MATH 25 CLASS 1 NOTES, SEPTEMBER 22 2010

1. Administrative information

Instructor Information: Name: Andrew Yang, Office: Kemeny 316, Email: Andrew.C.Yang@dartmouth.edu Office phone: 646-2960, Office hours: MWF 2:30pm - 3:30pm, or by appointment (use email or talk to me in person).

Book: *Elementary number theory*, by Gareth A. Jones and J. Mary Jones. Available at the bookstore. The website has several other books which cover similar material (and more) which you might find interesting or useful.

Webpage: `www.math.dartmouth.edu/~m25f10`. This page is very important as it will have a link to your weekly written homework assignments. It has comprehensive information about the class and will also be the place to go for updates as the class proceeds.

Grading: Based on homework and exams. Homework will constitute a third of the grade, while exams the remaining two thirds. There will be two midterms, to be held at times to be determined in the near future. The final will be sometime in December, of three hours in length, with the exact date to be determined. The two midterms will be a third of your grade, and the final exam will be another third.

Written homework assignments will be due once a week, on Friday at 2pm. You can either turn them in during class or at my office. Each week's homework will be listed on the course webpage. A grader will grade your assignments and they will be returned back in class, usually on the Monday after they have been turned in.

We are not only looking for correct answers on homework, but also clear, correct justification of the steps it took to reach that final answer. A correct answer without explanation is worth very little; on the flip side, an incorrect answer which has thorough justification but a small error somewhere will usually be worth quite a bit of partial credit. A corollary to this is that we expect your written assignments to be organized and legible.

X-hour: The X-hour for this class is on Tuesday, 12:00pm - 12:50pm. Keep this slot of time available – although we will not use it regularly, there will be at least a few weeks where we will use the X-hour as a replacement class for another day where I will not be in, or when a holiday occurs on one of the regularly scheduled class days.

Late homework policy: In general, unexcused late homework will not be accepted for credit, although you can turn in late homework assignments which will be returned with comments. The only general reasons we will grant extensions on homework are for illness or family emergencies. In these cases, please notify me before the assignment is due with the reason why you cannot turn in the assignment on time. If you have some other reason why you cannot finish an assignment on time, you can always email me and ask for an extension, although I cannot guarantee that you receive one.

Collaboration policy: Collaboration is allowed and even encouraged. On written assignments, you may work on problems with others. Please indicate who you collaborated with on your assignment. If you use a source besides our textbook in your solutions, please also cite that reference. However, it might be a good idea to try to work on every homework

problem on your own for some time before seeking outside help. Solving exercises is how you best learn mathematics, and trying to solve them on your own, even if it is difficult or frustrating, is how you most effectively learn. In any case, you might want to view homework problems as practice for the exams, which you will not be able to collaborate on.

Keep in mind that while you may collaborate with others on homework assignments, your written answers should be in your own words. As a general rule of thumb, it is okay to work with others to find the ideas needed to solve a problem, but when you write down those ideas, the style and words you use should be your own. If you find yourself copying sentences or even phrases from someone else's assignment, you're probably breaking the collaboration policy. You should indicate who you collaborated with and any outside sources (namely, anything not the required text) you consult on your homework assignment.

Assistance: In general, there is a good amount of assistance available for this class. If you are having trouble in the class, do not hesitate to seek help. This can mean talking with me during office hours, after class, or talking with fellow students in the class. You may also be fortunate enough to find someone who took Math 25 before; they may also be a good resource.

2. 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.

3. Preliminaries: sets, logical statements, and notation

Before delving into number theory proper, we will spend a few moments discussing some preliminary ideas. One of the most fundamental concepts in mathematics is that of a **set**. Instead of giving a precise definition (which turns out to be quite hard), we will content ourselves by informally defining a set as follows:

Definition 1 (Informal)**.** *A **set** is an unordered collection of distinct objects.*

A set can have either finitely many or infinitely many objects. We often use various letters or other symbols to denote a set. If we want to actually list the elements, in a set, we use curly braces, { and }, to delimit the objects in a set. For instance, if S consists of the numbers $1, 2, 3$, we may write $S = \{1, 2, 3\}$. If an object x is in the set S, we say that x is an **element** of S, and sometimes write this using the notation $x \in S$. That symbol looks like an epsilon, but isn't the same. An object can only belong to a set once or not at all – an object cannot be an element of a set more than once. The elements of a set do not have to be numbers; they can be whatever you want them to be. For example, the set of past and current US Presidents consists of forty-three men. (Notice that although Grover Cleveland was President on two non-consecutive occasions, he is only counted once in the above set.) Sets can contain not only numbers, but also functions, geometric objects, and even other sets, and we may freely mix and match any of these types of objects in a given set.

If a set has infinitely many elements, and we want to list the elements of that set, what do we do? Obviously we can't write them all down. In most situations, we will be able to describe the elements of an infinite set by describing some common property that 1) objects in the set satisfy, and 2) objects in the set do not satisfy. For instance, perhaps S is the set of all positive integers which end in the digit 5. Then we may write $S = \{x | x \text{ is a positive integer ending in } 5\}$. In general, if $P(x)$ is some statement about the number x, we write $\{x | P(x)\}$ for the set of elements which make $P(x)$ true. If we want to initially restrict our attention to elements in a set X, we write $\{x \in X | P(x)\}$. For example, $\{x \in \mathbb{Z} | x > 0\}$ is the set of positive integers, while $\{x \in \mathbb{R} | x > 0\}$ is the set of positive real numbers.

We may want to want to assemble new sets from old sets. Let A, B be two sets. Then we write $A \cup B$ for the set consisting of all elements either in A or in B and call this the **union** of A and B. Similarly, we write $A \cap B$ for the set consisting of all elements in both A and B, and call this the **intersection** of A and B. For example, if $A = \{0, 1, 2\}$ and $B = \{1, 3\}$, then $A \cup B = \{0, 1, 2, 3\}$ while $A \cap B = \{1\}$. (Again, notice that although 1 is in A and B, it still only appears once in the set $A \cup B$.)