Computational Algebraic Number Theory. by Michael E. Pohst. Birkhäuser Verlag, P.O. Box 133, CH-4010. Basel Switzerland. 1993. Price: S Fr 34. 104 pp.

Before we discuss the book, let me begin by motivating the problems which this book addresses itself to.

A very well-known problem, believed to have been posed by Archimedes, is the following: find a solution (with $Y \neq 0$)[1] in integers (= whole numbers), to the equation

$$X^2 - 4729494Y^2 = 1.$$

Another well-known theorem of Ramanujan-Nagell asserts that the only solution (in integers x, n) of the equation $X^2 + 7 = 2^n$ are $x = \pm 1, \pm 3, \pm 5, \pm 11, \pm 181$ and the corresponding values of n are $n = 3, 4, 5, 7, 15$.

These problems are by no means peculiar or special. Number theory addresses itself to solving equations in finite number of indeterminates, and with integer coefficients. The problem, almost always, is to find all integer solutions to a given equation or to determine the set of all rational solutions. For example, let us consider the equation of the Archimedes problem. We may obviously rewrite it as

$$X^2 - dY^2 = (X - \sqrt{d}Y)(X + \sqrt{d}Y) = 1,$$

where $d = 4729494$. It is immediate, upon writing $z = x + \sqrt{d}y$, $z' = x - \sqrt{d}y$, that if z_1, z_2 correspond in the above fashion to a pair of solutions (x, y), (x', y'), then $z_1 z_2 = xx' + dyy' + \sqrt{d}(xy' + x'y)$ corresponds to the solution $X = xx' + dyy'$, $Y = xy' + x'y$. Similarly, we may factorize $x^2 + 7 = (x + \sqrt{-7})(x - \sqrt{-7})$. Notice that in both the situations we are naturally led to consider properties of quantities of the form $x + y\sqrt{d}$ for suitable d and where x, y are either rational numbers or integers. This leads to the notion of algebraic numbers and algebraic number fields. Thus for example in the above situation the set $\mathbf{Q}(\sqrt{d}) = \{x + \sqrt{d}\,y \mid x, y \in \mathbf{Q}\}$ is an example of an algebraic number field. In general, an *algebraic number field* (or simply a *number field*) is obtained by considering all the expressions $\sum_{i=0}^{n-1} x_i \alpha^i$ where α is a root of some irreducible polynomial $f(X)$ with rational coefficients of degree n, and where x_i is rational number; these expressions can be added, subtracted, multiplied and divided in the usual way; the degree of f is called the *degree of* K (over $\mathbf{Q}$). The elements of a number field are called *algebraic numbers*. Every element of a number field satisfies a polynomial equation with integer coefficients. Number fields have many properties similar to the field, $\mathbf{Q}$, of rational numbers. Just as integers, $\mathbf{Z}$, form a ring contained in the field of all rational numbers, in every number field K, there is a special subring $R \subset K$, called the *ring of algebraic integers of* K and which consists of all elements of the field which satisfy monic polynomial with integer coefficients. This ring R is a free $\mathbf{Z}$-module of rank equal to the degree of the field K. By the phrase 'computation of ring of integers R' of K, we mean 'computation of a $\mathbf{Z}$-basis for the ring R'. It is possible to extend the familiar notions of arithmetic like divisibility etc. to elements of R. For instance, if $K = \mathbf{Q}(\sqrt{-7})$, is of degree two over $\mathbf{Q}$, and

$$R = \left\{ x + \frac{(1+\sqrt{-7})}{2} y \mid x, y \in \mathbf{Z} \right\}.$$

Then we are naturally led to the question whether the ring R shares any properties with the ring of integers $\mathbf{Z}$. In particular we can ask if the property of uniqueness of factorization is valid in R. For instance, the solution to the Ramanujan-Nagell problem rests on the fact that in the ring of integers of $\mathbf{Q}(\sqrt{-7})$, the property of unique factorization is valid.

It is known that not every number field has unique factorization property. For example consider the case $6 = 3.2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and it can be shown that uniqueness of factorization fails to be valid in the ring of integers of $\mathbf{Q}(\sqrt{-5})$. There is natural measure of the failure of unique factorization. This is the *class group* of the number field, defined as the group of all fractional ideals of the number field modulo the group of principal fractional ideals. The class group is a finite group and its order is called the class number of the field, and is denoted by h_K. An elementary result asserts that unique factorization is valid in K if and only if $h_K = 1$. The class group is a very complicated (and subtle) invariant of a number field and even for very simple fields class number can be very large, for instance, for $K = \mathbf{Q}(\sqrt{-23201})$, the class number is 292. Many questions of number theory can be solved by using information about the class group For example, a famous theorem of Kummer asserts that the famous equation of Fermat, $x^p + y^p = z^p$, where $p \geq 3$ is a prime number, has no solutions in integers x, y, z and all three nonzero, if p does not divide the class number of the field $\mathbf{Q}(e^{2\pi i/p})$, where $e^{2\pi i/p}$ is a primitive pth root of 1.

Similarly, in the problem of Archimedes, it is evident that any solution $z = x + \sqrt{d}\,y$ of the Archimedes equation is an algebraic integer in the corresponding field $\mathbf{Q}(\sqrt{d})$ and moreover as $x - \sqrt{d}\,y = 1/z$ shows that $1/z$ is also an algebraic integer in R. An algebraic integer z in R such that $1/z \in R$ is called a *unit* of R. Thus the problem of Archimedes can be solved if we can find a unit $X \pm \sqrt{4729494}Y$, with $Y \neq 0$, in the ring of integers of $\mathbf{Q}(\sqrt{4729494})$. One observes that the units of a number field form a commutative (= abelian) group, denoted by U_K, under multiplication. A well-known theorem of Dirichlet asserts that U_K is a finitely generated abelian group; in other words, up to elements of finite order, U_K has a finite basis as a $\mathbf{Z}$-module. The theorem even gives the exact number of basis elements required, this number is called the *rank* of the unit group U_K.

The determination of the group of units and the calculation of class number are important problems of algebraic number theory.

Having motivated the problems, let us discuss the book in detail. The book being reviewed is based on lectures by the author in a seminar at Düsseldorf, held in 1990. There has been a lot of progress in recent times on the computational aspects of algebraic number theory, and the author gives a rapid introduction to some of the recent developments in the subject.

[1] For the detailed discussion of this problem see *Diphantus of Alexandria* by T. L. Heath, page 21. The smallest values of X, Y satisfying this equation are 46, and 41 digit numbers!

After a brief introductory chapter, which provides motivation for the problems discussed in this book, the next two chapters introduce the basic tools which are used in the algorithms developed in this book.

Factorization of polynomials over finite fields is an important tool in algebraic number theory, and the author presents material needed for this in one chapter. There are several methods available to factorize polynomials in one variable over a finite field, and the author presents two of these – the Berlekamp's algorithm and the method of Cantor and Zassenhaus – which have become standard nowadays.

The next chapter starts with basic notions and results from matrix reduction theory like Hermite and Smith normal forms of matrices with integer entries, and proceeds to a discussion of lattices in $\mathbf{R}^n$ and a quick recapitulation of the main results from Geometry of Numbers like Minkowski's convex body theorem, and Minkowski's theorem on successive minima. A major part of the chapter is devoted to reduction theory of lattices. In this section, the author outlines one of the most notable, recent development in the subject: the development of LLL-reduction algorithm. This algorithm, proposed by A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász, has become a fundamental tool in computational aspects of algebraic number theory. For instance, as an application of this algorithm, Lenstra *et al.* proved that problem of factoring a polynomial (in one variable) with integer coefficients into irreducible factors, can be done in polynomial time (in other words, they produced an algorithm to do the factoring, in which the number of steps required is a polynomial in the degree of the polynomial).

Given two vectors u, v in $\mathbf{R}^n$, we can give an order relation between them by using their norms (the norms being taken with respect to the standard norm on $\mathbf{R}^n$). In other words we say $u < v$ if $\| u \| < \| v \|$. This gives a partial order on vectors in $\mathbf{R}^n$. In particular, if L is a lattice in $\mathbf{R}^n$, then this gives rise to a lexicographic partial order on the set of basis vectors for L. A basis of L which is minimal with respect to this order is called a *reduced basis* for L; such a basis has many nice properties. In general such a basis is not unique and also difficult to compute. A weaker notion of reduced basis was introduced by Lenstra *et al.* We briefly recall it here.

If L is a lattice with $v_1, \ldots, v_k$ as a basis, then let $v_1^*, \ldots, v_k^*$ be an orthogonal basis given by the Gram-Schmidt orthogonalization process: thus

$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^*$$

where $1 \le j < i \le k$ and where $\mu_{ij} = v_i^t v_j^* / \| v_j^* \|^2$ for $1 < i \le k$. Then we say that the basis $v_1, \ldots, v_k$ is LLL-reduced if the $\{v_i\}$ and $\{v_j^*\}$ satisfy

1. $| \mu_{ij} | \le 1/2$ for $1 \le j < i \le k$, and

2. $\| v_i^* + v_{i-1}^* \| \ge \frac{3}{4} \| v_{i-1} \|^2$ for $1 < i \le k$.

The LLL-reduced basis does not have as nice properties as a basis which is reduced in the earlier sense. The LLL-algorithm provides an LLL-reduced basis for the lattice L. The LLL-algorithm is a *polynomial time algorithm*, in the sense that the number of steps required to produce the basis is a polynomial in the number of basis vectors. The definition of LLL-reduced basis appears rather unwieldy but despite this, the LLL-algorithm and its variants have proved to be effective in solving a large number of problems – as can be seen from a large number of applications that have been found for it. There are two special applications of this algorithm discussed in this chapter. The first one is to the problem of factorization of a polynomial in one variable, with integer coefficients. As has been mentioned earlier, this problem was solved by Lenstra *et al.* The second application is to a problem of diophantine approximations which comes up frequently in Number Theory. Given vectors $v_1, \ldots, v_{n+1}$ in $\mathbf{R}^n$, we want to find integers $m_1, \ldots, m_{n+1}$ such that $\| \Sigma_i m_i v_i \|$ is small. Thus, for instance, if $v_1 = 1$, $v_2 = \sqrt{d} \in \mathbf{R}$ are two vectors, then we want to find m, n integers such that $|m + n\sqrt{d}|$ is small – and so – m/n is an approximation to $\sqrt{d}$. A large number of problems can be reduced to this problem. The approximation problem can also be solved by means of a suitable variant of LLL-algorithm, which was developed by the author of this book.

In this detailed chapter, the author treats the LLL-algorithm and related applications. This algorithm is explained very nicely by the author. The treatment, though lucid, is lacking in proofs. For instance, to illustrate the application of the LLL-algorithm to factoring polynomials, the author sketches the proof of the theorem of Lenstra, Lenstra and Lovász. For the proofs of the crucial lemmas, the reader is referred to the original paper of Lenstra *et al.* However, we note that for an applications-oriented reader, this treatment is sufficiently detailed and of remarkable clarity in its exposition of the LLL-algorithm. The author also discusses the variant of the LLL-algorithm, called the MLLL-algorithm, which solves the approximation problem alluded to above.

While it may be evident to the learned reader that most of the complexity analysis for the LLL-algorithm carries over to the MLLL-algorithm without much difficulty, it would have been convenient if the author had mentioned a word or two in this regard. Now that we are at it, we would like to point out some other oversights on the author's part: in Lemma 3.6 on page 20, we find that the symbol 't' appears twice in the statement and does so with two different meanings, in one context it is an indeterminate and in another context it appears as an integer subscript index. Such ambiguities, though not very serious, should be avoided.

There are two other algorithms of interest which are discussed in this chapter, but we shall mention them here briefly. Given a lattice L generated by $v_1, \ldots, v_k$ we want to find all vectors v in L such that $\| v \| \le C$, where $C > 0$ is some given constant. This can also be thought of as a problem of determining all the lattice points in a region bounded by a suitable ellipsoid. An algorithm which leads to a solution of this problem is discussed here (the 'quadratic supplement' algorithm). Another algorithm discussed here is the algorithm to find the 'nearest lattice point'.

The range of applications of the MLLL and LLL-algorithm becomes clear in the chapters on computations in number fields. In a short chapter, the author discusses the algorithms for basic arithmetic operations like addition, multiplication and division, in number fields. There is a brief discussion of the basic properties of number fields, like the fact that the ring of integers of number field is free $\mathbf{Z}$-module of rank

equal to the degree of the field. Addition, multiplication are carried out in number fields by means of this basis representation. Here the LLL and MLLL-algorithm find applications.

After this brief discussion of the computational aspects of arithmetic of number fields, the author embarks on a discussion of the problem which we have alluded to earlier: the computation of a **Z**-basis for the ring of integers of a number field, the calculation of a basis for the group of units, and finally the class number of the field.

Let $K = \mathbf{Q}(\alpha)$ be a number field, where α is a root of $f(X) = 0$, where f is an irreducible polynomial of degree n with integer coefficients. Then it is a standard fact that if the discriminant $d(f)$ of f is square-free then $Z[\alpha]$ is the ring of integers of K, and thus the algebraic integers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ form a basis. In practice, however, $Z[\alpha]$ is usually just a subring of K, which is a free module of rank n. Such a subring is called an *order* of K. Any order is contained in the ring of integers of K.

The problem of determining the basis for the ring of integers of a number field K is known (theorem of A. L. Chistov) to be of the 'same complexity' as the problem of finding square-free part of the discriminant $d(f)$, in the sense that if one of them can be done by means of a polynomial time algorithm then so can the other (we remark here that at the moment there is no algorithm available to determine square free part of an integer N and which is polynomial time in $\log|N|$).

There are two main algorithms which are available to determine the basis for the ring of integers of a number field. Both these approaches, called the 'Round-two-method' and the 'Round-four-method' respectively, are based on ideas of Hans Zassenhaus. The idea is to start with some standard order (for instance, in the field $K = \mathbf{Q}(\alpha)$, we take the order $\mathbf{Z}[\alpha]$) in the ring of integers and compute overorders (i.e. orders containing the given order) which are p-maximal for a prime p such that p^2 divides the discriminant. For an order R_0, if p^2 divides the discriminant of R_0, then its p-maximal overorder is defined by $R_p = \{x \in R \mid \exists m > 0, \quad p^m x \in R_0\}$. Once one has determined a basis for all p-maximal overorders, it is possible to write down a basis for the ring of integers. The author discusses the methods of Zassenhaus which are used in explicitly determining the p-maximal overorders. These proceed via calculation of 'p-radicals' and 'ring of multiplicators' of orders. Here some reductions are achieved by factoring polynomials modulo the prime p and lifting these factorizations by Henselian arguments to factorizations modulo higher powers of the prime.

Considering the importance of the problem of computing a basis for the ring of integers, it would have been nicer if the author had discussed the methods in more detail. For, we felt, that the treatment of these methods is a bit terse – and the reader coming across this material for the first time may find it difficult. It would have also been more convenient if the author had summarized the ideas involved in these two methods in an algorithmic form. We also note that the 'core' part of the 'Round-four-method' has not been presented here and so its description here is not quite complete, though the author assures us that in practice the 'core' part is not required, and the Round-two-method used instead.

As we have remarked earlier, a theorem of Dirichlet asserts that group of units U_K of a number field is a finitely generated abelian group of rank $r_1 + r_2 - 1$ where r_1 is the number of distinct embeddings of $K \to \mathbf{R}$ and r_2 is the number of embeddings into **C** up to complex conjugation. We will write ρ for any one of the r_1 embedding into real numbers and ι for any one of the embeddings into complex numbers, up to complex conjugation (thus there are r_2 of these ι's. Thus, for instance, for the field $\mathbf{Q}(\sqrt{4729494})$, $r_1 = 2$ and $r_2 = 0$, and so the unit group is generated (up to elements of finite order) by a single unit, and for the field $\mathbf{Q}(\sqrt{-23201})$ we have $r_1 = 0$, $r_2 = 1$ so that the unit group has rank = 0 and hence is finite. By the phrase 'computation of the unit group' one means the computation of a basis for the unit group, a basis for the unit group is usually referred to as 'fundamental units'. For fields like $\mathbf{Q}(\sqrt{d})$, with $d > 0$, there is a well-known algorithm due to Lagrange which gives a method of computing a fundamental unit is based on continued fraction expansion of $\sqrt{d}$. In general, the unit group is hard to compute. The proof of Dirichlet's theorem introduces a homomorphism from $D : U_K \to \mathbf{R}^{r_1+r_2}$, defined as $D(\varepsilon) = (\log|\rho(\varepsilon)|, 2\log|\iota(\varepsilon)|)_{\rho,\iota}$, whose image is a lattice contained in a suitable hyperplane. This homomorphism is of fundamental importance in the theory of the unit group U_K.

Roughly speaking, a basis for the unit group is computed in three steps. First one needs a lower bound on a fundamental invariant called the regulator of the unit group. The techniques to do this involve ideas from Geometry of Numbers; more specifically, the bound is obtained by means of results from the theory of successive minima. Then the next step (and the most important step) is to construct a subgroup of the group of units which is of finite index. Then the last step is to enlarge this subgroup of finite index. One needs a reasonable upper bound on the index of this subgroup. This is where the result of the first step comes in. Explicit lower bounds on regulator of the unit group and the regulator of the subgroup, together give an upper bound on the index. In the final step, we enlarge the subgroup by computing some additional units and using the MLLL-algorithm to compute a basis for the enlarged subgroup. The major step in the algorithm is the computation of a subgroup of finite index, and to do this the author discusses the two very interesting and efficient approaches which have now become available.

For the second step of the algorithm we have two different methods: 'Dirichlet's method' and 'Lagrange's method'. Both the methods provide a subgroup of finite index in the unit group. The method of constructing a subgroup of finite index in the unit group is based on the observation that the ring of integers of a K contains only finite number of non-associate (two elements are *associates* if their quotient is a unit) elements of bounded norm. Thus by listing a large number of elements of bounded norm, we can in principle generate units. For instance, in Dirichlet's method, for every $j \in \{1, \ldots, r_1 + r_2\}$ one constructs a sequence of elements $\{\gamma_{j,k}\}_{k \geq 0}$ of the ring of integers R, such that (1) $\gamma_{j,0} = 1$, (2) $|\gamma_{j,k+1}^{(j)}| < |\gamma_{j,k}^{(j)}|$, where the bracketed superscript indicates the embedding into **R** or **C**, (3) $|\gamma_{j,k+1}^{(i)}| \geq |\gamma_{j,k}^{(i)}|$ for $i \neq j$, and

finally (4) the $\gamma_{j,k+1}$ have norms bounded by some positive constant C. It follows from Minkowski's theorem that if the constant C is large enough then such a sequence exists. Also since the norms of elements in this sequence is bounded by the constant C, for some pair l, m, $\gamma_{j,l}$, $\gamma_{j,m}$ are associates, i.e. $\gamma_{j,l}/\gamma_{j,m}$ is a unit. One gets several units this way (in fact $r_1 + r_2 - 1$ units). Using the map D it is not hard to prove the linear independence of these units. The actual procedure of computing the sequence $\gamma_{j,k}$ is a modification of this approach, and the author describes the construction of the sequence $\gamma_{j,k}$ in detail. This construction is a generalization of the method of Buchmann-Pethö due to the author. The author also explains that Dirichlet's method can be viewed as a generalization of the continued fraction method. The method of Lagrange is also a generalization of the continued fraction method, based on ideas of Buchmann, and depends largely on methods of Geometry of Numbers. This method is also treated in depth here. This method also has applications to testing if a given ideal is principal or not – this comes up in the class number calculations.

In contrast to the discussion of the problem of determining a basis for the ring of integers, the exposition of the algorithms to compute a basis for the group of units is elaborate and lucid. The chapter ends with an example of a computation of units using the methods outlined in the chapter.

It has been mentioned earlier that the class group is a measure of failure of unique factorization in number fields. It is a very subtle invariant of the number field (and hence also the most interesting). The *class group* is defined as the quotient of the group of fractional ideals by the subgroup of principal fractional ideal; a *fractional ideal* in K is an R-submodule of K; a principal fractional ideal is an R submodule of K generated (as an R-module) by a single nonzero element of K. An R-submodule of K which is contained in R is an *ideal* of the ring R, an ideal I of R *divides* an ideal J of R if and only if $J \subset I$ ('to contain is to divide'). Thus one can extend the usual notion of divisibility and primality to ideals of R. It is a standard fact that every ideal of R can be uniquely expressed as a product of powers of prime ideals in R. In particular, it follows that every fractional ideal is a product of integer-powers of prime ideals. Thus with ideal arithmetic one has restored the uniqueness of factorization; moreover, if every prime ideal is principal in K then unique factorization is valid in the field K. However, note that there are examples of number fields where not every prime ideal of K is principal. For instance consider the case $K = \mathbf{Q}(\sqrt{-5})$, the prime ideal $(2, 1 + \sqrt{-5})$ is not principal. The fractional ideals form a group under ideal multiplication; and the principal fractional ideals form a subgroup. The class number is the index of the subgroup of principal fractional ideals in the group of fractional ideals. Two fractional ideals are said to be *equivalent* if they differ by a principal fractional ideal. An ideal class is an *equivalence class* of fractional ideals. Thus to study the class group we have to study arithmetic operations on fractional ideals. For fields like $\mathbf{Q}(\sqrt{\pm d})$, the class group has another equivalent interpretation in terms of quadratic forms (which was initiated by Gauss) and for these fields there exist alternative algorithms to compute the class group.

The chapter on computation of class number begins with a discussion of ideal arithmetic. It is evident that any discussion of algorithmic ideal arithmetic should be augmented with a discussion of presentations -(and representations) of ideals in number fields, and there are several ways of representing an ideal in a number field. For instance, any ideal can be thought of as a $\mathbf{Z}$-submodule of the ring of integers R, and hence be represented in terms of a $\mathbf{Z}$-basis or alternately, one can use the special fact that every ideal of R can be generated (as an R-module) by two elements, and hence can be specified by giving two generators.

A very well-known theorem of Minkowski asserts that every ideal class contains an ideal of bounded norm. Minkowski's theorem provides the bound explicitly. Using this bound, we first write down a list of all primes p which are less than or equal to this bound and then calculate all prime ideals in R which contain p; this gives a finite list S, of prime ideals (with norms bounded as above). The class group is generated by this finite set of prime ideals. The main problem which comes up at this stage is that most of the time, the list of prime ideals contains far too many elements (even if the class number is small) – for number fields of large degree and discriminant this can be a serious problem; another problem is to determine all the relations (in the class group) which exist amongst the prime ideals in our list. The first one can be tackled by trying to improve the norm bound – this can be done for small degree fields, in general reasonable bounds exist under some conjectural hypothesis. Thus it remains to find an efficient procedure to determine all relations (in the class group) amongst these prime ideals. This is the underlying principle of the algorithm presented in this chapter. The author discusses a method of calculating the class group which in principle mimicks the proof of Dirichlet's theorem on units. The idea is to use a suitable variant of the map D which we had described earlier, this time from S-units to a suitable real vector space, and whose image is a lattice. This approach, after suitable modifications, leads to a suitable matrix of 'relations', called the class-group matrix. In practice this tends to be large and rather unwieldy. Using the reduction theory of matrices developed in the earlier chapter, the author indicates a procedure to compute the class group. Note that this yields a bit more information than just the class number – it provides the complete structure of the class group.

On the whole, we felt that the discussion of the algorithm to compute the class group, which is presented here, is terse. We would like to reiterate that it would have been nice if the method was summarized in a convenient algorithmic form. One also notes that there is no discussion of alternate methods available to compute the class group: for small fields like quadratic fields, one has alternate methods available to compute the class group (using quadratic forms and theory of genera). There is no discussion of analytic methods, which rest on the class number formulae, and which can be used at least in some cases.

The book ends with a brief description of a package, KANT V2, which implements most of the algorithms presented in this book, the package was developed by a group of researchers based originally at Dusseldorf, and is available free of charge on most electronic networks (by ftp) It appears

that the package is no longer available from the Düsseldorf address as mentioned in the last paragraph of page 84, and so this information appears to be out of date.

The subject of constructive (or computational) algebraic number theory is rapidly developing branch of number theory and this book provides a quick introduction to this subject. Beginning with the basic notions, the author quickly takes the reader to the most recent developments in the subject. It is a suitable text for students who are familiar with some basic algebraic number theory, it contains a large number of exercises and some very explicit examples. Researchers in the field will also find the book stimulating. In recent years, number theory has found a number of applications in coding theory, cryptology and other branches of computer science and this book will also be valuable to researchers from these fields too.

The author has explained the fundamental ideas of the subject with remarkable clarity. The treatment of the subject, though lucid, is lacking in proofs – however this should not be considered a disadvantage, for the author gives detailed references to the proofs of the results which are used in the book. One thing, which we feel, is lacking: algorithms are presented in the last three chapters of the book without any reference to complexity analysis. Here the author should have mentioned if the analysis was not available or pointed to literature where it is carried out In a book as quintessentially algorithmic as this, the importance of complexity analysis need not be stressed.

We recommend this book as a 'must' for all those interested in computational aspects of algebraic number theory, and also for students of algebraic number theory. In recent years, there has been a resurgence of computational-experimental techniques in Number Theory. One need only recall the examples of Birch–Swinnerton–Dyer, Zagier conjectures which were discovered computationally and which have played a significant role in the development of the subject. This book is a good introduction to the computational aspects of the subject, written by one of the well-known experts in the area.

KIRTI JOSHI

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005, India

Boffin: A Personal Story of the Early Days of Radar, Radio Astronomy and Quantum Optics. R. Hanbury Brown, FRS. Adam Hilger, Techno House, Redcliffe Way, Bristol BS1 6NX, England. 1991. Price: unknown.

It is well recognized that World War II provided the technical training ground and much of the impetus for the expanded conception of astronomy which emerged in the immediate post-war period. Many of the radio astronomy pioneers, for instance, worked during the war on developing the air defence system which we now know as radar. Many went on to make major contributions to these growing new fields and subsequently became well known in astronomy circles. Some of the radar figures, in particular, have documented their experiences, and this small book joins the others in providing a detailed, personal account of the seriousness, excitement and romance of those years.

Indeed, just over half of Hanbury-Brown's *Boffin* is devoted to these formative 7 or 8 war years, and he writes of them with an almost monkish sense of vocation. Born in India of an Army family, perhaps he came to it naturally. For one whose '... greatest anxiety ... was to be self-supporting because my step-father had disappeared in a cloud of debt when I was sixteen ...', it took a considerable faith or trust to quit school well short of the PhD and take a secret, low-paid job with the Air Ministry on the sole strength of Sir Henry Tizard's advice. 'Looking back', he says, 'I am glad I did; sometimes the morrow does 'take thought for things of itself'.

Within a fortnight he found himself in the places and among the people most closely associated with the British pre-war effort to cadge together a workable 'RDF' system – that is, Radiolocation and Direction Finding – for immediate use in the anticipated air war with Germany. This was 1936 in the parlors and stables of Bawdsey Manor in Suffolk and at a disused World War airfield on the nearby 'island' of Orfordness. 'No one who worked at Bawdsey in those early days will even forget the place', he writes. 'It was magical. The Manor was a fairy castle on a distant shore and had the quality of a dream ...' 'On the "island" there was ... a WWI aerodrome, ... vast stretches of windswept shingle and some wooden huts on whose walls there were still notices signed by the Station Adjutant in 1918. It was a desolate, forbidding place whose only redeeming features were the birds.'

This early effort under Sir Robert Watson-Watt was aimed entirely at the development of what we would now call ground-based radar (in whose words the latter was 'a synthetic palindrome *invented by our friends the Americans*'). Technically, the group worked on increasing the range of detection and on refining the means for determining the direction and height of the aircraft. The wavelength was decreased first from 50 metres to 26 metres and ultimately to 13 – then a challengingly high frequency – and transmitter power to the 100 kW level in 20 microsecond pulses. Members of the crew became used to stringing wires at the top of high towers and to sparing no effort to keep the cranky equipment working during the visits of the *many air defence VIPs* – including Winston Churchill – who came to inspect the work. The personal effect of this experience on Hanbury-Brown is telling

Later, when we got the whole radar working, we spent most of our time measuring its performance on target aircraft. I never got tired of watching the radar echo from an aircraft as it appeared first as a tiny blip in the noise on the cathode-ray tube, and then grew slowly into a big deflection as the aircraft came nearer. The strange new power to 'see' things at great distances, through clouds or darkness, was a magical extension of our senses....

Hanbury-Brown remarks at length about how technically amateurish and bureaucracy-bound this whole effort was, 'more suited to bird-watching than to the development of advanced electronics.' 'We had ... no proper workshop and ... few tools [and] also had very little of the test gear which, even in those days, one might reasonably expect to find in a modest radio laboratory... As for books, the only one I can remember seeing is a copy of the *Radio Amateur's Handbook* which belonged to [a colleague] who was a devoted ham.' 'At first I could not understand why anyone ... could allow this to happen when the work was so