Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Ricky Aditya
Assignment title:	Periksa similarity
Submission title:	The Number of Irreducible Polynomials over a Finite Field - ...
File name:	ducible_Polynomials_over_a_Finite_Field_-_An_Algebraic_Proo...
File size:	77.75K
Page count:	6
Word count:	2,423
Character count:	10,056
Submission date:	01-Jul-2022 10:28AM (UTC+0700)
Submission ID:	1865274466

International Journal of Applied Mathematics and Statistics,
Int. J. Appl. Math. Stat.; Vol. 53; Issue No. 4; Year 2015,
ISSN 0973-1377 (Print), ISSN 0973-7545 (Online)

The Number of Irreducible Polynomials over a Finite Field : An Algebraic Proof

Ricky Aditya[1]

[1]Department of Mathematics
Bina Nusantara University
KH Syahdan Street 9, Palmerah, West Jakarta, Indonesia 11480
riaditya@binus.edu

ABSTRACT

The concepts of finite field are used in coding theory, in which the finite field is the set of alphabets. To construct a finite field of order p^n, where p is a prime integer and n is a natural number, an irreducible polynomial of degree n over $\mathbb{Z}_p$ is needed. In this article, the number of irreducible polynomial of degree n over $\mathbb{Z}_p$ is given and also proved using abstract algebra approach. Because the number is always positive, for any prime integer p and natural number n, an irreducible polynomial of degree n over $\mathbb{Z}_p$ always exists. Moreover, it implies that a finite field of order p^n always exists.

Keywords: Finite Fields, Irreducible Polynomials, Existence of Finite Fields.

2000 Mathematics Subject Classification: 12E05, 12E20.

1 Introduction

In the study of coding theory, some concepts from abstract algebra, such as finite fields and vector spaces over finite fields, are used. The finite field, which its basic concepts are given in (Adkins and Weintraub, 1992), is used as the set of alphabets and the vector space is used as the set of codewords. Cardinality of a finite field must be p^n, where p is a prime integer and n is a natural number. As in (Bose and Manvel, 1984) and (Ling and Xing, 2004), to construct a finite field with p^n elements, an irreducible polynomial of degree n over $\mathbb{Z}_p$ is needed.
In some books about coding theory, it is just stated that for any prime integer p and any natural number n, a finite field with p^n elements always exists. However, most of them do not give the proof of the existence. To prove that existence theorem, it is sufficient to show that for any prime integer p and any natural number n, an irreducible polynomial of degree n over $\mathbb{Z}_p$ always exists. In this article, the proof of that theorem will be shown using abstract algebra approach. The idea of the proof is based on (Ling and Xing, 2004). In the next section, more details about this will be discussed.

The Number of Irreducible Polynomials over a Finite Field - An Algebraic Proof

by Aditya Ricky

Submission date: 01-Jul-2022 10:28AM (UTC+0700)
Submission ID: 1865274466
File name: ducible_Polynomials_over_a_Finite_Field_-_An_Algebraic_Proof.pdf (77.75K)
Word count: 2423
Character count: 10056

International Journal of Applied Mathematics and Statistics,
Int. J. Appl. Math. Stat.; Vol. 53; Issue No. 4; Year 2015,
ISSN 0973-1377 (Print), ISSN 0973-7545 (Online)

The Number of Irreducible Polynomials over a Finite Field : An Algebraic Proof

Ricky Aditya[1]

[1]Department of Mathematics
Bina Nusantara University
KH Syahdan Street 9, Palmerah, West Jakarta, Indonesia 11480
riaditya@binus.edu

ABSTRACT

The concepts of finite field are used in coding theory, in which the finite field is the set of alphabets. To construct a finite field of order p^n, where p is a prime integer and n is a natural number, an irreducible polynomial of degree n over $\mathbb{Z}_p$ is needed. In this article, the number of irreducible polynomial of degree n over $\mathbb{Z}_p$ is given and also proved using abstract algebra approach. Because the number is always positive, for any prime integer p and natural number n, an irreducible polynomial of degree n over $\mathbb{Z}_p$ always exists. Moreover, it implies that a finite field of order p^n always exists.

Keywords: Finite Fields, Irreducible Polynomials, Existence of Finite Fields.

2000 Mathematics Subject Classification: 12E05, 12E20.

1 Introduction

In the study of coding theory, some concepts from abstract algebra, such as finite fields and vector spaces over finite fields, are used. The finite field, which its basic concepts are given in (Adkins and Weintraub, 1992), is used as the set of alphabets and the vector space is used as the set of codewords. Cardinality of a finite field must be p^n, where p is a prime integer and n is a natural number. As in (Bose and Manvel, 1984) and (Ling and Xing, 2004), to construct a finite field with p^n elements, an irreducible polynomial of degree n over $\mathbb{Z}_p$ is needed.

In some books about coding theory, it is just stated that for any prime integer p and any natural number n, a finite field with p^n elements always exists. However, most of them do not give the proof of the existence. To prove that existence theorem, it is sufficient to show that for any prime integer p and any natural number n, an irreducible polynomial of degree n over $\mathbb{Z}_p$ always exists. In this article, the proof of that theorem will be shown using abstract algebra approach. The idea of the proof is based on (Ling and Xing, 2004). In the next section, more details about this will be discussed.

2 Number of Irreducible Polynomials over a Finite Field and Its Proof

In abstract algebra, the field is defined as a nonempty set which is a commutative group with respect to both of two operations: addition and multiplication, and distributive law holds for those operations. The formal definition can be found in (Adkins and Weintraub, 1992). A finite field is a field with finite number of elements. Moreover, a finite field with q elements is denoted as F_q.

Polynomial over a field can also be defined. Some terminologies about polynomial over a field are similar with polynomial over real numbers. In (Adkins and Weintraub, 1992), a polynomial over a field is said to be reducible if it can be factorized as a product of two polynomials of lower degree. Otherwise, it is said to be irreducible.

In (Bose and Manvel, 1984) and (Ling and Xing, 2004), to construct a finite field with p^n elements, where p is prime integer and n is natural number, an irreducible polynomials of degree n over $\mathbb{Z}_p$ is needed. In order to prove that for any prime integer p and any natural number n, a finite field with p^n elements exists, it must be proved that the number of irreducible polynomial of degree n over $\mathbb{Z}_p$ is always positive.

Therefore, the main theorem of this article is about how many irreducible polynomials of degree n over $\mathbb{Z}_p$ exists. This is our main theorem:

Theorem 2.1 (Number of Irreducible Polynomials over $\mathbb{Z}_p$)**.** *The number of irreducible polynomials of degree n over $\mathbb{Z}_p$, denoted by $I_p(n)$, is:*

$$I_p(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d) \cdot p^{n/d} \tag{2.1}$$

where μ is the Mobius function.

Definition of Mobius function is also given in (Ling and Xing, 2004). The proof of Theorem 2.1 is not given now because in order to prove it, it is necessary to prove some lemmas first. These are the five lemmas (Lemma 2.2-2.6) that need to be proved, which some of them are based on (Ling and Xing, 2004). Now the proofs of all those lemmas and the relation between them will be given:

Lemma 2.2. *Any element of F_{p^n} is a root of an irreducible polynomial of degree d over $\mathbb{Z}_p$, where $d|n$.*

Proof. For any $\alpha \in F_{p^n}$, it can be found a polynomial $f(x) \in \mathbb{Z}_p[x]$ of smallest degree such that $f(\alpha) = 0$. The polynomial $f(x)$ is irreducible, because if it is reducible, then there will be a polynomial of smaller degree such that α is its root, which contradicts with the smallest degree condition. The set $\mathbb{Z}_p(\alpha)$ is defined as an extension field of $\mathbb{Z}_p$ that contains α. Let $\deg(f(x)) = d$, it needs to be proven that $d|n$. From the smallest degree condition, for any $g(x) \in \mathbb{Z}_p[x]$ with $\deg g(x) < d$, it is obtained that $g(\alpha) \neq 0$. Partitioning $\mathbb{Z}_p(\alpha)$ into its congruence classes, $\mathbb{Z}_p(\alpha)$ will be a finite field with p^d elements and contains both $\mathbb{Z}_p$ and α. In other side, all elements of $\mathbb{Z}_p(\alpha)$ are contained in F_{p^n} since $\alpha \in F_{p^n}$ and $\mathbb{Z}_p$ is a subfield of F_{p^n}. Therefore $\mathbb{Z}_p(\alpha)$ is a subfield of F_{p^n} and there is an inclusion $F_{p^n} \supseteq \mathbb{Z}_p(\alpha) \supseteq \mathbb{Z}_p$. If $\mathbb{Z}_p(\alpha)$ is a subfield of F_{p^n}, then the cardinality of $\mathbb{Z}_p(\alpha)$ must divides the cardinality of F_{p^n}. The last statement means $p^d|p^n$, which implies $d|n$. □

Lemma 2.3. *Any irreducible polynomial of degree d over $\mathbb{Z}_p$ which $d|n$ divides $x^{p^n}-x$.*

Proof. From Theorem 2.1, if $p(x)$ is an irreducible polynomial of degree d over $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/\langle p(x)\rangle$ is a finite field with p^d elements. Let $x \in \mathbb{Z}_p[x]/\langle p(x)\rangle$, then $x = x + \langle p(x)\rangle$. Therefore we have $x^2 = x^2 + \langle p(x)\rangle$, $x^3 = x^3 + \langle p(x)\rangle$, ..., $x^d = x^d + \langle p(x)\rangle$. Moreover, if we write $p(x) = p_0 + p_1x + p_2x^2 + \ldots + p_dx^d$, then we get:

$$p(x) = p(x+\langle p(x)\rangle) = (p_0+p_1x+p_2x^2+\ldots+p_dx^d)+\langle p(x)\rangle = p(x)+\langle p(x)\rangle = 0+\langle p(x)\rangle. \quad (2.2)$$

So, $x \in \mathbb{Z}_p[x]/\langle p(x)\rangle$ is a root of $p(x)$ in $\mathbb{Z}_p[x]/\langle p(x)\rangle$. In other hand, x is a root of $x^{p^d}-x$ over F_{p^d}. In other words, $x^{p^d}-x$ and $p(x)$ have common factor in $F_{p^d}[x]$.
Next we will show that $x^{p^d}-x$ and $p(x)$ have common factor in $\mathbb{Z}_p[x]$. Suppose that $x^{p^d}-x$ and $p(x)$ have no common factor in $\mathbb{Z}_p[x]$, we have $\gcd(x^{p^d}-x, p(x)) = 1$ in $\mathbb{Z}_p[x]$. Therefore, there are $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $g(x)\cdot(x^{p^d}-x)+h(x)\cdot p(x) = 1$. Because $\mathbb{Z}_p[x] \subseteq F_{p^d}[x]$, so $g(x), h(x) \in F_{p^d}[x]$. That means $\gcd(x^{p^d}-x, p(x)) = 1$ in $F_{p^d}[x]$, which is equivalent with $x^{p^d}-x$ and $p(x)$ have no common factor in F_{p^d}. It is contradiction with our previous result, so it is true that $x^{p^d}-x$ and $p(x)$ have common factor in $\mathbb{Z}_p[x]$. Because $p(x)$ is irreducible over $\mathbb{Z}_p$ and its degree is smaller than p^d, we get that $p(x)|x^{p^d}-x$. This means that all roots of $p(x)$ are also roots of $x^{p^d}-x$ in $F_{p^d}[x]$, which is equivalent with all roots of $p(x)$ are contained in F_{p^d}. Because F_{p^d} is a subfield of F_{p^n}, we conclude that all roots of $p(x)$ are contained in F_{p^n}. □

Lemma 2.4. *Two different irreducible polynomials $p(x), q(x) \in \mathbb{Z}_p[x]$ which $\deg(p(x))|n$ and $\deg(q(x))|n$ have no common factor in $F_{p^n}[x]$.*

Proof. Because both $p(x)$ and $q(x)$ are irreducible over $\mathbb{Z}_p$, they have no common factor in $\mathbb{Z}_p[x]$. So we can find $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $g(x)\cdot p(x) + h(x)\cdot q(x) = 1$. Because $g(x), h(x) \in F_{p^n}[x]$, this means $\gcd(p(x), q(x)) = 1$ in $F_{p^n}[x]$, i.e. $p(x)$ and $q(x)$ have no common factor in $F_{p^n}[x]$. □

Lemma 2.5. *(Ling and Xing, 2004). If $I_p(d)$ denotes the number of irreducible polynomials of degree d over $\mathbb{Z}_p$, then $\sum_{d|n} d\cdot I_p(d) = p^n$.*

Proof. We consider the elements of F_{p^n} as the roots of polynomial x^{p^n}. From Lemma 2.2, for any root α of $x^{p^n}-x$, there is an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\deg(f(x))|n$. In other side, from Lemma 2.3, any irreducible polynomial of degree d over $\mathbb{Z}_p$ which $d|n$ always divides $x^{p^n}-x$. Since, from Lemma 2.4, any two different irreducible polynomials over $\mathbb{Z}_p$ have no common factor in F_{p^n}, we can represent $x^{p^n}-x$ as a product of all irreducible polynomial of degree d over $\mathbb{Z}_p$ which $d|n$. Moreover we can write:

$$x^{p^n}-x = \prod_{\substack{p(x)\text{ irreducible}\\ \deg(p(x))|n}} p(x). \quad (2.3)$$

Equalling the number of factors of left and right hand side, we will get an equality:

$$p^n = \sum_{d|n} d \cdot I_p(d), \tag{2.4}$$

where $I_p(d)$ denotes the number of irreducible polynomials of degree d over $\mathbb{Z}_p$. □

Lemma 2.6. *(Ling and Xing, 2004). For any function H and h from $\mathbb{N}$ to $\mathbb{Z}$, we have:*

$$H(n) = \sum_{d|n} h(d) \Rightarrow h(n) = \sum_{d|n} \mu(d) \cdot H(\frac{n}{d}). \tag{2.5}$$

Proof. Write $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, where $p_1, p_2, \ldots, p_m$ are m distinct prime integers. Consider the form $\sum_{d|n} h(d)$. Partial sum of $\sum_{d|n} h(d)$ which does not contain $h(n)$ are $H(\frac{n}{d})$, where d is a factor of n and $d \neq 1$. All partial sums $H(\frac{n}{p_i^j})$, where $1 \leq j \leq k_i$, are contained in the partial sum $H(\frac{n}{p_i})$, for each $i = 1, 2, \ldots, m$. Therefore we can just consider all maximal partial sums which do not contain $h(n)$, those are $H(\frac{n}{p_1})$, $H(\frac{n}{p_2})$, ..., $H(\frac{n}{p_m})$. But any two of those partial sums $H(\frac{n}{p_i})$ and $H(\frac{n}{p_j})$ are intersected in $H(\frac{n}{p_i \cdot p_j})$, any three of those partial sums $H(\frac{n}{p_i})$, $H(\frac{n}{p_j})$ and $H(\frac{n}{p_k})$ are intersected in $H(\frac{n}{p_i \cdot p_j \cdot p_k})$, and so on. Using the inclusion-exclusion principle, we get the formula:

$$\begin{aligned} H(n) - h(n) = & \sum_{\substack{p|n \\ p \text{ prime}}} H(\tfrac{n}{p}) - \sum_{\substack{p_1|n, p_2|n, p_1 \neq p_2 \\ p_1, p_2 \text{ prime}}} H(\tfrac{n}{p_1 \cdot p_2}) \\ & + \sum_{\substack{p_1|n, p_2|n, p_3|n \\ p_1, p_2, p_3 \text{ distinct primes}}} H(\tfrac{n}{p_1 \cdot p_2 \cdot p_3}) - \ldots \\ & + (-1)^{m+1} \sum_{\substack{p_1|n, p_2|n, \ldots, p_m|n \\ p_1, p_2, \ldots, p_m \text{ distinct primes}}} H(\tfrac{n}{p_1 \cdot p_2 \cdot \ldots \cdot p_m}) \end{aligned}, \tag{2.6}$$

or equivalently:

$$\begin{aligned} h(n) = H(n) - & \sum_{\substack{p|n \\ p \text{ prime}}} H(\tfrac{n}{p}) + \sum_{\substack{p_1|n, p_2|n, p_1 \neq p_2 \\ p_1, p_2 \text{ prime}}} H(\tfrac{n}{p_1 \cdot p_2}) \\ & - \sum_{\substack{p_1|n, p_2|n, p_3|n \\ p_1, p_2, p_3 \text{ distinct primes}}} H(\tfrac{n}{p_1 \cdot p_2 \cdot p_3}) + \ldots \\ & + (-1)^{m+1} \sum_{\substack{p_1|n, p_2|n, \ldots, p_m|n \\ p_1, p_2, \ldots, p_m \text{ distinct primes}}} H(\tfrac{n}{p_1 \cdot p_2 \cdot \ldots \cdot p_m}) \end{aligned}, \tag{2.7}$$

Remember that $\mu(p_1 \cdot p_2 \cdot \ldots \cdot p_k) = (-1)^k$, where p_1, p_2, ..., p_k are distinct primes and $\mu(p^2 \cdot q) = 0$, where p is a prime integer. In other hand, contribution of $H(\frac{n}{p^2 \cdot q})$, where p is a prime integer and $p^2 \cdot q | n$, are ignored. Therefore, we can formulate above equation in the

form of Mobius function as below:

$$h(n) = \mu(1) \cdot H(\tfrac{n}{1}) + \sum_{p \mid n,\ p \text{ prime}} \mu(p) \cdot H(\tfrac{n}{p}) + \sum_{p_1 \mid n, p_2 \mid n,\ p_1 \neq p_2,\ p_1, p_2 \text{ prime}} \mu(p_1 \cdot p_2) \cdot H(\tfrac{n}{p_1 \cdot p_2}) + \sum_{p_1 \mid n, p_2 \mid n, p_3 \mid n,\ p_2, p_3 \text{ distinct primes}} \mu(p_1 \cdot p_2 \cdot p_3) \cdot H(\tfrac{n}{p_1 \cdot p_2 \cdot p_3}) + \ldots + \sum_{p_1 \mid n, p_2 \mid n, \ldots, p_m \mid n,\ p_1, p_2, \ldots, p_m \text{ distinct primes}} \mu(p_1 \cdot p_2 \cdot \ldots \cdot p_m) \cdot H(\tfrac{n}{p_1 \cdot p_2 \cdot \ldots \cdot p_m}), \quad (2.8)$$

and the proof is completed. □

Proof of Theorem 2.1 It is wanted to be shown that $I_p(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d) \cdot p^{n/d}$. First, from Lemma 2.5, we have $p^n = \sum_{d|n} d \cdot I_p(d)$. Let $H(n) = p^n$ and $h(n) = n \cdot I_p(n)$, that equation becomes $H(n) = \sum_{d|n} h(d)$. From Lemma 2.6, it will imply:

$$h(n) = \sum_{d|n} \mu(d) \cdot H(\tfrac{n}{d}) \Leftrightarrow n \cdot I_p(n) = \sum_{d|n} \mu(d) \cdot p^{n/d} \Leftrightarrow I_p(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d) \cdot p^{n/d}, \quad (2.9)$$

and it completes the proof.

□

One can show that for any natural number n, $I_p(n)$ is always a natural number. This means, for any natural number n, at least one irreducible polynomial of degree n over $\mathbb{Z}_p$ can be found. Therefore, a finite field with p^n elements always exists.

3 Conclusion

It has been proved that the number of irreducible polynomials of degree n over finite field $\mathbb{Z}_p$ is equal to $\frac{1}{n} \cdot \sum_{d|n} \mu(d) \cdot p^{n/d}$, where μ is the Mobius function. Because that number is always a natural number, so it guarantees the existence of irreducible polynomial $p(x)$ of degree n over $\mathbb{Z}_p$. Thus, $\mathbb{Z}_p[x]/\langle p(x) \rangle$ becomes a finite field with p^n elements. This implies that a finite field with p^n elements always exists, for any prime integer p and any natural number n. This fact is usually just used in some book about finite fields and its applications, such as (Ling and Xing, 2004), but seldom to be proven.

Acknowledgment

Author wishes to acknowledge his college friend, Albert Gunawan, who had helped author by giving some ideas to prove some lemmas in this article's main part.

References

Adkins, W. and Weintraub, S. 1992. *Algebra: An Approach via Module Theory*, Springer-Verlag, New York.

Bose, R. and Manvel, B. 1984. *Introduction to Combinatorial Theory*, John Wiley and Sons, New York.

Ling, S. and Xing, C. 2004. *Coding Theory : A First Course*, University Press, Cambridge.

The Number of Irreducible Polynomials over a Finite Field - An Algebraic Proof

ORIGINALITY REPORT

22%	7%	18%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Joseph N. Mamvong, Gokop L. Goteng, Bo Zhou, Yue Gao. "Efficient Security Algorithm for Power-Constrained IoT Devices", IEEE Internet of Things Journal, 2021 Publication	2%
2	C. Zinn. "A Computational Framework For Understanding Mathematical Discoursexy", Logic Journal of IGPL, 07/01/2003 Publication	2%
3	Submitted to Southern New Hampshire University - Continuing Education Student Paper	2%
4	International Journal of Intelligent Unmanned Systems, Volume 4, Issue 2 (2016) Publication	1%
5	Submitted to University of Nottingham Student Paper	1%
6	"Algebra of Polynomials, Rational Functions, and Power Series", Algorithms for Computer Algebra, 1992 Publication	1%
7	Submitted to Mahidol University Student Paper	1%
8	Submitted to The University of Manchester Student Paper	1%
9	Ivan Oseledets. "Improved n-Term Karatsuba-Like Formulas in GF(2)", IEEE Transactions on	1%

Computers, 2011
Publication

10	Submitted to Lebanese American University Student Paper	1 %
11	"p-adic Fields", Graduate Texts in Mathematics, 2007 Publication	1 %
12	Gilbert. "Rings and Fields", Pure and Applied Mathematics, 10/24/2003 Publication	1 %
13	tutorsonspot.com Internet Source	1 %
14	Louis J. Ratliff, David E. Rush, Kishor Shah. "Note on Cyclotomic Polynomials and Prime Ideals", Communications in Algebra, 2004 Publication	1 %
15	hdl.handle.net Internet Source	1 %
16	Submitted to Ohio University Student Paper	1 %
17	Submitted to University of Bahrain Student Paper	1 %
18	Submitted to University of Birmingham Student Paper	1 %
19	Hideaki Aoyama, Masatoshi Sato, Toshiaki Tanaka. "General forms of a -fold supersymmetric family", Physics Letters B, 2001 Publication	1 %
20	Submitted to University of Durham Student Paper	1 %
21	Manuel Kauers, Peter Paule. "Chapter 6 Algebraic Functions", Springer Science and	<1 %

Business Media LLC, 2011
Publication

22	Wayne Patterson. "Computational Number Theory", Wiley Encyclopedia of Computer Science and Engineering, 12/14/2007 Publication	<1 %
23	silo.pub Internet Source	<1 %
24	Submitted to California State University, San Bernadino Student Paper	<1 %
25	R.A. Haraty, H. Otrok, A.N. El-Kassar. "Attacking ElGamal based cryptographic algorithms using pollard's rho algorithm", The 3rd ACS/IEEE International Conference onComputer Systems and Applications, 2005., 2005 Publication	<1 %
26	arxiv.org Internet Source	<1 %
27	"Public Key Cryptography — PKC 2003", Springer Science and Business Media LLC, 2002 Publication	<1 %
28	Peter Borwein, Kwok-Kwong Stephen Choi. "On Cyclotomic Polynomials with ± 1 Coefficients", Experimental Mathematics, 1999 Publication	<1 %
29	ueaeprints.uea.ac.uk Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		