17 Lectures on Fermat Numbers
From Number Theory to Geometry
by Michal Krížek, Florian Luca, and Lawrence Somer
CMS Books in Mathematics
Springer-Verlag, New York, 2001
xxiv+257 pp

Most mathematics books restrict themselves to some well-defined area of mathematics and serve either as introduction on a certain level, or as monograph with various degrees of completeness. Occasionally, however, a book picks up a very specific topic and treats it from a variety of angles, often touching on different fields of mathematics. The book under review, “17 Lectures on Fermat Numbers: From Number Theory to Geometry” belongs to this second category. Even within this category it is quite unique in that the subject matter is narrower than in most other books. This approach may not always be successful, but in this case it does work, at least in principle.

It is certainly satisfying for the reader to have almost everything that is known on a particular subject collected in one place. Also, it contributes to a sense of mathematics as a unified subject to see several different areas enter, often in unexpected ways. While the authors of “17 Lectures” made good use of the advantages of such an approach, they also fell victim to some of its dangers. In particular, if a very narrow subject is treated to such a degree of completeness
then, almost by necessity, the book will contain parts that might better have been left out.

All these are general remarks; I will now turn to the subject matter, and how it is treated in this book. The Fermat numbers $F_m = 2^{2^m} + 1$, for $m = 0, 1, 2, \ldots$, are among the best known special number sequences. The reason for the double exponent $2^m$ lies in the fact that the polynomial $x^n + 1$ always factors when $n > 1$ is an odd integer; therefore $2^n + 1$ cannot possibly be a prime unless it has the form of $F_m$. In this connection, Fermat observed that the first five numbers in this sequence, namely 3, 5, 17, 257, and 65,537, are indeed prime, and he conjectured that all the $F_m$ are prime. However, in 1732 Euler found that $F_5 = 641 \cdot 6,700,417$, and thus disproved Fermat’s conjecture. To this date no other Fermat prime has been found, the smallest one in doubt being $F_{31}$. More than two hundred Fermat numbers are now known to be composite. All this would be no more than a mathematical curiosity were it not for the well-known connection between Fermat numbers and the construction of regular polygons with straightedge and compass, first found by Gauss. It is an important contribution of “17 Lectures” to show that there is more to Fermat numbers than the obvious connection with primality testing and factoring and with regular polygons, although the first chapter gives a brief historical account of just these topics. The book actually opens with a foreword by Alena Šolcová, a Czech historian of science; this is an interesting 11-page essay on the life and work of Fermat. All this is followed by a chapter on the fundamentals of number theory, a very nice introduction to those topics from elementary number theory, up to quadratic reciprocity, that are needed to understand much of the material in the rest of the book. An interesting feature of this chapter are the geometric interpretations of many of the concepts and results; the many historical remarks are also quite useful.

The next two chapters contain, with proofs, the most basic properties (mainly recurrence relations and congruences) and what the authors call “the most beautiful theorems” on Fermat numbers. Of course, beauty in mathematics, as anywhere, is rather subjective, but some of the results are indeed both important and striking, such as Gauss’s theorem mentioned above, and the theorem of Euler and Lucas on the shape of the factors of Fermat numbers.

Chapters 5–7 contain almost everything that is known on primality and factoring in connection with Fermat numbers. In particular, these chapters contain proofs and discussions on some general primality tests, Pepin’s famous test, the theorem of Lucas, Proth’s theorem, and various related results. This is probably the strongest and most useful part of the book. In fact, up to this point this book is excellent in many respects.

The results in Chapters 8 and 9 are more isolated and probably less important. Some of the proofs are quite sophisticated and lengthy, and this is where the reader may begin to get tired. A typical result states that a Fermat number is never perfect or part of an amicable pair.

The next chapter, on the irrationality of sums of certain reciprocals, is again very interesting; it contains a variety of results that are not restricted to Fermat numbers. However, Chapter 11, devoted entirely to a very special Diophan-
tine equation, should in my opinion not have been included in a book of this character. The proof of this one result takes up 12 pages, and detracts from, rather than adds to, the value of the book. The ups and downs continue in the next chapter, where an interesting and useful discussion on pseudoprimes and Carmichael numbers is followed by 6 heavy pages on superpseudoprimes, a concept that, according to MathSciNet, has not appeared in print before. Chapter 13, on generalized Fermat numbers and Cullen numbers, is once again useful as a reference for anyone interested in the subject or working in this area.

Several applications of Fermat numbers are given in Chapter 15; it contains the Fermat number transform (a variant of the discrete Fourier transform) and other related transforms. Other topics include pseudorandom number generators, minimal perfect hashing schemes, and even an excursion into chaos theory. This is once again a fascinating chapter with some unexpected results and connections to other parts of mathematics. The final two chapters contain a proof of Gauss’s theorem and a construction of the regular 17-gon; all of this is quite appropriate for this book.

A first appendix contains various useful tables of Fermat numbers and their factors, with just the right degree of completeness; later I will mention the other two appendices. The bibliography, with more than 350 entries, is very complete and contributes to the value of the book as a reference, as do the extensive name and subject indexes.

Altogether, this could have been a great book, were it not for two points that diminished its enjoyment. I have already hinted at my first point: Regardless of the value of the authors’ own very recent research, most of it should not have been included in a book of this nature. This research should first be disseminated by other means (most of it has been, or is being, published in journals), picked up by others, expanded on, changed, applied, etc., before it is ready for inclusion in an expository and historical text that this book wants to be and is best at.

My main criticism, however, is of a different nature, and begins with the title of the book. “17 Lectures” is clearly a variation on Paulo Ribenboim’s classic “13 Lectures on Fermat’s Last Theorem”. The only reason for having 17 lectures (why lectures?) is the fact that 17 is a Fermat number. This in itself wouldn’t be so bad; however, it dictates the entire structure of the book. The book would have profited from a more standard “Chapter - Section” structure. For instance, why are Gauss’s theorem and the construction of the 17-gon in different chapters? And why are Mersenne numbers in an appendix, instead of a chapter? But that’s not all: Chapter 14 contains 17 open problems, and the otherwise very useful list of internet addresses has 17 entries. And why is the chapter on open problems not at the end? I hope that I am wrong, but could it be that it’s Chapter 14 because $F_{14}$ is the smallest composite Fermat number without any known prime factor? The worst offense, in the same numerological vein, concerns the page count. Immediately upon opening the book I had noticed that the print size was smaller than usual, and strangely out of proportion (in contrast to the usually very well-proportioned Springer-Verlag look). The reason: The book ends with page 257, i.e., $F_3$!
The criticism in the last two paragraphs comes from my disappointment at seeing a potentially excellent book spoiled so needlessly. I can still recommend it to number-theorists and other mathematicians alike; everybody will find useful and interesting information in it. In the classroom, this book might be suitable for undergraduate projects or supplementary readings in a number theory, algebra, or history of mathematics course. It will also be accessible to bright high school students and interested amateurs. In fact, Fermat’s name in the title may attract such readers, and they will find a well written, interesting, and mathematically sound book, in spite of its shortcomings.