The key ideas are presented in a succinct and entertaining style. The book is carefully written (I spotted an occasional slip of the pen, e.g., the group G in the discussion on "Reynolds Operators and Lie Algebras" on page 206 should be connected), and is to be recommended as a pleasant introduction to advanced algorithmic methods in commutative algebra.

References

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Math., vol. 3, AMS, ISBN 0-8218-3804-0, Oxford University Press, Oxford, 1994.

[2] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, Berlin, ISBN 3-540-97847-X, 1992.

[3] T. Becker, H. Kredel, V. Weispfenning, *Gröbner bases, A computational approach*, GTM 141, Springer-Verlag, ISBN 0-387-97971-9, 1993.

[4] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Springer Verlag, 1995.

[5] Wolfram Decker, Gert-Martin Gruel, Gerhard Pfister, *Primary decomposition: Algorithms and comparisons*. Algorithmic algebra and number theory (Heidelberg, 1997), 187–220, Springer, Berlin, 1999.

[6] A. M. Cohen et al., *Some tapas of Computer Algebra*, Springer Verlag 1999.

[7] Theo de Jong, *An algorithm for computing the integral closure*, J. Symbolic Comput. **26** (1998), no. 3, 373–277.

[8] Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Vienna, 1993.

Arjeh M. Cohen

8[11-01]—*The Mathematics of Ciphers, Number Theory and RSA Cryptography*, by S. C. Coutinho, A. K. Peters, Ltd., Natick, MA, 1998, xv+196 pp., $23\frac{1}{2}$ cm, hardcover, $30.00

There is no shortage of books these days on the connection between number theory and cryptography, but in and amongst the plethora of such publications this book is unique. Primarily meant for junior undergraduates, this book is an enlightening invitation to number theory by way of the RSA cryptosystem. As the author states, this is a mathematical textbook and not so much a book on cryptography. Moreover, perhaps influenced by the style of his Brazilian compatriot Paulo Ribenboim, the book is written in a friendly, relaxed manner which gently winds its way through some of the fundamental concepts in elementary number theory, stopping along the way for historical asides, detailed examples, some philosophical remarks, and leading eventually to the final destination: the RSA cryptosystem. The book is self-contained, but with many pointers to further reading. There is an abundance of well thought out exercises, more than enough to familiarize the student with the subject matter. It is worth noting that this book would be most useful as an introductory textbook to postsecondary mathematics, as the ideas of theorem proving and generalization are carried out in significant detail and, more importantly, with great care. Even some more skilled high school students would find this book both accessible and inspiring.

The book is organized into eleven chapters, along with a preface on the matter of style, a wonderful introduction concerned with aspects of computation in number theory and some of the history of number theory, an addendum on the recent developments in the area of cryptography and number theory, and an appendix on computing roots and powers.

In Chapter 1 the author presents such fundamental algorithms as the division algorithm, the Euclidean algorithm, and the extended Euclidean algorithm, thereby enabling the student to immediately get "dirty hands". Moreover, a historical discussion on the origins of the word "algorithm" immediately shows that the author is not interested in presenting mathematics as a series of definitions, theorems, and proofs. In Chapter 2 unique factorization is covered, wherein the author very successfully incorporates such concepts as computational complexity, Fermat and Fibonacci numbers, Fermat's factoring method, Mersenne primes, perfect numbers, rep-units, and the irrationality of square roots of nonsquare integers. In Chapter 3 the author discusses prime numbers at length and includes two proofs of the infinitude of prime numbers, the sieve of Erathostenes, the statement of the prime number theorem and history surrounding it. Chapter 4 is concerned with modular arithmetic, an th author succeeds once again by taking a ground-up approach to this, starting with the general notion of an equivalence relation, and including many examples. Some applications to the solvability of Diophantine equations and the notion of invertibility are then presented. Chapter 5 is primarily concerned with finite induction but, more importantly, the essential theorem of this book holding it all together is presented: Fermat's little theorem. Many wonderful exercises are given in this chapter, including such topics as primality testing, the Legendre symbol, and Wieferich numbers. This leads naturally into Chapter 6 which deals with primality testing and Carmichael numbers in considerable detail. This chapter is chock-full of interesting historical tidbits, going back to Leibniz and ending with the famous result of Alford, Granville, and Pomerance. Chapter 7 is the leanest chapter, and covers the required topic of the Chinese Remainder Theorem, along with an application to secret sharing. Chapter 8 is a wonderful digression on the fundamentals of groups. It is a wonderfully laid out chapter, with substantial historical background on the contributions of Cardan, Tartaglia, and Galois. Topics such as modular unit groups, a proof of Fermat's little theorem (and Euler's theorem) all become immediately accessible. A seemingly endless set of exercises is given here. The last three chapters are, in some sense, the destination of the entire book. Chapter 9 has a fairly complete expository on Mersenne and Fermat numbers, including the Lucas–Lehmer primality test for Mersenne numbers, and the current state of the art on factoring and primality of Mersenne numbers. Chapter 10 goes quite a bit further into the topic of primality testing, and also touches on the topic of primitive roots. The Lucas primality test, Pepin's test, and the test of Brillhart, Lehmer, and Selfridge are all described in significant detail. Korselt's characterization of Carmichael numbers is given, along with the complete proof. The final chapter is devoted to the presentation and some implementation considerations of the RSA cryptosystem. Given the nature of the book, one can only expect this to be given in the most rudimentary form, which, nevertheless, the author succeeds in doing very well.

GARY WALSH
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OTTAWA
ONTARIO, CANADA
E-mail address: gwalsh@mathstat.uottawa.ca