Module 4 Congruence Arithmetic

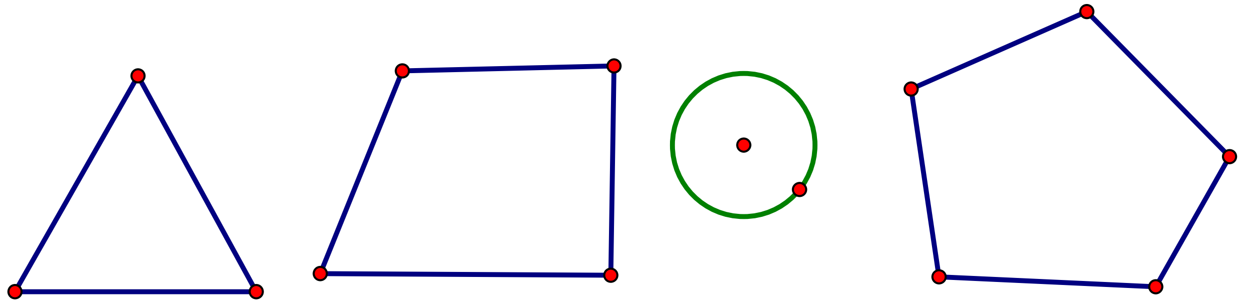
Popper 4
Introduction to what is like
Modulus choices
Partitions by modulus
- Mod 5
- Mod 7
- Mod 30

Modular Arithmetic
- Addition
- Subtraction
- Multiplication
  - INTEGERS!
- Mod 12
- Cayley Tables! And Groups!
- Powering up
- Division

Introduction

One of the exercises given to young children in several contexts is to indicate which of the items are the same/equivalent/similar and which are different.

Here's a fairly typical geometry assortment:



The business of "sorting and comparing" is quite serious and children are encouraged to develop skill at deciding what is similar and what is different and WHY. A young learner might note that there are objects with "points" and one that is different with only curving sides. A more mature student will discuss the polygons and the circle…different vocabulary, but still the same idea.

Another version of this same sorting and grouping behavior comes in learning algebra: grouping "like terms". In the math expression $3x+5b-x+16$, the terms with the "x" can be combined because they are "like" and the other two terms have to be left as is yielding $2x+5b+16$ as the simplified equivalent expression.

In high school, students studying for the SAT encounter questions like "which of the following is the next number in the sequence"?

1 4 9 16 25

This is a simple one: 36 is next because it's the sixth in the line of numbers and squaring is what is happening to each index number. The other answers of this multiple choice question will be "not like" and not in the pattern.

This type of question is just a more sophisticated version of which is similar and which is different. This is an important skill that people use constantly. Retailers group “like” items in departments and on shelves within those departments. Sometimes people are in groups according to “likes” and “dislikes” or by beliefs (such as in religion and politics!). When you are organizing a drawer you group similar objects and put them in a single container.

In this module we are going to look at a clever way of grouping numbers into “like” subsets. We will look at **congruent numbers**; this is a new idea. Congruent figures in geometry have the corresponding sides and angles measure the same…but what could be the same about two different numbers? Well, we’ve already looked at partitions using factors (abundant and deficient numbers as well as 1 plus prime and composite numbers) and partitions like even and odd (if the number divides evenly by 2 it is even; and if it leaves a remainder of 1 it is odd.). Now we will expand on this idea of dividing and checking the remainders.

Congruence with numbers is all about grouping and sorting whole numbers and integers into subsets and then exploring what can be done with those subsets.

First, let us set our criterion for “like”. This activity always starts with someone picking their favorite natural number and declaring it to be the “modulus”.

*

Note that when you are working with congruent numbers, you can pick your own modulus; or in a homework or test problem one might be declared for you to use in that problem.

There is no “understood modulus”. For example in the expression $5x^2 + x + \sqrt{x}$, the middle term has an “understood” coefficient and an “understood” exponent. Both are 1. In the third term, the radical is understood to be 2, square root. You must ALWAYS state your modulus, though, and it must be a natural number greater than one.

*

A modulus is a number chosen to be the measure against which we are going set each number in our chosen set. So we will be comparing whole numbers to the modulus by division and placing them in subsets – we will be partitioning our number set!

*

The number of partitions always equals the size of the modulus so using 5 means we will have 5 disjoint subsets of like numbers when we are done.

Mod 5/Whole numbers

*

> If two whole numbers are congruent, they have the SAME REMAINDER when divided by the modulus.

When two numbers are congruent, we use "$\equiv_b$" to denote that two numbers are congruent mod *b*.

*

Now, believe it or not, this is actually a useful way to group numbers. These subsets have an official name: congruence classes. They also have a uniform presentation: the smallest positive natural number in the set is put in square brackets to symbolize the whole list in that class. Some authors use the word "equivalence" instead of "congruence" so I will use this expression, too.

Let’s check the assertion that there are 5 disjoint subsets on a number line that lists quite a few whole numbers starting with zero and going past 15

Do you see the pattern?

What are the subsets?

*

Suppose we look at 5, 26, 31, 45, and 93 and sort them with a modulus of 5.

Which of these are congruent when 5 is the modulus? Which is to say “which of these have the same remainder when divided by 5”?
*

We will divide each number by 5 and record the remainder:

$5 \div 5$	$R = 0$
$26 \div 5$	$R = 1$
$31 \div 5$	$R = 1$
$45 \div 5$	$R = 0$
$93 \div 5$	$R = 3$

Aha! Two numbers 5 and 45 are congruent mod 5 because the remainder is 0 for each of them. Additionally 31 and 26 are congruent mod 5 because the remainder is 1. 93 has a reminder of 3 and 3 divided by 5 is zero with a remainder of 3 so 93 is congruent mod 5 to 3; it is the only one from the list in congruence class 3, but we can still use our new notation for it

So 5 $\equiv_5 45$, 26 $\equiv_5 31$, and $93 \equiv_5 3$.

*

Now we indicate the congruence class with remainder 0 as [0]. (We use square brackets around the remainder zero.)

Here are some alternate statements for this congruence class:

[0] =

A small list of [0] would be

*

*

We can also see that we have

[1] =

A small list of [1] would be

And there's that [3] with 93 as a set element! Do you see that one formula for [3] is $5n + 3$?

If $n = 3$, then $5(3) + 3$ is in our set and $18 \equiv_5 93$.

Let’s check our understanding of this notion.

Popper 4, Question 1

So we've got [0], [1], [3] as our equivalence classes for mod 5. I mentioned earlier that we would have as many congruence classes as the size of our modulus. So we've got three classes and need two more:

They are [2] and [4].

Here is a list of the formulas that generate each congruent class.
Remembering that n is a whole number:

$5n$ generates all of [0]
$5n + 1$ generates all of [1]
$5n + 2$ generates all of [2]
$5n + 3$ generates all of [3]
$5n + 4$ generates all of [4]

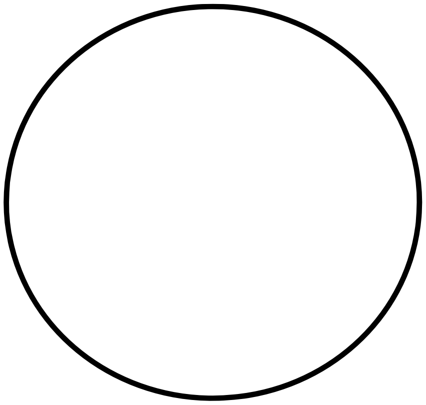
You just start with $n = 0$, then use $n = 1$, and so on forever in each class to make the list of elements in each set.

Partition on the WHOLE NUMBERS…why?

We can look more closely at the entries in [2]. If we look closely at 2, we can see that 2 = 5(0) + 2…that's why it is the smallest element and the conventional name of the congruence class. And we can look at the number 7 differently: 5 goes into 7 one time with a remainder of 2. Both of these ways of looking at 2 and 7 show that $2 \equiv_5 7$ is a true statement. 7 = 5(1) + 2.

In reality, because the whole numbers loop through the congruence classes in a dependable pattern, we most often use a circle or a clock to set up the classes.

Let’s look at the mod 5 clock:



So let us review our material up to this point.
*

Mod 7 on the whole numbers*

*

So we are going to partition the whole numbers into 7 disjoint sets. What are our labels? Since we start with a remainder of 0, the largest class will be labeled 6.

Here they are: {[0], [1], [2], [3], [4], [5], [6]}

*

We can pick [3] mod 7 as a nice one to work with. What numbers are in [3] mod 7? Well the set name itself tells you exactly which whole numbers are in there: all the $7n + 3$ numbers where n is a whole number are in there. We could also say that all the whole numbers with a remainder of 3 when divided by 7 are the set elements.

To list the elements in the set [3] mod 7. Start with *n* = 0 and use it in the formula. Then go to *n* = 1 and so on.

Well which ones are those?

We can set up a small table: we will list the whole numbers, *n*, down the left and the elements of [3] mod 7 down the right. Fill in the table with me. How am I calculating these set elements?

0	[3]
1	10
2	17
3	
4	
5	
n	

Ok. There's [3] mod 7.

Is 94 in [3] mod 7? Well, we can find out:

$7\sqrt{93}$

Let’s see, 7 goes into 93 thirteen times with a remainder of 2. Nope, 93 is in remainder class [2] mod 7. So 93 $\equiv_7 2$. We say “93 is congruent to 2 mod 7”. 93 is also congruent to 30 = 7(4) + 2. Do you know why? How would we write that?

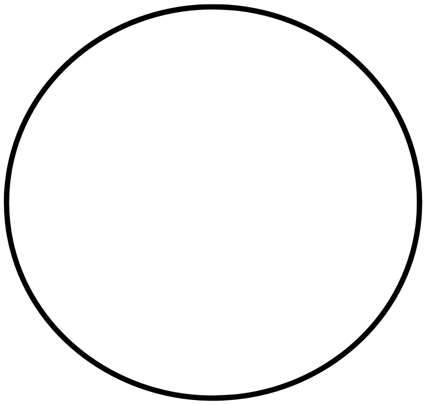
But did we not just find that $93 \equiv_5 3$? (nb mod 5!) This is why you need to specify the modulus clearly. The whole scene changes equivalence classes with each modulus!

What about [5] mod 7?

*

Popper 4, Question 2

Let’s look at the mod 7 clock now and think about what it gives us:



Popper 4, Question 3

One additional way to check congruence:

Theorem:

If a $\equiv_c$ b, then a – b $\equiv_c$ 0. [Note a and b are integers. C is natural.]

Let's translate this to Manglish:

Illustration of the theorem:

Is 47 $\equiv_3$ 32? If it is, then the difference of the two numbers is divisible by 3. (Look closely at the theorem again, see that "0". That's a number that is a multiple of *c*, the modulus).

47 – 32 = 15 which is in [0], a multiple of 3. Yes!

Let's check a more familiar way. 3 divides 47 with a remainder of 2 and 32 = 3(10) + 2. Yes again!

Proof of the theorem:

$a = c(p) + k$ and $b = c(q) + k$ where $[k]$ is the equivalence class they are in. If you subtract them $a - b = c(p) + k - (c(q) + k)) = c(p - q)$. A multiple of c is your answer.

Note that the theorem produces an easy way to check on congruence!

Popper 4, Question 4

If we have numbers that are "congruent", we can also talk about them being "equivalent". Here's part of a definition of equivalent from the internet:

e·quiv·a·lent

iˈkwivələnt/

adjective

- having the same or a similar effect as.

"some regulations are equivalent to censorship"

- Mathematics

belonging to the same equivalence class.

noun

noun: **equivalent**; plural noun: **equivalents**

2. **1**.

a person or thing that is equal to or corresponds with another in value, amount, function, meaning, etc.

"the French equivalent of the FBI"

synonyms: counterpart, parallel, alternative, match, analog, twin, clone, opposite number;

We will focus on "corresponds with another in value" and "comparable".

Mod 15

When we are working with a modulus of 15, note that $31 \equiv_{15} 46$ they are each in [1] mod 15. There are some theorems and facts we can explore about the situation of having equivalent or congruent numbers.

How many equivalence classes (aka congruence classes) are there?

Modular Arithmetic

*

This is true with congruent or equivalent numbers with any modulus.

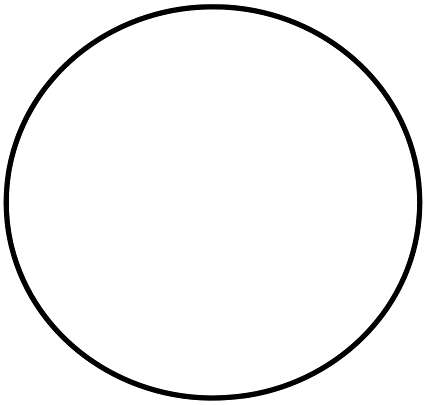
Example. Add 6 to each side of $31 \equiv_{15} 46$, are 37 and 52 equivalent?

Well, 37 is in [7] mod 15 and 52 = 15(3) + 7. This is saying they are congruent.

Let's apply the new theorem, too: 52 – 37 = 15 which is a multiple of 15…it is 15(1) and is in [0] so yes they are equivalent or congruent

Note that the results of the addition are NOT in [1] as they were when we started but they are each in [7] and still equivalent or congruent. The equivalence jumped from [1] to [7].

Example:
Checking the mod 7 clock, let’s see what addition and subtraction look like.



Let’s look at

[5] + [3]

[6] – [2]

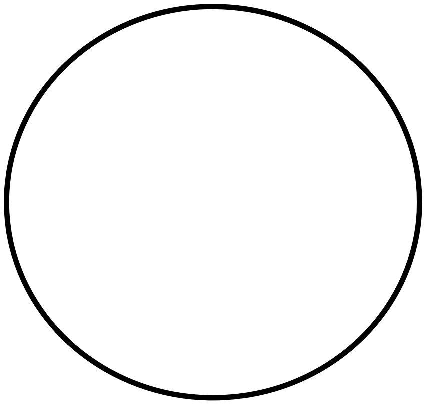
[4] + [3]

Mod 30

We can do another example with a different modulus: 30. 152 = 30(5) + 2 and 30(14) + 2 = 422. These are equivalent and in [2] mod 30. What happens if we say 152 $\equiv_{30}$ 422 and if we subtract 9 from each side of the equivalence relation? We will maintain equivalence and change the equivalence class.

152 – 9 = 143 and 422 – 9 = 413. Which equivalence class are we in?
143 = 30(4) + 23 and 413 = 30(13) + 23.

So we have moved from equivalence class [2] to equivalence class [23]. That seems odd…we subtracted 9. Check the mod 30 clock to see how this happens.



What's different about subtraction than addition? Do real clocks work this way?

Popper 4, Question 5

Multiplication/Powering up/Division:

Here are a pair of congruent numbers mod 3:

$1 \equiv_3 4$ if we multiply both sides of the equivalence by 2 we get

$2 \equiv_3 8$ Is this true? $8 - 2 = 6$, a multiple of three. Perfect!

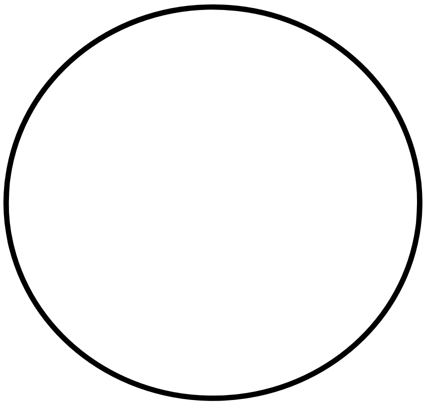
We were in [1] now we're in [2], though.

Here are a pair of numbers congruent mod 7:

$10 \equiv_7 31$ if we multiply both sides by -1. What do we get?

$-10 \equiv_7 -31$

Is this true? Well $-10 - -31 = 21$, a multiple of 3…BUT what about those negative numbers…we've suddenly gone into **integers**. (as promised!) Are there ways to work with integers? Sure, let's look at the mod 7 clock again…

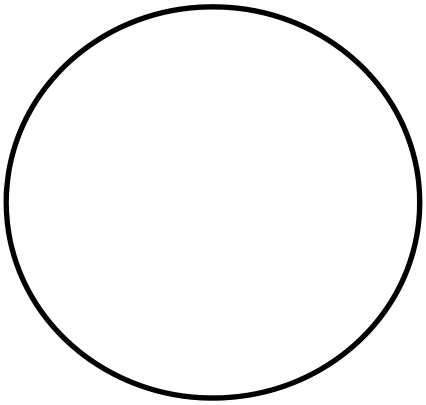


So we can rotate around anti-clockwise (most un-clocklike!) and put in those integers. Back at the beginning, I announced that we would work with whole numbers for a while and now I am branching into integers.

So, are these two integers $\{-8, -13\}$ congruent mod 5?

*

Let's look at a mod 5 clock:



Let’s do a number line of this, mod 5:

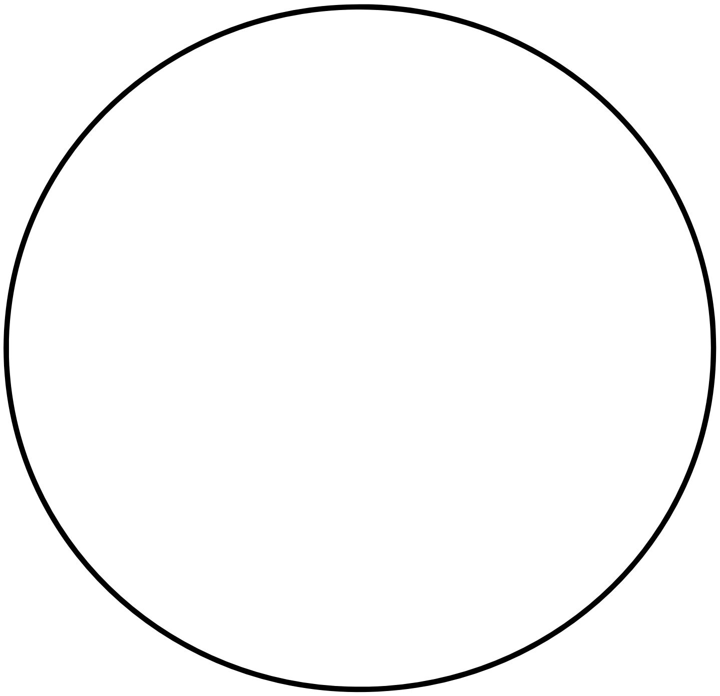
Popper 4, Question 6

So now, let's review with mod 12 and whole numbers as our set

How many equivalence classes and what are they?

Pick [7] mod 12: which whole numbers are in there? What is the formula for the numbers that are in there? How can we tell if 43 is in there?

Let’s look at a mod 12 clock



Is this looking somewhat familiar?

What clock do they use in Europe?
Can we do arithmetic with this clock? Sure we do it all the time.
It’s 11am. If I want to meet you in 3 hours when is that?
First let’s do it on the clock. Then let’s do it with equivalence classes.

This is all about teaching youngsters to tell time as opposed to teaching them to add numbers. Maybe it is a little natural for them to get confused when 11 + 3 is one number in one context and another number in another context.

How exciting it is to find that BOTH numbers are RELATED in fact. Here's the relationship: $14 \equiv_{12} 2$. Not equal, but equivalent mod 12.

Let's do some arithmetic, not with numbers but with equivalence classes. First we can do this with equivalence classes mod 12.

[0] + [6] = [6] What does this tell us?*

24 + 18 = 42 is 42 in [6] mod 12? 12(3) + 6 = 42

Why does this work? We can do a little proof.

We need to begin by picking arbitrary set elements not specific numbers:

Well some number in [0] is $12n$ and any number in [6] is $12m+ 6$.

And then we can add them and so some algebra with that sum

$12n + 12m + 6 =$

$12(n +m) + 6$.

There is the formula for a number in [6]…see the remainder added on the right? What can I say about that $n + m$? Is it some whole number? CLOSURE

So [0] + [6] = [6].

How about [10] + [5]?

Let's count it out on the mod 12 clock. Then look at it algebraically.

$12n + 10 + 12m + 5 =$

$12(n + m) + 15 =$

$12(n + m) + 12 + 3 =$

$12(n + m + 1) + 3.$

Is $n + m + 1$ a whole number? Does the " + 3" tell us everything?

Now, I'd like to go back to mod 5 and work with addition and subtraction.

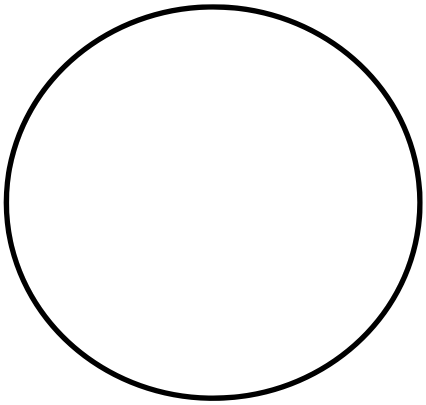
We can make a table of all the addition problems possible and multiplication problems.

We'll use Cayley tables in the effort. Two of them.

More addition, this time with a Cayley Table Mod 5

We have {[0], [1], [2], [3], [4]} to work with. Let’s look at the clock and keep track of our answers. To save time and energy I will leave the square brackets off the table.

+ mod 5					



Is this a group? How can you tell? What do you need to show?

So we’re going full circle here. We’re back at groups!

Let's look a bit closer at mod 6 and whole numbers. Let's do a list of the congruence classes and look at them closely for primes and composites.

[0]

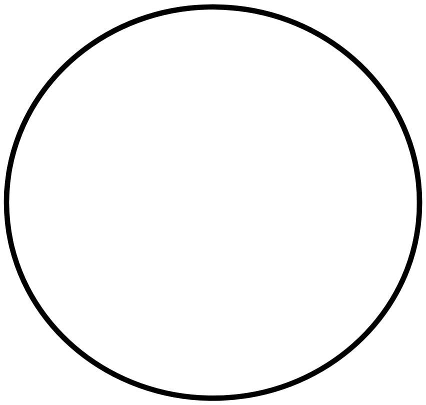
[1]

[2]

[3]

[4]

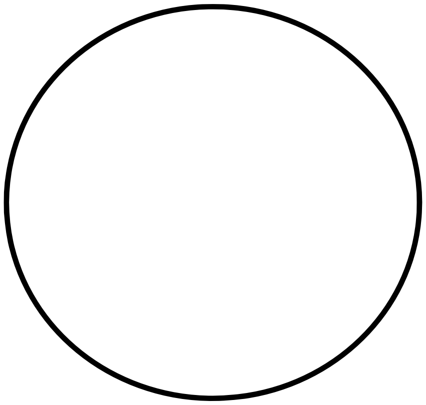
[5]



There is LOTS of ink expended on attributing mystical powers to the equivalence classes that contain the primes mod 6, but it's arithmetic not magic that makes that work!

Let's do some arithmetic mod 6

$[2] + [3] \equiv_6$ illustration:



Let's do a Cayley table and check for group properties. Note that this is both a partition on the whole numbers (how do we know) AND a group!

+ mod 6						

Check partition: i.e. doing the modular sorting

Check group: taking the partition and putting in a combining operation

These ideas are NOT separate!

Popper 4 Question 7

Let’s look at Mod 2 on the integers and review where we are. Let’s also expand from adding to multiplying.

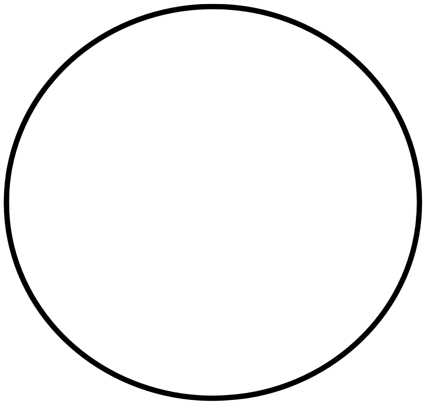
Mod 2 equivalence classes:

[0]

[1]

What do we call these?

Partition?



Addition Cayley Table:

+ mod 2		

Group?

Theorem 1

The sum of two even numbers is even.

Theorem 2

The sum of two odd numbers is even.

Theorem 3

The sum of an even number and an odd number is odd.

Popper 4 Problem 8

Multiplication Cayley Table:

Group?

Checking against our theorems:

Theorem 1

The product of two even numbers is even.

Theorem 2

The product of two odd numbers is odd.

Theorem 3

The product of an even number and an odd number is even.

Ok. Let's do some more addition and multiplication with equivalence classes:

$9 \equiv_4 25$ Check this:

Which congruence class?

Add 3 to both sides:

$12 \equiv_4 28$ True?

Which equivalence class?

Multiply both sides by 2

$18 \equiv_4 50$ True?

Popper 4 Question 9

Now for division, there's a wrinkle

Let's look at

$6 \equiv_4 14$ True?

Divide both sides by 2

BUT $4 \equiv_4 20$ divide both sides by 2 OOPS

What happened and why?

Division is a bit of a problem. Sometimes it works just fine and sometimes not?

When does it work?

When the modulus and the divisor are relatively prime it ALWAYS works. If they are NOT, then it sometimes works and sometimes doesn't.

Let's go back to mod 6

$15 \equiv_6 21$ divide both sides by 3…oops but $(3, 6) = 3$!

$5 \equiv_6 35$ divide both sides by 5 …works! $(5, 6) = 1$

So addition is nice, multiplication is nice BUT division is a bit tricky.

Popper 4 Question 10

It turns out that **powering up** by the same exponent is also nice.

Let’s check a couple of those:

$2 \equiv_6 8$ square both sides 4 ? 64…check!

$3 \equiv_4 7$ note mod 4, square both sides: 9 ? 49…check!

So now we’ve looked at addition, subtraction, multiplication, division, and exponentiation. That’s a LOT really.

Let’s do an illustration of why powering up works:

$8 \equiv_5 13$ both are in [3]

8 squared is (5(1) + 3) squared

25 + 2(5)(3) + 9 watch that “+ 9”

13 squared is (5(2) + 3) squared

100 + 2(10)(3) + 9…see that?

That’s the key…

So now WRAPPING up:

We can compare numbers mod x by division. We create a partition on our set with this comparison. When we make a Cayley table with the congruence classes we have a BIG PICTURE group with all the trimmings.

We can do arithmetic with the equivalence classes. It's NOT standard number arithmetic, but we can add, subtract, and multiply the classes. Division takes a bit more qualifying. Exponentiation works just fine.

This is a really new way to look at numbers and I'll be very interested in hearing from you how you learn about it!

dog@uh.edu