Math 417 – Sixth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 4, 2020

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

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

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).

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:

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:

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

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:

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:

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

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.

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

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

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

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

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.

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

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

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.

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.

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.

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;

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,

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

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

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, $e_H = \Phi(e_G)$.

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.

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.

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 $x = \Phi(u)$.

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,

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,

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

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 $x *_H y \in H_1$.

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.

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, $\langle a^r \rangle = \langle a^{gcd(r,n)} \rangle$.

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

We also studied

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

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

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 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.

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 $gcd(a, n) = 1$?

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

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

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

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

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 $([a]_2, [b]_2)$:

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

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 $G \times H$.

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

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

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

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

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

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 $2 \equiv 2 \mod 3$.

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.

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

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

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 $x \equiv y \mod mn$.

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

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

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

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 $F : \mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

I will now define a function $F : \mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

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

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 $n = 3$.

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

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.

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

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

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

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.

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,

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,

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

SECOND PROOF of the CRT: Maybe you didn't like that proof!

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

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

$$k = ans + brm$$

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

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

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

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 $\phi(n)$.

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

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

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.

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 $(p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1}$.

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

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

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

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. □

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

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 $gcd(k, mn) = 1$.

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 $gcd(k, m) = d > 1$. Then $d \mid k$ and $d \mid m$, which means that $d \mid mn$, so $gcd(k, mn) \geq d > 1$. 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.

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 $gcd(k, m) = d > 1$. Then $d \mid k$ and $d \mid m$, which means that $d \mid mn$, so $gcd(k, mn) \geq d > 1$. 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.

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 $\phi(m)\phi(n)$. □

THEOREM: We have the following formula.

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

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. $\square$

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,

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,

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \implies$$

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,

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \implies$$
$$\phi(5040) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0)$$

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,

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \implies$$

$$\phi(5040) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0)$$

$$= (16 - 8) \cdot (9 - 3) \cdot (5 - 1) \cdot (7 - 1)$$

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,

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 \implies$$

$$\phi(5040) = (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0)$$

$$= (16 - 8) \cdot (9 - 3) \cdot (5 - 1) \cdot (7 - 1) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152.$$

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.