REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 1980 Mathematics Subject Classification (1985 Revision) can be found in the December index volumes of Mathematical Reviews.

1[11–02].—DANIEL SHANKS, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985, xiv + 304 pp., $23\frac{1}{2}$ cm. Price $18.95.

This is the third edition of a book which has become something of a classic. The first edition, reviewed in [1], is a most entertaining introductory text on number theory, organized around a collection of problems, some famous and some not so famous. The second edition, reviewed in [2], contains an additional chapter (Chapter 4), describing the considerable progress which had been made on a number of the problems mentioned in the original edition. The style of this chapter is different from that of the earlier volume in that most of the topics are given a rather brief treatment and several references are provided. Thus, the number of references cited in the second edition increased to 154 from the 34 cited in the first.

The volume under review is the same as the second edition except for the inclusion of a second progress report in Chapter 4. The emphasis of this entire book is on computational number theory, and some indication of the increase in activity in this area of research can be obtained by noting that the second progress report is almost twice as long as the first. Also, there are now 236 entries in the bibliography.

The organization of the material in the second progress report is somewhat different from that of the first. While the latter is, for the most part, a simple compendium of results, the former is really made up of two interesting essays. One of these is about judging conjectures and the other discusses computing and algorithms. The points made in these essays are driven home by the use of many examples taken from recent computational and theoretical work in number theory.

Shanks feels that the word *conjecture* ought to be reserved for an abbreviation of the following statement by a conjecturer.

> "I think this proposition is true but know of no proof for it. I state this seriously, not casually. I have studied the question and examined all the numerical evidence and the heuristic argumentation that is known to me. It is my judgement, based upon this evidence and my current knowledge of the subject that, to a high degree of probability, this proposition is true. If I thought that this evidence were insufficient to warrant this conclusion I would not call this proposition a conjecture. If I were to bet on it I would offer odds."

0025-5718/87 $1.00 + $.25 per page

After offering this definition he goes on to justify it by using several illustrative examples and anecdotes. Indeed, he goes so far as to "deconjecture" his Conjecture 16, the famous Last "Theorem" of Fermat.

Included in the essay on computing and algorithms is a hilarious account of the recent discovery of the five large Mersenne primes $M_p = 2^p - 1$, where $p = 21701$, 23209, 44497, 86243, 132049. There must now be more to this saga, as Slowinski has since found that M_p is prime for $p = 216091$. Other topics which receive mention are: the Riemann Hypothesis, recent developments in primality testing, and class group structure. It is true that this latter topic is quite advanced, but Shanks points out simple pertinent facts about the class group and then uses cycle graphs to describe it. This treatment is quite understandable to the beginning student.

This is a stimulating, provocative, and informative volume, which should (and can) be read by anyone with an interest in number theory.

H. C. W.

1. Review **73**, *Math. Comp.*, v. 17, 1963, p. 464.
2. Review **1**, *Math. Comp.*, v. 38, 1982, pp. 331–332.

2[11–01, 11–04].—KENNETH H. ROSEN, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, Mass., 1984, xii + 452 pp., 24 cm. Price $29.95.

In an incautious moment, Gauss is supposed to have said that if mathematics is the queen of the sciences, then the theory of numbers is, because of its supreme uselessness, the queen of mathematics. Perhaps this reputation for uselessness has contributed to the recent decline in enrollment in elementary number theory classes, now that students demand immediate applications and subject matter which will help them get a good job. At last, here is a text for a number theory course which can satisfy their demands.

This volume covers such standard topics as factorization into primes, congruences, primitive roots and quadratic residues. What sets it apart from other introductory number theory texts is the large number of applications it contains.

After the Chinese Remainder Theorem is proved, its use in computer arithmetic with large integers is described. Later, it is applied to threshold schemes. There is a chapter on applications of congruences to calendar problems, round-robin tournaments and computer hashing functions for data storage. After the existence of primitive roots is established, the author discusses their use in generating pseudo-random numbers and splicing telephone cables to minimize interference and cross-talk.

Another chapter applies number theory to cryptology: The classical affine transformation substitution ciphers and block ciphers are cryptanalyzed. Two modular exponentiation ciphers, the Pohlig-Hellman scheme and the Rivest-Shamir-Adleman public-key cryptosystem, are described. The discussion covers many aspects of these ciphers from how to choose the primes to how to play poker by telephone. The author explains knapsack ciphers and mentions their weakness.

In another chapter, the author describes probable prime tests and Euler and strong pseudoprimes. He shows that a Carmichael number must have at least three

prime factors. He proves Pratt's theorem that every prime number has a succinct certificate of primality. He mentions the efficient primality test of Adleman, Pomerance, and Rumely. He describes Fermat's difference of squares factorization method. Draim factorization and Euler's factorization method appear in exercises. He proves Lagrange's theorem that an infinite simple continued fraction is periodic if and only if its value is a quadratic surd. However, he does not mention the continued fraction factoring algorithm or any other one of subexponential order. The book concludes with Pythagorean triples and the algorithmic solution of Pell's equation.

Five tables in an appendix give the least prime factor of each odd number below 10000, values of some arithmetic functions, the least primitive root for each prime below 1000, indices for primes below 100 and continued fractions for nonsquares below 100.

It is unfortunate that the book is marred by a number of typographical errors. Here are some that I noticed: On the copyright page, it should say that the cover refers to Problem 33 of Section 1.2. Problem 16 on page 180 is false. Two pairs of numbers are omitted from the ciphertext in the middle of page 199. On page 245, $p = 487$ is not the least prime for which there is a primitive root which is not also a primitive root modulo p^2. It is the least prime p so that 10 is a primitive root modulo p but not modulo p^2. The rows of the factor table on pages 412–418 are in the wrong order, probably the result of last minute reformatting.

In spite of these and a few other flaws, this volume is an excellent text for a course in elementary number theory with applications.

S. S. WAGSTAFF, JR.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

3[11A41, 11A51, 11N05, 11Y11, 11Y05].—HANS RIESEL, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985, xvi + 464 pp., 23 cm. Price $44.95.

This clearly written volume brings the reader from elementary facts in number theory to the level of current research in the areas mentioned in the title. Chapter 1 begins with the definition of prime number. Then the author describes the sieve of Eratosthenes and formulas for computing the exact number $\pi(x)$ of primes below x, such as those of Meissel, Lehmer, and Mapes. He mentions the recent improvement of these formulas by Lagarias, Miller, and Odlyzko.

Chapters 2 and 3 deal with the distribution of primes in the large and locally, respectively. The author compares the accuracy of several approximations to $\pi(x)$, such as $x/\ln x$, $\operatorname{li} x$ and Riemann's formula. He discusses the frequency of appearance of twin primes and other constellations. He mentions the inconsistency of the prime k-tuples conjecture with the triangle inequality $\pi(x + y) \leqslant \pi(x) + \pi(y)$, which was once conjectured to hold for all $x, y \geqslant 2$. He compares the distribution of primes in the two series $4n + 1$ and $4n + 3$ and discusses the growth rate of the maximal gaps between consecutive primes.

Chapter 4 concerns tests for primality and compositeness. It begins with probable prime tests and Carmichael numbers. Next, the Lucas-Lehmer test and its improvements due to Proth, Pocklington and Lehmer are discussed. The author gives the flavor of the new Adleman-Pomerance-Rumely primality test and its simplification by Cohen and Lenstra.

Chapter 5 on factorization is the longest chapter in the book. It begins with trial division and the GCD method of finding small factors. Then the following factoring algorithms are described: Fermat's difference of squares method and Lehman's improvement of it, Legendre's idea of finding a nontrivial solution to the congruence $x^2 \equiv y^2 \pmod{N}$, Euler's method of expressing $N = a^2 + Db^2$ in two different ways with the same D, Gauss' use of quadratic residues to restrict possible divisors of N, Legendre's use of the continued fraction expansion of $\sqrt{N}$ to produce small quadratic residues of N, Pollard's $p - 1$ and $p + 1$ methods, Pollard's ρ or Monte Carlo method and Brent's improvement of it, Shanks' square forms method, Morrison and Brillhart's continued fraction method and the quadratic sieve method. The author describes the distribution of sizes of prime factors of a typical integer. The factoring algorithms of Schroeppel, Dixon, and Schnorr and Lenstra are mentioned. The chapter closes with a thought-provoking argument that it may be possible to factor integers in polynomial time.

The brief Chapter 6 discusses the Rivest-Shamir-Adleman public-key cryptosystem and its safety.

Nine appendices discuss abstract algebra, elementary number theory, quadratic fields, continued fractions, cyclotomic polynomials, Aurifeuillian factorizations, multiple-precision integer arithmetic on computers, and Stieltjes integration. The book concludes with 34 tables. Most of them list factors of numbers of the form $a^n \pm b^n$ for various a and b up to 10. There is also a short table of primes, a list of primes between 10^n and $10^n + 1000$ for $5 \leqslant n \leqslant 15$, a table of $\pi(x)$ for various $x \leqslant 4 \cdot 10^{16}$, a table of quadratic residues, and tables of coefficients of Gauss' and Lucas' formulas for cyclotomic polynomials.

The author gives PASCAL programs for some of the algorithms he describes. For example, the book contains programs for the sieve of Eratosthenes, for computing $\pi(x)$ with Lehmer's formula, for strong probable primality tests, for Pollard's ρ factoring algorithm and for multiple-precision integer arithmetic.

This volume is the first modern text on factorization and prime testing. It must be welcomed by novices in the field. These subjects have a long history and are advancing swiftly at present, partly in response to the RSA cryptosystem, which requires large primes and whose security depends on the difficulty of factoring integers. This book went to press in February, 1985, and gives a fair description of the state of the art of these subjects at that time. In the same month, H. W. Lenstra, Jr., announced his discovery of the elliptic curve factoring algorithm. Naturally, the book does not mention this beautiful and powerful method, but the reader should be cognizant of it.

S. S. WAGSTAFF, JR.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

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.

6[12C20].—J. B. MUSKAT & K. S. WILLIAMS, *Cyclotomy of Order Twelve Over* GF(p^2), $p^2 \equiv 1 \pmod{12}$, One page of text and nine pages of tables, deposited in the UMT file, 1986.

Let $e \geqslant 2$ and $l \geqslant 1$ be integers and let p be an odd prime such that e divides $p^l - 1$. We set $q = p^l$ and define the positive integer f by $q = ef + 1$. The finite field with q elements is denoted by GF(q). We fix once and for all a generator γ of the multiplicative group GF(q)* = GF(q) − {0}. Further we set $g = \gamma^{1+p+\cdots+p^{l-1}}$, so that g is a primitive root modulo p. For $\alpha \in \mathrm{GF}(q)^*$ the index of α with respect to γ is the unique integer n such that $\alpha = \gamma^n$ $(0 \leqslant n \leqslant q-2)$ and is denoted by $\mathrm{ind}_\gamma \alpha$.

The number of solutions $\alpha \in \mathrm{GF}(q)^+ = \mathrm{GF}(q)^* - \{1\}$ of the pair of congruences

$$\begin{cases} \mathrm{ind}_\gamma(\alpha - 1) \equiv h \pmod{e}, \\ \mathrm{ind}_\gamma \alpha \equiv k \pmod{e}, \end{cases} \tag{1.1}$$

is denoted by $(h,k)_e$, where h and k are integers such that $0 \leqslant h \leqslant e-1$, $0 \leqslant k \leqslant e-1$. The numbers $(h,k)_e$ are called the cyclotomic numbers of order e over GF(q) and they depend on p, l, e, and γ. The cyclotomic numbers have the following properties:

$$(h,k)_e = (e-h, k-h)_e, \tag{1.2}$$

$$(h,k)_e = \begin{cases} (k,h)_e & \text{if } f \text{ is even,} \\ (k + \tfrac{1}{2}e,\ h + \tfrac{1}{2}e)_e & \text{if } f \text{ is odd,} \end{cases} \tag{1.3}$$

$$(h,k)_e = (ph, pk)_e. \tag{1.4}$$

It is a central problem in the theory of cyclotomy to obtain explicit formulae for these numbers. This has been done for a number of values of $e \leqslant 24$ and $l \geqslant 1$. The determination of the cyclotomic numbers of order twelve over GF(p), where $p \equiv 1 \pmod{12}$, was carried out by Whiteman in [5] (the case $e = 12$, $l = 1$). Whiteman gives the cyclotomic numbers of order twelve over GF(p) as linear combinations of p, 1, a, b, x, and y, where

$$p = a^2 + b^2 = x^2 + 3y^2, \quad a \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{6}. \tag{1.5}$$

Using the method described in [3] and the evaluation of the Eisenstein sums

$$E_e(\beta^m) = \sum_{c=0}^{p-1} \beta^{m \,\mathrm{ind}_\gamma(1 + c\gamma^{(p+1)/2})} \qquad (\beta = \exp(2\pi i/e)) \tag{1.6}$$

of order e over GF(p^2), when $e = 12$, given by Berndt and Evans [2], the authors have determined the cyclotomic numbers of order twelve over GF(p^2). Analogous to the results of Whiteman, we found that the cyclotomic numbers of order twelve over GF(p^2) can be expressed as linear combinations of p^2, p, 1, $a^2 - b^2$, $2ab$, $x^2 - 3y^2$, $2xy$, where

$$p^2 = (a^2 - b^2)^2 + (2ab)^2 = (x^2 - 3y^2)^2 + 3(2xy)^2. \tag{1.7}$$

The complete set of tables is given in the UMT file as well as in [4].

A summary of the results is as follows.

Since $p^2 \equiv 1 \pmod{12}$ we have $p \equiv 1, 5, 7$, or $11 \pmod{12}$. In the case $p \equiv 11 \pmod{12}$ the phenomenon of uniform cyclotomy occurs (see [1, Definition 1]) and there are just three different cyclotomic numbers [1, Theorem 1], namely

$$(2.1)\quad \begin{cases} 144(0,0)_{12} = p^2 + 110p - 35, \\ 144(0,i)_{12} = 144(i,0)_{12} = 144(i,i)_{12} = p^2 - 10p - 11, & i \neq 0, \\ 144(i,j)_{12} = p^2 + 2p + 1, & 0 \neq i \neq j \neq 0. \end{cases}$$

Here i and j denote integers with $0 \leqslant i, j \leqslant 11$.

For $p \equiv 1 \pmod{12}$ it is only necessary to evaluate thirty-one of the $e^2 = 144$ cyclotomic numbers, as the others can be deduced from them using (1.2) and (1.3). It is shown [4] that the thirty-one cyclotomic numbers $144(i, j)_{12}$ are integral linear combinations of p^2, 1, $a^2 - b^2$, $2ab$, $x^2 - 3y^2$, $2xy$, where the integers a, b, x, y are defined by

$$(2.2)\qquad E_{12}(\beta^3) = a + bi, \quad E_{12}(\beta^2) = x + yi\sqrt{3}, \quad \beta = \exp(2\pi i/12),$$

and satisfy

$$(2.3)\qquad p = a^2 + b^2, \quad a \equiv (-1)^k \pmod{4}, \quad p = 12k + 1,$$

$$(2.4)\qquad p = x^2 + 3y^2, \qquad x \equiv 1 \pmod{3}.$$

There are six sets of formulae depending upon $\operatorname{ind}_g 2 \pmod 3$ and which of a or b is divisible by 3.

For $p \equiv 5 \pmod{12}$ it is only necessary to evaluate twenty of the $e^2 = 144$ cyclotomic numbers, as the others can be deduced from them using (1.2), (1.3), and (1.4). It is shown [4] that each of the twenty numbers $144(i, j)_{12}$ can be expressed as an integral linear combination of p^2, p, 1, $a^2 - b^2$, $2ab$, where the integers a, b are defined by

$$(2.5)\qquad E_{12}(\beta^3) = a + bi, \qquad \beta = \exp(2\pi i/12),$$

and satisfy

$$(2.6)\qquad p = a^2 + b^2, \quad a \equiv (-1)^{k+1} \pmod{4}, \quad p = 12k + 5.$$

There are two sets of formulae depending on whether $a \equiv b \pmod 3$ or $a \equiv -b \pmod 3$.

For $p \equiv 7 \pmod{12}$ it is only necessary to evaluate twenty-two of the $e^2 = 144$ cyclotomic numbers as the others can be deduced from them using (1.2), (1.3), and (1.4). It is shown [4] that each of the twenty-two numbers $144(i, j)_{12}$ can be expressed as a linear combination of p^2, p, 1, $x^2 - 3y^2$, $2xy$, where the integers x, y are defined by

$$(2.7)\qquad E_{12}(\beta^2) = x + yi\sqrt{3}$$

and satisfy

$$(2.8)\qquad p = x^2 + 3y^2, \qquad x \equiv -1 \pmod{3}.$$

There are three sets of formulae depending upon the value of $\operatorname{ind}_g 2 \pmod 3$.

These formulae can be used to obtain new residuacity criteria. For example, the following theorem is proved in [4].

THEOREM. *Let* $p \equiv 5 \pmod{12}$ *be a prime. Let* γ *be a generator of* $\mathrm{GF}(p^2)^*$. *Set* $g = \gamma^{1+p}$ *so that* g *is a primitive root* $\pmod{p}$. *Then, with* a *and* b *as defined in* (2.5), *we have*

$$\text{(2.9)} \qquad \operatorname{ind}_g(-3) \equiv \begin{cases} 1 \pmod 4 & \text{if } a \equiv -b \pmod 3, \\ 3 \pmod 4 & \text{if } a \equiv b \pmod 3. \end{cases}$$

AUTHORS' SUMMARY

Department of Mathematics and Computer Sciences
Bar-Ilan University
Ramat-Gan, Israel

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6

1. L. D. BAUMERT, W. H. MILLS & R. L. WARD, "Uniform cyclotomy," *J. Number Theory*, v. 14, 1982, pp. 67–82.

2. B. C. BERNDT & R. J. EVANS, "Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer," *Illinois J. Math.*, v. 23, 1979, pp. 374–437.

3. C. FRIESEN, J. B. MUSKAT, B. K. SPEARMAN & K. S. WILLIAMS, "Cyclotomy of order 15 over $\mathrm{GF}(p^2)$, $p \equiv 4, 11 \pmod{15}$," *Internat. J. Math. Math. Sci.* (To appear.)

4. J. B. MUSKAT & K. S. WILLIAMS, *Cyclotomy of Order Twelve Over* $\mathrm{GF}(p^2)$, $p^2 \equiv 1 \pmod{12}$, Carleton Mathematical Series No. 217, January 1986, 73 pp.

5. A. L. WHITEMAN, "The cyclotomic numbers of order twelve," *Acta Arith.*, v. 6, 1960, pp. 53–76.