Math 417 – Third Day

Bruce Reznick
University of Illinois at Urbana-Champaign

August 28, 2020

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 $x \in G$, $x * e = e * x = x$.

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 $x * y = y * x = e$.

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 $x, y, z \in G$, $(x * y) * z = x * (y * z)$.

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 $i, j \in \{0, \ldots, n-1\}$

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 $i, j \in \{0, \ldots, n-1\}$

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

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 $i, j \in \{0, \ldots, n-1\}$

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

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

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 $k \equiv i + j \mod n$.

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 $\frac{2\pi}{n}$.

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 $n = 4$:

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 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 $x, y \in G_1$,

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

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 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 ,

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

$*$	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.

$*$	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.

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?

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

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.

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,

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

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 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.

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.

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.

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.

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

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.

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.

Back to number theory.

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

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

Back to number theory.

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

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

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.

Back to number theory.

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

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

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 $a \mid c$.

Back to number theory.

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

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

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 $a \mid mb + nc$.

Back to number theory.

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

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

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 $tu \in \mathbb{Z}$.

Back to number theory.

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

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

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 $n \in \mathbb{N}$, 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 $gcd(12, 417) = 3$.

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.

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 $gcd(m, n) = gcd(m, n - km)$.

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.

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 $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

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:

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:

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

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

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

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

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

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:

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

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

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

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

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

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?

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.

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.

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 $\{e, g, g^2, \ldots, g^9\}$, $g^{10} = e$.

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.

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:

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

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.

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.

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 $g^{gcd(i,n)}$.

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 $gcd(4, 10) = 2$.

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 $gcd(4, 10) = 2$.

And remember your job!

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 $gcd(4, 10) = 2$.

And remember your job!

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