CHINESE REMAINDER THEOREM

We are given two arrays num[0..k-1] and rem[0..k-1]. In num[0..k-1], every pair is coprime (gcd for every pair is 1). We need to find minimum positive number x such that:

x % num[0] = rem[0],

x % num[1] = rem[1],

....

x % num[k-1] = rem[k-1]

Basically, we are given k numbers which are pairwise coprime, and given remainders of these numbers when an unknown number x is divided by them. We need to find the minimum possible value of x that produces given remainders.

Examples :

Input: num[] = {5, 7}, rem[] = {1, 3}

Output: 31

Explanation:

31 is the smallest number such that:

(1) When we divide it by 5, we get remainder 1.

(2) When we divide it by 7, we get remainder 3.

Input: num[] = {3, 4, 5}, rem[] = {2, 3, 1}

Output: 11

Explanation:

11 is the smallest number such that:

(1) When we divide it by 3, we get remainder 2.

(2) When we divide it by 4, we get remainder 3.

(3) When we divide it by 5, we get remainder 1.

Chinese Remainder Theorem states that there always exists an x that satisfies given congruences.

Let num[0], num[1], …num[k-1] be positive integers that are pairwise coprime. Then, for any given sequence of integers rem[0], rem[1], … rem[k-1], there exists an integer x solving the following system of simultaneous congruences.

$$\begin{cases} x \equiv rem[0] & \pmod{num[0]} \\ \quad \ldots & \\ x \equiv rem[k-1] & \pmod{num[k-1]} \end{cases}$$

Furthermore, all solutions x of this system are congruent modulo the product, prod = num[0] * num[1] * ... * nun[k-1]. Hence

$$x \equiv y \pmod{num[i]}, \quad 0 \le i \le k-1 \qquad \Longleftrightarrow \qquad x \equiv y \pmod{prod}.$$

The first part is clear that there exists an x. The second part basically states that all solutions (including the minimum one) produce the same remainder when divided by-product of num[0], num[1], .. num[k-1]. In the above example, the product is 3*4*5 = 60. And 11 is one solution, other solutions are 71, 131, .. etc. All these solutions produce the same remainder when divided by 60, i.e., they are of form 11 + m*60 where m >= 0.
A **Naive Approach to find x** is to start with 1 and one by one increment it and check if dividing it with given elements in num[] produces corresponding remainders in rem[]. Once we find such an x, we return it.
Below is the implementation of Naive Approach.

Example 5. Use the Chinese Remainder Theorem to find an x such that

$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv 10 \pmod{11}$$

Solution. Set $N = 5 \times 7 \times 11 = 385$. Following the notation of the theorem, we have $m_1 = N/5 = 77$, $m_2 = N/7 = 55$, and $m_3 = N/11 = 35$.
We now seek a multiplicative inverse for each m_i modulo n_i. First: $m_1 \equiv 77 \equiv 2 \pmod 5$, and hence an inverse to m_1 mod n_1 is $y_1 = 3$.
Second: $m_2 \equiv 55 \equiv 6 \pmod 7$, and hence an inverse to m_2 mod n_2 is $y_2 = 6$.
Third: $m_3 \equiv 35 \equiv 2 \pmod{11}$, and hence an inverse to m_3 mod n_3 is $y_3 = 6$.
Therefore, the theorem states that a solution takes the form:

$$x = y_1 b_1 m_1 + y_2 b_2 m_2 + y_3 b_3 m_3 = 3 \times 2 \times 77 + 6 \times 3 \times 55 + 6 \times 10 \times 35 = 3552.$$

Since we may take the solution modulo $N = 385$, we can reduce this to 87, since $2852 \equiv 87 \pmod{385}$.

Chinese Remainder

↓ to reduce modular calculation
solve set of congruent equations
with one variable which are
relatively prime.

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_k \pmod{m_k}$.

Ex: $x \equiv 2 \pmod 3$ $\quad a_1 = 2 \; a_2 = 3 \; a_3 = 2$
$x \equiv 3 \pmod 5$ $\quad M = m_1 \times m_2 \times m_3$
$x \equiv 2 \pmod 7$. $\quad m_1 = 3 \; m_2 = 5 \; m_3 = 7$ $\quad$ (5,4)
$M = 3 \times 5 \times 7 = \underline{\underline{105}}$.

$M_1 = M/m_1 \Rightarrow M_1 = 105/3 = 35$
$M_2 = M/m_2 = M_2 = 105/5 = 21$
$M_3 = M/m_3 \Rightarrow M_3 = 105/7 = 15$

$p = 3$
$a^{p-2} =$

Next find $M_1^{-1} \bmod m_1 = (35)^{-1} \bmod 3$
$= 35 \bmod 3$
$= 2$

a^{p-2} $\quad p = 5$
a^3

$M_2^{-1} \bmod m_2 = (21)^{-1} \bmod 5$
$= (21)^3 \bmod 5$
$= 9261 \bmod 5$
$= \underline{\underline{1}}$

$M_3^{-1} \bmod m_3 = (15)^{-1} \bmod 7$
$= (15)^5 \bmod 7$
$= 759375 \bmod 7$
$= \underline{1}$.

$= a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} \bmod M$
$= (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) \bmod M$
$= (140 + 63 + 30) \bmod 105$
$= 233 \bmod 105$
$x = \underline{\underline{23}}$.

Example 6. Find all solutions x, if they exist, to the system of equivalences:

$$2x \equiv 6 \pmod{14}$$
$$3x \equiv 9 \pmod{15}$$
$$5x \equiv 20 \pmod{60}$$

Solution. As in Example 2, we first wish to reduce this, where possible, using the strategy outlined following the statement of Proposition 1. Since $\gcd 2, 14 = 2$, we can cancel a 2 from all terms in the first equivalence to write $x \equiv 3 \pmod 7$. Likewise, we simplify the other two equivalences to reduce the entire system to

$$x \equiv 3 \pmod 7$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod{12}.$$

We can now follow the strategy of the Chinese Remainder Theorem. Following the notation in the theorem, we have

$$m_1 = 5 * 12 = 60 \equiv 4 \pmod 7; \quad y_1 \equiv 4^5 \equiv 1024 \equiv 2 \pmod 7)$$
$$m_2 = 7 * 12 = 84 \equiv 4 \pmod 5; \quad y_2 \equiv 4^3 \equiv 64 \equiv 4 \pmod 5$$
$$m_3 = 7 * 5 = 35 \equiv 11 \pmod{12}; \quad y_3 \equiv 11^3 \equiv (-1)^3 \equiv -1 \equiv 11 \pmod{12}.$$

Hence, we have $x = y_1 m_1 b_1 + y_2 m_2 b_2 + y_3 m_3 b_3 = 2 * 60 * 3 + 4 * 84 * 3 + 11 * 35 * 4 = 2908$. Hence, we have any solution $x \equiv 2908 \equiv 388 \pmod{420}$.