Midterm review

Here are some of the topics we covered in lectures during the first half of the course. The midterm will consist of five or six short problems related to these topics. You should be familiar with each topic to some degree — just having been in class during the lectures and having tried to follow along should be almost enough preparation in itself. Having done assignments 1 through 3 should also be a big help, of course. If, however, any of the topics below seem unfamiliar to you, you might also look them up in your notes and review them a bit before the midterm.

The list of topics below does not include material on Pythagorean triples, rational solutions of algebraic equations (Diophantine problems), or the problem of finding triangles with rational sides and rational area. These will be covered on a future assignment (assignment 4).

- Principle of infinite descent.
- Proof of the irrationality of $\sqrt{2}$ using the principle of infinite descent.
- Euclid's proof that there are infinitely many primes.
- Euclidean algorithm for finding the greatest common divisor of two numbers.
- Proof, using the Euclidean algorithm, that the greatest common divisor of two numbers a and b can be written in the form $ax + by$, for some integers x and y. For want of a better name, let's call this the "g.c.d. theorem".
- Proof, using the g.c.d. theorem, of the "prime divisor property": if a prime p divides ab then p must divide either a or b.
- Proof, using the prime divisor property, of the "unique prime factorization" theorem for natural numbers (also called the "fundamental theorem of arithmetic"). This theorem says that any natural number can be written as a product of primes in a unique way. More precisely, there is essentially only one way to write a natural number n as a product of primes, $n = p_1 p_2 p_3 \cdots p_k$ (where the primes $p_1, p_2, \ldots, p_k$ are not necessarily distinct). The only other ways to write n as a product of primes would be to multiply together the same primes $p_1, p_2, \ldots, p_k$ in a different order, and of course this is not really a different factorization of n.
- Euclid's proof that if p is a prime of the form $p = 2^n - 1$, then the number $2^{n-1}p$ is perfect.
- Proof of the converse of the preceding theorem: if N is an even perfect number, then N is of the form $2^{n-1}p$, where $p = 2^n - 1$ and p is prime.
- Proof of the irrationality of $\sqrt{2}$ using "anthyphairesis", a fancy word for "chopping squares off a rectangle".
- Relation between anthyphairesis, the Euclidean algorithm, and "continued fractions".
- Ruler and compass constructions. Constructible points in the plane.
- Proof that any constructible point has coordinates obtainable by starting with the natural numbers and performing finitely many of the following operations: addition, subtraction, multiplication, division, and square root.
- Proof of the converse of the preceding result: any point with coordinates obtainable from the natural numbers by the above operations is a constructible point.
- Proof that $\sqrt[3]{2}$ is not constructible.
- Archimedes' method for trisecting the angle with compass and *marked* straightedge. (This is called a "neusis" construction.)
- The Greeks defined two polygons to have equal area if one could be cut into pieces which could be reassembled to form the other. Two such polygons are said to be "equidecomposable". It seems obvious that if one polygon P_1 contains a smaller polygon P_2, then P_1 should not be equidecomposable with P_2; i.e., a whole and its part should not be equidecomposable. However, the Greeks were never able to prove this (and not for want of trying). Today, we settle the issue by defining area in terms of numbers: first we define the area of a triangle to be one half its base times its height, and then we define the area of a general polygon to be the number obtained by cutting the polygon into triangles and adding up the areas of the triangles. If you want to get away with this definition, however, you have to prove that it leads to a consistent result: in other words, you need to prove that no matter how you cut a polygon

up into triangles, you always get the same number when you sum up the areas of the triangles. We did *not* do this in class (it was done by Hilbert in 1900).

- What was true for the Greek notion of area because of their *definition* of area now becomes a fact which needs to be *proved* for our modern notion of area. In other words, it has to be proved that two polygons which have the same area according to the modern definition are equidecomposable, and so also have the same area according to the Greek definition. We did not do this in the lectures, but it was done on the homework (Assignment 3).