Math 417 – Fourth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

August 31, 2020

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

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

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

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

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

Suppose $n \geq 2$. Let

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

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

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

Suppose $n \geq 2$. Let

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

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

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

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

Suppose $n \geq 2$. Let

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

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

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

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

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

Suppose $n \geq 2$. Let

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

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

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

Proof at the end of class.

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

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

I'll remind you of the table.

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

I'll remind you of the table.

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

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

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

I'll remind you of the table.

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

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

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

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

I'll remind you of the table.

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

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

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

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

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

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

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

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

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

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

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

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

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

From Friday: $gcd(x_0, x_1) = gcd(x_1, x_2) = \cdots = \text{gcd}(x_n, x_{n+1}) = x_{n+1}$. There's a numerical example on the next page. We'll also have a worksheet on Monday with smallish numbers.

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

$$\underline{417} = 1 \cdot \underline{341} + \underline{76},$$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

$$\underline{417} = 1 \cdot \underline{341} + \underline{76},$$
$$\underline{341} = 4 \cdot \underline{76} + \underline{37},$$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

$$\underline{417} = 1 \cdot \underline{341} + \underline{76},$$
$$\underline{341} = 4 \cdot \underline{76} + \underline{37},$$
$$\underline{76} = 2 \cdot \underline{37} + \underline{2},$$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

$$\underline{417} = 1 \cdot \underline{341} + \underline{76},$$
$$\underline{341} = 4 \cdot \underline{76} + \underline{37},$$
$$\underline{76} = 2 \cdot \underline{37} + \underline{2},$$
$$\underline{37} = 18 \cdot \underline{2} + \underline{1},$$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

so

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

so

$1 = 37 - 18 \cdot 2$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

so

$$
\begin{aligned}
1 = 37 - 18 \cdot 2 &= 37 - 18 \cdot (76 - 2 \cdot 37) = (1 + 2 \cdot 18) \cdot 37 - 18 \cdot 76 \\
&= 37 \cdot 37 - 18 \cdot 76
\end{aligned}
$$

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

so

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

This class was supposed to be in 341 Altgeld. Let's find $gcd(341, 417)$. I'll emphasize the x_j's by underlining them.

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

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

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

so

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Computable means that there is an algorithm to find them.

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

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

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

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

PROOF Rewrite the hypothesis in parametric form:

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

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

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

PROOF Rewrite the hypothesis in parametric form:

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

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

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

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

PROOF Rewrite the hypothesis in parametric form:

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

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

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

Now we are going to prove a collection of facts about the gcd that we'll be using later. They might seem not very interesting, but they will be very helpful.

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

PROOF Rewrite the hypothesis in parametric form:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thus, if d is a common divisor of ab and n, then $d \mid ab$ and $d \mid n$, so $d \mid 1$. That is, 1 is the only common divisor of ab and n. □

The final fact is the one that will be most useful to us.

The final fact is the one that will be most useful to us.

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

The final fact is the one that will be most useful to us.

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

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

The final fact is the one that will be most useful to us.

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

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

The final fact is the one that will be most useful to us.

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

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

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

The final fact is the one that will be most useful to us.

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

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

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

For example, $gcd(341, 417) = 1$ and $1 = 203 \cdot 341 - 166 \cdot 417$ imply that $203 \cdot 341 \equiv 1 \mod 417$, and we get as an automatic bonus that $gcd(203, 341) = 1$ as well.

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

It's important that here we are keeping the <u>same</u> operation $*$.

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

It's important that here we are keeping the <u>same</u> operation $*$.

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

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

It's important that here we are keeping the <u>same</u> operation $*$.

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

What are the conditions you need for a subset to be a subgroup? The first is that $*$ still has to be a binary operation: so you need that $h, h' \in H \implies h * h' \in H$.

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

It's important that here we are keeping the <u>same</u> operation $*$.

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

What are the conditions you need for a subset to be a subgroup? The first is that $*$ still has to be a binary operation: so you need that $h, h' \in H \implies h * h' \in H$. Groups need identities and so you need $e \in H$, and groups need inverses, so $h \in H$ implies that there exists $h' \in H$ so that $h * h' = e$. Because this is the same operation, we have to have $h' = h^{-1} \in H$.

Let's shift gears and return to groups. I'll begin with an important definition. Suppose $(G, *)$ is a group. and $H \subseteq G$ is a subset of the elements of G and suppose that if you just look at $(H, *)$, then you have a group. In this case, we say that H is a *subgroup* of G.

It's important that here we are keeping the <u>same</u> operation $*$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

. A cyclic group of order 3.

We also have

We also have

$$\begin{array}{c||cc} * & e & a^3 \\ \hline\hline e & e & a^3 \\ \hline a^3 & a^3 & e \end{array}$$

, This is a cyclic group of order 2.

We also have

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

, This is a cyclic group of order 2.

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

We also have

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

, This is a cyclic group of order 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We will spend a lot more time on finding subgroups.

We will spend a lot more time on finding subgroups.

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

We will spend a lot more time on finding subgroups.

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

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

We will spend a lot more time on finding subgroups.

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

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

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

We'll show that for any group G and $g \in G$, $\langle g \rangle$ is a subgroup of G. This was the case for C_6, since $\{e, a^2, a^4\} = \langle a^2 \rangle$ and $\{e, a^3\} = \langle a^3 \rangle$.

We will spend a lot more time on finding subgroups.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This is isomorphic to V.

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

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

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

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

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

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

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

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

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

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

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

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

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

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

Here's $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$.

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

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

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

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

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

I'll do some more examples on Wednesday,