tion of a few early ones that ask the reader to verify as yet undefined properties, quite appropriately located. Those following Chapters three and six, as has already been pointed out, are particularly lovely; no less so are those following Chapter seven. There are one or two lapses in the otherwise exceptionally smooth, unhesitating, yet comfortably paced exposition, most notably in the last eight lines of page 130, where the author's notation does not convey his intentions (what he has in mind is to be found on pp. 124 ff. of his notes "Abelian categories: the inside theory"), and again, to a lesser extent, in the second five lines of p. 128, where the desire for brevity has all but banished clarity. Everywhere else, the writing is crisp, informative, and unambiguous; and it sweeps the reader gently but unhesitatingly forward to its goal.

In sum, one may quibble about what else should have found room in Freyd's book, but considering it as it comes to us, it is well produced, has worthwhile things to say, and says them clearly and with determination. Any algebraist—indeed, any modern-minded mathematician, whether full-fledged or nestling—will probably want to read at least parts of it at least once.

F. E. J. LINTON

Number theory.[1] By Z. I. Borevich and I. R. Shafarevich, Moscow, 1964.

The Russian mathematicians have for many years been partial to number theory, and it is an interesting speculation why this should be so. Can it be due to the influence of Euler who spent many years in the later part of the eighteenth century in what was then called St. Petersburg, or perhaps to some characteristic of the Russian mind? Be it so or not, they have long been known for their numerous contributions to the subject. They have originated many new ideas and made a large number of really important and fundamental discoveries. These have opened up new avenues of investigation and have had far reaching effects and influence on the development of the theory.

One calls to mind the work of Tchebycheff on prime numbers, of Markoff on the minima of indefinite binary quadratic forms, the work of Korkine, Zolotareff, Voronoi on quadratic forms in several variables, the work of Khintchine on the density of sequences of numbers and on Diophantine approximation, Tartowski on Diophantine equations, Tchebotareff on the minimum of the product of linear poly-

[1] An English translation is being prepared by the Academic Press.

nomials, Delone on the number of representation of integers by binary cubic forms, the work of Romanoff and Schnirelman on the density of sequences and applications to prime number theory, the proof by Gelfond of the transcendance of a^b, Linnik's result on the representation of large numbers as the sum of seven positive cubes, and the estimate for a prime in an arithmetical progression, and also the numerous and far reaching results of Vinogradoff on many of the most difficult and interesting aspects of analytic number theory, e.g. the representation of large odd numbers as a sum of three primes, on the residues of polynomials mod 1, Waring's problem, and the number of lattice points in regions, and the prime number theorem.

This list, though incomplete, is most impressive. Hardly any part of number theory has not been enriched or remains untouched by the researches of the Russian mathematicians.

They have also written many worthwhile books on number theory. One notes the book by Nazimoff on applications of elliptic functions to number theory, of Venkov on number theory, of Delone and Faddeev on irrationalities of the third degree, Khintchine's three pearls of number theory, and also his book on continued fractions, Gelfond's book on transcendental numbers, of Vinogradoff's elements of number theory and the method of trigonometric sums in the theory of numbers, and lastly the book by Gelfond and Linnik on elementary methods in analytical number theory.

These books are characterized by a novelty in outlook, originality in presentation, a freshness of treatment, and by a wealth of material sometimes not often found elsewhere, and an appreciation of what is interesting and significant in number theory. Some are designed as text books but more often as treatises. They have been a most welcome and valuable addition to the literature and have rejoiced the hearts of their readers. Fortunately all of these books, Nazimoff in part, have been translated into English except Venkov (written about 25 years ago) and it is to be hoped that this will also be translated. Now there has appeared very recently another book on number theory by Borevich and Shafarevich. This is a worthy follower in the tradition established by their countrymen. It may be said at once that this is one of the most delightful and charming books it has been my good fortune to read. I have found it also suggestive and inspiring. The exposition is most attractive and a model of clarity. The details are so presented that reading is a pleasure. The authors really make themselves understood and set a good example to other writers.

The subject matter has been taken both from the classical theory and from recent developments and contains many important and

interesting results not to be found in other books. One is grateful to the authors for taking their readers on what seems like a personally conducted tour through a pleasant and extensive section of number theory.

There are also many interesting historical notes about recent advances in some of the topics dealt with. Though many references are given, there are theorems, demonstrations and problems to which no names are attached. It would have been interesting to have had them. Finally there is a very nice collection of problems at the end of most chapters not only often important in themselves, but also in amplifying the text.

This delectable book should be acquired by every one who has more than a passing interest in number theory. Fortunately the English translation will soon be available and so the book is sure to have many readers. All will join with me in thanking the authors for the treat provided for their readers.

As stated in the authors' preliminary remarks, the book is devoted to an account of the principal methods for the study of indeterminate equations, chiefly algebraic but also geometric and analytical. The book is divided into five parts, each containing seven or eight chapters. The parts deal respectively with (1) congruences, (2) the representation of numbers by decomposable forms, (3) the theory of divisibility, (4) local methods, (5) analytical methods. The book ends with some supplementary algebraic miscellanies and some tables.

The subject matter is so rich in content that it is well worthwhile to give some details.

Part I is devoted to congruences in their widest and most general aspect e.g. the congruences $f(x)=f(x_1, x_2, \cdots, x_n)\equiv 0 \pmod{p^r}$, where $f(x)$ is a polynomial in n variables and p is a prime number and r is any positive integer. There is Chevalley's theorem that if $r=1$ and n exceeds the degree of $f(x)$, then if there is one solution, there exists another, and further the number of solutions is divisible by p. When $r=1$, application is made of the formula $pN=\sum_{t=0}^{p-1}\sum_{(x)=0}^{p-1} e^{2\pi i t f(x)/p}$ for the number of solutions of $f(x)\equiv 0 \pmod{p}$, to the case $f(x)=\sum_{r=1}^{n} a_r x_r^k$, and Weil's results on these are proved. Gauss' sums are introduced. The p' adic numbers are dealt with at length. Their metric is defined by the usual valuation and their compactness property is proved. The relation between a p' adic equation $f(x)=0$, and congruences $f(x)\equiv 0 \pmod{p^r}$ is discussed when a non-singular solution of the congruence is known. Weil's estimate for the number of solutions of $f(x)\equiv 0 \pmod{p}$ is mentioned, and this is used to show that $f(x)\equiv 0 \pmod{p}$ is solvable for all large p.

Special attention is given to the case when $f(x)$ is a quadratic form in n variables with p' adic coefficients, and conditions are given that it should represent zero in the p' adic field. Consideration is then given to the case when the coefficients and the variables are rational integers. When $n=3$, this leads to the study of Hilberts norm residue symbol. When $n \geqq 3$, proof is given of the theorem of Minkowski-Hasse that $f(x)=0$ is solvable in rational integers if and only if $f(x)=0$ is solvable in the real field and p' adically, i.e. that the congruence $f(x) \equiv 0 \pmod{p^r}$ is solvable for all primes p and $r>0$. Finally, the equivalence of two quadratic form $f(x), g(x)$ is discussed from the same point of view.

Interesting remarks and results are given for congruences of higher degree and many variables. Thus an equation of degree n and with n^2 variables is constructed which does not represent zero in a p' adic field.

Part II is concerned with the representation of numbers by the decomposable forms appearing as the norm of linear forms in n variables whose coefficients are algebraic numbers in a field K of degree n. The coefficients of the linear forms define a module and the usual properties of modules are developed e.g. their bases, the geometric representation of the points given by the linear forms and estimates for the magnitude of numbers represented by them. Then the properties of the units in algebraic number fields and their group structure are investigated. This leads to the solution of the problem of representing a number as the norm of a number in the field K. Finally application is made to binary quadratic forms.

As an illustration of the interesting examples given in the book, one might mention an application of Minkowski's theorem on lattice points in convex bodies which has been used for the units of an algebraic number field. A proof is given of Cassels's theorem that the equation $ax^2+by^2+cz^2=0$, where a, b, c do not all have the same sign, are square free, are relatively prime in pairs, and $ax^2+by^2+cz^2 \equiv 0 \pmod{4abc}$ is solvable, has an integer solution $(x, y, z) \neq (0, 0, 0)$, such that $|a|x^2+|b|y^2+|c|z^2<4|abc|$. The inequality is new.

Section III deals with the most general aspect of the theory of divisibility and of factorization. It begins with the proof that the first case of Fermat's last theorem holds, namely, that the equation $x^l+y^l=z^l$ has no integer solutions for which $(xyz, l)=1$, provided that unique factorization holds in the cyclotomic field $R(e^{2\pi i/l})$, where l is an odd prime. Then a generalized Euclidean algorithm is discussed for the numbers of a ring Q in an algebraic number field.

Divisors and their properties are introduced and studied axiomati-

cally. Let Q be a commutative ring in an algebraic number field K with a unit. The fundamental problem is to imbed Q in an aggregate D in which multiplication can be defined and in which unique factorization holds. If this is possible, then a theory of divisors is said to exist for Q. In particular the ring Q is integrally closed in K.

Divisors lead naturally to the theory of non-archimedean valuations and their various properties, e.g. the basic approximation theorems, and to the continuation of the valuations to algebraic extensions of K.

An account is given of Dedekind rings and the relation of divisors to the usual ideals. It is shown that the number h of classes of divisors is finite. Then the first case of Fermat's theorem is shown to hold when $(l, h)=1$.

The factorization of small primes in the quintic field $R(\sqrt[5]{2})$ and in the cubic field $R(\theta)$, where $\theta^3-9\theta-6=0$ are given, and a class number is found. The section closes with a chapter on quadratic fields.

This section contains many of the fundamental properties of algebraic numbers. Again attention must be drawn to the really interesting problems at the end of the chapters.

Section IV is devoted to local methods. Here the fundamental problem is—is the equation $f(x_1, x_2, \cdots, x_n)=0$ solvable in integers if the congruence $f(x_1, x_2, \cdots, x_n)\equiv 0 \pmod{M}$ is solvable non-trivially for all M, or put slightly differently—does solution in all p' adic fields, i.e. local solutions, imply integer solutions, i.e. a global solution?

This will require the study of the p' adic fields. Let k be a field complete with respect to some non-archimedean valuation, O the ring of the integer elements of k, π the prime element of O and S a complete system of residues of the ring O mod π. Then every element of k can be expressed uniquely in the form

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i, \quad \text{in which} \quad a_i \in S, \qquad m \leqq i < \infty.$$

Then the finite extensions of such a field are considered and their properties and the decomposition of polynomials are discussed.

The object of this section is the application to Diophantine equations. This involves the study, in a complete field, of analytic functions defined by infinite series, in particular, of the exponential and logarithmic functions. Skolem was the first to apply p' adic methods. The equations considered are of the form

$$N(x_1\mu_1 + \cdots + x_m\mu_m) = a,$$

say

$$N(\alpha) = a, \qquad \alpha \in M,$$

where $\mu_1, \cdots, \mu_m$ are numbers in some algebraic number field K of degree n, and $M = \{\mu_1, \mu_2, \cdots, \mu_m\}$, $(m \leqq n)$ is the module generated by the μ. The module M can be imbedded in a complete module $M' = \{\mu_1, \mu_2, \cdots, \mu_m, \mu_{m+1}, \cdots, \mu_n\}$. The general theory gives a solution of

$$N(x_1\mu_1 + \cdots + x_n\mu_n) = \alpha$$

in rational integers $x_1, \cdots, x_n$.

The problem now is to determine those solutions for which $x_{m+1} = \cdots = x_n = 0$. The general solution can be written in the form

$$\alpha = y_j\epsilon_1^{u_1} \cdots \epsilon_r^{u_r},$$

where the y are a finite set satisfying $N(y) = a$ and the ϵ are a fundamental set of units in the field K. The condition that $x_{m+1} = \cdots = x_n = 0$ is given by $n - m$ equations of the form

$$\mathrm{Tr}(y_i\mu_i^*\epsilon_1^{u_1} \cdots \epsilon_r^{u_r}) = 0, \qquad i = m + 1, \cdots, n,$$

where Tr denotes the trace, and the μ_i^* are appropriate constants. Here $u_1, \cdots, u_r$ are unknown integers. The equations, however, are treated by considering the u to be p' adic integers. Thue's theorem that if $f(x, y)$ is an irreducible binary form with rational coefficients of degree $\geqq 3$, then $f(x, y) = c$ has only a finite number of integer solutions, is proved except for the particular case when the linear factors of $f(x, y)$ are all real.

The section ends with an account of local analytical manifolds. Their properties are similar to those in the usual theory.

Section V is concerned with analytical methods, really the discussion of the series obtained for various important arithmetical entities. Thus the formula for the number of classes of divisors of an algebraic number field requires the study of the Dedekind-zeta functions. For the cyclotomic field this leads to the L function and to Dirichlet theorem for the primes in an arithmetical progression, and also to the class number for quadratic field.

The formula for the cyclotomic field is discussed at length. The class number is expressed as the product of two factors and these are of significance in the application to Fermat's last theorem. Criteria in terms of the Bernoulli numbers are given for the cyclotomic field to be regular, and Fermat's last theorem is proved for regular primes. The properties of the Bernoulli numbers are discussed and it is shown that an infinity of irregular primes exist.

The book has a final section containing some algebraic miscellanies. Thus quadratic forms with coefficients in a number field are discussed. Witt's theorem is proved, namely, that if f, g, h are non-singular quadratic forms and the direct sum of $f+g$ is equivalent to the direct sum $f+h$ then g and h are equivalent. Brief accounts are given of algebraic extensions, finite fields, commutative rings, characters.

The tables at the end of the book contain the class numbers and the units for the quadratic fields $R(\sqrt{d})$ with $|d|<500$, the class numbers for the cubic fields $R(\sqrt[3]{m})$ for $m \leqq 47$ and for some other values of m, and also some results connected with Fermat's last theorem, e.g. the irregular primes $\leqq 400$.

The account given here may show what a really useful and satisfying book this is.

L. J. MORDELL