พหุนามเรียงสับเปลี่ยนดีกรีสามและเส้นโค้งเชิงวงรี

นายอรรถวุฒิ วงศ์ประดิษฐ์

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

5072562623

CUBIC PERMUTATION POLYNOMIALS AND ELLIPTIC CURVES

Mr. Attawut Wongpradit

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2010

Copyright of Chulalongkorn University

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

Thesis Title	CUBIC PERMUTATION POLYNOMIALS AND ELLIPTIC CURVES
By	Mr. Attawut Wongpradit
Field of Study	Mathematics
Thesis Advisor	Assistant Professor Yotsanan Meemark, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.... Chairman

(Associate Professor Ajchara Harnchoowong, Ph.D.)

.... Thesis Advisor

(Assistant Professor Yotsanan Meemark, Ph.D.)

.... Examiner

(Assistant Professor Tuangrat Chaichana, Ph.D.)

.... External Examiner

(Assistant Professor Pattira Ruengsinsub, Ph.D.)

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

อรรถวุฒิ วงศ์ประดิษฐ์: พหุนามเรียงสับเปลี่ยนดีกรีสามและเส้นโค้งเชิงวงรี. (CUBIC PERMUTATION POLYNOMIALS AND ELLIPTIC CURVES) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร.ยศนันต์ มีมาก, 25 หน้า.

วิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อศึกษาเส้นโค้งเชิงวงรี $E: y^2 = f(x)$ เมื่อ $f(x)$ เป็นพหุนามเรียงสับเปลี่ยนดีกรีสามบนริงสลับที่ที่มีขนาดจำกัด R เราพบว่าเมื่อ R คือฟีลด์จำกัด $\mathbb{F}_q$ กรุปของจุดตรรกยะบน E เป็นกรุปวัฏจักรที่มีขนาด $q+1$ และกรุปนี้จะอยู่ในรูปผลคูณของกรุปวัฏจักรเมื่อ $R = \mathbb{Z}_n$ ริงของจำนวนเต็มมอดุโล n ที่ไม่มีตัวประกอบเป็นกำลังสองของจำนวนเฉพาะ หรือ $R = \mathbb{Z}[i]/(\alpha)$ ริงของจำนวนเต็มเกาส์เซียนมอดุโล α ที่ไม่มีตัวประกอบเป็นกำลังสองของสมาชิกเฉพาะ อีกทั้งเรานิยามเส้นโค้งเชิงวงรีที่ไม่แปรเปลี่ยนต่อการเลื่อนซึ่งเป็นเส้นโค้งเชิงวงรี $E: y^2 = f(x)$ ซึ่ง $y^2 - f(x)$ เป็นพหุนามเรียงสับเปลี่ยนอย่างอ่อน เรายังได้ศึกษาเงื่อนไขที่จำเป็นและเพียงพอต่อการมีอยู่ของเส้นโค้งเชิงวงรีที่ไม่แปรเปลี่ยนต่อการเลื่อนบน $\mathbb{F}_q$, $\mathbb{Z}_n$ และ $\mathbb{Z}[i]/(\alpha)$ อีกด้วย

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา............คณิตศาสตร์.......... ลายมือชื่อนิสิต..
สาขาวิชา..........คณิตศาสตร์.......... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก..
ปีการศึกษา............2553...............

5072562623 : MAJOR MATHEMATICS

KEYWORDS : ELLIPTIC CURVE / PERMUTATION POLYNOMIAL

ATTAWUT WONGPRADIT : CUBIC PERMUTATION POLYNOMIALS AND ELLIPTIC CURVES. THESIS ADVISOR : ASSIT.PROF. YOTSANAN MEEMARK, Ph.D.,

25 pp.

In this thesis, we study the elliptic curve $E : y^2 = f(x)$, where $f(x)$ is a cubic permutation polynomial over some finite commutative ring R. In case R is the finite field $\mathbf{F}_q$, it turns out that the group of rational points on E is cyclic of order $q+1$. This group is a product of cyclic groups if $R = \mathbb{Z}_n$ or $\mathbb{Z}[i]/(\alpha)$, the ring of integers modulo a square-free n and the ring of Guassian integers modulo a square-free α, respectively. In addition, we introduce a shift-invariant elliptic curve which is an elliptic curve $E : y^2 = f(x)$, where $y^2 - f(x)$ is a weak permutation polynomial. We give a necessary and sufficient condition for the existence of a shift-invariant elliptic curve over $\mathbf{F}_q$, $\mathbb{Z}_n$ and $\mathbb{Z}[i]/(\alpha)$.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

Department : ....Mathematics.... Student's Signature : ....

Field of Study : ....Mathematics.... Advisor's Signature : Y. Meemark

Academic Year : ....2010...........

ACKNOWLEDGEMENTS

I have been indebted in the preparation of this thesis to my supervisor, Dr. Yotsanan Meemark, whose patience and kindness, as well as his academic experience, have been invaluable to me. Without his constructive suggestons and knowledgeable guidance in this study, this research would never have successfully been completed. Sincere thanks and deep appreciation are also extended to Associate Professor Dr. Ajchara Harnchoowong, the chairman, Assistant Professor Dr. Tuangrat Chaichana, and Assistant Professor Dr. Pattira Ruengsinsub, the commitee members, for their comments and suggestions.

I am also grateful to the Development and Promotion of Science and Technology Talents Project (DPST) for providing me support throughout my graduate study.

Finally, I would like to thank my family and friends for all their encouragement and support.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

CONTENTS

CHAPTER I

INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with q elements. An *elliptic curve* over $\mathbb{F}_q$, whose characteristic is greater than 3, is defined by an equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$. The point (x, y) in $\mathbb{F}_q \times \mathbb{F}_q$ on the curve E is called a *rational point*. Let $E(\mathbb{F}_q)$ denote the set of all rational points together with a distinguished point at infinity, denoted ∞. There is the addition $+$, which makes $(E(\mathbb{F}_q), +)$ become an abelian group [?], given as follows:

(a) [Identity] $P + \infty = \infty + P = P$ for all $P \in E(\mathbb{F}_q)$.

(b) [Negative] If $P = (x, y) \in E(\mathbb{F}_q)$, then $(x, y) + (x, -y) = \infty$. The point $(x, -y)$ is denoted by $-P$ and is called *the negative of* P.

(c) [Point addition] Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(\mathbb{F}_q)$ and $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

(d) [Point doubling] Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$ and $P \neq -P$. Then $2P = (x_3, y_3)$, where

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad \text{and} \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

Elliptic curves over finite fields play an important role in many areas of modern cryptology. Following the work of Lenstra, Jr. [?] on integer factorizations, many researchers have used this idea to work out primality proving algorithms [?, ?]. Recent work on these topics can be found in [?]. Another application is to construct the public keys. When using elliptic curves for constructing a public key, it is sometimes necessary to find elliptic curves with a known number of points and its group structure over a given finite field. We recall the number of rational points and the group structure of $E(\mathbb{F}_q)$ in the following theorem.

Theorem 1.0.1. *[?] Let E be an elliptic curve over $\mathbb{F}_q$. Then:*

1. *$|E(\mathbb{F}_q) - (q+1)| < 2\sqrt{q}$, and*
2. *$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ for some positive integers n_1 and n_2, and n_1 divides $\gcd(n_2, q-1)$.*

A *permutation polynomial* over $\mathbb{F}_q$ is a polynomial f whose function on $\mathbb{F}_q$ induced by f is a bijection. It is easy to see that every linear polynomial is a permutation polynomial. We observe that:

Theorem 1.0.2. *Let $\mathbb{F}_q$ be a finite field, $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$.*

1. *If $f(x)$ is a permutation polynomial over $\mathbb{F}_q$, then $f(x) + a$ and $f(x + a)$ are also permutation polynomials.*
2. *A monomial x^n is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.*

Proof. (1) They are just vertical and horizontal translations for a permutation $f(x)$.

(2) Clearly, $f(x) = x^n$ is an endomorphism on $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. Recall that $\mathbb{F}_q^\times$ is cyclic, say generated by a. We have thus f is a permutation polynomial $\Leftrightarrow$ $\langle a^n \rangle = \mathrm{im} f = \mathbb{F}_q^\times \Leftrightarrow \gcd(n, q-1) = 1$. $\square$

Permutation polynomials over finite fields and over the ring of integers modulo n have been widely studied. There are a lot of applications in combinatorics and cryptography [**?**, **?**] as well as many open problems. For the extensive studies, we refer the reader to Lidl and Niederreiter's book [**?**] Chapter 7.

In the next chapters, we study the group structure of elliptic curves $E : y^2 = f(x)$, where $f(x)$ is a cubic permutation polynomial. This work extends to an elliptic curve over a ring of integers modulo n and a ring of Gaussian integers modulo $\alpha \in \mathbb{Z}[i]$ in that chapter. In the final chapter, we define a shift-invariant elliptic curve, inspired by the property of a weak permutation polynomial, and characterize this type of elliptic curve on the finite fields, the ring of integers modulo n and a ring of Gaussian integers modulo α. We conclude this research by giving a remark on elliptic curve cryptography in Section3.3.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER II

ELLIPTIC CURVES WITH PERMUTATION POLYNOMIALS

In this chapter, we study elliptic curves with permutation polynimials over several structures, namely, finite fields, rings of integers modulo a positive integer $n > 1$ and rings of Gaussian integers modulo a nonzero nonunit $\alpha \in \mathbb{Z}[i]$.

2.1 Elliptic Curves with Permutation Polynomials over Finite Fields

Since $a^q = a$ for all $a \in \mathbb{F}_q$, as a function, we can work only on permutation polynomials modulo $x^q - x$, namely polynomials of degree $< q$. We record a further result on degree of permutation polynomials in:

Theorem 2.1.1. *[?] If $f(x)$ is a permutation polynomial over $\mathbb{F}_q$, then*

$$\deg(f(x)^t \bmod (x^q - x)) \leq q - 2$$

for all $t \leq q - 2$ and $\gcd(t, q) = 1$.

The following result characterizes permutation polynomials over finite fields of characteristic greater than 3.

Theorem 2.1.2. *Let q be a power of prime $p > 3$ and $f(x) = x^3 - ax + b$ a cubic polynomial over $\mathbb{F}_q$. Then f is a permutation polynomial if and only if* $\gcd(3, q-1) = 1$ *and* $a = 0$.

Proof. By Theorem 1.0.2 (1), it suffices to consider only when $b = 0$, i.e. $f(x) = x^3 - ax$. Assume that $a \neq 0$.

Case 1. $q \equiv 1 \mod 3$. Then $q - 1 = 3n$ for some $n \in \mathbb{N}$. We have $\gcd(n, q) = 1$ and $n < q - 2$. Also, $\deg(f(x)^n) = \deg(x^3 - ax)^n = 3n = q - 1 > q - 2$.

Case 2. $q \equiv 2 \mod 3$. Then $q - 2 = 3n$ for some $n \in \mathbb{N}$, so $q + 1 = 3(n+1)$. Thus, $\gcd(n+1, q) = 1$ and $n + 1 < q - 2$. Observe that

$$\begin{aligned} f(x)^{n+1} &= (x^3 - ax)^{n+1} \\ &= x^{3(n+1)} - (n+1)ax^{3n+1} + \text{ lower terms} \\ &\equiv -(n+1)ax^{3n+1} + \text{ lower terms} \mod x^q - x. \end{aligned}$$

Since $x^{3(n+1)} = x^{q+1} \equiv x^2 \mod x^q - x$. From $a \neq 0$ and $\gcd(n+1, q) = 1$, we conclude that $\deg(f(x)^{n+1} \mod x^q - x) = 3n + 1 = q - 1 > q - 2$.

Hence, both cases contradict Theorem 2.1.1, so $f(x) = x^3 - ax$ is not a permutation polynomial if $a \neq 0$. That is, $f(x) = x^3$ is the only permutation polynomial of this form. By Theorem 1.0.2, we also have $\gcd(3, q-1) = 1$.

The converse of this theorem follows directly from Theorem 1.0.2 (1) and (2). This completes our proof. $\square$

Finally, we count the number of points of $E(\mathbb{F}_q)$ for the elliptic curve $E : y^2 =$

$f(x) = x^3 + b$, $b \in \mathbb{F}_q$, where q is odd greater than 3, and determine its group structure. Observe that for each $x \in \mathbb{F}_q$, if

$$f(x) = \begin{cases} 0, & \text{then } (x,0) \text{ occurs in } E(\mathbb{F}_q); \\ r^2, & \text{then } (x,r) \text{ and } (x,-r) \text{ occur in } E(\mathbb{F}_q); \\ c, & \text{then there is no rational point in } E(\mathbb{F}_q), \end{cases}$$

where c is a non-square. Thus, in terms of χ, the quadratic character of $\mathbb{F}_q$, we obtain

$$|E(\mathbb{F}_q)| = 1 + \sum_{x\in\mathbb{F}_q}(1 + \chi(f(x))) = 1 + q + \sum_{x\in\mathbb{F}_q}\chi(f(x)).$$

Since $f(x)$ is a permutation polynomial, $\sum_{x\in\mathbb{F}_q}\chi(f(x)) = \sum_{x\in\mathbb{F}_q}\chi(x) = 0$. This implies $|E(\mathbb{F}_q)| = q + 1$.

From Theorem 1.0.1 (2), we know that $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ for some positive integers n_1 and n_2, and n_1 divides $\gcd(n_2, q-1)$. Since n_1 divides $|E(\mathbb{F}_q)| = q+1$, $n_1 = 1$ or 2. Assume that $n_1 = 2$. Then $E(\mathbb{F}_q) \cong \mathbb{Z}_2 \times \mathbb{Z}_{n_2}$ which contains 3 points of order two. Since $f(x) = x^3 + b$ has only one root in $\mathbb{F}_q$, say a, $(a, 0)$ is the unique double point in $E(\mathbb{F}_q)$. This contradiction gives $n_1 = 1$. Hence, $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_2}$. Therefore, we have shown:

Theorem 2.1.3. *Let $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{F}_q$. Then $E(\mathbb{F}_q)$ is a cyclic group of order $q+1$, i.e. $E(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$.*

2.2 Elliptic Curves with Permutation Polynomials over the Ring of Integers Modulo n

To extend the study, we consider elliptic curves with permutation polynomials over the ring of integers modulo n, where $n > 1$ is not prime. We start with the necessary and sufficient conditions to determine a cubic permutation polynomial over the ring $\mathbb{Z}_n$.

Theorem 2.2.1. *Let R_1 and R_2 be finite commutative rings, f a permutation polynomial over $R_1 \times R_2$. Then $f(R_1 \times \{0\}) = R_1 \times \{0\}$ and $f(\{0\} \times R_2) = \{0\} \times R_2$. In other words, f is also a permutation polynomial on the subrings $R_1 \times \{0\}$ and $\{0\} \times R_2$.*

Proof. Let $f(x) = \displaystyle\sum_{i=1}^{n} (a_i, b_i)x^i$ where $(a_i, b_i) \in R_1 \times R_2$. Since

$$f(r, 0) = \sum_{i=1}^{n} (a_i, b_i)(r, 0)^i = \sum_{i=1}^{n} (a_i r^i, 0) \in R_1 \times \{0\}$$

for all $r \in R_1$ and f is an injection, we have f is a bijection on $R_1 \times \{0\}$. The proof is similar for $\{0\} \times R_2$. $\square$

From the Chinese remainder theorem, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times ... \times \mathbb{Z}_{p_k^{r_k}}$, where $n = \prod_{i=1}^{k} {p_i}^{r_i}$. Using Theorem 2.2.1, we have the following results.

Theorem 2.2.2. *For any $n = \prod_{i=1}^{k} {p_i}^{r_i}$, $f(x)$ is a permutation polynomial over the ring of integers modulo n if and only if $f(x)$ is also a permutation polynomials over the rings of integers modulo $p_i^{r_i}$ for all i.*

Hence, it suffices to consider only a permutation polynomial over the rings $\mathbb{Z}_{p^r}$ studied in [**?**].

Theorem 2.2.3. *[**?**] If $f(x) = ax^3 - bx + c$ is a permutation polynomial over $\mathbb{Z}_{p^r}$, where $p > 3$ is a prime, then $r = 1$, $p \equiv 2 \mod 3$, $b = 0$ and $a \in \mathbb{Z}_{p^r}^{\times}$.*

This theorem yields an immediate corollary.

Corollary 2.2.4. *If there is an elliptic curve with a permutation polynomial over a ring of integers modulo n, then n is an odd square-free integer whose prime divisor is congruent to 2 modulo 3.*

We then work only the case of an elliptic curve with permutation polynomial over the ring $\mathbb{Z}_n$, that is, $n = \prod_{i=1}^{k} p_i$, where $p_i < p_{i+1}$ are odd primes which are congruent to 2 modulo 3. Let $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{Z}_n$. To define a group operation on $E(\mathbb{Z}_n)$, we apply the projections $\pi_i : P = (x, y) \mod n \mapsto P_{p_i} = (x, y) \mod p_i$ for all i. Using the Chinese remainder theorem, we know that the homomorphism $\pi = (\pi_1, \ldots, \pi_k) : E(\mathbb{Z}_n) \to E(\mathbb{Z}_{p_1}) \times \cdots \times E(\mathbb{Z}_{p_k})$ is a bijection. Thus, an addition $+$ for $E(\mathbb{Z}_n)$ can be defined by using the addition on $E(\mathbb{Z}_{p_i})$ and the projection map π.

The final theorem gives the group structure of an elliptic curve with permutation polynomial over $\mathbb{Z}_n$. Its proof is evident from the above observation.

Theorem 2.2.5. *Let $n = \prod_{i=1}^{k} p_i$, where $p_i < p_{i+1}$ are odd primes which are congruent to 2 modulo 3 and $E : y^2 = x^3 + b$ be an elliptic curve with permutation* *polynomial over* $\mathbb{Z}_n$. *Then*

$$E(\mathbb{Z}_n) \cong \mathbb{Z}_{p_1+1} \times \cdots \times \mathbb{Z}_{p_k+1}.$$

2.3 Elliptic Curves with Permutation Polynomials over the Ring of Gaussian Integers Modulo α

In this section, we consider elliptic curves with permutation polynomials over the rings of Gaussian integers modulo a nonzero nonunit $\alpha \in \mathbb{Z}[i]$. We start by determining cubic permutation polynomials over the ring $\mathbb{Z}[i]/(\pi^n)$, where π is a prime in $\mathbb{Z}[i]$ and n is a positive integer. Then we apply the Chinese remainder theorem to find necessary and sufficient conditions for the existence of a permutation polynomial over $\mathbb{Z}[i]/(\alpha)$, where α is a nonzero nonunit Gaussian integer. Finally, we end this section by classiflying elliptic curves with permutation polynomials over this ring.

Again, from the Chinese remainder theorem, we have $\mathbb{Z}[i]/(\alpha) \cong \mathbb{Z}[i]/(\pi_1^{r_1}) \times \cdots \times \mathbb{Z}[i]/(\pi_k^{r_k})$, where $\alpha = \prod_{j=1}^{k} \pi_j{}^{r_j}$ and π is a prime in $\mathbb{Z}[i]$. Applying Theorem 2.2.1 leads to the next theorem.

Theorem 2.3.1. *For any* $\alpha = \prod_{j=1}^{k} \pi_j{}^{r_j}$ *where* π *is a prime in* $\mathbb{Z}[i]$, $f(x)$ *is a permutation polynomial over the ring of Gaussian integers modulo* α *if and only if* $f(x)$ *is also a permutation polynomial over the rings of Gaussian integers modulo* $\pi_j^{r_j}$ *for all* j.

Therefore, it suffices to consider only a permutation polynomials over the ring $\mathbb{Z}[i]/(\pi^r)$. Write $N(\alpha) = |\alpha|^2$ for the *norm* of α.

Lemma 2.3.2. (Hensel's lemma on Gaussian integers) *Let $f(x)$ be a polynomial over $\mathbb{Z}[i]$, π a prime in $\mathbb{Z}[i]$ and n a positive integer. Then the number of the solutions of*

$$f(x) \equiv 0 \mod \pi^n \tag{2.3.1}$$

corresponding to the solution z of

$$f(x) \equiv 0 \mod \pi^{n-1} \tag{2.3.2}$$

is

(a) none, if $f'(z) \equiv 0 \mod \pi$ and z is not a solution of (2.3.1);

(b) one, if $f'(z) \not\equiv 0 \mod \pi$;

(c) $N(\pi)$, if $f'(z) \equiv 0 \mod \pi$ and z is a solution of (2.3.1).

Proof. Let $z \in \mathbb{Z}[i]$ be a root of (2.3.2) with $N(z) < N(\pi^{n-1})$ and s a Gaussian integer with $N(s) < N(\pi)$. Then we construct $w = z + s\pi^{n-1}$. By considering the Taylor's series of $f(x)$ around z, we have

$$\begin{aligned} f(w) = f(z + s\pi^{n-1}) &= f(z) + (s\pi^{n-1})f'(z) + \frac{(s\pi^{n-1})^2}{2!}f''(z) + \dots \\ &\equiv f(z) + (s\pi^{n-1})f'(z) \mod \pi^n \end{aligned}$$

since π^n divides $\frac{(s\pi^{n-1})^k}{k!} f^{(k)}(z)$ where $k > 1$. Then w is a root of (2.3.1) if and only if

$$f(z) \equiv -(s\pi^{n-1})f'(z) \mod \pi^n$$

or

$$\frac{f(z)}{\pi^{n-1}} \equiv -sf'(z) \mod \pi.$$

We now distinguish two cases.

Case 1 $f'(z) \not\equiv 0 \mod \pi$. Then $s = \frac{f(z)}{f'(z)\pi^{n-1}}$ is the unique Gaussian integer with $N(s) < N(\pi)$ which makes $w = z + s\pi^{n-1}$ a root of (2.3.1).

Case 2 $f'(z) \equiv 0 \mod \pi$. Then any Gaussian integer s could make $w = z + s\pi^{n-1}$ a root of (2.3.1), that is, $f(x)$ has distinct $N(\pi)$ roots in $\mathbb{Z}[i]/(\pi^n)$. □

Lemma 2.3.3. *Let π be a prime in $\mathbb{Z}[i]$, n a positive integer and $f(x)$ a polynomial over $\mathbb{Z}[i]$. Then $f(x)$ permutes the elements of $\mathbb{Z}[i]/(\pi^n)$, $n > 1$, if and only if it permutes the elements of $\mathbb{Z}[i]/(\pi)$ and $f'(z) \not\equiv 0 \mod \pi$ for every quadratic integer z in $\mathbb{Z}[i]$.*

Proof. Suppose $f(x)$ permutes the elements of $\mathbb{Z}[i]/(\pi^n)$, $n > 1$. That is $f(x)$ is onto $\mathbb{Z}[i]/(\pi^n)$. Thus $f(x)$ is also an onto map over $\mathbb{Z}[i]/(\pi)$. Since $\mathbb{Z}[i]/(\pi)$ is finite, $f(x)$ must be a permutation polynomial on $\mathbb{Z}[i]/(\pi)$. To consider $f'(a)$, $a \in \mathbb{Z}[i]/(\pi)$, we can see, by Lemma 2.3.2, that $f(x)$ cannot has exactly one root in $\mathbb{Z}[i]/(\pi^n)$ if $f'(\alpha) \equiv 0 \mod \pi$ for some $\alpha \in \mathbb{Z}[i]/(\pi)$.

Conversely, suppose that z is the root of

$$f(x) \equiv 0 \mod \pi$$

satisfying $0 < N(z) < N(\pi)$ and $f'(z) \equiv 0 \mod \pi$. Then, according to Lemma 2.3.2, $f(x) \equiv 0 \mod \pi^2$ has exactly one root corresponding to z. Repeating the argument we obtain $f(x) \equiv 0 \mod \pi^n$ has exactly one root corresponding to the solution z of $f(x) \equiv 0 \mod \pi$ for every $n > 1$. By replacing $f(x)$ with $f(x) - \alpha$ where α is an arbitary element in $\mathbb{Z}[i]$, we have f is a bijection over $\mathbb{Z}[i]/(\pi^n)$. $\square$

Remark. We follow the ideas of [?] on $\mathbb{Z}$ in showing Theorem 2.3.1, Lemmas 2.3.2 and 2.3.3 on the ring of Gaussian integers.

Theorem 2.3.4. *If $f(x) = ax^3 - bx + c$ is a permutation polynomial over $\mathbb{Z}[i]/(\pi^r)$, where π is a prime in $\mathbb{Z}[i]$ with $N(\pi) > 3$ and r is a positive integer, then $r = 1$, $N(\pi) \equiv 2 \mod 3$, $b = 0$ and $a \in (\mathbb{Z}[i]/(\pi^r))^\times$.*

Proof. If $r > 1$, by Lemma 2.3.3, f must be a permutation polynomial over $\mathbb{Z}[i]/(\pi)$ which is a field. By Theorem 1.0.2, $b \equiv 0 \mod \pi$. Then $f'(0) \equiv 0 \mod \pi$ which is contary to Lemma 2.3.3. Therefore $r = 1$, this means f is a cubic permutation polynomial over the field $\mathbb{Z}[i]/(\pi)$ which makes $b \equiv 0 \mod \pi$ by Theorem 1.0.2 and $a \in (\mathbb{Z}[i]/(\pi^r))^\times$. $\square$

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

The primes in $\mathbb{Z}[i]$ are characterized in the folllowing theorem.

Theorem 2.3.5. *[?] Up to multiplication by units, the primes π in $\mathbb{Z}[i]$ are of three types:*

(i) $\pi = a + bi$ or $\pi = b + ai$, where $N(\pi) = p = a^2 + b^2$ is a prime in $\mathbb{Z}$ and $p \equiv 1 \mod 4$;

(ii) $\pi = p$, *where* p *is a prime in* $\mathbb{Z}$ *and* $p \equiv 3 \mod 4$;

(iii) $\pi = 1 + i$.

By the above theorem, π is a prime in $\mathbb{Z}[i]$ with $N(\pi) > 3$ and $N(\pi) \equiv 2 \mod 3$ if and only if $\pi = a + bi$ or $b + ai$, where $N(\pi) = p = a^2 + b^2$ is a prime in $\mathbb{Z}$ and $p \equiv 1 \mod 4$. Hence, we have the following corollaries.

Corollary 2.3.6. *Let* π *be a prime in* $\mathbb{Z}[i]$ *with* $N(\pi) > 3$. *Then* $N(\pi) \equiv 2 \mod 3$ *if and only if* $\pi = a + bi$ *or* $b + ai$, *where* $N(\pi) = p = a^2 + b^2$ *is a prime in* $\mathbb{Z}$ *congruent to* 5 *modulo* 12.

Proof. If $\pi = p$ is an odd prime in $\mathbb{Z}$ and $p \equiv 3 \mod 4$, then $N(\pi) = p^2 \equiv 1 \mod 3$, so by Theorem 2.3.5, we have $\pi = a + bi$ or $b + ai$, where $N(\pi) = a^2 + b^2 = p \equiv 1 \mod 4$. Thus, $N(\pi) \equiv 2 \mod 3$ and $N(\pi) \equiv 1 \mod 4$, so $N(\pi) \equiv 5 \mod 12$. The converse is clear. $\square$

Corollary 2.3.7. *If there is an elliptic curve with a permutation polynomial over a ring of Gaussian integers modulo* α, *then* α *is square-free product of Gaussian primes whose norms are primes in* $\mathbb{Z}$ *congruent to* 5 *modulo* 12.

Our work mainly concerns the case of elliptic curves with permutation polynomials so the ring we are interested is $\mathbb{Z}[i]/(\alpha)$, where α satisfies the condition of Corrollary 2.3.7. Let $E : y^2 = x^3 + b$ be an elliptic curve with permutation polynomial over $\mathbb{Z}[i]/(\alpha)$. We can define a group operation on $\mathbb{Z}[i]/(\alpha)$ based on the structure of an elliptic curve over finite fields similar to the definition over $\mathbb{Z}_n$

in the previous section. The next corollary is obtained from combining Theorem 2.1.3 and Corollary 2.3.7.

Corollary 2.3.8. *Let* $\alpha = \prod_{j=1}^{k} \pi_j$, *where* π_j *is a Gaussian prime whose norm is a prime integer* p_j *congruent to* 5 *modulo* 12 *for all* $j \in \{1, ..., k\}$ *and let* $E : y^2 = x^3 + b$ *be an elliptic curve with permutation polynomial over* $\mathbb{Z}[i]/(\alpha)$. *Then*

$$E(\mathbb{Z}[i]/(\alpha)) \cong E(\mathbb{Z}[i]/(\pi_1)) \times \cdots \times E(\mathbb{Z}[i]/(\pi_k)) \cong \mathbb{Z}_{p_1+1} \times \cdots \times \mathbb{Z}_{p_k+1}.$$

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER III

SHIFT-INVARIANT ELLIPTIC CURVES

3.1 Permutation Polynomials in Two Variables

In this section, we study permutation polynomials in two variables over a finite ring. Let $f(x, y)$ be a polynomial in two variables with coefficients in a finite ring R. We say that f is a *weak permutation polynomial* if for every r in R, the inverse image of r under f is of cardinality $|R|$. We begin with a simple form of weak permutation polynomials over a finite field.

Theorem 3.1.1. *Let R be a finite ring. Let $g(y)$ and $f(x)$ be polynomials in $R[x, y]$. Then a polynomial in two variables $g(y) - f(x)$ is a weak permutation polynomial if $f(x)$ or $g(y)$ is a permutation polynomial over R.*

Proof. First, notice that for any permutation polynomial $p(x)$, the map $\phi : \{(x, y) \in R \times R \mid g(y) = p(x)\} \to R$ defined by $\phi(x, y) = y$ is a bijection. This makes $|\{(x, y) \in R \times R \mid g(y) = p(x)\}| = |R|$.

Without loss of generality, suppose $f(x)$ is a permutation polynomial. To show that $g(y) - f(x)$ is weak, we determine the cardinality of $\{(x, y) \in R \times R \mid g(y) - f(x) = r\}$ for an arbitrary r in R. Since $f(x) + r$ is also a permutation polynomial, we have

$$\left|\{(x,y)\in R\times R \mid g(y)-f(x)=r\}\right| = \left|\{(x,y)\in R\times R \mid g(y)=f(x)+r\}\right| = |R|,$$

for all $r \in R$. $\square$

Corollary 3.1.2. *1. If $E : y^2 = f(x)$ is an elliptic curve with permutation polynomial over $\mathbb{F}_q$, then $y^2 - f(x)$ is a weak permutation polynomial in $\mathbb{F}_q[x,y]$.*

2. If $E : y^2 = f(x)$ is an elliptic curve with permutation polynomial over $\mathbb{Z}_n$, then $y^2 - f(x)$ is a weak permutation polynomial in $\mathbb{Z}_n[x,y]$.

3. If $E : y^2 = f(x)$ is an elliptic curve with permutation polynomial over $\mathbb{Z}[i]/(\alpha)$, then $y^2 - f(x)$ is a weak permutation polynomial in $\mathbb{Z}[i]/(\alpha)[x,y]$.

3.2 Shift-invariant Elliptic Curves

For any elliptic curve $E : y^2 = f(x)$ and $a \in \mathbb{F}_q$, we let E_a denote the *a-shifted elliptic curve*, $y^2 = f(x) + a$. The previous corollary shows an interesting property of elliptic curves with permutation polynomials. Together with Theorem 2.1.3, we can see that $E(\mathbb{F}_q) \cong E_a(\mathbb{F}_q)$ for every a in $\mathbb{F}_q$, this leads us to define a *shift-invariant elliptic curve* as an elliptic curve E whose numbers of its rational points do not change when it is shifted by any constant in $\mathbb{F}_q$. Also, we may define a shift-invariant elliptic curve on $\mathbb{Z}_n$ and $\mathbb{Z}[i]/(\alpha)$ in the same way.

Theorem 3.2.1. *An elliptic curve E over a finite field $\mathbb{F}_q$ whose characteristic is greater than 3 is a shift-invariant elliptic curve if and only if it is an elliptic curve with permutation polynomial.*

Proof. Let $E : y^2 = f(x)$ be a shift-invariant elliptic curve. Then for any a in $\mathbb{F}_q$, the cardinality of the set of rational points of E_a must be the same, say $K \in \mathbb{N} \cup \{0\}$. For each $c \in f(\mathbb{F}_q)$, the image of $\mathbb{F}_q$ under f, let $n_c = |f^{-1}(c)|$. Note that $\sum_{c \in f(\mathbb{F}_q)} n_c = |\mathbb{F}_q| = q$.

Assume that $0 \notin f(\mathbb{F}_q)$. Then for any $c \in f(\mathbb{F}_q)$, $\chi(c) = 1$ or -1. Thus,

$$K = \sum_{c \in f(\mathbb{F}_q)} (1 + \chi(c)) = 2 \sum_{\substack{c \in f(\mathbb{F}_q) \\ \chi(c)=1}} n_c$$

must be even. For each $a \in f(\mathbb{F}_q)$, $0 \in f_{-a}(\mathbb{F}_q)$, the image set of $f(x) - a$. We then consider rational points of E_{-a} to obtain

$$K = \sum_{c \in f_{-a}(\mathbb{F}_q)} (1 + \chi(c)) = \sum_{\substack{c \in f_{-a}(\mathbb{F}_q) \\ \chi(c)=0}} (1 + \chi(c)) + \sum_{\substack{c \in f_{-a}(\mathbb{F}_q) \\ \chi(c)=1}} (1 + \chi(c))$$

$$= n_a + 2 \sum_{\substack{c \in f_{-a}(\mathbb{F}_q) \\ \chi(c)=1}} n_c$$

which forces n_a be even for any arbitrary a in $f(\mathbb{F}_q)$. This is contrary to the fact that $\sum_{c \in f(\mathbb{F}_q)} n_c = q$ is odd. Hence, $0 \in f(\mathbb{F}_q)$.

Finally, suppose f is not onto and let $b \notin f(\mathbb{F}_q)$. Counting rational points of E_{-b} gives $0 \notin f_{-b}(\mathbb{F}_q)$. Thus, $K = 2 \sum_{\substack{c \in f_{-b}(\mathbb{F}_q) \\ \chi(c)=1}} n_c$ and when we count rational points of E_{-a}, we still get $K = n_a + 2 \sum_{\substack{c \in f_{-a}(\mathbb{F}_q) \\ \chi(c)=1}} n_c$ for every a in $f(\mathbb{F}_q)$. A contradiction occurs in the same way because $\sum_{c\in f(\mathbb{F}_q)} n_c = q$ is odd. The opposite direction is clear. $\square$

Next, we study a shift-invariant elliptic curve $E : y^2 = f(x)$ on the ring of integers modulo n. For any $r \in \mathbb{Z}_n$, the cardinality of the set of rational points of E_r must equal the same constant K. Let $N_f(r) = |f^{-1}(r)|$ and let $s(r)$ be the number of roots of the equation $y^2 = r$ in $\mathbb{Z}_n$. We have

$$K = \sum_{r\in f(\mathbb{Z}_n)} s(r)\cdot N_f(r) = \sum_{(r+a)\in f_a(\mathbb{Z}_n)} s(r+a)\cdot N_{f+a}(r+a)$$

when E is shifted by a constant $a \in \mathbb{Z}_n$. Moreover,

$$\sum_{r\in\mathbb{Z}_n} s(r) = \sum_{r\in\mathbb{Z}_n} |\{y\in\mathbb{Z}_n : y^2 = r\}| = \left|\bigcup_{r\in\mathbb{Z}_n}\{y\in\mathbb{Z}_n : y^2 = r\}\right| = |\mathbb{Z}_n| = n.$$

Note that for all $r \in \mathbb{Z}_n$, $N_{f+a}(r+a) = N_f(r)$ and $\sum_{r\in f(\mathbb{Z}_n)} N_f(r) = \left|\bigcup_{r\in\mathbb{Z}_n} f^{-1}(r)\right| = |\mathbb{Z}_n| = n$.

To answer the next question *"Is there any shift-invariant elliptic curve in the ring of integer modulo n?"*. By the Chinese remainder theorem, it suffices to work only with the case n is a prime power. The following theorem gives us the number of square roots of an element in this type of ring.

Lemma 3.2.2 (Gauss, D.A., art.104 [?]). *Let p be an odd prime, n a positive integer, a a residue modulo p^n and $s(a)$ denote the number of square roots of a. Then*

(i) for $a = p^k t$ where $0 \le k < n$ and $p \nmid t$, if a is a quadratic residue, then k is even and $s(a) = 2p^{k/2}$, and

(iii) if $a \equiv 0 \mod p^n$*, then* $s(a) = p^{n-\lceil \frac{n}{2} \rceil}$.

In particular, $s(a)$ *is odd if and only if* $a \equiv 0 \mod p^n$.

The technique used in the proof Theorem 3.2.1 can be extended to prove the next theorem which describes a shift-invariant elliptic curve over the ring of integers modulo n.

Theorem 3.2.3. *Let* $n = \prod_{i=1}^{k} {p_i}^{n_i}$ *where* $p_i > 3$ *for all* i*. Then an elliptic curve* E *over a ring of integers modulo* n *is a shift-invariant elliptic curve if and only if it is an elliptic curve with permutation polynomial.*

Proof. In $\mathbb{Z}_{{p_i}^{n_i}}$, we know from the previous theorem that 0 is the only residue whose number of square roots is odd. Thus the equation

$$\vec{y}^2 = (y_1^2, y_2^2, \ldots, y_k^2) = (a_1, a_2, \ldots, a_k)$$

in $\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}} \cong \mathbb{Z}_n$ has odd roots only when $a_i = 0$ for all i. Suppose on the contrary that $(0, 0, \ldots, 0) \notin f(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}})$. Then

$$K = \sum_{\vec{r} \in f(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}})} s(\vec{r}) \cdot N_f(\vec{r})$$

is even. Shifting with $-\vec{s}$ gives

$$N_f(\vec{s}) = N_{f_{-\vec{s}}}(\vec{0}) = K - \sum_{\substack{\vec{r} \in f_{-\vec{s}}(\prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}}) \\ \vec{r} \neq (0,0,\ldots,0)}} s(\vec{r}) \cdot N_{f_{-\vec{s}}}(\vec{r})$$

which are even for all $\vec{s} \in \prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{n_i}}$. On the other hand, $\sum_{\vec{s} \in f(\mathbb{Z}_{{p_i}^{n_i}})} N_f(\vec{s}) = \prod_{i=1}^{k} {p_i}^{n_i} = n$ is odd. Hence, $(0, 0, \ldots, 0)$ is in the image of f. Again, f must be onto unless $(0,0,\ldots,0) \notin f_{-\vec{t}}(\prod_{i=1}^{k} \mathbb{Z}_{p_i{}^{n_i}})$ for some $\vec{t} \in \prod_{i=1}^{k} \mathbb{Z}_{p_i{}^{n_i}}$ which leads to a contradiction in the same way. This completes the proof. $\square$

Together with Corollary 2.2.4, we may conclude from Theorem 3.2.3 that:

Corollary 3.2.4. *If there is a shift-invariant elliptic curve over a ring of integers modulo n, then n is an odd composite square-free integer whose prime divisor is congruent to 2 modulo 3.*

We finish our work by giving similar results in the ring of Gaussian integers modulo α where α is in $\mathbb{Z}[i]$. Again, we start by a lemma involving the number of square in $\mathbb{Z}[i]/(\pi^k)$ where π is a Gaussian prime and k is a positive integer.

Lemma 3.2.5. *Let π be a Gaussian prime whose norm is not 2 or 9, n a positive integer, α a Gaussian integer and $s(\alpha)$ denote the number of square roots of α modulo π^n. Then*

(i) for $\alpha = \pi^k\gamma$ where $0 \leq k < n$ and $\pi \nmid \gamma$, if α is a quadratic residue, then k is even and $s(\alpha) = 2N(\pi^{k/2})$, and

(ii) if $\alpha \equiv 0 \mod \pi^n$, then $s(\alpha) = N(\pi^{n-\lceil \frac{n}{2} \rceil})$.

In particular, $s(\alpha)$ is odd if and only if $\alpha \equiv 0 \mod \pi^n$.

Proof. (i) Assume $\alpha = \pi^k\gamma$ is a quadratic residue. Then there exists β in $\mathbb{Z}[i]$ such that $\beta^2 \equiv \alpha = \pi^k\gamma \mod \pi^n$. This means $\beta^2 - \pi^k\gamma = \pi^n\delta$ for some δ in $\mathbb{Z}[i]$, thus $\beta^2 = \pi^k(\gamma + \pi^{n-k}\delta)$. Since $\pi \nmid (\gamma + \pi^{n-k}\delta)$, by the unique factorization of Gaussian integers, k must be even. Hence we write $k = 2u, u \in \mathbb{Z}$.

Case 1 $u = 0$. This means π does not divide α, then $h(x) = x^2$ is a homomorphism on $(\mathbb{Z}[i]/(\pi^n))^\times$. Thus, $s(\alpha) = |\ker(h)| = s(1) = 2$.

Case 2 $u \neq 0$. Then $\alpha = \pi^{2u}\gamma$ and we can see that γ is also a quadratic residue modulo π^n thus we write $\gamma \equiv \eta^2 \mod \pi^n$ for some $\eta \in \mathbb{Z}[i]$. Since $\pi^u \mid \beta$, we can write $\beta = \pi^u\sigma$ for some $\sigma \in \mathbb{Z}[i]$. To count $s(\alpha)$, we first show that π^{n-u} divides $\beta - \eta\pi^u$ or $\beta + \eta\pi^u$. Since $\beta^2 \equiv \alpha \mod \pi^n$, $\beta^2 - \alpha$ is divided by π^n, that is, $\pi^n \mid (\sigma^2 - \gamma)\pi^{2u}$. Hence $\pi^{n-u} \mid (\sigma^2 - \eta^2)\pi^u = (\sigma - \eta)(\sigma + \eta)\pi^u$. Since π is a prime which is not a divisor of σ or η , either $\pi \mid (\sigma + \eta)$ or $\pi \mid (\sigma - \eta)$. Consequently, we have π^{n-u} divides either $\beta - \eta\pi^u$ or $\beta + \eta\pi^u$. Next, we consider the case $\pi^{n-u} \mid \beta - \eta\pi^u$. We can see that all square root β of α are of the form $\xi\pi^{n-u} + \eta\pi^u$ where $\xi \in \mathbb{Z}[i]$. So there are totally $N(\pi^u)$ different elements of this form in $\mathbb{Z}[i]/(\pi^n)$. By considering together with the choice of η we have $s(\alpha) = 2N(\pi^u)$. It can be proven similary in the case $\pi^{n-u} \mid \beta + \eta\pi^u$.

(ii) π^n divides α. Then all square roots α are divisible by $\pi^{\lceil \frac{n}{2} \rceil}$. Thus they are of the form $\pi^{\lceil \frac{n}{2} \rceil}\delta$ where $N(\delta) \leq N(\pi^{n-\lceil \frac{n}{2} \rceil})$. Hence $s(\alpha) = N(\pi^{n-\lceil \frac{n}{2} \rceil})$, as required.

□

Finally, we can similarly prove Theorem 3.2.3 using the fact that 0 is the only residue in $\mathbb{Z}[i]/(\pi^n)$ whose number of square roots is odd to obtain the final result.

Theorem 3.2.6. *Let $\alpha = \prod_{i=1}^{k} \pi_i^{n_i}$ where $N(\pi_i) > 3$ for all i. Then an elliptic curve E over a ring of Gaussian integers modulo α is a shift-invariant elliptic curve if and only if it is an elliptic curve with permutation polynomial.*

Together with Corollary 2.3.7, we may conclude that:

Corollary 3.2.7. *If there is a shift-invariant elliptic curve over a ring of Gaussian integers modulo α, then α is square-free product of Gaussian primes whose norms are primes in $\mathbb{Z}$ congruent to* 5 *modulo* 12.

3.3 A Remark on an Elliptic Curve Cryptography

An Elliptic Curve Cryptography (ECC) is discovered in 1985 and have been used widely now as a public key cryptosystem for mobile/wireless environments. It is a secure cryptosystem with small key sizes, which results in fast computations. Its security concept is based on the difficulty of "*Elliptic Curve Discrete Logarithm Problem*" which is stated as follows:

Elliptic Curve Discrete Logarithm Problem. *Given an elliptic curve E over a finite field $\mathbb{F}_q$, and points P and Q in $E(\mathbb{F}_q) \setminus \infty$. Then find an integer n such that $nQ = P$, if such an integer exists.*

According to this problem, to construct a secure cryptosystem, it is necessary to find elliptic curves over a given finite field with a large number of points. Moreover, its group structure must not be too easy, e.g., a multiplication of small primes. Elliptic curves with permutation polynimials seem to fit for this situation. Unfortunately, it turns out that there is only one form of this type of elliptic curves, namely, $y^2 = x^3 + b$, where b is a constant, and this form is well studied and unfamous now.

However, we find in the Section3.2 that there is another advantage of elliptic curves with permutation polynimials, that is, they are a shift-invariant elliptic curve so we can generated a new cryptosystem without loss of security level by changing a constant b. Furthermore, we have proved that the shift-invariant property does not occur in any other types of elliptic curves over finite fields, the ring of integers modulo n and the ring of Guassian integers modulo α.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

REFERENCES

[1] Y. L. Chen, J. Ryu, and O. Y. Takeshita. A simple coefficient test for cubic permutation polynomials over integer rings. *IEEE Comm Lett*, 10(7):549–551, 2006.

[2] D. Coppersmith, A. M. Odlzyko, and R. Schroeppel. Discrete logarithms in GF(p). *Algorithmica*, 1(1):1–15, 1986.

[3] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans Inform Theor*, 22(6):644–654, 1976.

[4] D. S. Dummit and R. M. Foote. *Abstract Algebra*, volume 1999. Prentice Hall, 1991.

[5] C. F. Gauss. *Disquisitiones Arithmeticae, 1801. English translation by Arthur A. Clarke.* Springer-Verlag, 1986.

[6] H. W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of Math*, 126(3):649–673, 1987.

[7] R. Lidl. On cryptosystems based on polynomials and finite fields. *Lect Notes Comput Sci*, 126:10–15, 1985.

[8] R. Lidl and H. Niederreiter. *Finite Fields (Encyclopedia of Mathematics and its Applications).* Cambridge University Press, 2008.

[9] D. Liu, D. Huang, P. Luo, and Y. Dai. New schemes for sharing points on an elliptic curve. *Comput Math Appl*, 56(6):10–15, 2008.

[10] B. R. Shankar. Combinatorial properties of permutation polynomials over some finite rings $\mathbb{Z}_n$. *IJSDI age*, 1:1–6, 1985.

[11] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer Verlag, 2009.

[12] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall, 2008.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

VITA

Name	Mr. Attawut Wongpradit
Date of Birth	14 Febuary 1985
Place of Birth	Narathiwat, Thailand
Education	B.Ed. (Second Class Honours), Prince of Songkla University, 2007
Scholarship	Development and Promotion of Science and Technology talents project (DPST) supported by the Institute for the Promotion of Teaching Science and Technology (IPST).

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย