MONT 104Q – Mathematical Journeys: From Known to Unknown
Group Discussion Day 1 – Two proofs from Euclid in Hardy's *A Mathematician's Apology*
September 21, 2015

Background

On pages 92 to 96 of *A Mathematician's Apology*, Hardy gives two famous examples of proofs that he says exemplify "serious mathematics." Both appear in essentially the same form in the *Elements* of Euclid that we will study next, although not in the section on geometry that we will study in detail. In this discussion day, we want to work through the details of these proofs to understand the logic behind them. Second we want to think about what Hardy says about their usefulness, or lack thereof.

Questions

A. The first proof shows that there are *infinitely many different prime numbers.*

1. Exactly how do Hardy and Euclid present the concept of a prime number? Note that Hardy takes care to say that $n = 1$ is *not* considered to be prime (even though the only positive factors of 1 are 1 and $n = 1$, so it looks as though we might want to). Is this the way you saw primes defined in your previous mathematical work?
2. The beginning of this journey, so to speak, is to assume the opposite of the statement to be proved: "Let us suppose that [the series of primes **does** come to an end] and that
$$2, 3, 5, \ldots, P$$
is the complete series ... ." The strategy that will be used here is called *indirect proof* or *proof by contradiction*, or *reductio ad absurdum* in Latin. What does this mean?
3. Identify and carefully state (at least) two important facts about prime numbers and other integers that Euclid and Hardy are assuming to be *already known* in order to carry out this proof. Hint: Think about the way the reasoning goes after the formation of the integer
$$Q = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot P + 1.$$
4. A relatively subtle point: What is it about the process of dividing one integer into another that lets Euclid and Hardy conclude that the primes $2, 3, \ldots, P$ *do not divide* Q?
5. Exactly where does the contradiction that proves the result come from? If we had just "missed" one or more primes appearing in the factorization of Q, why couldn't we just include them in our list and say that we had the complete list of primes now?

B. The second proof, sometimes ascribed to Pythagoras or his school, shows that the number $\sqrt{2}$ cannot be written in the form $\sqrt{2} = \frac{a}{b}$ for integers a, b. (We say now that $\sqrt{2}$ is an *irrational number* to express this more succinctly.)

1. How is this proof similar to the first one? What is the key starting point for this journey? Hint: The most important thing here is a key assumption about the integers a, b.
2. How is a contradiction reached here?
3. A related but slightly different proof would be to consider the equation $a^2 = 2b^2$ where a, b are integers. If we write out *the prime factorizations* for a and b and substitute them into the equation $a^2 = 2b^2$, then count the number of 2's appearing on both sides, it can be seen that we get another contradiction. Explain how that proof would work. Does this seem easier or harder to understand to you than the proof Hardy describes? Why do you suppose Hardy presents the proof the way he does?

C. Hardy states on page 101 that "There is no doubt at all, then, of the 'seriousness' of either theorem. It is therefore the better worth remarking that neither of them has the slightest 'practical' importance." What evidence does Hardy give to justify this statement? The *RSA public key encryption system* is what almost all of today's web browsers use to make secure transmission of information over the internet possible. Look this up and try to identify the role of prime numbers in RSA. Was Hardy right about the lack of practical importance of the fact that there are infinitely many primes?

Assignment

One writeup from each group, due in class on September 23. These can be typed or hand-written as you prefer.