

國立交通大學

資訊科學與工程研究所

碩士論文

橢圓曲線上 SEA 演算法之加速

Speeding up SEA Algorithm for Elliptic Curves

研究生：劉用翔

指導教授：陳榮傑 教授

中華民國九十七年六月

橢圓曲線上 SEA 演算法之加速
Speeding up SEA Algorithm for Elliptic Curves

研究生：劉用翔

Student : Yung-Hsiang Liu

指導教授：陳榮傑

Advisor : Dr. Rong-Jaye Chen

國立交通大學
資訊科學與工程研究所
碩士論文

A Thesis

Submitted to Institute of Computer Science and Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年六月

橢圓曲線上 SEA 演算法之加速

學生：劉用翔

指導教授：陳榮傑 博士

國立交通大學資訊科學與工程研究所 碩士班

摘要

1985 年，Miller 與 Koblitz 先後提出將橢圓曲線使用在公開金鑰密碼系統上。橢圓曲線上的有理點會形成一個加法群，此加法群上的離散對數問題稱為橢圓曲線離散對數問題 (elliptic curve discrete logarithm problem)。目前沒有任何演算法可以快速的解決此問題，因此，橢圓曲線密碼系統基於此困難的問題上，只需比 RSA 還短的金鑰長度，就可達到與 RSA 相同的安全度。

在使用橢圓曲線密碼系統時，挑選一個安全性高的橢圓曲線是很重要的。選取橢圓曲線的方法共有三種。現在主要的方法是先隨機選取橢圓曲線，並計算曲線上的有理點個數，以判定此橢圓曲線是否符合安全要求。所以，在橢圓曲線密碼系統的設計上，計算一條橢圓曲線在有限體上的點數就扮演了很重要的角色。Schoof-Elkies-Atkin(SEA) 演算法是用於計算點數上重要的方法。在本篇論文中，我們將分別提出對於演算法中 Atkin 質數、Elkies 質數及 小步-大步 (Baby-step-giant-step) 的策略，用來計算定義於大質數體上橢圓曲線之點數，有很好的改良。

關鍵字：橢圓曲線、SEA 演算法、Atkin 質數、Elkies 質數。

Speeding up SEA Algorithm for Elliptic Curves

Student: Yung-Hsiang Liu

Advisor: Dr. Rong-Jaye Chen

Institute of Computer Science and Engineering
National Chiao Tung University

ABSTRACT

In 1985, Miller proposed the use of elliptic curves in public-key cryptosystem, and so did Koblitz in 1987. The rational points of an elliptic curve forms an additive group. The discrete logarithm problem of this group is called elliptic curve discrete logarithm problem (ECDLP). There is no method to solve ECDLP efficiently. The security of elliptic curve cryptosystem (ECC) is based on ECDLP. Therefore, The key of ECC can be shorter than that of RSA in order to reach the same secure strength.

In using the elliptic curve cryptosystem, it is important to select a secure elliptic curve. There are three methods to select secure elliptic curves. The suggested method is counting the number of rational points of elliptic curves generated randomly. Therefore, we can determine whether a randomly generated elliptic curve is suitable for the security consideration. Hence, solving the point counting problem plays a crucial role in the design of elliptic curve cryptosystems. Schoof-Elkies-Atkin(SEA) algorithm is an important method to solve the point counting problem. In this thesis, we propose strategies of Atkin primes, Elkies primes, and Baby-step-giant-step. It improves the original SEA algorithm a lot for elliptic curves defined over big prime fields.

Keywords: elliptic curve, SEA algorithm, Atkin prime, Elkies prime.

誌 謝

這篇碩士論文能夠順利完成，首先，要誠摯的感謝指導教授陳榮傑教授，老師悉心的教導使我得以了解橢圓曲線密碼學的內涵，也使我在求學期間獲益良多，老師對我在研究生涯的照顧，我也將永遠感念在心，謝謝老師。另外也感謝張仁俊教授、楊一帆教授與胡鈞祥博士擔任我的口試委員，在口試中給予的指點與建議，使論文能夠更完整。也感謝師母李惠慈女士給予我英文寫作上的建議，使論文能夠更流暢通順。

感謝 Cryptanalysis 實驗室的志賢學長、定宇學長、順隆學長、家瑋學長、嘉軒學長，及同學佩娟、輔國，謝謝你們這兩年不時的與我討論，以及陪伴，是我研究生生活中，很重要的一部份，謝謝你們。

感謝系計中的學長姐、同學以及學弟妹們，有你們的陪伴與合作，讓我的研究生生活更加充實，以及準備口試時的鼓勵，也讓我備感溫馨。還有應數系的學弟妹們，還是時常與我聯絡與交流，讓我在研究生生活中也感受到你們的活力，謝謝你們。

最後我也要謝謝我的家人，感謝父母在求學期間多年來的栽培，謝謝妹妹不時的關心，有你們的支持使我能夠無後顧之憂的專心求學、完成論文，謹以此文獻給我摯愛的家人。

Contents

中文摘要	i
Abstract	ii
Acknowledge	iii
Table of Contenes	iv
List of Tables	vi
List of Figures	vii
1 Introduction	1
2 Mathematical Backgrounds	5
2.1 Abstract Algebra	5
2.1.1 Group Theory	5
2.1.2 Homomorphisms and Factor Groups	7
2.1.3 Rings and Integral Domains	8
2.1.4 Algebraic Closure and Finite Fields	10
2.1.5 Separable Extension and Galois Theory	11
2.2 Elliptic Curves	15
2.2.1 Algebraic Varieties	15
2.2.2 General Elliptic Curves	16
2.2.3 Elliptic Curves over Prime Fields of Characteristic > 3	19



2.2.4	Isogenies	20
2.2.5	Elliptic Curves over \mathbb{C}	22
2.3	p -adic Arithmetic	24
2.3.1	p -adic Numbers	24
2.3.2	Hensel's Lemma	24
3	Schoof-Elkies-Atkin Algorithm	26
3.1	Before Schoof	26
3.2	Schoof's Idea	28
3.3	Atkin's Idea and Elkies' Idea	31
3.3.1	Modular Polynomial	31
3.3.2	Elkies' Improvement	33
3.3.3	Atkin's Method	37
3.3.4	Baby-step-giant-step(BSGS) Strategy	39
3.3.5	Complexity Analysis	41
4	Previous Improvements for SEA Algorithm	43
4.1	Isogeny Cycles	43
4.2	Re-ordering Atkin Primes	47
4.3	Virtual (Atkin/Isogeny cycles) Method	47
4.4	Chinese and Match Method	47
5	Our Three Heuristics for SEA Algorithm	49
5.1	Atkin Selection Heuristic	49
5.2	Elkies Isogeny Heuristic	53
5.3	Polynomial-Time BSGS Heuristic	57
5.4	Numerical Results	59
6	Conclusion & Future Work	62



List of Tables

1.1	NIST Recommended Key Sizes(bits)	2
5.1	Evaluation methods of Atkin primes	52
5.2	Average computing time of original SEA algorithm	59
5.3	Average computing time when applying Atkin selection heuristic	59
5.4	Average computing time when applying Elkies isogeny heuristic	60
5.5	Average computing time when applying polynomial-time BSGS heuristic	60
5.6	Average computing time when applying three heuristics	60



List of Figures

2.1	$E : y^2 = x^3 - x$	17
2.2	Group Law(chord process)	18
2.3	Group Law(tangent process)	18
2.4	Lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$	23
4.1	Isogeny cycle	45



Chapter 1

Introduction

The use of elliptic curves in public-key cryptography is first proposed in the works of Koblitz[13] and Miller[17]. Each elliptic curve defined over a finite field forms an abelian group. The secure strength is based on the discrete logarithm problem(DLP) of this group, which is called elliptic curve DLP(ECDLP). The public-key cryptosystems are based on hard mathematical problems. For example, integer factorization and the DLP on finite fields are hard mathematical problems, and so is ECDLP. The previous two problems can be solved in sub-exponential time via index calculus method and the number field sieve. However, there has been no known sub-exponential algorithm to solve ECDLP so far.

Generally, in order to break the elliptic curve cryptosystem, ECDLP needs to be solved. Because ECDLP is much harder than the other hard problems, elliptic curve cryptography(ECC) can reach the same secure strength as RSA with the key of shorter length. Table 1.1 is the key size comparison[26].

Some protocols based on ECC take advantage of shorter key size. In the use of ECC in public-key cryptosystem, there are ECDSA[11], ECIES[2], and ECMQV[14] corresponding to digital signature, encryption, and key-exchange protocols. The idea of identity-based en-

Symmetric Key	80	112	128	192	256
RSA and DH	1024	2048	3072	7680	15360
Elliptic Curve	160	224	256	384	521

Table 1.1: NIST Recommended Key Sizes(bits)

crypton scheme was proposed by Shamir in 1984. Boneh and Franklin proposed the practical scheme by using the Weil pairing, a bilinear pairing of elliptic curves. It is also called the pairing-based cryptography.

There is no efficient algorithm for solving ECDLP. Nevertheless, there are some properties which make elliptic curves weak. Let E be an elliptic curve defined over a finite field \mathbb{F}_q and $\#E(\mathbb{F}_q) = n$. The curves of $n = q$ is called anomalous curves, and $E(\mathbb{F}_q) \cong \langle \mathbb{F}_q, + \rangle$. The explicit isomorphism from $E(\mathbb{F}_q)$ to $\langle \mathbb{F}_q, + \rangle$ can be computed. So, ECDLP can be transformed to a division over the finite field \mathbb{F}_q . Additionally, the bilinear pairings, Weil pairing and Tate pairing, corresponding to MOV attack[16] and FR attack[7], are used for solving ECDLP. Let r be a big prime factor of $\#E(\mathbb{F}_q)$. ECDLP can be transformed to DLP over the extension field \mathbb{F}_{q^k} of \mathbb{F}_q , where k is the smallest positive integer, called the embedding degree of E , such that $r|q^k - 1$. Besides, if \mathbb{F}_q is an extension field of a base field, the curves can be transformed to the abelian variety by use of Weil descent method. Then, the index calculus can be applied to the DLP on the abelian variety[8]. It is feasible if $\mathbb{F}_q = \mathbb{F}_{\tilde{q}^s}$ for a small s .

The methods mentioned above are named “isomorphism attacks.” An elliptic curve which is suitable for cryptography needs to obstruct isomorphism attacks. Explicitly, a curve which is good for cryptography has to satisfy the following properties:

- (1) n has a large prime factor r , or $n = r$ is prime.
- (2) $n \neq q$.

(3) $n \nmid q^i - 1$ for $1 \leq i \leq 20$.

(4) $q = p^k$, where p is a prime, and k is either 1 or a prime.

There are three techniques to generate the secure curves. One is subfield curves[25], also called a curve of Koblitz type. The coefficients of this kind of curves are in a small subfield of \mathbb{F}_q . Another technique is complex multiplication[1]. These curves also have some features. Although there are no known attacks directed toward these curves, the security of these curves is in doubt. Nowadays, the point counting methods on random curves, a third technique, is most suggested because there is no character for these curves. By this method, we choose a finite field first, and generate the coefficients of elliptic curves randomly. Schoof gives the first polynomial time algorithm, of time complexity $O(\log^8 q)$, to count the number of rational points over \mathbb{F}_q [20]. This algorithm profits from the improvements of Elkies and Atkin, and is therefore called Schoof-Elkies-Atkin(SEA) algorithm[21]. SEA algorithm improves Schoof's original algorithm so that the complexity is $O(\log^6 q)$, instead.

In this thesis, we propose three heuristics for SEA algorithm. One is for the selection of Atkin primes. Another is to determine the power of the isogeny cycle method of Elkies primes. The other is to bound the time used in the baby-step-giant-step of SEA algorithm. These three heuristics can help us speed up SEA algorithm. The following shows how the rest of the thesis organized.

In Chapter 2, we describe relevant mathematical backgrounds for this thesis, including the theories and properties of abstract algebra, the definitions of groups, rings, and fields, and the properties of the group structure. Some mathematical definition of algebra used later is also listed properly. The general elliptic curves and the elliptic curves over prime fields of characteristic > 3 are introduced. We also introduce some theories developed on the elliptic curves

over \mathbb{C} for the reason that they are closely linked with Elkies' improvements. The last is p -adic numbers. In the implementation of SEA algorithm, the Hensel's Lemma for p -adic fields is used.

In Chapter 3, we introduce the point counting problem for elliptic curves over finite fields. The Schoof's idea for point counting, and the improvements from Atkin's and Elkies' works is also described here. After SEA algorithm is described, we give a rough complexity analysis of the algorithm. The previous improvements are listed in Chapter 4, including isogeny cycles[5], index of Atkin primes[9], virtual method[9], and "Chinese and Match" method[12].

In Chapter 5, we propose our two heuristics for SEA algorithm. We also describe the reason for the heuristics. Next, the implementation details and the numerical results are shown. The conclusion is given in section 6.



Chapter 2

Mathematical Backgrounds

The theories of SEA algorithm is developed from algebra and algebraic curves. Here, we introduce algebra first, and then elliptic curves of algebraic curves. After that, the p -adic number is also mentioned.



2.1 Abstract Algebra

The rational points of an elliptic curve forms a group. A lot of properties of elliptic curves are from the abstract algebra. So, here we introduce the theories first.

2.1.1 Group Theory

A binary operation $*$ on a set S is a function mapping $S \times S$ into S . In other words, S is closed under the operation $*$. And $\langle S, * \rangle$ is called a binary structure. An element $e \in S$ is an identity element for $*$ if $e * s = s * e = s$ for all $s \in S$. For some $a \in S$. The inverse element of a is $a' \in S$ such that $a' * a = a * a' = e$.

Definition 2.1 (Group). A group $\langle G, * \rangle$ is a binary structure such that the following axioms are satisfied:

1. (Associativity) For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c).$$

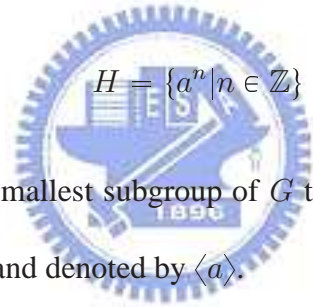
2. (Identity) G contains the identity element for $*$.

3. (Inverse) For all $a \in G$, there exists the inverse element a' of a in G .

If the cardinality of a group G is finite, then G is a finite group. The number of elements in G called the group order. A group $\langle G, * \rangle$ is abelian if $*$ is commutative.

If $H \subseteq G$ and $\langle H, * \rangle$ is a group, then H is a subgroup of G . It is denoted by $H \leq G$ or $G \geq H$, and $H < G$ or $G > H$ means $H \leq G$ but $H \neq G$.

Theorem 2.2. Let $\langle G, * \rangle$ be a group and $a \in G$. Denote $a * a$ by a^2 , and so on. Then


$$H = \{a^n | n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest subgroup of G that contains a . H is called the cyclic subgroup of G generated by a , and denoted by $\langle a \rangle$.

If there is some element a in a group G such that $\langle a \rangle = G$, then G is cyclic. And a is called a generator of G . Moreover, every cyclic group is abelian.

Definition 2.3 (Finitely generated group). Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i | i \in I\}$ is the subgroup generated by $\{a_i | i \in I\}$. If this subgroup is all of G , then $\{a_i | i \in I\}$ generates G and a_i are generators of G . If there is a finite set $\{a_i | i \in I\}$ that generates G , then G is finitely generated.

Note that every group of finite order is finitely generated.

Theorem 2.4 (Theorem of Lagrange). Let H be a subgroup of a finite group G . Then the order of H is a divisor of the order of G .

2.1.2 Homomorphisms and Factor Groups

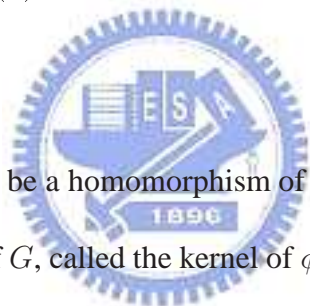
A map ϕ of a group $\langle G, * \rangle$ into a group $\langle G', \circ \rangle$ is a homomorphism if

$$\phi(a * b) = \phi(a) \circ \phi(b) \quad \text{for all } a, b \in G$$

Definition 2.5 (Image and inverse image). Let $\phi : X \mapsto Y$, and let $A \subseteq X$ and $B \subseteq Y$. The image $\phi[A]$ of A in Y under ϕ is $\{\phi(a) | a \in A\}$. The set $\phi[X]$ is the range of ϕ . The inverse image $\phi^{-1}[B]$ of B in X is $\{x \in X | \phi(x) \in B\}$.

Theorem 2.6. Let ϕ be a homomorphism of a group G into a group G' .

- (1) If e is the identity element of G , then $\phi(e) = e'$ is the identity element in G' .
 (2) If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$. (3) If $H \leq G$, then $\phi[H] \leq G'$. (4) If $K' \leq G'$, then $\phi^{-1}[K'] \leq G$.



Corollary 2.7. Let $\phi : G \mapsto G'$ be a homomorphism of groups and let e' be the identity of G' . Then, $\phi^{-1}[\{e'\}]$ is a subgroup of G , called the kernel of ϕ , and is denoted by $\text{Ker}(\phi)$. Moreover, ϕ is one-to-one if and only if $\text{Ker}(\phi) = \{e\}$.

A homomorphism of A into itself is an endomorphism of A .

Definition 2.8 (Isomorphism). Let $\phi : G \mapsto G'$ be a homomorphism, and ϕ is one-to-one and onto. Then ϕ is an isomorphism, and G is isomorphic to G' , denoted by $G \cong G'$. G and G' have the same group structure.

An automorphism of A into itself is an automorphism of A .

Theorem 2.9 (Fundamental Theorem of Finitely Generated Abelian Groups). Every finitely abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \dots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z},$$

where p_i are primes, not necessarily distinct, and r_i are positive integers.

Let $H \leq G$. The subset $aH = \{ah|h \in H\}$ of G is the left coset of H containing a , while the subset $Ha = \{ha|h \in H\}$ is the right coset of H containing a . A subgroup H of a group G is normal if $\forall g \in G$

$$gH = Hg.$$

Note that all subgroups of abelian groups are normal.

Theorem 2.10. Let H be a subgroup of a group G . Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G .

Let H be a normal subgroup of G . Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. The group G/H is the factor group (or quotient group) of G by H .



2.1.3 Rings and Integral Domains

Definition 2.11 (Ring). A ring $\langle R, +, \cdot \rangle$ is a set with two binary operations, which we called addition and multiplication, defined on R such that the following axioms are satisfied:

- (1) $\langle R, + \rangle$ is an abelian group.
- (2) Multiplication is associative.
- (3) $\forall a, b, c \in R,$

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad \text{and } (a + b) \cdot c = a \cdot c + b \cdot c$$

For rings R and R' , a map $\phi : R \mapsto R'$ is a homomorphism if $\forall a, b \in R$

$$(1) \phi(a + b) = \phi(a) + \phi(b).$$

$$(2) \phi(ab) = \phi(a)\phi(b).$$

An isomorphism $\phi : R \mapsto R'$ is a homomorphism that is one-to-one and onto. The rings R and R' are then isomorphic. A ring in which the multiplication is commutative is a commutative ring. The multiplication identity element of a ring is called “unity.” A ring which contains the unity is called ring with unity, and an element u is a unit of ring with unity if it has the multiplicative inverse. A division ring is a ring with unity of the property that every nonzero element is a unit.

Definition 2.12 (Field). A field is a commutative division ring. Hence, a field $\langle F, +, \cdot \rangle$ satisfies

(1) $\langle F, + \rangle$ is an abelian group.

(2) $F^* = F \setminus \{0\}$. $\langle F^*, \cdot \rangle$ is an abelian group.

(3) Distributive law.



Let R be a ring. The set $R[x]$ of all polynomials in an indeterminate x with coefficients in R is a ring under polynomial addition and multiplication.

Definition 2.13 (Ideal). An additive subgroup N of a ring satisfying the properties

$$aN \subseteq N \quad \text{and} \quad Nb \subseteq N \quad \text{for all } a, b \in R$$

is an ideal.

Let N be an ideal of a ring R . Then the additive cosets of N form a ring R/N with the binary operations defined by

$$(a + N) + (b + N) = (a + b) + N$$

and

$$(a + N)(b + N) = ab + N.$$

The ring R/N is the factor ring (or quotient ring) of R by N .

Definition 2.14 (Maximal ideal). A maximal ideal of a ring R is an ideal M different from R such that there is no proper ideal N of R such that $M \subset N \subset R$.

Definition 2.15 (Prime ideal). An ideal $N \neq R$ in a commutative ring R is a prime ideal if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are zero divisors. An integral domain is a commutative ring with unity and contains no zero divisors.

Theorem 2.16. Every finite integral domain is a field.

Theorem 2.17. For a commutative ring R with unity:

- (1) An ideal M of R is maximal if and only if R/M is a field.
- (2) An ideal N of R is prime if and only if R/N is an integral domain.
- (3) Every maximal ideal of R is a prime ideal.

Corollary 2.18. If p is a prime, then \mathbb{Z}_p is a field.

The characteristic of the ring R is the smallest positive integer n such that $n \cdot a = 0 \quad \forall a \in R$.

If no such positive integer exists, then R is of characteristic 0.

Theorem 2.19. Any integral domain D can be enlarged to a field F such that every element of F can be expressed as a quotient of two elements of D .

2.1.4 Algebraic Closure and Finite Fields

If a subset F' of a field F is a field, then F' is a subfield of F . A field E is an extension field of F if F is a subfield of E .

Definition 2.20 (Degree). If an extension field E of a field F is of finite dimension n as a vector space over F , then E is a finite extension of degree n over F . It is denoted by $[E : F] = n$.

Theorem 2.21 (Kronecker's Theorem). Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

A field F is algebraically closed if every non-constant polynomial in $F[x]$ has a root in F . An algebraic extension \overline{F} of F is the algebraic closure of F if \overline{F} is algebraically closed.

Theorem 2.22. Every field has an algebraic closure.

A field of finite order is called a finite field.

Theorem 2.23. Let p be a prime. If E is a finite field of characteristic p , then E contains exactly p^n elements for some positive integer n .

Theorem 2.24. Let E be a field of p^n elements contained in an algebraic closure $\overline{\mathbb{Z}_p}$ of \mathbb{Z}_p . The elements of E are precisely the zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Theorem 2.25. The multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a finite field F is cyclic.

A finite field $\text{GF}(p^n)$ of p^n elements exists for every prime power p^n .

Theorem 2.26. Let p be a prime and let $n \in \mathbb{Z}^+$. If E and E' are fields of order p^n , then $E \cong E'$.

2.1.5 Separable Extension and Galois Theory

Definition 2.27 (Conjugate). Let E be an algebraic extension of a field F . Two elements $\alpha, \beta \in E$ are conjugate over F if $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$, that is, if α and β are zeros of the same

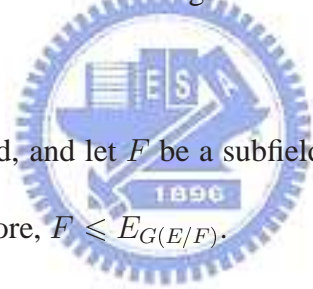
irreducible polynomial over F . Note that $\text{irr}(*, F)$ is the irreducible polynomial of $*$ over F .

Theorem 2.28 (Conjugation isomorphisms). Let F be a field, and let α and β be algebraic over F with $\deg(\alpha, F) = n$. The map $\psi_{\alpha, \beta} : F(\alpha) \mapsto F(\beta)$ defined by

$$\psi_{\alpha, \beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$$

for $c_i \in F$ is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F .

Let $\{\sigma_i \mid i \in I\}$ be a collection of automorphisms of a field E . Then the set $E_{\{\sigma_i\}}$ of all $a \in E$ left fixed by every σ_i for $i \in I$ forms a subfield of E . $E_{\{\sigma_i\}}$ is the fixed field of $\{\sigma_i \mid i \in I\}$. The set of all automorphisms of a field E is a group under function composition. The set $G(E/F)$ is the collection of automorphisms of E leaving F fixed. The group $\text{Aut}(E)$ is the group of all automorphisms of E .



Theorem 2.29. Let E be a field, and let F be a subfield of E . Then the set $G(E/F)$ forms a subgroup of $\text{Aut}(E)$. Furthermore, $F \leq E_{G(E/F)}$.

Definition 2.30 (Frobenius automorphism). Let F be a finite field of characteristic p . Then the map $\sigma_p : F \mapsto F$ defined by

$$\sigma_p(a) = a^p \quad \text{for } a \in F$$

is the Frobenius automorphism of F . Also, $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.

Theorem 2.31. Let \overline{F} and $\overline{F'}$ be two algebraic closures of F . Then \overline{F} is isomorphic to $\overline{F'}$ under an isomorphism leaving each element of F fixed.

Definition 2.32 (Index of E over F). Let E be a finite extension of a field F . The number of isomorphisms of E onto a subfield of \overline{F} leaving F fixed is the index $\{E : F\}$ of E over F .

Let F be a field with algebraic closure \overline{F} . Let $\{f_i(x) \mid i \in I\}$ be a collection of polynomials in $F[x]$. A field $E \leq \overline{F}$ is the splitting field of $\{f_i(x) \mid i \in I\}$ over F if E is the smallest subfield of \overline{F} containing F and all the zeros in \overline{F} of each of the $f_i(x)$ for $i \in I$. A field $K \leq \overline{F}$ is a splitting field over F if it is the splitting field of some set of polynomials in $F[x]$.

Theorem 2.33. A field E , where $F \leq E \leq \overline{F}$, is a splitting field over F if and only if every automorphism of \overline{F} leaving F fixed maps E onto itself and thus induces an automorphism of E leaving F fixed.

A polynomial $f(x) \in F[x]$ splits in E if it factors into a product of linear factors in $E[x]$.

Theorem 2.34. If $E \leq \overline{F}$ is a splitting field of finite degree over F , then

$$\{E : F\} = |G(E/F)|$$

Let $f(x) \in F[x]$. An element α of \overline{F} such that $f(\alpha) = 0$ is a zero of $f(x)$ of multiplicity ν if ν is the greatest integer such that $(x - \alpha)^\nu$ is a factor of $f(x)$ in $\overline{F}[x]$.

Theorem 2.35. Let $f(x)$ be irreducible in $F[x]$. Then all zeros of $f(x)$ in \overline{F} have the same multiplicity.

Theorem 2.36. If E is a finite extension of F , then $\{E : F\}$ divides $[E : F]$.

Definition 2.37 (Separable). A finite extension E of F is a separable extension of F if $\{E : F\} = [E : F]$. An element α of \overline{F} is separable over F if $F(\alpha)$ is a separable extension of F . An irreducible polynomial $f(x) \in F[x]$ is separable over F if every zero of $f(x)$ in \overline{F} is separable over F .

A field is perfect if every finite extension is a separable extension. Every field of characteristic zero is perfect. Every finite field is perfect.

Definition 2.38 (Totally inseparable). A finite extension E of a field F is a totally (purely) inseparable extension of F if $\{E : F\} = 1 < [E : F]$. An element α of \overline{F} is totally inseparable over F if $F(\alpha)$ is totally inseparable over F .

Theorem 2.39. Let F have characteristic $p \neq 0$, and let E be a finite extension of F . Then $\alpha \in E, \alpha \notin F$, is totally inseparable over F if and only if there is some integer $t \geq 1$ such that $\alpha^{p^t} \in F$.

Theorem 2.40 (Separable closure). Let F have characteristic $p \neq 0$, and let E be a finite extension of F . There is a unique extension K of F , with $F \leq K \leq E$, such that K is separable over F , and either $E = K$ or E is totally inseparable over K . The unique field K is the separable closure of F in E .

A finite extension K of F is a finite normal extension of F if K is a separable splitting field over F .



Theorem 2.41. If K is a finite normal extension of F , then

$$|G(K/F)| = \{E : F\} = [E : F].$$

Theorem 2.42. Let K be a finite normal extension of F , and let E be an extension of F , where $F \leq E \leq K \leq \overline{F}$. Then K is a finite normal extension of E , and $G(K/E)$ is precisely the subgroup of $G(K/F)$ consisting of all those automorphisms that leave E fixed.

Definition 2.43 (Galois group). If K is a finite normal extension of a field F , then $G(K/F)$ is the Galois group of K over F .

Theorem 2.44 (Galois Theory). Let K be a finite normal extension of a field F , with Galois group $G(K/F)$. For a field E , where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$

leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ :

(1) $\lambda(E) = G(K/E)$.

(2) $E = K_{G(K/E)} = K_{\lambda(E)}$.

(3) For $H \leq G(K/F)$, $\lambda(E_H) = H$.

(4) $[K : E] = |\lambda(E)|$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.

(5) E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. Furthermore,

$$G(E/F) \cong G(K/F)/G(K/E).$$

2.2 Elliptic Curves



In the section, we introduce the elliptic curves as the algebraic curves in algebraic geometry.

The important theories related to SEA algorithm are developed very well in algebraic geometry.

We focus on the case of elliptic curves.

2.2.1 Algebraic Varieties

Let K be a perfect field. An algebraic set is any set of the form V_I . If V is an algebraic set, the ideal of V is given by

$$I(V) = \{f \in \overline{K}[X] \mid f(P) = 0 \quad \forall P \in V\}.$$

If $I(V)$ is a prime ideal in $\overline{K}[X]$, V is called an variety.

Definition 2.45 (Coordinate ring). The coordinate ring of a variety V

$$\overline{K}[V] = \frac{\overline{K}[X]}{I(V)}.$$

It is an integral domain, and its quotient field, denoted by $\overline{K}(V)$, is called the function field of V .

2.2.2 General Elliptic Curves

Definition 2.46 (Weierstrass equation). The affine Weierstrass equation, given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$, is the general equation of elliptic curves.

Note that we also use

$$\mathcal{E}(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

to express elliptic curves.

Definition 2.47 (Elliptic curves). The elliptic curve over K is defined as the set of the solutions of E in K^2 , and the point at infinity ∞ . The set is so-called K -rational points of $E(K)$.

Figure 2.1 shows the elliptic curve $E : y^2 = x^3 - x$ over \mathbb{R} .

For the Weierstrass equation of elliptic curves the definition of the constants:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Definition 2.48 (Discriminant). The discriminant of the curve is defined as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

When the characteristic of $K \neq 2, 3$, the discriminant can also be expressed as

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

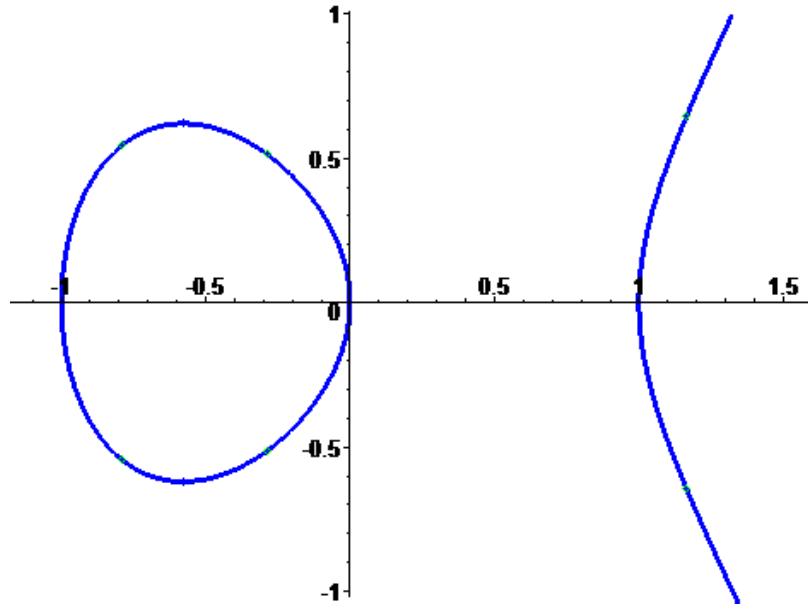


Figure 2.1: $E : y^2 = x^3 - x$

Definition 2.49 (j -invariant). When $\Delta \neq 0$, the j -invariant of the curve is defined by

$$j(E) = \frac{c_4^3}{\Delta}.$$

Theorem 2.50. Two elliptic curves that are isomorphic over K have the same j -invariant. Conversely, two elliptic curves with the same j -invariant are isomorphic over \overline{K} .

Definition 2.51 (Group law). Let P and Q be two distinct rational points on E . The straight line joining P and Q must intersect the curve at one further point, said R' . Then, we reflect R' in the x -axis to obtain another rational point R , then $R = P + Q$ (See Figure 2.2). To add P to itself, or to double P , we take the tangent to the curve at P instead of the line joining P and Q (See Figure 2.3). The group law is often called the chord-tangent process. We say that a vertical line also intersects the curve at ∞ .

Definition 2.52 (multiplication-by- m map). For a positive integer m , we let $[m]$ denote the multiplication-by- m map from the curve to itself. This map takes a point P to $P + P + \dots + P$

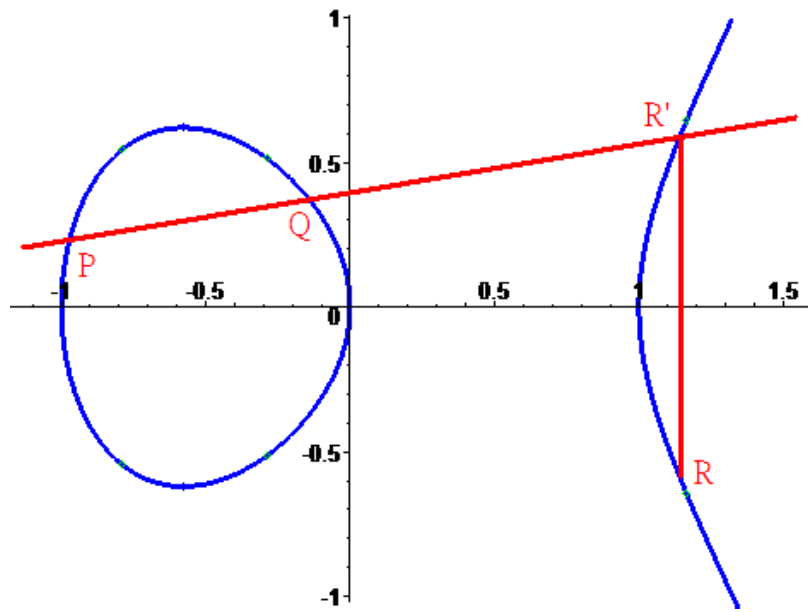


Figure 2.2: Group Law(chord process)

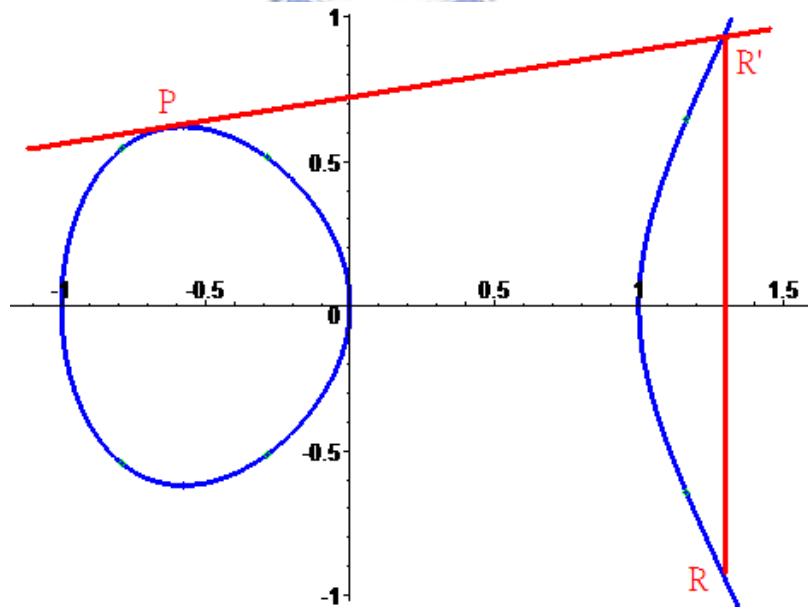


Figure 2.3: Group Law(tangent process)

(m summands). The notation $[m]$ is extended to $m \leq 0$ by defining $[0]P = \infty$, and $[-m]P = -([m]P)$.

2.2.3 Elliptic Curves over Prime Fields of Characteristic > 3

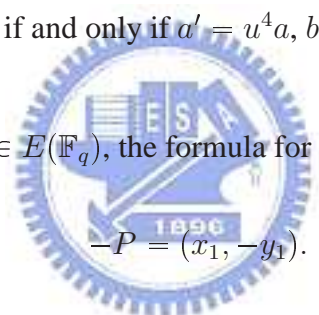
Definition 2.53 (Short Weierstrass form). Assume $K = \mathbb{F}_q$, where $q = p > 3$. The curve equation can be simplified to the short Weierstrass form

$$E_{[a,b]} : y^2 = x^3 + ax + b.$$

The discriminant of the curve then reduces to $\Delta = -16(4a^3 + 27b^2)$, and its j -invariant to $j(E) = -1728(4a^3)/\Delta$.

Theorem 2.54. $E_{[a,b]} \cong E_{[a',b']}$ if and only if $a' = u^4a$, $b' = u^6b$ for some $u \in \mathbb{F}_q^*$.

For points $P(x_1, y_1), Q(x_2, y_2) \in E(\mathbb{F}_q)$, the formula for the group law is



$$-P = (x_1, -y_1).$$

When $x_1 \neq x_2$, we set

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$

and when $x_1 = x_2, y_1 \neq 0$, we set

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

If

$$R(x_3, y_3) = P + Q \neq \infty,$$

then x_3 and y_3 are given by

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = (x_1 - x_3)\lambda - y_1.$$

The rational points of order two on the curve are of the form $(\xi, 0)$.

Theorem 2.55. The group structure of an elliptic curve E over a finite field \mathbb{F}_q satisfies

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}.$$

Moreover, $E(\mathbb{F}_q)$ is a finite abelian group, so d_1 divides both d_2 and $q - 1$, including the case of $d_1 = 1$.

Definition 2.56 (Twist curve). A twist of a curve given in short Weierstrass form $E_{[a,b]}$ is given by $E_{[a',b']}$, where $a' = v^2a$, $b' = v^3b$ for some quadratic non-residue $v \in \mathbb{F}_q$. and the j -invariant of these two curves are the same.

The twist is unique up to isomorphisms over \mathbb{F}_q , and it is itself isomorphic to the original curve over $\overline{\mathbb{F}_q}$ (in fact, it is so over \mathbb{F}_{q^2}). The orders of the groups of rational points of the two curves satisfy the relation

$$\#E_{[a,b]}(\mathbb{F}_q) + \#E_{[a',b']}(\mathbb{F}_q) = 2q + 2.$$

Definition 2.57 (Trace of Frobenius). The number of rational points of an elliptic curve E over a finite field \mathbb{F}_q is finite and is denoted by $\#E(\mathbb{F}_q)$. The quantity t defined by

$$t = q + 1 - \#E(\mathbb{F}_q)$$

is called the trace of Frobenius at q .

2.2.4 Isogenies

Definition 2.58 (Morphism). Let E_1 and E_2 be elliptic curves defined over a field K , with respective function fields $\overline{K}(E_1)$ and $\overline{K}(E_2)$. A morphism from E_1 to E_2 is a rational map which is regular (defined) at every point of E_1 .

Definition 2.59 (Isogeny). A non-constant morphism, ϕ , which maps the identity element on

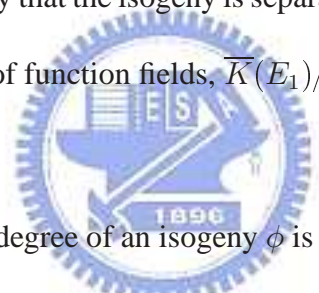
E_1 to the identity element on E_2 is called an isogeny,

$$\phi : E_1 \mapsto E_2.$$

The map which sends every point on E_1 to the identity element ∞ on E_2 is called the zero isogeny. It is the only constant isogeny. Every non-constant isogeny ϕ is surjective over \overline{K} , that is $\phi(E_1) = E_2$. An isogeny is always a group homomorphism, and the kernel of a non-constant isogeny ϕ is always a finite subgroup of $E_1(\overline{K})$. A non-constant isogeny ϕ induces an injection of function fields which fixed \overline{K} ,

$$\phi^* : \overline{K}(E_2) \mapsto \overline{K}(E_1)$$

defined by $\phi^*(f) = f \circ \phi$. We say that the isogeny is separable, inseparable or purely inseparable if the corresponding extension of function fields, $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is separable, inseparable or purely inseparable.



Definition 2.60 (Degree). The degree of an isogeny ϕ is

$$\deg \phi = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)].$$

Definition 2.61 (Frobenius map). The Frobenius map (endomorphism) on an elliptic curve $E(\mathbb{F}_q)$

is

$$\varphi : \begin{cases} E(\overline{\mathbb{F}}_q) & \rightarrow & E(\overline{\mathbb{F}}_q) \\ (x, y) & \mapsto & (x^q, y^q) \\ \infty & \mapsto & \infty \end{cases}$$

The degree n of a separable isogeny ϕ is equal to the size of the kernel of ϕ . The simplest example of a separable isogeny is the multiplication-by- m map. If K is a finite field, the simplest example of a purely inseparable isogeny is the Frobenius endomorphism φ .

Theorem 2.62. Let E denote an elliptic curve defined over a field K and let S denote a finite

subgroup of E which is Galois stable over K , that is, $\varphi(S) = S$. Then there exists an elliptic curve E' , also defined over K , and a unique separable isogeny $\phi : E \mapsto E'$ with kernel equal to S . The notation E/S is often used for the curve E' .

Theorem 2.63 (Dual isogeny). To every non-constant isogeny, ϕ , there is a unique dual isogeny

$$\hat{\phi} : E_2 \mapsto E_1.$$

Theorem 2.64. Two isogenous elliptic curves over a finite field have the same number of rational points.

2.2.5 Elliptic Curves over \mathbb{C}

An elliptic curve over \mathbb{C} defines a lattice in \mathbb{C} , and hence a torus. In Figure 2.4, the lattice will be denoted by $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where $\omega_1, \omega_2 \in \mathbb{C}$ are the periods of the associated, doubly periodic Weierstrass \wp -function

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

The periods, ω_1 and ω_2 , can be suitably chosen so that the quantity

$$\tau = \frac{\omega_1}{\omega_2}$$

lies in the upper half of the complex plane, $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. The map from \mathbb{C}/Λ to points on the corresponding elliptic curve $E_{[a,b]}$ is given by

$$z + \Lambda \mapsto \begin{cases} (\wp(z), \wp'(z)/2), & z \notin \Lambda, \\ \infty, & z \in \Lambda. \end{cases}$$

The coefficients of the elliptic curve are obtained with the formula

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6},$$

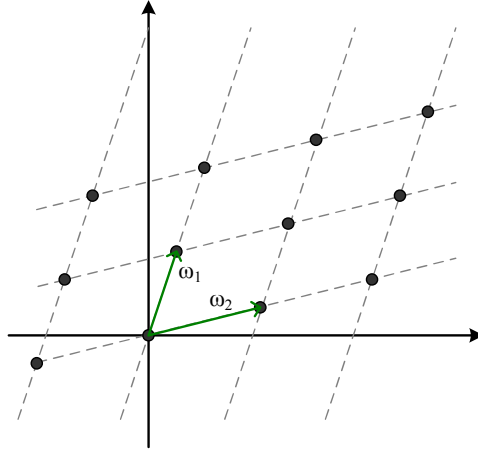


Figure 2.4: Lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

and $a = -g_2/\sqrt[3]{4}$, $b = -g_3$.

An elliptic curve over \mathbb{C} associated to τ is denoted by E_τ . Let $q = e^{2\pi i\tau}$.

Definition 2.65 (Dedekind's η -function).

$$\eta(\tau) = q^{1/24} \left(1 + \sum_{n=1}^{\infty} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right)$$

And $\Delta(\tau) = \eta(\tau)^{24}$. The function $\Delta(\tau)$ is also related to $j(\tau)$ using the formula

$$h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}, \quad j(\tau) = \frac{(256h(\tau) + 1)^3}{h(\tau)}.$$

Moreover, $j(\tau) = j(E_\tau)$ is periodic of period one. So the complex number $\tau \in \mathcal{F} = \{\tau \in \mathbb{C} \mid$

$\text{Im}(\tau) > 0, -1/2 \leq \text{Re}(\tau) \leq 1/2, |\tau| \geq 1\}$ characterizes elliptic curves up to isomorphism.

The Fourier series of $j(\tau)$

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n,$$

where the c_n are positive integers.

2.3 p -adic Arithmetic

The p -adic number system is described first by Hensel in 1897. Different from the real analysis or the complex analysis, it provides the p -adic analysis, alternatively. Here, we only introduce the basic of p -adic numbers.

2.3.1 p -adic Numbers

A p -adic number α can be uniquely written in the form

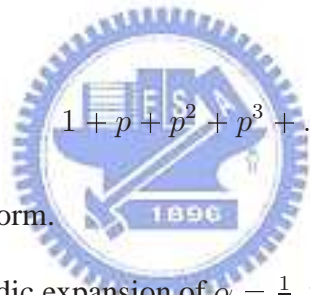
$$\alpha = \sum_{i=n}^{\infty} a_i p^i$$

where each of $a_i \in [0, p - 1]$ and the p -adic norm of the number α is defined as $\|\alpha\| = p^{-n}$.

Note that the series

$$1 + p + p^2 + p^3 + \dots$$

converges to $\frac{1}{1-p}$ in the p -adic norm.



Taking $p = 5$, we obtain 5-adic expansion of $\alpha = \frac{1}{3}$, which can be written in the form

$$\frac{1}{3} = .231313131\dots = .\overline{231}.$$

$$.\overline{231} = 2 + 5 \times \frac{3 + 1 \times 5}{1 - 5^2} = 2 - \frac{5}{3} = \frac{1}{3}.$$

2.3.2 Hensel's Lemma

The first form of Hensel's Lemma is related to our work, so I point out it here.

Lemma 2.66. Let $f(x)$ be a polynomial with integer coefficients, k an integer not less than two and p a prime number. Suppose that r is a solution of the congruence

$$f(r) \equiv 0 \pmod{p^{k-1}}$$

If $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique integer t , $0 \leq t \leq p - 1$, such that

$$f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$$

with t defined by

$$tf'(r) \equiv -\frac{f(r)}{p^{k-1}} \pmod{p}.$$

If, on the other hand, $f'(r) \equiv 0 \pmod{p}$, and in addition, $f(r) \equiv 0 \pmod{p^k}$, then

$$f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$$

for all integers t .

Also, if $f'(r) \equiv 0 \pmod{p}$ and $f(r) \not\equiv 0 \pmod{p^k}$, then $f(x) \equiv 0 \pmod{p^k}$ has no solution for any $x \equiv r \pmod{p^{k-1}}$.



Chapter 3

Schoof-Elkies-Atkin Algorithm

It is crucial for ECC to pick an appropriate elliptic curve. The point counting problem is performed to determine whether a curve is suitable for ECC. Let E be an elliptic curve defined over \mathbb{F}_q , the number of rational points $\#E(\mathbb{F}_q) = q + 1 - t$. Hasse pointed out an important property of the number of the rational points of an elliptic curve in 1933.

Theorem 3.1 (Hasse's Theorem). The t satisfies

$$|t| \leq 2\sqrt{q}$$

In other words, $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$.

3.1 Before Schoof

A naive way to solve the point counting problem is to check whether there are roots of y of $\mathcal{E}(x, y) = 0$ for all elements x of the finite field.

Example 3.2. Let E be an elliptic curve over a prime field \mathbb{F}_p .

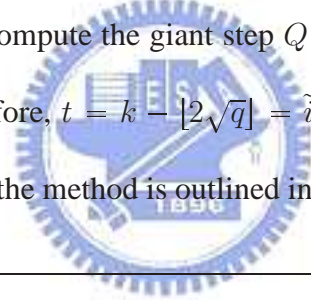
$$E : y^2 = x^3 + ax + b.$$

The number of rational points is

$$\#E(\mathbb{F}_p) = p + 1 - \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$$

where $\left(\frac{\cdot}{p} \right)$ is the Legendre symbol.

There is a sub-exponential time algorithm for point counting problem. It makes use of the concept of Shanks and Mestre Baby-step-giant-step(BSGS). First, it generates a random point P on the curve, and computes $Q = [q + 1 + \lfloor 2\sqrt{q} \rfloor]P$. Since $[q + 1 - t]P = \infty$, $Q = [t + \lfloor 2\sqrt{q} \rfloor]P$. In addition, $-2\sqrt{q} \leq t \leq 2\sqrt{q}$, $t + \lfloor 2\sqrt{q} \rfloor \in [0, 4\sqrt{q}]$. So this problem is reduced to search k satisfying $Q = kP$, and $k \in [0, 4\sqrt{q}]$. Let $m = \lfloor \sqrt{4\sqrt{q}} \rfloor = \lfloor 2q^{(1/4)} \rfloor$. Then k can be written as $a + bm$ for $a, b < m$. Compute each $[i]P$ for $i = 0, 1, \dots, m - 1$ in the baby step. For $j = 0, 1, \dots, m - 1$, compute the giant step $Q - [j]([m]P)$, and find (\tilde{i}, \tilde{j}) such that $[\tilde{i}]P = Q - [\tilde{j}]([m]P)$. Therefore, $t = k - \lfloor 2\sqrt{q} \rfloor = \tilde{i} + \tilde{j}m - \lfloor 2\sqrt{q} \rfloor$ is obtained. The time complexity is $O(q^{(1/4)+\epsilon})$. And the method is outlined in Algorithm 1.



Algorithm 1: BSGS Algorithm for Point Counting

INPUT: An elliptic curve E over a finite field \mathbb{F}_q

OUTPUT: $\#E(\mathbb{F}_q)$

1. Find a random point $P \in E(\mathbb{F}_q)$
2. Compute $Q = [q + 1 + \lfloor 2\sqrt{q} \rfloor]P$
3. Calculate $m = \lfloor 2q^{(1/4)} \rfloor$, and $R = [m]P$
4. For $i = 0, 1, \dots, m - 1$ (Baby step)
 5. Compute $[i]P$, and store $(i, [i]P)$
6. Sort $(i, [i]P)$ pairs by the x -coordinate of $[i]P$
7. For $j = 0, 1, \dots, m - 1$ (Giant step)
 8. Compute $S = Q - [j]R$

9. if there exists $[i]P = S$
 10. $t = i + jm - \lfloor 2\sqrt{q} \rfloor$
 11. Return $q + 1 - t$
-

3.2 Schoof's Idea

The BSGS algorithm for point counting introduced in the previous section is infeasible to find secure curves when q is large. The point counting problem is solved when the trace of Frobenius t is found. In Schoof's point of view, t can be recovered from some t_ℓ by Chinese Remainder Theorem (CRT), where $t_\ell \equiv t \pmod{\ell}$. Because t is bound in $[-2\sqrt{q}, 2\sqrt{q}]$, we have obtained enough t_ℓ such that $\prod \ell > 4\sqrt{q}$ to determine the exact t . From the Prime Number Theorem, the number of primes needed is $O(\log q / \log \log q)$. The largest prime needed is $O(\log q)$.

To find each t_ℓ , we use a zero map of $E(\overline{\mathbb{F}}_q)$. The zero map is related to t . The point of order ℓ can help obtain t_ℓ . Here we describe some materials which are helpful to find each t_ℓ .

The map $(\varphi^2 - [t]\varphi + [q])$ is a *zero map*. That is, $\forall P \in E(\overline{\mathbb{F}}_q)$, $\varphi^2(P) - [t]\varphi(P) + [q]P = \infty$.

The characteristic polynomial of Frobenius map is

$$F(x) = x^2 - tx + q \tag{3.1}$$

However, there may be not a point $P \in E(\mathbb{F}_q)$ of order ℓ for some ℓ . We cannot calculate t_ℓ because of lacking the point of order ℓ in the base field. The following is to avoid the computation on the extension field.

Definition 3.3 (Torsion points). For a positive integer m , m -torsion points of E , denoted by $E[m]$, is defined by

$$E[m] = \{P \in E(\overline{\mathbb{F}}_q) \mid [m]P = \infty\}.$$

Of course, $E[m]$ is a subgroup of $E(\overline{\mathbb{F}}_q)$. If $\gcd(m, q) \neq 1$,

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m.$$

Lemma 3.4. Let m be a positive integer. There exist polynomials $\psi_m, \theta_m, \omega_m \in \mathbb{F}_q[x, y]$. For $P = (x, y) \in E(\overline{\mathbb{F}}_q)$ where $[m]P \neq \infty$,

$$[m]P = \left(\frac{\theta_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3} \right).$$

The polynomial $\psi_m(x, y)$ is called the m -th division polynomial.

Theorem 3.5. Let $P = (x, y)$ be a point in $E(\overline{\mathbb{F}}_q)$, where $[2]P \neq \infty$, and let $m \geq 3$ be an odd integer. Note that $\psi_m(x, y)$ has no y term. Use $\psi_m(x)$, instead. Then, $P \in E[m]$ if and only if $\psi_m(x) = 0$.

Now, the points of order ℓ satisfy $\psi_\ell(x) = 0$. Also, the points satisfy the equation of the elliptic curve. So, the computation is on the polynomial ring $\mathbb{F}_q[x, y]$, and is reduced modulo the curve equation and $\psi_\ell(x)$. Besides, the zero map with respect to ℓ can be written as $(\varphi^2 - [t_\ell]\varphi + [q_\ell])$, here $q_\ell \equiv q \pmod{\ell}$.

The remaining is the case when $\ell = 2$. This case is easy. If the elliptic curve is defined over the field of characteristic two and is not supersingular, $t_2 = 1$. For the curves defined over the field of odd characteristic, $\#E(\mathbb{F}_q) = q + 1 - t$, and q is odd. So $t \equiv \#E(\mathbb{F}_q) \pmod{2}$. According to the group structure, $\#E(\mathbb{F}_q) \equiv 0 \pmod{2}$ if and only if there is a subgroup of order 2. Moreover, the y -coordinate of the points of order 2 is 0. Therefore, if $\mathcal{E}(x, 0)$ has a root in \mathbb{F}_q , $t_2 = 0$. So, t_2 is obtained from the degree of $\gcd(\mathcal{E}(x, 0), x^q - x)$.

This algorithm is briefly listed in Algorithm 2.

Algorithm 2: Schoof's Algorithm

INPUT: An elliptic curve E over a finite field \mathbb{F}_q

OUTPUT: $\#E(\mathbb{F}_q)$

1. Find t_2 , and store $(t_2, 2)$
2. $M = 2, \ell = 3$
3. While $M < 4\sqrt{q}$
4. Calculate $Q(X(x, y), Y(x, y)) = \varphi^2(P) + [q_\ell]P$, where $P(x, y) \in E[\ell]$
5. Calculate $R(X(x, y), Y(x, y)) = \varphi(P)$, where $P(x, y) \in E[\ell]$
6. For $t_\ell = 0, 1, \dots, \frac{\ell-1}{2}$
7. if x -coordinates of $[t_\ell]R$ and Q are the same
8. if y -coordinates of them are the same
9. store (t_ℓ, ℓ)
10. else
11. store $(\ell - t_\ell, \ell)$
12. break
13. $M = M \times \ell, \ell = \text{nextprime}(\ell)$
13. Compute t using (t_ℓ, ℓ) pairs and CRT
14. Return $q + 1 - t$

The routine $\text{nextprime}(\ell)$ will return the smallest prime larger than ℓ .

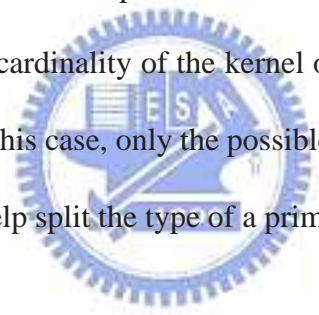
For each ℓ , the computation is in the polynomial ring reduced modulo $\psi_\ell(x)$ of degree $(\ell^2 - 1)/2$. The powers of y are reduced modulo the curve equation, and hence the degree

are at most one in y of the polynomials. The computation of $\varphi^2(P)$ and $\varphi(P)$ is $O(\ell^4 \log q)$ field multiplications. The number of primes needed is $O(\log q / \log \log q)$. So the total time complexity is $O(\log^6 q)$ field multiplications, and is $O(\log^8 q)$ bit operations.

3.3 Atkin's Idea and Elkies' Idea

Though Schoof proposed a polynomial time algorithm for point counting in 1985, it is still too slow to determine the group order of an elliptic curve. After the improvements of Atkin's and Elkies' works, the time complexity of SEA algorithm is $O(\log^6 q)$ bit operations.

The characteristic polynomial of Frobenius map is $x^2 - t_\ell x + q_\ell$ over \mathbb{F}_ℓ . If there is a root of $x^2 - t_\ell x + q_\ell = 0$ on \mathbb{F}_ℓ , ℓ is an Elkies prime. In this case, we can find another curve E_1 , and an isogeny from E to E_1 . The cardinality of the kernel of this isogeny is ℓ . If there is no root on \mathbb{F}_ℓ , ℓ is an Atkin prime. For this case, only the possible t_ℓ are obtained. While t is unknown, the modular polynomials can help split the type of a prime.



3.3.1 Modular Polynomial

The classical modular polynomials, $\Phi_m(x, y)$, play a significant role in SEA algorithm. Here we focus on the case: $m = \ell$, a prime.

Definition 3.6 (Classical modular polynomial).

$$\Phi_\ell(x, j(\tau)) = (x - j(\ell\tau)) \prod_{k=0}^{\ell-1} \left(x - j\left(\frac{\tau + k}{\ell}\right) \right).$$

Then, $\Phi_\ell(x, y) \in \mathbb{Z}[x, y]$.

Lemma 3.7. Let E_1, E_2 be two elliptic curves, there is an isogeny of degree ℓ from E_1 to E_2 if and only if $\Phi_\ell(j(E_1), j(E_2)) = 0$.

Theorem 3.8. [20] Let E be a non-supersingular elliptic curve over \mathbb{F}_q with j -invariant $j \neq 0, 1728$. For an odd prime ℓ , $\Phi_\ell(x, j) \in \mathbb{F}_q[x]$ is a univariate polynomial. Thus, there are three cases of the number of roots of $\Phi_\ell(x, j)$ on \mathbb{F}_q

- (1) One root, or $\ell + 1$ roots. Elkies prime, where $t^2 - 4q \equiv 0 \pmod{\ell}$.
- (2) Two roots. Elkies prime, where $t^2 - 4q$ is a square on \mathbb{F}_ℓ .
- (3) No root. Atkin prime, and all roots lie on \mathbb{F}_{q^r} for some $r \mid \ell + 1$.

In practice, the coefficients of the classical modular polynomial are very large as ℓ increases.

In 1995, Müller proposed alternative modular polynomials, which are $\Phi_\ell^c(x, y)$. First let

$$v = \frac{\ell - 1}{\gcd(12, \ell - 1)}, \quad s = \frac{12}{\gcd(12, \ell - 1)}, \quad f(\tau) = \left(\frac{\eta(\tau)}{\eta(\ell\tau)} \right)^{2s}.$$

Definition 3.9 (Alternative modular polynomials). There exist coefficients $a_{r,k} \in \mathbb{Z}$ such that

$$\sum_{r=0}^{\ell-1} \sum_{k=0}^v a_{r,k} f(\tau)^r j(\ell\tau)^k = 0$$

. Then the alternative modular polynomial is defined by

$$\Phi_\ell^c(x, y) = \sum_{r=0}^{\ell-1} \sum_{k=0}^v a_{r,k} x^r y^k \in \mathbb{Z}[x, y].$$

Alternative modular polynomials satisfy Theorem 3.8. So, the degree of $\gcd(\Phi_\ell^c(x, j), x^q - x)$ is sufficient to disjoin Elkies primes and Atkin primes. For the reason that the modular polynomials can be pre-computed, the complexity to decide the type of a prime ℓ is $O(\ell^2 \log q)$.

The following are the examples of two kinds of modular polynomials.

$$\Phi_3^c(x, y) = x^4 + 36x^3 + 270x^2 - xy + 756x + 729$$

$$\Phi_5^c(x, y) = x^6 + 30x^5 + 315x^4 + 1300x^3 + 1575x^2 - xy + 750x + 125$$

$$\begin{aligned} \Phi_3(x, y) = & x^4 - x^3y^3 + y^4 + 2232(x^3y^2 + x^2y^3) - 1069956(x^3y + xy^3) \\ & + 36864000(x^3 + y^3) + 2587918086x^2y^2 + 8900222976000(x^2y + xy^2) \\ & + 452984832000000(x^2 + y^2) - 770845966336000000xy \\ & + 1855425871872000000000(x + y). \end{aligned}$$

$$\begin{aligned}
\Phi_5(x, y) = & x^6 - x^5y^5 + y^6 + 3720(x^5y^4 + x^4y^5) - 4450940(x^5y^3 + x^3y^5) \\
& + 2028551200(x^5y^2 + x^2y^5) - 246683410950(x^5y + xy^5) \\
& + 1963211489280(x^5 + y^5) + 1665999364600x^4y^4 \\
& + 107878928185336800(x^4y^3 + x^3y^4) \\
& + 383083609779811215375(x^4y^2 + x^2y^4) \\
& + 128541798906828816384000(x^4y + xy^4) \\
& + 1284733132841424456253440(x^4 + y^4) \\
& - 441206965512914835246100x^3y^3 \\
& + 26898488858380731577417728000(x^3y^2 + x^2y^3) \\
& - 192457934618928299655108231168000(x^3y + xy^3) \\
& + 280244777828439527804321565297868800(x^3 + y^3) \\
& + 5110941777552418083110765199360000x^2y^2 \\
& + 36554736583949629295706472332656640000(x^2y + xy^2) \\
& + 6692500042627997708487149415015068467200(x^2 + y^2) \\
& - 264073457076620596259715790247978782949376xy \\
& + 53274330803424425450420160273356509151232000(x + y) \\
& + 141359947154721358697753474691071362751004672000
\end{aligned}$$

3.3.2 Elkies' Improvement

Let ℓ be an Elkies prime. There is an elliptic curve E_1 and an isogeny I_1 such that

$$I_1 : E \mapsto E_1.$$

The degree of I_1 is ℓ , so is the cardinality of $\ker(I_1)$. More precisely, let $P(x, y)$ be a point on $E(\overline{\mathbb{F}}_q)$, then

$$I_1(P(x, y)) = \left(\frac{k_1(x)}{(h_1(x))^2}, \frac{g_1(x, y)}{(h_1(x))^3} \right) \in E_1$$

Since $|\ker(I_1)| = \ell$ and $I_1(\infty) = \infty$, $\deg(h_1(x)) = (\ell - 1)/2$. Note that $\deg(k_1(x)) = \ell$

The curve E_1 and $h_1(x)$ can be derived from the root of $\Phi_\ell^c(x, j)$, $\Phi_\ell^c(x, y)$, and some invariants of E . Here we specify how to find $h_1(x)$ for fields of characteristic greater than three.

First, let $j = j(E)$, and compute a root, g , of the polynomial $\Phi_\ell^c(x, j(E))$. Set

$$\overline{E}_4 = -\frac{a}{3}, \quad \overline{E}_6 = -\frac{b}{2}, \quad \Delta = \frac{\overline{E}_4^3 - \overline{E}_6^2}{1728}.$$

After that,

$$D_g = g \left(\frac{\partial}{\partial x} \Phi_\ell^c(x, y) \right) (g, j), \quad D_j = j \left(\frac{\partial}{\partial y} \Phi_\ell^c(x, y) \right) (g, j)$$

The coefficient of the isogenous curve will be given by \tilde{a} , \tilde{b} and have the associated invariants

$$\overline{E}_4^{(\ell)}, \overline{E}_6^{(\ell)}, \Delta^{(\ell)}$$

$$\Delta^{(\ell)} = \ell^{-12} \Delta g^{\gcd(12, \ell-1)}$$

If $D_j = 0$,

$$\begin{aligned} \overline{E}_4^{(\ell)} &= \ell^{-2} \overline{E}_4, & \tilde{a} &= -3\ell^4 \overline{E}_4^{(\ell)}, & j^{(\ell)} &= \frac{(\overline{E}_4^{(\ell)})^3}{\Delta^{(\ell)}} \\ \tilde{b} &= \pm 2\ell^6 \sqrt{(j^{(\ell)} - 1728)\Delta^{(\ell)}}, & p_1 &= 0. \end{aligned}$$

Now assume $D_j \neq 0$

$$\begin{aligned} s &= \frac{12}{\gcd(12, \ell - 1)}, & \overline{E}_2^* &= \frac{-12\overline{E}_6 D_j}{s\overline{E}_4 D_g}, & g' &= -\frac{s}{12} \overline{E}_2^* g \\ j' &= -\overline{E}_4^2 \overline{E}_6 \Delta^{-1}, & \overline{E}_0 &= \overline{E}_6 (\overline{E}_4 \overline{E}_2^*)^{-1} \end{aligned}$$

Then, we need to compute the quantities

$$\begin{aligned} D'_g &= g' \left(\frac{\partial}{\partial x} \Phi_\ell^c(x, y) \right) (g, j) + \\ &\quad g \left[g' \left(\frac{\partial^2}{\partial x^2} \Phi_\ell^c(x, y) \right) (g, j) + j' \left(\frac{\partial^2}{\partial x \partial y} \Phi_\ell^c(x, y) \right) (g, j) \right] \\ D'_j &= j' \left(\frac{\partial}{\partial y} \Phi_\ell^c(x, y) \right) (g, j) + \\ &\quad j \left[j' \left(\frac{\partial^2}{\partial y^2} \Phi_\ell^c(x, y) \right) (g, j) + g' \left(\frac{\partial^2}{\partial y \partial x} \Phi_\ell^c(x, y) \right) (g, j) \right] \end{aligned}$$

Now, we can determine

$$\overline{E}'_0 = \frac{1}{D_j} \left(\frac{-s}{12} D'_g - \overline{E}_0 D'_j \right)$$

So, we have

$$\overline{E}_4^{(\ell)} = \frac{1}{\ell^2} \left(\overline{E}_4 - \overline{E}_2^* \left[12 \frac{\overline{E}'_0}{\overline{E}_0} + 6 \frac{\overline{E}_4^2}{\overline{E}_6} - 4 \frac{\overline{E}_6}{\overline{E}_4} \right] + \overline{E}_2^{*2} \right)$$

The j -invariant of the isogenous curve

$$j^{(\ell)} = \frac{\overline{E}_4^{(\ell)3}}{\Delta^{(\ell)}}$$

Setting $f = \ell^s g^{-1}$, $f' = \overline{E}_2^* f / \gcd(12, \ell - 1)$

$$D_g^* = \left(\frac{\partial}{\partial x} \Phi_\ell^c(x, y) \right) (f, j^{(\ell)}), \quad D_j^* = \left(\frac{\partial}{\partial y} \Phi_\ell^c(x, y) \right) (f, j^{(\ell)})$$

Finally, we compute

$$j^{(\ell)'} = -\frac{f' D_g^*}{\ell D_j^*} \frac{\overline{E}_6^{(\ell)}}{\overline{E}_4^{(\ell)}} = -\frac{\overline{E}_4^{(\ell)} j^{(\ell)'}}{j^{(\ell)}}$$

Thus, we have three desired quantities as

$$\tilde{a} = -3\ell^4 \overline{E}_4^{(\ell)}, \quad \tilde{b} = -2\ell^6 \overline{E}_6^{(\ell)}, \quad p_1 = -\ell \overline{E}_2^*$$

Therefore, we can use the special value p_1 and the coefficients \tilde{a} , \tilde{b} of curve E_1 , which are derived to find $h_1(x)$.

Let $E_{[a,b]}$ be an elliptic curve defined over a finite field \mathbb{F}_q , then

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

where the coefficients c_k are obtained from the following recursion:

$$c_1 = -\frac{a}{5}, \quad c_2 = \frac{b}{7},$$

and

$$c_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j}, \quad k \geq 3.$$

Let the \wp -Weierstrass functions of E and E_1 be $\wp(z)$ and $\wp_1(z)$, respectively.

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}, \quad \wp_1(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} \tilde{c}_k z^{2k}.$$

Then $h_1(x)$ satisfies the equation

$$z^{\ell-1} h_1(\wp(z)) = \exp \left(-\frac{1}{2} p_1 z^2 - \sum_{k=1}^{\infty} \frac{\tilde{c}_k - \ell c_k}{(2k+1)(2k+2)} z^{2k+2} \right).$$

Using the fact that $h_1(x)$ is a monic polynomial of degree $(\ell-1)/2$, we can figure out $h_1(x)$ by the comparison of the coefficients of z , where the right hand side is expanded by Taylor's series.

Because I_1 is a homomorphism, $\ker(I_1)$ is a subgroup of E . Moreover, $|\ker(I_1)| = \ell$. $\ker(I_1)$ contains a subgroup of $E[\ell]$, also a point of order ℓ . There is an important property that

$$\varphi(P) = [\lambda]P, \quad \text{for } P \in \ker(I_1)$$

where λ is a root of the characteristic polynomial of Frobenius map over \mathbb{F}_ℓ . λ is derived first, and then another root $\mu = q_\ell/\lambda$ on \mathbb{F}_ℓ . Therefore $t_\ell \equiv \lambda + \mu \pmod{\ell}$. Here we can only check the y -coordinates from Müller's work.

Algorithm 3: Elkies Procedure

INPUT: An elliptic curve E over a finite field \mathbb{F}_q , and an Elkies prime ℓ

OUTPUT: t_ℓ

1. Compute the polynomial $h_1(x)$
2. Calculate $Q(X(x, y), Y(x, y)) = \varphi(P)$, where $P \in E$ satisfies $h_1(x)$
3. For $\lambda = 0, 1, \dots, \frac{\ell-1}{2}$
4. if y -coordinates of $[\lambda]P$ and Q are the same
5. $\mu = q_\ell/\lambda$
6. break

7. if the sum of y -coordinates of $[\lambda]P$ and Q is 0
 8. $\lambda = \ell - \lambda, \mu = q_\ell/\lambda$
 9. break
 10. Return $(\lambda + \mu) \pmod{\ell}$
-

In Schoof's algorithm, the points of order ℓ is observed by using the division polynomial $\psi_\ell(x)$ of degree $(\ell^2 - 1)/2$. Elkies improved this part by using $h_1(x)$ of degree $(\ell - 1)/2$. Thus, the complexity of Elkies procedure is $O(\ell^2 \log^3 q)$ bit operations.

3.3.3 Atkin's Method

Let us consider that ℓ is an Atkin prime now. There is no root of $x^2 - t_\ell x + q_\ell = 0$ on \mathbb{F}_ℓ . But the two roots lie on \mathbb{F}_{ℓ^2} .



Theorem 3.10. If the roots of $\Phi_\ell^c(x, j)$ lie on \mathbb{F}_{q^r} , for the smallest r , the roots λ and μ of $x^2 - t_\ell x + q_\ell = 0$ satisfy that $\frac{\lambda}{\mu}$ is an element of order exactly r in \mathbb{F}_{ℓ^2}

Denote the r of Theorem 3.8 of an Atkin prime ℓ by r_ℓ . It can be found by observing the degree of $\gcd(\Phi_\ell^c(x, j), x^{q^i} - x)$ for increasing $i|\ell + 1$. The complexity is $O(\ell^3 \log^3 q)$ bit operations. When r_ℓ is derived, the following is a way to find the set of all possible t_ℓ .

We may let $\mathbb{F}_{\ell^2} = \mathbb{F}_\ell[\sqrt{d}]$ for a quadratic non-residue $d \in \mathbb{F}_\ell$. Since λ and μ lie in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, $\lambda = x_1 + \sqrt{d}x_2, \mu = x_1 - \sqrt{d}x_2$, for some $x_1, x_2 \in \mathbb{F}_\ell$. Also, the order of $\frac{\lambda}{\mu}$ is r_ℓ . Let $\gamma_{r_\ell} = g_1 + \sqrt{d}g_2$ is an element of order r_ℓ for some $g_1, g_2 \in \mathbb{F}_\ell$, then

$$\begin{aligned} g_1 + \sqrt{d}g_2 &= \gamma_{r_\ell} = \frac{\lambda}{\mu} = \frac{\lambda^2}{\lambda\mu} \\ &= \frac{1}{q} (x_1^2 + dx_2^2 + 2x_1x_2\sqrt{d}). \end{aligned}$$

Hence

$$qg_1 \equiv x_1^2 + dx_2^2 \pmod{\ell},$$

$$qg_2 \equiv 2x_1x_2 \pmod{\ell},$$

$$q \equiv x_1^2 - dx_2^2 \pmod{\ell}.$$

$x_1^2 = q(g_1 + 1)/2$, and $t_\ell \equiv 2x_1 \pmod{\ell}$. Hence, possible t_ℓ can be derived from g_1 of γ_{r_ℓ} .

Therefore, the rest of the work is to find out all elements on \mathbb{F}_{ℓ^2} of order exactly r_ℓ . It is easy

because the generator g of \mathbb{F}_{ℓ^2} can be searched quickly. And $\gamma_{r_\ell} = g^{\frac{i(\ell^2-1)}{r_\ell}}$ for $0 < i < r_\ell$ and $\gcd(i, r_\ell) = 1$. Note that the number of possible t_ℓ 's is $\phi(r_\ell)$, where ϕ is Euler totient function.

The procedure is given below.

Algorithm 4: Atkin Procedure

INPUT: An elliptic curve E over a finite field \mathbb{F}_q , and an Atkin prime ℓ

OUTPUT: a set of t_ℓ candidates

1. For $r_\ell = 2, 3, \dots, \ell + 1$, where $r_\ell | \ell + 1$ (Find r_ℓ)
 2. if $\gcd(\Phi_\ell^c(x, j), x^{q^{r_\ell}} - x) \neq 1$
 3. break
 4. Find a quadratic non-residue d
 5. Find a generator g of $\mathbb{F}_\ell[\sqrt{d}]^*$
 6. $S = \{\}$ 7. For $i = 1, 2, \dots, r_\ell - 1$, $\gcd(i, r_\ell) = 1$
 8. Compute $g_1 + \sqrt{d}g_2 = g^{\frac{i(\ell^2-1)}{r_\ell}}$
 9. Find a square root x_1 of $q(g_1 + 1)$ on \mathbb{F}_ℓ
 10. store $\{2x_1, -2x_1\}$ in S
 11. Return S
-

3.3.4 Baby-step-giant-step(BSGS) Strategy

The information from Elkies primes is determinate, while that from Atkin primes is not. Actually, the number of candidates of possible t

$$C = \prod_{\ell \text{ is Atkin}} \phi(r_\ell)$$

There is a sub-exponential time BSGS algorithm for this part.

First, the Atkin primes are partitioned into two sets S_1 and S_2 such that $\prod_{\ell \in S_1} \phi(r_\ell)$ and $\prod_{\ell \in S_2} \phi(r_\ell)$ are roughly the same. Let m_1, m_2 be the products of the primes in S_1, S_2 respectively, and m_3 be the product of Elkies primes. And $t_3 \equiv t \pmod{m_3}$ is determined by CRT.

Suppose $t_1 \equiv t \pmod{m_1}, t_2 \equiv t \pmod{m_2}$. Of course, $m_1 m_2 m_3 > 4\sqrt{q}$. Let

$$M_1 \equiv \frac{1}{m_2 m_3} \pmod{m_1}, M_2 \equiv \frac{1}{m_1 m_3} \pmod{m_2}, M_3 \equiv \frac{1}{m_1 m_2} \pmod{m_3}.$$

By use of CRT, we obtain

$$1 \equiv m_1 m_2 M_3 + m_1 m_3 M_2 + m_2 m_3 M_1 \pmod{m_1 m_2 m_3}$$

$$t \equiv t_3 m_1 m_2 M_3 + t_2 m_1 m_3 M_2 + t_1 m_2 m_3 M_1 \pmod{m_1 m_2 m_3}$$

Let $r_1 \equiv (t_1 - t_3)M_1 \pmod{m_1}, r_2 \equiv (t_2 - t_3)M_2 \pmod{m_2}$, then

$$\begin{aligned} t &\equiv t_3(1 - m_1 m_3 M_2 - m_2 m_3 M_1) + t_2 m_1 m_3 M_2 + t_1 m_2 m_3 M_1 \\ &\equiv t_3 + m_3(m_1 r_2 + m_2 r_1) \pmod{m_1 m_2 m_3} \end{aligned}$$

Now, we write $t = t_3 + m_3(m_1 r_2 + m_2 r_1)$.

Lemma 3.11. If $0 \leq t_3 < m_3$, and $\lfloor \frac{-m_1}{2} \rfloor < r_1 \leq \lfloor \frac{m_1}{2} \rfloor$, then

$$r_2 = \frac{1}{m_1 m_3} (t - t_3 - m_2 m_3 r_1).$$

Thus,

$$\begin{aligned}
|r_2| &\leq \frac{1}{m_1 m_3} (|t| + |t_3| + m_2 m_3 |r_1|) \\
&\leq \frac{2\sqrt{q}}{m_1 m_3} + \frac{1}{m_1} + \frac{m_2}{2} \\
&\leq \frac{m_2}{2} + \frac{1}{m_1} + \frac{m_2}{2}
\end{aligned}$$

So $|r_2| \leq m_2$

Since $\#E(\mathbb{F}_q) = q + 1 - t$, for a point $P \in E(\mathbb{F}_q)$, we have

$$[q + 1]P = [t]P = [t_3 + m_3(m_1 r_2 + m_2 r_1)]P.$$

Therefore,

$$[q + 1 - t_3]P - [r_1 m_2 m_3]P = [r_2 m_1 m_3]P.$$

For each possible t_1 , calculate the corresponding one r_1 , where $|r_1| \leq \frac{m_1}{2}$, and compute the left-hand side in the baby step. For a possible t_2 , calculate two r_2 , where $|r_2| \leq m_2$. Find the pair (r_1, r_2) such that $[q + 1 - t_3]P - [r_1 m_2 m_3]P = [r_2 m_1 m_3]P$. Then t is derived, so is the group order. The complexity of BSGS strategy is $O(\sqrt{C} \log^3 q)$ bit operations.

Algorithm 5: BSGS Strategy

INPUT: $E(\mathbb{F}_q)$, and information gathered from Elkies and Atkin procedure

OUTPUT: $\#E(\mathbb{F}_q)$

1. Divide Atkin primes into two sets S_1, S_2
2. Calculate $t_3 \equiv t \pmod{m_3}$
3. Find a random point $P \in E(\mathbb{F}_q)$
4. For all possible t_1
5. Calculate r_1 , where $|r_1| \leq \frac{m_1}{2}$
6. Compute $Q = [q + 1 - t_3]P - [r_1 m_2 m_3]P$, and store (Q, r_1)
7. Sort (Q, r_1) pairs by the x -coordinate of Q

8. For all possible t_2
 9. Calculate r_2 , where $|r_2| \leq m_2$
 10. Compute $R = [r_2 m_1 m_3]P$
 11. if there exists (Q, r_1) such that $Q = R$
 12. $t = t_3 + m_3(m_1 r_2 + m_2 r_1)$
 13. Return $q + 1 - t$
-

3.3.5 Complexity Analysis

The SEA algorithm uses Schoof's idea, and adds some improvements mentioned above. The following is the outline of SEA algorithm.

The Elkies primes make the complexity decrease. However, the number of Atkin primes is about one half the number of primes considered, which is $O(\log q / \log \log q)$. This means that C of BSGS strategy is exponential in $\log q$. Even though we use the concept of BSGS to speed up the algorithm, this is a sub-exponential time algorithm, unfortunately.

From a complexity-theoretic point of view, we can just use Elkies primes. On this condition, the larger primes are needed due to the skipping of Atkin ones, so are the modular polynomials of higher degree. The best practical compromise is to use some 'best' Atkin primes in order to avoid the use of larger primes and keep away from the sub-exponential time complexity.

Algorithm 6: SEA algorithm

INPUT: An elliptic curve E over a finite field \mathbb{F}_q

OUTPUT: $\#E(\mathbb{F}_q)$

1. $M = 2, \ell = 3, A = \{\}, E = \{\}$

2. Find t_2 , and $E = E \cup (t_2, 2)$
 3. While $M < 4\sqrt{q}$
 4. Determine the type of ℓ
 5. if ℓ is an Elkies prime
 6. Elkies procedure
 7. $E = E \cup (t_\ell, \ell)$
 8. if ℓ is an Atkin prime
 9. Atkin procedure
 10. $A = A \cup (T_\ell, \ell)$, T_ℓ is a set for all possible t_ℓ
 11. $M = M \times \ell$, $\ell = \text{nextprime}(\ell)$
 12. BSGS strategy to determine group order $\#E(\mathbb{F}_q)$
 13. Return $\#E(\mathbb{F}_q)$
-



Chapter 4

Previous Improvements for SEA

Algorithm

There are a lot of improvements of SEA algorithm in recent years. We introduce them in this chapter.



4.1 Isogeny Cycles

This method is proposed by Couveignes and Morain first in 1994[5]. It takes advantage of the Elkies primes. For an Elkies prime ℓ , we find $t_\ell \equiv t \pmod{\ell}$ originally. And the use of isogeny cycles can help us find $t_{\ell^k} \equiv t \pmod{\ell^k}$. The following are theories about the isogeny cycles.

In this section, we suppose that ℓ satisfies condition (2) of Theorem 3.8. The two roots of $\Phi_\ell^c(x, j)$ can be used to derive two different isogenies I_1, I_2 corresponding to the different curves E_1 , and E_2 . That is,

$$I_1 : E \mapsto E_1, \quad I_2 : E \mapsto E_2$$

From the theorem of classical modular polynomials, there are two isogenies of E of degree

ℓ . These isogenies map to E_1 and E_2 separately, where the j -invariant of E_1 and E_2 are roots of $\Phi_\ell(x, j)$. Besides, an isogeny from E to E_1 implies the existence of an dual isogeny from E_1 to E . It means $j = j(E)$ is a root of $\Phi_\ell(x, j(E_1))$. Since the field is finite, the j -invariant of curves found by isogenies are periodic. In addition, the group order of curves are the same. Then, the curves are periodic up to isomorphism. In other words, the curves form a cycle, called the isogeny cycle, and there are two directions to walk along the cycle.

Example 4.1. Let $E: y^2 = x^3 + 68x + 79$, the curves derived from isogenies are as follows:

$[a, b]$	$j(E_{[a,b]})$
[68, 79]	2
[27, 68]	82
[50, 89]	56
[31, 28]	10
[45, 15]	34
[47, 87]	90
[42, 63]	20
[97, 32]	15
[56, 31]	2

If direction 1 is the direction of the cycle of curves as in Example 4.2, direction 2 is in the reverse order of curves. Figure 4.1 represents explicitly the symbols used later on. Note that E_{1111} is $E_{1 \times 4}$ for short. The numbers on the circle are the j -invariants of elliptic curves. The clockwise is direction 1, and direction 2 is counterclockwise. Here the symbol E_{12} is the curve derived from direction 2 of E_1 . More precisely, E_{12} is back to E since $E_{12} \cong E$.

Theorem 4.2. In a direction of the isogeny cycle, suppose from E_1 to $E_{1 \times k}$ does not meet E ,

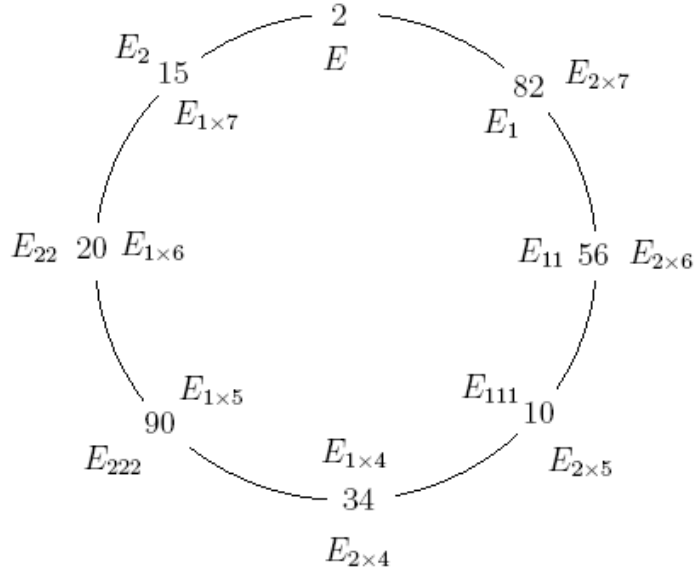


Figure 4.1: Isogeny cycle

that is, the j -invariant of $E_{1 \times i}$ are different for $i = 0, 1, \dots, k$. Then

$$\ker(I_{1 \times k} \circ I_{1 \times k-1} \dots \circ I_{11} \circ I_1) \subset E[\ell^k]$$

Recall that $I_{1 \times i} : E_{1 \times i-1} \mapsto E_{1 \times i}$ defined by

$$I_{1 \times i}(P(x, y)) = \left(\frac{k_{1 \times i}(x)}{(h_{1 \times i}(x))^2}, \frac{g_{1 \times i}(x, y)}{(h_{1 \times i}(x))^3} \right)$$

The points of $\ker(I_{11})$ satisfy $h_{11}(x)$, and the points of $\ker(I_{11} \circ I_1)$ satisfy the numerator of $h_{11} \circ I_1$. Hence, a factor of the division polynomial $\psi_{\ell^2}(x)$ of E is the numerator of

$$h_{11} \left(\frac{k_1(x)}{(h_1(x))^2} \right)$$

Generally, a factor of the division polynomial $\psi_{\ell^k}(x)$ of E is the numerator of $h_{1 \times k} \circ I_{1 \times k-1} \dots \circ I_{11} \circ I_1$. Thus, the degree of the division polynomial $\psi_{\ell^k}(x)$ is $\frac{\ell^{k-1}(\ell-1)}{2}$.

Suppose the characteristic of the field is greater than three. Let I be an isogeny from E to \tilde{E} , the method to figure out the $k_1(x)$ of I is by use of the theories of elliptic curves over \mathbb{C} . First, we have the \wp -Weierstrass functions $\wp(z)$, $\wp_1(z)$ of E and \tilde{E} . Then x -coordinate of the

points in $E(\mathbb{C})$ is $\wp(z)$, and that in $\tilde{E}(\mathbb{C})$ is $\wp_1(z)$. Therefore, there is a relation between them through the isogeny I

$$\wp_1(z) = \frac{k(\wp(z))}{(h(\wp(z)))^2}$$

Recall that

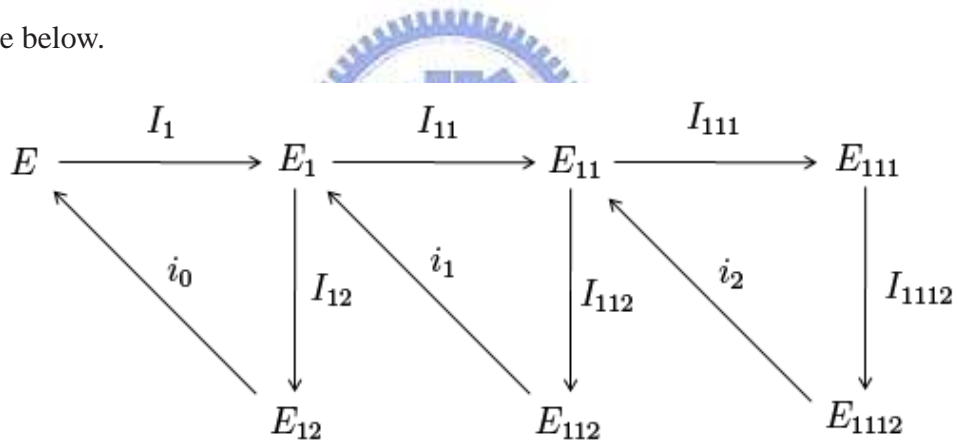
$$z^{\ell-1}h(\wp(z)) = \exp\left(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty} \frac{\tilde{c}_k - \ell c_k}{(2k+1)(2k+2)}z^{2k+2}\right)$$

So we have

$$z^{2\ell-2}k(\wp(z)) = \wp_1(z) \left(\exp\left(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty} \frac{\tilde{c}_k - \ell c_k}{(2k+1)(2k+2)}z^{2k+2}\right) \right)^2$$

Then $k(x)$ can be derived.

There is another strategy to compute a factor of the division polynomial[4]. Let us look at the picture below.



In the picture, i_n are the isomorphism of the curves. h_{12} is a factor of the division polynomial $\psi_\ell(x)$ of E_1 . Then the numerator of $h_{12} \circ i_1 \circ I_{112}$ yields a factor of f_{112} of the division polynomial $\psi_{\ell^2}(x)$ of E_{11} . Similarly, a factor f_{1112} of the division polynomial $\psi_{\ell^3}(x)$ of E_{111} is derived from $f_{112} \circ i_2 \circ I_{1112}$, and so on.

4.2 Re-ordering Atkin Primes

For an Atkin prime ℓ , suppose it produces $\phi(r_\ell)$ candidates of t_ℓ . Izu et al[9, 10] define “Atkin index” of ℓ by

$$i(\ell) = \frac{\phi(r_\ell)}{\ell}$$

They figured out that Atkin primes of smaller index can be used more efficiently for the computation of BSGS strategy. In the next chapter, we will propose another way to rank Atkin primes.

4.3 Virtual (Atkin/Isogeny cycles) Method

Izu et al proposed the virtual method in 1998[9]. The idea is simple. For a prime ℓ , no matter whether it is an Elkies prime or not, we have a set T_ℓ which contains all possible t_ℓ . Note that T_ℓ contains only one candidate for the Elkies prime ℓ . Then the T_{ℓ^2} is obtained as follows.

$$T_{\ell^2} = \{t_\ell + i\ell \mid t_\ell \in T_\ell, 0 \leq i < \ell\}$$

By using this method, it adds an Atkin-like prime into gathered information. However, This is a method worse than using information of Atkin primes. It means that the method does not apply to the case when it skips some information from Atkin. In this point of view, this method can just help speed up the point counting algorithm for elliptic curves defined over a finite field of small cardinality. So, we do not apply this.

4.4 Chinese and Match Method

The BSGS strategy introduced in Section 3.3 is a so-called “Match and Sort” method. The “Chinese and Match” method is proposed by Joux and Lercier in 2000[12]. It is an alternative

way for the same problem. The advantage of this method is to reduce the space complexity. Hence, they can count the number of points of an elliptic curve defined over $\mathbb{F}_{2^{1663}}$ on a network of four PII 300 MHz based PC's using only 12 MB of memory.

This is a method which saves the used space by spending more time. We want to speed up SEA algorithm, so it does not apply to our implementation. However, it is useful for the point counting problem of elliptic curves defined over a finite field of large cardinality.



Chapter 5

Our Three Heuristics for SEA Algorithm

In this chapter, we will introduce our three heuristics for the use of Atkin primes, and Elkies primes, and the method to avoid the sub-exponential time BSGS strategy. We implement SEA algorithm for elliptic curves defined over the prime field \mathbb{F}_q , where $q = p > 3$. We will also point out some ideas, and give a brief explanation.

We use the MIRACL[27](Multiprecision Integer and Rational Arithmetic C/C++ Library) library in our implementation. More than being a big number library, MIRACL provides univariate and bivariate polynomial type with big number coefficient, the big integer modulo n arithmetic, the polynomial ring, the elliptic curve arithmetic, and some tools of number theory, such as CRT, cryptographic secure random number generator, etc. Also, MIRACL contains a simple version of SEA algorithm implementation.

5.1 Atkin Selection Heuristic

Because of the sub-exponential time complexity while using information of Atkin primes, the ‘best’ Atkin primes have to be figured out by some evaluations. The goal is to reduce the number of candidates of possible t . The first approach ranks Atkin primes ℓ in order of $\phi(r_\ell)$. Thus, it is

straightforward to pick the Atkin primes of smaller $\phi(r_\ell)$. Izu et al proposed the index of Atkin primes introduced in the previous chapter.

Example 5.1. Let 5, 11, and 29 be Atkin primes, and let $r_5 = 3$, $r_{11} = 12$, $r_{29} = 15$.

ℓ	r_ℓ	$\phi(r_\ell)$	$i(\ell)$
5	3	2	0.4
11	12	4	$0.\overline{36}$
29	15	8	0.276

Here we can easily find that it is better to use 5 and 11 rather than 29 because the number of possibilities are the same while $5 \times 11 > 29$.

Let m_3 be the product of Elkies primes encountered, and A be the product of selected Atkin primes. Since Elkies primes are never skipped, the Atkin primes are selected enough such that $m_3 \times A > 4\sqrt{q}$. So A has the lower bound $4\sqrt{q}/m_3$. Also, the smaller C , the number of possible t , is better. In Izu's point of view,

$$\frac{C}{A} = \prod_{\ell \text{ selected Atkin primes}} \frac{\phi(r_\ell)}{\ell}$$

Therefore, if the smaller index of Atkin primes, the better. If the number of selected Atkin primes is fixed, this may work. However, we may use more small Atkin primes to gain the smaller $\frac{C}{A}$ as Example 5.1.

The problem of Izu's index is that it does not consider the length of ℓ . Here, we define the rank of an Atkin prime ℓ by

$$R(\ell) = \log \phi(r_\ell) / \log \ell$$

We can see $R(\ell)$ simply as the number of bits of C caused by each bit of ℓ averagely. Thus, the Atkin prime is 'best' if and only if the number of bits of C is less. Therefore, the 'best' Atkin prime are those of smaller $R(\ell)$.

Example 5.2. The same example as Example 5.1.

ℓ	r_ℓ	$\phi(r_\ell)$	$R(\ell)$
5	3	2	0.43
11	12	4	0.58
29	15	8	0.62

Here we can see that our method can figure out the error of the index of Atkin primes.

From the same point of view, now we consider the virtual method introduced in Section 4.3. The new information from it causes an imaginary Atkin prime of $R(\ell) = 1$. That is the worst one. We propose a real example below.

Example 5.3. Let $E : y^2 = x^3 - 3x + 10$ defined over \mathbb{F}_q , $q = 2^{384} - 317$ is a prime. 2, 3, 13, 23, 29, 31, 43, 47, 59, 61, 67, 71, 73, 89, 101, 107, 109, 131, 137, 139, 167, 173, 223, 233, 239 are Elkies primes. The lower bound of A is about 6.6×10^{13} . The following are the selected Atkin primes according to the three methods.

Rank in order of $\phi(r_\ell)$			Rank in order of $i(\ell)$				Rank in order of $R(\ell)$			
ℓ	$\phi(r_\ell)$	Selected	ℓ	$\phi(r_\ell)$	$i(\ell)$	Selected	ℓ	$\phi(r_\ell)$	$R(\ell)$	Selected
5	2	Drop	79	4	0.05	*	79	4	0.32	*
79	4	*	127	8	0.06	*	127	8	0.429	*
11	4	*	53	6	0.11	*	5	2	0.431	Drop
7	4	*	151	18	0.12	*	53	6	0.45	*
53	6	*	179	24	0.13	*	41	6	0.48	*
41	6	*	41	6	0.15	*	151	18	0.576	*
17	6	*	191	32	0.17	*	11	4	0.578	*
127	8	*	17	6	0.35		179	24	0.61	*

19	8	*	11	4	0.36	17	6	0.63	*
151	18	*	5	2	0.4	191	32	0.66	
179	24		19	8	0.42	19	8	0.706	
191	32		7	4	0.57	7	4	0.712	
$C = 15925248$			$C = 15925248$			$C = 11943936$			
$A = 8.2 \times 10^{13}$			$A = 1.1 \times 10^{14}$			$A = 1.1 \times 10^{14}$			

Table 5.1: Evaluation methods of Atkin primes

The Atkin primes are selected one by one until the product A of selected ones is larger than the lower bound. Then, the check goes through the selected Atkin primes in order to drop some selected ones if they are not necessary. In other words, the product A is larger than the lower bound. In Example 5.3, we can see the comparison of A and C of the previous two methods. The C of these are the same, but the index is much better due to the larger A . To compare the results of the last two, although the A of the two methods are almost the same, the rank of Atkin primes is better in the third by reason of the smaller C .

While using the information from Atkin primes, we just select some for the reason of avoiding a waste of time in BSGS strategy. We have mentioned that the complexity is $O(\ell^3 \log^3 q)$ to find r_ℓ for each Atkin prime ℓ . Thus, whenever we can choose enough Atkin primes such that $m_3 \times A > 4\sqrt{q}$, we can get the largest value R of $R(\ell)$ of the selected Atkin primes. After that, we never select the Atkin primes ℓ of $R(\ell)$ larger than R . Therefore, we do not need to collect the Atkin primes ℓ of $R(\ell) > R$. So, this can help us save time to find r_ℓ of ℓ if the candidate of r_ℓ makes $R(\ell) > R$.

5.2 Elkies Isogeny Heuristic

If an Elkies prime ℓ occurs, the factor $h_1(x)$ of the division polynomial is figured out. After that, λ , a root of the characteristic polynomial of Frobenius map over \mathbb{F}_ℓ , is computed via checking the y -coordinates of $\varphi(P) = (x^q, y^q)$ and $[\lambda]P$.

In our consideration, the curve

$$E_{[a,b]} : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q,$$

and the division polynomials simplify to

$$\begin{aligned} \psi_0 &= 0, \\ \psi_1 &= 1, \\ \psi_2 &= 2y, \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2, \\ \psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m/2y, \quad m > 2 \end{aligned}$$

For a positive integer $m > 2$, and a point $P(x, y)$ of E such that $[m]P \neq \infty$,

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3} \right)$$

The implementation of Elkies procedure of MIRACL library hides y term of ψ_{2m} but keeps it in mind. When y^2 occurs, it is replaced by using the curve equation. Therefore, the division polynomials are computed by the following recursion. Note that $\bar{f}_{2k+1} = \psi_{2k+1}$ and $y\bar{f}_{2k} = \psi_{2k}$

$$\begin{aligned}
\bar{f}_0 &= 0, \\
\bar{f}_1 &= 1, \\
\bar{f}_2 &= 2, \\
\bar{f}_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\bar{f}_4 &= 4x^6 + 20ax^4 + 80bx^3 - 20a^2x^2 - 16abx - 32b^2 - 4a^3, \\
\bar{f}_{4k+1} &= \psi_{2k+2}\psi_{2k}^3 - \psi_{2k-1}\psi_{2k+1}^3 \\
&= \bar{f}_{2k+2}\bar{f}_{2k}^3y^4 - \bar{f}_{2k-1}\bar{f}_{2k+1}^3 \\
&= \bar{f}_{2k+2}\bar{f}_{2k}^3(x^3 + ax + b)^2 - \bar{f}_{2k-1}\bar{f}_{2k+1}^3, \\
\bar{f}_{4k+3} &= \psi_{2k+3}\psi_{2k+1}^3 - \psi_{2k}\psi_{2k+2}^3 \\
&= \bar{f}_{2k+3}\bar{f}_{2k+1}^3 - \bar{f}_{2k}\bar{f}_{2k+2}^3y^4 \\
&= \bar{f}_{2k+3}\bar{f}_{2k+1}^3 - \bar{f}_{2k}\bar{f}_{2k+2}^3(x^3 + ax + b)^2, \\
\bar{f}_{4k} &= \psi_{4k}/y \\
&= ((\psi_{2k+2}\psi_{2k-1}^2 - \psi_{2k-2}\psi_{2k+1}^2)\psi_{2k}/2y)/y \\
&= ((y\bar{f}_{2k+2}\bar{f}_{2k-1}^2 - y\bar{f}_{2k-2}\bar{f}_{2k+1}^2)y\bar{f}_{2k}/2y)/y \\
&= (\bar{f}_{2k+2}\bar{f}_{2k-1}^2 - \bar{f}_{2k-2}\bar{f}_{2k+1}^2)\bar{f}_{2k}/2, \\
\bar{f}_{4k+2} &= \psi_{4k+2}/y \\
&= ((\psi_{2k+3}\psi_{2k}^2 - \psi_{2k-1}\psi_{2k+2}^2)\psi_{2k+1}/2y)/y \\
&= ((\bar{f}_{2k+3}y^2\bar{f}_{2k}^2 - \bar{f}_{2k-1}y^2\bar{f}_{2k+2}^2)\bar{f}_{2k+1}/2y)/y \\
&= (\bar{f}_{2k+3}\bar{f}_{2k}^2 - \bar{f}_{2k-1}\bar{f}_{2k+2}^2)\bar{f}_{2k+1}/2.
\end{aligned}$$

If we pre-compute the square and cube of a division polynomial and $(x^3 + ax + b)^2$, it costs five polynomial multiplication to compute a division polynomial, where two is for the pre-computation step.

The y -coordinate of $\varphi(P(x, y))$,

$$y^q = y(x^3 + ax + b)^{\frac{q-1}{2}}$$

Hence, let $Y_{q-1} = (x^3 + ax + b)^{\frac{q-1}{2}}$. Then, $y^q = yY_{q-1}$. The way to check the y -coordinates of $\varphi(P(x, y))$ and $[m]P$ is to compare

$$y^q = yY_{q-1}, \text{ and } \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3}$$

Thus, we compare $4y^2\psi_m^3Y_{q-1}$ and $(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$.

Case $m = 1$,

$$\frac{y}{yY_{q-1}} = \frac{1}{Y_{q-1}}$$

Case $m = 2k$,

$$\frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y^2\psi_m^3Y_{q-1}} = \frac{y\bar{f}_{2k+2}\bar{f}_{2k-1}^2 - y\bar{f}_{2k-2}\bar{f}_{2k+1}^2}{4y^5\bar{f}_{2k}^3Y_{q-1}} = \frac{\bar{f}_{2k+2}\bar{f}_{2k-1}^2 - \bar{f}_{2k-2}\bar{f}_{2k+1}^2}{4(x^3 + ax + b)^2\bar{f}_{2k}^3Y_{q-1}}$$

Case $m = 2k + 1$,

$$\frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y^2\psi_m^3Y_{q-1}} = \frac{\bar{f}_{2k+3}y^2\bar{f}_{2k}^2 - \bar{f}_{2k-1}y^2\bar{f}_{2k+2}^2}{4y^2\bar{f}_{2k+1}^3Y_{q-1}} = \frac{\bar{f}_{2k+3}\bar{f}_{2k}^2 - \bar{f}_{2k-1}\bar{f}_{2k+2}^2}{4\bar{f}_{2k+1}^3Y_{q-1}}$$

For each case above, whether the denominator and the numerator are the same, or the sum of them is 0, corresponding to $\lambda = m$ or $\lambda = \ell - m$, the check costs three polynomial multiplications for odd m , and four for even m . The expected number of polynomial multiplication needed is $(5 \times \frac{\ell}{4} + 3.5 \times \frac{\ell}{4}) = \frac{17}{8}\ell$.

As the concept indicates, there are two processes of isogeny cycles. The first one is to compute a factor of division polynomial $\psi_{\ell^k}(x)$, and search $\lambda \pmod{\ell^k}$. The expected number of polynomial multiplication needed is $(5 \times \frac{\ell^k}{4} + 3.5\frac{\ell^k}{4}) = \frac{17}{8}\ell^k$.

The second process is to find the $\lambda \pmod{\ell^i}$ for each $i < k$. That means finding $\lambda \pmod{\ell^i}$ by use of $\lambda \pmod{\ell^{i-1}}$. Suppose $\lambda \equiv a \pmod{\ell^{i-1}}$, then the candidates of $\lambda \pmod{\ell^i}$ are $a + h\ell^{i-1}$ for $h = 0, 1, \dots, \ell - 1$. It does not mean that the expected number of the division polynomials needed increases to $(\frac{\ell^k}{2})$ in this case. Here, we still can use the negative checking.

Example 5.4. Suppose $\lambda \equiv 3 \pmod{13}$, then $\lambda \equiv 3 + 13h \pmod{13^2}$ for some $0 \leq h \leq 12$.

Here assume $\lambda \equiv 3 + 13\tilde{h} \pmod{13^2}$. $\varphi(P) = [3 + 13\tilde{h}]P$. Since $P \in E[13^2]$,

$$-\varphi(P) = [-3 - 13\tilde{h}]P = [13^2 - 3 - 13\tilde{h}]P = [-3 + 13(13 - \tilde{h})]P$$

Therefore, in this example, we can do negative checking for $7 \leq h \leq 12$.

$$\varphi(P) = [3 + 13 \times 7]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 7)]P$$

$$\varphi(P) = [3 + 13 \times 8]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 8)]P$$

$$\varphi(P) = [3 + 13 \times 9]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 9)]P$$

$$\varphi(P) = [3 + 13 \times 10]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 10)]P$$

$$\varphi(P) = [3 + 13 \times 11]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 11)]P$$

$$\varphi(P) = [3 + 13 \times 12]P \Rightarrow -\varphi(P) = [-3 + 13(13 - 12)]P$$

Now, λ can be derived. To determine the $t \pmod{\ell^k}$, μ is needed. For the case $k = 1$, $\mu = q_\ell/\lambda \pmod{\ell}$. For the case $k = s > 1$, we have $\lambda \pmod{\ell^s}$, and $\mu \pmod{\ell^{s-1}}$. In fact, $\lambda\mu \equiv q_{\ell^s} \pmod{\ell^s}$. The $\mu \pmod{\ell^s}$ can be calculated from the Hensel's Lemma.

Example 5.5. Suppose $q = 157$, and $\lambda \equiv 1 \pmod{7}$, $\mu \equiv 3 \pmod{7}$. Also, $\lambda \equiv 22 \pmod{7^2}$. Then, let $f(x) = Ax - B$, where $A = 22 = \lambda \pmod{7^2}$, $B = 10 = 157 \pmod{7^2}$.

By Hensel's Lemma,

$$sf'(\mu) \equiv -\frac{f(\mu)}{7} \pmod{7}$$

So, $s = 6$, and $\mu = 3 + 6 \times 7 = 45$.

Therefore, in this case the expected number of polynomial multiplication needed is $(5 \times \frac{\ell^k}{4} + 3.5 \times \frac{\ell}{2}) = (\frac{5}{4}\ell^k + \frac{7}{4}\ell)$

Now, we analyze the computing cost. The complexity of the polynomial multiplication reduced modulo a polynomial of degree n is $O(n \log n)$ via fast Fourier transformation(FFT), say $w_1 n \log n$, where w_1 is a constant.

First, we define some terms for further analysis. First, T_{ℓ^1} denotes the computing time to derive t_ℓ for an Elkies prime ℓ . Then,

$$T_{\ell^1} = \log q \cdot w_1(\ell + 1) \log(\ell + 1) + \left(\log \left(\frac{q-1}{2} \right) + \frac{17}{8} \ell \right) \cdot w_1 \left(\frac{\ell-1}{2} \right) \log \left(\frac{\ell-1}{2} \right).$$

The first part is to determine a root of $\Phi_\ell^c(x, j(E))$. The second part is to compute Y_{q-1} and derive $\lambda \pmod{\ell}$. Similarly, T_{ℓ^k} denotes the computing time to derive t_{ℓ^k} for $k > 1$ where

$$T_{\ell^k} = \log q \cdot w_1(\ell+1) \log(\ell+1) + \left(\log \left(\frac{q-1}{2} \right) + \frac{5}{4} \ell^k + \frac{7}{4} \ell \right) \cdot w_1 \left(\frac{\ell^{k-1}(\ell-1)}{2} \right) \log \left(\frac{\ell^{k-1}(\ell-1)}{2} \right).$$

Since the information from Elkies primes is definite, it is important to increase the product of these primes and prime powers. The concept is the same as Section 5.1 that we select the prime ℓ or prime powers ℓ^k whose $T_{\ell^i} / \log \ell$ is small. This value represents the computing cost to gain the information caused by each bit of ℓ averagely.

Example 5.6. Let $q = 2^{512} - 569$, then the following is the value $T_{\ell^i} / \log \ell$ with respect to each ℓ, i pairs. Note that we set $w_1 = 1$ here.

ℓ	i	$T_{\ell^i} / \log \ell$	ℓ	i	$T_{\ell^i} / \log \ell$	ℓ	i	$T_{\ell^i} / \log \ell$	ℓ	i	$T_{\ell^i} / \log \ell$
3	1	1365	5	1	1695	3	2	1797	7	1	1939
11	1	2297	13	1	2438	17	1	2673	19	1	2774
23	1	2954	29	1	3183	31	1	3251	37	1	3438
41	1	3552	5	2	3555	43	1	3605	47	1	3708
53	1	3852	59	1	3986	61	1	4029	67	1	4153
3	3	4170	71	1	4232	73	1	4271	79	1	4384

5.3 Polynomial-Time BSGS Heuristic

Let us review the BSGS strategy in which lie some tricks to speed up. The Atkin primes are first divided into two sets S_1 , and S_2 . Let c_1 and c_2 be the number of possible t corresponding

to S_1 and S_2 . After that, the baby step performs c_1 times to calculate t_1 , and the corresponding $|r_1| < \frac{m_1}{2}$, and then $Q_{r_1} = [q + 1 - t_3]P - [r_1 m_2 m_3]P$. So, we can reduce the time of scalar multiplication of a point by pre-computation of $[m_2 m_3]P$. Therefore, the complexity of baby step is $O(c_1 \log m_1)$ elliptic curve point addition.

Similarly, in the giant step, the computation of $[m_1 m_3]P$ reduces the time to compute $[r_2 m_1 m_3]P$. Moreover, there are two r_2 , say r_{2_1} and r_{2_2} , for a t_2 . Since $|r_{2_1} - r_{2_2}| = m_2$, we can derive $[r_{2_2} m_1 m_3]P$ from $[r_{2_1} m_1 m_3]P$ and $[m_1 m_2 m_3]P$. Thus, the complexity of giant step is $O(c_2 \log m_2)$ elliptic curve point addition.

In addition, the baby step is performed completely, while the giant step is not. In probabilistic estimation, the giant step is half performed. Hence, it is better to choose the set of small number of possible t to perform the baby step. Hence, the computing cost B of BSGS strategy is about



$$B = w_2 \times \frac{3}{2} \sqrt{C} \log A,$$

where w_2 is a constant.

It costs much time in BSGS strategy if C is too large. The traditional way out of this problem is to set a threshold T for C . However, it does not seem a good way to decide the time to perform BSGS strategy. If T is big, it may cost more time in BSGS strategy of the algorithm. But the small T may cause a waste of time to use the larger primes. Here, we propose a method to estimate T dynamically. After the Atkin primes selection strategy, we can estimate the computing time B used by BSGS strategy. On the other hand, we also suppose that the next prime is Elkies, and estimate the time B' which is taken by gathering the information of the next prime, and then the BSGS strategy after we have the information from the next prime.

If $B < B'$, then our implementation will perform BSGS strategy. Otherwise, the information of the next prime is collected. Thus, the next stage of the algorithm depends on the gathered

information of each elliptic curve. Therefore, we can prevent from the use of larger primes, and can detect whether C is too big. This method can always be suitable for any curve.

5.4 Numerical Results

The computing environment we use is Intel Xeon 3040 Processor with 1.86GHz, 2G RAM on FreeBSD 7.0 with the MIRACL library version 5.3.2. At first, we calculated the order of 50, 40, 30, 20, 10 different elliptic curves corresponding to the prime of 160-bit, 192-bit, 256-bit, 384-bit, and 512-bit by use of the original SEA algorithm. The average time is listed in Table 5.2.

Bits of q	160	192	256	384	512
Average time(s)	9.91	26.51	90.73	607.8	2654

Table 5.2: Average computing time of original SEA algorithm

Next, we calculated the order of the same elliptic curves as before by applying the Atkin selection heuristic. The average time and the improvement rate compared with the original one are in Table 5.3.

# bits of q	160	192	256	384	512
Average time(s)	9.68	26.02	87.20	574.9	2412
Improve rate(%)	2.33	1.84	3.89	5.42	9.10

Table 5.3: Average computing time when applying Atkin selection heuristic

When the number of bits of q increases, we need to use more primes. Hence, we encounter more Atkin primes, which are almost useless for us. The Atkin selection heuristic can save the

time, whose complexity is $O(\ell^3 \log^3 q)$, to find out the r_ℓ of the ‘bad’ Atkin primes. Therefore, the impact is more evident when q is large.

Table 5.4 shows the numerical result of applying the Elkies isogeny heuristic.

# bits of q	160	192	256	384	512
Average time(s)	9.68	25.27	83.95	557.0	2296
Improve rate(%)	2.30	4.67	7.47	8.37	13.48

Table 5.4: Average computing time when applying Elkies isogeny heuristic

The effect of the isogeny cycle is to reuse the Elkies primes. This is necessary if q is larger because of the increasing number of the encountered Atkin primes. So, the result presents that the improvement is obvious when q is large.

The result of the improvement of the polynomial-time BSGS heuristic is shown in Table 5.5.

# bits of q	160	192	256	384	512
Average time(s)	9.49	25.43	80.02	545.1	2278
Improve rate(%)	4.19	4.07	11.81	10.31	14.16

Table 5.5: Average computing time when applying polynomial-time BSGS heuristic

# bits of q	160	192	256	384	512
Average time(s)	9.11	23.86	73.18	464.3	1899
Improve rate(%)	8.03	10.01	19.34	23.61	28.43

Table 5.6: Average computing time when applying three heuristics

This heuristic brings an effective way to improve the algorithm as we can see. The result

also tells that it can prevent from the use of larger primes, and can detect whether C is too big, indeed.

Finally, if the three heuristics are applied to original SEA algorithm, then we get the result in Table 5.6.



Chapter 6

Conclusion & Future Work

In this thesis, we propose three heuristics to speed up the SEA algorithm. These three heuristics are more effective for large q . Besides, we use the pre-computation skill to speed up the part of BSGS strategy. And we also propose the negative checking for the isogeny cycles.

Although our implementation is for the elliptic curves defined over prime fields, the heuristics can be applied to the SEA algorithm for elliptic curves defined over binary fields \mathbb{F}_q , where $q = 2^n$. Furthermore, the idea of analysis in the Atkin selection heuristic and also in the Elkies isogeny heuristic may be applied to others.

There are some improvements that mentioned by Couveignes[4]. It can help find a factor of the division polynomial of smaller degree.

In the future, we will prepare to implement SEA algorithm for elliptic curves defined over binary fields. Also, we will study the theoretical part of elliptic curves, especially the part related to SEA algorithm. Moreover, there exists Satoh's method[19], which uses p -adic analysis to find the order of elliptic curves defined over finite fields of small characteristic, such as binary fields.

Bibliography

- [1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993.
- [2] M. Bellare and P. Rogaway. Minimizing the use of random oracles in authenticated encryption schemes. In *ICIS: International Conference on Information and Communications Security (ICIS)*, LNCS, 1997.
- [3] I. F. Blake and N. P. Smart C. Seroussi. *Elliptic Curves in Cryptography*. Cambridge University Press, 2000.
- [4] J. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm, LIX/RR/96/03, 1996.
- [5] J. Couveignes and F. Morain. Schoof’s algorithm and isogeny cycles. In *ANTS*, pages 43–58, 1994.
- [6] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Proceedings of the Fifth International Conference on Finite Fields and Applications*, 2001. to appear. Also available from <http://www.exp-math.uni-essen.de/>.
- [7] G. Frey and H. Rück. A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.
- [8] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive, Report 2004/073, 2004. <http://eprint.iacr.org/2004/073/>.
- [9] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Parameters for secure elliptic curve cryptosystem - improvements on schoof’s algorithm. In *Public Key Cryptography*, volume 1431, pages 253–257, 1998.
- [10] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Efficient implementation of Schoof’s algorithm, *Advances in Cryptology – Asiacrypt ’98*, Lecture Notes in Computer Science, 1514 (1999), Springer-Verlag, 66–79.
- [11] D. Johnson and A. Menezes. D. Johnson and A. Menezes, The Elliptic Curve Digital Signature Algorithm (ECDSA), Univ. of Waterloo, 1999, <http://cacr.math.uwaterloo.ca>

- [12] A. Joux and R. Lercier. “chinese match”, an alternative to atkin’s “match and sort” method used in the sea algorithm.
- [13] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
- [14] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. An efficient protocol for authenticated key agreement. *Des. Codes Cryptography*, 28(2):119–134, 2003.
- [15] V. Müller. *Ein Algorithmus zur Bestimmung der Punktzahl elliptischer Kurven über endlichen Körpern der Charakteristik grösser drei*. PhD thesis, Universität des Saarlandes, 1995.
- [16] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *STOC ’91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, New York, NY, USA, 1991. ACM.
- [17] V. Miller. Use of elliptic curves in cryptography. In *CRYPTO ’85: Advances in Cryptology*, pages 417–426, London, UK, 1986. Springer-Verlag.
- [18] H. Rück. On the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 68(226):805–806, 1999.
- [19] T. Satoh. The canonical lift of an ordinary elliptic curve over a prime field and its point counting. *Journal of the Ramanujan Mathematical Society*, 15:247–270, 2000.
- [20] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Mathematics of Computation*, 44(170):483–494, 1985.
- [21] R. Schoof. Counting points on elliptic curves over finite fields. *J. Th’eor. Nombres Bordeaux* 7 (1995), 219–254.
- [22] D. Shanks. Class number, a theory of factorization, and genera. *Proceedings of Symposia in Pure Mathematics*, 20:415–440, 1971.
- [23] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1994.
- [24] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(3):193–196, 1999.
- [25] N. P. Smart. Elliptic curve cryptosystems over small fields of odd characteristic. *Journal of Cryptology*, 12(2):141–151, 1999.
- [26] NIST Recommended Key Sizes http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm
- [27] MIRACL (Multiprecision Integer and Rational Arithmetic C/C++ Library) <http://www.shamus.ie/>