**The Chinese Remainder Theorem**

Shubho

Jun 28, 2015, 11:59 PM

[**Previously Published Here**](https://sites.google.com/site/vinceandcode/number-theory/the-chinese-remainder-theorem)

|  |
| --- |
| The Great **Sun Tzu.**was a [Chinese](https://en.wikipedia.org/wiki/China) [mathematician](https://en.wikipedia.org/wiki/Mathematician) who lived some time between the 3rd and the 5th century during  the [Wei](https://en.wikipedia.org/wiki/Cao_Wei) or [Jin](https://en.wikipedia.org/wiki/Jin_Dynasty_(265%E2%80%93420)) dynasty. Interested in [astronomy](https://en.wikipedia.org/wiki/Chinese_astronomy) and trying to develop a [calendar](https://en.wikipedia.org/wiki/Chinese_calendar), he investigated  [Diophantine equations](https://en.wikipedia.org/wiki/Diophantine_equation). He is known only for his authorship of [*The Mathematical Classic of Sunzi*](https://en.wikipedia.org/wiki/The_Mathematical_Classic_of_Sunzi), which contains  the earliest known example of the [Chinese remainder theorem](https://en.wikipedia.org/wiki/Chinese_remainder_theorem). source: ([wiki](https://en.wikipedia.org/wiki/Sun_Tzu_(mathematician)))  **Well, The introduction is over, now lets come to the chinese Remainder Theorem**  **what is it?**  **If p1, p2, p3,...pn are  pair wise coprimes and  i1, i2,  i3,.....in are integers then**  **there is a distinct integer x  mod M =  p1. p2. p3...pn**  **that satisfies the system of linear congruences**  x is congruent to i1 (mod p1)  x is congruent to i2 (mod p2)  x is congruent to in (mod pn)  in a nutshell x is congruent to ***i1.M1.y1 + i2M2.y2 + i3.M3.y3 +...+in.Mn .yn  (mod M)***  ***[\*Mi  = M/pi];***  Miyi = 1 (mod pi)  where i = 1,2,3...n;  let's see an example:  lets say  x is congruent to 3 (mod 8)  x is congruent to 1 (mod 9)  x is congruent to 4 (mod 11)  what is x?  out M  = 8\*9\*11 = 792;  M1 = 792/8 = 99;  M2 = 792/9 = 88;  M3 = 792/11 = 72;  ***i1.M1.y1 + i2M2.y2 + i3.M3.y3 +...+in.Mn .yn  (mod M)***  3.99.         +1.88      +4.72.  Miyi = 1 (mod pi)  99 . y1 = 1 (mod 8); or 3 . y1 = 1 (mod 8); or 3 . y1 = 9 (mod 8); or y1 = 3;  88 . y2 = 1 (mod 9);   7. y2 = 1 (mod 9); or 7. y2 = 1 (mod 9); or 7 y2 = 28 (mod 9);  or y2=4;  72 . y3 = 1 (mod 11); or 6.y3 = 1 (mod 11); or 6.y3 = 12 (mod 11); or y3 = 2;   3.99. 3   +1.88.3     +4.72.2    = 1819;  (this is not the only value, you can find many more! )  so x = 1819  now grab your calculator and calculate, you'll see  1819 is congruent to 3 (mod 8)  1819 is congruent to 1 (mod 9)  1819 is congruent to 4 (mod 11)   and this is what Chinese Remainder Theorem is. Have a nice day |