Graduate Texts in
Mathematics

210

Number Theory in Functions Fields

Springer-Verlag

Michael Rosen

Number Theory in Function Fields

Springer

Michael Rosen
Department of Mathematics
Brown University
Providence, RI 02912-1917
USA
michael_rosen@brown.edu

Mathematics Subject Classification (2000): 11R29, 11R58, 14H05

Library of Congress Cataloging-in-Publication Data
Rosen, Michael I. (Michael Ira), 1938–
Number theory in function fields / Michael Rosen.
p. cm. — (Graduate texts in mathematics ; 210)
Includes bibliographical references and index.
ISBN 0-387-95335-3 (alk. paper)
1. Number theory. 2. Finite fields (Algebra). I. Title. II. Series.
QA241 .R675 2001
512'.7—dc21 2001042962

Printed on acid-free paper.

Production managed by Allan Abrams; manufacturing supervised by Jacqui Ashri.
Typeset by TeXniques, Inc., Boston, MA.
Printed and bound by R.R. Donnelley and Sons, Harrisonburg, VA.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-95335-3 SPIN 10844406

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Preface

Elementary number theory is concerned with the arithmetic properties of the ring of integers, $\mathbb{Z}$, and its field of fractions, the rational numbers, $\mathbb{Q}$. Early on in the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}[T]$, the ring of polynomials over a finite field. Both rings are principal ideal domains, both have the property that the residue class ring of any non-zero ideal is finite, both rings have infinitely many prime elements, and both rings have finitely many units. Thus, one is led to suspect that many results which hold for $\mathbb{Z}$ have analogues of the ring A. This is indeed the case. The first four chapters of this book are devoted to illustrating this by presenting, for example, analogues of the little theorems of Fermat and Euler, Wilson's theorem, quadratic (and higher) reciprocity, the prime number theorem, and Dirichlet's theorem on primes in an arithmetic progression. All these results have been known for a long time, but it is hard to locate any exposition of them outside of the original papers.

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions K of $\mathbb{Q}$, which are called algebraic number fields, and investigating properties of the ring of algebraic integers $O_K \subset K$, defined as the integral closure of $\mathbb{Z}$ in K. Similarly, we can consider $k = \mathbb{F}(T)$, the quotient field of A and finite algebraic extensions L of k. Fields of this type are called algebraic function fields. More precisely, an algebraic function fields with a finite constant field is called a global function field. A global function field is the true analogue of algebraic number field and much of this book will be concerned with investigating properties of global function fields. In Chapters 5 and 6, we will discuss function

fields over arbitrary constant fields and review (sometimes in detail) the basic theory up to and including the fundamental theorem of Riemann-Roch and its corollaries. This will serve as the basis for many of the later developments.

It is important to point out that the theory of algebraic function fields is but another guise for the theory of algebraic curves. The point of view of this book will be very arithmetic. At every turn the emphasis will be on the analogy of algebaic function fields with algebraic number fields. Curves will be mentioned only in passing. However, the algebraic-geometric point of view is very powerful and we will freely borrow theorems about algebraic curves (and their Jacobian varieties) which, up to now, have no purely arithmetic proof. In some cases we will not give the proof, but will be content to state the result accurately and to draw from it the needed arithmetic consequences.

This book is aimed primarily at graduate students who have had a good introductory course in abstract algebra covering, in addition to Galois theory, commutative algebra as presented, for example, in the classic text of Atiyah and MacDonald. In the interest of presenting some advanced results in a relatively elementary text, we do not aspire to prove everything. However, we do prove most of the results that we present and hope to inspire the reader to search out the proofs of those important results whose proof we omit. In addition to graduate students, we hope that this material will be of interest to many others who know some algebraic number theory and/or algebraic geometry and are curious about what number theory in function field is all about. Although the presentation is not primarily directed toward people with an interest in algebraic coding theory, much of what is discussed can serve as useful background for those wishing to pursue the arithmetic side of this topic.

Now for a brief tour through the later chapters of the book.

Chapter 7 covers the background leading up to the statement and proof of the Riemann-Hurwitz theorem. As an application we discuss and prove the analogue of the ABC conjecture in the function field context. This important result has many consequences and we present a few applications to diophantine problems over function fields.

Chapter 8 gives the theory of constant field extensions, mostly under the assumption that the constant field is perfect. This is basic material which will be put to use repeatedly in later chapters.

Chapter 9 is primarily devoted to the theory of finite Galois extensions and the theory of Artin and Hecke L-functions. Two versions of the very important Tchebatorov density theorem are presented: one using Dirichlet density and the other using natural density. Toward the end of the chapter there is a sketch of global class field theory which enables one, in the abelian case, to identify Artin L-series with Hecke L-series.

Chapter 10 is devoted to the proof of a theorem of Bilharz (a studentof Hasse) which is the function field version of Artin's famous conjecture on

primitive roots. This material, interesting in itself, illustrates the use of many of the results developed in the preceding chapters.

Chapter 11 discusses the behavior of the class group under constant field extensions. It is this circle of ideas which led Iwasawa to develop "Iwasawa theory," one of the most powerful tools of modern number theory.

Chapters 12 and 13 provide an introduction to the theory of Drinfeld modules. Chapter 12 presents the theory of the Carlitz module, which was developed by L. Carlitz in the 1930s. Drinfeld's papers, published in the 1970s, contain a vast generalization of Carlitz's work. Drinfeld's work was directed toward a proof of the Langlands' conjectures in function fields. Another consequence of the theory, worked out separately by Drinfeld and Hayes, is an explicit class field theory for global function fields. These chapters present the basic definitions and concepts, as well as the beginnings of the general theory.

Chapter 14 presents preliminary material on S-units, S-class groups, and the corresponding L-functions. This leads up to the statement and proof of a special case of the Brumer-Stark conjecture in the function field context. This is the content of Chapter 15. The Brumer-Stark conjecture in function fields is now known in full generality. There are two proofs — one due to Tate and Deligne, another due to Hayes. It is the author's hope that anyone who has read Chapters 14 and 15 will be inspired to go on to master one or both of the proofs of the general result.

Chapter 16 presents function field analogues of the famous class number formulas of Kummer for cyclotomic number fields together with variations on this theme. Once again, most of this material has been generalized considerably and the material in this chapter, which has its own interest, can also serve as the background for further study.

Finally, in Chapter 17 we discuss average value theorems in global fields. The material presented here generalizes work of Carlitz over the ring $A = \mathbb{F}[T]$. A novel feature is a function field analogue of the Wiener-Ikehara Tauberian theorem. The beginning of the chapter discusses average values of elementary number-theoretic functions. The last part of the chapter deals with average values for class numbers of hyperelliptic function fields.

In the effort to keep this book reasonably short, many topics which could have been included were left out. For example, chapters had been contemplated on automorphisms and the inverse Galois problem, the number of rational points with applications to algebraic coding theory, and the theory of character sums. Thought had been given to a more extensive discussion of Drinfeld modules and the subject of explicit class field theory in global fields. Also omitted is any discussion of the fascinating subject of transcendental numbers in the function field context (for an excellent survey see J. Yu [1]). Clearly, number theory in function fields is a vast subject. It is of interest for its own sake and because it has so often served as a stimulous to research in algebraic number theory and arithmetic geometry. We hope this book will arouse in the reader a desire to learn more and explore further.

I would like to thank my friends David Goss and David Hayes for their encouragement over the years and for their work which has been a constant source of delight and inspiration.

I also want to thank Allison Pacelli and Michael Reid who read several chapters and made valuable suggestions. I especially want to thank Amir Jafari and Hua-Chieh Li who read most of the book and did a thorough job spotting misprints and inaccuracies. For those that remain I accept full responsibility.

This book had its origins in a set of seven lectures I delivered at KAIST (Korean Advanced Institute of Science and Technology) in the summer of 1994. They were published in: "Lecture Notes of the Ninth KAIST Mathematics Workshop, Volume 1, 1994, Taejon, Korea." For this wonderful opportunity to bring my thoughts together on these topics I wish to thank both the Institute and my hosts, Professors S.H. Bae and J. Koo.

Years ago my friend Ken Ireland suggested the idea of writing a book together on the subject of arithmetic in function fields. His premature death in 1991 prevented this collaboration from ever taking place. This book would have been much better had we been able to do it together. His spirit and great love of mathematics still exert a deep influence over me. I hope something of this shows through on the pages that follow.

Finally, my thanks to Polly for being there when I became discouraged and for cheering me on.

December 30, 2000

Michael Rosen
Brown University

Contents

1

Polynomials over Finite Fields

In all that follows $\mathbb{F}$ will denote a finite field with q elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. This field has p elements. In general the number of elements in a finite field is a power of a prime, $q = p^f$. Of course, p is the characteristic of $\mathbb{F}$.

Let $A = \mathbb{F}[T]$, the polynomial ring over $\mathbb{F}$. A has many properties in common with the ring of integers $\mathbb{Z}$. Both are principal ideal domains, both have a finite unit group, and both have the property that every residue class ring modulo a non-zero ideal has finitely many elements. We will verify all this shortly. The result is that many of the number theoretic questions we ask about $\mathbb{Z}$ have their analogues for A. We will explore these in some detail.

Every element in A has the form $f(T) = \alpha_0 T^n + \alpha_1 T^{n-1} + \cdots + \alpha_n$. If $\alpha_0 \neq 0$ we say that f has degree n, notationally $\deg(f) = n$. In this case we set $\operatorname{sgn}(f) = \alpha_0$ and call this element of $\mathbb{F}^*$ the sign of f. Note the following very important properties of these functions. If f and g are non-zero polynomials we have

$$\deg(fg) = \deg(f) + \deg(g) \quad \text{and} \quad \operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g).$$

$$\deg(f+g) \leq \max(\deg(f), \deg(g)).$$

In the second line, equality holds if $\deg(f) \neq \deg(g)$.

If $\operatorname{sgn}(f) = 1$ we say that f is a monic polynomial. Monic polynomials play the role of positive integers. It is sometimes useful to define the sign of the zero polynomial to be 0 and its degree to be $-\infty$. The above properties of degree then remain true without restriction.

Proposition 1.1. *Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $\deg(r) < \deg(g)$. Moreover, q and r are uniquely determined by these conditions.*

Proof. Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \operatorname{sgn}(f)$, $\beta = \operatorname{sgn}(g)$. We give the proof by induction on $n = \deg(f)$. If $n < m$, set $q = 0$ and $r = f$. If $n \geq m$, we note that $f_1 = f - \alpha\beta^{-1}T^{n-m}g$ has smaller degree than f. By induction, there exist $q_1, r_1 \in A$ such that $f_1 = q_1 g + r_1$ with r_1 being either 0 or with degree less than $\deg(g)$. In this case, set $q = \alpha\beta^{-1}T^{n-m} + q_1$ and $r = r_1$ and we are done.

If $f = qg + r = q'g + r'$, then g divides $r - r'$ and by degree considerations we see $r = r'$. In this case, $qg = q'g$ so $q = q'$ and the uniqueness is established.

This proposition shows that A is a Euclidean domain and thus a principal ideal domain and a unique factorization domain. It also allows a quick proof of the finiteness of the residue class rings.

Proposition 1.2. *Suppose $g \in A$ and $g \neq 0$. Then A/gA is a finite ring with $q^{\deg(g)}$ elements.*

Proof. Let $m = \deg(g)$. By Proposition 1.1 one easily verifies that $\{r \in A \mid \deg(r) < m\}$ is a complete set of representatives for A/gA. Such elements look like

$$r = \alpha_0 T^{m-1} + \alpha_1 T^{m-2} + \cdots + \alpha_{m-1} \quad \text{with } \alpha_i \in \mathbb{F}.$$

Since the α_i vary independently through $\mathbb{F}$ there are q^m such polynomials and the result follows.

Definition. Let $g \in A$. If $g \neq 0$, set $|g| = q^{\deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|g|$ is the number of elements in A/gA. It is immediate that $|fg| = |f|\,|g|$ and $|f + g| \leq \max(|f|, |g|)$ with equality holding if $|f| \neq |g|$.

It is a simple matter to determine the group of units in A, A^*. If g is a unit, then there is an f such that $fg = 1$. Thus, $0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$. The only units are the non-zero constants and each such constant is a unit.

Proposition 1.3. *The group of units in A is $\mathbb{F}^*$. In particular, it is a finite cyclic group with $q - 1$ elements.*

Proof. The only thing left to prove is the cyclicity of $\mathbb{F}^*$. This follows from the very general fact that a finite subgroup of the multiplicative group of a field is cyclic.

In what follows we will see that the number $q - 1$ often occurs where the number 2 occurs in ordinary number theory. This stems from the fact that the order of $\mathbb{Z}^*$ is 2.

By definition, a non-constant polynomial $f \in A$ is irreducible if it cannot be written as a product of two polynomials, each of positive degree. Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime (for the definitions of divisibility, prime, irreducible, etc., see Ireland and Rosen [1]). These words will be used interchangeably. Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in A has a unique monic generator. This should be compared with the statement that evey non-zero ideal in $\mathbb{Z}$ has a unique positive generator. Finally, the unique factorization property in A can be sharpened to the following statement. Every $f \in A$, $f \neq 0$, can be written uniquely in the form

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t},$$

where $\alpha \in \mathbb{F}^*$, each P_i is a monic irreducible, $P_i \neq P_j$ for $i \neq j$, and each e_i is a non-negative integer.

The letter P will often be used for a monic irreducible polynomial in A. We use P instead of p since the latter letter is reserved for the characteristic of $\mathbb{F}$. This is a bit awkward, but it is compensated for by being less likely to lead to confusion.

The next order of business will be to investigate the structure of the rings A/fA and the unit groups $(A/fA)^*$. A valuable tool is the Chinese Remainder Theorem.

Proposition 1.4. *Let $m_1, m_2, \dots, m_t$ be elements of A which are pairwise relatively prime. Let $m = m_1 m_2 \dots m_t$ and ϕ_i be the natural homomorphism from A/mA to A/m_iA. Then, the map $\phi : A/mA \to A/m_1A \oplus A/m_2A \oplus \cdots \oplus A/m_tA$ given by*

$$\phi(a) = (\phi_1(a), \phi_2(a), \dots, \phi_t(a))$$

is a ring isomorphism.

Proof. This is a standard result which holds in any principal ideal domain (properly formulated it holds in much greater generality).

Corollary. *The same map ϕ restricted to the units of A, A^*, gives rise to a group isomorphism*

$$(A/mA)^* \simeq (A/m_1A)^* \times (A/m_2A)^* \times \cdots \times (A/m_tA)^*.$$

Proof. This is a standard exercise. See Ireland and Rosen [1], Proposition 3.4.1.

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$ is its prime decomposition. From the above considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where P is an irreducible polynomial and e is a positive integer. When $e = 1$ the situation is very similar to that is $\mathbb{Z}$.

Proposition 1.5. *Let $P \in A$ be an irreducible polynomial. Then, $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.*

Proof. Since A is a principal ideal domain, PA is a maximal ideal and so A/PA is a field. A finite subgroup of the multiplicative group of a field is cyclic. Thus $(A/PA)^*$ is cyclic. That the order of this group is $|P| - 1$ is immediate.

We now consider the situation when $e > 1$. Here we encounter something which is quite different in A from the situation in $\mathbb{Z}$. If p is an odd prime number in $\mathbb{Z}$ then it is a standard result that $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic for all positive integers e. If $p = 2$ and $e \geq 3$ then $(\mathbb{Z}/2^e\mathbb{Z})^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{e-2}. The situation is very different in A.

Proposition 1.6. *Let $P \in A$ be an irreducible polynomial and e a positive integer. The order of $(A/P^eA)^*$ is $|P|^{e-1}(|P| - 1)$. Let $(A/P^eA)^{(1)}$ be the kernel of the natural map from $(A/P^eA)^*$ to $(A/PA)^*$. It is a p-group of order $|P|^{e-1}$. As e tends to infinity, the minimal number of generators of $(A/P^eA)^{(1)}$ tends to infinity.*

Proof. The ring A/P^eA has only one maximal ideal PA/P^eA which has $|P|^{e-1}$ elements. Thus, $(A/P^eA)^* = A/P^eA - PA/P^eA$ has $|P|^e - |P|^{e-1} = |P|^{e-1}(|P| - 1)$ number of elements. Since $(A/P^eA)^* \to (A/PA)^*$ is onto, and the latter group has $|P| - 1$ elements the assertion about the size of $(A/P^eA)^{(1)}$ follows. It remains to prove the assertion about the minimal number of generators.

It is instructive to first consider the case $e = 2$. Every element in $(A/P^2A)^{(1)}$ can be represented by a polynomial of the form $a = 1 + bP$. Since we are working in characteristic p we have $a^p = 1 + b^pP^p \equiv 1 \pmod{P^2}$. So, we have a group of order $|P|$ with exponent p. If $q = p^f$ it follows that $(A/P^2A)^{(1)}$ is a direct sum of $f \deg(P)$ number of copies of $\mathbb{Z}/p\mathbb{Z}$. This is a cyclic group only under the very restrictive conditions that $q = p$ and $\deg(P) = 1$.

To deal with the general case, suppose that s is the smallest integer such that $p^s \geq e$. Since $(1 + bP)^{p^s} = 1 + (bP)^{p^s} \equiv 1 \pmod{P^e}$ we have that raising to the p^s-power annihilates $G = (A/P^eA)^{(1)}$. Let d be the minimal number of generators of this group. It follows that there is an onto map from $(\mathbb{Z}/p^s\mathbb{Z})^d$ onto G. Thus, $p^{ds} \geq p^{f \deg(P)(e-1)}$ and so

$$d \geq \frac{f \deg(P)(e-1)}{s}.$$

Since s is the smallest integer bigger than or equal to $\log_p(e)$ it is clear that $d \to \infty$ as $e \to \infty$.

It is possible to do a much closer analysis of the structure of these groups, but it is not necessary to do so now. The fact that these groups get very complicated does cause problems in the more advanced parts of the theory.

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$. We can give another characterization of this number which makes the relation to the Euler ϕ-function even more evident. We have seen that $\{r \in A \mid \deg(r) < \deg(f)\}$ is a set of representatives for A/fA. Such an r represents a unit in A/fA if and only if it is relatively prime to f. Thus $\Phi(f)$ is the number of non-zero polynomials of degree less than $\deg(f)$ and relatively prime to f.

Proposition 1.7.

$$\Phi(f) = |f| \prod_{P|f} (1 - \frac{1}{|P|}).$$

Proof. Let $f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$ be the prime decomposition of f. By the corollary to Propositions 1.4 and by Proposition 1.6, we see that

$$\Phi(f) = \prod_{i=1}^{t} \Phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i - 1}),$$

from which the result follows immediately.

The similarity of the formula in this proposition to the classical formula for $\phi(n)$ is striking.

Proposition 1.8. *If $f \in A, f \neq 0$, and $a \in A$ is relatively prime to f, i.e., $(a, f) = 1$, then*

$$a^{\Phi(f)} \equiv 1 \pmod{f}.$$

Proof. The group $(A/fA)^*$ has $\Phi(f)$ elements. The coset of a modulo f, $\bar{a}$, lies in this group. Thus, $\bar{a}^{\Phi(f)} = \bar{1}$ and this is equivalent to the congruence in the proposition.

Corollary. *Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then,*

$$a^{|P|-1} \equiv 1 \pmod{P}.$$

Proof. Since P is irreducible, it is relatively prime to a if and only if it does not divide a. The corollary follows from the proposition and the fact that for an irreducible P, $\Phi(P) = |P| - 1$ (Proposition 1.5).

It is clear that Proposition 1.8 and its corollary are direct analogues of Euler's little theorem and Fermat's little theorem. They play the same very important role in this context as they do in elementary number theory. By

way of illustration we proceed to the analogue of Wilson's theorem. Recall that this states that $(p-1)! \equiv -1 \pmod{p}$ where p is a prime number.

Proposition 1.9. *Let $P \in A$ be irreducible of degree d. Suppose X is an indeterminate. Then,*

$$X^{|P|-1} - 1 \equiv \prod_{0 \le \deg(f) < d} (X - f) \pmod{P}.$$

Proof. Recall that $\{f \in A \mid \deg(f) < d\}$ is a set of representatives for the cosets of A/PA. If we throw out $f = 0$ we get a set of representatives for $(A/PA)^*$. We find

$$X^{|P|-1} - \bar{1} = \prod_{0 \le \deg(f) < d} (X - \bar{f}),$$

where the bars denote cosets modulo P. This follows from the corollary to Proposition 1.8 since both sides of the equation are monic polynomials in X with the same set of roots in the field A/PA. Since there are $|P| - 1$ roots and the difference of the two sides has degree less than $|P| - 1$, the difference of the two sides must be 0. The congruence in the Proposition is equivalent to this assertion.

Corollary 1. *Let d divide $|P| - 1$. The congruence $X^d \equiv 1 \pmod{P}$ has exactly d solutions. Equivalently, the equation $X^d = \bar{1}$ has exactly d solutions in $(A/PA)^*$.*

Proof. We prove the second assertion. Since $d \mid |P| - 1$ it follows that $X^d - 1$ divides $X^{|P|-1} - 1$. By the proposition, the latter polynomial splits as a product of distinct linear factors. Thus so does the former polynomial. This establishes the result.

Corollary 2. *With the same notation,*

$$\prod_{0 \le \deg(f) < \deg P} f \equiv -1 \pmod{P}.$$

Proof. Just set $X = 0$ in the proposition. If the characteristic of $\mathbb{F}$ is odd $|P| - 1$ is even and the result follows. If the characteristic is 2 then the result also follows since in characteristic 2 we have $-1 = 1$.

The above corollary is the polynomial version of Wilson's theorem. It's interesting to note that the left-hand side of the congruence only depends on the degree of P and not on P itself.

As a final topic in this chapter we give some of the theory of d-th power residues. This will be of importance in Chapter 3 when we discuss quadratic reciprocity and more general reciprocity laws for A.

If $f \in A$ is of positive degree and $a \in A$ is relatively prime to f, we say that a is a d-th power residue modulo f if the equation $x^d \equiv a \pmod{f}$ is solvable in A. Equivalently, $\bar{a}$ is a d-th power in $(A/fA)^*$.

Suppose $f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$ is the prime decomposition of f. Then it is easy to check that a is a d-th power residue modulo f if and only if a is a d-th power residue modulo $P_i^{e_i}$ for all i between 1 and t. This reduces the problem to the case where the modulus is a prime power.

Proposition 1.10. *Let P be irreducible and $a \in A$ not divisible by P. Assume d divides $|P| - 1$. The congruence $X^d \equiv a \pmod{P^e}$ is solvable if and only if*

$$a^{\frac{|P|-1}{d}} \equiv 1 \pmod{P}.$$

There are $\frac{\Phi(P^e)}{d}$ d-th power residues modulo P^e.

Proof. Assume to begin with that $e = 1$.

If $b^d \equiv a \pmod{P}$, then $a^{\frac{|P|-1}{d}} \equiv b^{|P|-1} \equiv 1 \pmod{P}$ by the corollary to Proposition 1.8. This shows the condition is necessary. To show it is sufficient recall that by Corollary 1 to Proposition 1.9 all the d-th roots of unity are in the field A/PA. Consider the homomorphism from $(A/PA)^*$ to itself given by raising to the d-th power. It's kernel has order d and its image is the d-th powers. Thus, there are precisely $\frac{|P|-1}{d}$ d-th powers in $(A/PA)^*$. We have seen that they all satisfy $X^{\frac{|P|-1}{d}} - 1 = 0$. Thus, they are precisely the roots of this equation. This proves all assertions in the case $e = 1$.

To deal with the remaining cases, we employ a little group theory. The natural map (i.e., reduction modulo P) is a homomorphism from $(A/P^eA)^*$ onto $(A/PA)^*$ and the kernel is a p-group as follows from Proposition 1.6. Since the order of $(A/PA)^*$ is $|P| - 1$ which is prime to p it follows that $(A/P^eA)^*$ is the direct product of a p-group and a copy of $(A/PA)^*$. Since $(d, p) = 1$, raising to the d-th power in an abelian p-group is an automorphism. Thus, $a \in A$ is a d-th power modulo P^e if and only if it is a d-th power modulo P. The latter has been shown to hold if and only if $a^{\frac{|P|-1}{d}} \equiv 1 \pmod{P}$. Now consider the homomorphism from $(A/P^eA)^*$ to itself given by raising to the d-th power. It easily follows from what has been said that the kernel has d elements and the image is the subgroup of d-th powers. It follows that the latter group has order $\frac{\Phi(P^e)}{d}$. This concludes the proof.

Exercises

1. If $m \in A = \mathbb{F}[T]$, and $\deg(m) > 0$, show that $q - 1 \mid \Phi(m)$.

2. If $q = p$ is a prime number and $P \in A$ is an irreducible, show $(\mathbb{F}[T]/P^2A)^*$ is cyclic if and only if $\deg P = 1$.

3. Suppose $m \in A$ is monic and that $m = m_1 m_2$ is a factorization into two monics which are relatively prime and of positive degree. Show $(A/mA)^*$ is not cyclic except possibly in the case $q = 2$ and m_1 and m_2 have relatively prime degrees.

4. Assume $q \neq 2$. Determine all m for which $(A/mA)^*$ is cyclic (see the proof of Proposition 1.6).

5. Suppose $d \mid q-1$. Show $x^d \equiv -1 \pmod{P}$ is solvable if and only if $(-1)^{\frac{q-1}{d} \deg P} = 1$.

6. Show $\prod_{\alpha \in \mathbb{F}^*} \alpha = -1$.

7. Let $P \in A$ be a monic irreducible. Show

$$\prod_{\substack{\deg f < d \\ f \text{ monic}}} f \equiv \pm 1 \pmod{P} ,$$

where $d = \deg P$. Determine the sign on the right-hand side of this congruence.

8. For an integer $m \geq 1$ define $[m] = T^{q^m} - T$. Show that $[m]$ is the product of all monic irreducible polynomials $P(T)$ such that $\deg P(T)$ divides m.

9. Working in the polynomial ring $\mathbb{F}[u_0, u_1, \ldots, u_n]$, define $D(u_0, u_1, \ldots, u_n) = \det |u_i^{q^j}|$, where $i, j = 0, 1, \ldots, n$. This is called the Moore determinant. Show

$$D(u_0, u_1, \ldots, u_n) = \prod_{i=0}^{n} \prod_{c_{i-1} \in \mathbb{F}} \cdots \prod_{c_0 \in \mathbb{F}} (u_i + c_{i-1} u_{i-1} + \cdots + c_0 u_0) .$$

Hint: Show each factor on the right divides the determinant and then count degrees.

10. Define $F_j = \prod_{i=0}^{j-1} (T^{q^j} - T^{q^i}) = \prod_{i=0}^{j-1} [j-i]^{q^i}$. Show that

$$D(1, T, T^2, \ldots, T^n) = \prod_{j=0}^{n} F_j .$$

Hint: Use the fact that $D(1, T, T^2, \ldots, T^n)$ can be viewed as a Vandermonde determinant.

11. Show that F_j is the product of all monic polynomials in A of degee j.

12. Define $L_j = \prod_{i=1}^{j} (T^{q^i} - T) = \prod_{i=1}^{j} [i]$. Use Exercise 8 to prove that L_j is the least common multiple of all monics of degree j.