MATH CIRCLE TTU

Number Theory

Chinese Remainder Theorem

The Problem (Ancient Chinese Problem)

On a pirate ship there are 17 pirates who just stole a chest of gold coins. They try to divide these coins equally among the 17 pirates, but there are 3 left over.

The pirates begin a fight and one of them dies.

Once this pirate has died, the others calm down and try to divide all the gold coins equally again. Unfortunately, now there are 10 left over coins.

Another fight begins and another pirate dies.

After this new death, the pirates that are still alive try to divide the coins equally yet again. This time it is possible and there are no left over coins.

What is the minimum possible amount of gold coins that the pirates stole?

Systems of Congruences

Example. Solve the following system of congruences:

$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 3)\,, \\ x \equiv 4 \,(\mathrm{mod}\, 5)\,, \\ x \equiv 6 \,(\mathrm{mod}\, 7)\,. \end{cases}$$

As long as $\gcd(3,5) = \gcd(3,7) = \gcd(5,7) = 1$, there is a solution. Indeed, it is 'unique' modulo $3 \times 5 \times 7 = 105$.

How to Find the Solutions?

(i) We begin with the first congruence: $x \equiv 1 \,(\mathrm{mod}\, 3)$. This means $x = 1 + 3a$ for some integer a.

(ii) We use $x = 1 + 3a$ in the second congruence (that is, in $x \equiv 4 \,(\mathrm{mod}\, 5)$). We have:

$$1 + 3a \equiv 4 \,(\mathrm{mod}\, 5) \iff 3a \equiv 3 \,(\mathrm{mod}\, 5)\,.$$

(iii) We now need to "divide" by 3 modulo 5. Do you remember? Using the extended Euclidean algorithm we obtain:

$$1 = 2 \times 3 + (-1) \times 5\,.$$

That is, "dividing" by 3 modulo 5 is the same as "multiplying" by 2. Then,

$$3a \equiv 4 \,(\mathrm{mod}\, 5) \iff a \equiv 6 \,(\mathrm{mod}\, 5) \iff a \equiv 1 \,(\mathrm{mod}\, 5)\,,$$

because 6 is the same as 1, modulo 5. This means that $a = 1 + 5b$ for some integer b.

(iv) We go back and substitute this in x,

$$x = 1 + 3a = 1 + 3(1 + 5b) = 4 + 15b\,.$$

(v) We use $x = 4 + 15b$ in the last congruence (that is, in $x \equiv 6 \,(\mathrm{mod}\, 7)$). We have:

$$4 + 15b \equiv 6 \,(\mathrm{mod}\, 7) \iff 15b \equiv 2 \,(\mathrm{mod}\, 7)\,.$$

(vi) We need to "divide" by 15 modulo 7. From the extended Euclidean algorithm:

$$1 = 1 \times 15 + (-2) \times 7\,.$$

That is, "dividing" by 15 modulo 7 is the same as "multiplying" by 1. Then,

$$15b \equiv 2 \,(\mathrm{mod}\, 7) \iff b \equiv 2 \,(\mathrm{mod}\, 7)\,.$$

This means that $b = 2 + 7c$ for some integer c.

(vii) We go back again and substitute in x,

$$x = 4 + 15b = 4 + 15(2 + 7c) = 34 + 105c\,.$$

(viii) The solutions are: $x = 34 + 105c$. They are "unique" modulo 105.

Solve the Problem

Problem 1. On a pirate ship there are 17 pirates who just stole a chest of gold coins. They try to divide these coins equally among the 17 pirates, but there are 3 left over.

The pirates begin a fight and one of them dies.

Once this pirate has died, the others calm down and try to divide all the gold coins equally again. Unfortunately, now there are 10 left over coins.

Another fight begins and another pirate dies.

After this new death, the pirates that are still alive try to divide the coins equally yet again. This time it is possible and there are no left over coins.

What is the minimum possible amount of gold coins that the pirates stole?

Another Problem

Problem 2. The number of students in a school is between 500 and 600. If we group them into groups of 12, 20, or 36 each, 7 students are always left over. How many students are in this school?