Teaching at the mathematics department of UNC Charlotte regularly the course in geometry, and sometimes courses the number theory and algebra courses have been the beginning of my interest. After my retirement and three years of further rather intense work, I have decided to gather the material in my book *Number Theory and Modern Algebra Notes*. This book has been published by the internet company iUniverse, and is available online, and as ebook, too.

The motivation for this decision is more that the gathered material began to be overwhelming,—honestly much quicker than my ability to cover the material as completely as desirable. During the entire process of creation, I have been motivated by the following points. Firstly, I always like to solve clear-cut mathematical problems. Secondly, especially after my retirement, I needed a playground for programming in the lisp dialect DrRacket and in mathematica. Last not least, the excellent geometry textbook *Euclid and Beyond* gave me ample material from modern algebra and interesting problems.

The gathered material covers a range of topics from classical number theory and modern algebra. I keep the theoretical framework somehow in the background, still presupposing the reader has some elementary knowledge. Indeed, I am convinced that problem solving is one of the best routes to judge the importance and fruitfulness of theoretical concepts. Many proofs and solutions in the book do not follow the path usually taken. Others have been reworked to achieve more constructiveness and clarity.

The topic to begin with, is the Euclidean algorithm and the Chinese remainder theorem. Already here the extended algorithm is shaped into a more effective version than the backtracking often used in textbooks. Many examples are included. The algorithms are set up for the graphing calculator.

Concerning prime numbers, I stress from the beginning Euclid’s lemma which is so badly needed to prove the uniqueness of prime factorization. Euclid’s proof that there are infinitely many primes is generalized for obtain infinitely many primes in several arithmetic sequences. Bertrand’s postulate is proved by means of the prime factors of the middle binomial coefficient \( \binom{2n}{n} \). Legendre’s counting formula and Eratosthenes sieve for primes are explained. From this I get the divergence of the series over primes \( \sum_p \log p/(p-1) \), a bid different approach leads to the well series \( \sum_p 1/p \) by Euler.

The next topic is the Little Fermat Theorem, for which a new proof is given via counting the periodic orbits of an iterated tent mapping and the Moebius inversion formula. There follows a detailed treatment of the Euler totient function, including the Euler group of relatively prime residue classes for any given number. Its decomposition is obtained from the Chinese remainder theorem. For the Euler totient function, additional to the standard material, I give an algorithm to find all solutions of the equation \( \phi(n) = m \) for given
The text next completely covers Legendre and Jacobi symbols and a proof of quadratic reciprocity. I follow Gauss’ ideas, but do not restrict the discussion to primes. In that way the Jacobi symbols are defined from the beginning without use of the prime factorization. From the algorithmic calculation of the Jacobi symbols, which exploits quadratic reciprocity together with a generalization of the Euclidean algorithm, one obtains uniqueness. Finally this approach allows to prove the properties relating Jacobi symbols by means of prime factorization to Legendre symbols. I have not found this approach in any number theory text, where such consideration appear usually only hidden (and buried) in exercises.

Now, finally, are introduced the Fermat numbers, which are indeed a main focus of the book. Besides the material usually covered in number theory, I deal in great depth with the geometric construction of regular polygons by straightedge and compass. The construction of the 17-gon is obtained by a more elementary variant of Gauss’ method. I begin with the elementary trigonometric formula relating sums and products of cosine values. By means of this formula one rather quickly checks out which sums of two cosines for the x-coordinates of the vertices of the regular 17-gon have to be added, in order to obtain via quadratic equations in the end all these cosine values. Next, one backtracks to get the convenient sums of four such cosine values, from which the sum of two cosines sums are to be obtained, once more by solving quadratic equations. The Gaussian sums appear naturally, and the entire process of construction of the Gaussian sums is obtained,—without any use or knowledge about the powers of a primitive root.

Of course, the generalization to regular $F_n$-gons for any larger Fermat primes is not as straightforward to tackle by an elementary approach. Here one needs the genial idea of Gauss for the construction of the convenient sums. I continue to elaborate the construction of the regular 257-gon as well as the 65 537-gon. There occurs the additional problem to find out which pairs of Gaussian sums $S(n, q + 1, l)$ with $2^{q+1}$ terms appear as coefficients in the quadratic equations for the Gaussian sums $S(n, q, l)$ with $2^q$ terms. The relevant tree structure is gathered in the nonnegative integer coefficients $c_{q, l, k}$ of the formulas (see p. 150 in the book)

$$S(n, q + 1, l) \cdot S(n, q + 1, l + 2^q) = \sum_{0 \leq k < 2^q} c_{q, l, k} S(n, q, k)$$

I derive an algorithm for their calculation, and give implementations for the language DrRacket, as well as independently mathematica. With DrRacket I did not go on to the actually solving the resulting quadratic equations, but I used mathematica for this step. In principle, this step is possible even symbolically.
But the reader should not be so naïve and hope to see me writing down explicit formulas for the coordinates of the regular 257-gon or 65,537-gon containing all these boxed square roots! All paper or computer storage of the world would not be sufficient to this end. So the question remains to get a practicable check of the completeness and correctness of the results claimed for the construction of the large $F_n$-gons. A first partial check is to compare whether the results from DrRacket and from mathematica agree. But I can indeed go further and use numerical computation to check complete correctness. After having a complete list for the numerical values of the polygon coordinates at hand, they are used to recalculate the corresponding polar angles. In this way, I have checked that the Gauss formulas give the coordinates of the vertices with at least 5 correct decimals. It is not possible to see the final result of the algorithms in any other convenient way explicitly. I may be allowed to stress that my results about the geometric construction of the $F_n$ polygons are more complete and constructive than those available in the standard modern algebra texts.

The Gaussian sum appear, too, in the setup of regular $p$-gons for any prime $p$. They allow to get the intermediate fields between the rationals and the relevant field extension. The automorphism groups for these extensions are the Euler group of order $p - 1$, and its subgroups. Before exposing the general Galois theory, I obtain by elementary methods several results for these fields and their fixed groups. As examples, side and area of the regular 7-gon and 11-gon are expressed in terms of complex third and 5-th roots, respectively. The relevant cumbersome calculations could only be completed with the help of mathematica.

Compared to this depth and breath, my exposition of prime factorization is a bid too modest, and lacks the more modern developments in that area. Nevertheless some older results about testing Fermat primes are stated and proved.

I go on to comment the modern algebra part of the book. My exposition has grown from the theory of geometric construction by straightedge and compass, and more restrictive, by Hilbert tools. Hence focus points are the constructible field, the Hilbert field and totally positive algebraic numbers. Secondly I wanted to see a more concrete and constructive treatment of the cyclotomic polynomials than commonplace. The final chapters have been build from some special polynomials related to the Euler group, which I have invented during my search for interesting problems. Last not least, a treatment of Galois theory using the textbook of Gerd Fisher and the AMS book containing Artin’s outline of Galois theory. Following these sources, I have elaborated the fundamentals of Galois theory with all necessary accuracy.

An algebraic number of the rationals is called totally positive iff all its algebraic conjugates are positive. By a theorem of Emil Artin, all totally positive algebraic numbers can be written as sums of squares of real algebraic numbers. Similarly, one obtains each totally real algebraic number from the square root of such a sum of squares. The proof of this beautiful theorem is sketched as

---

1It would be worth while to investigate what has been worked out in the historical papers about that matter.
an exercise in Hartshorn’s book *Euclid and Beyond*. It took me some pain to completely work out this proof.

Here the axiom of choice is needed. The entire approach drifts away more and more from the constructive spirit of my book. Hence I could not stop after completing the rather long proof. Unable to get a practical algorithm, I have at least worked out several examples, and did myself boost up to the proof that the regular 17-gon is not only constructible by straightedge and compass, but even by the (more restrictive) Hilbert tools. In algebraic terms, this proof leads to the problem writing the positive coordinates for the vertices as sums of squares of real constructible numbers. In the end the solution is obtained, exploiting the power of mathematica.

Franz Rothe, November 2019