Graduate School ETD Form 9
(01/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis Acceptance

This is to certify that the thesis prepared

By Shuo Shen

Entitled Finite Fields of Low Characteristic in Elliptic Curve Crytography

Complies with University regulations and meets the standards of the Graduate School for originality and quality

For the degree of Doctor of Philosophy

Final examining committee members

Samuel Wagstaff, Chair

Andreas Stein

William Heinzer

Freydoon Shahidi

Approved by Major Professor(s): Samuel Wagstaff

Approved by Head of Graduate Program: Fabio A. Milner

Date of Graduate Program Head's Approval: 04/13/07

FINITE FIELDS OF LOW CHARACTERISTIC IN ELLIPTIC CURVE CRYPTOGRAPHY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Shuo Shen

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2007

Purdue University

West Lafayette, Indiana

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

dedicated to all of my family.

ACKNOWLEDGMENTS

I would like to express my deep gratitude to my advisor, Samuel Wagstaff, Professor of Mathematics and Computer Science at Purdue. His wide knowledge and attitude in research and study have been of great value for me. His understanding, encouragement and personal guidance have provided a good basis for the present thesis.

I am deeply grateful to my coadvisor, Professor Andreas Stein in the Department of Mathematics at the University of Wyoming, for his constant help in the research and valuable suggestions in career. I enjoyed the soccer games in Wyoming with Andreas and all the other players.

Also I am very grateful to Professor Michael Jacobson and Professor Renate Scheidler, which supervised the research project with Andreas in the summer school in Wyoming. Their constant help in and after the summer school helped me to enter a new research area.

I thank all the members of my committee, Professors Shahidi, Heinzer, Wagstaff and Stein. They always offered their kind help when I had questions. I appreciate their guidance, patience, and careful reading of this thesis.

I owe my loving thanks to my dear wife Ya Li, who is also a Ph.D student in Purdue Math Dept. Her warm support and love is my treasure of my whole life. I also deeply appreciate the help from my parents and parents in law, Furong and Manqiu, Xihai and Xiuzhi. Their unconditional help ensured my time and energy for my research. Also my lovely daughter, Xiaoyi, gave us great pleasure in my busy time.

I owe a lot of thanks to my friends; their support and friendship means a lot to me. I could always get their help during tough times.

Finally, I want to thank Jason Gower, also a student of Samuel, for his helpful comments, which I appreciate.

TABLE OF CONTENTS

ABSTRACT

Shen, Shuo Ph.D., Purdue University, May, 2007. Finite Fields of Low Characteristic in Elliptic Curve Cryptography. Major Professor: Samuel S. Wagstaff, Jr.

The use of finite fields of low characteristic can make the implementation of elliptic curve cryptography more efficient. There are two approaches to lower the characteristic of the finite field in ECC while maintaining the same security level: Elliptic curves over a finite field extension and hyperelliptic curves over a finite field. This thesis solves some problems in both approaches.

The group orders of elliptic curves over finite field extensions are described as polynomials. The irreducibility of these polynomials is proved, and hence the primality of the group orders can be studied. Asymptotic formulas for the number of traces of elliptic curves over field extensions with almost prime orders are given and a proof based on Bateman-Horn's conjecture is given. Hence the number of curves for cryptographic use is known. Experimental data is given. The formulas fit the actual data remarkably well.

Finally, the arithmetic of real hyperelliptic curves is studied. We study the algorithm for divisor addition on the real hyperlliptic curves and give the explicit formulas.

1. INTRODUCTION

1.1 Elliptic/Hyperelliptic Curve Cryptography

It is well known that the sets of rational points on elliptic curves over finite fields form finite groups and the sizes of these finite groups are of the same magnitude as the size of the base fields. Elliptic curve cryptosystems (ECC) were first proposed in 1985 independently by Neal Koblitz and Victor Miller based on the group structure of elliptic curves over finite fields. ECC's security depends on the computational complexity of the discrete logarithm problem(DLP) over elliptic curve groups, i.e., looking for m given rational points P and mP in an elliptic curve group, where m is a natural number less than the order of the elliptic curve group. Thus, large elliptic curve groups or prime order subgroups of elliptic curve groups are needed to guarantee that m can be large and the discrete logarithm problem hard. To reach the same security level[1] as 1024-bit RSA, the size of of the elliptic curve groups should be over 163 bits according to NIST guidelines for public key sizes. For more details about the ECC standard, see NIST FIPS 186-2.

The curves used in cryptography ares are those over $\mathbb{F}_{2^m}$:

$$y^2 + xy = x^3 + ax^2 + b \qquad \text{with } a, b \in \mathbb{F}_{2^m}, \tag{1.1}$$

and the elliptic curves over $\mathbb{F}_p$, where p is an odd prime greater than 3, in short Weierstrass form:

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{F}_p. \tag{1.2}$$

The use of hyperelliptic curves in cryptography was started in 1989 by Koblitz [18]. As with the elliptic curve cryptosystem, the discrete logarithm problem over the

[1] The security level usually refers to the size of key space, for example: one has to try 2^{1024} keys to launch a brute force attack on a 1024-bit security level cryptosystm.

Jacobian of hyperelliptic curves of low genus is computationally infeasible when the size of the Jacobians is large. See Müller et al. [26], Gaudry [13], Enge [10] and Theriault [34].

Hyperelliptic curves have the form $y^2 + h(x)y = f(x)$, where h and f are polynomials. The degree of f is $2g+1$ or $2g+2$ and the degree of h is no higher than $g+1$, where g is the genus of the curve; see Cohen et al. [7] for details. Formal definitions will be given in Chapter 3.

1.2 Elliptic Curves over Finite Fields

Elliptic curves over finite fields of characteristic 2 are very efficient and widely used because of their convenience in implementation, fast addition operation on binary computer systems and the key-per-bit-strength is good. But the elliptic curves with coefficients in $\mathbb{F}_2$ are very limited:

$$E(\mathbb{F}_2) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.3}$$

Of the $2^5 = 32$ possible curves, most are singular, supersingular or anomalous, which are either trivial or vulnerable curves in elliptic cryptography. $E(\mathbb{F}_{2^p})$ (p is a prime) are the most casually used elliptic curves.

The number of possible elliptic curves over a large prime order finite field $\mathbb{F}_p$ is enormous because for each integer $n \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$, we can find an elliptic curve with group order n (see Section 2.1.1). We want n to be a prime because we need a large prime order elliptic curve group to make the discrete logarithm problem hard. The number of group orders we could choose is the number of primes in $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ and the number of curves is even more than that.

Multiplications in extension fields of characteristic 2 are usually slower than in prime fields, while the the inversion in prime fields can be very expensive. To overcome these two difficulties, some optimal extension fields are explored, i.e., some special chosen small prime p and extension degree l make the extension field F_{q^l} have optimal performance in both multiplications and inversions. See Cohen et al. [7] for details. In this thesis, we generally study the amount of elliptic curves over extension fields that are possible for cryptographic use, further studies particular for the choices of p and l are expected to be done soon.

1.3 Contribution of This Thesis

Two approaches have been tried to make the algebraic operations fast while allowing many choices of elliptic curves. The first approach is to use elliptic curves over a finite field extension, with curve coefficients in a small finite field, i.e.:

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbb{F}_{q^k} \qquad (q \text{ and } k \text{ are odd primes}, A, B \in \mathbb{F}_q). \tag{1.4}$$

This type of curves over finite field extension and with coefficients in small finite field are called Koblitz curves. Group orders of such type of elliptic curves are easier to calculate and use of Frobenius equation (Theorem 2.1.2) make make scalar multiplication over such type of curves faster. See Section 2.1 for more details.

The implementation is faster than for elliptic curves over a huge prime order field and there are many more choices than for curves with binary coefficients. It turns out that the order of E in Formula (1.4) can not be prime when $k > 1$. However, the order may be "almost prime," that is, have one large prime factor near q^{k-1}. This size of order is good enough for use in cryptography.

In this thesis, we give and prove a condition for an elliptic curve over a finite field extension to have almost prime order. We also give and prove an asymptotic formula for the number of traces of elliptic curves with almost prime orders. Formulas and experimental data show that there is a huge space of such elliptic curves for use in ECC. The safety property of these curves under certain attacks is also studied.

The second approach is to use hyperelliptic curves. A hyperelliptic curve with genus g over $\mathbb{F}_q$ has Jacobian of size about q^g. To have the same size of Jacobian as the size of elliptic curve groups, the base field of a hyperelliptic curve is smaller, thus the parameters of the curve are smaller. Algorithms for imaginary hyperelliptic curves have been widely studied. In this thesis, the explicit formulas for for the addition operation for a real hyperelliptic curve is given. More improvements for algorithms for real hyperelliptic curves are being explored with other mathematicians.

1.4 Outline of the Thesis

Chapter 2 studies elliptic curves over finite field extensions. Necessary background and related material will be introduced briefly. Proofs and experimental data are given in detail. Chapter 3 focuses on the algorithms for real hyperelliptic curves. Further work in both approaches is mentioned in both chapters.

2. ELLIPTIC CURVES OVER FINITE FIELD EXTENTIONS

2.1 Background

The work in this part of the thesis was started with the counting of elliptic curves of “almost prime” order by MAGMA. It was found that the ratio $|E(\mathbb{F}_{q^k})|/|E(\mathbb{F}_q)|$ can be described by the value of an irreducible polynomial determined by q and k. This fact is proved below along with other interesting results. This expression as an irreducible polynomial makes it possible to find an asymptotic formula for the number of elliptic curves of “almost prime” order if we assume Bateman-Horn’s conjecture.

2.1.1 Basic Definitions

The classical theory of elliptic curves over a finite field is the basis of the work of this thesis. See Silverman [30] and Washington [36]. Some important related research in ECC and number theory will be introduced first.

All elliptic curves over finite fields of characteristic greater than 3 can be written in short Weierstrass normal form:

$$y^2 = x^3 + Ax + B \tag{2.1}$$

with A and B constants in some base field and the discriminant $\Delta = -4A^3 - 27B^2 \neq 0$. Modifications to the Weierstrass form must be made in characteristics 2 and 3. See Washington [36], page 11, for more details.

Let $\mathbb{F}_{q^k}$ be a finite field, $k \geq 1$ and $k \in \mathbb{Z}$. For fixed $A, B \in \mathbb{F}_{q^k}$, the set

$$E(\mathbb{F}_{q^k}) = \{\infty\} \cup \{(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \mid \; y^2 = x^3 + Ax + B\} \tag{2.2}$$

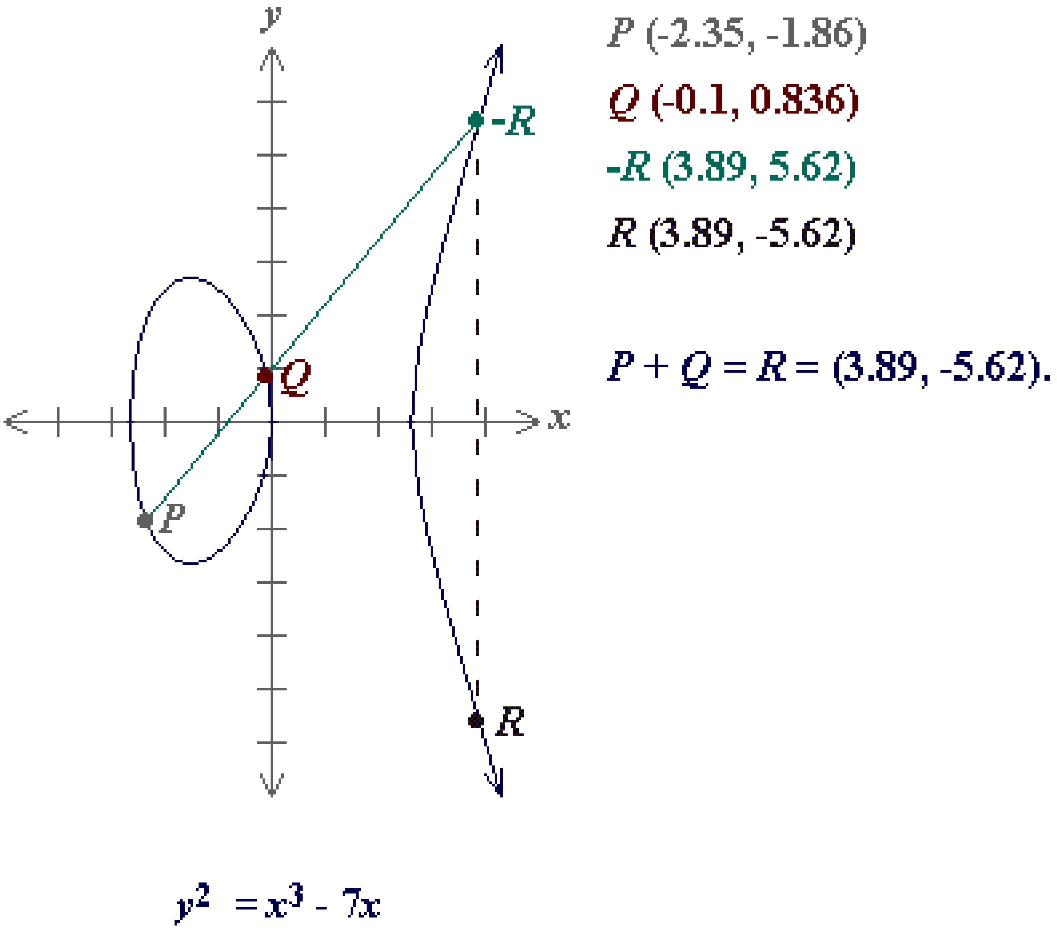

Figure 2.1. Addition on An Elliptic Curve over $\mathbb{R}$

is a finite Abelian group under an appropriate definition of addition. Since it is hard to draw meaningful pictures of elliptic curves over finite fields, for intuition, we give the graph of an elliptic curve over the real numbers and show a sample addition of points on it in Figure 2.1. Elliptic curves over finite fields have the same definition for addition as in the real case but have point coordinates restricted to a finite field.

For a natural number m and a point $P \in E(\mathbb{F}_q)$, mP means the sum of m of the same point P. Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$. Let $E = E(\overline{\mathbb{F}}_q)$.

First we consider the elliptic curve over $\mathbb{F}_q$, i.e., $k = 1$. The order of the group is bounded by this result of Hasse:

Theorem 2.1.1 *(Hasse) Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies*

$$|q+1-|E(\mathbb{F}_q)|| \leq 2\sqrt{q}. \tag{2.3}$$

See [36], Section 4.1, for a proof. This is called Hasse's bound for the order of an elliptic curve group. The trace of an elliptic curve $E(\mathbb{F}_q)$ is defined as:

$$t = q+1-|E(\mathbb{F}_q)|. \tag{2.4}$$

Let

$$\begin{aligned} \phi_q : \overline{\mathbb{F}}_q &\rightarrow \overline{\mathbb{F}}_q \\ x &\mapsto x^q \end{aligned}$$

be the Frobenius map for $\mathbb{F}_q$. Then ϕ_q acts on the points in $E(\mathbb{F}_q)$:

$$\phi_q(x,y) = (x^q, y^q), \;\; \phi_q(\infty) = \infty.$$

It is easy to see that ϕ_q is an endomorphism of $E(\mathbb{F}_q)$; see Washington [36], page 48. Here is an important property of ϕ_q:

Theorem 2.1.2 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let t be as in Formula* (2.3). *Then*

$$\phi_q^2 - t\phi_q + q = 0$$

as endomorphisms of E, and t is the unique integer s such that

$$\phi_q^2 - s\phi_q + q = 0.$$

In other words, if $(x,y) \in E(\overline{\mathbb{F}}_q)$, then

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x,y) = \infty$$

and t is the unique integer such that this relation holds for all $(x,y) \in E(\overline{\mathbb{F}}_q)$. The "$-$" and "$+$" signs denote the group operations on $E(\mathbb{F}_q)$ in the last formula.

Moreover, t is the unique integer satisfying

$$t \equiv Trace((\phi_q)_m) \ mod\ m$$

for all m with $\gcd(m,q) = 1$. $Trace((\phi_q)_m)$ is the trace of $(\phi_q)_m$, which is the matrix that describes the action of ϕ_q on $E[m] = \{P \in E(\overline{\mathbb{F}_q}) \mid mP = \infty\}$.

See Washington [36] Section 4.2 for a proof.

It is known that given the base field $\mathbb{F}_q$ and a trace value t, an elliptic curve of order $q+1-t$ can be found by the complex multiplication algorithm. For details see Morain [25] Section 5.3, Lay and Zimmer [22] or Cohen et al. [7] Section 18.1.5.

If we have an elliptic curve E defined over a small finite field $\mathbb{F}_q$, the order of $E(\mathbb{F}_{q^k})$ can be determined from $|E(\mathbb{F}_q)|$ and k because of the following theorem:

Theorem 2.1.3 *Let $E(\mathbb{F}_q)$ be the elliptic curve as defined by Formula (2.2), $A, B \in \mathbb{F}_q$ and $|E(\mathbb{F}_q)|$=$q+1-t$. Write $X^2 - tX + q = (X-\alpha)(X-\beta)$, with $\alpha, \beta \in \mathbb{C}$. Then*

$$\begin{aligned} |E(\mathbb{F}_{q^k})| &= q^k + 1 - (\alpha^k + \beta^k) && (2.5) \\ &= q^k + 1 - t_k, && (2.6) \end{aligned}$$

for all $k \geq 1$, and $t_k = \alpha^k + \beta^k$ is the trace of $E(\mathbb{F}_{q^k})$.

See Washington [36], Section 4.3, for a proof.

2.1.2 Almost Prime Order

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of q elements. Let $\mathbb{F}_{q^k}$ be an extension of $\mathbb{F}_q$ of degree k. We say that E has **almost prime order** over a degree-k extension $\mathbb{F}_{q^k}$ if

$$M_k := M_k(E/\mathbb{F}_q) = \frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|} \qquad (2.7)$$

is a prime; see Koblitz [19].

Note that $E(\mathbb{F}_{q^r})$ is a subgroup of $E(\mathbb{F}_{q^s})$ whenever $r|s$; this implies [19] that $|E(\mathbb{F}_{q^k})|$ is divisible by $|E(\mathbb{F}_q)|$, and that the ratio of these two numbers can be prime only if k is prime, except for these two cases:

Example 2.1.1 *When, $q = 2$ and $k = 4$, define a curve as:*

$$E : y^2 + y = x^3 + x.$$

Then $|E(\mathbb{F}_2)| = 5$ and $|E(\mathbb{F}_{2^4})| = 25$, thus $|E(\mathbb{F}_{2^4})|/|E(\mathbb{F}_2)| = 5$.

Example 2.1.2 *When, $q = 3$ and $k = 4$, define a curve as:*

$$E : y^2 = x^3 + 2x + 1.$$

Then $|E(\mathbb{F}_3)| = 7$ and $|E(\mathbb{F}_{3^4})| = 91$, thus $|E(\mathbb{F}_{3^4})|/|E(\mathbb{F}_3)| = 13$.

The reason for the above exceptions is that, generally, when k is a composite, the ratio M_k can be written explicitly as a product of two factors as shown in Section 2.2.2. But when q and k are small numbers, one of the factors can degenerate to be 1; thus, it's possible for M_k to be a prime in this case.

We will show, as long as k is a prime and q is large enough, there will be around $O(\sqrt{q}/((k-1)\log q)$ elliptic curves with almost prime order. We will do this by expressing the ratio in Formula (2.7) as an evaluation of an irreducible polynomial. Heuristic arguments in number theory (Bateman and Horn [4], [5]) suggest that there are many values making the value of the irreducible polynomial a prime. Thus k being a prime is almost a sufficient condition that we can find an elliptic curve $E(\mathbb{F}_{q^k})$ with almost prime order.

Further properties of the ratio of these two numbers in Formula (2.7) will be shown in next section.

2.1.3 The Bateman-Horn Conjecture

We will use a widely-accepted conjecture of Bateman and Horn to estimate the number of prime values of a polynomial $f(x)$ when $0 < x \leq B$ is an integer. We will apply this conjecture to $f(t) = M_k$ of Formula (2.7) after we express M_k as a polynomial in a variable t.

Note: All the logarithmic functions in this thesis are natural logarithmic functions. The equivalence relation "$\sim$" has this meaning: We write $f(n) \sim g(n)$ to mean $\lim_{n\to\infty} f(n)/g(n) = 1$.

Suppose f_1, f_2, …, $f_l \in \mathbb{Z}[x]$ are polynomials in one variable with all coefficients integral and leading coefficients positive. Suppose each of these polynomials is irreducible over the field of rational numbers and no two of them differ by a constant factor. Let $Q(f_1, f_2, \ldots, f_l; B)$ denote the number of integers n between 1 and B, inclusive, such that $f_1(n)$, $f_2(n)$, …, $f_l(n)$ are simultaneously prime. (Finitely many values of n for which some $f_l(i)$ is negative are ignored as $B \to \infty$. For our case, the irreducible polynomial we use always has positive value in $[1, B]$.) Bateman and Horn conjectured [4], [5]:

$$Q(f_1, f_2, \ldots, f_l; B) \sim C_{BH}(f_1, f_2, \ldots, f_l) \int_a^B \frac{du}{\log f_1(u) \log f_2(u) \cdots \log f_l(u)}, \tag{2.8}$$

where a is the first positive integer such that each of the polynomials f_1, f_2, …, f_l takes only values greater than 1 on the interval $[a, +\infty]$, and

$$C_{BH}(f_1, f_2, \ldots, f_l) = \prod_p \left\{ \left(1 - \frac{1}{p}\right)^{-l} \left(1 - \frac{\omega(p)}{p}\right) \right\}, \tag{2.9}$$

the product being taken over all primes and $\omega(p)$ being the number of solutions of the congruence

$$f_1 f_2 \cdots f_l \equiv 0 \pmod{p}. \tag{2.10}$$

If f_1, …, f_l are abelian polynomials, then $C_{BH}(f_1, f_2, \ldots, f_l)$ converges quickly and can be calculated efficiently by direct application of Formula (2.9). By an abelian polynomial we mean a polynomial such that any one of its zeros generates a normal extension of the rational numbers with an abelian Galois group.

When $l = 1$, for an irreducible polynomial f, Formula (2.8) can also be expressed as

$$Q(f; B) \sim C_{BH}(f) \int_a^B \frac{du}{\log f(u)}. \tag{2.11}$$

Bateman-Horn's conjecture is based on the fact that the chance that a large positive integer m is prime is around $1/\log m$ (Prime number theorem, see Apostol [1] for a reference). Since $f_1(n)$, $f_2(n)$, …, $f_l(n)$ are not quite random integers, a correction factor needs to be applied and $C_{BH}(f_1, f_2, \ldots, f_l)$ is the correction factor. See Bateman and Horn [4] for the details. We call $C_{BH}(f_1, f_2, \ldots, f_l)$ the Bateman-Horn constant and denote it as C_{BH} for simplicity in the experimental data later. It is shown that C_{BH} converges fast and can be easily computed when all f_i's are abelian polynomials. See Bateman and Horn [4], [5] for details. Many verifications have shown that the Formula (2.7) fits experimental data remarkably well.

Our experimental results show that the number of primes from our polynomial also fits the Bateman-Horn estimate well.

2.2 Polynomials A and B

For brevity, we let q be a prime unless otherwise specified. Thus $\mathbb{F}_q$ is a finite field with prime order. We will allow q to be a prime power in Section 2.5.

2.2.1 Irreducibility

In the following lemma we will see that $q+1-t_1|q^k+1-t_k$, where t_k is the trace of $E(\mathbb{F}_{q^k})$ for $k \geq 1$. We can express t_k inductively. Since $t_k = \alpha^k + \beta^k$, we can rewrite t_k as

$$t_k = \alpha^k + \beta^k = (\alpha+\beta)(\alpha^{k-1} + \beta^{k-1}) - \alpha\beta(\alpha^{k-2} + \beta^{k-2}).$$

Noticing the fact that $\alpha + \beta = t_1$ and $\alpha\beta = q$, we get:

$$t_1 = t_1, \tag{2.12}$$

$$t_2 = t_1^2 - 2q, \tag{2.13}$$

$$t_k = t_1 \cdot t_{k-1} - q \cdot t_{k-2}. \tag{2.14}$$

We will give an explicit formula for the ratio of the two numbers and study it as a polynomial.

Lemma 2.2.1 *As polynomials in $\mathbb{Z}[q]$, $q+1-t_1$ divides q^k+1-t_k, where t_k is the trace of $E(\mathbb{F}_{q^k})$ for $k \geq 1$.*

Proof Use mathematical induction. When $k=1$ and 2 we have:

$$\begin{aligned} q+1-t_1 &= q+1-t_1, \\ q^2+1-t_2 &= q^2+1-(t_1^2-2q) = (q+1-t_1)(q+1+t_1). \end{aligned}$$

For $k \geq 3$, assuming we already know:

$$\begin{aligned} q^{k-1}+1-t_{k-1} &= \lambda_{k-1}(q+1-t_1), \\ q^{k-2}+1-t_{k-2} &= \lambda_{k-2}(q+1-t_1), \end{aligned}$$

where the λ_j are in $\mathbb{Z}[q]$, we derive the useful formulas:

$$\begin{aligned} q^{k-1} &= \lambda_{k-1}(q+1-t_1)+t_{k-1}-1, \\ q^k &= \lambda_{k-1}q(q+1-t_1)+qt_{k-1}-q, \\ qt_{k-2} &= q^{k-1}+q-\lambda_{k-2}q(q+1-t_1). \end{aligned}$$

Using the above formulas and Formula (2.14), we get:

$$\begin{aligned} |E(\mathbb{F}_{q^k})| &= q^k+1-t_k \\ &= \lambda_{k-1}q(q+1-t_1)+qt_{k-1}-q+1-t_1t_{k-1}+qt_{k-2} \\ &= \lambda_{k-1}q(q+1-t_1)+qt_{k-1}-q+1-t_1t_{k-1}+q^{k-1}+q-\lambda_{k-2}q(q+1-t_1) \\ &= \lambda_{k-1}q(q+1-t_1)+qt_{k-1}-q+1-t_1t_{k-1}+\lambda_{k-1}(q+1-t_1) \\ &\quad +t_{k-1}-1+q-\lambda_{k-2}q(q+1-t_1) \\ &= (\lambda_{k-1}q+\lambda_{k-1}-\lambda_{k-2}q)(q+1-t_1)+qt_{k-1}-q-t_1t_{k-1}+q \\ &= (\lambda_{k-1}q+\lambda_{k-1}-\lambda_{k-2}q)(q+1-t_1)+t_{k-1}(q+1-t_1) \\ &= (\lambda_{k-1}q+\lambda_{k-1}-\lambda_{k-2}q+t_{k-1})(q+1-t_1). \end{aligned}$$

Thus,

$$\lambda_k = \lambda_{k-1}q+\lambda_{k-1}-\lambda_{k-2}q+t_{k-1}. \tag{2.15}$$

This completes the proof of the lemma. ■

To analyze the primality of the ratio in Formula (2.7), we need to express it as a polynomial.

If we let x replace t_1 and y replace q, then $q^k + 1 - (\alpha^k + \beta^k)$ becomes:

$$y^k + 1 - f_k(x, y),$$

where from Formulas (2.12), (2.13), (2.14):

$$\begin{aligned} f_1(x,y) &= x, & (2.16)\\ f_2(x,y) &= x^2 - 2y, & (2.17)\\ f_k(x,y) &= xf_{k-1}(x,y) - yf_{k-2}(x,y). & (2.18) \end{aligned}$$

In view of Lemma 2.2.1, we define:

$$\begin{aligned} A_k(x,y) &:= y^k + 1 - f_k(x,y) = (y+1-x)B_k(x,y), & (2.19)\\ \text{where}\quad B_k(x,y) &:= \frac{y^k + 1 - f_k(x,y)}{y+1-x} & (2.20) \end{aligned}$$

for some polynomial $B_k(x,y) \in \mathbb{Z}[x,y]$. Then $B_k(t_1,q)$ is the ratio in Formula (2.7). If we let $f_0(x,y) = 2$, the recurrence relation (2.18) holds for all $k \geq 2$.

Formulas for these functions are given in this simple lemma.

Lemma 2.2.2 *For any positive integer k, we have*

$$f_k(x,y) = \left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k + \left(\frac{x-\sqrt{x^2-4y}}{2}\right)^k, \quad (2.21)$$

$$A_k(x,y) = \left(\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1\right)\left(\left(\frac{x-\sqrt{x^2-4y}}{2}\right)^k - 1\right), \quad (2.22)$$

$$B_k(x,y) = \frac{\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1}{\frac{x+\sqrt{x^2-4y}}{2} - 1}\frac{\left(\frac{x-\sqrt{x^2-4y}}{2}\right)^k - 1}{\frac{x-\sqrt{x^2-4y}}{2} - 1}. \quad (2.23)$$

When k is a prime

$$B_k(x,y) = \Phi_k\left(\frac{x+\sqrt{x^2-4y}}{2}\right)\Phi_k\left(\frac{x-\sqrt{x^2-4y}}{2}\right), \quad (2.24)$$

where Φ_k is the k^{th} cyclotomic polynomial.

Proof Let

$$\alpha = \frac{x + \sqrt{x^2 - 4y}}{2}, \tag{2.25}$$

$$\beta = \frac{x - \sqrt{x^2 - 4y}}{2}. \tag{2.26}$$

Notice that $\alpha + \beta = x$ and $\alpha\beta = y$. From the recursive relation formula (2.18), f_k is a Lucas function with variables α and β (see Williams [38], Section 4.1). Then by properties of Lucas functions (see Williams [38], Section 4.1), we have:

$$f_k(x, y) = f_k(\alpha, \beta) = \alpha^k + \beta^k = \left(\frac{x + \sqrt{x^2 - 4y}}{2}\right)^k + \left(\frac{x - \sqrt{x^2 - 4y}}{2}\right)^k.$$

Then

$$\begin{aligned}
A_k(x, y) &= y^k + 1 - f_k(x, y) \\
&= \left(\frac{x + \sqrt{x^2 - 4y}}{2} \frac{x - \sqrt{x^2 - 4y}}{2}\right)^k + 1 \\
&\quad - \left(\left(\frac{x + \sqrt{x^2 - 4y}}{2}\right)^k + \left(\frac{x - \sqrt{x^2 - 4y}}{2}\right)^k\right) \\
&= \left(\left(\frac{x + \sqrt{x^2 - 4y}}{2}\right)^k - 1\right)\left(\left(\frac{x + \sqrt{x^2 - 4y}}{2}\right)^k - 1\right),
\end{aligned}$$

$$\begin{aligned}
B_k(x, y) &= \frac{y^k + 1 - f_k(x, y)}{y + 1 - x} \\
&= \frac{\left(\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1\right)\left(\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1\right)}{\frac{x+\sqrt{x^2-4y}}{2} \frac{x-\sqrt{x^2-4y}}{2} + 1 - \left(\frac{x+\sqrt{x^2-4y}}{2} + \frac{x-\sqrt{x^2-4y}}{2}\right)} \\
&= \frac{\left(\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1\right)\left(\left(\frac{x+\sqrt{x^2-4y}}{2}\right)^k - 1\right)}{\left(\frac{x+\sqrt{x^2-4y}}{2} - 1\right)\left(\frac{x-\sqrt{x^2-4y}}{2} - 1\right)}.
\end{aligned}$$

When k is a prime, it's easy to see

$$B_k(x, y) = \Phi_k\left(\frac{x + \sqrt{x^2 - 4y}}{2}\right)\Phi_k\left(\frac{x - \sqrt{x^2 - 4y}}{2}\right).$$

■

To analyze the primality of $\frac{q^k+1-t_k}{q+1-t_1} = \frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|} = M_k$, we focus on the polynomial $B_k(x,y)$. The following lemmas and theorems will show that $B_k(x,y)$ is actually an irreducible polynomial when k is an odd prime.

Lemma 2.2.3 *We have $f_n(0,y) = 0$ when n is an odd number. Also $f_n(x,0) = x^n$ for any positive integer n.*

Proof By plugging in $x = 0$ into formula (2.21) one gets

$$f_k(0,y) = \left(\sqrt{-y}\right)^k + (-1)^k \left(\sqrt{-y}\right)^k.$$

When k is odd, $(-1)^k = -1$ and the result follows.

Similarly, by plugging in $y = 0$ into Formula (2.21) one gets

$$f_k(x,0) = x^k.$$

■

Note that Formula (2.19) and Lemma 2.2.3 tell us that

$$A_k(0,y) \quad = \quad y^k + 1 - 0 \cdot f_{k-1}(0,y) - y \cdot f_{k-2}(0,y) = y^k + 1$$

for every odd positive integer k and that $A_k(x,0) = 1 - x^k$ for every positive integer k.

Lemma 2.2.4 *If k is an odd prime, then for any x and y*

$$B_k(0,y) \quad = \quad \Phi_{2k}(y), \tag{2.27}$$

$$B_k(x,0) \quad = \quad \Phi_k(x), \tag{2.28}$$

where $\Phi_{2k}(y)$ and $\Phi_k(x)$ are the $2k^{th}$ and k^{th} cyclotomic polynomials.

Proof For any odd prime k, by the remark following Lemma 2.2.3, we have $A_k(0, y) = y^k + 1$ since $k - 2$ is odd.

Then by Lemma 2.2.1

$$A_k(0, y) \quad = (1 + y)B_k(0, y).$$

So we get

$$B_k(0, y) = \frac{y^k + 1}{y + 1} = \Phi_{2k}(y)$$

for the odd prime k.

Also, by $A_k(x, 0) = 1 - x^k$ and Lemma 2.2.1,

$$A_k(x, 0) \quad = (1 - x)B_k(x, 0).$$

So we get

$$B_k(x, 0) = \frac{x^k - 1}{x - 1} = \Phi_k(x)$$

for the odd prime k. ■

Lemma 2.2.5 *The total degree of the polynomial $A_k(x, y)$ is k; the total degree of the polynomial $B_k(x, y)$ is $k - 1$ for each k. (k can be composite.)*

Proof It's easy to see from the definition of $f_k(x, y)$ (Formulas (2.16), (2.17) and (2.17)) that the total degree of $f_k(x, y)$ is k. Hence by the definitions of $A_k(x, y)$ and $B_k(x, y)$ in formulas (2.19) and (2.20), the degrees of $A_k(x, y)$ and $B_k(x, y)$ are k and $k - 1$. ■

Now we show that $B_k(x, y)$ is irreducible if k is an odd prime.

Theorem 2.2.1 *When k is an odd prime, $B_k(x, y)$ is irreducible in $\mathbb{Z}[x, y]$.*

Proof If $B_k(x, y)$ were not irreducible, then $B_k(x, y) = g(x, y)h(x, y)$, where $g(x, y)$ and $h(x, y)$ are both polynomials in $\mathbb{Z}[x, y]$ with degree at least 1. By Lemma 2.2.4,

$$\Phi_{2k}(y) = B_k(0, y) = g(0, y)h(0, y).$$

Since $\Phi_{2k}(y)$ is irreducible, without loss of generality, we have

$$\begin{aligned} g(0,y) &= \Phi_{2k}(y), & (2.29)\\ h(0,y) &= 1, & (2.30)\\ g(x,y) &= x\cdot g_0(x,y)+\Phi_{2k}(y), & (2.31)\\ h(x,y) &= x\cdot h_0(x,y)+1, & (2.32)\end{aligned}$$

where $g_0(x,y)$ and $h_0(x,y)$ are polynomials in x and y.

When we take y to be zero,

$$\begin{aligned} \Phi_k(x)=B_k(x,0) &= (x\cdot g_0(x,0)+\Phi_{2k}(0))(x\cdot h_0(x,0)+1)\\ &= (x\cdot g_0(x,0)+1)(x\cdot h_0(x,0)+1). \end{aligned}$$

Since $\Phi_k(x)$ is irreducible, either $x\cdot g_0(x,0)+1=1$ or $x\cdot h_0(x,0)+1=1$.

Case 1 $x\cdot g_0(x,0)+1=1$ and $x\cdot h_0(x,0)+1=\Phi_k(x)$.

In this case we have

$$\begin{aligned} g_0(x,0) &= 0,\\ h_0(x,0) &= (\Phi_k(x)-1)/x. \end{aligned}$$

The above equations imply

$$\begin{aligned} g_0(x,y) &= y\cdot g_1(x,y)+0,\\ h_0(x,y) &= y\cdot h_1(x,y)+(\Phi_k(x)-1)/x, \end{aligned}$$

and we have

$$B_k(x,y)=(xy\cdot g_1(x,y)+\Phi_{2k}(y))(xyh_1(x,y)+\Phi_k(x)). \qquad (2.33)$$

This is not possible because by Lemma 2.2.5 the total degree of $B_k(x,y)$ should be $k-1$, while Equation (2.33) shows that its total degree is at least $2k-2$ (unless $k=1$, but k is a prime here). Therefore, $B_k(x,y)$ must be irreducible.

Case 2 $x \cdot g_0(x,0) + 1 = \Phi_k(x)$ and $x \cdot h_0(x,0) + 1 = 1$.

Here we have

$$\begin{aligned} g_0(x,0) &= (\Phi_k(x) - 1)/x, \\ h_0(x,0) &= 0. \end{aligned}$$

Then

$$\begin{aligned} g_0(x,y) &= (\Phi_k(x) - 1)/x + y \cdot g_1(x,y), \\ h_0(x,y) &= y \cdot h_1(x,y). \end{aligned}$$

Therefore,

$$B_k(x,y) = (xy \cdot g_1(x,y) + \Phi_k(x) + \Phi_{2k}(y) - 1)(xyh_1(x,y) + 1). \tag{2.34}$$

By Lemma 2.2.5 the degree of $B_k(x,y)$ is $k-1$, so we must have $h_1(x,y) = 0$. Then $h_0(x,y) = 0$, so we get $h(x,y) = 1$, a contradiction with $h(x,y)$ having degree at least 1.

Therefore, $B_k(x,y)$ must be irreducible. This proves Theorem 2.2.1. ■

We now need Gauss's Lemma. (See "Algebra", by Hungerford, Lemma 6.13.) Let D be a unique factorization domain with quotient field F and f a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$. For two variable polynomials, the same result holds. See Appendix B for the proof.

Applying this to the *U.F.D.* $\mathbb{Z}$ with quotient field $\mathbb{Q}$ gives this theorem:

Theorem 2.2.2 *When k is an odd prime, $B_k(x,y)$ is an irreducible polynomial over $\mathbb{Q}$.*

As a polynomial in two variables, $B_k(x,y)$ is irreducible. But it is not true that it would become an irreducible polynomial in one variable when the other is fixed to be an arbitrary constant. For $B_k(x,y)$, it is not true that $B_k(x,c)$ would be an irreducible polynomial of one variable for any integer c. For example:

Example 2.2.1

If $y = 1$, then $B_k(x,1)$ is reducible for any prime k:

$$\begin{aligned}
B_3(x,1) &= x^2 + 2x + 1 \\
&= (x+1)^2, \\
B_5(x,1) &= x^4 + 2x^3 - x^2 - 2x + 1 \\
&= (x^2 + x - 1)^2, \\
B_7(x,1) &= x^6 + 2x^5 - 3x^4 - 6x^3 + 2x^2 + 4x + 1 \\
&= (x^3 + x^2 - 2x - 1)^2, \\
\ldots &
\end{aligned}$$

This result can be generalized to all $B_k(x,1)$ when k is a prime. See Theorem 2.2.5 for the proof.

By the Hilbert irreducibility theorem, if $B_k(x,y)$ is an irreducible polynomial over $\mathbb{Q}$, there will be infinitely many choices of a rational number c, such that $B_k(x,c)$ is also irreducible. But no result tells us which rational numbers c make $B_k(x,c)$ irreducible.

Fortunately for our application in elliptic curve cryptography, y only needs to be an odd prime number q. And we can show that $B_k(x,q)$ is irreducible. Actually, as long as $c \neq 1$, $B_k(x,c)$ will be irreducible. As we show in Theorem 2.2.4.

By Section 2.1.3 we know that it will be efficient to calculate the Bateman-Horn constant by using the definition provided the polynomials are abelian. The following theorem shows that $B_k(x,q)$ is an abelian polynomial.

Theorem 2.2.3 *For $q \in \mathbb{Z}$, $q > 1$, and an odd prime k, $B_k(x,q)$ is an abelian polynomial of x.*

Proof Since $A_k(x,q) = (q+1-x)B_k(x,q)$, the splitting field of $A_k(x,q)$ over $\mathbb{Q}$ equals the splitting field of $B_k(x,q)$ over $\mathbb{Q}$. To show $B_k(x,q)$ is abelian, it is enough to show that the zeros of $A_k(x,q)$ generate a normal extension of the rational numbers with an abelian Galois group.

By plugging in $y=q$ into Formula (2.22) in Lemma 2.2.2, we have

$$A_k(x,q) = \left(\left(\frac{x+\sqrt{x^2-4q}}{2}\right)^k - 1\right)\left(\left(\frac{x-\sqrt{x^2-4q}}{2}\right)^k - 1\right). \tag{2.35}$$

The roots of $A_k(x,q)$ can be expressed in terms of ζ_k, a k^{th} root of unity:

$$\begin{aligned} \left(\frac{x\pm\sqrt{x^2-4q}}{2}\right)^k &= 1, \\ \frac{x\pm\sqrt{x^2-4q}}{2} &= \zeta_k^i, \\ x\pm\sqrt{x^2-4q} &= 2\zeta_k^i, \\ \pm\sqrt{x^2-4q} &= 2\zeta_k^i - x, \\ x^2-4q &= (2\zeta_k^i - x)^2, \\ -4q &= 4\zeta_k^{2i} - 4\zeta_k^i x. \end{aligned}$$

Then we get:

$$x = q\zeta_k^{-i} + \zeta_k^i, \tag{2.36}$$

where $i \in 0,1,\ldots,k-1$. Then the splitting field of $A_k(x,q)$ is a subfield of $\mathbb{Q}(\zeta_k)$, the cyclotomic extension of $\mathbb{Q}$, which is an abelian extension. Since all the subgroups and quotient groups of abelian groups are abelian, by the fundamental theorem of Galois theory [14], Section 5.8, we see that every subfield containing $\mathbb{Q}$ of an abelian extension of $\mathbb{Q}$ is again an abelian extension of $\mathbb{Q}$. So the splitting field of $B_k(x,q)$ is abelian and $B_k(x,q)$ is an abelian polynomial. ■

Another important property for polynomial $B_k(x,q)$ is irreducibility. Actually, more is true.

Theorem 2.2.4 *If k is an odd prime, then $B_k(x,c)$ is irreducible over $\mathbb{Q}$ for any integer $c \neq 1$.*

Proof Assuming we have already proved $\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)$=$\mathbb{Q}(\zeta_k)$, the minimal polynomial of $c\zeta_k^{-1}+\zeta_k$ over $\mathbb{Q}$ should have degree $[\mathbb{Q}(\zeta_k),\mathbb{Q}]$=$k-1$. Since $B_k(c\zeta_k^{-1}+\zeta_k,q)=0$ and $B_k(x,q)$ is a monic polynomial with degree $k-1$, $B_k(x,q)$ must be the minimal polynomial of $(c\zeta_k^{-1}+\zeta_k)$. Hence it is irreducible.

Now we show $\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)$=$\mathbb{Q}(\zeta_k)$. Suppose $\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)\subsetneq\mathbb{Q}(\zeta_k)$, Then $Gal(\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)/\mathbb{Q})\subsetneq Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})$. Then there must be a nontrivial $\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)$-automorphism of $\mathbb{Q}(\zeta_k)$ in $Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})$. Denote it as $\sigma\in Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})$, so that $\sigma(c\zeta_k^{-1}+\zeta_k)=c\zeta_k^{-1}+\zeta_k$. Then we have:

$$\sigma(c\zeta_k^{-1}+\zeta_k)-c\zeta_k^{-1}-\zeta_k=c\sigma(\zeta_k^{-1})+\sigma(\zeta_k)-c\zeta_k^{-1}-\zeta_k=0.$$

Since $\sigma\in Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})$, $\sigma(\zeta_k)=\zeta_k^i$ for some integer $i\in\{2,\ldots,k-1\}$, we have:

$$c\zeta_k^{-i}+\zeta_k^i-c\zeta_k^{-1}-\zeta_k=0 \qquad \text{for some } i\in\{2,\ldots,k-1\}. \tag{2.37}$$

If $i=k-1$, we have:

$$\begin{aligned} c\zeta_k^1+\zeta_k^{k-1}-c\zeta_k^{k-1}-\zeta_k &= (1-c)\zeta_k^{k-1}-(1-c)\zeta_k \\ &= (1-c)\zeta_k(\zeta_k^{k-2}-1) \\ &= 0. \end{aligned}$$

This won't happen. Because if $c\neq 1$, one has $(1-c)\zeta_k\neq 0$. Thus $\zeta_k^{k-2}-1=0$, which contradicts the fact that ζ_k is a k^{th} root of unity.

If $i\in\{2,\ldots,k-2\}$, we have:

$$-c\zeta_k^{k-1}+\zeta_k^i+c\zeta_k^{k-i}-\zeta_k=0. \tag{2.38}$$

Add a c-multiple of the minimal polynomial of ζ_k to Equation (2.38), get:

$$c\zeta_k^{k-2}+\ldots+(c+1)\zeta_k^i+\ldots+2c\zeta_k^{k-i}+\ldots+(c-1)\zeta_k+c=0 \tag{2.39}$$

or

$$c\zeta_k^{k-2}+\ldots+2c\zeta_k^{k-i}+\ldots+(c+1)\zeta_k^i+\ldots+(c-1)\zeta_k+c=0. \tag{2.40}$$

Hence ζ_k is a root of a nontrivial polynomial of degree at most $k-2$, a contradiction to the fact that the minimal polynomial of ζ_k is of degree $k-1$. So we have proved $\mathbb{Q}(c\zeta_k^{-1}+\zeta_k)$=$\mathbb{Q}(\zeta_k)$. ■

Since $q > 1$ in particular, we have:

Corollary 2.2.1 *For odd primes k and q, $B_k(x,q)$ is irreducible over $\mathbb{Q}$.*

Proof Again, since $\mathbb{Z}$ is a *U.F.D.*, the irreducibility of a polynomial over $\mathbb{Z}$ and $\mathbb{Q}$ are the same. ■

We recently learned that the irreducibility of polynomial $B_k(x,y)$ and $B_k(x,q)$ was discussed by Qi Cheng and Ming-Deh Huang in [6]. It seems the proof of irreducibility of $B_k(x,y)$ in [6] is based on the irreducibility of $B_k(x,c)$ for any integer c, which is not always true, as we saw in Example 2.2.1.

Now we discuss $B_k(x,c)$ when $c=1$. As we saw in Example 2.2.1, $B_k(x,1)$ is a square of a polynomial when $k=3,5,7$. We can generalize this result to all prime k.

Theorem 2.2.5 *If k is an odd prime, $B_k(x,1)$ is a square of an irreducible polynomial. In fact,*

$$B_k(x,1) = \left(1+\sum_{i=1}^{\frac{k-1}{2}} f_i(x,1)\right)^2, \tag{2.41}$$

where the $f_i(x,y)$ are the polynomials defined in Equations (2.16)*,* (2.17) *and* (2.18)*.*

Proof From Lemma 2.2.2, we can get the roots of $A_k(x,1)$:

$$\begin{aligned}
A_k(x,1) &= 0,\\
\left(\frac{x\pm\sqrt{x^2-4}}{2}\right)^k - 1 &= 0,\\
\left(\frac{x\pm\sqrt{x^2-4}}{2}\right)^k &= 1,\\
\frac{x\pm\sqrt{x^2-4}}{2} &= \zeta_k^i,\\
\pm\sqrt{x^2-4} &= 2\zeta_k^i - x,\\
x &= \zeta_k^{-i}+\zeta_k^i,
\end{aligned}$$

where $i \in 0, 1, \cdots, k-1$. All $\zeta_k^{-i}+\zeta_k^i$ can be expressed by $\zeta_k^{-1}+\zeta_k$, just as in Equations (2.16), (2.17) and (2.18), and we have $\zeta_k^{-i} + \zeta_k^i = f_k(\zeta_k^{-1} + \zeta_k^1, 1)$. Thus the splitting field of $B_k(x, 1)$ over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_k^{-1} + \zeta_k)$. Notice that $\zeta_k^{-i} = \zeta_k^{k-i}$ for $k = 0, 1, \cdots, k-1$. We have

$$\begin{aligned} 1 + \sum_{i=1}^{\frac{k-1}{2}} f_i(\zeta_k^{-1} + \zeta_k, 1) &= 1 + \sum_{i=1}^{\frac{k-1}{2}} \zeta_k^{-i} + \zeta_k^i \\ &= \sum_{i=0}^{k-1} \zeta_k^i \\ &= 0, \end{aligned}$$

by definition of ζ_k^i. Because $f_i(x, 1)$ is a monic polynomial of degree i, $1+\sum_{i=1}^{\frac{k-1}{2}} f_i(x, 1)$ is a monic polynomial of degree $\frac{k-1}{2}$. Denote

$$b_k(x) = 1 + \sum_{i=1}^{\frac{k-1}{2}} f_i(x, 1). \tag{2.42}$$

Thus the minimal polynomial of $\zeta_k^{-1} + \zeta_k$ is of degree at most $\frac{k-1}{2}$. So $\mathbb{Q} \subsetneq \mathbb{Q}(\zeta_k^{-1} + \zeta_k) \subsetneq \mathbb{Q}(\zeta_k)$. Notice that $\zeta_k^2 - (\zeta_k^{-1} + \zeta_k)\zeta_k + 1 = 0$, so the minimal polynomial of ζ_k over $\mathbb{Q}(\zeta_k^{-1}+\zeta_k)$ is $x^2-(\zeta_k^{-1}+\zeta_k)x+1$. Thus $[\mathbb{Q}(\zeta_k) : \mathbb{Q}(\zeta_k^{-1}+\zeta_k)] = 2$. Because $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = [Q(\zeta_k) : \mathbb{Q}(\zeta_k^{-1} + \zeta_k)][\mathbb{Q}(\zeta_k^{-1} + \zeta_k) : \mathbb{Q}]$, we have $[\mathbb{Q}(\zeta_k^{-1} + \zeta_k) : \mathbb{Q}] = \frac{k-1}{2}$. Since we already proved $b_k(\zeta_k^{-1}+\zeta_k) = 0$ and $b_k(x)$ is a monic polynomial of degree $\frac{k-1}{2}$, $b_k(x)$ is the minimal polynomial of $\zeta_k^{-1}+\zeta_k$ over $\mathbb{Q}$. Hence it's irreducible.

To show $B_k(x, 1) = b_k^2(x)$, it's enough to show that

$$B_k(x, 1) = \prod_{i=1}^{k-1} \big(x - (\zeta_k^{-i} + \zeta_k^i)\big), \tag{2.43}$$

$$b_k(x) = \prod_{i=1}^{\frac{k-1}{2}} \big(x - (\zeta_k^{-i} + \zeta_k^i)\big). \tag{2.44}$$

Because $\zeta_k^{-i}+\zeta_k^i=\zeta_k^{-(k-i)}+\zeta_k^{k-i}$, we have

$$\begin{aligned}
B_k(x,1) &= \prod_{i=1}^{k-1}\left(x-(\zeta_k^{-i}+\zeta_k^i)\right)\\
&= \prod_{i=1}^{\frac{k-1}{2}}\left(x-(\zeta_k^{-i}+\zeta_k^i)\right)\prod_{i=\frac{k-1}{2}+1}^{k-1}\left(x-(\zeta_k^{-i}+\zeta_k^i)\right)\\
&= \prod_{i=1}^{\frac{k-1}{2}}\left(x-(\zeta_k^{-i}+\zeta_k^i)\right)\prod_{i=1}^{\frac{k-1}{2}}\left(x-(\zeta_k^{-i}+\zeta_k^i)\right)\\
&= b_k(x)^2.
\end{aligned}$$

To prove (2.38), we already know the roots of $A_k(x,1)$ are $\zeta_k^{-i}+\zeta_k^i$ for $i=0,1,\cdots,k-1$. And we know that $A_k(x,1)=(2-x)B_k(x,1)$. Thus the roots of $B_k(x,1)$ are $\zeta_k^{-i}+\zeta_k^i$ for $i=1,\cdots,k-1$. So (2.38) is proved.

To prove (2.39), for any $i=1,\cdots,\frac{k-1}{2}$, consider

$$\begin{aligned}
b_k(\zeta_k^{-i}+\zeta_k^i) &= 1+\sum_{j=1}^{\frac{k-1}{2}} f_j(\zeta_k^{-i}+\zeta_k^i,1)\\
&= 1+\sum_{j=1}^{\frac{k-1}{2}}\left(\zeta_k^{-ij}+\zeta_k^{ij}\right).
\end{aligned}$$

We need to show that

$$\left\{\zeta_k^{-ij}+\zeta_k^{ij}\mid j=1,\cdots,\frac{k-1}{2}\right\}=\left\{\zeta_k^{-j}+\zeta_k^{j}\mid j=1,\cdots,\frac{k-1}{2}\right\} \tag{2.45}$$

for all $i=1,\cdots,\frac{k-1}{2}$. Actually, $\forall a,b\in\{1,\cdots,\frac{k-1}{2}\}$, $ai\not\equiv bi \mod k$, otherwise $k|i$ or $k|a-b$, which is impossible since $i,a,b\in\{1,\cdots,\frac{k-1}{2}\}$; $ai+bi\not\equiv 0 \mod k$, otherwise $k|a+b$ or $k|i$, which is impossible since $i,a,b\in\{1,\cdots,\frac{k-1}{2}\}$. Hence Equation (2.45) is proved.

So

$$b_k(\zeta_k^{-i}+\zeta_k^i) = 1+\sum_{j=1}^{\frac{k-1}{2}}\left(\zeta_k^{-j}+\zeta_k^{j}\right)=0$$

and Equation (2.44) is proved. ■

2.2.2 Reducibility

As we mentioned in Section 2.1.2, when k is not a prime, $M_k = \frac{|E(F_{q^k})|}{|E(F_q)|}$ is usually a composite number. We can also prove that the polynomial $B_k(x, y)$ is reducible when k is not a prime.

When k is not a prime, let $k = rs$, where r and s are integers greater than 1. Notice that

$$\begin{aligned}
|E(F_{q^k})| &= q^k + 1 - (\alpha^k + \beta^k) \\
&= (\alpha^k - 1)(\beta^k - 1) \\
&= (\alpha^{rs} - 1)(\beta^{rs} - 1) \\
&= ((\alpha^r)^s - 1)((\beta^r)^s - 1) \\
&= (\alpha^r - 1)(\beta^r - 1)\sum_{i=0}^{s-1}(\alpha^r)^i \sum_{j=0}^{s-1}(\beta^r)^j \\
&= (\alpha - 1)(\beta - 1)\sum_{i=0}^{r-1}\alpha^i \sum_{j=0}^{r-1}\beta^j \sum_{i=0}^{s-1}(\alpha^r)^i \sum_{j=0}^{s-1}(\beta^r)^j.
\end{aligned}$$

When we let $x = \alpha + \beta$ and $y = \alpha\beta$, it's easy to see $(\alpha - 1)(\beta - 1) = y + 1 - x$. Also we can prove that

Lemma 2.2.6 *$\sum_{i=0}^{n}\alpha^i \sum_{j=0}^{n}\beta^j$ can be expressed as a polynomial in $h_n(x, y)$ for any $n \geq 1$.*

Proof Use induction on n. When $n = 1$:

$$(\alpha + 1)(\beta + 1) = (\alpha + \beta) + \alpha\beta + 1 = y + x + 1.$$

Suppose we have already proved that for $m = 1, 2, \ldots, n$, there are polynomials $h_m(x, y)$ such that $\sum_{i=0}^{m} \alpha^i \sum_{j=0}^{m} \beta^j = h_m(x, y)$. Then

$$\begin{aligned}
\sum_{i=0}^{n+1} \alpha^i \sum_{j=0}^{n+1} \beta^j &= \left(\alpha^{n+1} + \sum_{i=0}^{n} \alpha^i\right)\left(\beta^{n+1} + \sum_{j=0}^{n} \beta^j\right) \\
&= \alpha^{n+1}\beta^{n+1} + \alpha^{n+1}\sum_{j=0}^{n} \beta^j + \beta^{n+1}\sum_{i=0}^{n} \alpha^i + \sum_{i=0}^{n} \alpha^i \sum_{j=0}^{n} \beta^j \\
&= \alpha^{n+1}\beta^{n+1} + \sum_{i=0}^{n}(\alpha^i\beta^{n+1} + \alpha^{n+1}\beta^i) + \sum_{i=0}^{n} \alpha^i \sum_{j=0}^{n} \beta^j \\
&= \alpha^{n+1}\beta^{n+1} + \sum_{i=0}^{n}(\alpha\beta)^i(\alpha^{n+1-i} + \beta^{n+1-i}) + \sum_{i=0}^{n} \alpha^i \sum_{j=0}^{n} \beta^j.
\end{aligned}$$

From Equations (2.16), (2.17) and (2.18) we know that $\alpha^n + \beta^n = f_n(x, y)$ for any integer n. Hence

$$\sum_{i=0}^{n+1} \alpha^i \sum_{j=0}^{n+1} \beta^j = y^{n+1} + \sum_{i=0}^{n} y^i f_{n+1-i}(x, y) + h_n(x, y).$$

■

From the above lemma, we know $\sum_{i=0}^{n} \alpha^i \sum_{j=0}^{n} \beta^j = h_n(\alpha+\beta, \alpha\beta)$. Then it's easy to see that

$$\sum_{i=0}^{s-1} (\alpha^r)^i \sum_{j=0}^{s-1} (\beta^r)^j \quad = \quad h_{s-1}(\alpha^r + \beta^r, \alpha^r\beta^r).$$

Again if we let $x = \alpha + \beta$ and $y = \alpha\beta$, by Equations (2.16), (2.17) and (2.18), we have

$$\begin{aligned}
\alpha^r + \beta^r &= f_r(x, y), \\
\alpha^r\beta^r &= y^r.
\end{aligned}$$

Hence

$$\sum_{i=0}^{s-1} (\alpha^r)^i \sum_{j=0}^{s-1} (\beta^r)^j \quad = \quad h_{s-1}(f_r(x, y), y^r).$$

Also, by switching r and s, we get symmetric results. Thus we have

Theorem 2.2.6 *When $k = rs$, where r and s are integers greater than 1,*

$$\begin{aligned} A_k(x,y) &= (y+1-x)\cdot h_{r-1}(x,y)\cdot h_{s-1}(f_r(x,y),y^r) && (2.46)\\ &= (y+1-x)\cdot h_{s-1}(x,y)\cdot h_{r-1}(f_s(x,y),y^s) && (2.47)\end{aligned}$$

and

$$\begin{aligned} B_k(x,y) &= h_{r-1}(x,y)\cdot h_{s-1}(f_r(x,y),y^r) && (2.48)\\ &= h_{s-1}(x,y)\cdot h_{r-1}(f_s(x,y),y^s). && (2.49)\end{aligned}$$

2.3 Asymptotic Formula

2.3.1 Related works

The number of elliptic curves with large prime order subgroups is very important in both theory and application of elliptic curve cryptography, since it is directly related to the security of the cryptosystem. The larger the pool we can choose from, the more secure the cryptosystem will be.

Some important research related to this has been done. Neal Koblitz [19] generalized Wagstaff's conjecture [35] for Mersenne numbers as follows:

Koblitz's Conjecture: For fixed E over $\mathbb{F}_q$, let:

$$M_k = M_k(E/\mathbb{F}_q) = \frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|}. \tag{2.50}$$

The number $M(x)$ of $M_k < x$ that are prime is asymptotic to

$$\frac{e^\gamma}{\log q}\log\log x. \tag{2.51}$$

Qi Cheng and Ming-Deh Huang [6] gave a lower bound for the number of almost prime group orders under certain assumptions (that Bateman-Horn's conjecture is true and that a Siegel zero [29] does not exist).

We will prove an asymptotic formula under only the assumption that Bateman-Horn's conjecture is true.

2.3.2 A Formula Based on $B_k(x, q)$

From the previous section we know that the polynomial $B_k(x, q)$ is irreducible. We can estimate the probability that $\frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|}$ is a prime number since

$$\frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|} = B_k(t_1, q). \tag{2.52}$$

Bateman-Horn's conjecture tells us the asymptotic number of primes a one-variable irreducible polynomial produces when taking integer values. In our case, the variable x takes integer value t_1, which is the Frobenius trace of $E(\mathbb{F}_q)$. From Hasse's theorem 2.1.1, t_1 lies in $(-2\sqrt{q}, 2\sqrt{q})$.

Notice that in the Bateman-Horn's conjecture, the irreducible polynomials only take positive integer values. It would be straightforward to estimate the number of primes when t_1 takes values from 1 to $\lfloor 2\sqrt{q} \rfloor$. For the values from $-\lfloor 2\sqrt{q} \rfloor$ to -1, we consider another polynomial:

$$B'_k(x, q) = B_k(-x, q). \tag{2.53}$$

Then the number of primes with $t_1 < 0$ can be estimated by Bateman-Horn's formula applied to the polynomial $B'_k(x, q)$, with the variable x taking values from 1 to $\lfloor 2\sqrt{q} \rfloor$. This will give the number of primes when $B_k(x, q)$ takes values from $-\lfloor 2\sqrt{q} \rfloor$ to -1.

It is easy to show that the Bateman-Horn's constants for $B'_k(x, q)$ and $B_k(x, q)$ are the same:

Theorem 2.3.1 *The Bateman-Horn's constants for $B'_k(x, q)$ and $B_k(x, q)$ are the same.*

Proof From Formula (2.8), the Bateman-Horn's constants for the two polynomials are determined by $\omega(p)$, which is the number of solutions of the congruences

$$B_k(x, q) \equiv 0 \pmod{p}, \tag{2.54}$$

$$B'_k(x, q) \equiv 0 \pmod{p}. \tag{2.55}$$

The congruences (2.54) and (2.55) have the same number of solutions. Actually, if x_0 is a solution of (2.54), $B'_k(-x_0, q) = B_k(-(-x_0), q) = B_k(x_0, q)$, so $-x_0$ is a solution of (2.55). Similarly, when $-t_0$ is a solution of (2.55), t_0 is a solution of (2.54). Thus the Bateman-Horn's constants of $B'_k(x, q)$ and $B_k(x, q)$ are the same. ■

When x takes value zero, i.e., the elliptic curve is supersingular, Lemma 2.2.4 tells us

$$B_k(0, q) = \Phi_{2k}(q) = \frac{q^k + 1}{q + 1}.$$

Generally, $\Phi_{2k}(q)$ is not necessarily prime, even if both k and q are prime. For example: $\Phi_{14}(5) = 13021 = 29 \cdot 449$. Certainly the probability of polynomial $\Phi_{2k}(x)$ being prime can be estimated by the Bateman-Horn conjecture, but whether $B_k(0, q)$ is prime will not affect the estimate of the number of primes that $B_k(x, q)$ produces within the range $[-\lfloor 2\sqrt{q} \rfloor, \lfloor 2\sqrt{q} \rfloor]$ when q is large, i.e. $q \to \infty$.

Thus, Theorem 2.3.1 allows us to estimate the number of prime values of $B_k(t_1, q)$ when t_1 takes a value between $-\lfloor 2\sqrt{q} \rfloor$ and $\lfloor 2\sqrt{q} \rfloor$.

Notice that in the Bateman-Horn conjectured Formula (2.11), $\log f(u)$ is needed. The following examples and analysis will tell us the magnitude of $\log f(u)$.

Example 2.3.1

$$\begin{aligned} B_5(x, q) =& x^4 + qx^3 + x^3 + (q^2 - 3q + 1)x^2 + (q^3 - 2q^2 - 2q + 1)x \\ & + (q^4 - q^3 + q^2 - q + 1), \\ B_7(x, q) =& x^6 + (q + 1)x^5 + (q^2 - 5q + 1)x^4 + (q^3 - 4q^2 - 4q + 1)x^3 \\ & + (q^4 - 3q^3 + 6q^2 - 3q + 1)x^2 + (q^5 - 2q^4 + 3q^3 + 3q^2 - 2q + 1)x \\ & + (q^6 - q^5 + q^4 - q^3 + q^2 - q + 1). \end{aligned}$$

As we can see in the above examples, the constant terms are $O(q^{k-1})$. The leading terms of $B_k(x, q)$ are x^{k-1}. Since the largest values we will plug in for x are $2\sqrt{q}$, the value of the leading terms are $O(q^{\frac{k-1}{2}})$. Thus it's not the leading term which dominates $B_k(x, q)$.

If we look at the definitions for the polynomials $A_k(x,q)$ and $B_k(x,q)$, we will determine the size of $B_k(t_1,q)$ easily. $A_k(t_1,q)$ is the order of the elliptic curve $E(\mathbb{F}_{q^k})$. Thus from the Hasse's bound we have:

$$q^k + 1 - 2q^{k/2} \leq A_k(t_1,q) \leq q^k + 1 + 2q^{k/2}.$$

Since $-2q^{1/2} \leq t_1 \leq 2q^{1/2}$, we can also give upper and lower bounds for $B_k(t_1,q) = \frac{A_k(t_1,q)}{q+1-t_1}$ as follows:

$$\begin{array}{rcl} q^k + 1 - 2q^{k/2} \leq & A_k(t_1,q) & \leq q^k + 1 + 2q^{k/2}, \\ \dfrac{q^k + 1 - 2q^{k/2}}{q+1-t_1} \leq & B_k(t_1,q) & \leq \dfrac{q^k + 1 + 2q^{k/2}}{q+1-t_1}, \\ \dfrac{q^k + 1 - 2q^{k/2}}{q+1+2q^{1/2}} \leq & B_k(t_1,q) & \leq \dfrac{q^k + 1 + 2q^{k/2}}{q+1-2q^{1/2}}, \\ \dfrac{q^k - 2q^{k/2}}{q+3q^{1/2}} \leq & B_k(t_1,q) & \leq \dfrac{q^k + 3q^{k/2}}{q-2q^{1/2}}, \\ \dfrac{q^{k-1} - 2q^{k/2-1}}{1+3q^{-1/2}} \leq & B_k(t_1,q) & \leq \dfrac{q^{k-1} + 3q^{k/2-1}}{1-2q^{-1/2}}. \end{array}$$

When $0 < \delta < 1/2$, we have $1 - \delta < \frac{1}{1+\delta}$ and $\frac{1}{1-\delta} < 1 + 2\delta$, so we have

$$\begin{array}{rcl} \left(q^{k-1} - 2q^{k/2-1}\right)\left(1 - 3q^{-1/2}\right) \leq & B_k(t_1,q) & \leq \left(q^{k-1} + 3q^{k/2-1}\right)\left(1 + 4q^{-1/2}\right), \\ q^{k-1} - 2q^{\frac{k}{2}-1} - 3q^{k-\frac{3}{2}} + 6q^{\frac{k}{2}-\frac{3}{2}} \leq & B_k(t_1,q) & \leq q^{k-1} + 3q^{\frac{k}{2}-1} + 4q^{k-\frac{3}{2}} + 12q^{\frac{k}{2}-\frac{3}{2}}. \end{array}$$

As $q \to \infty$, we have

$$B_k(t_1,q) \sim q^{k-1}, \tag{2.56}$$

where $f(n) \sim g(n)$ means $\lim_{n\to\infty} f(n)/g(n) = 1$.

This leads to the following estimation:

Proposition 2.3.1 *Let q and k be odd primes and assume the Bateman-Horn conjecture. Then the number of traces of elliptic curves with almost prime order is asymptotically*

$$2C_{BH}(B_k(x,q))\frac{2\sqrt{q}}{(k-1)\log q}, \tag{2.57}$$

as $q \to \infty$.

Proof As proved in the previous section,

$$\frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|} = B_k(t_1, q).$$

Now $B_k(x, q)$ is an irreducible polynomial by Theorem 2.2.2. Thus the number of the traces t_1 in $[1, 2\sqrt{q}]$ can be estimated by the Bateman-Horn's conjectured Formula (2.11):

$$Q(B_k(x, q); 2\sqrt{q}) \sim C_{BH}(B_k(x, q)) \int_1^{2\sqrt{q}} \frac{du}{\log B_k(u, q)}.$$

By Formula (2.56) we have

$$\begin{aligned} Q(B_k(x, q); 2\sqrt{q}) &\sim C_{BH}(B_k(x, q)) \int_1^{2\sqrt{q}} \frac{du}{\log q^{k-1}} \\ &\sim C_{BH}(B_k(x, q)) \int_1^{2\sqrt{q}} \frac{du}{(k-1)\log q} \\ &\sim C_{BH}(B_k(x, q)) \frac{2\sqrt{q}}{(k-1)\log q}. \end{aligned}$$

Similarly, the same estimate can be made for $t_1 \in [-2\sqrt{q}, -1]$ by considering the irreducible polynomial $B_k'(x, q)$. By Theorem 2.3.1, the Bateman-Horn constants of $B_k'(x, q)$ and $B_k(x, q)$ are the same. Also the integral terms are the same, so the estimations for the negative and positive halves of Hasse's interval are same. Thus the total number of feasible t_1's in Hasse's interval is $2C_{BH}\frac{2\sqrt{q}}{(k-1)\log q}$ under the Bateman-Horn's conjecture.

■

2.4 Experimental Results

In this section, we give experimental results for some prime k's and q's of different sizes.

Generally, the size of the elliptic curve subgroup of prime order is $\log q^{k-1}$ bits, while the whole elliptic curve group has size $\log q^k$ bits. The ratio of the bit sizes of the prime order subgroup and the whole group is $r = \frac{k-1}{k}$. We would like this ratio r be close to one. So we start with $k = 5$ instead of $k = 3$ because the prime order subgroup of $E(F_{q^k})$ has only $\frac{2}{3}$ of the bit size of q^k, not a efficient scheme for an elliptic curve cryptosystem.

Because it's easy to calculate the group order of $E(\mathbb{F}_q)$, and hence get t_1, we can easily get the group order of $E(\mathbb{F}_{q^k})$ and the prime subgroup order $B_k(t_1, q)$.

Examples of curves with almost prime order will be given in the next section. All the curves in those examples have prime subgroup of order larger than 163.

2.4.1 Data for $k = 5, 7, 11, 13, 17, 19, 23, 29$.

The columns in the table are:

q $PP(2^i)$ is the largest prime number $\leq 2^i$

C_{BH} Bateman-Horn's constant

$Count_l$ The number of t_1 such that $B_k(t_1, q)$ is a prime, $t_1 \in [-\lfloor 2\sqrt{q} \rfloor, -1]$.

$Count_r$ The number of t_1 such that $B_k(t_1, q)$ is a prime, $t_1 \in [1, \lfloor 2\sqrt{q} \rfloor]$.

$Total$ $Count_l + Count_r$.

$BH - estimate$ The estimate based on Proposition 2.3.1.

$Ratio$ $Total/(BH - estimate)$

Table 1. Experimental data for $k = 5$.

q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
PP(2^{30})	2.9456	2362	2318	4680	4642	1.0082
PP(2^{31})	4.2328	4574	4502	9076	9129	0.9942
PP(2^{32})	2.6351	3853	3772	7625	7786	0.9793
PP(2^{33})	2.9427	6139	5997	12136	11924	1.0178
PP(2^{34})	2.8692	8035	7930	15965	15958	1.0004
PP(2^{35})	4.1494	15647	15817	31464	31704	0.9924
PP(2^{36})	3.3860	17869	17799	35668	35571	1.0027
PP(2^{37})	3.3631	24374	24323	48697	48615	1.0017
PP(2^{38})	2.9290	29050	29193	58243	58301	0.9990
PP(2^{39})	2.5855	35222	35604	70826	70916	0.9987
PP(2^{40})	3.0422	57583	57673	115256	115054	1.0018
PP(2^{41})	3.3849	88758	88653	177411	176623	1.0045

Table 2. Experimental data for $k = 7$.

q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
PP(2^{24})	4.4834	356	344	700	736	0.9511
PP(2^{25})	5.0679	549	550	1099	1129	0.9734
PP(2^{26})	4.4831	689	696	1385	1359	1.0191
PP(2^{27})	4.4831	919	872	1791	1850	0.9681
PP(2^{28})	4.5414	1347	1247	2594	2556	1.0149
PP(2^{29})	4.4951	1713	1770	3483	3454	1.0084
PP(2^{30})	4.4850	2307	2353	4660	4712	0.9890
PP(2^{31})	4.8753	3360	3507	6867	7009	0.9797
PP(2^{32})	4.7255	4625	4808	9433	9308	1.0134
PP(2^{33})	4.8736	6565	6601	13166	13165	1.0001
PP(2^{34})	4.9240	9033	9030	18063	18257	0.9894
PP(2^{35})	4.7600	12271	11906	24177	24246	0.9972
PP(2^{36})	4.4831	15488	15889	31377	31398	0.9993

Table 3. Experimental data for $k = 11$.

q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
PP(2^{17})	3.6492	19	23	42	45	0.9333
PP(2^{18})	4.7720	42	29	71	78	0.9103
PP(2^{19})	4.8730	65	55	120	107	1.1215
PP(2^{20})	5.0160	75	74	149	148	1.0068
PP(2^{21})	4.7808	105	111	216	190	1.1368
PP(2^{22})	3.7164	88	104	192	200	0.9600
PP(2^{23})	3.9172	142	141	283	285	0.9930
PP(2^{24})	5.4125	284	287	571	533	1.0713

Table 4. Experimental data for $k = 13$.

q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
PP(2^{13})	5.2410	5	8	13	18	0.7222
PP(2^{14})	5.2151	11	12	23	23	1.0000
PP(2^{15})	5.3830	15	15	30	31	0.9677
PP(2^{16})	5.8510	23	17	40	45	0.8889
PP(2^{17})	5.6373	29	34	63	58	1.0862
PP(2^{18})	5.9782	46	41	87	82	1.0610
PP(2^{19})	5.2638	42	52	94	96	0.9792
PP(2^{20})	5.2376	54	58	112	129	0.8682

Table 5. Experimental data for $k = 17, 19, 23, 29$.

k	q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
17	PP(2^{10})	6.4041	3	1	4	7	0.5714
	PP(2^{11})	6.5029	10	4	14	10	1.4000
	PP(2^{12})	7.1753	8	5	13	14	0.9286
	PP(2^{13})	6.4053	9	9	18	16	1.1250
	PP(2^{14})	6.4041	16	10	26	21	1.2381
	PP(2^{15})	6.6051	19	11	30	29	1.0345
	PP(2^{16})	6.9193	12	16	28	40	0.7000
19	PP(2^{9})	8.4058	1	6	7	7	1.0000
	PP(2^{10})	8.4058	4	6	10	9	1.1111
	PP(2^{11})	8.4144	7	8	15	11	1.3636
	PP(2^{12})	8.4058	6	4	10	14	0.7143
	PP(2^{13})	8.4058	12	9	21	19	1.1053
	PP(2^{14})	8.4232	18	18	36	25	1.4400
	PP(2^{15})	8.4058	15	14	29	33	0.8788
	PP(2^{16})	8.7544	31	21	52	45	1.1556
23	PP(2^{8})	6.2013	0	3	3	3	1.0000
	PP(2^{9})	4.0807	1	1	2	3	0.6667
	PP(2^{10})	5.7259	3	1	4	5	0.8000
	PP(2^{11})	5.7130	0	3	3	6	0.5000
	PP(2^{12})	5.7130	3	3	6	8	0.7500
29	PP(2^{6})	4.6120	1	2	3	1	3.0000
	PP(2^{7})	6.5371	0	0	0	2	0.0000
	PP(2^{8})	6.5371	1	1	2	3	0.6667
	PP(2^{9})	4.6057	1	1	2	2	1.0000

It is particularly interesting to have the bit sizes of q be multiples of 8, because in this case, the values of the elliptic curve parameters can fit in bytes (a byte is a unit with 8 bits) exactly. From the above tables we have:

Table 6. Experimental data for q whose bit size is a multiple of 8.

k	q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
5	PP(2^{32})	2.6351	3853	3772	7625	7786	0.9793
5	PP(2^{40})	3.0422	57583	57673	115256	115054	1.0018
7	PP(2^{24})	4.4834	356	344	700	736	0.9511
7	PP(2^{32})	4.7255	4625	4808	9433	9308	1.0134
11	PP(2^{24})	5.4125	284	287	571	533	1.0713
13	PP(2^{16})	5.8510	23	17	40	45	0.8889
17	PP(2^{16})	6.9193	12	16	28	40	0.7000
19	PP(2^{16})	8.7544	31	21	52	45	1.1556
23	PP(2^{8})	6.2013	0	3	3	3	1.0000
29	PP(2^{8})	6.5371	1	1	2	3	0.6667

Since the density of primes of bit size b is about $1/(b \log 2)$, there will be many choices for q with a certain bit size b. For example, by the prime number theorem, the number of q's with bit size b is $2^{b-1}/(b \log 2)$. Hence the space of proper elliptic curves is very large. Some example of curves with almost prime order will be given in the following examples, and the programs in MAGMA are in the Appendix A.2.

Example 2.4.1

When $k = 23$, $q = PP(2^8) = 251$. From Table 6, there are 3 traces t_1 which make $E(\mathbb{F}_{251^{23}})$ have almost prime order. They are t_1 =13, 21, 25:

- $t_1 = 13$*:*
  $E_1 : y^2 = x^3 + 238x + 26$ *over* $GF(251^{23})$,
  $E_2 : y^2 = x^3 + 235x + 32$ *over* $GF(251^{23})$,

$E_3 : y^2 = x^3 + 72x + 107$ *over* $GF(251^{23})$,

$E_4 : y^2 = x^3 + 35x + 181$ *over* $GF(251^{23})$.

The orders of E_1, E_2, E_3 *and* E_4 *are the same and they have a large prime factor, which means they all have a big prime order subgroup.*

$$\begin{aligned}&|E_1| = |E_2| = |E_3| = |E_4|\\ =&239 \cdot 65177499221329399385150258169642530377888359601374371.\end{aligned}$$

- $t_1 = 21$*:*

  $E_1 : y^2 = x^3 + 10x + 231$ *over* $GF(251^{23})$,

  $E_2 : y^2 = x^3 + 77x + 97$ *over* $GF(251^{23})$,

  $E_3 : y^2 = x^3 + 6x + 239$ *over* $GF(251^{23})$,

  $E_4 : y^2 = x^3 + 102x + 47$ *over* $GF(251^{23})$,

  $E_5 : y^2 = x^3 + 19x + 213$ *over* $GF(251^{23})$,

  $E_6 : y^2 = x^3 + 176x + 150$ *over* $GF(251^{23})$.

  The orders of E_1, E_2, E_3, E_4, E_5 *and* E_6 *are the same and they have a large prime factor, which means they all have a big prime order subgroup.*

$$\begin{aligned}&|E_1| = |E_2| = |E_3| = |E_4| = |E_5| = |E_6|\\ =&231 \cdot 67434728631591889407146803889272030271229106076460131.\end{aligned}$$

- $t_1 = 25$*:*

  $E_1 : y^2 = x^3 + 150x + 202$ *over* $GF(251^{23})$,

  $E_2 : y^2 = x^3 + 29x + 193$ *over* $GF(251^{23})$,

  $E_3 : y^2 = x^3 + 101x + 49$ *over* $GF(251^{23})$.

  The orders of E_1, E_2, *and* E_3 *are the same and they have a large prime factor, which means they all have a big prime order subgroup.*

$$\begin{aligned}&|E_1| = |E_2| = |E_3|\\ =&227 \cdot 68623005788095711246920315911144936702146215959138051.\end{aligned}$$

Note that in the factorization of the orders of the above curves, the first factors are $q+1-t_1$*, which could be composite numbers, and the second large factors are primes.*

Example 2.4.2

When $k=17$*,* $q=PP(2^{16})=65521$*. From Table 6 we know that there are 28* t_1*'s we can choose. We will just give one example when* $t_1=-477$*:*

$$
\begin{aligned}
y^2 &= x^3+16470x+32581 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+60026x+10990 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+51542x+27958 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+1985x+61551 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+30977x+3567 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+54919x+21204 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+41465x+48112 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+29278x+6965 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+33311x+64420 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+31588x+2345 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+21284x+22953 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+40772x+49498 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+1702x+62117 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+63902x+3238 && \textit{over } GF(65521^{17}),\\
y^2 &= x^3+8760x+48001 && \textit{over } GF(65521^{17}).
\end{aligned}
$$

The order of all of these elliptic curves is:

$$
\begin{aligned}
|E| = {}& 66999\cdot 1145332108243742991681899754426340066819676326930569115327140\backslash\\
& 32776326282148921.
\end{aligned}
$$

Again $66999=q+1-t_1$ *and the second large factor is a prime.*

2.4.2 Comments on Experimental Results

It can be seen from the previous section that when q is large enough, for example, when q is over 30 bits, the errors are within 3 percent. Usually, the errors are less than 10 percent.

When q is small, the relative error could be big. There are two reasons for this. First, the Bateman-Horn constant characterizes the polynomial $B_k(x, q)$ over the whole natural number domain and the larger the interval from which x may take values, the closer the estimate given by the formula; secondly, relative errors can be big when the experimental population counts are small.

Since we need this estimation only when the numbers are big (otherwise, we could just calculate the exact amount), the estimation in Proposition 2.3.1 is very accurate.

2.5 Further Work

2.5.1 q is A Power of A Prime

So far we have assumed the order of the small field to be a prime q. It's natural to generalize to a power of a prime, $q = p^r$, where p is a odd prime and r is a integer greater than 1. Then we consider the elliptic curve:

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbb{F}_{(p^r)^k} \qquad (A, B \in \mathbb{F}_{p^r}). \tag{2.58}$$

Also we hope the ratio:

$$M_k = M_k(E/\mathbb{F}_q) = \frac{|E(\mathbb{F}_{(p^r)^k})|}{|\mathbb{F}_{p^r}|} \tag{2.59}$$

will be a prime.

If we still let t_1 denote the trace of $E(\mathbb{F}_{p^r})$, the ratio in Formula (2.59) can still be expressed as $B_k(t_1, p^r)$, the evaluation of polynomial $B_k(x, p^r)$ at $x = t_1$. From Theorem 2.2.3 and Theorem 2.2.4, we know that $B_k(x, p^r)$ is also irreducible and abelian. Thus we can again use the modified Bateman-Horn's conjecture to estimate the number of t_1 which make $B_k(t_1, p^r)$ prime.

Again, if we want the prime orders of the elliptic curve subgroups to have bit size between 163 and 256, appropriate powers of primes should be chosen. For example, when $k = 7$, appropriate q's could be:

$$\begin{aligned}
&3^{18}, 3^{19}, \ldots, 3^{26};\\
&5^{13}, 5^{14}, \ldots, 5^{18};\\
&7^{10}, 7^{11}, \ldots, 7^{15};\\
&11^{9}, 11^{10}, \ldots, 11^{12};\\
&\ldots
\end{aligned}$$

These numbers are chosen so that the prime orders of the elliptic curve subgroups have between 163 and 256 bits.

Some experimental data shows that we can estimate the number of t_1 which make the order of $E(\mathbb{F}_{(p^r)^k})$ almost prime.

Table 9. Experimental data for random $E(\mathbb{F}_{(p^r)^k})$

k	q	C_{BH}	$Count_l$	$Count_r$	Total	BH-estimate	Ratio
7	PP(2^{18})	3.7452	1223	1208	2431	2485	0.9783
7	PP(2^{19})	4.4999	2355	2406	4761	4900	0.9716

In the implementation of finite fields, calculation over a prime order field is much slower than over an extension of a small field, assuming both have same sizes. This is one advantage of $E(\mathbb{F}_{(p^r)^k})$. Plus, for each k, there will be a few more elliptic curves for cryptographical application; most important, all the arithmetic is on the small finite field $\mathbb{F}_p$. Hence the speed of implementation will be faster.

2.5.2 Curves of "Almost" Almost Prime Order

To make the result even more general, we could also consider the case that the ratio $\frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|}$ is a prime times a small integer. For example:

$$\begin{aligned}\frac{|E(\mathbb{F}_{q^k})|}{|E(\mathbb{F}_q)|} &= 2 \cdot \text{a prime}\\ &= 3 \cdot \text{a prime}\\ &= 4 \cdot \text{a prime}\\ &\dots\end{aligned}$$

These are also acceptable in cryptographical implementations. This case is more complicated and will be explored in the future.

2.5.3 Some Possible Attacks

MOV Attack

In this section, we will show that our curves are safe under the MOV attack.

The MOV attack, named after Menezes, Okamoto, and Vanstone [23], uses the Weil pairing to convert a discrete logarithm problem in $E(\mathbb{F}_q)$ to one in $\mathbb{F}_{q^m}^*$, where m is called the the embedding degree of $E(\mathbb{F}_q)$. Since discrete logarithm problems in finite fields can be attacked by index calculus methods, they can be solved faster than elliptic curve discrete logarithm problems, as long as the field $\mathbb{F}_{q^m}$ is not much larger than $\mathbb{F}_q$. See Washington [36] Chapter 5.3 or Menezes et al. [23] for more details about the MOV attack.

To make sure an elliptic curve is safe under the MOV attack, the embedding degree has to be large enough so that the discrete logarithm problem in $\mathbb{F}_{q^m}^*$ is also computationally infeasible; practically, the size of $\mathbb{F}_{q^m}^*$ needs to be at least 2^{1024}.

Briefly, the embedding degree m is determined as follows. See Koblitz and Menezes [20]: Let E be the elliptic curve $y^2 = x^3 + Ax + b$ defined over a finite field $\mathbb{F}_q$. Let n be a large prime which divides $|E(\mathbb{F}_q)|$. Assume the discrete logarithm problem is over an elliptic curve subgroup of order n. It is assumed that n does not divide q. The embedding degree m is the multiplicative order of q modulo n; in another words, it is the smallest positive k such that $n \mid q^k - 1$.

Generally, the embedding degree m is large except for supersingular curves (See Washington [36], Chapter 5.3) or specially constructed curves (See Freeman [12]). Results of Balasubramanian and Koblitz [3] show that curves having a large prime order subgroup usually have a large embedding degree, i.e., m has size comparable to n.

In our case, the elliptic curve $E(\mathbb{F}_{q^k})$ has a large subgroup of prime order $n = B_k(t_1, q)$ for some integer t_1. From Formula (2.56) we know that

$$n = B_k(t_1, q) \sim q^{k-1}. \tag{2.60}$$

The curves we chose all have $\log_2 q^{k-1} \geq 163$. As long as $\log_2 q^{km} \geq 1024$, the discrete logarithm problem over $\mathbb{F}_{q^{km}}$ is still computational infeasible. To simplify the estimation we let $\log_2 q^{(k-1)m} \geq 1024$. We can see that when $m = 6$, $\log_2 q^{(k-1)6} \geq 978$ and when $m = 7$, $\log_2 q^{(k-1)6} \geq 1141$. So the embedding degree $m \geq 7$ will make the curve safe enough under MOV attack.

The condition $m \geq 7$ will hold almost all the time by the result of Balasubramanian and Koblitz [3]. As we can see from the randomly generated curves in Example 2.4.1 and Example 2.4.2 in Section 2.4.1, the embedding degrees are large:

Example 2.5.1

We calculated all the embedding degrees for the curves in Example 2.4.1 *and Example* 2.4.2 *in Section 2.4.1:*

- $E(\mathbb{F}_{251^{23}})$, $t_1 = 13$:

$$n = 651774992213293993851502581696425303778883596013743 71,$$

$$m = 20241459385506024653773372102373456639095763851358 5.$$

- $E(\mathbb{F}_{251^{23}})$, $t_1 = 21$:

$$\begin{aligned} n &= 67434728631591889407146803889272030271229106076460131, \\ m &= 586388944622538168757798294689322002358513965882262. \end{aligned}$$

- $E(\mathbb{F}_{251^{23}})$, $t_1 = 25$:

$$\begin{aligned} n &= 68623005788095711246920315911144936702146215959138051, \\ m &= 2983608947308509184648709387441084204441139824310350. \end{aligned}$$

- $E(\mathbb{F}_{65521^{17}})$, $t_1 = -477$:

$$\begin{aligned} n &= 11453321082437429916818997544263400668196763269305691\backslash \\ &\quad 1532714032776326282148921, \\ m &= 28633302706093574792047493860658501670491908173264227\backslash \\ &\quad 883178508194081570537230. \end{aligned}$$

Weil Descent

Weil descent is an attack technique against ECC. One can map the discrete logarithm problem from the elliptic curve to a hyperelliptic curve with high genus. For the background of hyperelliptic curves and reduced security of hyperelliptic curves, see Chapter 3.

The curves we studied in this thesis are all over $\mathbb{F}_{q^k}$ where both k and q are odd primes and the coefficients of the curve equation are in F_q. The Weil descent attack on this type of curve is not practical yet. When $k \geq 11$, the attack is computational infeasible; when $k = 3, 5, 7$, only some specially constructed curves with curve equation coefficients in $\mathbb{F}_{q^k}$ can be attacked. See Diem [9] for more details.

3. ARITHMETIC OF REAL HYPERELLIPTIC CURVES

3.1 Hyperelliptic Curves in Cryptography

Hyperelliptic curves have been considered for use in cryptography since 1989. See Koblitz [18]. It appears only hyperelliptic curves of low genus are suitable for cryptographic use. See Müller et al. [26], Gaudry [13], Enge [10] and Theriault [34]. In this part of the thesis, we focus on hyperelliptic curves of genus 2. (We define genus in Section 3.2.)

Hyperelliptic curves can be distinguished into two scenarios: the imaginary model and the real model. See the next subsection for details. Hyperelliptic curves of the imaginary model have been widely studied for cryptographic use. See Cohen et al. [7]. Algorithms for them were studied by Lange [21], Wollinger et al. [39] and many other researchers.

The use of real model hyperelliptic curves was started by Artin [2]. Recently, works by Jacobson, Scheidler, Stein and Williams [32], [15] show that schemes based on real hyperelliptic curves can be as efficient as those of the imaginary model.

In the summer school at the University of Wyoming in 2006, explicit formulas for operations on real hyperelliptic curves were developed by Erickson, Shang and the author under the supervision of Professors Stein, Jacobson and Scheidler. The following part of the thesis will give the explicit formulas for the addition operation of real hyperelliptic curves, which were developed during the summer school by the author. Some improvement has been made since and further work continues.

For details on the arithmetic of hyperelliptic curves we refer to Cohen et al. [7], Menezes et al. [24], Jacobson and Menezes [15] and Jacobson et al. [16]. For real hyperelliptic curves we refer to Paulus and Ruck [27], Stein [31], Jacobson et al. [16] and Jacobson et al. [17].

3.2 Function Fields and Curves

The details related to function fields and hyperelliptic curves can be found in the books of Cohen et al. [7], Stichtenoth [33] and Rosen [28]. We will just give the minimum necessary background in this section; refereed papers and locations in books will be specified when needed. Let K be a field and $\overline{K}$ be its algebraic closure.

Definition 3.2.1 *An algebraic function field F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K and $F/K(x)$ is separable. For brevity, we shall simply refer to F/K as a function field.*

The simplest example of an algebraic function field is the *rational function field*: F/K is called *rational* if $F = K(x)$ for some $x \in F$ transcendental over K.

An arbitrary function field F/K(which is not necessarily rational) is represented as a simple algebraic field extension of a rational function field $K(x)$, i.e., $F = K(x, y)$ where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in K(x)[T]$. See page 2 of [33]. For example, let $F = K(x, y)$, where x and y satisfy the curve equation $C: \ g(x, y) = 0$ and $g \in K[x, y]$. When we say a function field $F = K(x, y)$, where x and y satisfy a curve equation C, we refer to F as $K(C)$.

Definition 3.2.2 *A valuation ring of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:*

1. *$K \subsetneq \mathcal{O} \subsetneq F$, and*
2. *for any $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

This definition is motivated by the following observation in the case of a rational function field $K(x)$: given an irreducible polynomial $p(x) \in K[x]$, consider the set

$$\mathcal{O}_{p(x)} := \left\{ \frac{f}{g} \;\middle|\; f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}. \tag{3.1}$$

Theorem 3.2.1 *Let $\mathcal{O}$ be a valuation ring of the function field F/K. Then*

1. *$\mathcal{O}$ is a local ring, i.e., $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O}/\mathcal{O}^*$, where $\mathcal{O}^* = \{z \in \mathcal{O} \mid \text{there is a } w \in \mathcal{O} \text{ with } zw = 1\}$ is the group of units of $\mathcal{O}$.*

2. *For $0 \neq x \in F$, $x \in P \;\Leftrightarrow\; x^{-1} \notin \mathcal{O}$.*

3. *For the field $\tilde{K}$ of constants of F/K we have $\tilde{K} \subseteq \mathcal{O}$ and $\tilde{K} \cap P = 0$*

See Stichtenoth [33] Section **I.1** for a proof.

Definition 3.2.3 *A place P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Any element $t \in P$ such that $P = t\mathcal{O}$ is called a prime element for P. Let $\mathbb{P}_F := \{P \mid P \text{ is a place of } F/K\}$.*

If $\mathcal{O}$ is a valuation ring of F/K and P its maximal ideal, then $\mathcal{O}$ is uniquely determined by P, namely $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Hence $\mathcal{O}_P := \mathcal{O}$ is called the valuation ring of the place P. The place associated with $\mathcal{O}_{p(x)}$ as defined in Formula (3.1) is denoted as $P_{p(x)}$. See Stichtenoth [33] Section **I.1** for details.

There is a valuation ring of $K(x)/K$, namely

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in K[x], \deg f(x) \leq g(x) \right\}, \tag{3.2}$$

with maximal ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in K[x], \deg f(x) < g(x) \right\}. \tag{3.3}$$

P_∞ is called the *place at infinity.*

Theorem 3.2.2 *There are no places of the rational function field $K(x)/K$ other than the places $P_{p(x)}$ and P_∞.*

See Stichtenoth [33] Section **I.2** for a proof.

Definition 3.2.4 *A discrete valuation of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:*

1. *$v(x) = \infty \Leftrightarrow x = 0$.*

2. *$v(x, y) = v(x) + v(y)$ for any $x, y \in F$.*

3. *$v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$.*

4. *There exists an element $z \in F$ with $v(z) = 1$.*

5. *$v(a) = 0$ for any $0 \neq a \in K$.*

It's easy to see that the image of v_P is in $\mathbb{Z}$. Two valuations of P are said to be *equivalent* if they are positive multiples of each other. A valuation v_P is said to be *normalized* if its image covers the whole of $\mathbb{Z}$. See Weiss [37] Chapter 2.

Theorem 3.2.3 *To any place $P \in \mathbb{P}_F$ we associate a function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ that is proved to be a discrete valuation of F/K: Choose a prime element t for P. Then every $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_P^*$ and $n \in \mathbb{Z}$, define $v_P(z) := n$ and $v_P(0) := \infty$. Moreover, we have*

$$\mathcal{O}_P = \{z \in F \mid v_P \geq 0\}, \tag{3.4}$$

$$\mathcal{O}_P^* = \{z \in F \mid v_P = 0\}, \tag{3.5}$$

$$P = \{z \in F \mid v_P > 0\}. \tag{3.6}$$

See Stichtenoth [33] Section **I.1** for a proof.

According to Theorem 3.2.3, places, valuation rings and discrete valuations of a function field refer to the same thing.

Definition 3.2.5 *Let $P \in \mathbb{P}_F$. $F_P := \mathcal{O}_P/P$ is the residue class field of P. Define $x(P) \in \mathcal{O}/P$ to be the residue class of x modulo P; for $x \in F \backslash \mathcal{O}_P$ we put $x(P) := \infty$. The map $x \mapsto x(P)$ is called the residue class map with respect to P. We can also use the notation $x + P := x(P)$ for $x \in \mathcal{O}_P$. $\deg P := [F_P : K]$ is called the degree of P.*

Definition 3.2.6 *The (additively written) free abelian group generated by the places of F/K is denoted by $\mathcal{D}_F$, the divisor group of F_K. The elements of $\mathcal{D}_F$ are called divisors of F/K. In other words, a divisor is a formal sum*

$$D = \sum_{P\in\mathbb{P}_F} n_P P \quad \textit{with } n_P \in \mathbb{Z}, \textit{ and almost all } n_P = 0. \tag{3.7}$$

The support of D is defined by

$$\textit{supp } D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}. \tag{3.8}$$

It will often be found convenient to write

$$D = \sum_{P\in S} n_P P, \tag{3.9}$$

where $S \subseteq \mathbb{P}_F$ is a finite set with $S \supseteq$ supp D.

A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called a prime divisor. Two divisors $D = \sum n_P P$ and $D' = \sum n_P^{'} P$ are added coefficientwise:

$$D + D^{'} = \sum_{P\in\mathbb{P}_F} (n_P + n_P^{'})P. \tag{3.10}$$

The zero element of the divisor group $\mathcal{D}_F$ is the divisor

$$0 \ := \sum_{P\in\mathbb{P}_F} r_P P, \quad \textit{all } r_P = 0. \tag{3.11}$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathcal{D}_F$ we define $v_Q(D) := n_Q$. Therefore

$$\textit{supp } D \ = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \ \textit{ and } \ D = \sum_{P\in supp\ D} v_P(D) \cdot P. \tag{3.12}$$

A partial ordering on $\mathcal{D}_F$ is defined by

$$D_1 \leq D_2 \ :\Leftrightarrow \ v_P(D_1) \leq v_P(D_2) \ \textit{ for every } P \in \mathbb{P}_F. \tag{3.13}$$

A divisor $D \geq 0$ is called positive (or effective). The degree of a divisor is defined by

$$\deg D \ := \sum_{P\in\mathbb{P}_F} v_P(D) \cdot \deg P. \tag{3.14}$$

Note that $\deg :\ \mathcal{D}_F \to \mathbb{Z}$ *is a group homomorphism.*

See Stichtenoth [33] Section **I.4** for details.

Definition 3.2.7 *Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (poles) of x in $\mathbb{P}_F$. Then we define*

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \quad \textit{the zero divisor of } x, \tag{3.15}$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P, \quad \textit{the pole divisor of } x, \tag{3.16}$$

$$(x) := (x)_0 - (x)_\infty. \tag{3.17}$$

Clearly $(x)_0 \geq 0$, $(x)_\infty \geq 0$ and

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P. \tag{3.18}$$

The elements $0 \neq x \in F$ which are constant are characterized by

$$x \in K \Leftrightarrow (x) = 0. \tag{3.19}$$

Definition 3.2.8

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\} \tag{3.20}$$

is called the group of principal divisors of F/K. This is a subgroup of $\mathcal{D}_F^0$, since for $0 \neq x, y \in F$, $(xy) = (x) + (y)$ by 3.18. *The factor group*

$$\mathcal{C}_F := \mathcal{D}_F / \mathcal{P}_F \tag{3.21}$$

is called the divisor class group. For a divisor $D \in \mathcal{D}_F$, the corresponding element in the factor group $\mathcal{C}_F$ is denoted by $[D]$, the divisor class of D. Two divisors $D, D^{'} \in \mathcal{D}_F$ are said to be equivalent, written

$$D \sim D^{'}, \tag{3.22}$$

if $[D] = [D^{'}]$, i.e., $D = D^{'} + (x)$ for some $x \in F \backslash \{0\}$. It is known that degree of a principal divisor is zero, the degree function gives rise to a homomorphism from $\mathcal{C}_F$ to $\mathbb{Z}$. The kernel of this map is denoted $\mathcal{C}_F^0$, the group of divisor classes of degree zero.

See Rosen [28], Chapter 5, for details.

Definition 3.2.9 *For a divisor $A \in \mathcal{D}_F$ we set*

$$\mathcal{L}(A) \ := \{x \in F \mid (x) \geq -A\} \cup \{0\}. \tag{3.23}$$

One can prove that $\mathcal{L}(A)$ is a finite-dimensional vector space over K for any $A \in \mathcal{D}_F$. The integer $\dim A := \dim \mathcal{L}(A)$ *is called the dimension of the divisor. The genus g of F/K is defined by*

$$g := \max\{\ \deg A - \dim A + 1 \mid A \in \mathcal{D}_F\}. \tag{3.24}$$

For details about the definition of genus, see Stichtenoth [33], Section **I.4**.

Definition 3.2.10 *Consider an algebraic extension F'/K' of F/K. A place $P' \in \mathbb{P}_{F'}$ is said to lie over $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say that P' is an extension of P or that P lies under P', and we write $P'|P$. Let $P' \in \mathbb{P}_{F'}$ be a place of F'/K' lying over $P \in \mathbb{P}_F$. The integer $e(P'|P) := e$ with*

$$v_{P'}(x) = e \cdot v_P(x), \quad for\ any\ x \in F, \tag{3.25}$$

is called the ramification index of P' over P. We say that $P'|P$ is ramified if $e(P'|P) > 1$, and $P'|P$ is unramified if $e(P'|P) = 1$.

For a place $P \in \sum_{F/K}$ we define its conorm (with respect to F'/F) by

$$Con_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P', \tag{3.26}$$

where the sum runs over all places $P' \in \mathbb{P}_{F'}$ lying over P.

We also need this definition.

Definition 3.2.11 *A hyperelliptic function field over K is an algebraic function field F/K of genus $g \geq 1$ which contains a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$.*

Note: Here we consider elliptic curves as hyperelliptic curves of genus 1.

Let $F = K(C)$. The *ring of integers* of F is defined as $K[C] = K[x,y]/(y^2 + h(x)y - f(x))$. It can be proved that $K[C]$ is a Dedekind domain. Then the notion of fractional ideal is defined over $K[C]$, and the ideal class group $\mathrm{CL}(K)$ of F in $K[C]$ is the abelian group of fractional ideals of $K[C]$ modulo principal fractional ideals of $K[C]$. See Cohn [8] for definitions of principal fractional ideal and ideal class group. The relation between divisor classes and ideals will be given later in this section.

We will focus on hyperelliptic curves of genus 2 over a finite field. More particularly, we will develop algorithms for hyperelliptic curves over odd characteristic finite fields. We let $\mathbb{F}_q$ be a finite field with $q = p^l$ elements, where p is a odd prime and let $\overline{\mathbb{F}}_q$ be its algebraic closure.

We give the following definition for hyperelliptic curves over $\mathbb{F}_q$ with explicit equations. For a more general definition, we refer to Jacobson et al. [11].

Definition 3.2.12 *Let $\mathbb{F}_q$ have odd characteristic. A hyperelliptic curve C of genus 2 defined over $\mathbb{F}_q$ is an absolutely irreducible*[1] *nonsingular curve defined by an equation of the form*

$$C \ : \ y^2 = f(x), \tag{3.27}$$

where $f \in \mathbb{F}_q[x]$, $y^2 - f(x)$ is absolutely irreducible, and $\deg f \leq 6$. Denote $G(x,y) = y^2 - f(x)$. If $G(a,b) = 0$ for some $(a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$, then either $G_x(a,b) \neq 0$ or $G_y(a,b) \neq 0$. The hyperelliptic curve is called

1. *an imaginary hyperelliptic curve if:*

$$f(x) = x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0. \qquad (f_i \in \mathbb{F}_q) \tag{3.28}$$

2. *a real hyperelliptic curve if:*

$$f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0. \qquad (f_i \in \mathbb{F}_q) \tag{3.29}$$

[1] An absolutely irreducible polynomial is irreducible, even in any finite extension of the field of coefficients.

From now on, we only consider the real model hyperelliptic curves of genus 2.

For $\mathbb{F}_q(C)$, the pole divisor ∞ of x in $F_q(x)$ decomposes into two different prime divisors ∞_1 and ∞_2 for real model of hyperelliptic curve. Let v_1 and v_2 be the normalized valuations of $\mathbb{F}_q(C)$ corresponding to ∞_1 and ∞_2. See Paulus and Ruck [27]

For a real hyperelliptic curve C, a divisor can be written in the form:

$$D = D_0 - deg(D_0)\infty_2 + v_1(D)(\infty_1 - \infty_2), \tag{3.30}$$

where D_0 is a divisor not divisible by ∞_1 or ∞_2. D is called semi-reduced if D_0 is effective and not divisible by the conorm of any divisor in $\mathbb{F}_q(x)$; it's called reduced if it's semi-reduced and $\deg(D_0) \leq 2$.

For a real hyperelliptic curve C, Paulus and Ruck [27] showed that each divisor class $\overline{D} \in \mathcal{C}_F^0$ can be uniquely represented by the reduced divisor

$$D = \sum_{i=1}^{r} P_i - r'\infty_2 + v_1(D)(\infty_1 - \infty_2)\ , \tag{3.31}$$

where $\sum_{i=1}^{r} P_i$ is effective and $\deg A \leq 2$; $\sum_{i=1}^{r} P_i$ is not divisible by ∞_1, ∞_2 or the conorm of a divisor of $\mathbb{F}_q(x)$. Also, $0 \leq r + v_1(D) \leq 2 = g$.

The order of the degree 0 divisor class containing $\infty_1 - \infty_2$ is called the *regulator* R of $\mathbb{F}_q(C)$ in $\mathbb{F}_q[C]$. The regulator plays an important role in real hyperelliptic curve cryptography. In Stein et al. [32], a secure key-exchange protocol was developed by making use of the arithmetic in real quadratic function fields. Computation of the regulator is itself an instance of computing a discrete logarithm as defined in Stein et al. [32]; furthermore, the size of the regulator also provides a measure for the key space.

It is known that $R = O(q^{(1/2)\deg f})$ (See Paulus and Ruck [27]), where f is as in Definition 3.2.12.

Example 3.2.1

$$\begin{aligned} E_1: \;\; & y^2 = f(x) \;\; \textit{over}\; \mathbb{F}_{10000000007}, \\ & f(x) = x^4 + 557289x^3 + 722527380x^2 + 352336240x + 641315936, \\ & R = 1000041901. \\ E_2: \;\; & y^2 = f(x) \;\; \textit{over}\; \mathbb{F}_{1073741741}, \\ & f(x) = x^6 + 205912371x^5 + 859304427x^4 + 77543919x^3 + 603307144x^2 \\ & \qquad + 131571390x + 807786564, \\ & R = 288230461703812884. \end{aligned}$$

A fractional ideal $\mathfrak{a} \in \mathbb{F}_q[C]$ can be represented as $\mathfrak{a} = \mathbb{F}_q[x][d(x)u(x), d(x)(v(x)+y)]$ where, u, $v \in \mathbb{F}_q[x]$ and $u \mid f - v^2$. $\mathfrak{a}$ is *primitive* when $d(x) = 1$, and in that case we can write $\mathfrak{a} = [u(x), v(x) + y]$. If $\mathfrak{a}$ is primitive and $\deg u \leq g$, it is called *reduced.* The degree of $\mathfrak{a}$ is defined as $\deg(\mathfrak{a}) = \deg(u)$. The basis $\{u(x), v(x) + y\}$ of a primitive ideal is called *adapted* or *standard* if $\deg(v) < \deg(u)$ and u is monic; the basis is called *reduced* if $\deg(v - y) < \deg(u) < \deg(v + y)$ and u is monic. Hence a fractional ideal can be represented by a unique pair of polynomials $[u, v]$. Hence the ideal (or equivalently the divisor class) in $\mathcal{R}$ can be represented by a unique pair of polynomials.

Paulus and Ruck [27] showed that there is a one-to-one correspondence between $\mathcal{C}_F^0$ and the set of reduced ideals in $\mathbb{F}_q[C]$. More specifically, there is a canonical bijection between $\mathcal{C}_F^0$ and the set of pairs $\{(\mathfrak{a}, n)\}$, where $\mathfrak{a}$ is a reduced ideal of $\mathbb{F}_q[C]$ and n is an integer with $0 \leq \deg(\mathfrak{a}) + n \leq 2 = g$. We will just focus on a group of principal reduced ideals: $\mathcal{R} = \{(\mathfrak{a}, 0) \mid \mathfrak{a} \text{ is reduced and principal}\}$. Or we can abuse the notation and let $\mathcal{R} = \{\overline{D} \mid \overline{D} \text{ coresponds to } (\mathfrak{a}, 0), \text{ where } \mathfrak{a} \text{ is reduced and principal}\}$ because of the one-to-one correspondence.

Now we introduce an ordering for $\mathcal{R}$. Fix $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C] \in \mathcal{R}$. For any ideal $\mathfrak{b} \in \mathcal{R}$, since $\mathfrak{a}_1$ and $\mathfrak{b}$ in the same principal ideal class, $\exists\ \alpha \in K^*$ with $\mathfrak{b} = (\alpha)\mathfrak{a}_1$. Let $\delta(\mathfrak{b}, \mathfrak{a}_1) = -v_1(\alpha) \pmod{R}$. Note that the distance is defined modulo R, there will be up to R many reduced ideals in each ideal class. Thus, we can write $\mathcal{R} =$

$\{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m\}$ where $m \leq R$ and $\delta(\mathfrak{a}_1) = 0 < \delta(\mathfrak{a}_2) < \ldots < \delta(\mathfrak{a}_m)$. (Also we can denote $\mathcal{R} = \{\overline{D}_1, \overline{D}_2, \ldots, \overline{D}_m\}$, where $\delta(\overline{D}_1) = 0 < \delta(\overline{D}_2) < \ldots < \delta(\overline{D}_m)$). $\mathcal{R}$ is called the *infrastructure* of the principal ideal class. See Jacobson et al. [17] for details.

As we said before, each ideal or divisor class in $\mathcal{R}$ can be represented by a pair of polynomials. Hence for a hyperelliptic curve of real model as in 3.2.12, we may denote $\overline{D} = \mathrm{div}(u, v)$, where u and v satisfy:

(P1) u is monic,

(P2) $\deg u \leq g$,

(P3) $u \mid v^2 - f$, and

(P4) one of the following degree conditions is satisfied, namely,

a. for the reduced basis: $-v_1(v - y) < -v_1(u) = \deg(u) < -v_1(v + y)$, or

b. for the adapted (standard) basis: $\deg(v) < \deg(u)$.

See Jacobson et al. [17] or Erickson et al. [11] for details.

$\overline{D} \in \mathcal{R}$ is uniquely determined by its distance $\delta(\overline{D})$. In practice, it is infeasible to actually determine $\delta(\overline{D})$ from u and v; in fact, the security of the cryptographic schemes (Stein et al. [32]) is based on the fact that computing $\delta(\overline{D})$ is infeasible.

Because the divisor class can be uniquely represented by a reduced divisor in it, in practice, we really just deal with the reduced divisors. So we can write $\mathcal{R} = \{D_1, D_2, \ldots, D_m\}$, where D_i is the reduced divisor representing $\overline{D_i}$.

Two operations on the elements of $\mathcal{R}$ are defined and studied (see Jacobson et al. [16], Stein [32], Paulus and Ruck [27]: baby step, $D_i \rightarrow D_{i+1}$, and giant step, $D \oplus D'$. It is important to know the properties of distance of the elements of $R_{\mathfrak{a}}$ and also how distances behave under the operations on $\mathcal{R}$:

Distance Properties:

1. $\delta_1 = 0$, $\delta_2 = g+1$, and $1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$;

2. $g + i + 1 \leq \delta_i \leq (i-1)g + 1$ for $2 \leq i \leq |\mathcal{R}|$;

3. $\delta(D \oplus D') = \delta(D) + \delta(D') - d$, where $0 \leq d \leq 2g$, for $D, D' \in \mathcal{R}$.

Notice that δ is defined modulo R and the set $\mathcal{R}$ is closed under giant steps.

It can be seen from the above properties that the distance after a baby step and after a giant step is not definitely determined by $\delta(D)$ and $\delta(D')$, but some heuristics are available to help to simplify the protocols:

Heuristics: (Jacobson et al. [16])

For sufficiently large q, the following properties hold with probability $1 - O(q^{-1})$:

(H1) $\delta(D_{i+1}) - \delta(D_i) = 1$ for all $D \in \mathcal{R} \setminus \{0\}$.

(H2) The quantity d in Property 3 is always equal to $\lceil g/2 \rceil$. That is, for all $D, D' \in \mathcal{R} \backslash \{0\}$, we have $\delta(D \oplus D') = \delta(D) + \delta(D') - \lceil g/2 \rceil$.

There is overwhelming numerical evidence as well as plausible theoretical considerations to support the above heuristics, especially for large q. See Jacobson et al. [16].

Although $\mathcal{R}$ is closed under giant steps, it is not associative, i.e., it is not necessarily the case that $\delta((D \oplus D') \oplus D'') = \delta((D) \oplus (D' \oplus D''))$ for $D, D', D'' \in \mathcal{R}$. However, $\mathcal{R}$ is "almost" associative in the sense that the operation $\oplus$ is almost distance preserving (Distance Property 3). d can be efficiently computed (see Paulus and Ruck [27]). It follows that the distance of the divisor $D \oplus D'$ is extremely close to, and just below, the sum of the distances of the divisors D and D', with a "shortfall" d of at most $2g$. Thus the use of the terms "baby step" and "giant step" is justified: the former yields a very small advance in distance, namely at most linear in g, whereas the latter generally results in a large jump.

In this thesis, we will focus on the explicit formulas for giant step: given two divisor classes in $\mathcal{R}$, $\overline{D}_1 = [u_1, v_1], \overline{D}_2 = [u_2, v_2] \in \mathcal{R}$, find $\overline{D}' = [u', v'] = \overline{D}_1 \oplus \overline{D}_2$ such that D' is reduced.

3.3 Algorithm

Algorithm 3.3.1 Basic Addition Algorithm.

Composition.

INPUT: $\overline{D}_1 = [u_1, v_1]$, $\overline{D}_2 = [u_2, v_2]$, $C : \; y^2 = f(x)$.

OUTPUT: $\overline{D} = [u, v]$, *D semi-reduced and* $\overline{D} = \overline{D}_1 \oplus \overline{D}_2$.

```
1. Compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$;
2. Compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2(v_1 + v_2 + h)$;
3. Let $s_1 = c_1 e_1$, $s_2 = c_1 e_2$, $s_3 = c_2$;
4. Let $u = u_1 u_2 / d^2$;
   $v = (s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 f))/d \mod u$.
```

Reduction.

INPUT: $\overline{D} = [u, v]$, *D semi-reduced,*

OUTPUT: $\overline{D'} = [u', v']$, *D' reduced with* $\overline{D'} = \overline{D}$.

```
1. Compute $u' = (f - v^2)/u$, $v' = (-v) \mod u'$;
2. If $\deg u' > g$ put $u = u'$, $v = v'$;
   go to step 1;
3. Make $u'$ monic;
```

In most cases $D = [u, v]$ has u of degree 2, i.e., $u = x^2 + u_1 x + u_0$, especially when q is large. Thus, when we care about the speed of the giant step operation on divisors, we just need to focus on the case when $\deg u = 2$. Operations on divisors with $\deg u \leq 2$ need less time, actually, they can be considered as a degenerate case of the general case. We give the formulas only for $\deg u = 2$.

Also, we assume that when we calculate $[u_1, v_1] \oplus [u_2, v_2]$ with $\deg u_1 = \deg u_2 = 2$, u_1 and u_2 do not have a common root. The special case when there does exist a common root will cost less; see Cohen et al. [7] Section 14.3.1.

To optimize the computations we do not follow Algorithm 3.3.1 literally. Instead, we outline our algorithm as follows and prove that it produces the right solution:

Algorithm 3.3.2 Optimized Addition Algorithm.

INPUT*:* $\overline{D}_1 = [u_1, v_1]$, $\overline{D}_2 = [u_2, v_2]$, $\gcd(u_1, u_2) = 1$. $C : y^2 = f(x)$.

OUTPUT*:* $\overline{D} = [u', v']$, *D reduced with* $\overline{D} = \overline{D}_1 \oplus \overline{D}_2$.

$$s \leftarrow \frac{v_1 - v_2}{u_2} \mod u_1 \qquad (\deg s = 1), \tag{3.32}$$

$$k \leftarrow \frac{f - v_2^2}{u_2} \qquad (\deg k = 4), \tag{3.33}$$

$$l \leftarrow su_2 \qquad (\deg l = 3), \tag{3.34}$$

$$u \leftarrow \frac{k - s(l + 2v_2)}{u_1} \qquad (\deg u = 2), \tag{3.35}$$

$$u' \leftarrow u \text{ made monic} \qquad (\deg u' = 2), \tag{3.36}$$

$$v' \leftarrow (-(l + v_2)) \mod u' \qquad (\deg v' = 1). \tag{3.37}$$

Proposition 3.3.1 *Algorithm* 3.3.2 *produces the same result as Algorithm* 3.3.1*.*

Proof Since $\gcd(u_1, u_2) = 1$, we have $d = 1$ in Algorithm 3.3.1. We can choose e_1 and e_2 to have $e_1u_1 + e_2u_2 = 1$; choose $c_1 = 1$ and $c_2 = 0$ to make $s_1 = e_1$, $s_2 = e_2$ and $s_3 = 0$. Then $u = u_1u_2$ and $v = s_1u_1v_2 + s_2u_2v_1 \mod u_1u_2$. By using $s_1u_1 + s_2u_2 = 1$, one has

$$v \equiv v_1 \pmod{u_1}, \tag{3.38}$$

$$v \equiv v_2 \pmod{u_2}. \tag{3.39}$$

By the Chinese remainder theorem, one can obtain v by solving the above system of equations (note that $\gcd(u_1, u_2) = 1$). In other words, as long as a v satisfies Equations (3.38) and (3.39), it is the result of the composition part of Algorithm 3.3.1. Now we can verify that in Algorithm 3.3.2, $v = l + v_2$ satisfies Equations (3.38) and (3.39). Notice that

$$v = \left(\frac{v_1 - v_2}{u_2} \mod u_1\right) u_2 + v_2.$$

Equation (3.39) can be verified by straightforward calculation. For Equation (3.38) we can see

$$v \equiv \left(\frac{v_1 - v_2}{u_2}\right) u_2 + v_2 \equiv \left(\frac{v_1 - v_2}{u_2}\right) u_2 + v_2 \equiv u_1 \pmod{u_1}.$$

Now we can see Equation (3.35) gives

$$\begin{aligned} u &= \frac{k - s(l + 2v_2)}{u_1} \\ &= \frac{\left(f - v_2^2\right)/u_2 - s(su_2 + 2v_2)}{u_1} \\ &= \frac{f - v_2^2 - s^2u_2^2 - 2su_2v_2}{u_1u_2} \\ &= \frac{f + (su_2 + v_2)^2}{u_1u_2} \\ &= \frac{f + v^2}{u_1u_2}, \end{aligned}$$

the same as the composition part of Algorithm 3.3.1. After making u monic and letting $v' = (-h - v) \mod u'$, we obtain the same result of u' and v' as Algorithm 3.3.1.

■

3.3.1 Formulas

In this section we give the explicit formulas in Table 10. It is a straightforward algorithm with input of two divisors and output of the sum of the two divisors. (Numerical results based on the improved version of this algorithm can be seen in Erickson et al. [11]). Notes about some tricks in the algorithm and detailed derivation of the formulas are given after the table.

Table 10 gives the formulas for curves on an odd characteristic field and the number of operations on a finite field. The even characteristic case is very similar and costs the same number of operations on a finite field. See Erickson et al. [11] for more details. We count only inversions, squarings and multiplications, which constitute the main part of the computation when compared with additions and subtractions. In the tables below, we let I, S and M denote “inversion,” “squaring,” and “multiplication,” respectively. In finite field arithmetic, a squaring and a multiplication cost similar time, while an inversion costs about 50 to 80 times that of a multiplication. In each step of the following table, the underlined part summarizes what that particular step calculates.

The property (**P4**) gives different forms for the pair $[u, v]$. (**P4.a**) gives

$$u = x^2 + u_1 x + u_0, \tag{3.40}$$

$$v = x^3 + v_1 x + v_0. \tag{3.41}$$

(**P4.b**) gives

$$u = x^2 + u_1 x + u_0, \tag{3.42}$$

$$v = v_1 x + v_0. \tag{3.43}$$

To achieve algorithms with fewer operations, we find the (**P4.a**) form is slightly better.

Here we only give the formulas for curves over $\mathbb{F}_q$ of odd characteristic. We also assume that characteristic of the base field is not 3, such that we may assume $f_5 = 0$ in Formula (3.29) (by applying $x \mapsto x - f_5/6$). The addition algorithm for curves with even characteristic is slightly different but the number of the operations is similar to that of curves over an odd characteristic $\mathbb{F}_q$.

Table 10. Formulas for Addition of Divisors

Addition, deg u_1=deg $u_2 = 2$	
Input	$u_1 = x^2 + u_{11}x + u_{10}$, $v_1 = x^3 + v_{11}x + v_{10}$ $u_2 = x^2 + u_{21}x + u_{20}$, $v_2 = x^3 + v_{21}x + v_{20}$ $\gcd(u_1, u_2) = 1$, $C:\ y^2 = f(x)$.
Output	$[u',v']=[u_1, v_1] \oplus [u_2, v_2]$

Step	Expression	Operations
1	$\underline{k = k_2x^2 + k_1x + k_0}$ $k_2 = f_4 - 2v_{21}$	
2	$\underline{\text{resultant } r \text{ and } (rs \mod u_1) = s_1'x + s_0'}$ $z_1 = u_{11} - u_{21}$, $z_2 = u_{20} - u_{10}$, $z_3 = u_{11} \cdot z_1 + z_2$; $w_1 = v_{11} - v_{12}$, $w_0 = v_{10} - v_{20}$; $r = z_1 \cdot z_1 \cdot u_{10} + z_2 \cdot z_3$; $s_1' = w_0 \cdot z_1 + w_1 \cdot (2z_2 - z_3)$, $s_0' = w_0 \cdot z_2 - w_1 \cdot z_1u_{10}$ (denote $s = s_1x + s_0$)	8 **M**
3	$\underline{s = x + \frac{s_0}{s_1},\ \frac{s_0}{s_1},\ \frac{1}{s_1+2}, \frac{1}{s_1(s_1+2)},\ s_1,\ s_0}$ $I = (r \cdot (s_1' + 2r) \cdot s_1')^{-1}$, $\frac{s_0}{s_1} = r(s_1' + 2r) \cdot s_0' \cdot I$, $\frac{1}{s_1+2} = s_1' \cdot r^2 \cdot I$ $\frac{1}{s_1(s_1+2)} = r \cdot r^2I$, $s_1 = (s_1')^2 \cdot (s_1' + 2r) \cdot I$, $s_0 = s_1 \cdot \frac{s_0}{s_1}$	I, 10 M, 2 S
4	$\underline{u' = x^2 + u_1'x + u_0'}$ $u_1' = \frac{s_0}{s_1} + \frac{1}{s_1+2} \cdot (s_0 - 2u_{21}) + u_{21} - u_{11}$ $u_0' = \frac{1}{s_1(s_1+2)} \cdot (s_0^2 - k_2) + \frac{1}{s_1+2} \cdot (2s_0 \cdot u_{21} - 2u_{20} + 2v_{21}) + u_{20} -$ $u_{10} - u_1' \cdot u_{11}$	5 M, 1 S
5	$\underline{v' = x^3 + v_1'x + v_0'}$ $\lambda_3 = -s_1 - 1$, $\lambda_2 = -s_0 - s_1 \cdot u_{21}$ $\lambda_1 = -s_0u_{21} - s_1 \cdot u_{20} - v_{21}$, $\lambda_0 = -s_0 \cdot u_{20} - v_{20}$ $v_1' = [\lambda_1 - u_0' \cdot (\lambda_3 - 1)] - u_1' \cdot [\lambda_2 - u_1' \cdot (\lambda_3 - 1)]$ $v_0' = \lambda_0 - u_0' \cdot [\lambda_3 - u_1'(\lambda_3 - 1)]$	7 M
Total		I, 3 S, 30 M

Notes:

1. Step 2 calculates the coefficients of $s = s_1x + s_0 = (v_1 - v_2) \cdot (u_2)^{-1} \mod u_1$. Instead of calculating s_1 and s_0, we calculate $s_1' = r \cdot s_1$ and $s_0' = r \cdot s_0$ so that there is no inversion calculation until step 3. The details are: We know

$$s = (v_1 - v_2)u_2^{-1} \mod u_1.$$

Instead of calculating $u_2^{-1} \mod u_1$, we calculate $ru_2^{-1} \mod u_1$ without an inverse operation on the base field, where $r \in K^*$. In more detail, denote

$$ax + b = u_2^{-1} \mod u_1 \quad \text{where } a, b \in K^*.$$

Then

$$\begin{aligned}(ax + b)(x^2 + u_{21}x + u_{20}) &= 1 \mod u_1,\\ a(u_{21} - u_{11})x^2 + [a(u_{20} - u_{10}) + b(u_{21} - u_{11})]x + b(u_{20} - u_{10}) &= 1 \mod u_1.\end{aligned}$$

We will have

$$\begin{aligned}a(u_{21} - u_{11})x^2 + [a(u_{20} - u_{10}) + b(u_{21} - u_{11})] - a(u_{21} - u_{11})u_{11} &= 0,\\ b(u_{20} - u_{10}) - a(u_{21} - u_{11})u_{10} &= 1,\end{aligned}$$

i.e.,

$$\begin{pmatrix} (u_{20} - u_{10}) - (u_{21} - u_{11})u_{11} & (u_{21} - u_{11}) \\ -(u_{21} - u_{11})u_{10} & (u_{20} - u_{10}) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Denote

$$A = \begin{pmatrix} (u_{20} - u_{10}) - (u_{21} - u_{11})u_{11} & (u_{21} - u_{11}) \\ -(u_{21} - u_{11})u_{10} & (u_{20} - u_{10}) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}. \tag{3.44}$$

By linear algebra,

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} = \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Hence

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} ra \\ rb \end{pmatrix} = \begin{pmatrix} -a_2 \\ a_1 \end{pmatrix}.$$

Then we get

$$\begin{aligned} r &= a_1 a_4 - a_2 a_3 && (3.45) \\ &= [(u_{20} - u_{10}) - (u_{21} - u_{11})u_{11}](u_{20} - u_{10}) && (3.46) \end{aligned}$$

and

$$\begin{aligned} rs &= (v_1 - v_2)(rax + rb) \mod u_1, \\ rs_1 x + rs_0 &= [(v_{11} - v_{21})x + (v_{10} - v_{20})](-a_2 x + a_1) \mod u_1, \\ rs_1 x + rs_0 &= [a_1(v_{11} - v_{21}) - a_2(v_{10} - v_{20}) - u_{11}(v_{11} - v_{21})(-a_2)]x \\ &\quad + a_1(v_{10} - v_{20}) - u_{10}(v_{11} - v_{21})(-a_2). \end{aligned}$$

Hence

$$\begin{aligned} rs_1 &= a_1(v_{11} - v_{21}) - a_2(v_{10} - v_{20}) - u_{11}(v_{11} - v_{21})(-a_2), && (3.47) \\ rs_2 &= a_1(v_{10} - v_{20}) - u_{10}(v_{11} - v_{21})(-a_2). && (3.48) \end{aligned}$$

2. In Step 3, we need to calculate m_4^{-1} to make m monic and r^{-1} to get s_1 and s_0. The two inverses can be calculated by just one inversion operation plus several multiplication operations in the finite field. Namely, calculate $(m_4 \cdot r)^{-1}$ first, let $r^{-1} = (m_4 \cdot r)^{-1} \cdot m_4$ and $m_4^{-1} = (m_4 \cdot r)^{-1} \cdot r$.

3.3.2 Derivations of Formulas in the Previous Subsection

The details for deriving the operation counts in Table 10 and the whole process are as follows:

Step 1. In this step, we calculate $k = (f - v_2^2)/u_2$. We have

$$\begin{aligned}\frac{f - v_2^2}{u_2} &= \frac{x^6 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 - (x^3 + v_{21}x + v_{20})^2}{x^2 + u_{21}x + u_{20}} \\ &= k_2x^2 + k_1x + k_0,\end{aligned}$$

where

$$\begin{aligned}k_2 &= f_4 - 2v_{21}, \\ k_1 &= f_3 - v_{20} - k_2u_{21}, \\ k_0 &= f_2 - v_{21}^2 - k_2u_{20} - k_1u_{21}.\end{aligned}$$

Since we only need k_2 later, this step is free.

Step 2. In this step, we calculate r and $ru_2^{-1} \mod u_1$.

One inversion operation on the finite field is needed to obtain $u_2^{-1} \mod u_1$, but we postpone inversion until the next step. Notice that

$$\begin{aligned}rs \mod u_1 &= r\frac{v_1 - v_2}{u_2} \mod u_1 \\ &= (v_1 - v_2)\left(\frac{r}{u_2} \mod u_1\right).\end{aligned}$$

No inversion is needed to obtain $ru_2^{-1} \mod u_1$. Given u_1, u_2, v_1 and v_2, let $z_1{=}u_{11} - u_{21}$, $z_2{=}u_{20} - u_{10}$, $z_3{=}u_{11}z_1 + z_2$. Then

$$\begin{aligned}r &= z_1^2u_{10} + z_2z_3, \\ \frac{r}{u_2} \mod u_1 &= z_1x + z_2.\end{aligned}$$

Next

$$\begin{aligned}rs \mod u_1 &= (v_1 - v_2)\left(\frac{r}{u_2} \mod u_1\right) \\ &= [(v_{11} - v_{12})x + (v_{10} - v_{20})][z_1x + z_2] \mod u_1.\end{aligned}$$

Let w_0=v_{10}-v_{20}, w_1=v_{11}-v_{21},

$$\begin{aligned}rs \mod u_1 &= w_1 z_1 x^2 + (w_0 z_1 + w_1 z_2)x + w_0 z_2 \mod u_1\\ &= (w_0 z_1 + w_1 z_2 - u_{11} w_1 z_1)x + (w_0 z_2 - u_{10} w_1 z_1)\\ &= (w_0 z_1 + w_1(z_2 - u_{11} z_1))x + (w_0 z_2 - u_{10} w_1 z_1)\\ &= (w_0 z_1 + w_1(2z_2 - z_3))x + (w_0 z_2 - u_{10} w_1 z_1)\\ &= s_1' x + s_0',\end{aligned}$$

where

$$\begin{aligned}s_1' &= w_0 z_1 + w_1(2z_2 - z_3),\\ s_0' &= w_0 z_2 - u_{10} w_1 z_1.\end{aligned}$$

(We denote $s = s_1 x + x_0$.)

Step 3. In this step we calculate $\frac{s_0}{s_1}$ $\left(s = x + \frac{s_0}{s_1} = x + \frac{s_0'}{s_1'}\right)$, s_1 and s_0. We have r, $s_1' = rs_1$ and $s_0' = rs_0$, then

$$\begin{aligned}I &= \frac{1}{r \cdot (s_1' + 2r) \cdot s_1'},\\ \frac{s_0}{s_1} &= r(s_1' + 2r) \cdot s_0' \cdot I,\\ \frac{1}{s_1 + 2} &= s_1' \cdot r^2 \cdot I,\\ \frac{1}{s_1(s_1 + 2)} &= r \cdot r^2 I,\\ s_1 &= (s_1')^2 \cdot (s_1' + 2r) \cdot I,\\ s_0 &= s_1 \cdot \frac{s_0}{s_1}.\end{aligned}$$

Step 4. In this step we calculate $u' = x^2 + u_1'x + u_0'$, where u' is a monic version of $(s(l+2v_2)-k)/u_1$.

We can rewrite $(s(l+2v_2)-k)/u_1$ as

$$
\begin{aligned}
&\frac{s(l+2v_2)-k}{u_1} \\
= &\frac{(s_1x+s_0)\left[(s_1x+s_0)(x^2+u_{21}x+u_{20})+2(x^3+v_{21}x+v_{20})\right]-k}{x^2+u_{11}x+u_{10}} \\
= &\{(s_1x+s_0)[(s_1+2)x^3+(s_0+s_1u_{21})x^2+(s_0u_{21}+s_1u_{20+2v_{21}})x \\
&\quad +(s_0u_{20}+u_{20})]-(k_2x^2+k_1x+k_0)\}/u_1 \\
= &\big\{s_1(s_1+2)x^4+[s_0(s_1+2)+s_1(s_0+s_1u_{21})]x^3 \\
&\quad +[s_0(s_0+s_1u_{21})+s_1(s_0u_{21}+s_1u_{10}+2v_{21}-k_2)]x^2+\lambda_1x+\lambda_0\big\}/u_1 \\
= &s_1(s_1+2)\left\{x^4+\left(\frac{s_0}{s_1}+\frac{s_0+s_1u_{21}}{s_1+2}\right)x^3+\left(\frac{s_0(s_0+s_1u_{21})}{s_1(s_1+2)}+\frac{s_1(s_0u_{21}+s_1u_{20}+2v_{21})}{s_1(s_1+2)}\right.\right. \\
&\quad \left.\left.-\frac{k_2}{s_1(s_1+2)}\right)x^2+\lambda_1x+\lambda_0\right\}\Big/u_1 \\
= &s_1(s_1+2)(x^2+u_1{\prime}x+u_0{\prime}),
\end{aligned}
$$

where u_1' and u_0' are the coefficients of

$$
\frac{x^4+\left(\frac{s_0}{s_1}+\frac{s_0+s_1u_{21}}{s_1+2}\right)x^3+\left(\frac{s_0(s_0+s_1u_{21})}{s_1(s_1+2)}+\frac{s_1(s_0u_{21}+s_1u_{20}+2v_{21})}{s_1(s_1+2)}-\frac{k_2}{s_1(s_1+2)}\right)x^2+\lambda_1x+\lambda_0}{u_1}.
$$

We get:

$$
\begin{aligned}
u_1' &= \frac{s_0}{s_1}+\frac{s_0+s_1u_{21}}{s_1+2}-u_{11}, \\
u_0' &= \frac{s_0(s_0+s_1u_{21})}{s_1(s_1+2)}+\frac{s_1(s_0u_{21}+s_1u_{20}+2v_{21})}{s_1(s_1+2)}-\frac{k_2}{s_1(s_1+2)}-u_{10}-u_1'u_{11}.
\end{aligned}
$$

To simplify the calculation, we rewrite the formulas as

$$
\begin{aligned}
u_1' &= \frac{s_0}{s_1}+\frac{1}{s_1+2}\cdot(s_0-2u_{21})+u_{21}-u_{11}, \\
u_0' &= \frac{1}{s_1(s_1+2)}\cdot\left(s_0^2-k_2\right)+\frac{1}{s_1+2}\cdot(2s_0\cdot u_{21}-2u_{20}+2v_{21})+u_{20}-u_{10}-u_1'\cdot u_{11}.
\end{aligned}
$$

Step 5. In this step we calculate $v' = -(l + v_2) \mod u'$.

By straightforward calculation,

$$\begin{aligned} -(l + v_2) &= -[(s_1 x + s_0)u_2 + v_2] \\ &= -[(s_1 + 1)x^3 + (s_0 + s_1 u_{21})x^2 + (s_0 u_{21} + s_1 u_{20} + v_{21})x + (s_0 u_{20} + v_{20})] \\ &= \lambda_3 x^3 + \lambda_2 x^2 + \lambda_1 x + \lambda_0, \end{aligned}$$

where

$$\begin{aligned} \lambda_3 &= -s_1 - 1, \\ \lambda_2 &= -s_0 - s_1 \cdot u_{21}, \\ \lambda_1 &= -s_0 u_{21} - s_1 \cdot u_{20} - v_{21}, \\ \lambda_0 &= -s_0 \cdot u_{20} - v_{20}. \end{aligned}$$

Note: $s_0 u_{21}$ has been calculated in the previous step. To make v' be in reduced basis form, one uses the long division algorithm to get:

$$\begin{aligned} -(l + v_2) = u'[(\lambda_3 - 1)x + [\lambda_2 - u'_1(\lambda_3 - 1)]] \\ + x^3 + v'_1 x + v'_0, \end{aligned}$$

where

$$\begin{aligned} v'_1 &= [\lambda_1 - u'_0 \cdot (\lambda_3 - 1)] - u'_1 \cdot [\lambda_2 - u'_1 \cdot (\lambda_3 - 1)], \\ v'_0 &= \lambda_0 - u'_0 \cdot [\lambda_3 - u'_1(\lambda_3 - 1)]. \end{aligned}$$

3.4 Comparison and Current Update

The best known arithmetic formulas for addition on imaginary hyperelliptic curves are given by Lange [21]. The number of finite field operations in her formulas is {1 Inversion, 22 Multiplications, 3 Squarings}. Since the degree of f in real hyperelliptic curves is higher than in the imaginary curves, we need several more multiplications.

However, more improvements were made in cooperation with colleagues Erickson et al. [11], and the number of finite field operations for addition has been reduced to {1 Inversion, 26 Multiplications, 3 Squarings}.

LIST OF REFERENCES

LIST OF REFERENCES

[1] Tom Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1976.

[2] Emil Artin. Quadratische körper im gebiete de hoheren kongruenzen. *Math. Zeitschr.*, 19:153–206, 1924.

[3] Ramachandran Balasubramnnian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, volume 877 of Lecture Notes in Computer Science:141–145, 1998.

[4] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[5] Paul T. Bateman and Roger A. Horn. Primes represented by irreducible polynomials in one variable. In *Proceedings of Symposium on Pure Math*, volume VIII, pages 119–132. American Math. Society, 1965.

[6] Qi Cheng and Ming-Deh Huang. On counting and generating curves over small finite fields. *Journal of Complexity*, 20(2-3):284–296, 2004.

[7] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Fredrik Vercauteren. *Elliptic and Hyperelliptic Curve Cryptography.* Chapman Hall/CRC, 2006.

[8] Harvey Cohn. *Introduction to the Construction of Class Fields.* Dover Publications, Inc., New York, 1994.

[9] Claus Diem. The GHS attack in odd characteristic. *Journal of Ramanujan Math. Soc*, 18:1–32, 2004.

[10] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time. *Math. Comp.*, 71(238):729–742, 2002.

[11] Stefan Erickson, Michael J. Jacobson, Jr., Ning Shang, Shuo Shen, and Andreas Stein. Explicit formulas for real hyperelliptic curves of genus 2 in affine representation. Accepted by WAIFI 2007.

[12] David Freeman. Methods for comstructing pairing-friendly elliptic curves. In *10th Workshop on Elliptic Curve Cryptography*, Fields Institute, Toronto, Canada, 19 September 2006.

[13] Pierrick Gaudry, Florian Hess, and Nigel Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, (19):19–46, 2002.

[14] Thomas W. Hungerford. *Algebra.* Springer-Verlag, New York·Heidelberg·Berlin, 1987.

[15] Michael J. Jacobson, Jr., Alfred J. Menezes, Jr., and Andreas Stein. Hyperelliptic curves and cryptography. In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of H.C.Williams*, volume 41 of *Fields Institute Communications*, pages 255–282. American Math. Society, 2004.

[16] Michael J. Jacobson, Jr., Renate Scheidler, and Andreas Stein. Cryptographic protocols on real hyperelliptic curves. Submitted to Advances in Math. Comm. 2006.

[17] Michael J. Jacobson, Jr., Renate Scheidler, and Andreas Stein. Fast arithmetic on hyperelliptic curves via continued fraction expansions, 43 pages. To appear in Advances in Coding Theory and Cryptology, Series on Coding Theory and Cryptology, 2. World Scientific Publishing 2007.

[18] Neal Koblitz. Hyperelliptic cryptosystem. *Journal of Cryptology*, 1:139–150, 1989.

[19] Neal Koblitz. Almost primality of group orders of elliptic curves defined over small finite fields. *Experiment. Math.*, 10:553–558, 2001.

[20] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. *Proceedings of the Tenth IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science*, 3796:13–36, 2005.

[21] Tanja Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Appl. Aglebra Eng. Commun. Comput.*, 15:295–329, 2005.

[22] Georg-Johann Lay and Horst G. Zimmer. Constructing elliptic curves with given group order over large finite. In *Algorithmic Number Theory, LNCS*, volume 877. Springer-Verlag, 1994.

[23] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[24] Alfred J. Menezes, Yi-Hong. Wu, and Robert J. Zuccherato. *An Elementary Introduction to Hyperelliptic Curves,Technical Report CORR 96-19.* Springer-Verlag, Berlin Heidelberg New York (1998), Waterloo, Ontario, 1996.

[25] François Morain. *Implementation of the Atkin-Goldwasser-Kilian: Primality Testing Algorithm.*

[26] Volker Müller, Andreas Stein, and Christoph Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.*, 68(226):807–822, 1999.

[27] Sachar Paulus and Hans-Georg Ruck. Real and imaginary quadratic representations of hyperelliptic function fields. *Math. Comp.*, 68:1233–1241, 1999.

[28] Michael Rosen. *Number Theory in Function Fields.* Graduate Texts in Mathematics, 210, Springer-Verlag, New York, 2002.

[29] Carl L. Siegel. Über die Klassenzahl quadratischer Zahlkörper. *Acta Arithmetica*, 1, 1936.

[30] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1991.

[31] Andreas Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *Journal of the Ramanujan Mathematical Society*, 9-16(2):1–86, 2001.

[32] Andreas Stein, Renate Scheidler, and Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography*, 7(1/2):153–174, 1996.

[33] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer, MR 94k:14016, Berlin; Heidelberg, 1993.

[34] Nicolas Theriault. Index calculus attack for hyperelliptic curves of small genus. In *ASIACRYPT 2003, LNCS*, volume 2894, pages 75–92. Springer-Verlag.

[35] Samuel S Wagstaff, Jr. Divisors of Mersenne numbers. *Math. Comp.*, 40(161):385–397, 1983.

[36] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman Hall/CRC, 2003.

[37] Edwin Weiss. *Algebraic Number Theory.* Dover Publication, Inc., Mineola, NY, 1998.

[38] Hugh C. Williams. *Édouard Lucas and Primality Testing.* Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, Wiley-Interscience, New York, 1998.

[39] Thomas Wollinger, Jan Pelzl, and Christof Paar. Cantor versus Harley: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems. *IEEE Trans. Computers*, 54:861–872, 2005.

APPENDICES

A. Source Codes

The source codes in this part are all written in MAGMA.

A.1 Proposition 2.3.1 Verification

```
//*******************************************************
// This program calculates the Bateman-Horn's constant and
// the number of t_1 such that B_k(t_1,q) is a prime.
//*******************************************************
NumOfK:=1; NumOfQ:=13; k:=5; //initial value of k

for i in [1..NumOfK] do
        k:=NextPrime(k);
        print "k=",k;
        print "q   C_BH   Count_l  Count_r  Total   BH_estimate  Ratio";

        for j in [1..NumOfQ] do
                q_bitsize:=24+j-1;
                q:=PreviousPrime(2^q_bitsize);

                // Calculate Bateman-Horn's constants;
                loop:=10000;
                C:=1;
                p:=2;
                for r in [1..loop] do
                        P<x>:=PolynomialRing(GF(p));
        lambda:=q+1-x;
        Bm2:=x;
        Bm1:=x^2-2*q;
        for i in [1..(k-2)] do
                B:=x*Bm1-q*Bm2;
                Bm2:=Bm1;
                Bm1:=B;
        end for;

        A:=q^k+1-B;
        B:=A div lambda;

        X:=Roots(B);
        NmbOfRt:=# X;

        C:=C*Real((p-NmbOfRt)/(p-1));

        p:=NextPrime(p);
end for;
C_BH:=C;

P<x,y>:=PolynomialRing(IntegerRing(),2);

lambda:=y+1-x;
Bm2:=x;
Bm1:=x^2-2*y;
for r in [1..(k-2)] do
        B:=x*Bm1-y*Bm2;
```

```
                        Bm2:=Bm1;
                        Bm1:=B;
                end for;

                A:=y^k+1-B;
                B:=A div lambda;
                countleft:=0;
                for h in [-Floor(2*Sqrt(q))..0] do
                        if IsPrime(Evaluate(B,[h,q])) then
                                countleft:=countleft+1;
                        end if;
                end for;

                countright:=0;
                for h in [1..Floor(2*Sqrt(q))] do
                        if IsPrime(Evaluate(B,[h,q])) then
                                countright:=countright+1;
                        end if;
                end for;

                total:=countleft+countright;
                BH_estimate:=Round(Real(2*2*Sqrt(q)*C_BH/Log(q^(k-1))));
                ratio:=Real(total/BH_estimate);
                printf "PP(2^%o)  %o   %o   %o   %o   %o   %o \n",
                       q_bitsize, C_BH,countleft,countright,total,
                       BH_estimate,ratio;
        end for;
end for;
```

A.2 Curve Generation

```
//********************************************
// Complex Multiplication Algorithm:
// Given trace F_q and trace t_1, generate a
// curve over F_q with trace t_1.
//********************************************
q:=PreviousPrime($2^{16}$); t1:=-477; D:=$t1^2$-4*q; n:=q+1-t1;
print "Order of wanted curve is:  ",n;
R:=Roots(HilbertClassPolynomial(D),FiniteField(q));

for i in [1..sizeof(R)] do
        E:=WeierstrassModel(EllipticCurveFromjInvariant(R[i,1]));
        if Order(E) eq n then
                E;
        end if;
end for;
```

B. Gauss's Lemma for Two Variable Polynomials

The results in this appendix are similar to those in Hungerford [14], page 162, which gives the proof for one variable polynomials.

Definition B.0.1 *A polynomial over a unique factorization domain (such as the integers) is primitive if the greatest common divisor of its coefficients is* 1.

Lemma B.0.1 *If* $\mathbb{R}$ *is a U.F.D, and* $f(x,y)$ *and* $g(x,y)$ *are both primitive polynomials in* $\mathbb{R}[x,y]$*, then so is* $f(x,y)g(x,y)$*.*

Proof Clearly the product $f(x,y)g(x,y)$ of two primitive polynomials has integer coefficients. Therefore, if it is not primitive, there must be a common divisor d of all its coefficients, which can not divide all the coefficients of the either $f(x,y)$ or $g(x,y)$ (otherwise they would not be primitive). We can order the terms of $f(x,y)$ and $g(x,y)$ by degrees. We order the terms by total degree of x and y first. For the terms with same total degree, we put the terms with higher degree in y in front. Thus, we have

$$f(x,y) = \cdots + (a_r^r y^r + a_{r-1}^r y^{r-1} x^1 + \cdots + a_0^r x^r) + \cdots \, , \tag{B.1}$$

$$g(x,y) = \cdots + (a_s^s y^s + a_{s-1}^s y^{s-1} x^1 + \cdots + a_0^s x^s) + \cdots \, . \tag{B.2}$$

Let a_i^r be the first coefficient of $f(x,y)$ not divisible by d and let b_j^s be the first coefficient of $g(x,y)$ not divisible by d. Now consider the term $y^{i+j}x^{r+s-i-j}$ in the product. Its coefficients must take the following form, in which the indices in the sums go downward,

$$\sum_{k=r+s}^{0} \sum_{l=\min(i+j,k)}^{0} a_l^k b_{i+j-l}^{r+s-k}. \tag{B.3}$$

In (B.3), if $k > r$, a_l^k is divisible by d because it is before a_i^r in (B.1); if $k < r$, b_{i+j-l}^{r+s-k} is divisible by d because it is before b_j^s in (B.2). If $k = r$ and $l > i$, a_l^k is divisible by d because it is before a_i^r in (B.1). If $k = r$ and $l < i$, b_{i+j-l}^{r+s-k} is divisible by d because it is before b_j^s in (B.2). If $k = r$ and $l = i$, $a_l^k b_{i+j-l}^{r+s-k} = a_i^r b_j^s$ is not divisible by d. Hence the entire sum can not be divisible by d. We assumed that all coefficients in the product were divisible by d, leading to a contradiction. Therefore, the coefficients of the product can have no common divisor and thus the polynomial is primitive. This completes the proof. ■

Lemma B.0.2 *If $\mathbb{R}$ is a U.F.D and $\mathbb{F}$ is its field of fractions, then if a polynomial $f(x, y)$ in $\mathbb{R}[x, y]$ is irreducible over $\mathbb{R}[x, y]$, then it is also irreducible over $\mathbb{F}[x, y]$.*

Proof Without loss of generality we may assume $f(x, y)$ is primitive. Assume $f(x, y)$ is reducible over $\mathbb{F}[x, y]$. Then there exist $f(x, y)$ and $h(x, y)$ in $\mathbb{F}[x, y]$ such that $f(x, y) = g(x, y)h(x, y)$. There exist a, b in $\mathbb{F}$ such that both $a \cdot g(x, y)$ and $b \cdot h(x, y)$ are in $\mathbb{R}[x, y]$ and are primitive. By the lemma B.0.1 $(a \cdot g(x, y) \cdot (b \cdot h(x, y))) = (ab) \cdot f(x, y)$ is also primitive, and hence $ab = \pm 1$. This implies $f(x, y)$ is reducible over $\mathbb{R}[x, y]$. ■

VITA

VITA

Shuo Shen was born in Fuxin, a city in northeast China. After graduating from in Fuxin High School, he went to Mathematics department at University of Science and Technology of China (USTC), where his father graduated 30 years ago.

Shuo graduated from USTC in 2000 with a bachelors degree in mathematics. He is studying for his Ph.D degree mathematics at Purdue University. During his Ph.D study, he earned a masters degree in electrical and computer engineering at Purdue.