Discrete Mathematics

Chinese remainder theorem, CRT map, Euler's Phi function, group

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Chinese Remainder Theorem

THEROEM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise relatively prime and let $n = n_1 \cdots n_k$. Then for any $b_1, \ldots, b_k \in \mathbb{Z}$, then the system

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

always has a solution. Furthermore, if $b \in \mathbb{Z}$ is a solution, then any solution x must satisfy $x \equiv b \pmod{n}$.

- Let $N_i = n/n_i$ for every $i \in [k]$.
  - $\gcd(N_i, n_i) = 1$ for every $i \in [k]$.
  - $\exists\, s_i, t_i, N_i s_i + n_i t_i = 1$.
- Let $b = b_1(N_1 s_1) + \cdots + b_k(N_k s_k)$.
  - Then $b \equiv b_i \pmod{n_i}$ for every $i \in [k]$.

- $x \equiv b_i \pmod{n_i}$ for all i
  $\Rightarrow x \equiv b \pmod{n_i}$ for all i
  $\Rightarrow n_i \mid (x - b)$ for all i
  $\Rightarrow (n_1 n_2 \cdots n_k) \mid (x - b)$
  $\Rightarrow x \equiv b \pmod{n}$

Solution to Sun-Tsu's Question

EXAMPLE: Solve the system $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5. \\ x \equiv 2 \pmod 7 \end{cases}$

- $n_1 = 3, n_2 = 5, n_3 = 7;\ n = n_1 n_2 n_3 = 105;\ b_1 = 2, b_2 = 3, b_3 = 2$
  - $N_1 = n_2 n_3 = 35, N_2 = n_1 n_3 = 21, N_3 = n_1 n_2 = 15$
  - $12\, n_1 - N_1 = 1; -4 n_2 + N_2 = 1; -2\, n_3 + N_3 = 1$
  - $t_1 = 12, s_1 = -1; t_2 = -4, s_2 = 1; t_3 = -2, s_3 = 1$
- $b = b_1(N_1 s_1) + b_2(N_2 s_2) + b_3(N_3 s_3)$

  $= 2\,(-35) + 3\,(21) + 2(15)$

  $= 23$
- $x \in \mathbb{Z}$ is a solution of the system iff $x \equiv 23 \pmod{105}$
  - Solutions: $[23]_{105}$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$ is a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- ***θ* is well-defined**, i.e., $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
  - $[x]_n = [y]_n$
  - $x \equiv y \pmod{n}$
  - $x \equiv y \pmod{n_i}$ for every $i \in [k]$;
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$
    $= \left([y]_{n_1}, \ldots, [y]_{n_k}\right)$
    $= \theta([y]_n)$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$ is a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- ***θ* is injective**, i.e., $\theta([x]_n) = \theta([y]_n) \Rightarrow [x]_n = [y]_n$
  - $\theta([x]_n) = \theta([y]_n)$
  - $\left([x]_{n_1}, \ldots, [x]_{n_k}\right) = \left([y]_{n_1}, \ldots, [y]_{n_k}\right)$
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $n_i | (x - y)$ for every $i \in [k]$
  - $n | (x - y)$
  - $[x]_n = [y]_n$
- ***θ* is surjective,** i.e., every element in $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ has a preimage
  - This is obvious, because $|\mathbb{Z}_n| = \left|\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}\right|$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

- **θ is well-defined**:
  - show that $\theta([x]_n) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ for every $[x]_n \in \mathbb{Z}_n^*$
    - $[x]_n \in \mathbb{Z}_n^*$
    - $\gcd(x, n) = 1$
    - $\gcd(x, n_i) = 1$ for every $i \in [k]$
    - $[x]_{n_i} \in \mathbb{Z}_{n_i}^*$ for every $i \in [k]$
  - show that $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
    - see the previous theorem
- **θ is injective**: see the previous theorem

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = \left([x]_{n_1}, \ldots, [x]_{n_k}\right)$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

- ***θ* is surjective**: Let $\left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Preimage?
  - Due to CRT, the system $x \equiv b_i \pmod{n_i}$, $i = 1, \ldots, k$, has a solution b
  - $b \equiv b_i \pmod{n_i}$ for all $i \in [k]$
  - Since $[b_i]_{n_i} \in \mathbb{Z}_{n_i}^*$, $\gcd(b, n_i) = 1$ for all $i \in [k]$
  - $\gcd(b, n_1 n_2 \cdots n_k) = 1$
  - $\theta([b]_n) = \left([b]_{n_1}, \ldots, [b]_{n_k}\right) = \left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right)$
  - $[b]_n$ is a preimage of $\left([b_1]_{n_1}, \ldots, [b_k]_{n_k}\right)$

Euler's Phi Function

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise relatively prime. Let $n = n_1 \cdots n_k$. Then $\phi(n) = \phi(n_1) \cdots \phi(n_k)$.

- θ: $\mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ is bijective
- $\phi(n) = \phi(n_1) \times \cdots \times \phi(n_k)$

COROLLARY: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and integers $e_1, \ldots, e_k \geq 1$, then $\phi(n) = n(1 - p_1^{-1}) \cdots \left(1 - p_k^{-1}\right)$.

- $\phi(n) = \phi\left(p_1^{e_1}\right) \cdots \phi\left(p_k^{e_k}\right)$
  $= n(1 - p_1^{-1}) \cdots \left(1 - p_k^{-1}\right)$

EXAMPLE: $\phi(10) = \phi(2)\phi(5) = 4; n = 10; n_1 = 2, n_2 = 5$

- θ: $\mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$
  - $1 \mapsto (1,1)$; $3 \mapsto (1,3)$; $7 \mapsto (1,2)$; $9 \mapsto (1,4)$

$(\mathbb{Z}_n, +)$

EXAMPLE: For $n \in \mathbb{Z}^+$, $\mathbb{Z}_n$ and $+$ satisfy the following properties.

- **Closure**: $[a]_n + [b]_n \in \mathbb{Z}_n$
  - $[a]_n + [b]_n = [a + b]_n \in \mathbb{Z}_n$
- **Associative**: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$
  - $$([a]_n + [b]_n) + [c]_n = [a + b]_n + [c]_n = [(a + b) + c]_n$$
    $$= [a + (b + c)]_n = [a]_n + [b + c]_n$$
    $$= [a]_n + ([b]_n + [c]_n)$$
- **Identity**: $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$
  - $[a]_n + [0]_n = [a + 0]_n = [0 + a]_n = [0]_n + [a]_n$
- **Inverse**: $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$
  - $[a]_n + [-a]_n = [a + (-a)]_n = [0]_n$
- **Commutative**: $[a]_n + [b]_n = [b]_n + [a]_n$
  - $[a]_n + [b]_n = [a + b\,]_n = [b + a]_n = [b]_n + [a]_n$

Group

DEFINITION: A **group** is a set G together with a binary operation $\star$ on G such that

- **Closure**: $\forall a, b \in G, a \star b \in G$
- **Associative**: $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
- **Identity**: $\exists e \in G, \forall a \in, a \star e = e \star a = a$
- **Inverse**: $\forall a \in G, \exists b \in G\ , a \star b = b \star a = e$

DEFINITION: A group G is said to be an **Abelian group** if it additionally satisfies the following property:

- **Commutative**: $\forall a, b \in G, a \star b = b \star a$

Group $\mathbb{Z}_n^*$

THEOREM: $\mathbb{Z}_n^*$ is an Abelian group for any integer $n > 1$.

- **Closure**: $\forall\, [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n \in \mathbb{Z}_n^*$
- **Associative**:$\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n^*, [a]_n \cdot ([b]_n \cdot [c]_n) = [abc]_n = ([a]_n \cdot [b]_n) \cdot [c]_n$
- **Identity element**: $\exists [1]_n \in \mathbb{Z}_n^*, \forall [a]_n \in \mathbb{Z}_n^*, [a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$
- **Inverse**: $\forall [a]_n \in \mathbb{Z}_n^*, \exists [s]_n \in \mathbb{Z}_n^*$ such that $[a]_n \cdot [s]_n = [s]_n \cdot [a]_n = [1]_n$
- **Commutative**: $\forall [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n = [ba]_n = [b]_n \cdot [a]_n$

REMARK: we are interested in two types of Abelian groups

- **Additive Group**: binary operation +; identity 0
  - Example: $(\mathbb{Z}, +), (n\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Z}_n, +)$
- **Multiplicative Group**: binary operation ·; identity 1 //$(\mathbb{Z}_n^*, \cdot)$
  - Example: $(\mathbb{Q}^*, \times), (\{\pm 1\}, \times), (\mathbb{Z}_n^*, \cdot)$