Wolfgang M. Schmidt

Equations over Finite Fields
An Elementary Approach

有限域上的方程





Lecture Notes 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. 一影印本. 一北京: 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 0122.2

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

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

Mathemat

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.
QA3.128 vol.536 [QA242] 510°.88 [512.9°4]

Reprint from English language edition: Equations over Finite Fields: An Elementary Approach by Wolfgang M. Schmidt Copyright © Springer -Verlag Berlin Heidelberg 1975 This Springer imprint is published by Springer Nature The registered company is Springer-Verlag GmbH

This reprint has been authorised by Springer-Verlag GmbH for distribution in China Mainland.

Preface was one tobast a not III.I.I

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

此为试读、需要完整PDF请访问: www.ertongbook.com

- 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

- F is the multiplicative group of a field F.
- F^n is the product F x ... x F , i.e., the set of n-tuples (x_1,\dots,x_n) with x_i \in F (i = 1,...,n) .
- $[F_1:F_2]$ denotes the degree of a field extension $F_1\supseteq F_2$.
- I denotes the trace and M the norm.
- F will denote the finite field with q elements.
- p will be the characteristic.
- Q is the field of rational numbers,
- R the field of reals,
- C the field of complex numbers,
- Z the ring of (rational) integers.
- ≥ denotes isomorphism of fields or groups.

Quite often, x,y,z... will be elements which lie in a ground field or are algebraic over a ground field, X,Y,Z,... will be variables, i.e., will be algebraically independent over a ground field, and \mathfrak{X} , \mathfrak{J} ,... will be algebraic functions, i.e., they will be algebraically dependent on some of X,Y,... 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,M), or similar, will be the field obtained by adjoining x or X or X,Y or X,M 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)).

 $|_{\varpi}|$ denotes the number of elements of a finite set ϖ . Given sets $A\subseteq B$, the set theoretic difference is denoted by $B\curvearrowright A$.

east the test deriver with the selection of selection of the selection of

varie oryen, x,r,z... will be elements which lie in a ground

Color of the All of the allegent districtly transport over a product transport over the Allegent Colors of the All

and the property of any or and any forther bankong and transmitted and

or thrown has not appeared in print yet. It is perhaps impelesses and all particles and off all transfers of the control of th

enderton a un anottomo tenester to plant and all (K), which or as an election

2 at a fallocation to sain the describe that the control of the co

Table of Contents

Chapte	r		Page
	Int	roduction	.81 1
I.	Equ	ations $y^d = f(x)$ and $y^q - y = f(x)$	dA .I
	1.	Finite Fields	. 3
	2.	Equations $y^d = f(x) \dots \dots$	8
	3.	Construction of certain polynomials	16
	4.	Proof of the Main Theorem	21
	5.	Removal of the condition (m,d) = I	22
	6.	Hyperderivatives	27
	7.	Removal of the condition that $q = p \text{ or } p^2 \dots$	31
	8.	The Work of Stark	32
	9.	Equations $y^{q} - y = f(x) \dots$	34
IEII.	Cha	aracter Sums and Exponential Sums	
	1.	Characters of Finite Abelian Groups	38
	2.	Characters and Character Sums associated with	41
		Finite Fields	
	3.	Gaussian Sums	46
	4.	The low road	50
	5.	Systems of equations $y_1^{d}1 = f_1(x), \dots, y_n^{d}n =$	
		$f_n(x)$	52
	6.	Auxiliary lemmas on $w_1^{\vee} + \ldots + w_{\ell}^{\vee} \cdot \ldots \cdot$	57
	7.	Further auxiliary lemmas	60
	8.	Zeta Function and L-Functions	62
	9.	Special L-Functions	65
	10.	Field extensions. The Davenport - Hasse relations	72
	11.	Proof of the Principal Theorems	. 877

er		Page
12.	Kloosterman Sums	84
13.	Further Results	88
Abs	olutely Irreducible Equations $f(x,y) = 0$	
1.	Introduction	92
2.	Independence results	97
3.	Derivatives	105
4.	Construction of two algebraic functions	107
5.	Construction of two polynomials	114
6.	Proof of the Main Theorem	116
7.	Valuations	119
8.	Hyperderivatives again	125
9.	Removal of the condition that $q = p \dots$	131
Equ	nations in Many Variables	
1.	Theorems of Chevalley and Warning	134
2.	Quadratic forms	140
3.	Elementary upper bounds. Projective zeros	147
4.	The average number of zeros of a polynomial	157
5.	Additive Equations: A Chebychev Argument	160
6.	Additive Equations: Character Sums	166
7.	Equations $f_1(y)x_1^d 1 + \ldots + f_n(y)x_n^d n = 0 \ldots$	173
Abi		
1.	Elimination Theory	177
2.	The absolute irreducibility of polynomials (I)	190
3.		194
4.		204
	12. 13. Abs 1. 2. 3. 4. 5. 6. 7. 8. 9. 4. 5. 6. 7. Abi 1. 2. 3.	12. Kloosterman Sums 13. Further Results. Absolutely Irreducible Equations $f(x,y) = 0$ 1. Introduction

Chapter											Page
5. The number of polynomials in									•	irue ioni	210
VI. Rudiments of Algebrain Varieties over				The	Nun	ber	of	Poi	int	s	
1. Varieties											216
2. Dimension											228
3. Rational Maps											235
4. Birational Map	os										244
5. Linear Disjoin	ntness	of Fi	elds			٠.					250
6. Constant Field	Extens	sions									254
7. Counting Point	ts in Va	ariet	ies	Over	Fir	ite	Fie	lds	s.		260
BIBLIOGRAPHY											265

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

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

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

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

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

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

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) the proved the famous theorem (the "Riemann Hypothesis for Curves over Finite Fields") that

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

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 $g \le \frac{1}{2}(d-1)(d-2)$, hence that $\left|N-q\right| \le (d-1)(d-2)\sqrt{q} + c_1(d) \ .$

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

$$|N - q| \le c_2(d) \sqrt{q}$$

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), Annual Mark 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 <u>prime subfield</u> of F, and either $k = \mathbb{Q}$ or $k = \mathbb{F}_p$, the integers modulo a prime p. In the first case F is of characteristic O, in the second case of characteristic p. In the case when F is finite, $k = \mathbb{F}_p$, and $[F: \mathbb{F}_p]$ is finite. If, say, $[F: \mathbb{F}_p] = \mathbb{K}$, then $|F| = p^K$. Hence if \mathbb{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, $X^q-x=\prod\limits_{x\in F_q}(x-x)$. 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, \dots, 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

$$(x_i x_j)^q = x_i^q x_j^q = x_i x_j$$
, (2701) Hass

and similarly x_i/x_j is a root if $x_j \neq 0$. These roots clearly form a field, so, in fact, $F = \{x_1, x_2, \dots, x_q\}$. 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.

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

The theorem follows immediately, since χ^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|d. Let ψ (e) be the number of elements of G whose order is e. Either ψ (e) = 0 or ψ (e) \neq 0. Suppose ψ (e) \neq 0, and let $y \in G$ have order e. Then the elements $y, y^2, \dots, y^e = 1$ 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 $z = y^1$ $(1 \le i \le e)$. Notice that $z = y^1$ has order e precisely if (i,e) = 1. Hence $\psi(e) = \phi(e)$, where ϕ is the Euler ϕ -function. So, in general, $\psi(e) \le \phi(e)$, taking into account the possibility that $\psi(e) = 0$. But

$$d = \sum_{e \mid d} \psi(e) \le \sum_{e \mid d} \phi(e) = d .$$

Hence, for every divisor e of d, ψ (e) = ϕ (e); in particular, ψ (d) = ϕ (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 $r=q^{\aleph}$. 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 w is then one-one of a finite set to itself, hence is onto. Moreover, w is an automorphism of F_r , since

$$w(x + y) = (x + y)^{q} = x^{q} + y^{q} = w(x) + w(y)$$

and $w(xy) = (xy)^{q} = x^{q} y^{q} = w(x) w(y)$.

In fact, ω is an automorphism of "F over F" (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 over F . The map is called the "Frobenius automorphism".

If $r = q^{\kappa}$, then $1, \omega, \omega^2, \dots, \omega^{\kappa-1}$ are automorphisms of F over F , and they are distinct because if

$$w^{i} = w^{j} \qquad (0 \le i, j \le K - 1),$$
then
$$w^{i}(x) = w^{j}(x) \quad \text{for all } x \in F_{r},$$

$$x^{q^{i}} = x^{q^{j}} \quad \text{for all } x \in F_{r},$$
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 Fr over F is of the form ω^i (0 \leq i \leq 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 = F, the trace of an element $x \in F_r$ is $\chi(x) = x + x^q + x^{q^2} + ... + x^{q^{K-1}}$.

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