BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 38, Number 1, Pages 117–121
S 0273-0979(00)00890-9
Article electronically published on October 2, 2000

Elementary methods in number theory, by Melvyn B. Nathanson, Springer, New York, 2000, xiii + 513 pp., $49.95, ISBN 0-38798912-9

Number theory is perhaps as old as civilization. Since the dawn of history, humanity has been fascinated by numbers and their properties. In fact, the ancient Pythagorean philosophy that "all is number" is literally true in our modern digitalized world. Central to the study of numbers has been the distribution of prime numbers, for these are the building blocks of all numbers, so to speak. Analytic number theory has been largely focussed on understanding the distribution of prime numbers.

Over the centuries, methods have evolved to study prime numbers, and one of the main tools has been the Riemann zeta function. If we let $\pi(x)$ denote the number of primes up to x, Gauss conjectured that

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

as $x \to \infty$. In a fundamental paper of 1860, Riemann outlined, but did not prove, how the complex analytic study of the ζ-function would lead to a proof of the Gauss conjecture (also known as the prime number theorem (PNT)). In later decades, largely due to the efforts of Hadamard and de la Vallée Poussin, the necessary complex analysis was developed, culminating in the proof of the prime number theorem in 1896. Much of their work was simplified and streamlined to create the beautiful "Tauberian theorem" of Wiener and Ikehara. Because of the equivalence of the prime number theorem to the non-vanishing of the ζ-function on the line $Re(s) = 1$, it was suspected (in the early part of the 20th century) that an "elementary" proof of PNT which avoids the use of complex analysis either does not exist or is difficult to find. Amongst the pundits, the former view held sway for almost half a century. We shall discuss this history later.

In this way, the word 'elementary' had evolved to have two meanings in number theory. The first meaning is the standard one, signifying 'simplicity'. The second meaning is the technical one, meaning the avoidance of complex analysis. Both of these meanings are implied by the title of the book under review. However, for the most part, it is 'simplicity' that characterizes the methods of proof in this book.

The book is divided into three parts. The first part is called "a first course in number theory". The second is called "divisors and primes in multiplicative number theory". The third is devoted to "three problems in additive number theory".

The first part, which deals with the standard elementary topics of divisibility, prime numbers, congruences, primitive roots and quadratic reciprocity law, can be used to form the basis of an undergraduate course in elementary number theory. After discussing Fermat's little theorem and Euler's generalization of it, there is a section on public key cryptography.

We also find here a chapter on Fourier analysis on finite abelian groups and a proof of the law of quadratic reciprocity using this formalism. (A serious typo occurs on page 138: in line 4, the equal sign should be replaced by $\leq$.) Perhaps this chapter is a bit too abstract for undergraduate fare, and its full significance can

2000 *Mathematics Subject Classification.* Primary 11-01, 11Axx, 11B13, 11Pxx.

only be appreciated if the reader gets to Chapter 10 in Part 2, where Dirichlet's theorem on primes in arithmetic progressions is done. It is even debatable whether this qualifies as a chapter in a book dedicated to 'elementary methods'.

Included in part 1 is a chapter devoted to the ABC conjecture. This exceedingly beautiful conjecture has the remarkable feature of unifying diverse strands of thought in arithmetic and analysis. It was formulated by Masser and Oesterlé in 1980 and says the following: Let $\epsilon > 0$ be fixed. Given any three mutually coprime integers A, B, C with $A + B = C$, we have

$$\max(|A|, |B|, |C|) \leq \kappa(\epsilon)\Big(\prod_{p|ABC} p\Big)^{1+\epsilon}$$

where the constant $\kappa(\epsilon)$ depends only on ϵ. Following Silverman [S], this conjecture is then used to show that there are infinitely many primes p such that

$$2^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2).$$

Part 2 is devoted to the elementary proof of the prime number theorem. After discussing basic properties of arithmetical functions, Nathanson derives Chebyshev's estimates for $\pi(x)$, the number of primes $\leq x$, in Chapter 8. In Chapter 9, he gives the elementary proof of the prime number theorem due to Erdös [E2] and Selberg [Se] and in Chapter 10, the elementary proof of Dirichlet's theorem on primes in arithmetic progressions.

As alluded to above, the elementary proof of the prime number theorem has a curious history, a part of which is described in the notes at the end of Chapter 9. In 1921, G.H. Hardy [B] wrote "No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent ... to the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem, not fundamentally dependent upon the ideas of the theory of functions, seems to be extraordinarily unlikely. It is rash to assert that a mathematical theorem *cannot* be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say 'lie deep' and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten."

In a sense, Hardy was wrong. Erdös and Selberg did succeed in providing an elementary proof. In 1949, reviewing the work of Erdös and Selberg, A. E. Ingham [I] wrote, "What Selberg and Erdös do is to deduce the prime number theorem directly ... without the explicit intervention of the analytical fact ... How far the practical effects of this revolution of ideas will penetrate into the structure of the subject, and how much of the theory will ultimately have to be rewritten, it is too early to say."

Nathanson writes that "number theorists of Hardy's and Ingham's generation believed that there could be no elementary proof of the prime number theorem. They were also convinced that if, by some miracle, an elementary proof were discovered, then the ideas in that proof would lead to tremendous progress in our knowledge of the distribution of prime numbers and the zeros of the zeta function. Both statements are false. Erdös and Selberg produced elementary proofs, but their beautiful method has not led to any extraordinary new discoveries in number

theory or analysis." Perhaps it is too early to tell. It may be fair to say that we have a greater understanding of the more 'complicated' proof than the 'elementary' proof.

E.G. Straus writes cautiously in an undated manuscript, "The elementary proof has so far not produced the exciting innovations in number theory that many of us expected to follow. So what we witnessed in 1948 may in the course of time prove to have been a brilliant but somewhat incidental achievement without the historic significance it then appeared to have. My own inclination is to believe that it was the beginning of important new ideas not yet fully understood and that its importance will grow over the years."

This looks like a fairer assessment. We do not understand the elementary proof and its curious relationship to sieve theory. At present, the elementary proof sits as an isolated chapter of number theory. But this may change. There are now at least two different elementary proofs of the prime number theorem, one by Daboussi [Da] and another by Hildebrand [Hi]. Further research may validate the position of Strauss.

The third part of the book is devoted to three problems in additive number theory. The first problem is Waring's problem. This problem states that for every positive integer k, there is an integer $g(k)$ such that every natural number can be written as a sum of $g(k)$ k-th powers. For instance, $g(2) = 4$ is the celebrated theorem of Lagrange asserting that every natural number can be written as a sum of 4 squares. For $k = 3$, that $g(3) = 9$ is a theorem of Wieferich and Kempner, proved in 1912. In 1909, Hilbert [H] established the existence of $g(k)$ for every k. His method, being an existence proof, led to no effective estimates. Later, developing the circle method, Hardy, Littlewood and Vinogradov gave transparent analytic proofs that opened the way for quantitative results.

It is fascinating that we even have a conjectural formula for $g(k)$ as $2^k+[(3/2)^k]-2$, where the square brackets indicate the greatest integer function. It is easy to see that this is a lower bound for $g(k)$ by considering $n = 2^k[(3/2)^k] - 1$. This formula tallies with $g(2) = 4$, $g(3) = 9$ and predicts $g(4) = 19$. Though $g(3)$ was known as far back as 1912, the fact that $g(4) = 19$ was established as late as 1986 by Balasubramanian, Dress and Deshouillers [BDD] and that $g(5) = 37$ by Chen [C] in 1964. In 1940, Pillai [P2] had shown $g(6) = 73$. In fact, in 1936, Dickson [D] and Pillai.[1] [P1] independently proved that if we write $3^k = q2^k + r$ with $0 < r < 2^k$, then $g(k) = 2^k + [(3/2)^k] - 2$ **provided** $r + q \leq 2^k$. It is conjectured and still unproved that this condition always holds, though Mahler [M], using Roth's theorem, showed in 1957 that there are only finitely many exceptions to the condition. These tantalizing facts about Waring's problem are not mentioned in the book. Their inclusion would have stimulated the interest of budding mathematicians in the problem.

The second problem involves deriving formulas for the number of representations of a given integer n as a sum of s squares. In this, Nathanson follows an old method of Liouville, which he labels as a "mysterious method". This method is based on the following identity. Let $F(x, y, z)$ be a function defined on all triples of integers (x, y, z) such that $F(-x, y, z) = -F(x, y, z)$ and $F(x, -y, -z) = F(x, y, z)$ for all

[1]It seems that Pillai had proved this a year earlier in 1935, as is written in his obituary [Ch] by K. Chandrasekharan. Unfortunately, Pillai died in a plane crash in 1950 on his way to the International Congress in Cambridge, Massachusetts.

triples of integers (x, y, z). If n is not a perfect square,

$$2 \sum_{u^2+de=n} F(e-2u, u+d, 2u+2d-e) = \sum_{u^2+de=n} F(d+e, u, d-e).$$

If n is a perfect square, there is a simple correction term in the identity. Even though one can give an 'elementary' proof of this identity, its origins would be mysterious to the reader. In fact, Liouville himself was motivated by the theory of elliptic functions in deriving it, and today, after Hecke's work, it is best understood in the context of modular forms. Here again we see that an elementary proof does not lead to greater insight, though it does give 'quick' proofs of classical theorems of Fermat and Lagrange. This section is essentially a re-working of Chapter 13 of the classic book of Uspensky and Heaslet [UH].

The third problem of the last section concerns the partition function $p(n)$ and the derivation, by simple methods, of the asymptotic formula $\log p(n) \sim c\sqrt{n}$ for some constant c. Hardy and Ramanujan [HR], by using the circle method (this is where the method formally appears for the first time in the mathematical literature), showed in 1918 that

$$p(n) \sim \frac{e^{c\sqrt{n}}}{4\sqrt{3}n}$$

as $n \to \infty$. Their methods were not 'elementary' in the technical sense. In a paper of 1942, Erdös [E1] gave an elementary proof (again in the technical sense) of the result of Hardy and Ramanujan, basing it on the easily derived recursion

$$np(n) = \sum_{v=1}^{n} \sigma(v) p(n-v)$$

where $\sigma(v)$ denotes the sum of the positive divisors of v.

In summary, Nathanson's book is well-written and can be recommended for a first course in analytic number theory at the graduate level. Each chapter contains interesting exercises. A few chapters make for difficult reading, like Chapter 12, giving Linnik's proof of the Waring problem, and Chapter 9, giving the elementary proof of the prime number theorem. Perhaps they are necessary to reveal the other meaning of the word 'elementary'. The book is appropriately dedicated to Pál Erdös, who was without argument a master of the 'elementary' art.

References

[BDD] R. Balasubramanian, J.-M. Deshouillers and F. Dress, Problème de Waring pour les bicarrés 1, 2, *C.R. Acad. Sci. Paris Sér. I Math.,* **303** (1986) 85-88, and 161-163. MR **87m:**11099; MR **88e:**11095

[B] H. Bohr, Address of Professor Harald Bohr, in *Proceedings of the International Congress of Mathematicians,* Cambridge, 1950, Volume 1, pp. 127-134, Providence, 1952, American Math. Society. MR **13:**550c

[Ch] K. Chandrasekharan, Obituary: S.S. Pillai, *Journal of the Indian Math. Society,* **15** (1951) 1-10. MR **13:**198d

[C] J.-R. Chen, Waring's problem for $g(5) = 37$, *Scientia Sinica,* **13** (1964) 335 and 1547-68. MR **34:**135

[Da] H. Daboussi, Sur le théorème des nombres premiers, *C. R. Acad. Sci. Paris Sér. 1 Math.,* **298** (1984), no. 8, 161-164. MR **85f:**11065

[D] L.E. Dickson, The Waring problem and its generalizations, *Bulletin of the Amer. Math. Soc.,* **42** (1936) 833-842.

[HR] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.*, **17** (1918) 75-115.

[E1] P. Erdös, On an elementary proof of some asymptotic formulas in the theory of partitions, *Annals of Math.,* **43** (1942) 437-450. MR **4:**36a

[E2] P. Erdös, On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. Nat. Acad. Sci. U.S.A.,* **35** (1949) 374-384. MR **10:**595c

[H] D. Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem), *Math. Annalen,* **67** (1909) 281-300.

[Hi] A. Hildebrand, The prime number theorem via the large sieve, *Mathematika,* **33** (1986), no. 1, 23-30. MR **88a:**11085

[I] A. Ingham, Review of the papers of Selberg and Erdös, *Math. Reviews,* **10** (1949) 595b, 595c.

[M] K. Mahler, On the fractional parts of the powers of a rational number (II), *Mathematika,* **4** (1957) 122-124. MR **20:**33

[P1] S. Pillai, On Waring's Problem, *Journal of Indian Math. Soc.,***2** (1936) 16-44.

[P2] S. Pillai, On Waring's Problem $g(6) = 73$, *Proc. Indian Acad. Sci.,* **12A** (1940) 30-40. MR **2:**146c

[Se] A. Selberg, An elementary proof of the prime number theorem, *Annals of Math.,* **50** (1949) 305-313. MR **10:**595b

[S] J. Silverman, Wieferich's criterion and the abc conjecture, *Journal of Number Theory,* **30** (1988), 226-237. MR **89m:**11027

[UH] J.V. Uspensky and M.A. Heaslet, Elementary Number Theory, McGraw Hill Book Company, 1939. MR **1:**38d

M. Ram Murty
Queen's University
E-mail address: murty@mast.queensu.ca