MATH 144 HANDOUT 0:
A TASTE OF NUMBER THEORY

This worksheet is a bit of a trial by fire. You are being asked to prove things, perhaps without properly seeing a proof. Part of what I want you to do is to think about what a proof should be. The idea is for you to work things out in your groups and with help from me or your TA.

It is important to note that we are diving in head first here. There are going to be some subtle issues that you will bump into and our goal will be to see what those issues are, and then we will take a step back and start again in the coming classes. There is no expectation that you will complete the whole handout, and some of these problems may appear on later handouts.

See what you can do!

Group work skills (adapted from Diana Davis):

(1) Contribute to class every day.
(2) Speak to classmates, not to the instructor(s).
(3) Share your thoughts about difficult problems, even if you are convinced you are wrong.
(4) Use other students' names.
(5) Ask lots of questions.
(6) Answer other students' questions.
(7) Suggest an alternate solution method.
(8) Draw lots of pictures.
(9) Connect similar problems.
(10) Summarize the discussion of a problem.

Discussion

On this worksheet, we will work with the set of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The goal is to get started with proving some theorems about numbers and study the properties of $\mathbb{Z}$. Because you are so familiar with properties of the integers, one of the issues that we will bump into knowing which facts about the integers we can take for granted. As a general rule of thumb, you should attempt to use the definitions provided without relying too much on your prior knowledge. We will likely need to discuss this further as issues arise.

Recall that the symbol "$\in$" is an abbreviation for "is an element of" or sometimes simply "in." For example, the mathematical expression "$n \in \mathbb{Z}$" means "n is an element of the integers", i.e., "n is an integer".

Here are the relevant definitions for this handout:

Definition 1. *An integer n is **even** if $n = 2k$ for some $k \in \mathbb{Z}$.*

Definition 2. *An integer n is **odd** if $n = 2m + 1$ for some $m \in \mathbb{Z}$.*

Definition 3. *Suppose that n and m are integers. We say n **dvides** m and write $n|m$ if there exists an integer $k \in \mathbb{Z}$ so that $m = nk$. In the same context, we may also write that m is **divisible** by n.*

Exercises

(1) Prove each of the following statements:

(a) The sum of two consecutive integers is odd.

- What are you implicitly assuming about the result of adding two integers?

(b) If n is an even integer, then n^2 is an even integer.

- What are you implicitly assuming about the result of multiplying two integers?

(2) Prove or provide a counterexample: The sum of an even integer and an odd integer is odd.

(3) Conceptual question:

   (a) Did Question 1a need to come before Question 2? Could we have used Question 2 to prove Question 1a? If so, outline how this alternate proof would go.
   (b) Perhaps your original proof utilized the approach I'm hinting at. If this is true, can you think of a proof that does not rely directly on Question 2? Is one approach better than the other?

(4) For each of the following, prove or provide a counterexample:

   (a) The product of an odd integer and an even integer is an odd integer.

   (b) The product of an odd integer and an odd integer is odd.

   (c) The product of two even integers is even.

(5) For integers n and m, how are the following mathematical expressions similar and how are they different?

   (a) $m|n$ (b) $\frac{m}{n}$ (c) m/n

(6) Let $n \in \mathbb{Z}$. Prove or provide a counterexample: If 6 divides n, then 3 divides n.

(7) Let $n \in \mathbb{Z}$. Prove or provide a counterexample: If 6 divides n, then 4 divides n.

(8) Suppose we have integers $n, m, a \in \mathbb{Z}$. Prove that if $a|n$ then $a|mn$.

(9) Use the previous problem to prove the following: If $a, n \in \mathbb{Z}$ and $a|n$, then $a|n^2$.

(10) Prove or provide a counterexample: If $a, n \in \mathbb{Z}$ and $a|n^2$, then $a|n$.

(11) Suppose that $a, n \in \mathbb{Z}$. Prove that if a divides n, then a divides $-n$.

(12) Suppose that $a, n, m \in \mathbb{Z}$. Prove that if $a|n$ and $a|m$, then a divides $n + m$.

(13) Prove or provide a counterexample: Suppose that $a, n, m \in \mathbb{Z}$. If a divides $m+n$, then $a|n$ and $a|m$

- The above statement is the **converse** of the statement in the previous problem.

Using previous work: Once we have proven a few theorems, we should be on the look out to see if we can utilize any of our current results to prove new results. There is no point in reinventing the wheel if we don?t have to. Try to use a couple of our previous results to prove the next theorem.

(14) If $a, n, m \in \mathbb{Z}$ and $a|m$ and $a|n$, then a divides $n - m$.