Lecture Notes in Mathematics 536

Wolfgang M. Schmidt

Equations over Finite Fields
An Elementary Approach

有限域上的方程

Springer

世界图书出版公司
www.wpcbj.com.cn

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

536

Wolfgang M. Schmidt

Equations over Finite Fields
An Elementary Approach

Springer-Verlag
Berlin · Heidelberg · New York 1976

图书在版编目（CIP）数据

有限域上的方程 = Equations over Finite Fields : An Elementary Approach : 英文 /（美）W. M. 施密特（Wolfgang M. Schmidt）著 . — 影印本 . — 北京 : 世界图书出版有限公司北京分公司 , 2017.10
ISBN 978-7-5192-2928-3

Ⅰ . ①有… Ⅱ . ① W… Ⅲ . ①有限域—方程—研究—英文 Ⅳ . ① O122.2

中国版本图书馆 CIP 数据核字 (2017) 第 110145 号

中文书名 有限域上的方程
英文书名 Equations over Finite Fields: An Elementary Approach

著　　者 Wolfgang M. Schmidt
责任编辑 刘　慧　高　蓉
装帧设计 蔡　彬

出版发行 世界图书出版有限公司北京分公司
地　　址 北京市东城区朝内大街 137 号
邮　　编 100010
电　　话 010-64038355（发行）　64037380（客服）　64033507（总编室）
网　　址 http://www.wpcbj.com.cn
邮　　箱 wpcbjst@vip.163.com
销　　售 新华书店
印　　刷 三河市国英印务有限公司
开　　本 711 mm × 1245 mm　1/24
印　　张 12
字　　数 230 千字
版　　次 2017 年 10 月第 1 版　　2017 年 10 月第 1 次印刷
版权登记 01-2016-6781
国际书号 ISBN 978-7-5192-2928-3
定　　价 48.00 元

Author
Wolfgang M. Schmidt
Department of Mathematics
University of Colorado
Boulder, Colo., 80309/USA

Library of Congress Cataloging in Publication Data

Schmidt, Wolfgang M
Equations over finite fields.

(Lecture notes in mathematics ; 536)
Bibliography: p.
1. Diophantine analysis. 2. Modular fields.
I. Title. II. Series: Lecture notes in mathematics (Berlin) ; 536.
QA3.L28 vol.536 [QA242] 510'.8s [512.9'4]
76-26612

Preface

These Lecture Notes were prepared from notes taken by M. Ratliff and K. Spackman of lectures given at the University of Colorado.

I have tried to present a proof as simple as possible of Weil's theorem on curves over finite fields. The notions of "simple" or "elementary" have different interpretations, but I believe that for a reader who is unfamiliar with algebraic geometry, perhaps even with algebraic functions in one variable, the simplest method is the one which originated with Stepanov. Hence it is this method which I follow.

The length of these Notes is perhaps shocking. However, it should be noted that only Chapters I and III deal with Weil's theorem. Furthermore, the style is (I believe) leisurely, and several results are proved in more than one way. I start in Chapter I with the simplest case, i.e., with curves $y^d = f(x)$. At first I do the simplest subcase, i.e., the case when the field is the prime field and when d is coprime to the degree of f. This special case is now so easy that it could be presented to undergraduates. The general equation $f(x,y) = 0$ is taken up only in Chapter III, but a reader in a hurry could start there. The second chapter, on character sums and exponential sums, is included at such an early stage because of the many applications in number theory. Chapters IV, V and VI deal with equations in an arbitrary number of variables.

Possible sequences are chapters

I by itself, or

I, III for Weil's theorem, or

I.1,III for a reader who is in a hurry, or

I, II for character sums and exponential sums, or

I, II, IV, or

I, III, IV.3 and V .

Originally I had planned to include Bombieri's version of the Stepanov method. I did include it in my lectures at the University of Colorado, but I first had to prove the Riemann-Roch Theorem and basic properties of the zeta function of a curve. A proof of these basic properties in the Lecture Notes would have made these unduly long, while their omission would have made the Bombieri version not self complete. Hence I decided after some hesitation to exclude this version from the Notes.

Recently Deligne proved far reaching generalizations of Weil's theorem to non-singular equations in several variables, thereby confirming conjectures of Weil. It is to be noted, however, that Deligne's proof rests on an assertion of Grothendieck concerning a certain fixed point theorem. To the best of my knowledge, a proof of this fixed point theorem has not appeared in print yet. It is perhaps needless to say that at present there is no elementary approach to such a generalization of Weil's theorem. But it is to be hoped that some day such an approach will become available, at least for those cases which are used most often in analytic number theory.

November, 1975 W. M. Schmidt

Notation

F^* is the multiplicative group of a field F.

$\bar{F}$ is the algebraic closure of a field F.

F^n is the product $F \times \ldots \times F$, i.e., the set of n-tuples $(x_1,\ldots,x_n)$ with $x_i \in F$ $(i = 1,\ldots,n)$.

$[F_1 : F_2]$ denotes the degree of a field extension $F_1 \supset F_2$.

$\mathfrak{T}$ denotes the trace and $\mathfrak{N}$ the norm.

F_q will denote the finite field with q elements.

p will be the characteristic.

$\mathbb{Q}$ is the field of rational numbers,

$\mathbb{R}$ the field of reals,

$\mathbb{C}$ the field of complex numbers,

$\mathbb{Z}$ the ring of (rational) integers.

$\cong$ denotes isomorphism of fields or groups.

Quite often, $x,y,z\ldots$ will be elements which lie in a ground field or are algebraic over a ground field, $X,Y,Z,\ldots$ will be variables, i.e., will be algebraically independent over a ground field, and $\mathfrak{x}, \mathfrak{y},\ldots$ will be algebraic functions, i.e., they will be algebraically dependent on some of $X,Y,\ldots$. Thus $f(X_1,\ldots,X_n)$ is a polynomial, and $f(x_1,\ldots,x_n)$ is the value of this polynomial at $(x_1,\ldots,x_n)$.

$F(x)$ or $F(X)$ or $F(X,Y)$ or $F(X,\mathfrak{y})$, or similar, will be the field obtained by adjoining x or X or X,Y or $X,\mathfrak{y}$ to a ground field F. Thus $F(X)$ is the field of rational functions in a variable X with coefficients in F. $R[X]$ denotes the ring of polynomials in X with coefficients in the ring R.

If a,b are in Z, we write $a|b$ (or $a+b$) if a does (or does not) divide b. Occasionally we shall write $d|q-1$ instead of the more proper notation $d|(q-1)$. Again, we shall write $f(X)|g(X)$ if the polynomial $f(X)$ divides $g(X)$. Further $(f(X))$ (or $(f(X),g(X))$) will be the ideal generated by $f(X)$ (or by $f(X)$ and $g(X)$).

$|\omega|$ denotes the number of elements of a finite set ω. Given sets $A \subseteq B$, the set theoretic difference is denoted by $B \sim A$.

Table of Contents

Introduction

Gauss (1801) made an extensive study of quadratic congruences modulo a prime p. He also obtained the number of solutions of the cubic congruence

$$ax^3 - by^3 \equiv 1 \pmod{p}$$

for primes $p = 3n+1$, and of the quartic congruence

$$ax^4 - by^4 \equiv 1 \pmod{p}$$

for primes $p = 4n+1$. He studied the congruence

$$ax^4 - by^2 \equiv 1 \pmod{p}$$

for arbitrary primes p.

Artin (1924) considered the congruence $y^2 \equiv f(x) \pmod{p}$, where $f(X)$ is a polynomial whose leading coefficient is not divisible by p and which has no multiple factors modulo p, and made the following conjecture: The number N of solutions satisfies

$$|N - p| \leq 2\sqrt{p} \quad \text{if} \quad \deg f = 3,$$

$$|N+1 - p| \leq 2\sqrt{p} \quad \text{if} \quad \deg f = 4.$$

This conjecture was proved by Hasse (1936 b,c.). In fact, let F_q be the finite field with q elements, and let N be the number of solutions $(x,y) \in F_q^2$ of the equation $y^2 = f(x)$, where $f(X)$ is a polynomial with coefficients in F_q and with distinct roots. Then

$$|N - q| \leq 2\sqrt{q} \quad \text{if} \quad \deg f = 3,$$

$$|N+1 - q| \leq 2\sqrt{q} \quad \text{if} \quad \deg f = 4.$$

Suppose $f(X,Y)$ is a polynomial of total degree d, with coefficients in F_q and with N zeros (x,y) with coordinates in F_q. Suppose $f(X,Y)$ is absolutely irreducible, i.e., irreducible not only over F_q, but also over every algebraic extension thereof.

Weil (1940,1948a)† proved the famous theorem (the "Riemann Hypothesis for Curves over Finite Fields") that

$$|N - q| \leqq 2g\sqrt{q} + c_1(d) \tag{1}$$

where g is the "genus" of the curve $f(x,y) = 0$ and where $c_1(d)$ is a constant depending on d. It can be shown that $g \leqq \frac{1}{2}(d-1)(d-2)$, hence that

$$|N - q| \leqq (d-1)(d-2)\sqrt{q} + c_1(d) .$$

Weil's proof depends on algebraic geometry, in particular on Castelnuovo's inequality. A somewhat simpler proof was given by Roquette (1953); see also Lang (1961), Eichler (1963).

More recently, Stepanov (1969, 1970, 1971, 1972a, 1972b, 1974) gave a new proof of special cases of Weil's result which does not depend on algebraic geometry, but which is related to Thue's (1908) method in diophantine approximation. This method consists in the construction of a polynomial in one variable with rather many zeros. The construction is by the method of undetermined coefficients.

In particular, Stepanov proved that

$$|N - q| \leqq c_2(d)\sqrt{q} \tag{2}$$

if $f(X,Y)$ is of some special type, for instance if

$$f(X,Y) = Y^d - f(X)$$

where d and the degree of f are coprime. Later Bombieri (1973) and Schmidt proved (2) for absolutely irreducible $f(X,Y)$ by the Thue - Stepanov method. It follows from the theory of the zeta function that (2) implies (1).

In these Lectures we shall prove (2) by the Stepanov method.

---

†The 1940 paper is only an announcement.

I. Equations $y^d = f(x)$ and $y^q - y = f(x)$.

References: Stepanov (1969, 1970, 1971, 1972a), Mitkin (1972), Stark (1973).

§ 1. Finite Fields (Galois fields).

Let F be any field. There is a smallest subfield $k \subseteq F$ (the intersection of all subfields of F), called the prime subfield of F, and either $k = \mathbb{Q}$ or $k = F_p$, the integers modulo a prime p. In the first case F is of characteristic 0, in the second case of characteristic p. In the case when F is finite, $k = F_p$, and $[F : F_p]$ is finite. If, say, $[F : F_p] = K$, then $|F| = p^K$. Hence if F_q is a field with q elements, then $q = p^K$, p prime.

Let F_q be a finite field and let F_q^* be the multiplicative group of F_q. Then $|F_q^*| = q - 1$. If $x \in F_q^*$, then $x^{q-1} = 1$; hence, for $x \in F_q$, we have $x^q - x = 0$. Therefore, $X^q - X = \prod_{x \in F_q} (X - x)$. So F_q is the splitting field of $X^q - X$ over F_p, and F_q is a normal extension of F_p. Moreover, as a splitting field, F_q is unique up to isomorphisms.

Conversely, let F be the splitting field of $X^q - X$ over F_p, where $q = p^K$. Let $x_1, \ldots, x_q$ be the roots of this polynomial in F. These roots are distinct since the derivative $D(X^q - X) = -1 \neq 0$. Now $x_i + x_j$ is a root of $X^q - X$, since,

$$(x_i + x_j)^q - (x_i + x_j) = x_i^q + x_j^q - x_i - x_j = 0 ,$$

and similarly for $x_i - x_j$. Also $x_i x_j$ is a root, since

$$(x_i x_j)^q = x_i^q x_j^q = x_i x_j ,$$

and similarly x_i/x_j is a root if $x_j \neq 0$. These roots clearly form a field, so, in fact, $F = \{x_1, x_2, \ldots, x_q\}$. Thus a field with q elements does exist.

Considering the above, we have:

THEOREM 1A. If F_q is a finite field of order q, then $q = p^K$, p prime. For every such q, there exists exactly one field F_q. This field is the splitting field of $X^q - X$ over F_p, and all of its elements are roots of $X^q - X$.

THEOREM 1B. The multiplicative group F_q^* is cyclic.

For the proof of this theorem we need

LEMMA 1C. Let G be a finite group of order d. Suppose for every divisor e of d, there are at most e elements $x \in G$ with $x^e = 1$. Then G is cyclic.

The theorem follows immediately, since $X^e - 1$ has at most e roots in F_q^*. It only remains to give a

Proof of Lemma 1C. Every element of G is of some order e, where $e \mid d$. Let $\psi(e)$ be the number of elements of G whose order is e. Either $\psi(e) = 0$ or $\psi(e) \neq 0$. Suppose $\psi(e) \neq 0$, and let $y \in G$ have order e. Then the elements $y, y^2, \ldots, y^e = 1$ are distinct and all satisfy $x^e = 1$. Since there are e of these elements, by hypothesis there can be no other elements $x \in G$ satisfying $x^e = 1$.

Now let $z \in G$ be any element of order e; then $z = y^i$ $(1 \le i \le e)$. Notice that $z = y^i$ has order e precisely if $(i,e) = 1$. Hence $\psi(e) = \varphi(e)$, where φ is the Euler φ-function. So, in general, $\psi(e) \le \varphi(e)$, taking into account the possibility that $\psi(e) = 0$. But

$$d = \sum_{e|d} \psi(e) \le \sum_{e|d} \varphi(e) = d .$$

Hence, for every divisor e of d, $\psi(e) = \varphi(e)$; in particular, $\psi(d) = \varphi(d) \neq 0$. That is, there exists an element of order d; hence, G is cyclic.

COROLLARY 1D. Let $q = p^K$. Then $F_q = F_p(x)$ for some x.

Proof. Let x be a generator of F_q^*.

Let $F_q \subseteq F_r$ be finite fields; then $r = q^\kappa$. Consider the mapping $\omega : F_r \to F_r$ such that $\omega(x) = x^q$. This mapping is one-one. For suppose $x^q = y^q$, then

$$0 = x^q - y^q = (x - y)^q ,$$

whence $x - y = 0$ and $x = y$. The mapping ω is then one-one of a finite set to itself, hence is onto. Moreover, ω is an automorphism of F_r, since

$$\omega(x + y) = (x + y)^q = x^q + y^q = \omega(x) + \omega(y)$$

and $$\omega(xy) = (xy)^q = x^q y^q = \omega(x)\,\omega(y) .$$

In fact, ω is an automorphism of "F_r over F_q" (leaving F_q fixed), since if $x \in F_q$, $\omega(x) = x^q = x$. In other words,

ω is a member of the Galois group of F_r over F_q. The map ω is called the "Frobenius automorphism".

If $r = q^K$, then $1, \omega, \omega^2, \ldots, \omega^{K-1}$ are automorphisms of F_r over F_q, and they are distinct because if

$$\omega^i = \omega^j \qquad (0 \le i, j \le K - 1),$$

then $$\omega^i(x) = \omega^j(x) \quad \text{for all } x \in F_r,$$

$$x^{q^i} = x^{q^j} \quad \text{for all } x \in F_r,$$

so $$x^{q^i} - x^{q^j} = 0 \quad \text{for all } x \in F_r.$$

But the degree of the polynomial $X^{q^i} - X^{q^j}$ is less than $q^K = r$, so the above cannot hold identically for all $x \in F_r$, unless $X^{q^i} - X^{q^j}$ is identically zero and $i = j$. Since the order of the Galois group is K, these are the only automorphisms of F_r over F_q. We have shown:

THEOREM 1E. Every automorphism of F_r over F_q is of the form ω^i $(0 \le i \le K - 1)$, where $\omega(x) = x^q$. That is, the Galois group of F_r over F_q is cyclic with generator ω.

Recall that the trace of an element is the sum of its conjugates. For the case $F_q \subseteq F_r$, the trace of an element $x \in F_r$ is

$$T(x) = x + x^q + x^{q^2} + \ldots + x^{q^{K-1}}.$$