# Problem 1

**(i)** We have that this is true. That is, we have that the cyclic group $C_m$ is commutative. To prove this, we will consider two arbitrary $x, y \in G$. Now we must show that $xy = yx$. Since $C_m$ is a cyclie group, it has a generator $g$, and we can write $x = g^k$ and $y = g^j$. Then, we have that

$$xy = g^k g^j$$

$$yx = g^j g^k$$

But clearly, this means that

$$xy = g^{k+j}$$

$$yx = g^{j+k}$$

since we are just applying the group operation to the same thing (the generator) multiple times (it was also given in lecture 18 that we can do this with powers). Then, it follows that

$$xy = g^{k+j} = g^{j+k} = yx$$

Note that we assumed here that $k + j$ is less than $m$. If this is not true, then we just take the modulus of it (with respect to $m$), and both sides are still equal. Thus, we have proved the desired statement.

**(ii)** This is false. We can give a counterexample. Let $x$ be rotation 90 and let $y$ be vertical flip. Consider a starting square

| | |
|---|---|
| A | B |
| C | D |

Let us first consider what happens when we apply $x$, then $y$. Applying $x$ (rotation 90) gives us

| | |
|---|---|
| C | A |
| D | B |

Then, applying $y$ (vertical flip) gives us

| | |
|---|---|
| D | B |
| C | A |

Now let us consider what happens when we apply $y$, then $x$, to the starting square. Applying $y$ (vertical flip) gives us

| | |
|---|---|
| C | D |
| A | B |

Then, applying $x$ (rotation 90) gives us

| | |
|---|---|
| A | C |
| B | D |

So clearly applying $x$ then $y$ and applying $y$ then $x$ results in different squares. So for this example, $xy \neq yx$. So we have found a counterexample and shown that the group of symmetries of the square is not commutative.

**(iii)** This is true. Let $G$'s operation be represented as $*$. We have that $G$ satisfies $(ab)^2 = a^2b^2$ for every $a, b \in G$. This is the same as saying that $G$ satisfies $abab = aabb$ for every $a, b \in G$. So, we have that $abab = aabb$. Then we have that $abab = aabb \implies bab = abb$. This is because $bab \neq abb \implies abab \neq aabb$, since to go from the left side of the implies to the right we are just applying the operation $*$ to the same thing ($a$) and two unequal things ($bab$ and $abb$). And doing this cannot possibly turn it into an equality. Then we have that $bab = abb \implies ba = ab$. This is because $ba \neq ab \implies bab \neq abb$, since to go from the left side of the implies to the right we are just applying the operation $*$ to the same thing ($b$) and two unequal things ($ba$ and $ab$). And doing this cannot possibly turn it into an equality. So now we have that $G$ satisfies $ba = ab$ for every $a, b \in G$. But this means that $G$ is commutative. So we have proved that any group $G$ that satisfies $(ab)^2 = a^2b^2$ for every $a, b \in G$ is commutative.

# Problem 2

We have that $\gcd(m, n) \neq 1$, and we wish to prove that $C_m \times C_n$ is not cyclic. We have that we can write

$$C_m = \{1, g, \cdots, g^{m-1}\}$$
$$C_n = \{1, h, \cdots, h^{n-1}\}$$

Now, to show that $C_m \times C_n$ is not cyclic, it suffices to show that $C_m \times C_n$ does not have a generator. So, WLOG, we can consider any element from $(a, b)$ from $C_m \times C_n$. Consider $(a, b)^{mn}$. We have that this takes $a$ through $n$ cycles and $b$ through $m$ cycles, since $m$ divides $mn$ and $n$ divides $mn$. Now consider $k < mn$, where $m$ divides $k$ and $n$ divides $k$. Let $k/m = i$ and $k/n = j$ (since $m$ and $n$ divide $k$, $i$ and $j$ are whole numbers). We have that $k$ exists because $\gcd(m, n) \neq 1$ (more specifically, we can pick $k$ to be $\text{lcm}(m, n) = mn/\gcd(m, n)$). Now consider $(a, b)^k$. We have that this takes $a$ through $k/m = i$ cycles and $b$ throught $k/n = j$ cycles. Now we have that $(a, b)^{mn} = (a, b)^k$, since $a$ going through $\alpha$ cycles, where $\alpha$ is some whole number, is the same as $a$ going through $\beta$ cycles, where $\beta$ is some other whole number (and the same holds for $b$). This basically means that no matter what element we try to pick as our generator, we will repeat elements when we raise the generator to $k$ and to $mn$. But since we have these repeat elements, we cannot generate the entire group. So we have that no element $(a, b)$ from $C_m \times C_n$ can be a generator, and thus that $C_m \times C_n$ is not cyclic.

# Problem 3

**(a)** We will prove this. Consider all elements $a \in G$ where $|a| > 2$. Then we have that $a^{-1} \neq a$ and that $|a^{-1}| > 2$. To see this, consider an arbitrary $a$ where $|a| > 2$. Let $b = a^{-1}$, the unique inverse for $a$ (the fact that such a unique inverse exists was proved in class 18). We have that $a^k = e$ and that $ab = e$, where $k = |a|$. So then we have that $a^k b = a^{k-1} \implies eb = a^{k-1} \implies b = a^{k-1}$. Then, since $b$ is just a power of $a$, it follows that if $|a| > 2$, then $|b| > 2$ (in fact, the orders will be equal). This gives us that elements in $G$ that have order greater than 2 come in pairs. Then we have that $G$ must contain the identity $e$, which clearly has an order less than 2. So overall, we have that of all the elements in the group, an odd number of them are not of order 2. This means that an odd number of the elements are of order 2. So we are done.

**(b)** We have that the number of symmetries of the regular hexagon is $2 * 6 = 12$. We can see this in the following way. There is no action, and 5 rotations. Then there are 6 flips (we can flip along lines drawn from corner to corner and along lines drawn from midpoint to middpoint). So the order for the group of symmetries of the regular hexagon is 12. Then we have that the order for the alternating group $A_4$ is 3. We have that this is true because the order of $A_n$ is half the order of $S_n$ (class 20), and the order of $S_n$ is just $n!$. So here, $|A_4| = \frac{4!}{2} = 12$. So the order of our groups are the same. However, we have that $A_4$ only contains permutations from $S_n$. So basically, permuations of the form (12)(34) or (123), and so on. With this being true, it is clear that there cannot exist an isomorphism between these two groups, because we cannot clearly map from the permutations to the hexagon symmetries and back. In order to do so, we would need permutations from $S_6$, because then we would be able to map every edge to another edge using such permutations. However, as it is, we do not have complex enough permutations to sufficiently map back and forth between the two groups. Shown below is an example of why there cannot be an isomorphism.

# Problem 4

Recall the bound on the size of the harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n} \leq \ln(n) + 1$$

Now we want to show that for every $n$, we have $\bar{t}(n) \leq \ln(n) + 1$. Given the bound on the size of the harmonic series, we can instead show that for every $n$, the following bound holds:

$$\bar{t}(n) = \frac{1}{n} \sum_{j=1}^{n} t(j) \leq \sum_{j=1}^{n} \frac{1}{j}$$

Which is equivalent to the following:

$$\sum_{j=1}^{n} t(j) \leq n \sum_{j=1}^{n} \frac{1}{j}$$

To show this inequality, we can use double counting. So we will make a table as follows:

| | 1 | 2 | 3 | 4 | ... | n |
|---|---|---|---|---|---|---|
| s(1) | x | | | | | |
| s(2) | x | x | | | | |
| s(3) | x | | x | | | |
| s(4) | x | x | | x | | |
| ... | | | | | | |
| s(n) | x | ? | ? | ? | | x |

Here, $s(i)$ denotes the set of elements in $\{1, 2, 3, \cdots, i\}$ that divide $i$, and there is a mark in a box $(i, j)$ if $s(i)$ contains the number $j$. So the number of marks in a given row $i$ is equivalent to $t(i)$, which means that the number of marks total in the table is just equal to $\sum_{j=1}^{n} t(j)$. Now, notice that for each column $j$, we have that the number of marks in that column is bounded above by $\frac{n}{j}$. That is equivalent to saying that the number of numbers from 1 to $n$ that are divisible by $j$ is bounded above by $\frac{n}{j}$. This is true for the following reason. Consider the numbers $1, 2, 3, \cdots, \lfloor \frac{n}{j} \rfloor$. Multiplying each of these numbers by $j$ gives us all the numbers that are divisible by $j$ and that range from 1 to $n$. And the cardinality of that set of numbers is bounded above by $\frac{n}{j}$. So clearly, if we had more than $\frac{n}{j}$ numbers from 1 to $n$ that were divisible by $j$, we would have a contradiction. Now that we have that the number of marks in each column $j$ is bounded above by $\frac{n}{j}$, we can get an upper bound on the number of marks in the table as follows:

$$\sum_{j=1}^{n} t(j) \leq \sum_{j=1}^{n} \frac{n}{j} = n \sum_{j=1}^{n} \frac{1}{j}$$

We got this sum by just summing along the columns, and using the simple fact that summing the number of marks in all the columns just gives us the total number of marks in the table. Then we have that this is exactly the bound that we wanted. So, we can conclude that for every $n$, we have $\bar{t}(n) \leq \ln(n) + 1$.

# Problem 5

Note: all congruences in this problem will be mod $a$. So, we have that $a$ is a composite number which is not a Carmichael number, and that we are choosing a $q \in \{1, 2, 3, \cdots, a-1\}$. We can break this problem down into two.

The first case is when $\gcd(a, q) = g \neq 1$. In this case, the test always finds that $a$ is composite because $q^{a-1} \not\equiv 1$ will always be true (which is right, because $\gcd(a, q) \neq 1$). We have that this is the case because $q^{a-1} = gx$, where $x$ is an integer. We also have that $a = gy$, where $y$ is an integer. So clearly, $gx \not\equiv 1 \mod gy$.

The second case is when $\gcd(a, q) = 1$. In this case, since $a$ is not a Carmichael number, we have that there exists at least one $q$ such that

$$q^{a-1} \not\equiv 1$$

We will call this $q$ $q_0$. We also have a set of $q$s such that

$$q^{a-1} \equiv 1$$

We will call this set $A$. This set will be under mod $a$. Then we have that

$$A = \{q \mid q^{a-1} \equiv 1\}$$

Let $|A| = n$. Now we want to show that we can generate a set $B$ of the form

$$B = \{q \mid q^{a-1} \not\equiv 1\}$$

such that $|B| \geq n$. To do this, consider the set

$$B = \{q_0q_1, q_0q_2, \cdots, q_0q_n\}$$

where $q_1, \cdots, q_n \in A$. This set will also be under mod $a$. Now, consider an arbitrary element $q_0q_i$ of $B$. We want to show that $(q_0q_i)^{a-1} \not\equiv 1$. So, since we have that $q_i^{a-1} \equiv 1$, we get the following:

$$(q_0q_i)^{a-1} \equiv q_0^{a-1}q_i^{a-1} \equiv q_0^{a-1} \not\equiv 1$$

Now we just need to show that each element in $B$ is unique. To show this, assume to the contrary that $q_0q_i \equiv q_0q_j$. Now notice that, since $\gcd(a, q_0) = 1$, we have that there exists a modular multiplicative inverse $q_0^{-1}$ such that $q_0q_0^{-1} \equiv 1$. Thus we can multiply both sides of $q_0q_i \equiv q_0q_j$ by $q_0^{-1}$ to obtain $q_i \equiv q_j$. But this means that whenever two elements of $B$ are the same, the elements of $A$ are the same, which means that $i = j$ since $A$ is a set under mod $a$. Then, given how we constructed $B$, this means that whenever two elements of $B$ are the same, those two elements must be the exact same element. So we have shown that when $\gcd(a, q) = 1$, there exists a set of unique false witnesses $A$ of size $n$, and there exists a set of unique witnesses $B$ of at least size $n$.

Now we can put our two cases together. First we have that there exists an $\epsilon$ probability of getting $\gcd(a, q) \neq 1$. In this case the test succeeds. Then we have that, in the case that this doesn't happen, there is at most a $1/2$ probability of the test failing (because we have at least as many elements in $B$, which are witnesses, as in $A$, which are false witnesses). This is the probability of the second case failing. So, more precisely, the probability that the second case fails is $(1/2)(1 - \epsilon) = 1/2 - \epsilon/2$. So, putting these two cases together (which are clearly disjoint) we have that the probability that the test fails to discover that $a$ is composite when using a uniformly chosen $q \in \{1, 2, 3, \cdots, a-1\}$ is bounded above by

$$\frac{1}{2} - \frac{\epsilon}{2}$$