Chinese Remainder Theorem

https://www.cut-the-knot.org/blue/chinese.shtml

> There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

- Sun Tsu Suan-Ching

Let r and s be positive integers which are relatively prime. As a simple example let $r = 4$ and $s = 5$.

Now, write the integers from 1 to $r \times s$:

```
   |   |   |   |   |
o o o o o o o o o o o o o o o o o o o o
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
    |    |    |    |
```

Consider the numbers $n = [1 - rs]$

Compute n mod r and mod s, and write the result as a pair or tuple. For example:

$$10 \equiv (2, 0), \quad 18 \equiv (2, 3)$$

Starting from 1 and ending at 20:

```
(1,1),(2,2),(3,3),(0,4),(1,0),
(2,1),(3,2),(0,3),(1,4),(2,0),
(3,1),(0,2),(1,3),(2,4),(3,0),
```

`(0,1),(1,2),(2,3),(3,4),(0,0)`

It's clear that no two are the same, and since $r \times s = 20$, all possible pairs of remainders are found within this set.

Let a and b be *any* two positive integers. Call their remainders

$$a' = a \bmod r, \quad b' = b \bmod r$$

Then there exists an integer N between $[1 - 20]$ such that

$$N \equiv (a', b') \bmod (r, s)$$

Furthermore, N is uniquely determined.

In addition, there is a family of numbers $N+krs$ $(k = 0, 1, 2 \dots)$. Every number in the family has the same remainder mod r and, similarly, has the same remainder mod s, because krs gives zero remainder with both r and s.

example

Let $r = 5$ and $s = 6$. Suppose $a = 8$ and $b = 11$.

$$a = 8 \equiv 3 \bmod 5$$

$$b = 11 \equiv 5 \bmod 6$$

There must be some $N < rs$ (namely 23), with the same remainders: $N \equiv 3 \bmod 5$ and $N \equiv 5 \bmod 6$. The next such number is $N + rs$.

```
 3   8 13 18 23 28 33 38 43 48 53
 5 11 17 23 29 35 41 47 53
```