John Friedlander

Producing Prime Numbers via Sieve Methods (4 lectures)

1. Background on classical sieve theory and its limitations.

2. Parity-sensitive sieves.

3. Overview of the proof that there are infinitely many primes of the form $X^2 + Y^4$.

4. Continuation of 3: Details of some aspects of the proof.

Exponential Sums, Uniform Distribution and Cryptographic Applications (2 lectures)

5. Overview of some interrelations amongst the three areas mentioned in the title.

6. Detailed proofs of results.

Background

We shall try to be as self-contained as possible and for those in analytic number theory no preparation is necessary.

For others, one course each in elementary and analytic number theory is sufficient background. This may be from any of the standard texts, for example:

Niven and Zuckerman, *An Introduction to the Theory of Numbers* (Wiley) and one of

E. Bombieri, *Le Grand Crible dans la théorie analytique des nombres* (Astérisque)

H. Davenport, *Multiplicative Number Theory* (Springer)

A background in sieve theory is not necessary but for those with none at all a tiny bit would not be a bad idea, for example the first chapter of

G. Greaves, *Sieves in Number Theory* (Springer)

In cryptography no background will be assumed.

Roger Heath-Brown

Counting Rational Points on Algebraic Varieties

Overall Aims

These lectures will discuss the frequency of rational points on algebraic varieties, particularly hypersurfaces. In very concrete terms, let $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be a non-zero form, and define $N(B, F)$, for $B \geq 1$, as the number of essentially different solutions $F(x_1, \dots, x_n) = 0$ with integers $x_1, \dots, x_n$, not all zero, satisfying $\max |x_i| \leq B$. Here two solutions are regarded as being essentially the same if they are proportional to each other. The fundamental question is: *How does $N(B, F)$ behave, as $B \to \infty$?*

Many questions in number theory ask for upper bounds for $N(B, F)$, for particular forms F. Sometimes these are an end in their own right. Sometimes they are a key tool in establishing other results. Thus, in Waring's problem for example, upper bounds for the case

$$x_1^k + \dots + x_m^k - x_{m+1}^k - \dots - x_{2m}^k = 0, \quad (*)$$

can be used in proving asymptotic formulae for other representation functions.

The lectures will look both at methods for bounding $N(B, F)$, and at applications.

Detailed Synopsis

We will begin with a survey of examples, to illustrate the different ways that $N(B, F)$ can behave, and to describe what has been achieved in some of the 'classical' problems. We will then look at the main conjectures about $N(B, F)$.

The next task will be to examine the various methods which have been used to tackle such problems in the past. Some of the old methods are still very valuable, but others have been superseded — and it is interesting to see why.

We will then move to the central topic of the lecture series, which will be the method of Bombieri and Pila, as developed by the lecturer [3]. The fundamental theorem will be proved in full.

Since many of the applications relate to diagonal forms of the type $(*)$ we shall examine possible parameterizations of $(*)$ by both polynomials and elliptic functions. Finally, we will go on to handle questions concerning: equal sums of two powers, representations as a sum of three powers and representations by binary forms.

Prerequisites

The subject area lies on the interface between analytic number theory and algebraic geometry, and will be treated from the perspective of the analytic number theorist. Those whose background is primarily in geometry will need to be confident with the use of $O(\ldots)$, $\sim$ and $\ll$ notation, but apart from that no deep tools will be required. Chapter 18 of Hardy and Wright [1] provides suitable material. An understanding of the circle method, say Chapters 1 and 2 (and for the more dedicated, Chapters 4 and 9) of Vaughan's book [4], would be useful background for geometers to acquire, but not essential.

For those whose background is in analytic number theory, it will be necessary to handle some basic concepts from algebraic geometry: Projective space, Varieties, Dimension and Degree. The book by Harris [2] treats these at a sufficient level. While it will suffice to understand the statements of the key theorems, rather than the proofs, those attending will need to be happy with geometric language, which will be used throughout the lectures.

Finally, we shall use a little bit about p-adic numbers—in particular Hensel's lemma.

References

[1] G. Hardy and E.M. Wright, *The theory of numbers,* (Oxford University Press, Oxford, 1960).

[2] J. Harris, *Algebraic geometry,* (Springer, Berlin, 1995).

[3] D.R. Heath-Brown, The Density of Rational Points on Curves and Surfaces, *Ann. Math.,* (to appear).

[4] R.C. Vaughan, *The Hardy-Littlewood method*, Cambridge tracts in mathematics, 125 (Cambridge University Press, Cambridge, 1981).

Henryk Iwaniec

Automorphic L-Functions

These lectures intend to present basic facts from analytic theory of L-functions associated with automorphic forms, and to give detailed surveys of current research as well as the modern techniques. I will assume some familiarity with automorphic forms and analytic number theory, nevertheless I try to make these lectures to be accessible for non-experts. Here are selected topics:

1. Automorphic forms (overview) – holomorphic forms – Maass cusp forms – Hecke operators – spectral theory – summation formulas

2. L-functions (overview) – Dirichlet – Hecke – Artin – Rankin-Selberg – the symmetric powers – triple products

3. The functional equation and the explicit formula

4. Subconvexity bounds with applications – amplification methods – the equidistribution on sphere – unique ergodicity conjecture

5. Zeros of families of L-functions – mollification methods – central values of L-functions – low lying zeros

6. The class number problem – the exceptional zero – subnormal spacing of zeros – L-functions of elliptic curves

For the beginners I would recommend to look up before the lectures the following publications:

H.Iwaniec, *Topics in Classical Automorphic Forms*, Grad.Stud.in Math. vol.17, AMS 1997.

P.Sarnak, *Some Applications of Modular Forms*, Cambridge University Press 1990.

J.H.Silverman, *The Arithmetic of Elliptic Curves*, Springer 1985.

N.V.Katz and P.Sarnak, *Zeros of L-functions and symmetry*, Bull. AMS 36 (1999), 1-26.

H.Iwaniec and P.Sarnak, *Perspectives on the analytic theory of L-functions*; in Visions in Mathematics Towards 2000, Part II, pp.705-741, Birkhauser, Basel 2000.

Jerzy Kaczorowski

Axiomatic Theory of L-Functions: the Selberg Class

1. Motivations, basic definitions and examples.
2. Functional equations, transformation of gamma factors, invariants.
3. Conjectures and their consequences.
4. Structure theorems in degree ≤ 1.
5. Structure theorems in degree $1 < d < 2$.
6. Prime number theorems, limiting distributions and general race problem.

For analytic number theorists no preparation is necessary. Beginners should be familiar with some basic examples of L-functions.