

Chinese Remainder Theorem

I have a large bag of sweets. If I share them equally among my 10 children there are 2 sweets left over. If I share them equally among my 7 grandchildren there are 3 sweets left over. How many sweets are in my bag?

If there are x sweets in the bag then $x \equiv 2 \pmod{10}$ and $x \equiv 3 \pmod{7}$

Theorem

This problem has a unique solution for $x = 1, 2, \dots, 70$

Proof (by contradiction)

Assume there are two solutions $x = p$ and $x = q$

$$p \equiv 2 \pmod{10} \quad p \equiv 3 \pmod{7}$$

$$q \equiv 2 \pmod{10} \quad q \equiv 3 \pmod{7}$$

Say $p > q$

$$p \equiv 2 \pmod{10} \quad q \equiv 2 \pmod{10}$$

So $p = q + 10m$ for some positive integer m

$$p \equiv 3 \pmod{7} \quad q \equiv 3 \pmod{7}$$

So $p = q + 7n$ for some positive integer n

So $q + 10m = q + 7n$ so $10m = 7n$

So $10m$ is a multiple of 7

But 10 and 7 have no common factor so m is a multiple of 7

So $m = 7k$ for some positive integer k

So:

$$p = q + 10m \quad m = 7k$$

So $p = q + 70k$

But:

$$1 \leq p \leq 70 \quad 1 \leq q \leq 70$$

Contradiction!

In general:

The simultaneous equations:

$$x \equiv a \pmod{m} \quad x \equiv b \pmod{n} \quad \text{where } m \text{ and } n \text{ have no common factor}$$

have a unique solution for $x=1,2,\dots,mn$

A tedious method to find this solution:

$x=2, \text{mod } 10$ so $x=2,12,22,32,42,52,62$

$x=3, \text{mod } 7$ so $x=3,10,17,24,31,38,45,52,59,66$

This gives the solution $x=52$

Note:

The smallest number of sweets I could have in my bag is 52.

But I could have $52+70L$ sweets in my bag where L is any positive integer.

Can you see why?