

Chinese Remainder Theorem

Around 100 A.D., a Chinese mathematician solved the problem of finding an integer x , that satisfied

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$x = 23$ is one solution, but so is $23 + 105k$, for all $k \in \mathcal{Z}$. The method of general solution goes under the name the “Chinese Remainder Theorem.”

Let $n = \prod_{i=1}^k n_i$, where $\gcd(n_i, n_j) = 1$, for $i \neq j$, then we will study the structure of \mathcal{Z}_n and see it to be the Cartesian product of

$$\mathcal{Z}_{n_1} \times \mathcal{Z}_{n_2} \times \cdots \times \mathcal{Z}_{n_k}$$

This lets us work in the smaller groups, and piece the solution to the larger group up from them. This often saves considerable computing time.

- **Theorem:**(Chinese Remainder) Let $n = \prod_{i=1}^k n_i$, where $\gcd(n_i, n_j) = 1$, for $i \neq j$, and consider the correspondence:

$$a \longleftrightarrow (a_1, a_2, \dots, a_k)$$

$$a \in \mathcal{Z}_n, a_i \in \mathcal{Z}_{n_i}, \text{ and}$$

$$a_i = a \pmod{n_i}, \text{ for } i = 1, 2, \dots, k$$

The this mapping is one-to-one and onto from \mathcal{Z}_n to $\mathcal{Z}_{n_1} \times \mathcal{Z}_{n_2} \times \cdots \times \mathcal{Z}_{n_k}$, and if also we have

$$b \longleftrightarrow (b_1, b_2, \dots, b_k)$$

we get

$$(a * b) \pmod{n} = (a_1 * b_1 \pmod{n}, \dots, a_k * b_k \pmod{n})$$

where $*$ means addition, subtraction, and multiplication.

Proof: Given a , we compute $a_i \equiv a \pmod{n_i}$

Given the a_i 's, we obtain a as

$$a \equiv \sum_{i=1}^k a_i c_i \pmod{n} \text{ with} \\ c_i = m_i(m_i^{-1} \pmod{n_i}) \text{ with } m_i = n/n_i$$

Thus $m_i \equiv 0 \pmod{n_j}$ for $i \neq j$

Note: $\gcd(n_i, n_j) = 1$ so $m_i^{-1} \pmod{n_i}$ is well defined. Also

$$c_j \equiv \delta_{ij} \pmod{n_i} \text{ so } c_i \longleftrightarrow (0, 0, \dots, 0, 1, 0, \dots, 0)$$

where i is in the i th place

Thus the c_i 's form the "basis."

$$\begin{aligned} a &\equiv a_i c_i \pmod{n_i} \\ &\equiv a_i m_i(m_i^{-1} \pmod{n_i}) \pmod{n_i} \\ &\equiv a_i \pmod{n_i} \end{aligned}$$

This establishes the result. ■

- **Corollary:** If n and n_i are as above, then for all $a_1, a_2, \dots, a_k \in \mathcal{Z}_n$, $x \equiv a_i \pmod{n_i}$ for $i = 1, 2, \dots, k$ has a unique solution modulo n .
- **Corollary:** If n and n_i are as above, then for all a and $x \in \mathcal{Z}_n$, $x \equiv a \pmod{n_i}$ for $i = 1, 2, \dots, k$, if and only if $x \equiv a \pmod{n}$
- Example:

$$\begin{aligned} a &\equiv 2 \pmod{5} \\ a &\equiv 3 \pmod{13} \end{aligned}$$

$$a_1 = 2, n_1 = m_1 = 5, a_2 = 3, n_2 = m_2 = 13, n = 65$$

Also $13^{-1} \equiv 2 \pmod{5}$ and $5^{-1} \equiv 8 \pmod{13}$

$$c_1 = 13 \cdot 2 = 26, c_2 = 5 \cdot 8 = 40,$$

$$\begin{aligned} a &\equiv 2 \cdot 26 + 3 \cdot 40 \pmod{65} \\ &\equiv 172 \pmod{65} \\ &\equiv 42 \pmod{65} \end{aligned}$$

This example shows the Chinese remainder theorem in action.

	0	1	2	3	4	5	6	7	8	9	10
0	0	40	15	55	30	5	45	20	60	35	10
1	26	1	41	16	56	31	6	46	21	61	36
2	52	27	2	42	17	57	32	7	47	22	62
3	13	53	28	3	43	18	58	33	8	48	23
4	39	14	54	29	4	44	19	59	34	9	49

Figure 1: An illustration for the Chinese remainder theorem for $n_1 = 5$ and $n_2 = 13$. For this example, $c_1 = 26$ and $c_2 = 40$. In row i , column j is shown the value of a , modulo 65, such that column 12 contains a 64 (equivalent to -1).