This week I graded problems 2 and 7, which cover set theory and induction. These were worth 3 points each, and were pretty well answered overall. The other problems were worth half a point each, based on how much effort you seemed to put in. To speed up the grading, at some point I stopped writing checkmarks or numbers if you got full credit. This means that you should compare your answers to the ones below: even if you got full credit, you might have done some of them wrong. Of course there will be some differences between our solutions; if you're not sure that you got something right, I'm always happy to go over it with you.

Problems 4, 5, 6 and 10 seemed to cause the most issues. I tried to be lenient for 5 and 10, since they were more difficult than the others. Problem 6 was kind of a trick question, so I tended not to take off points (even if you just copied the argument from Euclid's proof). If you did get this one wrong, make sure you understand which part of Euclid's argument breaks down.

For problem 4 (which should not have taken much effort to solve) I tended to only give points to those who got it (mostly) right. If you did lose points on this one, feel free to come and talk to me about it. In most cases it just wasn't clear that you understood what the problem was asking, and you might be able to convince me otherwise in person.

To those of you who turned in blank or almost-blank answers to some problems, you should be aware that most of your learning in this course will come from attempting the homework problems. In order to encourage this, I will probably give you credit if you just say something like "I tried doing it like this . . . , it didn't work because . . . ." Ideally I'd like to see that you tried a few different approaches before giving up, but this can vary based on the question.

If you turn in an incomplete or incorrect solution, you are likely to get more points if you acknowledge it. Otherwise, I tend to assume that you were unaware of the mistake. I want to encourage you to look for gaps in your own logic, with the hope that you'll get better at picking apart other's arguments too.

1. Let $a \in A$. Since $A \subseteq B$, $a \in B$. It follows that $a \in C$ (as $B \subseteq C$). Therefore $A \subseteq C$.

2. If $x \in (A - B) \cup (B - A)$, then $x \in A - B$ or $x \in B - A$. In the former case $x \notin B$, so $x \notin A \cap B$. Moreover $x \in A \subseteq A \cup B$, and hence $x \in (A \cup B) - (A \cap B)$. This can be also be shown in the latter case, by the same argument. Therefore

$$(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B).$$

To prove the converse, let $x \in (A \cup B) - (A \cap B)$. If $x \in A$ then $x \notin B$ (since $x \notin A \cap B$) so $x \in (A - B) \subseteq (A - B) \cup (B - A)$. Otherwise (i.e. if $x \notin A$), then $x \in B$ (as $x \in A \cup B$), which means $x \in (B - A) \subseteq (A - B) \cup (B - A)$. This shows that

$$(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A).$$

Therefore $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

3. If A and B are disjoint, i.e. $A \cap B = \varnothing$, then (by definition, if you like)

$$m(A \cup B) = m(A) + m(B).$$

In general $A \cup B$ is the disjoint union of A and $(B - A)$, so

$$m(A \cup B) = m(A) + m(B - A).$$

Since B is the disjoint union of $(B - A)$ and $(A \cap B)$,

$$m(B) = m(B - A) + m(A \cap B).$$

After some rearranging this gives $m(A \cup B) = m(A) + m(B) - m(A \cap B)$.

4. Define $f : S \to S$ by

$$f(s) = \begin{cases} s_2 & \text{if } s = s_1, \\ s_1 & \text{if } s = s_2, \\ s & \text{otherwise.} \end{cases}$$

Strictly speaking we should also show that f is a bijection (but I think this is obvious enough to leave out). This follows from the fact that $f^2 = i$ (so that $f^{-1} = f$).

5. We know from the book that S_n has $n!$ elements, which we can list as $f_1, \ldots, f_{n!}$. Given one of these elements f_k, the list $f_k^0, \ldots, f_k^{n!}$ has to repeat itself somewhere (by the pigeonhole principle). So $f_k^a = f_k^b$ for some integers $a < b$. It follows that $f_k^{b-a} = i$.

So far we've shown that, for each f_k, there is a positive integer t_k such that $f_k^{t_k} = i$. What we want is one number t that works for all k. Since $f_k^{mt_k} = (f_k^{t_k})^m = i^m = i$ for all $m \in \mathbb{Z}$, we can just set $t = t_1 \times \cdots \times t_{n!}$.

6. Nope: it turns out that $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$, which is $59 \cdot 509$.

7. If $n = 0$ the result is obvious. Let n be a positive integer such that $n^3 - n$ is divisible by 3. In other words $n^3 - n = 3k$ for some $k \in \mathbb{Z}$. Observe that

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = 3(k + n^2 + n)$$

is also divisible by 3. By induction, this shows that 3 divides $n^3 - n$ for all $n \in \mathbb{N}$.

If you also want to handle negative integers, note that $-(n^3 - n) = (-n)^3 - (-n)$.

8. Write $z = a + bi$ and $w = x + yi$ for $a, b, x, y \in \mathbb{R}$ and check it yourself.

9. Let $z \in \mathbb{C}$ and write $z = re^{i\theta}$ for $r \in [0, \infty)$ and $\theta \in \mathbb{R}$. Since $i = e^{i\pi/2}$,
$$zi = re^{i\theta + i\pi/2} = re^{i(\theta + \pi/2)}.$$
In other words zi has the same length as z, but the angle between zi and the positive x-axis is 90° larger (or 270° smaller, same thing really).

10. There are a few ways to do this. Since this is a group theory course, the following seems the most appropriate. You can check that the nth roots of unity form a subgroup of $\mathbb{C}^\times$ (the multiplicative group of nonzero complex numbers). This subgroup is finite because the polynomial $z^n - 1$ has (at most) n zeros. It turns out that, if G is *any* nontrivial finite subgroup of $\mathbb{C}^\times$, its elements add up to 0.

    To prove this, start by choosing some $x \in G$ with $x \neq 1$. Note that
$$x \sum_{g \in G} g = \sum_{g \in G} xg$$
is just $\sum_{g \in G} g$. The reason is that the map from G to itself sending $g \mapsto xg$ is a bijection (its inverse is just $g \mapsto x^{-1}g$). In other words, when summing up xg for all $g \in G$, each element of G appears in the sum exactly once (the only difference might be the order they appear in, which doesn't matter). Therefore
$$(x - 1) \sum_{g \in G} g = x \sum_{g \in G} g - \sum_{g \in G} g = 0,$$
so either $x - 1 = 0$ or $\sum_{g \in G} g = 0$. The latter must be true because we chose $x \neq 1$.

    Extra comments: in doing it this way I hoped to show you that using groups can make a statement more general without really changing the proof. However, in this particular example we didn't really gain anything: it turns out that any finite subgroup $G \subseteq \mathbb{C}^\times$ is the group of $|G|$th roots of unity!

    If you want to prove this, first check that any $z \in \mathbb{C}^\times$ with $|z| \neq 1$ generates an infinite subgroup of $\mathbb{C}^\times$. The upshot is that the finite subgroups of $\mathbb{C}^\times$ all live in the unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. We can think of S^1 as the set of angles $\theta \in [0, 2\pi)$, together with the operation "addition modulo 2π" (later in the course, we will recognise this as the *quotient group* $\mathbb{R}/2\pi\mathbb{Z}$). Any nontrivial finite subgroup $G \subseteq S^1$ will contain a smallest angle $\theta \in (0, 2\pi)$. You can show (as in problem 5) that $e^{i\theta}$ has finite order. This implies that $\theta = \frac{2\pi k}{n}$ for some positive coprime integers k and n. Using Euclid's result that $1 = ak + bn$ for some $a, b \in \mathbb{Z}$, you can show that $\frac{2\pi}{n}$ belongs to G. Since θ is supposed to be the smallest positive angle, it follows that $k = 1$. In other words $e^{i\theta} = e^{i\frac{2\pi}{n}}$ generates the group of nth roots of unity. To show that G is no bigger than this, you can argue by contradiction using the minimality of θ.