M.Tech.(Computer Science) Dissertation Series

Counting The Number of Points on Elliptic Curve over Finite Field of Characteristic greater than Three

A dissertation submitted in partial fulfillment of the requirements for the M.Tech.(Computer Science) degree of the Indian Statistical Institute

By

Tapas Pandit

Roll No : CS0610

Under the supervision of

Prof. Rana Barua

Indian Statistical Institute
203, B.T. Road
Kolkata- 700108

INDIAN STATISTICAL INSTITUTE
203, B.T.Road
Kolkata - 700108

Certificate of Approval

This is certify that this dissertation thesis titled “Counting the number of points on Elliptic Curve of characteristic greater than three” submitted by Mr. Tapas Pandit, in partial fulfillment of the requirements for the M.Tech. (Computer Science) degree of the Indian Statistical Institute, Kolkata, embodies the work done under my supervision.

....
Prof. Rana Barua
Stat-Math Unit
Indian Statistical Institute, Kolkata
Kolkata - 700108

Acknowledgements

With great pleasure and sense of obligation I express my heartfelt gratitude to my guide and supervisor **Prof**. **Rana Barua** of Stat-Math Unit, Indian Statistical Institute, Kolkata. I am highly indebted to him for his invaluable guidance and ever ready support. His persisting encouragement, perpetual motivation, everlasting patience and excellent expertise in discussions, during progress of Project Work, have benefited to an extent, which is beyond expression.

The chain of my gratitude would be definitely incomplete without expressing my gratitude to all my batch mates, for their support and encouragement throughout the entire M.Tech course.I sincerely thank all my friends and well wishers who helped me directly or indirectly towards the completion of this work. Lastly I must acknowledge the consistent encouragement and support from my senior Sumit da.

Tapas pandit
CS0610,
Indian Statistical Institute,
Kolkata - 700108.

Contents

1 Introduction **5**

1.1 **Elliptic curve over prime field $\mathbb{F}_p$ with $p > 3$** 6

1.1.1 **Newtons formula** 6

1.1.2 **Finding discriminant of $y^2 = x^3 + Ax + B$** 6

1.1.3 **Addition law** 7

2 Sketch of Schoof's Algorithm **10**

2.1 **Algebra and Number Theory** 10

2.2 **Torsion Points** 10

2.3 **Endomorphism** 11

2.3.1 **Frobenius map** 12

2.4 **Division Polynomials** 13

2.5 **The Weil Pairing** 14

2.6 **Counting number of points on Elliptic Curve over Finite Field** 15

2.6.1 **Schoof's Algorithm** 16

3 Modified Schoof's Algorithm **21**

3.1 **Analysis of the degree of $\phi_p - 1$** 21

3.2 **Some result using type of the elliptic curves** 22

3.3 **Discriminant Analysis** 23

3.3.1 **Discriminant based algorithm for irreducibility testing** 26

3.3.2 **Complexity** 29

3.3.3 **Examples** 30

3.4 **Conclusion** 30

4 Appendix **31**

Chapter 1

Introduction

The security of discrete logarithm based cryptosystem relies mainly on the order of the underlying group, unless special structures allow more efficient algorithms for breaking the system. If the group order is large enough, then square root attacks like Shank's baby-step giant-step or pollard's p-methods are not applicable. Also it is a good strategy to make sure that the group order contains a large prime factor, to prevent the Pohlig-Hellman attack. There are many way to choose an elliptic curves so that above attacks are not possible. The most secure way of selecting a curve is to fix an underlying field, randomly choose a curve and compute the group order until it is divisible by large prime and an Elliptic Curve Cryptosystem is designed using that elliptic curve. There are many algorithm to count such number. First Hasse gave a bound for that count. After that Baby step, Giant step method used Hasse bound to find the count. But most popular algorithm that use Hasse bound is Schoof's algorithm. Here we basically have designed an algorithm that can test irreducibility of any polynomial(Weierstrass form) of degree 3 without using gcd method. We have used our algorithm to find whether cardinality is even or odd where Schoof used to use gcd method. We have studied the problem to find degree of Frobenius Endomorphism directly. Also we have got some result related to count if we know the type of elliptic curve. Throughout this thesis p(prime) stands for characteristic of the underlying field and q(some power of p) stands for cardinality of the underlying field. Here we are considering only the fields with characteristic $p \; > \; 3$.

Definition An elliptic curve E over the field $\mathbb{F}$ is of the form

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6, \; where \; a_i \in \mathbb{F}$$

This equation also called generalized Weierstrass equation.
We let $E(\mathbb{F})$ denotes the set points $(x, y) \;\in\; \mathbb{F}^2$ that satisfy this equation, along with a "point at infinity" denoted by ∞.

1.1 Elliptic curve over prime field $\mathbb{F}_p$ with $p > 3$

The above equation is very useful when working with field with characteristic 2 and characteristic 3. Now if characteristic of the field is not 2 then we can divide by 2 and complete the square as

$$(y + a_1x/2 + a_3/2)^2 = x^3 + \left(a_2 + a_1^2/4\right) x^2 + a_4x + \left(a_3^2/4 + a_6\right)$$

which can be written as

$$y_1^2 = x^3 + b_2x^2 + b_4x + b_6$$

with $y_1 = y + a_1x/2 + a_3/2$ and for some constants $b_2,\ b_4,\ b_6$. If the characteristic is also not 3, then we let $x_1 = x + b_2/3$ and obtain

$$y_1^2 = x_1^3 + Ax + B$$

for some constants $A, B \in \mathbb{F}_p$.
The above equation is called Weierstrass form.

Definition *Discriminant* of polynomial is defined to be product of the square of the difference of the roots.

1.1.1 Newtons formula

Let $\alpha_1, \alpha_2, \alpha_3, ...\alpha_n$ be the roots of the equation

$$f(x) = x^n + p_1x^{n-1} + p_2x^{n-2} + ... + p_n = 0$$

let $s_r = \alpha_1^r + \alpha_2^r + ... + \alpha_n^r$, where $r \geq 0$ an integer
then (i) $s_r + p_1s_{r-1} + p_2s_{r-2} + ... + p_{r-1}s_1 + rp_r = 0 \ if \ 1 \leq r < n$
(ii) $s_r + p_1s_{r-1} + ... + p_ns_{r-n} = 0 \ if \ r \geq n$

1.1.2 Finding discriminant of $y^2 = x^3 + Ax + B$

Let $y^2 = x^3+Ax+B$ be an elliptic curve over $\mathbb{F}_p$. Let $\alpha_1, \alpha_2, \alpha_3$ are the roots of the equation x^3+Ax+B. So discriminant $d = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2$ i.e

$$\mathbf{d} = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{vmatrix}$$

and

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix} \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{vmatrix} = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}$$

(by know result)
where $s_0 \;=\; 3$

$$\begin{aligned} s_1 &= \alpha_1 + \alpha_2 + \alpha_3 \;=\; 0 \\ s_2 &= -p_1 s_1 - 2p_2 \;=\; -2A \\ s_3 &= -p_1 s_2 - p_2 s_1 - p_3 s_0 \;=\; -3B \\ s_4 &= -p_1 s_3 - p_2 s_2 - p_3 s_1 \;=\; 2A^2 \end{aligned}$$

Hence

$$\mathbf{d} \;=\; \begin{vmatrix} 3 & 0 & -2A \\ 0 & -2A & -3B \\ -2A & -3B & 2A^2 \end{vmatrix} \;=\; -\,(4A^3 + 27B^2)$$

With the notion of discriminant we redefine the definition of elliptic curve as

Definition An elliptic curve E over finite field $\mathbb{F}_q$ where $q \;=\; p^r$ for some integer $r \;\geq\; 1$ and p is the characteristic of finite field $\mathbb{F}_q$ is of the form

$$y^2 \;=\; x^3 + Ax + B, where\ A, B \in \mathbb{F}_q$$

with $4A^3 + 27B^2 \;\neq\; 0$.

This equation is called Weierstrass equation. We let $E(\mathbb{F}_q)$ denote the set points $(x, y) \;\in\; \mathbb{F}_q^2$ that satisfy the above equation along with a "point at infinity", called ∞. i.e

$$E(\mathbb{F}_q) \;=\; \{(x, y) \in \mathbb{F}_q^2 \mid y^2 \;=\; x^3 + Ax + B\} \cup \{\infty\}$$

1.1.3 Addition law

In order to define a cryptosystem on the set points on elliptic curve, we need to define an algebric structure on the points. The easiest algebric structure which provides us with all necessary tools is the group. Therefore we need to define identity element (zero element), inverse elements, and the addition of two elliptic curve points which need to be associative.
Let E: $y^2 \;=\; x^3{+}Ax{+}B$ be an elliptic curve over $\mathbb{F}_q$. Let $P_1 \;=\; (x_1, y_1), P_2 \;=\; (x_2, y_2)$ be two points from $E(\mathbb{F}_q^2)$ with $P_1, P_2 \;\neq\; \infty$.
Define $P_1 + P_2 \;=\; P_3 \;=\; (x_3, y_3)$ as follows

1. If $x_1 \;\neq\; x_2$ then
draw a line through P_1 and P_2 which cuts the elliptic curve at a point $R \;=\; (x, y)$ (say) then reflection of R which is $(x, -y)$, the sum of the points P_1 and P_2 and which is given by (see Figure 1.1)

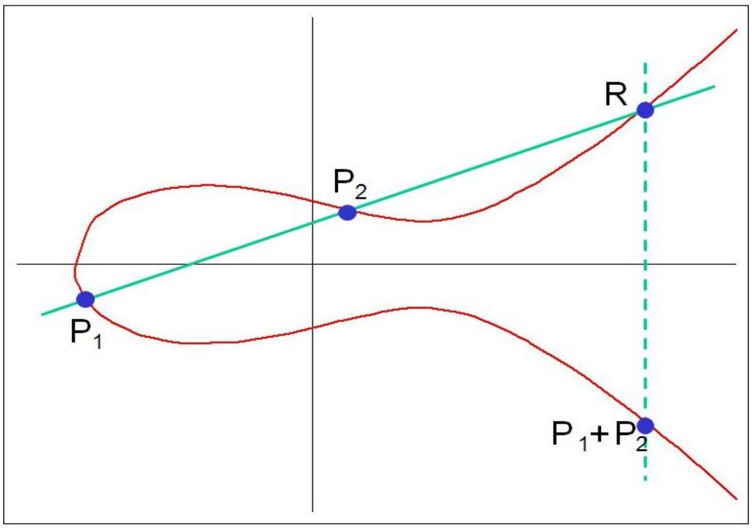

Figure 1.1: Addition two distinct points on elliptic curve

$x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

2. If $x_1 = x_2$ but $y_1 \neq y_2$ then $P_1 + P_2 = \infty$. (see Figure 1.2)

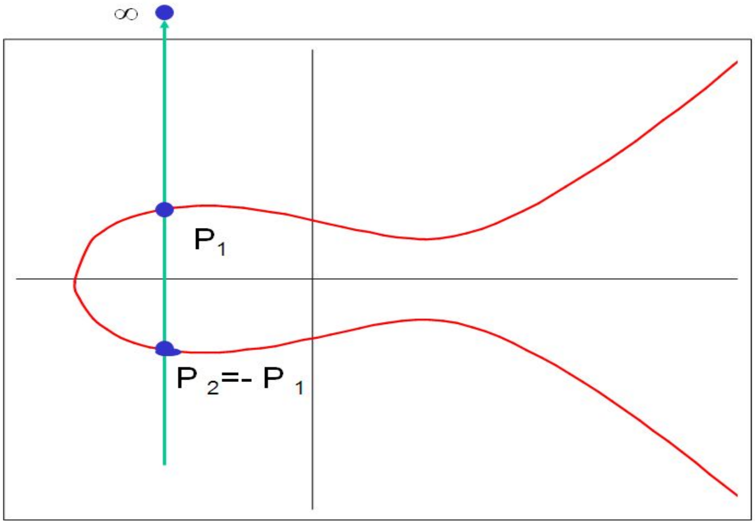

Figure 1.2: Inverse of a point on elliptic curve

3. If $P_1 = P_2$ and $y_1 \neq 0$ then
draw a tangent line through P_1 and the tangent cuts at a point $R = (x, y)$

(say), then reflection of R is taken to be double of the point P_1 and is given by (see Figure 1.3)
$x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{3x_1^2+A}{2y_1}$.

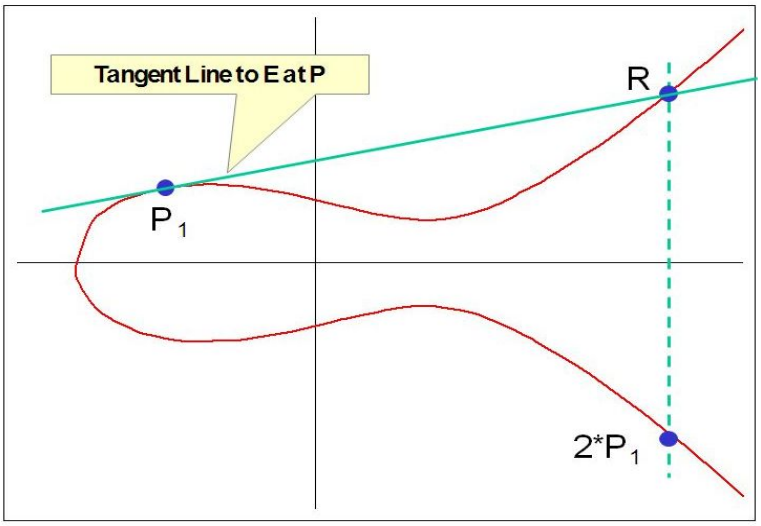

Figure 1.3: Doubling a point on elliptic curve

4. If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = \infty$.

5. $\forall P \in E(\mathbb{F}_q)$, $P + \infty = P$.
With respect to addition $E(\mathbb{F}_q)$ forms a commutative group with ∞ as zero element and inverse of (x, y) is $(x, -y)$.

Chapter 2

Sketch of Schoof's Algorithm

2.1 Algebra and Number Theory

Definition Suppose p is an odd prime and a is an integer. a is defined to be a quadratic residue modulo p if $a \not\equiv 0 \ (mod\ p)$ and the congruence $y^2 \equiv a \ (mod\ p)$ has a solution $y \in Z_p$. a is defined to be a quadratic non residue *mod p* if $a \not\equiv 0 \ (mod\ p)$ and a is not a quadratic residue *mod p.*

Theorem 2.1.1 ***(Euler's Criterion)*** *Let p be an odd integer. Then a is a quadratic residue mod p if and only if*

$$a^{(p-1)/2} \equiv 1 \ (mod\ p).$$

In the proof of the above theorem, we have used the fact that $a^{p-1} \equiv 1 \ (mod\, p)$ due to Fermat. But this result also holds for finite field $\mathbb{F}_q$, because $\mathbb{F}_q \diagdown \{0\}$ forms a cyclic group of order $q-1$. Hence

Corollary 2.1.2 *An element a is quadratic residue in $\mathbb{F}_q$ if and only if*

$$a^{(q-1)/2} \equiv 1 \ (mod\ p).$$

Theorem 2.1.3 *Let $p(x)$ be a minimal polynomial over $\mathbb{F}_q$ of an element say a and $q(x)$ is any polynomial over $\mathbb{F}_q$ such that a is a root of $q(x)$. Then $p(x) \mid q(x)$.*

2.2 Torsion Points

Let E be an elliptic curve over field K. Let n be a positive integer. A point $P \in E(\overline{K})$ is said to be n torsion point if order of P divides n. Where $\overline{K}$ is the algebric closure of K. We are interested in

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty \}.$$

Definition An elliptic curve E over a field K of characteristic $p > 0$ is said to be *supersingular* if $E[p] \backsimeq \{\infty\}$ and is said to be *ordinary* if $E[p] \backsimeq z_p$.

Theorem 2.2.1 *Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n or is 0 ,then*

$$E[n] \backsimeq z_n \oplus z_n.$$

If the characteristic of K is $p > 0$ and $p|n$, write $n = p^r n_1$ with $p \nmid n_1$. Then

$$E[n] \backsimeq z_{n_1} \oplus z_{n_1} \quad or \quad z_n \oplus z_{n_1}.$$

Hence by above theorem every elliptic curve either supersingular or ordinary.

2.3 Endomorphism

By an endomorphism of E, we mean a homomorphism $\alpha : E(\overline{K}) \rightarrow E(\overline{K})$ that is given by rational functions. In other words, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ and there are rational functions $R_1(x, y), R_2(x, y)$ with coefficients in $\overline{K}$ such that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

for all $(x, y) \in E(\overline{K})$. Since $y^2 = x^3 + Ax + B$ for all $(x, y) \in \overline{K}$, we can replace any even power of y by a polynomial in x and replace any odd power of y by y times a polynomial in x and obtain a rational function that gives the same function as $R(x, y)$ on points in $E(\overline{K})$. Therefore, we assume that

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}$$

Moreover, we can rationalize the denominator by multiplying the numerator and denominator by $p_3 - p_4 y$ and then replacing y^2 by $x^3 + Ax + B$. This yields

$$R(x, y) = \frac{q_1(x) + q_2 y}{q_3(x)} \tag{1}$$

Consider an endomorphism given by

$$\alpha(x, y) = (R_1 x, y, R_2(x, y))$$

Since α is a homomorphism,

$$\alpha(x, -y) = -\alpha(x, y).$$

This means that

$$R_1(x,-y) \;=\; R_1(x,y) \; and \; R_2(x,-y) \;=\; -R_2(x,y)$$

Therefore, if R_1 is written of the form (1), then $q_2(x) \;=\; 0$, and if R_2 is written in the form (1). then the corresponding $q_1(x) \;=\; 0$. Therefore we may assume that

$$\alpha(x,y) \;=\; (r_1(x), r_2(x)y)$$

with rational function $r_1(x), r_2(x)$. write

$$r_1(x) \;=\; p(x)/q(x)$$

with polynomial $p(x)$ and $q(x)$ that do not have a common factor. If $q(x) \;=\; 0$ for some point (x,y), then we assume that $\alpha(x,y) \;=\; \infty$.

Definition The degree of α is defined to be

$$deg(\alpha) \;=\; Max\{degp(x), degq(x)\}$$

if α is nontrivial. When $\alpha \;=\; 0$, let $deg(0) \;=\; 0$.

Definition Define $\alpha \;\neq\; 0$ to be a separable endomorphism if the derivative $r_1'(x)$ is not identically zero. i.e at least one of $p'(x)$ and $q'(x)$.

2.3.1 Frobenius map

Suppose E is defined over the finite field $\mathbb{F}_q$. Let

$$\phi_q \;:\; \overline{\mathbb{F}}_q \;\rightarrow\; \overline{\mathbb{F}}_q$$

i.e if $(x,y) \;\in\; E(\overline{\mathbb{F}}_q)$ then $\phi_q(x,y) \;=\; (x^q, y^q)$, $\phi_q(\infty) \;=\; \infty$.

Lemma 2.3.1 *Let E be defined over $\mathbb{F}_q$. Then ϕ_q is an endomorphism of E of degree q, and ϕ_q is not separable.*

Lemma 2.3.2 *Let $\alpha \;\neq\; 0$ be a separable endomorphism of an elliptic curve E. Then*

$$deg\;\alpha \;=\; \#Ker(\alpha),$$

where $Ker(\alpha)$ is the kernel of the homomorphism $\alpha \;:\; E(\overline{K}) \;\rightarrow\; E(\overline{K})$. If $\alpha \;\neq\; 0$ is not separable, then

$$deg\;\alpha \;>\; \#Ker(\alpha).$$

Lemma 2.3.3 *Let E be defined over $\mathbb{F}_q$, and let $(x,y) \in E(\overline{\mathbb{F}}_q)$.*
1. $\phi_q(x,y) \in E(\overline{\mathbb{F}}_q)$.
2. $(x,y) \in E(\mathbb{F}_q)$ *if and only if* $\phi_q(x,y) = (x,y)$.

This Lemma gives a way to find cardinality of elliptic curve over $\mathbb{F}_q$. Since ϕ_q is an endomorphism of E, so are $\phi_q^2 = \phi_q \circ \phi_q$ and also $\phi_q^n = \phi_q \circ \phi_q \circ ... \circ \phi_q$ for every $n \geq 1$.Since multiplication by -1 is also an endomorphism, the sum $\phi_q^n - 1$ is an endomorphism of E.

Lemma 2.3.4 *Let E be defined over finite field $\mathbb{F}_q$ and let $n \geq 1$.*
1. $Ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. $\phi_q^n - 1$ *is a separable endomorphism, so* $\#E(\mathbb{F}_{q^n}) = deg(\phi^n - 1)$.

2.4 Division Polynomials

Let A ,B be two constants in a field K. Define the division polynomials $\psi_n \in Z[x,y,A,B]$ by
$\psi_0 = 0$
$\psi_1 = 1$
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \; for \; m \geq 2$
$\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m-2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \; for \; m \geq 2.$

Lets define another two polynomials ϕ_m *and* ω_m by
$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$
$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m+1}^2 - \psi_{m-2}\psi_{m-1}^2)$

Lemma 2.4.1

$$\psi_n = \begin{cases} y(nx^{n^2-4/2} + \ldots) & ; \textit{if } n \textit{ is even} \\ nx^{n^2-1/2} + \ldots & ; \textit{if } n \textit{ is odd} \end{cases}$$

Lemma 2.4.2 *Let $P(x,y)$ be a point on the elliptic curve E over a field K and let n be a positive integer then*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x)}{\psi_n^3(x)} \right)$$

Lemma 2.4.3 *Let n be a odd integer then for $(x,y) \in E(\overline{\mathbb{F}}_q)$*

$$(x,y) \in E[n] \Leftrightarrow \psi_n(x) = 0.$$

2.5 The Weil Pairing

Let E be an elliptic curve over a field K and let n be a positive integer not divisible by the characteristic of K. Then $E[n] \backsimeq z_n \oplus z_n$. Let

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}$$

be the group of nth roots of unity in $\overline{K}$. Since the characteristic of K does not divide n, the equation $x^n = 1$ has no multiple roots, hence has n roots in $\overline{K}$. Therefore, μ_n is a cyclic group of order n.

Theorem 2.5.1 *Let E be an elliptic curve define over a field K and let n be a positive integer. Assume that the characteristic of K does not divide n.Then there is a pairing*

$$e_n : E[n] \times E[n] \rightarrow \mu_n,$$

called the Weil Pairing, that satisfy the following properties:

1. *Identity: For all $P \in E[n]$, $e_n(P, P) = 1$.*

2. *Alternation: For all $P_1, P_2 \in E[n]$, $e_n(P_1, P_2) = e_n(P_1, P_2)^{-1}$.*

3. *Bilinearity: For all $P_1, P_2, P_3 \in E[n]$, $e_n(P_1 + P_2, P_3) = e_n(P_1, P_3)e_n(P_2, P_3)$,*

and $e_n(P_1, P_2 + P_3) = e_n(P_1, P_2)e_n(P_1, P_3)$.

4. *Non-degeneracy: If $P_1 \in E[n]$, then $e_n(P_1, \infty) = 1$.If $e_n(P_1, P_2) = 1$ for all $P_2 \in E[n]$, then $P_1 = \infty$.*

5. *$e_n(\sigma P_1, \sigma P_2) = \sigma(e_n(P_1, P_2))$ for all automorphisms σ of $\overline{K}$ such that σ is an identity map on the coefficients of E(if E is in Weierstrass form, this means that $\sigma(A) = A$ and $\sigma(B) = B$)*

6. *$e_n(\alpha(P_1), \alpha(P_2)) = \alpha(P_1, P_2)^{deg(\alpha)}$ for all separable endomorphism α of E. If the coefficients of E lie in finite field $\mathbb{F}_q$, then the statement also holds when α is the Frobenius endomorphism ϕ_q.*

Lemma 2.5.2 *Let $\{P_1, P_2\}$ be a basis of $E[n]$. Then $e_n(P_1, P_2)$ is a primitive nth root of unity.*

Theorem 2.5.3 *Let α and β endomorphism of E and let a, b be integers, then*

$$deg(a\alpha + b\beta) = a^2 deg(\alpha) + b^2 deg(\beta) - ab(deg(\alpha + \beta) - deg(\alpha) - deg(\beta))$$

2.6 Counting number of points on Elliptic Curve over Finite Field

Let E be an elliptic curve over finite field $\mathbb{F}_q$. Let trace $a = q + 1 - \#E(\mathbb{F}_q)$. Then by Hasse's theorem $|a| \leq 2\sqrt{q}$. The basis approach in Schoof's algorithm is Chinese Remainder theorem. Victor Shoup[2] also took the same approach but he used to compute modular polynomials. The Schoof-Elkies-Atkin reduced the complexity of Schoof's algorithm. Here We basically have modified the Schoof's algorithm by justifying whether a is even or odd.

Lemma 2.6.1 *Let r, s be integers with $gcd(s, q) = 1$. Then $deg(r\phi_q - s) = r^2q + s^2 - rsa$.*

Theorem 2.6.2 ***(Hasse)*** *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Let $a = q + 1 - E(\mathbb{F}_q)$. Then a satisfies*

$$|a| \leq 2\sqrt{q}.$$

Proof Since $\deg(r\phi_p - s) \geq 0$, the Lemma 2.6.1 implies that
$r^2q + s^2 - rsa \geq 0$
$\Rightarrow q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$
for all r, s with $\gcd(s, q) = 1$. The set of rational numbers r/s such that $\gcd(s, q) = 1$ is dense in $\mathbb{R}$. (Proof: Take s to be a power of 2 or power of 3, one of which must be relatively prime with q. The rationals of the form $r/2^m$ and those of the form $r/3^m$ are easily seen to be dense in $\mathbb{R}$.)Therefore,

$$qx^2 - ax + 1 \geq 0$$

for all real numbers x. Therefore the discriminant if the polynomial is negative or 0, which means that $a^2 - 4q \leq 0$, hence $|a| \leq 2\sqrt{q}$.

Theorem 2.6.3 *Let E be an elliptic curve over $\mathbb{F}_q$. Let $a = q+1-\#E(\mathbb{F}_q)$. Then*

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

as endomorphism of E.

The polynomial $x^2 - ax + q$ is often called the characteristic polynomial of Frobenius.

Theorem 2.6.4 *Let $\#E(\mathbb{F}_q) = q + 1 - a$. Write $x^2 - ax + q = (x - \alpha)(x - \beta)$. Then*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geq 1$.

Remark If we know the cardinality of elliptic curve over prime field, then we can calculate the cardinality of the elliptic curve over any finite field of order power of the given prime.

Corollary 2.6.5 *Suppose $p \geq 5$ is a prime. Then E is supersingular if and only if $\#E(\mathbb{F}_p) = p+1$.*

2.6.1 Schoof's Algorithm

Suppose E is an elliptic curve given by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. We know, by Hasse's theorem, that

$$E(\mathbb{F}_q) = q + 1 - a. \quad with\ |a| \leq 2\sqrt{q}.$$

Let $S = \{2, 3, 5, 7..., L\}$ be a set of primes such that

$$\prod_{l \in S} l > 4\sqrt{q}.$$

If we can determine $a\ mod\ l$ for each prime $l \in S$, then we know $a\ mod \prod l$, and therefore a is uniquely determined(by Chinese Remainder theorem).

Let l be a prime. For simplicity, we assume $l \neq p$, where p is the characteristic of $\mathbb{F}_q$. We also assume that q is odd. We want to compute $a\ (mod\ l)$.

Case $l = 2$: If $x^3 + Ax + B$ has a root $e \in \mathbb{F}_q$, then $(e, 0) \in E[2]$ and $(e, 0) \in E(\mathbb{F}_q)$, so $E(\mathbb{F}_q)$ has even order. In this case, $q+1-a \equiv 0\ (mod\, p)$, so a is even. If $x^3 + Ax + B$ has no roots in $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ has no points of order 2, and a is odd. To determine whether $x^3 + Ax + B$ has a root in $E(\mathbb{F}_q)$, we could try all the elements in $E(\mathbb{F}_q)$, but there is a faster way. Recall that the roots of $x^3 + Ax + B$ are exactly the elements of $E(\mathbb{F}_q)$. Therefore, $x^3 + Ax + B$ has a root in $E(\mathbb{F}_q)$ if and only if it has a root in common with $x^q - x$. The Euclidean algorithm, applied to polynomials, yields the gcd of two polynomials.

If q is very large, the polynomial x^q has very large degree. Therefore, it is more efficient to compute $x_q \equiv x^q\ (mod\ x^3 + Ax + B)$ by successive squaring and then use the result to compute

$$gcd(x_q - x,\ x^3 + Ax + B) = gcd(x^q - x,\ x^3 + Ax + B).$$

If the gcd is 1, then there is no common root and a is odd.

else a is even. This finishes the case $l = 2$.

Let ϕ_q be the Frobenius endomorphism. So by definition

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

By Theorem 2.6.3

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

Let (x, y) be a point of order l. Then

$$\left(x^{q^2}, y^{q^2}\right) + q(x, y) \;=\; a(x^q, y^q).$$

Let

$$q_l \;=\; q \;(mod\; l), \quad |q_l| \;<\; l/2.$$

Then $q(x, y) \;=\; q_l(x, y)$, so

$$\left(x^{q^2}, y^{q^2}\right) + q(x, y) \;=\; a(x^q, y^q).$$

Since (x^q, y^q) is also a point of order l, those relation determines $a \;(mod\; l)$. The idea is to compute all the terms except a in this relation, then determine a value of a that makes the relation hold. Note that if the relation holds for one point $(x, y) \;\in\; E[l]$, then we have determined $a \;(mod\; l)$; hence, it holds for all $(x, y) \;\in\; E[l]$.

Assume first that $\left(x^{q^2}, y^{q^2}\right) \;\neq\; \pm\, q_l(x, y)$ for some $(x, y) \;\in\; E[l]$. Then

$$(x', y') \;=^{def}\; \left(x^{q^2}, y^{q^2}\right) + q_l(x, y) \;\neq\; \infty,$$

so $a \;\not\equiv\; 0 \;(mod\; l)$. In this case, the $x-$coordinate of $\left(x^{q^2}, y^{q^2}\right)$ and (x, y) are distinct, so the sum of the two points are found by the formula using the line through the two points, rather than a tangent line or a vertical line. Write

$$j(x, y) \;=\; (x_j, y_j)$$

for integers j. We may compute x_j and y_j using division polynomials see Lemma 2.4.2. We have

$$x' \;=\; \left(\frac{y^{q^2} - y_{q_l}}{x^{q^2} - x_{q_l}}\right)^2 - x^{q^2} - x_{q_l}.$$

Writing

$$\begin{aligned}\left(y^{q^2} - y\right)^2 \;&=\; y^2\left(y^{q^2-1} - 1\right)^2\\ &=\; (x^3 + Ax + B)\left((x^3 + Ax + B)^{(q^2-1)/2-1}\right)^2.\end{aligned}$$

and noting that x_{q_l} is a function of x, we change x' into a rational function of x. We want to find j such that

$$(x', y') \;=\; (x_j^q, y_j^q).$$

First, we look at the $x-$coordinates. Starting with $(x, y) \;\in\; E[l]$, we have $(x', y') \;=\; \pm\,(x_j^q, y_j^q)$ if and only if $x' \;=\; x_j^q$. As pointed out above, if this happens for one point in $E[l]$, it happens for all(finite) points in $E[l]$. Since the roots of ψ_l are the $x-$coordinates of the points in $E[l]$ (as in Lemma 2.4.3), this implies that

$$x^i - x_j^q \ \equiv \ 0 \ (mod \ \psi_l) \tag{2}$$

(this means that the numerator of $x' - x_j^q$ is a multiple of ψ_l). We are using here the fact that the roots of ψ_l are simple(otherwise, we would obtain only that ψ_l divides some power of $x' - x_j^q$). This is proved by noting that there are $l^2 - 1$ distinct points of order l, since l is assumed not to be the characteristic of $\mathbb{F}_q$. There are $(l^2-1)/2$ distinct $x-$coordinates of these points, and all of them are roots of ψ_l, which has degree $(l^2-1)/2$. Therefore, the roots of ψ_l must be simple.

Assume now that we have found j such that (2) holds. Then

$$(x', y') \ = \ \pm\,(x_j^q, y_j^q) \ = \ (x_j^q, \ \pm\, y_j^q).$$

To determined the sign, we need to look at the $y-$coordinates. Both y'/y and y_j^q/y can be written as function of x. If

$$(y' - y_j^q)/y \ \equiv \ 0 \ (mod \ \psi_l),$$

then $a \ \equiv \ j \ (mod \ l)$. Otherwise, $a \ \equiv \ -j \ (mod \ l)$. Therefore, we have found $a \ (mod \ l)$.

It remains to consider the case where $\left(x^{q^2}, y^{q^2}\right) \ = \ \pm\, q(x,y)$ for all $(x,y) \ \in \ E[l]$. If

$$\phi_q^2(x,y) \ = \ \left(x^{q^2}, y^{q^2}\right) \ = \ q(x,y),$$

then

$$a\phi_q(x,y) \ = \ \phi_q^2(x,y) + q(x,y) \ = \ 2q(x,y),$$

hence

$$a^2 q(x,y) \ = \ a^2\phi_q^2(x,y) \ = \ (2q)^2(x,y).$$

Therefore, $a^2 q \ \equiv \ 4q^2 \ (mod \ l)$, so q is a square *mod l*. If q is not a square *mod l*, then we cannot be in this case. If q is square *mod l*, let $\omega^2 \ \equiv \ q \ (mod \ l)$. We have

$$(\phi_q + \omega)(\phi_q - \omega)(x,y) \ = \ (\phi_q^2 - q)(x,y) \ = \ \infty$$

for all $(x,y) \ \in \ E[l]$. Let P be any point in $E[l]$. Then either $(\phi_q - \omega)P \ = \ \infty$, so $\phi_q P \ = \ \omega P$, or $P' \ = \ (\phi_q - \omega)P$ is a finite point with $(\phi_q + \omega)P' \ = \ \infty$. Therefore, in either case, there exists a point $P \ \in \ E[l]$ with $\phi_q P \ = \ \pm\,\omega P$.

Suppose there exists a point $P \ \in \ E[l]$ such that $\phi_q P \ = \ \omega P$. Then

$$\infty \ = \ (\phi_q^2 - a\phi_q + q)P \ = \ (q - a\omega + q)P,$$

so $a\omega \equiv 2q \equiv 2\omega^2 \ (mod\, l)$. Therefore $a \equiv 2\omega \ (mod\, l)$. Similarly, if there exists P such that $\phi_q P = -\omega P$, then $a \equiv -2\omega \ (mod\, l)$. We can check whether we are in this case as follows. We need to know whether or not

$$(x^q, y^q) = \pm\,\omega(x,y) = \pm\,(x_\omega, y_\omega) = (x_\omega, \ \pm\, y_\omega)$$

for some $(x,y) \in E[l]$. Therefore, we compute $x^q - x_\omega$, which is rational function of x. If

$$gcd(numerator(x^q - x_\omega), \ \psi_l) \neq 1,$$

then there is some point $(x,y) \in E[l]$ such that $\phi_q(x,y) = \pm\,\omega(x,y)$. If this happens then use the y-coordinates to determine sign.

If we have $gcd(numerator(x^q - x_\omega), \ \psi_l) = 1$, then we cannot be in the case $\left(x^{q^2}, y^{q^2}\right) = q(x,y)$, so the only remaining case is $\left(x^{q^2}, y^{q^2}\right) = -q(x,y)$. In this case, $aP = (\phi_q^2 + q)P = \infty$ for all $P \in E[l]$. Therefore, $a \equiv 0 \ (mod\, l)$.

We summarize Schoof's algorithm[1] as follows. We start with an elliptic curve E over $\mathbb{F}_q$ given by $y^2 = x^3 + Ax + B$. We want to compute $\#E(\mathbb{F}_q) = q + 1 - a$

1. Choose a set of primes $S = \{2, 3, 4, ..., L\}$ (with $P \notin S$) such that

$$\prod_{l \in S} l > 4\sqrt{q}.$$

2. If $l = 2$, we have $a \equiv 0 \ (mod\ 2)$ if and only if $gcd(x^3 + Ax + B, \ x^q - x) \neq 1$.

3. For each odd prime $l \in S$, do the following.

(a) Let $q_l \equiv q \ (mod\, l)$ with $|q_l| < l/2$.
(b) Compute the x-coordinate x' of

$$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q_l(x,y) \ mod\ \psi_l.$$

(c) For $j = 1, 2, ..., (l-1)/2$, do the following.
i. Compute the x-coordinate x_j of $(x_j, y_j) = j(x,y)$.

ii. If $x' - x_j^q \equiv 0 \ (mod\, \psi_l)$, go to step ($iii$). If not, try the next value of j (in step (c)). If all values $1 \leq j \leq (l-1)/2$ have been tried, go to step (d).

iii Compute y' and y_j. If $(y' - y_j)/y = 0 \ (mod\, \psi_l)$. then $a \equiv j \ (mod\, l)$. If not, then $a \equiv -j \ (mod\, l)$.

(d) If all values $1 \leq j \leq (l-1)/2$ have been tried without success, let $\omega^2 \equiv q\ (mod\ l)$. If ω does not exist, then $a \equiv 0\ (mod\ l)$.

(e) If gcd$(numerator(x^q - x_\omega),\ \psi_l) = 1$, then $a \equiv 0\ (mod\ l)$. Otherwise, compute

$$gcd(numerator((y^q - y_w)/y),\ \psi_l).$$

If this gcd is not 1, then $a \equiv 2\omega\ (mod\ l)$. Otherwise, $a \equiv -2\omega\ (mod\ l)$.
4. Use the knowledge of $a\ (mod\ l)$ for each $l \in S$ to compute $a\ (mod\ \prod l)$. Choose the value of a that satisfies this congruence and such that $|a| \leq 2\sqrt{q}$. The number of points in $E(\mathbb{F}_q)$ is $q + 1 - a$.

Chapter 3

Modified Schoof's Algorithm

3.1 Analysis of the degree of $\phi_p - 1$

Lets first study the Lemma 2.3.3. Condition 2 says that $(x, y) \in E(\mathbb{F}_q)$ iff $\phi_q(x, y) = (x, y)$ i.e $(x, y) \in Ker(\phi_q - 1)$. So $\#E(\mathbb{F}_q) = \#Ker(\phi_q - 1)$. Since $\phi_q - 1$ is separable so

$$\#E(\mathbb{F}_q) \ = \ \#Ker(\phi_q - 1) \ = \ deg(\phi_q - 1).$$

Lets see what happens to find the degree of $\phi_q - 1$. Here we assume that $q = p$ because if we know $\#E(\mathbb{F}_p)$ then we can calculate $\#E(\mathbb{F}_{p^n})$ for all $n \geq 1$ by Theorem 2.6.4. To find degree of $\phi_p - 1$. Let $(x, y) \in E(\mathbb{F}_p)$ then

$$\begin{aligned} (\phi_p - 1)(x, y) &= (x^p, y^p) - (x, y) \\ &= (x^p, y^p) + (x, -y) \\ &= (x', y'). \end{aligned}$$

where x' is given by

$$\begin{aligned} x' &= \left(\frac{y^p + y}{x^p - x}\right)^2 - (x^p + x) \\ &= \frac{(y^p + y)^2 - (x^p + x)(x^p - x)^2}{(x^p - x)^2} \end{aligned}$$

Before going to take maximum of the degree of polynomials in denominator and numerator, we have to find

$$gcd((y^p + y)^2 - (x^p + x)(x^p - x)^2, (x^p - x)^2)$$

Now see that roots of denominator $(x^p - x)^2$ are also the roots of $(x^p + x)(x^p - x)^2$. Hence the common factors of $(x^p - x)^2$ and $(y^p + y)^2$ will be the gcd. Let for some $x \in \mathbb{F}_p$,

$$(y^p + y)^2 \ = \ 0$$

Now

$$\begin{aligned}(y^p + y)^2 &= y^2(y^{p-1} + 1)^2 \\ &= y^2((y^2)^{(p-1)/2} + 1)^2 \\ &= (x^3 + Ax + B)((x^3 + Ax + B)^{(p-1)/2} + 1)^2 \\ &= 0\end{aligned}$$

case-1. If $x^3 + Ax + B = 0$ then $x^3 + Ax + B$ has a root in F_p
case-2. If $(x^3 + Ax + B)^{(p-1)/2} + 1 = 0$ i.e
$x^3 + Ax + B$ is quadratic non residue.
Both case-1 and case-2 may happen simultaneously. Here problem is that finding number of quadratic non residue in $\mathbb{F}_p$. So in this way calculating degree of $\phi_p - 1$ is reduced to finding number of $x \in \mathbb{F}_p$ for which x^3+Ax+B is quadratic non residue which we want to calculate. So in this it is difficult to find the cardinality of elliptic curve over prime field.

3.2 Some result using type of the elliptic curves

Elliptic curve cryptosystem are based on the elliptic curve discrete logarithm problem(ECDLP). There are different attack has been made on elliptic curve cryptosystem. The MOV-attack[4],[3] and FR-Reduction attack[3] are very common for supersingular elliptic curve cryptosystem. Also FR-reduction attack has been done on special type of ordinary curve called MNT curve. MOV-reduction reduces ECDLP to discrete logarithm problem(DLP) by using Weil pairing. FR-reduction reduces ECDLP to DLP by using Tate pairing. We are explaining the main mechanism in shortcut. Let E be an elliptic curve over $\mathbf{F}_q$. Let $P \in E(\mathbf{F}_q)$ be point of order N with $gcd(p, N) = 1$. Suppose $Q \in E(\mathbf{F}_q)$ such that $Q = lP$. We have to calculate the value of l. The main idea is to find smallest k with $k \geq 1$ for which $E[N] \subset E(\mathbf{F}_{q^k})$. In case of supersingular curve value of k are $1, 2, 3, 4$ or 6. Finding such k in ordinary curve is a very hard problem. But in case of special type ordinary curve(MNT curve), such k can be calculated. So if such a k is found , then ECDLP on $E(\mathbf{F}_q)$ tp DLP on $\mathbf{F}^{\star}_{q^k}$. Ultimately it is implied that we need to know about type of the elliptic curve.
Let E be a supersingular elliptic curve over $\mathbf{F}_q$. If $q = p$ and $q \geq 5$ then by Corollary 2.6.5, $\#E(\mathbf{F}_q) = q + 1$.
Now for ordinary case, we have the following result.

Theorem 3.2.1 *If $E(\mathbf{F}_p)$ contains a point of order p. Then $\#E(\mathbf{F}_p) = p$, for $p > 5$.*

Proof
Since $E(\mathbf{F}_p)$ contains a point of order $p \Rightarrow p \mid \#E(\mathbf{F}_p) \Rightarrow \#E(\mathbf{F}_p) = rp$ for some integer r. Since $E(\mathbf{F}_p)$ contains atleast one point $\Rightarrow r > 0$. Since in worst case $\#E(\mathbf{F}_p) = 2p+1$ so either $r = 1$ or $r = 2$. Suppose $r = 2$

i.e $\#E(\mathbf{F}_p) \ = \ 2p$ then trace $a \ = \ p+1-\#E(\mathbf{F}_p) \ = \ 1-p$. Now by Hasse's theorem $|a| \ \leq \ 2\sqrt{p}$
$\Rightarrow \quad |p-1| \ \leq \ 2\sqrt{p}$.
$\Rightarrow \quad p^2-6p+1 \ \leq \ 0$.
$\Rightarrow \quad (p-(3+2\sqrt{2}))(p-(3-2\sqrt{2})) \ \leq \ 0$.
$\Rightarrow \quad (p-5.828)(p-0.172) \ \leq \ 0$.
So the case $r \ = \ 2$ satisfies the Hasse's theorem when p lies in the interval $(0.172, \ 5.828)$. Hence $\#E(\mathbf{F}_p) \ = \ p$, for $p \ > \ 5$.

3.3 Discriminant Analysis

Definition Suppose p is an odd prime and a is an integer. a is defined to be a *cubic residue* modulo p if $a \ \not\equiv \ 0 \ (mod \ p)$ and the congruence $y^3 \ \equiv \ a \ (mod \ p)$ has a solution $y \ \in \ Z_p$. a is defined to be a *cubic non residue mod p* if $a \ \not\equiv \ 0 \ (mod \ p)$ and a is not a *cubic residue mod p*.

Theorem 3.3.1 ***(Cubic's Criterion)*** *Let p be an odd integer and p is of the form $3k+1$. Then a is a cubic residue mod p if and only if*

$$a^{(p-1)/3} \ \equiv \ 1 \ (mod \ p).$$

Proof
Suppose a is cubic residue, then $a \ \equiv \ y^3 \ (mod \ p)$. Now

$$\begin{aligned} a^{(p-1)/3} \ &\equiv \ (y^3)^{(p-1)/3} \ (mod \ p) \\ &\equiv \ y^{p-1} \ (mod \ p) \\ &\equiv \ 1 \ (mod \ p) \ \ (by \ Fermat \ theorem) \end{aligned}$$

Conversely, suppose $a^{(p-1)/3} \ \equiv \ 1 \ (mod \ p)$. Let b be a primitive element *mod p*. Then $a \ \equiv \ b^i \ (mod \ p)$ for some positive integer i. Then we have

$$\begin{aligned} a^{(p-1)/3} \ &\equiv \ (b^i)^{(p-1)/3} \ (mod \ p) \\ &\equiv \ b^{i(p-1)/3} \ (mod \ p) \end{aligned}$$

Since b has order $p-1$, it must be the case that $(p-1)$ divides $i(p-1)/3$. Hence i is a multiple of 3 and the cubic root of a are $\pm b^{i/2} \ (mod \ p)$. This complete the proof.
As in corollary 2.1.2we can write

Corollary 3.3.2 *An element a is cubic residue in $\mathbb{F}_q$ if and only if*

$$a^{(q-1)/3} \ \equiv \ 1 \ (mod \ p).$$

Let E be an elliptic curve over finite field $E(\mathbb{F}_q)$. we want to verify whether x^3+Ax+B has a root in $\mathbb{F}_q$ or not. The algorithm which are used through finding $gcd(x^q-x, x^3+Ax+b)$. If gcd is 1 then x^3+Ax+B are irreducible else reducible.
Discriminant of x^3+Ax+B is

$$\begin{aligned} D &= (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2 \\ &= -(4A^3+27B^2) \end{aligned}$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $x^3+Ax+B = 0$. So

$$\begin{cases} \alpha_1+\alpha_2+\alpha_3 = 0 \\ \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 = A \\ \alpha_1\alpha_2\alpha_3 = -B \end{cases}$$

Theorem 3.3.3 *Let E be an elliptic curve over a field $\mathbb{F}_q$. If D is quadratic non residue then $x^3+Ax+B = 0$ has exactly one root in $\mathbb{F}_q$. If D is quadratic residue then either $x^3+Ax+B = 0$ has no root in $\mathbb{F}_q$ or $x^3+Ax+B = 0$ has exactly three roots.*

Proof
Since $D \neq 0$ so $\alpha_1, \alpha_2, \alpha_3$ are distinct roots of $x^3+Ax+B = 0$
(a) Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q$, then

$$(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1) \in \mathbb{F}_q$$

$\Rightarrow$ D is quadratic residue in $\mathbb{F}_q$.

(b) Let $\alpha_1 \in \mathbb{F}_q$ but $\alpha_2, \alpha_3 \notin \mathbb{F}_q$, then

$$x^3+Ax+B = (x-\alpha_1)(x^2+\alpha_1 x+(A+\alpha_1^2))$$

then $x^2+\alpha_1 x+(A+\alpha_1^2)$ has no root in $\mathbb{F}_q$. Let $D' = (\alpha_2-\alpha_3)^2 = -(4A+3\alpha_1^2) \in \mathbb{F}_q$. Then D' is quadratic non residue
infact if $D' = (\alpha_2-\alpha_3)^2$ is quadratic residue.
$\Rightarrow$

$$\alpha_2-\alpha_3 \in \mathbb{F}_q \tag{3.1}$$

Now $\alpha_1+\alpha_2+\alpha_3 = 0 \in \mathbb{F}_q$ and $\alpha_1 \in \mathbb{F}_q$
$\Rightarrow$

$$\alpha_2+\alpha_3 \in \mathbb{F}_q \tag{3.2}$$

from (3.1) *and* (3.2) we have $\alpha_2 \in \mathbb{F}_q$, a contradiction.
since α_2 and α_3 are the roots of the equation $x^2+\alpha_1 x+(A+\alpha_1^2) = 0$, we can write

$$(x-\alpha_2)(x-\alpha_3) = x^2+\alpha_1 x+(A+\alpha_1^2)$$

$\Rightarrow (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \; = \; A + 3\alpha_1^2 \; \in \; \mathbb{F}_q$
$\Rightarrow (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2$ is quadratic residue.
$D \; = \; \underbrace{(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2}\underbrace{(\alpha_2 - \alpha_3)^2}$
D is product of quadratic residue and quadratic non residue. Hence D is quadratic non residue.

(c) Let $\alpha_1, \alpha_2 \; \in \; \mathbb{F}_q$ and $\alpha_3 \; \notin \mathbb{F}_q$.
Since $\alpha_1 + \alpha_2 + \alpha_3 \; = \; 0 \; \in \; \mathbb{F}_q$
$\Rightarrow \alpha_3 \; \in \; \mathbb{F}_q$, a contradiction.
Hence not a case.

(d) Let $\alpha_1, \alpha_2, \alpha_3 \; \notin \; \mathbb{F}_q$.
$\Rightarrow x^3 + Ax + B$ is irreducible over $\mathbb{F}_q$
Let $d \; = \; (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$.
Consider field extension of $\mathbb{F}_q$

$$\mathbb{F}_{q^3} \; \backsimeq \; \frac{\mathbb{F}_q(x)}{< x^3 + Ax + B >}$$

Here $\alpha_1 \; = \; x \; \in \; \mathbb{F}_{q^3}$ and $\mathbb{F}_{q^3}$ is finite field of q^3 numbers of elements and is given by

$$\prod_{\beta \in \mathbb{F}_{q^3}} (x - \beta) \; = \; \left(x^{q^3} - x\right)$$

Now $\exists$ an element in $\mathbb{F}_{q^3}$ for which $x^3 + Ax + B$ is the minimal polynomial. Infact $x^3 + Ax + B$ is the minimal polynomial of x. Since $x^3 + Ax + B$ is a polynomial of α_1 and α_1 is a root of $x^{q^3} - x$ by Theorem 2.1.3, we have
$x^3 + Ax + B \mid x^{q^3} - x$
$\Rightarrow \alpha_1, \alpha_2, \alpha_3 \; \in \; \mathbb{F}_{q^3}$
$\Rightarrow d \; \in \; \mathbb{F}_{q^3}$
Now $d^2 \; = \; D$ in $\mathbb{F}_q \Rightarrow d^2 - D \; = \; 0$ in $\mathbb{F}_q$
Suppose D is quadratic non residue in $\mathbb{F}_q$
$\Rightarrow x^2 - D$ is irreducible in $\mathbb{F}_q$.
Consider the field extension

$$\mathbb{F}_{q^2} \; \backsimeq \; \frac{\mathbb{F}_q[x]}{< x^2 - D >}$$

and we get $x^2 - D \mid x^{q^2} - x$ (same as previous argument)
Since d satisfies $x^2 - D \; = \; 0$ in $\mathbb{F}_q$
$\Rightarrow d \; \in \; \mathbb{F}_{q^2}$. Since degree of minimal polynomial of d is 2 in $\mathbb{F}_q$, so any element of $c \; \in \; \mathbb{F}_{q^2}$ is of the form $c \; = \; a + bd$, where $a, b \; \in \; \mathbb{F}_q$.
Now since $\mathbb{F}_q \; \subset \; \mathbb{F}_{q^3}$ and $d \; \in \; \mathbb{F}_{q^3}$
$\Rightarrow c \; = \; a + bd \; \in \; \mathbb{F}_{q^3}$.
$\Rightarrow \mathbb{F}_{q^2}$ is a subfield of $\mathbb{F}_{q^3}$

$\Rightarrow \left[\mathbb{F}_{q^3} \; : \; \mathbb{F}_{q^2}\right]$ is an integer, which is a contradiction.
Hence D is a quadratic residue.

Remark Whatever proof we have done for x^3+Ax+B have the same proof for any cubic polynomial except case (c).

When D is quadratic residue either $x^3 + Ax + B$ has exactly three roots or no root in $\mathbb{F}_q$. We were unable to distinguish this case. But using following theorem we can do that (for details see the reference [5]).

Theorem 3.3.4 *The necessary and sufficient conditions that*

$$x^3 + Ax + B$$

be irreducible in the $\mathbb{F}_q$*,* $p \; > \; 3$*, are the following two:*
(1) D *is square* $\neq \; 0$ *in* $\mathbb{F}_q$*, let say* $D \; = \; 81\mu^2$*;*
(2) $\frac{1}{2}(-B + \mu\sqrt{-3})$ *a not cubic in the field* $(\mathbb{F}_q, \; \sqrt{-3})$*.*

Remark By above two theorem, we can say how many roots the polynomial $x^3{+}Ax{+}B$ can have in $\mathbf{F}_q$ by analysis the discriminant $D \; = \; -(4A^3{+}27B^2)$.

Now We are giving the complete algorithm whether the given polynomial $x^3 + Ax + B$ is reducible over $\mathbf{F}_q$ or not.

3.3.1 Discriminant based algorithm for irreducibility testing

Let $x^3 + Ax + B$ be a polynomial over $\mathbf{F}_q$ with discriminant $D \; = \; -(4A^3 + 27B^2) \; \not\equiv \; 0 \; (mod \; q)$. First evaluate the value $D^{(q-1)/2} \; (mod \; q)$. If this value is 1, then D is quadratic residue.
else D is quadratic non residue.
case(1.) D is quadratic non residue.
So by Theorem 3.3.3 $x^3 + Ax + B$ has exactly one root. i.e $x^3 + Ax + B$ is reducible.
case(2.) D is quadratic residue.
Then $D \; = \; -(4A^3 + 27B^2) \; = \; 81\mu^2$ say. i.e $D \; = \; (9\mu)^2$. Then applying the following algorithm for finding square root D.
Computing Square Roots Modulo p
Input: An element a of $\mathbf{F}_p$ which is quadratic residue.
Output: A square root $x \; \in \; \mathbf{F}_p$ of the given element a.

1. First check form of prime p.

2. If $p \; = \; 4k + 3$ for some $k \; \geq \; 0$ then a square root x is given by $x \; = \; a^{(p+1)/4} \; (mod \; p)$.

3. If $p = 8k+5$ for some $k \geq 0$, then calculate $a^{(p-1)/4}$ $(mod\ p)$.

4. If the value is 1, then $x = a^{(p+3)/8}$ $(mod\ p)$ is a square root of a.

5. If the value is -1, then $x = 2a.(4a)^{(p-5)/8}$ $(mod\ p)$ is a square root of a.

6. If $p = 8k+1$ for some $k \geq 0$ then we use algorithm of Tonelli and Shanks as

Let $p-1 = 2^e.s$ with s odd.

6a. Choose number n at random until n is quadratic non residue. Then set $z \longleftarrow n^s$ $(mod\ p)$.

6b. Let $y \leftarrow z$, $r \leftarrow e$, $x \leftarrow a^{(s-1)/2}$ $(mod\,p)$, $b \leftarrow ax^2$ $(mod\,p)$, $x \leftarrow ax$ $(mod\,p)$.

6c. If $b \equiv 1$ $(mod\ p)$, then x is a square root. Otherwise find smallest $m \geq 1$ such that $b^{2^m} \equiv 1$ $(mod\ p)$.

6d. Set $t \leftarrow y^{2^{r-m-1}}$, $y \leftarrow t^2$, $r \leftarrow m$, $x \leftarrow xt$, $b \leftarrow by$ (all operation done under modulo p) and go to step c.

Then $\mu = 9^{-1}\sqrt{D}$ $(mod\ q)$. Now study -3 which is either quadratic residue or quadratic non residue

subcase(2a.) -3 is quadratic residue

then $\sqrt{-3} \in \mathbf{F}_q \Rightarrow \gamma = \frac{1}{2}(-B+\mu\sqrt{-3}) \in \mathbf{F}_q$. We define a mapping ψ

$$\psi : \mathbf{F}_q^\star \longrightarrow \mathbf{F}_q^\star$$

by $\psi(x) = x^3$ for all $x \in \mathbf{F}_q$. If $Ker(\psi) = 1$ then ψ is one one $\Rightarrow \psi$ is bijective. Since $\gamma \in \mathbf{F}_q$ and ψ is bijective $\Rightarrow \exists x \in \mathbf{F}_q$ such that $\gamma = x^3$. Now $Ker(\psi) = 1 \Longleftrightarrow 3 \nmid q-1$. So in this case if $3 \nmid q-1$ them x^3+Ax+B is reducible.

If $3 \mid q-1$ then apply Cubic's Criterion. i.e calculate $\gamma^{(q-1)/3}$ $(mod\ q)$. If this value is 1 then γ has a cubic root in $\mathbf{F}_q$ and hence x^3+Ax+B is reducible.

If this value is not 1 then γ has no cubic root in $\mathbf{F}_q$ and hence x^3+Ax+B is irreducible.

subcase(2b.) -3 is quadratic non residue

Then $\sqrt{-3} \notin \mathbf{F}_q$

$\Rightarrow x^2+3$ is irreducible over $\mathbf{F}_q$

Consider the field extension of $\mathbf{F}_q$ which is

$$\mathbf{F}_{q^2} \backsimeq \frac{\mathbf{F}_q}{\langle x^2+3\rangle}$$

since $\sqrt{-3} \in \mathbf{F}_{q^2} \Rightarrow \gamma \in \mathbf{F}_{q^2}$
Now write $\gamma = \frac{1}{2}(-B) + \mu\sqrt{-3} = -\frac{B}{2} + \frac{\mu}{2}\sqrt{-3} = c + d\sqrt{-3}\ (say)$ let call it (c,d), where $c, d \in \mathbf{F}_q$. Now define the product of same element in $\mathbf{F}_{q^2}$ as

$$\begin{aligned}(c,d)^2\ (mod\ q) &= (c + d\sqrt{-3})^2\ (mod\ q)\\ &= c^2 - 3d^2 + 2\sqrt{-3}cd\ (mod\ q)\\ &= (c^2 - 3d^2\ (mod\ q),\ 2cd\ (mod\ q))\end{aligned}$$

Now define the product of two distinct elements $(c_1,d_1),(c_2,d_2) \in \mathbf{F}_{q^2}$ as

$$\begin{aligned}(c_1,d_1)(c_2,d_2)\ (mod\ q) &= (c_1 + d_1\sqrt{-3})(c_2, +d_2\surd - 3)\ (mod\ q)\\ &= ((c_1c_2 - 3d_1d_2) + \sqrt{-3}(c_1d_2 + c_2d_1)\ (mod\ q)\\ &= (c_1c_2 - 3d_1d_2\ (mod\ q),\ c_1d_2 + c_2d_1\ (mod\ q))\end{aligned}$$

Now calculate $\gamma^{(q^2-1)/3\ (mod\ q)}$ by efficient algorithm as follows.
Let $(q^2-1)/2 = \sum_{i=0}^{r} k_i 2^i$, where $k_i's \in 0, 1$

```
($P \longleftarrow \gamma = (c,d)$).
for($i = 1$ $to$ $r$) do:
    if ($k_{r-i} = 1$) then
        $P \longleftarrow P^2\ (mod\ q)$.
        $P \longleftarrow P \star \gamma\ (mod\ q)$
    else $P \longleftarrow P^2\ (mod\ q)$.
end for.
return $P$.
```

If $P = (1,0)$, then the polynomial $x^3 + Ax + B$ over $\mathbf{F}_q$ is reducible. Otherwise irreducible.

Remark The algorithm for finding square root works on prime field. So when we will apply our algorithm, it will be assumed that $q = p$.

We summarize the algorithm as follows: We start with a cubic polynomial of the form $x^3 + Ax + B$ over the finite field $\mathbf{F}_q$. We want to check whether $x^3 + Ax + B$ is irreducible over $\mathbf{F}_q$ or not. Let discriminant $D = -(4A^3 + 27B^2) \neq 0$

Input: coefficients of Weierstrass equation i.e A, B and q.
Output: A message reducible or irreducible.
1. Check whether D is quadratic residue over $\mathbf{F}_q$ or not.

2. If D is quadratic non residue, then $x^3 + Ax + B$ is reducible.

3. If D is quadratic residue, then D is square and $D = (9\mu)^2$. then $\mu = 9^{-1}\sqrt{D}$. Then find $\gamma = \frac{1}{2}(-B + \mu\sqrt{-3}) = (c + d\sqrt{-3})$, call it (c,d)

where $c, d \in \mathbf{F}_q$

4. Check whether -3 is quadratic residue over $\mathbf{F}_q$ or not.

5. If -3 is quadratic residue, then $\sqrt{-3} \in \mathbf{F}_q$. So $\gamma = (c, d) \in \mathbf{F}_q$.

6. Now check whether $3 \mid q-1$ or not.

7. If $3 \nmid q-1$ then $x^3 + Ax + b$ is reducible over $\mathbf{F}_q$.

8. If $3 \mid q-1$, check whether γ is cubic residue over $\mathbf{F}_q$ or not.

9. If γ is cubic residue, then $x^3 + Ax + B$ is reducible.

10. If γ is cubic non residue, then $x^3 + Ax + B$ is irreducible.

11. If -3 is quadratic non residue, then $\sqrt{-3} \notin \mathbf{F}_q$

12. Consider field extension $\mathbf{F}_{q^2} \backsimeq \frac{\mathbf{F}_q}{\langle x^2+3 \rangle}$. Then $\gamma = \frac{1}{2}(-B+\mu\sqrt{-3}) = (c, d) \in \mathbf{F}_{q^2}$, where $c, d \in \mathbf{F}_q$.

13. Now check whether γ is cubic residue over $\mathbf{F}_{q^2}$ or not.

14. If γ is cubic residue, then $x^3 + Ax + B$ is reducible.

15. If γ is cubic non residue, then $x^3 + Ax + B$ is irreducible.

3.3.2 Complexity

Step 1. takes time $\mathbf{o}(\log q)$.
Step 3. takes time $\mathbf{o}(\log q)$ when $p = 4k+3$ *or* $8k+5$ and $\mathbf{o}(\log q)^4$ when $p = 8k+1$
Step 4. takes time $\mathbf{o}(\log q)$.
Step 8. takes time $\mathbf{o}(\log q)$.
Step 13. takes time $\mathbf{o}(\log q)$.
And other step will take constant time. So total time complexity is $\mathbf{o}(\log q)$ when $p = 4k+3$ *or* $8k+5$ and $\mathbf{o}(\log q)^4$ when $p = 8k+1$.
Note:- When we will use our algorithm for irreducibility testing, mind that $q = p$.

3.3.3 Examples

Here we have taken some example for different form of prime p. We are using some notation in the table. We write D for discriminant in 2nd column, QR for quadratic residue in 3rd column, $\sqrt{D}$ for square root D in 5th column, μ for $9^{-1}\sqrt{D}$ in 6th column, γ for $\frac{1}{2}(-B+\mu\sqrt{-3}) = (c,d)$ in 7th column, cubic root of γ in last column of the table. The entry in the last column "-" means the roots are not distinct. The roots that have been included may be in the extension of $\mathbf{F}_p$. Here some entries in the last column are polynomial, that means the roots are belonging in the corresponding field extension of $\mathbf{F}_p$. For $p = 5$ see the Table 4.1, for $p = 7$ see the Table 4.2 and for $p = 13$ see the Table 4.3, Table 4.4, Table 4.5 and Table 4.6 in the appendix.

3.4 Conclusion

We have modified the Schoof's Algorithm only in the case $l = 2$ which is equivalent to test irreducibility of the Weierstrass equation $x^3 + Ax + B$. Since complexity of our algorithm is $\mathbf{o}(\log p)$ when $p = 4k+3$ or $p = 8k+5$ and $\mathbf{o}(\log p)^4$ when $p = 8k+1$. And existance algorithms can not find $gcd(x^p - x,\ x^3 + Ax + B)$ with complexity less than our algorithm. Also the special achievement of our algorithm is that if we you the type of elliptic curve that already have been discussed. So our algorithm is better than the Schoof's algorithm in the case $l = 2$.

Chapter 4

Appendix

Table 4.1: Table for prime 5 which is of the form $p = 8k + 5$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	**cubic root of** γ	**root of the polynomial**
$x^3 + 1x + 0$	1	Y	1	4	(0,2)	(0,1)	0,2,3
$x^3 + 1x + 1$	4	Y	2	3	(2,4)	-	$x, x^2 + 3x + 4, 4x^2 + x + 1$
$x^3 + 1x + 2$	3	N	-	-	-	-	4
$x^3 + 1x + 3$	3	N	-	-	-	-	1
$x^3 + 1x + 4$	4	Y	2	3	(3,4)	-	$x, x^2 + x + 4, 4x^2 + 3x + 1$
$x^3 + 2x + 0$	3	N	-	-	-	-	0
$x^3 + 2x + 1$	1	Y	1	4	(2,2)	-	$x, x^2 + 3, 4x^2 + 4x + 2$
$x^3 + 2x + 2$	0	0	-	-	-	-	-
$x^3 + 2x + 3$	0	0	-	-	-	-	-
$x^3 + 2x + 4$	1	Y	1	4	(3,2)	-	$x, x^2 + 4x + 3, 4x^2 + 2$
$x^3 + 3x + 0$	2	N	-	-	-	-	0
$x^3 + 3x + 1$	0	0	-	-	-	-	-
$x^3 + 3x + 2$	4	Y	2	3	(4,4)	-	$x, 2x^2 + 4, 3x^2 + 4x + 1$
$x^3 + 3x + 3$	4	Y	2	3	(1,4)	-	$x, 2x^2 + 4x + 4, 3x^2 + 1$
$x^3 + 3x + 4$	0	0	-	-	-	-	-
$x^3 + 4x + 0$	4	Y	2	3	(0,4)	(0,3)	0,1,4
$x^3 + 4x + 1$	2	N	-	-	-	-	3
$x^3 + 4x + 2$	1	Y	1	4	(4,2)	-	$x, 2x^2 + 3x + 2, 3x^2 + x + 3$
$x^3 + 4x + 3$	1	Y	1	4	(1,2)	-	$x, 2x^2 + x + 2, 3x^2 + 3x + 3$
$x^3 + 4x + 4$	2	N	-	-	-	-	2

Table 4.2: Table for prime 7 which is of the form $p \ = \ 4k+3$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	**cubic root of** γ	**root of the polynomial**
x^3+1x+0	3	N	-	-	-	-	0
x^3+1x+1	4	Y	2	1	(3,4)	-	$x, 2x^2+6, 5x^2+6x+1$
x^3+1x+2	0	0	-	-	-	-	-
x^3+1x+3	5	N	-	-	-	-	5
x^3+1x+4	5	N	-	-	-	-	2
x^3+1x+5	0	0	-	-	-	-	-
x^3+1x+6	4	Y	2	1	(4,4)	-	$x, 2x^2+6x+6, 5x^2+1$
x^3+2x+0	3	N	-	-	-	-	0
x^3+2x+1	4	Y	2	1	(3,4)		$x, 3x^2+6x+4, 4x^2+3$
x^3+2x+2	0	0	-	-	-	-	-
x^3+2x+3	5	N	-	-	-	-	6
x^3+2x+4	5	N	-	-	-	-	1
x^3+2x+5	0	0	-	-	-	-	-
x^3+2x+6	4	Y	2	1	(4,4)	-	$x, 3x^2+6x+4, 4x^2+3$
x^3+3x+0	4	Y	2	1	(0,4)	(0,1)	0,2,5
x^3+3x+1	5	N	-	-	-	-	4
x^3+3x+2	1	Y	1	4	(6,2)	-	$x, 2x^2+x+4, 5x^2+5x+3$
x^3+3x+3	6	N	-	-	-	-	1
x^3+3x+4	6	N	-	-	-	-	6
x^3+3x+5	1	Y	1	4	(1,2)	-	$x, 2x^2+5x+4, 5x^2+x+3$
x^3+3x+6	5	N	-	-	-	-	3
x^3+4x+0	3	N	-	-	-	-	0
x^3+4x+1	4	Y	2	1	-	-	$x, x^2+5, 6x^2+6x+2$
x^3+4x+2	0	0	-	-	-	-	-
x^3+4x+3	5	N	-	-	-	-	3
x^3+4x+4	5	N	-	-	-	-	4
x^3+4x+5	0	0	-	-	-	-	-
x^3+4x+6	4	Y	2	1	(4,4)	-	$x, x^2+6x+5, 6x^2+2$
x^3+5x+0	4	Y	2	1	(0,4)	(0,1)	0,3,4
x^3+5x+1	5	N	-	-	-	-	1
x^3+5x+2	1	Y	1	4	(6,2)	-	$x, x^2+x+1, 6x^2+5x+6$
x^3+5x+3	6	N	-	-	-	-	2
x^3+5x+4	6	N	-	-	-	-	5
x^3+5x+5	1	Y	1	4	(1,2)	-	$x, x^2+5x+1, 6x^2+x+6$
x^3+5x+6	5	N	-	-	-	-	6
x^3+6x+0	4	Y	2	1	(0,4)	(0,1)	0,1,6
x^3+6x+1	5	N	-	-	-	-	2
x^3+6x+2	1	Y	1	4	(6,2)	-	$x, 3x^2+5x+5, 4x^2+x+2$
x^3+6x+3	6	N	-	-	-	-	4
x^3+6x+4	6	N	-	-	-	-	3

Table 4.3: Table for prime 13 which is of the form $p = 8k + 5$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	$\gamma^{\frac{1}{3}}$	**root of the polynomial**
$x^3 + 1x + 0$	9	Y	3	9	(0,11)	(0,7)	0,5,8
$x^3 + 1x + 1$	8	N	-	-	-	-	7
$x^3 + 1x + 2$	5	N	-	-	-	-	12
$x^3 + 1x + 3$	0	0	-	-	-	-	-
$x^3 + 1x + 4$	6	N	-	-	-	-	10
$x^3 + 1x + 5$	10	Y	6	5	(4,9)	-	$x, 6x^2 + 4, 7x^2 + 12x + 9$
$x^3 + 1x + 6$	12	Y	5	2	(10,1)	-	$x, 2x^2 + 10, 11x^2 + 11x + 3$
$x^3 + 1x + 7$	12	Y	5	2	(3,1)	-	$x, 2x^2 + 11x + 10, 11x^2 + x + 3$
$x^3 + 1x + 8$	10	Y	6	5	(9,9)		$x, 6x^2 + 12x + 4, 7x^2 + 9$
$x^3 + 1x + 9$	6	N	-	-	-	-	3
$x^3 + 1x + 10$	0	0	-	-	-	-	-
$x^3 + 1x + 11$	5	N	-	-	-	-	1
$x^3 + 1x + 12$	8	N	-	-	-	-	6
$x^3 + 2x + 0$	7	N	-	-	-	-	0
$x^3 + 2x + 1$	6	N	-	-	-	-	2
$x^3 + 2x + 2$	3	Y	4	12	(12,6)	-	$x, 5x^2 + 5x + 11, 8x^2 + 7x + 2$
$x^3 + 2x + 3$	11	N	-	-	-	-	12
$x^3 + 2x + 4$	4	Y	2	6	(11,3)	-	$x, 3x^2 + 10x + 4, 10x^2 + 2x + 9$
$x^3 + 2x + 5$	8	N	-	-	-	-	8
$x^3 + 2x + 6$	10	Y	6	5	(10,9)	(1,8)	3,4,6
$x^3 + 2x + 7$	10	Y	6	5	(3,9)	(2,1)	7,9,10
$x^3 + 2x + 8$	8	N	-	-	-	-	5
$x^3 + 2x + 9$	4	Y	2	6	(2,3)	-	$x, 3x^2 + 2x + 4, 10x^2 + 10x + 9$
$x^3 + 2x + 10$	11	N	-	-	-	-	1
$x^3 + 2x + 11$	3	Y	4	12	(1,6)	-	$x, 5x^2 + 7x + 11, 8x^2 + 5x + 2$
$x^3 + 2x + 12$	6	N	-	-	-	-	11
$x^3 + 3x + 0$	9	Y	3	9	(0,11)	(0,7)	0,6,7
$x^3 + 3x + 1$	8	N	-	-	-	-	11
$x^3 + 3x + 2$	5	N	-	-	-	-	4
$x^3 + 3x + 3$	0	0	-	-	-	-	-
$x^3 + 3x + 4$	6	N	-	-	-	-	12
$x^3 + 3x + 5$	10	Y	6	5	(4,9)	-	$x, 5x^2 + 10, 8x^2 + 12x + 3$
$x^3 + 3x + 6$	12	Y	5	2	(10,1)	-	$x, 6x^1 + x + 12, 7x^2 + 11x + 1$
$x^3 + 3x + 7$	12	Y	5	5	(3,1)	-	$x, 6x^2 + 11x + 12, 7x^2 + x + 1$
$x^3 + 3x + 8$	10	Y	6	5	(9,9)	-	$x, 5x^2 + 12x + 10, 8x^2 + 3$
$x^3 + 3x + 9$	6	N	-	-	-	-	1
$x^3 + 3x + 10$	0	0	-	-	-	-	-
$x^3 + 3x + 11$	5	N	-	-	-	-	9
$x^3 + 3x + 12$	8	N	-	-	-	-	2

Table 4.4: Table for prime 13 which is of the form $p = 8k + 5$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	$\gamma^{\frac{1}{3}}$	**root of the polynomial**
$x^3 + 4x + 0$	4	Y	2	6	(0,3)	(0,4)	0,3,10
$x^3 + 4x + 1$	3	Y	4	12	(6,6)	-	$x, 3x^2 + 8, 10x^2 + 12x + 5$
$x^3 + 4x + 2$	0	0	-	-	-	-	-
$x^3 + 4x + 3$	8	N	-	-	-	-	11
$x^3 + 4x + 4$	1	Y	1	3	(11,8)	-	$x, x^2 + 11x + 7, 12x^2 + x + 6$
$x^3 + 4x + 5$	5	N	-	-	-	-	12
$x^3 + 4x + 6$	7	N	-	-	-	-	7
$x^3 + 4x + 7$	7	N	-	-	-	-	6
$x^3 + 4x + 8$	5	N	-	-	-	-	1
$x^3 + 4x + 9$	1	Y	1	3	(2,8)	-	$x, x^2 + x + 7, 12x^2 + 11x + 6$
$x^3 + 4x + 10$	8	N	-	-	-	-	2
$x^3 + 4x + 11$	0	0	-	-	-		-
$x^3 + 4x + 12$	3	Y	4	12	(7,6)	-	$x, 3x^2 + 12x + 8, 10x^2 + 5$
$x^3 + 5x + 0$	7	N	-	-	-	-	0
$x^3 + 5x + 1$	6	N	-	-	-	-	6
$x^3 + 5x + 2$	3	y	4	12	(12,6)	-	$x, 6x^2 + 5x + 7, 7x^2 + 7x + 6$
$x^3 + 5x + 3$	11	N	-	-	-	-	10
$x^3 + 5x + 4$	4	Y	2	6	(11,3)	-	$x, x^2 + 10x + 12, 12x^2 + 2x + 1$
$x^3 + 5x + 5$	8	N	-	-	-	-	11
$x^3 + 5x + 6$	10	Y	6	5	(10,9)	(1,8)	5,9,12
$x^3 + 5x + 7$	10	Y	6	5	(3,9)	(2,1)	1,4,8
$x^3 + 5x + 8$	8	N	-	-	-	-	2
$x^3 + 5x + 9$	4	Y	2	6	(2,3)	-	$x, x^2 + 2x + 12, 12x^2 + 10x + 1$
$x^3 + 5x + 10$	11	N	-	-	-	-	3
$x^3 + 5x + 11$	3	Y	4	12	(1,6)	-	$x, 6x^2 + 7x + 7, 7x^2 + 5x + 6$
$x^3 + 5x + 12$	6	N	-	-	-	-	7
$x^3 + 6x + 0$	7	N	-	-	-	-	0
$x^3 + 6x + 1$	6	N	-	-	-	-	5
$x^3 + 6x + 2$	3	Y	4	12	(12,6)	-	$x, 2x^2 + 5x + 8, 11x^2 + 7x + 5$
$x^3 + 6x + 3$	11	N	-	-	-	-	4
$x^3 + 6x + 4$	4	Y	2	6	(11,3)	-	$x, 4x^2 + 2x + 3, 9x^2 + 10x + 10$
$x^3 + 6x + 5$	8	N	-	-	-	-	7
$x^3 + 6x + 6$	10	Y	6	5	(10,9)	(1,8)	1,2,10
$x^3 + 6x + 7$	10	Y	6	5	(3,9)	(2,1)	3,11,12
$x^3 + 6x + 8$	8	N	-	-	-	-	6
$x^3 + 6x + 9$	4	Y	2	6	(2,3)	-	$x, 4x^2 + 10x + 3, 9x^2 + 2x + 10$
$x^3 + 6x + 10$	11	N	-	-	-	-	9
$x^3 + 6x + 11$	3	Y	4	12	(1,6)	-	$x, 2x^2 + 7x + 8, 11x^2 + 5x + 5$
$x^3 + 6x + 12$	6	N	-	-	-	-	8

Table 4.5: Table for prime 13 which is of the form $p = 8k + 5$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	$\gamma^{\frac{1}{3}}$	**root of the polynomial**
$x^3 + 7x + 0$	6	N	-	-	-	-	0
$x^3 + 7x + 1$	5	N	-	-	-	-	9
$x^3 + 7x + 2$	2	N	-	-	-	-	6
$x^3 + 7x + 3$	10	Y	6	5	(5,9)	-	$x, 3x^2 + 5x + 1, 10x^2 + 7x + 12$
$x^3 + 7x + 4$	3	Y	4	12	(11,6)	(1,3)	2,3,8
$x^3 + 7x + 5$	7	N	-	-	-	-	1
$x^3 + 7x + 6$	9	Y	3	9	(10,11)	-	$x, 6x^2 + 2x + 2, 7x^2 + 10x + 11$
$x^3 + 7x + 7$	9	Y	3	9	(3,11)	-	$x, 6x^2 + 10x + 2, 7x^2 + 2x + 11$
$x^3 + 7x + 8$	7	N	-	-	-	-	12
$x^3 + 7x + 9$	3	Y	4	12	(2,6)	(1,7)	5,10,11
$x^3 + 7x + 10$	10	Y	6	5	(8,9)	-	$x, 3x^2 + 7x + 1, 10x^2 + 5x + 12$
$x^3 + 7x + 11$	2	N	-	-	-	-	7
$x^3 + 7x + 12$	5	N	-	-	-		4
$x^3 + 8x + 0$	6	N	-	-	-	-	0
$x^3 + 8x + 1$	5	N	-	-	-	-	3
$x^3 + 8x + 2$	2	N	-	-	-	-	2
$x^3 + 8x + 3$	10	Y	6	5	(5,9)	-	$x, 4x^2 + 7x + 4, 9x^2 + 5x + 9$
$x^3 + 8x + 4$	3	Y	4	12	(11,6)	(1,3)	1,5,7
$x^3 + 8x + 5$	7	N	-	-	-	-	9
$x^3 + 8x + 6$	9	Y	3	9	(10,11)	-	$x, 5x^2 + 2x + 5, 8x^2 + 10x + 8$
$x^3 + 8x + 7$	9	Y	3	9	(3,11)	-	$x, 5x^2 + 10x + 5, 8x^2 + 2x + 8$
$x^3 + 8x + 8$	7	N	-	-	-	-	4
$x^3 + 8x + 9$	3	Y	4	12	(2,6)	(1,7)	6,8,12
$x^3 + 8x + 10$	10	Y	6	5	(8,9)	-	$x, 4x^2 + 5x + 4, 9x^2 + 7x + 9$
$x^3 + 8x + 11$	2	N	-	-	-	-	11
$x^3 + 8x + 12$	5	N	-	-	-	-	10
$x^3 + 9x + 0$	9	Y	3	9	(0,11)	(0,7)	0,2,11
$x^3 + 9x + 1$	8	N	-	-	-	-	8
$x^3 + 9x + 2$	5	N	-	-	-	-	10
$x^3 + 9x + 3$	0	0	-	-	-	-	-
$x^3 + 9x + 4$	6	N	-	-	-	-	4
$x^3 + 9x + 5$	10	Y	6	4	(4,9)	-	$x, 2x^2 + 12, 11x^2 + 12x + 1$
$x^3 + 9x + 6$	12	Y	5	2	(10,1)	-	$x, 5x^2 + x + 4, 8x^2 + 11x + 9$
$x^3 + 9x + 7$	12	Y	5	2	(3,1)	-	$x, 5x^2 + 11x + 4, 8x^2 + x + 9$
$x^3 + 9x + 8$	10	Y	6	5	(9,9)	-	$x, 2x^2 + 12x + 12, 11x^2 + 1$
$x^3 + 9x + 9$	6	N	-	-	-	-	9
$x^3 + 9x + 10$	0	0	-	-	-	-	-
$x^3 + 9x + 11$	5	N	-	-	-	-	3
$x^3 + 9x + 12$	8	N	-	-	-	-	5

Table 4.6: Table for prime 13 which is of the form $p = 8k+5$

polynomial	**D**	**QR**	$\sqrt{D}$	μ	γ	$\gamma^{\frac{1}{3}}$	**root of the polynomial**
$x^3+10x+0$	4	Y	2	6	(0,3)	(0,4)	0,4,9
$x^3+10x+1$	3	Y	4	12	(6,6)	-	$x, x^2+11, 12x^2+12x+2$
$x^3+10x+2$	0	0	-	-	-	-	-
$x^3+10x+3$	8	N	-	-	-	-	7
$x^3+10x+4$	1	Y	1	3	(11,8)	-	$x, 4x^2+x+5, 9x^2+11x+8$
$x^3+10x+5$	5	N	-	-	-	-	10
$x^3+10x+6$	7	N	-	-	-	-	8
$x^3+10x+7$	7	N	-	-	-	-	5
$x^3+10x+8$	5	N	-	-	-	-	3
$x^3+10x+9$	1	Y	1	3	(2,8)	-	$x, 4x^2+11x+5, 9x^2+x+8$
$x^3+10x+10$	8	N	-	-	-	-	6
$x^3+10x+11$	0	0	-	-	-	-	-
$x^3+10x+12$	3	Y	4	12	(7,6)	-	$x, x^2+12x+11, 12x^2+2$
$x^3+11x+0$	6	N	-	-	-		0
$x^3+11x+1$	5	N	-	-	-	-	1
$x^3+11x+2$	2	N	-	-	-	-	5
$x^3+11x+3$	10	Y	6	5	(5,9)	-	$x, x^2+5x+3, 12x^2+7x+10$
$x^3+11x+4$	3	Y	4	12	(11,6)	(1,3)	6,9,11
$x^3+11x+5$	7	N	-	-	-	-	3
$x^3+11x+6$	9	Y	3	9	(10,11)	-	$x, 2x^2+2x+6, 11x^2+10x+7$
$x^3+11x+7$	9	Y	3	9	(3,11)	-	$x, 2x^2+10x+6, 11x^2+2x+7$
$x^3+11x+8$	7	N	-	-	-	-	3
$x^3+11x+9$	3	Y	4	12	(2,6)	(1,7)	2,4,7
$x^3+11x+10$	10	Y	6	5	(8,9)	-	$x, x^2+7x+3, 12x^2+5x+10$
$x^3+11x+11$	2	N	-	-	-	-	8
$x^3+11x+12$	5	N	-	-	-	-	12
$x^3+12x+0$	4	Y	2	6	(0,3)	(0,4)	0,1,12
$x^3+12x+1$	3	Y	4	12	(6,6)	-	$x, 4x^2+12x+6, 9x^2+7$
$x^3+12x+2$	0	0	-	-	-	-	-
$x^3+12x+3$	8	N	-	-	-	-	8
$x^3+12x+4$	1	Y	1	3	(11,8)	-	$x, 3x^2+11x+11, 10x^2+x+2$
$x^3+12x+5$	5	N	-	-	-	-	4
$x^3+12x+6$	7	N	-	-	-	-	11
$x^3+12x+7$	7	N	-	-	-	-	2
$x^3+12x+8$	5	N	-	-	-	-	9
$x^3+12x+9$	1	Y	1	3	(2,8)	-	$x, 3x^2+x+11, 10x^2+11x+2$
$x^3+12x+10$	8	N	-	-	-	-	5
$x^3+12x+11$	0	0	-	-	-	-	-
$x^3+12x+12$	3	Y	4	12	(7,6)	-	$x, 4x^2+6, 9x^2+12x+7$

Bibliography

[1] R.Schoof. Counting points on elliptic curves over finite field.*J. Thor. Nombres Bordeaux,* $7:219\ -\ 254,\ \ 1995.$

[2] Counting the number of points on elliptic curves over finite field of characteristic greater than three, with F.Lehmann, M. Mauerer, and V. Mueller, in Proc.*First Algorithmic Number Theory Symposium, pp.* $60-70$*,* 1994.

[3] New Explicit Conditions of Elliptic Curve Traces For FR-Reduction, A.Miyaji, M.Nakabayashi, S.Takano .*IEICE TRANS. FUNDAMENTALS. vol.E*84*-A, NO.*5 *MAY* 2001.

[4] Reducing Elliptic Curve Logarithms to a Logarithms in a Finite Field, Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone *IEEE TRANSACllONS ON INFORMATION THEORY, VOL.* 39*, NO.* 5*, SEPTEMBER* 1993.

[5] Criteria for the Irreducibility of Functions in a Finite Field. Read. Sept. 3,1906. Bulletin of the American Mathematical Society, vol.13.