An Introduction to Sieve Methods and Their Applications
Principles exist. We don’t create. We only discover them.

Vivekananda
Contents

Preface xi

1 Some basic notions 1
  1.1 The big ‘O’ and little ‘o’ notation 1
  1.2 The Möbius function 2
  1.3 The technique of partial summation 4
  1.4 Chebycheff’s theorem 5
  1.5 Exercises 10

2 Some elementary sieves 15
  2.1 Generalities 15
  2.2 The larger sieve 17
  2.3 The square sieve 21
  2.4 Sieving using Dirichlet series 25
  2.5 Exercises 27

3 The normal order method 32
  3.1 A theorem of Hardy and Ramanujan 32
  3.2 The normal number of prime divisors of a polynomial 35
  3.3 Prime estimates 38
  3.4 Application of the method to other sequences 40
  3.5 Exercises 43

4 The Turán sieve 47
  4.1 The basic inequality 47
  4.2 Counting irreducible polynomials in $\mathbb{F}_p[x]$ 49
  4.3 Counting irreducible polynomials in $\mathbb{Z}[x]$ 51
  4.4 Square values of polynomials 53

© in this web service Cambridge University Press www.cambridge.org
Contents

4.5 An application with Hilbert symbols 55
4.6 Exercises 58

5 The sieve of Eratosthenes 63
5.1 The sieve of Eratosthenes 63
5.2 Mertens’ theorem 65
5.3 Rankin’s trick and the function $\Psi(x, z)$ 68
5.4 The general sieve of Eratosthenes and applications 70
5.5 Exercises 74

6 Brun’s sieve 80
6.1 Brun’s pure sieve 81
6.2 Brun’s main theorem 87
6.3 Schnirelman’s theorem 100
6.4 A theorem of Romanoff 106
6.5 Exercises 108

7 Selberg’s sieve 113
7.1 Chebycheff’s theorem revisited 113
7.2 Selberg’s sieve 118
7.3 The Brun–Titchmarsh theorem and applications 124
7.4 Exercises 130

8 The large sieve 135
8.1 The large sieve inequality 136
8.2 The large sieve 139
8.3 Weighted sums of Dirichlet characters 142
8.4 An average result 147
8.5 Exercises 151

9 The Bombieri–Vinogradov theorem 156
9.1 A general theorem 157
9.2 The Bombieri–Vinogradov theorem 167
9.3 The Titchmarsh divisor problem 172
9.4 Exercises 174

10 The lower bound sieve 177
10.1 The lower bound sieve 177
10.2 Twin primes 185
10.3 Quantitative results and variations 193
Contents

10.4 Application to primitive roots 195
10.5 Exercises 199

11 New directions in sieve theory 201
11.1 A duality principle 201
11.2 A general formalism 205
11.3 Linnik’s problem for elliptic curves 207
11.4 Linnik’s problem for cusp forms 209
11.5 The large sieve inequality on GL(n) 213
11.6 Exercises 216

References 218

Index 222
Preface

It is now nearly 100 years since the birth of modern sieve theory. The theory has had a remarkable development and has emerged as a powerful tool, not only in number theory, but in other branches of mathematics, as well. Until 20 years ago, three sieve methods, namely Brun’s sieve, Selberg’s sieve and the large sieve of Linnik, could be distinguished as the major pillars of the theory. But after the fundamental work of Deshouillers and Iwaniec in the 1980’s, the theory has been linked to the theory of automorphic forms and the fusion is making significant advances in the field.

This monograph is the outgrowth of seminars and graduate courses given by us during the period 1995–2004 at McGill and Queen’s Universities in Canada, and Princeton University in the US. Its singular purpose is to acquaint graduate students to the difficult, but extremely beautiful area, and enable them to apply these methods in their research. Hence we do not develop the detailed theory of each sieve method. Rather, we choose the most expedient route to introduce it and quickly indicate various applications. The reader may find in the literature more detailed and encyclopedic accounts of the theory (many of these are listed in the references). Our purpose here is didactic and we hope that many will find the treatment elegant and enjoyable.

Here are a few guidelines for the instructor. Chapters 1 through 5 along with Chapter 7 can be used as material for a senior level undergraduate course. Each chapter includes a good number of exercises suitable at this level. The book contains more than 200 exercises in all. Chapter 6 along with chapters 8 and 9 are certainly at the graduate level and require further prerequisites. Finally, Chapters 10 and 11 are at the ‘seminar’ level and require further mathematical sophistication. For the last chapter, in particular, a modest
xii Preface

background in the theory of elliptic curves and automorphic representations may make the reading a bit smoother. Whenever possible, we have tried to provide suitable references for the reader for these prerequisites. Our list of references is by no means exhaustive.