QR 28
CHINESE REMAINDER THEOREM
NOVEMBER 15, 2008

David Roe

Suppose that I have an integer a, and I know

$$a \equiv 11 \pmod{20}.$$

Question 1. *Can I conclude anything about $a \pmod{n}$ for other n?*

The investigation of this question will lead us to the Chinese Remainder Theorem.

REDUCING MODULO DIVISORS

If we unravel the statement that $a \equiv 11 \pmod{20}$, what is it saying? What are the possibilities for a?

We've specified the remainder after dividing a by 20, so a must be one of the following sequence of numbers:

$$\ldots, -29, -9, 11, 31, 51, 71, \ldots$$

and moreover, any of these are possible given that our only restriction on a is that $a \equiv 11 \pmod{20}$.

Let's try reducing each of the numbers in this list modulo different n and seeing what we get.

n	Our list $\pmod{n}$
2	$\ldots, 1, 1, 1, 1, 1, 1, \ldots$
3	$\ldots, 1, 0, 2, 1, 0, 2, \ldots$
4	$\ldots, 3, 3, 3, 3, 3, 3, \ldots$
5	$\ldots, 1, 1, 1, 1, 1, 1, \ldots$
6	$\ldots, 1, 3, 5, 1, 3, 5, \ldots$
7	$\ldots, 6, 5, 4, 3, 2, 1, \ldots$
8	$\ldots, 3, 7, 3, 7, 3, 7, \ldots$
9	$\ldots, 7, 0, 2, 4, 6, 8, \ldots$
10	$\ldots, 1, 1, 1, 1, 1, 1, \ldots$

The first pattern that jumps out at us from this table is that some of the sequences are constant. In these cases, knowing that $a \equiv 11 \pmod{20}$ *determines* $a \pmod{n}$. This happens for the following n among those we considered:

$$2, 4, 5, 10.$$

Question 2. *How are these numbers (2, 4, 5, 10) related to* 20*?*

While you think about that for a bit, let's take a look at other patterns in the table. Modulo 3, apparently we learn nothing from the statement that $a \equiv 11 \pmod{20}$. All three possibilities mod 3 are appearing, and they seem to be appearing equally frequently. Similarly, all possibilities seem to be occurring modulo 7 and 9.

Question 3. *How are these numbers (3, 7, 9) related to* 20*?*

There are two other ns in our table, namely 6 and 8. For these n, we seem to have gained some sort of partial information: knowing that $a \equiv 11 \pmod{20}$ is not enough to determine $a \pmod{6}$, but it is enough to rule out the possibility that $a \equiv 4 \pmod{6}$.

Question 4. *How are these numbers (6, 8) related to* 20*? How are they distinguished from the other kinds of numbers in Questions 2 and 3?*

Think about all of this for a bit. Can you figure out what's going on?

Answer.

(a) The numbers in Question 2 (2, 4, 5, 10) are all divisors of 20*.*

(b) The numbers in Question 3 (3, 7, 9) are all relatively prime to 20 *(ie they have no common factors with* 20*).*

(c) The numbers in Question 4 (6, 8) all share a common factor with 20*, but are not themselves divisors.*

What's going on here? Let's address Question 2 first. Suppose that n is a divisor of 20. Then we already know what the remainder after dividing a by n is! Since 20 is a multiple of n, the remainder after dividing a by n is the same as the remainder after dividing 11 by n. For example, the remainder after dividing a by 4 is the same as dividing 11 by 4, namely 3.

Let's rephrase this another way. Knowing that $a \equiv 11 \pmod{20}$ means that $a = 11 + 20k$, where k is allowed to be anything. If we reduce a modulo a divisor d of 20 ($d = 4$ for example), then $20k$ will still be zero, and we'll get $a \equiv 11 \pmod{d}$. More generally, we have

Proposition 1. *Knowing an integer modulo* m *determines it modulo any divisor of* m*.*

What about Question 3? Suppose that n is relatively prime to 20, say $n = 3$ for example. We know that $a = 11 + 20k$ for some k. But this gives us nothing now! Let's try to figure out what a is modulo 3. We know that $a \equiv 2 + 2k \pmod{3}$. But since 2 is relatively prime to 3, a can be anything modulo 3. Namely, if we fix a modulo 3 (say we want $a \equiv 1 \pmod{3}$), then we can find a k to make it so: the equation $1 \equiv 2 + 2k \pmod{3}$ is solvable since 3 is relatively prime to 2 (or equivalently, to 20).

Proposition 2. *Knowing an integer modulo* m *gives no information about it modulo anything relatively prime to* m*.*

The answer to Question 4 lies somewhere in between. I'll leave it to you to work out the details in this case, because we have another important question to ask.

Question 5. *What if we're stubborn, and don't take the fact that we can't figure out* $a \pmod{3}$ *calmly. Suppose that we require that* $a \equiv 0 \pmod{3}$*, in addition to our earlier requirement that* $a \equiv 11 \pmod{20}$*. What can we say about* a *now?*

The Chinese Remainder Theorem

From our list of possibilities for a, we cross off the ones that are not $0 \pmod{3}$. This gives

$$\ldots, -69, -9, 51, 111, \ldots$$

Notice that, in the resulting list, each possibility differs from the next by 60. This means that we've determined a modulo 60!

This idea generalizes.

Theorem 1 (Chinese Remainder Theorem)**.** *Suppose that* m *and* n *are relatively prime. Given a number* $a \pmod{m}$ *and another number* $b \pmod{n}$*, there is some* x *such that* $x \equiv a \pmod{m}$ *and* $x \equiv b \pmod{n}$*. Moreover, this* x *is uniquely determined modulo* mn*.*

Since Proposition 1 tells us that knowing x modulo mn determines x modulo m and x modulo n, we can rephrase the theorem as

Theorem 2 (CRT, version 2)**.** *Suppose that* m *and* n *are relatively prime. Then knowing a number modulo* mn *is equivalent to knowing it modulo* m *and knowing it modulo* m*.*

How about some more examples. We've already seen that

$$\left.\begin{array}{l} a \equiv\ 11 \pmod{20} \\ a \equiv\ 0 \quad \pmod{3} \end{array}\right\} \qquad \Leftrightarrow \qquad a \equiv 51 \pmod{60}.$$

If we impose the conditions that $a \equiv 4 \pmod{45}$ and $a \equiv 3 \pmod{4}$ then we need to find something that's $3 \pmod{4}$ from the sequence $4, 49, 94, 139, 184, \ldots$, the first of which is 139. So

$$\left.\begin{array}{l} a \equiv\ 4 \pmod{45} \\ a \equiv\ 3 \pmod{4} \end{array}\right\} \qquad \Leftrightarrow \qquad a \equiv 139 \pmod{180}.$$

If we know instead that $a \equiv 8 \pmod{21}$ and $a \equiv 4 \pmod{10}$ then we consider the possible $a \equiv 8 \pmod{21}$, and find one that ends in a 4: $29, 50, 71, 82, 103, 124$ and so

$$\left.\begin{array}{l} a \equiv\ 8 \pmod{21} \\ a \equiv\ 4 \pmod{10} \end{array}\right\} \qquad \Leftrightarrow \qquad a \equiv 124 \pmod{210}.$$

An Algorithm

So far we've been finding a solution using what is basically brute force. There is a better way.

Since the m and n in the statement of the Chinese Remainder Theorem are relatively prime, we can find an x and y with

$$mx + ny = 1.$$

Then

$$mx \equiv 1 \pmod{n} \text{ and } mx \equiv 0 \pmod{m},$$

while

$$ny \equiv 0 \pmod{n} \text{ and } ny \equiv 1 \pmod{m}.$$

So

$$\begin{aligned} bmx + any &\equiv b \cdot 1 + a \cdot 0 \pmod{n} \\ &\equiv b \qquad\qquad\quad \pmod{n}, \end{aligned}$$

and

$$\begin{aligned} bmx + any &\equiv b \cdot 0 + a \cdot 1 \pmod{n} \\ &\equiv a \qquad\qquad\quad \pmod{n}. \end{aligned}$$

Thus $bmx + any$ is a solution modulo mn.

To summarize,

Algorithm (Chinese Remainder Theorem)**.**

Objective: find a number congruent to $a \pmod{m}$ *and* $b \pmod{n}$*:*

1. *Use the Euclidean algorithm to express 1 as a combination of* m *and* n*:* $1 = mx + ny$*.*
2. *The answer is* $bmx + any \pmod{mn}$*.*

Let's take a look at this algorithm in action.

Problem 1. *Suppose that* $a \equiv 73 \pmod{101}$ *and* $a \equiv 44 \pmod{99}$*. Find* $a \pmod{99}$*.*

Answer.

1. *Use the Euclidean algorithm to express 1 as a combination of* 101 *and* 99*.*

$$\begin{aligned} 101 &= 1 \cdot 99 + 2 \\ 99 &= 49 \cdot 2 + 1 \end{aligned}$$

So $1 = 99 - 49 \cdot 2 = 99 - 49 \cdot (101 - 99) = 50 \cdot 99 - 49 \cdot 101$*.*

2. *Thus the answer is* $50 \cdot 99 \cdot 73 - 49 \cdot 101 \cdot 44 \equiv 3608 \pmod{9999}$*.*

Problem 2. *Suppose that you have a deck of playing cards. After playing with them for a while, you notice that some of the cards are missing. You deal them out into piles of five, and notice that there are four left over. Similarly, when you deal them out into piles of nine, there are three left over. How many cards are there in the deck?*

Answer.

1. *Use the Euclidean algorithm to express 1 as a combination of* 5 *and* 9*. Well, you can do so, or just note that* $2 \cdot 5 - 1 \cdot 9 = 1$.

2. *So the answer is* $2 \cdot 5 \cdot 3 - 1 \cdot 9 \cdot 4 = 30 - 36 = -6 \equiv 39 \pmod{45}$.

Because there were 52 cards in the deck before any cards were lost, there must be at most 52 now. Since $39 + 45 = 84 > 52$*, there must in fact be 39 cards left in the deck.*

Generalizations

The Chinese Remainder Theorem has been generalized greatly, though most of those generalizations are beyond the scope of this class. But I do want to mention two generalizations. You will not be responsible for using these versions of the CRT, but one provides an explanation of the name, and the other drops an assumption that might have been bothering you.

Theorem 3 (CRT, version 3)**.** *Suppose that* $m_1, m_2, \ldots, m_l$ *have the property that every pair of them is relatively prime. Then given* $a_1, a_2, \ldots, a_l$*, there is some* x *with*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \vdots\ &\ \ \vdots \qquad\quad \vdots \\ x &\equiv a_l \pmod{m_l}, \end{aligned}$$

and moreover x *is uniquely determined modulo* $m_1 m_2 \cdots m_l$.

Let's see an example.

Problem 3. *There's a legend that in ancient China, the armies gathered by emperors were so massive that counting the soldiers posed a major problem. Suppose that the general in command of the army orders the soldiers to form ranks, each rank 100 soldiers wide. There are 12 soldiers left over. When they line up in ranks of 101, there is only 1 soldier left over. In ranks of 103, there are 62 soldiers remaining, and in groups of 99 one of the groups is 14 short. How many soldiers are in the army?*

Answer.

We use a modification of the algorithm for two numbers. Our first task is to solve the equation

$$100 \cdot 101 \cdot 103 \cdot x_1 + 99 \cdot 101 \cdot 103 \cdot x_2 + 99 \cdot 100 \cdot 103 x_3 + 99 \cdot 100 \cdot 101 \cdot x_4 = 1.$$

Actually, we only need to solve it modulo $99 \cdot 100 \cdot 101 \cdot 103$*. This lets us solve for* $x_1 \pmod{99}$*,* $x_2 \pmod{100}$*,* $x_3 \pmod{101}$*,* $x_4 \pmod{103}$*.*

$$\begin{aligned} 8x_1 &\equiv 1 \pmod{99} & &\Rightarrow & x_1 &\equiv -37 \pmod{99}, \\ -3x_2 &\equiv 1 \pmod{100} & &\Rightarrow & x_2 &\equiv 33 \pmod{100}, \\ 4x_3 &\equiv 1 \pmod{101} & &\Rightarrow & x_3 &\equiv -25 \pmod{101}, \\ -24x_4 &\equiv 1 \pmod{103} & &\Rightarrow & x_4 &\equiv 30 \pmod{103}, \end{aligned}$$

Then, analogously to the two variable case, the answer is

$$\begin{aligned} 100 \cdot 101 \cdot 103 \cdot (-37) \cdot (-14) + 99 \cdot 101 \cdot 103 \cdot 33 \cdot 12 + 99 \cdot 101 \cdot 103 \cdot (-25) \cdot 1 + 99 \cdot 100 \cdot 101 \cdot 30 \cdot 62 \\ \equiv 314212 \pmod{99 \cdot 100 \cdot 101 \cdot 103}. \end{aligned}$$

Since $99 \cdot 100 \cdot 101 \cdot 103$ *is about 100 million, which is larger than possible even in ancient China, there must be 314212 soldiers in the army.*

Our final version of the CRT drops the assumption that m and n are relatively prime.

Theorem 4 (CRT, version 4)**.** *Given m and n, not necessarily relatively prime, and any a and b, then there is an x satisfying*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

if and only if

$$a \equiv b \pmod{\gcd(m,n)},$$

in which case x is uniquely determined modulo $\operatorname{lcm}(m,n)$.

Let's see an example of this final version of the CRT.

Problem 4. *What one condition on x is equivalent to the two equations*

$$\begin{aligned} 9x &\equiv 15 \pmod{16} \\ 5x &\equiv 11 \pmod{28}? \end{aligned}$$

Answer.

We first rewrite these equations in forms suitable to applying CRT.

For the first, we can either solve it using the Euclidean algorithm or note that $63 = 3{\cdot}16{+}15 = 9{\cdot}7$. *For the second, we similarly use the Euclidean algorithm or note that $-45 = -2 \cdot 28 + 11 = 5$ $cdot(-9)$. Thus the given equations are equivalent to*

$$\begin{aligned} x &\equiv 7 \pmod{16} \\ x &\equiv 19 \pmod{28} \end{aligned}$$

The greatest common divisor of 16 and 28 is 4, and $7 \equiv 19 \equiv 3 \pmod{4}$*, so the CRT guarantees that there is a solution, unique modulo* $\operatorname{lcm}(16,28) = 112$. *In this case, since every prime dividing the gcd divides 16 a larger number of times than it divides 28, we can use a trick. Reducing the second equation modulo 7 doesn't lose any information, so our equations are equivalent to*

$$\begin{aligned} x &\equiv 7 \pmod{16} \\ x &\equiv 5 \pmod{7}, \end{aligned}$$

and we've now reduced the problem to the relatively prime case. We find that

$$7 \cdot 7 - 3 \cdot 16 = 1,$$

so the answer is

$$7 \cdot 7 \cdot 7 - 3 \cdot 16 \cdot 5 \equiv 103 \pmod{112}.$$

The one condition equivalent to the given two is

$$x \equiv 103 \pmod{112}.$$