Z}$

Ex.

	4	5
	2	3
3 is a lift to $\mathbb{Z}/6\mathbb{Z}$	0	1
$\downarrow$	$\downarrow$	$\downarrow$
of $1 \in \mathbb{Z}/2\mathbb{Z}$.	0	1

$\mathbb{Z}/6\mathbb{Z}$ $\downarrow$ $\mathbb{Z}/2\mathbb{Z}$

Example. CRT says $a \bmod m$ has exactly one lift $x \bmod mn$ satisfying $x \equiv b \pmod{n}$

CRT
$\rightarrow x \equiv a \pmod{m}$
$\Rightarrow x \equiv b \pmod{n}$

Example. Solve $x^2 \equiv 1 \pmod{35}$. $35 = \underline{5} \cdot \underline{7}$.

$\gcd(5,7) = 1$

$\overset{\text{CRT}}{\iff}$ Solve $\begin{cases} x^2 \equiv 1 \pmod 5 \\ x^2 \equiv 1 \pmod 7 \end{cases}$

$\iff$ (since prime modulus) $\begin{cases} x \equiv \pm 1 \pmod 5 \\ x \equiv \pm 1 \pmod 7 \end{cases}$

$\iff \begin{pmatrix} x \equiv 1 & (5) \\ x \equiv 1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv 1 & (5) \\ x \equiv -1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv -1 & (5) \\ x \equiv 1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv -1 & (5) \\ x \equiv -1 & (7) \end{pmatrix}$

$\downarrow$ CRT

$\overset{\text{CRT}}{\iff}$ ($\times 4$) $x \equiv 1 \pmod{35}$ or $x \equiv 6 \pmod{35}$ or $x \equiv 29 \pmod{35}$ or $x \equiv 34 \pmod{35}$

$\equiv -6$ (CRT $\leftarrow -1$)

Answer: $x \equiv 1, 6, 29, 34 \pmod{35}$

Example. Solve $x^2 \equiv 1 \pmod{35}$. $35 = 5 \cdot 7$. $\gcd(5,7) = 1$

$\overset{\text{CRT}}{\iff}$ Solve $\begin{cases} x^2 \equiv 1 \pmod 5 \\ x^2 \equiv 1 \pmod 7 \end{cases}$

$\iff$ (since prime modulus) $\begin{cases} x \equiv \pm 1 \pmod 5 \\ x \equiv \pm 1 \pmod 7 \end{cases}$

$\iff \begin{pmatrix} x \equiv 1 & (5) \\ x \equiv 1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv 1 & (5) \\ x \equiv -1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv -1 & (5) \\ x \equiv 1 & (7) \end{pmatrix}$ or $\begin{pmatrix} x \equiv -1 & (5) \\ x \equiv -1 & (7) \end{pmatrix}$

$\downarrow$ CRT

$\overset{\text{CRT}}{\iff}$ ($\times 4$) $x \equiv 1 \pmod{35}$ or $x \equiv 6 \pmod{35}$ or $x \equiv 29 \pmod{35}$ $\equiv -6$ or $x \equiv 34 \pmod{35}$

Answer: $x \equiv 1, 6, 29, 34 \pmod{35}$

$x \equiv -1 \ (5)$, $x \equiv 1 \ (7)$

Solve $5s + 7t = 1$. $s = 3, t = -2$ → tells us $5s \equiv 1 \pmod 7$, $7t \equiv 1 \pmod 5$

Then $x = 5s - 7t$.

$= 5 \cdot 3 - 7(-2)$

$= 15 + 14 = 29$.

Usefulness of Extended Euclidean Algorithm

(1) CRT
⇒ proving the formula for $\varphi(n)$ ⟸

(2) Solving linear Diophantine equations $ax+by=c$.

(3) Finding modular inverses & solving linear congruences
$ax \equiv 1 \pmod n$ (linear equations mod n).

Thm. If $\gcd(m,n)=1$ then $\boxed{\varphi(mn)=\varphi(m)\varphi(n)}$

Recall: $\varphi(n) = \#\{0<a<n : a \text{ is invertible mod } n\}$ $\quad(\Leftrightarrow \gcd(a,n)=1.)$

$$= |(\mathbb{Z}/n\mathbb{Z})^*|$$

Pf. Suppose $a \in \mathbb{Z}/mn\mathbb{Z}$.

a is invertible mod mn $\iff$ $ax \equiv 1 \pmod{mn}$ has solution

$\overset{\text{CRT}}{\iff}$ $\begin{cases} ax \equiv 1 \pmod m \\ ax \equiv 1 \pmod n \end{cases}$ has solution

$\iff$ a is invertible mod m and mod n.

$(\mathbb{Z}/mn\mathbb{Z})^*$ in bijection w/ $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

$\Rightarrow$ $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Thm. If $\gcd(m,n)=1$ then $\boxed{\varphi(mn)=\varphi(m)\varphi(n)}$

Recall: $\varphi(n) = \#\{0<a<n : a \text{ is invertible mod } n\}$ $\quad(\Leftrightarrow \gcd(a,n)=1.)$

$$= |(\mathbb{Z}/n\mathbb{Z})^*|$$

Pf. Suppose $a \in \mathbb{Z}/mn\mathbb{Z}$.

a is invertible mod mn $\iff$ $ax \equiv 1 \pmod{mn}$ has solution

$\overset{\text{CRT}}{\iff}$ $\begin{cases} ax \equiv 1 \pmod m \\ ax \equiv 1 \pmod n \end{cases}$ has solution

$\iff$ a is invertible mod m and mod n.

$(\mathbb{Z}/mn\mathbb{Z})^*$ in bijection w/ $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

$\Rightarrow$ $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

What is $\varphi(p^k)$ for a prime p?

In other words, how many $0 < x < p^k$ are coprime to p?

How many are <u>not</u>? The multiples of p!

$$\frac{p^k}{p} = p^{k-1}.$$

(every p^{th} residue)

So $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

$\{0, 1, \ldots, p^k - 1\}$ $\quad$ $\{0, p, 2p, 3p \ldots, (p^{k-1})p\}$

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_m^{e_m})$$

<u>Ex.</u>

$\varphi(45)$

$= \varphi(3^2 \cdot 5)$

$= \varphi(3^2)\varphi(5)$

$= 3(3-1)(5-1)$

$= 3 \cdot 2 \cdot 4$

$= 24$