Chinese Remainder Theorem

We discuss two types of simultaneous congruences.

1. Systems with one variable and more than one modulus.
2. Systems with more than one variable and one modulus.

First we discuss type 1.

Theorem 4.13 (Chinese Remainder Theorem):

Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$ be s.t. $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_r$.

Proof: Define $M_k = M/m_k$.

Then, $\gcd(M_k, m_k) = \gcd(m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r, m_k)$

$= 1$ (prove this!)

Then, by Theorem 4.11, each M_k has an inverse y_k modulo m_k.

Then, $M_k y_k \equiv 1 \pmod{m_k}$ $\forall k$

Now, let $x_0 = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$.

We show that x_0 is a simultaneous solution of the given system of r congruences.

First note that

$$M_j \equiv 0 \pmod{m_k} \quad \forall j \neq k.$$

This is because $m_k \mid M_j$ for $j \neq k$.

$$\therefore a_j M_j y_j \equiv 0 \pmod{m_k} \quad \forall j \neq k.$$

$$\therefore a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_{k-1} M_{k-1} y_{k-1} + a_{k+1} M_{k+1} y_{k+1} + \cdots + a_r M_r y_r \equiv 0 \pmod{m_k}$$

$$\therefore x_0 - a_k M_k y_k \equiv 0 \pmod{m_k}$$

$$\therefore x_0 \equiv a_k \underbrace{M_k y_k}_{\equiv 1} \pmod{m_k}$$

$\therefore\ x_0 \equiv a_k \pmod{m_k} \ \forall k$

Now, let's show that any two solutions are congruent modulo M.

Let x_1 be another solution of the given system.

Then, $x_1 \equiv a_k \pmod{m_k} \ \forall k$.

Then,

Then, $x_0 \equiv x_1 \pmod{m_k} \ \forall k$

Then, by Theorem 4.9,

$$x_0 \equiv x_1 \pmod{\operatorname{lcm}(m_1, m_2, \ldots, m_k)}$$

It can easily be seen that

$$\operatorname{lcm}(m_1, m_2, \ldots, m_k) = m_1 m_2 \cdots m_k = M$$

because m_i's are pairwise disjoint.

$$\therefore\ x_0 \equiv x_1 \pmod{M}$$

and the result follows.

<u>ex</u>: A Chinese puzzle, written in the 3rd century C.E. is the following.

"Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7."

Let's solve this puzzle.

We've to solve the system

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

We've

$$M = 3 \cdot 5 \cdot 7 = 105$$
$$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15$$

Let's find y_1, y_2 and y_3.

We need to solve

$$35 y_1 \equiv 1 \pmod 3$$
$$21 y_2 \equiv 1 \pmod 5$$
$$15 y_3 \equiv 1 \pmod 7$$

They reduce to

$$2 y_1 \equiv 1 \pmod 3$$
$$y_2 \equiv 1 \pmod 5$$
$$y_3 \equiv 1 \pmod 7$$

(Note that $am + b \equiv c \pmod m$ is

equivalent to $b \equiv c \pmod{m}$)

Now, $2y_1 \equiv 1 \pmod{3} \Rightarrow \bar{2}2y \equiv \bar{2} \pmod{3}$
where $\bar{2}$ is the inverse 2 modulo 3.
Since 3 is prime, by Theorem 4.12,
$\bar{2} = 2$. Hence, $y_1 = 2 \pmod{3}$

Hence, we can take $y_1 = 2$, $y_2 = 1$ and $y_3 = 1$.
Therefore,

$$
\begin{aligned}
x_0 &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\
&= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \\
&= 157 \\
&\equiv 52 \pmod{105}
\end{aligned}
$$

It can easily be checked that
$x = 52 \pmod{105}$ satisfies the given system of congruences.

Thus, the smallest such number is 52.

There is an iterative method to solve systems of congruences. It is illustrated in the following example.

ex: Let's solve the following system.

$$x \equiv 1 \pmod{5} \quad \text{——} (1)$$

$$x \equiv 2 \pmod 6 \quad \text{--- (2)}$$
$$x \equiv 3 \pmod 7 \quad \text{--- (3)}$$

By Theorem 4.1, (1) $\Rightarrow x = 1 + 5t$ for some t.

Substitute this in (2) to get

$$1 + 5t \equiv 2 \pmod 6$$

$$\Rightarrow \quad 5t \equiv 1 \pmod 6$$
$$\Rightarrow \quad t \equiv 5 \pmod 6$$
$$\Rightarrow \quad t = 5 + 6u \text{ for some } u.$$

$$\therefore \; x = 1 + 5(5 + 6u) = 26 + 30u.$$

Substitute this in (3) to get

$$26 + 30u \equiv 3 \pmod 7$$

$$\Rightarrow \quad 30u \equiv -23 \pmod 7$$
$$\Rightarrow \quad 2u \equiv 5 \pmod 7$$

This is equivalent to $2u - 7v = 5$.
We can solve this using the Euclidean algorithm to get

$$u \equiv 6 \pmod 7$$

$$\therefore \; u = 6 + 7v \text{ for some } v.$$

Hence, $x = 26 + 30(6 + 7v)$

$$= 206 + 210v$$
$$\equiv 206 \pmod{210}$$

$\therefore\ x \equiv 206 \pmod{210}$
is the simultaneous solution.

Chinese remainder theorem can be used to perform computer arithmetic with large integers.

ex: Suppose the word size of a computer is 100 and we want to add $x = 123,684$ and $y = 413,456$.
We proceed as follows.

1. Choose several integers that are pairwise relatively prime and each less than the word size. Also, the product of these integers should be greater than $x+y$.
So, let's choose

$$m_1 = 99,\ m_2 = 98,\ m_3 = 97,\ m_4 = 95$$

2. Write each of x and y modulo each m_i.
Then, we get

$x \equiv 33 \pmod{99}$ $\quad$ $y \equiv 32 \pmod{99}$

$x \equiv 8 \pmod{98}$ $\quad$ $y \equiv 92 \pmod{98}$

$x \equiv 9 \pmod{97}$ $\quad$ $y \equiv 42 \pmod{97}$

$x \equiv 89 \pmod{95}$ $\quad$ $y \equiv 16 \pmod{95}$

3. Find $x+y$ modulo each m_i.

$$x+y \equiv 65 \pmod{99}$$
$$x+y \equiv 2 \pmod{98}$$
$$x+y \equiv 51 \pmod{97}$$
$$x+y \equiv 10 \pmod{95}$$

4. Use Chinese remainder theorem to find unique $x+y$ modulo $99 \times 98 \times 97 \times 95$.
We find that

$$x+y \equiv 537{,}140 \pmod{89{,}403{,}930}.$$

5. Since $x+y < 89{,}403{,}930$, we conclude that

$$x+y = 537{,}140.$$

Usually, the word size of a computer is a large power of 2, such as 2^{64}. In such a case, we need integers each less than 2^{64} and pairwise relatively prime. Also, they should multiply together to give a very large integer. Such numbers are usually chosen in the form $2^m - 1$. We prove some results related to these.

<u>Lemma 4.2:</u> Let $a, b \in \mathbb{Z}^+$. Then, the least positive residue of $2^a - 1$ modulo $2^b - 1$ is $2^r - 1$ where r is the least positive residue of a modulo b.

<u>ex</u>: Consider $2^7 - 1 = 127$ and $2^4 - 1 = 15$.

Then, $2^7 - 1 \equiv \underset{\substack{\| \\ 2^3 - 1}}{7} \pmod{2^4 - 1}$; here 3 is such that $7 \equiv 3 \pmod 4$

Proof: Given $a, b \in \mathbb{Z}^+$, from the division algorithm, $\exists$ q, r s.t.

$$a = bq + r \; ; \; 0 \leq r < b.$$

$$\therefore 2^a - 1 = 2^{bq+r} - 1$$
$$= (2^b - 1)(2^{b(q-1)+r} + 2^{b(q-2)+r} + \cdots + 2^{b+r} + 2^r) + 2^r - 1$$

$$\therefore 2^a - 1 \equiv 2^r - 1 \pmod{2^b - 1}$$

and $2^r - 1$ is the least positive residue of 2^a-1 modulo 2^b-1 sin $0 \le 2^r-1 < 2^b-1$.

Lemma 4.3: Let $a, b \in \mathbb{Z}^+$. Then

$$\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1.$$

Proof: Exercise

Theorem 4.14: The positive integers 2^a-1 and 2^b-1 are relatively prime if and only if a and b are relatively prime.

Proof: This follows quickly from Lemma 4.3.

ex: On a computer of word length 2^{64}, choose the six large integers that satisfy the requirements to perform operations of large numbers.

We can pick $m_1 = 2^{63}-1$, $m_2 = 2^{62}-1$, $m_3 = 2^{61}-1$, $m_4 = 2^{59}-1$, $m_5 = 2^{57}-1$ and $m_6 = 2^{55}-1$.

Since the integers 63, 62, 61, 59, 57 and 55 are pairwise coprime, so are the integers $m_1, m_2, \ldots, m_6$ (by Theorem 4.14).

It can be shown that

$$M = m_1 m_2 m_3 m_4 m_5 m_6 > 2^{356}$$

$\therefore$ numbers up to 2^{356} can be handled.