Modular Arithmetic Stretch

Modular arithmetic is a system of integer arithmetic that enables us obtain information and draw conclusions about large quantities and calculations. It would be extremely helpful, for instance, when asked to find the units digit of 2^{2015} if we didn't really have to calculate the value of the expression to get that information. Modular arithmetic allows us to do just that!

THE BASICS:

The simplest example of modular arithmetic is commonly referred to as "clock arithmetic." Suppose it is 3 o'clock now and I want to know what time it will be in 145 hours. We could count from 3 o'clock for 145 consecutive hours. We certainly wouldn't be expected to count 145 hours starting with 3 o'clock. Suppose we did counting the hours from 3 o'clock. What happens when we get to 12 o'clock? We continue counting but begin a new 12-hour cycle. Instead of counting 145 hours, we can just see how many of these 12-hour cycles we'd go through counting 145 hours. More importantly, we need to determine how many hours would remain after making it through the last full 12-hour cycle.

In this example, the value 12 is called the ***modulus*** and what is left over is called the remainder. In this case, we can determine fairly quickly that there are 12 full 12-hour cycles in 145 hours, with a remainder of 1 hour (since $12 \times 12 = 144$ and $145 - 144 = 1$).

Standard arithmetic: $145 = 12 \times 12 + 1$

Modular arithmetic we write: $145 \equiv 1 \pmod{12}$ ☞ *Read **"145 is congruent to 1 modulo 12"***

The remainder of 1 tells me that it will be the same time 145 hours after 3 o'clock that it will be 1 hour after 3 o'clock. And that time is 4 o'clock.

Here's another example of modular arithmetic. Suppose today is Tuesday. What day of the week will it be 417 days from now? Since the days of the week are on a 7-day repeating cycle, the modulus here is 7. If we divide 417 by 7, we get

Standard arithmetic: $417 = 59 \times 7 + 4$

Modular arithmetic we write: $417 \equiv 4 \pmod{7}$

Thus, 417 days from Tuesday will be the same day of the week as 4 days from Tuesday, Saturday.

TRY THESE

241.__________ If the current month is July, what month will it be in 152 months?

242.__________ a.m. / p.m. If the time is currently 8 a.m., what time will it be in 255 hours? *Circle a.m. or p.m. in answer blank.*

243.__________ m Jennie goes out every morning and jogs on the school track. The track is 400 meters around. If Jennie runs 5310 meters then how far will she be from where she started once she finished her run?

Modular Addition: What is the remainder when 9813 + 7762 + 11252 is divided by 10?

$$9813 + 7762 + 11252 = (981 \times 10 + 3) + (776 \times 10 + 2) + (1125 \times 10 + 2)$$
$$= (981 + 776 + 1125) \times 10 + (3 + 2 + 2)$$

Since we are only interested in the remainder, we need only focus on the last part. We see that the remainder is 3 + 2 + 2 = **7**. Written in modular arithmetic notation it would look like this:

$$9813 + 7761 + 11252 \equiv 3 + 2 + 2 \equiv 7 \pmod{10}$$

Modular Multiplication: What is the remainder whsen 9813×7762 is divided by 10?

$$9813 \times 7762 = (981 \times 10 + 3) \times (776 \times 10 + 2)$$
$$= (981 \times 776 \times 10^2) + (981 \times 2 \times 10) + (776 \times 3 \times 10) + (3 \times 2)$$

The first three terms are multiples of 10, and once again last term is the remainder 3×2 = **6**. Written in modular arithmetic notation would look like this:

$$9813 \times 7762 \equiv 3 \times 2 \equiv 6 \pmod{10}$$

More Mod Shortcuts: There are many useful applications of modular arithmetic. Here are just a few more.

- Consider the powers of 3: $3^0 = 1$; $3^1 = 3$; $3^2 = 9$; $3^3 = 27$; $3^4 = 81$; $3^5 = 243$; $3^6 = 729$
  Notice that the units digits are repeated every four powers of 3, so the modulus is 4. Repeating units digits correspond to remainders 1, 2, 3 and 0.
- Suppose you want the unit digit of 3^{53}. First, we note that $53 \equiv 1 \pmod 4$ since the remainder 1 corresponds to units digit 3, thus, the expansion of 3^{53} has a units digit of 3.
- The smallest number that has remainder 1 when divided by 2 and 3 is 7. Why?
  $1 \equiv 7 \pmod 2$ and $1 \equiv 7 \pmod 3$

MODULAR ARITHMETIC PRACTICE

244.__________ What is the last digit of 2^{2015}?

245.__________ What is the value of 122×71 modulo 11?

246.__________ What is the remainder when $5981 \times 8162 \times 476$ is divided by 5?

247.__________ Jon has 29 boxes of donuts with 51 donuts in each box. He wants to divide them into groups of a dozen each. Once he groups them again, how many donuts will be left over?

248.__________ What is the least integer greater than 6 that leaves a remainder of 6 when it is divided by 7 and by 11?

249.__________ When organizing her pencils, Faith notices that when she puts them in groups of 3, 4, 5, or 6, she always has exactly one pencil left over. If Faith has between 10 and 100 pencils, how many pencils does she have?

250.__________ When organizing her pens, Faith notices that when she puts them in groups of 3, 4, 5, or 6, she is always one pen short of being able to make full groups. If Faith has between 10 and 100 pens, how many pens does she have?