Modular Arithmetic

Mckinley Xie

August 27, 2021

Modular arithmetic was recently removed from the IB curriculum for some reason. That makes me sad. So I'm just going to teach it here!

The method feels *really* unmotivated at first, so we'll try to build up to it. Without further ado...

§1 Intruduction

Example 1.1

Find the ones digit of 3^8

We don't really know how to start, but this number doesn't look *too* big, so let's just multiply it out and see what happens.

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 9 \\ 3^3 &= 27 \\ 3^4 &= 81 \\ 3^5 &= 243 \\ 3^6 &= 729 \\ 3^7 &= 2187 \\ 3^8 &= 6561 \end{aligned}$$

so our answer is $\boxed{1}$.

However...

Example 1.2

Find the ones digit of 3^{2021}.

Our previous approach obviously won't work. Can we find some sort of pattern? Well, look at the last digit for each term from our first example. Do you notice it?

You might notice that the digits repeat $3, 9, 7, 1, 3, 9, 7, 1 \ldots$, such that the last digit of 3^n is the same as the last digit of 3^{n+4}. But this might just be a coincidence. Can we prove it?

Let $3^n = 10a + b$ for some $a, b \in \mathbb{Z}$ and $0 \leq b < 10$. (in other words, b is the last digit of $10a + b$.)

What happens when we multiply this by $3^4 = 81$? Well, we have $81(10a + b) = 80(10a + b) + 10a + b$, and since $b < 10$ and everything else is divisible by 10, the last digit of $3^4 \cdot (10a + b)$ is still b. So this obviously works, and we know that $3^{2021} = 3^{4 \cdot 505 + 1}$, so the last digit of 3^{2021} is equal to the last digit of 3^1, so our answer is $\boxed{3}$.

But our previous proof was a bit messy. This is where we introduce the idea of **modular arithmetic**.

Definition 1.3. $a \equiv b \pmod{n}$ if both a and b have the same remainder when divided by n. More formally, $a \equiv b \pmod{n}$ if, for some (possibly negative) integer k, $a + kn = n$.

So, for example, $4 \equiv 14 \equiv 24 \equiv \cdots \pmod{10}$. Similarly, $1 \equiv 7 \equiv 12 \equiv \cdots \pmod{6}$.

We now have the following theorems:

Theorem 1.4

If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$.

This implies the property we observed above, since $81 \equiv 1 \pmod{10} \implies 81 \cdot n \equiv 1 \cdot n \pmod{10}$.

Theorem 1.5

If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.

Proof. By definition, $a = kn + b$ for some integer k, so $a + c = kn + b + c$ and $a + c \equiv b + c$. □