Lecture Notes in Mathematics

J. B. Friedlander
D. R. Heath-Brown
H. Iwaniec
J. Kaczorowski

Analytic Number Theory

1891

Cetraro, Italy 2002

Editors: A. Perelli, C. Viola

Springer

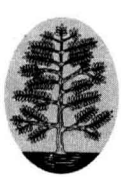
Fondazione C.I.M.E.

J.B. Friedlander · D.R. Heath-Brown
H. Iwaniec · J. Kaczorowski

Analytic Number Theory

Lectures given at the
C.I.M.E. Summer School
held in Cetraro, Italy,
July 11–18, 2002

Editors: A. Perelli, C. Viola



Springer

Fondazione
C.I.M.E.

Authors and Editors

J.B. Friedlander
Department of Mathematics
University of Toronto
40 St George street
Toronto, ON M5S 2E4
Canada
e-mail: frdlndr@math.toronto.edu

D.R. Heath-Brown
Mathematical Institute
University of Oxford
24-29 St Giles
Oxford OX1 3LB
England
e-mail: rhb@maths.ox.ac.uk

H. Iwaniec
Department of Mathematics
Rutgers University
110 Frelinghuysen road
Piscataway, NJ 08854
USA
e-mail: iwaniec@math.rutgers.edu

J. Kaczorowski
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
ul. Umultowska 87
61-614 Poznan
Poland
e-mail: kjerzy@amu.edu.pl

Alberto Perelli
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
16146 Genova
Italy
e-mail: perelli@dima.unige.it

Carlo Viola
Dipartimento di Matematica
Università di Pisa
Largo Pontecorvo 5
56127 Pisa
Italy
e-mail: viola@dm.unipi.it

Library of Congress Control Number: 2006930414

Mathematics Subject Classification (2000): 11D45, 11G35, 11M06, 11M20, 11M36, 11M41, 11N13, 11N32, 11N35, 14G05

ISSN print edition: 0075-8434
ISSN electronic edition: 1617-9692
ISBN-10 3-540-36363-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-36363-7 Springer Berlin Heidelberg New York

DOI 10.1007/3-540-36363-7

Typesetting by the authors and SPi using a Springer LaTeX package
Cover design: WMXDesign GmbH, Heidelberg

Printed on acid-free paper SPIN: 11795704 41/SPi 5 4 3 2 1 0

Preface

The origins of analytic number theory, i.e. of the study of arithmetical problems by analytic methods, can be traced back to Euler's 1737 proof of the divergence of the series $\sum 1/p$ where p runs through all prime numbers, a simple, yet powerful, combination of arithmetic and analysis. One century later, during the years 1837-40, Dirichlet produced a major development in prime number theory by extending Euler's result to primes p in an arithmetic progression, $p \equiv a \pmod{q}$ for any coprime integers a and q. To this end Dirichlet introduced group characters χ and L-functions, and obtained a key result, the non-vanishing of $L(1, \chi)$, through his celebrated formula on the number of equivalence classes of binary quadratic forms with a given discriminant.

The study of the distribution of prime numbers was deeply transformed in 1859 by the appearance of the famous nine pages long paper by Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, where the author introduced the revolutionary ideas of studying the zeta-function $\zeta(s) = \sum_1^\infty n^{-s}$ (and hence, implicitly, also the Dirichlet L-functions) as an analytic function of the complex variable s satisfying a suitable functional equation, and of relating the distribution of prime numbers with the distribution of zeros of $\zeta(s)$. Riemann considered it highly probable ("sehr wahrscheinlich") that the complex zeros of $\zeta(s)$ all have real part $\frac{1}{2}$. This still unproved statement is the celebrated Riemann Hypothesis, and the analogue for all Dirichlet L-functions is known as the Grand Riemann Hypothesis. Several crucial results were obtained in the following decades along the way opened by Riemann, in particular the Prime Number Theorem which had been conjectured by Legendre and Gauss and was proved in 1896 by Hadamard and de la Vallée Poussin independently.

During the twentieth century, research subjects and technical tools of analytic number theory had an astonishing evolution. Besides complex function theory and Fourier analysis, which are indispensable instruments in prime number theory since Riemann's 1859 paper, among the main tools and

contributions to analytic number theory developed in the course of last century one should mention at least the circle method introduced by Hardy, Littlewood and Ramanujan in the 1920's, and later improved by Vinogradov and by Kloosterman, as an analytic technique for the study of diophantine equations and of additive problems over primes or over special integer sequences, the sieve methods of Brun and Selberg, subsequently developed by Bombieri, Iwaniec and others, the large sieve introduced by Linnik and substantially modified and improved by Bombieri, the estimations of exponential sums due to Weyl, van der Corput and Vinogradov, and the theory of modular forms and automorphic L-functions.

The great vitality of the current research in all these areas suggested our proposal for a C.I.M.E. session on analytic number theory, which was held at Cetraro (Cosenza, Italy) from July 11 to July 18, 2002. The session consisted of four six-hours courses given by Professors J. B. Friedlander (Toronto), D. R. Heath-Brown (Oxford), H. Iwaniec (Rutgers) and J. Kaczorowski (Poznań). The lectures were attended by fifty-nine participants from several countries, both graduate students and senior mathematicians. The expanded lecture notes of the four courses are presented in this volume.

The main aim of Friedlander's notes is to introduce the reader to the recent developments of sieve theory leading to prime-producing sieves. The first part of the paper contains an account of the classical sieve methods of Brun, Selberg, Bombieri and Iwaniec. The second part deals with the outstanding recent achievements of sieve theory, leading to an asymptotic formula for the number of primes in certain thin sequences, such as the values of two-variables polynomials of type $x^2 + y^4$ or $x^3 + 2y^3$. In particular, the author gives an overview of the proof of the asymptotic formula for the number of primes represented by the polynomial $x^2 + y^4$. Such an overview clearly shows the role of bilinear forms, a new basic ingredient in such sieves.

Heath-Brown's lectures deal with integer solutions to Diophantine equations of type $F(x_1, \ldots, x_n) = 0$ with absolutely irreducible polynomials $F \in \mathbb{Z}[x_1, \ldots, x_n]$. The main goal here is to count such solutions, and in particular to find bounds for the number of solutions in large regions of type $|x_i| \leqslant B$. The paper begins with several classical examples, with the relevant problems for curves, surfaces and higher dimensional varieties, and with a survey of many results and conjectures. The bulk of the paper deals with the proofs of the main theorems where several tools are employed, including results from algebraic geometry and from the geometry of numbers. In the final part, applications to power-free values of polynomials and to sums of powers are given.

The main focus of Iwaniec's paper is on the exceptional Dirichlet character. It is well known that exceptional characters and exceptional zeros play a relevant role in various applications of the L-functions. The paper begins with a survey of the classical material, presenting several applications to the class number problem and to the distribution of primes. Recent results are then

outlined, dealing also with complex zeros on the critical line and with families of L-functions. The last section deals with Linnik's celebrated theorem on the least prime in an arithmetic progression, which uses many properties of the exceptional zero. However, here the point of view is rather different from Linnik's original approach. In fact, a new proof of Linnik's result based on sieve methods is given, with only a moderate use of L-functions.

Kaczorowski's lectures present a survey of the axiomatic class S of L-functions introduced by Selberg. Essentially, the main aim of the Selberg class theory is to prove that such an axiomatic class coincides with the class of automorphic L-functions. Although the theory is rich in interesting conjectures, the focus of these lecture notes is mainly on unconditional results. After a chapter on classical examples of L-functions and one on the basic theory, the notes present an account of the invariant theory for S. The core of the theory begins with chapter 4, where the necessary material on hypergeometric functions is collected. Such results are applied in the following chapters, thus obtaining information on the linear and non-linear twists which, in turn, yield a complete characterization of the degree 1 functions and the non-existence of functions with degree between 1 and 5/3.

We are pleased to express our warmest thanks to the authors for accepting our invitation to the C.I.M.E. session, and for agreeing to write the fine papers collected in this volume.

Alberto Perelli Carlo Viola

Contents

Producing Prime Numbers via Sieve Methods

John B. Friedlander

Department of Mathematics, University of Toronto
40 St George street, Toronto, ON M5S 2E4, Canada
e-mail: frdlndr@math.toronto.edu

These notes represent an expanded version of the lectures on sieve methods which were delivered at the C.I.M.E. summer school in analytic number theory in Cetraro, Italy during the period July 11 to July 18, 2002. As such they are produced here in the same informal style and with the same goals as were those lectures.

The basic purpose for which the sieve was invented was the successful estimation of the number of primes in interesting integer sequences. Despite some intermittent doubts that this could ever be achieved, the objective has in recent years finally been reached in certain cases. One main goal of these lectures was to provide an introduction to these developments. Such an introduction would not have been appropriate to many in the target audience without some of the relevant background and a second objective was the provision during the first half of the lectures of a quick examination of the development of sieve methods during the past century and of the main ideas involved therein. As a result of these twin goals, the second half of the material is necessarily a little more technical than is the first part. It is hoped that these notes will provide a good starting point for graduate students interested in learning about sieve methods who will then go on to a more detailed study, for example [Gr, HR], and also for mathematicians who are not experts on the sieve but who want a speedy and relatively painless introduction to its workings. In both groups it is intended to develop a rough feeling for what the sieve is and for what it can and cannot do.

The sieve has over the years come to encompass an extensively developed body of work and the goals of these notes do not include any intention to give a treatment which is at all exhaustive, wherein one can see complete proofs, nor even to provide a reference from which one can quote precise statements of the main theorems. For those purposes the references provided are more than sufficient.

Acknowledgements

Over the past thirty years the author has had on many occasions the opportunity to discuss the topic of sieve methods with many colleagues, in particular with A. Selberg, E. Bombieri, and most frequently of all with H. Iwaniec. Indeed the current notes, together with the lecture notes [Iw5], form the starting points for a book on the subject which Iwaniec and I have begun to write. After years of extensive collaborations one cannot help but include thoughts which originated with the other person; indeed one cannot always remember which those were.

During the preparation of this work the author has received the generous support of the Canada Council for the Arts through a Killam Research Fellowship and also from the Natural Sciences and Engineering Research Council of Canada through Research Grant A5123.

1 "Classical" sieve methods

Eratosthenes

The sieve begins with Eratosthenes. We let x be a positive integer and

$$\mathcal{A} = \{n \leqslant x\},$$

the set of integers up to x. We are going to count the number of primes in this set.

For purposes of illustration let us choose $x = 30$. Thus we begin with the integers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

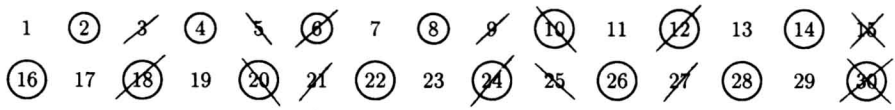
and from these we are going to delete the ones that are composite, counting the number that remain. Our first step is to cross out those that are even, the multiples of two. This leaves with the following picture.

1	(2)	3	(4)	5	(6)	7	(8)	9	(10)	11	(12)	13	(14)	15
(16)	17	(18)	19	(20)	21	(22)	23	(24)	25	(26)	27	(28)	29	(30)

Turning to the next prime, three, we cross out all of its multiples. This leaves us with the following.

1	(2)	~~3~~	(4)	5	~~(6)~~	7	(8)	~~9~~	(10)	11	~~(12)~~	13	(14)	~~15~~
(16)	17	~~(18)~~	19	(20)	~~21~~	(22)	23	~~(24)~~	25	(26)	~~27~~	(28)	29	~~(30)~~

Note that there are some numbers, namely the multiples of six, which have been crossed out twice. If we are keeping a count of what has been left behind we should really add these back in once. Next we progress to the next prime number, five, and delete the multiples of that one. This gives us the following picture.



Here again we find more numbers, the multiples of ten and of fifteen, that have been removed twice and so should be added back in once to rectify the count. But now we have even come to a number, thirty, which has been crossed out as a multiple of each of three primes. In this case, it has been crossed out three times (once each as a multiple of two, three and five), then added back in three times (once each as a multiple of six, ten and fifteen). Since thirty is composite we want to remove it precisely once so we have now to subtract it out one more time.

We are now ready to proceed to the multiples of the next prime, seven. However, before we do so it is a very good idea to notice that all of the remaining numbers on our list, apart from the integer one, are themselves prime numbers. This is a consequence of the fact that every composite positive integer must be divisible by some number (and hence some prime number) which is no larger than its square root. In our case all of the numbers are less than or equal to thirty and hence we only need to cross out multiples of primes $p \leqslant \sqrt{30}$ and five is the largest such prime. As a result we are ready to stop this procedure.

Let's think about what we have accomplished. On the one hand, totalling up the results of the count of our inclusion–exclusion, we began (in the case $x = 30$) with $[x]$ integers, for each prime $p \leqslant \sqrt{x}$ we subtracted out $[x/p]$ multiples of p, then for each pair of distinct primes $p_1 < p_2 \leqslant \sqrt{x}$ we added back in the $[x/p_1p_2]$ multiples of p_1p_2, and so on. In all, we are left with the final count

$$[x] - \sum_{p \leqslant \sqrt{x}} \left[\frac{x}{p}\right] + \sum\sum_{p_1 < p_2 \leqslant \sqrt{x}} \left[\frac{x}{p_1\, p_2}\right] - \sum\sum\sum_{p_1 < p_2 < p_3 \leqslant \sqrt{x}} \left[\frac{x}{p_1\, p_2\, p_3}\right] + - \cdots$$

On the other hand, this was after all just the count for the number of integers not crossed out and these integers are just the primes less than or equal to x, other than those which are less than or equal to $\sqrt{x}$, together with the integer one.

Equating the two we obtain the

Legendre Formula

$$\pi(x) - \pi(\sqrt{x}\,) + 1 = \sum_{\substack{d \\ p|d \Rightarrow p \leqslant \sqrt{x}}} \mu(d) \left[\frac{x}{d}\right].$$

Here, as usual, $\pi(x)$ denotes the prime counting function

$$\pi(x) = \sum_{p \leqslant x} 1,$$

and, throughout, the letter p will always be a prime. As usual, the Möbius function $\mu(d)$ is $(-1)^\nu$ when d is the product of $\nu \geqslant 0$ distinct primes and is zero if d has a repeated prime factor. This function provides a concise way of expressing the right hand side of the formula.

It will turn out that $\pi(x)$ is considerably larger than $\sqrt{x}$, hence (since trivially $\pi(\sqrt{x}\,) \leqslant \sqrt{x}\,$) the left side of the Legendre formula is approximately $\pi(x)$. In order to estimate $\pi(x)$ we thus want to develop the right side.

The obvious starting point for an estimation of the right hand side is the replacement everywhere of the awkward function $[t]$, the integral part of t, by the simpler function t. This makes an error of $\{t\}$, the fractional part. More precisely, we have

$$\text{right side} = x \sum_d \frac{\mu(d)}{d} + E = x \prod_{p \leqslant \sqrt{x}} \left(1 - \frac{1}{p}\right) + E$$

where the error term E is

$$E = -\sum_d \mu(d) \left\{\frac{x}{d}\right\}.$$

At first glance, the best we can expect to do is to use the trivial bound $\{t\} < 1$ which leads us to bound the error term by

$$|E| \leqslant \sum_d 1 = 2^{\pi(\sqrt{x}\,)},$$

which is absolutely enormous, much larger even than the number of integers $[x]$ that we started with. Of course, we have been particularly stupid here, for example, sieving out multiples of d even for certain integers d exceeding x, so the above bound can certainly be improved somewhat. Unfortunately however, E is genuinely large. In fact, using old ideas due to Chebyshev and to Mertens, one knows that

$$\prod_{p \leqslant \sqrt{x}} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log \sqrt{x}}$$

so what we have been expecting to be our main term is actually wrong. Since, by the prime number theorem,

$$\pi(x) \sim \frac{x}{\log x},$$

we see that the quantity E we have been referring to as the error term has the same order of magnitude as the main term.

Brun

The sieve of Eratosthenes lay in such a state, virtually untouched for almost two thousand years. The modern subject of sieve methods really begins with Viggo Brun. Although he later developed significant refinements to what we shall describe here, Brun's first attempts to make the error term more manageable were based on the following quite simple ideas.

Although one cannot greatly improve the trivial bound in the error term for each individual d on the right side, one can try to cut down on the number of terms in the sum. One way to do this is to cut the process off earlier, sifting out multiples of primes only up to some chosen z which is smaller than $\sqrt{x}$. Moreover, re-examining the inclusion–exclusion procedure and truncating this, we see that, if we truncate after d with a specified even number of prime factors, say $\nu(d) = 2r$, we get an upper bound, while if we truncate after an odd number $\nu(d) = 2r + 1$, we get a lower bound.

Although not an asymptotic formula, such bounds can be valuable. For example, an upper bound will, a fortiori, provide an upper bound for $\pi(x) - \pi(z)$ and hence (when combined with the trivial bound $\pi(z) \leqslant z$) an upper bound for $\pi(x)$. A positive lower bound will demonstrate the existence of integers without any small prime factors, and hence with few prime factors (the latter are referred to as "almost-primes"). Thus for example, an integer $n \leqslant x$ having no prime factor $p \leqslant x^{1/4}$ can have at most three prime factors.

Some Generality

So far we are in the rather depressing position that we have a method which fails to give us good estimates for the number $\pi(x)$ of primes up to x, but even worse, the only reason we even know that it is doomed to fail is because other techniques, from analytic number theory, succeed (to prove the prime number theorem), thereby telling us so. What then is the value of the sieve is that it can be generalized to give some information in cases where the analytic machinery is lacking. Therefore, to consider the situation more generally is not merely worthwhile; it is the sieve's only raison d'être.

We consider a finite sequence of non-negative reals

$$\mathcal{A} = (a_n), \quad n \leqslant x,$$

and a set $\mathcal{P}$ of primes. It is convenient to denote

$$P(z) = \prod_{\substack{p\in\mathcal{P}\\ p<z}} p.$$

Our goal is to estimate the "sifting function"

$$S(\mathcal{A}, z) = \sum_{\substack{n\leqslant x\\ (n,P(z))=1}} a_n.$$

We proceed just as in our original example, but phrased in slightly different fashion. We need the basic property of the Möbius function

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1,\\ 0 & \text{if } n > 1. \end{cases}$$

We also use the simple fact from elementary number theory that $\delta|a$, $\delta|b \iff \delta|(a,b)$, that is, the set of common divisors of two positive integers is just the same as the set of divisors of their greatest common divisor.

Inserting these two facts and then interchanging the order of summation we obtain

$$\begin{aligned} S(\mathcal{A}, z) &= \sum_n a_n \sum_{d|(n,P(z))} \mu(d) = \sum_n a_n \sum_{\substack{d|n\\ d|P(z)}} \mu(d)\\ &= \sum_{d|P(z)} \mu(d) \sum_{n\equiv 0 \,(\mathrm{mod}\, d)} a_n = \sum_{d|P(z)} \mu(d) A_d(x), \end{aligned}$$

say. This is just (a more general version of) the Legendre formula and here as before we need information about the sums

$$A_d(x) = \sum_{\substack{n\leqslant x\\ n\equiv 0\,(d)}} a_n$$

which give the mass of the subsequence running over multiples of d, that is $\mathcal{A}_d = (a_{md})$, $m \leqslant x/d$, and which in our beginning example was $[x/d]$. Specifically, we need a useful approximation formula. We assume we can write this in the form

$$(*) \qquad A_d(x) = A(x)g(d) + r_d(x),$$

where

$$A(x) = A_1(x) = \sum_{n\leqslant x} a_n$$

is the total mass of our sequence, where $g(d)$ is a "nice" function (equal to $1/d$ in our example) and $r_d(x)$ is a "remainder" which is small, at least on average over d (this was $-\{x/d\}$ in our example). Inserting our approximation formula $(*)$ the sifting function becomes

$$S(\mathcal{A}, z) = A(x) \sum_{d|P(z)} \mu(d)g(d) + \sum_{d|P(z)} \mu(d)r_d(x)$$

which is basic to all that follows. The function $g(d)$ behaves like a probability in a number of respects, describing approximately the fraction of the total mass coming from multiples of d. (It is useful to keep in mind $g(d) = 1/d$ as the prototype for such a function.) Hence, we shall assume $g(1) = 1$ and that, for each $d > 1$, we have $0 \leqslant g(d) < 1$. If for some $d > 1$ we had $g(d) = 1$ virtually everything would be a multiple of d and there would not be much point in looking for primes. We also assume that g is a multiplicative function, that is whenever $(d_1, d_2) = 1$ we have

$$g(d_1 d_2) = g(d_1)g(d_2).$$

The essence of this is that we are assuming that divisibility by two relatively prime integers are independent events. In practice this is true only to a rather limited extent and this fact is in large measure responsible for the failure of the method to do better.

Some Examples

We consider some examples. In many of the most basic examples the sequence $\mathcal{A}$ is just the characteristic function of an interesting set of integers. In such a case we shall sometimes abuse notation by failing to distinguish between the function and the set on which it is supported.

Example 1 We begin by repeating once again our original example. Thus, we have

$$\mathcal{A} = \{m \mid m \leqslant x\}, \qquad \mathcal{P} = \{\text{all primes}\},$$

$$A_d(x) = \left[\frac{x}{d}\right] = \frac{x}{d} - \left\{\frac{x}{d}\right\},$$

$$g(d) = \frac{1}{d}, \qquad r_d(x) = -\left\{\frac{x}{d}\right\}.$$

Example 2 Now for something a little different, consider

$$\mathcal{A} = \{m^2 + 1 \leqslant x\}, \qquad \mathcal{P} = \{p,\ p \not\equiv 3 \pmod 4\},$$

$$g(p) = \begin{cases} 2/p & p \equiv 1 \pmod 4 \\ 1/2 & p = 2, \end{cases} \qquad |r_d| \leqslant 2^{\nu(d)},$$

this last estimate following from the bound $|r_p| \leqslant 2$ and the Chinese Remainder Theorem. Here, there is no need to sieve by the primes congruent to three modulo four since none of the integers in our set is divisible by any such prime (although we could, equivalently, sieve by the set of all primes and simply set $g(p) = 0$ for these additional primes). In this example if we were able to get a positive lower bound for $S(\mathcal{A}, \sqrt{x}\,)$ we would be producing primes of the form $m^2 + 1$. It is a famous problem to show that there are infinitely many such primes.

Example 3 For another famous conjecture, we consider the following example.

$$\mathcal{A} = \{m(m+2) \leqslant x\}, \qquad \mathcal{P} = \{\text{all primes}\},$$

$$g(p) = \begin{cases} 2/p & p \text{ odd} \\ 1/2 & p = 2, \end{cases} \qquad |r_d| \leqslant 2.$$

Here, if we could give a positive lower bound for $S\big(\mathcal{A}, x^{1/4}\big)$ we would be producing integers $m(m+2)$ where both factors are prime and differ by two. The "twin prime conjecture" predicts that there are infinitely many such pairs of primes.

Example 4 There is an alternative appraoch via the sieve to attack this last conjecture. As our fourth example we consider the following sequence.

$$\mathcal{A} = \{p - 2 \leqslant x\}, \qquad \mathcal{P} = \{\text{odd primes}\},$$

$$A_d(x) = \pi(x; d, 2),$$

$$g(p) = \frac{1}{p-1}, \qquad g(d) = \frac{1}{\varphi(d)},$$

where $\pi(x; d, a)$ is the number of primes up to x which are congruent to a modulo d and where $\varphi(d)$, the Euler function, counts the number of units in the ring of residue classes modulo d. This example offers some advantages over the previous one for studying the twin prime problem and at this point in time it gives stronger results, although this was not always the case. Most significantly, we are starting from the beginning with the knowledge that one of our two numbers p, $p-2$ is a prime. On the other hand, the remainder term is more complicated, namely $r_d(x) = \pi(x; d, 2) - \pi(x)/\varphi(d)$, and it is much more difficult to bound it successfully. In the current state of knowledge, a reasonably good bound can only be given on average over d; the most famous bound of this type being the celebrated Bombieri–Vinogradov theorem [Bo1]. Once again, if we could be successful in giving a positive lower bound, this time for $S(\mathcal{A}, \sqrt{x}\,)$, then we would produce twin primes.