Chinese Remainder Problem (CRP_n)

Given: $r_1, r_2, \cdots, r_n \in D$ (remainders), $m_1, m_2, \cdots, m_n \in D^*$ (moduli), pairwise relatively prime, i.e., $\gcd(m_i, m_j) = 1$.

Find: $r \in D$ such that $r \equiv r_i \mod m_i$ for $1 \leq i \leq n$.

Algorithm for CRA_2

Input: r_1, r_2, m_1, m_2.

Output: r solve the CRP_2.

Step 1. $c := m_1^{-1} \mod m_2$.

Step 2. $r_1' := r_1 \mod m_1$.

Step 2. $\sigma := (r_2 - r_1')c \mod m_2$.

Step 3. Return $r := r_1' + \sigma m_1$.

Algorithm for CRA_n

Input: $r_1, r_2, \cdots, r_n$, $m_1, m_2, \cdots, m_n$.

Output: r solve the CRP_n.

Step 1. $M := m_1$.

Step 2. $r := r_1 \mod m_1$.

Step 3. For $k = 2$ to n do

1. $r := \mathrm{CRA}_2(r, r_k, M, m_k)$;
2. $M := M \cdot m_k$.

Step 4. Return r.

Interpolation Problem (IP)

Given: $\alpha_1, \cdots, \alpha_n \in K$, $\beta_1, \cdots, \beta_n \in K$ such that $\beta_i \neq \beta_j$ for $i \neq j$.

Find: $r(x) \in K[x]$ such that $r(\beta_i) = \alpha_i$ for $1 \leq i \leq n$.

Hensel's Lifting Algorithm(linear version).

Input: $f(x), g_1(x), h_1(x)$, satisfy $f = g_1 h_1 \mod p$, p is a prime and k is a positive integer.

Output: $g_k(x)$ and $h_k(x)$ such that $f = g_k h_k \mod p^k$ and $g_k = g_1 \mod p, h_k = g_1 \mod p$.

1. Set $g(x) := g_1(x)$;
$h(x) := h_1(x)$;
apply Extend Euclidean alogorithm to obtain $u(x)$ and $v(x)$ satisfy $u(x)g_1(x) + v(x)h_1(x) = 1 \mod q$.

2. For $i := 2..k$ do

2.1. $r(x) := \frac{f(x)-g(x)h(x) \mod p^i}{p^{i-1}}$;

2.2. $u_1(x) := r(x) * u(x) \mod (p, h_1(x))$;
$v_1(x) := r(x) * v(x) \mod (p, g_1(x))$.

2.3. $g(x) := g(x) + p^{i-1}v_1(x)$;
$h(x) := h(x) + p^{i-1}u_1(x)$.

3. Return g and h.

Hensel's Lifting Algorithm(quadritic version).

Input: $f(x), g_1(x), h_1(x)$, satisfy $f = g_1 h_1 \mod p$, p is a prime and k is a positive integer.

Output: $g_k(x)$ and $h_k(x)$ such that $f = g_k h_k \mod p^k$ and $g_k = g_1 \mod p, h_k = g_1 \mod p$.

1. Set $g(x) := g_1(x)$;
$h(x) := h_1(x)$;
$q := p$.

2. For $i := 2..\lceil \log_2 k \rceil$ do

2.1. $r(x) := \frac{f(x) - g(x)h(x) \mod q^2}{q}$;

2.2. Apply Extend Euclidean alogorithm to obtain $u(x)$ and $v(x)$ satisfy $u(x)g(x) + v(x)h(x) = 1 \mod q$;

2.3. $u_1(x) := r(x) * u(x) \mod (q, h(x))$;
$v_1(x) := r(x) * v(x) \mod (q, g(x))$;

2.4. $g(x) := g(x) + q * v_1(x)$;
$h(x) := h(x) + q * u_1(x)$;
$q := q^2$.

3. Return g and h.