Math 417 – Fifth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 2, 2020

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.

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.

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.

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 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,

Thus we have in G,

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

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 $x^i \in \langle x \rangle$,

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

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. □

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.

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 $k \mid n$.

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

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

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

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:

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. □

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?

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 $\langle a^k \rangle = \langle a^d \rangle$.

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,

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,

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

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

Remember that $k = dr$ and $n = ds$. Since $gcd(r, s) = 1$, there exist $v, w \in \mathbb{Z}$ so that

$$vr + ws = 1 \implies vrd + wsd = d \implies v(dr) + w(ds) = d$$

$$vk + wn = d \implies a^d = a^{vk+wn} = a^{vk} * (a^n)^w = a^{vk} * e^w = a^{vk},$$

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. $\square$.

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}.

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}.

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

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 $n = 12$.

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.

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 $(\mathbb{Z}/p\mathbb{Z})^*$:

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 $(\mathbb{Z}/p\mathbb{Z})^*$:

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

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.

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:

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:

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

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 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.

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.

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 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.

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

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

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

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

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 $\phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$, $\phi(5) = \phi(8) = \phi(10) = \phi(12) = 4$, $\phi(7) = \phi(9) = 6$, $\phi(11) = 10$.

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:

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

It turns out that

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

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,

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $p \in \mathcal{P}$.

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)

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)

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

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 $c_p \leq a_p$.

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.

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

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

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

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

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 $v_p \leq \min(a_p, b_p)$.

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 $v_p = \min(a_p, b_p)$. □

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

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

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.

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

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.

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 $x \equiv y \mod d$.

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 $y \equiv x \mod d$.

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 $x \equiv y \mod mn$.

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 $x \equiv y \mod n$.

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 $n \mid y - x = mt$.

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.

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

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

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:

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

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 $x \equiv 3 \mod 5$.

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.

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 $x \equiv 20 \mod 24$.

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.