New Applications of Elliptic Curves and Function Fields in Cryptography

by

Robert Zuccherato

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 1997

©Robert Zuccherato 1997

National Library of Canada
Acquisitions and Bibliographic Services
395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale du Canada
Acquisitions et services bibliographiques
395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced with the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-21407-9

Canada

The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

Public key cryptography based on elliptic curves over finite fields was proposed by Miller and Koblitz in 1985. Elliptic curves over finite fields have been used to implement the Diffie-Hellman key passing scheme and the ElGamal, Schnorr and NIST signature schemes. Elliptic curves have also been used over the ring $\mathbb{Z}_n$ to implement an RSA type scheme. In the first part of this thesis however, we propose using elliptic curves over the ring $\mathbb{Z}_n$ in a new way. In this system the information is carried in the exponent space and not in the group itself. Also security depends on the difficulty of factoring a 150 digit number in order to trapdoor the discrete logarithm problem.

The continued fraction expansion and infrastructure for quadratic congruence function fields of odd characteristic have been well studied. Recently, these ideas have even been used to produce cryptosystems. Much less is known concerning the continued fraction expansion and infrastructure for quadratic function fields of even characteristic. In the second part of this thesis we will explore these ideas, and show that the situation is very similar to the odd characteristic case. This exploration will result in a method for computing the regulator for quadratic function fields of characteristic 2. We will also be able to show that cryptosystems proposed for the infrastructure of function fields of odd characteristic can be implemented in even characteristic and give a possible attack. Most importantly we will be able to show that the elliptic curve discrete logarithm problem is equivalent to a discrete logarithm problem in the infrastructure of certain quadratic function fields. This is a modification of a result by Stein for fields of odd characteristic.

Acknowledgments

I would like to thank my supervisor, Scott Vanstone, for encouraging and supporting me both while I was an undergrad and a graduate student. He has helped me accomplish more than I would ever imagine, and for this I am most grateful.

My research has benefited from discussions with and instruction from many people. In particular I would like to thank Volker Müller, who helped develop some of the material in Chapter 6, and Andreas Stein, who introduced me to infrastructures of function fields and was a valuable resource when I met barriers in my research.

The following people read preliminary versions of this thesis and provided valuable comments that have improved the final product: Steven Galbraith, Jeff Higham, Alan Ling and Alfred Menezes.

Over the past 5 years as a graduate student and the previous 4 years as an undergrad I have met many other students that have enriched my time here. I would like to thank them all since they are too numerous to mention. In particular, I would like to thank Andreas Sashegyi for always being a shoulder to lean on when times got tough and someone to celebrate with when things were going well.

I would also like to thank my thesis committee, Ian Blake, Ron Mullin, Cam Stewart and Hugh Williams for taking the time to read and evaluate this thesis and provide helpful comments. As well, I would like to thank Paul Schellenberg and Steven Furino for acting as Dr. Blake's and Dr. Mullin's delegates at my defence.

Finally, I would like to thank the Department of Combinatorics and Optimization, the Faculty of Mathematics, the Natural Sciences and Engineering Research Council, the Government of Ontario and Ron Mullin for their financial support. I

would also like to thank the University of St. Jerome's College, Certicom Corp., the Department of National Defence and the University of Waterloo for providing valuable learning and work experiences.

Robert Zuccherato

To my parents

for their continued encouragement and support,

and to Laila,

for her love and devotion.

Contents

1 Introduction 1

1.1 Motivation 1

1.2 A Brief Overview 3

2 Elliptic Curves and Their Orders 5

2.1 Number Theory Background 5

2.2 Elliptic Curves over Prime Fields 6

2.3 Elliptic Curves over $\mathbb{Z}_n$ 8

2.4 Elliptic Curves over F_{2^M} 9

2.5 Producing Primes and Curves of Smooth Order Modulo These Primes 10

2.5.1 Background 11

2.5.2 The General Idea 12

2.5.3 Specific Cases 13

2.6 Producing Curves of Smooth Order Modulo a Given Prime 16

2.6.1 Review 16

2.6.2 The Algorithm 18

2.7 On the Equivalence of the Discrete Log Problem and the Diffie-Hellman Problem 20

3 A New Cryptosystem **22**

3.1 Required Algorithms 22

3.1.1 Discrete Logarithm Algorithms 22

3.1.2 Elliptic Curve Factorization 24

3.2 The Cryptosystem 25

3.3 The Signature Scheme 26

3.4 Prespecifying Some of the Bits 27

3.5 On The Koyama-Maurer-Okamoto-Vanstone Signature Scheme . . . 29

4 Function Fields of Characteristic 2 **31**

4.1 Introduction 31

4.2 Continued Fractions in $k(X)(Y)$ 33

4.3 Reduced Quadratic Irrationals 36

4.4 Period and Symmetry in the Continued Fraction Expansion 39

4.5 The Fundamental Unit and Regulator 54

5 Finding the Regulator **58**

5.1 Ideals in $\mathcal{O}$ 59

5.2 Baby-Steps and Equivalent Reduced Ideals 65

5.3 Distances and the Giant Step 71
5.4 Algorithms 76
5.5 Some Examples 82
5.5.1 Example 1 82
5.5.2 Example 2 87

6 A Cryptosystem in the Infrastructure 89

6.1 Algorithms 89
6.2 The Key Exchange and Signature Schemes 103
6.3 Security Issues 106

7 Equivalent Discrete Logarithm Problems 112

7.1 The Divisors of an Elliptic Curve 112
7.2 An Overview 116
7.3 The Correspondence 118
7.4 Periodicity of the Continued Fraction Expansion and Orders of Points 120
7.5 The Discrete Logarithm Problems 130
7.6 Some Examples 134
7.6.1 Example 1 134
7.6.2 Example 2 135

8 Implementation And Practical Results 137

8.1 Running Times and Security Considerations for the Cryptosystem Over $\mathbb{Z}_n$ 137

8.2 Running Time and Implementation of Regulator Algorithms 140

8.3 Implementation of the Function Field Key Exchange 144

9 Suggestions for Further Research **147**

A **150**

B **152**

Bibliography **153**

List of Tables

5.1 The continued fraction algorithm for K_2. 88

7.1 The elliptic curve equivalence for K_3. 136

8.1 Times for computing regulators using Baby-Step and Optimized Giant-Step Baby-Step algorithms. 142

8.2 Times for computing regulators using Baby-Step and Optimized Giant-Step Baby-Step algorithms (cont'd). 143

8.3 Times for **Diffie-Hellman Key Exchange** Implementation. 145

8.4 Times for **Diffie-Hellman Key Exchange** Implementation (cont'd). 146

Chapter 1

Introduction

1.1 Motivation

Public-key cryptography based on elliptic curves over finite fields was proposed by Miller [31] and Koblitz [20] in 1985. Elliptic curves over finite fields have been used to implement the Diffie-Hellman key passing scheme [13] and the ElGamal [14], Schnorr [43] and NIST [36] signature schemes. Elliptic curves have also been used over the ring $\mathbb{Z}_n$ to implement an RSA [38] type system [12, 21]. One of the topics considered in this thesis is the use of elliptic curves over the ring $\mathbb{Z}_n$ in a new way. In this system the plaintext is carried in the exponent space and not in the group element itself. Also, security depends on the difficulty of factoring a 150 decimal digit number in order to trapdoor the discrete logarithm problem.

Shanks [45] introduced the concept of the infrastructure of a quadratic number field. This was an exploration of the inner structure of an equivalence class in the ideal class group. These ideas were used by Scheidler, Buchmann and Williams [40] to implement a key exchange scheme in such an infrastructure. Recently, Stein and

Williams [47, 49] extended Shanks' infrastructure ideas to real quadratic congruence function fields and applied these techniques to computing the regulator of these fields. In [41] a key exchange scheme was introduced using real quadratic congruence function fields that improved upon the one using number fields. Only fields of odd characteristic were considered. It is of much practical interest to consider the case of function fields of even characteristic. This thesis will develop the theory of the infrastructure of a quadratic function field of characteristic 2.

The main tool used in the study of the infrastructure for both number and function fields is the continued fraction algorithm. Little is known concerning the continued fraction algorithm for function fields of even characteristic. It was first discussed by Baum and Sweet in [6] and also in [7, 30]. Their discussions are incomplete however, and so do not extend the complete continued fraction theory. Thus, we will first explore the continued fraction algorithm in characteristic 2.

This thesis will also show that the key exchange protocol proposed for odd characteristic quadratic function fields also works in even characteristic. For the first time an ElGamal-based digital signature scheme [14] in this non-group structure is also introduced, as well as a Pohlig-Hellman attack [37] on these schemes.

To accomplish these goals, we will first examine the infrastructure of quadratic function fields. This will provide us with the two basic operations in the infrastructure: the Baby-Step and the Giant-Step. A Baby-Step corresponds to one iteration of the continued fraction algorithm and a Giant-Step corresponds to ideal multiplication and reduction. We will also encounter the concept of distance, which is similar to a discrete logarithm in a finite cyclic group. We will then be able to develop algorithms for computing ideals with distance "closest to the left of" a given value. It is these algorithms that we will use to produce the key exchange and digital signature schemes.

Stein [48] has been able to show, using results of Adams and Razar [1], that if we are working in odd characteristic, breaking elliptic curve systems is polynomial time equivalent to breaking systems based on the infrastructure of certain function fields. This provides further evidence of the security of elliptic curve systems as there is no known feasible way to break systems based on the infrastructure. His result does not apply to characteristic 2. This thesis will show that breaking elliptic curve cryptosystems of even characteristic is also equivalent to breaking infrastructure cryptosystems of a certain type. This is accomplished by showing that the problems on which these systems are based, the elliptic and infrastructure discrete logarithm problems, are polynomial time equivalent. Our explanation closely follows that of [1].

1.2 A Brief Overview

The remainder of this thesis is organized as follows. In Chapter 2, we give a brief introduction to elliptic curves and discuss some results concerning the generation of these curves with smooth orders. In Chapter 3, a cryptosystem is introduced that uses curves over the ring $\mathbb{Z}_n$ by storing the message in the exponent space of the group. Chapter 4 introduces the quadratic function fields of even characteristic that we will be using and describes the regulator of these fields. In Chapter 5, the infrastructure is introduced and used to develop algorithms for computing the regulator. In Chapter 6, the infrastructure is used to develop key exchange and digital signature schemes and a possible attack on these schemes is given. In Chapter 7, it is shown that solving the discrete logarithm problem for elliptic curves is equivalent to solving the discrete logarithm problem for the infrastructure of certain quadratic function fields. Finally, Chapter 8 discusses implementation issues and

practical results and Chapter 9 presents some suggested topics for further research.

Chapter 2

Elliptic Curves and Their Orders

The material in Sections 2.2, 2.3, 2.5-2.7, 3.2-3.5 and 8.1 are

©1997 IEEE. Reprinted with permission from (*IEEE Transactions on Information Theory*, Vol. 43, No. 4; July/1997).

2.1 Number Theory Background

This section will give a brief overview of some results in algebraic number theory. For a more detailed description, the reader is referred to [52].

An *algebraic number* is a complex number ζ that satisfies an equation

$$a_0\zeta^n + a_1\zeta^{n-1} + \cdots + a_n = 0,$$

where $a_0, a_1, \cdots, a_n \in \mathbb{Q}$, not all zero. The degree of ζ is the lowest degree of any such monic polynomial that ζ satisfies (called the minimal polynomial). A number which is not algebraic is called transcendental. If the minimal polynomial has $a_0 = 1$ and $a_i \in \mathbb{Z}$ for $i = 1, \ldots, n$ then ζ is called an *algebraic integer*.

An *algebraic number field* $\mathbb{Q}(\zeta)$ is the set of all the numbers of the form $R(\zeta) = P(\zeta)/S(\zeta)$, where ζ is a given algebraic integer of degree n, $P(\zeta)$ and $S(\zeta)$ are polynomials in ζ over $\mathbb{Q}$ of degree at most $n-1$, and $S(\zeta) \neq 0$. It can easily be shown that these numbers form a field. Also, the set of algebraic integers in $\mathbb{Q}(\zeta)$ form a subring known as the *ring of integers.*

Let i be the complex number that satisfies $i^2 = -1$. Then the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. Similarly, if $\omega = (-1+\sqrt{-3})/2$, so $\omega^3 = 1$, then the ring of integers of $\mathbb{Q}(\omega)$ is $\mathbb{Z}[\omega]$.

Let $\mathbb{Q}(\zeta)$ be a number field of degree n and let f be the minimal polynomial of ζ. Let $\sigma_1, \ldots, \sigma_n$ be the monomorphisms that take ζ to each of the n not necessarily distinct roots of f in the complex numbers. For any $\alpha \in \mathbb{Q}(\zeta)$ we define the *norm*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Now $N(\alpha) \in \mathbb{Q}$, and if α is an algebraic integer, then $N(\alpha) \in \mathbb{Z}$.

We call an integer *l-smooth* for $l \in \mathbb{Z}$, if all of its prime factors have less than or equal to l decimal digits.

2.2 Elliptic Curves over Prime Fields

We give a brief introduction to elliptic curves over finite fields of prime order exceeding 3. For more detailed information see [9, pp. 360–411], [28, pp. 15–48], [46, pp. 130–144].

Let $k = F_p$ be a finite field of characteristic $p \neq 2, 3$, and let $a, b \in k$ satisfy the inequality $4a^3 + 27b^2 \neq 0$. An *elliptic curve*, $E_p(a,b)$, is defined as the set of points $(x,y) \in k \times k$ which satisfy the equation

$$y^2 = x^3 + ax + b,$$

together with a special point, ∞, called the *point at infinity*. These points form an abelian group under a well-defined addition operation which we now describe.

Let $E_p(a,b)$ be an elliptic curve and let P and Q be two points on $E_p(a,b)$. If $P = \infty$, then $-P = \infty$, and $P+Q = Q+P = Q$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then $-P = (x_1, -y_1)$ and $P+(-P) = \infty$. If $Q \neq -P$ then $P+Q = (x_3, y_3)$ where

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P = Q. \end{cases}$$

Let N_p be the number of points on the curve $E_p(a,b)$. There is a well-known theorem of Hasse which states that $N_p = p + 1 - t$ where $|t| \leq 2\sqrt{p}$.

Let K be a field such that $k \subseteq K$ and let $E_p(a,b) : y^2 = x^3 + ax + b$ and $E_p(a',b') : y^2 = x^3 + a'x + b'$ be elliptic curves. Then $E_p(a,b)$ and $E_p(a',b')$ are said to be *isomorphic over* K or *K-isomorphic* if there exits a nonzero $c \in K$ such that $a = c^4a'$ and $b = c^6b'$.

A *twist* of $E_p(a,b)$ is an elliptic curve that is isomorphic to $E_p(a,b)$ over $\overline{k}$, the algebraic closure of k. We identify two twists if they are isomorphic over k. The set of twists of $E_p(a,b)$, modulo k-isomorphism, is denoted $Twist(E_p(a,b)/k)$. Let the characteristic of k be greater than 3 and $a, b \neq 0$. Then the two elliptic curves $E_p(a,b)$ and $E_p(ac^2, bc^3)$ are the representative elements of $Twist(E_p(a,b)/k)$ where $c \in k^* \setminus (k^*)^2$.

Definition 1 *Let $E_p(a,b)$ be an elliptic curve*

$$E_p(a,b) : y^2 = x^3 + ax + b$$

defined over the finite field $k = F_p$ and let $P = (x_1, y_1)$ be a point of order n on the curve. Then the elliptic discrete logarithm problem *is, given a point Q, also on the curve, to find the integer l, $0 \leq l \leq n-1$ such that $Q = lP$ if such an l exists; otherwise return "No solution".*

2.3 Elliptic Curves over $\mathbb{Z}_n$

Let $n = pq$ for distinct primes p and q each greater than 3. Let a and b be positive integers with $\gcd(n, 4a^3+27b^2) = 1$. We will now generalize our definition of elliptic curves over F_p to curves over $\mathbb{Z}_n$. An *elliptic curve* over $\mathbb{Z}_n$, $E_n(a,b)$, is defined to be the set of points $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ such that $y^2 = x^3 + ax + b$, together with a *point at infinity*, ∞. An addition operation can be defined on the points of $E_n(a,b)$ in the same way addition on $E_p(a,b)$ is defined by simply replacing all operations in F_p with operations in $\mathbb{Z}_n$. Since division is not always possible modulo n, the elliptic curve addition operation will not always be defined modulo n. Hence, an elliptic curve over $\mathbb{Z}_n$ does not form a group.

By the Chinese Remainder Theorem, any $c \in \mathbb{Z}_n$ can be uniquely represented by a pair of elements $[c_p, c_q]$ where $c_p \in \mathbb{Z}_p$ and $c_q \in \mathbb{Z}_q$. Thus, every point $P = (x,y) \in E_n(a,b)$ can be uniquely represented by a pair of points $[P_p, P_q] = [(x_p, y_p), (x_q, y_q)]$ such that $P_p \in E_p(a,b)$ and $P_q \in E_q(a,b)$, with the convention that ∞ is represented by $[\infty_p, \infty_q]$, where ∞_p and ∞_q are the points at infinity on $E_p(a,b)$ and $E_q(a,b)$ respectively. It is now easy to see that when it is defined, the addition operation on $E_n(a,b)$ is equivalent to the component-wise addition

operation on $E_p(a,b) \times E_q(a,b)$. Note that the addition on $E_n(a,b)$ is undefined when the resulting point, interpreted as an element of $E_p(a,b) \times E_q(a,b)$, has exactly one of its components being a point at infinity.

For large p and q we would expect the addition operation to be undefined for only a negligible number of possibilities. Notice that if the operation is undefined, then trying to perform the required inversion would give a non-trivial factor of n in polynomial time, and this would be an effective factoring algorithm.

Also note that if $Q = kP$ is defined where $P \in E_n(a,b)$ then $Q_p = kP_p$; therefore it is reasonable to define the *order* of $E_n(a,b)$ to be the least common multiple of the orders of $E_p(a,b)$ and $E_q(a,b)$.

2.4 Elliptic Curves over F_{2M}

This material is well known and can be found in [28] and [46].

Let $k = F_q$ be a finite field with $q = 2^M$. We define a *non-supersingular elliptic curve* over k by the equation

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

for $a_2, a_6 \in k$ and $a_6 \neq 0$. The set of solutions in $k \times k$ to this equation along with the point at infinity, ∞, produce a group under a well-defined addition operation, similar to the odd characteristic case, which we will now give.

The identity of the group operation is the point ∞. For $P = (x_1, y_1)$ a point on the curve, we define $-P$ to be $(x_1, y_1 + x_1)$, so

$$P + (-P) = (-P) + P = \infty.$$

Now suppose P and Q are not ∞, and $P \neq -Q$. Let P be as above and $Q = (x_2, y_2)$, then $P + Q = (x_3, y_3)$, where

$$x_3 = \begin{cases} \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + \frac{y_2 + y_1}{x_2 + x_1} + x_1 + x_2 + a_2 & \text{if } P \neq Q \\ \\ x_1^2 + \frac{a_6}{x_1^2} & \text{if } P = Q, \end{cases}$$

and

$$y_3 = \begin{cases} \left(\frac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + x_3 + y_1 & \text{if } P \neq Q \\ \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3 & \text{if } P = Q. \end{cases}$$

If N_q is the number of points on a non-supersingular elliptic curve, then there is a version of Hasse's Theorem for even characteristic. It states that $N_q = q + 1 - t$ where $|t| \leq 2\sqrt{q}$ and t is odd.

Definition 2 *Let E be a non-supersingular elliptic curve*

$$E : y^2 + xy = x^3 + a_2x^2 + a_6$$

defined over the finite field $k = F_{2^M}$ and let $P = (x_1, y_1)$ be a point on the curve of order n. Then the elliptic discrete logarithm problem *is, given a point Q, also on the curve, to find the integer l, $0 \leq l \leq n - 1$ such that $Q = lP$ if such an l exists; otherwise return "No solution".*

2.5 Producing Primes and Curves of Smooth Order Modulo These Primes

In [23] a method is presented that, given an integer $m > 3$ will find a prime p and an elliptic curve E over the finite field F_p of order $\#E(F_p) = m$. The method seems

to be very efficient in that it produces groups with order having 51 decimal digits in just over 6 minutes on a SPARC 2. It is also quite similar to the method we describe in Section 2.6 for producing smooth curves modulo a given prime. This section describes a method to generate primes p and elliptic curves of smooth order over F_p that is somewhat simpler but not quite as efficient.

2.5.1 Background

These results from [18, pp. 203–207, 297–317] are necessary for what follows. Let m be a positive integer, and $\mathcal{O}_m$ be the ring of integers of $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m'th root of unity. For a prime ideal $\mathcal{P}$ in $\mathcal{O}_m$ let the *norm of* $\mathcal{P}$ be the size of the quotient ring $\frac{\mathcal{O}_m}{\mathcal{P}}$, so $N(\mathcal{P}) = \left|\frac{\mathcal{O}_m}{\mathcal{P}}\right|$.

Definition 3 *For $\alpha \in \mathcal{O}_m$ and $\mathcal{P}$ a prime ideal not containing m, define the m'th power residue symbol, $\left(\frac{\alpha}{\mathcal{P}}\right)_m$ as follows:*

1. *If $\alpha \in \mathcal{P}$ then $\left(\frac{\alpha}{\mathcal{P}}\right)_m = 0$.*
2. *If $\alpha \notin \mathcal{P}$ then $\left(\frac{\alpha}{\mathcal{P}}\right)_m$ is the unique m'th root of unity that is congruent to $\alpha^{(N(\mathcal{P})-1)/m} \bmod \mathcal{P}$.*

Definition 4 *Suppose $\mathcal{A} \subset \mathcal{O}_m$ is an ideal prime to m. Let $\mathcal{A} = \mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ be the prime decomposition of $\mathcal{A}$. For $\alpha \in \mathcal{O}_m$ define $\left(\frac{\alpha}{\mathcal{A}}\right)_m = \prod_{i=1}^{n}\left(\frac{\alpha}{\mathcal{P}_i}\right)_m$. If $\beta \in \mathcal{O}_m$ and β is prime to m define $\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m$.*

Theorem 1 *Let D be a nonzero integer. Suppose $p \neq 2$ and p does not divide D. Consider the elliptic curve $y^2 = x^3 - Dx$ over F_p. If $p \equiv 3 \pmod 4$ then*

$N_p = p+1$. *If* $p \equiv 1 \pmod 4$ *let* $p = \pi\overline{\pi}$ *with* $\pi \in \mathbb{Z}[i]$ *and* $\pi \equiv 1 \pmod{2+2i}$. *Then*

$$N_p = p + 1 - \overline{\left(\frac{D}{\pi}\right)_4}\pi - \left(\frac{D}{\pi}\right)_4\overline{\pi}.$$

Theorem 2 *Let* D *be a nonzero integer. Let* $\omega = (-1+\sqrt{-3})/2$. *Suppose* $p \neq 2$ *or 3, and* p *does not divide* D. *Consider the elliptic curve* $y^2 = x^3 + D$ *over* F_p. *If* $p \equiv 2 \pmod 3$ *then* $N_p = p+1$. *If* $p \equiv 1 \pmod 3$ *let* $p = \pi\overline{\pi}$ *with* $\pi \in \mathbb{Z}[\omega]$ *and* $\pi \equiv 2 \pmod 3$. *Then*

$$N_p = p + 1 + \overline{\left(\frac{4D}{\pi}\right)_6}\pi + \left(\frac{4D}{\pi}\right)_6\overline{\pi}.$$

2.5.2 The General Idea

Using Theorems 1 and 2 we can produce curves with smooth order by computing the order as a product of small algebraic integers. There are two types of curves that can be produced; curves of the form $y^2 = x^3 - Dx$ and curves of the form $y^2 = x^3 + D$. We will describe the general idea for the case $y^2 = x^3 - Dx$. The other case is very similar and both cases are described in detail for 75-digit primes in the next section.

We wish to produce a k digit prime p and an elliptic curve modulo p whose order is not divisible by any prime factor greater than l digits. First obtain an algebraic number $u + vi \in \mathbb{Z}[i]$ whose norm is l-smooth. This can be done by building it up from numbers of smaller norm. We also require u to be an integer of about $k/4$ digits and v to be an integer of less than $k/4$ digits such that $\gcd(u, v) = 1$.

Solve $cv + du = 1$ for integers c and d. Notice that a solution can be chosen so that c is about $k/4$ digits and d is less than $k/4$ digits. Let $a = cu - dv$, which is a $k/2$-digit number. If $a \not\equiv 3 \pmod 4$ repeat the process. Now $a+i = (u+vi)(c+di)$,

and $a^2+1 = N(u+vi)N(c+di)$. The number $u+vi$ was chosen to have smooth norm but $N(c+di)$ may not be smooth, so repeat until it is. The probability of a $k/2$-digit number $N(c+di)$ being l-smooth is approximately $e^{-(k/2l)\ln(k/2l)}$ (this is an approximation to the value given in [8]). Note that we will have to repeat the process an exponential number of times, but for numbers we will consider, the number of repetitions is reasonable (see Section 2.5.3). Elliptic curve factorization [24] can determine if $N(c+di)$ is smooth.

Having determined a suitable a, let $p = a^2+4 = (a+2i)(a-2i)$ and again repeat until p is prime. Notice that p is k digits, $p \equiv 1 \pmod 4$ and that $(a+2i) \equiv 1 \pmod{2+2i}$. It is now a simple matter to find an integer D such that $\left(\frac{D}{a+2i}\right)_4 = i$. The curve $y^2 = x^3 - Dx$ will have $p-3 = a^2+1$ points over F_p, with the group order l-smooth.

Since the probability of a random integer x being prime is $\frac{1}{\ln x}$, we would expect to have to choose about $4\left(\ln 10^k\right)\left(e^{(k/2l)\ln(k/2l)}\right)$ algebraic numbers $u+vi$ until getting a k-digit prime and an elliptic curve whose order is l-smooth. Thus, we would expect to perform about $\left(\ln 10^k\right)\left(e^{(k/2l)\ln(k/2l)}\right)$ primality tests and about $e^{(k/2l)\ln(k/2l)}$ smoothness tests.

2.5.3 Specific Cases

Consider the particular case where p is 75 digits. We will describe in detail how to produce primes of this size and elliptic curves of 16-smooth order modulo these primes.

To find a 75-digit prime and an integer D such that the curve $y^2 = x^3 - Dx$ over F_p has order that factors into primes of no more than 15-16 digits, choose x_1 and x_2 to be positive integers of about 9 digits, and y_1 and y_2 to be positive

integers of about 5 digits. Let $u = x_1x_2 - y_1y_2$ and $v = x_1y_2 + x_2y_1$ so that $u + vi = (x_1 + y_1i)(x_2 + y_2i)$. Now u is 18 or 19 digits and v is 14 or 15 digits.

If $\gcd(u, v) = 1$ solve $cv + du = 1$ for integers c and d; otherwise, choose new values x_1, x_2, y_1, y_2 until $\gcd(u, v) = 1$. Note that c and d can be chosen so that c is about 18 or 19 digits and d is 14 or 15 digits. Let $a = cu - dv$ so that a is 37 or 38 digits. Now $(c + di)(x_1 + y_1i)(x_2 + y_2i) = a + i$. Repeat this process until $a \equiv 3 \pmod 4$ (about 4 times).

Now,

$$\begin{aligned} a^2 + 1 &= (a + i)(a - i) \\ &= N(a + i) \\ &= N(c + di)N(x_1 + y_1i)N(x_2 + y_2i) \\ &= (c^2 + d^2)(x_1^2 + y_1^2)(x_2^2 + y_2^2). \end{aligned}$$

Notice that $x_1^2 + y_1^2$ and $x_2^2 + y_2^2$ are 18 or 19 digits and $c^2 + d^2$ is 37 or 38 digits. With probability at least 0.74, $x_1^2 + y_1^2$ and $x_2^2 + y_2^2$ have largest prime factors with at most 15 or 16 digits. Also, $c^2 + d^2$ has probability of about 0.13 of having largest prime factor with at most 15 or 16 digits [19]. This process is repeated until $a^2 + 1$ has all factors with at most 15 or 16 digits (about 10 times).

Let $p = a^2 + 4$. Note that p is about 75 digits, $p \equiv 1 \pmod 4$ and $p = (a + 2i)(a - 2i)$ with $a \equiv 3 \pmod 4$ so $(a + 2i) \equiv 1 \pmod{2 + 2i}$. Again repeat until p is prime (in total about 2000 times). By [16] it seems reasonable that the expected number of prime factors of $p - 1$ for p a prime is the same as the expected number of prime factors of a random integer. Thus, it seems reasonable that the expected number of prime factors of $p - 3$ for p a prime is the same as the expected number of prime factors of a random integer and that

$\Pr(p \text{ is prime and } p-3 \text{ is smooth}) = \Pr(p \text{ is prime})\Pr(p-3 \text{ is smooth})$. Under this assumption, the probability that p will be prime given that $p-3$ is smooth is the same as the probability that p is prime given that p is a random positive integer. To see this note that $\Pr(p \text{ prime} \mid p-3 \text{ is smooth}) = \Pr(p \text{ is prime and } p-3 \text{ is smooth})/\Pr(p-3 \text{ is smooth})$.

Find D with $\left(\frac{D}{a+2i}\right)_4 = i$ (i.e. $D^{(p-1)/4} \equiv i \pmod{a+2i}$). The curve $y^2 = x^3 - Dx$ has

$$\begin{aligned} N_p &= p+1-(-i)(a+2i)-i(a-2i) \\ &= p-3 \\ &= a^2+1 \end{aligned}$$

points, which was chosen to have at most 15 or 16 digits.

Theorem 2 also can be used to construct a 75-digit prime and an integer D such that the curve $y^2 = x^3 + D$ over F_p has order that factors into primes of no more than 15-16 digits. Let $\omega = (-1+\sqrt{-3})/2$ and note that $1+\omega+\omega^2 = 0$ and $\overline{\omega} = \omega^2$. Again choose x_1 and x_2 to be positive integers of about 9 digits, and y_1 and y_2 to be about 5 digits. Let $u = x_1x_2 - y_1y_2$ and $v = x_1y_2 + x_2y_1 - y_1y_2$ so that $u + v\omega = (x_1 + y_1\omega)(x_2 + y_2\omega)$ where u is 18 or 19 digits and v is 14 or 15 digits.

If $\gcd(u,v)|4$ solve $c'v + d'u = 4$ for integers c' and d'. Otherwise, choose new values x_1, x_2, y_1 and y_2 until $\gcd(u,v)|4$. Let $d = d'$ and $c = c' + d'$. Then c is 18 or 19 digits and d is 14 or 15 digits. Let $a = cu - dv$ so that a is 37 or 38 digits. Now note that $(c+d\omega)(x_1+y_1\omega)(x_2+y_2\omega) = a + 4\omega$. Repeat this process until $a \equiv 2 \pmod 3$.

Now, $a^2 - 4a + 16 = N(a+4\omega) = N(c+d\omega)N(x_1+y_1\omega)N(x_2+y_2\omega)$. Notice that $N(x_1+y_1\omega)$ and $N(x_2+y_2\omega)$ are 18 or 19 digits and $N(c+d\omega)$ is 37 or 38 digits. Repeat this process until $a^2 - 4a + 16$ is smooth.

Let $p = a^2 - 3a + 9 = (a + 3\omega)(a + 3\omega^2)$. Note that p is about 75 digits, $p \equiv 1 \pmod 3$ and $p = (a + 3\omega)(a + 3\omega^2)$ with $a \equiv 2 \pmod 3$ so $a + 3\omega \equiv 2 \pmod 3$. Again repeat until p is prime.

Find D with $\left(\frac{4D}{a+3\omega}\right)_6 = \omega$ (i.e. $(4D)^{(p-1)/6} \equiv \omega \pmod{a + 3\omega}$). The curve $y^2 = x^3 + D$ has $N_p = p + 1 + (a + 3\omega)\omega^2 + (a + 3\omega^2)\omega = a^2 - 4a + 16$ which was chosen to be smooth.

These procedures may be feasible for primes p up to about 117 digits ($\approx 2^{390}$) at which point the probability that $N(c + d\omega)$ or $N(c + di)$ has at most 15 or 16 digit prime factors is about 0.009.

2.6 Producing Curves of Smooth Order Modulo a Given Prime

In this section we will first review some results dealing with Hilbert class polynomials and elliptic curves, and then give a method for producing curves of smooth order modulo a given prime p. We will use these curves in the cryptosystem described in Chapter 3.

2.6.1 Review

Various properties of elliptic curves and the Hilbert class polynomial are required for the sequel. These results are well known (see for example [9, pp. 369–379], [11, pp. 285–298], [22, pp. 39–41,123–143], [46, pp. 338-351]).

Let $E_p(a, b)$ be an elliptic curve over the field $k = F_p$. The *j-invariant* of $E_p(a, b)$ is a function from the set of elliptic curves modulo p to k such that:

- Two elliptic curves are isomorphic over $\overline{k}$ if and only if they have the same j-invariant.

- For any element $j_0 \in k$, there exists an elliptic curve defined over k with j-invariant equal to j_0. If $j_0 \neq 0, 1728$ and k has characteristic greater than 3, then $j(E_p(a,b))$ equals j_0 for $a = 3j_0/(1728 - j_0) \pmod{p}$ and $b = 2j_0/(1728 - j_0) \pmod{p}$.

Given elliptic curves $E_p(a,b)$ and $E_p(a',b')$ an *isogeny* from $E_p(a,b)$ to $E_p(a',b')$ is a rational map from $E_p(a,b)$ to $E_p(a',b')$ (here we assume that the curves are defined over $\overline{k}$). An isogeny is also a group homomorphism. The group of isogenies from $E_p(a,b)$ back to $E_p(a,b)$ is called the *endomorphism ring* of $E_p(a,b)$ and is denoted by $\mathrm{End}_{\overline{k}}(E_p(a,b))$.

Theorem 3 *If $E_p(a,b)$ is an elliptic curve with $p \neq 2,3$, then the endomorphism ring $End_{\overline{k}}(E_p(a,b))$ is either an order in an imaginary quadratic field (in which case the curve is called ordinary) or an order in a quaternion algebra (in which case it is called supersingular).*

Let $D < -4$ be an integer and $D \equiv 0, 1 \pmod{4}$. Also let $4p = x^2 - Dy^2$ for integers x and y. Then there exists a polynomial $H_D(X)$ called the *Hilbert class polynomial* with the following properties.

- $H_D(X)$ is a monic polynomial with integer coefficients.

- The degree of $H_D(X)$ equals $h(D)$ where $h(D)$ is the class number of the order of an imaginary quadratic field of discriminant D.

- $H_D(X)$ splits completely modulo p. If j_0 is a root of $H_D(X)$ modulo p then j_0 gives the j-invariant of an elliptic curve with $p + 1 \pm x$ points.

- $H_D(X) = \prod(X - j(E_p(a,b)))$ where the product is over all isomorphism classes of elliptic curves with endomorphism ring the order in an imaginary quadratic field of discriminant D.

There is an algorithm due to Cornacchia that given prime p and $D < 0$, $D \equiv 0, 1 \pmod 4$ will determine integers x and y such that $4p = x^2 - Dy^2$ or determine that no such x and y exist (see [9, pp. 34–36]). Computing the Hilbert class polynomial can be accomplished by means of an algorithm given in [9, pp. 407–409] or by an algorithm given in [11, pp. 286–298]. The Hilbert class polynomial, however, has very large coefficients and the calculations required to produce it are real valued and must be computed to a high degree of precision. In order to avoid these computational difficulties the Weber polynomials, which are polynomials closely related to the j-invariant, are better suited to the task at hand. These polynomials have coefficients which are much smaller than the Hilbert class polynomial and provide the same desired result. For more information on the Weber class polynomial see [4, 23].

2.6.2 The Algorithm

This algorithm is based on a portion of Atkin's primality proving algorithm (see [4]). It is also very similar to the method presented in [23] for producing primes and curves with specific orders and to the method presented in [32] for producing curves over F_p with p elements.

Given a prime p our objective is to determine $a, b \in F_p$ such that $E_p(a,b)$ has order that factors into primes less than or equal to some bound H. To do this, first choose an integer $D < -4$, $D \equiv 0, 1 \pmod 4$. Using Cornacchia's algorithm determine x and y such that $4p = x^2 - Dy^2$ if such an x and y exist. If no such x

and y exist choose a new D and repeat. Calculate $p+1 \pm x$ and determine if either of these values is smooth with respect to H. This can be done using elliptic curve factorization [24]. If neither is smooth choose a new D and repeat. Otherwise, compute $H_D(X) \bmod p$. Let j_0 be a root of $H_D(X) \bmod p$ and compute the curve $y^2 = x^3 + ax + b$ with j-invariant j_0. If the curve has a smooth number of points, output a and b. Otherwise, compute and output its twist.

In the above algorithm, the numbers D should be chosen in increasing complexity. This means they should be chosen in terms of increasing class numbers $h(D)$. This will help to decrease the computation that must be performed when computing the Hilbert polynomials since the degree of the polynomial increases with $h(D)$ and the degree of precision increases with D and $h(D)$. Determining which of the twists has a smooth number of points can be accomplished as follows. Let N_p be either $p+1-x$ or $p+1+x$, whichever is smooth. Then to determine whether or not $E_p(a,b)$ has N_p points find $P \in E_p(a,b)$ such that $\gcd(p+1-x, p+1+x)P \neq \infty$. If $N_pP = \infty$ then $E_p(a,b)$ has N_p points.

Also note that since we must choose different D's until $p+1 \pm x$ is smooth with respect to H, this algorithm will run in exponential time. For a 75-digit prime however, the probability that N_p is 15-smooth is about .0004 [19] so one would expect to have to choose about 1250 different D's that can be written as $4p = x^2 - Dy^2$ before getting a curve whose order is 15-smooth. This computation may be feasible as a one time cost.

2.7 On the Equivalence of the Discrete Log Problem and the Diffie-Hellman Problem

Let G be a group and α an element of G. The *Diffie-Hellman Problem* [13] is to determine α^{ab} given α^a and α^b. The *Discrete Log Problem* is to determine a given α^a. Clearly, a solution to the Discrete Log Problem implies a solution to the Diffie-Hellman Problem. The converse is not known.

The following result is due to Maurer [25].

Assume $\#G = p$. Let $E_p(a,b)$ be an elliptic curve over F_p such that discrete logarithms are easily computed in $E_p(a,b)$. Suppose that we have an oracle which when given α^a, α^b returns α^{ab}. Then the oracle and the group operation allow us to compute $\alpha^{f(x)}$ for any polynomial function $f(x)$ with integer coefficients. Since $x^{-1} \equiv x^{p-2} \pmod{p}$ we can compute $\alpha^{g(x)}$ for any rational function $g(x)$.

Suppose that $\beta = \alpha^x$ and the oracle are given. Can one determine x, the discrete logarithm of β? Suppose x is the x-coordinate of some point $Q = (x,y)$ on $E_p(a,b)$. Compute

$$\alpha^{x^3+ax+b} = \alpha^{y^2}.$$

Using a square root algorithm determine α^y. Now let $P = (u,v)$ generate a subgroup of $E_p(a,b)$ that contains (x,y) and then $(x,y) = \gamma P$.

Using (α^x, α^y) for (x,y) and (α^u, α^v) for P, the oracle and group operation will allow us to perform the Baby-Step Giant-Step algorithm with P on $E_p(a,b)$ and determine γ. Note that given $(\alpha^{u_1}, \alpha^{v_1})$, $(\alpha^{u_2}, \alpha^{v_2})$ where $(u_1,v_1), (u_2,v_2) \in E_p(a,b)$ we can find $(\alpha^{u_3}, \alpha^{v_3})$ where $(u_3,v_3) = (u_1,v_1) + (u_2,v_2)$ on $E_p(a,b)$. Having found γ we can then compute x, i.e. $(x,y) = \gamma P$.

Now, using the methods of Sections 2.5 and 2.6 as well as a recent generalization

of these schemes by Maurer and Wolf [26], we can compute a curve over F_p such that solving the discrete logarithm problem is relatively easy using the Pohlig-Hellman and Baby-Step Giant-Step Algorithms (see Section 3.1). Unfortunately, for a given prime p, this computation is not polynomial time and thus we do not have a polynomial time reduction from the Diffie-Hellman problem to the Discrete Log problem. It remains an open question as to whether these algorithms for producing curves can be modified to work in polynomial time.

Chapter 3

A New Cryptosystem

3.1 Required Algorithms

In this section we will examine some algorithms that will be needed to construct a new cryptosystem using elliptic curves over $\mathbb{Z}_n$.

3.1.1 Discrete Logarithm Algorithms

In Sections 2.2 and 2.4 we encountered the elliptic curve discrete logarithm problem. The best known attack on this problem is an algorithm which works in any general group. For this reason we will first consider the discrete logarithm problem defined over a general group.

Let G be a finite cyclic group generated by the element α and let $\beta \in G$. Given G, α, and β the *discrete logarithm problem* is to find an integer x, $1 \leq x \leq |G|$ such that $\beta = \alpha^x$. We call x the *discrete logarithm* of β to the base α and write $x = \log_\alpha \beta$.

The best algorithm known for solving the discrete logarithm problem over a general group G is the Pohlig-Hellman algorithm [37] combined with the Baby-Step Giant-Step algorithm.

Baby-Step Giant-Step Algorithm

Let G be a group of order n and let $m = \lceil \sqrt{n} \rceil$. Notice that x can be written uniquely as $x = jm + i$ where $0 \leq i, j < m$. In order to compute i and j, a list of pairs (α^i, i) is computed and sorted. Then $\beta(\alpha^{-m})^j$ is computed for each $1 \leq j < m$. This value is then compared with the values in the table to determine if there exists an i with $\beta(\alpha^{-m})^j = \alpha^i$. If so, then $x = im + j$.

This algorithm requires $O(m \log m)$ group operations.

Pohlig-Hellman Algorithm

Let G be a group of order $n = \prod_{i=1}^{r} p_i^{e_i}$ in which the factorization of n is known. This algorithm determines $x \bmod p_i^{e_i}$ for each i. The Chinese Remainder Theorem is then used to determine x. Let $z \equiv x \pmod{p_1^{e_1}}$ with $1 \leq z < p_1^{e_1}$.

Suppose that $z = \sum_{i=0}^{e_1-1} z_i p_1^i$, where $0 \leq z_i < p_1$ for $i = 0, \ldots, e_1 - 1$. The z_i will be determined one at a time. Let $\gamma = \alpha^{n/p_1}$. Then $\beta^{n/p_1} = \alpha^{xn/p_1} = \gamma^x = \gamma^{z_0}$. The Baby-Step Giant-Step algorithm can then be used to determine $z_0 = \log_\gamma \beta^{n/p_1}$. Then similarly $(\beta\alpha^{-z_0})^{n/p_1^2} = \gamma^{z_1}$, and z_1 can be determined. The process can be repeated to determine all of the z_i. In a similar fashion $x \bmod p_i^{e_i}$ can be computed for all p_i.

This algorithm has a running time of $O(\sum_{i=1}^{r} e_i(\log n + \sqrt{p_i}))$.

3.1.2 Elliptic Curve Factorization

In Section 2.3 we encountered elliptic curves defined over the ring $\mathbb{Z}_n$. These elliptic curves can be used to produce a factoring algorithm that works well when the number to be factored has a relatively small prime divisor. This algorithm, known as the Elliptic Curve Factorization Method is due to Lenstra [24].

Let n be the integer we wish to factor and let p and q be two primes that divide n. Let $E_n(a,b)$ be an elliptic curve and P be a point on this curve. If we had some integer m such that $mP_p = \infty_p$ but $mP_q \neq \infty_q$ then mP would not be defined. If we then tried to compute mP, at some point while trying to take an inverse which is required for the addition formula, we would get a non-trivial factorization of n. Thus, we would like m to divide the order of $E_p(a,b)$ but not the order of $E_q(a,b)$, which would happen if the order of $E_p(a,b)$ was smooth with respect to some bound, but $E_q(a,b)$ was not and m was chosen as a product of small primes. This is the idea behind the factoring algorithm.

Elliptic Curve Factorization Method

1. Choose $a, x, y \in \mathbb{Z}_n$.
2. Let $b \equiv y^2 - x^3 - ax \pmod{n}$.
3. If $\gcd(4a^3 + 27b^2, n) = n$, then return to Step 1.
4. Otherwise if $\gcd(4a^3 + 27b^2, n) > 1$, then n has been factored.
5. Choose a bound L and let

$$m = \prod_{q \leq L} q^{\lfloor \log_q n \rfloor},$$

where the product is over primes q.

6. Set $P = (x, y)$ and compute mP in $E_n(a, b)$. If at some point in trying to invert an element of $\mathbb{Z}_n$ a nontrivial factor is obtained, n has been factored. Else, return to Step 1.

In this algorithm, elliptic curves over $\mathbb{Z}_n$ are chosen at random and it is hoped that mP is not defined. For this reason, the algorithm works best when n has a small prime factor. The expected running time to remove a factor p from n is (making some heuristic assumptions) $O(e^{\sqrt{2 \log p \log \log p}})$.

3.2 The Cryptosystem

The idea is to trapdoor the discrete log problem in such a way that messages can be encoded in the exponent space of the group. Suppose we have an elliptic curve defined over the integers modulo $n = pq$ for primes p and q. Then the points on the elliptic curve form a "pseudo-group" in the sense that when the addition is defined, it corresponds to elliptic curve addition modulo p and modulo q. Now, let p and q be large enough so that factoring n is infeasible. As a lower bound consider, for example, p and q to be 75 decimal digits each.

Then let $y^2 = x^3 + ax + b$ be an elliptic curve modulo n such that when it is taken modulo p and modulo q the orders are known to the user and are smooth (e.g. each prime factor has fewer than 15 or 16 decimal digits). These can be computed using the methods in Sections 2.5 and 2.6. Computing discrete logs on the curve modulo p and the curve modulo q is feasible using the Pohlig-Hellman method and the Baby-Step Giant-Step method. In order to use the Pohlig-Hellman method the group orders must be known. Thus, if the factorization of n is known, the group orders can be found in polynomial time using Schoof's [44], Atkin's [3]

and Elkies' [15] methods, and computing discrete logs on the curve modulo n is feasible. However, using the elliptic curve factoring method, or any other method to factor n, is still infeasible. (See Section 8.1.)

Let n, the curve $E_n(a,b)$, and a point P on the curve be the user's public key. To send a message, $\tilde{M}$, to this user, where $\tilde{M} \in \mathbb{Z}$, $0 < \tilde{M} < \#P$ (here $\#P$ is the order of the point P) simply compute $\tilde{M}P$. Now, in order to read the message, the discrete logarithm problem must be solved. Since p and q are 75 digit primes with $E_p(a,b)$ and $E_q(a,b)$ smooth, the Pohlig-Hellman method is the only known method to compute the discrete logarithm. If we try to use Pohlig-Hellman directly on $E_n(a,b)$ we must know its order. However, Schoof's and Atkin's methods do not seem to generalize to $\mathbb{Z}_n$, so determining the order of $E_n(a,b)$ is intractable unless p and q are known. An eavesdropper cannot solve these problems as she cannot factor n to obtain p and q and thus get the order of the curves. Our user however knows p and q and can solve the discrete log problem relatively easily.

3.3 The Signature Scheme

This system can be used to create digital signatures as well. Again let n, the curve and a point, P, on the curve be a users public key. Also here assume that the elliptic curve group being used is cyclic and that P is a point of maximal order. Then let $\tilde{M}$ be a $(\lceil \log_2(n) \rceil - C - 2\lceil \log_2 \ln(n) \rceil)$-bit message that our user wishes to sign, where C is an appropriately defined integer constant. We wish to determine a point $Q = (x,y)$ such that the first $\lceil \log_2(n) \rceil - C - 2\lceil \log_2 \ln(n) \rceil$ bits of the x-coordinate are the message $\tilde{M}$ or a hash of the message $\tilde{M}$. To do this, $C + 2\lceil \log_2 \ln(n) \rceil$ zeros can be appended to $\tilde{M}$ resulting in $\tilde{M}'$. Define x to be the smallest integer greater than $\tilde{M}'$ such that $x^3 + ax + b$ is a quadratic residue modulo n and let y be one of

its square roots modulo n. Note that since the factorization of n is known to the signer, taking square roots is feasible. Then let $Q = (x, y)$.

It seems reasonable that the first $\lceil \log_2(n) \rceil - C - 2\lceil \log_2 \ln(n) \rceil$ bits will be $\tilde{M}$ since assuming the Generalized Riemann Hypothesis, the smallest quadratic non-residue occurs in the interval $[1, t]$ where $t = O(\ln(n)^2)$ (see [5]). Thus, it seems reasonable that $x^3 + ax + b$ would be a quadratic residue after at most $C' \ln(n)^2$ attempts for some constant C' and this would not affect our message $\tilde{M}$.

In order to sign the message, compute the discrete log of Q to the base P on the elliptic curve. If $Q = kP$ then the signature is k. To check the signature the receiver of the message simply computes kP and checks that this equals Q. The point Q can be identified since the first t bits of the x-coordinate are $\tilde{M}$.

This scheme can be modified for non-cyclic curves by appending more zeros to $\tilde{M}$ and requiring as well that x and y satisfy $Q = (x, y) \in \langle P \rangle$.

3.4 Prespecifying Some of the Bits

Vanstone and Zuccherato [54] showed how to prespecify some of the bits of an RSA public-key modulus so that the number of bits that had to be transmitted and stored could be reduced. For example, the key length for a 1024-bit RSA scheme could be shortened by about 512 bits. A similar operation can be performed here so that the public key length gets reduced.

In order to specify $t < \lceil \log_2(n) \rceil - C - 2\lceil \log_2 \ln(n) \rceil$ bits of the public key point P the following procedure could be followed. Let α be a t-bit number that we want to be contained in P. Then α is appended with sufficient redundancy, for example by appending zeros, to give a $\lceil \log_2(n) \rceil$ bit integer α'. Now define x to be an integer

greater than α' such that α is the first t bits of x and $x^3 + ax + b$ is a quadratic residue modulo n. Let y be one of the square roots of this number modulo n. As in the previous section, under reasonable assumptions, such an x and y exist. Note that the person setting up this system is the only one that can do this computation, since he is the only person that knows the factorization of n. Now $P = (x, y)$ and the first t bits of x are α. If P has large order then we accept it as the public key point, otherwise we choose a new x and repeat.

This could be used on a large network where everyone has to use the same t bits in their public key point. Thus, storage space would be reduced as these t bits need only be stored once as a system-wide parameter. It could also be used if a person wanted some of their publicly known identification information to be used as part of their public key. This gives rise to a possible use of this system as an ID-based key exchange system [17, 27].

In such a system a trusted central authority chooses primes p and q, an elliptic curve $y^2 = x^3 + ax + b$ whose order is smooth modulo p and q, and a point P on the curve. The central authority and only the central authority can compute discrete logarithms on the curve modulo $n = pq$. The curve and n are made public. To register a public key, Albert presents himself to this central authority. The central authority can then compute a point on the curve $P_{ID(A)}$ containing his identification information $ID(A)$ as the first t bits of the x-coordinate. The central authority computes s_A such that $s_A P = P_{ID(A)}$ on the curve and gives s_A to Albert. (Remember that the central authority is the only entity that can do all these calculations.)

To exchange keys, Albert obtains Betty's identification point $P_{ID(B)}$ and computes the key $K = s_A P_{ID(B)} = s_A s_B P$. Betty computes the same key as $K = s_B P_{ID(A)} = s_B s_A P$. The key can now be used in a conventional private key ci-

pher system. Exchanging keys in this way provides key authentication since the only person (besides the trusted authority) that knows the discrete logarithm of an identification point is the person to which it belongs.

3.5 On The Koyama-Maurer-Okamoto-Vanstone Signature Scheme

Koyama *et al* [21] describe a digital signature scheme using elliptic curves modulo n that cannot be used to encrypt messages. The scheme is set up as follows:

- The signer A chooses two primes p and q and parameters a and b such that $\gcd(4a^3 + 27b^2, n) = 1$ where $n = pq$.
- A computes the orders of $E_p(a, b)$ and $E_q(a, b)$.
- A chooses a public encryption multiple e relatively prime to N_p and N_q (the orders of $E_p(a, b)$ and $E_q(a, b)$ respectively).
- A computes $d \equiv e^{-1} \pmod{\text{lcm}(N_p, N_q)}$.
- A makes public n, a, b, and e.

To sign a message $\tilde{M}$, A associates a point $P = (x, y) \in E_n(a, b)$ with $\tilde{M}$ in a publicly-known way and computes $Q = dP$. The signature for $\tilde{M}$ is Q. Verification of the signature is done by computing $eQ \stackrel{?}{=} P$.

Since finding points on the curve $E_n(a, b)$ is infeasible without the knowledge of p and q, it was claimed [21] that encryption is not possible. Notice however, that after any one message is signed both parties now have the point Q. If the

curve has been chosen so that the discrete logarithm problem is easy (for example in Sections 2.5 and 2.6), this point can now be used, along with the curve $E_n(a, b)$ to encrypt and send messages as described in Section 3.2. Thus using this digital signature scheme could provide a covert channel to convey secret information. The question still remains, given a, b and $n = pq$, whether one can detect a trapdoor on the discrete log problem for $y^2 = x^3 + ax + b$ over $\mathbb{Z}_n$ and thus on the digital signature scheme. It appears that p and q must be recovered and the orders of $E_p(a, b)$ and $E_q(a, b)$ calculated, which is infeasible.

Chapter 4

Function Fields of Characteristic 2

The material in Sections 4.1-4.5, 5.1-5.4 and 8.2 are

©1997 Academic Press. Reprinted with permission from (*Journal of Algebra*; in press).

For an introduction to function field theory and to valuation theory see [10, 53]. Valuations are also defined in Section 7.1.

4.1 Introduction

Let k be a field with $q = 2^M$ elements, X a transcendental element over k, and K a field of degree 2 over $k(X)$ which is not an algebraic extension of k. The field K can be obtained by adjoining to $k(X)$ an element Y which satisfies the equation $Y^2 + BY = C$ where $B, C \in k[X]$ with C monic. We require the polynomials B and C to have the property that $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have a solution with $y \in k[X]$ for each non-constant polynomial D that divides B. If $P \in k[X]$

satisfies $P^2 + BP + C = C'D^2$ for some such D, then let $Y' = \frac{P+Y}{D}$ and $B' = \frac{B}{D}$. Then notice that $Y^2 + BY + C = 0$ gives us $Y'^2D^2 + P^2 + BDY' + BP + C = 0$, so $Y'^2 + B'Y' + C' = 0$. Now, $\deg(B') < \deg(B)$, and we can repeat until we have a B, C and corresponding Y with the desired properties. This condition is equivalent to $Y^2 + BY + C = 0$ having no singular points $(X, Y) = (u, v) \in \overline{k} \times \overline{k}$. (See Appendix A.)

The valuation at the place at infinity in $k(X)$ is the negative of the degree function in $k(X)$ and the completion of $k(X)$ with respect to the place at infinity is $k((\frac{1}{X}))$. We need $k(X)(Y) \subseteq k((\frac{1}{X}))$, so we need $Y \in k((\frac{1}{X})) \setminus k(X)$. This is equivalent to saying that the place at infinity, $\mathcal{P}_\infty$ splits completely as $\mathcal{P}_\infty = \mathcal{P}_1 \cdot \mathcal{P}_2$ in K. Thus we are in the "real" case [55]. It is therefore necessary that $\deg(B) > 1$. For the remainder we will assume that this is the case. Since there are two embeddings of $K \subseteq k((\frac{1}{X}))$, we must choose one. If Y is one solution to $Y^2 + BY + C = 0$ then $Y + B$ is the other. Thus, if $Y = \sum_{i=-\infty}^{t} c_i X^i$ and $b \in k$ is the leading coefficient of B, then $c_{\deg(B)}^2 + bc_{\deg(B)} = \gamma'$ for some $\gamma' \in k$. So, the two embeddings correspond to the two solutions in k of $x^2 + x = \gamma$ for $\gamma = \frac{\gamma'}{b^2} \in k$. We will consider k as being represented by the polynomial basis whose defining polynomial has smallest Gray Code rank. We will then choose as the solution to $x^2 + x = \gamma$, the one whose binary vector representation has smallest Gray Code rank. This fixes our embedding.

For example, consider the equation

$$Y^2 + (X + 1)Y = X^6 + X^2 + X + 1.$$

We wish to obtain the Laurent expansion for Y. It is easy to see that $c_i = 0$ for $i > 3$. Now, if we substitute $Y = \sum_{i=-\infty}^{3} c_i X^i$ and equate coefficients we get

$$c_3^2 = 1 \quad \text{so} \quad c_3 = 1,$$

$$\begin{aligned} c_2^2 + c_3 = 0 \quad &\text{so} \quad c_2 = 1, \\ c_1^2 + c_1 + c_2 = 1 \quad &\text{so} \quad c_1 = 0 \text{ or } 1, \\ c_0 + c_1 = 1 \quad &\text{so} \quad c_0 = 1 \text{ or } 0, \\ c_0^2 + c_{-1} + c_0 = 1 \quad &\text{so} \quad c_{-1} = 1, \\ &\vdots \quad . \end{aligned}$$

This report follows very much the explanation given in [47, 49]. Many of the results are characteristic 2 function field analogues of well known theorems given in [2, 39, 47, 49, 50, 51, 56]. The purpose of including this chapter here is to provide much of the machinery needed for subsequent chapters.

4.2 Continued Fractions in $k(X)(Y)$

Let the ring of integers of K be the set of all elements in K that satisfy a monic polynomial over $k[X]$. Denote this ring by $\mathcal{O}_K$. Let $\mathcal{O}$ be the order $k[X][Y] \subseteq \mathcal{O}_K$. For $\alpha = u + vY \in K$, $(u, v \in k(X))$, define its *conjugate* by $\overline{\alpha} = u + v(Y + B)$. Then $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = u^2 + uvB + v^2C$.

Let $\alpha = \sum_{i=-\infty}^{t} c_i X^i \in k((\frac{1}{X}))$ with $c_i \in k$ and $c_t \neq 0$. Then define

$$\begin{aligned} \deg(\alpha) &= t \\ |\alpha| &= q^t \\ \mathrm{sgn}(\alpha) &= c_t \\ \lfloor \alpha \rfloor &= \sum_{i=0}^{t} c_i X^i \end{aligned}$$

with $|0| = 0$ and $\deg(0) = -\infty$. These definitions will be important for what follows.

We now present the continued fraction algorithm over fields of even characteristic. Let $\alpha \in k(X)(Y)$. Also let $\alpha_0 = \alpha$ and $a_0 = \lfloor \alpha_0 \rfloor$. We calculate the continued fraction expansion of α by

$$\begin{aligned} \alpha_i &= \frac{1}{\alpha_{i-1} + a_{i-1}} \\ a_i &= \lfloor \alpha_i \rfloor \end{aligned}$$

for all $i \geq 1$.

Now define

$$\begin{aligned} p_{-2} &= 0 & q_{-2} &= 1 \\ p_{-1} &= 1 & q_{-1} &= 0 \\ p_i &= a_i p_{i-1} + p_{i-2} & q_i &= a_i q_{i-1} + q_{i-2} \end{aligned}$$

for all $i \geq 0$. By induction, it is easy to see that

$$\alpha = \frac{p_i \alpha_{i+1} + p_{i-1}}{q_i \alpha_{i+1} + q_{i-1}}$$

for all $i \geq -1$.

The value

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}}$$

is called the *k-th convergent* to α and is denoted $[a_0; a_1, a_2, \ldots, a_k]$. We also use the notation $[a_0; a_1, a_2, \ldots]$ for the value

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}.$$

It can be shown that $\alpha = [a_0; a_1, a_2, \ldots]$.

As is the case with continued fraction expansions of real numbers, we can show by induction that $[a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k}$.

Lemma 1 *Let $\alpha \in k((\frac{1}{X}))$ then $\alpha = \frac{P}{Q}$ for $P, Q \in k[X]$ if and only if the continued fraction expansion of α is finite.*

Proof: The proof is similar to the proof for the continued fraction expansion of real numbers. See [39]. □

This theory was first discussed by Baum and Sweet in [6] and also in [7, 30]. Their discussions were incomplete however, and so we now present a more complete description of the theory of continued fractions over fields of even characteristic.

If $\alpha = \frac{P+Y}{Q}$ where $Q, P \in k[X]$, $Q \neq 0$ and $Y \in k((\frac{1}{X}))$ satisfies $Y^2 + BY = C$ for $B, C \in k[X]$ with the property that $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have a solution with $y \in k[X]$ for each $D|B$, $D \notin k$ and $Q|P^2 + PB + C$ then we call α a *quadratic irrational.*

Let $Q_0 = Q$, $P_0 = P$, $\alpha_0 = \alpha$ and $Q_{-1} = \frac{P^2+PB+C}{Q}$. Define the recursions

$$\begin{aligned} P_{i+1} &= a_i Q_i + P_i + B \\ Q_{i+1} &= \frac{P_{i+1}^2 + P_{i+1}B + C}{Q_i} \end{aligned}$$

for all $i \geq 0$. Again by induction it is easy to see that

$$\alpha_i = \frac{P_i + Y}{Q_i}$$

and $Q_i | P_i^2 + P_i B + C$ for all $i \geq 0$. Let $d = \lfloor Y \rfloor$, the *polynomial part* of Y. Now, $a_i = \lfloor \alpha_i \rfloor = \left\lfloor \frac{P_i+Y}{Q_i} \right\rfloor = (P_i + d) \text{ div } Q_i$ and $Q_{i+1} = Q_{i-1} + a_i(P_{i+1} + P_i)$.

Define $r_i \in k[X]$ to be the remainder when $P_i + d$ is divided by Q_i, or in other words $P_i + d = a_i Q_i + r_i$ where $0 \leq \deg(r_i) < \deg(Q_i)$. We then get the simpler recursions

$$P_{i+1} = d + r_i + B$$

$$\begin{aligned} Q_{i+1} &= Q_{i-1} + a_i(r_i + r_{i-1}) \\ a_i &= (P_i + d) \text{ div } Q_i \\ r_i &= (P_i + d) \bmod Q_i \end{aligned}$$

for $i \geq 1$.

Recall from the continued fraction expansion that $\alpha = \frac{p_i\alpha_{i+1}+p_{i-1}}{q_i\alpha_{i+1}+q_{i-1}}$ so we get $\alpha_{i+1} = \frac{p_{i-1}+\alpha q_{i-1}}{p_i+\alpha q_i}$ for $i \geq -1$. Combining this with $\alpha_i = \frac{P_i+Y}{Q_i}$ and comparing rational and irrational parts we get that

$$Cq_{i-1} = Q_i(Q_0p_{i-2} + P_0q_{i-2}) + P_i(Q_0p_{i-1} + P_0q_{i-1})$$

and

$$Q_0p_{i-1} = Q_iq_{i-2} + P_iq_{i-1} + P_0q_{i-1} + Bq_{i-1}$$

for $i \geq 0$.

Let $\theta_1 = 1$ and $\theta_{i+1} = \prod_{j=1}^{i} \frac{1}{\alpha_j}$ for $i \geq 1$. Then by induction $\theta_{i+1} = p_{i-1} + \alpha q_{i-1}$ for $i \geq 0$. Now $\alpha_j = \frac{P_j+Y}{Q_j}$ so $\frac{1}{\alpha_j} = \frac{P_j+Y+B}{Q_{j-1}}$. Thus $\mathrm{N}(\theta_{i+1}) = \theta_{i+1}\overline{\theta_{i+1}} = \frac{Q_i}{Q_0}$.

For a complete example of the continued fraction expansion of a quadratic irrational, the reader is referred to Section 5.5.1.

4.3 Reduced Quadratic Irrationals

A quadratic irrational α is called *reduced* if $|\overline{\alpha}| < 1 < |\alpha|$. Since $\overline{\alpha} = \frac{P+Y+B}{Q}$, we get that α is reduced if

$$|P + Y + B| < |Q| < |P + Y|\,.$$

Thus, if α is reduced, $|P + Y| = |B|$ and $\mathrm{sgn}(P + Y) = \mathrm{sgn}(B)$. Also, the second highest coefficient of $P + Y$ must equal the second highest coefficient of B. So, either

- $|B| = |P| > |Y|$ and $\text{sgn}(B) = \text{sgn}(P)$,
- $|B| = |Y| > |P|$ and $\text{sgn}(B) = \text{sgn}(Y)$
- $|B| = |Y| = |P|$, $\text{sgn}(B) = \text{sgn}(Y) + \text{sgn}(P)$ and $\text{sgn}(Y) \neq \text{sgn}(P)$ or
- $|B| < |Y| = |P|$ and $\text{sgn}(Y) = \text{sgn}(P)$

and $|Q| < |B|$. Notice that in all cases $|B| \geq |P|$ or $|Y| = |P|$. Now, let $a = (P + d)$ div Q. Then $|aQ| = |P + d| = |P + Y| = |B|$, so $|aQ| = |B|$. Hence, $1 \leq |Q| < |B|$ and $1 < |a| \leq |B|$. So, if α is reduced then we have bounds on $|P|$ and $|Q|$.

Lemma 2 *Let* $\alpha_i = \frac{P_i+Y}{Q_i}$ *be reduced for some* $i \geq 0$. *Then* $\alpha_{i+1} = \frac{P_{i+1}+Y}{Q_{i+1}}$ *where*

$$\begin{array}{rclcl} P_{i+1} & = & d + r_i + B & = & a_i Q_i + P_i + B \\ Q_{i+1} & = & Q_{i-1} + a_i(r_i + r_{i-1}) & = & \frac{P_{i+1}^2 + P_{i+1}B + C}{Q_i} \\ a_i & = & (P_i + d) \ div \ Q_i & = & \lfloor \alpha_i \rfloor \\ r_i & = & (P_i + d) \bmod Q_i & & \end{array}$$

is reduced.

Proof: Since α_i is reduced, $|P_i + Y + B| < |Q_i| < |P_i + Y|$. So $|P_{i+1} + Y| = |a_i Q_i + P_i + B + Y| = |a_i Q_i| > |Q_i|$. Thus,

$$|Q_{i+1}| = \left| \frac{(P_{i+1} + Y + B)(P_{i+1} + Y)}{Q_i} \right| > |P_{i+1} + Y + B| .$$

Notice $|P_i + Y + a_i Q_i| = |P_i + d + a_i Q_i| = |r_i| < |Q_i|$. So $|P_{i+1} + Y + B| = |P_i + Y + a_i Q_i| < |Q_i|$. Thus, from above, $|Q_{i+1}| < |P_{i+1} + Y|$. So we get that

$$|P_{i+1} + Y + B| < |Q_{i+1}| < |P_{i+1} + Y| .$$

Hence, if α_i is reduced then so is α_{i+1}. □

By induction it is easy to see that $q_i p_{i-1} + p_i q_{i-1} = 1$ for all $i \geq -1$. From this we get that $\alpha + \frac{p_i}{q_i} = \frac{p_i a_{i+1} + p_{i-1}}{q_i a_{i+1} + q_{i-1}} + \frac{p_i}{q_i} = \frac{1}{q_i(q_i a_{i+1} + q_{i-1})}$. So $\left|\alpha + \frac{p_i}{q_i}\right| = \frac{1}{|q_i||q_{i+1}|}$.

The following results show that, as in the odd characteristic case, the continued fraction expansion will produce reduced quadratic irrationals. We get a bound on when the reduced quadratic irrationals will appear and an easy way to tell which irrationals are reduced.

Theorem 4 *Let $\alpha_0 = \frac{P_0+Y}{Q_0}$ be a quadratic irrational. Then α_i is reduced for all $i > \max\left\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{2}\deg(B) + 1\right\}$.*

Proof: Let $i > \max\left\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{2}\deg(B) + 1\right\}$ be as above. Then $i - 1 > \frac{1}{2}\deg\left(\frac{Q_0}{B}\right)$ and so $\frac{|Q_0|}{|B|} < q^{2i-2}$. It is also easy to see by induction that $|q_i| \geq q^i$. From this we get $|\alpha_0 + \overline{\alpha_0}| = \left|\frac{P_0+Y}{Q_0} + \frac{P_0+Y+B}{Q_0}\right| = \left|\frac{B}{Q_0}\right| > \frac{1}{q^{2i-2}} \geq \frac{1}{|q_{i-1}|^2}$.

Now assume that α_i is not reduced. Since $i \geq 1$, we can see that $\deg(\lfloor \alpha_{i-1} \rfloor + \alpha_{i-1}) < 0$, so $|\alpha_i| > 1$. Also, $|\overline{\alpha_i}| \geq 1$ since α_i is not reduced. So,

$$\begin{aligned}
|\alpha_0 + \overline{\alpha_0}| &= \left|\frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})} + \frac{1}{q_{i-1}(q_{i-1}\overline{\alpha_i} + q_{i-2})}\right| \\
&\leq \max\left\{\left|\frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})}\right|, \left|\frac{1}{q_{i-1}(q_{i-1}\overline{\alpha_i} + q_{i-2})}\right|\right\} \\
&= \frac{1}{|q_{i-1}|}\max\left\{\frac{1}{|q_{i-1}\alpha_i|}, \frac{1}{|q_{i-1}\overline{\alpha_i}|}\right\} \\
&\leq \frac{1}{|q_{i-1}|^2}.
\end{aligned}$$

This contradiction proves the result. □

Theorem 5 *Let α be a quadratic irrational and $i \geq 0$. Then α_{i+1} is reduced if and only if $|Q_i| < |B|$.*

Proof: ($\Rightarrow$) Let α_{i+1} be reduced. Then $|\overline{\alpha_{i+1}}| < 1$ and $|P_{i+1}+Y| = |B|$. Now $\overline{\alpha_{i+1}} = \left(\frac{P_{i+1}+Y+B}{Q_{i+1}}\right)\left(\frac{P_{i+1}+Y}{P_{i+1}+Y}\right) = \frac{Q_i}{P_{i+1}+Y}$.

So $|Q_i| = |\overline{\alpha_{i+1}}|\,|P_{i+1}+Y| < |B|$.

($\Leftarrow$) Let $i \geq 0$ with $|Q_i| < |B|$. We need only show that $|\overline{\alpha_{i+1}}| < 1$, or in other words, $|P_{i+1}+Y+B| < |Q_{i+1}|$.

We know that $P_{i+1} = d + r_i + B$ where $0 \leq |r_i| < |Q_i| < |B|$. Thus, $|P_{i+1}+Y| = |P_{i+1}+d| = |r_i+B| = |B|$.

So, $|Q_{i+1}| = \frac{|P_{i+1}^2+P_{i+1}B+C|}{|Q_i|} = \frac{|B|}{|Q_i|}\,|P_{i+1}+Y+B| > |P_{i+1}+Y+B|$. □

Lemma 3 *Let $\alpha_0 = \frac{P_0+Y}{Q_0}$ be a quadratic irrational. If there exists a minimal $i_0 \geq 1$ such that $|Q_{i_0}| < |B|$, then α_{i_0} is not reduced.*

Proof: Now $|\overline{\alpha_{i_0}}| = \frac{|Q_{i_0-1}|}{|P_{i_0}+Y|} \geq \frac{|B|}{|P_{i_0}+Y|}$. If α_{i_0} is reduced then $|P_{i_0}+Y| = |B|$. But then $|\overline{\alpha_{i_0}}| \geq 1$ contradicting the fact that α_{i_0} is reduced. □

4.4 Period and Symmetry in the Continued Fraction Expansion

This section examines the periodic and symmetric aspects of the continued fraction expansion. These results will aid us in producing an algorithm to compute the regulator of K.

We say the continued fraction expansion of α is *quasi-periodic* if there exist integers $\nu > \nu_0 \geq 0$ and $c \in k^*$ such that

$$\alpha_\nu = c\alpha_{\nu_0}.$$

The smallest integer $m = \nu - \nu_0$ for which this holds is called the *quasi-period.* The expansion is called *periodic* if it holds with $c = 1$ and then $n = \nu - \nu_0$ is called the *period.*

If α has a periodic continued fraction expansion starting at ν_0 with period n then notice that

$$\begin{aligned} a_{\nu_0} &= a_{\nu_0+n} \\ a_{\nu_0+1} &= a_{\nu_0+n+1} \\ &\vdots \quad . \end{aligned}$$

We therefore write $\alpha = [a_0; a_1, a_2, \ldots, a_{\nu_0-1}, \overline{a_{\nu_0}, a_{\nu_0+1}, \ldots, a_{\nu_0+n-1}}]$.

Let α_0 be a quadratic irrational. Since α_i is reduced for $i > \max\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{2}\deg(B) + 1\}$ we know that either $|P_i| \leq |B|$ or $|P_i| = |Y|$ and also that $|Q_i| < |B|$. Thus the continued fraction expansion of $\alpha = \alpha_0$ is ultimately periodic when k is a finite field.

Lemma 4 *Let α be a quadratic irrational. Let the continued fraction expansion of α be quasi-periodic, so that*

$$c\alpha_{\nu_0} = \alpha_{\nu_0+m}$$

for some $c \in k^*$. Then $c^{(-1)^l}\alpha_{\nu_0+l} = \alpha_{\nu_0+m+l}$ for all $l \in \mathbb{Z}_{\geq 0}$.

Proof: We know that $\alpha_{\nu_0+m} = \frac{P_{\nu_0+m}+Y}{Q_{\nu_0+m}}$ and $\alpha_{\nu_0} = \frac{P_{\nu_0}+Y}{Q_{\nu_0}}$. So $P_{\nu_0+m} = P_{\nu_0}$ and $Q_{\nu_0} = cQ_{\nu_0+m}$.

Since

$$\begin{aligned} P_{\nu_0} + d = P_{\nu_0+m} + d &= a_{\nu_0}Q_{\nu_0} + r_{\nu_0} \\ &= a_{\nu_0}cQ_{\nu_0+m} + r_{\nu_0} \\ &= a_{\nu_0+m}Q_{\nu_0+m} + r_{\nu_0+m} \end{aligned}$$

we get that $a_{\nu_0+m} = ca_{\nu_0}$ and $r_{\nu_0} = r_{\nu_0+m}$.

Thus, $P_{\nu_0+1} = P_{\nu_0+m+1}$ and

$$\begin{aligned} Q_{\nu_0+1} &= \frac{P_{\nu_0+1}^2 + P_{\nu_0+1}B + C}{Q_{\nu_0}} \\ &= \frac{P_{\nu_0+m+1}^2 + P_{\nu_0+m+1}B + C}{cQ_{\nu_0+m}} \\ &= c^{-1}Q_{\nu_0+m+1}. \end{aligned}$$

So, $c^{-1}\alpha_{\nu_0+1} = \alpha_{\nu_0+m+1}$ and inductively we get $c^{(-1)^l}\alpha_{\nu_0+l} = \alpha_{\nu_0+m+l}$ for all $l \in \mathbb{Z}_{\geq 0}$. □

Proposition 1 *Let α be a quadratic irrational. If the continued fraction expansion of α is periodic with period n, then it is quasi-periodic with quasi-period m, and m divides n.*

Proof: Let $\nu \geq 0$ be such that $\alpha_\nu = \alpha_{\nu+n} = \alpha_{\nu+2n} = \cdots$.

Since the continued fraction expansion is periodic, by definition it must also be quasi-periodic. Let its quasi-period be $m \leq n$. Let $\nu_0 \geq \nu$ be such that $c\alpha_{\nu_0} = \alpha_{\nu_0+m}$ for some $c \in k^*$.

By Lemma 4 we get $c^{(-1)^{n-m}}\alpha_{\nu_0+(n-m)} = \alpha_{\nu_0+n} = \alpha_{\nu_0}$, the last equality following by periodicity. Now, since m is the quasi-period, either $m = n$ or $m \leq n - m$.

Assume $m \neq n$, then $c^{(-1)^m}\alpha_{\nu_0+m} = \alpha_{\nu_0+2m}$, so $c^{(-1)^m+1}\alpha_{\nu_0} = \alpha_{\nu_0+2m}$. Since $2m \leq n$, $(c^{(-1)^m+1})^{(-1)^{n-2m}}\alpha_{\nu_0+(n-2m)} = \alpha_{\nu_0+n} = \alpha_{\nu_0}$. Again, since m is the quasi-period, either $n = 2m$ or $m \leq n - 2m$.

Continuing in this fashion we get that m must divide n. □

It is easy to see that for a quadratic irrational α, the period n and quasi-period m start at the same index ν_0. We therefore define the non-negative integer ν_0 to

be minimal such that $\alpha_{\nu_0+m} = c\alpha_{\nu_0}$ and $\alpha_{\nu_0+n} = \alpha_{\nu_0}$ with $c \in k^*$. If $\nu_0 = 0$ then we say the expansion is *purely periodic.*

Lemma 5 *Let α be a quadratic irrational. If the continued fraction expansion of α is quasi-periodic so that $c\alpha_{\nu_0} = \alpha_{\nu_0+m}$, we have*

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}}\alpha_i$$

where $i \geq \nu_0$, $\lambda \geq 0$ and $c_i := c^{(-1)^{i-\nu_0}}$.

Proof: This proof will be by induction on λ. Let $i \geq \nu_0$.

Now, $\alpha_i = \alpha_{i+0m} = c_i^0\alpha_i$.

Also, $\alpha_{i+m} = \alpha_{(\nu_0+m)+(i-\nu_0)} = c^{(-1)^{i-\nu_0}}\alpha_{\nu_0+(i-\nu_0)} = c_i\alpha_i$, by Lemma 4.

So the result holds for $\lambda = 0, 1$. Let $\lambda \geq 1$ and assume that

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}}\alpha_i.$$

Then

$$\begin{aligned}
\alpha_{i+(\lambda+1)m} &= \alpha_{i+m+\lambda m} \\
&= c_i^{(-1)^{\lambda m}}\alpha_{i+\lambda m} \\
&= c_i^{(-1)^{\lambda m}}c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}}\alpha_i \\
&= c_i^{1+(-1)^m+\cdots+(-1)^{\lambda m}}\alpha_i.
\end{aligned}$$

With the second equality following from the case when $\lambda = 1$ and Lemma 4.

So, by the Principle of Mathematical Induction, the lemma holds. □

Corollary 1 *Let α be a quadratic irrational.*

1. *If the continued fraction expansion of α is quasi-periodic with odd quasi-period m, then it is periodic with period n and $n = m$ or $n = 2m$.*

2. *If the continued fraction expansion of α is periodic with odd period, then it is quasi-periodic with quasi-period $m = n$.*

Proof:

1. Let the expansion be quasi-periodic with quasi-period m, where m is odd. Then $\alpha_{\nu_0+2m} = c^{1+(-1)^m}\alpha_{\nu_0} = \alpha_{\nu_0}$. Thus, the expansion has period m or $2m$.

2. Let the expansion be periodic with odd period n. Then it is quasi-periodic with quasi-period m and m divides n. So m is odd. Thus, $n = m$ or $n = 2m$. Since n is odd, $n = m$.

□

For future reference and to summarize, we state the following theorem.

Theorem 6 *If α is a quadratic irrational over k (recall $|k| = 2^M$) then the continued fraction expansion of α is both periodic and quasi-periodic.*

Proof: The periodicity follows from the limits placed on reduced quadratic irrationals and the fact that α_i is reduced for all $i > \max\left\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{2}\deg(B) + 1\right\}$. The quasi-periodicity follows since if an expansion is periodic, then it is quasi-periodic, with $c = 1$ for example. □

Theorem 7 *Let α be a quadratic irrational, then the continued fraction expansion of α is purely periodic if and only if α is reduced.*

Proof: ($\Leftarrow$) Let α be reduced. Then we know that α_i is reduced for $i \geq 0$.

Let $k \geq 0$. Then $\alpha_{k+1} = \frac{1}{\alpha_k + a_k}$. So $\overline{\alpha_k} = a_k + \frac{1}{\overline{\alpha_{k+1}}}$.

Since α_k is reduced, we know that $|\overline{\alpha_k}| < 1$, thus $\left|a_k + \frac{1}{\overline{\alpha_{k+1}}}\right| < 1$. Now, it follows from the definition of a_k that $a_k \in k[x]$, so we get that $a_k = \left\lfloor \frac{1}{\overline{\alpha_{k+1}}} \right\rfloor$.

Since α is a quadratic irrational, its continued fraction expansion is periodic, so there exist $i, j \in \mathbb{Z}_{\geq 0}$, $i < j$ such that $\alpha_i = \alpha_j$, so $\frac{1}{\overline{\alpha_i}} = \frac{1}{\overline{\alpha_j}}$. Therefore, $a_{i-1} = a_{j-1}$ and $\alpha_{i-1} = \alpha_{j-1}$. Continuing in this way we get $\alpha_0 = \alpha_{j-i}$ and the continued fraction expansion is purely periodic with period less than or equal to $j - i$.

($\Rightarrow$) Let α have a purely periodic continued fraction expansion. We can assume without loss of generality that α is monic since if $c = \operatorname{sgn}(\alpha)$ then

$$c^{-1}\alpha = c^{-1}a_0 + \cfrac{1}{ca_1 + \cfrac{1}{c^{-1}a_2 + \cfrac{1}{ca_3 + \cfrac{1}{\ddots}}}}.$$

Now, $c^{-1}\alpha$ is monic and is still purely periodic, also α is reduced if and only if $c^{-1}\alpha$ is.

Let α have period $k+1$ so that $\alpha = \alpha_0 = \alpha_{k+1}$. Notice that $|\alpha| = |\alpha_{k+1}| > 1$. Thus, $\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$, and so $q_k\alpha^2 + (q_{k-1} + p_k)\alpha + p_{k-1} = 0$.

Now let $\beta = [\overline{a_k; a_{k-1}, \ldots, a_1, a_0}]$. Then it is easy to see that

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0] = \frac{p'_k}{q'_k}$$

and

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_1] = \frac{p'_{k-1}}{q'_{k-1}}$$

where $\frac{p'_k}{q'_k}$ and $\frac{p'_{k-1}}{q'_{k-1}}$ are the convergents to β.

Since α is monic, so is a_0 and thus $\operatorname{sgn}(p_k) = \operatorname{sgn}(q_k)$ and $\operatorname{sgn}(p_{k-1}) = \operatorname{sgn}(q_{k-1})$. Also, since $p'_k = a'_k p'_{k-1} + p'_{k-2} = a_0 p'_{k-1} + p'_{k-2}$, $\operatorname{sgn}(p'_k) = \operatorname{sgn}(p'_{k-1})$. Similarly, $\operatorname{sgn}(q'_k) = \operatorname{sgn}(q'_{k-1})$.

Since $p_k q_{k-1} + p_{k-1} q_k = 1$ and $p'_k q'_{k-1} + p'_{k-1} q'_k = 1$ we get $\gcd(p'_{k-1}, q'_{k-1}) = \gcd(p'_k, q'_k) = \gcd(p_k, p_{k-1}) = \gcd(q_k, q_{k-1}) = 1$. Also, $\frac{p_k}{\operatorname{sgn}(p_k)} = \frac{p'_k}{\operatorname{sgn}(p'_k)}$, $\frac{p_{k-1}}{\operatorname{sgn}(p_{k-1})} = \frac{q'_k}{\operatorname{sgn}(q'_k)}$, $\frac{q_k}{\operatorname{sgn}(q_k)} = \frac{p'_{k-1}}{\operatorname{sgn}(p'_{k-1})}$ and $\frac{q_{k-1}}{\operatorname{sgn}(q_{k-1})} = \frac{q'_{k-1}}{\operatorname{sgn}(q'_{k-1})}$.

Also, since β is periodic with period $k+1$,

$$\begin{aligned}
\beta &= \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}} \\
&= \frac{\beta \frac{\operatorname{sgn}(p'_k)}{\operatorname{sgn}(p_k)} p_k + \frac{\operatorname{sgn}(p'_{k-1})}{\operatorname{sgn}(q_k)} q_k}{\beta \frac{\operatorname{sgn}(q'_k)}{\operatorname{sgn}(p_{k-1})} p_{k-1} + \frac{\operatorname{sgn}(q'_{k-1})}{\operatorname{sgn}(q_{k-1})} q_{k-1}} \\
&= \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}.
\end{aligned}$$

So, $q_k \left(\frac{1}{\beta}\right)^2 + (q_{k-1} + p_k)\left(\frac{1}{\beta}\right) + p_{k-1} = 0$.

Now, α and $\frac{1}{\beta}$ both satisfy the same quadratic, so $\overline{\alpha} = \frac{1}{\beta}$. Since $|a_k| > 1$, we get $|\beta| > 1$, and so $|\overline{\alpha}| = \left|\frac{1}{\beta}\right| < 1$. Thus, α is reduced. □

Proposition 2 *If the continued fraction expansion of a quadratic irrational α is quasi-periodic with quasi-period m and $\nu_o \geq 0$, $c \in k^*$, then*

$$\begin{aligned}
P_i &= P_{i+\lambda m} \\
Q_i &= c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}} Q_{i+\lambda m}
\end{aligned}$$

for all $i \geq \nu_0$ and for all $\lambda \geq 0$, where $c_i := c^{(-1)^{i-\nu_0}}$.

Proof: Follows immediately from Lemma 5 and the fact that $\alpha_i = \frac{P_i + Y}{Q_i}$. □

Recall that Y satisfies $Y^2 + BY = C$ where $B, C \in k[X]$, C is monic, $Y \in k((\frac{1}{X}))$ and it has the additional property that $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have

a solution with $y \in k[X]$ for each $D|B$, $D \notin k$. So Y is a quadratic irrational with $P = 0$ and $Q = 1$. We would like to consider the continued fraction expansion of $\alpha = Y$. First notice that if $B = \lfloor Y \rfloor$ then Y is reduced and otherwise it is not.

If $B \neq \lfloor Y \rfloor$ then by Theorem 4 we know that α_i is reduced for all $i \geq 1$. Thus, the period starts at $\nu_0 = 1$. Let n be the period and m be the quasi-period and let $c \in k^*$ be such that $\alpha_{1+m} = c\alpha_1$ and $\alpha_{1+n} = \alpha_1$.

Consider $\beta = (B + \lfloor Y \rfloor) + Y$. Now β is reduced, so it has a purely periodic continued fraction expansion with period n'. Let its continued fraction expansion be $[\overline{a_0; a_1, \ldots, a_{n'-1}}]$. Notice that $a_0 = \lfloor \beta \rfloor = B$, so that $\beta = [\overline{B; a_1, \ldots, a_{n'-1}}]$. Thus $Y = [\lfloor Y \rfloor ; \overline{a_1, a_2, \ldots, a_{n'-1}, B}]$. So $n = n'$. Now $\lfloor Y \rfloor + Y = [0; \overline{a_1, a_2, \ldots, a_{n-1}, B}]$.

From our proof of Theorem 7 we can show that

$$\frac{1}{\overline{\beta}} = \frac{1}{\lfloor Y \rfloor + Y} = [\overline{a_{n-1}; a_{n-2}, \ldots, a_1, B}].$$

From above we get that

$$\frac{1}{\lfloor Y \rfloor + Y} = [\overline{a_1; a_2, \ldots, a_{n-1}, B}].$$

Thus, $a_1 = a_{n-1}$, $a_2 = a_{n-2}$, etc. So we have the continued fraction expansion of Y being $[d; \overline{a_1, a_2, \ldots, a_2, a_1, B}]$.

It is now easy to deduce that $\frac{1}{\overline{\alpha_{n-i}}} = \alpha_{i+1}$ for $i = 0, \ldots, n-1$. From this we get that $P_{i+1} = P_{n-i}$ for $i = 0, \ldots, n-1$ and $Q_i = Q_{n-i}$ for $i = 1, \ldots, n$.

On the other hand if $B = \lfloor Y \rfloor$ then Y is reduced. Thus it is periodic with period n starting at $\nu_0 = 0$ and $a_0 = B$. So $Y = [\overline{B; a_1, \ldots, a_{n-1}}]$ and $\frac{1}{Y+B} = [\overline{a_{n-1}; a_{n-2}, \ldots, a_1, B}]$. But $Y + B = [0; \overline{a_1, \ldots, a_{n-1}, B}]$ so $\frac{1}{Y+B} = [\overline{a_1; \ldots, a_{n-1}, B}]$ and thus $a_1 = a_{n-1}$, $a_2 = a_{n-2}$, etc.

As above we get that $Y = [d; \overline{a_1, a_2, \ldots, a_2, a_1, B}]$. Similarly we get $\frac{1}{\overline{\alpha_{n-i}}} = \alpha_{i+1}$ for $i = 0, \ldots, n-1$, $P_{i+1} = P_{n-i}$ for $i = 0, \ldots, n-1$ and $Q_i = Q_{n-i}$ for $i = 1, \ldots, n$.

From now on, if m is the quasi-period of $\alpha = Y$, then $c \in k^*$ is such that $c\alpha_1 = \alpha_{m+1}$.

Theorem 8 *If the continued fraction expansion of Y is periodic with period n and quasi-period m, then $Q_s \in k^*$ if and only if $s = \lambda m$ with $\lambda \geq 0$.*

Proof: ($\Rightarrow$) Let $Q_s = b \in k^*$. If $s = 0$ then the assertion is true. So, let $s \geq 1$ be the least such s. It suffices to show that $s = m$. In Proposition 2 let $i = m$ and $(\lambda + 1)m = n$, then $Q_m = c_m^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}} \in k^*$, so $m \geq s$.

We know that $P_1 = d + B$ and $Q_1 = d^2 + dB + C$. Furthermore, $\alpha_s = \frac{P_s+Y}{Q_s} = \frac{1}{b}(P_s + Y)$ is reduced, so $|P_s + Y + B| < 1$ and thus $P_s = d + B$. Hence, $a_s = \frac{B}{b}$. This gives $P_{s+1} = B + d = P_1$ and $Q_{s+1} = \frac{d^2+dB+C}{b} = \frac{1}{b}Q_1$. But this says that $\alpha_{s+1} = b\alpha_1$. Since m is the quasi-period, we must have $m \leq s$. Thus, $s = m$.

($\Leftarrow$) Let $s = \lambda m$. If $s = 0$ or $n = m$, there is nothing to show. Thus, let $n = lm$ where $l \geq 2$ and define $c_m = c^{(-1)^{m-1}}$ where c is defined as previously.

Now, again from Proposition 2 we know that for all $\lambda \geq 1$,

$$Q_m = c_m^{1+(-1)^m+\cdots+(-1)^{(\lambda-2)m}} Q_{\lambda m}.$$

We also have $Q_m = c_m^{1+(-1)^m+\cdots+(-1)^{(l-2)m}} Q_{lm}$ and $Q_{lm} = Q_n = 1$, so $Q_m \in k^*$, and the result follows. □

Corollary 2 *If the continued fraction expansion of Y is periodic with period n and quasi-period m, then*

$$N(\overline{\theta_{\lambda m+1}}) = p_{\lambda m-1}^2 + p_{\lambda m-1}q_{\lambda m-1}B + q_{\lambda m-1}^2 C \in k^*$$

for $\lambda \geq 0$.

Proof: We know that $N(\overline{\theta_{\lambda m+1}}) = N(\theta_{\lambda m+1}) = \frac{q_{\lambda m}}{Q_0} \in k^*$. We also know $\theta_{\lambda m+1} = p_{\lambda m-1} + Y q_{\lambda m-1}$ and the result follows. □

Lemma 6 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n and quasi-period m. Then, for each $\lambda \geq 1$ there exists a constant $\tilde{c}(\lambda) \in k^*$ such that*

$$\theta_{\lambda m+1} = \tilde{c}(\lambda)(\theta_{m+1})^{\lambda}.$$

Proof: We know that for all $i \geq 1$,

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}} \alpha_i$$

where $c_i := c^{(-1)^{i-1}}$.

Recalling that $\theta_{i+1} = \prod_{j=1}^{i} \frac{1}{\alpha_j}$, it follows that

$$\prod_{j=\lambda m+1}^{\lambda m+m} \frac{1}{\alpha_j} = \prod_{j=1}^{m} \frac{1}{\alpha_{\lambda m+j}} = \hat{c} \cdot \theta_{m+1}$$

where $\hat{c} = \prod_{j=1}^{m} c_j^{-1-(-1)^m-\cdots-(-1)^{(\lambda-1)m}}$. The assertion now follows by a simple induction. □

Theorem 9 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n.*

1. *If there exists a $1 \leq \nu \leq n-1$ with $P_\nu = P_{\nu+1}$ then $n = 2\nu$. Conversely, if $n = 2\nu$, then $P_\nu = P_{\nu+1}$.*

2. *If there exists a $0 \leq \mu \leq n-1$ with $Q_\mu = Q_{\mu+1}$ then $n = 2\mu + 1$. Conversely, if $n = 2\mu + 1$, then $Q_\mu = Q_{\mu+1}$.*

Proof:

1. Let $1 \leq \nu \leq n-1$ with $P_\nu = P_{\nu+1}$. Then $P_\nu = P_{\nu+1} = P_{n-\nu}$. We also know $Q_\nu = Q_{n-\nu}$ so $\alpha_\nu = \alpha_{n-\nu}$. Thus, $\nu = n - \nu$ or $2\nu = n$. Conversely, if $n = 2\nu$ then $P_\nu = P_{n-\nu} = P_{\nu+1}$.

2. Let $0 \leq \mu \leq n-1$ with $Q_\mu = Q_{\mu+1}$. Then $Q_{\mu+1} = Q_\mu = Q_{n-\mu}$. We also know $P_{\mu+1} = P_{n-\mu}$ so $\alpha_{\mu+1} = \alpha_{n-\mu}$. Thus, $\mu+1 = n-\mu$ or $n = 2\mu+1$. Conversely, if $n = 2\mu+1$ then $Q_\mu = Q_{n-\mu} = Q_{\mu+1}$.

□

Corollary 3 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n and quasi-period m. Then either*

1. *$n = m$ odd*

2. *$n = m$ even or*

3. *$n = 2m$ even, m odd.*

Proof: If the period is odd then we know that $n = m$ and both are odd. Now, let n be even and assume that $n \neq m$. Then we know that $n = lm$ with $l \geq 2$. So $P_{m+1} = P_{m+1+(l-2)m} = P_{(l-1)m+1} = P_{n-(l-1)m} = P_m$ so from Theorem 9, $n = 2m$. Assume also that m is even, so $m = 2s$. Then, $P_{s+1} = P_{m+s+1} = P_{n-(m+s)} = P_s$, so again $n = 2s = m$ contradicting the fact that $n \neq m$. Thus m must be odd. □

Theorem 10 *If the continued fraction expansion of $\alpha = Y$ is periodic with period n and quasi-period m, then we have the following symmetric properties with respect to the quasi-period*

$$\begin{aligned} P_{i+1} &= P_{m-i} && i = 0, \ldots, m-1 \\ Q_i &= c^{(-1)^{i-1}} Q_{m-i} && i = 0, \ldots, m \\ \frac{1}{\alpha_{m-i}} &= c^{(-1)^i} \alpha_{i+1} && i = 0, \ldots, m-1. \end{aligned}$$

Proof: If $n = m$ there is nothing to prove since the symmetric properties can be deduced from the symmetric properties for the period. Therefore, let $n = 2m$ with m odd. We know $P_{i+1} = P_{i+m+1}$ and $Q_i = c^{(-1)^{i-1}} Q_{i+m}$. Also, $P_{i+m+1} = P_{n-(i+m)}$ and $Q_{i+m} = Q_{n-(i+m)}$. The first two symmetries follow since $n = 2m$. Finally, $c^{(-1)^i} \alpha_{i+1} = c^{(-1)^i} \left(\frac{P_{i+1}+Y}{Q_{i+1}} \right) = \frac{P_{m-i}+Y}{Q_{m-i-i}} = \frac{1}{\alpha_{m-i}}$. □

Theorem 11 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n and quasi-period m.*

1. *If there exists a $1 \leq \nu \leq m-1$ with $P_\nu = P_{\nu+1}$ then $m = 2\nu = n$. Conversely, if $m = 2\nu$, then $P_\nu = P_{\nu+1}$ and $n = m$.*

2. *If there exists a $0 \leq \mu \leq m-1$ with $Q_{\mu+1} = c' Q_\mu$ for some $c' \in k^*$, then $m = 2\mu + 1$. If $c' = 1$ then $n = m$. If $c' \neq 1$ then $n = 2m$. Conversely, if $m = 2\mu + 1$, then there is a $c' \in k^*$ such that $Q_{\mu+1} = c' Q_\mu$.*

Proof:

1. If $P_\nu = P_{\nu+1}$ then we know that $n = 2\nu$. Since $\nu \leq m-1$ we get that $m = 2\nu = n$. Conversely, if $m = 2\nu$ we know that $n = m$ and the assertion follows from the similar result for the period.

2. If $Q_{\mu+1} = c' Q_\mu$ then we can derive that

$$\alpha_{m-\mu} = \frac{P_{m-\mu} + Y}{Q_{m-\mu}} = c^{(-1)^{\mu-1}} \left(\frac{P_{\mu+1} + Y}{Q_\mu} \right) = c' c^{(-1)^{\mu-1}} \alpha_{\mu+1}.$$

   Thus $m - \mu = \mu + 1$ or $m = 2\mu + 1$. Conversely, if $m = 2\mu + 1$, Theorem 10 gives that $Q_{\mu+1} = c^{(-1)^\mu} Q_\mu$. The remainder of the proof is trivial.

□

Notice that c' can be calculated as $\frac{\mathrm{sgn}(Q_{\mu+1})}{\mathrm{sgn}(Q_\mu)}$.

Let $c(\mu) = \prod_{j=0}^{\mu} c^{(-1)^j} \in k^*$ where c is defined as before.

Remark 1 *1.* $c' = c^{(-1)^\mu}$

2. If μ *is even then* $c(\mu) = c'$, *otherwise* $c(\mu) = 1$.

Theorem 12 *Let the continued fraction expansion of* $\alpha = Y$ *be periodic with period* n *and quasi-period* m.

1. *If there exists a* $1 \leq \nu \leq m-1$ *with* $P_\nu = P_{\nu+1}$ *then*

$$\overline{\theta_{m+1}} = \frac{\overline{\theta_{\nu+1}}}{\theta_{\nu+1}} = \frac{\overline{\theta_{\nu+1}}^2}{Q_\nu} = \frac{Q_\nu}{\theta_{\nu+1}^2}.$$

2. *If there exists a* $1 \leq \mu \leq m-1$ *with* $Q_{\mu+1} = c'Q_\mu$ *for some* $c' \in k^*$, *then with* $c(\mu)$ *as defined above*

$$\overline{\theta_{m+1}} = c(\mu)\frac{\overline{\theta_{\mu+1}\theta_{\mu+2}}}{Q_{\mu+1}} = c(\mu)\overline{\theta_{\mu+1}}^2\frac{\alpha_{\mu+1}}{Q_\mu} = c(\mu)\frac{\alpha_{\mu+1}Q_\mu}{\theta_{\mu+1}^2}.$$

Proof:

1. We know that $n = m = 2\nu$ which allows us to do the following

$$\prod_{j=\nu+1}^{m}\frac{1}{\overline{\alpha_j}} = \prod_{j=0}^{\nu-1}\frac{1}{\overline{\alpha_{m-j}}} = \prod_{j=0}^{\nu-1}\alpha_{j+1} = \frac{1}{\theta_{\nu+1}}.$$

So,

$$\overline{\theta_{m+1}} = \prod_{j=1}^{m}\frac{1}{\overline{\alpha_j}} = \prod_{j=1}^{\nu}\frac{1}{\overline{\alpha_j}}\prod_{j=\nu+1}^{m}\frac{1}{\overline{\alpha_j}} = \frac{\overline{\theta_{\nu+1}}}{\theta_{\nu+1}}.$$

The last two equalities follow since $\theta_{\nu+1}\overline{\theta_{\nu+1}} = \frac{Q_\nu}{Q_0}$.

2. Let c and $c(\mu)$ be defined as always. We know that $m = 2\mu + 1$ which allows us to do the following

$$\prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha_j}} = \prod_{j=0}^{\mu} \frac{1}{\overline{\alpha_{m-j}}} = c^{(-1)^0+(-1)^1+\cdots+(-1)^\mu} \prod_{j=0}^{\mu} \alpha_{j+1} = \frac{c(\mu)}{\theta_{\mu+2}}.$$

So

$$\overline{\theta_{m+1}} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha_j}} = \prod_{j=1}^{\mu} \frac{1}{\overline{\alpha_j}} \prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha_j}} = \frac{c(\mu)\overline{\theta_{\mu+1}}}{\theta_{\mu+2}} = c(\mu)\frac{\overline{\theta_{\mu+1}\theta_{\mu+2}}}{Q_{\mu+1}}.$$

The last two equalities follow since $\alpha_{\mu+1}\overline{\alpha_{\mu+1}} = \frac{Q_\mu}{Q_{\mu+1}}$.

□

We can now define $A_{i+1} = \sum_{j=1}^{i} \deg(a_j)$ for $i \geq 0$. Since $\theta_{i+1} = \prod_{j=1}^{i} \frac{1}{\alpha_j}$, we see that $A_{i+1} = -\deg(\theta_{i+1})$. Also, since $\theta_{i+1}\overline{\theta_{i+1}} = Q_i$ (recall we are looking at the continued fraction expansion of $\alpha = Y$, so $Q_0 = 1$), we get $A_{i+1} = \deg(\overline{\theta_{i+1}}) - \deg(Q_i)$.

Corollary 4 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n and quasi-period m.*

1. *If there exists a $1 \leq \nu \leq m-1$ with $P_\nu = P_{\nu+1}$ then*

$$\begin{aligned} \deg(\overline{\theta_{m+1}}) &= 2\deg(\overline{\theta_{\nu+1}}) - \deg(Q_\nu) \\ &= 2A_{\nu+1} + \deg(Q_\nu). \end{aligned}$$

2. *If there exists a $0 \leq \mu \leq m-1$ with $Q_{\mu+1} = c'Q_\mu$ for some $c' \in k^*$, then*

$$\begin{aligned} \deg(\overline{\theta_{m+1}}) &= 2\deg(\overline{\theta_{\mu+1}}) - \deg(Q_\mu) + \deg(a_{\mu+1}) \\ &= 2A_{\mu+1} + \deg(B). \end{aligned}$$

Proof:

1. The result follows since $\overline{\theta_{m+1}} = \frac{\overline{\theta_{\nu+1}}^2}{Q_\nu}$.

2. The result follows since $\overline{\theta_{m+1}} = c(\mu)\frac{\overline{\theta_{\mu+1}}^2 a_{\mu+1}}{Q_\mu}$ and $|a_{\mu+1}Q_{\mu+1}| = |B|$.

□

Corollary 5 *Let the continued fraction expansion of $\alpha = Y$ be periodic with period n and quasi-period m.*

1. *If there exists a $1 \leq \nu \leq m-1$ with $P_\nu = P_{\nu+1}$ then*

$$p_{m-1} = p_\nu q_{\nu-1} + p_{\nu-1}q_{\nu-2}$$

and

$$q_{m-1} = q_{\nu-1}q_\nu + q_{\nu-1}q_{\nu-2}.$$

2. *If there exists a $0 \leq \mu \leq m-1$ with $Q_{\mu+1} = c'Q_\mu$, where $c' \in k^*$ then with $c(\mu)$ as defined before, we have*

$$p_{m-1} = \frac{c(\mu)}{c'}(p_\mu q_\mu + c' q_{\mu-1}p_{\mu-1})$$

and

$$q_{m-1} = \frac{c(\mu)}{c'}(c' q_{\mu-1}^2 + q_\mu^2).$$

Proof:

1. Comparing rational and irrational parts of $Q_\nu\overline{\theta_{m+1}} = \overline{\theta_{\nu+1}}^2$ we get that

$$Q_\nu p_{m-1} = Q_\nu q_{m-1}B + p_{\nu-1}^2 + Cq_{\nu-1}^2 + B^2q_{\nu-1}^2$$

and

$$Q_\nu q_{m-1} = Bq_{\nu-1}^2.$$

We know that $N(\theta_{\nu+1}) = p_{\nu-1}^2 + Bp_{\nu-1}q_{\nu-1} + Cq_{\nu-1}^2 = Q_\nu$ and $p_\nu q_{\nu-1} + p_{\nu-1}q_\nu = 1$. Also since $P_\nu = P_{\nu+1}$ we can deduce that $a_\nu Q_\nu = B$. Using these results and the formula for q_ν the assertion can be proven.

2. Comparing rational and irrational parts of $Q_{\mu+1}\overline{\theta_{m+1}} = c(\mu)\overline{\theta_{\mu+1}\theta_{\mu+2}}$ we get that

$$Q_{\mu+1}p_{m-1} = Q_{\mu+1}q_{m-1}B + c(\mu)(p_\mu p_{\mu-1} + Bp_{\mu-1}q_\mu + Bp_\mu q_{\mu-1} + Cq_{\mu-1}q_\mu + B^2 q_{\mu-1}q_\mu)$$

and

$$Q_{\mu+1}p_{m-1} = c(\mu)(p_{\mu-1}q_\mu + p_\mu q_{\mu-1} + Bq_{\mu-1}q_\mu).$$

Using the formulas for P_{i+1}, Cq_{i-1}, $Q_0 p_{i-1}$, and q_i given in Section 4.2 the assertion can be deduced.

□

4.5 The Fundamental Unit and Regulator

We are now in a position to examine the fundamental unit of $\mathcal{O}^*$ and define the regulator. We will first state some results which will be useful in finding the form of the fundamental unit.

Recall that the continued fraction algorithm gives

$$\begin{aligned} p_{-2} &= 0 & q_{-2} &= 1 \\ p_{-1} &= 1 & q_{-1} &= 0 \\ p_i &= a_i p_{i-1} + p_{i-2} & q_i &= a_i q_{i-1} + q_{i-2} \end{aligned}$$

for all $i \geq 0$.

Theorem 13 *Let α be a quadratic irrational. If the two polynomials $p', q' \in k[X]$, $q' \neq 0$ satisfy $\left|\alpha + \frac{p'}{q'}\right| < \frac{1}{|q'|^2}$, then there exists $l \in \mathbb{Z}_{\geq 0}$ such that $\frac{p'}{q'} = \frac{p_l}{q_l}$.*

Proof: We can easily see that $1 = |q_0| < |q_1| < \cdots < |q_i| < |q_{i+1}| < \cdots$ for all $i \geq 0$. Since $0 \neq q' \in k[X]$ we know $|q'| \geq 1$. Thus there exists an $l \geq 0$ such that $|q_l| \leq |q'| < |q_{l+1}|$.

From this it follows that $\left|\alpha + \frac{p'}{q'}\right| < \frac{1}{|q'|^2} \leq \frac{1}{|q'||q_l|}$.

On the other hand we know that $\left|\alpha + \frac{p_l}{q_l}\right| = \frac{1}{|q_{l+1}||q_l|} < \frac{1}{|q'||q_l|}$.

Altogether, we get

$$\begin{aligned}
\frac{|p'q_l + p_l q'|}{|q'|\,|q_l|} &= \left|\frac{p'}{q'} + \frac{p_l}{q_l}\right| \\
&= \left|\left(\alpha + \frac{p'}{q'}\right) + \left(\alpha + \frac{p_l}{q_l}\right)\right| \\
&\leq \max\left\{\left|\alpha + \frac{p'}{q'}\right|, \left|\alpha + \frac{p_l}{q_l}\right|\right\} \\
&< \frac{1}{|q'|\,|q_l|}.
\end{aligned}$$

Thus, $|p'q_l + p_l q'| < 1$ and since they are all polynomials, we know $p'q_l + p_l q' = 0$. The result follows. □

Corollary 6 *Let α be a quadratic irrational. If the two polynomials $p', q' \in k[X]$, $q' \neq 0$ satisfy $\left|\alpha + \frac{p'}{q'}\right| < \frac{1}{|q'|^2}$ then there exist $l \geq 0$ and $r \in k[X]$ such that $p' = rp_l$ and $q' = rq_l$. Also if $\gcd(p', q') = 1$, then $p' = cp_l$ and $q' = cq_l$ for some $c \in k^*$.*

Proof: By the above theorem we know that $p'q_l = q'p_l$. Thus, $q_l | q'p_l$ and $p_l | p'q_l$. Since $\gcd(p_l, q_l) = 1$ we get $q_l | q'$ and $p_l | p'$.

Therefore, there exist $r, s \in k[X]$ such that $q' = sq_l$ and $p' = rp_l$. But $\frac{p_l}{q_l} = \frac{p'}{q'} = \frac{rp_l}{sq_l}$, so we must have $r = s$.

If $\gcd(p', q') = 1$ then it must be the case that $r \in k^*$. □

Remark 2 *Let $\eta = U + VY \in \mathcal{O}$, where U and V are polynomials in $k[X]$. Then η is a unit in $\mathcal{O}$ if and only if $N(\eta) \in k^*$.*

The fundamental unit can be found, as in the odd characteristic case by the continued fraction expansion of Y.

Theorem 14 *Let Y satisfy $Y^2 + BY = C$, for $B, C \in k[X]$, C is monic, $Y \in k((\frac{1}{X}))$ and it has the additional property that $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have a solution with $y \in k[X]$ for each $D|B$, $D \notin k$. If the quasi-period of the continued fraction expansion of Y is m and $\epsilon = p_{m-1} + q_{m-1}(Y + B)$ then*

$$\mathcal{O}^* = k^* \times \langle \epsilon \rangle = k^* \times \langle \overline{\theta_{m+1}} \rangle.$$

Proof: We already know that the continued fraction expansion of Y is periodic and quasi-periodic and that $\epsilon = \overline{\theta_{m+1}}$.

We also know that $N(\overline{\theta_{m+1}}) \in k^*$ so $\overline{\theta_{m+1}}$ is a unit in $\mathcal{O}$.

Let $\eta = U + V(Y + B) \in \mathcal{O}^*$ be a unit, where U and V are polynomials in $k[X]$. If $|\eta| = 1$ we are done. So, let $|\eta| > 1$. Since η is a unit, $N(\eta) \in k^*$ and so $|N(\eta)| = 1 = |\eta|\,|\overline{\eta}|$.

Now $|U + YV| = |\overline{\eta}| = \frac{1}{|\eta|} < 1 < |VB|$, since $|V| \geq 1$ and $|B| > 1$. Also,

$$\begin{aligned} |\eta| &= |U + V(Y + B)| \\ &= |(U + YV) + VB| \\ &= |\overline{\eta} + VB| \\ &= \max\{|\overline{\eta}|, |VB|\} \\ &= |VB| \\ &> |V|. \end{aligned}$$

Since $|B| > 1$.

This tells us that

$$\begin{aligned}\left|Y + \frac{U}{V}\right| &= \frac{|VY + U|}{|V|} \\ &= \frac{|\overline{\eta}|}{|V|} \\ &= \frac{1}{|\eta|\,|V|} \\ &< \frac{1}{|V|^2}.\end{aligned}$$

Since η is a unit we must have $\gcd(U, V) = 1$, so there exists a $c_0 \in k^*$, and a $j \geq 1$ such that $U = c_0 p_{j-1}$ and $V = c_0 q_{j-1}$ or equivalently $\eta = c_0\overline{\theta_{j+1}}$. Therefore, $N(\eta) = c_0^2 N(\overline{\theta_{j+1}}) = c_0^2 Q_j \in k^*$. Hence $j = \lambda m$ for some $\lambda \geq 0$.

This tells us that

$$\begin{aligned}\eta &= c_0\overline{\theta_{\lambda m+1}} \\ &= c_0\tilde{c}(\lambda)(\overline{\theta_{m+1}})^{\lambda}.\end{aligned}$$

If $|\eta| < 1$ we can use $\frac{1}{\eta}$ and get the same result. Thus the assertion is proved.

□

We are now in a position to define the *regulator*, R, of $k(X)(Y)$. It is the degree of the fundamental unit of $\mathcal{O}^*$. From the last theorem we can see that $R = \deg(\overline{\theta_{m+1}})$ where m is the quasi-period in the continued fraction expansion of $\alpha = Y$. Since $\deg(Q_m) = 0$ we get $R = A_{m+1}$.

Chapter 5

Finding the Regulator

This chapter will examine the infrastructure of quadratic function fields and use it to compute the regulator. The infrastructure is the inner structure of the set of all reduced ideals in the ideal class group of $\mathcal{O}$ with the property that given one ideal in a class, the continued fraction algorithm will produce the remaining reduced ideals in that class. First we must examine ideals in $\mathcal{O}$ and their relationship with the material in the previous chapter. We will then define a distance function which will allow us to compute the regulator. We will also define an operation called a Giant-Step. This corresponds to ideal multiplication, which may give an ideal not in the infrastructure, followed by reduction using the continued fraction algorithm, which will bring us back to an ideal in the infrastructure.

We are still in the same situation as the previous chapter. So k is a field with $q = 2^M$ elements and X is transcendental over k. Now $K = k(X)(Y)$ where $Y^2 + BY = C$ for some $B, C \in k[X]$ with C monic. Also $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have a solution with $y \in k[X]$ for each non-constant polynomial D that divides B and $K \subseteq k((\frac{1}{X}))$.

5.1 Ideals in $\mathcal{O}$

Let $\mathcal{O} = k[X][Y] \subseteq \mathcal{O}_K$ where $K = k(X)(Y)$. We call a subset $\mathcal{A} \neq \{0\}$ of K an *$\mathcal{O}$-ideal* if $\mathcal{A}$ possesses the properties:

1. If $\lambda_1, \lambda_2 \in \mathcal{O}$ and $\alpha_1, \alpha_2 \in \mathcal{A}$ then $\lambda_1\alpha_1 + \lambda_2\alpha_2 \in \mathcal{A}$.
2. There exists a $\lambda \in \mathcal{O}$, $\lambda \neq 0$ such that $\lambda\mathcal{A} \subseteq \mathcal{O}$.

If Property 2 holds with $\lambda = 1$, we say that $\mathcal{A}$ is an *integral* $\mathcal{O}$-ideal.

For elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ the set

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) := \left\{ \sum_{i=1}^{r} \lambda_i\alpha_i | \lambda_i \in \mathcal{O}, i = 1, \ldots, r \right\}$$

is clearly an $\mathcal{O}$-ideal. This is the ideal generated by $\alpha_1, \alpha_2, \ldots, \alpha_r$. If $\mathcal{A}$ is generated by just $\alpha \in K$ then we say that $\mathcal{A}$ is a *principal* $\mathcal{O}$-ideal.

For $\omega_1, \omega_2, \ldots, \omega_r \in \mathcal{O}$ we let

$$[\omega_1, \omega_2, \ldots, \omega_r] := \left\{ \sum_{i=1}^{r} A_i\omega_i | A_i \in k[X], i = 1, \ldots, r \right\} \subseteq \mathcal{O}.$$

If this set is an integral $\mathcal{O}$-ideal and $\omega_1, \omega_2, \ldots, \omega_r$ are linearly independent over $k[X]$ then $\{\omega_1, \omega_2, \ldots, \omega_r\}$ is called a $k[X]$-basis of the $\mathcal{O}$-ideal. It is easy to see that every $k[X]$-basis of an $\mathcal{O}$-ideal, $\mathcal{A}$, has exactly two elements. (See Appendix B.)

Theorem 15 *A nonzero subset $\mathcal{A}$ of $\mathcal{O}$ is an integral ideal if and only if there exist $S, P, Q \in k[X]$ with $Q|P^2 + PB + C$ such that $\mathcal{A} = [SQ, SP + SY]$.*

Proof: ($\Rightarrow$) Let $\mathcal{A}$ be an integral ideal. Then $\mathcal{A} = [Q', P' + SY]$ for some $P', Q', S \in k[X]$. Then $Q'Y \in \mathcal{A}$, so $S|Q'$ or $Q' = SQ$. Clearly $N(P' + SY) \in \mathcal{A}$, so $Q'|N(P' +$

SY) and since $N(P'+SY) = P'^2 + P'SB + S^2C$ we get $S|P'^2$. From this we can deduce $S|P'$, so $P' = SP$. Hence, $\mathcal{A} = S[Q, P+Y]$ for some $P, Q, S \in k[X]$ where $Q|P^2 + PB + C$.

($\Leftarrow$) Let $S, P, Q \in k[X]$ with $Q|P^2 + PB + C$ and $\mathcal{A} = [SQ, SP + SY]$. Let $U_1, U_2, V_1, V_2 \in k[X]$ so that $U_1 + V_1Y, U_2 + V_2Y \in \mathcal{O}$. Also let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in k[X]$.

Notice

$$\begin{aligned}(U_1 + V_1Y)(\alpha_1 SQ + \beta_1 SP + \beta_1 SY) + (U_2 + V_2Y)(\alpha_2 SQ + \beta_2 SP + \beta_2 SY) = \\ (SP + SY)\left((P+B)(V_1\beta_1 + V_2\beta_2) + U_1\beta_1 + U_2\beta_2 + Q(V_1\alpha_1 + V_2\alpha_2)\right) + \\ SQ\left(U_1\alpha_1 + U_2\alpha_2 + P(V_1\alpha_1 + V_2\alpha_2) + (V_1\beta_1 + V_1\beta_2)\frac{P^2 + PB + C}{Q}\right) \\ \in \mathcal{A}.\end{aligned}$$

Notice also that $\mathcal{A} \subseteq \mathcal{O}$. Thus $\mathcal{A}$ is an integral ideal. □

We say that $\mathcal{A}$ is *primitive* if S can be chosen to be 1.

A $k[X]$-basis of an integral $\mathcal{O}$-ideal can be chosen in *adapted form*, which means that $\mathcal{A} = [SQ, SP+SY]$ where $\deg(P) < \deg(Q)$ and Q is monic. The polynomials P and Q are unique and S is unique up to a constant factor.

Let $\mathcal{A}$ be an integral $\mathcal{O}$-ideal with $k[X]$-basis $\{\omega_1, \omega_2\}$. Then $\mathcal{A} = [\omega_1, \omega_2]$. We define the *norm* of $\mathcal{A}$, $N(\mathcal{A})$ by

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{vmatrix}^2 = c^2(N(\mathcal{A})^2)B^2$$

where $c \in k^*$ is chosen to make $\operatorname{sgn}(N(\mathcal{A})) = 1$. The norm doesn't depend on the given $k[X]$-basis $\{\omega_1, \omega_2\}$. If $\mathcal{A} = [SQ, SP + SY]$ then $N(\mathcal{A}) = \frac{S^2Q}{\operatorname{sgn}(S^2Q)} \in k[X]$.

We define the product of two $\mathcal{O}$-ideals $\mathcal{A} = [\alpha_1, \alpha_2]$ and $\mathcal{B} = [\beta_1, \beta_2]$ by $[\alpha_1, \alpha_2][\beta_1, \beta_2] = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$. Also, $(\beta)[\alpha_1, \alpha_2] = [\beta\alpha_1, \beta\alpha_2]$.

Let $\mathcal{A}$ be any $\mathcal{O}$-ideal, then

$$\overline{\mathcal{A}} := \{\overline{\alpha} | \alpha \in \mathcal{A}\}$$

is called the *conjugate ideal* of $\mathcal{A}$. If $\mathcal{A} = [\alpha_1, \alpha_2]$ then notice that $\overline{\mathcal{A}} = [\overline{\alpha_1}, \overline{\alpha_2}]$.

Lemma 7 *1. If $\mathcal{A}$ is an integral $\mathcal{O}$-ideal then $\mathcal{A}\overline{\mathcal{A}} = (N(\mathcal{A}))$.*

2. If $\mathcal{A}$ and $\mathcal{B}$ are integral $\mathcal{O}$-ideals then $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$.

3. If $\mathcal{A} = (\alpha)$ where $\alpha \in \mathcal{O}$, then there exists $c \in \mathcal{O}^*$ such that $N(\mathcal{A}) = cN(\alpha)$.

Proof:

1. Let $\mathcal{A} = [SQ, SP + SY]$. Then

$$\begin{aligned} \mathcal{A}\overline{\mathcal{A}} &= (S^2Q)(Q, P+Y, P+Y+B, \frac{P^2+BP+C}{Q}) \\ &= (S^2Q)(Q, B, \frac{P^2+BP+C}{Q}, P+Y). \end{aligned}$$

Let $\delta = \gcd(Q, B, \frac{P^2+BP+C}{Q})$. Then $\delta | B$, and since $\delta | Q$ and $\delta | \frac{P^2+BP+C}{Q}$, $\delta^2 | P^2 + BP + C$. We know from our restrictions on B and C in the introduction to this chapter that this is only possible if $\delta \in k$.

Thus, $\gcd(Q, B, \frac{P^2+BP+C}{Q}) = 1$ and

$$\begin{aligned} \mathcal{A}\overline{\mathcal{A}} &= (S^2Q)(1, Y) \\ &= (S^2Q) \\ &= (N(\mathcal{A})). \end{aligned}$$

2. From Part 1 we get

$$\begin{aligned}(N(\mathcal{AB})) &= \mathcal{AB}\overline{\mathcal{AB}} \\ &= \mathcal{A}\overline{\mathcal{A}}\mathcal{B}\overline{\mathcal{B}} \\ &= (N(\mathcal{A}))(N(\mathcal{B})) \\ &= (N(\mathcal{A})N(\mathcal{B})).\end{aligned}$$

   Thus, $N(\mathcal{AB}) = \epsilon N(\mathcal{A})N(\mathcal{B})$ for some $\epsilon \in \mathcal{O}^*$. Since norms are monic polynomials in X alone, $\epsilon = 1$.

3. If $\mathcal{A} = (\alpha)$ then $\overline{\mathcal{A}} = (\overline{\alpha})$. So $(N(\mathcal{A})) = (\alpha)(\overline{\alpha}) = (N(\alpha))$. So $N(\mathcal{A}) = cN(\alpha)$ for some $c \in \mathcal{O}^*$.

□

Two integral $\mathcal{O}$-ideals $\mathcal{A}$ and $\mathcal{B}$ are said to be *equivalent* if there exist nonzero $\alpha, \beta \in \mathcal{O}$ such that $(\alpha)\mathcal{A} = (\beta)\mathcal{B}$. In this situation we write $\mathcal{A} \sim \mathcal{B}$.

Let $\mathcal{A}_i = [Q_i, P_i + Y]$ for $i = 1, 2$ where $Q_i | P_i^2 + P_i B + C$. Without loss of generality assume $\text{sgn}(Q_i) = 1$ and $\deg(P_i) < \deg(Q_i)$. Also let $\mathcal{A}_1\mathcal{A}_2 = (S)\mathcal{C}$ where $\mathcal{C} = [Q, P + Y]$ and $Q | P^2 + PB + C$, $\deg(P) < \deg(Q)$ and $\text{sgn}(S) = \text{sgn}(Q) = 1$.

Then $N(\mathcal{A}_1)N(\mathcal{A}_2) = N((S))N(\mathcal{C})$. So, $Q_1Q_2 = S^2Q$ and

$$\boxed{Q = \frac{Q_1Q_2}{S^2}}.$$

Let $S' = \gcd(Q_1, Q_2, P_1 + P_2 + B)$ with $\text{sgn}(S') = 1$.

Now $SP + SY \in \mathcal{A}_1\mathcal{A}_2$ so there exist $Z, U, V, W \in k[X]$ such that

$$\begin{aligned}SP + SY &= ZQ_1Q_2 + U(Q_1P_2 + Q_1Y) + V(Q_2P_1 + Q_2Y) + \\ &\quad W(P_1P_2 + C + (P_1 + P_2 + B)Y).\end{aligned}$$

Comparing irrational parts of the above equation we get $S = UQ_1 + VQ_2 + W(P_1 + P_2 + B)$. So $S' | S$.

Also $Q_1P_2 + Q_1Y \in \mathcal{A}_1\mathcal{A}_2$. So there exist $A_1, A_2 \in k[X]$ such that $Q_1P_2 + Q_1Y = A_1SQ + A_2(SP + SY)$. Comparing irrational parts gives $Q_1 = A_2S$ so $S|Q_1$. Similarly $S|Q_2$. Also $P_1P_2 + C + (P_1 + P_2 + B)Y \in \mathcal{A}_1\mathcal{A}_2$ so we likewise get $S|P_1 + P_2 + B$.

Therefore $S|\gcd(Q_1, Q_2, P_1 + P_2 + B) = S'$ and hence

$$\boxed{S = \gcd(Q_1, Q_2, P_1 + P_2 + B)}.$$

Now, there exist $U, V, W \in k[X]$ such that $S = UQ_1 + VQ_2 + W(P_1 + P_2 + B)$. So

$$\begin{aligned} U(Q_1P_2 + Q_1Y) + V(Q_2P_1 + Q_2Y) + W(P_1P_2 + C + (P_1 + P_2 + B)Y) \\ = UQ_1P_2 + VQ_2P_1 + W(P_1P_2 + C) + SY \in \mathcal{A}_1\mathcal{A}_2. \end{aligned}$$

Thus, there exist $A_1, A_2 \in k[X]$ such that

$$A_1SQ + A_2(SP + SY) = UQ_1P_2 + VQ_2P_1 + W(P_1P_2 + C) + SY.$$

Comparing irrational parts of the above equation gives that $A_2S = S$ so $A_2 = 1$. Now comparing rational parts gives

$$A_1SQ + SP = UQ_1P_2 + VQ_2P_1 + W(P_1P_2 + C).$$

So

$$SP \equiv UQ_1P_2 + VQ_2P_1 + W(P_1P_2 + C) \pmod{SQ}.$$

Using that $VQ_2 = S + UQ_1 + WP_1 + WP_2 + WB$ and dividing through by S we finally get

$$\boxed{P \equiv P_1 + \tfrac{Q_1}{S}\left(U(P_1 + P_2) + W\left(\tfrac{P_1^2 + BP_1 + C}{Q_1}\right)\right) \pmod{Q}}.$$

Thus, given $\mathcal{A}_1 = [Q_1, P_1 + Y]$ and $\mathcal{A}_2 = [Q_2, P_2 + Y]$ we can easily compute $C = [Q, P + Y]$ and $S \in k[X]$ such that $\mathcal{A}_1\mathcal{A}_2 = (S)\mathcal{C}$.

Lemma 8 *If $\mathcal{A}$ and $\mathcal{B}$ are equivalent, integral $\mathcal{O}$-ideals, there exists some $\gamma \in \mathcal{A}$ such that $(\gamma)\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A}$ and $0 < |\gamma| \leq |N(\mathcal{A})|$.*

Proof: Since $\mathcal{A}$ and $\mathcal{B}$ are equivalent we have $(\alpha)\mathcal{A} = (\beta)\mathcal{B}$ for some nonzero $\alpha, \beta \in \mathcal{O}$. So taking norms we get $c_1\alpha\overline{\alpha}N(\mathcal{A}) = c_2\beta\overline{\beta}N(\mathcal{B})$, for some $c_1, c_2 \in \mathcal{O}^*$.

Let $\gamma' = c_1\frac{\overline{\alpha}}{\beta}N(\mathcal{A}) = c_2\frac{\beta}{\alpha}N(\mathcal{B})$. Since $N(\mathcal{B}) \in \mathcal{B}$ we know that $\gamma' \in \mathcal{A}$.

Also, $(\alpha)(\gamma')\mathcal{B} = (\beta)\,(N(\mathcal{B}))\,\mathcal{B} = (\alpha)\,(N(\mathcal{B}))\,\mathcal{A}$. So, $(\gamma')\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A}$.

Let ϵ be the fundamental unit of $\mathcal{O}^*$, so $|\epsilon| > 1$. Let $n_0 \in \mathbb{Z}_{\geq 0}$ be such that $\frac{|\gamma'|}{|\epsilon^{n_0}|} < |N(\mathcal{A})|$.

The result follows with $\gamma = \epsilon^{-n_0}\gamma'$. □

An integral $\mathcal{O}$-ideal, $\mathcal{A}$, is called *reduced* if $\mathcal{A}$ is primitive and there exists a $k[X]$-basis $\{Q, P + Y\}$ for $\mathcal{A}$ with $Q, P \in k[X]$, $Q|P^2 + C + PB$ and

$$|P + Y + B| < |Q| = |N(\mathcal{A})| < |P + Y|\,.$$

It is easy to see that this is equivalent to $\alpha = \frac{P+Y}{Q}$ being a reduced quadratic irrational.

Theorem 16 *A primitive $\mathcal{O}$-ideal $\mathcal{A}$ is reduced if and only if $|N(\mathcal{A})| < |B|$.*

Proof: ($\Rightarrow$) Let $\mathcal{A}$ be a reduced $\mathcal{O}$-ideal. Then there exist $P, Q \in k[X]$ such that $\mathcal{A} = [Q, P + Y]$ and $\alpha = \frac{P+Y}{Q}$ is a reduced quadratic irrational. We know then that $|Q| < |B|$. Since $|N(\mathcal{A})| = |Q|$ we are done.

($\Leftarrow$) Let $|N(\mathcal{A})| < |B|$ for a primitive $\mathcal{O}$-ideal $\mathcal{A} = [Q, P + Y]$ with $Q, P \in k[X]$.

Let $P' = P + \left\lfloor \frac{P+Y+B}{Q} \right\rfloor Q$. Clearly $\mathcal{A} = [Q, P' + Y]$ and

$$\left| \frac{P' + Y + B}{Q} \right| = \left| \frac{P + Y + B}{Q} + \left\lfloor \frac{P + Y + B}{Q} \right\rfloor \right| < 1.$$

So $|P' + Y + B| < |Q|$. Thus we also have, $|P' + Y| = |(P' + Y + B) + B| = |B| > |Q|$. Hence, a reduced basis for $\mathcal{A}$ is $\{Q, P' + Y\}$. □

Lemma 9 *If $\mathcal{A}$ is a reduced $\mathcal{O}$-ideal then there does not exist any nonzero $\alpha \in \mathcal{A}$ such that $|\alpha| < |N(\mathcal{A})|$ and $|\overline{\alpha}| \leq |N(\mathcal{A})|$.*

Proof: We know $\mathcal{A} = [Q, P + Y]$ where $P, Q \in k[X]$ and $|P + Y + B| < |Q| = |N(\mathcal{A})| < |P + Y|$.

Let $\alpha \in \mathcal{A}$ with $\alpha \neq 0$, then there exist $U, V \in k[X]$ such that $\alpha = UQ + V(P + Y)$ and $\overline{\alpha} = UQ + V(P + Y + B)$.

Since $\alpha \neq 0$, if $V = 0$ then $U \neq 0$ or in other words $|U| \geq 1$ and $|\alpha| = |\overline{\alpha}|$. Hence $|\alpha| = |UQ| \geq |Q| = |N(\mathcal{A})|$ and the assertion is true.

On the other hand if $V \neq 0$ then $|V| \geq 1$. If in addition $|U| \leq |V|$ then $|UQ| < |V|\,|P + Y|$ so $|\alpha| = |V|\,|P + Y| \geq |P + Y| > |N(\mathcal{A})|$. Similarly, if $|U| > |V|$ then $|UQ| > |V|\,|P + Y + B|$ so $|\overline{\alpha}| = |UQ| > |Q| = |N(\mathcal{A})|$. Thus, the assertion holds. □

5.2 Baby-Steps and Equivalent Reduced Ideals

We can now examine the way in which the continued fraction algorithm acts on the primitive reduced ideals of $\mathcal{O}$.

Let $\mathcal{A}$ be a primitive $\mathcal{O}$-ideal. Then there exist $P, Q \in k[X]$, $Q | P^2 + BP + C$ such that $\mathcal{A} = [Q, P + Y]$. If $\alpha = \frac{P+Y}{Q}$, then α is a quadratic irrational and we can apply the continued fraction algorithm to α.

Define Q_i, P_i as in the continued fraction algorithm for α. Then let $\mathcal{A}_1 := \mathcal{A}$ and $\mathcal{A}_{i+1} := [Q_i, P_i + Y]$ for $i \geq 0$. We can now talk abut performing the continued fraction algorithm on $\mathcal{A}$ in this way.

We know that $\alpha_i = \frac{P_i+Y}{Q_i}$ for $i \geq 0$ where $Q_i, P_i \in k[X]$, $Q_i \neq 0$ and $Q_i | P_i^2 + P_i B + C$. We call each step of the continued fraction algorithm on $\mathcal{A}$ a *Baby-Step*.

Obviously, $\mathcal{A}_{i+1}$ is a primitive integral $\mathcal{O}$-ideal. Now

$$\begin{aligned} \mathcal{A}_i &= [Q_{i-1}, P_{i-1} + Y] \\ &= [Q_{i-1}, P_i + B + Y] \end{aligned}$$

since $P_i = a_i Q_i + P_{i-1} + B$. Using this result we get that

$$\begin{aligned} (Q_i)\,\mathcal{A}_i &= [Q_i Q_{i-1}, Q_i P_i + Q_i B + Q_i Y] \\ &= (P_i + B + Y)\,[Q_i, \frac{Q_i Q_{i-1}}{P_i + B + Y}] \\ &= (P_i + B + Y)\,[Q_i, P_i + Y]. \end{aligned}$$

So

$$(Q_i)\,\mathcal{A}_i = (P_i + B + Y)\,\mathcal{A}_{i+1}.$$

Theorem 17 *If $\mathcal{A} = \mathcal{A}_1 = [Q_0, P_0 + Y]$ is any primitive $\mathcal{O}$-ideal then each $\mathcal{A}_i$ is a primitive $\mathcal{O}$-ideal and for $i \geq 1$,*

$$(Q_0 \theta_i)\,\mathcal{A}_i = (Q_{i-1})\,\mathcal{A}_1$$

where $Q_0 \theta_i \in \mathcal{O}$.

Proof: Since $\theta_i = p_{i-2} + \frac{P_0+Y}{Q_0} q_{i-2}$, we get that $Q_0\theta_i = Q_0 p_{i-2} + (P_0 + Y)q_{i-2} \in \mathcal{O}$.

Since $\theta_1 = 1$ we have trivially that $(Q_0\theta_1)\,\mathcal{A}_1 = (Q_0)\,\mathcal{A}_1$.

Assume that $(Q_0\theta_i)\,\mathcal{A}_i = (Q_{i-1})\,\mathcal{A}_1$ for some $i \geq 1$.

Notice that $\alpha_i = \frac{P_i+Y}{Q_i}\frac{P_i+Y+B}{P_i+Y+B} = \frac{Q_{i-1}}{P_i+Y+B}$. So

$$Q_{i-1}\theta_{i+1} = Q_{i-1}\theta_i \frac{1}{\alpha_i} = (P_i + Y + B)\theta_i.$$

We know that

$$(Q_i)\,\mathcal{A}_i = (P_i + B + Y)\,\mathcal{A}_{i+1}$$

from the statement before this theorem. Now multiplying through by $(Q_0\theta_i)$ and using the above result we get

$$(Q_i)\,(Q_0\theta_i)\,\mathcal{A}_i = (Q_{i-1})\,(Q_0\theta_{i+1})\,\mathcal{A}_{i+1}.$$

From the Induction Hypothesis we deduce that

$$(Q_i)\,(Q_{i-1})\,\mathcal{A}_1 = (Q_{i-1})\,(Q_0\theta_{i+1})\,\mathcal{A}_{i+1}.$$

After dividing through by (Q_{i-1}) we conclude by the Principle of Mathematical Induction that the result holds. □

Since $N(\mathcal{A}_i) = \frac{Q_{i-1}}{\mathrm{sgn}(Q_{i-1})}$ and $\mathcal{A} = \mathcal{A}_1$, the above result is equivalent to

$$\boxed{(N(\mathcal{A})\theta_i)\,\mathcal{A}_i = (N(\mathcal{A}_i))\,\mathcal{A}}.$$

So, $\mathcal{A}$ and $\mathcal{A}_i$ are equivalent for all $i \geq 1$.

Corollary 7 *If $\mathcal{A} = \mathcal{A}_1 = [Q_0, P_0 + Y]$ is any primitive $\mathcal{O}$-ideal then we have that for $i \geq 1$*

$$\mathcal{A}_1 = [Q_0\theta_i, Q_0\theta_{i+1}].$$

Proof: Since $Q_{i-1}\theta_{i+1} = (P_i + Y + B)\theta_i$ and $\mathcal{A}_i = [Q_{i-1}, P_i + B + Y]$ we see

$$\begin{aligned}(Q_{i-1})\,[Q_0\theta_i, Q_0\theta_{i+1}] &= [Q_0Q_{i-1}\theta_i, Q_0Q_{i-1}\theta_{i+1}] \\ &= [Q_0Q_{i-1}\theta_i, (P_i + Y + B)\theta_i Q_0] \\ &= (Q_0\theta_i)\,[Q_{i-1}, P_i + Y + B] \\ &= (Q_0\theta_i)\,\mathcal{A}_i.\end{aligned}$$

Using Theorem 17 the assertion immediately follows. □

We now examine the relationship between the reduction of α and the reduction of $\mathcal{A}$.

Remark 3 *If in the continued fraction expansion of* $\alpha = \alpha_0 = \frac{P_0+Y}{Q_0}$ *there is an* $i \geq 0$ *such that* $\alpha_i = \frac{P_i+Y}{Q_i}$ *is reduced then obviously* $\mathcal{A}_{i+1}$ *is reduced because a basis for* $\mathcal{A}_{i+1}$ *is* $\{Q_i, P_i + Y\}$ *which is reduced.*

Theorem 18 *If* $\mathcal{A} = \mathcal{A}_1 = [Q_0, P_0 + Y]$ *is any primitive* $\mathcal{O}$*-ideal then* $\mathcal{A}_{i+1}$ *is reduced for all*

$$i > \max\left\{0, \frac{1}{2}\deg(Q_0) - \frac{1}{2}\deg(B) + 1\right\}.$$

Proof: The result follows from Theorem 4 and the above remark. □

Notice however, that it may be possible for $\mathcal{A}_{i+1}$ to be reduced but the basis given by the continued fraction expansion not to be reduced. Then α_i would not be reduced. We do have the following result though.

Theorem 19 *If* $\mathcal{A} = \mathcal{A}_1 = [Q_0, P_0 + Y]$ *is any primitive* $\mathcal{O}$*-ideal and* $\mathcal{A}_{i+1}$ *is reduced for some* $i \geq 0$ *then* α_{i+1} *is reduced.*

Proof: Let $\mathcal{A}_{i+1}$ be reduced and then $|N(\mathcal{A}_{i+1})| = |Q_i| < |B|$. By Theorem 5, α_{i+1} is then reduced. □

Theorem 20 *Let α be a quadratic irrational. If in the continued fraction expansion on $\alpha = \alpha_0 = \frac{P_0+Y}{Q_0}$ there exists a minimal $l \geq 0$ such that $|Q_l| < |B|$ then $\mathcal{A}_{l+1}$ is reduced and $\left|\overline{\theta_{l+1}}\right| \leq 1$, $|\theta_{l+1}| \geq \frac{|Q_l|}{|Q_0|}$.*

Proof: We have that $|Q_l| = |N(\mathcal{A}_{l+1})| < |B|$. So $\mathcal{A}_{l+1}$ is reduced.

If $l = 0$, then $Q_l = Q_0$ and $\left|\overline{\theta_1}\right| = 1 = |\theta_1|$.

Let $l \geq 1$. If $|\overline{\alpha_j}| < 1$ for some $j \in \{1, \ldots, l-1\}$ then α_j is reduced. This would say that $|Q_j| < |B|$ which contradicts our assumption. Thus, $|\overline{\alpha_j}| \geq 1$.

We also know from Lemma 3 that α_l is not reduced, so $|\overline{\alpha_l}| \geq 1$. Hence,

$$\left|\overline{\theta_{l+1}}\right| = \prod_{j=1}^{l} \frac{1}{|\overline{\alpha_j}|} \leq 1.$$

Since $\left|\overline{\theta_{l+1}}\right| |\theta_{l+1}| = \frac{|Q_l|}{|Q_0|}$ we get also that

$$|\theta_{l+1}| \geq \frac{|Q_l|}{|Q_0|}.$$

□

Not only will the continued fraction expansion produce equivalent reduced ideals, but it will produce all equivalent reduced ideals, as shown in the following result. This result shows that the infrastructure is the inner structure of a class in the ideal class group.

Theorem 21 *Let $\mathcal{A} = \mathcal{A}_1$ and $\mathcal{B}$ be two equivalent, reduced, integral $\mathcal{O}$-ideals and $\gamma \in \mathcal{A}$ with*

$$(\gamma)\,\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A},$$

where $0 < |\gamma| \leq |N(\mathcal{A})|$. *Then there exists some* $\nu \geq 1$ *and* $c \in k^*$ *such that* $\mathcal{B} = \mathcal{A}_\nu$ *and* $\gamma = cN(\mathcal{A})\theta_\nu$.

Proof: We already know that such a γ exists by Lemma 8.

Since $\mathcal{A}_1$ is reduced, so is α_i for all $i \geq 1$ and hence $|\overline{\alpha_i}| < 1 < |\alpha_i|$. Thus $|\theta_{i+1}| < |\theta_i|$, $|\theta_1| = 1$ and $\left|\overline{\theta_{i+1}}\right| > \left|\overline{\theta_i}\right|$. Since $|\alpha_i| \geq q$ for all $i \geq 1$, we see that $|\theta_i| \leq \frac{1}{q^i}$. Thus $\{|\theta_i|\}_{i\geq 1}$ is strictly decreasing and converges to 0. Since $|\gamma| \leq |N(\mathcal{A})|$ there must exist some ν with $|\theta_{\nu+1}| < \frac{|\gamma|}{|N(\mathcal{A})|} \leq |\theta_\nu|$. Thus

$$|\theta_{\nu+1}N(\mathcal{A})| < |\gamma| \leq |N(\mathcal{A})\theta_\nu|\,.$$

Since $N(\mathcal{A}) \in \mathcal{A}$, we have $N(\mathcal{A})\theta_{\nu+1} \in \mathcal{A}$ so

$$N(\mathcal{A})\theta_{\nu+1}N(\mathcal{B}) \in (N(\mathcal{B}))\,\mathcal{A} = (\gamma)\,\mathcal{B}.$$

Thus, $N(\mathcal{A})\theta_{\nu+1}N(\mathcal{B}) = \gamma\beta$ for some $0 \neq \beta \in \mathcal{B}$.

By above we can deduce that $|\gamma|\,|N(\mathcal{B})| > |\gamma|\,|\beta|$, so $|N(\mathcal{B})| > |\beta|$. Since $\mathcal{B}$ is reduced we must then have $\left|\overline{\beta}\right| > |N(\mathcal{B})|$ by Lemma 9. But then using the definition of β we conclude

$$\left|N(\mathcal{A})\overline{\theta_{\nu+1}}\right| > |\overline{\gamma}|\,.$$

Since $\gamma \in \mathcal{A}$ we can use Corollary 7 to deduce that there exist $U, V \in k[X]$ such that

$$\begin{aligned} \gamma &= UN(\mathcal{A})\theta_\nu + VN(\mathcal{A})\theta_{\nu+1} \\ \overline{\gamma} &= UN(\mathcal{A})\overline{\theta_\nu} + VN(\mathcal{A})\overline{\theta_{\nu+1}}. \end{aligned}$$

If $|U| \leq |V|$ then $|\overline{\gamma}| = \left|VN(\mathcal{A})\overline{\theta_{\nu+1}}\right| > |V|\,|\overline{\gamma}|$. So $1 > |V|$ and thus $U = V = 0$. This is not possible since γ is nonzero.

If $|U| > |V|$, then $|\gamma| = |UN(\mathcal{A})\theta_\nu| \geq |U|\,|\gamma|$. So $1 \geq |U|$. Thus $U = c \in k^*$ and $V = 0$. Hence

$$\gamma = cN(\mathcal{A})\theta_\nu.$$

Since $(N(\mathcal{A})\theta_\nu)\,\mathcal{A}_\nu = (N(\mathcal{A}_\nu))\,\mathcal{A}$ we can take norms to get that

$$N(\mathcal{A})N(\theta_\nu) = c_1 N(\mathcal{A}_\nu)$$

for some $c_1 \in k^*$. From above we can then deduce

$$\begin{aligned} N(\gamma) &= c_2 N(\mathcal{A})^2 N(\theta_\nu) \\ &= c_3 N(\mathcal{A}) N(\mathcal{A}_\nu) \end{aligned}$$

for some $c_2, c_3 \in k^*$.

Since $(\gamma)\,\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A}$ we again take norms and get $N(\gamma) = c_4 N(\mathcal{B})N(\mathcal{A})$ for some $c_4 \in k^*$. Since $\mathrm{sgn}(N(\mathcal{B})) = \mathrm{sgn}(N(\mathcal{A}_\nu)) = 1$ we deduce that $N(\mathcal{B}) = N(\mathcal{A}_\nu)$.

Thus $(\gamma)\,\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A} = (N(\mathcal{A}_\nu))\,\mathcal{A}$. Since $(N(\mathcal{A})\theta_\nu)\,\mathcal{A}_\nu = (N(\mathcal{A}_\nu))\,\mathcal{A}$ and $\gamma = cN(\mathcal{A})\theta_\nu$ we finally get

$$(\gamma)\,\mathcal{B} = (\gamma)\,\mathcal{A}_\nu$$

from which the result follows. □

This result says that the continued fraction algorithm will produce all primitive, reduced ideals equivalent to the starting ideal. It is this set of equivalent reduced ideals that we call the *infrastructure*.

5.3 Distances and the Giant Step

Let $\mathcal{A} = \mathcal{A}_1$ and $\mathcal{B}$ be two equivalent, reduced, integral $\mathcal{O}$-ideals. By Theorem 21 there exists $\nu \geq 1$ such that $\mathcal{B} = \mathcal{A}_\nu$. We also know that $(N(\mathcal{A})\theta_\nu)\,\mathcal{A}_\nu = (N(\mathcal{A}_\nu))\,\mathcal{A}$,

so

$$(N(\mathcal{A})\theta_\nu)\,\mathcal{B} = (N(\mathcal{B}))\,\mathcal{A}.$$

Define the *distance from $\mathcal{A}$ to $\mathcal{B}$* by

$$\delta(\mathcal{B},\mathcal{A}) = \delta(\mathcal{A}_\nu,\mathcal{A}) := \deg(\overline{\theta_\nu}).$$

Also when $\mathcal{A}$ is understood by context, we write $\delta_\nu := \delta(\mathcal{A}_\nu,\mathcal{A})$.

Definition 5 *Let $k = F_{2^M}$ and $K = k(X)(Y)$ be a function field defined by the non-singular equation $Y^2 + BY = C$ for $B, C \in k[X]$, C monic and the place at infinity splitting completely. Let $\mathcal{O} = [1, Y]$ and R be the regulator. Then the* infrastructure discrete logarithm problem *is, given a primitive reduced ideal $\mathcal{A}$, to find $\delta(\mathcal{A},\mathcal{O}) < R$ if it exists; otherwise return, "No solution".*

We have defined this logarithm problem in terms of the starting point $\mathcal{O}$, of the continued fraction algorithm. It is also possible to define it in terms of any other starting point, $\mathcal{A}_1$, that is a reduced $\mathcal{O}$-ideal.

Notice that the distance function is only defined between reduced, equivalent, integral ideals. Since $\left|\overline{\theta_{i+1}}\right| > \left|\overline{\theta_i}\right|$ we know that the distance function strictly increases with i. Also since $\delta_i \in \mathbb{Z}$, we get $\delta_{t+i} \geq \delta_t + i$. Thus, if $\delta_i = \delta_j$ then $\mathcal{A}_i = \mathcal{A}_j$ and if $\delta_i = 0$ then $\mathcal{A}_i = \mathcal{A}$.

Conversely, if $\mathcal{A}_i = \mathcal{A}_j$ then

$$(N(\mathcal{A})\theta_i)\,\mathcal{A}_i = (N(\mathcal{A}_i))\,\mathcal{A} = (N(\mathcal{A}_j))\,\mathcal{A} = (N(\mathcal{A})\theta_j)\,\mathcal{A}_j.$$

Hence we get that $(N(\mathcal{A})\theta_i) = (N(\mathcal{A})\theta_j)$, and so $\theta_i = \epsilon\theta_j$ for some $\epsilon \in \mathcal{O}^*$. We know that $\epsilon = c(\overline{\theta_{m+1}})^l$ for some $c \in k^*$ and $l \in \mathbb{Z}$ so $\deg(\theta_i) = \deg(\theta_j) + lR$ where R is the regulator of $k(X)(Y)$. Thus, if $\mathcal{A}_i = \mathcal{A}_j$ then

$$\delta_i = \delta_j + lR$$

for some $l \in \mathbb{Z}$. In particular note that $\delta_{m+1} = R$.

Using the facts that $\theta_i\overline{\theta_i} = \frac{Q_{i-1}}{Q_0}$, $\theta_i = \prod_{j=1}^{i-1} \frac{1}{\alpha_j}$ and $|a_{i-1}Q_{i-1}| = |B|$ we conclude

$$\delta_i = \deg(B) - \deg(Q_0) + \sum_{j=1}^{i-2} \deg(a_j)$$

for $i \geq 2$. It is easy to see that $\delta_1 = 0$.

For the remainder of this chapter let $\mathcal{A} = \mathcal{A}_1 = (1) = \mathcal{O} = [1, Y]$. Then we have $P_0 = P = 0$, $Q_0 = Q = 1$ and $\alpha_0 = \alpha = Y$.

Since $|N(\mathcal{A})| = 1 < |B|$, we have that $\mathcal{A}$ is reduced and thus $\mathcal{A}_i$ is reduced for all $i \geq 1$ and so δ_i is defined for all $i \geq 1$. Also $(Q_0\theta_i)\,\mathcal{A}_i = (Q_{i-1})\,\mathcal{A}_1$ from which we conclude

$$\mathcal{A}_i = \left(\overline{\theta_i}\right) = [Q_{i-1}, P_{i-1} + Y].$$

So $\mathcal{A}_i$ is principal for all $i \geq 1$.

Now let $\mathcal{B}$ be any arbitrary primitive reduced $\mathcal{O}$-ideal. Let the quantities associated with the continued fraction expansion of $\mathcal{B}$ be P_i', Q_i', θ_i' and $\delta_i' := \delta(\mathcal{B}_i, \mathcal{B})$.

For any $s, t \geq 1$ we can find an $S \in k[X]$ and a primitive $\mathcal{O}$-ideal $\mathcal{C}$ such that

$$\mathcal{A}_s\mathcal{B}_t = (S)\mathcal{C}.$$

We can then apply the continued fraction expansion to $\mathcal{C}$. We denote the quantities associated with this expansion by P_i'', Q_i'' and θ_i''. Notice that there is no distance defined since the ideal $\mathcal{C}$ may or may not be reduced.

We know that there exists a minimal l such that $\left|Q_{l-1}''\right| < |B|$ or in other words, such that $\mathcal{C}_l$ is reduced. Then notice that

$$\mathcal{C}_l \sim \mathcal{C} \sim (S)\mathcal{C} = \mathcal{A}_s\mathcal{B}_t = \left(\overline{\theta_s}\right)\mathcal{B}_t \sim \mathcal{B}_t \sim \mathcal{B}.$$

Hence $\mathcal{C}_l \sim \mathcal{B}$. Since they are both reduced ideals there exists a $\nu \geq 1$ such that $\mathcal{C}_l = \mathcal{B}_\nu$.

Theorem 22 *In the above situation we have*

$$\theta'_\nu = c\theta_s\theta'_t\frac{\theta''_l}{S}$$

where $c \in k^*$. *Further*

$$\delta'_\nu = \delta'_t + \delta_s + f$$

where $f := \deg(\overline{\theta''_l}) - \deg(S) \in \mathbb{Z}$ *and* $2 - 2\deg(B) \leq f \leq 0$.

Proof: From Theorem 17 we know $(\theta_s)\mathcal{A}_s = (N(\mathcal{A}_s))$, $(N(B)\theta'_t)\mathcal{B}_t = (N(\mathcal{B}_t))\mathcal{B}$ and $(N(C)\theta''_l)\mathcal{C}_l = (N(\mathcal{C}_l))\mathcal{C}$. Since $\mathcal{A}_s\mathcal{B}_t = (S)\mathcal{C}$ we can take norms to get

$$N(\mathcal{A}_s)N(\mathcal{B}_t) = c_1S^2N(C)$$

for some $c_1 \in k^*$. Using all of the above, we can deduce that

$$(N(B)\theta_s\theta'_t\theta''_l)\mathcal{C}_l = (SN(\mathcal{C}_l))\mathcal{B}.$$

Let $\gamma = \frac{N(B)\theta_s\theta'_t\theta''_l}{S} \in \mathcal{B}$ and so $(\gamma)\mathcal{C}_l = (N(\mathcal{C}_l))\mathcal{B}$.

Since $|\theta_s|, |\theta'_t|, |\theta''_l| \leq 1$, we get that $0 < |\gamma| \leq |N(B)|$. Thus, by Theorem 21, there must exist some $\nu \geq 1$ and $c_2 \in k^*$ such that $\gamma = c_2N(B)\theta'_\nu$ and $\mathcal{C}_l = \mathcal{B}_\nu$. Therefore,

$$\theta'_\nu = c_3\theta_s\theta'_t\frac{\theta''_l}{S}$$

for some $c_3 \in k^*$, from which we get

$$\delta'_\nu = \delta_s + \delta'_t + f$$

with $f = \deg(\overline{\theta''_l}) - \deg(S)$.

Notice that

$$\begin{aligned}\frac{\left|\overline{\theta_l''}\right|}{|S|} &\geq \frac{\left|\overline{\theta_l''}\theta_l''\right|}{|S|} \\ &= \frac{|N(C_l)|}{|S|\,|N(C)|} \\ &\geq \frac{|S|}{|N(\mathcal{A}_s)|\,|N(\mathcal{B}_t)|} \\ &\geq \frac{1}{|N(\mathcal{A}_s)|\,|N(\mathcal{B}_t)|}.\end{aligned}$$

Since $\mathcal{A}_s$ and $\mathcal{B}_t$ are both reduced, $|N(\mathcal{A}_s)|, |N(\mathcal{B}_t)| < |B|$ and so $f \geq -2(\deg(B) - 1)$.

Theorem 20 says that $\left|\overline{\theta_l''}\right| \leq 1$, so $\deg(\overline{\theta_l''}) \leq 0$, which gives $f \leq 0$. □

Using the above notation, we define a *Giant-Step* by the operation

$$\mathcal{A}_s * \mathcal{B}_t := (\mathcal{B}_\nu, f) = (C_l, f).$$

So a Giant Step consists of taking the product of two primitive ideals and then reducing the primitive part of the product using the continued fraction algorithm.

Let m be the quasi-period of the continued fraction expansion of $\alpha = Y$. Since $Q_{\lambda m} = c \in k^*$, we get that

$$\mathcal{A}_{\lambda m+1} = [c, P_{\lambda m} + Y] = [1, Y] = \mathcal{A}_1 = \mathcal{O}.$$

So $\delta_{\lambda m+1} = \delta_1 + lR$ where R is the regulator and $l \in \mathbb{Z}_{\geq 1}$. In fact,

$$\begin{aligned}\delta_{\lambda m+1} &= \deg(\overline{\theta_{\lambda m+1}}) \\ &= \deg(\overline{\theta_{m+1}}^{\lambda}) \\ &= \lambda R.\end{aligned}$$

Since $P_i = P_{i+\lambda m}$ and $Q_i = c_i^{1+(-1)^m+\cdots+(-1)^{(\lambda-1)m}} Q_{i+\lambda m}$ for all $\lambda \geq 1$ and all $i \geq 1$ we know that

$$\mathcal{A}_{\lambda m+i+1} = \mathcal{A}_{i+1}.$$

So, $\delta_{\lambda m+i+1} = \delta_{i+1} + lR$ for all $\lambda \geq 1$, $i \geq 1$ and for some $l \in \mathbb{Z}_{\geq 1}$. Since $\deg(\alpha_{i+\lambda m}) = \deg(\alpha_i)$ for all $i \geq 0$ and $\lambda \geq 0$, and since $\alpha_m = \frac{d+B+Y}{c}$, we also get that

$$\delta_{\lambda m+i+1} = \delta_{i+1} + \lambda R$$

for all $i \geq 1$ and $\lambda \geq 1$ by examining the formula for $\delta_{\lambda m+i+1}$.

We have also that $\delta_i = \deg(B) + \sum_{j=1}^{i-2} \deg(a_i)$, so $\delta_i \geq \deg(B) + i - 2$.

5.4 Algorithms

This section gives three algorithms to compute the regulator of K. They are based on similar algorithms which originally appeared in [47, 49] in the context of odd characteristic function fields.

The first algorithm is the naive method of computing the regulator. We simply start with the ideal $\mathcal{A} = [1, Y]$ and produce the continued fraction expansion until $Q_m \in k^*$. Then $R = \delta_{m+1}$. We call this the Baby-Step algorithm.

The second algorithm is a basic Giant-Step Baby-Step type of algorithm. It uses Baby-Steps to produce a table of equivalent reduced ideals. Then the Giant-Step algorithm is performed, which "jumps over" the sequence of equivalent reduced ideals quickly, until we obtain an ideal that is in the table. The regulator is then the difference in distances.

Original Regulator (Giant-Step Baby-Step) Algorithm

input: $q = 2^M, B, C$

output: R

1. Put $c_0 := \frac{3}{2}$ and $s := \left\lfloor c_0 q^{\frac{1}{2}\deg(B)} \right\rfloor$.

2. By developing the continued fraction expansion for $\alpha = Y$, compute $\mathcal{A}_i$ and δ_i for $i = 1, \ldots, s$ starting with $\mathcal{A}_1 = (1) = \mathcal{O}$. Store them in the form

$$(\mathcal{A}_i, \delta_i) = (N(\mathcal{A}_i), P_{i-1}, \delta_i)\,.$$

   If $Q_j \in k^*$ for a minimal $1 \leq j \leq s-1$ then $R = \delta_{j+1}$; **return**(R).

3. $\mathcal{B}_1 := \mathcal{A}_s$; $f_1 := 0$; $\delta'_1 := \delta_s$; $j := 0$.

4. **do** {

$$\begin{aligned} j &:= j+1; \\ (\mathcal{B}_{j+1}, f_{j+1}) &:= \mathcal{A}_s * \mathcal{B}_j; \\ \delta'_{j+1} &:= \delta_s + \delta'_j + f_{j+1}; \end{aligned}$$

   } **while** $(\mathcal{B}_{j+1} \notin \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s\})$.

5. We have $\mathcal{B}_{j+1} = \mathcal{A}_i \in \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s\}$ and then

$$R := \delta'_{j+1} - \delta_i;$$

   return(R).

Proof: If the algorithm terminates in step 2, then $Q_j \in k^*$ and by Theorem 8, $j = m$, so the output is R.

Otherwise, we must show that the algorithm will terminate in Step 5 with the correct output. Now, $s = \left\lfloor \frac{3}{2} q^{\frac{1}{2}\deg(B)} \right\rfloor$, so $s > \deg(B)$ and $\delta_s > 2\deg(B) - 2$. Thus $\delta'_{j+1} = \delta_s + \delta'_j + f_{j+1} > 2\deg(B) - 2 + \delta'_j - 2\deg(B) + 2 = \delta'_j$ for all $j \geq 0$.

So $\delta'_j \in \mathbb{Z}_{\geq 0}$ increases with j. Thus, there must exist a least ν with the property that $\delta'_\nu < R \leq \delta'_{\nu+1}$. Now, $\delta'_{\nu+1} - \delta'_\nu = \delta_s + f_{\nu+1} \leq \delta_s$. So, $\delta'_{\nu+1} = \delta_{m+1} + l$ for some $l \leq \delta_s$.

Now, $\delta'_{\nu+1} = \delta_{\lambda_{\nu+1}}$ for some $\lambda_{\nu+1}$ and $\delta_{m+1} \leq \delta_{\lambda_{\nu+1}} \leq \delta_{m+1} + \delta_s$. Thus, $\delta_{\lambda_{\nu+1}} = \delta_{m+i}$ for some $i \geq 1$.

But then

$$\begin{aligned} \delta_{m+i} &= \delta_{m+(i-1)+1} \\ &= \delta_{(i-1)+1} + R \\ &= \delta_i + R. \end{aligned}$$

So, $l = \delta_i \leq \delta_s$.

Now consider $\mathcal{A}_i$ and $\mathcal{B}_{\nu+1} = \mathcal{A}_{m+i}$. By Proposition 2, $\mathcal{A}_i$=$\mathcal{A}_{m+i}$ so the algorithm will terminate and $R = \delta'_{\nu+1} - \delta_i$. □

We examine the conjugate of an ideal as follows. If $\mathcal{A}_i = [Q_{i-1}, P_{i-1} + Y]$ then the conjugate is

$$\begin{aligned} \overline{\mathcal{A}_i} &= [Q_{i-1}, P_{i-1} + B + Y] \\ &= [Q_{i-1}, P_i + a_{i-1}Q_{i-1} + Y] \\ &= [Q_{i-1}, P_i + Y]. \end{aligned}$$

Proposition 3 *Let m be the quasi-period of the continued fraction expansion of $\alpha = Y$.*

1. $\overline{\mathcal{A}_i} = \mathcal{A}_{m-i+2}$ *for* $i = 1, 2, \ldots, m+1$.

2. *If we set* $\tilde{\delta}_i := \delta(\overline{\mathcal{A}_i}, \mathcal{A}) = \delta_{m-i+2}$ *we get for* $i = 1, 2, \ldots, m+1$;

$$R = \tilde{\delta}_i + \delta_i - \deg(Q_{i-1}).$$

Proof:

1. By Theorem 10 we know that $P_{i+1} = P_{m-i}$ for $i = 0, \ldots, m-1$ and that $Q_i = c^{(-1)^{i-1}} Q_{m-i}$ for $i = 0, \ldots, m$ and some $c \in k^*$. So

$$\begin{aligned} \overline{\mathcal{A}_i} &= [Q_{i-1}, P_i + Y] \\ &= [c^{(-1)^{i-2}} Q_{m-(i-1)}, P_{m-(i-1)} + Y] \\ &= \mathcal{A}_{m-i+2} \end{aligned}$$

for $i = 1, \ldots, m$. Also

$$\begin{aligned} \overline{\mathcal{A}_{m+1}} &= [Q_m, P_{m+1} + Y] \\ &= [c^{(-1)^{m-1}}, P_{m+1} + Y] \\ &= \mathcal{A}_1. \end{aligned}$$

2. Notice that

$$\begin{aligned} \theta_{m+1} &= \prod_{j=1}^{i-1} \frac{1}{\alpha_j} \prod_{j=i}^{m} \frac{1}{\alpha_j} \\ &= \theta_i C \prod_{j=i}^{m} \overline{\alpha_{m-j+1}} \\ &= \theta_i C \prod_{j=1}^{m-i+1} \overline{\alpha_j} \\ &= \theta_i C \left(\overline{\theta_{m-i+2}}\right)^{-1} \end{aligned}$$

by Theorem 10 for some $C \in k^*$. Which after conjugation gives that

$$\begin{aligned} \overline{\theta_{m+1}} &= \overline{\theta_i} C \left(\theta_{m-i+2}\right)^{-1} \\ &= \overline{\theta_i} C \frac{\overline{\theta_{m-i+2}}}{Q_{m-i+1}} \end{aligned}$$

from which the result immediately follows.

□

The third algorithm utilizes symmetry and conjugate ideals to effectively double the size of the stored table. This is the most efficient algorithm presented.

Optimized Regulator (Giant-Step Baby-Step) Algorithm

input: $q = 2^M, B, C$

output: R

1. Put $s := \left\lfloor \frac{3}{2} q^{\frac{1}{2}\deg(B)} \right\rfloor$ and $T := \left\lfloor \frac{1}{2}\deg(B) + 1 \right\rfloor$.
2. By developing the continued fraction expansion for $\alpha = Y$, compute $\mathcal{A}_i$ and δ_i for $i = 1, \ldots, s+T$ starting with $\mathcal{A}_1 = (1) = \mathcal{O}$. Store them in the form
$$(\mathcal{A}_i, \delta_i) = (N(\mathcal{A}_i), P_{i-1}, \delta_i)\,.$$
If $P_\nu = P_{\nu+1}$ for a minimal $1 \leq \nu < s+T$ then $R = 2\delta_{\nu+1} - \deg(Q_\nu)$; **return**$(R)$.
If $\frac{Q_\mu}{\mathrm{sgn}(Q_\mu)} = \frac{Q_{\mu+1}}{\mathrm{sgn}(Q_{\mu+1})}$ for a minimal $1 \leq \mu < s+T$ then $R = 2\delta_{\mu+1} - \deg(Q_\mu) + \deg(a_{\mu+1})$; **return**$(R)$.
3. $(\mathcal{B}_1, f_1) := \mathcal{A}_s * \mathcal{A}_s$; $\delta_1' := 2\delta_s + f_1$; $j := 1$.
4. **while** $\left(\mathcal{B}_j \notin \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{s+T}\} \cup \left\{\overline{\mathcal{A}_1}, \overline{\mathcal{A}_2}, \ldots, \overline{\mathcal{A}_{s+T}}\right\}\right)$ {
$$\begin{aligned} (\mathcal{B}_{j+1}, f_{j+1}) &:= \mathcal{B}_1 * \mathcal{B}_j \\ \delta_{j+1}' &:= \delta_1' + \delta_j' + f_{j+1} \\ j &:= j+1. \end{aligned}$$
}
5. We have $\mathcal{B}_j = \mathcal{A}_i \in \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{s+T}\} \cup \left\{\overline{\mathcal{A}_1}, \overline{\mathcal{A}_2}, \ldots, \overline{\mathcal{A}_{s+T}}\right\}$.

If $\mathcal{B}_j = \mathcal{A}_i \in \{\mathcal{A}_1, \ldots, \mathcal{A}_{s+T}\}$ then $R := \delta'_j - \delta_i$; **return**$(R)$.

If $\mathcal{B}_j = \overline{\mathcal{A}_l} \in \left\{\overline{\mathcal{A}_1}, \ldots, \overline{\mathcal{A}_{s+T}}\right\}$ then $R := \delta'_j + \delta_l - \deg(Q_{l-1})$; **return**$(R)$.

Proof: If the algorithm terminates in Step 2, then by Corollary 4, the output is the regulator. Otherwise we must show that the algorithm will terminate with the correct answer in Step 5.

For all $j \geq 1$, we know that $\mathcal{B}_j = \mathcal{A}_{\lambda_j}$ for some $\lambda_j \geq 1$. Also $\delta'_{j+1} - \delta'_j = \delta'_1 + f_{j+1} = 2\delta_s + f_1 + f_{j+1} \geq 2\delta_s - 4\deg(B) + 4$. Since $s = \left\lfloor \frac{3}{2} q^{\frac{1}{2}\deg(B)} \right\rfloor$, then $s > \deg(B)$ and $\delta_s > 2\deg(B) - 2$. So $\delta'_{j+1} > \delta'_j$.

Now let $\nu \in \mathbb{Z}$ be minimal such that

$$\delta'_\nu \leq \tilde{\delta}_{s+T} = \delta_{m-s-T+2} < \delta'_{\nu+1},$$

then

$$\delta_{\lambda_{\nu+1}} = \delta'_{\nu+1} = \delta_{m-s-T+2} + l$$

for some $l \leq 2\delta_s$.

If $\delta'_{\nu+1} \leq R$ then $\delta'_{\nu+1} = \tilde{\delta}_i = \delta_{m-i+2}$ for some $i < s+T$. Now $\mathcal{B}_{\nu+1} = \mathcal{A}_{m-i+2} = \overline{\mathcal{A}_i}$. So

$$\begin{aligned} R &= \tilde{\delta}_i + \delta_i - \deg(Q_{i-1}) \\ &= \delta'_{\nu+1} + \delta_i - \deg(Q_{i-1}). \end{aligned}$$

Otherwise $\delta'_{\nu+1} > R$. Since

$$\begin{aligned} \delta_{m+s+T} - \tilde{\delta}_{s+T} &= R + \delta_{s+T} - R + \delta_{s+T} - \deg(Q_{s+T-1}) \\ &= 2\delta_{s+T} - \deg(Q_{s+T-1}) \\ &\geq 2\delta_s + 2T - \deg(Q_{s+T-1}) \\ &\geq 2\delta_s + \deg(B) - \deg(Q_{s+T-1}) \\ &> 2\delta_s \end{aligned}$$

we know that $\delta'_{\nu+1} < \delta_{m+s+T}$ and we are in the situation of the proof of the Original Regulator algorithm. □

5.5 Some Examples

We will now present some examples of quadratic function fields of even characteristic and explore their infrastructures.

5.5.1 Example 1

Let $k = F_{2^3} = F_2(\delta)$ where δ satisfies $\delta^3 + \delta + 1 = 0$. Then let $K_1 = k(X)(Y)$ be defined by the equation

$$Y^2 + (X^2 + X + \delta)Y = X^3 + \delta.$$

Notice that this equation has no singular points and that letting $Y = \sum_{i=-\infty}^{2} c_i X^i$ and equating coefficients gives

$$Y = X + \frac{\delta}{X} + \frac{\delta^2}{X^3} + \cdots$$

so we are in the situation as described in Section 4.1.

We will examine in detail the infrastructure for this field starting with the ideal $\mathcal{A}_1 = [1, Y]$. We have that $d = \lfloor Y \rfloor = X$ and that $Q_0 = 1$, $P_0 = 0$ and $\alpha_0 = Y$. The polynomials B and C are $B = X^2 + X + \delta$ and $C = X^3 + \delta$.

We will first compute

$$\begin{aligned} a_0 &= (P_0 + d) \text{ div } Q_0 \\ &= (0 + X) \text{ div } 1 \\ &= X \end{aligned}$$

and

$$\begin{aligned} r_0 &= (P_0 + d) \bmod Q_0 \\ &= (0 + X) \bmod 1 \\ &= 0. \end{aligned}$$

Which allows us to compute

$$\begin{aligned} P_1 &= d + r_0 + B \\ &= X + 0 + X^2 + X + \delta \\ &= X^2 + \delta. \end{aligned}$$

Since we do not have a value for r_{-1} we must use the following formula for Q_1:

$$\begin{aligned} Q_1 &= \frac{P_1^2 + P_1 B + C}{Q_0} \\ &= \frac{X^4 + \delta^2 + X^4 + \delta^2 + X^3 + \delta X + X^3 + \delta}{1} \\ &= \delta X + \delta. \end{aligned}$$

Thus, $\alpha_1 = \frac{P_1 + Y}{Q_1} = \frac{X^2 + \delta + Y}{\delta X + \delta}$. Also,

$$\begin{aligned} \theta_2 &= \frac{1}{\alpha_1} \\ &= \frac{P_1 + Y + B}{Q_0} \\ &= \frac{X^2 + \delta + Y + X^2 + X + \delta}{1} \\ &= X + Y \end{aligned}$$

so

$$\begin{aligned} \mathcal{A}_2 &= [Q_1, P_1 + Y] \\ &= [\delta X + \delta, X^2 + \delta + Y] \end{aligned}$$

$$\begin{aligned} &= [X+1, \delta^3 + Y] \\ &= \left(\overline{\theta_2}\right) \\ &= \left(X^2 + \delta + Y\right). \end{aligned}$$

The distance to this ideal is $\delta_2 = \deg(B) - \deg(Q_0) = 2$.

We can now continue with the next Baby-Step to get

$$\begin{aligned} a_1 &= (P_1 + d) \text{ div } Q_1 \\ &= (X^2 + \delta + X) \text{ div } \delta X + \delta \\ &= \delta^6 X \end{aligned}$$

and

$$\begin{aligned} r_1 &= (P_1 + d) \bmod Q_1 \\ &= (X^2 + \delta + X) \bmod \delta X + \delta \\ &= \delta. \end{aligned}$$

From which we can compute

$$\begin{aligned} P_2 &= d + r_1 + B \\ &= X + \delta + X^2 + X + \delta \\ &= X^2 \end{aligned}$$

and

$$\begin{aligned} Q_2 &= Q_0 + a_1(r_1 + r_0) \\ &= 1 + \delta^6 X(\delta + 0) \\ &= X + 1. \end{aligned}$$

So $\alpha_2 = \frac{X^2+Y}{X+1}$ and

$$\begin{aligned}\theta_3 &= \theta_2 \frac{1}{\alpha_2} \\ &= (X+Y)\frac{X^2+Y+X^2+X+\delta}{\delta X+\delta} \\ &= (X+Y)\frac{X+\delta+Y}{\delta X+\delta} \\ &= \delta^6 X^2 + 1 + \delta^6 XY.\end{aligned}$$

Thus we get the ideal

$$\begin{aligned}\mathcal{A}_3 &= [Q_2, P_2+Y] \\ &= [X+1, X^2+Y] \\ &= [X+1, 1+Y] \\ &= \left(\overline{\theta_3}\right) \\ &= \left(\delta^6 X^3 + X + 1 + \delta^6 XY\right)\end{aligned}$$

which has distance $\delta_3 = \delta_2 + \deg(a_1) = 3$.

Continuing in this way we get

$$\begin{aligned}a_2 &= (P_2+d) \text{ div } Q_2 \\ &= (X^2+X) \text{ div } X+1 \\ &= X\end{aligned}$$

and

$$\begin{aligned}r_2 &= (P_2+d) \bmod Q_2 \\ &= (X^2+X) \bmod X+1 \\ &= 0.\end{aligned}$$

So

$$\begin{aligned} P_3 &= d + r_2 + B \\ &= X + 0 + X^2 + X + \delta \\ &= X^2 + \delta \end{aligned}$$

and

$$\begin{aligned} Q_3 &= Q_1 + a_2(r_2 + r_1) \\ &= \delta X + \delta + X(0 + \delta) \\ &= \delta. \end{aligned}$$

Then $\alpha_3 = \frac{X^2+\delta+Y}{\delta}$ and

$$\begin{aligned} \theta_4 &= \theta_3 \frac{1}{\alpha_3} \\ &= (\delta^6 X^2 + 1 + \delta^6 XY)\frac{X+Y}{X+1} \\ &= \delta^6 X^3 + (\delta^6 X^2 + 1)Y. \end{aligned}$$

This gives the ideal

$$\begin{aligned} \mathcal{A}_4 &= [Q_3, P_3 + Y] \\ &= [\delta, X^2 + \delta + Y] \\ &= [1, Y] \\ &= \left(\overline{\theta_4}\right) \\ &= \left(\delta^6 X^4 + X + \delta + (\delta^6 X^2 + 1)Y\right) \end{aligned}$$

with distance $\delta_4 = \delta_3 + \deg(a_2) = 4$. Notice that since $Q_3 \in k$ the regulator is $R = \delta_4 = 4$. Also, consistent with Theorem 11 we have $Q_1 = \delta Q_2$.

5.5.2 Example 2

Let $k = F_{2^2} = F_2(\gamma)$ where $\gamma^2 + \gamma + 1 = 0$ and $\gamma' = \gamma + 1$. Let $K_2 = k(X)(Y)$ where

$$Y^2 + (X^4 + X^2 + X + \gamma)Y = X^6 + \gamma.$$

Notice that this equation has no singular points and that $Y \in k((\frac{1}{X}))$ so again we are in the situation of Section 4.1.

We will examine the infrastructure for K_2 starting with the ideal $\mathcal{A}_1 = [1, Y]$. Table 5.1 shows the results of the continued fraction expansion on $\mathcal{A}_1$ giving P_i, Q_i, $\deg(a_i)$ and δ_{i+1} for all $i \geq 0$ until we can determine the regulator. For this field we have $d = \lfloor Y \rfloor = X^2$.

Notice that $P_{10} = P_{11}$, so by Theorem 11, both the quasi-period and period of this expansion are 20. Now, by Theorem 12, we have $R = 2\delta_{11} - \deg(Q_{10}) = 30 - 1 = 29$.

Of interest in this example is that when $i = 6, 9$, and 10 we get $\deg(a_i) > 1$ and so $\delta_{i+2} - \delta_{i+1} > 1$. This shows how the distance function can increase in steps greater than 1, and so, for example, there will be no ideal with distance 10.

i	P_i	Q_i	$\deg(a_i)$	δ_{i+1}
0	0	1	2	0
1	$X^4+X+\gamma$	$X^3+\gamma X^2+\gamma$	1	4
2	$X^4+\gamma X^2+\gamma X+\gamma'$	$\gamma X^3+\gamma'$	1	5
3	$X^4+\gamma' X^2+X+1$	$\gamma X^3+X+\gamma$	1	6
4	$X^4+X^2+X+\gamma'$	$\gamma' X^3+X+\gamma'$	1	7
5	$X^4+\gamma X^2+X+1$	$\gamma' X^3+\gamma X+\gamma$	1	8
6	$X^4+\gamma' X+\gamma'$	$\gamma' X^2+\gamma X+\gamma'$	2	9
7	$X^4+\gamma'$	$\gamma X^3+\gamma' X^2+\gamma$	1	11
8	$X^4+\gamma X^2+\gamma'$	$X^3+X^2+\gamma X+\gamma'$	1	12
9	$X^4+\gamma$	$X^2+X+\gamma'$	2	13
10	$X^4+X+\gamma$	$X+\gamma'$	3	15
11	$X^4+X+\gamma$	$X^2+X+\gamma'$	2	18

Table 5.1: The continued fraction algorithm for K_2.

Chapter 6

A Cryptosystem in the Infrastructure

This chapter will introduce key exchange and signature schemes that can be implemented in the infrastructure discussed in the previous chapter. We will first introduce the algorithms needed in the description of these schemes, then we will discuss the schemes and their security.

We are still in the same situation as the previous two chapters. So k is a field with $q = 2^M$ elements and X is transcendental over k. Now $K = k(X)(Y)$ where $Y^2 + BY = C$ for some $B, C \in k[X]$ with C monic. Also $Y^2 + BY + C = 0$ has no singular points $(X, Y) = (u, v) \in \overline{k} \times \overline{k}$ and $K \subseteq k((\frac{1}{X}))$. Let $d = \lfloor Y \rfloor$.

6.1 Algorithms

In this section we will give detailed descriptions of all the algorithms necessary to implement the key exchange and signature schemes to be described in Section 6.2.

Let $\mathfrak{R} = \{\mathcal{A}_1 = \mathcal{O}, \mathcal{A}_2, \ldots, \mathcal{A}_m\}$ be the sequence of reduced ideals produced by the continued fraction expansion of $\alpha = Y$. A *Baby-Step* consists of performing one step of the continued fraction algorithm on a primitive $\mathcal{O}$-ideal. The following algorithm will apply a Baby-Step to an ideal in $\mathfrak{R}$ and compute the distance of the resulting ideal.

BABYSTEP

Precomputed: $\mathcal{A}_{i-1} = [Q_{i-2}, P_{i-2} + Y], \mathcal{A}_i = [Q_{i-1}, P_{i-1} + Y] \in \mathfrak{R}$, $r_{i-2} = (P_{i-2} + d) \bmod Q_{i-2}$, $\delta_i = \delta(\mathcal{A}_i, \mathcal{A}_1)$.

Input: $(Q_{i-2}, Q_{i-1}, P_{i-1}, r_{i-2}, \delta_i)$

Output: $(Q_{i-1}, Q_i, P_i, r_{i-1}, \delta_{i+1})$

1. Set

$$\begin{aligned} a_{i-1} &:= (P_{i-1} + d) \text{ div } Q_{i-1} \\ r_{i-1} &:= (P_{i-1} + d) \bmod Q_{i-1} \\ P_i &:= d + r_{i-1} + B \\ Q_i &:= Q_{i-2} + a_{i-1}(r_{i-1} + r_{i-2}) \\ \delta_{i+1} &:= \delta_i + \deg(a_{i-1}) \end{aligned}$$

so $\mathcal{A}_{i+1} = [Q_i, P_i + Y]$ and $\delta_{i+1} = \delta(\mathcal{A}_{i+1}, \mathcal{A}_1)$.

Each application of **BABYSTEP** requires a fixed number of polynomial operations. Each of these polynomials has degree bounded by $\max\left\{\deg(B), \frac{1}{2}\deg(C)\right\}$.

Given two primitive ideals $\mathcal{A}$ and $\mathcal{B}$, we can multiply them together to obtain $\mathcal{AB} = (S)\mathcal{C}$ where $S \in k[X]$ and $\mathcal{C}$ is a primitive ideal. The following algorithm will perform this operation.

MULT

Input: $\mathcal{A} = [Q_a, P_a + Y], \mathcal{B} = [Q_b, P_b + Y] \in \mathfrak{R}$.

Output: $\mathcal{C} = [Q_c, P_c + Y]$ and $S \in k[X]$ such that $(S)\mathcal{C} = \mathcal{AB}$.

1. Solve $S_1 := \gcd(Q_a, Q_b) \equiv U_1 Q_a \pmod{Q_b}$ for $S_1, U_1 \in k[X]$.
2. Solve $S := \gcd(S_1, P_a + P_b + B) = U_2 S_1 + W(P_a + P_b + B)$ for $S, U_2, W \in k[X]$.
3. Set $Q_c := \frac{Q_a Q_b}{S^2}$.
4. Set $P_c :\equiv P_a + \frac{Q_a}{S}\left(U_1 U_2 (P_a + P_b) + W\left(\frac{P_a^2 + BP_a + C}{Q_a}\right)\right) \pmod{Q_c}$.

Theorem 23 *The output $\mathcal{C}$ and S computed by* **MULT** *satisfies $(S)\mathcal{C} = \mathcal{AB}$. Furthermore, $\deg(S) < \deg(B)$ and $\deg(P_c) < \deg(Q_c) < 2\deg(B)$. Also,* **MULT** *performs $O(\deg(B))$ polynomial arithmetic operations.*

Proof: The first claim was proved in Section 5.1. Since S divides both Q_a and Q_b and also $\mathcal{A}$ and $\mathcal{B}$ are both reduced we know that $\deg(S) \leq \deg(Q_a), \deg(Q_b) < \deg(B)$. Also, $\deg(P_c) < \deg(Q_c) \leq \deg(Q_a) + \deg(Q_b) < 2\deg(B)$. The algorithm performs a fixed number of polynomial operations and 2 Extended Euclidean Algorithms. The number of polynomial operations the Extended Euclidean Algorithm performs is linear in the degree of the polynomials. Here the degree of the polynomials is $O(\deg(B))$. This is because $|P_a + Y| = |P_b + Y| = |B|$, so we have $|P_a + P_b + B| \leq |B|$. Thus, the final claim has been shown. □

Let $\mathcal{A}, \mathcal{B} \in \mathfrak{R}$. Then using the above algorithm we can produce an $S \in k[X]$ and ideal $\mathcal{C}$ such that $\mathcal{AB} = (S)\mathcal{C}$. The ideal $\mathcal{C}$ may or may not be reduced. From Theorem 18 we know that by applying the continued fraction algorithm to $\mathcal{C}$ we can

produce a reduced ideal $\mathcal{R}$ in a relatively small number of steps. In Chapter 5 we introduced the notation $\mathcal{R} = \mathcal{A} * \mathcal{B}$ for this operation which we called a Giant-Step. Theorem 22 says that $\mathcal{R} \in \mathfrak{R}$ and that $\delta(\mathcal{R}, \mathcal{O}) = \delta(\mathcal{A}, \mathcal{O}) + \delta(\mathcal{B}, \mathcal{O}) + \epsilon$ where $2 - 2\deg(B) \leq \epsilon \leq 0$. The next algorithm performs a Giant-Step.

GIANTSTEP

Input: $\mathcal{A} = [Q_a, P_a + Y], \mathcal{B} = [Q_b, P_b + Y] \in \mathfrak{R}$.

Output: $\mathcal{R} = [Q, P + Y] = \mathcal{A} * \mathcal{B}$, and $\epsilon \in \mathbb{Z}_{\leq 0}$ such that $\epsilon = \delta(\mathcal{R}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$.

1. $(C, S) :=$ **MULT** $(\mathcal{A}, \mathcal{B})$, so $(S)C = \mathcal{A}\mathcal{B}$, $C = [P_c, Q_c + Y]$, $S \in k[X]$.
2. If $\deg(Q_c) < \deg(B)$, then set $\mathcal{R} := C$, $\epsilon := -\deg(S)$ and **return**.
3. Set

$$\begin{aligned} j &:= 1 \\ Q'_{j-1} &:= Q_c \\ P'_{j-1} &:= P_c \\ r'_{j-1} &:= \left(P'_{j-1} + d\right) \bmod Q'_{j-1} \\ P'_j &:= d + r'_{j-1} + B \\ Q'_j &:= \frac{P'^2_j + P'_j B + C}{Q'_{j-1}} \\ d_j &:= -\deg(Q'_{j-1}) \end{aligned}$$

4. **while** $\left(\deg(Q'_j) \geq \deg(B)\right)$ **do** {

$$\begin{aligned} j &:= j + 1 \\ a'_{j-1} &:= \left(P'_{j-1} + d\right) \text{ div } Q'_{j-1} \\ r'_{j-1} &:= \left(P'_{j-1} + d\right) \bmod Q'_{j-1} \end{aligned}$$

$$\begin{aligned} P'_j &:= d + r'_{j-1} + B \\ Q'_j &:= Q'_{j-1} + a'_{j-1}\left(r'_{j-1} + r'_{j-2}\right) \\ d_j &:= d_{j-1} + \deg(a'_{j-1}) \end{aligned}$$

}

5. Set $Q := Q'_j$, $P := P'_j$, $\mathcal{R} := [Q, P+Y]$ and $\epsilon := d_j + \deg(a'_j) - \deg(S) + \deg(Q'_j)$.

Theorem 24 *The ideal $\mathcal{R}$ computed in* **GIANTSTEP** *is reduced. Furthermore, $2-2\deg(B) \leq \epsilon \leq 0$ and $|d_j| < 2\deg(B)$ throughout steps 3 and 4. All polynomials computed in steps 3 and 4 have degree bounded by $\max\left\{2\deg(B), \frac{1}{2}\deg(C)\right\}$ and the number of polynomial operations performed is $O(\deg(B))$.*

Proof: Let $j \geq 1$ be the first index such that $\left|Q'_j\right| < |B|$, then the loop in Step 4 exits and $\mathcal{R}$ is reduced. At this point $d_j = -\deg(Q'_0) + \sum_{i=1}^{j-1} \deg(a'_i)$ so

$$\begin{aligned} \epsilon &= d_j + \deg(a'_j) - \deg(S) + \deg(Q'_j) \\ &= \deg(Q'_j) - \deg(Q'_0) + \sum_{i=1}^{j} \deg(a'_i) - \deg(S). \end{aligned}$$

Notice that $\deg(a'_j)$ can be calculated as $\deg(P+d) - \deg(Q)$. Since $\theta'_{j+1}\overline{\theta'_{j+1}} = \frac{Q'_j}{Q'_0}$ and $\theta'_{j+1} = \prod_{i=1}^{j} \frac{1}{a'_i}$, we get that

$$\epsilon = \deg(\overline{\theta'_{j+1}}) + \deg(S).$$

By Theorem 22 we obtain that $\epsilon = \delta(\mathcal{R}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$ and $2 - 2\deg(B) \leq \epsilon \leq 0$.

On the other hand, if the algorithm exits in Step 2, then $|Q_c| < |B|$ so $\mathcal{R}$ is reduced and $\epsilon = -\deg(S) = \deg(\overline{\theta'_1}) - \deg(S)$, so again by Theorem 22 $\epsilon = \delta(\mathcal{R}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$. By the proof of the **MULT** algorithm we know $\deg(S) < \deg(B)$ so $2 - 2\deg(B) \leq -\deg(S) \leq 0$.

It is easy to see also by the proof of **MULT** that for all $i \in \{2, 3, \ldots, j\}$

$$-2\deg(B) < -\deg(Q_0') = d_1 \leq d_i.$$

Also, since $j \geq 1$ we know $\left|a_j'\right| > 1$ and then

$$d_i < d_j + \deg(a_j') = \epsilon + \deg(S) - \deg(Q_j') \leq \deg(S) < \deg(B).$$

So, $|d_i| < 2\deg(B)$.

We also have that $\deg(P_0') < \deg(Q_0') < 2\deg(B)$. If $1 \leq i < j$ then $\alpha_i' = \frac{P_i'+Y}{Q_i'}$ is not reduced, so $\overline{\alpha_i'} \geq 1$ and $\left|\overline{\theta_{i+1}'}\right| \leq 1$. Thus, we know that $\frac{|Q_i'|}{|Q_0'|} \leq \left|\theta_{i+1}'\right| \leq 1$, so $\deg(Q_i') \leq \deg(Q_0') < 2\deg(B)$. Certainly $|r_i'| \leq |Q_i'|$ so $\deg(r_i') < 2\deg(B)$. Also, $P_i' = d + r_{i-1}' + B$. So

$$\begin{aligned} \deg(P_i') &\leq \max\{\deg(d), 2\deg(B)\} \\ &\leq \max\left\{\frac{1}{2}\deg(C), 2\deg(B)\right\}. \end{aligned}$$

Finally,

$$\begin{aligned} \deg(a_i') &\leq \max\{\deg(P_i'), \deg(d)\} \\ &\leq \max\left\{\frac{1}{2}\deg(C), 2\deg(B)\right\} \end{aligned}$$

so all polynomials computed in Steps 3 and 4 have degree bounded by

$$\max\left\{\frac{1}{2}\deg(C), 2\deg(B)\right\}.$$

Step 1 takes $O(\deg(B))$ polynomial operations. Step 3 and the inside of the loop take a fixed number of polynomial operations. However, the loop is executed at most $\max\left\{0, \frac{1}{2}\deg(Q_0') - \frac{1}{2}\deg(B) + 1\right\} < \frac{1}{2}\deg(B)$ times. So at most $O(\deg(B))$ polynomial operations will be performed. □

Since a reduced ideal with a given distance from $\mathcal{A}_1$ may not exist, we define the *reduced ideal closest to the left of* $l \in \mathbb{Z}_{\geq 0}$ to be the ideal $\mathcal{A}_i$ such that $l - \delta_i$ is minimal and positive.

Given an ideal $\mathcal{R} \in \mathfrak{R}$ the next algorithm will find the ideal closest to the left of $\delta(\mathcal{R}) + l$, for small $l \in \mathbb{Z}$, by performing Baby-Steps until the desired ideal is found.

CLOSESTINT

Input: $\mathcal{R} = [Q, P + Y] \in \mathfrak{R}$, $l \in \mathbb{Z}_{\geq 0}$.

Output: $\mathcal{S} \in \mathfrak{R}$ and $f \in \mathbb{Z}_{\leq 0}$ such that $\delta(\mathcal{S}) \leq \delta(\mathcal{R}) + l$ and $f = \delta(\mathcal{S}) - \delta(\mathcal{R}) - l$ is maximal.

1. Set $d_2 := \deg(B) - \deg(Q)$. If $d_2 > l$, then set $\mathcal{S} := \mathcal{R}$, $f := -l$ and **stop**.

2. Set

$$\begin{aligned} j &:= 1 \\ Q_{j-1} &:= Q \\ P_{j-1} &:= P \\ r_{j-1} &:= (P_{j-1} + d) \bmod Q_{j-1} \\ P_j &:= d + r_{j-1} + B \\ Q_j &:= \frac{P_j^2 + P_j B + C}{Q_{j-1}}. \end{aligned}$$

3. **while** $(d_{j+1} \leq l)$ {

$$\begin{aligned} j &:= j + 1 \\ (Q_{j-1}, Q_j, P_j, r_{j-1}, d_{j+1}) &:= \mathbf{BABYSTEP}(Q_{j-2}, Q_{j-1}, P_{j-1}, r_{j-2}, d_j) \end{aligned}$$

}

4. Set $S := [Q_{j-1}, P_{j-1} + Y]$, $f = d_j - l$.

Before proving the correctness of this algorithm, we first require the following lemma.

Lemma 10 *Let $\mathcal{A}_1 = \mathcal{O}, \mathcal{A}_2, \ldots$ be the sequence of reduced ideals produced by the continued fraction algorithm. Then the following holds*

$$\delta(\mathcal{A}_i, \mathcal{A}_1) = \delta(\mathcal{A}_j, \mathcal{A}_1) + \delta(\mathcal{A}_i, \mathcal{A}_j)$$

for all $1 \leq j \leq i$.

Proof: If $j = 1$ then the result is trivially true. Thus assume that $j > 1$. We know that

$$\begin{aligned}\delta(\mathcal{A}_i, \mathcal{A}_1) &= \deg(B) - \deg(Q_0) + \sum_{k=1}^{i-2} \deg(a_k) \\ &= \deg(B) - \deg(Q_0) + \sum_{k=1}^{j-2} \deg(a_k) + \deg(a_{j-1}) + \sum_{k=j}^{i-2} \deg(a_k).\end{aligned}$$

Since $j > 1$, $\mathcal{A}_j$ is represented by a reduced basis, so $|B| = |a_{j-1}Q_{j-1}|$ and $\deg(a_{j-1}) = \deg(B) - \deg(Q_{j-1})$. Thus,

$$\begin{aligned}&\delta(\mathcal{A}_i, \mathcal{A}_1) \\ &= \deg(B) - \deg(Q_0) + \sum_{k=1}^{j-2} \deg(a_k) + \deg(B) - \deg(Q_{j-1}) + \sum_{k=j}^{i-2} \deg(a_k) \\ &= \delta(\mathcal{A}_j, \mathcal{A}_1) + \delta(\mathcal{A}_i, \mathcal{A}_j)\end{aligned}$$

as required. □

Theorem 25 *The ideal $\mathcal{S}$ computed by* **CLOSESTINT** *is the ideal closest to the left of $\delta(\mathcal{R}) + l$. Furthermore, $-l \leq f \leq 0$ and $0 < d_j \leq l$ for all $j \geq 2$ except for the last value d_{j+1} which satisfies $0 < d_{j+1} \leq l + \deg(B)$. The total number of polynomial operations performed is $O(l)$.*

Proof: Let $\mathcal{A}'_1 = \mathcal{R}, \mathcal{A}'_2, \ldots, \mathcal{A}'_s, \mathcal{A}'_{s+1}$ be the sequence of reduced ideals produced. Then since

$$\delta(\mathcal{A}'_i, \mathcal{A}'_1) = \deg(B) - \deg(Q_0) + \sum_{k=1}^{i-2} \deg(a_k)$$

for $i \geq 2$, $d_i = \delta(\mathcal{A}'_i, \mathcal{A}'_1)$ for $2 \leq i \leq s$. The algorithm obviously produces the ideal with $d_s \leq l < d_{s+1}$, so $\delta(\mathcal{A}'_s, \mathcal{A}'_1) \leq l < \delta(\mathcal{A}'_{s+1}, \mathcal{A}'_1)$. Thus we get that $\mathcal{A}'_s = \mathcal{S}$ is the ideal closest to the left of $\delta(\mathcal{R}) + l$.

Also, $0 \geq f = d_s - l \geq -l$, and $0 < d_2 = \deg(B) - \deg(Q) \leq d_j \leq d_s \leq l$ for all $2 \leq j \leq s$. For the last value d_{s+1} we get that $0 < d_{s+1} \leq d_s + \deg(B) \leq l + \deg(B)$ since $\deg(a_s) \leq \deg(B)$.

Finally, since $d_{i+1} > d_i$ and $d_s \leq l$ the loop is executed at most l times and each iteration requires a fixed number of polynomial operations. □

Performing a Giant-Step operation on $\mathcal{A}$ and $\mathcal{B}$ will produce an ideal $\mathcal{R}$ such that $\delta(\mathcal{R}) \leq \delta(\mathcal{A}) + \delta(\mathcal{B})$. Although $\delta(\mathcal{A}) + \delta(\mathcal{B}) - \delta(\mathcal{R})$ is small, it may not be minimal. The purpose of the next algorithm is to minimize this quantity.

CLOSESTSUM

Input: $\mathcal{A}, \mathcal{B} \in \mathfrak{R}$.

Output: $\mathcal{C} \in \mathfrak{R}$, $f \in \mathbb{Z}_{\leq 0}$ such that $\delta(\mathcal{C}) \leq \delta(\mathcal{A}) + \delta(\mathcal{B})$ and $f = \delta(\mathcal{C}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$ is maximal.

1. $(\mathcal{R}, \epsilon) :=$ **GIANTSTEP**$(\mathcal{A}, \mathcal{B})$ so $\epsilon = \delta(\mathcal{R}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$.

2. $(\mathcal{C}, f) :=$ **CLOSESTINT**$(\mathcal{R}, -\epsilon)$ so $f = \delta(\mathcal{C}) - \delta(\mathcal{R}) + \epsilon = \delta(\mathcal{C}) - \delta(\mathcal{A}) - \delta(\mathcal{B})$ is maximal.

Theorem 26 *The ideal $\mathcal{C}$ computed by* **CLOSESTSUM** *is the reduced ideal closest to the left of $\delta(\mathcal{A}) + \delta(\mathcal{B})$. Furthermore, $2 - 2\deg(B) \leq \epsilon \leq f \leq 0$ and the algorithm performs $O(\deg(B))$ polynomial operations.*

Proof: By the previous theorems the first statement is trivial. By **GIANTSTEP** we know that $2 - 2\deg(B) \leq \epsilon \leq 0$. By **CLOSESTINT** we know that $\epsilon \leq f \leq 0$. Also **GIANTSTEP** takes $O(\deg(B))$ polynomial operations while **CLOSESTINT** takes $O(-\epsilon) = O(\deg(B))$ polynomial operations giving us our running time. □

We can now develop an algorithm for computing the ideal closest to the left of $n\delta(\mathcal{A})$ given $\mathcal{A}$. First we will give a purely technical algorithm.

BINARY

Input: $i \in \{1, 0\}$, $\mathcal{A}, \mathcal{B} \in \Re$, $f \in \mathbb{Z}_{\leq 0}$ such that $\delta(\mathcal{B}) \leq s\delta(\mathcal{A})$ for some $s \in \mathbb{Z}_{\geq 1}$ and $f = \delta(\mathcal{B}) - s\delta(\mathcal{A})$ is maximal.

Output: $\mathcal{C} \in \Re$, $l \in \mathbb{Z}_{\leq 0}$ such that $\delta(\mathcal{C}) \leq (2s+i)\delta(\mathcal{A})$ and $l = \delta(\mathcal{C}) - (2s+i)\delta(\mathcal{A})$ is maximal.

1. $(\mathcal{M}, g) :=$ **CLOSESTSUM**$(\mathcal{B}, \mathcal{B})$, so $\delta(\mathcal{M}) \leq 2\delta(\mathcal{B})$ and $g = \delta(\mathcal{M}) - 2\delta(\mathcal{B})$ is maximal.
2. $(\mathcal{N}, h) :=$ **CLOSESTINT**$(\mathcal{M}, -(g+2f))$, so $\delta(\mathcal{N}) \leq \delta(\mathcal{M}) - (g+2f)$ and $h = \delta(\mathcal{N}) - \delta(\mathcal{M}) + g + 2f$ is maximal.
3. If $i = 0$, then set $\mathcal{C} := \mathcal{N}$, $l = h$ and **stop**.

4. $(\mathcal{Q}, k) :=$ **CLOSESTSUM**$(\mathcal{A}, \mathcal{N})$, so $\delta(\mathcal{Q}) \leq \delta(\mathcal{A}) + \delta(\mathcal{N})$ and $k = \delta(\mathcal{Q}) - \delta(\mathcal{A}) - \delta(\mathcal{N})$ is maximal.
5. $(\mathcal{C}, l) :=$ **CLOSESTINT**$(\mathcal{Q}, -(k+h))$, so $\delta(\mathcal{C}) \leq \delta(\mathcal{Q}) - (k+h)$ and $l = \delta(\mathcal{C}) - \delta(\mathcal{Q}) + k + h$ is maximal.

Theorem 27 *The ideal $\mathcal{C}$ computed in* **BINARY** *is the ideal closest to the left of $(2s+i)\delta(\mathcal{A})$. Furthermore $|g|, |h|, |k|, |l| = O(\max\{2\deg(B), |f|\})$ and the algorithm performs $O(\max\{2\deg(B), |f|\})$ polynomial operations.*

Proof: If $i = 0$, then by substituting for g and f we get

$$\delta(\mathcal{C}) = \delta(\mathcal{N}) \leq \delta(\mathcal{M}) - g - 2f = 2s\delta(\mathcal{A}).$$

Also by substituting for g and f we have

$$l = h = \delta(\mathcal{N}) - \delta(\mathcal{M}) + g + 2f = \delta(\mathcal{C}) - 2s\delta(\mathcal{A}).$$

If $i = 1$, then by substituting for k, h, g and f we get

$$\delta(\mathcal{C}) \leq \delta(\mathcal{Q}) - k - h = (2s+1)\delta(\mathcal{A}).$$

Also by substituting for k, h, g and f we have

$$l = \delta(\mathcal{C}) - \delta(\mathcal{Q}) + k + h = \delta(\mathcal{C}) - (2s+1)\delta(\mathcal{A}).$$

Since in both cases l was produced to be maximal, the first claim is true.

From **CLOSESTSUM**, $2 - 2\deg(B) \leq g \leq 0$. Since $f \leq 0$, we then get $g + 2f \leq 0$. From **CLOSESTINT**, $g + 2f \leq h \leq 0$ so

$$|h| \leq 2\deg(B) - 2 + 2|f|.$$

Also from **CLOSESTSUM**, $2 - 2\deg(B) \leq k \leq 0$ so $h + k \leq 0$. Again by **CLOSESTINT**, $h + k \leq l \leq 0$ so

$$|l| \leq 2(2\deg(B) - 2 + |f|).$$

Thus, $|g|, |h|, |k|, |l| = O(\max\{2\deg(B), |f|\})$.

Steps 1 and 4 take $O(\deg(B))$ polynomial operations by **CLOSESTSUM**. Steps 3 and 4 take $O(|g + 2f|)$ and $O(|h + k|)$ polynomial operations respectively. Both of these quantities are $O(\max\{2\deg(B), |f|\})$. Thus **BINARY** takes

$$O(\max\{2\deg(B), |f|\})$$

polynomial operations. □

POWER

Input: $\mathcal{A} \in \mathfrak{R}$, $n \geq 1$.

Output: $\mathcal{B} \in \mathfrak{R}$ such that $\delta(\mathcal{B}) \leq n\delta(\mathcal{A})$ and $f = \delta(\mathcal{B}) - n\delta(\mathcal{A})$ is maximal.

1. Compute the binary representation of $n = \sum_{i=0}^{t} b_i 2^{t-i}$ where $b_0 = 1$ and $b_i \in \{0, 1\}$ for $1 \leq i \leq t$.
2. Set $\mathcal{B}_0 := \mathcal{A}$, $s_0 := 1$, $f_0 := 0$.
3. **for** $i := 1$ **to** t {

$$\begin{aligned} s_i &:= 2s_{i-1} + b_i \\ (\mathcal{B}_i, f_i) &:= \textbf{BINARY}(b_i, \mathcal{A}, \mathcal{B}_{i-1}, f_{i-1}) \end{aligned}$$

[At this point $\mathcal{B}_i \in \mathfrak{R}$, $f_i \in \mathbb{Z}_{\leq 0}$ are such that $\delta(\mathcal{B}_i) \leq s_i\delta(\mathcal{A})$ and $f_i = \delta(\mathcal{B}_i) - s_i\delta(\mathcal{A})$ is maximal.]

}

4. Set $\mathcal{B} := \mathcal{B}_t$ and $f := f_t$.

Theorem 28 *The ideal computed by* **POWER** *is the reduced ideal closest to the left of* $n\delta(\mathcal{A})$. *Furthermore,* $1 \leq s_i \leq n$, $|f_i| = O(\deg(B))$ *for* $0 \leq i \leq t$ *and the algorithm performs* $O(\deg(B)\log_2 n)$ *polynomial operations.*

Proof: By the proof of **BINARY** we know that

$$\delta(\mathcal{B}) = \delta(\mathcal{B}_t) \leq s_t\delta(\mathcal{A}) = n\delta(\mathcal{A})$$

and $f = f_t$ is maximal, so $\mathcal{B}$ is the ideal closest to the left of $n\delta(\mathcal{A})$.

Obviously, $1 \leq s_{i-1} < s_i \leq n$ for $1 \leq i \leq t$. Also, $f_0 = 0$ and again from **BINARY** we get by induction that

$$\begin{aligned} |f_i| &= O(\max\{2\deg(B), |f_{i-1}|\}) \\ &= O(\deg(B)). \end{aligned}$$

The loop is performed $t = \log_2 n$ times and each iteration of **BINARY** takes

$$O\left(\max\{2\deg(B), |f_i|\}\right) = O\left(\deg(B)\right)$$

polynomial operations. So in total **POWER** requires

$$O\left(\deg(B)\log_2 n\right)$$

polynomial operations. □

If n is polynomially bounded by $|B|$, then we can compute the ideal closest to the left of $n\delta(\mathcal{A})$ in $O(\deg(B)^2)$ polynomial operations. Hence, in order to get a polynomially bounded running time both parties in our key exchange should bound their respective "exponents" by a polynomial in $|B|$ that is sufficiently large

to discourage brute force attacks. We will choose our bound to be $|B|^{\frac{1}{2}}$ which roughly corresponds to the choice made in [41]. (See Sections 6.2, 8.2 and 8.3.)

The following two algorithms are variations on **POWER** and can easily be seen to have the same running time. The first will produce the ideal closest to the left of $n\delta(\mathcal{A})$ given $\mathcal{A}$ along with it's distance.

POWERDIST

Input: $\mathcal{A} \in \Re$, $n \geq 1$, $\delta_a \geq 1$ where $\delta_a = \delta(\mathcal{A})$.

Output: $\mathcal{B} \in \Re$, $\delta_b \geq 1$ such that $\delta_b = \delta(\mathcal{B}) \leq n\delta(\mathcal{A})$ and δ_b is maximal.

1. $(\mathcal{B}, f) :=$ **POWER**$(\mathcal{A}, n)$ so $\delta(\mathcal{B}) \leq n\delta(\mathcal{A})$ and $f = \delta(\mathcal{B}) - n\delta(\mathcal{A})$ is maximal.
2. $\delta_b := n\delta_a + f$.

The next algorithm will produce reduced ideals closest to the left of $l \in \mathbb{Z}_{\geq 1}$ for large l.

CLOSESTLEFT

Input: $l \in \mathbb{Z}_{\geq 1}$.

Output: $\mathcal{C} \in \Re$, $\delta_c \in \mathbb{Z}_{\geq 1}$ such that $\mathcal{C}$ is the ideal closest to the left of l and has $\delta_c = \delta(\mathcal{C})$.

1. Set

$$\begin{aligned} \delta_a &:= \deg(B) \\ P &:= d + B \\ Q &:= d^2 + dB + C \\ \mathcal{A} &:= [Q, P + Y] \end{aligned}$$

so $\mathcal{A}$ has $\delta(\mathcal{A}) = \delta_a$.

2. Set

$$\begin{aligned} n &:= \left\lfloor \frac{l}{\delta_a} \right\rfloor \\ r &:= l \bmod \delta_a \\ (\mathcal{B}, f) &:= \mathbf{POWER}(\mathcal{A}, n) \end{aligned}$$

so $\mathcal{B}$ is closest to the left of $n\delta_a = \delta_a \left\lfloor \frac{l}{\delta_a} \right\rfloor$ and $f = \delta(\mathcal{B}) - n\delta_a$.

3. Set $(\mathcal{C}, e) := \mathbf{CLOSESTINT}(\mathcal{B}, r - f)$ and $\delta_c := l + e$. Now $\mathcal{C}$ is closest to the left of

$$\delta(\mathcal{B}) + r - f = n\delta_a + r = \delta_a \left\lfloor \frac{l}{\delta_a} \right\rfloor + (l \bmod \delta_a) = l$$

and $e = \delta(\mathcal{C}) - \delta(\mathcal{B}) - r + f = \delta(\mathcal{C}) - l$ is maximal.

6.2 The Key Exchange and Signature Schemes

We now describe a method of key exchange based on the Diffie-Hellman Key Agreement scheme [13], but using the non-group structure of the infrastructure of a quadratic function field of characteristic 2.

DIFFIE-HELLMAN KEY EXCHANGE

System-wide Parameters:

1. Choose $M \geq 1$ and set $q = 2^M$, $k = F_q$.
2. Generate $B, C, \in k[X]$ such that C is monic, $|B| > 1$, $Y^2 + BY + C = 0$ has no singular points and if $Y^2 + BY = C$ then $Y \in k((\frac{1}{X})) \setminus k(X)$.

3. Compute $d = \lfloor Y \rfloor$ where $Y^2 + BY = C$.
4. Make (q, B, C, d) public; these are the system parameters.

Protocol:

1. Alice does the following:
   (a) secretly generates $k_a \geq 1$, $k_a < |B|^{\frac{1}{2}}$.
   (b) computes $(\mathcal{A}, \delta_a) := \mathbf{CLOSESTLEFT}(k_a)$; here $\mathcal{A} = [Q_a, P_a + Y]$.
   (c) transmits (Q_a, P_a) to Bob, keeps δ_a secret.
2. Bob does the following:
   (a) secretly generates $k_b \geq 1$, $k_b < |B|^{\frac{1}{2}}$.
   (b) computes $(\mathcal{B}, \delta_b) := \mathbf{CLOSESTLEFT}(k_b)$; here $\mathcal{B} = [Q_b, P_b + Y]$.
   (c) transmits (Q_b, P_b) to Alice, keeps δ_b secret.
3. Alice computes $\mathcal{T}_a := \mathbf{POWER}(\mathcal{B}, \delta_a)$.
4. Bob computes $\mathcal{T}_b := \mathbf{POWER}(\mathcal{A}, \delta_b)$.

Shared Information: Alice has computed $\mathcal{T}_a$, the ideal closest to the left of $\delta(\mathcal{B})\delta_a = \delta_b\delta_a$. Similarly, Bob computed the ideal $\mathcal{T}_b$, the ideal closest to the left of $\delta(\mathcal{A})\delta_b = \delta_a\delta_b$. So $\mathcal{T}_a = \mathcal{T}_b = [Q_t, P_t + Y]$ which Alice and Bob share. They can use this for a key to a symmetric-key cryptosystem by determining the polynomial $Q_t' = \frac{Q_t}{\mathbf{sgn}(Q_t)}$. This polynomial is an invariant of the ideal. Also the polynomial $P_t' \equiv P_t \pmod{Q_t'}$, $\deg(P_t') < \deg(Q_t')$ is an invariant of the ideal and can be used as secret information.

We will now describe a digital signature scheme similar to an ElGamal type system [14], which uses the infrastructure of quadratic function fields of characteristic 2. After suitable modifications, this signature scheme is also applicable to

the infrastructure of quadratic number fields and quadratic function fields of odd characteristic. An ElGamal type encryption scheme can also be developed in a similar way.

ELGAMAL DIGITAL SIGNATURE SCHEME

System-wide Parameters:

1. Choose $M \geq 1$ and set $q = 2^M$, $k = F_q$.
2. Generate $B, C, \in k[X]$ such that C is monic, $|B| > 1$, $Y^2 + BY + C = 0$ has no singular points and if $Y^2 + BY = C$ then $Y \in k((\frac{1}{X})) \setminus k(X)$.
3. Compute $d = \lfloor Y \rfloor$ where $Y^2 + BY = C$.
4. Make (q, B, C, d) public; these are the system parameters.

Private and Public Key:

Alice does the following:

1. secretly generates $k_a \geq 1$, $k_a < |B|^{\frac{1}{2}}$.
2. computes $(\mathcal{A}, \delta_a) :=$ **CLOSESTLEFT**(k_a); here $\mathcal{A} = [Q_a, P_a + Y]$.
3. makes (Q_a, P_a) public (this is her public key) and keeps δ_a private (her private key).

Signature Generation:

To sign a message $\tilde{M}$, Alice does the following:

1. secretly generates $l \in \mathbb{Z}$ with $|B| < l < |B|^2$.
2. computes $(\mathcal{R}, \delta_r) :=$ **CLOSESTLEFT**(l); here $\mathcal{R} = [Q_r, P_r + Y]$.

3. computes $e := h(\tilde{M} \| \frac{Q_r}{\mathrm{sgn}(Q_r)} \| P_r \bmod \frac{Q_r}{\mathrm{sgn}(Q_r)})$ where h is a cryptographically secure hash function which takes on values less than $|B|^{\frac{1}{2}}$.
4. computes $s := -\delta_a e + \delta_r$ (notice that $s > 0$) and releases $(\mathcal{R}, s)$ as her signature for $\tilde{M}$.

Signature Verification:

To verify Alice's signature on the message $\tilde{M}$, Bob does the following:

1. obtains Alice's public key (Q_a, P_a).
2. computes $e := h(\tilde{M} \| \frac{Q_r}{\mathrm{sgn}(Q_r)} \| P_r \bmod \frac{Q_r}{\mathrm{sgn}(Q_r)})$.
3. computes $(\mathcal{B}, f) := \mathbf{POWER}(\mathcal{A}, e)$.
4. computes $(\mathcal{C}, g) := \mathbf{CLOSESTLEFT}(s)$.
5. computes $(\mathcal{D}, h) := \mathbf{CLOSESTSUM}(\mathcal{B}, \mathcal{C})$.
6. computes $(\mathcal{R}', l) := \mathbf{CLOSESTINT}(\mathcal{D}, f + g + h)$.
7. if $\mathcal{R}' = \mathcal{R}$ then he accepts the signature; otherwise, he rejects the signature.

Bob has computed the ideal $\mathcal{R}'$ which is the ideal closest to the left of $s + \delta_a e$. Thus, $\mathcal{R}'$ is the ideal closest to the left of δ_r and so must equal $\mathcal{R}$ if the signature is valid.

6.3 Security Issues

It is easy to see that solving the discrete log problem for quadratic function fields allows one to break the Diffie-Hellman Key Exchange or ElGamal Digital Signature

Schemes described in Section 6.2. We now describe an attack based on the Pohlig-Hellman method [37] to solve the discrete log problem when the regulator and its factorization are known.

Let $\mathcal{A} \in \mathfrak{R}$ be a primitive reduced ideal and δ be its discrete logarithm. We will describe how to determine $x \equiv \delta \pmod{p}$ where the regulator is $R = pq'$ and p is prime.

POHLIG-HELLMAN

Input: A quadratic function field K defined by $B, C \in k[X]$, the regulator R, p and q' such that $R = pq'$ and p is prime, and $\mathcal{A} \in \mathfrak{R}$.

Output: $x \equiv \delta(\mathcal{A}) \pmod{p}$.

1. Set $(\mathcal{B}, f) := \mathbf{POWER}(\mathcal{A}, q')$
   So $\delta(\mathcal{B}) = q'\delta(\mathcal{A}) + f$, $\mathcal{B}$ is closest to the left of $q'\delta(\mathcal{A})$.
2. Set

$$\begin{aligned} (\mathcal{C}, \delta_c) &:= \mathbf{CLOSESTLEFT}(q') \\ \epsilon &:= \delta_c - q' \end{aligned}$$

3. {Make table}

$$\begin{aligned} i &:= 0 \\ \mathcal{D}_i &:= \mathcal{B} \\ f_i &:= f \end{aligned}$$

for $i := 1$ **to** $\left\lceil \sqrt{p} \right\rceil - 1$ {

$$(\mathcal{T}, g) := \textbf{CLOSESTSUM}(\mathcal{C}, \mathcal{D}_{i-1})$$
$$(\mathcal{D}_i, f_i) := \textbf{CLOSESTINT}(\mathcal{T}, -(\epsilon + f_{i-1} + g))$$

if $(\mathcal{D}_i = \mathcal{O})$ **and** $f_i \equiv 0 \bmod R$ **then** $x \equiv -i \pmod{p}$.
Since $iq' + \delta(\mathcal{A})q' + f_i \equiv 0 \pmod{R}$.

}

4.

$$(\mathcal{E}_1, e_1) := \textbf{CLOSESTLEFT}(\lceil\sqrt{p}\rceil\, q')$$
$$i := 1$$

while $(\mathcal{E}_i \neq \mathcal{D}_j$ for $j = 0, 1, \ldots, \lceil\sqrt{p}\rceil - 1)$ {

$$i := i + 1$$
$$(\mathcal{T}, g) := \textbf{CLOSESTSUM}(\mathcal{E}_{i-1}, \mathcal{E}_1)$$
$$(\mathcal{E}_i, e_i) := \textbf{CLOSESTINT}(\mathcal{T}, -(e_{i-1} + e_1 + g))$$

}

5. **if** $f_j \equiv e_i \pmod{R}$ **then** $x :\equiv i\lceil\sqrt{p}\rceil - j \pmod{p}$.
otherwise return to Step 4.

After Step 4 has completed we have $\mathcal{D}_j = \mathcal{E}_i$, so $\delta(\mathcal{D}_j) \equiv \delta(\mathcal{E}_i) \pmod{R}$. Thus,

$$jq' + \delta(\mathcal{A})q' + f_j \equiv i\lceil\sqrt{p}\rceil\, q' + e_i \pmod{R}.$$

Let $x = s\lceil\sqrt{p}\rceil - r$ where $0 < r \leq \lceil\sqrt{p}\rceil$ and $s \geq 1$. Then $s\lceil\sqrt{p}\rceil\, q' \equiv \delta(\mathcal{A})q' + rq'$ (mod R). When $s = i$ and $r = j$ then $\mathcal{D}_j$ is closest to the left of $rq' + \delta(\mathcal{A})q'$ and

$\mathcal{E}_i$ is closest to the left of $s\left\lceil\sqrt{p}\right\rceil q'$ and so the algorithm will stop. Since these two values are congruent mod R, so will be f_j and e_i and the algorithm will terminate.

Steps 3 and 4 take at most $\left\lceil\sqrt{p}\right\rceil$ iterations, each requiring $O(\deg(B))$ polynomial operations. Also, the **POWER** computations will require $O(\deg(B)\log_2 R)$ polynomial operations, thus the algorithm runs in

$$O\left(\left(\lceil\sqrt{p}\rceil + \log_2 R\right)\deg(B)\right)$$

polynomial operations. It is therefore only feasible when R factors as the product of small primes.

If $R = q''p^i$ for $i \geq 2$ then the following algorithm will determine $\delta(\mathcal{A}) \bmod p^i$. It is easy to see that it has the same running time as **POHLIG-HELLMAN**. We will assume inductively that we already have $x \equiv \delta(\mathcal{A}) \pmod{p^{i-1}}$.

POHLIG-HELLMAN-POWERS

Input: A quadratic function field K defined by $B, C \in k[X]$, the regulator R, p, q'' and i such that $R = q''p^i$ and p is prime, $\mathcal{A} \in \mathfrak{R}$, and $x \equiv \delta(\mathcal{A}) \pmod{p^{i-1}}$, $0 \leq x < p^{i-1}$.

Output: $x' \equiv \delta(\mathcal{A}) \pmod{p^i}$.

1. Set $(\mathcal{B}, f) :=$ **CLOSESTINT**$(\mathcal{A}, p^{i-1} - x)$.
   So if $\delta(\mathcal{A}) = sp^{i-1} + x$, then $\mathcal{B}$ is closest to the left of $(s+1)p^{i-1}$ and $\delta(\mathcal{B}) = (s+1)p^{i-1} - f$.
2. Set $(\mathcal{C}, g) :=$ **POWER**$(\mathcal{B}, q'')$.
   So $\mathcal{C}$ is closest to the left of $q''\delta(\mathcal{B}) = q''(s+1)p^{i-1} - q''f$ and $\delta(\mathcal{C}) - q''(s+1)p^{i-1} + q''f = g$.

3. Set $(\mathcal{D}, \delta_d) :=$ **CLOSESTLEFT**$(q''f - g)$.
   Let $\delta := \delta_d - q''f + g$.
4. Set $(\mathcal{E}, h) :=$ **CLOSESTSUM**$(\mathcal{C}, \mathcal{D})$.
   So $\mathcal{E}$ is closest to the left of
   $$\delta(\mathcal{C}) + \delta_d = q''(s+1)p^{i-1} - q''f + g + q''f - g + \delta.$$
5. Set $(\mathcal{F}, \epsilon) :=$ **CLOSESTINT**$(\mathcal{E}, \delta + h)$.
   Now $\mathcal{F}$ is closest to the left of $q''p^{i-1}(s+1)$.
6. Starting **POHLIG-HELLMAN** at Step 2 with $q' := q''p^{i-1}$, $\mathcal{B} := \mathcal{F}$ and $f := \epsilon$ gives
   $$jq''p^{i-1} + (s+1)q''p^{i-1} + f_j \equiv i\lceil\sqrt{p}\rceil\, q''p^{i-1} + e_i \pmod{R}.$$
   So, $s + 1 \equiv i\left\lceil\sqrt{p}\right\rceil - j \pmod{p}$. Let $y :\equiv i\left\lceil\sqrt{p}\right\rceil - j - 1 \pmod{p}$, then $x' :\equiv yp^{i-1} + x \pmod{p^i}$.

At this time, the best known algorithm to find R runs in time

$$O\left(q^{\frac{1}{2}\deg(B)+\epsilon}\right).$$

(See Section 8.2.) Thus, finding R is infeasible when B and C are chosen so that $q^{\frac{1}{2}\deg(B)}$ is large. Since the Pohlig-Hellman algorithm requires the knowledge of R, it does not appear to pose a serious threat.

We remark that this Pohlig-Hellman attack is also valid on the cryptosystems proposed for the infrastructure of quadratic function fields of odd characteristic.

In [33] a probabilistic subexponential algorithm is given for computing discrete logarithms in the infrastructure of quadratic function fields of odd characteristic. It would appear natural that this algorithm could be modified to work in even

characteristic. However, it only works for function fields of sufficiently large genus. At this point, it does not appear to be a serious threat to cryptosystems of practical size.

As shown in Section 8.2,

$$m = O\left(q^{\deg(B)}\right)$$

and

$$R = O\left(q^{\deg(B)}\right).$$

In order to prevent against brute force attacks on the discrete log problem, we would suggest that q, B and C be chosen so that

$$q^{\deg(B)} \approx 10^{100}.$$

This would also make finding R and using the subexponential attack infeasible.

Chapter 7

Equivalent Discrete Logarithm Problems

This chapter will show how non-supersingular elliptic curves over fields of characteristic 2 are related to the function fields we have been studying in the previous three chapters. This analysis is similar to that of [1] for underlying fields of odd characteristic.

7.1 The Divisors of an Elliptic Curve

In this section we will state some well known results concerning divisors of elliptic curves (see [10, 28, 29]).

Let E be a non-supersingular elliptic curve defined over $k = F_q$ where $q = 2^M$. If E is defined by the equation

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

then let $K = k(x, y)$ be the function field associated with E. In Section 7.3 we will see the connection between this function field and those discussed in the previous chapters. At this point, the connection should not be obvious.

Definition 6 *A divisor D is a formal sum of points in E*

$$D = \sum_{P \in E} m_P (P), m_P \in \mathbb{Z}$$

where only a finite number of the m_P are non-zero. Define the degree of D to be $\sum_{P \in E} m_P$.

The set of all divisors associated with E forms a free abelian group over $\mathbb{Z}$ generated by the points of E.

Let $R \in K$, and let $P = (x_0, y_0) \in E$, $P \neq \infty$. Then R is said to be *defined at P* if there exist polynomial functions $a(x) + yb(x), c(x) + yd(x) \in k[x, y]$ where $a(x), b(x), c(x), d(x) \in k[x]$ such that $R = \frac{a(x)+yb(x)}{c(x)+yd(x)}$ and $c(x_0) + y_0 d(x_0) \neq 0$; if no such $a(x) + yb(x)$ and $c(x) + yd(x)$ exist, then $R(P)$ is *not defined.* If R is defined at P, the *value of R at P* is defined to be $R(P) := \frac{a(x_0)+y_0 b(x_0)}{c(x_0)+y_0 d(x_0)}$.

Define $\deg(a(x) + yb(x)) = \max\{2 \deg_x(a(x)), 3 + 2 \deg_x(b(x))\}$.

Let $R = \frac{a(x)+yb(x)}{c(x)+yd(x)} \in K$ for some $a(x), b(x), c(x), d(x) \in k[x]$.

1. If $\deg(a(x) + yb(x)) < \deg(c(x) + yd(x))$ then define $R(\infty) := 0$.

2. If $\deg(a(x) + yb(x)) > \deg(c(x) + yd(x))$ then $R(\infty)$ is *not defined.*

3. If $\deg(a(x) + yb(x)) = \deg(c(x) + yd(x))$ then $R(\infty)$ is defined to be the ratio of the leading coefficients (with respect to deg) of the numerator and denominator.

Let $R \in K$ and $P \in E$. If $R(P) = 0$ then R has a *zero* at P. If $R(P)$ is not defined then R has a *pole* at P and we write $R(P) = \infty$.

Notice that if $P = (x_0, y_0) \in E$ then $x(P) = x_0$ and $y(P) = y_0$.

Theorem 29 *Let $P \in E$. Then there exists a function $U \in K$ with $U(P) = 0$ such that for each function $G \in K$, there exists an integer e and function $S \in K$ such that $S(P) \neq 0, \infty$ and $G = U^e S$. Furthermore, the number e does not depend on the choice of U.*

Call this integer e, the *order of G at P* and write $\mathrm{ord}_P(G) = e$. The function U is called a *uniformizing parameter* for P.

1. If $P = (x_0, y_0) \in E$ with $P, 2P \neq \infty$ then $x + x_0$ is a uniformizing parameter for P.

2. If $P = (x_0, y_0) \in E$ with $P \neq \infty$, $2P = \infty$ then $y + y_0$ is a uniformizing parameter for P.

3. If $P = \infty \in E$ then $\frac{x}{y}$ is a uniformizing parameter for P.

Let $R \in K$. Define the *divisor of R* as

$$\mathrm{div}\,(R) = \sum_{P \in E} \mathrm{ord}_P(R)\,(P)\,.$$

It is well known (see [29]) that $\sum_{P \in E} \mathrm{ord}_P(R) = 0$. Thus $\mathrm{div}\,(R)$ has degree 0.

A divisor D of degree 0 is called *principal* if $D = \mathrm{div}\,(R)$ for some $R \in K$. Two divisors D_1 and D_2 of degree 0 are said to be *equivalent* if $D_1 - D_2$ is principal. If D_1 and D_2 are equivalent then we write $D_1 \sim D_2$. The relation $\sim$ is an equivalence relation.

It is also known that if we let $P_1, P_2 \in E$ and $P_3 = P_1 + P_2$ then $D_1 \sim D_2$ if $D_1 = (P_1)+(P_2)-2(\infty)$ and $D_2 = (P_3)-(\infty)$. Also, if $(P_1)+(P_2)-(P')-(\infty) \sim (0)$ then $P' = P_3$.

Let $R \in K$. Define the *divisor of poles* of R to be

$$\operatorname{div}(R)_\infty = -\sum_P \operatorname{ord}_P(R)(P)$$

where the sum is over all poles of R. Similarly, the *divisor of zeros* is

$$\operatorname{div}(R)_0 = \sum_P \operatorname{ord}_P(R)(P)$$

where the sum is over all zeros of R.

A *valuation* on K is a function $\operatorname{val} : K \to \mathbb{Z} \cup \{\infty\}$ such that

1. $\operatorname{val}(R) \in \mathbb{Z}$ if $R \neq 0$, and $\operatorname{val}(0) = \infty$.
2. $\operatorname{val}(R+S) \geq \min\{\operatorname{val}(R), \operatorname{val}(S)\}$.
3. $\operatorname{val}(RS) = \operatorname{val}(R) + \operatorname{val}(S)$.

It is easy to see that ord_P for $P \neq \infty$ is a valuation. We say that it corresponds to the *place at* P. Also, $\operatorname{ord}_\infty$ is the *valuation at the place* ∞.

We can similarly define valuations for the field $k(X)$ where X is a transcendental element over k. If $u \in k$ then the valuation at the place corresponding to $X + u$ is simply the usual multiplicity of u as a zero or pole in a rational function. The valuation at the place at infinity is the negative of the degree function in $k(X)$.

7.2 An Overview

The remainder of this chapter will describe the equivalence between the elliptic discrete logarithm problem and certain instances of the infrastructure discrete logarithm problem. This section will give an outline of the proof of this equivalence.

In Section 2.4 we defined what we mean by a non-supersingular elliptic curve over a field, k, of characteristic 2. We also stated the group law for this curve. Thus, given a point $P = (a, b)$ on an elliptic curve, E, we can compute all multiples of this point. Since an elliptic curve of this type is a finite group, P has a finite order, μ.

In Section 7.3 we will show how to use the curve E and the point P to produce an equation E_P. We will give a birational transformation between E and E_P so that given a point on E, $(x, y) \neq P, \infty$, we will be able to easily produce the corresponding point (X, Y) on E_P. We will be interested in the multiples of P, as shown in the following diagram.

$$
\begin{array}{cccc}
 & E, P & & E_P \\
 & \left.\begin{array}{r} 0P = \infty \\ P = (a,b) \end{array}\right\} & \longrightarrow & \infty \\
 & 2P = (x_2, y_2) & \longrightarrow & (X_2, Y_2) \\
\text{multiples} & 3P = (x_3, y_3) & \longrightarrow & (X_3, Y_3) \\
\text{of } P & \vdots & & \vdots \\
 & iP = (x_i, y_i) & \longrightarrow & (X_i, Y_i) \\
 & \vdots & & \vdots \\
 & (\mu - 1)P = (x_{\mu-1}, y_{\mu-1}) & \longrightarrow & (X_{\mu-1}, Y_{\mu-1})
\end{array}
$$

The equation E_P will be of the form $Y^2 + BY = C$ with $Y \in k((\frac{1}{X}))$ and E_P will be non-singular, so we will be able to use the results of Chapters 4 and 5. In particular, we will be able to compute the continued fraction expansion of elements of $K = k(X)(Y)$. Section 7.4 will introduce a family of elements of K, f_Q for all $Q \in E$, $Q \neq P$. We will examine the continued fraction expansion of f_Q and see that its quasi-period is related to the order of P. In fact, the quasi-period of f_∞ is $m = \mu - 1$ and the elements of K produced by the continued fraction expansion of f_∞ are (up to scalar factors) $f_\infty, f_{2P}, f_{3P}, \ldots, f_{(\mu-1)P}$.

Since we can compute the continued fraction expansion of f_∞, we can use the results of Section 5.2 to produce $\mathcal{O}$-ideals, $\mathcal{A}_i$, corresponding to each of these quadratic irrationals. Section 7.5 will show that the ideal $\mathcal{A}_i$, which corresponds to f_{iP} for $2 \leq i \leq m$, has the form $\mathcal{A}_i = [X + X_i, \overline{Y_i} + Y]$ where (X_i, Y_i) is, as before, the point on E_P corresponding to $iP = (x_i, y_i)$ on E. It is this final correspondence that will show that the two discrete logarithm problems are equivalent. This is outlined in the following diagram.

$$
\begin{array}{cc}
f_Q \in K & \mathcal{O}\text{-ideals} \\
\text{obtained from the continued fraction expansion of } f_\infty & \left\{ \begin{array}{ccc}
f_\infty & \longrightarrow & \mathcal{A}_1 = [1, Y] \\
f_{2P} & \longrightarrow & \mathcal{A}_2 = [X + X_2, \overline{Y_2} + Y] \\
f_{3P} & \longrightarrow & \mathcal{A}_3 = [X + X_3, \overline{Y_3} + Y] \\
\vdots & & \vdots \\
f_{iP} & \longrightarrow & \mathcal{A}_i = [X + X_i, \overline{Y_i} + Y] \\
\vdots & & \vdots \\
f_{mP} & \longrightarrow & \mathcal{A}_m = [X + X_m, \overline{Y_m} + Y]
\end{array} \right.
\end{array}
$$

For completed examples of this equivalence, see Section 7.6.

7.3 The Correspondence

Assume that we have a non-supersingular elliptic curve defined over $k = F_q$ where $q = 2^M$. Let the curve be defined by

$$E : y^2 + xy = x^3 + a_2x^2 + a_6$$

for $a_2, a_6 \in k$, $a_6 \neq 0$. In order to avoid confusion with divisor addition, for the remainder of this chapter we will denote the usual addition on the curve E by the symbol $\oplus$. Let $P = (a, b)$ be a point on the curve with $a, b \in k$ and $2P \neq \infty$ (i.e. P is not a point of order 2). Then $K = k(E) = k(x, y)$ is the function field for E. Now let

$$\begin{aligned} X &= \frac{y+b+a}{x+a} \\ Y &= x + \left(\frac{y+b+a}{x+a}\right)^2 + a_2. \end{aligned}$$

Notice that X and Y are functions of x and y (i.e. $X, Y \in K$). Substituting into E we get the following equation:

$$E_P : Y^2 + (X^2 + X + a + a_2)Y = X^3 + a_2X + a^2 + b + a$$

which we will call the *quadratic model* for E. It is the transformation between E and E_P that will give the connection between the elliptic curve group and the infrastructure.

Also, we have the following formulae for x and y in terms of X and Y:

$$\begin{aligned} x &= Y + X^2 + a_2 \\ y &= X(x+a) + b + a. \end{aligned}$$

Since this is a birational transformation between E and E_P we see that K can also be written as $k(E_P) = k(X, Y)$. Notice that $Y \in k((\frac{1}{X}))$ and that E_P is non-singular, so K is a quadratic function field as described in Chapters 4 and 5.

We would now like to find the divisors of poles of X and Y. Since P is not a point of order 2, it is easy to see from the formula for X that P is a pole of X of order 1. Also, since $\frac{x}{y}$ is a uniformizing parameter for ∞ there is a pole of order 1 at ∞. These are the only poles, so

$$\operatorname{div}(X)_\infty = (\infty) + (P).$$

Similarly, it is easy to see that

$$\operatorname{div}(Y)_\infty = 2(P) + (\infty).$$

There is a $k(X)$-automorphism of K that takes Y to $Y + X^2 + X + a + a_2$. That is, if $f = g(X) + Yh(X)$ is in K with $g(X), h(X) \in k(X)$, write $f^* = g(X) + Yh(X) + (X^2 + X + a + a_2)h(X)$. This is the conjugate automorphism described in Section 4.2 for general function fields. Notice that $X^* = X$ and $Y^* = Y + X^2 + X + a + a_2$. Also

$$x^* = Y + X + a$$

and

$$y^* = X(x^* + a) + b + a.$$

So

$$x + x^* = X^2 + X + a + a_2$$

and

$$xx^* = aX^2 + b + a + aa_2 + a^2.$$

If $Q_0 = (X_0, Y_0) \in k \times k$ is a solution to the equation E_P, then so is $Q_0^* = (X_0, Y_0 + X_0^2 + X_0 + a + a_2)$. For $Q \in E$, $Q \neq P, \infty$, we can define $Q^* = (x^*(Q), y^*(Q))$. Also define $\infty^* = P$ and $P^* = \infty$.

If we start with the curve E_P then ∞ and P are the two points at infinity. We will now distinguish between the two. Now xx^* has double poles at ∞ and P. If x and x^* both have simple poles at ∞ (and at P), then $x + x^*$ has at most a simple pole at ∞ (and at P). This contradicts the fact that $x + x^*$ has double poles at ∞ (and P). Thus x has a double pole at one of ∞ or P and x^* has a double pole at the other. Using the uniformizing parameter for ∞ we can see that ∞ is a double pole of x and so P is a double pole of x^*. Thus

$$\operatorname{div}(x)_\infty = 2(\infty) \quad , \quad \operatorname{div}(x^*)_\infty = 2(P).$$

There are two possibilities for Y expressed as a Laurent series in $\frac{1}{X}$. We have chosen, as in Section 4.1, $Y = X + \cdots$, and hence $x = X^2 + X + a_2 + \cdots$. Also, $Y^* = X^2 + (a + a_2) + \cdots$ and $x^* = a + \cdots$. From this we get $d = \lfloor Y \rfloor = X$.

Notice that the place at infinity, $\mathcal{P}_\infty$, of $k(X)$ extends to the place at ∞ in K. This follows from our choice for Y. If we had made the other choice, then $\mathcal{P}_\infty$ would have extended to the place at P.

Since $\operatorname{div}(X + X(Q)) = (Q) + (Q^*) - (\infty) - (P)$ for $Q \in E$, $Q \neq \infty, P$ we get that $Q \oplus Q^* = P$.

If $Q = (x_0, y_0) \in E$, then $-Q = (x_0, y_0 + x_0)$. So, if $Q \neq \infty$, then $x(-Q) = x(Q)$ and $y(-Q) = y(Q) + x(Q)$.

7.4 Periodicity of the Continued Fraction Expansion and Orders of Points

This section will examine the continued fraction expansion of a specific function in K, f_Q. Its periodicity will be related to the order of the point P and its special

form will therefore give us the equivalence we want.

Definition 7 *Let Q be any k-rational point on E, with $Q \neq P$. Define*

$$f_Q = \begin{cases} \frac{x+x(Q^*)}{X+X(Q)} & \text{if } Q \neq \infty \\ \\ x + x(Q^*) = x + a & \text{if } Q = \infty. \end{cases}$$

Lemma 11 *Let Q be any k-rational point on E, with $Q \neq P$. Then, up to multiplication by a non-zero constant, there is one and only one function f on E such that $div(f)_\infty = (\infty) + (Q)$ and $f(P) = 0$. It is given by $f = f_Q$. Furthermore,*

$$div(f_Q) = (P) + (-Q^*) - (\infty) - (Q).$$

Proof: If $Q \neq \infty$, then $\operatorname{div}(x + x(Q^*)) = (Q^*) + (-Q^*) - 2(\infty)$. Since $X(Q) = X(Q^*)$ we have $\operatorname{div}(X + X(Q)) = (Q) + (Q^*) - (\infty) - (P)$. Hence

$$\operatorname{div}(f_Q) = (P) + (-Q^*) - (Q) - (\infty).$$

If $Q = \infty$ then $\operatorname{div}(f_Q) = \operatorname{div}(x + x(Q^*) = (Q^*) + (-Q^*) - 2(\infty)$. Since $Q^* = P$,

$$\operatorname{div}(f_Q) = (P) + (-Q^*) - (Q) - (\infty).$$

Let $\operatorname{div}(f) = (P) + (Q') - (\infty) - (Q)$ for any point Q'. Then $\operatorname{div}(f^{-1}f_Q) = (-Q^*) - (Q')$ which says that $-Q^* = Q'$ and that $f^{-1}f_Q$ is a constant. Thus, up to multiplication by a non-zero constant, f_Q is unique. □

Definition 8 *Let*

$$\varphi(f) := \frac{1}{f + \lfloor f \rfloor}$$

for any $f \in K^*$. This is one step in the continued fraction algorithm performed on f, or one Baby-Step.

Lemma 12 *Let Q be a k-rational point on E, with $Q \neq P$. Let f be a function such that $div(f)_\infty = (\infty) + (Q)$. Then*

$$div(\varphi(f)) = \begin{cases} (P) + (Q) - (\infty) - (Q') & \text{if } Q \neq \infty \\ 2(P) - (\infty) - (Q') & \text{if } Q = \infty \end{cases}$$

where

$$Q' = \begin{cases} P \oplus Q & \text{if } Q \neq \infty \\ 2P & \text{if } Q = \infty. \end{cases}$$

Thus, $\varphi(f)$ is a constant multiple of $f_{Q'}$.

Proof: Let $Q \neq \infty$. Since P is not a pole of f, f is not a polynomial in X and so $f + \lfloor f \rfloor \neq 0$ has a zero at ∞. Thus, $\varphi(f)$ has a pole at ∞. Now f has a simple pole at ∞, so $\lfloor f \rfloor$ is a linear polynomial in X, and hence has a simple pole at P. So $\varphi(f)$ has a zero at P. Also, f has a simple pole at Q and $\lfloor f \rfloor$ does not, so $\varphi(f)$ has a zero at Q.

Since f has poles at ∞ and Q, and $\lfloor f \rfloor$ has poles at P and ∞, we get that $\varphi(f)$ has no other zeros. Thus,

$$\text{div}\,(\varphi(f)) = (P) + (Q) - (\infty) - (Q')$$

and then $Q' = P \oplus Q$.

If $Q = \infty$ then again $\varphi(f)$ has a pole at ∞. Also, f has a double pole at ∞, so $\lfloor f \rfloor$ is a quadratic polynomial in x and has a double pole at P. This tells us that $\varphi(f)$ has a double zero at P. There are no other poles of f or $\lfloor f \rfloor$, so

$$\text{div}\,(\varphi(f)) = 2(P) - (\infty) - (Q')$$

and $Q' = 2P$. □

Let $Q \neq \infty, P$. From the definition of f_Q,

$$\begin{aligned} f_Q + (X + X(Q) + 1) &= \frac{x + x(Q^*) + X^2 + X(Q)^2 + X + X(Q)}{X + X(Q)} \\ &= \frac{x^* + a + a_2 + X(Q)^2 + x(Q^*) + X(Q)}{X + X(Q)} \\ &= \frac{x^* + x(Q)}{X + X(Q^*)} \\ &= f^*_{Q^*} \end{aligned}$$

since $x = x^* + X^2 + X + a + a_2$, $x^*(Q) = x(Q^*)$ and $X(Q) = X(Q^*)$.

Since f_{Q^*} has a zero at P, $f^*_{Q^*}$ has a zero at $P^* = \infty$. Thus, $\deg(f^*_{Q^*}) < 0$ and so,

$$\lfloor f_Q \rfloor = X + X(Q) + 1.$$

Using this fact, it follows that

$$\begin{aligned} \varphi(f_Q) &= \frac{1}{f^*(Q^*)} \\ &= \frac{X + X(Q^*)}{x^* + x(Q)} \\ &= \frac{(X + X(Q^*))(x + x(Q))}{(x^* + x(Q))(x + x(Q))} \\ &= \frac{(X + X(Q^*))(x + x(Q))}{x^*x + (x + x^*)x(Q) + x(Q)^2} \\ &= \frac{(X + X(Q^*))(x + x(Q))}{(a + x(Q))X^2 + x(Q)X + b + a + aa_2 + a^2 + ax(Q) + a_2x(Q) + x(Q)^2} \\ &= cf_{Q \oplus P} \end{aligned}$$

for some $c \in k^*$, by the previous lemma. Thus $c = \frac{1}{a + x(Q)}$ if $x(Q) \neq a$ and $c = \frac{1}{x(Q)}$ if $x(Q) = a$. (Note that if $x(Q) = a$ then $Q = -P$ since we are not allowing $Q = P$.)

Now let $Q = \infty$, so that $f_Q = x + a$. We get

$$(x+a)^* = (x+a) + X^2 + X + a + a_2.$$

Since $x+a$ has a zero at P, $(x+a)^*$ has a zero at $P^* = \infty$. Thus, $\deg((x+a)^*) < 0$ and so $\lfloor f_Q \rfloor = X^2 + X + a + a_2$. Also, as before

$$\begin{aligned}
\varphi(f_Q) &= \frac{1}{(x+a)^*} \\
&= \frac{x+a}{(x^*+c)(x+a)} \\
&= \frac{x+a}{xx^* + a(x+x^*) + a^2} \\
&= \frac{x+a}{aX + b + a + a^2} \\
&= cf_{2P}
\end{aligned}$$

for some $c \in k^*$. Thus, $c = \frac{1}{a}$.

These results allow us to state the following lemma.

Lemma 13 *Let Q be a k-rational point on E with $Q \neq P$. Then*

$$\lfloor f_Q \rfloor = \begin{cases} X + X(Q) + 1 & \text{if } Q \neq \infty \\ X^2 + X + a + a_2 & \text{if } Q = \infty \end{cases}$$

and

$$\varphi(f_Q) = \begin{cases} \frac{1}{x(Q)+a} f_{Q \oplus P} & \text{if } Q \neq \infty, -P \\ \frac{1}{a} f_\infty & \text{if } Q = -P \\ \frac{1}{a} f_{2P} & \text{if } Q = \infty. \end{cases}$$

For $Q \neq P$, we define

$$\lambda(Q) = \begin{cases} \frac{1}{x(Q)+a} & \text{if } Q \neq \infty, -P \\ \\ \frac{1}{a} & \text{if } Q = \infty, -P \end{cases}$$

and

$$\psi(Q) = \begin{cases} Q \oplus P & \text{if } Q \neq \infty \\ \\ 2P & \text{if } Q = \infty. \end{cases}$$

As a consequence of the previous lemma

$$\varphi(f_Q) = \lambda(Q) f_{\psi(Q)}.$$

We will use the notation φ_j, λ_j and ψ_j for $j \in \mathbb{Z}_{\geq 0}$, to mean the j-fold composition of φ, λ and ψ with themselves. It is easy to see that

$$\varphi_\nu(cf) = c^{(-1)^\nu} \varphi_\nu(f).$$

Let

$$\rho_\nu(Q) = \prod_{j=0}^{\nu-1} \lambda(\psi_j(Q))^{(-1)^{\nu-1-j}}$$

and we get the following proposition.

Proposition 4 *Let $Q \neq P$ be a k-rational point on E. Then for $\nu \in \mathbb{Z}_{\geq 0}$,*

$$\varphi_\nu(f_Q) = \rho_\nu(Q) f_{\psi_\nu(Q)}$$

and

$$\lfloor \varphi_\nu(f_Q) \rfloor = \begin{cases} \rho_\nu(Q)\,(X + X(\psi_\nu(Q)) + 1) & \text{if } \psi_\nu(Q) \neq \infty \\ \\ \rho_\nu(Q)\,(X^2 + X + a + a_2) & \text{if } \psi_\nu(Q) = \infty. \end{cases}$$

Moreover, the formulae for $\psi_\nu(Q)$ in terms of the group law on E are:

Case 1: *$-Q$ is not a non-negative multiple of P and P has finite order μ. Write $\nu = q\mu + r$ for $q, r \in \mathbb{Z}$, $0 \leq r < \mu$. Then*

$$\psi_\nu(Q) = Q \oplus rP.$$

Case 2: *$-Q = \nu_0 P$ and P has finite order μ. We may assume that $0 \leq \nu_0 < \mu - 1$ (since $Q = P$ is not allowed). Write $\nu - \nu_0 = q(\mu-1)+r$ for $q, r \in \mathbb{Z}$, $1 \leq r \leq \mu-1$. Then*

$$\psi_\nu(Q) = (r+1)P.$$

Proof: These follow directly from repeated applications of Lemma 13 and the above definitions. To see Case 2, notice that if $l(\mu-1) \geq \nu - \nu_0 > (l-1)(\mu-1)$ for some $l \in \mathbb{Z}_{\geq 1}$, then

$$\begin{aligned}
\psi_\nu(Q) &= \psi_r(\psi_{(l-1)(\mu-1)}(\psi_{\nu_0}(Q))) \\
&= \psi_r(\psi_{(l-1)(\mu-1)}(\infty)) \\
&= \psi_r(\infty) \\
&= (r+1)P.
\end{aligned}$$

If $\nu - \nu_0 \leq 0$ then $\nu \leq \nu_0$ and $r = \nu - \nu_0 + \mu - 1$, so we simply get

$$\begin{aligned}
\psi_\nu(Q) &= Q \oplus \nu P \\
&= (\nu - \nu_0)P \\
&= (\nu - \nu_0 + \mu)P \\
&= (r+1)P.
\end{aligned}$$

□

Corollary 8 *Let $\nu \geq 1$ be an integer and P be a point of finite order μ. Write $\nu = q(\mu - 1) + r$ with $q, r \in \mathbb{Z}$ and $1 \leq r \leq \mu - 1$. Then*

$$\varphi_\nu(f_\infty) = \rho_\nu(\infty) f_{(r+1)P}.$$

Proof: This follows directly from Proposition 4 and the fact that $\infty = -\nu_0 P$ when $\nu_0 = 0$. □

From Corollary 1 we know that if α is a quadratic irrational then the following hold.

1. If the continued fraction expansion of α is quasi-periodic with odd quasi-period m, then it is periodic with period n and $n = m$ or $n = 2m$.
2. If the continued fraction expansion of α is periodic with odd period, then it is quasi-periodic with quasi-period $m = n$.

Theorem 30 *Let $Q \neq P$ be any k-rational point on E. Then the continued fraction expansion of f_Q is quasi-periodic. Indeed, it is pure quasi-periodic. Moreover, if P has order μ and the continued fraction expansion of f_Q has quasi-period $m(Q)$ then*

$$\mu = \begin{cases} m(Q) + 1 & \text{if } -Q = \nu_0 P,\ \nu_0 \geq 0 \\ \\ m(Q) & \text{otherwise.} \end{cases}$$

Proof: Let P have finite order μ. Then if $-Q$ is not a non-negative multiple of P,

$$\psi_\mu(Q) = Q \oplus 0P = Q.$$

So $\varphi_\mu(f_Q) = \rho_\mu(Q) f_{\psi_\mu(Q)} = \rho_\mu(Q) f_Q$. Thus, f_Q has pure quasi-period $m(Q) \leq \mu$.

If $-Q = \nu_0 P$ for $0 \leq \nu_0 < \mu - 1$, then

$$\psi_{\mu-1}(Q) = (\mu - \nu_0)P = \mu P - \nu_0 P = Q.$$

So

$$\begin{aligned} \varphi_{\mu-1}(f_Q) &= \rho_{\mu-1}(Q) f_{\psi_{\mu-1}(Q)} \\ &= \rho_{\mu-1}(Q) f_Q \end{aligned}$$

and f_Q has pure quasi-period $m(Q) \leq \mu - 1$.

Now $m(Q) \leq \mu$ (resp. $\mu - 1$). Since $m(Q)$ is the quasi-period of f_Q

$$\varphi_{m(Q)}(f_Q) = \rho_{m(Q)}(Q) f_{\psi_{m(Q)}(Q)} = c f_Q$$

for some $c \in k^*$. Then $\psi_{m(Q)}(Q) = Q$ by the uniqueness of f_Q. This is only possible when $m(Q) = \mu$ (resp. $\mu - 1$). □

Theorem 31 *Let P have order μ, let $\nu_0 \not\equiv 1 \pmod{\mu}$ be an integer, and let n be the period of the continued fraction expansion of $f_{\nu_0 P}$. Then*

$$n = \begin{cases} \mu - 1 & \text{if } \rho_{\mu-1}(\nu_0 P) = 1 \\ 2(\mu - 1) & \text{if } \rho_{\mu-1}(\nu_0 P) \neq 1 \end{cases}$$

where the second case can only occur if μ is even.

Proof: We can assume without loss of generality that $2 \leq \nu_0 \leq \mu$, and let $Q = \nu_0 P$. Then the continued fraction expansion of f_Q has pure quasi-period $\mu - 1$. Of course if $\rho_{\mu-1}(Q) = 1$, then $n = \mu - 1$. If μ is even, then $\mu - 1$ is odd and so the period of f_Q must be either $n = \mu - 1$ or $n = 2(\mu - 1)$.

We must show that if μ is odd, then $\rho_{\mu-1}(Q) = 1$. Since we are in Case 2,

$$\psi_j(Q) = \psi_j((\nu_0 - \mu)P) = \begin{cases} (j+\nu_0)P & \text{if } 0 \le j \le \mu - \nu_0 \\ \\ (j+\nu_0+1)P & \text{if } \mu - \nu_0 < j \le \mu - 2. \end{cases}$$

So,

$$\begin{aligned} \rho_{\mu-1}(\nu_0 P) &= \prod_{j=0}^{\mu-2} \lambda(\psi_j(\nu_0 P))^{(-1)^{\mu-2-j}} \\ &= \prod_{j=0}^{\mu-\nu_0} \lambda((j+\nu_0)P)^{(-1)^{\mu-2-j}} \prod_{j=\mu-\nu_0+1}^{\mu-2} \lambda((j+\nu_0+1)P)^{(-1)^{\mu-2-j}} \\ &= \prod_{i=\nu_0}^{\mu} \lambda(iP)^{(-1)^{\mu-2-i+\nu_0}} \prod_{i=\mu+2}^{\mu+\nu_0-1} \lambda(iP)^{(-1)^{\mu-1-i+\nu_0}} \\ &= \prod_{i=\nu_0}^{\mu} \lambda(iP)^{(-1)^{i-\nu_0+1}} \prod_{i=\mu+2}^{\mu+\nu_0-1} \lambda(iP)^{(-1)^{i-\nu_0}} \\ &= \prod_{i=2}^{\mu-2} \lambda(iP)^{(-1)^{i-\nu_0+1}} \lambda(-P)^{(-1)^{\mu-\nu_0}} \lambda(\infty)^{(-1)^{\mu-\nu_0+1}} \\ &= 1, \end{aligned}$$

since $\lambda(iP) = \lambda((\mu - i)P)$ and $\lambda(-P) = \lambda(\infty)$. □

Corollary 9 *The continued fraction expansion of Y is periodic. If the order of P is μ and the period of Y is n, then*

$$n = \begin{cases} \mu - 1 & \text{if } \rho_{\mu-1}(\infty) = 1 \\ \\ 2(\mu-1) & \text{if } \rho_{\mu-1}(\infty) \neq 1 \end{cases}$$

where the second case can only occur when μ is even.

Proof: Notice that

$$f_\infty + Y = x + a + Y$$

$$= X^2 + Y + a_2 + a + Y$$
$$= X^2 + a_2 + a.$$

So the continued fraction expansion for Y differs from that of f_∞ only in the first term. Thus for all $\nu \geq 1$,

$$\varphi_\nu(Y) = \varphi_\nu(f_\infty).$$

The result now follows from Theorem 31. □

7.5 The Discrete Logarithm Problems

This section shows an equivalence between two types of discrete logarithm problems using underlying fields of characteristic 2 for which implementations of Diffie-Hellman [13] and ElGamal [14] type cryptosystems have been based. These are the *elliptic discrete logarithm problem* and the *infrastructure discrete logarithm problem.* The equivalence follows from the next two theorems.

Theorem 32 *Let E be a non-supersingular elliptic curve defined over $k = F_{2^M}$ and let P be a point on the curve. Let E_P be the quadratic model for E which defines the quadratic function field $K = k(X)(Y)$. If the elliptic discrete logarithm problem for E can be solved in polynomial time, then the infrastructure discrete logarithm problem for E_P can also be solved in polynomial time.*

Proof: Let $\mathcal{A}$ be a primitive reduced ideal in $\mathcal{O}$. If $\mathcal{A} = \mathcal{O}$, then the solution to the infrastructure discrete logarithm problem is $\delta(\mathcal{A}, \mathcal{O}) = 0$.

We will therefore assume that $\mathcal{A} = [X + X_0, \overline{Y_0} + Y]$ is the ideal in adapted form for some $X_0, \overline{Y_0} \in k$. Let $Y_0 = X_0^2 + X_0 + a + a_2 + \overline{Y_0}$. Then

$$\mathcal{A} = [X + X_0, X_0^2 + X_0 + a + a_2 + Y_0 + Y].$$

Since $\mathcal{A}$ is an ideal, $X + X_0 | \overline{Y_0}^2 + (X^2 + X + a + a_2)\overline{Y_0} + (X^3 + a_2 X + a^2 + b + a)$ and thus, $(X_0, \overline{Y_0})$ is a solution to the equation E_P. Notice that $\overline{Y_0} = Y_0^*$, so (X_0, Y_0) is also a solution to the equation E_P. Let $Q = (x_0, y_0)$ be the corresponding point on E using the formulae of Section 7.3. Notice that $Q \neq P, \infty$.

Let (X_i, Y_i) be a solution to the equation E_P corresponding to $iP \in E$, $iP \neq \infty, P$. We will assume that $2 \leq i < \mu$ where μ is the order of P. By Theorem 30 we know that $\mu - 1$ is the quasi-period of Y. Now

$$\varphi_{i-1}(Y) = \varphi_{i-1}(f_\infty) = \rho_{i-1}(\infty) f_{\psi_{i-1}(\infty)} = \rho_{i-1}(\infty) f_{iP}.$$

If $\alpha_0 = Y = \frac{0+Y}{1}$ then $\varphi_{i-1}(Y) = \alpha_{i-1} = \frac{P_{i-1}+Y}{Q_{i-1}}$ since φ just performs one step in the continued fraction algorithm. Thus,

$$\frac{P_{i-1} + Y}{Q_{i-1}} = \rho_{i-1}(\infty) \frac{X^2 + X_i + a + a_2 + Y_i + Y}{X + X_i}.$$

This implies that

$$\begin{aligned} P_{i-1} &= X^2 + X_i + a + a_2 + Y_i \\ Q_{i-1} &= \frac{1}{\rho_{i-1}(\infty)} (X + X_i). \end{aligned}$$

So, we get the reduced ideal in adapted form

$$\mathcal{A}_i = [X + X_i, X_i^2 + X_i + a + a_2 + Y_i + Y].$$

Thus, if $X_i = X_0$ and $Y_i = Y_0$ then $Q = iP$ and also $\mathcal{A}_i = \mathcal{A}$, and if no such X_i and Y_i exist, then $\delta(\mathcal{A}, \mathcal{O})$ does not exist. Now

$$\delta(\mathcal{A}_i, \mathcal{O}) = \deg(B) - \deg(Q_0) + \sum_{j=1}^{i-2} \deg(a_j)$$

$$= 2 - 0 + (i - 2)$$
$$= i$$

since for $1 \leq j < \mu - 1$, $\deg(a_j) = 1$.

If we can solve the elliptic discrete logarithm problem on E, (e.g. find $i \geq 2$ such that $iP = Q$ or determine that no such i exists) then we can solve the infrastructure discrete logarithm problem. Since x_0 and y_0 can be computed in polynomial time, the infrastructure discrete logarithm problem can be computed in polynomial time if the elliptic discrete logarithm problem can be solved in polynomial time. □

Theorem 33 *Let E be a non-supersingular elliptic curve defined over $k = F_{2^M}$ and let P be a point on the curve. Let E_P be the quadratic model for E which defines the quadratic function field $K = k(X)(Y)$. If the infrastructure discrete logarithm problem for E_P can be solved in polynomial time, then the elliptic discrete logarithm problem for E can also be solved in polynomial time.*

Proof: Let Q be a point on E. If $Q = \infty$ then the solution to the elliptic discrete logarithm problem is 0. If $Q = P$ then the solution to the elliptic discrete logarithm problem is 1.

We will assume that $Q = (x_0, y_0)$ is the point on E, and that (X_0, Y_0) is the corresponding solution to the equation E_P. Now let $\mathcal{A} = [X + X_0, X_0^2 + X_0 + a + a_2 + Y_0 + Y]$ be a primitive reduced ideal. As was shown in the proof to Theorem 32, if we can find $\delta(\mathcal{A}, \mathcal{O})$ or determine that it does not exist, then we have found i such that $Q = iP$ or determined that such an i does not exist. Again, we are able to compute X_0 and Y_0 in polynomial time, so if the infrastructure discrete logarithm problem can be solved in polynomial time then so can the elliptic discrete logarithm problem. □

We have just shown that solving the elliptic discrete logarithm problem on E is equivalent to solving the infrastructure discrete logarithm problem on E_P. A discussion of the difficulty of solving the infrastructure discrete logarithm problem appears in Section 6.3. None of the methods discussed there combined with this correspondence give an improvement over known methods for solving the elliptic logarithm problem. Since we know of no other way of solving the infrastructure discrete logarithm problem, this provides further evidence of the intractability of the elliptic discrete logarithm problem.

It is easy to see that the proofs of the above theorems give a bijection between the sets

$$\{Q \in E \mid Q = iP, 2 \leq i \leq \mu - 1\}$$

and

$$\{\mathcal{A} \subset \mathcal{O}, \mathcal{A} \neq \mathcal{O} \mid \mathcal{A} \text{ can be obtained from the continued fraction expansion of } \mathcal{O}\}$$

and that $\mu - 1$ equals the quasi-period, m, of the continued fraction expansion of Y. Now, since $R = \delta_{m+1} = m + 1$, we get that R is also the order of P.

Thus, computing the order of a point, P, on E is equivalent to finding the regulator of the function field defined by E_P. Also, producing a point on a curve with a given order is equivalent to producing a function field of the form given by E_P with a given regulator. The problem of finding curves and points with large prime order is of great interest in elliptic curve cryptography. Thus, it would be of interest if we could efficiently compute regulators of such fields. Stein has observed that in the odd characteristic case there are certain classes of function fields that tend to have large order [48]. At the present time it is unclear if there is a characteristic 2 analog of these classes.

7.6 Some Examples

In this section we will consider some examples of quadratic function fields for which the infrastructure discrete logarithm problem is equivalent to the discrete logarithm problem in an elliptic curve group.

7.6.1 Example 1

Consider the function field presented in Section 5.5.1. We have $k = F_{2^3} = F_2(\delta)$ where $\delta^3 + \delta + 1 = 0$ and $K_1 = k(X)(Y)$ defined by

$$E_P : Y^2 + (X^2 + X + \delta)Y = X^3 + \delta.$$

Also, $d = [Y] = X$.

Using the formulae from Section 7.3 we see that $a_2 = 0$, $a = \delta$ and $b = \delta^2$. The elliptic curve is

$$E : y^2 + xy = x^3 + \delta^4$$

and the point is $P = (\delta, \delta^2)$.

From Section 5.5.1 we have that $\mathcal{A}_2 = [X + 1, \delta^3 + Y]$, so we have $X_2 = 1$ and $\overline{Y_2} = \delta^3$. Now $\overline{Y_2} = X_2^2 + X_2 + a + a_2 + Y_2$, so $Y_2 = 1 + 1 + \delta + \delta^3 = 1$. Converting (X_2, Y_2) into a point on the elliptic curve E, we get $(0, \delta^2)$. Using the addition formula for elliptic curves we get $2P = (0, \delta^2)$, as we would expect.

We also had $\mathcal{A}_3 = [X + 1, 1 + Y]$, so $X_3 = 1$ and $\overline{Y_3} = 1$. We need Y_3, so

$$\begin{aligned} Y_3 &= X_3^2 + X_3 + a + a_2 + \overline{Y_3} \\ &= 1 + 1 + \delta + 1 \\ &= \delta + 1. \end{aligned}$$

We need the point on the elliptic curve corresponding to (X_3, Y_3); this point is (δ, δ^4). When we compute $2P \oplus P$ we also get $3P = (\delta, \delta^4)$.

Since $\mathcal{A}_4 = [1, Y] = \mathcal{A}_1$, we have computed all of the multiples of P that can be computed using the continued fraction expansion. The point P satisfies $4P = \infty$ as we would expect, since for this field $R = 4$.

7.6.2 Example 2

For this example, assume $k = F_{2^3} = F_2(\delta)$ where $\delta^3 + \delta + 1 = 0$. Let $K_3 = k(X)(Y)$ where X and Y satisfy

$$E_P : Y^2 + (X^2 + X + \delta^5)Y = X^3 + \delta^3 X + \delta^5.$$

Clearly $a_2 = \delta_3$, $a = \delta^2$ and $b = \delta^6$. The elliptic curve is

$$E : y^2 + xy = x^3 + \delta^3 x^2 + 1$$

and the point on the curve is $P = (\delta^2, \delta^6)$.

Table 7.1 shows the correspondence between the infrastructure discrete logarithm and elliptic curve discrete logarithm for this field. It gives, for each $2 \leq i \leq 7$, P_{i-1}, Q_{i-1}, X_i, $\overline{Y_i}$, Y_i, and iP.

Performing one more Baby-Step gives $Q_7 = \delta^4 X = Q_6$, so by Theorem 11, the quasi-period is $m = 13$. Now, $R = m + 1 = 14$, and so we would expect that $14P = \infty$. In fact, $2(7P) = \infty$.

i	P_{i-1}	Q_{i-1}	X_i	$\overline{Y_i}$	Y_i	iP
2	$X^2+\delta^5$	$\delta^2X+\delta^5$	δ^3	δ	δ^3	(δ^6,δ)
3	$X^2+\delta^4$	$\delta^5X+\delta^2$	δ^4	δ^2	δ^5	(δ^4,δ^4)
4	$X^2+\delta^6$	$\delta^3X+\delta^2$	δ^6	δ	δ^5	(δ^3,δ^5)
5	X^2	$\delta^2X+\delta^3$	δ	δ^2	δ^6	(δ,δ^4)
6	X^2+1	$\delta^2X+\delta^4$	δ^2	δ^5	δ	(δ^5,δ^4)
7	$X^2+\delta^2$	δ^4X	0	δ^2	δ^3	$(0,1)$

Table 7.1: The elliptic curve equivalence for K_3.

Chapter 8

Implementation And Practical Results

8.1 Running Times and Security Considerations for the Cryptosystem Over $\mathbb{Z}_n$

In [23] an algorithm similar to the one given in Section 2.6 is implemented to produce curves of a given order modulo a prime p. A curve with order twice a 51 decimal digit prime is computed in just over 6 minutes using the computer algebra system SIMATH. It therefore seems feasible to compute elliptic curves of a given order and to use similar techniques as described in Section 2.6 to compute curves of smooth order.

In Section 2.5 a method to produce a prime and an elliptic curve modulo that prime with smooth order was given. From arguments in that section, the majority of the work to produce 75 digit primes and their associated curves would be to

perform approximately 10 elliptic curve factorizations to determine smoothness of 38 digit integers and approximately 2000 primality tests for 75 digit integers. Assuming 1 minute on each factorization, this could be completed in less than an hour, which is a feasible one time start up cost.

Once two elliptic curves with smooth order have been computed, say $E_p(a_p, b_p)$ and $E_q(a_q, b_q)$, one can produce a curve over $\mathbb{Z}_n$ with the desired properties. Using the Chinese Remainder Theorem one computes $a, b \in \mathbb{Z}_n$ such that $a \equiv a_p \pmod{p}$, $a \equiv a_q \pmod{q}$, $b \equiv b_p \pmod{p}$ and $b \equiv b_q \pmod{q}$. The curve is $E_n(a, b)$.

Decryption is performed using the Pohlig-Hellman algorithm with the Baby-Step Giant-Step algorithm and the trapdoor information p and q. For a curve with order a 75-digit integer divisible by one 16 digit prime and the remaining prime factors less than 16 digits, this decryption will take approximately 10^8 elliptic curve operations (additions and doublings). Assuming that a special purpose device is used to decrypt at 100,000 elliptic curve operations in a second, decryption would take a few minutes to perform. Although feasible, this is not useful for decrypting large amounts of data. It may be suitable for certain key agreement schemes where one-time encryption is needed.

It is easy to see that recovering a message $\tilde{M}$ given $Q = \tilde{M}P$ in any of the above schemes is equivalent to solving the discrete logarithm problem on the curve modulo n. The security of the system is dependent on the discrete log problem being difficult.

The integer n was chosen so that general purpose factoring algorithms are not feasible. The elliptic curve factoring algorithm may however be used to factor n. Assume that the order of our public point P is divisible by 16 digit primes

modulo p and modulo q. Then by computing $\left(\prod_{p<10^{16}} p\right) P$ one prime at a time, the factorization of n can be obtained (see [24]). This would require approximately $\sum_{p<10^{16}} \log_2 p \sim 10^{16}$ elliptic curve operations. The work required to factor is 10^8 more operations than required by the signer. Assuming that one could decrypt in 1 minute (which is optimistic with present technology), factoring n by this method would take about 190 years. As our ability to compute discrete logarithms improves, we will be able to use curves divisible by larger primes. If the curves are smooth with respect to 10^k then decryption will take on the order of $10^{k/2}$ operations and factoring n will take about 10^k operations. Thus, as k increases so will the factor of extra work required to break the system.

A further problem that could occur with this system is that if two messages $\tilde{M}_1$ and $\tilde{M}_2$ are sent with $\tilde{M}_1 - \tilde{M}_2$ a small integer, then upon computing $\tilde{M}_1 P - \tilde{M}_2 P = (\tilde{M}_1 - \tilde{M}_2)P$ an eavesdropper could determine $\tilde{M}_1 - \tilde{M}_2$ using exhaustive search and thus obtain information about the messages. For example, if $\tilde{M}_1$ and $\tilde{M}_2$ consist of 8 bit fields with only one field differing, information could be obtained about the value of this field. In order to combat this attack, 56 bits of the public point could be used as a DES [35] key K. Then to encrypt the message $\tilde{M}$ let the ciphertext be $\mathrm{DES}_K(\tilde{M})P$ where $\mathrm{DES}_K(\tilde{M})$ is DES applied to $\tilde{M}$ using the key K. Now, $\mathrm{DES}_K(\tilde{M}_1)P - \mathrm{DES}_K(\tilde{M}_2)P$ has no special structure. In fact, any encryption algorithm E such that $E(\tilde{M}_1) - E(\tilde{M}_2) \neq E(\tilde{M}_1 - \tilde{M}_2)$ could be used.

8.2 Running Time and Implementation of Regulator Algorithms

We present details of the running times and implementation of the algorithms presented in Section 5.4 for computing the regulator. We are in the same situation as Chapter 5, so k is a field with $q = 2^M$ elements and X is transcendental over k. Now $K = k(X)(Y)$ where $Y^2 + BY = C$ for some $B, C \in k[X]$ with C monic. Also $Y^2 + BY + C = 0$ has no singular points $(X, Y) = (u, v) \in \overline{k} \times \overline{k}$ and $K \subseteq k((\frac{1}{X}))$.

Recall $\mathcal{O} = [1, Y]$. Let h' be the ideal class number of $\mathcal{O}$ and let h be the divisor class number of K. Also let g be the genus of the curve $Y^2 + BY = C$. Then it appears that a result of Schmidt [42] also applies here:

$$h = Rh'.$$

From [53, Proposition III.7.8] we can see that K is an Artin-Schreier extension and that

$$g \leq \deg(B) - 1.$$

It is well known (see [53]) that the *L-polynomial*, $L(t)$, of K satisfies

1. $L(1) = h$.
2. $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ where $\alpha_1, \ldots, \alpha_{2g}$ are algebraic integers.
3. $|\alpha_i| = q^{\frac{1}{2}}$ for $i = 1, \ldots, 2g$. (This is the Hasse-Weil Theorem.)

Thus, $(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}$ and we conclude that $h = O(q^{\deg(B)})$. Since $h = Rh'$, we get

$$R = O\left(q^{\deg(B)}\right).$$

Now, notice that $\deg(B) + (i-2) \leq \delta_i \leq (i-1)\deg(B)$ for all $i \geq 2$. Since $R = \delta_{m+1}$, we then get $\frac{R}{\deg(B)} \leq m \leq R - \deg(B) + 1$, so $m = O(R)$. Finally, we conclude

$$m = O\left(q^{\deg(B)}\right).$$

Thus, the optimal choice for the number of Baby-Steps and Giant-Steps is

$$O \approx O\left(q^{\frac{1}{2}\deg(B)}\right).$$

Now, all operations in a Baby-Step and Giant-Step are polynomial operations performed in k. We know also that all polynomials involved in these operations are bounded by $\deg(B)$ or $\frac{1}{2}\deg(C)$. Thus, the complexity of a Baby-Step and of a Giant-Step is bounded by a polynomial in $\log(q)$, $\deg(B)$ and $\deg(C)$.

So the total complexity to find R is

$$O(q^{\frac{1}{2}\deg(B)+\epsilon})$$

polynomial operations.

Tables 8.1 and 8.2 give the times to find the regulators of quadratic function fields defined by $Y^2 + BY = C$ over F_{2^M} for various values of M between 2 and 10. For all function fields, the degree of the polynomial C was 3 and the polynomial was constant for all trials with a given field size 2^M. The routines were written in C on a SPARC 20 running SunOS 4.1.4. The column M gives the degree of the field extension, $\deg(B)$ gives the degree of the polynomial B, Opt. G.B. gives the time to perform the Optimized Giant-Step Baby-Step algorithm, Baby gives the time to find the regulator using just the Baby-Step algorithm and no information about symmetry, R gives the regulator and m gives the quasi-period of the continued fraction expansion.

M	deg(B)	Opt. G.B.	Baby	R	m
2	3	.01 s	.01 s	24	18
2	4	.01 s	.01 s	10	7
2	5	.01 s	.01 s	27	12
2	6	.01 s	.02 s	50	30
2	7	.24 s	.84 s	1622	1214
2	8	.42 s	3.84 s	9078	6764
2	9	.88 s	18.36 s	36 111	27 150
2	10	2.15 s	4.49 s	10 221	7 636
2	11	4.8 s	1 m 6.05 s	113 535	84 954
2	12	10.46 s	12 m 11.59 s	1 193 199	894 728
2	14	1 m 14.58 s	12 h 30 m 57.85 s	62 150 892	46 614 415
2	15	1 m 39.07 s	9 h 26 m 54.31 s	44 190 784	33 144 168
2	15	1 m 25.89 s	2 h 7 m 34.09 s	9 914 639	7 441 130
2	16	3 m 17.77 s	12 h 54 m 46.49 s	57 561 629	43 173 458
2	16	2 m 57.37 s	6 h 23 m 0.46 s	28 494 758	21 373 264
3	4	.10 s	.16 s	341	296
3	6	.14 s	.24 s	591	514
3	8	7.25 s	2 m 12.75 s	225 214	196 672
3	10	1 m 15.01 s	3 h 4 m 50.21 s	15 088 794	13 203 808
3	10	1 m 20.38 s	8 h 1 m 14.01 s	39 603 476	34 655 407

Table 8.1: Times for computing regulators using Baby-Step and Optimized Giant-Step Baby-Step algorithms.

M	deg(B)	Opt. G.B.	Baby	R	m
4	3	.03 s	.03 s	109	100
4	4	.04 s	.06 s	163	156
4	5	.82 s	.98 s	2 236	2 088
4	6	6.73 s	1 m 9.73 s	126 240	118 481
4	7	35.93 s	2 h 59 m 2.71 s	16 964 951	15 904 783
4	7	32.03 s	56 m 5.76 s	5 576 825	5 228 167
4	8	2 m 47.63 s	2 d 14 h 38 m 54.88 s	317 911 602	298 042 663
4	8	2 m 18.03 s	6 h 0 m 3.49 s	30 394 684	28 494 664
5	4	1.41 s	4.41 s	8 424	8 154
5	6	59.54 s	41 m 33.38 s	4 014 324	3 888 694
5	6	1 m 1.38 s	34 m 29.46 s	3 206 647	3 106 044
6	3	.36 s	.40 s	1 239	1 211
6	4	6.23 s	1 m 9.63 s	153 898	151 425
6	5	52.55 s	18 m 6.77 s	1 927 877	1 897 221
6	5	55.26 s	1 h 31 m 48.29 s	9 718 005	9 565 921
10	3	45.88 s	8 m 4.78 s	1 027 173	1 026 169
10	3	48.37 s	3 m 33.5 s	508 172	507 648

Table 8.2: Times for computing regulators using Baby-Step and Optimized Giant-Step Baby-Step algorithms (cont'd).

8.3 Implementation of the Function Field Key Exchange

We implemented the **Diffie-Hellman Key Exchange** algorithm using the C programming language on a SPARC 20 running SunOS 4.1.4. All of our computations were done over finite fields with 2^M elements that contained an optimal normal basis for increased efficiency [34].

We attempted to choose M, B and C such that $q^{\deg(B)} \approx 10^{100}$ as was suggested in Section 6.3 to avoid brute force and subexponential attacks. Our restriction to finite fields that contained optimal normal bases meant that we chose our parameters such that $10^{92} < q^{\deg(B)} < 10^{120}$. The polynomial C was kept constant with degree 3 for all examples and the degree of B was varied as was the degree of the field extension. In this implementation, the private keys were chosen at random in the range $\left[1, q^{\frac{\deg(B)}{2}}\right]$, as was suggested in Section 6.1.

Tables 8.3 and 8.4 give the results of this implementation. The first column gives the degree of B and the second column gives the degree of the field extension. The approximate work required to obtain the regulator R is given in the next column. This is $q^{\frac{\deg(B)}{2}}$. Finally, the time for each party to compute the common key is displayed. While these times are not quite as impressive as those given in [41] for fields of odd characteristic, there appears to be much room for improvement by making use of more advanced coding techniques.

$\deg(B)$	M	$q^{\frac{\deg(B)}{2}}$	Time
30	11	4.7×10^{49}	145.7 sec
29	11	1.0×10^{48}	137.9 sec
28	12	3.7×10^{50}	130.3 sec
27	12	5.8×10^{48}	119.2 sec
26	12	9.1×10^{46}	106.4 sec
25	14	4.8×10^{52}	115.1 sec
24	14	3.7×10^{50}	94.7 sec
23	14	2.9×10^{48}	101.1 sec
22	18	4.0×10^{59}	148.6 sec
21	18	7.8×10^{56}	135.3 sec
20	18	1.5×10^{54}	122.9 sec
19	18	2.9×10^{51}	104.8 sec
18	18	5.8×10^{48}	79.6 sec
17	23	7.1×10^{58}	104.3 sec
16	23	2.5×10^{55}	81.1 sec

Table 8.3: Times for **Diffie-Hellman Key Exchange** Implementation.

$\deg(B)$	M	$q^{\frac{\deg(B)}{2}}$	Time
15	23	8.5×10^{51}	74.3 sec
14	23	2.9×10^{48}	56.7 sec
13	26	7.5×10^{50}	49.5 sec
12	28	3.7×10^{50}	38.4 sec
11	30	4.7×10^{49}	35.5 sec
10	33	4.7×10^{49}	49.9 sec
9	39	6.8×10^{52}	43.8 sec
8	41	2.3×10^{49}	37.7 sec
7	50	4.8×10^{52}	40.0 sec
6	58	2.4×10^{52}	25.3 sec
5	66	4.7×10^{49}	35.6 sec
4	83	9.4×10^{49}	27.8 sec
3	113	1.1×10^{51}	25.5 sec
2	172	6.0×10^{51}	14.6 sec

Table 8.4: Times for **Diffie-Hellman Key Exchange** Implementation (cont'd).

Chapter 9

Suggestions for Further Research

We will now present some suggestions for further research based on results contained in this thesis.

1. In order to make the cryptosystem described in Chapter 3 that uses elliptic curves over $\mathbb{Z}_n$ more feasible, it is of great interest to be able to produce elliptic curves with a given group order more efficiently. A related problem which would serve the same goal is to improve methods for counting points on elliptic curves. These problems are interesting also because all cryptosystems using elliptic curves require the knowledge of the number of points on the curve being used.

2. The cryptosystem in Chapter 3 uses the fact that it is not possible to efficiently obtain the order of $E_n(a, b)$ if the factorization of n is not known. This is because the present methods for counting points on elliptic curves (Schoof's, Atkin's and Elkies' algorithms) do not work in $\mathbb{Z}_n$. It is not known however what effect these algorithms have on the curve $E_n(a, b)$ and what information can be obtained concerning these curves. For example, is it possible to

identify elliptic curves over $\mathbb{Z}_n$ for which the discrete logarithm problem has a trapdoor?

3. The basic operations performed in the infrastructure of quadratic function fields are the Baby-Step and the Giant-Step. At present, these operations are relatively costly to perform. Arithmetic in the infrastructure would be more feasible if more efficient algorithms for performing these operations were found.

4. Chapter 5 presents a method to find the regulator of a quadratic function field that runs in time $O(q^{\frac{1}{2}\deg(B)+\epsilon})$. More efficient algorithms for finding the regulator of such function fields would be useful. Because of the correspondence with elliptic curves presented in this thesis, this may also give a method for efficiently counting points on elliptic curves.

   In [49] a method is given that determines the regulator of quadratic function fields of odd characteristic in $O(q^{\frac{1}{5}\deg(D)+\epsilon})$ operations where $Y^2 = D(X)$ defines the function field. It is unclear if this method generalizes to function fields of even characteristic.

5. The cryptosystem introduced in Chapter 6 is based on the difficulty of computing infrastructure discrete logarithms. Does a subexponential algorithm exist for computing these discrete logarithms? If such an algorithm does exist, then this would also give a subexponential algorithm for finding elliptic curve discrete logarithms.

6. In Chapter 7 an equivalence is shown between the infrastructure discrete logarithm for function fields of a certain type and non-supersingular elliptic curve discrete logarithms. Does an equivalence of this type exist for hyperelliptic

curves of higher genus? If it does, then the infrastructure of a function field would be the "same" as the jacobian of a hyperelliptic curve. This would give a different way of studying these curves of higher genus which have also been proposed for cryptographic purposes.

7. The equivalence presented in Chapter 7 was for non-supersingular elliptic curves in characteristic 2 only. Does such an equivalence also exist for supersingular elliptic curves in even characteristic? One would suspect that it would, but what is the corresponding quadratic model?

8. Do there exist certain classes of function fields (and hence elliptic curves) whose regulators tend to be of an "interesting" type? Interesting types could include smooth with respect to a bound B or divisible by a large prime. There are results that certain classes of number fields tend to have large regulators, but nothing has been proven for function fields. Stein [48] has obtained some empirical results for odd characteristic function fields.

Appendix A

We will now give a proof that the conditions given for our quadratic function fields in Section 4.1 are equivalent to the curve having no singular points.

Theorem 34 *Let $B, C \in k[X]$ where k is a field of characteristic 2. Then $y^2 + By + C \equiv 0 \pmod{D^2}$ does not have a solution with $y \in k[X]$ for each non-constant polynomial, D, that divides B if and only if $Y^2 + BY + C = 0$ has no singular points $(X, Y) = (u, v) \in \overline{k} \times \overline{k}$.*

Proof: ($\Rightarrow$) Let $(u, v) \in \overline{k} \times \overline{k}$ be a singular point on $F(X, Y) = Y^2 + BY + C = 0$. This means that

$$\left.\frac{\partial F}{\partial X}\right|_{(X,Y)=(u,v)} = B'(u)v + C'(u) = 0$$

and

$$\left.\frac{\partial F}{\partial Y}\right|_{(X,Y)=(u,v)} = B(u) = 0.$$

Let $D(X)$ be the minimal polynomial for u over k. Then $D(X)|B(X)$.

Let $y = B(X) + v \in k[X]$. Then

$$\begin{aligned} y^2 + B(X)y + C(X) &= B^2(X) + v^2 + B^2(X) + B(X)v + C(X) \\ &= v^2 + B(X)v + C(X). \end{aligned}$$

Let $f(X) = v^2+B(X)v+C(X)$. Since (u, v) is a point on $Y^2+BY+C = 0$, we know $v^2 + B(u)v + C(u) = 0$ and thus $D(X)|f(X)$. Also note $f'(X) = B'(X)v + C'(X)$, so $f'(u) = B'(u)v + C'(u) = 0$. Hence $D^2(X)|f(X)$.

Thus,

$$f(X) = y^2 + B(X)y + C(X) \equiv 0 \pmod{D^2(X)}$$

where $y \in k[X]$ as defined.

($\Leftarrow$) Let $D(X)|B(X)$ and $y \in k[X]$ be such that

$$y^2 + B(X)y + C(X) \equiv 0 \pmod{D^2(X)}.$$

Then

$$g(X) = y^2 + B(X)y + C(X) + D^2(X)Q(X) = 0$$

for some $Q(X) \in k[X]$.

Let u be any root of $D(X)$ in $\overline{k}$ and $v = y(u)$. Then

$$g(u) = v^2 + B(u)v + C(u) + 0 = 0$$

and so (u, v) is on the curve $Y^2 + BY + C = 0$. In fact, since $D(u) = 0$, we also know $B(u) = 0$.

Now, since $g(X) = 0$, it is also true that $g'(X) = 0$ and thus

$$B'(X)y + y'B(X) + C'(X) + D^2(X)Q'(X) = 0.$$

Also, then $g'(u) = 0$ and so

$$B'(u)v + 0 + C'(u) + 0 = 0.$$

Hence (u, v) is a point on the curve that satisfies both partial derivatives. It is therefore a singular point on $Y^2 + BY + C = 0$. □

Appendix B

Theorem 35 *Let $\mathcal{A}$ be an integral $\mathcal{O}$-ideal. Every $k[X]$-basis of $\mathcal{A}$ has exactly two elements.*

Proof: Let $\mathcal{A} = [\omega]$ for some $\omega \in \mathcal{O}$. Either $\omega \in k[X]$ or $\omega \in \mathcal{O} \setminus k[X]$.

If $\omega \in k[X]$, then $\omega Y \in \mathcal{A}$ as well. It is not possible to write $\omega Y = \omega\alpha$ for any $\alpha \in k[X]$ though, so $\omega \in \mathcal{O} \setminus k[X]$. Let $\omega = a + bY$ for $a, b \in k[X]$, $b \neq 0$. Then $N(\omega) \in k[X]$ is in $\mathcal{A}$ as well. Again, it is impossible to write $N(\omega) = \omega\alpha$ for any $\alpha \in k[X]$. Thus, it is not possible for $\mathcal{A} = [\omega]$.

Let $\omega_1, \omega_2, \omega_3 \in \mathcal{O}$ be in the $k[X]$-basis for $\mathcal{A}$. Then $\omega_i = a_i + b_i Y$ where $a_i, b_i \in k[X]$ for $i = 1, 2, 3$ and $\omega_1, \omega_2, \omega_3$ are linearly independent. Now let

$$\begin{aligned} \lambda_1 &= a_3^2 b_2 + a_2 a_3 b_3 \neq 0 \\ \lambda_2 &= a_3^2 b_1 + a_1 a_3 b_3 \neq 0 \\ \lambda_3 &= a_1 a_3 b_2 + a_2 a_3 b_1 \neq 0 \end{aligned}$$

and notice that

$$\lambda_1\omega_1 + \lambda_2\omega_2 + \lambda_3\omega_3 = 0.$$

Thus, $\omega_1, \omega_2, \omega_3$ cannot be linearly independent and so a $k[X]$-basis for $\mathcal{A}$ cannot have any more that 2 elements. □

Bibliography

[1] W.A. Adams and M.J. Razar, Multiples of points on elliptic curves and continued fractions, *Proceedings of the London Mathematical Society* **41** (1980), pp. 481-498.

[2] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I., *Mathematische Zeitschrift* **19** (1924), pp. 153-206.

[3] A.O.L. Atkin, The number of points on an elliptic curve modulo a prime, manuscript, 1991.

[4] A.O.L. Atkin and F. Morain, Elliptic curves and primality proving, *Mathematics of Computation* **61** (1993), pp. 29-68.

[5] E. Bach, Explicit bounds for primality testing and related problems, *Mathematics of Computation* **55** (1990), pp. 355-380.

[6] L.E. Baum and M.M. Sweet, Continued fractions of algebraic power series in characteristic 2, *Annals of Mathematics* **103** (1976), pp. 593-610.

[7] L.E. Baum and M.M. Sweet, Badly approximable power series in characteristic 2, *Annals of Mathematics* **105** (1977), pp. 573-580.

[8] E.R. Canfield, P. Erdös, and C. Pomerance, On a problem of Oppenheim concerning 'Factorisatio Numerorum' , *Journal of Number Theory* **17** (1983), pp. 1-28.

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag:Berlin, 1993.

[10] P.M. Cohn, *Algebraic Numbers and Algebraic Functions*, Chapman & Hall: London, 1991.

[11] D.A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons:New York, 1989.

[12] N. Demytko, "A new elliptic curve based analogue of RSA," in *Advances in Cryptology - EUROCRYPT '93*, Lecture Notes in Computer Science **765** (1993), Springer-Verlag, pp. 40-49.

[13] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), pp. 644-654.

[14] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory* **31** (1985), pp. 469-472.

[15] N.D. Elkies, Explicit isogenies, manuscript, 1991.

[16] P. Erdös, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function, *The Quarterly Journal of Mathematics, Oxford Series* **6** (1935), pp. 205-213.

[17] C.G. Günther, "An identity-based key exchange protocol," in *Advances in Cryptology - EUROCRYPT '89*, Lecture Notes in Computer Science **434** (1989), Springer-Verlag, pp. 29-37.

[18] K. Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag:New York, 1990.

[19] D.E. Knuth and L.T. Pardo, Analysis of a simple factorization algorithm, *Theoretical Computer Science* **3** (1976), pp. 321-348.

[20] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* **48** (1987), pp. 203-209.

[21] K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone, "New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$," in *Advances in Cryptology - CRYPTO '91*, Lecture Notes in Computer Science **576** (1991), Springer-Verlag, pp. 252-266.

[22] S. Lang, *Elliptic Functions*, Springer-Verlag:New York, 1987.

[23] G. Lay and H. Zimmer, "Constructing elliptic curves with given group order over large finite fields," in *Algorithmic Number Theory: First International Symposium*, Lecture Notes in Computer Science **877** (1994), Springer-Verlag, pp. 250-263.

[24] H.W. Lenstra, Jr., Factoring with elliptic curves, *Annals of Mathematics* **126** (1987), pp. 649-673.

[25] U.M. Maurer, "On the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms," in *Advances in Cryptology - CRYPTO*

'94, Lecture Notes in Computer Science **839** (1994), Springer- Verlag, pp. 271-281.

[26] U.M. Maurer and S. Wolf, "Diffie-Hellman oracles", in *Advances in Cryptology - CRYPTO '96*, Lecture Notes in Computer Science **1109** (1996), Springer-Verlag, pp. 268-282.

[27] U.M. Maurer and Y. Yacobi, "Non-interactive public key cryptography,", in *Advances in Cryptology - EUROCRYPT '91*, Lecture Notes in Computer Science **547** (1991), Springer-Verlag, pp. 498-507.

[28] A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers:Boston, 1993.

[29] A.J. Menezes, Y.H. Wu and R.J. Zuccherato, An elementary introduction to hyperelliptic curves, Combinatorics & Optimization Research Report CORR 96-19, University of Waterloo, Canada, 1996.

[30] J.P. Mesirov and M.M. Sweet, Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2, *Journal of Number Theory* **27** (1987), pp. 144-148.

[31] V. Miller, "Uses of elliptic curves in cryptography," in *Advances in Cryptology - CRYPTO '85*, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, pp. 417-426.

[32] A. Miyaji, Elliptic curve cryptosystems immune to any reduction into the discrete logarithm problem, *preprint.*

[33] V. Müller, A. Stein and C. Thiel, Computing discrete logarithms in real quadratic congruence function fields of large genus, *preprint.*

[34] R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Applied Mathematics* **22** (1988/1989), pp. 149-161.

[35] National Bureau of Standards, "Data encryption standard," *Federal information processing standard*, U.S. Department of Commerce, FIPS PUB 46, Washington, DC, 1977.

[36] National Institute for Standards and Technology, "Digital signature standard," *Federal information processing standard*, U.S. Department of Commerce, FIPS PUB 186, Washington, DC, 1994.

[37] S. Pohlig and M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Transactions on Information Theory* **24** (1978), pp. 106-110.

[38] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21** (1978), pp. 120-126.

[39] K.H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley:Reading, 1984.

[40] R. Scheidler, J.A. Buchmann and H.C. Williams, A key-exchange protocol using real quadratic fields, *Journal of Cryptology* **7** (1994), pp. 171-199.

[41] R. Scheidler, A. Stein and H.C. Williams, Key-exchange in real quadratic congruence function fields, *Designs, Codes and Cryptography* **7** (1996), pp. 153-174.

[42] F.K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, *Mathematische Zeitschrift* **33** (1931), pp. 1-32.

[43] C. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology* **4** (1991), pp. 161-174.

[44] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Mathematics of Computation* **44** (1985), pp. 483-494.

[45] D. Shanks, The infrastructure of a real quadratic field and its applications, *Proceedings of the 1972 Number Theory Conference* (1972), pp. 217-224.

[46] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag:New York, 1986.

[47] A. Stein, *Baby Step-Giant Step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2.* Diplomarbeit, Saarbrücken 1992.

[48] A. Stein, Equivalences between elliptic curves and real quadratic congruence function fields, *preprint.*

[49] A. Stein and H.C. Williams, Baby step-giant step in real quadratic congruence function fields, *preprint.*

[50] A. Stephens and H.C. Williams, Some computational results on a problem concerning powerful numbers, *Mathematics of Computation* **50** (1988), pp. 619-632.

[51] A. Stephens and H.C. Williams, Computation of real quadratic fields with class number one, *Mathematics of Computation* **51** (1988), pp. 809-824.

[52] I.N. Stewart and D.O. Tall, *Algebraic Number Theory*, second edition, Chapman and Hall:London, 1987.

[53] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag:Berlin, 1993.

[54] S.A. Vanstone and R.J. Zuccherato, Short RSA keys and their generation, *Journal of Cryptology* **8** (1995), pp. 101-114.

[55] B. Weiss and H.G. Zimmer, Artin's Theorie der quadratischen Kongruenzfunkionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengrupen, *Mitteilungen der Mathematischen Gesellschaft in Hamburg* **XII** (1991), pp. 261-286.

[56] H.C. Williams and M.C. Wunderlich, On the parallel generation of the residues for the continued fraction factoring algorithm, *Mathematics of Computation* **48** (1987), pp. 405-423.