

BOOK REVIEW

1. *Computational and algorithmic problems in finite fields*, by Igor E. Shparlinski. Kluwer Academic Publishers, Dordrecht, Boston, and London, 1992, 240 pp., \$118.00. ISBN 0-7923-2057-3
2. *Dickson polynomials*, by R. Lidl, G. L. Mullen, and G. Turnwald. Longman Scientific & Technical, Harlow, 1993, 207 pp., \$95.00. ISBN 0-582-091195
3. *Arithmetic of finite fields*, by Charles Small. Marcel Dekker, Inc., New York, Basel, and Hong Kong, 1991, 216 pp., \$99.75. ISBN 0-8247-8526-6
4. *Finite fields, coding theory, and advances in communications and computing*, edited by G. L. Mullen and P. J.-S. Shiue. Marcel Dekker, Inc., New York, Basel, and Hong Kong, 1993, 443 pp., \$145.00. ISBN 0-8247-8805-2
5. *Finite fields: structure and arithmetics*, by Dieter Jungnickel. Wissenschaftsverlag, Mannheim, Leipzig, Wien, and Zürich, 1993, 339 pp., Sch 609. ISBN 3-411-16111-6
6. *Applications of finite fields*, by Alfred J. Menezes, editor, and Ian F. Blake, Xuhong Gao, Ronald C. Mullin, Scott A. Vanstone, and Tomik Yaghoobian. Kluwer Academic Publishers, Dordrecht, Boston, and London, 1993, 218 pp., \$72.00. ISBN 0-7923-9282-5

A finite field is a field that has only finitely many elements, such as the ring of integers modulo a prime number. The *definition* already places the area of finite fields at the crossroads of algebra and combinatorics, with number theory showing up right away! The area has seen a rapid growth in recent years due to its many new applications and connections with other subjects such as computer science, coding theory, discrete mathematics, algebraic geometry, number theory, and group theory. As a result at least six books on finite fields have been published during the last three years.

A typical problem recently studied in finite fields is to classify all cases for which a known inequality (trivial or nontrivial) becomes an equality. These problems may be properly placed in a growing subject called extremal finite field theory. Theoretically, it may be more interesting to understand the generic or average case of a problem than a special case. However, what is often more useful in applications is the extreme case. It is generally harder to understand the extreme

case in the sense that one may often require various ad hoc methods to deal with extremal problems. It seems to be especially interesting and instructive when an extremal problem can be approached and solved using a general and systematic method. A remarkable feature of recent developments in extremal finite field theory is the increasing and successful use of various general, powerful and systematic methods such as the Riemann-Roch theorem, the Weil-Deligne estimate, modular curves, and the classification of finite simple groups. Before discussing the six books individually, we will briefly explain a problem which intersects the first four books under review, namely, the theory of permutation polynomials.

Let \mathbf{F}_q be a finite field of q elements with characteristic p . Let $f(x)$ be a polynomial in $\mathbf{F}_q[x]$. As x runs over the q elements of the field \mathbf{F}_q , the polynomial $f(x)$ takes on at most q distinct values. The extremal question here is to classify all polynomials $f(x) \in \mathbf{F}_q[x]$ which take exactly q distinct values. Such polynomials are called permutation polynomials over \mathbf{F}_q . Thus, a polynomial $f(x) \in \mathbf{F}_q[x]$ of positive degree is called a permutation polynomial if and only if $f(x)$ induces a one-to-one map from \mathbf{F}_q onto itself. For example, the monomial x^n is a permutation polynomial if and only if n and $q-1$ are relatively prime. Since $x^q = x$ for all $x \in \mathbf{F}_q$, one can always assume that the degree of $f(x)$ is smaller than q . By Lagrange interpolation any map from \mathbf{F}_q into itself can be uniquely represented by a polynomial in $\mathbf{F}_q[x]$ of degree smaller than q . Thus, the set of all permutation polynomials of degree smaller than q forms a group isomorphic to the symmetric group S_q on q letters. One may hope then to use polynomials over \mathbf{F}_q to understand some group theory questions. In fact, the first systematic study of permutation polynomials, which was carried out in Dickson's thesis [Di1] in 1896, was motivated by his study of finite simple groups. Dickson devoted an entire chapter to permutation polynomials in his classical book [Di2]. Recently, permutation polynomials have received significantly wider attention because of their potential applications in cryptosystems and various combinatorial designs.

Our fundamental question here is the construction and classification of permutation polynomials over \mathbf{F}_q . This question can be formulated in a geometric way. By definition a polynomial $f(x) \in \mathbf{F}_q[x]$ is a permutation polynomial if and only if the plane curve $f(x) - f(y) = 0$ has no \mathbf{F}_q -rational points other than the points on the diagonal $x = y$. Thus, we need to estimate the number of \mathbf{F}_q -rational points on the plane curve $f(x) - f(y) = 0$. This last question can be solved using Weil's theorem (the Riemann hypothesis for function fields). Recall that a polynomial $g(x, y) \in \mathbf{F}_q[x, y]$ of positive degree is called absolutely irreducible if it remains irreducible over the algebraic closure of the constant field \mathbf{F}_q . Weil's theorem implies that if a polynomial $g(x, y) \in \mathbf{F}_q[x, y]$ is absolutely irreducible of degree n , then the curve $g(x, y) = 0$ has $q + O_n(\sqrt{q})$ points rational over \mathbf{F}_q .

For q sufficiently large compared to the degree n of $f(x)$, if $f(x) - f(y)$ has an absolutely irreducible factor over \mathbf{F}_q other than $x - y$, Weil's estimate shows that the plane curve $f(x) - f(y) = 0$ has at least $q + O_n(\sqrt{q})$ points (x, y) rational over \mathbf{F}_q with $x \neq y$, and thus $f(x)$ cannot be a permutation polynomial. It turns out that the converse is also true. Namely, if $f(x) - f(y)$ has no absolutely irreducible factor over \mathbf{F}_q other than $x - y$ (in this case, $f(x)$ is called exceptional), then $f(x)$ is a permutation polynomial whether q is large or not. Thus, for q large compared to n the construction and classification of permutation polynomials are reduced to the construction and classification of exceptional polynomials. We shall restrict ourselves to this case because it is mathematically better understood. If n

is close to q (the case that is useful in combinatorial designs), the distribution of permutation polynomials is somewhat random and not well understood. See [EGN] for a conjecture in this direction.

Our goal then is to classify exceptional polynomials. If $g_1(x)$ and $g_2(x)$ are both exceptional, their composition $g_1(g_2(x))$ is also exceptional. One may then restrict to indecomposable polynomials (namely, those polynomials which cannot be written as a composition $g_1(g_2(x))$ for some $g_i \in \mathbf{F}_q[x]$ with $\deg(g_i) > 1$). If $f(x)$ is exceptional and $a \in \mathbf{F}_q^*$, then $af(x+b)+c$ is also exceptional for all $b, c \in \mathbf{F}_q$. Thus, one may normalize $f(x)$ so that $f(x)$ is of the form $x^n + a_1x^{n-1} + \cdots + a_{n-1}x$, where $a_1 = 0$ if n is not divisible by p .

Currently, there are only two known classes of normalized indecomposable exceptional polynomials. The first class consists of certain Dickson polynomials:

$$\begin{aligned} D_n(x, a) &= \left(\frac{x + \sqrt{x^2 + 4a}}{2} \right)^n + \left(\frac{x - \sqrt{x^2 + 4a}}{2} \right)^n \\ &= \sum_{0 \leq i \leq n/2} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}. \end{aligned}$$

For $a = 0$ the polynomial $D_n(x, a)$ is simply the monomial x^n , which is exceptional if and only if $(n, q-1) = 1$. The monomial x^n was used in the first construction of the RSA public key cryptosystem. For $a \neq 0$ the Dickson polynomial $D_n(x, a)$ is exceptional if and only if $(n, q^2-1) = 1$. The polynomials $D_n(x, a)$ can also be used to construct a similar RSA cryptosystem. The Dickson polynomials are closely related to the classical Chebyshev polynomials of the first kind in the following way: $D_n(x, 1) = 2T_n(x/2)$, where $T_n(x) = \cos(n \arccos x)$ is the Chebyshev polynomial of the first kind.

The second class consists of certain semilinearized polynomials of the form $f(x) = x(\sum_i a_i x^{(p^i-1)/d})^d$ recently discovered by Cohen [Co1]. Such a polynomial $f(x)$ is exceptional if and only if $f(x) = 0$ has no nonzero roots in \mathbf{F}_q . In the special case $d = 1$ one gets the well-known subclass of p -linearized polynomials $\sum_i a_i x^{p^i}$. In the special case when there are at most two nonzero a_i 's, one essentially gets the subclass $x(x^{(p^r-1)/d} + a)^d$, first discovered by Dickson (Theorem 83 in [Di2]). It is currently unknown whether it is possible to find any new indecomposable exceptional polynomials.

Most of the complication in the classification of exceptional polynomials occurs when the degree n is divisible by the characteristic p . In fact, Schur (1923) conjectured that if n is not divisible by p (the tame case), then any normalized indecomposable exceptional polynomial of degree n is a Dickson polynomial. This conjecture was proved by Fried [Fr] using the covering theory of algebraic curves and group theory. Using Fried's theorem, Cohen [Co2] proved a conjecture of Chowla and Zassenhaus which asserts that there is at most one exceptional polynomial in the linear family $f(x) + \lambda x$ if the degree of $f(x)$ is larger than one and not divisible by p . The wild case (n divisible by p) is at present not well understood.

A weaker question is to classify all the possible degrees n ($n > 1$) of exceptional polynomials over \mathbf{F}_q . It is conjectured that there is an exceptional polynomial of degree n over \mathbf{F}_q if and only if $(n, q-1) = 1$. If $(n, q-1) = 1$, the monomial x^n is exceptional, and one direction of the conjecture is proved. In the special case when n is even and q is odd, the above conjecture reduces to a well-known conjecture of

Carlitz made in 1966 which asserts that there are no exceptional polynomials of even degree if q is odd. See Hayes [Ha] where the case $n = 10$ was first proved. For a long time little progress was made toward the Carlitz conjecture. Several years ago it was independently proved by Cohen [Co3] using the theory of primitive permutation groups and by Wan [Wa] using the technique of resolution of singularities that the Carlitz conjecture is true for $n = 2r$, where r is a prime. Very recently the Carlitz conjecture was completely proved by Fried, Guralnick, and Saxl [FGS]. Their proof is rather complicated and involves the use of the covering theory of algebraic curves in characteristic p and a very nontrivial application of the classification of finite simple groups! As a consequence of their work, they showed that for $p > 3$, any normalized indecomposable exceptional polynomial over \mathbf{F}_q is either a Dickson polynomial or has the property that its degree is a power of the characteristic p . Another consequence of their work is the affirmative solution of a version of a conjecture from Dickson's thesis: any normalized exceptional polynomial of degree p (automatically indecomposable) must be of the form $x(x^{(p-1)/d} + a)^d$. These results are consistent with the two known classes of normalized indecomposable exceptional polynomials.

Shparlinski's book surveys the recent results on the computational and algorithmic aspects of finite fields. My impression of the book is somewhat mixed. The main advantage is its comprehensive list of literature and the vast amount of interesting material covered. The book contains 1,306 references (most of them published during the last five years) and an addendum describing many more recent papers which were too late to be included in its main list of references. These occupy about one third of the book. A particularly interesting feature of the book is the many applications to finite fields of Weil's character sum estimate, the theory of algebraic curves and analytic methods. The author also raises many open problems; most of them follow a standard form, such as "Generalize (or improve) the theorems, the results, the bounds, etc."

On the other hand, I have the impression that the author tried to include everything he has seen in the literature. As a result the author spent at least another one third of his book describing (without details) the vast number of problems recently being studied and listing the many (sometimes incorrect) reference numbers. Part of the material and literature in the book is about number fields instead of finite fields. The author states that the required background for the book "is essentially limited to a knowledge of basic facts on finite fields such as one can readily find in the excellent book by R. Lidl and H. Niederreiter." On the contrary, most of the mathematical arguments in this book use either techniques of analytic number theory or the theory of algebraic curves over finite fields. Neither is seriously treated in Lidl-Niederreiter's book [LN]. In addition, there are many mistakes and typographical errors. For example, on page 19 Theorem 1.8 (similarly Theorem 1.7 and also the main theorem in [Sh]) says that there is a deterministic polynomial time algorithm that factors almost all bivariate polynomials $f(x, y) \in \mathbf{F}_p[x, y]$ of total degree n . This formulation is misleading, because almost all polynomials of two (or more) variables of degree n over \mathbf{F}_p are already irreducible for large p (this fact follows from a direct counting argument without using Hilbert's irreducibility theorem). Therefore, factorization is not needed for almost all bivariate polynomials of degree n . The correct formulation of Theorem 1.8 should be something like this: For almost all *homogeneous* $f_n(x, y) \in \mathbf{F}_p[x, y]$ of degree n , any bivariate polynomial over \mathbf{F}_p of the form $f_n(x, y) + g(x, y)$ with $\deg(g) < n$ can be deterministically

factored in polynomial time.

In conclusion, this book is an encyclopedic synthesis of recent activities related to finite fields. Despite my critical remarks Shparlinski's book does provide a very useful source of new references, new results, and open problems, particularly for those who are interested in applying the theory of algebraic curves and analytic methods to finite fields.

Lidl, Mullen, and Turnwald's book is a comprehensive monograph devoted exclusively to the theory of Dickson polynomials and applications. For the most part the book is concrete, well written, and self-contained. The exercises and historical notes at the end of each chapter are helpful for students as well as researchers who are interested in Dickson polynomials. A complete proof of the Schur conjecture is also included in Chapter 6. This chapter is, however, substantially harder to read than other chapters. The book is a very valuable reference for people interested in Dickson polynomials and their applications to finite fields.

Small's book is primarily a textbook for undergraduate students and beginning graduate students who are interested in certain arithmetic aspects of finite fields. It gives a clear but only partial introduction to several topics in finite fields, such as permutation polynomials, the Chevalley-Waring theorem, Gauss sums, diagonal equations, and zeta functions.

Mullen and Shiue's book is the refereed proceedings of the International Conference on Finite Fields held at the University of Nevada at Las Vegas in August 1991. The topics included are quite mixed, ranging from finite fields to coding theory, algorithms, and various applications. Even though some of the applied articles have no mathematical significance, the book does contain several interesting and well-written papers on finite fields. In particular, the expository papers written by experts provide a clear introduction to several basic topics in finite fields. In addition, the book contains a number of interesting open problems raised by the conference participants.

Jungnickel's book and Menezes's book are primarily directed to engineering problems. Emphasis is on the constructive and computational side of finite fields. However, the treatment of material in both books is from a mathematical point of view. Therefore, they should be of interest to mathematicians working on areas related to finite fields.

Jungnickel's book essentially focuses on normal bases in finite fields, namely, a basis of \mathbf{F}_{q^n} over \mathbf{F}_q of the form $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$. This is currently a very active research area. The main question studied is to construct normal bases satisfying additional properties motivated by problems in computational complexity. Examples of such bases are self-dual normal bases and optimal normal bases (an extremal question again). Jungnickel's book is well structured, focused and beautifully written. He proceeds at a leisurely pace and leads to such recent developments as the theorem of Gao and Lenstra [GL], which completely classifies all optimal normal bases. The presentation is very concrete, coherent and readable. It is an excellent textbook and reference for people interested in normal bases and in the applications of finite fields to combinatorics.

Menezes's book consists of independent chapters written by six active workers in the field. Each chapter surveys a different topic, includes a number of research problems, and is reasonably self-contained. The various chapters are clearly written and well coordinated (with some overlap). The book includes much more material than Jungnickel's book. In addition to normal bases, Menezes's book also includes

factorization of polynomials, construction of irreducible polynomials, discrete logarithms, the use of elliptic curves in public key cryptosystems, and algebra-geometric codes. The presentation is mostly brief but engaging. The book is an excellent reference for people interested in the algorithmic and applied aspects of finite fields.

To conclude this combined review, I would like to remark that it does not seem to be widely known in the mathematical community that there are many people working on finite fields. This is an area which provides a fruitful and productive meeting ground for mathematicians, computer scientists, and engineers. Much collaborative work among the different groups of people is being done and will undoubtedly continue to be done. As a result of this diverse and explosive growth, finite field theory will likely divide into several branches. One would thus expect to see many new books about finite fields in the near future. The above-mentioned books serve as an introduction to what we can expect.

ACKNOWLEDGMENT

I would like to thank Hendrik Lenstra, Jr., for many stimulating suggestions and several colleagues for helpful comments.

REFERENCES

- [Co1] S. D. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials*, L'Enseign. Math. **36** (1990), 53–65.
- [Co2] ———, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, Canad. Math. Bull. **33** (1990), 230–234.
- [Co3] ———, *Permutation polynomials and primitive permutation groups*, Arch. Math. **57** (1991), 417–423.
- [Di1] L. E. Dickson, *The analytic representation of substitutions on a prime power of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.
- [Di2] ———, *Linear groups with an exposition of the Galois field theory*, B. G. Teubner, Leipzig, 1901.
- [EGN] R. J. Evans, J. Greene, and H. Niederreiter, *Linearized polynomials and permutation polynomials of finite fields*, Michigan Math. J. **39** (1992), 405–413.
- [Fr] M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.
- [FGS] M. Fried, R. Guralnick, and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
- [GL] X. Gao and H. W. Lenstra, Jr., *Optimal normal bases*, Des. Codes, Cryptogr. **2** (1992), 315–323.
- [Ha] D. R. Hayes, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J. **34** (1967), 293–305.
- [LN] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
- [Wa] D. Wan, *Permutation polynomials and resolution of singularities over finite fields*, Proc. Amer. Math. Soc. **110** (1990), 303–309.
- [Sh] I. Shparlinski, *On bivariate polynomial factorization over finite fields*, Math. Comp. **60** (1993), 787–791.

DAQING WAN

UNIVERSITY OF NEVADA AT LAS VEGAS AND INSTITUTE FOR ADVANCED
STUDY

E-mail address: `dwan@math.ias.edu`