Linear Algebra I : Chinese Remainder Algorithms

September 21, 2023 9:23 AM

The Chinese Remainder Theorem for integers.

Let $m_1, m_2, \ldots, m_n$ be positive pairwise relatively prime integers, i.e. $\gcd(m_i, m_j) = 1$. Let $u_1, u_2, \ldots, u_n$ be integers. Thee exists a unique integer u s.t.

$$0 \le u < M = \prod_{i=1}^{n} m_i \text{ and } u \equiv u_i \bmod m_i \quad (1 \le i \le n).$$

$m_1 = 3 \quad m_2 = 5$
$u_1 = 2 \quad u_2 = 3 \qquad u = 2, 5, 8$ ✓

Lagrange representation for u:

$$u = v_1 \cdot \frac{M}{m_1} + v_2 \cdot \frac{M}{m_2} + \cdots + v_n \frac{M}{m_n} \quad \text{where } 0 \le v_i < m_i.$$

mod m_i $\quad u_i = 0 + \cdots + v_i \frac{M}{m_i} + 0 + \cdots + 0 \bmod m_i$

It will often happen that $u \geq M$.

$u \leftarrow u \bmod M$.

Mixed radix representation for u.

$\rightarrow u = v_1 + v_2 m_1 + v_3 \cdot m_1 \cdot m_2 + \cdots + v_n m_1 m_2 \cdots m_{n-1}$.

where $0 \le v_i < m_i$.

(mod m_1) $\quad u_1 \equiv v_1 \bmod m_1 \Rightarrow \underline{v_1} = u_1 \bmod m_1$.

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

(mod m_3) $\quad u_3 = v_1 + v_2 m_1 + v_2 m_1 m_2 \Rightarrow v_3 = (u_3 - v_1 \ \ v_2 m_1) \cdot (\underline{m_1 m_2})^{-1} \bmod m_3$

$m_1 = 3, m_2 = 5, m_3 = 2$
$u_1 = 2, u_2 = 3, u_3 = 1$

$u = v_1 + v_2 m_1 + v_3 m_1 m_2$ $\qquad$ mod 3
$2 = v_1 + 0 \Rightarrow v_1 = 2$.
$3 = 2 + v_2 \cdot 3 \quad$ mod 5
$1 = v_2 \cdot 3 \quad$ mod 5
$v_2 = 3^{-1} = 2$.
mod 2 $\quad 1 = \cancel{2} + \cancel{2 \cdot 3} + v_3 \cdot 1\cancel{5} \qquad 2$
$1 = v_3 \bmod 2 \quad v_3 = 1$.

$u = 2 + 2 \cdot 3 + 1 \cdot 15 = 23. \quad m_1 m_2 m_3 = 30.$

Maple `chrem([u1,u2,...,un],[m1,m2,...,mn]);`

The construction guarantees that $u \equiv u_i \bmod m_i$.
But is $0 \le u < M = \prod_{i=1}^{n}$?
The v_i satisfy $0 \le v_i < m_i$ by construction.

$$u = v_1 + v_2 m_1 + v_3 m_1 m_2 + \dots + v_n m_1 m_2 \cdots m_{n-1}.$$

The biggest value for u is when $v_i = m_i - 1$

$n=4$ $$u \le (m_1-1) + (m_2-1)m_1 + (m_3-1)m_1m_2 + (m_4-1)m_1m_2m_3$$
$$= \cancel{m_1} - 1 + \cancel{m_2m_1} - \cancel{m_1} + \cancel{m_1m_2}m_3 - \cancel{m_1m_2} + m_1m_2m_3m_4 - \cancel{m_1m_2m_3}$$
$$= m_1m_2m_3m_4 - 1 = M - 1.$$

Algorithm CRT. Input $u_1, u_2, \dots, u_n \in \mathbb{Z}$
$m_1, m_2, \dots, m_n \in \mathbb{N}$ s.t. $\gcd(m_i, m_j) = 1$.

$u = \underbrace{v_1 + v_2 m_1 + v_3 m_1 m_2}_{S} + v_4 m_1 m_2 m_3$.

$p=1$ $\quad p = p \cdot m_1$ $\quad p = p \cdot m_2$ $\quad p = p \cdot m_3$

$\rightarrow$ $v_4 = (u_4 - S) \cdot p^{-1} \bmod m_4$

for $k = 1, 2, \dots, n$ do
  # Compute v_k
  $S = 0 \quad p = 1$.
  for $i = 1, 2, \dots, k-1$ do
    $S = \underline{S + v_i \cdot p}$ mod m_k
    $p = p \cdot m_i$ mod m_k.
  $v_k = (u_k - S) \cdot p^{-1} \bmod m_k$.

TRAP

$u = v_1 + v_2 m_1 + v_3 m_1 m_2 + v_4 m_1 m_2 m_3$.

$p=1$ $\quad p = p \cdot m_1$ $\quad p = p \cdot m_2$ $\quad p = p \cdot m_3$

$u = v_1 + m_1(v_2 + m_2(v_3 + m_4(v_4)))$.

u

$u = v_n$
for $k = n-1, n-2, \dots, 1$ do
  $u = v_k + m_k \cdot u$.
return u.

$< 2^{63}$

$\llcorner$ return u.

Cost? If $m_i < B = 2^{63}$ then $O(n^2)$ bit operations.

constant.

Solve $u(x) \equiv 1 \cdot x + 1 \mod 5$

$\mathbb{Z}[x] \equiv 2 \cdot x + 3 \mod 7$

$\equiv 3 \cdot x + 5 \mod 6$

$u(x) \quad 51 \cdot x + 101. \mod 5 \cdot 7 \cdot 6 = 210.$

chrem([x+1, 2x+3, 3+5], [5,7,6]);

How can we recover -ve integers in $u(x)$?

$u = \underline{11} \mod 15 = 3 \cdot 5$ $\quad \mathbb{Z}_{15}$ symmetric range $-7 \leq x \leq +7.$

$11 \to -4$

$0 \leq x < 15$