BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 50, Number 2, April 2013, Pages 359–366
S 0273-0979(2012)01390-3
Article electronically published on October 5, 2012

An introduction to sieve methods and their applications, by Alina Carmen Cojocaru and M. Ram Murty, London Mathematical Society Student Texts, 66, Cambridge University Press, Cambridge, 2006, xii+224 pp., ISBN 978-0-521-64275-3

Opera de cribro, by John Friedlander and Henryk Iwaniec, American Mathematical Society Colloquium Publications, 57, American Mathematical Society, Providence, RI, 2010, xx+527 pp., ISBN 978-0-8218-4970-5

How many prime numbers are there?

This simple question has inspired the subject of *analytic number theory*. The sharpest known results use the theory of complex variables, and of the *Riemann zeta function* in particular.[1]

However, our original question is purely elementary (if not easy!), inviting study by elementary methods. Generally speaking, these elementary methods are known as *sieve methods*, and they run from the very simple to the extraordinarily sophisticated. Sieve methods are valued not only for their aesthetic value as an elementary approach, but also for their flexibility: they have proved useful in studying a wide variety of questions related to the primes, in some cases where zeta function techniques are not applicable.

Reading the Latin title of the second book under review, one might wonder, Is the study of sieves really 2,000 years old, dating back to ancient Rome? In fact, the authors might have titled their book Συγγράμματα περὶ τοῦ κοσκίνου, for the subject goes back further, to ancient Greece.

1. Two theorems on prime numbers

The first theorem on primes is due to Euclid: there are infinitely many. Proof: If $p_1, p_2, \ldots, p_n$ is the complete list of primes, then $p_1 p_2 \cdots p_n + 1$ must be prime also, a contradiction.

As we have not exhausted our page limit, we have space to prove a second theorem. Suppose then that one wants to find all the primes less than 30.[2] We may do this by the *sieve of Eratosthenes*. Write out the integers from 1 to 30:

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

We ignore 1, as it is neither prime nor composite. The next integer, 2, is the first prime. We circle it and then cross out any subsequent multiples of 2:

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

2010 *Mathematics Subject Classification.* Primary 11N35, 11N36.

[1] A new proof of the same results has recently been given by Koukoulopoulos [14], based on Granville and Soundararajan's theory [6] of *pretentious* multiplicative functions. Although his proof does use complex variables, it does not rely on the analytic continuation of the zeta function.

[2] We have taken this part of the discussion straight from the very beginning of *Opera de cribro.* Although there is plenty of room for creativity in the advanced variations of the sieve, the beginning is essentially a one-way street, and one can almost not help but plagiarize.

We proceed two more steps in the same fashion, obtaining:

$$\begin{array}{ccccccccccccccc} 1 & 2 & 3 & \cancel{4} & 5 & \cancel{6} & 7 & \cancel{8} & \cancel{9} & \cancel{10} & 11 & \cancel{12} & 13 & \cancel{14} & \cancel{15} \\ \cancel{16} & 17 & \cancel{18} & 19 & \cancel{20} & \cancel{21} & \cancel{22} & 23 & \cancel{24} & \cancel{25} & \cancel{26} & \cancel{27} & \cancel{28} & 29 & \cancel{30} \end{array}$$

Continuing, one would circle the primes through 30. However, the remaining numbers already must be prime: any composite number less than 30 has a prime factor less than $\sqrt{30}$.

As this procedure allows us to *find* primes, *a fortiori* it allows us to *count* them. Counting the primes $\leq x$ seems to be difficult[3] for large x, so one might be happy with an *asymptotic formula*. Such a formula, namely the *prime number theorem* $\pi(x) \sim \frac{x}{\log x}$ (here $\pi(x)$ is the number of primes $\leq x$), was proved by Hadamard and de la Vallée Poussin in 1896. As the proof is difficult and uses complex analysis, the impatient reader might settle for *any* nontrivial theorem, beyond Euclid's, about $\pi(x)$.

To this end, Legendre observed that Eratosthenes' algorithm can be adapted to prove an upper bound for $\pi(x)$. This can be seen already, from the first three steps of the sieve: if we start with the integers between 1 and x, then we eliminate $\frac{11}{15}x$ of them ($1 - \frac{11}{15} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$). We might hope to conclude that $\pi(x) \leq \frac{4}{15}x$; in fact, we conclude that $\pi(x) \leq \frac{4}{15}x + O(1)$, where the error term depends on the number of steps taken.

For large x, we can improve our bound by increasing the number of steps. We will formalize this argument and prove a nontrivial upper bound for $\pi(x)$. This fairly simple argument will illustrate the flavor of more advanced sieve proofs.

Choose a parameter Y then, which may depend on x, and we run the sieve until we have circled all the primes $< Y$. The remaining integers will either be prime, or else have each of their prime factors at least Y.

More formally speaking, write $\mathcal{P}(Y)$ for the product of all primes $< Y$, and $\mu(n)$ for the *Möbius function*: If $n = p_1 p_2 \cdots p_r$ is a product of r distinct primes, then $\mu(n) := (-1)^r$; otherwise $\mu(n) = 0$. Then, the inclusion-exclusion principle (or *Möbius inversion*) gives the identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1, \end{cases} \tag{1.1}$$

valid for any positive integer n. In particular, this implies that

$$\sum_{d|(n,\mathcal{P}(Y))} \mu(d) = \begin{cases} 1 & \text{if } n \text{ has no prime factor } < Y, \\ 0 & \text{if } n \text{ has a prime factor } < Y, \end{cases}$$

where $(n, \mathcal{P}(Y))$ denotes the greatest common divisor of n and $\mathcal{P}(Y)$.

Therefore,

$$\pi(x) \leq Y + \sum_{1 \leq n \leq x} \sum_{d|(n,\mathcal{P}(Y))} \mu(d); \tag{1.2}$$

[3]As of the writing of this article, the primes have been counted up to approximately 10^{24}. If this number seems large, note that Bays and Hudson [1] have proved that

$$\pi(x) > \lim_{\epsilon \to 0} \left(\int_0^{1-\epsilon} \frac{dt}{\log t} + \int_{1+\epsilon}^{x} \frac{dt}{\log t} \right)$$

for some $x < 1.4 \times 10^{316}$, but no particular x is known to satisfy this inequality.

this is equivalent to sieving up to Y as explained before. The first term of Y is there because the prime numbers $< Y$ have not survived the sieve, despite being perfectly good prime numbers.

The next step of any analytic number theory argument is usually to switch the order of the sums (or else to apply Poisson summation, but that does not seem to help here). We thus see that

$$\pi(x) \leq Y + \sum_{d|\mathcal{P}(Y)} \mu(d) \sum_{\substack{1\leq n\leq x \\ d|n}} 1. \tag{1.3}$$

The inner sum is $\frac{x}{d} + O(1)$, so that

$$\begin{aligned} \pi(x) &\leq Y + \sum_{d|\mathcal{P}(Y)} \mu(d)\left(\frac{x}{d} + O(1)\right) \\ &= Y + x\sum_{d|\mathcal{P}(Y)} \frac{\mu(d)}{d} + \sum_{d|\mathcal{P}(Y)} O(1) \\ &= Y + x\prod_{p<Y}\left(1-\frac{1}{p}\right) + \sum_{d|\mathcal{P}(Y)} O(1). \end{aligned} \tag{1.4}$$

The product over $p < Y$ generalizes the $\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}$ term we saw earlier. There is an $O(1)$ term for every divisor of $\mathcal{P}(Y)$, and since $\mathcal{P}(Y)$ is the product of all primes $< Y$ we observe to our horror that the error term is *exponential in Y*.

The product over p converges to zero as $Y \to \infty$ (this is not trivial, but neither is it difficult), and so allowing Y to grow slowly with x, one sees that

$$\pi(x) = o(x). \tag{1.5}$$

With a little effort, one can prove that the choice $Y = \log(x)$ establishes the bound $\pi(x) = O\left(\frac{x}{\log\log x}\right)$. But one cannot help but be annoyed by the error term—it remains stubbornly difficult to obtain even the slightest bit of cancellation, let alone to prove that

$$\pi(x) = \int_2^x \frac{dx}{\log x} + O\left(x^{1/2}\log^2 x\right), \tag{1.6}$$

as is widely expected.[4]

2. Refinements of the sieve

This proof can be refined to show that $\pi(x) = O\left(\frac{x\log\log x}{\log x}\right)$. But the prime number theorem is known, and so our efforts seem wasted. (It is not as if complex analysis is forbidden.) But what of similar problems, those that zeta function methods seem unable to touch? For example, the *twin prime conjecture* which says that there are infinitely many twin prime pairs $p,\ p+2$? Or the *Goldbach conjecture* which says that every even integer ≥ 4 is the sum of two primes?

These questions were taken up by Viggo Brun in the early twentieth century. Despite his striking and original results, apparently Brun's papers were difficult to read. Cojocaru and Murty's book suggests that Brun's papers sat unread on Edmund Landau's desk for eight years, and Greaves' book [7] recommends them to

[4]This is equivalent to the famous *Riemann hypothesis*, for which there is an open million dollar bounty.

the "adventurous reader". Less adventurous readers might prefer the books under review, where Brun's sieve is given a very readable treatment.

Brun proved that there are infinitely many twin *almost* prime pairs $q, q+2$, where each of q and $q+2$ has at most nine prime factors, and Atle Selberg developed another sieve and improved upon this. The strongest result along these lines is due to Jing-run Chen, who proved that there are infinitely many primes p for which $p+2$ has at most two prime factors. This is at least *close* to the twin prime conjecture.

All of this is treated in detail by Halberstam and Richert's 1974 classic *Sieve methods* [9], which is newly back in print. The reader of [9] might be forgiven for believing that sieve methods had already achieved most of their potential. The book starts with the Eratosthenes, Brun, and Selberg sieves, and in large part presents a series of more and more complicated iterations of the same techniques, culminating in a proof of Chen's theorem.

Their book was relied upon by many, and the chapter endnotes suggested that the theory had further room for improvement. Their prediction proved accurate: one may see the books of Diamond and Halberstam [3], Greaves [7], and Harman [10], among many other books and papers, for further improvements and applications. Nevertheless, barring a resolution of the twin prime conjecture, the book [9] seemed to offer a relatively complete description of the possibilities and limitations of sieve methods.

The twin prime problem remains open. But a variety of mathematicians have refined the sieve and found an ever-increasing range of applications for it. John Friedlander and Henryk Iwaniec (among others) have been at the forefront of this effort, so it is not surprising that *Opera de cribro* is already the definitive source for the modern theory.

Before getting to the books, we discuss a few interesting sieve results which have been proved in recent years. One obvious standout is the theorem of Goldston, Pintz, and Yıldırım [5], who proved that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n} = 0, \tag{2.1}$$

where p_n denotes the nth prime. The prime number theorem implies that $\frac{p_{n+1}-p_n}{\log n}$ equals 1 on average, so their result implies the existence of many small gaps between primes. Moreover, the same authors proved that

$$\liminf_{n\to\infty} \Big(p_{n+1}-p_n\Big) \leq 16 \tag{2.2}$$

if the so-called *Elliott–Halberstam conjecture* is true; namely, if the primes are well distributed in arithmetic progressions on average.

Much of their technique can be seen from the formula

(2.3)
$$S(x) := \sum_{x\leq n\leq 2x} \Big(\chi(n)+\chi(n+2)+\chi(n+4)+\cdots+\chi(n+1000)-1\Big)\Bigg(\sum_{d\mid n(n+2)\cdots(n+1000)} \lambda_d\Bigg)^2,$$

where $\chi(n)$ is the characteristic function of the primes, and the λ_d are real numbers. If $S(x) > 0$, then on *weighted* average over n, the quantity $\chi(n)+\cdots+\chi(n+1000)$ is larger than 1. It follows that there is some $n \in [x, 2x]$ for which two of the $n+2k$ are primes; i.e., there is a bounded prime gap in $[x, 2x]$. In other words, if one proved that $S(x) > 0$ for all sufficiently large x, this would show that $\liminf_{n\to\infty} \big(p_{n+1} - p_n\big) \leq 1000$.

We will carry out one more step of the proof. Multiplying out the square and rearranging the sums, one obtains

$$S(x) = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{x \leq n \leq 2x \\ [d,e] | n(n+2)\cdots(n+1000)}} \Big(\chi(n) + \cdots + \chi(n+1000) - 1\Big), \tag{2.4}$$

where $[d, e]$ is the least common multiple of d and e. We will require that $\lambda_d = 0$ for $d > D$ (for some D) to prevent the error terms from spiraling out of control. The condition in the inner sum restricts n to certain arithmetic progressions (mod $[d, e]$), and we must estimate the number of primes in these progressions. This explains the utility of the Elliott–Halberstam conjecture, and it also illustrates how sieve methods can effectively use theorems from other parts of analytic number theory.

This technique led quite directly to (2.2), and a variation led to (2.1). Needless to say, there are considerable technical difficulties. It is easy to define coefficients λ_d for which $S(x)$ is presumably positive, and it is easy to define coefficients for which $S(x)$ can be reasonably evaluated, but it is difficult to satisfy these constraints simultaneously, especially for (2.1).

Another remarkable result is due to Friedlander and Iwaniec [4], who proved that the polynomial $x^2 + y^4$ represents infinitely many primes. Adapting their methods, Heath-Brown [12] proved the same for the polynomial $x^3 + 2y^3$. A novice may not know to be impressed; for example, every book on algebraic number theory proves that the related polynomial $x^2 + y^2$ represents precisely the primes 2 and those $\equiv 1 \pmod 4$.

The difference is that $x^2 + y^4$ is not the norm form of any number field to $\mathbb{Q}$, and so the usual algebraic methods do not suffice. Friedlander and Iwaniec indeed work in the Gaussian field $\mathbb{Q}(i)$ (where their polynomial factors), but their work critically relies on further development of the sieve.

A key input is a result on the *level of bilinear distribution* of this sequence. As we saw in (2.4), it is useful to understand the average distribution of primes (and other sequences) in arithmetic progressions. If one can estimate these up to modulus D, with sufficiently good error terms, one says that the sequence being sieved has *level of (absolute) distribution D*. Bombieri, Friedlander, and Iwaniec's recent work on the asymptotic sieve has highlighted the importance of related estimates for certain bilinear forms. In many applications it is both useful and possible to prove such estimates—especially when it is hoped that the sieve will detect primes.

A discussion of recent results on the primes would be incomplete without mentioning Green and Tao's exciting result [8] that the primes contain arbitrarily long arithmetic progressions. Their work substantially overlaps with sieve methods; notably, they use the variant Selberg sieve weights appearing in Goldston, Pintz, and Yıldırım [5]. Their work also applies ergodic theory, placing it outside the purview of the books under review. Nevertheless, many of the technical details overlap, and *Opera de cribro* in particular would make an excellent companion to works on this family of ideas.

3. The books under review

Let us say something, then, about the books under review.

We begin with the Cojocaru and Murty book. The authors, in their own words, aim "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. We hope that many will find the treatment elegant and enjoyable." In my estimation, the authors succeed admirably.

The absolute beginner to analytic number theory can do no better than to start with Chapter 1 and do all thirty-six of the exercises. The book then proceeds with a variety of sieve methods, including those of Brun and Selberg, the "large" sieve of Linnik, and a variety of lesser-known but interesting sieves. The authors emphasize applications throughout, and not only the most well-known ones.

At only 224 pages it is the shortest and simplest book on sieve methods that I have seen. Experts will note that much of the material is readily available elsewhere, but beginners will appreciate the clear path laid out towards the modern theory. Although the authors stop short of the state of the art (for example, settling for a proof that $p+2$ has four prime factors infinitely often, in contrast to Chen's two) they come closer than one might expect, and I enthusiastically recommend their book to any newcomer to the subject.

This, then, leaves the door open for a modern treatment of sieve methods, written for the aspiring expert, which connects classical work to ongoing progress. This is brilliantly accomplished by *Opera de cribro*. On the back cover Enrico Bombieri calls the book "a true masterpiece", and your reviewer found no cause to disagree.

Caveat emptor, however: the book is not for the faint of heart. This can be seen, for example, in their treatment of the sieve of Eratosthenes. To my surprise, they do not present the simple proof above that $\pi(x) = O\big(\frac{x}{\log\log x}\big)$. After discussing this circle of ideas at the beginning of the book, they seemingly decide that the error term will be too large to be interesting, and abandon it. They return to this sieve in Chapter 4, but only in cases (i.e., for sequences $\mathcal{A}$ which are not of the form $\{n :\ 1 \leq n \leq x\}$) where they can obtain an asymptotic.

This book, then, is recommended for those who have already read an introductory book on analytic number theory, such as those by Davenport [2] or Montgomery and Vaughan [15]. The authors freely use techniques such as Mellin integration and Poisson summation, which are familiar to the seasoned analytic number theorist but which could catch the novice by surprise. Occasionally the authors appeal to more sophisticated results from the subject, for which it would be handy to also have Iwaniec and Kowalski's book [13] at hand.

Although the casual reader might prefer to look elsewhere, the serious and prepared reader will recognize this book as a goldmine. Among many other places, this can be seen in Chapter 7.2, "Comments on the Λ^2-Sieve". Having presented the main theorem of the Selberg sieve in Chapter 7.1, the authors now offer five full pages of discussion of the result. The formulas for the sieve coefficients are (unavoidably) complicated, and so this section reads like a burst of fresh air. The serious student no longer has any excuse to treat the Selberg sieve as a mysterious black box, as Friedlander and Iwaniec take great pains to provide not only the details but also the motivation.

The authors discuss technical details such as "composition of sieves" early in the book, and they do the difficult work of establishing the fundamental theorems of sieve theory in the middle (roughly Chapters 7–11). The payoff is apparent later in the book, where the authors present a dizzying variety of variations and applications—far more than in any book on sieves that I have seen. By then the authors can say, e.g., "we choose (λ_v), (λ_{v_2}) to be upper-bound sieves of level $D < z$ and with λ_v supported on numbers coprime to β", and the diligent reader will know what is meant.

This last point should really be emphasized. It is typical of sieve results that there are a large number of technical hypotheses to be verified, leading to some complicated, technical conclusion. *Opera de cribro* does an impressive job of presenting sieve methods as a genuine theory, where the technical underpinnings are well motivated and for the most part encapsulated, and one really can just "introduce an upper-bound sieve".

A further treat can be found near the end of the book, where the authors use sieve methods to prove Linnik's theorem: given any arithmetic progression $a \pmod q$, there is a prime $p \equiv a \pmod q$ with $p < q^L$, where L is an absolute constant. The usual proof, using L-functions, is notoriously difficult, where standard methods are stymied by the possibility of an *exceptional zero*, violating the Riemann hypothesis, lying very close to 1. Such a zero does not exist—but this cannot be proved. The usual proof of Linnik's theorem (see, e.g., that in [13]) establishes an "exceptional zero repulsion" principle, akin to proving that at most one of Santa Claus and the Tooth Fairy exist.

Friedlander and Iwaniec do not avoid zeros of L-functions, but they make clever use of the exceptional zero:[5] if it does not exist, then the standard methods work easily; if it does exist, then a sieve problem of very low dimension is set up, and primes $\equiv a \pmod q$ can be found. As the authors say, "No wonder then that we welcome the exceptional characters into the arsenal of tools in analytic number theory, even though we perceive them as ghosts in the house who will eventually disappear forever."

This last proof illustrates how sieve methods can be applied in concert with other tools from analytic number theory, a theme that runs throughout the book. To give another example, the authors repeatedly demonstrate how Poisson summation can be used to establish good levels of distribution for various sequences, thereby preparing the ground for the sieve.

This exciting and innovative book will introduce the reader to a fascinating area of contemporary research, which is very much intertwined with the rest of analytic number theory, and which has a promising future—even if it does not prove the twin prime conjecture. The authors are sure to be rewarded for their efforts by the sight of ratty, worn-out copies of their book in the offices of a generation of analytic number theorists.

Acknowledgments

The author would like to thank Nicolas Addington, Andrew Granville, Heini Halberstam, Anders Hendrickson, Asher Kach, Robert Lemke Oliver, and Loizos Solomou for detailed comments and suggestions.

[5]This idea has precedents, for example in Heath-Brown's proof [11] that the existence of an infinite sequence of exceptional zeros implies the twin prime conjecture.

References

[1] C. Bays and R.H. Hudson, *A new bound for the smallest x with $\pi(x) > \mathrm{li}(x)$*, Math. Comp. **69** (1999), no. 231, 1285–1296. MR1752093 (2001c:11138)

[2] H. Davenport (as revised by H. Montgomery), *Multiplicative number theory*, Springer-Verlag, New York, 2000. MR1790423 (2001f:11001)

[3] H. Diamond and H. Halberstam, with an appendix by W. Galway, *A higher-dimensional sieve method*, Cambridge University Press, Cambridge, 2008. MR2458547 (2009h:11151)

[4] J. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. (2) **148** (1998), no. 3, 945–1040. MR1670065 (2000c:11150a)

[5] D. Goldston, J. Pintz, and C. Y. Yıldırım, *Primes in tuples. I*, Ann. of Math. (2) **170** (2009), no. 2, 819–862. MR2552109 (2011c:11146)

[6] A. Granville and K. Soundararajan, *Multiplicative number theory*, book in preparation.

[7] G. Greaves, *Sieves in number theory*, Springer-Verlag, Berlin, 2001. MR1836967 (2002i:11092)

[8] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547. MR2415379 (2009e:11181)

[9] H. Halberstam and H.-E. Richert, *Sieve methods*, Dover, 2011. (Reprint of Academic Press 1974 edition.) MR0424730 (54:12689)

[10] G. Harman, *Prime-detecting sieves*, Princeton University Press, Princeton, 2007. MR2331072 (2008k:11097)

[11] D. R. Heath-Brown, *Prime twins and Siegel zeros*, Proc. London Math. Soc. (3) **47** (1983), no. 2, 193–224. MR703977 (84m:10029)

[12] D. R. Heath-Brown, *Primes represented by $x^3 + 2y^3$*, Acta Math. **186** (2001), no. 1, 1–84. MR1828372 (2002b:11122)

[13] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, 2004. MR2061214 (2005h:11005)

[14] D. Koukoulopoulos, *Pretentious multiplicative functions and the prime number theorem for arithmetic progressions*, preprint, `http://arxiv.org/abs/1203.0596`

[15] H. Montgomery and R. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge University Press, Cambridge, 2007. MR2378655 (2009b:11001)

Frank Thorne
Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, South Carolina 29208
E-mail address: `thorne@math.sc.edu`