MATH 25 CLASS 1 NOTES, SEPTEMBER 21 2011

1. A very brief and vague introduction to number theory

What's number theory about? How is it different from, say, calculus or linear algebra, which are two staples of an introductory college mathematics curriculum? It might not be too much of a simplification to say that number theory is the study of *integers* and associated mathematical objects, such as rational numbers. This is in contrast to a subject like calculus, which is more concerned with functions on real numbers, and properties of such functions (such as rate of change, area under curve, etc.).

As a sample of the flavor of question you might encounter in number theory, consider the polynomial equation

$$x^2 + y^2 = z^2.$$

If you permit x, y, z to be any real numbers, then this has infinitely many solutions and they can be graphically described by a cone in $\mathbb{R}^3$. This is a type of graph you might consider in analytic geometry or calculus. On the other hand, in number theory you might only be interested in solutions where x, y, z all must be integers. If we require that $x, y, z > 0$ (which does not appreciably change the problem, since $(-x)^2 = x^2$), then such a triple (x, y, z) is known as a *Pythagorean triple*, because they form the lengths of the sides of various right-angled triangles.

The ancient Greeks had a philosophical belief that numbers governed the universe, and after the discovery of the Pythagorean theorem they became interested in determining the form of every Pythagorean triple: that is, they wanted to find a formula which would generate every Pythagorean triple. The Greeks were indeed able to do this, and perhaps at some point in this class we will explain how they found their solution. (If you want, you can either read this on your own, or try to derive it yourself!)

One of the defining characteristics of number theory is that frequently one can change the statement of a problem only slightly and end up with a dramatically more difficult problem. For example, consider the polynomial

$$y^2 = x^3 - x.$$

Over the real numbers, this obviously has infinitely many solutions. However, what happens if we only permit integer solutions? A bit of inspection indicates that $(0, 0), (-1, 0), (1, 0)$ are all solutions to this equation. Are there any more? This turns out to be quite a difficult question to answer – the solution requires techniques substantially beyond the scope of this class. Yet the only change we made between this question and the previous question was to increase the degree of the polynomial by one – we even reduced the number of variables! (If you are curious, the answer is that there are no more integer solutions, and even no more rational solutions.)

Even though we said that number theory tries to answer various questions about integers, there are still times when it might be useful to use calculus, linear algebra, or tools from other branches of mathematics. As a matter of fact, it is a hallmark of modern number theory to use techniques from virtually every branch of mathematics to help solve problems, and some of the greatest innovations come precisely when someone discovers how to apply a new technique from seemingly unrelated parts of mathematics to number-theoretic

problems. In this class, though, we will almost entirely restrict ourselves to *elementary* techniques, which roughly speaking can be considered techniques which only require mathematics up to trigonometry. (Do not confuse elementary with easy. Some of the most difficult mathematics revolve around elementary techniques!)

As a matter of fact, not only might number theory draw on ideas from all across mathematics, it may find itself asking questions about mathematical objects which are not integers. For example, consider the number $\sqrt{2}$. This is defined to be the positive number x which satisfies $x^2 = 2$; a geometric description of this number is as the length of the hypotenuse of a right triangle whose other two sides both have length 1. This is obviously not an integer, but we can ask, is this a *rational number*? (A rational number is a number expressible as a fraction with integer numerator and denominator, such as $1/2, 4/3, -7/5$.) Again, the ancient Greeks were very interested in problems of this kind. It came as a massive shock to the school of Pythagoras when they discovered and proved that $\sqrt{2}$ is *irrational* – that is, not rational. We will describe their proof of this fact in a few weeks.

Another broad class of questions number theory attempts to deal with are those concerning *prime numbers*. A prime number is a positive integer which only has two positive divisors – 1 and itself. For instance, $2, 3, 5, 7, 11, \ldots$, is the beginning of the sequence of prime numbers. Somewhat because of convention, 1 is not considered a prime number. As soon as we write down the first few prime numbers, a few questions naturally present themselves. For instance, are there finitely many or infinitely many primes? Is there an 'easy' formula to generate prime numbers? If there are infinitely many primes, 'about' how many are there less than X, where X is some positive number?

We will learn in the first few weeks of class that there are infinitely many prime numbers, and give an simple and elegant proof of this fact. However, the other questions turn out to be substantially harder to answer. And a question like 'Are there infinitely many twin primes; that is, prime numbers p such that $p+2$ is also prime?' is still unanswered, despite hundreds of years of effort on this problem. Another, somewhat related problem, which is also unanswered, is the *Goldbach conjecture*, which asks whether every even number greater than 2 is the sum of two prime numbers. The general belief is that there are infinitely many twin primes and that the Goldbach conjecture is true, but no one has any real idea how to go about proving these statements.

These different types of questions are all simple to state and are natural questions to ask. In some sense, they are far removed from any practical applications in the real world. Contrast this to calculus, which was developed precisely to understand gravitation, or differential equations, which is strongly motivated by mathematical descriptions of various natural phenomena (gravitation, fluid motion, heat transfer, etc.) Nevertheless, we will spend a small amount of time illustrating how number theory can be used in very important everyday applications – in particular, how number theory is used in the theory of cryptography. It is number theory which forms the theoretical basis of secure transmission of information; for instance, when you shop over the Internet, more likely than not, when you submit credit card information, you do so on sites with an 'https' and a secure lock in the status bar. This means that your data is encrypted in such a way so that it is very hard (perhaps practically impossible?) for someone who intercepts the encrypted data to read your information. The economic, financial, and military applications of this technology are obvious, so it should not be too much of a surprise that the National Security Agency is the single largest employer of mathematicians in the United States.

So there are a lot of reasons to learn number theory. First and foremost, it is fun, and it deals with very natural and attractive questions. The methods used to answer those questions are diverse, and the difficulty of solutions to these questions range from fairly simple to exceedingly complex. Number theory is a fantastic place to learn how to write

complete, clear, and correct mathematical proofs, and is an ideal subject to teach logical thinking. Not only does it have tremendous theoretical appeal, number theory also has many applications in the 21st century.