UNIVERSITY OF WATERLOO
Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 6/7/8 Math Circles

April 1/2, 2014

Modular Arithmetic

Modular Arithmetic

Modular arithmetic deals primarily with operations and applications regarding remainders. Essentially, it's just another way to express remainders, and has many useful applications!

Division and Remainder

When doing long division, we have learned to use remainders. For example, when we divide 11 by 5, we see a remainder of 1. Let's look at how we can write this in two different ways:

$$5\overline{)\ 11}\quad 2\ R1 \qquad \text{which is also written as} \qquad 11 \equiv 1 (mod\ \ 5)$$

As we can see above there is a relationship between modulo notation and long division! When working with modulo notation, a common phrase we use is *"x is congruent to A mod B"*. A can be any number that has the same remainder as X when divided by B. In this lesson, A will be the smallest positive integer between 0 and B. We can then make a general statement about the relationship between modulo form and division:

$$B\overline{)\ X}\quad (Ans)\ RA \qquad \text{which is also written as} \qquad X \equiv A (mod\ \ B)$$

Modulo With Calculators

Let's go through an example step-by-step to understand where this is useful:

Find 373 in modulus 6:

Divide 373 by the mod we want, which is 6:	$373 \div 6 = 62.17$
Round this number down to a whole number:	$62.17 = 62$
Multiply this number by the mod we are working with:	$62 \times 6 = 372$
Subtract this new number from our original number:	$373 - 372 = 1$
Express this in modulo notation:	$373 \equiv 1 (mod\ \ 6)$

Therefore, we can say that 373 has a remainder of 1 when divided by 6, and can be expressed in modulo notation as $373 \equiv 1 (mod\ \ 6)$.

Congruence Class

A **Congruence Class** is a way to organize the set all numbers who have the same remainder when divided by some modulo m. We denote a congruence class as $[a]$ where a is the remainder. Let's look at the numbers 0 - 11 and what they are congruent to in modulo 4:

$$0 \equiv 0 \ (mod \ \ 4) \qquad 6 \equiv 2 \ (mod \ \ 4)$$
$$1 \equiv 1 \ (mod \ \ 4) \qquad 7 \equiv 3 \ (mod \ \ 4)$$
$$2 \equiv 2 \ (mod \ \ 4) \qquad 8 \equiv 0 \ (mod \ \ 4)$$
$$3 \equiv 3 \ (mod \ \ 4) \qquad 9 \equiv 1 \ (mod \ \ 4)$$
$$4 \equiv 0 \ (mod \ \ 4) \qquad 10 \equiv 2 \ (mod \ \ 4)$$
$$5 \equiv 1 \ (mod \ \ 4) \qquad 11 \equiv 3 \ (mod \ \ 4)$$

Now let's organize all of our answers into congruence classes. Clearly these are infinite sets that spread from negative infinity to positive infinity. We can even make equations to summarize every number that can be in the set using any integer k:

$$[0] = \{... \ -4, \ 0, \ 4, \ 8 \ ...\} = \{\text{for all x such that } \ x \equiv 0 \ (mod \ 4)\} = 4k + 0$$
$$[1] = \{... \ -3, \ 1, \ 5, \ 9 \ ...\} = \{\text{for all x such that } \ x \equiv 1 \ (mod \ 4)\} = 4k + 1$$
$$[2] = \{... \ -2, \ 2, \ 6, \ 10 \ ...\} = \{\text{for all x such that } \ x \equiv 2 \ (mod \ 4)\} = 4k + 2$$
$$[3] = \{... \ -1, \ 3, \ 7, \ 11 \ ...\} = \{\text{for all x such that } \ x \equiv 3 \ (mod \ 4)\} = 4k + 3$$

An interesting thing to notice is that congruence classes for the modulo m only exist from 0 to $m - 1$. As shown above, for modulo 4, there only exists congruence classes [0], [1], [2] and [3].

Exercises I

1. Fill in the blanks:
   (a) $55 \equiv$ __ $(mod \ \ 7)$
   (b) $2048 \equiv$ __ $(mod \ \ 3)$
   (c) $406 \equiv$ __ $(mod \ \ 1056)$
2. What congruence classes exist for modulo 3?
   (a) List 3 numbers that belong to each of these classes.
3. What congruence classes exist for modulo 7?
   (a) List 3 numbers that belong to each of these classes.

Modular Operations

Just like many different mathematical concepts, modular arithmetic has its own unique set of operations.

Modular Addition

Modular Addition is used to add congruence classes. To think of this concept, let's look at the additions of 14 and 15 using modulo 6:

Transferring both into modulo notation we get: $17 \equiv 5 \ (mod \ \ 6)$ and $15 \equiv 3 \ (mod \ \ 6)$

Let us add in the following manner:

$$\begin{aligned} 17 \equiv 5 \ (mod \ \ 6) + 15 \equiv 3 \ (mod \ \ 6) &= (17 + 15) \equiv (5 + 3) \ (mod \ \ 6) \\ &= 32 \equiv 8 \ (mod \ \ 6) \\ &= 32 \equiv 2 \ (mod \ \ 6) \end{aligned}$$

If we were to find 32 in modulo 6 using the algorithm, we would get $32 \equiv 2 \ (mod \ \ 6)$. We can extend this to say that any number that is 5 $(mod \ \ 6)$ added to any number that is 3 $(mod \ \ 6)$ will have a sum that is 2 $(mod \ \ 6)$.

Let's create an addition chart for all the congruence classes for modulo 6. The addition charts are different for every modulo based on reducing and how we add. When we add a class from a column and a row we change the sum into the modulo we are working with. This chart for example, shows that the sum of two numbers in modulo 6 with remainder 2 and 3 will result in a number with remainder 5:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Modular subtraction is the exact opposite of this concept and can be thought of as adding a negative number to find a sum. Remember that congruence classes stretch to negative infinity and therefore negative sums exist in congruence classes!

Modular Multiplication

Modular Multiplication is used to multiply congruence classes. To think of this concept, let's look at the multiplication of 17 and 15 using modulo 6:

Transferring both into modulo notation we get: $17 \equiv 2 \ (mod \ \ 6)$ and $15 \equiv 3 \ (mod \ \ 6)$

Let us multiply in the following manner:

$$\begin{aligned} 17 \equiv 5 \ (mod \ \ 6) \times 15 \equiv 3 \ (mod \ \ 6) &= (17 \times 15) \equiv (5 \times 3) \ (mod \ \ 6) \\ &= 255 \equiv 15 \ (mod \ \ 6) \\ &= 255 \equiv 3 \ (mod \ \ 6) \end{aligned}$$

If we were to find 255 in modulo 6 using the algorithm, we would get $255 \equiv 3 \ (mod \ \ 6)$. We can extend this to say that any number that is 5 $(mod \ \ 6)$ multiplied by any number that is 3 $(mod \ \ 6)$ will have a product that is 3 $(mod \ \ 6)$.

Let's create a multiplication chart for all the congruence classes for modulo 6. When we multiply, we change the product into a modulo 6 as well. This chart for example, shows that the product of two numbers in modulo 6 with remainder 2 and 3 will result in a number with remainder 0:

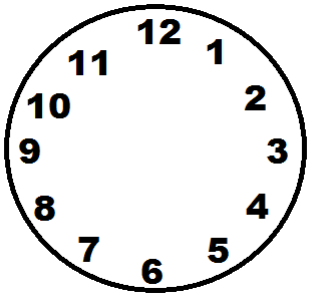
×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Exercises II

1. $X \equiv 6 \ (mod \ \ 7)$ and $Y \equiv 16 \ (mod \ \ 7)$.
   (a) What is X + Y equivalent to in modulo 7?
   (b) What is X - Y equivalent to in modulo 7?
   (c) What is Y - X equivalent to in modulo 7?
   (d) What is X × Y equivalent to in modulo 7?

Applications of Congruences

Let's look at a 12-hour analog clock. It is easy to tell from this what hour it is currently, it is up to us to know if it is am or pm. However, what if we have a 24-hour digital clock?



When it comes to using 24-hour clocks, we have probably used tricks such as subtracting 12 from the number to get that 13:00 is the same as 1:00. We can very much write this as a mod: $13 \equiv 1 \ (mod \ \ 12)$. A useful thing to remember is that the number of total items there are in the question is usually the modulo we are working in. In this case, 12 hours means we are working in modulo 12.

Example: Let's say that today is a Monday. What day of the week will it be in:

(a) 280 days?

(b) 365 days?

(c) 1000 days?

Solution:

(a) Let's change 280 into modulo notation. Since we are concerned with the day it will be, we will use modulo 7 as there are 7 days.

$$280 \equiv 0 \ (mod \ \ 7)$$

This means that in 280 days, it will be a Monday.

(b) Let's change 365 into modulo notation. Since we are concerned with the day it will be, we will use modulo 7 as there are 7 days.

$$365 \equiv 1 \ (mod \ \ 7)$$

This means that in 365 days, it will be one day later, a Tuesday.

(c) Let's change 1000 into modulo notation. Since we are concerned with the day it will be, we will use modulo 7 as there are 7 days.

$$1000 \equiv 6 \ (mod \ \ 7)$$

This means that in 1000 days, it will be six days later, a Sunday.

Problem Set

NOTE: A leap year occurs every four years. A leap year occurs on any year that is divisible by 4 (**ex:** 4, 8, 12 ... 1996, 2000, 2004, 2008, 2012)

1. Solve the following:
   (a) What is 84 (mod 9)?
   (b) What is 52 (mod 5)?
   (c) What is -4 (mod 10)?
2. Create the following tables:
   (a) Addition table for modulo 7
   (b) Multiplication table for modulo 7
3. 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!)
4. One year on Venus lasts 225 Earth days. Alysha 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.
5. It is 8:00 AM in our 24 hour world. What time is it in a 3 hour world?
6. Using a standard 52 card deck I deal all the cards out to Vince, Tim, and myself. Were the cards dealt evenly?
7. Luc is facing West, he rotates 1260° clockwise. What direction is he now facing? (**Note:** A circle has 360 degrees)
8. ** 1 year on Jupiter is equal to approximately 12 Earth years. On what day of the week did you celebrate your 1^{st} Jovian (or Jupiterian) birthday? (If you haven't turned 1 on Jupiter yet, calculate on which day of the week your 1^{st} birthday will fall)
9. *** Tim 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?