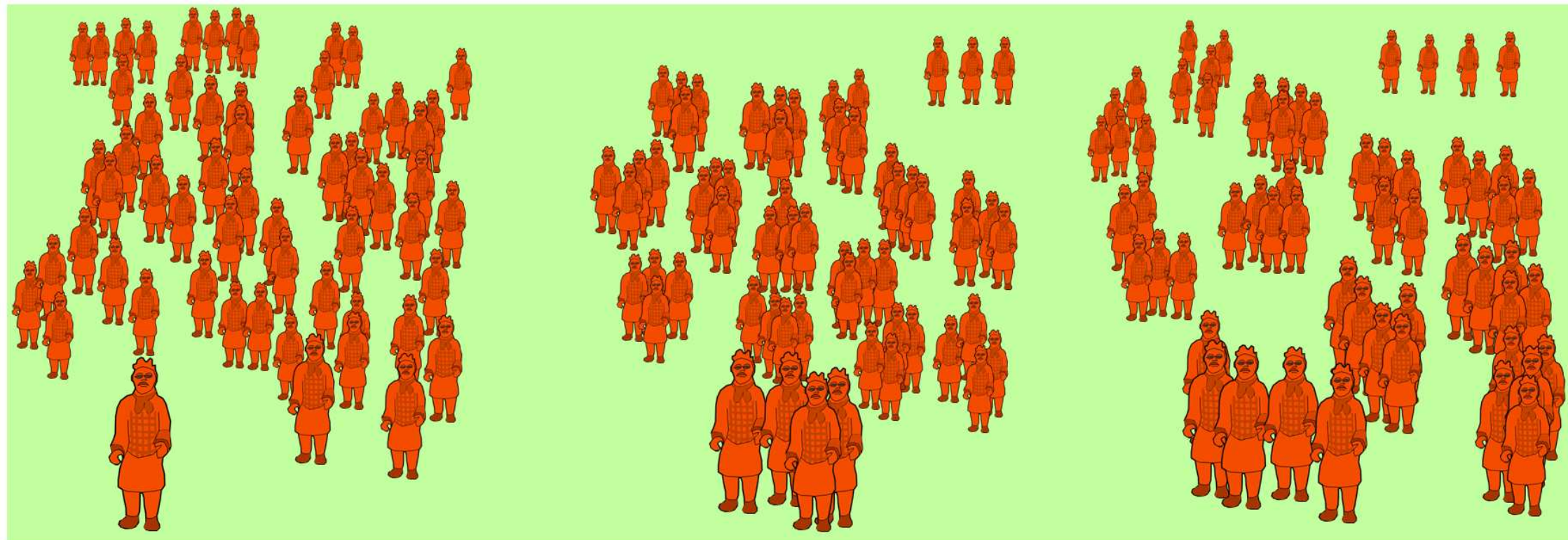




# THEOREM OF THE DAY

**The Chinese Remainder Theorem** Suppose  $n_1, n_2, \dots, n_r$  are mutually coprime positive integers (that is, no integer greater than 1 dividing one may divide any other.) Let  $y_1, y_2, \dots, y_r$  be any integers. Then there is a number  $x$  whose remainder on division by  $n_i$  is  $y_i$ , for each  $i$ . That is, the system of linear congruences  $x \equiv y_i \pmod{n_i}$  has a solution. Moreover this solution is unique modulo  $N = n_1 \times n_2 \times \dots \times n_r$ .



How many people  
What is  $x$ ?

Divided into 4s: remainder 3  
 $x \equiv 3 \pmod{4}$

Divided into 5s: remainder 4  
 $x \equiv 4 \pmod{5}$

Let  $N_i = N/n_i$ , for each  $i$ . Here,  $N = 4 \times 5 = 20$ , so  $N_1 = 5$  and  $N_2 = 4$ . There will be a smallest number, the **inverse** of  $N_i$ , denoted by  $N_i^{-1}$ , for which  $N_i \times N_i^{-1}$  has remainder 1 on division by  $n_i$ ; we write  $N_i N_i^{-1} \equiv 1 \pmod{n_i}$ . We find that  $N_1^{-1} = 1$ , since  $5 \times 1 = 5 = 1 \times 4 + 1$ . Similarly,  $N_2^{-1} = 4$ . Now all solutions are congruent, modulo  $N$ , to  $x = y_1 N_1 N_1^{-1} + y_2 N_2 N_2^{-1} + \dots + y_r N_r N_r^{-1}$ , which for our problem means some multiple of  $N = 20$  plus  $3 \times 5 \times 1 + 4 \times 4 \times 4 = 79$ . In fact  $-1 \times 20 + 79 = 59$  is the correct answer but 79 itself also looks like a possibility for the size of the crowd. We could narrow down the possibilities by dividing the crowd again, into 3s, since 3 is coprime to 4 and 5. Then we get  $x \equiv 359 \pmod{60}$ , giving 59 and 119 as the nearest choices: 59 must be right!

The Chinese Remainder Theorem dates back at least as early as the 3rd century, where it is used in the Mathematical Manual of Sun Zi. It may be applied when the  $n_i$  are not coprime, given suitable conditions on the  $y_i$ .

**Web link:** [crypto.stanford.edu/pbc/notes/numbertheory](http://crypto.stanford.edu/pbc/notes/numbertheory); and the history: [www.math.harvard.edu/~knill/crt/lib.html](http://www.math.harvard.edu/~knill/crt/lib.html).

**Further reading:** *Chinese Remainder Theorem: Applications In Computing, Coding, Cryptography* by Cunsheng Ding, Dingyi Pei and Arto Salomaa, World Scientific, 1996.

