At the end of week 3, on top of what you reviewed for Midterm 1, you should be able to do the following:

- **Decide if you want to prove a statement by direct proof or proof by contrapositive.** We did several examples in class among which:
  1. For $a \in \mathbb{Z}$, if $a^2$ is even then $a$ is even.
  2. For $(x, y) \in \mathbb{Z}^2$, if 5 does not divide $xy$, then 5 does not divide $x$ and 5 does not divide $y$.
  3. For $x \in \mathbb{R}$, if $x^3 - x > 0$ then $x > -1$. (We did a direct and a contrapositive proof. This is Chapter 5 Problem 6).
  4. For $(a, b, c, d) \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n \geq 1$, if $a \equiv b \mod n$ and $c \equiv d \mod n$ then $ac \equiv bd \mod n$.
  5. Check out the problems covered in the text of Chapter 4 and 5. You will recognize several results we proved in class. Of course also feel free to go over the problems of these sections.

- **Prove that two statements are equivalent.** For example, we proved that for $n \in \mathbb{Z}$, the following are equivalent:
  i. 2 divides $n$ and 3 divides $n$,
  ii. 6 divides $n$.

- **Start (even if we haven’t covered Chapter 7 yet) realizing that some proofs are about proving that "something exists" and this will require a new kind of reasoning** (it won’t be "assume statement P and deduce statement Q" or, "suppose that $x$ is in set $A$ and deduce that $x$ is in set $B$")...
  1. Proof of the Euclidean Division theorem which I recalled on HW1. It involved the Well Ordering Principle in $\mathbb{N}$.
     Note that this proof is about checking that something exists (namely the pair $(q, r)$ in question in the theorem) but also about checking that this pair is unique (with the required properties). So this was a preview Problem 28 Chapter 7. For the existence part of the proof, see also Section 1.9 of the book (page 30).
  2. We gave the following definition: for $x \in \mathbb{R}$, there is a unique integer $\lfloor x \rfloor \in \mathbb{Z}$ such that $x \in \left[ \lfloor x \rfloor, \lfloor x \rfloor + 1 \right)$. For example $\lfloor -2.6789 \rfloor = -3$ and $\lfloor 3.235 \rfloor = 3$. This allowed us to prove the following:

\[
\bigcup_{n \in \mathbb{N}, n \geq 1} \left[ \frac{1}{n} - 1 \right] = (0, 1].
\]

$\square$ Let $x \in \bigcup_{n \in \mathbb{N}, n \geq 1} \left[ \frac{1}{n} - 1 \right]$. It means that $x$ is in (at least) one of the sets of this collection namely there is (at least) one $n \in \mathbb{N}$ with $n \geq 1$ such that $x \in \left[ \frac{1}{n}, 1 \right]$. Since $\left[ \frac{1}{n}, 1 \right] \subseteq (0, 1]$, it implies $x \in (0, 1]$.

$\square$ Let $x \in (0, 1]$. We have $\frac{1}{x} > 1$. Let $m_0$ denote the integer $\lfloor \frac{1}{x} \rfloor$. Since $\frac{1}{x} > 1$, it satisfies $m_0 \geq 1$. We have, by definition, $\frac{1}{x} \in \left( m_0, m_0 + 1 \right)$. Let $n_0$ denote the
integer $m_0 + 1$. Notice that $n_0 \geq 1$ (since $m_0 \geq 1$). We have $\frac{1}{x} \in [n_0 - 1, n_0)$ so $0 < \frac{1}{x} < n_0$ and $x > \frac{1}{n_0} > 0$. Therefore $x \in (\frac{1}{n_0}, 1] \subseteq [\frac{1}{n_0}, 1]$. This proves that $x \in \bigcup_{n \in \mathbb{N}, n \geq 1} \left[ \frac{1}{n}, 1 \right]$. I consider this proof a proof of "existence" since, given $x \in (0, 1]$ we had to prove that there exists $n_0 \in \mathbb{N}$ with $n_0 \geq 1$ such that $x \in [\frac{1}{n_0}, 1]$.

(3) In week 4 we will do the last problem on our list (from Friday June 1st):
A natural number $n \in \mathbb{N}$ satisfying $n \geq 2$ has (at least) one divisor which is a prime number. This will use the Well Ordering Principle of $\mathbb{N}$.

• Compute the gcd of two integers using the Euclidean algorithm and understand why the algorithm works.
We proved in class the following result which is a generalization of Problem 29 Chapter 5 (in class we actually started by solving Problem 29 Chapter 5 so you have the solution of that problem in your notes – alternatively, notice that Problem 29 Chapter 5 is the following proposition when we take $k = 1$):

**Proposition.** Let $(a, b) \in \mathbb{Z} \setminus \{(0, 0)\}$ and let $k \in \mathbb{Z}$. We have:

$$\gcd(a, b) = \gcd(b, a - kb).$$

**Proof.** Let $(a, b, k) \in \mathbb{Z}^3$. We are going to prove that the following two sets are equal:

$$\{d \in \mathbb{Z} \setminus \{0\} \text{ such that } d|a \text{ and } d|b\} = \{d' \in \mathbb{Z} \setminus \{0\} \text{ such that } d'|b \text{ and } d|a - kb\}$$

- Let $d \in \mathbb{Z} \setminus \{0\}$ such that $d$ divides $a$ and $b$. It means that there is $(x, y) \in \mathbb{Z}^2$ such that $a = xd$ and $b = yd$. So $a - kb = d(x - ky)$ and $d$ divides also $a - kb$.
- Let $d' \in \mathbb{Z} \setminus \{0\}$ such that $d'$ divides $a - kb$ and $b$. It means that there is $(x', y') \in \mathbb{Z}^2$ such that $a - kb = x'd$ and $b = y'd$. So $a = (a - kb) + kb = d(x' + ky')$ and $d$ divides also $a$.

Now suppose that $(a, b) \neq (0, 0)$. It implies that $(b, a - kb) \neq (0, 0)$ why? because, by contrapositive: if $(b, a - kb) = (0, 0)$ then $b = 0$ and $a - kb = a = 0$.

Then the gcd of $a$ and $b$ is defined to be the largest element in the left hand side set, and the gcd of $b$ and $a - kb$ is defined to be the largest element in the right hand side set. Since we just proved that these two sets are equal, we have

$$\gcd(a, b) = \gcd(b, a - kb).$$

□

We deduce the following, which is Problem 31 of Chapter 5:

**Corollary.** Let $a, b \in \mathbb{Z}$ such that $0 < b \leq a$ and $a = bq + r$ the Euclidean division of $a$ by $b$. Then

$$\gcd(a, b) = \gcd(b, r).$$
Proof. This is a direct application of the proposition since $b > 0$ implies that $(a, b) \neq (0, 0)$ (so we are indeed allowed to apply the proposition).

Applying. Compute the gcd of 68 and 119.

Solution. We write the successive Euclidean divisions:

$(119 \text{ by } 68) 119 = 1 \times 68 + 51$
$(68 \text{ by } 51) 68 = 1 \times 51 + 17$
$(51 \text{ by } 17) 51 = 3 \times 17 + 0$

So $\gcd(119, 68) = \gcd(68, 51) = \gcd(51, 17) = \gcd(17, 0) = 17$.

In this context we also proved the following proposition. (We related this proposition to an observation on the multiplication table of the integers mod $n$— we talked about the integers $a$ which are "invertible modulo $n$"). This is an introduction to the statements proved in Chapter 7 which we will cover in week 4. This should also resonate with HW3.

Proposition. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n \geq 1$. Suppose that there is $x \in \mathbb{Z}$ such that $ax \equiv 1 \mod n$, then $\gcd(a, n) = 1$.

Proof. Let $a$ and $x$ be as in the proposition and suppose that there is $x \in \mathbb{Z}$ such that $ax \equiv 1 \mod n$. Then there is $y \in \mathbb{Z}$ such that $ax = 1 + ny$. Now let $d \in \mathbb{Z} \setminus \{0\}$ dividing both $a$ and $n$. Then it divides $ax - ny$ which is equal to 1. So $d = 1$ or $d = -1$. This proves that $\gcd(a, n) = 1$.

This means for example that there is no integer $x \in \mathbb{Z}$ such that $21x \equiv 1 \mod 14$. 

□