Math 104A, Number Theory, Fall 2002.
Summary of Lecture 1.

Lecturer's Introduction. Hi! I am not a specialist in number theory. I work in geometric analysis, predominantly in spectral geometry. For those of you who don't know what that is, I just want to take five minutes to tell you, so that you'll understand some of my comments during the course. The most famous question in spectral geometry is the question "*Can you hear the shape of a drum?*" What this means is the following. If someone blindfolds you and hits a strange shaped drum, can you tell what shape the drum is from the sound it makes? Actually the drum sound is composed of resonant notes of different pitches (frequencies). In a "mathematically perfect" drum, there is an infinite sequence of frequencies in the drum sound. The general question spectral geometers ask is the question "*what can you tell about the shape of a drum (or other object) from it's sequence of resonant frequencies?*.

Number Theory is the study of properties of numbers, in particular properties of the integers

$$\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots \quad .$$

For simple mathematical objects, the sequence of resonant frequencies are occasionally simple to write down. For example, the violin string of length π has resonant frequencies

$$1,\ 4,\ 9,\ 16,\ 25,\ \ldots \qquad .$$

A square drum of sidelength π has resonant frequencies of the form

$$a^2\ +\ b^2 \qquad\qquad \text{for } a \text{ and } b \text{ integers,}$$

and a cube of sidelength π has resonant frequencies of the form

$$a^2\ +\ b^2\ +\ c^2 \qquad\qquad \text{for } a,\ b \text{ and } c \text{ integers.}$$

Number theory has powerful methods to understand in great detail these very special sets of numbers. In spectral geometry we are interested in the sets of numbers which arise as frequencies. My purpose in teaching this course is to gain a deeper understanding of the methods of number theory to help me solve certain more general problems in spectral geometry. This means I am a bit biased as to the topics we should cover this year. I am more interested in the pure theory than the applications such as cryptography. However, since these applications are so important, we will certainly cover them this quarter. Towards the end of the quarter we will discuss next quarter's syllabus.

What sort of questions are studied in number theory?

The operations/relations we have on the integers:

$$+, \quad -, \quad \times, \quad =, \quad <, \quad >,$$

This quarter we will mainly discuss **questions concerning divisibility.**

Definition. The integer a divides the integer b (write $a|b$) if there exists an integer c such that $b = ac$.

(we gave some examples)

Definition. The integer $p > 1$ is prime, if the only positive divisors of p are 1 and p. Otherwise p is said to be composite.

(we gave some examples)

Every positive number can be decomposed as a product of primes, so primes are the basic building blocks.

There are infinitely many primes, but nobody has ever written down an explicit function which lists infinitely many. The number of primes less than n is denoted by $\pi(n)$. The prime number theorem asserts that

$$\pi(n) \sim \frac{n}{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}} \left(\sim \frac{n}{\log n}\right), \qquad \text{as } n \to \infty.$$

This is proved using the *Riemann zeta function*

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$$

In spectral geometry we understand quite a lot about the more general function obtained by replacing the numbers 1, 2, 3, ... by the resonant frequencies of any object. We won't discuss $\zeta(s)$ this quarter.

Testing whether numbers are prime and factoring numbers into primes using the computer are important problems which we will discuss. It was recently shown by three students in India (M. Agrawal, N. Kayal and N. Saxena) that you can test whether a number n is prime by doing on the order of $(\log n)^{12}$ computations. This is a big breakthrough. However, the fact that we don't know how to *factor* large numbers in a realistic amount of time is the basis for widely used coding systems.

Next quarter we will also study **questions involving addition**. Examples of such questions are
1. What are the pythagorean triples - that is positive integers a, b, c with $a^2 + b^2 = c^2$? (This was understood by the Greeks. You will find out the answer in this week's homework, although we won't show this gives all the solutions until next quarter.)
What are the integer solutions of $a^n + b^n = c^n$ with $n > 2$? (Fermat's last theorem proved by Wiles says they are all trivial - that is $a = 0$ or $b = 0$. The proof is lengthy.)
2. Which numbers can be written
a). as a sum of squares of two integers $x^2 + y^2$? (We'll answer this next quarter.)
b). as a sum of squares of three integers $x^2 + y^2 + z^2$? (You could write a computer program to discover this.)
c). as a combination of squares of the form $x^2 + 5y^2$? (You can find this out by reading Chapter 1!)
d). as a sum of two primes? (Goldbach's conjecture says that any even number can be.)

Mathematical induction.

We showed that the sum of the first n odd numbers is n^2:

$$1 + 3 + 5 + \ldots + (2n-1) = n^2.$$

We showed using the principle of mathematical induction that $n^2 < 2^n$ for $n \geq 5$.