Math Circles - Elementary Number Theory - Fall 2023

Week 2 (Nov 22)

Modular Arithmetic

Before jumping into the theory, let's start with an example.

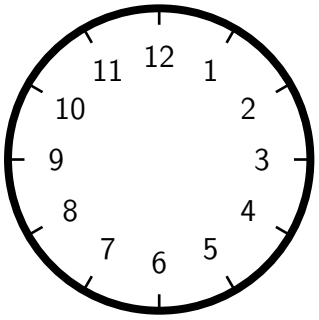
Example. *Suppose we're telling time using a 12-hour clock (ignoring AM and PM), and that it is 7:00 right now.*

(a) What time will it be in 3 hours? How did you get this answer?

Solution. It will be 10:00, because $7 + 3 = 10$. ■

(b) What time will it be in 6 hours? How did you get this answer?

Solution. It will be 1:00. Let's look at a clock:



If we count 6 hours around the clock from 7:00, we would get 8:00, 9:00, 10:00, 11:00, 12:00, 1:00.

Can we apply the strategy we used in part(a), instead of counting? Yes... with a catch. We have that $7 + 6 = 13$, but 13 is not a number on our clock. Every time we pass 12:00, we start over at 1:00, so what we really care about is the remainder when 13 is divided by 12. Since $13 = 12 + 1$, the remainder is 1, so we get that the answer is 1:00. ■

(c) What time will it be in 43 hours? How did you get this answer?

Solution. We can look at this problem slightly differently using the two strategies from part (b).

- *Strategy 1:* Every 12 hours, we end up back at the same time we started at. Since $43 = 3(12) + 7$, if we count forward 43 hours from 7, we will go around in 3 full circles on the clock, and then have to count forwards 7 hours from 7:00. This gives us that it will be 2:00.
- *Strategy 2:* We only need to consider the remainder when $7 + 43 = 50$ is divided by 12. We have that $50 = 4(12) + 2$, so the remainder is 2. So, in 43 hours it will be 2:00.

■

In the example above, regardless of which strategy we used, the key idea is that we were grouping together all integers that have the same remainder when divided by 12, and treating them as equivalent, since they correspond to the same number on a basic 12-hour clock. Since we were only asked what number the clock will be displaying at various times, we didn't need to distinguish between times that occurred in the morning or the afternoon, or even on different days. This doesn't mean that all the times are the same (asking someone to meet you at 1:00 Monday morning is not the same as asking someone to meet you at 1:00 on Tuesday afternoon), it just means that we can treat them the same in this context.

This is an example of *modular arithmetic*.

Formally, this is defined as follows:

Definition. *Let a, b, and n be integers. We say that $a \equiv b \mod n$ ("a is equivalent to b modulo n") if $n \mid b - a$.*

But wait... this definition looks different than the intuition we gained from dealing with "clock numbers," where we treated two integers as equivalent if they have the same remainder when divided by 12. As it turns out, this is equivalent to the definition above, which we'll show in the following theorem:

Theorem. *$a \equiv b \mod n$ if and only if[1] a and b have the same remainder when divided by n.*

Proof. By the Division Theorem, there are integers q_a, q_b, r_a, r_b, where $0 \leq r_a, r_b < n$, such that $a = q_a n + ra$ and $b = q_b n + r_b$. We'll use this fact in both directions of the proof.
First, suppose $a \equiv b \mod n$. Then, $n \mid b - a$. Subbing in what we have above from the Division Theorem, this means that $n \mid (q_b n + r_b) - (q_a n + r_a)$, and hence that $n \mid (q_b - q_a)n + (r_b - r_a)$. Since n clearly divides $(q_b - q_a)n$, it must also be the case that $n \mid r_b - r_a$. But $0 \leq r_b, r_a < n$, so $-n < r_b - r_a < n$, so it must be the case that $r_b - r_a = 0$, and hence that $r_a = r_b$.

Now, suppose that a and b have the same remainder when divided by n; that is, suppose that $r_a = r_b$. Then

$$b - a = (q_b n + r_b) - (q_a n + r_a) = (q_b - q_a)n + (r_b - r_a) = (q_b - q_a)n,$$

which is divisible by n. So, $a \equiv b \mod n$. ■

When we talk about integers modulo n, to keep things simple, we often look only at the integers $\{0, 1, 2, \ldots, n-1\}$. Doing modular arithmetic is very similar to the kind of arithmetic that you learned in school. For instance, we can add, subtract, and multiply numbers the same way that we usually do, as long as we apply the " $\mod n$ operation" (i.e., only consider the remainder after division by n) again afterwards to end up with an integer between 0 and $n - 1$.

Example. *(a)* $3 + 2 \equiv 1 \mod 4$

(b) $7 - 5 \equiv 2 \mod 10$

(c) $5 - 7 \equiv 8 \mod 10$

(d) $2 \cdot 5 \equiv 3 \mod 7$

(e) $3 \cdot 9 \equiv 7 \mod 20$

Okay, so addition, subtraction, and multiplication are fairly straightforward. What about division?

[1]The statement *A if and only if B* means that "if A is true then B must be true, and if B is true then A must be true". So, to prove an "A if and only if B" statement, we must first prove that if A is true, B must also be true, and then prove that if B is true, then A must also be true.

Example.

$10/2 \equiv 5 \mod 11$

$3/2 \equiv 4 \mod 5$

Wait... what? How did we get $3/2 \equiv 4 \mod 5$? Well, let's think about what division really is. Solving for x in the equation

$$\frac{3}{2} \equiv x \mod 5$$

is equivalent to solving for x in the equation

$$3 \equiv 2x \mod 5.$$

We can do this by trial and error:

$$\begin{aligned} 2(0) &\equiv 0 \mod 5 \\ 2(1) &\equiv 2 \mod 5 \\ 2(2) &\equiv 4 \mod 5 \\ 2(3) &\equiv 1 \mod 5 \\ 2(4) &\equiv 3 \mod 5 \end{aligned}$$

So, we get that $x = 4$ is the one that works. Let's try a few more examples:

Example. *Compute x:*

(a) $\frac{3}{4} \equiv x \mod 7$

Solution. We have that

$$\begin{aligned} 4(0) &\equiv 0 \mod 7 \\ 4(1) &\equiv 4 \mod 7 \\ 4(2) &\equiv 1 \mod 7 \\ 4(3) &\equiv 5 \mod 7 \\ 4(4) &\equiv 2 \mod 7 \\ 4(5) &\equiv 6 \mod 7 \\ 4(6) &\equiv 3 \mod 7 \end{aligned}$$

So, $x = 6$. ■

(b) $\frac{5}{6} \equiv x \mod 8$

Solution. We have that

$$\begin{aligned} 6(0) &\equiv 0 \mod 8 \\ 6(1) &\equiv 6 \mod 8 \\ 6(2) &\equiv 4 \mod 8 \\ 6(3) &\equiv 2 \mod 8 \\ 6(4) &\equiv 0 \mod 8 \\ 6(5) &\equiv 6 \mod 8 \\ 6(6) &\equiv 4 \mod 8 \\ 6(7) &\equiv 2 \mod 8 \end{aligned}$$

■

So there is no value of x which works...

Hmmm, okay, so this doesn't always work. Let's think about what we're really doing, to try and find a pattern. When we do division over the real numbers (i.e., "normal" division), dividing by k is the same as multiplying by $\frac{1}{k}$. Notice that $\frac{1}{k} \cdot k = 1$. We call such a number the *inverse* of k, and we have an equivalent notion in modular arithmetic.

Definition. *The inverse of x modulo n is an integer x^{-1} such that $xx^{-1} \equiv 1 \mod n$.*

So, in the equation

$$kx \equiv \ell \mod n,$$

if we can compute k^{-1}, then we can compute

$$k^{-1}kx \equiv k^{-1}\ell \mod n$$

and hence

$$x \equiv k^{-1}\ell \mod n.$$

Let's try a few examples.

Example. *(a) Compute $5^{-1} \mod 7$.*

Solution. Since $5 \cdot 3 \equiv 1 \mod 7$, we have that $5^{-1} \equiv 3 \mod 7$. ■

(b) Compute $6^{-1} \mod 8$.

Solution. We have that

$$\begin{aligned} 6(0) &\equiv 0 \mod 8 \\ 6(1) &\equiv 6 \mod 8 \\ 6(2) &\equiv 4 \mod 8 \\ 6(3) &\equiv 2 \mod 8 \\ 6(4) &\equiv 0 \mod 8 \\ 6(5) &\equiv 6 \mod 8 \\ 6(6) &\equiv 4 \mod 8 \\ 6(7) &\equiv 2 \mod 8 \end{aligned}$$

So 6 doesn't have an inverse modulo 8. ■

The natural question to ask is: which numbers have an inverse modulo n? As it turns out, there's a nice answer to this.

Theorem. *An integer x has an inverse modulo n if and only if $\gcd(x, n) = 1$.*

Proof. First, suppose that x has an inverse modulo n. Then there is an integer r such that $xr \equiv 1 \mod n$. By definition of equivalence modulo n, this means that $n \mid xr-1$. By definition of divisibility, this means that there is an integer s such that $ns = xr - 1$, and hence that $xr + ns = 1$. Now, let $d = \gcd(x, n)$. Since $d \mid x$ and $d \mid n$, we have that $d \mid xr + ns$, and hence $d \mid 1$. So, $d = 1$.

Now, suppose that $\gcd(x, n) = 1$. By Bezout's Lemma, there exist integers r and s such that $xr + ns = 1$. So, $xr - 1 = ns$. By definition of divisibility, this means that $n \mid xr - 1$, and by definition of modular equivalence, this means that $xr \equiv 1 \mod n$. So, r is the inverse of x. ■

It would be really nice if we didn't have to worry about some numbers having inverses and others not. And in some cases, we don't! Before reading on, try to figure out for which integers n it is the case that every number in $\{1, \ldots, n-1\}$ has a multiplicative inverse modulo n.

Theorem. *Every element of* $\{1, \ldots, n-1\}$ *has a multiplicative inverse modulo* n *if and only if* n *is prime.*

Proof. First, suppose that every element of $\{1, \ldots, n-1\}$ has a multiplicative inverse modulo n. Then for each $x \in \{1, \ldots, n-1\}$, $\gcd(x, n) = 1$. In particular, this means that for all $x \in \{2, \ldots, n-1\}$, $x \nmid n$. So, n has no divisors other than 1 and n, therefore n is prime.

Now, suppose that n is prime. Then n has no divisors other than 1 and n. In particular, this means that $\gcd(n, m) = 1$ for all m such that $n \nmid m$, which is the case for all integers in $\{1, \ldots, n-1\}$. So, every element of $\{1, \ldots, n-1\}$ has a multiplicative inverse modulo n. ■

Once again, the natural next question to ask is "how can we find the modular inverse of a number?" As it turns out, we already have the tools we need to do this! If we want to compute the inverse of x modulo n, if we have an equation that looks like

$$ax + bn = 1 \mod n,$$

then we know that $ax \equiv 1 \mod n$, and so a is the inverse of x modulo n. We can get such an equation through the Euclidean Algorithm. It's easiest to explain using an example.

Example. *Find the inverse of 17 modulo 29.*

Solution. Using the Euclidean Algorithm, we get that:

$$29 = 1(17) + 12 \tag{1}$$
$$17 = 1(12) + 5 \tag{2}$$
$$12 = 2(5) + 2 \tag{3}$$
$$5 = 2(2) + 1 \tag{4}$$
$$2 = 2(1) + 0 \tag{5}$$
$$\tag{6}$$

We can rewrite these equations as follows:

$$29 = 1(17) + 12 \implies 12 = 29 - 1(17) \tag{7}$$
$$17 = 1(12) + 5 \implies 5 = 17 - 1(12) \tag{8}$$
$$12 = 2(5) + 2 \implies 2 = 12 - 2(5) \tag{9}$$
$$5 = 2(2) + 1 \implies 1 = 5 - 2(2) \tag{10}$$
$$2 = 2(1) + 0 \tag{11}$$

By subbing equation (3) into equation (4), we can write 1 in terms of 12 and 5:

$$1 = 5 - 2(2) = 5 - 2(12 - 2(5)) = -2(12) + 5(5).$$

We can sub equation (2) into this new equation to write 1 in terms of 17 and 12:

$$1 = -2(12) + 5(5) = -2(12) + 5(17 - 1(12)) = -7(12) + 5(17).$$

We can sub equation (1) into this new equation to write 1 in terms of 29 and 17

$$1 = -7(12) + 5(17) = -7(29 - 1(17)) + 5(17) = -7(29) + 12(17).$$

Taking this equation modulo 29 gives us that

$$-7(29) + 12(17) \equiv 1 \mod 29$$

and hence that

$$12(17) \equiv 1 \mod 29,$$

so 12 is the inverse of 17 modulo 29. ■