Chinese Remainder Theorem

Chinese Remainder Theorem: general version

What about multi-variables version of Chinese Remainder Theorem?

Theorem 6.2.1 (Chinese remainder theorem)

Suppose m_i $(i \in I)$ be moduli which are coprime to each other. Let M be the product of them. Then there is a bijection

$$f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$$

such that whenever $f((a_i)_{i \in I}) = A$, we have

$$\left\{ x \in \mathbb{Z} \,\middle|\, x \equiv a_i \pmod{m_i}, \forall i \in I \right\} = \left\{ x \in \mathbb{Z} \,\middle|\, x \equiv A \pmod{M} \right\}.$$

Chinese Remainder Theorem: general version

Proof. By theorem 6.1.1, we can always replace two congruence equations by a single one with the modulus being the product of former. Apply this to an induction on $|I|$, we get the theorem. □

Proof. By theorem 6.1.1, we can always replace two congruence equations by a single one with the modulus being the product of former. Apply this to an induction on $|I|$, we get the theorem. □

Example 6.2.2

For the original puzzle, we have

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \Rightarrow \begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7 \end{cases} \Rightarrow x \equiv 23 \pmod{105}.$$

Chinese Remainder Theorem: general version

In what follows, we will explain the original method in *Sun-tzu Suan-ching* and generalize it into a proof of theorem 6.2.1.

- count them by 3s and left over $2 \Rightarrow$ Put number 140.
- count them by 5s and left over $3 \Rightarrow$ Put number 63.
- count them by 7s and left over $2 \Rightarrow$ Put number 30.
- Their total gives 233.
- Subtract 210 from it, we get the final 23.

Chinese Remainder Theorem: general version

Proof. (Of 6.2.1) Let's construct the map $f: \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$.

Proof. (Of 6.2.1) Let's construct the map $f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$.

First, let $M_i = \frac{M}{m_i}$. By lemma 2.2.7, each M_i is coprime to m_i. Therefore, by Bézout's identity, there exist integers N_i and n_i such that

$$M_i N_i + m_i n_i = 1.$$

Chinese Remainder Theorem: general version

Proof. (Of 6.2.1) Let's construct the map $f: \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$.

First, let $M_i = \frac{M}{m_i}$. By lemma 2.2.7, each M_i is coprime to m_i. Therefore, by Bézout's identity, there exist integers N_i and n_i such that

$$M_i N_i + m_i n_i = 1.$$

Then the map f maps $([a_i]_{m_i})_{i \in I}$ to the congruence class of

$$\sum_{i \in I} a_i M_i N_i \pmod{M}.$$

$\equiv a_i m_i N_i \mod m_i$
$+ a_i m_i n_i$
$= a_i$

It is straightforward to verify the requirements of f and the inverse map of f is given by $[A]_M \mapsto ([A]_{m_i})_{i \in I}$. □

Chinese Remainder Theorem: abstract version

Theorem 6.2.3 (Chinese remainder theorem, abstract version)

Suppose m_i ($i \in I$) be moduli which are coprime to each other. Let M be the product of them. Then there is an isomorphism (bijective map preserving the structures)

$$f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M.$$

Here the ring structure (i.e. addition, multiplication, and their neutral elements) on the product $\prod_{i \in I} \mathbb{Z}/m_i$ is defined term wise.

Chinese Remainder Theorem: abstract version

Theorem 6.2.3 (Chinese remainder theorem, abstract version)

Suppose m_i ($i \in I$) be moduli which are coprime to each other. Let M be the product of them. Then there is an isomorphism (bijective map preserving the structures)

$$f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M.$$

Here the ring structure (i.e. addition, multiplication, and their neutral elements) on the product $\prod_{i \in I} \mathbb{Z}/m_i$ is defined term wise.

Equivalently, the theorem states that the natural reduction map

$$\mathbb{Z}/M \longrightarrow \prod_{i \in I} \mathbb{Z}/m_i : [A]_M \mapsto ([A]_{m_i})_{i \in I}$$

is an isomorphism.

Proof. We first verify that the natural reduction map preserves the structures.

- $[A]_M + [B]_M = [A+B]_M \mapsto ([A+B]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} + ([B]_{m_i})_{i\in I}$.
- $[A]_M \cdot [B]_M = [AB]_M \mapsto ([AB]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} \cdot ([B]_{m_i})_{i\in I}$.
- $[0]_M \mapsto ([0]_{m_i})_{i\in I}$ and $[1]_M \mapsto ([1]_{m_i})_{i\in I}$.

Proof. We first verify that the natural reduction map preserves the structures.

- $[A]_M + [B]_M = [A+B]_M \mapsto ([A+B]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} + ([B]_{m_i})_{i\in I}$.
- $[A]_M \cdot [B]_M = [AB]_M \mapsto ([AB]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} \cdot ([B]_{m_i})_{i\in I}$.
- $[0]_M \mapsto ([0]_{m_i})_{i\in I}$ and $[1]_M \mapsto ([1]_{m_i})_{i\in I}$.

Next, we show that the natural reduction map is injective. For this, we first note that the only preimage of $([0]_{m_i})_{i\in I}$ is $[0]_M$. Indeed, if $[A]_M$ is preimage of $([0]_{m_i})_{i\in I}$, then we have $m_i \mid A$. Since m_i are coprime to each other, by lemma 2.2.7, their product M also sivides A. Namely, $[A]_M = [0]_M$.

Proof. We first verify that the natural reduction map preserves the structures.

- $[A]_M + [B]_M = [A+B]_M \mapsto ([A+B]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} + ([B]_{m_i})_{i\in I}$.
- $[A]_M \cdot [B]_M = [AB]_M \mapsto ([AB]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} \cdot ([B]_{m_i})_{i\in I}$.
- $[0]_M \mapsto ([0]_{m_i})_{i\in I}$ and $[1]_M \mapsto ([1]_{m_i})_{i\in I}$.

Next, we show that the natural reduction map is injective. For this, we first note that the only preimage of $([0]_{m_i})_{i\in I}$ is $[0]_M$. Indeed, if $[A]_M$ is preimage of $([0]_{m_i})_{i\in I}$, then we have $m_i \mid A$. Since m_i are coprime to each other, by lemma 2.2.7, their product M also sivides A. Namely, $[A]_M = [0]_M$.

Finally, we conclude that the natural reduction map is bijective since it is an injection between two sets of the same size. □

Chinese Remainder Theorem: applications

Corollary 6.2.4

The Euler's totient φ is a multiplicative function.

Corollary 6.2.4

The Euler's totient φ is a multiplicative function.

Proof. The isomorphism on the left induces one on the right

$$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n \qquad \Rightarrow \qquad \Phi(mn) \cong \Phi(m) \times \Phi(n).$$

This is because if a is invertible modulo mn, then it is also invertible modulo m. □

$a \in \Phi(mn) \longrightarrow ([a]_m, [a]_n)$

b $\quad [b]_m \quad [0]_n$

$\varphi(mn) = \varphi(m) \cdot \varphi(n)$