From Counting Eggs to Sharing Secrets

How the Chinese Remainder Theorem can help you!

Joe Long

Secret Sharing Problem

Problem: Suppose you are in charge of the missile defense codes of your country and want to give your subordinates the codes in such a manner that they need at least k of them to gather together to launch the missiles, but with any fewer they will be unable to.

Fun(?) Example

Say we encounter a crazy old man with a basket of eggs who has trouble with counting big numbers who tells us that:

1. If he takes out eggs 3 at a time, he is left with 2 in the end.

2. If he takes out eggs 4 at a time, he is left with 3 in the end.

3. If he takes out eggs 5 at a time, he is left with 1 in the end.

Say that an egg basket is not big enough to hold more than 60 eggs.

Answer

He has 11!

Less Fun Example

Say we encounter a crazy old man with a suitcase full of eggs who has trouble with counting big numbers who tells us that:

1. If he takes out eggs 5 at a time, he is left with 4 in the end.

2. If he takes out eggs 8 at a time, he is left with 6 in the end.

3. If he takes out eggs 9 at a time, he is left with 8 in the end.

Say that an suitcase is not big enough to hold more than 360 eggs.

Answer

He has 134...

Chinese Remainder Theorem

Suppose $n_1, \ldots, n_k \in \mathbb{Z}_+$, and n_i, n_j are coprime for all $i \neq j$.

Then, for any $a_1, \ldots, a_k \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$x \equiv a_i \pmod{n_i} \text{ for all } i \in \{1, \ldots, k\}$$

Furthermore, this x is unique modulo $\prod_{i=1}^{k} n_i$.

Secret Sharing Problem

I have a suitcase that I want to lock

I have 3 subordinates

I want all 3 to be there in order to open the suitcase

Secret Sharing Problem

I have a suitcase that I want to lock

I have 3 subordinates

I want any 1 of them to be there in order to open the suitcase

Secret Sharing Problem

I have a suitcase that I want to lock

I have 3 subordinates

I want any 2 of them to be there in order to open the suitcase

Shamir Secret Sharing

Adi Shamir (1979). "How to Share a Secret."

Lagrange Polynomial Interpolation

Suppose $x_1, \ldots, x_k \in F$, F a field.

Then, for any $y_1, \ldots, y_k \in F$, there exists $P(x) \in F[x]$ such that :

$$P(x) \equiv y_i \ (\text{mod} x - x_i) \text{ for all } i \in \{1, \ldots, k\}$$

Furthermore, this $P(x)$ is unique modulo $\prod_{i=1}^{k}(x - x_i)$.

Chinese Remainder Theorem

Suppose $n_1, \ldots, n_k \in \mathbb{Z}_+$, and n_i, n_j are coprime for all $i \neq j$.

Then, for any $a_1, \ldots, a_k \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$x \equiv a_i \pmod{n_i} \text{ for all } i \in \{1, \ldots, k\}$$

Furthermore, this x is unique modulo $\prod_{i=1}^{k} n_i$.