Chinese Remainder Theorem

Math Circle at Washington University

Chinese Remainder Theorem is originally form of the theorem, contained in a third-century AD book Sun Zi suanjing (孫子算經 The Mathematical Classic by Sun Zi) by Chinese mathematician Sun Tzu and later republished in a 1247 book by Qin Jiushao, the Shushu Jiuzhang (數書九章 Mathematical Treatise in Nine Sections) is a statement about simultaneous congruences (see modular arithmetic).

Today, we are going to spend 90 minutes here on solving the original problem with step by step questions and at last, we solve the more general problem.

Activity 1: Solve an easier problem

We start it from a easier question other than the original one. what is the single lowest number which, if repeatedly divided by 2 gives a remainder of 1, when divided by 3 gives a remainder of 1?

Step I: Let's break up these conditions

How many conditions we encountered here? Can you denote them as "condition 1", "condition 2", and so on.

Step II: Now, consider the only first condition

Can you find 5 lowest numbers which has a remainder of 1 if divided by 2. Circle the lowest.(Please make sure, we have two conditions.)

Step III: Combine condition 2 with condition 1:

Can you find 5 lowest numbers which has a remainder of 1 if divided by 2, and a remainder of 1 if divided by 3? Again, circle the lowest one. Please note: The candidates are those numbers you got in Step II.

And the lowest one in the Step III is the solution of Activity 1. Can you check it if satisfy condition 1 and condition 2.

Activity 2: Solve the Original Problem

The Original Question is what is the single lowest number which, if repeatedly divided by 3 gives a remainder of 2, when divided by 5 gives a remainder of 3, and when divided by 7 gives a remainder of 2?

Step I: Let's break up those conditions

How many conditions we encountered here? Can you denote them as "condition 1", "condition 2", and so on.

Step II: Now, just consider the first condition:

Can you find the 4 lowest numbers which has a remainder of 2 if divided by 3, which one is the lowest.

Step III: Now, the following one is not too hard, right?

Can you find 4 lowest numbers which has a remainder of 2 if divided by 3, and a remainder of 3 if divided by 5? Please note: The candidates are those numbers you got in Step II.

Step IV: Let's finish this original question:

Can you find 2 lowest numbers which has a remainder of 2 if divided by 3, a remainder of 3 if divided by 5 and a remainder of 2 if divided by 7? Again, tell me the lowest one.

Activity 3: Make It a Little Further

A woman who tells a policeman that she lost her basket of eggs, and that if she took three at a time out of it, she was left with 1 if she took five at a time out of it, she was left with 2, if she took eleven at a time out of it she was left with 9, and to tell her how many eggs she must have had at least.

Let's imitate the procedure of last activity.

Step I: Break up conditions:

How many conditions we have it here?

Step II: Consider the first condition:

Can you find 4 lowest numbers which has a remainder of 1 if divided by 3, circle the lowest.

Step III: Now, bring the second condition here?

Can you find 4 lowest numbers which has a remainder of 1 if divided by 3, and a remainder of 2 if divided by 5. Circle the lowest one.

Step IV: Let's finish this question:

Can you find a number in result of the Step III which has a remainder of 1 if divided by 3, a remainder of 2 if divided by 5 and a remainder of 9 if divided by 11. Is it the lowest one that the lady can have?

Activity 4: Do the following question on your own:

Find the two lowest numbers which has remainder of 2 if divided by 3, remainder of 7 if divided by 11 and remainder of 4 if divided by 13. And tell me the lowest one. You'll be appreciated, if you can find three lowest numbers.

Activity 5: Observation

Let's look at the Activity 3, we have gotten the lowest number, but if we want to obtain the second lowest number, what should we do? Certainly, it is enough if we know the difference between the lowest number and the second lowest one. Let's revise our Activity 1 and Activity 2 firstly.

Step I: The law hidden in Activity 1

Write 5 lowest numbers in Step II and III of Activity 1. Compute the difference of adjacent numbers for each step. Can you find the law of difference? What do they equal to?

Step II: Look at the Activity 2:

Write 4 lowest numbers in Step II, III and of Activity 2 and two lowest numbers in Step IV of Activity 2. Compute the difference of adjacent numbers for each step. Can you find the law now? What do they equal to? (Hint: compute 3×5 and $3\times5\times7$ also.)

Step III: Revise the Activity 3

Did you find the law of difference of adjacent numbers? So can you guess what's the answer I asked at the beginning of Activity 5?

Activity 6: The General Formula

Absolutely, we can make a table for Activity 2. Let n_1, n_2 and n_3 be the numbers we used to divide the unknown, and a_1, a_2 and a_3 be the remainders. And can you complete the table below

n_1	n_2	n_3	a_1	a_2	a_3	the lowest one	the difference between the adjacent numbers
3	5	7	2	3	2		

Can you make a similar table for Activity 3?

n_1	n_2	n_3	a_1	a_2	a_3	the lowest one	the difference between the adjacent numbers

Now, we obtain a general theorem.

Suppose n_1, n_2, n_3 are positive integers which are pairwise coprime.(if you don't understand these words, that's OK. Skip them) Then, for any given sequence of integers a_1,a_2,a_3, there exists an integer x such that it has a remainder of a_1 if divided by n_1, a remainder of a_2, if divided by n_2 and a remainder of a_3, if divided by n_3.Moreover, two adjacent numbers have difference of $n_1n_2n_3$. Can you verify it with numbers in Activity 4 and make a table for it?.

Activity 7: The General Formula (You might finish it at home)

You have seen the general formula for 3 conditions. Can you imagine a general formula for 4 conditions, 5 conditions and so on?