REFERENCES

1. P. Dembowski, *Finite geometries*, Springer-Verlag, Berlin and New York, 1968.

2. D. Foulser, *Replaceable translation nets*, Proc. London Math. Soc. **22** (1971), 235–264.

3. C. Hering, *A new class of quasifields*, Math. Z. **118** (1970), 56–57.

4. _____, *On shears of translation planes*, Abh. Math. Sem. Ham. **37** (1972), 258–268.

5. D. R. Hughes and F. C. Piper, *Projective planes*, Springer-Verlag, Berlin and New York, 1973.

6. M. J. Kallaher, *On finite affine planes of rank 3*, J. Algebra **13** (1969), 544–553.

7. _____, *A survey of weak rank 2 affine planes*, Proc. Internat. Conf. on Projecture Planes, (M. J. Kallaher and T. G. Ostrom (eds.)), Wash. St. Univ. Press, Pullman, Washington, 1973.

8. M. J. Kallaher and T. G. Ostrom, *Collineation groups irreducible on the components of a translation plane*, Geom. Dedicata **9** (1980), 153–194.

9. R. A. Liebler, *Finite affine planes of rank three are translation planes*, Math. Z. **116** (1970), 89–93.

10. _____, *On finite line transitive affine planes of rank 3*, Proc. Internat. Conf. on projective Planes, Wash. St. Univ. Press, Pullman, Washington, 1973.

11. T. G. Ostrom, *Linear transformations and collineations of translation planes*, J. Algebra **14** (1970), 405–416.

12. _____, *Finite translation planes*, Lecture Notes in Math., vol. 158, Springer-Verlag, Berlin and New York, 1970.

13. _____, *Classification of finite translation planes*, Proc. Internat. Conf. on Projective Planes, Wash. St. Univ. Press, Pullman, Washington, 1970.

14. _____, *Recent advances in finite translation planes*, Foundations of Geometry, (P. Scherk (ed.)), Univ. Toronto Press, Toronto, Canada, 1976.

15. _____, *Finite translation planes, an exposition*, Aequationes Math. **15** (1977), 121–133.

16. U. Ott, *Über eine neue Klasse endlicher Translationsebene*, Math. Z. **143** (1975), 181–185.

17. G. Pickert, *Projektive Ebenen*, Springer-Verlag, Berlin and New York, 1955.

18. A. Wagner, *On finite affine line transitive planes*, Math. Z. **87** (1965), 1–11.

<div style="text-align: right">T. G. OSTROM</div>

Fermat's last theorem, a genetic introduction to algebraic number theory, by Harold M. Edwards, Graduate Texts in Math. Springer-Verlag, Berlin and New York, 1977, xv + 410 pp.

13 Lectures on Fermat's last theorem, by Paulo Ribenboim, Springer-Verlag, Berlin and New York, 1979, xvi + 302 pp.

For more than three centuries many good and many not so good mathematicians have attempted to prove Fermat's last theorem. While the collected efforts of these mathematicians have not yet led to a solution of this problem, much is now known about the problem and more importantly much new mathematics has been discovered in the process of working on the conjecture.

Fermat's last theorem can be simply stated as: Show that $x^n + y^n = z^n$ has no integral solutions with $n > 2$ and $xyz \neq 0$. It clearly suffices to prove this result for $n = 4$ and $n = p$, an odd prime. When $n = p$, the theorem has been traditionally separated into two parts called case 1 and case 2. The first case is to show the equation has no solution with $xyz \not\equiv 0 \pmod{p}$ and the second is to show no solution exists with $xyz \equiv 0 \pmod{p}$.

The history of the problem can roughly be divided into three eras which I shall call the pre-Kummer, the Kummer and the post-Kummer eras. The pre-Kummer developments were largely limited to proving special cases of the theorem. Various proofs were given of the theorem for the exponents 3, 4, 5 and 7. A very different and beautiful result of the era is the Theorem of Sophie Germain (1823) which says: If p is an odd prime such that $q = 2p + 1$ is also prime then the first case of Fermat's last theorem holds for the exponent p. Her result was soon generalized by Legendre to the cases where $q = 4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$ and $16p + 1$ is a prime. Using these results Germain and Legendre established the first case of Fermat's last theorem for all primes p less than 100.

As the Kummer era approached, mathematicians began using complex roots of unity to factor the left-hand side of the equation $x^p + y^p = z^p$. The question soon arose as to whether or not the unique factorization theorem held in the so-called rings of cyclotomic integers. Kummer soon realized that the answer to this question was no in general, and developed a theory of ideal numbers which restored a type of unique factorization to the cyclotomic rings. This theory enabled Kummer to prove Fermat's last theorem for the so called regular primes. Since Kummer's theory of ideal numbers has been superseded by Dedekind's theory of ideals, Kummer's work is a bit of a mystery to most of us. More than a decade ago, when I was a graduate student, A. Frohlich visited our university and I asked him about Kummer's work. I remember him replying, "I don't know too much about this historical stuff, but using what we know today it is not too difficult to see what Kummer had in mind". I never fully understood this statement until I began reading Edward's book. I shall attempt to explain Frohlich's statement below.

Kummer's theory only applies to subfields of cyclotomic fields; that is, to absolutely abelian fields. To simplify matters further, we shall only consider the case where $K = Q(\zeta)$ is the λth cyclotomic field with λ a prime. For a prime $p \neq \lambda$ let f be the order of p modulo λ and $g = (\lambda - 1)/f$. There exists a subfield L of K of degree g over Q such that p splits completely in L and each prime factor of p in L remains prime in K. (L is the decomposition field of any prime ideal divisor of p in K.) Thus if P is any prime ideal divisor of p in L and α is an integer of L then there exists a unique rational integer a reduced modulo p such that

$$\alpha \equiv a \pmod{P}.$$

The essence of Kummer's definition of ideal prime numbers is to give a rule for a cyclotomic integer to be divisible by a power of the prime ideal P^n without explicitly defining P. We shall use the term ideal divisor instead of ideal number and use $\tilde{P}$ to denote the ideal divisor associated with the prime ideal P. Kummer showed that the g cyclotomic periods $\eta_1, \ldots, \eta_g$ of length f form an integral basis for L over Q and that

$$g(x) = \mathrm{irr}(\eta_1, Q) = (x - \eta_1) \cdots (x - \eta_g)$$

splits completely modulo p, i.e.

$$g(x) \equiv (x - a_1) \cdots (x - a_g) \pmod{p}$$

for some integers $a_1, \ldots, a_g$ reduced modulo p. Hence by proper numbering we have

$$\eta_i \equiv a_i \,(\bmod\ P) \quad \text{for } i = 1, \ldots, g.$$

Since $g(x)$ has no multiple roots modulo p, the numbers $a_1, \ldots, a_g$ are all distinct modulo p. Let

$$\psi(\eta) = \prod_{i=1}^{g} \prod_{j \neq i} (\eta_i - a_j)$$

and $\alpha \in K$ be a cyclotomic integer. For any positive integer n, define

$$\alpha \equiv 0 \,(\bmod\ \tilde{P}^n)$$

to mean

$$\psi^n(\eta)\alpha \equiv 0 \,(\bmod\ p^n).$$

Moreover, if η_1 is assigned to a_i for $1 \leqslant i \leqslant g$ then there exists exactly one assignment of the remaining η_j's to the remaining a_j's which gives an ideal prime divisor of p. That is, p determines exactly g distinct ideal prime divisors of K. The integer $(1 - \zeta)$ is a prime number of K which divides λ to the $\lambda - 1$ power and is the only prime divisor of λ.

The prime divisors of K are exactly the prime divisors of the rational primes and every divisor is by definition the product of prime divisors. A cyclotomic integer is said to be divisible by the product of two relatively prime divisors if and only if it is divisible by each of the two factors.

A divisor $\tilde{A}$ of K is said to be *principal* if there exists an integer γ of K such that for every integer α of K, $\tilde{A}$ divides α if and only if γ divides α. Two divisors $\tilde{A}$ and $\tilde{B}$ are said to be *equivalent* if for any divisor $\tilde{C}$, $\tilde{A}\tilde{C}$ is principal exactly when $\tilde{B}\tilde{C}$ is principal.

Kummer proved the following fundamental results: (1) any algebraic integer of an abelian field K can be uniquely expressed as the product of prime divisors and (2) the divisors fall into finitely many equivalence classes. The number of such equivalence classes for the field $K = Q(\zeta)$ will be denoted by $h(\lambda)$. A prime λ is called *regular* if λ does not divide $h(\lambda)$. In addition to using his theory of ideal prime numbers to prove Fermat's last theorem for regular primes, he characterized the regular primes as those primes λ which do not divide the numerators of the Bernoulli numbers B_2, $B_4, \ldots, B_{\lambda-3}$.

Post-Kummer results about the Fermat problem can roughly be divided into three types: (1) congruence conditions, (2) class number conditions and (3) computational methods. In order to illustrate the nature of these results, we will mention a few examples of each type.

Wieferich made a significant contribution in 1909 when he proved: If the first case of Fermat's last theorem fails for the exponent p then p must satisfy the congruence

$$2^{p-1} \equiv 1 \,(\bmod\ p^2).$$

The only primes known (i.e. less than $3 . 10^9$) to satisfy this congruence are $p = 1093$ and $p = 3511$. In 1910 Mirimanoff proved that 2 could be replaced

with 3 in the above congruence and subsequently similar conditions have been proved for all primes up to 43, although the correctness of the proofs for the three highest primes is in doubt. Despite the fact that these conditions seem very restrictive, no one has yet been able to prove the first case of Fermat's last theorem for infinitely many prime exponents.

What remained after Kummer was to prove Fermat's last theorem for irregular primes. It seems natural to seek further sufficient conditions on the class number $h(p)$ of the pth cyclotomic field for Fermat's last theorem to be true. We can write $h(p) = h = h^+h^*$ where h^+ is the class number of maximal real subfield of the pth cyclotomic field and h^* is an integer. Kummer proved in 1850 that if p divides h then p divides h^*. Since Kummer's time many results of the following type have been proved: If the first case of Fermat's last theorem fails for the exponent p then p^a divides h^*. This was done by Hecke for $a = 2$, Furtwängler for $a = 4$, Vandiver for $a = 8$ and Morishima and Lehmer for $a = 12$. However, a much better result was proved by Eichler in 1965. Namely, if the first case fails for the exponent p then $p^{[\sqrt{p}]-1}$ divides h^* and the class group of the pth cyclotomic field must have p-rank greater than $\sqrt{p} - 2$.

During the past three decades several articles have been written with the title, "Fermat's last theorem holds for all prime exponents less than B", where B is some constant. The largest such bound $B = 125,000$ was obtained by Wagstaff in 1977. In order to prove such results, practical computational methods were needed first to decide whether a given prime is regular or irregular and then for proving Fermat's last theorem for irregular primes. A convenient solution to the first problem was given by Stafford and Vandiver [2] in 1930 and to the second by Lehmer, Lehmer and Vandiver [1] in 1954.

While the two books being reviewed here both contain the words, "Fermat's last theorem", in their titles, the two authors strive to achieve quite different goals. Edwards' goal is to give a "genetic introduction to algebraic number theory", while Ribenboim's objective is to give a historical survey of the main lines of work on Fermat's last theorem.

The *genetic method* is defined as "the explanation or evaluation of a thing or event in terms of its origin and development". While Edwards' book may in a puristic sense achieve its author's goals, I found the book to be somewhat of a disappointment. As I share Edwards' interest in the work of our mathematical ancestors and his enthusiasm for computations, I had high expectations for his book. My main criticism concerns the style of presentations: Many of the explanations and proofs are very longwinded and cumbersome. Although the proofs generally contain a lot of detailed notation, equations and congruences are seldom displayed on separate lines. Reading this book is often like trying to find ones way through a rhododendron thicket.

Edwards' discussion of Fermat's last theorem ends with the Kummer era. The book concludes with chapters on the Gauss theory of binary quadratic forms and on Dirichlet's class number formula for abelian fields. The author promises a second volume to cover developments of the post-Kummer era.

In sharp contrast to Edwards' verbose style, Ribenboim's presentation is clear, concise and elegant. The thirteen lectures cover the major events of all three eras with a heavy emphasis on the post-Kummer era. The book is a true work of art. The lectures are well organized and present the mathematics underlying seemingly isolated results in a very cohesive manner. In order to avoid too much technical detail, the proofs of the more difficult theorems are sometimes only sketched and other times omitted completely. An extensive bibliography is given at the end of each section so the reader can easily locate sources which cover material missing in the text. Ribenboim also promises a second volume which is intended to contain much of the technical development which was omitted in these thirteen lectures. His first book should stimulate interest in and promote a better understanding of the mathematics related to Fermat's last theorem. One can only have high expectations for Ribenboim's second book on this subject.

REFERENCES

1. D. H. Lehmer, E. Lehmer and H. S. Vandiver, *An application of high speed computing to Fermat's last theorem*, Proc. Nat. Acad. Sci U.S.A. **40** (1954), 25–33.

2. E. Stafford and H. S. Vandiver, *Determination of some properly irregular cyclotomic fields*, Proc. Nat. Acad. Sci. U.S.A. **18** (1932), 139–150.

CHARLES J. PARRY

Classification theory and the number of non-isomorphic models, by Saharon Shelah, Studies in Logic and the Foundations of Mathematics, Volume 92, North-Holland Publishing Company, Amsterdam-New York, 1978, xvi + 544 pp., $62.25.

Can the dimension theory of vector spaces, algebraically closed fields, countable torsion Abelian groups (Ulm's Theorem) etc. be generalized to provide a means of characterizing the models of an arbitrary first order theory? If not, can the obstacle to such an extension be identified and the program carried through in its absence? A vector space or an algebraically closed field is determined by a single cardinal (the number of independent elements); a countable torsion Abelian group is determined by an infinite sequence of cardinals. Thus by a generalized dimension theory we mean a method of attaching to each model a sequence of cardinals which determine it up to isomorphism. The first test of such a generalized dimension theory is its ability to solve the spectrum problem: i.e., to count the number of models of a theory. In fact, Shelah's answer to these questions arose from the study of the following problem. For a first order theory T, let $n(T, \lambda)$ denote the number of non-isomorphic models of T with cardinality λ. Determine the