COMMUNICATION SCIENCES INSTITUTE

"Irreducible Polynomials which Divide Trinomials over GF(2)"

by

Pey-Feng Lee

CSI-05-05-03

USC VITERBI SCHOOL OF ENGINEERING
UNIVERSITY OF SOUTHERN CALIFORNIA
ELECTRICAL ENGINEERING — SYSTEMS
LOS ANGELES, CA 90089-2565

IRREDUCIBLE POLYNOMIALS WHICH DIVIDE TRINOMIALS OVER GF(2)

by

Pey-Feng Lee

A Dissertation Presented to the
FACULTY OF THE GRADUATE SCHOOL
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PHILOSOPHY
(ELECTRICAL ENGINEERING)

May 2005

Dedication

Dedicated with love to my mother, my wife, and my daughters.

Acknowledgements

I would like to express my enormous gratitude and appreciation to Professor Solomon W. Golomb, the chairman of my dissertation committee, for his consistent encouragement, concern, and guidance throughout my graduate studies at USC. I have benefited greatly from his extensive knowledge, remarkable experience, and ample resources.

My deep appreciation is also given to Professor William C. Lindsey and Professor Robert Guralnick for taking their precious time and efforts to serve on both my guidance and dissertation committees, and for their constructive comments and suggestions. Also, I would like to thank Professor Charles L. Weber and Professor Alan E. Willner for serving on my guidance committee.

A special acknowledgment is due to Professor Lloyd R. Welch for providing the clever testing criterion and a sample program. I also wish to thank Professor John Brillhart, University of Arizona, and Professor Ram Murty, Queen's University, for patiently replying to my e-mails. Also, I would like to thank all the faculty and students at EE/Systems and Mathematics for offering many invaluable classes and discussions, and I am grateful

to Milly Montenegro, Mayumi Thrasher, and Gerrielyn Ramos for their capable administrative help.

Last but not least, I wish to acknowledge my wife Yuhsuan, who was awaiting our second baby during the time of my preparation of this thesis, for her continuing support, patience, and understanding.

Table of Contents

Dedication **ii**

Acknowledgements **iii**

List of Tables **vi**

List of Figures **vii**

Abstract **viii**

1 Introduction **1**
1.1 Motivations 1
1.2 Outline of the thesis 5

2 Theorems and Results **7**
2.1 Basic Theorems and Results 7
2.2 Further Theorems and Results 16

3 The Multiplicative Module **30**
3.1 Introduction 30
3.2 Prime Generators of the Multiplicative Module M 31
3.3 Composite Generators of the Multiplicative Module M 34

4 Some Related Problems **39**
4.1 Generalized Artin's Conjecture 39
4.2 Generalized TZZ and BGL Conjectures 50

5 Conclusion **55**

Bibliography **57**

List of Tables

2.1 Frequency distribution of the index r of the first $1,000,000$ odd primes ($1 \leq r \leq 100$) 28

3.1 Prime generators of the multiplicative module M (non-Mersenne primes) 34

3.2 Composite generators of the multiplicative module M ($g \mid \Phi_n(2)$) 37

3.3 Composite generators of the multiplicative module M ($g \mid \Phi_n(2)\Phi_{2n}(2)$) . 37

3.4 Factors of $\Phi_n(2)$ versus members of the multiplicative module M ($2 \leq n \leq 61$) 38

4.1 Numerical results of $F_2(r)$ for the first $1,000,000$ odd primes ($1 \leq r \leq 100$) 44

4.2 Numerical results of $F_3(r)$, $F_5(r)$, $F_7(r)$ of the first $1,000,000$ odd primes ($1 \leq r \leq 100$) 46

4.3 Collections of possible indices r of the first $100,000$ odd primes ($2 \leq a \leq 100$) 48

List of Figures

1.1 The n-stage binary linear feedback shift register 2

Abstract

Shift-register sequences, also known as pseudorandom sequences, or pseudonoise sequences, have played increasingly important roles in many important applications. The simplest linear feedback shift registers to generate binary sequences involve only two taps, which corresponds to a trinomial over GF(2). It is therefore of interest to know which irreducible polynomials $f(x)$ divide trinomials over GF(2), since the output sequences corresponding to $f(x)$ can be obtained from a two-tap linear feedback shift register (with a suitable initial state) if and only if $f(x)$ divides some trinomial $t(x) = x^m + x^a + 1$ over GF(2).

In this thesis we develop the theory of irreducible polynomials which do, or do not, divide trinomials over GF(2). Abundant theorems and results are presented relating to the primitivity t and the index r, which is the number of irreducible factors of the t^{th} cyclotomic polynomial $\Phi_t(x)$ over GF(2). The set of all positive (odd) integers t such that the irreducible polynomials of odd primitivity $t > 1$ divide trinomials over GF(2) form a multiplicative module M, which is closed with respect to multiplication by odd

numbers. The set G of generators of M is quite sparse, and its members seem related to numbers of the form $\Phi_n(2)$.

The distribution of the values of r among the set of all odd primes p leads to a generalization of Artin's Conjecture concerning primitive roots modulo p. We generalized the conjectures of Blake, Gao and Lambert, and of Tromp, Zhang and Zhao, and proved the generalization of the Blake, Gao and Lambert conjecture.

Chapter 1

Introduction

1.1 Motivations

Linear feedback shift register sequences have been used in a variety of important applications, such as CDMA (Code Division Multiple Access) communications, spread spectrum communications, CW radar, bit error rate measurements, error correcting codes, and stream ciphers. There are two main advantages for using linear feedback shift register sequences: they are extremely fast and easy to implement both in hardware and software, and they can be readily analyzed using algebraic techniques. A thorough introduction to the theory of shift register sequences is in the book by Golomb [5].

A typical n-stage binary linear feedback shift register (known as a Fibonacci configuration) is illustrated in Figure 1.1. Both the feedback coefficients

$$c_1, c_2, \ldots, c_n$$

and the initial state

$$a_{-1}, a_{-2}, \ldots, a_{-n}$$

of the shift register are elements of GF(2). During each unit of time, the contents of each stage i shifts to next stage $i-1$ synchronously for $1 \leq i \leq n-1$, and the new content of stage $n-1$ is computed as the sum

$$\sum_{i=1}^{n} c_i a_{j-i} \text{ (modulo 2)},$$

where the c_i's indicate whether the contents of stage $n-i$ is to be be included in the sum or not, and

$$\{a_j\} = \{a_0, a_1, a_2, a_3, \ldots\}$$

is the output sequence generated by this device.

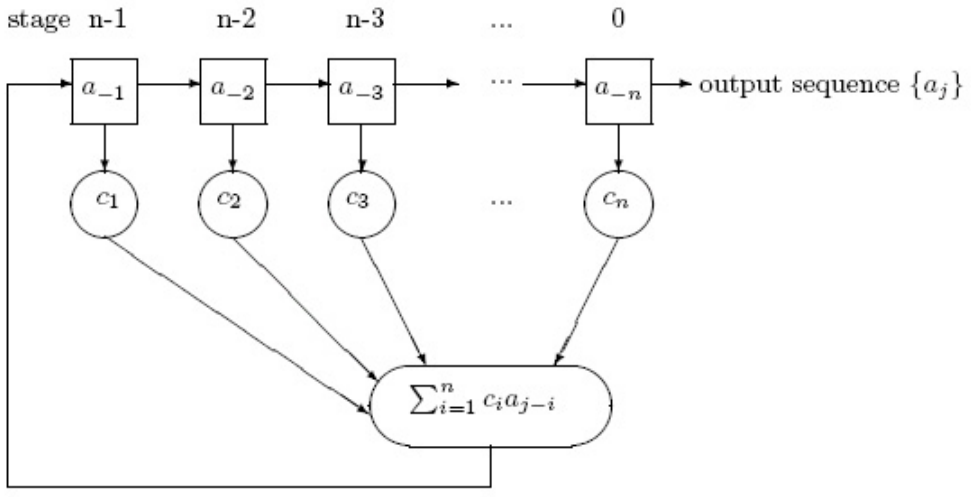

Figure 1.1: The n-stage binary linear feedback shift register

The polynomial

$$f(x) = 1 + \sum_{i=1}^{n} c_i x^i \tag{1.1}$$

associated with the shift register in Figure 1.1 is call the characteristic polynomial of the shift register. In fact, the characteristic polynomial $f(x)$ is even independent of the initial condition. If α is a root of an irreducible polynomial $f(x)$ of degree n over GF(2), then the primitivity t of α (and also of $f(x)$) is defined as the smallest positive integer t such that

$$\alpha^t = 1 \quad (\text{or } f(x) \mid (x^t - 1).)$$

As shown in [5], the output sequence of a binary linear feedback shift register is periodic, and if $f(x)$ is irreducible, the primitivity t of $f(x)$ will always be a divisor of $2^n - 1$. When $t = 2^n - 1$, $f(x)$ is called a primitive polynomial over GF(2), which corresponds to a maximum-length sequence (or m-sequence for short).

It is a fact that every primitive polynomial is also irreducible over GF(2), but the converse is not true. The number of primitive polynomials of degree n over GF(2) is given by

$$\lambda_2(n) = \frac{\phi(2^n - 1)}{n} \geq 1 \tag{1.2}$$

for each $n \geq 1$; and the number of irreducible polynomials of degree n over GF(2) is given by

$$\psi_2(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d} \geq 1 \tag{1.3}$$

for each $n \geq 1$. (Here $\phi(n)$ is the Euler phi-function, and $\mu(n)$ is the Möbius mu-function.)

Generally, different initial states of the shift register may give rise to different output sequences. If the corresponding polynomial $f(x)$ is irreducible, the period of the shift register sequence does not depend on the initial state, except for the initial condition all 0's. Specifically, if $f(x)$ is a primitive polynomial, all the non-zero initial states of the shift register will generate the very same m-sequence except for phase shifts.

For certain values of n, there are primitive trinomials $x^n + x^a + 1$ of degree n. These correspond to shift registers in which only two taps are involved in the feedback modulo 2 adder. This is the simplest way to generate an m-sequence, which is why primitive (and irreducible) trinomials have been of special interest among the set of all primitive (and irreducible) polynomials. Tables of primitive (and irreducible) trinomials can be found in [5] [10] [13] [14]. It is easy to show that there are irreducible (though not primitive) trinomials over GF(2) for infinitely many different degrees n. It is also conjectured (and highly likely) but still unproved that there are primitive trinomials for infinitely many degrees n. However, by a theorem of R. Swan [11], there are infinitely many degrees n (including all multiples of 8) for which there are no irreducible trinomials, and a fortiori no primitive trinomials, over GF(2).

When a primitive trinomial of degree n does not exist, an almost primitive trinomial may be used as an alternative. (A polynomial $p(x)$ of degree n is *almost primitive* if $p(x) \neq 0$ and $p(x)$ has a primitive factor of degree $> n/2$.) Algorithms for finding almost primitive trinomials can be found in [3]. Moreover, as shown in [9], the moments of the

partial-period correlation of an m-sequence are related to the number of trinomials of bounded degree (determined by the particular partial period under consideration) that the characteristic polynomial of the m-sequence divides.

It is therefore of interest to know which irreducible polynomials $f(x)$ divide trinomials over GF(2), since the output sequence corresponding to $f(x)$ can be obtained from a two-tap linear feedback shift register (with a suitable initial state) if and only if $f(x)$ divides some trinomial $t(x) = x^m + x^a + 1$ over GF(2).

1.2 Outline of the thesis

In this thesis we develop the theory of which irreducible polynomials do, or do not, divide trinomials over GF(2).

In Chapter 2, useful theorems and results are presented relating to the primitivity t and the index r. An irreducible polynomial $f(x)$ either divides infinitely many trinomials, or divides no trinomials. If $f(x)$ divides trinomials, $f(x)$ must divide some trinomial of degree less than its primitivity t. We prove that every primitive polynomial divides trinomials, and also present a whole family of irreducible polynomials $x^{t-1} + x^{t-2} + \ldots + x + 1$ which never divide trinomials. Once $f(x)$ divides any trinomial, then all the polynomials having the same primitivity t divide trinomials. Then a clever criterion is introduced to determine whether a given irreducible polynomial $f(x)$ divides trinomials, for every odd primitivity $t > 1$. Further theorems and results are presented in terms of the index r, which is the number of irreducible factors of the t^{th} cyclotomic polynomial

$\Phi_t(x)$ over GF(2). We show how the index r contributes to determining whether a given irreducible polynomial $f(x)$ of primitivity t divides trinomials when t is a prime number.

In Chapter 3, the multiplicative module M is introduced, which is the set of positive (odd) integers t such that the irreducible polynomials of odd primitivity $t > 1$ divide trinomials over GF(2). The set G of generators of M consists of certain prime and composite values. Then computational results are presented. These results show that the set G is quite sparse, and its members seem related to numbers of the form $\Phi_n(2)$.

In Chapter 4, Artin's Conjecture [1] concerning primitive roots is discussed. The distribution of the values of r for members of the set of all odd primes p leads to a generalization of Artin's Conjecture concerning primitive roots modulo p. Then we generalize the conjecture of Blake, Gao and Lambert (BGL) [2], and of Tromp, Zhang and Zhao (TZZ) [12]. We prove the former generalization, and ascertain that the latter generalization is true if the original TZZ conjecture is true.

Finally, this thesis is summarized, and possible future research work is presented, in the last chapter.

Chapter 2

Theorems and Results

In this chapter, we primarily focus on the question of which irreducible polynomials divide (any) trinomials, and which ones never divide trinomials, over GF(2). The main theorems and results are presented, relating to the primitivity t and the index r.

2.1 Basic Theorems and Results

In what follows, we assume that $f(x)$ is an irreducible polynomial of degree $n > 1$ over GF(2) having a root α and primitivity t, which means that $\alpha^t = 1$ (i.e. that $f(x)$ divides $x^t - 1$), where t is the smallest positive integer with this property. The following facts, many of which depend on the primitivity t of $f(x)$, have been established.

Lemma 1. $f(x)$ divides $h(x)$ if and only if every root α of $f(x)$ is also a root of $h(x)$.

Proof. Suppose $h(x) = f(x)q(x)$. Then

$$h(\alpha) = f(\alpha)q(\alpha) = 0 \cdot q(\alpha) = 0.$$

Conversely, if $h(\alpha) = 0$, we can divide $h(x)$ by $f(x)$ to get

$$h(x) = f(x)q(x) + r(x), \text{ where } \deg(r(x)) < deg(f(x)).$$

Then

$$0 = h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = 0 \cdot q(\alpha)) + r(\alpha) = r(\alpha),$$

from which $r(x)$ also has α as a root. This contradicts the choice of the irreducible polynomial $f(x)$ as the lowest degree polynomial (the minimal polynomial) having α as a root. Hence $r(x) = 0$ and $f(x)$ divides $h(x)$.

□

Theorem 1. $f(x)$ divides some trinomial if and only if there exist distinct positive integers i and j with $\alpha^i + \alpha^j = 1$.

Proof. By the previous Lemma, the trinomial $h(x) = x^i + x^j + 1$ is divisible by $f(x)$ if and only if

$$h(\alpha) = \alpha^i + \alpha^j + 1 = 0, \ i.e. \ \alpha^i + \alpha^j = 1.$$

□

Theorem 2. If $f(x)$ divides any trinomial, then $f(x)$ divides infinitely many trinomials.

Proof. If $f(x)$ divides a trinomial $x^m + x^a + 1$, we have

$$\alpha^m + \alpha^a + 1 = 0.$$

Since also $\alpha^t = 1$, we get

$$\alpha^{m+st} + \alpha^{a+rt} + 1 = 0$$

for all positive integers r and s, from which $f(x)$ divides

$$x^{m+st} + x^{a+rt} + 1.$$

□

Theorem 3. If $f(x)$ divides any trinomials, then $f(x)$ divides some trinomial of degree $< t$.

Proof. If $f(x)$ divides $x^m + x^a + 1$, we have $\alpha^m + \alpha^a + 1 = 0$.

Since $\alpha^t = 1$, this gives

$$\alpha^{m'} + \alpha^{a'} + 1 = 0$$

where

$$m' \equiv m(mod\ t) \quad \text{and} \quad a' \equiv a(mod\ t),$$

from which we can pick m' and a' on the range from 0 to $t-1$. Then $f(x)$ must divides some trinomial

$$x^{m'} + x^{a'} + 1$$

of degree $< t$.

□

Hence, if $f(x)$ divides no trinomial of degree $< t$, then $f(x)$ will never divide any trinomials. This provides a finite decision procedure for whether a given irreducible polynomial ever divides trinomials. Also, an irreducible polynomial $f(x)$ either divides infinitely many trinomials, or divides no trinomials. In the following, we show that every primitive polynomial divides infinitely many trinomials, and present a whole family of irreducible polynomials $x^{t-1} + x^{t-2} + \ldots + x + 1$ which divide no trinomials.

Theorem 4. If $f(x)$ is a primitive polynomial of degree n (i.e. if $t = 2^n - 1$), then $f(x)$ divides trinomials.

Proof. Since α is a root of $f(x)$, the powers

$$1, \alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{t-1}$$

are all distinct, and constitute all the non-zero elements of the field GF(2^n).

Hence, for all $i, 0 < i < t$,

$$1 + \alpha^i = \alpha^j \quad \text{for some} \quad j \neq i,\ 0 < j < t.$$

Thus, $f(x)$ divides $x^i + x^j + 1$ for each such pair (i, j).

□

In fact, when $f(x)$ is a primitive polynomial, it divides exactly $(t-1)/2$ trinomials of degree less than t. Since the primitive polynomials precisely correspond to m-sequences,

this theorem says that every m-sequence can be obtained from a two-tap linear shift register. This is a very simple and efficient way to generate an m-sequence.

Theorem 5. For odd $t > 3$, if $f(x) = \frac{(x^t-1)}{(x-1)} = x^{t-1} + x^{t-2} + \ldots + x + 1$ is irreducible, then $f(x)$ divides no trinomials.

Proof. The lowest degree polynomial having the root α of $f(x)$ as a root is the irreducible polynomial

$$f(x) = \frac{(x^t - 1)}{(x - 1)} = x^{t-1} + x^{t-2} + \ldots + x + 1,$$

which has $t > 3$ terms. Suppose $f(x)$ divides some trinomial $x^m + x^a + 1$, so that

$$\alpha^m + \alpha^a + 1 = 0.$$

Then

$$\alpha^{m'} + \alpha^{a'} + 1 = 0,$$

where m' and a' are m and a reduced modulo t, respectively, and are less than t. Thus α is a root of

$$x^{m'} + x^{a'} + 1,$$

a trinomial of degree $\leq t - 1$. But the only polynomial of degree $\leq t - 1$ with α as a root is its minimal polynomial, the t-term irreducible polynomial $f(x)$ of degree $t - 1$.

□

This occurs if and only if 2 is a primitive root modulo t with t prime. Examples include

$$t = 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, \ldots.$$

By Artin's Conjecture [1], there are infinitely many primes p for which 2 is a primitive root (i.e. where 2 is a generator of the multiplicative group of GF(p)). Artin's Conjecture includes the assertion that every prime q is a primitive root — i.e. a generator of the multiplicative group — modulo p, for infinitively many primes p. This has been proved for all primes q assuming the Generalized Riemann Hypothesis; and without that hypothesis, for all primes q with at most two exceptions. It is therefore extremely unlikely that $q = 2$ is an exception. Hence, we believe there are infinitely many irreducible polynomials of this kind which never divide trinomials.

Definition 1. The t^{th} cyclotomic polynomial is given by

$$\Phi_t(x) = \prod_{d|t} (x^{t/d} - 1)^{\mu(d)} \tag{2.1}$$

where $\mu(d)$ is the Möbius mu-function.

For any odd integer $t > 3$, let

$$\Phi_t(x) = f_1(x) f_2(x) \ldots f_r(x)$$

be the factorization of the t^{th} cyclotomic polynomial into irreducible factors over GF(2).

It is known that all the $f_i(x)$'s have the same degree (say, n) and the same primitivity t. These factors are all the irreducible polynomials having primitivity t.

Theorem 6. If any one of the $f_i(x)$'s divides a trinomial, then all r of the $f_i(x)$'s divide trinomials.

Proof. Collectively, the roots of the polynomials

$$f_1(x), f_2(x), \ldots, f_r(x)$$

are all the powers

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{t-1},$$

of a single root α of $\Phi_t(x)$, which can be taken to be a root of any one of the polynomials $f_i(x)$. Also, the roots of $\alpha^t = 1$ always form a cyclic group under multiplication. If α is a primitive root of $\alpha^t = 1$, then every other primitive root will be a power of α. Suppose $f_i(x)$ divides the trinomial $x^m + x^a + 1$. Then

$$\alpha^m + \alpha^a + 1 = 0,$$

where we selected α to be a root of $f_i(x)$. For any other polynomial $f_j(x)$ from the set of divisors of $\Phi_t(x)$, let one of its roots be $\beta = \alpha^u$, with

$$GCD(t, u) = 1 \quad (i.e.\ rt + su = 1 \text{ for some } r, s).$$

Then for some s, $1 \leq s \leq t-1$, we have $\alpha = \beta^s$, from which

$$(\beta^s)^m + (\beta^s)^a + 1 = \beta^{sm} + \beta^{sa} + 1 = 0,$$

whereby $f_j(x)$ divides the trinomial

$$x^{sm} + x^{sa} + 1.$$

□

Specifically, if any one of the $f_i(x)$'s is already a trinomial, then all the $f_i(x)$'s divide trinomials. The theorem provides that for any odd t, either all the $f_i(x)$'s divide trinomials or none divides trinomials. Next, a clever criterion for testing whether an irreducible polynomial divides trinomials is the following.

Theorem 7 (Welch's Criterion). For any odd integer t, the irreducible polynomials of primitivity t divide trinomials if and only if $GCD(1 + x^t, 1 + (1 + x)^t)$ has degree greater than 1.

Proof. Let $c_t(x) = \frac{(x^t-1)}{(x-1)}$ (not necessary the t^{th} cyclotomic polynomial). Then

$$(1 + x^t) = (1 + x)c_t(x),$$

and

$$(1 + (1 + x)^t) = xc_t(1 + x).$$

Thus, except for possible linear factors,

$$GCD(1+x^t, 1+(1+x)^t) = GCD(c_t(x), c_t(1+x)).$$

Let

$$c_t(x) = \frac{(x^t-1)}{(x-1)} = f_1(x)f_2(x)\dots f_r(x)$$

be the factorization of $c_t(x)$ into irreducible factors. Then the roots of

$$f_1(x), f_2(x), \dots, f_r(x)$$

collectively are

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{t-1}$$

where $\alpha \neq 1$ and $\alpha^t = 1$. Thus, the roots of the irreducible factors of $c_t(1+x)$ are

$$1+\alpha, 1+\alpha^2, 1+\alpha^3, \dots, 1+\alpha^{t-1}.$$

Hence, the GCD in question has degree > 1 if and only if one of the roots (say $1+\alpha^j$) from $c_t(1+x)$ equals one of the roots (say α^i) from $c_t(x)$ (i.e. $1+\alpha^j = \alpha^i$). This is the precise condition that a factor of $c_t(x)$ with α as a root divides the trinomial $x^i + x^j + 1$.

□

This computationally useful criterion, due to L.R. Welch, determines whether the irreducible polynomials of primitivity t divide trinomials, for any odd integer $t > 3$, without directly identifying which irreducible polynomial divides which trinomial.

2.2 Further Theorems and Results

When the primitivity t is a prime p, let

$$\Phi_p(x) = \frac{(x^p - 1)}{(x - 1)} = f_1(x) f_2(x) \dots f_r(x)$$

be the factorization of the p^{th} cyclotomic polynomial into irreducible factors over GF(2). Here the index

$$r = \phi(p)/n = (p - 1)/n$$

is the number of irreducible factors of $\Phi_p(x)$ over GF(2), and $(p - 1)/r$ is the order of 2 in the multiplicative group modulo p. Again, all the $f_i(x)$'s have the same degree (say, n) and the same primitivity p, and they are all the irreducible polynomials having primitivity p over GF(2). Let α be a root of $f_i(x)$. The following results relate to the index r.

Definition 2. Let $f(x)$ be an irreducible polynomial of degree n. The reciprocal of $f(x)$ is defined as

$$f^*(x) = x^n f(\frac{1}{x}).$$

When

$$f^*(x) = f(x),$$

then we say $f(x)$ is self-reciprocal (i.e. if α is a root of $f(x)$, then α^{-1} is also a root of $f(x)$).

Lemma 2. For prime values $p > 3$ with $\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)\dots f_r(x)$ as a product of $r > 1$ irreducible polynomials, if any of the $f_i(x)$'s is self-reciprocal, then $f_i(x)$ cannot be a trinomial.

Proof. Since $f_i(x)$ is self-reciprocal, we have

$$f_i(x) = x^{(p-1)/r} f_i(\frac{1}{x}).$$

If $f_i(x)$ is a trinomial, it must be

$$x^{(p-1)/r} + x^{(p-1)/2r} + 1,$$

which divides

$$x^{3(p-1)/2r} + 1,$$

whereby

$$\alpha^{3(p-1)/2r} = 1,$$

but

$$3(p-1)/2r < p$$

for all $r > 1$, which contradicts p being the smallest positive exponent with $\alpha^p = 1$.

□

Theorem 8. For prime $p > 3$, if any of the $f_i(x)$'s is self-reciprocal, then none of the $f_i(x)$'s divide trinomials.

Proof. Since $f_i(x)$ is self-reciprocal, it cannot be a trinomial by the previous Lemma. Suppose $f_i(x)$ divides some trinomial. WLOG, $f_i(x)$ divides a trinomial $t_i(x) = x^m + x^a + 1$ with $1 \leq a < m < p$. Write

$$t_i(x) = x^m + x^a + 1 = f_i(x)g_i(x).$$

Then

$$t_i^*(x) = x^m + x^{m-a} + 1 = f_i(x)g_i^*(x)$$

where $g_i^*(x) = x^d g_i(\frac{1}{x})$ and $d = \text{degree}(g_i(x))$. Thus

$$t_i(x) + t_i^*(x) = x^{m-a} + x^a = f_i(x)(g_i(x) + g_i^*(x))$$

and $f_i(x)$ divides

$$x^{m-a} + x^a = x^a(1 + x^{|m-2a|}),$$

where $0 \leq |m - 2a| < p$, which contradicts α, the root of $f_i(x)$, having primitivity p, unless $m - 2a = 0$. In this case,

$$g_i^*(x) = g_i(x) \quad \text{and} \quad t_i^*(x) = t_i(x),$$

so that

$$t_i(x) = x^m + x^{m/2} + 1,$$

which divides $x^{3m/2} + 1$, so that

$$\alpha^{3m/2} = 1,$$

whereas also $\alpha^p = 1$. This requires

$$\alpha^{|p-3m/2|} = 1,$$

but since $(p-1)/r < m < p$ and $r > 1$, we have

$$3(p-1)/2r < 3m/2 < 3p/2,$$

from which

$$0 < |p - 3m/2| < p,$$

contradicting α having primitivity p.

□

Corollary 1. Let $p > 3$ be a prime and $\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)\dots f_r(x)$ be a product of r irreducible polynomials. If $r > 1$ is an odd number, then the $f_i(x)$'s divide no trinomials.

Proof. When $r > 1$ is odd, then at least one of the $f_i(x)$'s is self-reciprocal. The result follows from the theorem.

□

Hence, if the index r of the p^{th} cyclotomic polynomial $\Phi_p(x)$ is any odd number, then all the irreducible factors of $\Phi_p(x)$ divide no trinomials, except for the trinomial $x^2 + x + 1$ with $r = 1$ and $p = 3$, which is already a trinomial. When r is an even number, it no longer guarantees that at least one of the $f(x)$'s is self-reciprocal. But there are only two cases: either at least one of the $f(x)$'s is self-reciprocal, or none of them is self-reciprocal. In the former case, all the $f(x)$'s divide no trinomials by the above theorem. In the latter case, the polynomials appear in pairs (i.e. if α is a root of $f_i(x)$, then α^{-1} is a root of $f_i^*(x)$). Then the $f_i(x)$'s may or may not divide trinomials.

Theorem 9. Let $p > 7$ be a prime and $\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)$ be a product of two irreducible polynomials (i.e. $r = 2$). Then the $f_i(x)$'s divide no trinomials.

Proof. If either one of the $f_i(x)$'s is self-reciprocal, then the $f_i(x)$'s divide no trinomials by the previous theorem. Otherwise, the $f_i(x)$'s form a reciprocal pair. If α is a root of

$f_1(x)$, then α^{-1} is a root of $f_2(x)$. Suppose $f_1(x)$ divides some trinomial $t_1(x)$ (including the case that $f_1(x)$ itself is a trinomial). Then we can write

$$t_1(x) = x^m + x^a + 1 = f_1(x)g_1(x),$$

with $1 \leq a < m < p$, and replacing α by α^{-1} for all roots of $t_1(x)$, we get

$$f_2(x)g_1^*(x) = t_1^*(x) = x^m + x^{m-a} + 1.$$

Then the product

$$\begin{aligned} & t_1(x)t_1^*(x) \\ =& f_1(x)f_2(x)g_1(x)g_1^*(x) \\ =& \Phi_p(x)g_1(x)g_1^*(x) \\ =& x^{2m} + x^{2m-a} + x^{m+a} + x^m + x^a + x^{m-a} + 1, \end{aligned}$$

and this 7-nomial must have both α and α^{-1} as roots, which must satisfy both $\alpha^p = 1$ and $\alpha^{-p} = 1$. We may therefore reduce all exponents in $t_1(x)t_1^*(x)$ modulo p, to get an at most 7-term polynomial of degree $< p$, but which has all $p-1$ roots of $\Phi_p(x)$ as roots, contradicting the fact that the only (non-zero) polynomial of degree $< p$ with all roots of $\Phi_p(x)$ as roots is $\Phi_p(x)$ itself, which has $p > 7$ terms.

□

Note that when $r = 2$ and $p = 7$, neither of the $f_i(x)$'s is self-reciprocal, where

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$$

has only 7 terms, and the two factors of $\Phi_7(x)$ are already trinomials.

Theorem 10. Let p be a prime and $\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)f_3(x)f_4(x)$ be a product of four irreducible polynomials (i.e. $r = 4$). Then the $f_i(x)$'s divide no trinomials.

Proof. If any one of the $f_i(x)$'s is self-reciprocal, then the $f_i(x)$'s divide no trinomials by Theorem 8. Otherwise, the $f_i(x)$'s come in pairs. Let α be a root of $f_1(x)$ and α^{-1} be a root of $f_2(x)$. Similarly, let $\beta = \alpha^u$ be a root of $f_3(x)$ and β^{-1} be a root of $f_4(x)$. Suppose $f_1(x)$ divides some trinomial $t_1(x)$ (including the case that $f_1(x)$ itself is a trinomial). Then we can write

$$t_1(x) = x^m + x^a + 1 = f_1(x)g_1(x),$$

with $1 \leq a < m < p$. Replacing α by α^{-1} for all roots of $t_1(x)$, we get

$$f_2(x)g_1^*(x) = t_1^*(x) = x^m + x^{m-a} + 1.$$

Then the product

$$\begin{aligned} & t_1(x)t_1^*(x) \\ =& f_1(x)f_2(x)g_1(x)g_1^*(x) \\ =& x^{2m} + x^{2m-a} + x^{m+a} + x^m + x^a + x^{m-a} + 1 \end{aligned}$$

is a 7-term polynomial which has both α and α^{-1} as roots. Similarly, suppose $f_3(x)$ divides some trinomial $t_3(x)$ (including the case that $f_3(x)$ itself is a trinomial). Then we can write

$$t_3(x) = x^k + x^b + 1 = f_3(x)g_3(x),$$

with $1 \leq b < k < p$. Replacing β by β^{-1} for all roots of $t_3(x)$, we get

$$f_4(x)g_3^*(x) = t_3^*(x) = x^k + x^{k-b} + 1.$$

Then the product

$$\begin{aligned} & t_3(x)t_3^*(x) \\ =& f_3(x)f_4(x)g_3(x)g_3^*(x) \\ =& x^{2k} + x^{2k-b} + x^{k+b} + x^k + x^b + x^{k-b} + 1 \end{aligned}$$

is also a 7-term polynomial which has both β and β^{-1} as roots.

Then

$$\begin{aligned} & t_1(x)t_1^*(x)t_3(x)t_3^*(x) \\ =& f_1(x)f_2(x)f_3(x)f_4(x)g_1(x)g_1^*(x)g_3(x)g_3^*(x) \\ =& \Phi_p(x)g_1(x)g_1^*(x)g_3(x)g_3^*(x) \end{aligned}$$

has at most 49 terms, and has α, α^{-1}, β and β^{-1} as roots, satisfying $\alpha^p = 1$, $\alpha^{-p} = 1$, $\beta^p = 1$ and $\beta^{-p} = 1$. We may therefore reduce all exponents in $t_1(x)t_1^*(x)t_3(x)t_3^*(x)$ modulo p, to get an at most 49-term polynomial of degree $< p$, but which has all $p-1$ roots of $\Phi_p(x)$ as roots, contradicting the fact that the only (non-zero) polynomial of degree $< p$ with all roots of $\Phi_p(x)$ as roots is $\Phi_p(x)$ itself, which has $p > 49$ terms. Since the first

$$\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)f_3(x)f_4(x),$$

with four irreducible factors, happens at $p = 113 > 49$, the result follows.

□

Theorem 11. Let p be a prime and $\Phi_p(x) = \frac{(x^p-1)}{(x-1)} = f_1(x)f_2(x)\dots f_r(x)$ be a product of r irreducible polynomials. If the index r is any even number, then the $f_i(x)$'s divide no trinomials if $p > 7^{r/2}$.

Proof. If any one of the $f_i(x)$'s is self-reciprocal, then the $f_i(x)$'s divide no trinomials by the above theorem. Otherwise, the $f_i(x)$'s appear in pairs. By using similar arguments, let α_i be a root of $f_i(x)$ and α_i^{-1} be a root of $f_{i+1}(x)$ with $1 \leq i < r$, where i is

odd. Suppose $f_i(x)$ divides some trinomial $t_i(x)$ (including the case that $f_i(x)$ itself is a trinomial). Then we can write

$$t_i(x) = x^m + x^a + 1 = f_i(x)g_i(x),$$

with $1 \leq a < m < p$. Replacing α_i by α_i^{-1} for all roots of $t_i(x)$, we get

$$f_{i+1}(x)g_i^*(x) = t_i^*(x) = x^m + x^{m-a} + 1.$$

Then the product

$$\begin{aligned} & t_i(x)t_i^*(x) \\ =& f_i(x)f_{i+1}(x)g_i(x)g_i^*(x) \\ =& x^{2m} + x^{2m-a} + x^{m+a} + x^m + x^a + x^{m-a} + 1 \end{aligned}$$

is a 7-term polynomial which has both α_i and α_i^{-1} as roots. Therefore,

$$\begin{aligned} & t_1(x)t_1^*(x)t_3(x)t_3^*(x)\dots t_{r-1}(x)t_{r-1}^*(x) \\ =& f_1(x)f_2(x)f_3(x)f_4(x)\dots f_r(x)g_1(x)g_1^*(x)g_3(x)g_3^*(x)\dots g_{r-1}(x)g_{r-1}^*(x) \\ =& \Phi_p(x)g_1(x)g_1^*(x)g_3(x)g_3^*(x)\dots g_{r-1}(x)g_{r-1}^*(x) \end{aligned}$$

has at most $7^{r/2}$ terms, and has α_i's and α_i^{-1}'s as roots, satisfying $\alpha_i^p = 1$ and $\alpha_i^{-p} = 1$ for every odd integer $i < r$.

We may therefore reduce all exponents in

$$t_1(x)t_1^*(x)t_3(x)t_3^*(x)\dots t_{r-1}(x)t_{r-1}^*(x)$$

modulo p, to get an at most $7^{r/2}$-term polynomial of degree $< p$, but which has all $p-1$ roots of $\Phi_p(x)$ as roots, contradicting the fact that the only (non-zero) polynomial of degree $< p$ with all roots of $\Phi_p(x)$ as roots is $\Phi_p(x)$ itself, which has $p > 7^{r/2}$ terms.

□

The above theorem also provides a finite decision procedure for whether a given irreducible polynomial of prime primitivity p divides trinomials, in terms of the index r. Among the first $1,000,000$ odd primes (i.e. 3 to $15,485,867$), about 98.9% have their index $r \leq 100$; 95.7% have $r \leq 24$; and 93.5% have $r \leq 16$. As predicted by Artin's Conjecture, about 37.4% have $r = 1$. We also found that about 28.1% have $r = 2$; 6.6% have $r = 3$; 4.7% have $r = 4$; 1.9% have $r = 5$; 5.0% have $r = 6$; 0.9% have $r = 7$; 3.5% have $r = 8$; 0.7% have $r = 9$; and 1.4% have $r = 10$. (The probabilistic argument used in Artin's Conjecture for $r = 1$ can be modified for these larger values of r.) The frequency distribution of the index $r(1 \leq r \leq 100)$ of the first $1,000,000$ odd primes is presented in Table 2.1.

According to the index r $(1 \leq r \leq 16)$, we summarize the test results for whether or not the irreducible polynomials of prime primitivity p divide trinomials as follows:

1. When $r = 1$, $f_1(x)$ divides trinomials only at $p = 3$.

2. When $r = 2$, the $f_i(x)$'s divide trinomials only at $p = 7$.

3. When $r = 4$, the $f_i(x)$'s divide no trinomials.

4. When $r = 6$, the $f_i(x)$'s divide trinomials only at $p = 31$.

5. When $r = 8$, the $f_i(x)$'s divide trinomials only at $p = 73$.

6. When $r = 10$, the $f_i(x)$'s divide no trinomials.

7. When $r = 12$, the $f_i(x)$'s divide no trinomials.

8. When $r = 14$, the $f_i(x)$'s divide no trinomials.

9. When $r = 16$, the $f_i(x)$'s divide no trinomials.

10. When $r > 1$ is an odd number, the $f_i(x)$'s divide no trinomials.

Table 2.1: Frequency distribution of the index r of the first $1,000,000$ odd primes ($1 \leq r \leq 100$)

r	-100k	-200k	-300k	-400k	-500k	-600k	-700k	-800k	-900k	-1000k	$f(r)$
1	37470	37345	37503	37399	37394	37351	37243	37461	37398	37460	374024
2	28059	28111	28022	28050	28084	28004	28169	28125	27956	28212	280792
3	6633	6677	6595	6642	6641	6633	6713	6648	6699	6583	66464
4	4680	4645	4712	4710	4602	4752	4679	4666	4628	4571	46645
5	1858	1883	1876	1914	1888	1981	1944	1888	1915	1838	18985
6	5015	4971	5102	4936	4945	5095	4963	4973	5003	4953	49956
7	893	899	892	890	883	887	870	857	857	884	8812
8	3525	3515	3433	3502	3493	3472	3534	3599	3504	3552	35129
9	744	731	748	733	719	722	755	737	767	739	7395
10	1382	1416	1468	1448	1430	1404	1396	1381	1376	1416	14117
11	350	322	324	345	309	294	356	355	367	331	3353
12	813	826	823	870	799	796	820	841	824	891	8303
13	242	241	228	228	280	239	233	230	239	257	2417
14	695	630	660	676	643	702	646	662	684	693	6691
15	316	339	327	348	354	328	333	318	352	361	3376
16	883	849	860	922	883	897	947	846	843	840	8770
17	139	145	145	140	125	136	148	128	135	108	1349
18	538	621	529	507	538	564	544	530	556	539	5466
19	95	126	111	98	121	108	100	108	91	103	1061
20	244	247	243	254	258	234	232	229	247	246	2434
21	176	170	167	163	168	158	159	139	157	164	1621
22	259	274	261	260	255	256	228	254	256	228	2531
23	87	97	83	68	75	68	73	84	75	73	783
24	608	653	636	614	626	596	588	634	620	639	6214
25	83	73	69	72	59	73	79	74	62	75	719
26	173	154	167	187	174	174	184	197	178	174	1762
27	88	74	82	85	88	86	89	80	82	88	842
28	111	116	102	108	112	114	111	118	110	114	1116
29	50	37	35	48	62	46	31	40	38	44	431
30	255	246	214	259	259	248	243	237	271	244	2476
31	43	41	50	46	40	43	36	31	48	40	418
32	221	220	219	208	217	229	199	207	227	226	2173
33	64	63	65	69	60	56	74	61	64	46	622
34	81	101	96	101	118	101	95	101	105	96	995
35	46	46	51	47	45	45	34	41	49	41	445
36	73	91	75	96	93	89	93	81	90	89	870
37	32	22	29	26	36	24	35	32	34	25	295
38	78	97	83	90	82	76	81	87	92	81	847
39	45	52	38	38	45	43	44	46	39	44	434
40	176	179	170	140	181	171	176	194	179	191	1757
41	22	24	29	17	30	21	25	20	27	22	237
42	109	111	118	117	129	135	126	126	110	111	1192
43	18	29	17	21	31	22	14	26	23	23	224
44	41	52	45	43	40	44	43	47	34	55	444
45	41	38	33	26	43	39	34	41	44	32	371
46	51	45	52	48	58	57	53	47	59	66	536
47	21	17	12	17	20	19	20	14	22	17	179
48	145	143	162	125	149	166	158	153	173	157	1531
49	25	11	13	13	27	15	17	17	17	27	182
50	58	65	67	59	66	54	63	41	62	49	584

Table 2.1 (Continued...)

r	-100k	-200k	-300k	-400k	-500k	-600k	-700k	-800k	-900k	-1000k	$f(r)$
51	22	30	25	21	22	23	31	28	23	29	254
52	38	35	39	29	23	32	27	25	36	38	322
53	11	11	21	12	10	13	17	15	12	13	135
54	62	62	60	66	66	46	60	47	52	52	573
55	15	16	19	20	25	18	18	17	12	23	183
56	78	75	100	90	94	71	85	72	92	76	833
57	11	15	14	27	25	18	25	22	8	15	180
58	40	33	28	29	36	38	37	39	36	42	358
59	4	11	15	10	12	10	12	11	7	14	106
60	38	38	35	38	45	34	42	43	38	41	392
61	13	12	11	6	15	10	15	13	13	9	117
62	25	38	28	28	22	26	34	28	28	28	285
63	18	19	18	15	19	14	14	19	13	22	171
64	56	65	48	50	61	38	42	70	44	46	520
65	14	16	9	11	10	12	5	10	12	8	107
66	53	32	44	40	56	53	47	50	55	46	476
67	14	14	8	5	9	6	16	6	12	13	103
68	11	16	17	17	9	14	15	13	24	18	154
69	7	12	13	15	15	9	15	12	10	11	119
70	35	33	34	41	21	40	37	30	37	38	346
71	5	8	2	13	8	4	8	6	13	8	75
72	70	58	63	57	58	73	70	73	61	54	637
73	6	8	11	7	4	3	11	5	5	5	65
74	27	22	26	24	27	19	20	16	29	26	236
75	18	14	11	10	20	16	9	10	13	15	136
76	11	11	13	7	11	12	18	11	15	10	119
77	3	10	10	8	5	11	8	9	10	5	79
78	40	32	32	31	29	35	33	26	36	21	315
79	5	6	7	7	7	10	4	11	3	7	67
80	47	40	50	44	34	42	40	43	60	37	437
81	7	4	5	6	8	13	6	4	8	7	68
82	11	10	14	12	18	20	13	16	13	13	140
83	4	7	8	11	5	10	8	8	2	3	66
84	15	20	15	21	15	17	23	18	19	21	184
85	3	10	6	5	3	10	5	4	7	5	58
86	17	23	13	15	26	13	9	16	16	14	162
87	7	6	5	8	9	13	13	16	12	9	98
88	34	32	30	31	29	35	28	35	27	29	310
89	3	4	7	4	7	5	6	11	7	7	61
90	27	28	35	25	22	24	34	30	29	24	278
91	3	6	7	5	12	3	8	4	3	6	57
92	20	8	13	8	11	4	11	16	6	14	111
93	12	7	4	9	8	4	8	10	10	10	82
94	7	17	10	10	10	17	13	15	6	11	116
95	4	2	7	3	5	3	6	4	8	6	48
96	42	45	40	34	40	46	41	47	37	39	411
97	0	3	5	3	6	5	4	6	2	8	42
98	12	19	12	17	9	11	13	19	17	12	141
99	1	6	10	4	12	10	10	6	6	4	69
100	7	8	9	6	9	14	9	11	13	10	96

Chapter 3

The Multiplicative Module

In this chapter, the multiplicative module M is introduced, which is the set of positive (odd) integers t such that the irreducible polynomials of odd primitivity $t > 1$ divide trinomials over GF(2). The computational results are presented, and the set G of generators of M is discussed.

3.1 Introduction

It is a simple fact that if the irreducible polynomials of primitivity t divide trinomials, then the irreducible polynomials of primitivity mt also divide trinomials for every odd integer $m \geq 1$. Therefore, let M be the set of positive (odd) integers t such that the irreducible polynomials of odd primitivity $t > 1$ divide trinomials. Then, in view of the closure property, we call M a multiplicative module. That is, for every $t \in M$, we also have $mt \in M$ for every odd integer $m \geq 1$.

An element g of M is a generator of M if and only if $g \in M$ but no proper factor h of g is in M. Let G be the subset of M consisting of the generators of M. From Theorem

4 in Chapter 2, the polynomials of primitivity $t = 2^n - 1$ divide trinomials for every integer $n > 1$. Hence each of these numbers

$$\{3,\ 7,\ 15,\ 31,\ 63,\ 127,\ 255,\ 511,\ 1023,\ \ldots\}$$

is in M, and each has (at least) one factor in G. From the computational results, the set G of the generators of M consists of both prime and composite values, and these numbers also suggest some interesting patterns.

3.2 Prime Generators of the Multiplicative Module M

Clearly, all the Mersenne primes ($2^n - 1$ being prime) are members of G. These include

$$\{3;\ 7;\ 31;\ 127;\ 8,191;\ 131,071;\ 524,287;\ 2,147,483,647;\ \ldots\}.$$

Aside from the Mersenne primes, there are other primes in G. The first non-Mersenne-prime generator of M is 73, corresponding to eight irreducible polynomials of degree 9 and primitivity $t = 73$, which do divide trinomials. (In fact, two of these eight irreducible polynomials are already trinomials; therefore all eight of them must divide trinomials by Theorem 6.)

By complete computer search for all odd primes $t \leq 3,000,000$, only five other prime elements of G (not Mersenne primes) exist:

$$\{73;\ 121,369;\ 178,481;\ 262,657;\ 599,479\}.$$

It was mentioned that among the eight irreducible factors of $\Phi_{73}(x)$, two of them are already trinomials. However, none of the irreducible factors of $\Phi_t(x)$ are trinomials for $t = 121,369$ or $178,481$ or $262,657$ or $599,479$. It is not necessary that if the irreducible factors of $\Phi_t(x)$ divide trinomials, then at least one of the factors has to be a trinomial.

Let $\Phi_n(2)$ denote the n^{th} cyclotomic polynomial evaluated at 2. All the elements of G currently known can be expressed fairly simply in terms of the numbers $\Phi_n(2)$. The Mersenne primes are precisely the numbers $\Phi_n(2)$ when n is prime and $2^n - 1$ is prime.

Of the other five known prime numbers in G, three are values of $\Phi_n(2)$:

$$73 = \Phi_9(2),\ 262,657 = \Phi_{27}(2),\ \text{and } 599,479 = \Phi_{33}(2).$$

This suggests the possibility that whenever $\Phi_n(2)$ is prime, where n is an odd prime, then $\Phi_n(2) \in G$. From [4], which lists the factorizations of $2^n - 1$ for all odd integers $n \leq 1,200$, the first counterexample occurs at

$$151 = \Phi_{15}(2),$$

which is not in G, and the next non-Mersenne-prime case

$$4,432,676,798,593 = \Phi_{49}(2)$$

is too large to test by current methods.

Besides $73 = \Phi_9(2),\ 262,657 = \Phi_{27}(2)$, and $599,479 = \Phi_{33}(2)$, the other two cases result from dividing $\Phi_n(2)$ by a small prime factor:

$$121,369 = \Phi_{39}(2)/79,$$

and

$$178,481 = \Phi_{23}(2)/47.$$

These two are both instances where $\Phi_n(2)$ has two prime factors, and t is the much larger of these two factors. While this may be a good way to look for likely values of t, it is not a reliable indicator. For example,

$$\Phi_{35}(2) = 71 \cdot 122,921,$$

but $t = 122,921$ is not in G, and the next non-Mersenne-prime cases,

$$\Phi_{37}(2) = 223 \cdot 1,616,318,177$$

and

$$\Phi_{41}(2) = 13,367 \cdot 164,511,353,$$

are also too large to test by current methods. The five known prime generators which are not Mersenne primes are listed in Table 3.1 along with their patterns.

Table 3.1: Prime generators of the multiplicative module M (non-Mersenne primes)

generators	patterns
73	$\Phi_9(2)$
121,369	$\Phi_{39}(2)/79$
178,481	$\Phi_{23}(2)/47$
262,657	$\Phi_{27}(2)$
599,479	$\Phi_{33}(2)$

3.3 Composite Generators of the Multiplicative Module M

If $g \in G$ is composite, then (by the definition of G) no prime factor of g is in G. The smallest composite $g \in G$ is $85 = 5 \cdot 17$, where $85 \in G$ but $5 \notin G$ and $17 \notin G$. All the eight irreducible factors of $\Phi_{85}(x)$ divide trinomials, even though none of them is a trinomial. By complete computer search, there are ten composite elements of G up to $t \leq 1,000,000$. These are:

$$\{85;\ 2,047;\ 3,133;\ 4,369;\ 11,275;\ 49,981;\ 60,787;\ 76,627;\ 140,911;\ 486,737\}.$$

Seven other larger composite elements of G are currently known:

$$\{1,826,203;\ 2,304,167;\ 2,528,921;\ 8,727,391;\ 14,709,241;\ 15,732,721;\ 23,828,017\}.$$

Among these seventeen composite elements of G known so far, most of them are either divisors of $\Phi_n(2)$ or of $\Phi_n(2)\Phi_{2n}(2)$ for various values of n. For example,

$$2,047 = 23 \cdot 89 = \Phi_{11}(2),$$

$$8,727,391 = 71 \cdot 122,921 = \Phi_{35}(2),$$

$$14,709,241 = 631 \cdot 23,311 = \Phi_{45}(2)$$

are of the form $\Phi_n(2)$;

$$486,737 = 233 \cdot 2,089 = \Phi_{29}(2)/1,103,$$

$$2,304,167 = 1,103 \cdot 2,089 = \Phi_{29}(2)/233,$$

$$23,828,017 = 11,119 \cdot 2,143 = \Phi_{51}(2)/103$$

are of the form $\Phi_n(2)/c$, where c is a prime factor of $\Phi_n(2)$;

$$85 = 5 \cdot 17 = \Phi_4(2)\Phi_8(2),$$

$$3,133 = 13 \cdot 241 = \Phi_{12}(2)\Phi_{24}(2),$$

$$4,369 = 17 \cdot 257 = \Phi_8(2)\Phi_{16}(2),$$

$$49,981 = 151 \cdot 331 = \Phi_{15}(2)\Phi_{30}(2),$$

$$140,911 = 43 \cdot (29 \cdot 113) = \Phi_{14}(2)\Phi_{28}(2),$$

$$15,732,721 = 241 \cdot (97 \cdot 673) = \Phi_{24}(2)\Phi_{48}(2)$$

are of the form $\Phi_n(2)\Phi_{2n}(2)$;

$$60,787 = 89 \cdot 683 = \Phi_{11}(2)\Phi_{22}(2)/23,$$

$$76,627 = 19 \cdot (37 \cdot 109) = \Phi_{18}(2)\Phi_{36}(2)/3,$$

$$1,826,203 = 337 \cdot 5,419 = \Phi_{21}(2)\Phi_{42}(2)/7,$$

$$2,528,921 = 41 \cdot 61,681 = \Phi_{20}(2)\Phi_{40}(2)/5$$

are of the form $\Phi_n(2)\Phi_{2n}(2)/c$, where c is a prime factor of $\Phi_n(2)$. The only exception so far, which is neither a divisor of $\Phi_n(2)$ nor of $\Phi_n(2)\Phi_{2n}(2)$, is

$$11,275 = 11 \cdot (5 \cdot 41) \cdot 5 = \Phi_{10}(2)\Phi_{20}(2)\Phi_5(2).$$

All these composite generators of M are listed in Table 3.2 and Table 3.3, respectively, according to their patterns, which also suggests testing the following kinds of numbers for membership in G.

1. If $\Phi_n(2)$ is prime and both of $\Phi_n(2)$ and $\Phi_{2n}(2) \notin M$, then $\Phi_n(2)\Phi_{2n}(2) \in G$, though this is not true for $n = 10$.

2. If $\Phi_n(2)$ is composite and $\Phi_{2n}(2) \notin M$, then $\Phi_n(2)\Phi_{2n}(2)/c \in G$, where c is a prime factor of $\Phi_n(2)$.

Also, it seems possible that $\Phi_{4n}(2) \notin M$ for all integers $n > 0$ (for all n up to 15 this has been verified); and $\Phi_n(2) \notin M$ implies $\Phi_{2n}(2) \notin M$ (for all n up to 20 this has been verified). The factorization of $\Phi_n(2)$ up to $n = 61$, along with its membership in M, is listed in Table 3.4.

Table 3.2: Composite generators of the multiplicative module M $(g \mid \Phi_n(2))$

generators	factors	patterns
2,047	$23 \cdot 89$	$\Phi_{11}(2)$
486,737	$233 \cdot 2,089$	$\Phi_{29}(2)/1,103$
2,304,167	$1,103 \cdot 2,089$	$\Phi_{29}(2)/233$
8,727,391	$71 \cdot 122,921$	$\Phi_{35}(2)$
14,709,241	$631 \cdot 23,311$	$\Phi_{45}(2)$
23,828,017	$11,119 \cdot 2,143$	$\Phi_{51}(2)/103$

Table 3.3: Composite generators of the multiplicative module M $(g \mid \Phi_n(2)\Phi_{2n}(2))$

generators	factors	patterns
85	$5 \cdot 17$	$\Phi_4(2)\Phi_8(2)$
4,369	$17 \cdot 257$	$\Phi_8(2)\Phi_{16}(2)$
60,787	$89 \cdot 683$	$\Phi_{11}(2)\Phi_{22}(2)/23$
3,133	$13 \cdot 241$	$\Phi_{12}(2)\Phi_{24}(2)$
140,911	$43 \cdot (29 \cdot 113)$	$\Phi_{14}(2)\Phi_{28}(2)$
49,981	$151 \cdot 331$	$\Phi_{15}(2)\Phi_{30}(2)$
76,627	$19 \cdot (37 \cdot 109)$	$\Phi_{18}(2)\Phi_{36}(2)/3$
2,528,921	$41 \cdot 61,681$	$\Phi_{20}(2)\Phi_{40}(2)/5$
1,826,203	$337 \cdot 5,419$	$\Phi_{21}(2)\Phi_{42}(2)/7$
15,732,721	$241 \cdot (97 \cdot 673)$	$\Phi_{24}(2)\Phi_{48}(2)$

note: $11{,}275 = 11 \cdot (5 \cdot 41) \cdot 5 = \Phi_{10}(2)\Phi_{20}(2)\Phi_5(2) \in G$.

Table 3.4: Factors of $\Phi_n(2)$ versus members of the multiplicative module M $(2 \leq n \leq 61)$

n	factorization of $\phi_n(2)$	$\phi_n(2) \in M$?	n	factorization of $\phi_n(2)$	$\phi_n(2) \in M$?
2	3	Yes	32	$65,537$	No
3	7	Yes	33	$599,479$	Yes
4	5	No	34	$43,691$	No
5	31	Yes	35	$71 \cdot 122,921$	Yes
6	3	Yes	36	$37 \cdot 109$	No
7	127	Yes	37	$223 \cdot 616,318,177$	Yes
8	17	No	38	$174,763$	No
9	73	Yes	39	$79 \cdot 121,369$	Yes
10	11	No	40	$61,681$	No
11	$23 \cdot 89$	Yes	41	$164,511,353 \cdot 13,367$	Yes
12	13	No	42	5419	No
13	$8,191$	Yes	43	$431 \cdot 2,099,863 \cdot 9,719$	Yes
14	43	No	44	$397 \cdot 2,113$	No
15	151	No	45	$631 \cdot 23,311$	Yes
16	257	No	46	$2,796,203$	No
17	$131,071$	Yes	47	$13,264,529 \cdot 2,351 \cdot 4,513$	Yes
18	$3 \cdot 19$	Yes	48	$97 \cdot 673$	No
19	$524,287$	Yes	49	$4,432,676,798,593$	Unknown
20	$5 \cdot 41$	No	50	$251 \cdot 4,051$	No
21	$7 \cdot 337$	Yes	51	$103 \cdot 11,119 \cdot 2,143$	Yes
22	683	No	52	$53 \cdot 157 \cdot 1,613$	No
23	$47 \cdot 178,481$	Yes	53	$69,431 \cdot 20,394,401 \cdot 6,361$	Yes
24	241	No	54	$3 \cdot 87,211$	Yes
25	$601 \cdot 1,801$	No	55	$881 \cdot 3,191 \cdot 201,961$	Unknown
26	$2,731$	No	56	$15,790,321$	No
27	$262,657$	Yes	57	$1,212,847 \cdot 32,377$	Unknown
28	$29 \cdot 113$	No	58	$59 \cdot 3,033,169$	Unknown
29	$233 \cdot 1,103 \cdot 2,089$	Yes	59	$3,203,431,780,337 \cdot 179,951$	Yes
30	331	No	60	$61 \cdot 1,321$	No
31	$2,147,483,647$	Yes	61	$2,305,843,009,213,693,951$	Yes

Chapter 4

Some Related Problems

In this chapter, some related problems are discussed. The distribution of the values of r for members of the set of all odd primes p leads to a generalization of Artin's Conjecture concerning primitive roots modulo p. We also generalize the conjectures of Blake, Gao and Lambert (BGL) and of Tromp, Zhang and Zhao (TZZ), and prove the former generalization.

4.1 Generalized Artin's Conjecture

Conjecture 1 (Artin's Primitive Root Conjecture). Every nonzero integer a not equal to -1 or a square number is a primitive root modulo p for infinitely many primes p, with a proposed density for the set of such primes p for given a which is always a rational multiple of a constant C_a known as Artin's Constant.

A remarkable quantitative version (for each such a) of this conjecture is: Let $\pi_a(x)$ be the number of primes less than or equal to x for which a is a primitive root.

Then $\pi_a(x)$ is asymptotic to

$$\frac{C_a x}{\ln x}, \quad \text{as} \quad x \to \infty,$$

where C_a (Artin's constant) is defined by:

$$C_a = \sum_{p=2}^{\infty} [1 - \frac{1}{p(p-1)}] = 0.3739558136...$$

In 1967, Hooley [8] proved both Artin's conjecture and the asymptotic formula for $\pi_a(x)$ subject to the assumption of the Generalized Riemann Hypothesis (GRH). In 1984, R. Gupta and M. R. Murty [6] proved, without any hypothesis, that in any set of thirteen prime numbers, Artin's conjecture is true for at least one of them. In 1986 Heath-Brown [7] refined the result to show that in any set of three prime numbers, such as $\{2, 3, 5\}$, Artin's conjecture is true for at least one of them. However, no specific value of a is known, so far, for which Artin's Conjecture has been proved unconditionally.

With

$$C_a = C_a^1,$$

we generalize to C_a^r, where a has order $(p-1)/r$ modulo p. When $a = 2$, by observing the first $1,000,000$ odd primes and their corresponding indices r, we propose the following results:

1. All $C_2^r > 0$, where 2 has order $(p-1)/r$ modulo p.

2. If $d|m$, then $C_2^d > C_2^m$.

3. $C_2^r = \frac{F_2(r)}{r \cdot \phi(r)} C_2^1$, where

$$F_2(r) \cong \begin{cases} 3 & \text{if 8 divides r} \\ 1.5 & \text{if 2 divides r but 4 does not divide r} \\ 1 & \text{otherwise} \end{cases}$$

and $\phi(r)$ is the Euler's phi-function.

The numerical results relating to C_2^r and $F_2(r)$ $(1 \leq r \leq 100)$ for the first $1,000,000$ odd primes are tabulated in Table 4.1.

It is interesting that the values of

$$F_2(r) = r \cdot \phi(r) \cdot C_2^r / C_2^1$$

seem limited to a set of only three members. A similar situation happens when $a = 3$, 5, and 7, where

$$F_3(r) \cong \begin{cases} 3.2 & \text{if 12 divides r} \\ 1.6 & \text{if 2 divides r but 6 does not divide r} \\ 1.2 & \text{if 4 divides r but 12 does not divide r} \\ 1 & \text{otherwise} \end{cases}$$

$$F_5(r) \cong \begin{cases} 3 & \text{if 10 divides r} \\ 1.4 & \text{if 2 divides r but 10 does not divide r} \\ 0 & \text{if 5 divides r but 10 does not divide r} \\ 1 & \text{otherwise} \end{cases}$$

and

$$F_7(r) \cong \begin{cases} 3 & \text{if 28 divides r} \\ 1.4 & \text{if 2 divides r but 7 does not divide r} \\ 1 & \text{otherwise.} \end{cases}$$

The numerical results relating to $F_3(r)$, $F_5(r)$, and $F_7(r)$ $(1 \leq r \leq 100)$ for the first $1,000,000$ odd primes are tabulated in Table 4.2. Similarly, let $\pi_a(x)$ be the number of primes less than or equal to x for which a has order $(p-1)/r$ modulo p. Then $\pi_a(x)$ is asymptotic to

$$\frac{C_a^r x}{\ln x}, \quad \text{as} \quad x \to \infty.$$

It is noteworthy that not all of the $C_a^r > 0$. For example, when r is an odd multiple of 5, then $C_5^r = 0$. In Table 4.3, we list all integers a $(2 \leq a \leq 100)$ and their corresponding indices r $(1 \leq r \leq 256)$ of the first $100,000$ odd primes. Then we have the following results:

1. If a is a perfect square, all the indices must be even numbers.

2. If $a = a_1 a_2^2$ is not a perfect square, and $a = 4m + 1$ $(m \in N)$, then all the indices occur except for the odd multiples of a_1.

3. Otherwise, all the indices occur.

Hence, it seems reasonable to generalize Artin's conjecture for primitive roots as follows:

Conjecture 2 (Generalized Artin's Conjecture). Every nonzero integer a not equal to -1 or a square number has each of the orders $(p-1)$, $(p-1)/2$, and $(p-1)/3$, modulo p, for infinitely many primes p.

Table 4.1: Numerical results of $F_2(r)$ for the first $1,000,000$ odd primes ($1 \leq r \leq 100$)

r	$f(r)$	C_2^r/C_2^1	$1/r \cdot \phi(r)$	$F_2(r)$
1	374024	1.000000000	1.000000000	1.000000000
2	280792	.7507325733	.5000000000	1.501465147
3	66464	.1776998267	.1666666667	1.066198960
4	46645	.1247112485	.1250000000	.9976899880
5	18985	.5075877484e-1	.5000000000e-1	1.015175497
6	49956	.1335636216	.8333333333e-1	1.602763459
7	8812	.2355998546e-1	.2380952381e-1	.9895193893
8	35129	.9392178042e-1	.3125000000e-1	3.005496973
9	7395	.1977145852e-1	.1851851852e-1	1.067658760
10	14117	.3774356726e-1	.2500000000e-1	1.509742690
11	3353	.8964665369e-2	.9090909091e-2	.9861131906
12	8303	.2219911022e-1	.2083333333e-1	1.065557291
13	2417	.6462152161e-2	.6410256410e-2	1.008095737
14	6691	.1788922636e-1	.1190476190e-1	1.502695015
15	3376	.9026158749e-2	.8333333333e-2	1.083139050
16	8770	.2344769320e-1	.7812500000e-2	3.001304730
17	1349	.3606720424e-2	.3676470588e-2	.9810279554
18	5466	.1461403546e-1	.9259259259e-2	1.578315830
19	1061	.2836716360e-2	.2923976608e-2	.9701569952
20	2434	.6507603790e-2	.6250000000e-2	1.041216606
21	1621	.4333946485e-2	.3968253968e-2	1.092154514
22	2531	.6766945437e-2	.4545454545e-2	1.488727996
23	783	.2093448549e-2	.1976284585e-2	1.059284966
24	6214	.1661390713e-1	.5208333333e-2	3.189870169
25	719	.1922336535e-2	.2000000000e-2	.9611682675
26	1762	.4710927641e-2	.3205128205e-2	1.469809424
27	842	.2251192437e-2	.2057613169e-2	1.094079524
28	1116	.2983765748e-2	.2976190476e-2	1.002545291
29	431	.1152332471e-2	.1231527094e-2	.9356939661
30	2476	.6619896049e-2	.4166666667e-2	1.588775052
31	418	.1117575343e-2	.1075268817e-2	1.039345069
32	2173	.5809787607e-2	.1953125000e-2	2.974611255
33	622	.1662994888e-2	.1515151515e-2	1.097576626
34	995	.2660257096e-2	.1838235294e-2	1.447179860
35	445	.1189763224e-2	.1190476190e-2	.9994011086
36	870	.2326053943e-2	.2314814815e-2	1.004855303
37	295	.7887194405e-3	.7507507508e-3	1.050574295
38	847	.2264560563e-2	.1461988304e-2	1.548959425
39	434	.1160353346e-2	.1068376068e-2	1.086090732
40	1757	.4697559515e-2	.1562500000e-2	3.006438090
41	237	.6336491776e-3	.6097560976e-3	1.039184651
42	1192	.3186961265e-2	.1984126984e-2	1.606228478
43	224	.5988920497e-3	.5537098560e-3	1.081599042
44	444	.1187089599e-2	.1136363636e-2	1.044638847
45	371	.9919149573e-3	.9259259259e-3	1.071268154
46	536	.1433063119e-2	.9881422925e-3	1.450259876
47	179	.4785789147e-3	.4625346901e-3	1.034687614
48	1531	.4093320215e-2	.1302083333e-2	3.143669926
49	182	.4865997904e-3	.4859086492e-3	1.001422369
50	584	.1561397130e-2	.1000000000e-2	1.561397130

Table 4.1 (Continued...)

r	$f(r)$	C_2^r/C_2^1	$1/r \cdot \phi(r)$	$F_2(r)$
51	254	.6791008064e-3	.6127450980e-3	1.108292516
52	322	.8609073215e-3	.8012820513e-3	1.074412337
53	135	.3609394050e-3	.3628447025e-3	.9947490001
54	573	.1531987252e-2	.1028806584e-2	1.489091609
55	183	.4892734156e-3	.4545454545e-3	1.076401514
56	833	.2227129810e-2	.7440476190e-3	2.993262465
57	180	.4812525399e-3	.4873294347e-3	.9875302119
58	358	.9571578294e-3	.6157635468e-3	1.554424315
59	106	.2834042735e-3	.2922267680e-3	.9698094238
60	392	.1048061087e-2	.1041666667e-2	1.006138643
61	117	.3128141510e-3	.2732240437e-3	1.144899793
62	285	.7619831882e-3	.5376344086e-3	1.417288730
63	171	.4571899129e-3	.4409171076e-3	1.036906722
64	520	.1390285115e-2	.4882812500e-3	2.847303916
65	107	.2860778987e-3	.3205128205e-3	.8925630440
66	476	.1272645606e-2	.7575757576e-3	1.679892200
67	103	.2753833979e-3	.2261420172e-3	1.217745385
68	154	.4117382842e-3	.4595588235e-3	.8959425065
69	119	.3181614014e-3	.3293807642e-3	.9659380145
70	346	.9250743268e-3	.5952380952e-3	1.554124869
71	75	.2005218916e-3	.2012072435e-3	.9965938011
72	637	.1703099266e-2	.5787037037e-3	2.942955532
73	65	.1737856394e-3	.1902587519e-3	.9134173207
74	236	.6309755524e-3	.3753753754e-3	1.680918871
75	136	.3636130302e-3	.3333333333e-3	1.090839091
76	119	.3181614014e-3	.3654970760e-3	.8704895943
77	79	.2112163925e-3	.2164502164e-3	.9758197336
78	315	.8421919449e-3	.5341880342e-3	1.576583321
79	67	.1791328899e-3	.1622849724e-3	1.103816868
80	437	.1168374222e-2	.3906250000e-3	2.991038008
81	68	.1818065151e-3	.2286236854e-3	.7952216971
82	140	.3743075311e-3	.3048780488e-3	1.227728702
83	66	.1764592646e-3	.1469291801e-3	1.200981755
84	184	.4919470408e-3	.4960317460e-3	.9917652343
85	58	.1550702629e-3	.1838235294e-3	.8435822302
86	162	.4331272859e-3	.2768549280e-3	1.564455757
87	98	.2620152717e-3	.2052545156e-3	1.276538404
88	310	.8288238188e-3	.2840909091e-3	2.917459842
89	61	.1630911385e-3	.1276813075e-3	1.277329796
90	278	.7432678117e-3	.4629629630e-3	1.605458473
91	57	.1523966376e-3	.1526251526e-3	.9985027697
92	111	.2967723996e-3	.2470355731e-3	1.201334674
93	82	.2192372682e-3	.1792114695e-3	1.223343957
94	116	.3101405257e-3	.2312673450e-3	1.341047633
95	48	.1283340107e-3	.1461988304e-3	.8778046332
96	411	.1098859966e-2	.3255208333e-3	3.375697816
97	42	.1122922593e-3	.1073883162e-3	1.045665518
98	141	.3769811563e-3	.2429543246e-3	1.551654439
99	69	.1844801403e-3	.1683501684e-3	1.095812033
100	96	.2566680213e-3	.2500000000e-3	1.026672085

Table 4.2: Numerical results of $F_3(r)$, $F_5(r)$, $F_7(r)$ of the first $1,000,000$ odd primes ($1 \leq r \leq 100$)

r	$f_3(r)$	$F_3(r)$	$f_5(r)$	$F_5(r)$	$f_7(r)$	$F_7(r)$
1	373959	1.000000000	393818	1.000000000	374120	1.000000000
2	299639	1.602523271	265842	1.350075416	282791	1.511766278
3	66531	1.067459267	69966	1.065964481	66417	1.065171602
4	56131	1.200794739	66341	1.347647898	68468	1.464086390
5	18912	1.011447779	0	0.	18934	1.012188603
6	33183	1.064811918	47125	1.435942492	50079	1.606297445
7	8941	1.004179603	9407	1.003240075	8918	1.001165401
8	14044	1.201757412	16786	1.363960002	17135	1.465626002
9	7421	1.071598758	7778	1.066512958	7369	1.063631990
10	14976	1.601886838	28461	2.890776958	14333	1.532449482
11	3417	1.005110186	3654	1.020623740	3387	.9958569443
12	24992	3.207881078	11818	1.440421718	12150	1.558858121
13	2394	.9986763255	2458	.9736680396	2459	1.025350155
14	7060	1.585842299	6267	1.336729150	4572	1.026536941
15	3287	1.054768036	0	0.	3444	1.104672298
16	3379	1.156575988	4147	1.347871352	4221	1.444156955
17	1443	1.049569605	1455	1.004931212	1349	.9807762216
18	3638	1.050660634	5289	1.450446653	5625	1.623810542
19	1116	1.020625256	1135	.9856583497	1086	.9927616808
20	2808	1.201415128	7109	2.888237714	3439	1.470758046
21	1628	1.097061443	1689	1.080773352	1568	1.056174490
22	2724	1.602528620	2335	1.304409651	2504	1.472468727
23	738	.9985800582	779	1.000903971	703	.9508125734
24	6258	3.213015331	2911	1.419213952	2945	1.511386721
25	740	.9894132780	0	0.	720	.9622580990
26	1920	1.601886838	1679	1.330177899	1827	1.523639474
27	762	.9903010759	875	1.079813518	834	1.083406394
28	1287	1.156362061	1609	1.372776257	3325	2.986207634
29	462	1.003168796	510	1.051551731	470	1.020100502
30	1625	1.042895077	4997	3.045264564	2540	1.629423714
31	411	1.022117398	431	1.017805179	417	1.036592537
32	920	1.259603325	1030	1.339095725	1083	1.482134074
33	606	1.069529013	622	1.042410454	629	1.109643965
34	1136	1.652544798	1034	1.428314602	1064	1.547139955
35	479	1.075946828	0	0.	445	.9991446599
36	2757	3.184905297	1260	1.382161303	1363	1.573869346
37	279	.9937666963	304	1.028211001	286	1.018261520
38	865	1.582152054	791	1.373842740	844	1.543077087
39	395	.9886645327	476	1.131324623	402	1.005752166
40	664	1.136381261	1719	2.793574697	847	1.448946862
41	225	.9867391880	236	.9827890039	226	.9906981716
42	753	1.014849221	1173	1.501180749	816	1.099283653
43	221	1.067298822	205	.9401043121	229	1.105458142
44	485	1.141301587	608	1.358597119	601	1.413664066
45	384	1.108998580	0	0.	392	1.131615524
46	584	1.580408547	541	1.390215785	589	1.593253502
47	184	1.063774371	178	.9771925103	186	1.074874372
48	1541	3.164753356	715	1.394349675	805	1.652517909
49	211	1.161191467	201	1.050378601	175	.9626590399
50	643	1.719439832	1089	2.765236734	599	1.601090559

Table 4.2 (Continued. . .)

r	$f_3(r)$	$F_3(r)$	$f_5(r)$	$F_5(r)$	$f_7(r)$	$F_7(r)$
51	230	1.003746400	246	1.019435374	243	1.060023522
52	363	1.211426921	424	1.343646050	449	1.497786807
53	110	.8106771061	148	1.035727163	121	.8913610605
54	428	1.112464201	552	1.362416142	605	1.571848605
55	183	1.076588610	0	0.	172	1.011440180
56	315	1.132102717	364	1.242238801	851	3.057158131
57	187	1.026112488	210	1.094211031	195	1.069549877
58	378	1.641548939	312	1.286604472	352	1.527980327
59	107	.9791287279	117	1.016647284	123	1.125056132
60	1248	3.203773675	1241	3.025153750	603	1.547311023
61	97	.9493554106	94	.8736015113	123	1.203303753
62	304	1.512037416	294	1.388560198	296	1.471613386
63	205	1.243291377	160	.9214408686	175	1.060889554
64	232	1.270556398	263	1.367697769	273	1.494450978
65	120	1.001179274	0	0.	115	.9590505719
66	303	1.069529012	438	1.468089320	427	1.506575430
67	88	1.040584663	87	.9768827223	83	.9810381695
68	185	1.076481647	235	1.298467820	271	1.576221533
69	131	1.063528355	136	1.048443697	142	1.152336149
70	340	1.527440174	655	2.794184116	229	1.028333155
71	95	1.262571565	92	1.161043934	61	.8103549662
72	680	3.142162643	314	1.377773489	344	1.588880573
73	72	1.011961204	73	.9742774582	81	1.137966428
74	230	1.638468388	193	1.305557389	207	1.473986956
75	147	1.179273664	0	0.	133	1.066502727
76	159	1.163293302	178	1.236632150	178	1.301742756
77	74	.9142178691	76	.8915793590	80	.9879183152
78	203	1.016196963	300	1.426039440	320	1.601197477
79	60	.9886645327	63	.9857497625	64	1.054121672
80	181	1.239066315	429	2.788699348	230	1.573826580
81	91	1.064378716	90	.9995987997	72	.8417833851
82	160	1.403362401	161	1.340923980	174	1.525499839
83	50	.9099928068	53	.9159510235	67	1.218865605
84	597	3.218406295	271	1.387280419	604	3.254741794
85	63	.9164641042	0	0.	76	1.105099968
86	152	1.468139555	145	1.329903661	164	1.583363627
87	99	1.289788453	94	1.162892503	69	.8985566128
88	136	1.280140336	146	1.304968285	153	1.439538116
89	48	1.005286675	64	1.272790984	46	.9629851378
90	195	1.126326683	559	3.065984795	256	1.478028440
91	51	.8935525022	56	.9316791006	56	.9807334548
92	125	1.353089510	120	1.233463174	125	1.352507217
93	58	.8654424682	90	1.275208345	80	1.193200043
94	140	1.618787086	119	1.306583244	130	1.502512563
95	48	.8779572090	0	0.	44	.8044477707
96	389	3.195558872	196	1.528909293	179	1.469817171
97	33	.8217371419	41	.9694630513	43	1.070287607
98	139	1.529911033	126	1.316892575	101	1.111183578
99	67	1.064234314	77	1.161399428	64	1.016144552
100	111	1.187295934	281	2.854110274	130	1.389928365

Table 4.3: Collections of possible indices r of the first $100,000$ odd primes ($2 \leq a \leq 100$)

a	factorization	possible indices	% of the least r
2	2	All	.37470
3	3	All	.37391
4	2^2	Even	.56202
5	5	All but odd multiples of 5.	.39347
6	$2 \cdot 3$	All	.37367
7	7	All	.37487
8	2^3	All	.22534
9	3^2	Even	.59924
10	$2 \cdot 5$	All	.37523
11	11	All	.37541
12	$2^2 \cdot 3$	All	.37559
13	13	All but odd multiples of 13.	.37677
14	$2 \cdot 7$	All	.37429
15	$3 \cdot 5$	All	.37471
16	2^4	Even	.37453
17	17	All but odd multiples of 17.	.37578
18	$2 \cdot 3^2$	All	.37495
19	19	All	.37497
20	$2^2 \cdot 5$	All but odd multiples of 5.	.39288
21	$3 \cdot 7$	All but odd multiples of 21.	.37272
22	$2 \cdot 11$	All	.37682
23	23	All	.37364
24	$2^3 \cdot 3$	All	.37498
25	5^2	Even	.57151
26	$2 \cdot 13$	All	.37476
27	3^3	All but $\{$ 4, 8, 16, 20, 28, $\ldots\}$.	.22436
28	$2^2 \cdot 7$	All	.37410
29	29	All but odd multiples of 29.	.37338
30	$2 \cdot 3 \cdot 5$	All	.37516
31	31	All	.37536
32	2^5	All	.29563
33	$3 \cdot 11$	All but odd multiples of 33.	.37380
34	$2 \cdot 17$	All	.37426
35	$5 \cdot 7$	All	.37295
36	$2^2 \cdot 3^2$	Even	.56082
37	37	All but odd multiples of 37.	.37510
38	$2 \cdot 19$	All	.37495
39	$3 \cdot 13$	All	.37420
40	$2^3 \cdot 5$	All	.37448
41	41	All but odd multiples of 41.	.37562
42	$2 \cdot 3 \cdot 7$	All	.37440
43	43	All	.37396
44	$2^2 \cdot 11$	All	.37509
45	$3^2 \cdot 5$	All but odd multiples of 5.	.39469
46	$2 \cdot 23$	All	.37416
47	47	All	.37404
48	$2^4 \cdot 3$	All	.37376
49	7^2	Even	.56647
50	$2 \cdot 5^2$	All	.37500

Table 4.3 (Continued...)

a	factorization	possible indices r	% of the least r
51	$3 \cdot 17$	All	.37443
52	$2^2 \cdot 13$	All but odd multiples of 13.	.37644
53	53	All but odd multiples of 53.	.37444
54	$2 \cdot 3^3$	All	.37448
55	$5 \cdot 11$	All	.37472
56	$2^3 \cdot 7$	All	.37284
57	$3 \cdot 19$	All but odd multiples of 57.	.37388
58	$2 \cdot 29$	All	.37487
59	59	All	.37520
60	$2^2 \cdot 3 \cdot 5$	All	.37455
61	61	All but odd multiples of 61.	.37604
62	$2 \cdot 31$	All	.37381
63	$3^2 \cdot 7$	All	.37522
64	2^6	Even	.33755
65	$5 \cdot 13$	All but odd multiples of 65.	.37365
66	$2 \cdot 3 \cdot 11$	All	.37418
67	67	All	.37543
68	$2^2 \cdot 17$	All but odd multiples of 17.	.37581
69	$3 \cdot 23$	All but odd multiples of 69.	.37432
70	$2 \cdot 5 \cdot 7$	All	.37258
71	71	All	.37533
72	$2^3 \cdot 3^2$	All	.37533
73	73	All but odd multiples of 73.	.37452
74	$2 \cdot 37$	All	.37337
75	$3 \cdot 5^2$	All	.37466
76	$2^2 \cdot 19$	All	.37389
77	$7 \cdot 11$	All but odd multiples of 77.	.37452
78	$2 \cdot 3 \cdot 13$	All	.37375
79	79	All	.37406
80	$2^4 \cdot 5$	All but odd multiples of 5.	.39384
81	3^4	Even	.37483
82	$2 \cdot 41$	All	.37316
83	83	All	.37314
84	$2^2 \cdot 3 \cdot 7$	All but odd multiples of 21.	.37246
85	$5 \cdot 17$	All but odd multiples of 85.	.37474
86	$2 \cdot 43$	All	.37592
87	$3 \cdot 29$	All	.37420
88	$2^3 \cdot 11$	All	.37601
89	89	All but odd multiples of 89.	.37388
90	$2 \cdot 3^2 \cdot 5$	All	.37461
91	$7 \cdot 13$	All	.37486
92	$2^2 \cdot 23$	All	.37347
93	$3 \cdot 31$	All but odd multiples of 93.	.37516
94	$2 \cdot 47$	All	.37455
95	$5 \cdot 19$	All	.37612
96	$2^5 \cdot 3$	All	.37456
97	97	All but odd multiples of 97.	.37519
98	$2 \cdot 7^2$	All	.37445
99	$3^2 \cdot 11$	All	.37435
100	$2^2 \cdot 5^2$	Even	.56268

4.2 Generalized TZZ and BGL Conjectures

In the generation of pseudorandom sequences, one may only require that

$$GCD(x^m + x^k + 1, x^{2^n-1} + 1)$$

contain a primitive factor of degree n over GF(2). In 1994, Tromp, Zhang and Zhao [12] conjectured that $GCD(x^m + x^k + 1, x^{2^n-1} + 1)$ is a primitive polynomial of each degree n over GF(2) for some integers m, k, and verified that the answer is yes for $n \leq 171$. In 1996, Blake, Gao and Lambert [2] extended the computational results for n up to 500, and also slightly relaxed the condition and asked: given an integer n, do there exist integers m, k such that $GCD(x^m + x^k + 1, x^{2^n-1} + 1)$ contains a primitive factor of degree n over GF(2)? Using Theorem 4, the latter question can be easily generalized and answered.

Theorem 12 (Generalized BGL Conjecture). Every primitive polynomial $f(x)$ divides some trinomial $x^m + x^k + 1$ for every k, $1 \leq k < 2^n - 1$, with $m \neq k$, $1 \leq k < m < 2^n - 1$.

Proof. If α is a root of $f(x)$, then the powers

$$1, \alpha^1, \alpha^2, \cdots, \alpha^{2^n-2}$$

are all distinct, and constitute all the non-zero elements of the field GF(2^n). Hence, for all k, $1 \leq k < 2^n - 1$,

$$1 + x^k = x^m$$

for some $m \neq k$, $1 \leq k < m < 2^n - 1$. Thus, $f(x)$ divides $x^m + x^k + 1$ for each such pair (k, m).

□

Hence, given an integer n, there do exist integers m, k such that

$$GCD(x^m + x^k + 1, x^{2^n - 1} + 1)$$

contains a primitive factor of degree n over GF(2). Furthermore, there exist $(2^{n-1} - 1)$ such (k, m) pairs for any given primitive polynomial of degree n, and this is also true for every primitive polynomial of degree n over GF(2).

Though Tromp, Zhang and Zhao's question is not yet answered, it is reasonable to strengthen their conjecture as follows.

Conjecture 3 (Generalized TZZ Conjecture). Every primitive polynomial $f(x)$ divides some trinomials $x^m + x^k + 1$ for $1 \leq k < m < 2^n - 1$ such that $GCD(x^m + x^k + 1, x^{2^n - 1} + 1) = f(x)$.

In fact, the following is known [2].

Theorem 13. If there is a primitive polynomial $f(x)$ of degree n for which a trinomial $x^m + x^k + 1$ exists with $1 \leq k < m < 2^n - 1$ and $GCD(x^m + x^k + 1, x^{2^n-1} + 1) = f(x)$, then this is true for every primitive polynomial of the same degree n.

Proof. Suppose that $f(x)$ is a primitive polynomial of degree n and

$$GCD(x^m + x^k + 1, x^{2^n-1} + 1) = f(x).$$

Let α be a root of $f(x)$ and β be a root of $g(x)$, where $g(x)$ is any primitive polynomial of degree n over GF(2). Then $\beta = \alpha^u$ for some integer u with $GCD(2^n - 1, u) = 1$, as both α and β are primitive elements in GF(2^n). Let v be an integer such that $uv \equiv 1$ (modulo $2^n - 1$). Then $\alpha = \beta^v$, and

$$GCD(x^{mv} + x^{kv} + 1, x^{2^n-1} + 1) = g(x),$$

from which

$$\beta^{mv} + \beta^{kv} + 1 = \alpha^{muv} + \alpha^{kuv} + 1 = \alpha^m + \alpha^k + 1 = 0;$$

that is, β is a root of $x^{mv} + x^{kv} + 1$. We see that

$$g(x) \mid (x^{mv} + x^{kv} + 1).$$

Therefore it suffices to show that

$$(x^{mv} + x^{kv} + 1)/g(x)$$

has no roots in GF(2^n). Consider the roots of $x^{mv} + x^{kv} + 1$ and $x^m + x^k + 1$ in some extension field of GF(2). Since

$$f(x) = \prod_{i=0}^{n-1}(x - \alpha^{2^i}),$$

we have

$$x^m + x^k + 1 = \prod_{i=0}^{n-1}(x - \alpha^{2^i}) \prod_{\gamma}(x - \gamma)$$

where every γ in the second product is not in GF(2). Hence

$$x^{mv} + x^{kv} + 1 = \prod_{i=0}^{n-1}(x - \alpha^{2^i}) \prod_{\gamma}(x^v - \gamma).$$

Obviously, every root of $x^v - \gamma$ is not in GF(2^n) when γ is not in GF(2^n). The only roots of $x^{mv} + x^{kv} + 1$ which are in GF(2^n) come from $x^v - \alpha^{2^i}$, $0 \leq i \leq n-1$. Let η be a primitive v^{th} root of unity over GF(2). Then

$$x^v - \alpha^{2^i} = x^v - \beta^{v2^i} = \prod_{j=0}^{v-1}(x - \beta^{2^i}\eta^j).$$

Since $GCD(2^n - 1, v) = 1$, $\eta^j \in \mathrm{GF}(2^n)$ iff $v \mid j$. This means that $\beta^{2^i}\eta^j \notin \mathrm{GF}(2^n)$ for $1 \leq j \leq v-1$. Hence $x^v - \alpha^{2^i}$ has only one root, i.e. β^{2^i} in $\mathrm{GF}(2^n)$ for $1 \leq i \leq n-1$. As

$$g(x) = \prod_{i=0}^{n-1}(x - \beta^{2^i}),$$

we see that $(x^{mv} + x^{kv} + 1)/g(x)$ has no roots in $\mathrm{GF}(2^n)$, which completes the proof.

□

Chapter 5

Conclusion

The theory of the irreducible polynomials which divide trinomials over GF(2) has an interesting structure. All the polynomials of (odd) primitivity t are the r irreducible factors of $\Phi_t(x)$ over GF(2), and either all or none of them divide trinomials.

Whether it is all or none depends to a considerable extent on r. (For all odd $t > 3$ and all odd r, the answer is none. For $r = 4, 10, 12, 14,$ and 16, the answer is none for all odd primes t. There is only one prime value of t, for each of $r = 2, 6,$ and 8, for which the answer is all rather than none. For each even $r > 16$, there is only a finite range, $t \leq 7^{r/2}$, for prime values of t where the answer *might* be all.)

The odd values of $t > 1$ such that polynomials of primitivity t divide trinomials form a multiplicative module M, which is closed with respect to multiplication by odd numbers. The set G of generators of M is quite sparse, and its members seem related to numbers of the form $\Phi_n(2)$.

The distribution of the values of r among the set of all odd primes p leads to a generalization of Artin's Conjecture concerning primitive roots modulo p. We generalized the

conjectures of Blake, Gao and Lambert (BGL), and of Tromp, Zhang and Zhao (TZZ). We proved the former generalization, and ascertained that the latter generalization is true if the original TZZ conjecture is true.

Bibliography

[1] E. Artin, The Collected Papers of Emil Artin, (ed. by Serge Lang and John T. Tate), Addison-Wesley 1965; Springer-Verlag 1982, viii-ix.

[2] I. F. Blake, S. Gao and R. Lambert, Construction and distribution problems for irreducible trinomials over finite fields, in Applications of Finite Fields (D. Gollmann, ed.), Oxford, Clarendon Press, 1996, 19-32.

[3] R. P. Brent and P. Zimmermann, Algorithms for Finding Almost Irreducible and Almost Primitive Trinomials, Proceedings of a Conference in Honor of Professor H.C. Williams, The Fields Institute, May 2003.

[4] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff, Jr., Factorizations of $b^n \pm 1$(b = 2, 3, 5, 6, 7, 10, 11, 12) up to high powers, Contemporary Mathematics, Third Edition, Vol. 22, American Math. Soc. 2003.

[5] S.W. Golomb, Shift Register Sequences, Holden-Day, Inc. 1967; Second Edition, Aegean Park Press 1982.

[6] R. Gupta and M. R. Murty, A remark on Artin's Conjecture, Inventiones Math. 78 (1984), 127-130.

[7] D.R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford 37 (1986), 27-38.

[8] C. Hooley, Artin's conjecture for primitive roots, J. Reine Angew. Math. 225 (1967), 209-220.

[9] J. H. Lindholm, An Analysis of the Pseudo-Randomness Properties of Subsequences of Long m-Sequences, IEEE Transactions on Information Theory, Vol. IT-14, No. 4, July, 1968, 569-576.

[10] G. Seroussi, Table of Low-Weight Binary Irreducible Polynomials, Computer Systems Laboratory, HPL-98-135, 1998.

[11] R.G. Swan, Factorization of Polynomials over Finite Fields, Pacific J. Mathematics 12 (1962), 1099-1106.

[12] J. Tromp, L. Zhang and Y. Zhao, Small weight bases for Hamming codes, Theoretical Computer Science 181(2), 1997, 337-345.

[13] N. Zierler and J. Brillhart, On Primitive Trinomials (mod 2), Information and Control 13, 1968, 541-554.

[14] N. Zierler and J. Brillhart, On Primitive Trinomials (mod 2) II, Information and Control 14, 1969, 566-569.