MATH 417 – FIRST WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Notes: This is a quick and sloppy version of the notes from the first week of the semester. No attempt to make it look nice, and color is gone, because of the kind of document-type this is.

August 24, 2020, in advance

Hello, and welcome to Math 417. This first lecture is intended to be very informal. No proofs and no "official" definitions, but an introduction to some of the ideas we'll be working with. And, as a warning: these lectures won't be filled with fancy imagery or video or sound effects: I'm not so good at that, and the mathematics is more important, anyway.

The mathematical objects I'll be talking about today are motions of objects, like rotations and flips, as well as what happens to the last digits of integers when you write them out in base 10 and multiply them. These are introductions to permutations and to arithmetic "mod n". Everything I talk about will be given a more careful definition later.

The first thing I want to talk about is the idea of abstraction, which sounds harder than it really is. The key idea is that you can look at two very different objects and find a fundamental commonality between them. Here's an example from food.

Consider the following four items to eat (visualize them!):

(1) A grilled cheese sandwich.
(2) A slice of pizza.
(3) A quesadilla.
(4) A toasted bagel with cream cheese.

These are obviously different foods, and if you ordered one of them at a restaurant and got another, you would not be happy.

On the other hand, they have a common structure: a hot bread-like object at the bottom and melted cheese. The breads are all different, and some also have bread on top, or sauces, but these are still somehow in the same category.

Now I'd like to talk about a couple of examples of what we will soon call a cyclic group with two elements.

The integers divide up into even integers and odd integers, and these properties behave in a consistent way when you add them. By this, I mean that an even number plus an even number is always even, an even number plus an odd number (in either order) is always odd and an odd number plus an odd number is always even. To put this in table form:

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

I hope the interpretation of this table is clear. We're going to be using such tables a lot. (I found the coding format at overleaf.com. If you want to do a paper in LaTeX, I highly recommend this site.) Here's another example. I have a sheet of paper, and two motions. I can either do nothing, or flip the paper front to back. What happens when we combine these operations?

Doing nothing, well, does nothing, but two front-to-back flips take us where we started, and it's like doing nothing. Let's make a table.

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Look familiar?

I'll put the two tables together:

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

These are very similar. In fact, if you define the function Φ so that Φ(Combine)= Plus, Φ(Nothing)=Even and Φ(Flip)=Odd, then Φ exactly maps the first table to the second. The inverse function Φ^{-1} would map the second table to the first.

We will say (with a more formal definition later) that these two situations are "isomorphic", and Φ is the isomorphism.

Here's another example. Imagine a square S with vertices labeled 1,2,3,4 in clockwise order:

$$S \quad = \quad \begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$$

Let T define a clockwise rotation by $\frac{\pi}{2}$. Using what I hope is an obvious notation, let T^2 denote two instances of T, which amounts to a clockwise rotation by π and let T^3 denote three instances of T, which

amounts to a clockwise rotation by $\frac{3\pi}{2}$, or a counterclockwise rotation by $\frac{\pi}{2}$. I don't have to define anything else. Why? Because if I do four instances of T, or T^4, then it's rotation by 2π, which is as if I did nothing at all.

The combined diagram for these rotations is:

$$S = \begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix} \qquad T(S) = \begin{matrix} 4 & 1 \\ 3 & 2 \end{matrix}$$

$$T^2(S) = \begin{matrix} 3 & 4 \\ 2 & 1 \end{matrix} \qquad T^3(S) = \begin{matrix} 2 & 3 \\ 1 & 4 \end{matrix}$$

Some more notation. Usually, when we do nothing we refer to it either as "I" or the identity, as if we were multiplying matrices, or "e", which means the same thing when objects are lower case. So $T^4 = I$ (the identity), and also, by convention $I = T^0$, or doing T zero times, which is the same as doing nothing.

Notice that T^5 would be rotation by $\frac{5\pi}{2} = 2\pi + \frac{\pi}{2}$, so doing five rotations is like doing one rotation and $T^5 = T$, etc.

In short, the "multiplication table" for rotations of a square looks like this:

Mult	I	T	T^2	T^3
I	I	T	T^2	T^3
T	T	T^2	T^3	I
T^2	T^2	T^3	I	T
T^3	T^3	I	T	T^2

A nice cyclic pattern. In fact, we will soon see that the set $\{I, T, T^2, T^3\}$ is an example of what is called a **cyclic group of order 4** and denoted C_4.

If you've seen arithmetic "mod 4", you might notice that, since $T^4 = I$, $T^5 = T$ and $T^6 = T^2$, *multiplication* in this table is like *addition* of the exponents of T mod 4.

Mult	I	T	T^2	T^3
I	I	T	T^2	T^3
T	T	T^2	T^3	I
T^2	T^2	T^3	I	T
T^3	T^3	I	T	T^2

,

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The wrap-around pattern of the second table has a rhythm that we'll see a lot of. I hope you can imagine what a table of size $n \times n$ would look like. In fact, if $n = 10$, what it would look like is the addition table for the usual decimal expression of the last digits of integers.

Let me give you a different instance of a C_4. One nice property of positive integers is that if you know the last digit of m and the last digit of n, then you know the last digit of mn. (This follows from the multiplication algorithm you're taught in school, but it is also true if you look at number is bases other than 10, as we'll soon see.) For example, anything ending in "3" times anything ending in "7" will end in "1".

$$3 * 17 = 51, \qquad 13 * 7 = 91, \qquad 33 * 27 = 891, \quad \text{etc.}$$

Now look at the powers of 3: $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^5 = 243$, $3^6 = 729$, $3^7 = 2187$, $3^8 = 6561$, we see a repeating pattern in the last digit: 1,3,9,7,1,3,9,7,1,... .

This suggests consideration of a multiplication table for all integers "ending" in 1, 3, 7, 9 in base 10.

I'll write the table in two ways, both of which convey the same information. The entries in the first are in increasing order; the entries in the second show the structure.

$*$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$*$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

I hope you see that the second table is the same as the "$\{0, 1, 2, 3\}$" table we saw a few pages ago, except that the names are changed. Also notice that if we take the "subtable" only involving $\{1, 9\}$, we get a table like the cyclic groups of order two:

$*$	1	9
1	1	9
9	9	1

One final example of motions. Now allow two different motions of our square S: X is rotation around a vertical axis through the center of the square, so that 1 and 2 flip and 3 and 4 flip, and Y is rotation around a horizontal axis, so that 1 and 4 flip and 2 and 3 flip. (Try to guess what happens when you do X followed by Y or Y followed by X.)

$$S = \begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix} \qquad X(S) = \begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix} \qquad Y(S) = \begin{matrix} 4 & 3 \\ 1 & 2 \end{matrix}$$

$$X(Y(S)) = XY(S) = Y(X(S)) = YX(S) = \begin{matrix} 3 & 4 \\ 2 & 1 \end{matrix}$$

Yes, XY and YX are the same as T^2, a rotation by π. This is not too surprising: both X and Y flip front to back, so doing them twice keeps the front in front, which means we have a rotation. Notice also that if you do any of these rotations twice, you get back to doing nothing, which I'll call I again. Here's the multiplication table, where I've written $Z = XY$:

*	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Notice that the product of any two of $\{X, Y, Z\}$ gives the third.

Also notice that this is *not* like the C_4 we saw before: every element squares to I (look at the main diagonal!) and there is no element whose powers give the whole set.

For historical reasons, this is called V, the *Klein four-group*, after Felix Klein (1849-1925): V is *not* isomorphic to C_4. We are nearly done with this first lecture, but there are a few things I wanted to say about these examples, and which we'll be returning to in later classes.

I didn't give a numerical example for V, but one example, as we'll see later, multiplication of odd integers mod 8.

Consider all rotations and flips of a square. It turns out that there are eight of them, and the multiplication is *not* commutative. (That is, not *abelian*.) Check this out yourself: see what happens when you rotate a square by $\frac{\pi}{2}$ and flip on a vertical axis, or do it in the other order. We'll spend a lot of time with this situation later. It leads to what is called D_4 or the *dihedral group of order eight*.

Now consider a regular polygon with n vertices. The rotations of the n-gon give a nice example of C_n, the cyclic group with n elements, and its rotations and flips comprise D_n, the dihedral group with $2n$ elements, which is *not* abelian.

Because $\{1, 3, 7, 9\}$ are the numbers less than 10 which have no common factor with 10, we'll give their group of multiplication the fancy name of $(\mathbb{Z}/10\mathbb{Z})^*$, and also look at the analogous set $(\mathbb{Z}/n\mathbb{Z})^*$ for any positive integer n. It takes a little work, but we'll show that this is always a group too.

In case $n = p$ is a prime number, it turns out that there are $p - 1$ elements in $(\mathbb{Z}/p\mathbb{Z})^*$, and it is a non-trivial theorem that they form a

cyclic group. If you've had Math 453, this is what the "primitive root" is all about.

Everything I've talked about today is an example of a group. If we considered the "one's place" decimal digit addition, together with multiplication, we would have an example of a ring. Strange things can happen in a ring: for example $4 * 5 = 0$ in this ring, even though neither 4 nor 5 equals 0. Other examples of rings include polynomials.

Finally, don't worry if you don't understand these hints I'm making about future topics. We'll deal with them more carefully later.

Email me any questions you might have on this presentation, so I can talk about them in class on Monday.

Thank you for lasting this far. We've actually made it through the first day.

August 26, 2020, in advance

We're going to talk about two main things today: the definition of a group and the definition of modular arithmetic, which will give us many nice examples of a group.

First, some standard notation:

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

are the *integers*, and

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

are the *natural numbers* and

$$\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\right\}$$

are the *rational numbers*.

As with V, these names come from the German; e.g. "integer" in German is "zahl".

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

(1) There is an element $e \in G$ so that, for all $x \in G$, $x*e = e*x = x$. (identity)
(2) For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$. (inverse)
(3) For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$. (associativity)

The following notations are standard: the inverse of x is usually written as x^{-1}. For $n \in N$:

$$x^1 := x, \quad x^2 := x * x, \quad x^n := x * x^{n-1} \quad \text{if } n > 2.$$

We also define $x^0 := e$ and for $n \in N$, $x^{-n} := (x^n)^{-1}$.

It is a boring but true result that $x^m * x^n = x^{m+n}$ for $m, n \in \mathbb{Z}$. I think it's in the book, but if you want me to write it up I can. It uses induction.

Every set with a multiplication table I gave on Monday is a group. I've changed the look a little. Remember

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

?

Let me write these tables again in a more abstract way:

$*$	g	h
g	g	h
h	h	g

This table should be read as saying that $g * g = g$, $g * h = h$, $h * g = h$, and $h * h = g$. I hope you can see that g is the identity here, because whenever you $*$ it with x (x can be g or h), you get x, and since $h * h = g$, this means that h is its own inverse: $h = h^{-1}$. One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

Here's the table for one of the two C_4's we had on Monday

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Notice that the element 0 is the identity and $0 + 0 = 1 + 3 = 2 + 2 = 3 + 1 = 0$, so the inverses of $0, 1, 2, 3$ in order are $0, 3, 2, 1$.

As we'll see at the end, this is just addition mod 4. Just to finish the review, let me remind you of the multiplication table for the Klein 4-group V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Since the identity is I and $g^2 = g * g = I$ for every $g \in V$, this means that $g = g^{-1}$ for every $g \in V$. Again, it's not obvious that $*$ is associative from the table, but this follows from the interpretation of the elements as motions. I'll return to this later.

I should make the idea of a multiplication table more formal. Suppose we have a group $(G, *)$ and $G = \{g_1, \ldots, g_n\}$ is a finite set. Then we define the *multiplication table of* G as follows:

$*$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\cdots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\cdots$	$g_2 * g_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$g_n * g_1$	$g_n * g_2$	$\cdots$	$g_n * g_n$

There are two conventions: we usually write the first element of the product down the left and the second element of the product across the top and in the same order. Usually, $g_1 = e$. There's a convention that we usually put the identity in the first row and the first column and that we have both in the same order. Now I'm going to prove our first theorem about groups. It's not hard, and you could easily imagine this just being given as part of the definition. But mathematicians practice Jenga. We try to assume as few properties as possible which keep the whole structure intact.

THEOREM 1 If $(G, *)$ is a group and $x, y, z \in G$, then

$$x * y = x * z \implies y = z.$$

The proof won't fit here, so I'll start it on the next page. PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

But now, remember that a group is associative, so

$$x^{-1} * (x * y) = (x^{-1} * x) * y; \qquad x^{-1} * (x * z) = (x^{-1} * x) * z$$

And since x^{-1} is the inverse of x,

$$(x^{-1} * x) * y = e * y = y; \qquad x^{-1} * (x * z) = e * z = z,$$

so to review and put it all in two lines:

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z) \implies$$
$$(x^{-1} * x) * y = (x^{-1} * x) * z \implies e * y = e * z \implies y = z. \quad \square$$

If any part of that is unclear, try to prove it in the opposite direction:
THEOREM 2: $y * x = z * x \implies y = z$.

But be careful with the order in which you apply the operations. We will have examples later where $y * x = x * z$, but $y \neq z$.

By Theorem 1, if $G = \{g_1, \ldots, g_n\}$ and $g_i \in G$, then

$$\{g_i * g_1, \ldots g_i * g_n\}$$

are different elements and they are all in G, so this means that this set is just a rearrangement or *permutation* of G.

In other words, each rows of the multiplication table contains the elements of G in some order. Theorem 2 implies that the columns are a permutation too. Those of you who do Sudoku will recognize the pattern.

Let's check this out with V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

We can use this to identify groups. Suppose $(G, *)$ is a group and $|G|$, the number of elements in G is 2. One of them has to be the identity e. Call the other one g. Let's write out the table knowing this fact and knowing that e is the identity:

$*$	e	g
e	e	g
g	g	g*g

What can $g * g = g^2$ be? We know from Theorem 1 that the set $\{g * e, g * g\} = \{g, g^2\}$ is a permutation of $G = \{e, g\}$, so we are forced to conclude that $g^2 = e$. In other words the group we wrote down with 2 elements is basically the only one possible.

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

$$m \in \mathbb{Z} \implies m + 0 = 0 + m = m.$$

Is there an inverse? Sure:

$$m + (-m) = (-m) + m = 0,$$

and since 0 is the identity, $-m$ is the inverse of m in this group.

Addition in $\mathbb{Z}$ is also associative. The exact same argument shows that $(\mathbb{Q}, +)$ and even our friend $(\mathbb{R}, +)$ is a group too.

What about $\mathbb{N}$? Several problems: $0 \notin \mathbb{N}$ so there is no identity, and in fact, none of the elements in $\{1, 2, \dots\}$ has an inverse! So, $(\mathbb{N}, +)$ is not a group. What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

Is there an inverse? Well, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, so these elements have inverses, but $2 \cdot x = 1$ has no solution for $x \in \mathbb{Z}$ and $0 \cdot x = 1$ has no solution of any kind, so $(\mathbb{Z}, \cdot)$ is not a group.

What about $(\mathbb{Q}, \cdot)$, the rational numbers with multiplication, so that $m * n = m \cdot n$? This has identity element 1, and also

$$\frac{m}{n} \cdot \frac{n}{m} = 1.$$

So inverses exist? Well, almost. This doesn't work with $m = 0$, but every non-zero rational has an inverse. We let $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ denote the set of non-zero rationals.

Persuade yourself that $(\mathbb{Q}^*, \cdot)$ satisfies all the conditions, and is a group. I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

$$d\mathbb{Z} = \{\dots, -4d, -3d, -2d, -d, 0, d, 2d, 3d, 4d, \dots\}$$

Then $(d\mathbb{Z}, +)$ is a group. It's a subset of $\mathbb{Z}$, so we'll be calling this a subgroup before too long.

Let me look at the first two non-trivial examples. It's easy to check that there are both groups, with 0 as the identity and the obvious elements as inverses.

$$2\mathbb{Z} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\},$$
$$3\mathbb{Z} = \{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}.$$

Is $(G_1, *) := (2\mathbb{Z}, +) \cup (3\mathbb{Z}, +)$ a group? No, and for a strange reason. Our definition of the binary operation requires that $x * y \in G_1$. This is what fails here! We have $-2 \in (2\mathbb{Z}, +)$ and $3 \in (3\mathbb{Z}, +)$, but $-2+3 = 1$ is not in $(2\mathbb{Z}, +) \cup (3\mathbb{Z}, +)$.

Intersections, on the other hand, will always be a group. Let $(G_2, *) = (2\mathbb{Z}, +) \cap (3\mathbb{Z}, +)$. We'll show before too long that this intersection is precisely $(6\mathbb{Z}, +)$, and more generally,

$$(m\mathbb{Z}, +) \cap (n\mathbb{Z}, +) = (LCM(m, n)\mathbb{Z}, +),$$

where $LCM(m, n)$ denotes the least common multiple of m and n.

One more infinite group. This is called $\mathbb{Z} \oplus \mathbb{Z}$. The elements are (m, n) where $m, n \in \mathbb{Z}$ and the operation is component-wise addition; that is,

$$(m_1, n_1) * (m_2, n_2) = (m_1 + m_2, n_1 + n_2).$$

You should be able to check that the identity element is (0,0), that the inverse of (m, n) is $(-m, -n)$ and that $*$ is associative.

Time to do some number theory. Based on class Monday, I think this should all be review. (Let me know if I'm wrong.) We'll be working with $\mathbb{Z}$ here.

Suppose $m, n \in \mathbb{Z}$, $m \neq 0$. We say that $m \mid n$ (or m is a *divisor* or a *factor* of n or n is a *multiple* of m) if there exists $t \in \mathbb{Z}$ so that $n = mt$, or equivalently if $\frac{n}{m} \in \mathbb{Z}$. Even though $0 \mid n$ is impossible, it is always the case that if $m \neq 0$, then $m \mid 0$, because $0 = m \cdot 0$. For example, $417 = 3 \cdot 139$; divisors of 417 are 1, 3, 139, and 417.

Suppose $d \in \mathbb{N}$, $d \geq 2$ and $m, n \in \mathbb{Z}$. The notation

$$m \equiv n \mod d$$

means that $d \mid n - m$, or $n - m = dt$ for some integer t or, equivalently $n = m + dt$ or $m = n - dt$.

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t + 1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

Why is r unique? Suppose $n = dt_1 + r_1$ and $n = dt_2 + r_2$ and $r_1, r_2 \in \{0, 1, \ldots, d-1\}$. Subtract the two equations for n to get $0 = d(t_1 - t_2) + (r_1 - r_2)$, so that $r_1 - r_2 = d(t_2 - t_1)$ is a multiple of d. But $-(d-1) \leq r_1 - r_2 \leq d - 1$, and the only multiple of d in $\{-(d-1), \ldots, d-1\}$ is 0, so $r_1 - r_2 = 0$ and $r_1 = r_2$ and $t_1 = t_2$. $\square$

When $d = 1$, $r = 0$ and this is a boring case we ignore.

Let's look at this for $d = 2$. I will write $\mathbb{Z}$ and put the elements $\equiv 0 \mod 2$ in red, and the elements $\equiv 1 \mod 2$ in blue. Notice that this is unambiguous. The red elements are the even integers and the blue elements are the odds. (Lost in translation)

$$\{\ldots,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4, \ldots\}$$

Now for $d = 3$, I'll write these out in three rows:

$$0 \mod 3 = \{\dots, -12, -9, -6, -3, 0, 3, 6, 9 \dots\},$$
$$1 \mod 3 = \{\dots, -11, -8, -5, -2, 1, 4, 7, 10 \dots\},$$
$$2 \mod 3 = \{\dots, -10, -7, -4, -1, 2, 5, 8, 11 \dots\},$$

I hope you can imagine these as forming a *partition* of $\mathbb{Z}$; that is, every integer is in exactly one of these sets.

I now want to formalize this with another bit of notation. First reach back into Math 347 for the definition of equivalence relation and equivalence classes.

LEMMA The condition $a \sim b \iff a \equiv b \mod d$ forms an equivalence relation.

PROOF. We have three things to check. First: is $a \equiv a \mod d$? Yes, because d always divides $a - a = 0$. Second, suppose $a \equiv b \mod d$. Is $b \equiv a \mod d$? Sure. We have $d \mid b - a$, so $b - a = dt$ for some integer t and so $a - b = d(-t)$ and $-t \in \mathbb{Z}$, so $b \equiv a \mod d$. Finally, suppose $a \equiv b \mod d$ and $b \equiv c \mod d$. Then $b - a = dt$ and $c - b = du$ for integers t and u. If we add these, we get that $c - a = (b - a) + (c - b) = d(t + u)$, so $a \equiv c \mod d$. □

So now, suppose $d \in \mathbb{N}$, and $a \in \mathbb{Z}$. We define $[a]_d$ to be

$$\{n \in \mathbb{Z} \mid n \equiv a \mod d\} = \{a + dt \mid t \in \mathbb{Z}\} = a + d\mathbb{Z}.$$

If $a \equiv b \mod d$, then $[a]_d = [b]_d$, because it's an equivalence relation. We often say that $[a]_d$ is the set of integers *congruent to a mod d*.

Theorem 3 can now be rephrased as saying that for all d,

$$\mathbb{Z} = [0]_d \cup [1]_d \cup \cdots \cup [d-1]_d$$

We saw this fact earlier for $d = 2$ and $d = 3$. The next theorem is critical for our work and the method of proof is a very useful one which is rarely taught explicitly. If you want to prove something, it is often helpful to take one of your hypotheses and parameterize it.

THEOREM 4: Suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $d \in \mathbb{N}$ with $d \geq 2$. Then

$$a_1 \equiv a_2 \mod d \quad \textbf{and} \quad b_1 \equiv b_2 \mod d \implies$$
$$a_1 + b_1 \equiv a_2 + b_2 \mod d \quad \textbf{and} \quad a_1 b_1 \equiv a_2 b_2 \mod d.$$

PROOF: We can write $a_2 = a_1 + dt$ and $b_2 = b_1 + du$ for some $t, u \in \mathbb{Z}$. Then

$$(a_2 + b_2) - (a_1 + b_1) = a_1 + dt + b_1 + du - (a_1 + b_1) = d(t + u);$$
$$a_2 b_2 - a_1 b_1 = (a_1 + dt)(b_1 + du) - a_1 b_1 =$$
$$a_1 b_1 + a_1 du + b_1 dt + d^2 tu - a_1 b_1 = d(a_1 u + b_1 t + dtu),$$

so the difference in each case is a multiple of d, and the claimed congruence equations are true. □

Why is this important? We now define the set

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

This is a set with d elements, each element is an infinite set. The union of these elements is all of $\mathbb{Z}$, but remember that $\mathbb{Z}/d\mathbb{Z}$ is a finite set. For example

$$\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} = \{\text{even integers, odd integers}\}.$$

The point of the theorem is that we can now define two binary operations of addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ by

$$[a]_d \oplus [b]_d = [a+b]_d, \qquad [a]_d \odot [b]_d = [ab]_d.$$

This is a subtle point. We have $[a]_d = [a+d]_d = [a-417d]_d$ etc. The set can be given with lot of different names, but it doesn't matter when we are doing the operations, because the sums and the products will always be the same, no matter what name you use.

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

PROOF. We have the group and the operation. And from the definition,

$$[a]_d \oplus [0]_d = [a+0]_d = [a]_d,$$

so $[0]_d$ is the identity element. Further,

$$[a]_d \oplus [-a]_d = [a-a]_d = [0]_d,$$

so every element $[a]_d$ has the inverse $[-a]_d$. Finally,

$$([a]_d \oplus [b]_d) \oplus [c]_d = [a+b]_d \oplus [c]_d = [a+b+c]_d$$
$$[a]_d \oplus ([b]_d \oplus [c]_d) = [a]_d \oplus [b+c]_d = [a+b+c]_d$$

so associativity holds. □

Remember here $+$ is addition in $\mathbb{Z}$ and $\oplus$ is addition in $\mathbb{Z}/d\mathbb{Z}$. I will finish up with the group table for $\mathbb{Z}/4\mathbb{Z}$. It will look familiar.

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Yes, this is our old friend C_4.

So, for example $[3]_4 \oplus [2]_4 = [5]_4 = [1]_4$. After today, when d is understood, we'll write "$[a]_d$" as "a" to simplify things. It saves me four extra characters in LaTeX!

One last thought. Multiplication? We can write out the binary operation

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is not a group! Even though $[1]_4$ is an identity element, neither $[0]_4$ nor $[2]_4$ has an inverse.

What do you think happens with $(\{[1]_4, [3]_4\}, \odot)$?

Tune in on Friday.

And remember your job!

August 26, 2020, in class

I'd like to highlight a few things from the lecture I distributed Tuesday evening, and based on your emails. I got some questions about THEOREM 3

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t+1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

On the next page, I will give an illustration of the proof when $n = 12$ and $d = 5$.

We have $\frac{12}{5} = 2.4$, and the largest integer ≤ 2.4 is 2. So the first part of the last equation is

$$2 \leq 2.4 < 3$$

We got 2.4 from dividing by 5, so now I'll multiply through by 5

$$2 \cdot 5 \leq 12 < 3 \cdot 5$$

Now I'll subtract $2 \cdot 5$ from this equation

$$0 \leq 12 - 2 \cdot 5 < 5$$

In general, we have $d(t+1) - dt = d$ and an integer r which satisfies $0 \leq r < d$ must be one of $\{0, 1, \ldots, d-1\}$.

Here, $r = 12 - 2 \cdot 5 = 12 - 10 = 2 \in \{0, 1, 2, 3, 4\}$, and what we really want is that

$$12 \equiv 2 \mod 5.$$

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

Why is r unique? Suppose we had two different representations:

$$n = dt_1 + r_1, \qquad r_1 \in \{0, 1, \ldots, d-1\}$$
$$n = dt_2 + r_2, \qquad r_2 \in \{0, 1, \ldots, d-1\}$$

Subtract these two equations to get

$$n - n = 0 = d(t_1 - t_2) + (r_1 - r_2) \implies r_1 - r_2 = -d(t_1 - t_2) = d(t_2 - t_1).$$

This means that $r_1 - r_2$ is a multiple of d. But $0 \leq r_1, r_2 \leq d-1$. The largest $r_1 - r_2$ can be is $(d-1) - 0 = d - 1$ and the smallest $r_1 - r_2$ can be is $0 - (d-1) = -(d-1)$:

$$r_1 - r_2 \in [-(d-1), (d-1)].$$

The multiples of d are $\{\ldots, -2d, -d, 0, d, 2d, \ldots\}$ and so the only multiple of d in $[-(d-1), (d-1)]$ is 0, so $r_1 - r_2 = 0$ and $r_1 = r_2$ and $t_1 = t_2$, and the two representations are the same.

Now something different. In the lecture part, We've seen that the only group with two elements is the cyclic one. What about three?

Suppose $G = \{e, x, y\}$, three different elements, where e is the identity. What we already know about the multiplication table:

$*$	e	x	y
e	e	x	y
x	x	?	?
y	y	?	?

What can $x * x$ be? It has to be one of $\{e, x, y\}$ and, since $e * x = x$, if $x * x = x$, then $e = x$, which is impossible, so $x * x \neq x$. Thus, either $x * x = e$ or $x * x = y$. We'll explore these cases now.

Suppose $x * x = e$. Then the table becomes

$*$	e	x	y
e	e	x	y
x	x	e	?
y	y	?	?

What about $x * y$?

It has to be different from $x*e = x$ and $x*x = e$, because remember that the rows have to be a permutation of $G = \{e, x, y\}$. This means that $x * y = y$. But $e * y = y$, and that shows that this is impossible. (Columns have to be permutations too.)

In other words, this multiplication table cannot be completed and no such group exists!

Since $x*x = e$ is impossible, we are forced to conclude that $x*x = y$

*	e	x	y
e	e	x	y
x	x	y	?
y	y	?	?

And now, to complete the row, we have to have $x * y = e$, and by looking at the columns, we can complete the last row:

*	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

This table actually has a nice interpretation. I'll write it again, but with $y = x * x = x^2$:

*	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

This is basically the same thing as $(\mathbb{Z}/3\mathbb{Z}, \oplus)$. I'll just write "0" for "$[0]_3$", etc

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

August 28, 2020, in advance

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.

What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$\begin{aligned}
&(g*g*g)*(g*g*g*g*g)\\
&= g*g*g*g*g*g*g*g\\
&= \ g*g*g*g*g*g*g*g\\
&= (\ g*g*g*g*g*g*g)*g*g\\
&= e*g*g = g^2
\end{aligned}$$

Or, you can think of a C_6 as the rotations of a regular hexagon, where g is clockwise rotation by $\frac{2\pi}{6} = 60$ degrees. Then g^k is rotation by $60 \cdot k$ degrees. So g^3 is rotation by 180 degrees and g^5 is rotation by 300 degrees, so $g^3 * g^5 = g^8$ is rotation by 480 degrees, but g^6 is rotation by 360 degrees, which is like doing nothing, so the net effect is rotation by $480 - 360 = 120$ degrees.

Another way to do this is to think of the cyclic group of order 6 as addition mod 6, and then $3 + 5 = 8 \equiv 2 \mod 6$.

You could also think of an elaborate 6×6 multiplication table, which might take me 10 minutes to write, so think of those southwest to northeast diagonals.

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.

Here are their multiplication tables, which we've seen before.

$*_1$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$*_2$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Suppose Φ is the isomorphism map. We have by definition for all i,

$$\Phi(g^i) = \Phi(e *_1 g^i) = \Phi(e) *_2 \Phi(g^i),$$

so $\Phi(e)$ has to be the identity element in V and so $\Phi(e) = I$.

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have

three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\Phi(g) = X \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$
$$\Phi(g) = Y \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Y *_2 Y = I = \Phi(e),$$
$$\Phi(g) = Z \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Z *_2 Z = I = \Phi(e) \ .$$

There is no way to define $\Phi(g)$ that works and so there is no isomorphism. The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

In the other direction, suppose $d \in D(m) \cap D(n - km)$. Then, again, $d \mid m$, but also $d \mid n - km$. We have $m = dt$ and $n - mk = dv$, so $n = (n - mk) + km = d(v + kt)$, so the other inclusion holds: $D(m) \cap D(n - km) \subseteq D(m) \cap D(n)$. Thus the two sets are equal.

Let $A = D(m)$, $B = D(n)$ and $C = D(n - km)$. The logic is that if $x \in A \cap B$, then $x \in A, x \in B$. Work implies that $x \in C$, so $x \in A \cap C$, and this means formally that $A \cap B \subseteq A \cap C$. Similarly, if $x \in A \cap C$, then $x \in B$ so $x \in A \cap B$ and $A \cap C \subseteq A \cap B$ so $A \cap B = A \cap C$.

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

$$417 = 34 \cdot 12 + 9,$$
$$12 = 1 \cdot 9 + 3,$$
$$9 = 3 \cdot 3,$$

We have $gcd(12, 417) = 3$, and we want to write 3 as a linear combination of 12 and 417. First, $3 = 12 - 1 \cdot 9$. Then, $9 = 417 - 34 \cdot 12$, so

$$3 = 12 - 1 \cdot (417 - 34 \cdot 12) = 35 \cdot 12 - 417 = 420 - 417.$$

The same thing works in general. We have $x_{n-1} = c_{n-1}x_n + x_{n+1}$, so this gives the x_{n+1} the gcd, in terms of x_{n-1} and x_n. But also $x_{n-2} = c_{n-2}x_{n-1} + x_n$, so we have x_n in terms of x_{n-2} and x_{n-1}; plug it in to get x_{n+1} in terms of x_{n-2} and x_{n-1}. You just work your way back up the ladder.

I did a pathetic job of explaining this on Whiteboard; here's a better version. We define $(\mathbb{Z}/d\mathbb{Z})^*$ to be the set of integers a in $\{1,\ldots,d-1\}$ which are relatively prime to d, and then we're going to show that this is a group under $\odot$.

Let $d = 12$, so $a \in \{1,2,3,4,5,6,7,8,9,10,11\}$ and $D(12) = \{1,2,3,4,6,12\}$. Notice that 2 divides 12 and $\{2,4,6,8,10\}$ and 3 divides 12 and $\{3,6,9\}$ and this leaves $(\mathbb{Z}/12\mathbb{Z})^* = \{1,5,7,11\}$.

We have $5 \cdot 5 = 25 \equiv 1 \mod 12$, $5 \cdot 7 = 35 \equiv 11 \mod 12$, $5 \cdot 11 = 55 \equiv 7 \mod 12$, $7 \cdot 7 = 49 \equiv 1 \mod 12$, $7 \cdot 11 = 77 \equiv 5 \mod 12$, $11 \cdot 11 = 121 \equiv 1 \mod 12$, so, on the next page:

Here is the multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$, where the elements are to be technical, $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$.

$\odot$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

I hope you can see that this is isomorphic to one of our popular groups!

Today, we're going to do some group theory and some number theory and see how they are related. First, to review, a set G and a binary operation $*$ on G give a group $(G,*)$ provided we have an identity element, inverses, and $*$ is associative:

(1) There is an element $e \in G$ so that, for all $x \in G$, $x*e = e*x = x$.
(2) For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$.
(3) For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$.

Now I want to formalize some terminology I've already used. In case G is a finite set, we define $|G|$, the *order* of G to be the number of elements in G. We have already worked out all possible multiplication tables for groups of order two and three. If G is infinite, we won't talk about $|G|$.

I've talked about cyclic groups without being precise. Here is a definition of a cyclic group of order n. In this case G consists of n elements which are named $\{e = g^0, g = g^1, \ldots, g^{n-1}\}$. Informally, the elements are powers of g and $g^n = e$. More formally, we need to define what $g^i * g^j$ is for $i, j \in \{0,\ldots,n-1\}$

$$\text{If } i+j < n, \text{ then} \qquad g^i * g^j = g^{i+j}.$$
$$\text{If } i+j \geq n, \text{ then} \qquad g^i * g^j = g^{i+j-n}.$$

Here is an example we've already seen of a cyclic group of order n.

$*$	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

The identity element is $e = g^0$ and the inverse of g^i is g^{n-i} because $g^i * g^{n-i} = g^{i+(n-i)-n} = g^0 = e$. Another way of saying the rule is that $g^i * g^j = g^k$, where $k \equiv i + j \mod n$.

One concrete example of a cyclic group of order n is the set of rotations of a regular n-gon, where g represents rotation by $\frac{2\pi}{n}$.

Another concrete example is $(\mathbb{Z}/n\mathbb{Z}, \oplus)$, which we saw last time was a group. I'll repeat the group table for $n = 4$:

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

What do we mean when we say that two groups are "the same"?

What we mean is that they are isomorphic. Here is a formal definition. An isomorphism between two groups: $(G_1, *_1)$ and $(G_2, *_2)$. consists of a bijection Φ from $G_1 \mapsto G_2$: that is, a one-to-one onto map which "preserves" the binary operation: for all $x, y \in G_1$,

$$\Phi(x *_1 y) = \Phi(x) *_2 \Phi(y).$$

Don't panic about the notation! Since $x, y \in G_1$ and $\Phi(x), \Phi(y) \in G_2$, the choice of the binary operation is forced.

What this means in practice is that if you think of Φ as just changing names, then the multiplication tables of G_1 and G_2 are the same. The next page begins with an example with two cyclic groups of order three:

$*$	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g ,

$\oplus$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Let $G_1 = \{e, g, g^2\}$ and $G_2 = \{[0]_3, [1]_3, [2]_3\}$ and define $*_1$ and $*_2$ as the operations in the tables. If we now define

$$\Phi(e) = [0]_3, \quad \Phi(g) = [1]_3, \quad \Phi(g^2) = [2]_3,$$

then the multiplication tables are the same, and so G_1 and G_2 are isomorphic.

If $(G_1, *_1)$ and $(G_2, *_2)$ are isomorphic, we werite. $G_1 \approx G_2$. Here are some not very interesting statements that are easy to prove. I'll only talk about them if you want.

$$G \approx G, \qquad G_1 \approx G_2 \implies G_2 \approx G_1,$$
$$G_1 \approx G_2 \quad \text{and} \quad G_2 \approx G_3 \implies G_1 \approx G_3.$$

In other words, $\approx$ is an equivalence relation.

What we did earlier was to show that up to isomorphism, the only group of order 2 is C_2 and the only group of order 3 is C_3.

We already know two groups of order 4 which are not isomorphic: C_4 and V. Why are these not isomorphic?

Suppose they are isomorphic. I'll get a contradiction. The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.

Here are their multiplication tables, which we've seen before.

$*_1$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$*_2$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Suppose Φ is the isomorphism map. We have by definition for all i,

$$\Phi(g^i) = \Phi(e *_1 g^i) = \Phi(e) *_2 \Phi(g^i).$$

This means that $\Phi(e)$ has to be the identity in G_2; that is $\Phi(e) = I$ and $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$, since Φ is a bijection.

Suppose $\Phi(g) = X$. We have

$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$

but Φ was supposed to be one-to-one, so that's a contradiction. The same thing happens if $\Phi(g)$ is Y or Z.

This is a subtle argument, and I'll be happy to go through it again on Friday if you like.

One more point. Isomorphism can seem forbidding, and I've been telling you that it's easy: just look at the multiplication tables.

The problem with that idea is that, except for putting the identity first, there's no guarantee that the order of the elements will be the same in both groups. The following is a perfectly reasonable multiplication table for a cyclic group of order 4.

$\oplus$	$[0]_4$	$[2]_4$	$[1]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[2]_4$	$[1]_4$	$[3]_4$
$[2]_4$	$[2]_4$	$[0]_4$	$[3]_4$	$[1]_4$
$[1]_4$	$[1]_4$	$[3]_4$	$[2]_4$	$[0]_4$
$[3]_4$	$[3]_4$	$[1]_4$	$[0]_4$	$[2]_4$

If you don't look carefully, you might think this is the table for V. It isn't. Look at the main diagonal.

Back to number theory.

Remember that we talked about divisibility: for $a, b \in \mathbb{Z}$, $b \neq 0$,

$$a \mid b \iff \tfrac{b}{a} \in \mathbb{Z} \iff b = at, \quad \text{for some } t \in \mathbb{Z}.$$

This is *not* an equivalence relation, because $a \mid b$ and $b \mid a$ together imply that $a = b$. It still has some nice properties, though.

LEMMA (i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ and $a \mid c$, then for every $m, n \in \mathbb{Z}$, we have $a \mid mb + nc$.

PROOF (i) Let us write $b = at$ and $c = bu$, with $t, u \in \mathbb{Z}$. Then $c = (at)u = a(tu)$ and $tu \in \mathbb{Z}$.

(ii) Now with different hypotheses, write $b = at$ and $c = av$.Then $mb + nc = m(at) + n(av) = a(mt + nv)$ and $mt + nv \in \mathbb{Z}$.

For $n \in \mathbb{N}$, define $D(n)$ to be the set of positive divisors of n, all a with the property that $a \mid n$. For example, $D(12) = \{1, 2, 3, 4, 6, 12\}$ and $D(7) = \{1, 7\}$. A natural number $n \geq 2$ is *prime* if $D(n) = \{1, n\}$.

For $m, n \in \mathbb{N}$, the *greatest common divisor* of m and n or $gcd(m, n)$ is defined to be the largest number in $D(m) \cap D(n)$. If $g = gcd(m, n)$, then $g \mid m$ and $g \mid n$ and if $d \mid m$ and $d \mid n$, then $d \leq g$. It happens that 139 is prime and $417 = 3 \cdot 139$, so $D(417) = \{1, 3, 139, 417\}$ and $D(12) \cap D(417) = \{1, 3\}$, so $gcd(12, 417) = 3$.

An important special case is that, if $m \mid n$, then $gcd(m, n) = m$. The reason is that $m \mid m$ always, so $m \in D(m) \cap D(n)$, but if $d \in D(m)$, then $d \leq m$, so m has to be the largest.

Factoring integers is a hard problem, but calculating gcd's is easy, thanks to the Euclidean Algorithm, which is probably the oldest known algorithm still in use. Before we give the Algorithm, we need to prove an important lemma.

LEMMA: For $n, m, \in \mathbb{N}$, $k \in \mathbb{Z}$, if $n - km \in \mathbb{N}$, then $gcd(m, n) = gcd(m, n - km)$.

PROOF I want to show that $D(m) \cap D(n) = D(m) \cap D(n - km)$, and since the sets are equal, their largest elements are equal.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

In the other direction, suppose $d \in D(m) \cap D(n - km)$. Then, again, $d \mid m$, but also $d \mid n - km$. We have $m = dt$ and $n - mk = dv$, so $n = (n - mk) + km = d(v + kt)$, so the other inclusion holds: $D(m) \cap D(n - km) \subseteq D(m) \cap D(n)$. Thus the two sets are equal. □

The Euclidean algorithm is based on this. Remember 12 and 417? By one of Wednesday's results, we can write 417 as a sum of a multiple of 12 and an integer between 0 and 11. In fact:

$$417 = 12 \cdot 34 + 9 \implies 9 = 417 - 12 \cdot 34.$$

By the lemma, $gcd(12, 417) = gcd(12, 417 - 12 \cdot 34) = gcd(12, 9)$. That is much easier! We can repeat the process, noting that

$$12 = 9 \cdot 1 + 3.$$

Now, $gcd(12, 9) = gcd(9, 12) = gcd(9, 12 - 9 \cdot 1) = gcd(9, 3)$.

If we do this one more step, then $9 = 3 \cdot 3$, so $3 \mid 9$ and $gcd(9, 3) = 3 = gcd(12, 417)$.

More formally, start with $x_0, x_1 \in \mathbb{N}$ and write:

$$\begin{aligned}
x_0 &= c_0 x_1 + x_2, && c_0 \in \mathbb{N}, \quad x_2 \in \{0, \ldots, x_1 - 1\} \\
x_1 &= c_1 x_2 + x_3, && c_1 \in \mathbb{N}, \quad x_3 \in \{0, \ldots, x_2 - 1\} \\
&\vdots \\
x_n &= c_n x_{n+1}, && c_n \in \mathbb{N}.
\end{aligned}$$

Then $gcd(x_0, x_1) = gcd(x_1, x_2) = \cdots = gcd(x_n, x_{n+1}) = x_{n+1}$.

$$\begin{aligned}
417 &= 34 \cdot 12 + 9, \\
12 &= 1 \cdot 9 + 3, \\
9 &= 3 \cdot 3,
\end{aligned}$$

so $gcd(12, 417) = gcd(417, 12) = gcd(12, 9) = gcd(9, 3) = 3$. How do we know this is an algorithm; that is, that it will stop?

Notice that from the construction, $x_1 > x_2$ and $x_2 > x_3$, etc. Since $x_i \in \mathbb{N}$, this process can take at most x_1 or so steps.

If the last $x_{n+1} = 1$, then we know we are done, because 1 divides everything.

If $gcd(m,n) = 1$, then m and n are called *relatively prime*. This will be a big deal.

Let's return to cyclic groups, and let's look at C_{10}. There are ten elements $\{e, g, g^2, \ldots, g^9\}$, $g^{10} = e$.

What would we we took the powers of other elements? It's coming to the end, so I won't do all ten, but I'll show you g^3 and g^4.

The powers of g^3 are:

$$(g^3)^0 = e, (g^3)^1 = g^3, (g^3)^2 = g^6, (g^3)^3 = g^9, (g^3)^4 = g^{12} = g^2,$$
$$(g^3)^5 = g^{15} = g^5, (g^3)^6 = g^{18} = g^8, (g^3)^7 = g^{21} = g,$$
$$(g^3)^8 = g^{24} = g^4, (g^3)^9 = g^{27} = g^7$$

Everything is there. Getting g is key.

$$(g^4)^0 = e, (g^4)^1 = g^4, (g^4)^2 = g^8,$$
$$(g^4)^3 = g^{12} = g^2, (g^4)^4 = g^{16} = g^6, (g^4)^5 = g^{20} = e,$$

and we can stop here because $(g^4)^5 = e$, and we'll just be repeating ourselves. What we get are $\{e, g^2, g^4, g^6, g^8\}$, the powers of g^2.

The theorem here, which we'll get to eventually, is that if you have $C_n = \{g^i\}, g^n = e$, then the powers of g^i are equal to the powers of $g^{gcd(i,n)}$.

You should check for yourself that $gcd(3,10) = 1$ and $gcd(4,10) = 2$.

August 28, 2020, in class

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.

What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$(g*g*g)*(g*g*g*g*g)$$
$$= g*g*g*g*g*g*g*g$$
$$= g*g*g*g*g*g*g*g$$
$$= (g*g*g*g*g*g)*g*g$$
$$= e*g*g = g^2$$

Or, you can think of a C_6 as the rotations of a regular hexagon, where g is clockwise rotation by $\frac{2\pi}{6} = 60$ degrees. Then g^k is rotation by $60 \cdot k$ degrees. So g^3 is rotation by 180 degrees and g^5 is rotation by 300 degrees, so $g^3 * g^5 = g^8$ is rotation by 480 degrees, but g^6 is rotation by 360 degrees, which is like doing nothing, so the net effect is rotation by $480 - 360 = 120$ degrees.

Another way to do this is to think of the cyclic group of order 6 as addition mod 6, and then $3 + 5 = 8 \equiv 2 \mod 6$.

You could also think of an elaborate 6×6 multiplication table, which might take me 10 minutes to write, so think of those southwest to northeast diagonals.

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.

Here are their multiplication tables, which we've seen before.

$*_1$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$*_2$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Suppose Φ is the isomorphism map. We have by definition for all i,

$$\Phi(g^i) = \Phi(e *_1 g^i) = \Phi(e) *_2 \Phi(g^i),$$

so $\Phi(e)$ has to be the identity element in V and so $\Phi(e) = I$.

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\begin{gathered}
\Phi(g) = X \implies \\
\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e), \\
\Phi(g) = Y \implies \\
\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Y *_2 Y = I = \Phi(e), \\
\Phi(g) = Z \implies \\
\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Z *_2 Z = I = \Phi(e) \ .
\end{gathered}$$

There is no way to define $\Phi(g)$ that works and so there is no isomorphism. The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

In the other direction, suppose $d \in D(m) \cap D(n - km)$. Then, again, $d \mid m$, but also $d \mid n - km$. We have $m = dt$ and $n - mk = dv$, so $n = (n - mk) + km = d(v + kt)$, so the other inclusion holds: $D(m) \cap D(n - km) \subseteq D(m) \cap D(n)$. Thus the two sets are equal.

Let $A = D(m)$, $B = D(n)$ and $C = D(n - km)$. The logic is that if $x \in A \cap B$, then $x \in A, x \in B$. Work implies that $x \in C$, so $x \in A \cap C$, and this means formally that $A \cap B \subseteq A \cap C$. Similarly, if $x \in A \cap C$, then $x \in B$ so $x \in A \cap B$ and $A \cap C \subseteq A \cap B$ so $A \cap B = A \cap C$.

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

$$\begin{aligned} 417 &= 34 \cdot 12 + 9, \\ 12 &= 1 \cdot 9 + 3, \\ 9 &= 3 \cdot 3, \end{aligned}$$

We have $gcd(12, 417) = 3$, and we want to write 3 as a linear combination of 12 and 417. First, $3 = 12 - 1 \cdot 9$. Then, $9 = 417 - 34 \cdot 12$, so

$$3 = 12 - 1 \cdot (417 - 34 \cdot 12) = 35 \cdot 12 - 417 = 420 - 417.$$

The same thing works in general. We have $x_{n-1} = c_{n-1}x_n + x_{n+1}$, so this gives the x_{n+1} the gcd, in terms of x_{n-1} and x_n. But also $x_{n-2} = c_{n-2}x_{n-1} + x_n$, so we have x_n in terms of x_{n-2} and x_{n-1}; plug it in to get x_{n+1} in terms of x_{n-2} and x_{n-1}. You just work your way back up the ladder.

I did a pathetic job of explaining this on Whiteboard; here's a better version. We define $(\mathbb{Z}/d\mathbb{Z})^*$ to be the set of integers a in $\{1, \ldots, d-1\}$ which are relatively prime to d, and then we're going to show that this is a group under $\odot$.

Let $d = 12$, so $a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and $D(12) = \{1, 2, 3, 4, 6, 12\}$. Notice that 2 divides 12 and $\{2, 4, 6, 8, 10\}$ and 3 divides 12 and $\{3, 6, 9\}$ and this leaves $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$.

We have $5 \cdot 5 = 25 \equiv 1 \mod 12$, $5 \cdot 7 = 35 \equiv 11 \mod 12$, $5 \cdot 11 = 55 \equiv 7 \mod 12$, $7 \cdot 7 = 49 \equiv 1 \mod 12$, $7 \cdot 11 = 77 \equiv 5 \mod 12$, $11 \cdot 11 = 121 \equiv 1 \mod 12$, so, on the next page:

Here is the multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$, where the elements are to be technical, $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$.

$\odot$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

I hope you can see that this is isomorphic to one of our popular groups!