Modular Arithmetic

Franklin High School — DeVon Herr

December 2017

1 Introduction

Modular arithmetic is a subset of a vast field of Math known as number theory. To be brief, number theory deals with the math of integers, their properties as objects and in equations. Luckily (or unluckily), number theory is one of the "big-four" math fields in math competitions. A lot of number theory is obvious, and a decent amount of it is dedicated to making obvious statements easy to talk about, so one can move onto much *weirder* things regarding integers. One knows that any integer that ends in a 0 is a multiple of 10. But it's not as simple to deduce if a Fibonacci number that is simultaneously a prime *AND* of form $n^7 - 77$. With modular arithmetic, one is now prepared to approach such problems. Modular arithmetic is an example of math that although isn't very often taught in schools *(Authors Note: Though I do admit I have a small sample size of N=1)*, it is one of the most useful tools for a competition mathematician.

2 Motivations

The following problems will become accessible:

- What is the last digit of 6032^{31}?
- Find a number that leaves a remainder of 0 when divided by 5, remainder 6 when divided by 7, and remainder 10 when divided by 12.
- That one problem I mentioned above but am too lazy to rewrite in problem form

3 What Time is it?

You do modular arithmetic everyday! Consider the following situation:

One goes to bed at 11:00 PM *(AN: weird! who goes to bed at night? I only sleep after midnight)*, and then sleeps for 7 hours. At what time does this person awake?

You know the answer to be 6:00 AM, but this doesn't follow that naturally in regular mathematics. Simply put, $11 + 7 \neq 6$. What's going on? After the "time" pasts 12:00, it "loops around" back to 1. We only care about what's left after we take away multiples of 24. In a way, we're looking at residues. In other words, remainders!

3.1 I'd eat a Clock. Would you?

Consider the following situation: What hour is is it 71 hours after 2:00 AM?

The mathematical process is as follows. You want to find the time, but multiples of 24 don't change the time, since it just loops back. So you can take your number, divide it by 24, and only use the remainder. In this way, we are working *only* with remainders.

Since $\frac{71}{3} = 2R23$, we only have to do $23 + 2$ instead of $71 + 2$. This gives us $23 + 2 = 25$. Since we only care about the remainder (as we are *only* caring about the time, instead of the actual days elapsed), we take the remainder of 25 when divided by 24. $\frac{25}{24} = 1R1$. Since the remainder of 25 is 1 when divided by 24, the time will be 1:00 AM.

Modular arithmetic is also known as clock arithmetic because it uses virtually the same process as what you do with time/clocks. If you are comfortable with this, you are ready!

4 When in Rome, do as the Romans do

Like how Descartes developed the language of variables and algebra to make solving math problems more efficient, a similar process exists for modular arithmetic. We introduce only one new term, and one familiar symbol.

Modular arithmetic deals solely with remainders of numbers.

Our clock has 12 hours, but in math, a "clock" can have any number. This number just tells when to wrap around or loop back and start at 0. This is known as the modulus. In particular, this means "take everything's remainder when divided by this number." Symbolically to say that we are working in modulus n, one tacks on $(modn)$ to the end of the equation.

An example would be "12 and 6 are the same, mod 3, since when both are divided by 3, their remainders are the same."

We don't use equal signs very often in modular arithmetic (although you still can, it's just *technically* incorrect. No one actually cares, though, do what you want), because for the most part, numbers aren't actually equal to each other. Only their remainders are. To scoot around this issue, statements generally use $\equiv$.

Our example would therefore be $12 \equiv 6 \pmod 3$

4.1 Translation Nation Participation

(*I highly recommend you do these practice problems. While the concepts may seem relatively straightforward, doing this will give you very useful mental muscle memory.*)

1. Convert the following English statements to modular arithmetic statements.
   (a) 5's remainder, when divided by 3, is the same as 17's remainder when divided by 3.
   (b) 17 and 27 have the same remainder when divided by 10.
   (c) x's remainder is equal to 5's remainder when divided by 2.
2. Convert the following modular arithmetic statements to English statements.
   (a) $2 \equiv 320480932482 \pmod{10}$
   (b) $14 \equiv 28 \pmod 7$
   (c) $x^2 = y^3 \pmod z$

4.2 Solutions

1. (a) $5 \equiv 3 \pmod 3$
   (b) $17 \equiv 27 \pmod{10}$
   (c) $x \equiv 5 \pmod{10}$
2. Your actual answers may vary because English is well, English.
   (a) 2's remainder, when divided by 10, is the same as 320480932482's remainder when divided by 10.
   (b) 14 and 28 have the same remainder when divided by 7.
   (c) The square of x's remainder is equal to the cube of y's remainder when divided by z.

5 Talk "Mathy" to Me

These examples are meant to both expose you to the mechanics of modular arithmetic, but also to show you how useful it is. Do each problem, once by taking the remainder only at the very end, and then once by taking the remainder for every number possible.

1. 420+69 (mod 7)
2. Prove $12 + 89 \equiv 48 + 89 \pmod{36}$
3. Prove $-2 \equiv 6 \pmod 2$

5.1 Solutions

1. (a) $420 + 69 \equiv 489 \pmod 7$
   $489 \equiv 6 \pmod 7$
   $\therefore 420 + 69 \equiv 6 \pmod 7$
   (b) $420 + 69 \pmod 7 = 420 \pmod 7 + 69 \pmod 7$
   $420 \pmod 7 + 69 \pmod 7 = 0 \pmod 7 + 6 \pmod 7$
   $\therefore 420 + 69 \equiv 6 \pmod 7$
2. (a) $12 + 89 \equiv 48 + 89 \pmod{36}$
   $101 \equiv 137 \pmod{36}$
   Since $101 \equiv 29 \pmod{36}$; $137 \equiv 29 \pmod{36}$,
   $101 \equiv 137 \pmod{36} \rightarrow 29 \equiv 29 \pmod{36}$
   $\therefore 12 + 89 \equiv 48 + 89 \pmod{36}$
   (b) $12 + 89 \equiv 48 + 89 \pmod{36}$
   Since $12 + 89 \equiv 12 + 17 \pmod{36}$; $12 + 89 \equiv 29 \pmod{36}$
   Since $48 + 89 \equiv 12 + 17 \pmod{36}$; $48 + 89 \equiv 29 \pmod{36}$
   $29 \equiv 29 \pmod{36}$
   $\therefore 12 + 89 \equiv 48 + 89$