Modular Arithmetic

Muhammed Yaseen

OIS Math Club

August 4, 2022

Motivation

Think of a clock. If the time right now was 2 AM, and I asked what the time would be after 12 hours, you would say 2 PM. What about 36 hours? 48 hours? 72? $12n$ hours?

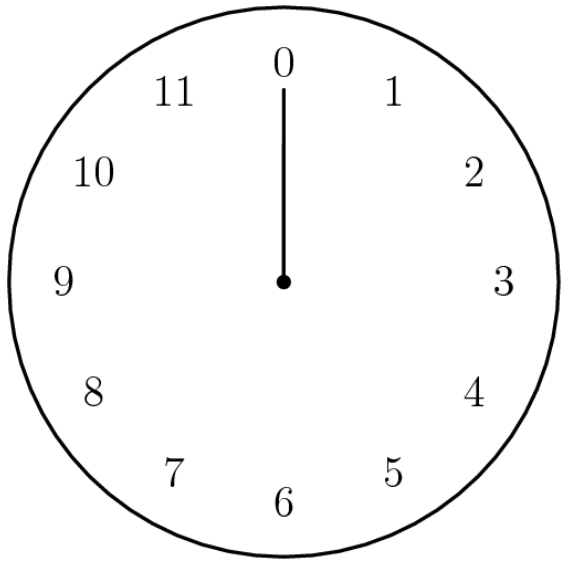

Figure: Clock

What if we counted hours using a 15 hour system?

Cont.

Building on the previous slide, we see that if the time is 2 right now (ignore AM/PM for now), and we check the clock 12 hours later, we are going to read it off as 2. In reality, it should show 14. Thus, 2 is somewhat "congruent" or similar to 14 in some way.

Easy-to-Understand Definition

For $a, b, n \in \mathbb{Z}$, we write

$$a \equiv b \pmod{n} \iff r_a = r_b$$

Where r_a, r_b are the respective remainders obtained when a, b are divided by n.

Examples:

1. $4 \equiv 6 \pmod{2}$
2. $200 \equiv 0 \pmod{200}$
3. $4 \equiv 25 \pmod{7}$
4. $14 \equiv 2 \pmod{12}$

Properties of Modular Arithmetic

Given

1. $a \equiv 0 \pmod{n} \implies n|a$
2. $a \equiv b \pmod{n} \implies a - b \equiv 0 \pmod{n}$
3. Given $a \equiv b \pmod{n}$, $a^k \equiv b^k \pmod{n}$ $(k \in \mathbb{Z})$.
4. $a \equiv b \pmod{n} \implies ka \equiv kb \pmod{n}$. (Converse doesn't hold generally).
5. $a \equiv b \pmod{n} \implies \mathrm{a}+\mathrm{k} \equiv b + k \pmod{n}$
6. $a \equiv b \pmod{n}, b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

An Interesting Result

Consider the numbers a, n. Using the Euclid Division Lemma, we can write (for suitable $q, r \in \mathbb{Z}$)

$$a = qn + r$$

Taking modulo n both sides,

$$a \equiv qn + r \pmod{n}$$

But $qn \equiv 0 \pmod{n}$ (why?)

$$a \equiv r \pmod{n}$$

So if someone tells you to compute $x \pmod{n}$, they're simply asking you to calculate the remainder when you divide x by n.

Rigorous Definition

For $a, b, n \in \mathbb{Z}$, we write

$$a \equiv b \pmod{n} \iff n \mid a - b$$

Quite something to digest!

How did we get that?

Rigorous Proof. We know that $r_a = r_b$ because $a \equiv b \pmod{n}$. Then, by Euclid's division lemma, we can write

$$a = q_a n + r_a$$

$$b = q_b n + r_b$$

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

$a - b$ is an integral multiple of n. This means $a - b$ is divisible by n. Thus

$$a \equiv b \pmod{n} \implies n | a - b$$

What does it mean?

We go back to our clock. 2 is equivalent to 14 in some way. We're using a 12 hour system. Hmm...
The remainder that both 2 and 14 leave upon divison by 12 is 2!

How is it useful?

It is currently 7:00 PM. What time (in AM or PM) will it be in 100 hours?

Solution

Time can be counted either modulo 12 or 24. We count modulo 24 if we also wish to specify AM/PM. So we do just that. 7 PM is 19. The time after 100 hours is going to be 119. So the time is going to be

$$19 + 100 \pmod{24}$$

which is 23. So its going to be $\boxed{11PM}$.

What is the last digit of 19^{17}?

The last digit of a number n is just $n \pmod{10}$. Why? Just expand the number. For example, we know trivially that the last digit of 342 is 2. Lets do it the mod way. $342 = 10^2 \times 3 + 10^1 \times 4 + 2$. Taking the residue mod 10 on both sides gives you

$$342 \equiv 2 \pmod{10}$$

Therefore, 2 is the last digit of 342. On to the actual question now!

Solution

We begin by noting $19 \equiv 9 \pmod{10}$. Since -10 is a multiple of 10, $-10 \equiv 0 \pmod{10}$. So we can add -10 on both sides of the congruency without affecting anything.

$$19 + (-10) \equiv 9 + (-10) \pmod{10} \implies 19 \equiv -1 \pmod{10}$$

What remains is simply to exponentiate to 17.

$$19^{17} \equiv (-1)^{17} \equiv -1 \equiv 9 \pmod{10}$$

Thus, the last digit of 19^{17} is $\boxed{9}$.
Exercise: What is the last digit of 16^{20034}