

CHINESE REMAINDER THEOREM
MATH CIRCLE AT WASHINGTON UNIVERSITY IN ST. LOUIS, APRIL 19, 2009
Baili MIN

In a third-century A. D. Chinese book “*Sun Tzu’s Calculation Classic*” one problem is recorded which can be translated into English as:

Suppose we have an unknown number of objects. When counted in threes, 2 are left over, when counted in fives, 3 are left over, and when counted in sevens, 2 are left over. How many objects are there?

For today’s adventure we are going to explore the solutions to this kind of problems to see if we can learn some general method. Let’s go!

**1 “I wandered lonely as a cloud,
That floats on high o’er vales and hills”**

Problem 1.1 Find the smallest positive integer d_1 that can be evenly divided by 5 and 7 but has remainder 1 when divided by 3.

Remark: There are some notations we will use a lot later. If you divide 5 by 3 you get the remainder 2, so we write $5 \equiv 2 \pmod{3}$. More generally, if you divide x by z and get a remainder y , so we can imagine that $x = y + k \times z$ for some integer k , and therefore we write $x \equiv y \pmod{z}$. (Notice the positions for x , y and z .)

Perhaps you want to do some exercises before putting your hands on this problem.

$$\begin{aligned} 5 &\equiv \bigcirc \pmod{2} \\ 8 &\equiv \bigcirc \pmod{3} \\ 100 &\equiv \bigcirc \pmod{7} \end{aligned}$$

So far so good? Return to the problem, then notations for those conditions are:

$$\begin{aligned} d_1 &\equiv 1 \pmod{3} \\ d_1 &\equiv 0 \pmod{5} \\ d_1 &\equiv 0 \pmod{7} \end{aligned}$$

What to do next?

Hint: The condition of being exactly divided 5 and 7 is equivalent to that being exactly divided by $35 = 5 \times 7$, or d_1 is a multiple of 35, or $d_1 = k \times 35$ where $k = 1, 2, 3, \dots$. So for this condition, you can write a list of numbers:

Then from those numbers, just pick the smallest number which satisfies the first condition: the remainder of d_1 divided by 3 is 1, or $d_1 \equiv 1 \pmod{3}$. So, what is your answer?

We can do more similar problems, and these problems(together with the previous one) will help us to solve the classic problem at the beginning.

Problem 1.2 Find the smallest positive integer d_2 which is evenly divided by 3 and 7(or mathematically $d_2 \equiv 0 \pmod{3}$ and $d_2 \equiv 0 \pmod{7}$) and its remainder if divided by 5 is 1(or mathematically $d_2 \equiv 1 \pmod{5}$).

Hint: Again, from the last two conditions, you can write a list of numbers which are multiples of (some integer you want to find), or of the form $k \times \bigcirc$ where $k = 1, 2, \dots$. (How to fill in this circle? Refer to the first step in the previous problem.)

Then from those numbers, just pick the smallest number which satisfies the first condition: the remainder of d_2 divided by 5 is 1 or $d_2 \equiv 1 \pmod{5}$. So, what is your answer?

One more:

Problem 1.3 Find the smallest positive integer d_3 such that $d_3 \equiv 0 \pmod{3}$, $d_3 \equiv 0 \pmod{5}$ and $d_3 \equiv 1 \pmod{7}$.

Hint: What do the three conditions tell us?

Same steps as in the previous two problems. But remember to make some necessary modifications.

Problem 1.4 Now go to our classic problem, which reads mathematically:

Suppose x is a positive integer and it satisfies three conditions:
 $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$. Find such x .

We solve that in the following way:

The remainders are different from those three problems we have done. Calculate the number $d = 2 \times d_1 + 3 \times d_2 + 2 \times d_3$.

Does d solve our classic problem?

Does $d - 2 \times 105$, if $d > 2 \times 105$, solve the problem?

Does $d - 105$, if $d > 105$, solve the problem?

Does $d + 105$ also solve the problem?

Does $d + 2 \times 105$ also solve the problem?

Does $d + 3 \times 105$ also solve the problem?

Does $d + 10 \times 105$ also solve the problem?

Now can you guess what the for the general expression for the solution to our classic problem is?

If you have got an expression as $X = Y + k \times Z$, where k is any integer, you can reexpress it as a shorter mathematical formula: $X \equiv Y \pmod{Z}$. After you finish this, please turn to the next page to compare the result. :)

2 “More welcome notes to weary bands, Of travellers in some shady haunt, Among Arabian sands.”

“*Sun Tzu’s Calculation Classic*” provided the solution: “ those integers x with $x \equiv 233 \pmod{105}$.” But this is only true for that specific problem with those divisors and remainders. What if we change the divisors and remainders? It didn’t say.

In his book “*Mathematical Treatise in Nine Sections*” written in 1247 A.D. , a Chinese mathematician Jiushao QIN gave an algorithm which could be used to solve more generalized problem. This is the origin of “**Chinese Remainder Theorem**”.

Notice the number 105, it can be factorized as $105 = 3 \times 5 \times 7$. So to summarize what we have done:

Step 1 Solve those three problems separately. (We solved three things: $d_1 \equiv 1 \pmod{3}$ but is a multiple of 5×7 ; $d_2 \equiv 1 \pmod{5}$ but is a multiple of 3×7 and $d_3 \equiv 1 \pmod{7}$ but is a multiple of 3×5 .)

Step 2 Multiply the remainder of those results respectively and find their summation d . (d_1 corresponds to the divisor 3, whose remainder is 2, so we have $2 \times d_1$; d_2 corresponds to the divisor 5, whose remainder is 3, so we have $3 \times d_2$ and d_3 corresponds to the divisor 7, whose remainder is 2, so we have $2 \times d_3$, and putting these together we get the summation $d = 2 \times d_1 + 3 \times d_2 + 2 \times d_3$.)

Step 3 Find the product of these divisors, denoted by m . ($m = 3 \times 5 \times 7 = 105$ in the previous case.)

Step 4 Express the final solution x by the formula $x \equiv d \pmod{m}$. (like $x \equiv 233 \pmod{105}$.)

One remark is that this expression contains ALL solutions to this problem. You may spend some time checking integers from 1 to 500, and will see that there are no exceptions.

We will continue to explore this method.

Problem 2.1 Suppose x is an integer which satisfies $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{11}$ and $x \equiv 3 \pmod{17}$. Find all such x .

Step 1 Solve those three problems separately:

$d_1 \equiv 1 \pmod{3}$ and $d_1 \equiv 0 \pmod{\circ \times \circ}$, or equivalently $d_1 = k \times \circ \times \circ$ where k is any integer:

$d_2 \equiv 1 \pmod{11}$ and $d_2 \equiv 0 \pmod{\circ \times \circ}$, or equivalently $d_2 = k \times \circ \times \circ$ where k is any integer:

$d_3 \equiv 1 \pmod{17}$ and $d_3 \equiv 0 \pmod{\circ \times \circ}$, or equivalently $d_3 = k \times \circ \times \circ$ where k is any integer:

Step 2 Find d .

$$d = \circ \times d_1 + \circ \times d_2 + \circ \times d_3 =$$

Step 3 Find m .

$$m = \circ \times \circ \times \circ = \circ$$

Step 4 Express the final solution.

$$x = \circ + k \times \circ, \text{ where } k \text{ is any integer or } x \equiv \circ \pmod{\circ}$$

You should list some numbers from your final expression and verify that they solve the problem!

3 “Sometime too hot the eye of heaven shines, And often is his gold complexion dimm’d”

Is this method always valid? Let’s try this problem:

Problem 3.1 *Suppose x is a positive integer which satisfies $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{4}$ and $x \equiv 1 \pmod{5}$. Find all such x .*

By our previous method, what do you get?

Have troubles? Please turn to the next page.

I am guessing that you were stuck at even the first step using the previous method: you should get $d_1 \equiv 1 \pmod{2}$ and $d_1 \equiv 0 \pmod{4 \times 5}$. But for the first condition we know that d_1 should be an odd number, and for the second one we know that d_1 should be an even number. Obviously, that is impossible!

So, what went wrong?

For our first project, the divisors are 3, 5 and 7. You can see that for each pair of them, they are coprime, that is, the common divisor is only 1. For the second project, the divisors are 3, 11 and 17, each pair of which is still coprime. But is that the same for the third project? Very unfortunately, no, because of 2, 4 and 5, the pair of 2 and 4 is not coprime as 2 is a common divisor for both of them.

Actually for that method we require that all divisors are pairwise coprime.

What if not all pairs are coprime? The idea is natural: “convert” them so that they are coprime. But the process is a little complicated and tricky. We will see that from the following problem.

Problem 3.2 List all numbers x greater or equal to 1 but less than 30, such that

(a) $x \equiv 1 \pmod{2}$

(b) $x \equiv 1 \pmod{4}$.

Can you see some relation between those two groups of numbers?

Problem 3.3 So one condition is unnecessary and you can drop it. What is it?

Problem 3.4 Now after dropping the unnecessary condition, are the divisors pairwise coprime?

Problem 3.5 If so, apply our original method again. What solutions can you get?

4 “And then, there were none.”

Let’s continue with the trick of converting divisors which are not pairwise coprime. The big problem we are going to solve is actually from the course *Number Theory and Polynomials* I took in my college.

Solve for x which satisfies $x \equiv 3 \pmod{8}$, $x \equiv 11 \pmod{20}$, and $x \equiv 1 \pmod{15}$.

We are going to crack it by solving the following problems:

Problem 4.1 Find a positive integer i_1 such that $x \equiv 11 \pmod{4}$ is equivalent to $x \equiv i_1 \pmod{4}$.

Hint: Filling the circles: $x \equiv 11 \pmod{4}$ means

$$\begin{aligned}x &= 11 + k \times 4 \\ &= \bigcirc + 2 \times 4 + k \times 4 \text{ (breaking 11 into two parts)} \\ &= \bigcirc + (k + 2) \times 4\end{aligned}$$

So $x \equiv 11 \pmod{4}$ is equivalent to $x \equiv \bigcirc \pmod{4}$, thus i_1 is just the number \bigcirc .

Problem 4.2 Find a positive integer i_2 such that $x \equiv 11 \pmod{5}$ is equivalent to $x \equiv i_2 \pmod{4}$.

Hint: Filling the circles: $x \equiv 11 \pmod{5}$ means

$$\begin{aligned}x &= 11 + k \times 5 \\ &= \bigcirc + 2 \times 5 + k \times 5 \text{ (breaking 11 into two parts)} \\ &= \bigcirc + (k + 2) \times 5\end{aligned}$$

So $x \equiv 11 \pmod{5}$ is equivalent to $x \equiv \bigcirc \pmod{5}$, thus i_2 is just the number \bigcirc .

One important result we need to know is $x \equiv 11 \pmod{20}$, or $x \equiv 11 \pmod{4 \times 5}$ is equivalent to two equations: $x \equiv 11 \pmod{4}$ and $x \equiv 11 \pmod{5}$.

And I believe you have simplified the last two equations. So now we have an equivalent series of conditions(fill in those circles):

$$x \equiv 3 \pmod{8}, x \equiv \bigcirc \pmod{4}, x \equiv \bigcirc \pmod{5} \text{ and } x \equiv 1 \pmod{15}$$

Examine the first two conditions:

Problem 4.3 $x \equiv 3 \pmod{8}$ and $x \equiv \bigcirc \pmod{4}$ (\bigcirc is whatever you got previously) can be reduced to one condition. What is that?

Hint: Refer to a problem on Page 7. So your answer would be $x \equiv \bigcirc \pmod{\bigcirc}$.

Before rushing to the next step, we summarize what we have done so far: The original conditions are now converted to:

$$x \equiv \bigcirc \pmod{\bigcirc}, x \equiv \bigcirc \pmod{5} \text{ and } x \equiv 1 \pmod{15}$$

Very unluckily, 5 and 15 are still not relatively coprime. So there is still some work to do. We want to convert the case for the divisor $15 = 3 \times 5$

Problem 4.4 $x \equiv 1 \pmod{15}$ is equivalent to two equations: $x \equiv i_3 \pmod{3}$ and $x \equiv i_4 \pmod{5}$. Find positive integers i_3 , which should be less or equal to 3, and i_4 , which should be less or equal to 5.

Hint: Mimicking the stated result at the bottom on Page 8, you should guess $x \equiv \bigcirc \pmod{3}$ and $x \equiv \bigcirc \pmod{5}$. Make sure your two numbers are no greater than 3 and 5 respectively.

Again, we summarize that the new conditions we need to consider to solve the problem are (fill in those circles):

$$x \equiv \bigcirc \pmod{\bigcirc}, x \equiv \bigcirc \pmod{5}, x \equiv \bigcirc \pmod{3} \text{ and } x \equiv \bigcirc \pmod{5}$$

Notice that the second and the fourth should be identical. Otherwise you must have made some mistakes somewhere. For those two identical conditions, you can just cross one of them out. After you get your results, you can turn to the next page to check.

The new conditions are $x \equiv 3 \pmod{8}$, $x \equiv 1 \pmod{5}$ and $x \equiv 1 \pmod{3}$. Now we are able to solve our final problem:

Problem 4.5 Find x which satisfies $x \equiv 3 \pmod{8}$, $x \equiv 1 \pmod{5}$ and $x \equiv 1 \pmod{3}$.

Just mimic the steps on Page 5 (Ah, a good chance to review the method!). Try to solve this problem here. And, since this problem is under equivalent conditions as the problem on Page 8, we can kill two birds with one stone! :D

5 “And miles to go before I sleep, And miles to go before I sleep.”

The mathematics related to this topic is something about congruence relation, or even further, something about rings, ideals. If you are interested, you may try to read some textbooks on number theory. You don't need any calculus knowledge to do that.