Chinese Remainder Theorem

Jiman Hwang

March 7, 2015

This document is for self-study only.

1 Chinese Remainder Theorem

1.1 Statement

Let $n_1, n_2, ..., n_k \in \mathbb{Z}$ such that $(n_i, n_j) = 1$ for $i \neq j$. Then for any integers $a_1, a_2, ..., a_k$, the system

$$\begin{gathered} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ ... \\ x \equiv a_k \mod n_k \end{gathered}$$

has a solution.

1.2 Proof

Proof. Let

$$p_{1i} \equiv in_1 + a_1 \mod n_2 \tag{1}$$

$$h_{1i} \equiv a_2 + i \mod n_2 \tag{2}$$

$$where \quad i = 0, 1, 2, ..., n_2 - 1 \tag{3}$$

and

$$P_1 = \{p_{10},\ p_{11},\ ...\ ,\ p_{1(n_2-1)} - 1\} \tag{4}$$

$$H_1 = \{h_{10},\ h_{11},\ ...\ ,\ h_{1(n_2-1)} - 1\} \tag{5}$$

For $i \neq j$, assume that $p_{1i} \equiv p_{1j} \mod n_2$, then

$$\begin{aligned} & in_1 + a_1 \equiv jn_1 + a_1 \mod n_2 \\ \rightarrow\ & in_1 \equiv jn_1 \mod n_2 \\ \rightarrow\ & i \equiv j \mod n_2 && \because (n_1, n_2) = 1 \\ \rightarrow\ & i = j && \because\ i, j < n_2 \end{aligned}$$

This is a contradiction.
$\therefore$ All elements in P_1 are distinguished, and $|P_1| = n_2$
But, $|H_1| = n_2$, so by Pigeon holes Principle, (Pigeons: p_i, Pigeon holes: h_i)

$$P_1 = H_1 \tag{6}$$

, and there is an x_{12} such that

$$
\begin{aligned}
x_{12} &\equiv a_1 \mod n_1 \\
x_{12} &\equiv a_2 \mod n_2
\end{aligned}
$$

Do the similar process as follow. Let

$$
\begin{aligned}
p_{2i} &= in_1n_2 + a_2 \mod n_3 && (7)\\
h_{2i} &= a_3 + i \mod n_3 && (8)\\
P_2 &= \{p_{21},\ p_{22},\ ...,\ p_{2(n_3-1)}\} && (9)\\
H_2 &= \{h_{21},\ h_{22},\ ...,\ h_{2(n_3-1)}\} && (10)
\end{aligned}
$$

For $i \neq j$, assume $p_{2i} \equiv p_{2j} \mod n_3$, then

$$
\begin{aligned}
& in_1n_2 + a_2 \equiv jn_1n_2 + a_2 \mod n_3 \\
\rightarrow\ & in_1n_2 \equiv jn_1n_2 \mod n_3 \\
\rightarrow\ & i \equiv j \mod n_3 \quad \because n_1,\ n_2,\ n_3 \textit{ are pairwise coprimes} \\
\rightarrow\ & i = j \quad \because i,\ j < n_3
\end{aligned}
$$

This is a contradiction.
$\therefore$ All elements in P_2 are distinguished, and $|P_2| = n_3$
But, $|H_2| = n_3$, so by Pigeon holes Principle, (Pigeons: p_i, Pigeon holes: h_i)

$$P_2 = H_2 \tag{11}$$

, and there is an x_{13} such that

$$
\begin{aligned}
x_{13} &\equiv a_1 \mod n_1 \\
x_{13} &\equiv a_2 \mod n_2 \\
x_{13} &\equiv a_3 \mod n_3
\end{aligned}
$$

Doing this process continuously finishes the proof. □