Lecture 7 Chinese Remainder Theorem

Ex. Suppose we want to simultaneously solve the following congruences
$x \equiv 1 \pmod{7},\ x \equiv 3 \pmod{11}$

$x \equiv 1 \pmod{7} \Rightarrow x = 1 + 7y$ for some integer y. Substitute into the second congruence.

$1 + 7y \equiv 3 \pmod{11} \Rightarrow y \equiv 2 \pmod{11}$
$7^{-1} \equiv 8 \pmod{11}$
$8 * 7y \equiv 8 * 2 \pmod{11}$
$y \equiv 16 \equiv 5 \pmod{11}$
$x = 1 + 7 * 5 = 36$

The final equation is the smallest positive solution. The general solution would be
$x \equiv 36 \pmod{77} \Rightarrow x = 36 + 77y$

Chinese Remainder Theorem
Let $m_1, m_2, ..., m_k$ be pairwise relatively prime (i.e., for each pair m_i, m_j, $\gcd(m_i, m_j) = 1$). Let $a_1, a_2, ..., a_k$ be arbitrary integers. Then the following system

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k}$$

has a solution $x = c$. Any other solution $x = c'$ satisfies $c \equiv c' \pmod{m_1 m_2 \cdots m_k}$.

Pf: By induction on k

If $k = 1$ then $x \equiv a_1 \pmod{m_1}$ has the solution $x = a_1$.

Assume $x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k}$ has a solution. $x = c_k$. The general solution is $x = c_k + (m_1 m_2 \cdots m_k) y$

Consider the system with one additional congruence (we assume $m_1, m_2, ..., m_k, m_{k+1}$ are pairwise relatively prime)
$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k}, x \equiv a_{k+1} \pmod{m_{k+1}}$

Let $a = (m_1 m_2 \cdots m_k)^{-1} \pmod{m_{k+1}}$. We solve the new congruence as follows.

$x \equiv a_{k+1} \pmod{m_{k+1}}$
$c_k + (m_1 m_2 \cdots m_k) y \equiv a_{k+1} \pmod{m_{k+1}}$
$(m_1 m_2 \cdots m_k) y \equiv (a_{k+1} - c_k) \pmod{m_{k+1}}$
$y \equiv a(a_{k+1} - c_k) \pmod{m_{k+1}}$

Ex:

(1) Solve $x \equiv 3 \pmod 5,\ x \equiv 2 \pmod 7,\ x \equiv 4 \pmod 8$. This has a solution since 5,7,8 are pairwise relatively prime.

$$x \equiv 3 \pmod 5 \Rightarrow x = 3 + 5y$$
$$x \equiv 2 \pmod 7 \Rightarrow$$
$$3 + 5y \equiv 2 \pmod 7$$
$$5y \equiv -1 \equiv 6 \pmod 7$$
$$5^{-1} \pmod 7 = 3$$
$$3 * 5y \equiv 3 * 6 \equiv 4 \pmod 7$$
$$y \equiv 4 \pmod 7 \Rightarrow x = 3 + 5 * 4 = 23$$

The general solution to the first two equations is:

$$x = 23 + 5 * 7z = 23 + 35z$$
$$x \equiv 4 \pmod 8 \Rightarrow$$
$$23 + 35z \equiv 4 \pmod 8$$
$$35z \equiv -19 \equiv 5 \pmod 8$$
$$35 \equiv 3 \pmod 8 \Rightarrow 35^{-1} \equiv 3^{-1} \equiv 3 \pmod 8$$
$$3 * 35z \equiv 3 * 5 \pmod 8$$
$$z \equiv 15 \equiv 7 \pmod 8$$
$$x = 23 + 35 * 7 = 268$$

The general solution is $x = 268 + 5 * 7 * 8k = 268 + 280k$

(2) Solve $x \equiv 3 \pmod 4,\ x \equiv 2 \pmod 9,\ x \equiv 1 \pmod{13}$. This has a solution because 4,9,13 are pairwise relatively prime.

$$x \equiv 3 \pmod 4 \Rightarrow x = 3 + 4y$$
$$3 + 4y \equiv 2 \pmod 9$$
$$4y \equiv -1 \equiv 8 \pmod 9$$
$$4^{-1} \bmod 9 = 7$$
$$7 * 4y \equiv 7 * 8 \equiv 2 \pmod 9$$
$$y \equiv 2 \pmod 9$$
$$x = 3 + 4 * 2 = 11$$

The general solutions to the first two equations is

$$x = 11 + 4 * 9z = 11 + 36z$$
$$x \equiv 1 \pmod{13} \Rightarrow$$
$$11 + 36z \equiv 1 \pmod{13}$$
$$36z \equiv -10 \equiv 3 \pmod{13}$$
$$36^{-1} \bmod 13 = 4$$
$$4 * 36z \equiv 4 * 3 \equiv 12 \pmod{13}$$
$$z \equiv 12 \pmod{13}$$
$$x = 11 + 36 * 12 = 443$$

The general solution is $x = 443 + 8 * 9 * 13k = 443 + 993k$