Lecture 8

This week we start a new chapter, one on number theory. Number theory and geometry are the oldest parts of mathematics. Although the Greeks "majored" in geometry, they were also involved in number theory. It frustrated them greatly that the diagonal and edge of a square were not commensurate, i.e., if the edge is one unit, then the diagonal is $\sqrt{2}$ units, an irrational number.

For those who are haven't studied number theory in a long time, I recommend starting with Problem 4.1, which is a list of terms that are used throughout the chapter and will be used in this lecture as well.

One thing that may not come up in your search on the web for these terms is that the greatest common divisor of a, b is the least positive linear combination of a and b. So if a, b are relatively prime, $1 = ax + by$ for some integers x and y. You may use this to prove that, if a prime p divides ab, then p divides a or p divides b. You might find this theorem useful in the uniqueness part of Exercise 4.1 for which you might find "strong" induction useful for existence.

In problems such as Exercise 4.3 and Problem 4.1, the different letters stand for different digits among $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. The subscript base b in Exercise 4.3 means to work in base b. We usually work in base 10, so $173 = 1 \times 10^2 + 7 \times 10 + 3$. If we worked in base 8, then $173 = 1 \times 8^2 + 7 \times 8 + 3 \times 8^0$ in base 10. Notice that we can't have a $173_{\text{base 5}}$ because $7 > 5$ and $7_{\text{base 10}} = 12_{\text{base 5}}$.

We say an integer n divides an integer b and write $n|b$ if there is an integer c such that $b = cn$. So $a \equiv b \Leftrightarrow n|b - a \Leftrightarrow b - a = cn \Leftrightarrow b = a + cn$. Another way to think of it is that a and b have the same remainder when divided by n. All of these ways of think of mod n are useful.

Another useful function is the floor function, $\lfloor x \rfloor =$ the greatest integer less than or equal to x. So $\lfloor 3 \rfloor = 3 = \lfloor \pi \rfloor$. I needed to use this function to find $f(m)$ in part 2 of Exercise 4.6.

Next time we'll work with more modular arithmetic and prove some neat theorems.