BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 2, Number 2, March 1980

0002-9904/80/0000-0108/$02.75

BOOK REVIEWS

Algebraic number theory, by Robert L. Long, Pure and Applied Mathematics, Marcel Dekker, New York and Basel, 1977, ix + 192 pp., $18.50.

A classical invitation to algebraic numbers and class fields, by Harvey Cohn, with two appendices by Olga Taussky, Universitext, Springer-Verlag, New York and Berlin, 1978, xvi + 328 pp.,$14.80

Number fields, by Daniel A. Marcus, Universitext, Springer-Verlag, New York and Berlin, 1977, viii + 279 pp.,$14.00

Virtually the entire development of modern algebraic number theory was motivated by the attempt to explain and to generalize a simple but very surprising fact about positive whole numbers which Euler first discovered in the 1740s. He was pursuing some problems Fermat had posed relating to numbers of the form $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$ and $x^2 + 5y^2$. For a given integer n, a prime p is said to "divide $x^2 + ny^2$ nontrivially" if there exist integers x and y, not both divisible by p, such that p divides $x^2 + ny^2$. Euler's surprising discovery was that *the answer to the question of whether p divides* $x^2 + ny^2$ *nontrivially depends only on the class of p* mod $4n$.

To say that there is no obvious reason why this should be so is an extreme understatement. Euler was relatively young when he first made the discovery, and, although he clearly understood the importance of the phenomenon and returned to it many times throughout the rest of his life, he never made any substantial progress toward a proof except in a few special cases like $n = 1$, ± 2, ± 3. His knowledge of the phenomenon rested purely on the empirical evidence of many numerical examples.

He observed another, equally puzzling phenomenon, which is closely related to the first. For a given n, let $\chi_p(n)$ be $+1$ if the prime p divides $x^2 - ny^2$ nontrivially and -1 otherwise. (The sign is changed in order to make χ_p a character mod p. As far as Euler's theorems are concerned, the sign of n is immaterial.) The statement above is that $\chi_p(n)$ depends only on the class of p mod $4n$. Euler went on to observe that *the mapping* $p \mapsto \chi_p(n)$ *is a homomorphism* in the sense that if p_1, p_2, p_3 are primes with $p_1 p_2 \equiv p_3$ mod $4n$ then $\chi_{p_1}(n)\chi_{p_2}(n) = \chi_{p_3}(n)$. Moreover, this homomorphism is *onto* the two element group $\{\pm 1\}$ except when $n = a^2$ for some integer a (in which case the choice $x = a$, $y = 1$ gives $x^2 - ny^2 = 0$ so that *all* primes p divide $x^2 - ny^2$ nontrivially). Note that, for fixed p, the map $n \mapsto \chi_p(n)$ obviously depends only on the class of n mod p; almost as obviously (see below) it is a homomorphism from the group of classes of integers relatively prime to p mod p to the group $\{\pm 1\}$, and this homomorphism is onto. Euler's observations about $p \mapsto \chi_p(n)$ are of a different order of difficulty altogether from these facts about $n \mapsto \chi_p(n)$.

Assuming the truth of these theorems, it is easy to find, for given n, the primes which divide $x^2 - ny^2$ nontrivially. For example, let $n = -5$. Then $1^2 + 5 \cdot 1^2 = 6 = 2 \cdot 3$ shows that $\chi_3(-5) = +1$. Therefore $\chi_p(-5) = +1$

whenever p is congruent to a power of 3 mod $4n$, that is, whenever $p \equiv 3, 9, 7, 1 \bmod 20$. With the exceptions of 2 and 5 (which obviously divide $x^2 + 5y^2$ nontrivially) every prime is in one of the 8 classes 1, 3, 7, 9, 11, 13, 17, 19 mod 20. These classes form a multiplicative group and $p \mapsto \chi_p(-5)$ defines a homomorphism of this group onto $\{\pm 1\}$. The kernel of this homomorphism has 4 elements, so the elements in the kernel already found account for them all and $\chi_p(-5) = -1$ if $p \equiv 11, 13, 17, 19 \bmod 20$.

It is trivial to show that $\chi_p(n) = +1$ if and only if the congruence $x^2 \equiv n \bmod p$ has a solution (on the one hand $x^2 - n \cdot 1^2 \equiv 0 \bmod p$ gives a nontrivial division by p, and on the other hand if $x^2 - ny^2 \equiv 0 \bmod p$ is a nontrivial division by p then $y \not\equiv 0 \bmod p$ and division by $y \bmod p$ solves the congruence) and it is in this way, rather than in terms of divisors of $x^2 - ny^2$, that the number denoted $\chi_p(n)$ above has most often been described since Euler's time.

In particular, Legendre defined his famous symbol (n/p), for p prime and n not divisible by p, to be $\chi_p(n)$, that is, to be $+1$ if the congruence $x^2 \equiv n \bmod p$ has an integer solution and to be -1 otherwise. He used this symbol to express an amazing fact which he discovered in the late 1780s: *Let p and q be distinct odd primes. If either $p \equiv 1 \bmod 4$ or $q \equiv 1 \bmod 4$ then $(p/q) = (q/p)$ but if $p \equiv q \equiv 3 \bmod 4$ then $(p/q) = -(q/p)$.* He called this, for obvious reasons, the *law of reciprocity*. His efforts to prove it fell short of the mark.

Legendre apparently did not recognize the relationship between his law of reciprocity and Euler's work, but Gauss, who was the first to give a rigorous proof of the reciprocity law, noticed how close the connection was, saying that it would be easy to deduce Legendre's law if Euler's theorems were known. Kronecker gave [2] an explicit deduction of the law of reciprocity from the two theorems of Euler stated above and from an additional theorem, also observed by Euler, which says that if n is positive and $p \equiv -1 \bmod 4n$ then $\chi_p(n) = +1$. (See [1, pp. 291–292]. The essential observation is that $\chi_p(q) = +1$ whenever $p \equiv \pm k^2 \bmod 4q$, that is, q is a square mod p if and only if $\pm p$ is a square mod $4q$.)

The term "law of reciprocity" caught the imaginations of later generations of number theorists. This had an unfortunate effect on the development of the subject, because it forced the generalizations of the law into a form that they did not seem to want to take. Indeed, the modern generalization known as the "Artin reciprocity law" expresses no reciprocal relationship whatsoever and is instead a generalization of Euler's original version of the law. In short, the notion of reciprocity has had to be separated from the law of reciprocity.

About the only later number theorist who did not use the term "law of reciprocity" was Gauss, who gave the first rigorous proof of the law. He called it the "fundamental theorem" and, as is well known, he published six different proofs of it. It is less well known that he devoted so much effort to these proofs not just out of an interest in the theorem itself but also out of an interest in its generalizations, which, as he said in his introduction to his treatise of 1818 giving the 5th and 6th proofs, he had found long before by an empirical study of the evidence but which long resisted his efforts at a proof.

Gauss's generalizations, which were almost immediately named (by others) the laws of "cubic and biquadratic reciprocity", were, very briefly, as follows. First, he observed after extensive examination of examples that the study of 3rd or 4th roots mod p in the integers becomes intelligible only when the integers are *extended* by the adjunction of a 3rd root of unity ω or a 4th root i respectively. For example, in the case of 4th roots, this means that 5 should no longer be regarded as prime because $5 = (2 + i)(2 - i)$. Thus, in the case of 4th powers one considers what are now called the *Gaussian integers*, the ring $Z[i]$. If p is any prime Gaussian integer then $Np = p\bar{p}$ is always an integer that is congruent to 1 mod 4 and the multiplicative group of nonzero Gaussian integers mod p is *cyclic* of order $Np - 1$. Therefore, provided $D \not\equiv 0 \bmod p$, D is a 4th power mod p if and only if $D^{(Np-1)/4} \equiv 1 \bmod p$. Since the fourth power of $D^{(Np-1)/4}$ is 1 mod p, it must be one of the four fourth roots of unity ± 1, $\pm i$ mod p. Define $\chi_p(D)$ by $\chi_p(D) \equiv D^{(Np-1)/4}$ mod p, $\chi_p(D) = \pm 1$ or $\pm i$.

For fixed p, the mapping $D \mapsto \chi_p(D)$ is obviously a homomorphism from the multiplicative group of nonzero Gaussian integers mod p to the four element group $\{\pm 1, \pm i\}$. Gauss found that the unexpected phenomenon from the quadratic case carried over to fourth powers as well, namely, the mapping $p \mapsto \chi_p(D)$ is a homomorphism in p, not mod D but mod a multiple of D. Specifically, *the value of* $\chi_p(D)$ *depends only on the class of* p mod $16D$ *and* $p \mapsto \chi_p(D)$ *defines a homomorphism from the group of classes of Gaussian integers* mod $16D$ *relatively prime to* $16D$ to $\{\pm 1, \pm i\}$. There is a little more to Gauss's law of biquadratic reciprocity than this, relating the value of $\chi_p(q)$ for q prime to that of $\chi_q(p)$, but the real surprise is that $p \mapsto \chi_p(D)$ is a homomorphism mod $16D$.

Gauss never published a proof of the theorem for 4th powers, and for third powers he never even published the *statement* of the law. Naturally this stimulated younger mathematicians–notably Jacobi, Dirichlet, Eisenstein, and Kummer–to try to discover them for themselves. This, more than anything else, led to the creation of modern algebraic number theory.

It was quickly discovered that the cases of 2nd, 3rd, and 4th powers were especially simple in that the fields Q, $Q(\sqrt[3]{1})$, $Q(\sqrt[4]{1})$ have a *finite number of units*–so that a prime modulus corresponds to only a finite number of prime numbers–whereas this no longer holds for $Q(\sqrt[n]{1})$ for $n \geqslant 5$ ($\sqrt[n]{1}$ = a primitive nth root of unity). The problem was further complicated by Kummer's discovery in 1844 that unique factorization does not generally hold in $Q(\sqrt[n]{1})$, so that it is not even meaningful to speak of "primes" in the general case unless one means "ideal primes" in the sense defined by Kummer in 1847.

In 1847, Kummer overcame these difficulties and discovered what he believed to be the correct statement of the law for λth powers in all cases where λ is a prime which is "regular" (that is, λ does not divide the class number of $Q(\sqrt[\lambda]{1})$). However, as Gauss had found in the cases 2, 3, and 4, the discovery of the statement of the law was much easier than a discovery of the proof.

After three years of unsuccessful efforts to prove the law himself, Kummer

"in the interest of science" published it in 1850 in order to make it "the common property of all mathematicians working toward the advancement of number theory." One's admiration of Kummer's altruism in publishing the law and running the risk that someone else might prove it is diminished somewhat by the fact that Eisenstein only a few weeks later published on the same subject, stating and even *proving* Kummer's law in a special, very restricted, case. Could it be that Kummer knew of Eisenstein's impending publication and wanted at least to establish his priority in the discovery of the statement?

In any case, Kummer did after all have the distinction of giving the first proof of the general law, although it took him another 9 years to find it. In the final proof a central role is played by the fields which Hilbert later named "Kummer fields", namely, fields of the form $Q(\sqrt[\lambda]{1}, \sqrt[\lambda]{D})$ where $D \in Q(\sqrt[\lambda]{1})$, and the *theory of factorization* in such fields, including the "ideal primes" and the "class group" which Kummer had first defined in connection with the cyclotomic fields $Q(\sqrt[\lambda]{1})$.

Kummer's theorem was by no means the end of the story. As always seems to be the case in mathematics, the new questions it raised were more numerous than the old ones it resolved. Could the proof be simplified? What about primes such as $\lambda = 37$ which are not regular? What about composite values of λ? And, perhaps most interesting of all, the following question, which is a clear generalization of the original question raised by Euler's observation: Kummer's reciprocity law implies that when one passes from a cyclotomic field $Q(\sqrt[\lambda]{1})$ to a Kummer field $Q(\sqrt[\lambda]{1}, \sqrt[\lambda]{D})$ containing it, the way in which a prime p in the small field factors in the big field *depends only on its class* mod λD. What underlies this phenomenon, and for what field extensions do similar phenomena occur?

This is the central question of the subject of modern number theory that goes by the awe-inspiring name of "class field theory".

Robert L. Long begins the Preface of his book *Algebraic number theory* with the words, "As one question gives rise to another, pure mathematics arises from the conceptual framework within which man organizes his experience." When a book has such a beginning, one expects something other than the usual *ad hoc* style of contemporary mathematical writing. Unfortunately, this expectation is not fulfilled.

On the contrary, the exposition is almost entirely unleavened by motivation or insight. There are very few connective passages. A typical one is the one on p. 46:

> We now turn to the more detailed study of finite extensions of a field which is complete under a discrete valuation. Those results which do not depend on completeness are given first. The separate consideration of totally ramified and unramified extensions is justified in Exercise 31. . . .

So much for one question giving rise to another. By the way, Exercise 31 has no apparent connection with ramified or unramified extensions, and reference should probably be made to Exercise 32 instead.

The experience of reading a book like this reminds me of the game in which one is required to eat a certain number of dry crackers and then

whistle. After reading for a few minutes I find my mathematical juices entirely dried up and feel incapable of whistling even the simplest tune–not to mention working 31 exercises.

This is the more regrettable because the book covers a great deal of important material. The author has a good command of the subject and his treatment is basically sound. His style is unpretentious and direct, and his proofs are clear. The problem, for this reader at least, is that the material is so condensed that it is indigestible.

It is a shock to see the book referred to as a "textbook" on the back cover. I think the book has utility as a monograph for readers already versed in the subject who want to review it from another point of view, or as a sort of encyclopedia article giving condensed treatments of various topics. And I am prepared to entertain the notion that we have raised a generation of automata able to plow their way through this kind of mathematics and store it in their databanks. But I would not recommend this book even for a very highly motivated beginner in algebraic number theory, much less for an ordinary graduate student.

In fairness to the author, who is clearly a dedicated and able mathematician, I should say that the book's failing is the same as that of most contemporary books on mathematics, and particularly of those on pure and abstract subjects. Why is there such a dearth of readable mathematical writing? Why are there so few books in which the reader has some sense of where he is going and why he is going there? Why can't *meaning* be imparted as well as definitions and theorems? Indeed, why can't one see pure mathematics arising from the conceptual framework within which man organizes his experience?

A welcome contrast to Long's dry and example-free formality is provided by Harvey Cohn's book *A classical invitation to algebraic numbers and class fields*. The word "invitation" in the title is well chosen. The frequent examples, the informal style, and the many loose ends in the treatment make it a book that one is able to get something out of even without reading word-for-word from the beginning, as well as a book that will involve the reader and send him off in pursuit of the many references that it recommends.

Cohn seems to want to make a point about the way in which mathematics is normally written in our time. As a frontispiece he presents the following quotation from George Orwell's novel 1984:

> The purpose of Newspeak was not only to provide a medium of expression, but to make all other modes of thought impossible. It was intended that when Newspeak had been adopted once and for all and Oldspeak forgotten, a heretical thought should be literally unthinkable, at least so far as thought is dependent on words. This was done chiefly by eliminating undesirable words and by stripping such words as remained of unorthodox meanings, and so far as possible of all secondary meanings whatever.

The reader is left to interpret for himself the relationship between Newspeak and modern algebraic number theory.

Cohn's unorthodox style will not please everyone as much as it pleases this reviewer. For one thing, there is the matter of proofs. He says in his Introduction that he found it necessary "to permit the completeness of proofs

to decrease exponentially as the text progresses, until the culminating Weber-Takagi and Artin correspondences are left unproved." This is to be regretted, of course, but if he did not choose to make these proofs a part of his "invitation" and if he did not feel he wanted to add anything to the published proofs in the works he cites, why should he not omit them? (The two proofs he cites are both in German. Perhaps he should have prefaced his invitation with a warning that invitees will feel ill at ease and a bit left out at the algebraic number theory party if they aren't able to read German.) More to be regretted is his failure to deliver on his promise (p. 229) to justify the use of the word "reciprocity" in the name of the Artin Reciprocity Law. He does explain the relationship between the generalized Legendre symbol, which occurs in the statement of the classical reciprocity laws, and the Artin symbol, but he says nothing that explains how the Artin Reciprocity Law involves a reciprocal relationship between (q/p) and (p/q).

Some other explanations are disappointing. On p. 177, after stating a theorem which he calls the gem of class field theory, he promises to show "how naturally it comes as a conjecture" but then gives only an *ad hoc* illustration in a single case that does not, to this reader at least, show how it comes naturally as a conjecture *even in this one case*. Still, even though it doesn't do what is claimed for it, this illustration is interesting and informative, and its inclusion enlivens the book.

The flavor of the book is well represented by a passage on pp. 97 and 98:

> *G. DISCRIMINANTAL DIVISORS*
>
> THEOREM 10.55 (DEDEKIND [1882]). *The rational primes which ramify in an extension field are exactly the divisors of the discriminant.*
>
> REMARK 10.56. This theorem is of supreme ideological significance. From the point of view of function theory, it tells us that the ramified primes must determine a field in the same way that the singularities determine a rational function. From the point of view of class field theory it leads us to expect that the modulus of the arithmetic progressions (called the "conductor" also, see Chapter 7) is related to the ramified primes and discriminant. (Compare Theorem 10.23 and Corollary 10.35 for the quadratic field and Theorem 10.45 and Corollary 10.51 for the cyclotomic field).
>
> Although we avoid a complete proof (for convenience of presentation), a limited proof of a stronger result is more illuminating as it stresses the "local" analysis of an ideal in terms of individual prime ideals. (This is analogous with points of a Riemann Surface in Chapter 8).

What other book would assign "ideological significance" to a theorem? And who else "avoids" proofs instead of simply omitting them?

This informal and discursive style can lead to difficulties for the reader and can sometimes be rather irritating. The two factors which mitigate these problems are, first, the fact that the reader can ignore the difficult passages and skip to some other part of the book while waiting for the light to dawn, and second, the fact that the book contains many examples and illustrations of a very specific and computational type. The theory, after all, is a way of systematizing and clarifying the understanding of specific algebraic number fields. When the theory becomes too far removed from the reader's experience there is no better remedy than a specific example to reestablish contact with computational reality. Cohn's examples are numerous, substantial, and well chosen.

Two appendices by Olga Taussky make the book even more valuable than it would otherwise have been. The first of these is particularly important because it contains, in English, the three famous lectures which Artin gave on class field theory in Göttingen in 1932, here published for the first time in any language.

A healthy balance between theory and examples is also a praiseworthy feature of the third book under review, *Number fields* by Daniel A. Marcus. This book is much less ambitious than Cohn's, and it is commensurately better organized and easier to read. It covers the basic theory of factorization in number fields–ideals, units, the ideal class group, the class number formula–and ends with an "introduction to class field theory."

Unfortunately, in this book the theory invariably *precedes* the examples, which would probably make it very difficult for a beginner to read on his own. However, it is not written as a book for a beginner to read on his own, but as a textbook, and as a textbook it should be quite effective. There are numerous exercises, and with a teacher to assign and read the exercises, and to explain those that the student is unable to do, and, most importantly, with a teacher to give lectures that motivate and illustrate the material in the text, this book should be an excellent basis for an introductory graduate course in algebraic number theory. (Question: How many such courses are being taught today, and how many will be taught in the next ten years?)

On p. 4, the book contains a serious historical misstatement that needs to be corrected. There it states that "Kummer attempted to prove Fermat's [last theorem] by assuming that the unique factorization property of Z and $Z[i]$ generalizes to $Z[\omega]$. Unfortunately it does not." It goes on to say that the argument can be salvaged for certain prime exponents, including $p = 23$, and that "this results from *Dedekind's* amazing discovery of the correct generalization of unique factorization" (italics added). The fact is that the work here ascribed to Dedekind is entirely due to Kummer and was completed before Dedekind left gymnasium; on the other hand, the "attempt" ascribed to Kummer is undocumented and very likely never occurred (see [1, pp. 79–80]).

It is gratifying to see that algebraic number theory remains a subject of vital interest and inspires the publication of works of such quality as the three under review. However, the vitality of the subject stems more from its illustrious history and from the fascination of the phenomena that it studies than from a widespread appreciation of its content and recent advances. These books leave ample room for others that will make more accessible and attractive the great tradition of number theory and give it renewed vitality for the next generation of mathematicians.

BIBLIOGRAPHY

1. Harold M. Edwards, *Fermat's last theorem*, Springer-Verlag, New York and Berlin, 1977.

2. L. Kronecker, *Zur Geschichte des Reciprocitätsgesetztes*, Monat. Akad. Wiss. Berlin, 1875, pp. 267–274 (Werke, vol. 2, 1–10).

HAROLD EDWARDS[1]

[1]The author gratefully acknowledges support from the Vaughn Foundation and from the National Science Foundation (Grant No. SOC77-05420).