



Grade 7 & 8 Math Circles

October 12, 2011

Modular Arithmetic

To begin: Before learning about modular arithmetic (or “mods” for short), let us first talk about remainders.

Question 1: What is the remainder when 51 is divided by 6?

Question 2: What are all possible remainders when a number is divided by 6? By 4? By 9?

In General: For any number n , all possible remainders when n is the divisor are $0, 1, \dots, n - 1$.

We can sort our dividends into groups of like remainders for certain divisors (or *moduli*, the plural of *modulus*), you have actually seen this before:

Example 1

Sort the numbers 1 through 10 into even numbers and odd numbers.

Odd	Even

Notice that the _____ numbers have remainder 0 when divided by 2, and the _____ numbers have remainder 1 when divided by 2.

We can do this with any modulus.

Example 2

Sort the numbers 1 through 10 depending on their remainder when divided by 3.

Remainder:

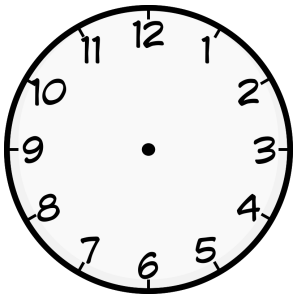
What we have just done is broken up our numbers into their “*congruence classes*” for the modulus 3 (i.e. a group of integers who all have the same remainder when divided by 3). There is one congruence class for each possible remainder of 3.

Why are remainders so important to us?

Modular Arithmetic

Modular arithmetic uses remainders to state possibly big numbers in a compact way. It is useful when events repeat, which is where you’ve seen it before...

Modular arithmetic is also sometimes called “Clock Arithmetic”



On a clock face, the numbers ascend from 1 to 12. However, when 1:00 PM rolls around, we typically don’t say “13 O’clock”, we simply wrap back around to 1:00 again. Similarly 24-hour clocks wrap back around from 23:00 to 0:00.

Mods use this “wrapping” concept too, except we *always* start (and wrap back to) 0 when working with mods.

Looking back at Question 1:

When 51 is divided by 6, the remainder is 3. This means that 51 belongs in the congruence class of 3 for the modulus 6.

A shorthand for this is:

$$51 \equiv 3 \pmod{6}$$

This is read as “51 is congruent to 3 mod 6”, and interpreted as “The remainder when 51 is divided by 6 is 3”.

NOTE: Congruent (\equiv) does **not** mean equal, it means that both numbers have the same remainder when divided by the modulus.

This also means that $51 \equiv 45 \equiv 39 \equiv 33 \equiv \dots \equiv 15 \equiv 9 \equiv 3 \pmod{6}$

Finding Congruences

With smaller numbers it is simple to find their congruence under a certain modulus, as long as you know your multiplication/division tables.

Example 3

- a) What is $84 \pmod{9}$? b) What is $52 \pmod{5}$? c) What is $-4 \pmod{10}$?

To find congruences in larger numbers for a certain modulus, follow these steps:

1. Divide your number by your modulus, using either your calculator or the mental methods learned last week.
2. Take the whole number part of your answer and multiply it by your modulus.
3. Subtract this from your original number, what you get is your remainder and also your congruence.

Example 4

What is $3,686,132 \pmod{7}$?

Applications of Congruences

Dates and Times

Since the days of the week, and the hours of the day are repeated events, we can use modular arithmetic to find past or future dates and times.

Examples:

1. Today is Wednesday, what day of the week will it be:
 - a) 165 days from now?
 - b) 365 days from now?
 - c) 1000 days from now?

2. I celebrated my 21st birthday on Wednesday, July 27th, 2011. On what day of the week was I born? (Don't forget about leap years!)

3. One year on Venus lasts 225 Earth days. Rachel is 13 years and 83 days old. How many days until her next Venusian birthday? How old will she be turning (in Venusian years)? Omit leap years for simplicity.

Cryptography: Shift Ciphers

If we assign each letter of the alphabet a number from 0 to 25 (ex. A=0, B=1, C=2, etc...), a shift cipher can be used to encode and decode messages with a known shift number (which we'll call k).

To encode our message, we encrypt each letter individually using the formula:

$$\text{coded} = (\text{original} + k)(\text{mod } 26)$$

If we are given an encoded message and a shift number, we can decrypt the letters using the formula:

$$\text{original} = (\text{coded} + 26 - k)(\text{mod } 26)$$

Why do we add 26? This step will ensure we will not have to work with negative dividends. Infact we can actually add *any multiple* of 26, as we are only concerned about remainders.

Examples:

1. encode the message "MODULAR ARITHMETIC" using $k = 20$

2. What do you say when you see an empty parrot cage? Decode the answer "FEBOWED" using $k = 16$

Exercises:

- What day of the week were you born?
 - What day of the week will you turn 100?
- 1 year on Jupiter is equal to approximately 12 Earth years. On what day of the week did you celebrate your 1st Jovian (or Jupiterian) birthday? (If you haven't turned 1 on Jupiter yet, calculate on which day of the week your 1st birthday will fall)
- It is 8:00 AM in our 24 hour world. What time is it in a 3 hour world?
- In Example 3 on Page 4, our final answer is not quite accurate. A day on Venus (i.e. How long it takes the planet to make one rotation on its axis) is 243 Earth days. Notice that a day on Venus is longer than its year. Given this new information, in how many Venusian days will Rachel celebrate her next birthday?
- Given that one day on Jupiter lasts 10 earth hours, calculate how many Jovian days ago you celebrated your 1st birthday (Exercise 2).
- Find a partner to work with. Think of a secret message to send to them and encode it using a shift cipher with a shift number of your choice. Give your partner their coded message and the shift number. Decode your partner's message to you.
- What did the acorn say when he grew up? The answer "VTDBTIGN" Has been first encoded with a shift number of 21, and then encoded a second time using a shift of 20. Find the original message. Is there are way to do this in only one step?
- Using a standard 52 card deck I deal all the cards out to Leah, Matt, and myself. Were the cards dealt evenly?
- Jon is facing East, he rotates 1260° clockwise. What direction is he now facing?
- Philippa counted the loonies in her pocket. When she put them in groups of 4, she had 2 loonies left over. When she put them in groups of 5, she had one loonie left over. If Philippa has more than 10 loonies, what is the smallest possible number of loonies she could have?