Chinese Reminder Theorem: 7.9.20

If $n_1, n_2, \dots n_k$ pairwise coprime positive integers, i.e. $(n_i, n_j) = 1$ for $i \neq j$, then there is unique x modulo product

$$N = n_1 n_2 \cdots n_k$$

for satisfying any given residues $a_1, a_2, \dots a_k$ such that

$$a_i = x \bmod n_i \quad i = 1, 2, \dots k.$$

Example: Let $n_1 = 2$, $n_2 = 3$, $n_3 = 5$. and $a_1 = 1$, $a_2 = 1$, $a_3 = 2$. Find x such that

$$1 = x \bmod 2 \quad (1)$$
$$1 = x \bmod 3 \quad (2)$$
$$2 = x \bmod 5 \quad (3)$$

(1) $\Rightarrow$ x is odd. Let $x = 2m+1$ $m \neq 0, 1, \dots$

(2) $\Rightarrow$ $2m+1 = 1 \bmod 3$

$\Leftrightarrow$ $2m = 0 \bmod 3$ $\Leftrightarrow$ $m = \frac{3}{2} n$ n-even.

let $n = 2r$, then $m = 3r$.

(3) $\rightarrow$ $2 = 6r+1 \bmod 5$

$\Leftrightarrow$ $6r - 1 = 0 \bmod 5$

for $r = 1$ $6r - 1 = 0 \bmod 5$

$\Rightarrow$ $m = 3$, $x = 7$. Next $r = 6$ for which $x = 37 > (2 \cdot 3 \cdot 5) = 30$

Mo. / Day / Yr. _____ day

Event: _____

Venue:

CRT: General Algorithm & Proof

$n_1 \; n_2 \; \cdots \; n_k$

given numbers $(n_i, n_j) = 1$ for $i \neq j$.

Define: $N = \prod_{i=1}^{k} n_i$

$$N_i = \frac{N}{n_i}$$

$a_i = x \bmod n_i$ Given Congruences

$N_i \bmod n_j = 0$ for $j \neq i$. since $(n_i, n_j) = 1$

$N_i \bmod n_i \neq 0$ ✗

Hence

$$a_i N_i N_i^{-1} \bmod n_i = a_i$$

Consider

$$x = \left(\sum_{i=1}^{k} a_i N_i N_i^{-1} \bmod n_i \right) \bmod N$$

Then x is the unique number in $[0, N)$ which satisfies the given congruences.

Mo. / Day / Yr. _____ day

Event: _____

Venue:

Structure of $\mathbb{Z}_N$ $\mathbb{Z}_N^*$

Given $a_i = x \bmod n_i$

where n_i are pairwise coprime.

For any $x \in \mathbb{Z}_N$ $a_i = x \bmod n_i \in \mathbb{Z}_{n_i}$

Hence we have the map

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

$$x \longmapsto (a_1 \ a_2 \ \cdots \ a_k)$$

Let $\phi(x) = (a_1 \ a_2 \ \cdots a_k)$

If $y \in \mathbb{Z}_N$ and $b_i = y \bmod n_i$

then $\phi(x+y) = (x+y)_{\mathbb{Z}_N} \bmod n_i$

$$= a_i + b_i \bmod n_i$$

$$= \phi(x) + \phi(y).$$

$$\phi(xy) = (xy)_{\mathbb{Z}_N} \bmod n_i$$

$$= a_i b_i \bmod n_i$$

Since there is unique x for each

$(a_1 \ a_2 \cdots a_k)$

$\phi(\cdot)$ is 1-1 (Homomorphism of rings) additively and (Homomorphism of groups) multiplicatively.

Hence CRT proves that

$$\mathbb{Z}_N \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \cdots \times \mathbb{Z}_{n_k}^*$$

as isomprphisms of rings and groups.

Application of these isomorphisms in computation of $\phi(n)$ is described in the note Euclidean Division.