Chinese remainder theorem

m_1, m_2 rel. prime

$m = m_1 m_2 \qquad m_1 | m \ , \ m_2 | m$

$$\mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1}$$
$$[a]_m \longmapsto [a]_{m_1}$$

$$\theta : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \qquad \text{homom. of rings.}$$
$$[a]_m \longmapsto ([a]_{m_1}, [a]_{m_2})$$

$$\ker \theta = \{ [a]_m \mid m_1 | a, \ m_2 | a \}$$
$$= \{ [a]_m \mid m_1 m_2 | a \} \qquad m = m_1 m_2$$
$$= \{ [0]_m \}$$

$\rightsquigarrow$ θ IS INJECTIVE

but $|\mathbb{Z}_m| = |\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}| = m$

$\rightsquigarrow$ θ is surjective too $\rightsquigarrow$ θ ISOMORPHISM.

Consequence: if $a, b \in \mathbb{Z}$ then $\exists x \in \mathbb{Z}$ s.t.

$$\theta([x]_m) = ([a]_{m_1}, [b]_{m_2})$$

that is the system of equations

$$\begin{cases} x \equiv a \mod m_1 \\ x \equiv b \mod m_2 \end{cases}$$

admits a solution.

CRT: if $m_1, \dots, m_k$ are integers s.t. $\gcd(m_i, m_j) = 1$ if $i \neq j$ then for every $a_1, \dots, a_k \in \mathbb{Z}$ the system

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

admits a solution, unique modulo $m_1 m_2 \dots m_k$.

Example

$$\begin{cases} x \equiv 5 \mod 13 \leftarrow \\ x \equiv 7 \mod 19 \leftarrow \end{cases}$$

$\gcd(13, 19) = 1 \rightsquigarrow$ apply CRT

The general solution of the first eq is

$x \equiv 5 + 13k$

Substituting in the second eq.

$5 + 13k = 7 \mod 19$

$5 + 13k = 7 + 19h$ for some $h \in \mathbb{Z}$

$13k - 19h = 2 \rightsquigarrow$ diophantine linear equation in two variables

$\rightsquigarrow \quad x \equiv 83 \mod 13 \cdot 19$

Exercise

Solve the system

$$\begin{cases} x \equiv 4 & \mod 11 \\ x \equiv 5 & \mod 13 \\ x \equiv 1 & \mod 17. \end{cases}$$

Corollary : Isomorphism of mult. gps

$$\mathbb{Z}_m^\times \simeq \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times \quad \underline{\underline{\text{if}}} \quad \gcd(m_1, m_2) = 1.$$

Definition For every $m \geq 1$ we define

$$\varphi(m) = |\mathbb{Z}_m^\times| \quad \text{Euler } \varphi \text{ function}$$

$\varphi(1) = 1$

$\varphi(p) = p - 1$ if p is prime

$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$ if $\gcd(m_1, m_2) = 1$

$\hookrightarrow$ φ is multiplicative

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

$\varphi(p^n) = |\mathbb{Z}_{p^n}^\times|$

$\mathbb{Z}_{p^n}^\times = \{ \bar{a} \in \mathbb{Z}_{p^n} \mid p \nmid a \}$

$\mathbb{Z}_{p^n} = \{ \bar{0}, \bar{1}, \bar{2}, \ldots \quad p^n - 1 \}$

Multiples of p between 0 and $p^n - 1$

$0, p, 2p, 3p, \dots, (p^{n-1}-1)p$

They are p^{n-1}

$\rightsquigarrow \quad |\mathbb{Z}_{p^n}^{\times}| = p^n - p^{n-1} = p^{n-1}(p-1)$

$$\varphi(p^n) = p^{n-1}(p-1)$$

<u>Consequence</u>: for every $n > 0$

if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ $\quad p_i$ primes distinct

then

$$\boxed{\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p-1)}$$

<u>Example</u>

$n = 360 = 2^3 \cdot 3^2 \cdot 5$

$\varphi(n) = \varphi(2^3)\,\varphi(3^2)\,\varphi(5)$ $\qquad \varphi(2^3) = 2^{3-1}(2-1)$

$= 4 \cdot 6 \cdot 4$ $\qquad = 4$

$= 96.$ $\qquad \varphi(3^2) = 3(3-1)$

$\mathbb{Z}_n^{\times}$ is a group.

if G is a finite group and $|G| = N$

then $x^N = e \quad \forall x \in G$

Then $\forall\ [a]_m \in \mathbb{Z}_m^\times$ we have

$$[a]_m^{\varphi(m)} = [1]_m \quad \text{in } \mathbb{Z}_m^\times$$

EULER IDENTITY

that is $\forall a \in \mathbb{Z}$ if $\gcd(a,n) = 1$ then

$$a^{\varphi(n)} \equiv 1 \mod n$$

(LTF is a particular instance)

If we have to calculate $a^M \mod m$

and $\gcd(a, m) = 1$

$$a^{\varphi(n)} \equiv 1 \mod m$$

Consider the remainder of the division of M by $\varphi(m)$

$$M = q\varphi(m) + r \qquad 0 \leq r < \varphi(m)$$

$$a^M = a^{\varphi(m)\cdot q + r} = \big(\underbrace{a^{\varphi(m)}}_{\equiv 1}\big)^q \cdot a^r \equiv a^r \mod N$$

<u>Example</u>

Want to find the last two digits in the decimal representation of 3^{256}.

$\rightsquigarrow$ find the canonical representative of

$3^{256} \mod 100$

$\gcd(3, 100) = 1 \rightsquigarrow 3^{\varphi(100)} \equiv 1 \mod 100$

$\varphi(100) = 40$

$100 = 5^2 \cdot 2^2$

$\varphi(100) = 40$

$256 = 40 \cdot 6 + 16$

$$3^{256} = \underbrace{(3^{40})^6}_{\equiv 1} \cdot 3^{16} \equiv 3^{16} \mod 100$$

$3^2 \equiv 9 \mod 100$

$3^4 \equiv 81$ "

$3^8 \equiv 81^2 \equiv 61 \mod 100$

$3^{16} \equiv 61^2 \equiv 21 \mod 100$.

Structure of $\mathbb{Z}_n^\times$

$\mathbb{Z}_n^\times$ is not in general cyclic

$$\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

Thm. $\mathbb{Z}_n^\times$ cyclic $\iff$ $n = 2, 4, p^k, 2p^k$

$k \geq 0$

p odd prime