

18.785: Analytic Number Theory, MIT, spring 2006 (K.S. Kedlaya)
Introduction to the course

Welcome to 18.785! This course is meant to be an introduction to analytic number theory; this handout provides an overview of what we will be talking about in the course. It also fixes some notation that I'll be using throughout.

1 An overview of the course

The fundamental questions in analytic number theory, and the ones which we focus on in this course, concern the interplay between the additive and multiplicative structures on the integers. Specifically, it is quite natural to ask questions of an additive nature about constructions which are intrinsically multiplicative. In rare cases, these questions lead us to interesting algebraic structures; for instance, the fact (due to Fermat) that every prime $p \equiv 1 \pmod{4}$ can be written uniquely as the sum of two squares leads to the study of the ring of Gaussian integers, and the fact (due to Lagrange) that every positive integer can be written as the sum of four squares ties in nicely to quaternions. However, most additive questions about multiplicative structures admit insufficiently useful algebraic structure; for instance, one cannot use algebraic techniques alone to determine which primes can be written as the sum of two cubes.

We thus turn instead to techniques from analysis; that is, we apply *continuous* techniques to study *discrete* phenomena. This tends to be most successful when proving *average* statements; for instance, one cannot give an exact formula for the number of primes in an interval $[1, x]$, but we can establish an *asymptotic* formula, and give some upper bounds for the discrepancy between the exact and asymptotic formulas.

Although this methodology turns out to be unexpectedly powerful, we must remain humbled by the fact that it is comically easy to pose open and probably extremely hard questions about prime numbers, including the following old chestnuts.

- (Twin primes problem) Are there infinitely many pairs of consecutive primes which differ by 2?
- (Sophie Germain problem) Are there infinitely many pairs of primes p, q such that $q = 2p - 1$?
- (Goldbach problem) Is every even integer $n > 2$ equal to the sum of two primes?

2 Basic structure of the course

In the first part of the course, our use of analysis will mainly involve the theory of complex functions, specifically the notions of analytic (holomorphic) and meromorphic functions. (One can argue that one is really using properties of *real harmonic* functions, since the real and imaginary parts of a holomorphic function have that property, and in other situations

one gets number-theoretic information by considering harmonic functions in a setting where there is no complex structure. Indeed, there is a lot of research in this direction to back up this point of view, but I am completely unqualified to talk about it!

In the second part of the course, we will draw on a second set of ideas, related to the notion of *sieving*. I will give an appropriate introduction to that idea in due course; in the interim, you should have in mind the Sieve of Eratosthenes as a technique for isolating the primes among all positive integers. You may also keep in mind the target application: the Bombieri-Vinogradov theorem, which gives a quantitative statement to the effect that if one looks at all of the arithmetic progressions of a single modulus which contain any primes at all, then the primes tend to distribute themselves uniformly among these.

In the third part of the course, we will prove a very explicit theorem about the distribution of primes, due to Goldston, Pintz, and Yıldırım (sic) from 2005. It states the following: if p_n denotes the n -th prime, then

$$\inf_n \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

The proof combines the Bombieri-Vinogradov theorem, from the second part of the course, with some estimates on divisor sums using techniques of complex analysis, as in the first part.

If there is time for a fourth part (which I expect there will be), we will consider some classes of “nonabelian” L -functions, and see how to use analyticity properties of these L -functions (which I will not be proving, as they are much deeper than anything I plan to discuss) to prove some equidistribution results in the spirit of Dirichlet’s theorem. One class of examples is the Artin L -functions, leading to the Chebotarev density theorem: for L a number field which is Galois over \mathbb{Q} with Galois group G , this theorem predicts (among other things) the density of primes p for which the prime ideal (p) in \mathbb{Z} factors in a given way in the ring of integers of L . A second class of examples is the L -functions associated to elliptic curves, leading to the Sato-Tate conjecture: for E an elliptic curve over \mathbb{Q} , this theorem predicts the distribution of the number of points on the reduction of E modulo p , as the prime p varies. (The latter is the subject of a recent breakthrough by Clozel, Harris, and Taylor.)

3 Notations

I want to try to keep my notation consistent throughout the semester. Here are a few conventions I have in mind; I may add more later.

Basics

Throughout this course, \mathbb{N} denotes the set of *positive* integers. Whether \mathbb{N} should include 0 is a matter of some controversy, but in this course it will be more convenient to omit 0. I might write \mathbb{N}_0 for the nonnegative integers.

We reserve the letter p for a prime number, and a sum or product over p without further explanation means p runs over all prime numbers. (If a condition is imposed, like $p \equiv 1 \pmod{4}$, instead take all primes obeying that condition.)

Asymptotics

Suppose we are interested in limiting behavior of some functions of x as x tends to some limit. (If otherwise unspecified we will mean $x \rightarrow \infty$, but it should be clear from context.) We write $f(x) \sim g(x)$ to mean that $\lim f(x)/g(x) = 1$. We write $O(f(x))$ to denote any function $g(x)$ such that $\limsup g(x)/f(x) < \infty$. We write $o(f(x))$ to denote any function $g(x)$ such that $\limsup g(x)/f(x) = 0$.

Beware that sometimes we talk about limiting behavior in one variable of functions that also depend on other variables. Unless otherwise specified, you should assume the limits are *not* uniform in the other variables. When they are, I will make that more clear.

Miscellaneous

It may happen sometimes during a proof that there are a number of auxiliary constants whose values I don't care about. I may use a single letter (like c) to refer to every such constant; if I do this, I'll make this abundantly clear beforehand.