The Chinese remainder theorem

Many times, one is required to solve system of simultaneous linear congruence's. These multiple congruence's arise while solving problems with large numbers, in effort to make computations easier. It may not be out that of interest to mention, that, these are also found in the equations formed to solve word puzzles written by ancient Hindu and Chinese mathematicians.

Let us begin with a small and simple illustration.
Suppose, we wish to solve set of two simultaneous linear congruence's

$$x \equiv 4(mod\ 7)\ and\ x \equiv 1(mod\ 6)$$

Observe that gcd (6, 7) = 1. An x, satisfying the first congruence: $x \equiv 4(mod\ 7)$, would be of the form; $7\,i + 4$, where i is an integer. The x must also satisfy the second congruence $x \equiv 1(mod\ 6)$, so, x should be expressible as $6\,j + 1$ for some integer j.
$\therefore 7\,i + 4 = 6\,j + 1$ for some integers i and j, giving $7\,i = 6\,j - 3$ or $6\,j = 7i + 3$
We may try substituting $i = 1, 2, 3, \ldots$ in the preceding equation. When $i = 3$, the equation is satisfied with $j = 4$. So, smallest value of x satisfying both the congruence's $7\,i + 4 = 6\,j + 1$, is $x = 25$. We can verify $25 \equiv 4(mod)7$ and $25 \equiv 1(mod\ 6)$. So, smallest value of x, satisfying the given set of preceding two simultaneous linear congruences is 25.

As per D. wells, Chinese mathematician San-Tsu in first century around 100 A.D. posed a puzzle, "There are certain things whose number is unknown; but when divided by 3, the remainder is 2; when divided by 5 the remainder is 3 and when divided by 7, the remainder is 2. What can be the number? The mathematical formulation of this puzzle is : Solve the system of linear congruence's given by

$$x \equiv 2(mod\ 3), x \equiv 3(mod\ 5), x \equiv 2(mod\ 7)$$

The system can be solved, using approach shown in preceding illustration, but it is not suitable for systematic solving and would be difficult when n in the modulo is large.

We present here a theorem called the *Chinese remainder theorem* named after Chinese heritage of puzzles and contributions of Chinese mathematicians in its solution. This theorem ensures unique solution of system of linear congruences if modulo in them are pairwise relatively prime.

The Chinese remainder theorem: Let $m_1, m_2, \ldots, m_r$, be pairwise relatively prime positive integers. Then the system of congruences:

$$x \equiv a_1(mod\ m_1)$$
$$x \equiv a_2(mod\ m_2)$$
$$\ldots\ldots$$
$$x \equiv a_r(mod\ m_r)$$

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

Proof: Proof of above theorem is constructive. It not only proves the existence but gives us the method for obtaining the unique solution. Let $M_k = \frac{M}{m_k}, k = 1,2, \dots, r$, that is, M_k is the product of all $m_i's \;\; 1 \leq i \leq r$ except m_k. So, $M_k = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$. As $m_1, m_2, \dots, m_r$ are pairwise relatively primes, $\gcd(m_j, m_k) = 1 \; for \; j \neq k$ giving $\gcd(M_k, m_k) = 1$. Therefore, $M_k^{-1}(mod\ m_k)$ exists. Denote $M_k^{-1}(mod\ m_k)$ as y_k, so that $y_k M_k \equiv 1(mod\ m_k)$. Next, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r$$

We claim, x is the desired unique solution of the r congruences. Firstly, we shall show that x is a solution to the given simultaneous congruences, by establishing, $x \equiv a_k(mod\ m_k)$, for $1 \leq k \leq r$. As M_j is the product of all $m_k's \; for \; k = 1,2, \dots, r$; except for m_j, M_j contains m_k as one of the factors for $j \neq k$. Therefore, $m_k | M_j$, meaning by $M_j \equiv 0(mod\ m_k) \; for \; j \neq k$. This gives, $a_j M_j y_j \equiv 0 \; (mod\ m_k) \; for \; j \neq k$, yielding $x \equiv a_k M_k y_k \; (mod\ m) \equiv a_k(mod\ m)$ as $y_k M_k \equiv 1(mod\ m_k)$ for $1 \leq k \leq r$. To show uniqueness of the solution modulo M, we show that any two solutions are congruent modulo M. Let x_1 and x_2 be two solutions to the simultaneous system of r congruences. Then, $x_1 \equiv a_k(mod\ m_k)$ and $x_2 \equiv a_k(mod\ m_k)$ for $1 \leq k \leq r$, giving $x_1 \equiv x_2 \equiv a_k(mod\ m_k)$. So, $m_k | (x_1 - x_2)$ for each $k, 1 \leq k \leq r$. As $m_1, m_2, \dots, m_r$ are pairwise relatively prime, M being product of them, it follows that $M | (x_1 - x_2)$. Hence, $x_1 \equiv x_2 (mod\ M)$. This shows, that there is unique solution with $0 \leq x \leq M$, and other solutions are congruent modulo M.

Now, let us use Chinese remainder theorem to resolve the multiple congruences introduced at the beginning of the article, namely $x \equiv 4(mod\ 7) \; and \; x \equiv 1(mod\ 6)$. Here $a_1 = 4, m_1 = 7, a_2 = 1, m_2 = 6, \gcd(7,6) = 1, M = 7 \cdot 6 = 42, M_1 = \frac{M}{m_1} = \frac{42}{7} = 6$ $M_2 = \frac{M}{m_2} = \frac{42}{6} = 7$. Now, $y_k \equiv M_k^{-1}(mod\ m_k)$; for $k = 1, 2$. $y_1 \equiv M_1^{-1}(mod\ m_1)$; $y_1 \equiv 6^{-1}(mod\ 7) \equiv 6(mod\ )7 = 6$ and $y_2 \equiv 7^{-1}(mod\ 6) \equiv 1^{-1}(mod\ )6 \equiv 1(mod\ )6 = 1$. $x = a_1 M_1 y_1 + a_2 M_2 y_2 = 4 \cdot 6 \cdot 6 + 1 \cdot 7 \cdot 1 = 144 + 7 = 151(mod\ 42) = 25$

Let us apply Chinese remainder theorem to the Chinese puzzle.

Example 1 : Solve the system of linear congruences

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 5)$$
$$x \equiv 2(mod\ 7)$$

Solution: Here $a_1 = 2, m_1 = 3, a_2 = 3, m_2 = 5, a_3 = 2, m_3 = 7$. m_1, m_2, m_3 are pairwise relatively prime nos, $M = 3 \cdot 5 \cdot 7 = 105, M_1 = \frac{M}{m_1} = \frac{105}{3} = 35, M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$, and $M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$. Now, $y_k \equiv M_k^{-1}(mod\ m_k)$; for $k = 1, 2, 3$. So, $y_1 \equiv M_1^{-1}(mod\ m_1)$; $\equiv 35^{-1}(mod\ 3)$. As $35(mod\ 3) \equiv 2(mod\ 3)$, it gives $35^{-1}(mod\ 3) \equiv 2^{-1}(mod\ 3) \equiv$

$2(mod\ 3)$. Similarly, $y_2 \equiv M_2^{-1}(mod\ m_2) \equiv 21^{-1}(mod\ 5) \equiv 1^{-1}(mod\ 5) \equiv 1(mod\ 5)$ and $y_3 \equiv 15^{-1}(mod\ 7) \equiv 1^{-1}(mod\ 7) \equiv 1(mod\ 7)$. Now, form the sum
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23(mod\ 105)$.

23 is the smallest positive integer that simultaneously satisfies the three given linear congruences. If one wishes to verify the solution, it can be seen that $23 \equiv 2(mod\ 3), 23 \equiv 3(mod\ 5), 23 \equiv 2(mod\ 7)$.

Oystein Ore mentions a puzzle with a dramatic element from Brahma-sphuta-siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

Example 2 : An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?
Solution : Let the number of broken eggs be x. x satisfies :

$$x \equiv 1(mod\ 2)$$
$$x \equiv 1(mod\ 3)$$
$$x \equiv 1(mod\ 4)$$
$$x \equiv 1(mod\ 5)$$
$$x \equiv 1(mod\ 6)$$
$$x \equiv 0\ (mod\ 7)$$

The first congruence says that x is odd, let us keep this in mind and ignore this congruence. To be able to use the Chinese remainder theorem, we need to omit the congruence $x \equiv 1(mod\ 6)$ so that the moduli of the remaining congruences (3, 4, 5 and 7) are relatively prime in pairs. Application of Chinese remainder theorem gives $x = 301$. It can be verified that 301 satisfies the ignored congruences and hence 301 is the smallest number of eggs.

We know, that 561 is a composite number, $561 \equiv 3 \cdot 11 \cdot 17$. The number 561 is the number, which serves as an example to illustrate that converse of Fermat's theorem does not always hold true. (https://www.savitagandhi.com/articles/fermats-little-theorem, (---------book cryptography, ch 4, p …). Let us show that $2^{560} \equiv 1(mod\ 561)$, so that 561 satisfies Fermat's theorem, but is not prime. We shall be using Chinese remainder theorem and Fermat's little theorem.

Example 3 : Show that $2^{560} \equiv 1(mod\ 561)$.
Solution: Fermat's theorem states that if p is prime and a is a positive number, such that p does not divide a, then $a^{p-1} \equiv 1(mod\ p)$. Hence, from Fermat's theorem, with a as 2, and p as 3, $2^2 \equiv 1(mod\ 3)$, giving $2^{560} = (2^2)^{280} \equiv 1(mod\ 3)$. Similarly, $2^{560} = (2^{10})^{56} \equiv 1(mod\ 11)$ and $2^{560} = (2^{16})^{35} \equiv 1(mod\ 17)$. That is,

$$2^{560} \equiv 1(mod\ 3)$$
$$2^{560} \equiv 1(mod\ 11)$$
$$2^{560} \equiv 1(mod\ 17)$$

Let us apply, Chinese remainder theorem now. 2^{560} is a solution of these three congruences, with $x = 2^{560}, m_1 = 3, m_2 = 11, m_3 = 17, a_1 = 1, a_2 = 1, a_3 = 1$, giving

$$2^{560} = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \equiv (M_1y_1 + M_2y_2 + M_3y_3)(mod\ M),$$

where, $M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 11 \cdot 17 = 561,$

$$M_1 = \frac{M}{m_1} = 11 \cdot 17 = 187,\ M_2 = \frac{M}{m_2} = 3 \cdot 17 = 51,\ M_3 = \frac{M}{m_3} = 3 \cdot 11 = 33;$$

and, $y_1 = {M_1}^{-1}(mod\ m_1) \equiv (187)^{-1}\ (mod\ 3) \equiv (1)^{-1}\ (mod\ 3) \equiv 1(mod 3) = 1$

$$y_2 = {M_2}^{-1}(mod\ m_2) \equiv (51)^{-1}\ (mod\ 11) \equiv (7)^{-1}\ (mod\ 11) \equiv 8(mod\ 11) = 8$$

$$y_3 = {M_3}^{-1}(mod\ m_3) \equiv (33)^{-1}\ (mod\ 17) \equiv (16)^{-1}\ (mod\ 17) \equiv 16(mod\ 17) = 16$$

Now, $2^{560} \equiv (M_1y_1 + M_2y_2 + M_3y_3)(mod\ M) \equiv ((187 \cdot 1) + (51 \cdot 8) + (33 \cdot 16))(mod\ 561)$

$$\equiv (187 + 408 + 528)(mod\ 561) \equiv 1123(mod\ 561) \equiv 1(mod\ 561).$$

This proves the result.

****