Math 417 – Fifth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

September 2, 2020

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Here are the connections among these groups.

Here are the connections among these groups.

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

Here are the connections among these groups.

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

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

Here are the connections among these groups.

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

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

So, for example, if $\Phi_1([0]_6) = e, \Phi_1([1]_6) = a$, etc, then Φ_1 gives an isomorphism from $(\mathbb{Z}/6\mathbb{Z}, \oplus)$ to C_6. There are six such isomorphisms, one from any column to any other. Just think of the similarity in the multiplication tables.

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

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

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

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

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

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

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

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

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

The first two columns should be clear. For the third, remember that $a \iff [3]_7$, and so $a^2 \iff [3^2]_7 = [9]_7 = [2]_7$, $a^3 \iff [3^3]_7 = [27]_7 = [6]_7$, and $a^6 = (a^2)^3 \iff [2^3]_7 = [8]_7 = [1]_7$.

Here's another picture which will illustrate both the Chinese Remainder Theorem and the Euler Φ function. This is a table of $[a]_{20}$ versus $[a]_5$ and $[a]_4$. (Note that $gcd(4,5) = 1, 20 = 4 \cdot 5$.)

Here's another picture which will illustrate both the Chinese Remainder Theorem and the Euler Φ function. This is a table of $[a]_{20}$ versus $[a]_5$ and $[a]_4$. (Note that $gcd(4,5) = 1, 20 = 4 \cdot 5$.)

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

Here's another picture which will illustrate both the Chinese Remainder Theorem and the Euler Φ function. This is a table of $[a]_{20}$ versus $[a]_5$ and $[a]_4$. (Note that $gcd(4,5) = 1, 20 = 4 \cdot 5$.)

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

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

Here's another picture which will illustrate both the Chinese Remainder Theorem and the Euler Φ function. This is a table of $[a]_{20}$ versus $[a]_5$ and $[a]_4$. (Note that $gcd(4,5) = 1, 20 = 4 \cdot 5$.)

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

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

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

I have indicated the elements of $(\mathbb{Z}/20\mathbb{Z})^*$ in red. I hope you can see how this interacts with the rows and columns. Theorems will follow.

I have indicated the elements of $(\mathbb{Z}/20\mathbb{Z})^*$ in red. I hope you can see how this interacts with the rows and columns. Theorems will follow.

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

I have indicated the elements of $(\mathbb{Z}/20\mathbb{Z})^*$ in red. I hope you can see how this interacts with the rows and columns. Theorems will follow.

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

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

Today's worksheet questions:

Today's worksheet questions:

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

Today's worksheet questions:

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

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

Today's worksheet questions:

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

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

The group $((\mathbb{Z}/13\mathbb{Z})^*, \odot)$ is then a cyclic group of order 12. Find a subgroup of order 3.

1. The divisors of 12 are $D(12) = \{1, 2, 3, 4, 6, 12\}$, so the proper subgroups are

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

$$\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$$

$$\langle a^4 \rangle = \{e, a^4, a^8\}$$

$$\langle a^6 \rangle = \{e, a^6\}$$

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

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

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

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

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

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

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

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

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

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