MATH 417 – SECOND WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

August 31, 2020, in advance

Welcome to the beginning of the second week. We're going to start with number theory and apply it to group theory. It might not be obvious why I'm doing this. Patience will be rewarded.

Our ultimate goal is to give you another family of groups based on modular arithmetic. Here's a definition. I'll prove that these are groups at the end of the talk.

Suppose $n \geq 2$. Let

$$(\mathbb{Z}/n\mathbb{Z})^* := \{[a]_n \mid a \in \{1, \ldots, n-1\} \quad \text{and} \quad gcd(a, n) = 1\}$$

The set consists of the classes $x \equiv a \mod n$, where a and n are relatively prime. Let the operation be multiplication mod n, then

THEOREM For $n \geq 2$, $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is a group.

Proof at the end of class.

We already has an example for $n = 10$ on the first day. The possible values for a are taken from $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and we want their gcd with 10 to be 1. Since $D(10) = \{1, 2, 5, 10\}$, we take out the multiples of 2 ($\{2, 4, 6, 8\}$) and the multiple of 5 ($\{5\}$). This means that $(\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$.

I'll remind you of the table.

$\odot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\odot$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

The natural way to write the table is on the left, but from the right, I hope you can see that $((\mathbb{Z}/10\mathbb{Z})^*, \odot)$ is isomorphic to C_4.

Not every $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is cyclic, as we'll soon see.

Number theory. Remember that if $m, n \in \mathbb{N}$, then $gcd(m, n)$ is the largest integer g so that $g \mid m$ and $g \mid n$. If $gcd(m, n) = 1$, then m and n are said to be relatively prime.

We had the Euclidean Algorithm to calculate the gcd quickly. The basis of the idea is the division algorithm.

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

From Friday: $gcd(x_0, x_1) = gcd(x_1, x_2) = \cdots = \gcd(x_n, x_{n+1}) = x_{n+1}$. There's a numerical example on the next page. We'll also have a worksheet on Monday with smallish numbers. This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

$$\begin{aligned}
\underline{417} &= 1 \cdot \underline{341} + \underline{76},\\
\underline{341} &= 4 \cdot \underline{76} + \underline{37},\\
\underline{76} &= 2 \cdot \underline{37} + \underline{2},\\
\underline{37} &= 18 \cdot \underline{2} + \underline{1},\\
\underline{2} &= 2 \cdot \underline{1}.
\end{aligned}$$

So $gcd(341, 417) = 1$. We have

$$1 = 37 - 18 \cdot 2, 2 = 76 - 2 \cdot 37, 37 = 341 - 4 \cdot 76, 76 = 417 - 1 \cdot 341,$$

so

$$\begin{aligned}
1 = 37 - 18 \cdot 2 \ &= 37 - 18 \cdot (76 - 2 \cdot 37) = (1 + 2 \cdot 18) \cdot 37 - 18 \cdot 76\\
&= 37 \cdot 37 - 18 \cdot 76 \ = 37 \cdot (341 - 4 \cdot 76) - 18 \cdot 76\\
&= 37 \cdot 341 - 166 \cdot 76 \ = 37 \cdot 341 - 166 \cdot (417 - 341)\\
&= 203 \cdot 341 - 166 \cdot 417.
\end{aligned}$$

By calculation, $203 \cdot 341 = 69223$ and $166 \cdot 417 = 69222$.

If you remember, the divisors of 417 are 1, 3, 139 and 417, and it's not hard to check that the divisors of 341 are 1, 11, 31 and 341, and 1 is the only common divisor, so it's the greatest one. It is also true that $175 * 417 - 214 * 341 = 1$, and there are infinitely many such equations.

In precisely this way, we obtain a theorem whose proof I can give in detail on request. The idea is to use the calculations of the general Euclidean Algorithm in general the way we did just now.

THEOREM If $g = gcd(m, n)$, then there exist "computable" $r, s \in \mathbb{Z}$ so that $g = rm + sn$.

Computable means that there is an algorithm to find them. Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

LEMMA If $g = gcd(m, n)$, then $gcd(m/g, n/g) = 1$.

PROOF Rewrite the hypothesis in parametric form:

$$m = gr, \quad n = gs, \qquad m/g = r, \quad n/g = s, \qquad r, s \in \mathbb{N}.$$

I'll argue by contradiction that $gcd(r, s) = 1$. Suppose $h \in \mathbb{N}$ and $h \mid r$ and $h \mid s$. Then there exist $u, v \in \mathbb{N}$ so that $r = hu$ and $s = hv$. Combining this with the hypothesis gives

$$m = gr = g(hu) = (gh)u, \quad n = gs = g(hv) = (gh)v.$$

This means that gh is a common divisor of m and n, but g was the largest one, so $gh \leq g$, so $h = 1$. In other words, the only common divisor of r and s is 1, so it has to be the gcd. □

LEMMA If $a, b, c \in \mathbb{N}$, $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

PROOF. Since $gcd(a, b) = 1$, there exist $r, s \in \mathbb{N}$ so that $1 = ar + bs$, and since $a \mid bc$, there exists $t \in \mathbb{N}$ so that $bc = at$. Now we get sneaky and multiply the first equation by c: $c = arc + bsc$. But now

$$c = arc + bsc = arc + (bc)s = arc + (at)s = a(rc + ts).$$

so c is written as a multiple of a; that is, $a \mid c$. □

LEMMA If $gcd(a, n) = 1$ and $gcd(b, n) = 1$, then $gcd(ab, n) = 1$.

PROOF This is also sneaky. There exist $r, s, t, u \in \mathbb{Z}$ so that $1 = ar + ns$ and $1 = bt + nu$. Now multiply these together:

$$1 = 1 \cdot 1 = (ar + ns)(bt + nu) = abrt + naru + nsbt + n^2su$$
$$= ab(rt) + n(aru + sbt + nsu).$$

Thus, if d is a common divisor of ab and n, then $d \mid ab$ and $d \mid n$, so $d \mid 1$. That is, 1 is the only common divisor of ab and n. □ The final fact is the one that will be most useful to us.

THEOREM (i) If $ab \equiv 1 \mod n$, then $gcd(a, n) = gcd(b, n) = 1$.

(ii) If $gcd(a, n) = 1$, then there is an integer b so that $ab \equiv 1 \mod n$.

PROOF. For (i), if $ab \equiv 1 \mod n$, then there is an integer t so that $ab = 1 + nt$, which implies $1 = ab - nt$. If $d \mid a$ and $d \mid n$, then $a = dr, n = ds$. Therefore, $1 = ab - nt = a(dr) - (ds)t = d(ar - st)$, so $d \mid 1$, so $d = 1$.

For (ii), since $gcd(a,n) = 1$, we can write $1 = ar + ns$ for some integers r, s. This means that $ar = 1 - ns \equiv 1 \mod n$ (!). $\square$

For example, $gcd(341, 417) = 1$ and $1 = 203 \cdot 341 - 166 \cdot 417$ imply that $203 \cdot 341 \equiv 1 \mod 417$, and we get as an automatic bonus that $gcd(203, 341) = 1$ as well. Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G. **It's important that here we are keeping the same operation $*$.**

There are two automatic subgroups of any group G. One is $\{e\}$ the identity. The other is G itself. Any subgroup that is not one of these two is called a *proper* subgroup.

What are the conditions you need for a subset to be a subgroup? The first is that $*$ still has to be a binary operation: so you need that $h, h' \in H \implies h * h' \in H$. Groups need identities and so you need $e \in H$, and groups need inverses, so $h \in H$ implies that there exists $h' \in H$ so that $h * h' = e$. Because this is the same operation, we have to have $h' = h^{-1} \in H$. We don't have to worry about associativity! (Explanation on next page.)

If $h_i \in H$ then $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$ in H, because this equation holds for them as elements in G, which is a group, and so is associative. To sum up:

THEOREM If $(G, *)$ is a group and $H \subseteq G$, then $(H, *)$ is a group (and a subgroup of $(G, *)$) if and only if

$$e \in H, \quad h \in H \implies h^{-1} \in H, \quad h, h' \in H \implies h * h' \in H.$$

What are the subgroups of $G = C_6$? Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

The obvious subgroups of G are $\{e\}$ and C_6. I claim there are two others: $\{e, a^2, a^4\}$ and $\{e, a^3\}$. Here are the multiplication tables:

$*$	e	a^2	a^4
e	e	a^2	a^4
a^2	a^2	a^4	e
a^4	a^4	e	a^2

. A cyclic group of order 3.

We also have

$*$	e	a^3
e	e	a^3
a^3	a^3	e

, This is a cyclic group of order 2.

One more. Here is the Klein 4-group V. I'll remind you of its multiplication table.

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

What are the proper subgroups of V? Well any subgroup H has to have the identity, so $I \in H$. But there has to be another element.

Suppose it's X. The set $\{I, X\}$ is a cyclic group of order 2, so it's a subgroup. Similarly, $\{I, Y\}$ and $\{I, Z\}$ are both subgroups.

Can there be more? If a subgroup H has two of $\{X, Y, Z\}$, say X, Y, then it must have $X * Y = Z$, so it's all of V.

We've found that V has five subgroups, three of which are proper.

$$\{I\}, \quad \{I, X\}, \quad \{I, Y\}, \quad \{I, Z\}, \quad \{I, X, Y, Z\}.$$

We will spend a lot more time on finding subgroups.

Two hints for later in the semester. We'll show that if H is a subgroup of G, then $|H| \mid |G|$, that is, the order of H divides the order of G. Since $|V| = 4$, this will tell us automatically that any proper subgroup of V has an order dividing 4, but not equal to 1 or 4, so it has to be 2, as we've seen.

Suppose $(G, *)$ is a group and $g \in G$. Suppose m is the smallest integer so that $g^m = e$. Then m is called the *order* of m. We define *the subgroup generated by* g to be

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$$

We'll show that for any group G and $g \in G$, $\langle g \rangle$ is a subgroup of G. This was the case for C_6, since $\{e, a^2, a^4\} = \langle a^2 \rangle$ and $\{e, a^3\} = \langle a^3 \rangle$. We will also show that if $G = \langle a \rangle$ is a cyclic group of order n and $H = \langle a^k \rangle$, then $|H| = n/gcd(n, k)$. But that's for Wednesday and for the homework.

Finally, here's the proof that $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is a group.

1. If $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, then $[ab]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. We've seen that

$$gcd(a, n) = 1, \quad gcd(b, n) = 1 \implies gcd(ab, n) = 1.$$

2. The class $[1]_n$ is the identity: $[a]_n = [1 \cdot a]_n = [1]_n[a]_n$ and $gcd(1, n) = 1$ because 1 has no divisors larger than 1.

3. Inverses. We showed earlier that if $gcd(a,n) = 1$ then there exists b so that $ab \equiv 1 \mod n$ and $gcd(b,n) = 1$. This means that $[b]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ and $[a]_n[b]_n = [ab]_n = [1]_n$, so $[b]_n = [a]_n^{-1}$, and we have inverses.

Finally, associativity is automatic, because multiplication in $\mathbb{Z}$ is associative. □

I showed you $((\mathbb{Z}/10\mathbb{Z})^*, \odot)$ earlier. How about $((\mathbb{Z}/8\mathbb{Z})^*, \odot)$?

Which of $\{1,2,3,4,5,6,7\}$ are relatively prime to 8? Well, $D(8) = \{1,2,4,8\}$, so we're looking at odd numbers: $(\mathbb{Z}/8\mathbb{Z})^* = \{1,3,5,7\}$. How does the multiplication go mod 8?

$$3 \cdot 3 = 9 \equiv 1 \mod 8, 3 \cdot 5 = 15 \equiv 7 \mod 8, 3 \cdot 7 = 21 \equiv 5 \mod 8$$
$$5 \cdot 5 = 25 \equiv 1 \mod 8, 5 \cdot 7 = 35 \equiv 3 \mod 8, 7 \cdot 7 = 49 \equiv 1 \mod 8$$

This leads to this multiplication table. (I've written "a" for "$[a]_8$")

$\odot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

This is isomorphic to V. Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

Since 5 is prime, each of $\{1,2,3,4\}$ is relatively prime to 5, and it is easy to write the multiplication table:

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We see that 1 and 4 are their own inverses and $2 \cdot 3 = 1$. In fact, 2 has order 4: the powers of 2 are

$$2^0 = 1 \mod 5, \qquad 2^1 \equiv 2 \mod 5,$$
$$2^2 \equiv 4 \mod 5, \qquad 2^3 = 8 \equiv 3 \mod 5.$$

So the powers of 2 give $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$, and it's isomorphic to C_4.

I'll do some more examples on Wednesday,

August 31, 2020 in class

The Euclidean Algorithm computes $gcd(56, 200)$.

$$\underline{200} = 3 \cdot \underline{56} + \underline{32}$$
$$\underline{56} = 1 \cdot \underline{32} + \underline{24}$$
$$\underline{32} = 1 \cdot \underline{24} + \underline{8}$$
$$\underline{24} = 3 \cdot \underline{8}.$$

$$8 = 32 - 1 \cdot 24; \quad 24 = 56 - 1 \cdot 32 \implies$$
$$8 = 32 - (56 - 32) = 2 \cdot 32 - 56; \quad 32 = 200 - 3 \cdot 56 \implies$$
$$8 = 2 \cdot (200 - 3 \cdot 56) - 56 = 2 \cdot 200 - (2 \cdot 3 + 1) \cdot 56.$$
$$2 \cdot 200 = 400; \quad 7 \cdot 56 = 392, \qquad 400 - 392 = 8 \quad \checkmark$$

And, as predicted, $gcd(\frac{56}{8}, \frac{200}{8}) = gcd(7, 25) = 1$. You can find the Euclidean Algorithm for this by dividing everything above by 8.

I'd like to spend a little more time on C_6 and on powers of elements forming a subgroup. Remember

$$G = \{e, a, a^2, a^3, a^4, a^5\}, \qquad a^6 = e.$$

I'll talk about what the powers of a^j look like and $\langle a^j \rangle$.

The powers of e aren't exciting, because $e * e = e$, so $\langle e \rangle = \{e\}$. Since a generates the group, $\langle a \rangle = C_6$. I talked about $\langle a^2 \rangle$ and $\langle a^3 \rangle$ without details in the lecture. Here they are:

$$a^2, (a^2)^2 = a^4, (a^2)^3 = a^6 = e; \qquad a^3, (a^3)^2 = a^6 = e.$$

We can always stop when we get back to e because, for example, $(a^2)^4 = (a^2)^3 * a^2 = e * a^2 = a^2$. They just start repeating. So, as before,

$$\langle a^2 \rangle = \{e, a^2, a^4\}, \quad \langle a^3 \rangle = \{e, a^3\}.$$

This leaves $\langle a^4 \rangle$ and $\langle a^5 \rangle$. We have

$$a^4, (a^4)^2 = a^8 = a^2, (a^4)^3 = a^{12} = e;$$
$$a^5, (a^5)^2 = a^{10} = a^4, (a^5)^3 = a^{15} = a^3, (a^5)^4 = a^{20} = a^2,$$
$$(a^5)^5 = a^{25} = a, (a^5)^6 = a^{30} = e.$$

That is,

$$\langle a^4 \rangle = \{e, a^4, a^2\} = \langle a^2 \rangle$$

and

$$\langle a^5 \rangle = \{e, a^5, a^4, a^3, a^2, a\} = \langle a \rangle = G.$$

There is a general principle at work. Note that $a^2 * a^4 = a * a^5 = e$.

THEOREM If G is a group, $k \in \mathbb{N}$, and $x \in G$, then $\langle x^k \rangle \subseteq \langle x \rangle$.

PROOF By definition, $\langle g \rangle = \{g^i : i \in \mathbb{N}\}$. Thus if $y \in \langle x^k \rangle$, then $y = (x^k)^i$ for some i. That is, $y = x^{ki} \in \langle x \rangle$. $\square$

THEOREM If $x \in G$ has order m, then $\langle x \rangle = \langle x^{-1} \rangle$.

PROOF The situation is that $\{e, x, x^2, \ldots, x^{m-1}\}$ are distinct and $x^m = e$. Then $x * x^{m-1} = x^{1+(m-1)} = x^m = e$, so $x^{-1} = x^{m-1}$. What are the powers of x^{-1}? We have

$$(x^{-1})^2 = x^{-1} * x^{-1} = x^{m-1} * x^{m-1} = x^{2m-2} = x^m * x^{m-2} = x^{m-2},$$

and, more generally,

$$(x^{-1})^k = (x^{m-1})^k = x^{km-k} = x^{(k-1)m+m-k} = (x^m)^{k-1} x^{m-k} = x^{m-k}.$$

Thus, $\langle x^{-1} \rangle = \{e, x^{m-1}, x^{m-2}, \ldots x\} = \langle x \rangle$. □

Taking powers of x^{-1} just gives us the same elements in reverse order, as we saw with $x = a, x = a^2$ in C_6.

One thing new that I wanted to prove was to show that the only groups of order 4 are C_4 and V up to isomorphism. This will use the fact that the rows and the columns of a group multiplication table have to be different.

Suppose G is a group of order 4. I want to distinguish two cases:
(i) For every $g \in G$, $g^2 = e$.

(ii) There exists (at least one) element $x \in G$ so that $x^2 \neq e$.

We'll fill out the multiplication tables and show that (i) forces an isomorphism to V and (ii) forces an isomorphism to C_4.

(i) So, let's call the elements of the group $\{e, x, y, z\}$, so they are all different and we know by hypothesis that $x^2 = y^2 = z^2 = e$.

G	e	x	y	z
e	e	x	y	z
x	x	e	?	?
y	y	?	e	?
z	z	?	?	e

What can $x * y$ be? It can't be x or e because it shares a row with them and it can't be y because it shares a column, and it has to be in G, so it has to be z. Similarly, any product of two of these gives the third. So we have, on the next page,

G	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

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

There is an isomorphism ϕ between G and V and it is defined by $\phi(e) = I$, $\phi(x) = X$, $\phi(y) = Y$, $\phi(z) = Z$.

Now we consider (ii). There is an element $x \in G$ so that $x^2 = x * x \neq e$. Let's write the elements of the group as $\{e, x, x^2, y\}$, and complete the table as far as we can.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	?
x^2	x^2	?	?	?
y	y	?	?	?

The first thing you might think about is $x * x^2$, but all the table tells you is that it's not x, x^2, so it has to be e or y.

It is faster to look at $x * y$, which can't be x, x^2 or y, so it has to be e. The same thing holds for $y * x$, as we'll see on the next page.

G	e	x	x^2	y
e	e	x	x^2	y
x	x	x^2	?	e
x^2	x^2	?	?	?
y	y	e	?	?

Now we can fill out the rows and see that $x * x^2$ has to be y and $x^2 * x$ has to be y, so $y = x^3$, and the table starts to look familiar

G	e	x	x^2	x^3
e	e	x	x^2	x^3
x	x	x^2	x^3	e
x^2	x^2	x^3	?	?
x^3	x^3	e	?	?

We don't even have to finish the table, we have $x * x^3 = e = x^4$ and $G = \{e, x, x^2, x^3\}$, so this is a cyclic group of order 4.

TWO WORKSHEET PROBLEMS

Divide into groups. Calculators are ok, but not necessary.

1. Determine $g = gcd(30, 72)$ and find integers r, s so that $g = 30r + 72s$.

2. Recall that $((\mathbb{Z}/7\mathbb{Z})^*, \odot)$ is the multiplicative group mod 7 of relatively prime classes. Since 7 is prime,

$$(\mathbb{Z}/7\mathbb{Z})^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

For each a, determine $\langle [a]_7 \rangle$. Which a have the property that $\langle [a]_7 \rangle = (\mathbb{Z}/7\mathbb{Z})^*$?

SOLUTION to 1:

$$\underline{72} = 2 \cdot \underline{30} + \underline{12}$$
$$\underline{30} = 2 \cdot \underline{12} + \underline{6}$$
$$\underline{12} = 2 \cdot \underline{6}.$$

$gcd(30, 72) = 6$.

$$6 = 30 - 2 \cdot 12; 12 = 72 - 2 \cdot 30 \implies 6 = 30 - 2(72 - 2 \cdot 30)$$
$$= (1 + 2 \cdot 2)30 - 2 * 72 = 5 \cdot 30 - 2 \cdot 72 = 150 - 144 \qquad \checkmark$$

Note that $gcd(\frac{30}{6}, \frac{72}{6}) = gcd(5, 12) = 1$.

SOLUTION to 2

I'll just write a for $[a]_7$ a lot of the time.

As always, $\langle 1 \rangle = 1$. Since $2^2 = 4$, $2^3 = 8 \equiv 1 \mod 7$, $[2]_7$ has order 3, and $[2]_7^{-1} = [2]_7^2 = 4$, so

$$\langle 2 \rangle = \{1, 2, 4\} = \{1, 4, 2\} = \langle 4 \rangle$$

The powers of 3 are 1, 3, $3^2 = 9 \equiv 2 \mod 7$, $3^3 = 27 \equiv 6 \mod 7$, $3^4 = 81 \equiv 4 \mod 7$, $3^5 = 243 \equiv 5 \mod 7$, $3^6 = 729 \equiv 1 \mod 7$,

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}/7\mathbb{Z})^* = \langle 5 \rangle$$

Note that $[3]_7^{-1} = [3]_7^5 = 5$. Also, $3 * 5 = 15 \equiv 1 \mod 7$. You can simplify powers by working mod 7 all along, so $3^2 \equiv 2 \mod 7$ implies that $3^4 = (3^2)^2 \equiv 2^2 = 4 \mod 7$, etc.

Finally, $6^2 = 36 \equiv 1 \mod 7$, so $\langle 6 \rangle = \{1, 6\}$. This always happens: $(m-1)^2 = m^2 - 2m + 1 = m(m-2) + 1 \equiv 1 = (-1)^2 \mod m$.

September 2, 2020, in advance

Suppose G is a finite group and $x \in G$. We have defined $\langle x \rangle = \{x^n, n \in \mathbb{N}\}$. (There is a slightly different definition in infinite groups that we can ignore for now.) One reason we make the definition is the following theorem.

THEOREM 1: If $(G, *)$ is a finite group and $x \in G$, then $\langle x \rangle$ is a subgroup of G.

PROOF We have to prove that $\langle x \rangle$ is closed under $*$, has the identity and has inverses.

The first part is easy: two typical elements in $\langle x \rangle$ are x^m and x^n, where $m, n \in \mathbb{N}$, and $x^m * x^n = x^{m+n} \in \langle x \rangle$. (Note, I haven't formally proved this, but see p.50 of the book).

Suppose $|G| = n$. Then two elements of the set $\{x, x^2, \ldots x^{n+1}\}$ have to be equal (maybe more). This is the pigeonhole principle. To

be specific, say $x^i = x^j$, where $1 \leq i < j < n+1$. Thus we have in G,

$$x^i * e = x^i, \quad x^i * x^{j-i} = x^j = x^i$$
$$\implies x^i * e = x^i * x^{j-i} \implies e = x^{j-i}.$$

Let $m = j - i \in \mathbb{N}$, so that $e = x^m \in \langle x \rangle$. Thus the identity is in $\langle x \rangle$. Furthermore, $x * x^{m-1} = e$, so $x^{-1} \in \langle x \rangle$, and more generally, for any $x^i \in \langle x \rangle$,

$$x^i * x^{(m-1)i} = x^{i+(m-1)i} = x^{mi} = (x^m)^i = e^i = e,$$

so each x^i has an inverse. □

In general, these are not the *only* subgroups that G can have, but the first examples in which that happens have $|G| \geq 8$. However, it turns out that this is the case for cyclic groups. In fact, we can be much more specific.

THEOREM 2: If $G = \langle a \rangle$ is a cyclic group of order n, then the subgroups of G are given precisely by $H = \langle a^k \rangle$, where $k \mid n$.

PROOF First, suppose H is a subgroup of G, so all the elements of H can be written as a^i for some i. Let k denote the *smallest* positive exponent so that $a^k \in H$. Now let a^j denote *any* element in H. By the division algorithm, we can write

$$j = k \cdot s + r, \quad r \in \{0, \ldots, k-1\}.$$

Thus, $a^j = a^{ks+r}$. Since $a^k \in H$, $(a^k)^{-1} = a^{-k} \in H$ as well. We then have $(a^{-k})^s a^j = a^{-ks+ks+r} = a^r \in H$, because it is a product of two elements of H and H is a group. But $0 \leq r \leq k-1$, and k was the smallest *positive* exponent, so $r = 0$ and $a^j = a^{ks} = (a^k)^s \in \langle a^k \rangle$. In particular, $a^n = e \in H$, so we have $k \mid n$. That's the harder part of the proof. Here is the easier part. Suppose $H = \langle a^k \rangle$, where $k \mid n$. We know from Theorem 1 that H is a subgroup of G, and if we write $n = k\ell$, then we can exactly determine the elements of H:

$$\langle a^k \rangle = \{a^k, a^{2k}, \ldots, a^{(\ell-1)k}, a^{\ell k} = a^n = e\}.$$

So $|H| = \ell = \frac{n}{k}$ is the order of the subgroup. □

What happens with $\langle a^k \rangle$ when k is not a divisor of n?

THEOREM 3. Let $d = gcd(k, n)$. Then $\langle a^k \rangle = \langle a^d \rangle$.

PROOF. Write $k = dr$ and $n = ds$. We know that $gcd(r, s) = gcd(\frac{k}{d}, \frac{n}{d}) = 1$. In one direction,

$$\langle a^k \rangle = \{(a^k)^i\} = \{(a^{dr})^i\} = \{(a^d)^{ir}\} \subseteq \langle a^d \rangle.$$

If we can show that $a^d = a^{vk}$ for some v, then

$$\langle a^d \rangle = \{(a^d)^i\} = \{(a^{vk})^i\} = \{(a^k)^{iv}\} \subseteq \langle a^k \rangle,$$

so $\langle a^k\rangle \subseteq \langle a^d\rangle$ and $\langle a^d\rangle \subseteq \langle a^k\rangle$ imply they're equal. Remember that $k = dr$ and $n = ds$. Since $gcd(r,s) = 1$, there exist $v, w \in \mathbb{Z}$ so that

$$vr + ws = 1 \implies vrd + wsd = d \implies v(dr) + w(ds) = d$$
$$vk + wn = d \implies a^d = a^{vk+wn} = a^{vk} * (a^n)^w = a^{vk} * e^w = a^{vk},$$

and we have what we need. □.

Here's an example. Let $G = C_{10}$. What is $\langle a^6\rangle$? Theorem 3 says it is $\langle a^{gcd(6,10)}\rangle = \langle a^2\rangle$. Another way to look at it is to calculate directly and take the powers of a^6 in C_{10}.

$$a^6, (a^6)^2 = a^{12} = a^2, (a^6)^3 = a^{18} = a^8,$$
$$(a^6)^4 = a^{24} = a^4, (a^6)^5 = a^{30} = e.$$

We've reached e, and $\{a^6, a^2, a^8, a^4, e\} = \{a^2, a^4, a^6, a^8, e\}$, as promised. I promised some more examples of $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$. We've already seen it for $n = 5, 8, 10$ and the class worksheet on Monday dealt with $n = 7$. I'll take us up to $n = 12$.

For $n = 2$, $(\mathbb{Z}/2\mathbb{Z})^* = \{[1]_2\}$, so we get the *trivial group* consisting only of the identity.

For any prime p, $(\mathbb{Z}/p\mathbb{Z})^* = \{[1]_p, \ldots, [p-1]_p\}$, and it's a difficult theorem that this group is always isomorphic to C_{p-1}. I'll illustrate this in a few cases by finding a generator $[a]_p$ of order $p-1$ so that the set of its powers comprise $(\mathbb{Z}/p\mathbb{Z})^*$:

$$\langle [a]_p\rangle = \{[a]_p, [a^2]_p, \ldots, [a^{p-1}]_p\} = (\mathbb{Z}/p\mathbb{Z})^*.$$

This was the point of Monday's worksheet with $p = 7$ and the generator $[3]_7 = [5]_7$. For $p = 3$: $(\mathbb{Z}/3\mathbb{Z})^* = \{[1]_3, [2]_3\}$, and multiplication mod 3 is pretty easy: $2^2 = 4 \equiv 1 \mod 3$. This gives a cyclic group of order 2.

We've already done $p = 5$; the powers of 2 generate $(\mathbb{Z}/5\mathbb{Z})^*$: $2, 2^2 = 4, 2^3 = 8 \equiv 3, 2^4 = 16 \equiv 1$. That is, $(\mathbb{Z}/5\mathbb{Z})^* = \langle [2]_5\rangle$.

The next prime is 7, which we've done, and the last one is $p = 11$, and I'll write down the powers of 2 mod 11:

$$2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5,\ 2^5 = 32 \equiv 10,\ 2^6 \equiv 9,$$
$$2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6,\ 2^{10} \equiv 1.$$

And $\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \{1, \ldots, 10\}$, so $[2]_{11}$ is a generator of $(\mathbb{Z}/11\mathbb{Z})^*$.

The remaining undiscussed cases are $n = 4, 6, 9, 12$. The first two are easy. Since $gcd(a, 4) = 1$, $a \neq 2$, so $(\mathbb{Z}/4\mathbb{Z})^* = \{[1]_4, [3]_4\}$, which you should check gives a cyclic group of order 2.

For $n = 6$, $gcd(a, 6) = 1$ means that a is not divisible by 2 or 3, and $(\mathbb{Z}/6\mathbb{Z})^* = \{[1]_6, [5]_6\}$, which is also a cyclic group of order 2.

For $n = 9$, we only rule out multiples of 3, so

$$(\mathbb{Z}/9\mathbb{Z})^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}.$$

The powers of 2 mod 9 are: $\{2, 4, 8, 7, 5, 1\}$, so this is a cyclic group of order 6 with generator $[2]_9$.

The last case, $n = 12$, takes a little more effort. We want those $[a]_{12}$ for which $gcd(a, 12) = 1$. Thus, a is not divisible by 2 or 3, so $(\mathbb{Z}/12\mathbb{Z})^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$. The group is not cyclic, and here is its multiplication table. It's isomorphic to V.

mod 12	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

It turns out to be a theorem in 453 that $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is cyclic if and only if n is 2 or 4 or p^k or $2 \cdot p^k$ for an odd prime p. This is why it was cyclic for $n = 6 = 2 \cdot 3$, $n = 9 = 3^2$ and $n = 10 = 2 \cdot 5$, and why the groups for $n = 8, 12$ were not cyclic. More number theory. What's the order of the group $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$? It's a function of n called the *Euler phi function*, and written as $\phi(n)$. It has another direct interpretation

$$\phi(n) = \{a \mid a \in \{1, \ldots, n-1\} \text{ and } gcd(a, n) = 1\}.$$

What we've seen so far is that $\phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$, $\phi(5) = \phi(8) = \phi(10) = \phi(12) = 4$, $\phi(7) = \phi(9) = 6$, $\phi(11) = 10$.

There is a formula that depends on the *prime factorization* of the integer n. (If you're not familiar with this, I can talk about it in class.) Every integer can be written uniquely as a product of powers of primes:

$$n = \prod_{k=1}^{r} p_k^{a_k} = p_1^{a_1} \cdots p_r^{a_r}, \quad p_1 < \cdots < p_r.$$

It turns out that

$$n = \prod_{k=1}^{r} p_k^{a_k} \implies \phi(n) = \prod_{k=1}^{r} (p_k^{a_k} - p_k^{a_k - 1}) = n \cdot \prod_{k=1}^{r} \frac{p_k - 1}{p_k}.$$

For example,

$$12 = 2^2 \cdot 3^1$$

$$\implies \phi(12) = (2^2 - 2^1)(3^1 - 3^0) = (4 - 2)(3 - 1) = 2 \cdot 2 = 4$$

$$\text{or} \quad \phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{24}{6} = 4.$$

and $14 = 2 \cdot 7 \implies \phi(14) = (2 - 1) \cdot (7 - 1) = 6$.

You can use this formula even before we prove it.

Another thing we can do with prime factorization is look at gcd. I will use the notation $\mathcal{P} = \{2, 3, 5, 7, \dots\}$ to denote the set of all primes, so, as strange as it looks, every $n \in \mathbb{N}$ can be written as

$$n = \prod_{p \in \mathcal{P}} p^{a_p}, \quad a_p \geq 0.$$

For example, $12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \dots$ and

$$417 = 2^0 \cdot 3^1 \cdot 5^0 \cdot \dots \cdot 137^0 \cdot 139^1 \cdot 149^0 \dots .$$

Notice that

$$n = \prod_{p \in \mathcal{P}} p^{a_p}, \quad m = \prod_{p \in \mathcal{P}} p^{b_p} \implies n \cdot m = \prod_{p \in \mathcal{P}} p^{a_p + b_p}.$$

LEMMA Suppose $d, n \in \mathbb{N}$ and

$$d = \prod_{p \in \mathcal{P}} p^{c_p}, \quad n = \prod_{p \in \mathcal{P}} p^{a_p}.$$

Then $d \mid n$ if and only if $c_p \leq a_p$ for all $p \in \mathcal{P}$.

PROOF: First suppose $d \mid n$, so that $de = n$ for some $e \in \mathbb{N}$. Now write (as we can)

$$e = \prod_{p \in \mathcal{P}} p^{b_p}, \quad b_p \geq 0 \implies de = \prod_{p \in \mathcal{P}} p^{b_p + c_p},$$

Since $n = de$ and prime factorization is unique, we have that for all $p \in \mathcal{P}$, $a_p = b_p + c_p$, and since $b_p \geq 0$, we have $c_p \leq a_p$.

But if $c_p \leq a_p$, we can define $b_p = a_p - c_p \geq 0$ and define e as above, and then $de = n$, so $d \mid n$. □

THEOREM 4: We can compute the gcd using prime factorizations.

$$m = \prod_{p \in \mathcal{P}} p^{a_p}, \quad n = \prod_{p \in \mathcal{P}} p^{b_p} \implies gcd(m, n) = \prod_{p \in \mathcal{P}} p^{\min(a_p, b_p)}.$$

PROOF. From the lemma, if

$$g = \prod_{p \in \mathcal{P}} p^{v_p},$$

then g is a common divisor of m and n if and only if $v_p \leq a_p$ and $v_p \leq b_p$, which both hold if and only if $v_p \leq \min(a_p, b_p)$.

The maximum occurs when v_p is as large as possible under the circumstances; that is, when $v_p = \min(a_p, b_p)$. □

For example, $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \dots$ and $72 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^0 \dots$, so

$$gcd(30, 72) = 2^{\min(1,3)} \cdot 3^{\min(1,2)} \cdot 5^{\min(1,0)} \cdot 7^{\min(0,0)} \dots$$
$$= 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdots = 2 \cdot 3 = 6.$$

The disadvantage of this method is that it doesn't tell you how to write $\gcd(m, n)$ as a combination of m and n, as the Euclidean algorithm does.

One more bonus that we won't be using: the same reasoning implies that

$$m = \prod_{p \in \mathcal{P}} p^{a_p}, n = \prod_{p \in \mathcal{P}} p^{b_p} \implies lcm(m, n) = \prod_{p \in \mathcal{P}} p^{\max(a_p, b_p)}.$$

Finally, I'll start talking on the Chinese Remainder Theorem. This is a small subset of the discussion of CRT in Math 453.

LEMMA: If $d \mid n$, $d, n \in \mathbb{N}$ and $x, y \in \mathbb{Z}$ and $x \equiv y \mod n$, then $x \equiv y \mod d$.

PROOF: Since $d \mid n$, $n = de$ for some $e \in n$. Since $x \equiv y \mod n$, $y - x = nt$ for some $t \in \mathbb{Z}$. Thus, $y - x = (de)t = (et)d$, and so $y \equiv x \mod d$.

THEOREM 5: Suppose $gcd(m, n) = 1$. Then $x \equiv y \mod m$ and $x \equiv y \mod n$ if and only if $x \equiv y \mod mn$.

PROOF: One direction is easy from the lemma: since $m \mid mn$ and $n \mid mn$, if $x \equiv y \mod mn$, then $x \equiv y \mod m$ and $x \equiv y \mod n$.

For the converse, suppose $x \equiv y \mod m$ and $x \equiv y \mod n$. Then from the first equation, there exists t so that $y - x = mt$ and the second equation implies that $n \mid y - x = mt$.

But $gcd(m, n) = 1$ so $n \mid mt$ implies $n \mid t$ by an old lemma, and so $t = nu$ for some $u \in \mathbb{N}$. Thus $y - x = mt = m(nu) = u(mn)$, so $mn \mid y - x$ and $x \equiv y \mod mn$. □ That is how the Chinese Remainder Theorem is usually presented.

CRT: If $gcd(m, n) = 1$, then for any $a, b \in \mathbb{Z}$, there exists c so that

$$x \equiv a \mod m \quad \text{and} \quad x \equiv b \mod n \iff x \equiv c \mod mn.$$

Before I give the proof, which I'll save for another day, I want to show you one example:

Take $m = 3$ and $n = 5$ and look at all combinations of $x \mod 3$ with $x \mod 5$:

	0 mod 5	1 mod 5	2 mod 5	3 mod 5	4 mod 5
$[0]_3$	0 mod 15	6 mod 15	12 mod 15	3 mod 15	9 mod 15
$[1]_3$	10 mod 15	1 mod 15	7 mod 15	13 mod 15	4 mod 15
$[2]_3$	5 mod 15	11 mod 15	2 mod 15	8 mod 15	14 mod 15

I've written "$[a]_3$" instead of "$a \mod 3$," so the table would fit on the screen. What I mean here is that, for example, $13 \mod 15$ is at the intersection of $[1]_3$ and $3 \mod 5$. Why?

If $x \equiv 13 \mod 15$, then $x \equiv 13 \mod 3$ so $x \equiv 1 \mod 3$; If $x \equiv 13 \mod 15$, then $x \equiv 13 \mod 5$ so $x \equiv 3 \mod 5$.

The wonderful fact of the Chinese Remainder Theorem is that the grid is perfectly populated. Each choice gives exactly one outcome.

This may not be true if $gcd(m, n) > 1$. For example, there is no x so that $x \equiv 0 \mod 4$ and $x \equiv 1 \mod 6$, because the first equation says that x is even and the second says that x is odd. On the other hand, $x \equiv 0 \mod 4$ and $x \equiv 2 \mod 6$ can be shown to be equivalent to $x \equiv 8 \mod 24$ and $x \equiv 20 \mod 24$.

But this is a question best studied in Math 453 not Math 417.

September 2, 2020, in class

First, a correction to HW1. Please ignore problem 1c. There is no proper subgroup!

Second, don't worry yet about the Chinese Remainder Theorem. I'll have a lot more to say about that, and about the formula for the Euler phi function $\phi(n)$ on Friday.

I'd like to try to tie things together with some examples of cyclic groups of order six. We know three examples.

The first one is the additive group of integers mod 6, $(\mathbb{Z}/6\mathbb{Z}, \oplus)$: $\{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$, where e.g., $[2]_6 + [5]_6 = [7]_6 = [1]_6$.

The second one is abstract: $C_6 = \{e, a, a^2, a^3, a^4, a^5\}$, where $a^6 = e$ and e.g. $a^2 * a^5 = a^7 = a$.

The third one is $(\mathbb{Z}/7\mathbb{Z}, \odot)$, which you found was $\langle [3]_7 \rangle$; that is, $\{[1]_7, [3]_7, [3^2]_7 = [2]_7, [3^3]_7 = [6]_7, [3^4]_7 = [4]_7, [3^5]_7 = [5]_7\}$ and, e.g. $[5]_7 * [2]_7 = [3]_7$, or $[3^5]_7 * [3^2]_7 = [3^7]_7 = [3]_7$. Here are the connections among these groups.

$$(\mathbb{Z}/6\mathbb{Z}, \oplus) \iff C_6 \iff ((\mathbb{Z}/7\mathbb{Z})^*, \odot)$$

$$\begin{aligned}
[0]_6 &\iff e \iff [1]_7 \\
[1]_6 &\iff a \iff [3]_7 \\
[2]_6 &\iff a^2 \iff [2]_7 \\
[3]_6 &\iff a^3 \iff [6]_7 \\
[4]_6 &\iff a^4 \iff [4]_7 \\
[5]_6 &\iff a^5 \iff [5]_7
\end{aligned}$$

So, for example, if $\phi_1([0]_6) = e, \phi_1([1]_6) = a$, etc, then ϕ_1 gives an isomorphism from $(\mathbb{Z}/6\mathbb{Z}, \oplus)$ to C_6. There are six such isomorphisms, one from any column to any other. Just think of the similarity in the multiplication tables.

It is not hard to show that if $\phi : G \mapsto H$ is an isomorphism, then ϕ maps subgroups of G to subgroups of H.

Since C_6 is a cyclic group, its subgroups are $\langle a^k \rangle$ where $k \mid 6$. This means $k \in \{1, 2, 3, 6\}$. If $k = 1$, you get C_6, if $k = 6$ you get $\{e\}$. There are two other cases, and here they are

$$\begin{aligned} \{[0]_6, [2]_6, [4]_6\} &\iff \{e, a^2, a^4\} = \langle a^2 \rangle \iff \{[1]_7, [2]_7, [4]_7\} \\ \{[0]_6, [3]_6\} &\iff \{e, a^3\} = \langle a^3 \rangle \iff \{[1]_7, [6]_7\} \end{aligned}$$

The first two columns should be clear. For the third, remember that $a \iff [3]_7$, and so $a^2 \iff [3^2]_7 = [9]_7 = [2]_7$, $a^3 \iff [3^3]_7 = [27]_7 = [6]_7$, and $a^6 = (a^2)^3 \iff [2^3]_7 = [8]_7 = [1]_7$. Here's another picture which will illustrate both the Chinese Remainder Theorem and the Euler ϕ function. This is a table of $[a]_{20}$ versus $[a]_5$ and $[a]_4$. (Note that $gcd(4, 5) = 1, 20 = 4 \cdot 5$.)

	0 mod 4	1 mod 4	2 mod 4	3 mod 4
0 mod 5	0 mod 20	5 mod 20	10 mod 20	15 mod 20
1 mod 5	16 mod 20	1 mod 20	6 mod 20	11 mod 20
2 mod 5	12 mod 20	17 mod 20	2 mod 20	7 mod 20
3 mod 5	8 mod 20	13 mod 20	18 mod 20	3 mod 20
4 mod 5	4 mod 20	9 mod 20	14 mod 20	19 mod 20

For example, $x \equiv 3 \mod 5$ and $x \equiv 1 \mod 4$ if and only if $x \equiv 13 \mod 20$.

We'll talk later about how to do this systematically. We know from the CRT that $x \equiv 3 \mod 5$ and $x \equiv 1 \mod 4$ if and only if $x \equiv c \mod 20$ for some c. The integers $x \equiv 3 \mod 5$ are 3, 8, 13, 18, etc., and if you look at them mod 4, you get 3,0,1,2, etc, so you can pick out 13 experimentally.

I have indicated the elements of $(\mathbb{Z}/20\mathbb{Z})^*$ in red (on the slides, not the pdf. They are in the columns corresponding to 1mod4 and 3 mod 4 and all rows except 0 mod 5I hope you can see how this interacts with the rows and columns. Theorems will follow.

	0 mod 4	1 mod 4	2 mod 4	3 mod 4
0 mod 5	0 mod 20	5 mod 20	10 mod 20	15 mod 20
1 mod 5	16 mod 20	1 mod 20	6 mod 20	11 mod 20
2 mod 5	12 mod 20	17 mod 20	2 mod 20	7 mod 20
3 mod 5	8 mod 20	13 mod 20	18 mod 20	3 mod 20
4 mod 5	4 mod 20	9 mod 20	14 mod 20	19 mod 20

Notice that 9 is not prime, but it is *relatively* prime to 20.

Today's worksheet questions:

1. Write down the proper subgroups of $C_{12} = \langle a \rangle$, with $a^{12} = e$ in terms of their elements.

2. Consider the powers of $[2]_{13}$ mod 13. Remember that you can reduce. If you know that $2^5 = 32 \equiv 6 \mod 13$, then it is ok, and even recommended to write $2^6 = 2 * 2^5 \equiv 2 \cdot 6 \mod 13$. This will keep the arithmetic from getting out of hand.

The group $((\mathbb{Z}/13\mathbb{Z})^*, \odot)$ is then a cyclic group of order 12. Find a subgroup of order 3. 1. The divisors of 12 are $D(12) = \{1, 2, 3, 4, 6, 12\}$, so the proper subgroups are

$$\langle a^2 \rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\}$$
$$\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$$
$$\langle a^4 \rangle = \{e, a^4, a^8\}$$
$$\langle a^6 \rangle = \{e, a^6\}$$

2. The powers of $[2]_{13}$ in order are: 2,4,8,3,6,12,11,9,5,10,7,1 mod 13

This is a cyclic group of order 12 with generator $[2]_{13}$, which corresponds to a. By your answer to 1., the cyclic subgroup of order 3 should be the one which corresponds to $\langle a^4 \rangle$. Since $2^4 = 16 \equiv 3 \mod 13$, the subgroup should be

$$\langle [3]_{13} \rangle = \{[1]_{13}, [3]_{13}, [3^2]_{13}\}$$

And, $3^2 = 9$, $3^3 = 27 \equiv 1 \mod 13$, so it checks out.

September 4, 2020, in advance

Today seems like a good time to sum up what we know about groups so far.

Given a set G and a binary operation $*$, defined so that $x, y \in G \implies x * y \in G$, we say that $(G, *)$ is a group if: (i) There is an identity element $e \in G$ so that $x * e = e * x = x$ for every $x \in G$ (ii) for every

$x \in G$ there exists $y \in G$ so that $x * y = e$ and (iii) The operation is associative (for all $x, y, z \in G$, $(x * y) * z = x * (y * z)$).

If G is a finite set, $(G, *)$ is called a finite group, and $|G|$ is called the order of the group. If the operation is obvious, or the instructor is lazy, we refer to G, rather than $(G, *)$ and will sometimes write xy for $x * y$, even though the operation might not correspond to multiplication.

An important property is cancellation: if $a, b, c \in G$ and $a * b = a * c$, then $b = c$ and if $a * b = c * b$ then $a = c$. Side remark: If $x * y = e$, then $y * (x * y) = y * e \implies (y * x) * y = e * y \implies y * x = e$, so we only need one direction in (ii).

I should also have mentioned this fact:

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

That is, if you take the inverse of a product, you reverse the order of the factors. (This may be familiar to you from matrices). The proof uses the associative law:

$$(x * y) * (y^{-1} * x^{-1}) = ((x * y) * (y^{-1})) * x^{-1} =$$
$$(x * (y * (y^{-1})) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e.$$

So, $y^{-1} * x^{-1}$ is an element which, when $*$'d with $x * y$, gives you the identity, so it's the inverse.

It is often more information than we need, but we can completely understand a finite group from its multiplication table.

$*$	g_1	g_2	$\dots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\dots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\dots$	$g_2 * g_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_n	$g_n * g_1$	$g_n * g_2$	$\dots$	$g_n * g_n$

A group is *abelian* if for $x, y \in G$, $x * y = y * x$. The groups we've seen (so far) are all abelian, but don't get too comfortable about this.

A subset H of G is a subgroup of G if $(H, *)$ is a group. (We use the same operation.) The conditions of being a subgroup are that $h_1, h_2 \in H \implies h_1 * h_2 \in H$, $e \in H$, and $h \in H \implies h^{-1} \in H$.

Two groups $(G, *_G)$ and $(H, *_H)$ are isomorphic if there is a function Φ so that Φ is a bijection from G to H (as sets) and Φ preserves the operation. That is, for $g_1, g_2 \in G$, $\Phi(g_1 *_G g_2) = \Phi(g_1) *_H \Phi(g_2)$. From the point of view of multiplication tables, two groups are isomorphic if there is a function Φ which relabels the elements so that the tables of the same.

I didn't mention it explicitly, but there is a useful lemma about isomorphisms.

LEMMA (i) If $\Phi : G \mapsto H$ is an isomorphism, and e_G is the identity in G, then $\Phi(e_G) = e_H$, the identity in H;

(ii) $\Phi(g^{-1})$ is the inverse of $\Phi(g)$ in H.

PROOF (i) For $g \in G$, we have $g = e_G *_G g$, so since e_H is the identity in H,

$$e_H *_H \Phi(g) = \Phi(g) = \Phi(e_G *_G g) = (\Phi(e_G)) *_H \Phi(g)$$

so by right cancellation, $e_H = \Phi(e_G)$.

For (ii), $g *_G g^{-1} = e_G \implies \Phi(g) *_H \Phi(g^{-1}) = \Phi(e_G) = e_H$, so $\Phi(g^{-1})$ is the inverse of $\Phi(g)$ in H.

To illustrate this, let me prove a theorem I've already announced.

THEOREM 1: Suppose the group $(G, *_G)$ is isomorphic to the group $(H, *_H)$ and suppose G_1 is a subgroup of G. Then

$$H_1 = \Phi(G_1) := \{\Phi(g) : g \in G_1\}$$

is a subgroup of H.

PROOF: If $x \in H_1$, then there is $u \in G_1$ so that $x = \Phi(u)$. All we have to do is prove the conditions for a subgroup. First closure. Suppose $x, y \in H_1$. We need to prove that $x *_H y \in H_1$. But $x, y \in H_1$ means that there exist $u, v \in G_1$ so that $x = \Phi(u)$ and $y = \Phi(v)$. Because Φ is an isomorphism,

$$\Phi(u *_G v) = \Phi(u) *_H \Phi(v) = x *_H y.$$

Since G_1 is a subgroup, $u *_G v \in G_1$, so this means that $x *_H y$ is the image of an element of G_1 under Φ, which means that $x *_H y \in H_1$.

The other two are easier. Since G_1 is a subgroup, $e_G \in G_1$ and so $\Phi(e_G) \in H_1$. By the lemma, this means $e_H \in H_1$: it has the identity. If $x \in H_1$, then $x = \Phi(u)$ for $u \in G_1$ and then $u^{-1} \in G_1$, because G_1 is a subgroup and by the lemma, $\Phi(u^{-1}) \in H_1$ is the inverse of $x = \Phi(u)$. □

If $x \in G$ and G is a finite group, we found that there exists m so that $\{e, x, \ldots, x^{m-1}\}$ are different and $x^m = e$. This set of powers is called $\langle x \rangle$, and is always a subgroup of G. The integer m is called the order of x in G.

We know several different kinds of groups. The simplest is the "abstract" cyclic group $C_n = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$, with $a^n = e$. The subgroups of C_n are given by $\langle a^k \rangle$, where $k \mid n$ and for any r, $\langle a^r \rangle = \langle a^{gcd(r,n)} \rangle$.

I should mention explicitly the fact that messed up HW Problem 1c. Suppose p is prime.

The subgroups of C_p are given by $\langle a^k \rangle$, where $k \mid p$, but the only such k are $k = 1, p$, and $\langle a \rangle = C_p$ and $\langle a^p \rangle = \langle e \rangle = \{e\}$ (the trivial group), so C_p has no proper subgroups.

We also studied

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\},$$

where $[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}$. Under addition mod n, $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is a cyclic group of order n. With the definition

$$(\mathbb{Z}/n\mathbb{Z})^* := \{[a]_n \mid gcd(a, n) = 1\}$$

we proved in general and gave many examples in the specific to show that $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is an abelian group of order $\phi(n)$, where ϕ is the currently-mysterious Euler phi-function.

To answer an email question, why do we assume $gcd(a, n) = 1$? Well, we want a group, so we want inverses, and so we want there to exist b so that $[a]_n[b]_n = [1]_n$. This means that $ab \equiv 1 \mod n$, and we saw earlier that this implies $gcd(a, n) = 1$.

We've also looked at rotation groups (we'll be doing a lot of that soon) and the peculiar group V. Here's more about V. Let

$$G = \{([0]_2, [0]_2), ([0]_2, [1]_2), ([1]_2, [0]_2), ([1]_2, [1]_2)\}$$

be the set of all ordered pairs of $[a]_2$'s. Define $*$ on G by

$$([a]_2, [b]_2) * ([c]_2, [d]_2) = ([a + c]_2, [b + d]_2).$$

This is component-wise addition. Here is the table, where I will write ab for $([a]_2, [b]_2)$:

$*$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

This is isomorphic to V (of course!), but it also can be called $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We can also look at $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and even, given groups G and H, the *Cartesian product* of G and H, written $G \times H$.

In fact, one of the worksheet problems on Friday will be to look at $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; that is, the set of all pairs $([a]_2, [b]_3)$, with the operation

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

Thus, for example

$$([1]_2, [1]_3) * ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3),$$

because $2 \equiv 0 \mod 2$ and $2 \equiv 2 \mod 3$.

In the worksheet, you will prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 6.

I also want to talk about the Chinese Remainder Theorem (CRT) and give you two stylistically different proofs.

CRT If $gcd(m,n) = 1$ then for every a, b, there exists c so that

$$x \equiv a \mod m \quad \text{and} \quad x \equiv b \mod n \iff x \equiv c \mod mn$$

It's important to remember our earlier result that if $gcd(m,n) = 1$, then $x \equiv y \mod m$ and $x \equiv y \mod n$ iff $x \equiv y \mod mn$.

FIRST PROOF of the CRT: This is a longish, abstract, Math 347 style proof. Assume $gcd(m,n) = 1$. Consider the three sets $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$: these have m, n and mn elements respectively. Define

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \{([a]_m, [b]_n) : [a]_m \in \mathbb{Z}/m\mathbb{Z}, \quad [b]_n \in \mathbb{Z}/n\mathbb{Z}\}$$

This is the Cartesian product of the two sets, and it has $|\mathbb{Z}/m\mathbb{Z}||\mathbb{Z}/n\mathbb{Z}| = mn$ elements. I will now define a function $F : \mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$,

$$F([k]_{mn}) = ([k]_m, [k]_n).$$

Here is an example of the function when $m = 2$ and $n = 3$.

$$F([0]_6) = ([0]_2, [0]_3), \quad F([1]_6) = ([1]_2, [1]_3), \quad F([2]_6) = ([0]_2, [2]_3),$$
$$F([3]_6) = ([1]_2, [0]_3), \quad F([4]_6) = ([0]_2, [1]_3), \quad F([5]_6) = ([1]_2, [2]_3),$$

You can see in this case that F is a bijection: it is injective (or one-to-one) and surjective (or onto). This is true in general.

In every case, F is a function from one finite set to another finite set, and the sets have the same number of elements, mn.

I want to show that F is injective. Suppose $F([k]_{mn}) = F([j]_{mn})$. Then

$$([k]_m, [k]_n) = ([j]_m, [j]_n) \iff [k]_m = [j]_m \quad \text{and} \quad [k]_n = [j]_n.$$

So $k \equiv j \mod m$ and $k \equiv j \mod n$, and the earlier result shows that this is equivalent to $[k]_{mn} = [j]_{mn}$. Thus F is one-to-one. Since the sets have the same cardinality, F is onto. That is, for every $([a]_m, [b]_n)$, there is a $[k]_{mn}$ so that $F([k]_{mn}) = ([a]_m, [b]_n)$; that is,

$$x \equiv a \mod m \quad \text{and} \quad x \equiv b \mod n \iff x \equiv k \mod mn \quad \square$$

SECOND PROOF of the CRT: Maybe you didn't like that proof! Here's another one. Since $gcd(m,n) = 1$, there exist $r, s \in \mathbb{Z}$ so that $rm + ns = 1$. I won't spend time to tell you how we found this, so it's a "magic formula". But, given, a, b, define

$$k = ans + brm$$

I'll show that $k \equiv a \mod m$ and $k \equiv b \mod n$. Using the formula $rm + ns = 1$ twice, we have

$$k = ans + brm = a(1 - rm) + brm = a + m(-ar + br)$$
$$k = ans + brm = ans + b(1 - ns) = b + n(as - bs). \quad \square$$

If this were Math 453, I'd have an example of this on the worksheet. I can still do that if you want.

Finally, I want to tell you how to compute $\phi(n)$.

LEMMA: If p is prime, then $\phi(p^k) = p^k - p^{k-1}$.

PROOF: We want to count the number of integers in $\{1, \ldots, p^k - 1\}$ which are relatively prime to p^k. But since p is prime, $gcd(a, p^k) = 1$ if and only if $gcd(a, p) = 1$; that is $p \not| a$. So, there are $p^k - 1$ possible values of a (*), and we rule out $\{1 \cdot p, 2 \cdot p, \ldots, (p^{k-1} - 1)p\}$ multiples of p, leaving $(p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1}$.

(*) We want to count multiples of p between 1 and $p^k - 1$. Let tp be one such multiple, then

$$1 \leq tp \leq p^k - 1 \iff \frac{1}{p} \leq t \leq p^{k-1} - \frac{1}{p} \iff 1 \leq t \leq p^{k-1} - 1,$$

where the last implication comes because t is an integer. $\square$

LEMMA: If $gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$.

PROOF: We consider the integers in $k \in \{0, \ldots, mn-1\}$, and as before, look at $(k \mod m, k \mod n)$. If you change the letters around, we've shown already that $gcd(k, m) = 1$ and $gcd(k, n) = 1$ imply $gcd(k, mn) = 1$. On the other hand, suppose $gcd(k, mn) = d > 1$. Then $d \mid k$ and $d \mid m$, which means that $d \mid mn$, so $gcd(k, m) \geq d > 1$. The same thing holds if $gcd(k, n) = d > 1$. So NOT($gcd(k, m) = 1$ and $gcd(k, n) = 1$) implies NOT($gcd(k, mn) = 1$), and taking the contrapositive gives the other direction. $\square$

So we count those k, and its enough to assume that $gcd(k, m) = 1$ and $gcd(k, n) = 1$, There are $\phi(m)$ choices for the first and $\phi(n)$ choices for the second, and since F is a bijection, this tells us that there $\phi(m)\phi(n)$ cases altogether, and so the number of k, which is $\phi(mn)$ is also $\phi(m)\phi(n)$. I gave a picture for that earlier when $m = 3$ and $n = 5$ where the relatively prime elements were in red.

THEOREM: We have the following formula.

$$n = \prod_{k=1}^{r} p_k^{a_k} \implies \phi(n) = \prod_{k=1}^{r} (p_k^{a_k} - p_k^{a_k - 1}).$$

SKETCH OF PROOF: The proof is by induction on r, the number of prime factors. If $r = 1$, this is the lemma. Suppose $r = 2$, then

$n = p_1^{a_1} \cdot p_2^{a_2}$. Since $p_1 < p_2$, $gcd(p_1^{a_1}, p_2^{a_2}) = 1$, and we can apply the other lemma. □

For example,

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \implies$$
$$\phi(5040) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0)$$
$$= (16 - 8) \cdot (9 - 3) \cdot (5 - 1) \cdot (7 - 1) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152.$$

This means that about 80% of the integers less than 5040 are *not* relatively prime to 5040.

September 4, 2020, in class

I've gotten some requests to talk about isomorphisms, and first, an apology. The letter commonly used for the function is Φ, and some were trying to connect it to the Euler phi function uses the lower-case version ϕ. There is *no* connection between the two. I'm sorry if this was confusing!

I've also gotten a request to talk about isomorphisms and the theorem in the lecture, so let me first review. Let's start with a familiar picture:

C_4	e	a	a^2	a^3
e	e	a	a^2	a^3
e	e	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

$(\mathbb{Z}/4\mathbb{Z}, \oplus)$	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 isomorphism implicit from these tables is given by

$$\Phi(e) = [0]_4,\ \Phi(a) = [1]_4,\ \Phi(a^2) = [2]_4,\ \Phi(a^3) = [3]_4.$$

In this case, we can put the isomorphism in words: $\Phi(a^k) = [k]_4$. This is not always possible.

Since the divisors of 4 are 1, 2, 4, the group $C_4 = \langle a \rangle$ has three subgroups: $\langle a \rangle$, $\langle a^2 \rangle$ and $\langle a^4 \rangle$. Of these, $\langle a \rangle = C_4$ and $\langle a^4 \rangle = \langle e \rangle = \{e\}$. The other one is $\langle a^2 \rangle = \{e, a^2\}$.

What happens when we apply Φ to these sets? First, Φ is a bijection, so $\Phi(C_4) = \mathbb{Z}/4\mathbb{Z}$. Second, Φ maps the identity to the identity, so $\Phi(\{e\}) = [0]_4$. The interesting case is

$$\Phi(\{e, a^2\}) = \{\Phi(e), \Phi(a^2)\} = \{[0]_4, [2]_4\}.$$

Both sides give a cyclic group of order 2, because $(a^2)^2 = e$ and $[2]_4 + [2]_4 = [0]_4$.

Here are the multiplication tables of the subgroups.

	e	a^2
e	e	a^2
a^2	a^2	e

	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[2]_4$
$[2]_4$	$[2]_4$	$[0]_4$

Let's use a different cyclic group of order 4:$((\mathbb{Z}/5\mathbb{Z})^*, \odot)$. Recall that $(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$.

What we found earlier was that $[1]_5$ is the identity, $[2]_5$ is a generator, and $[2]_5^2 = [2^2]_5 = [4]_5$ and $[2]_5^3 = [2^3]_5 = [8]_5 = [3]_5$ and $[2]_5^4 = [2^4]_5 = [16]_5 = [1]_5$.

The multiplication tables, written to emphasize that $((\mathbb{Z}/5\mathbb{Z}^*, \odot)$ is cyclic.

C_4	e	a	a^2	a^3
e	e	a	a^2	a^3
e	e	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

,

$((\mathbb{Z}/5\mathbb{Z})^*, \odot)$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Again, if we define Φ_1 by

$$\Phi_1(e) = [1]_5,\ \Phi_1(a) = [2]_5,\ \Phi_1(a^2) = [4]_5,\ \Phi_1(a^3) = [3]_5,$$

we see that it is an isomorphism, and the proper subgroup of $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$ is $\{\Phi_1(e), \Phi_1(a^2)\} = \{[1]_5, [4]_5\}$.

I'll finish with a request to go over the isomorphism proofs from last night. I will not repeat them in the "Weekly Summary". [Note: I didn't repeat the text here because it's the same thing.

WORKSHEET PROBLEMS

1. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$, and define the operation $*$ by

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

Thus, for example

$$([1]_2, [1]_3) * ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3),$$

because $2 \equiv 0 \mod 2$ and $2 \equiv 2 \mod 3$.

Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 6 by working out $\langle([1]_2, [1]_3)\rangle$.

2. Same situation. Consider $C_6 = \langle a\rangle, a^6 = e$. There is an isomorphism Φ which takes C_6 to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and for which $\Phi(a) = ([1]_2, [1]_3)$. Write out the other values of $\Phi(a^k)$, and $\Phi(\langle a^2\rangle)$ and $\Phi(\langle a^3\rangle)$. These are subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ that will be "obviously" subgroups.

WORKSHEET SOLUTIONS

From the definition of the group

$$([1]_2,[1]_3)^1 = ([1]_2,[1]_3)$$
$$([1]_2,[1]_3)^2 = ([1]_2,[1]_3) * ([1]_2,[1]_3) = ([0]_2,[2]_3)$$
$$([1]_2,[1]_3)^3 = ([1]_2,[1]_3) * ([1]_2,[1]_3)^2 = ([1]_2,[0]_3)$$
$$([1]_2,[1]_3)^4 = ([1]_2,[1]_3) * ([1]_2,[1]_3)^3 = ([0]_2,[1]_3)$$
$$([1]_2,[1]_3)^5 = ([1]_2,[1]_3) * ([1]_2,[1]_3)^4 = ([1]_2,[2]_3)$$
$$([1]_2,[1]_3)^6 = ([1]_2,[1]_3) * ([1]_2,[1]_3)^5 = ([0]_2,[0]_3)$$

So the first five powers are different and the sixth gives the identity and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 6.

2. If $\Phi(a) = ([1]_2,[1]_3)$, then because Φ is an isomorphism. $\Phi(a^k) = ([1]_2,[1]_3)^k$, so $\Phi(a^2) = ([0]_2,[2]_3)$, $\Phi(a^3) = ([1]_2,[0]_3)$, $\Phi(a^4) = ([0]_2,[2]_3)$, $\Phi(a^5) = ([1]_2,[2]_3)$ and $\Phi(e) = \Phi(a^6) = ([0]_2,[0]_3) = e_G$. Actually, $\Phi(a^k) = ([k]_2,[k]_3)$.

The images of $\Phi(\langle a^2\rangle) = \Phi(\{e,a^2,a^4\})$ and $\Phi(\langle a^3\rangle) = \Phi(\{e,a^3\}$ are then

$$\{([0]_2,[0]_3),([0]_2,[1]_3),([0]_2,[2]_3)\}$$

and

$$\{([0]_2,[0]_3),([1]_2,[0]_3)\}$$