4[20–00, 20C30, 20D06, 20D08].—J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER & R. A. WILSON, *Atlas of Finite Groups—Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford, 1985, xxxiii + 252 pp., 42 cm. Price $45.00.

This is indeed an atlas in which a "map", frequently of just one page, is devoted to each of 93 of the finite simple groups, starting with A_5, the smallest simple group, of order 60, and ending with the exceptional group $E_8(2)$, whose order requires 75 digits, and including all 26 of the sporadic simple groups. The main item on each map that is for the most part not readily available elsewhere is a complete character table of the group in question, but also included are: the order of the group, its Schur multiplier, its automorphism group, its principal occurrences in mathematics and in nature, its conjugacy classes and how they behave when powers are taken and how they, as well as the characters, relate to those of its Schur covering group and automorphism group, a presentation in terms of generators and relations, and a list of its maximal subgroups.

The atlas per se is preceded by a long introduction, describing the set of all finite simple groups according to the recently completed classification and containing instructions for the use of the atlas, and it is followed by other fragments of information including a bibliography which is especially extensive for the sporadic groups. By putting much thought into not only the choice of their material, but also its arrangement, the authors have been able to present a great deal of concrete information about a representative collection of the finite simple groups. For this they are to be congratulated.

R. STEINBERG

Department of Mathematics
University of California at Los Angeles
Los Angeles, California 90024

5[10-04, 10A25, 10A15, 10H08, 68C05].—ERIC BACH, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, An ACM Distinguished Dissertation 1984, The MIT Press, Cambridge, Mass., 1985, 48 pp., $23\frac{1}{2}$ cm. Price $ 15.00.

Suppose N is an odd natural number and $N - 1 = 2^k m$ where m is odd. Given an integer b, we say N is a "strong probable prime to the base b" if either

(i) $b^m \equiv 1 \bmod N$ or

(ii) $b^{2^i m} \equiv -1 \bmod N$ for some $i \in \{0, 1, \ldots, k-1\}$.

If N is actually prime, it is an elementary consequence of Fermat's Little Theorem that N is a strong probable prime to every base b coprime to N. However, it also can occur that a composite integer N passes the test for some b. An example with $b \neq 1$ is $N = 65$, $b = 8$. Nevertheless, the terminology "strong probable prime" is justified on both empirical and theoretical grounds: Examples with N composite for a fixed base $b \neq 1$ are rare (see [11]).

In particular, it is known from [10] that for a fixed $b \neq 1$, the number of composite strong probable primes to the base b that are at most x grows much more slowly than the number of primes that are at most x. In addition, for a fixed odd composite N, the number of bases b in $\{1, 2, \ldots, N-1\}$ for which N is a strong probable prime is always smaller than $N/4$ (see [7], [12]) and is both usually and on average much smaller (see [4]). Thus, Rabin has proposed the following random test for compositeness: Given an odd composite number N, the expected number of random choices of numbers b until one is found for which N is *not* a strong probable prime to the base b (and so N has been proved composite) is bounded. Such a number b is called a "witness" for N.

To test if N is a strong probable prime to the base b where $b \in \{1, 2, \ldots, N-1\}$ takes only $O((\log N)^3)$ bit operations if the naive multiplication algorithm is used. Thus, Rabin's test has expected running time $O((\log N)^3)$ to prove N composite if it really is. A similar random compositeness test was also proposed in [14].

It has long been a goal of computational number theorists to use the Fermat congruence and its generalizations such as the one above as a test to prove primality. In his thesis, Miller [6] proved the remarkable result that if N is odd and composite, then there is a witness b for N that satisfies

$$1 < b < c(\log N)^2 \tag{1}$$

for some explicit $c > 0$, provided the Extended Riemann Hypothesis (ERH) is true. Thus, by not choosing b at random, but rather exhausting the interval $(1, c(\log N)^2)$, one has an ERH-conditional primality test for N with running time $O((\log N)^5)$. In particular, the ERH implies that the prime recognition problem is in the complexity class P.

Miller's proof was based on a result of Ankeny [2] which in slightly more general form (due to Montgomery [8]) states that if G is a proper subgroup of the multiplicative group of integers mod N, then some b in the range (1) is not in G.

The main result in the monograph under review is that we may choose $c = 2$ in (1) for the Ankeny-Montgomery theorem and thus also for Miller's primality test. This represents a considerable improvement on an earlier result of Oesterlé [9] who had shown we can take $c = 70$ in (1). Bach's proof assumes a working knowledge of some standard techniques of analytic number theory. It is written in an engaging, conversational style and is most pleasant to read.

The fastest unconditional primality test is the APR test (see [1]) which has running time $O((\log N)^{c \log\log\log N})$ for some $c > 0$. A practical variant of this test due to Cohen & Lenstra [3] can establish primality of numbers in the 200 decimal digit range in only a few minutes on a good mainframe computer. In this range, the Miller test, even with Bach's constant $c = 2$, should take longer. Thus a proof of the ERH will not automatically speed up primality testing in the feasible range.

A very recent development in primality testing is a new test of Goldwasser & Kilian [5] that can be proved to run in expected polynomial time for almost all primes and is conjectured to do so for all primes. Although it is a random algorithm and the expected running time is a bit uncertain, when the algorithm halts with a proof that N is prime, this proof is valid and unconditional. The test is not based on the Fermat congruence, but rather the arithmetic of elliptic curves and in particular

the (nonpractical) algorithm of Schoof [13] for computing the order of the group of points on an elliptic curve over a finite field.

The second half of the book is devoted to the provocative problem of giving a polynomial time algorithm for selecting an integer in the interval $(N/2, N]$ with the uniform distribution and also producing the prime factorization of the selected integer. By first choosing an integer and then factoring it, we have a method that is usually too time-consuming, owing to the current intractability of factoring. Bach solves this problem by choosing the factorization first. That is, assuming primality testing as a primitive operation, primes are randomly chosen, with respect to a particular distribution such that their product lies in the interval $(N/2, N]$. The problem that must be solved is to choose the primes in such a manner that the products are uniformly distributed in $(N/2, N]$. This is roughly done as follows. Consider a random analog of Achilles and the tortoise, where you start with the unit interval and at each stage, instead of taking half of what's left, you take a fraction of what's left, where the fraction is chosen in $[0, 1]$ with the uniform distribution. Bach chooses the primes for his random number similarly. The first prime p is chosen so that $\log p/\log N$ is roughly uniformly distributed in $[0, 1]$. The next prime q is chosen so that $\log q/\log(N/p)$ is roughly uniformly distributed in $[0, 1]$, etc. That this ends up giving uniformly distributed integers in $(N/2, N]$ seems remarkable.

CARL POMERANCE

Department of Mathematics
University of Georgia
Athens, Georgia 30602

1. L. M. ADLEMAN, C. POMERANCE & R. S. RUMELY, "On distinguishing prime numbers from composite numbers," *Ann. of Math.*, v. 117, 1983, pp. 173–206.

2. N. C. ANKENY, "The least quadratic non-residue," *Ann. of Math.*, v. 55, 1952, pp. 65–72.

3. H. COHEN & H. W. LENSTRA, JR., "Primality testing and Jacobi sums," *Math. Comp.*, v. 42, 1984, pp. 297–330.

4. P. ERDÖS & C. POMERANCE, "On the number of false witnesses for a composite number," *Math. Comp.*, v. 46, 1986, pp. 259–279.

5. S. GOLDWASSER & J. KILIAN, *Almost All Primes Can be Quickly Certified*, Proc. 18th Annual ACM Sympos. on Theory of Computing (STOC), Berkeley, May 28–30, 1986, pp. 316–329.

6. G. L. MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

7. L. MONIER, "Evaluation and comparison of two efficient probabilistic primality testing algorithms," *Theoret. Comput. Sci.*, v. 12, 1980, pp. 97–108.

8. H. L. MONTGOMERY, *Topics in Multiplicative Number Theory*, Lecture Notes in Math., vol. 227, Springer-Verlag, Berlin and New York, 1971.

9. J. OESTERLÉ, "Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée," *Astérisque*, v. 61, 1979, pp. 165–167.

10. C. POMERANCE, "On the distribution of pseudoprimes," *Math. Comp.*, v. 37, 1981, pp. 587–593.

11. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, JR., "The pseudoprimes to $25 \cdot 10^9$," *Math. Comp.*, v. 25, 1980, pp. 1003–1026.

12. M. O. RABIN, "Probabilistic algorithm for testing primality," *J. Number Theory*, v. 12, 1980, pp. 128–138.

13. R.SCHOOF, "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.*, v. 44, 1985, pp. 483–494.

14. R. M. SOLOVAY & V. STRASSEN, "A fast Monte-Carlo test for primality," *SIAM J. Comput.*, v. 6, 1977, pp. 84–85; erratum, *ibid*, v. 7, 1978, p. 118.