Math 229: Introduction to Analytic Number Theory

What is analytic number theory?

One may reasonably define analytic number theory as the branch of mathematics that uses analytical techniques to address number-theoretical problems. But this "definition", while correct, is scarcely more informative than the phrase it purports to define. (See [Wilf 1982].) What kind of problems are suited to "analytical techniques"? What kind of mathematical techniques will be used? What style of mathematics is this, and what will its study teach you beyond the statements of theorems and their proofs? The next few sections briefly answer these questions.

The problems of analytic number theory. The typical problem of analytic number theory is an enumerative problem involving primes, Diophantine equations, or similar number-theoretic objects, and usually concerns what happens for large values of some parameter. Such problems are of long-standing intrinsic interest, and the answers that analytic number theory provides often have uses in mathematics (see below) or related disciplines (notably in various algorithmic aspects of primes and prime factorization, including applications to cryptography). Examples of problems that we shall address are:

- How many 100-digit primes are there, and how many of these have the last digit 7? More generally, how do the prime-counting functions $\pi(x)$ and $\pi(x, a \bmod q)$ behave for large x? [For the 100-digit problems we need $\pi(10^{100}) - \pi(10^{99})$ and $\pi(10^{100}, 7 \bmod 10) - \pi(10^{99}, 7 \bmod 10)$.]
- Given a prime $p > 0$, a nonzero $c \bmod p$, and integers a_1, b_1, a_2, b_2 with $a_i < b_i$, how many pairs (x_1, x_2) of integers are there such that $a_i < x_i < b_i$ $(i = 1, 2)$ and $x_1 x_2 \equiv c \bmod p$? For how small an H can we guarantee that if $b_i - a_i > H$ then there is at least one such pair?
- Is there an integer n such that the first eleven digits of $n!$ are 31415926535? Are there infinitely many such n? How many such n are there of at most 1000 digits?
- Given integers n, k, how many ways are there to represent n as a sum of k squares? For instance, how many integer solutions has the equation $a^b + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2 = 10^{100}$?

As often happens in mathematics, working on such down-to-earth questions quickly leads us to problems and objects that appear to belong to completely different mathematical disciplines:

- Analyze the Riemann zeta function $\zeta(s) := \sum_{n=1}^{\infty} 1/n^s$ and Dirichlet L-functions such as

$$L(s) := 1 - 3^{-s} - 7^{-s} + 9^{-s} + 11^{-s} - 13^{-s} - 17^{-s} + 19^{-s} + - - + \cdots$$

as functions of a *complex* variable s.

- Prove that the "Kloosterman sum"

$$K(p;a,b) := \sum_{x=1}^{p-1} \exp\left(\frac{2\pi i}{p}(ax + bx^{-1})\right)$$

(with x^{-1} being the inverse of x mod p) has absolute value at most $2\sqrt{p}$.

- Show that if a function $f : \mathbf{R} \to \mathbf{R}$ satisfies reasonable smoothness conditions then for large N the absolute value of the exponential sum

$$\sum_{n=1}^{N} \exp(if(n))$$

grows no faster than N^θ for some $\theta < 1$ (with θ depending on the conditions imposed on f).

- Investigate the coefficients of modular forms such as

$$\eta^8\eta_2^8 = q\prod_{n=1}^{\infty}(1-q^n)^8(1-q^{2n})^8 = q - 8q^2 + 12q^3 + 64q^4 - 210q^5 - 96q^6 \cdots.$$

Fortunately it will turn out that the route from (say) $\pi(x)$ to $\zeta(s)$ is not nearly as long and tortuous as that from $x^n + y^n = z^n$ to deformations of Galois representations... [1]

The techniques of analytic number theory. A hallmark of analytic number theory is the treatment of number-theoretical problems (usually enumerative, as noted above) by methods often relegated to the domain of "applied mathematics": elementary but clever manipulation of sums and integrals; asymptotic and error analysis; Fourier series and transforms; contour integrals and residues. While there is still good new work to be done along these lines, much contemporary analytic number theory also uses advanced tools from within and outside number theory (for instance, modular forms beyond the upper half-plane, Laplacian spectral theory). Nevertheless, in this introductory course we shall emphasize the classical methods characteristic of analytic number theory, on the grounds that they are rarely treated in this Department's courses, while our program already offers ample exposure to the algebraic/geometric tools. As already noted in the pseudo-syllabus, we shall on a few occasions invoke results that depend on deep (non-analytic) techniques, but we shall treat them as *deus ex mathematica*, developing only their analytic applications.

The style of analytic number theory. It has often been said that there are two kinds[2] of mathematicians: theory builders and problem solvers. In

[1] See for instance [Stevens 1994] and [Faltings 1995].

[2] Actually there are three kinds of mathematicians: those who can count, and those who cannot.

twentieth-century mathematics, these two styles are epitomized respectively by A. Grothendieck and P. Erdös. The Harvard math curriculum leans heavily towards the systematic, theory-building style; analytic number theory as usually practiced falls in the problem-solving camp. This is probably why, despite its illustrious history (Euclid, Euler, Riemann, Selberg, ...) and present-day vitality, analytic number theory has rarely been taught here — in the past quarter-century there have been only a handful of undergraduate seminars, research/Colloquium talks, and Catalog-listed courses. Now we shall see that there is more to analytic number theory than a bag of unrelated ad-hoc tricks, but it is true that partisans of contravariant functors, adèlic tangent sheaves, and étale cohomology will not find them in the present course. Still, even ardent structuralists can benefit from this course. First, specific results of analytic number theory often enter as necessary ingredients in the only known proofs of important structural results. Consider for example the arithmetic of elliptic curves: the many applications of Dirichlet's theorem on primes in arithmetic progression, and its generalization to Čebotarev's density theorem,[3] include the ground-breaking work of Kolyvagin and of Wiles and Taylor; in [Serre 1981] sieve methods are elegantly applied to the study of the distribution of traces of an elliptic curve;[4] in [Merel 1996] a result (Lemme 5) on the $x_1 x_2 \equiv c \bmod p$ problem is required to bound the torsion of elliptic curves over number fields. Second, the ideas and techniques apply widely. Sieve inequalities, for instance, are also used in probability theory to analyze nearly independent variables; the "stationary phase" methods for obtaining the asymptotic growth of the partition function are also used to estimate oscillatory integrals in enumerative combinatorics, quantum physics, special functions, and elsewhere; even the van der Corput estimates on exponential sums have found combinatorial application [CEP 1996]. Third, working on asymptotic results and error terms can be a healthy complement to the usual quest for exact answers that we might focus on too exclusively. Finally, An ambitious theory-builder should regard the absence thus far of a Grand Unified Theory of analytic number theory not as an insult but as a challenge. Both machinery- and problem-motivated mathematicians should note that some of the more exciting recent work in number theory depends critically on symbiosis between the two styles of mathematics. This course will introduce the main analytic techniques needed to appreciate, and ultimately to extend, this work.

References

[CEP 1996] Cohn, H., Elkies, N.D., Propp, J.: Local statistics for random domino tilings of the Aztec diamond, Duke Math J. **85** #1 (Oct.96), 117–166.

[3] We shall describe Čebotarev's theorem briefly in the course but not develop it in detail. Given Dirichlet's theorem and the asymptotic formula for $\pi(x, a \bmod q)$, the extra work needed to get Čebotarev is not analytic but algebraic: the development of algebraic number theory and the arithmetic of characters of finite groups. Thus a full treatment of Čebotarev does not alas belong in this course.

[4] My doctoral work on the case of trace zero (see for instance [Elkies 1987]) also used Dirichlet's theorem.

[Elkies 1987] Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.* **89** (1987), 561–567.

[Faltings 1995] Faltings, G.: The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles. *Notices of the AMS*, July 1995, 743–746 (translated by U.F. Mayer from *Testausdruck DMV Mitteilungen* **27**, 3/1995).

[Merel 1996] Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996), 437–449.

[Serre 1981] Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *IHES Publ. Math.* **54** (1981), 123–201.

[Stevens 1994] Stevens, G.: *Fermat's Last Theorem*, PROMYS T-shirt, Boston University 1994.

[Wilf 1982] Wilf, H.S.: What is an Answer? *Amer. Math. Monthly* **89** (1992), 289–292.