Lecture 8b Chinese Remaindering

February 4, 2021 3:29 PM

The integer Chinese remainder problem.

$\gcd(m_i, m_j) = 1$ for $i \neq j$

Given pairwise relatively prime integers $m_1, m_2, \ldots, m_n$ (moduli) and integers $u_1, u_2, \ldots, u_n$ (images) find $u \in \mathbb{Z}$ s.t.

$$u \equiv u_i \bmod m_i.$$

Example $m_1 = 5$ $u_1 = 4$ $u \equiv 4 \bmod 5$ $4, 9, 14, \boxed{19}, 24, \ldots, \boxed{54}$

$m_2 = 7$ $u_2 = 5$ $u \equiv 5 \bmod 7.$ $u = 19 + k \cdot 35$

The Chinese Remainder Theorem. Let $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

There exists a unique $u \in \mathbb{Z}$ on $0 \le u < M$ s.t. $u \equiv u_i \bmod m_i$.

Proof of uniqueness.

Suppose $0 \le v < M$ and $0 \le w < M$ satisfying

$v \equiv u_i \bmod m_i$

$w \equiv u_i \bmod m_i$

$\left.\begin{matrix} 6 \mid x \\ 5 \mid x \end{matrix}\right\} \Rightarrow 30 \mid x.$

$\Rightarrow v - w \equiv 0 \bmod m_i \Rightarrow m_i \mid v - w$

$\Rightarrow m_1 \mid v - w$ and $m_2 \mid v - w$ and .... and $m_n \mid v - w$

$(\gcd(m_i, m_j) = 1)$

$\Rightarrow m_1 m_2 \cdot \ldots \cdot m_n \mid v - w.$

$\Rightarrow M \mid v - w$ $\quad |v - w| < M.$

$\Rightarrow v - w = 0. \Rightarrow v = w.$

Proof of existence.

Let $M = \prod m_i$. Find $0 \le u < M$ s.t. $u \equiv u_i \bmod m_i$.

Method ① (Lagrange reprentation)

Let $u = w_1 \cdot \frac{M}{m_1} + w_2 \cdot \frac{M}{m_2} + \cdots + w_n \frac{M}{m_2}.$

$(\bmod m_1)$ $u_1 = w_1 \cdot (m_2 \cdot m_3 \cdots m_n) + 0 + \cdots + 0$

$\Rightarrow w_1 = u_1 \cdot (m_2 \cdot m_3 \cdots m_n)^{-1} \bmod m_1$ $[\gcd(m_1, m_i) = 1$ for $i \ge 2]$

$(\bmod m_i) \Rightarrow u_i = w_i \cdot \frac{M}{m_i} + 0 \Rightarrow w_i = u_i \cdot \left(\frac{M}{m_i}\right)^{-1} \bmod m_i.$

$n = 3$. We have. $u \le (m_1 - 1) \cdot m_2 m_3 + (m_2 - 1) m_1 m_3 + (m_3 - 1) m_1 m_2$

$n=3$. We have $u \le (m_1-1)\cdot m_2m_3 + (m_2-1)m_1m_3 + (m_3-1)m_1m_2$

$$= 3m_1m_2m_3 - m_1m_2 - m_2m_3 - m_1m_3$$
$$= 3M - m_1m_2 - m_2m_3 - m_1m_3$$

So $u \ge M$. Must reduce this u mod M.

Method 2 (Mixed radix representation).

Let $u = v_1 + v_2m_1 + v_3m_1m_2 + \cdots + v_n m_1m_2\cdots m_{n-1}$

gcd$(m_1,m_2)=1$.

(mod m_1) $u_1 = v_1 \bmod m_1 \Rightarrow v_1 \leftarrow u_1 \bmod m_1$

(mod m_2) $u_2 = v_1 + v_2\cdot m_1 + 0 \Rightarrow v_2 = (u_2 - v_1)\cdot m_1^{-1} \bmod m_2$

(mod m_3) $u_3 = v_1 + v_2m_1 + v_3m_1m_2 \bmod m_3$

$v_3 = (u_3 - v_1 - v_2m)(m_1m_2)^{-1} \bmod m_3$.

$n=3$

$$u = v_1 + v_2m_1 + v_3m_1m_2$$
$$\le m_1 - 1 + (m_2-1)m_1 + (m_3-1)m_1m_2$$
$$= \cancel{m_1} - 1 + \cancel{m_2m_1} - \cancel{m_1} + m_3m_1m_2 - \cancel{m_1m_2}$$
$$= M - 1.$$

Example. $m_1 = 5$ $u_1 = 2$

$m_2 = 7$ $u_2 = 1$

$m_3 = 3$ $u_3 = 1$

$M = 3\cdot 5\cdot 7 = 105$.

$u = v_1 + v_2\cdot m_1 + v_3\cdot m_1\cdot m_2$

$\longrightarrow u = v_1 + 5v_2 + 35\cdot v_3$

mod 5. $2 = v_1 + 0 \Rightarrow v_1 = 2$.

mod 7 $1 = 2 + 5\cdot v_2$

$v_2 = 4$

mod 3 $1 = 2 + 5\cdot 4 + 2\cdot v_3$

$\Rightarrow 1 = 1 + 2\cdot v_3 \Rightarrow v_3 = 0$.

$u = 2 + 5\cdot 4 + 0$
$= 22$.

Cost? For n primes $m_i < B = 2^{63}$ both methods have $O(n^2)$ bit complexity.

Maple: chrem([$u_1, u_2, \ldots, u_n$], [$m_1, m_2, \ldots, m_n$]);

Note: chrem([$3x+1$, $5x+2$], [5, 7]);

Solve $u(x) \equiv 3x + 1 \bmod 5$

$u(x) \equiv 5x + 2 \bmod 7$

$0 \le u < M$

Solve $u(x) \equiv 3x + 1 \mod 5$
$ u(x) \equiv 5x + 2 \mod 7$

$0 \le u < M$

$-5 + 35 = 30$

$33x + 16$

? What if $u(x)$ has $-$ve integers?
Solve for $0 \le u < M$ then put u in the symmetric range for $\mathbb{Z}_M$. E.g. $M = 35$ $\quad -17 \le u \le 17$

$-2x + 16$

Maple: mods(u, M) uses $-\lfloor \frac{M}{2} \rfloor < u \le \lfloor \frac{M}{2} \rfloor$
modp(u, M) uses $0 \le u < M$.