Taller ProgComp: Track Matemática

Teorema Chino del Resto

Gabriel Carmona Tabja

Universidad Técnica Federico Santa María,
Università di Pisa

June 10, 2024

Part I

TEOREMA CHINO DEL RESTO

CRT

Origen

Descubierto por el matemático Sun Zi.

CRT

Origen

Descubierto por el matemático Sun Zi.

Teorema

- $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ (coprimos entre ellos).
- a_i constante dada $\forall i, 1 \leq i \leq k$

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \\ \vdots & \\ a \equiv & a_k \pmod{m_k} \end{cases}$$

CRT

Origen

Descubierto por el matemático Sun Zi.

Teorema

- $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ (coprimos entre ellos).
- a_i constante dada $\forall i, 1 \leq i \leq k$

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \\ \vdots & \\ a \equiv & a_k \pmod{m_k} \end{cases}$$

Consequencia

$$\begin{cases} x \equiv & a \pmod{m} \end{cases}$$

Equivalente al sistema anterior.

Solución con dos modulos

Caso dos modulos

Considere el sistema de dos equaciones para dos coprimos m_1 y m_2:

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \end{cases}$$

Solución con dos modulos

Caso dos modulos

Considere el sistema de dos equaciones para dos coprimos m_1 y m_2:

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \end{cases}$$

Problema

- Encontrar solución para $x \equiv a \pmod{m}, m = m_1 m_2$

Solución con dos modulos

Caso dos modulos

Considere el sistema de dos equaciones para dos coprimos m_1 y m_2:

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \end{cases}$$

Problema

- Encontrar solución para $x \equiv a \pmod{m}, m = m_1 m_2$
- Utilizando Extended Euclidean Algorithm:

$$n_1 \cdot m_1 + n_2 \cdot m_2 = 1$$

Solución con dos modulos

Caso dos modulos

Considere el sistema de dos equaciones para dos coprimos m_1 y m_2:

$$\begin{cases} a \equiv & a_1 \pmod{m_1} \\ a \equiv & a_2 \pmod{m_2} \end{cases}$$

Problema

- Encontrar solución para $x \equiv a \pmod{m}, m = m_1 m_2$
- Utilizando Extended Euclidean Algorithm:

$$n_1 \cdot m_1 + n_2 \cdot m_2 = 1$$

- Queda

$$x = (a_1 n_2 m_2 + a_2 n_1 m_1) \bmod m_1 m_2$$

CASO GENERAL

Solución Inductiva

Si $m_1 m_2$ es comprimo con m_3 se puede aplicar inductivamente la solución para dos modulos:

1. Solucion $b_2 = a \pmod{m_1 m_2}$
2. Solución $b_3 = a \pmod{m_1 m_2 m_3}$ usando:
    - $a \equiv b_2 \pmod{m_1 m_2}$
    - $a \equiv a_3 \pmod{m_3}$

Caso General

Solución Inductiva

Si $m_1 m_2$ es comprimo con m_3 se puede aplicar inductivamente la solución para dos modulos:

1. Solucion $b_2 = a \pmod{m_1 m_2}$
2. Solución $b_3 = a \pmod{m_1 m_2 m_3}$ usando:
   - $a \equiv b_2 \pmod{m_1 m_2}$
   - $a \equiv a_3 \pmod{m_3}$

Construcción Directa

- $M_i = \Pi_{i \neq j} m_j$
- $N_i = M_i^{-1} \pmod{m_i}$

Caso General

Solución Inductiva

Si $m_1 m_2$ es comprimo con m_3 se puede aplicar inductivamente la solución para dos modulos:

1. Solucion $b_2 = a \pmod{m_1 m_2}$
2. Solución $b_3 = a \pmod{m_1 m_2 m_3}$ usando:
   - $a \equiv b_2 \pmod{m_1 m_2}$
   - $a \equiv a_3 \pmod{m_3}$

Construcción Directa

- $M_i = \Pi_{i \neq j} m_j$
- $N_i = M_i^{-1} \pmod{m_i}$
- La solución del sistema sería

$$a \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{m_1 m_2 \dots m_k}$$

Caso General

Solución Inductiva

Si $m_1 m_2$ es comprimo con m_3 se puede aplicar inductivamente la solución para dos modulos:

1. Solucion $b_2 = a \pmod{m_1 m_2}$
2. Solución $b_3 = a \pmod{m_1 m_2 m_3}$ usando:
   - $a \equiv b_2 \pmod{m_1 m_2}$
   - $a \equiv a_3 \pmod{m_3}$

Construcción Directa

- $M_i = \Pi_{i \neq j} m_j$
- $N_i = M_i^{-1} \pmod{m_i}$
- La solución del sistema sería

$$a \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{m_1 m_2 \ldots m_k}$$

Una implementación de CRT la podrán encontrar aquí Implementación, la complejidad es $O(n \log n)$.

References I