Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics

Fumiyuki Momose†, Jinhui Chao‡

† Department of Mathematics, Chuo Univeristy, Tokyo Japan
‡Department of Information and System Engineering,
Chuo University, Tokyo Japan

Contents

Abstract

In this paper, we present a classification of classes of elliptic curves defined over cubic extension of finite fields with odd characteristics, which have coverings over the finite fields therefore can be attacked by the GHS attack. We then show the density of these weak curves with hyperelliptic and non-hyperelliptic coverings respectively. In particular, we shown for elliptic curves defined in Legendre forms, about half of them are weak.

keywords

Elliptic curves, Hyperelliptic curves, Non-hyperelliptic curves, Index calculus, GHS attack, Cover attack

1 Introduction

Cryptosystems based on elliptic curves and hyperelliptic curves of genus 2,3 are widely believed to be secure and have been used in many applications. In fact, only special therefore a small number of curves e.g. anomalous or supersingular ones have been attacked until now. In this paper, we show that in certain cases, a large number of elliptic curves can be attacked by GHS attack.

Let q be a power of an odd prime. $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}$.

General attacks to discrete logarithm on an abelian group G with $l := \#G$ (known as key-length in cryptosystems), such as the Baby-step-giant-step attack or Pollard's rho-method or lambda-method are called as "square-root" attacks, i.e., their computional costs equal to the square-root of the group order $\tilde{O}(l^{1/2})$). ($\tilde{O}(x) := O(x \log^m x)$). For elliptic and genus 2 hyperelliptic curves, these attacks are the most powerful attacks at the present.

Besides the square-root algorithms there are two main attacks to algebraic curve based cryptosystems, variations of the index calculus attack [12][9][26][13][24] and the GHS attack [10] [14][11] [20][6] [17][18] [27][28][8][4].

For a hyperelliptic curve cryptosystem, the most powerful attack is the double-large-prime variation of index calculus by Gaudry-Theriault-Thome-Diem and Nagao [13], [24], with complexities $\tilde{O}(q^{2-\frac{2}{g}})$. In particular for $g = 3$, the cost is $\tilde{O}(q^{4/3}) = \tilde{O}(l^{4/9})$, a little faster than the square-root attacks. However, the hyperelliptic curves of genera 5 to 9 can be attacked by these algorithms more effectively than the square-root attacks.

In spite of a common belief that non-hyperelliptic curves should be harder to attack than hyperelliptic ones, Diem recently showed an attack under which non-hyperelliptic curves of low degrees and genera greater than or equal to 3 are actually weaker than hyperelliptic curves[7]. More specifically, when C is a non-hyperelliptic curve of genus $g \geq 3$, one can almost always find a birational transform over k

$$C \overset{birat}{\dashrightarrow} C' \subset \mathbb{P}^2$$

such that $\deg C' = d \geq g + 1$. (Notice that when C' is a hyperelliptic curve, one has $\deg C' = d \geq g + 2$).) Then when C' is defined over k, the complexity of Diem's double-large-prime variation [7] are $\tilde{O}(q^{2-\frac{2}{d-2}})$. When $d = g+1$, it is $\tilde{O}(q^{2-\frac{2}{g-1}})$. In particular, genus 3 non-hyperelliptic curves over $\mathbb{F}_q$ can be attacked in an expected time $\tilde{O}(q) = \tilde{O}(l^{1/3})$. Recently, Smith shown that a certain fraction of hyperelliptic curves of genus three can be transformed to nonhyperelliptic curves [25].

Another attack to algebraic-curve-based cryptosystems is the GHS and related attacks. It was G. Frey who induced the use of Weil descent into elliptic curve cryptosystem[10], which is then generalized to the cover attack[6][8]. Let E/k_d be an elliptic curve, $W := Res_{k_d/k}E$ its Weil restriction. Then since $E(k_d) \simeq W(k)$, if there is a covering curve C/k of E, it may be possible to transfer the DLP on $E(k_d)$ to the Jacobian of the covering curve $J(C)(k)$. The GHS attack proposed in [14] then used the norm-conorm map to transfer the DLP from $Cl(E/k_d)$ to $Cl(C/k)$.

A natural and important question is what kind and how many of curves are vulnerable to this attacks. Until now, certain weak classes of curves have been discovered [8][27][28]. However, totality of the weak curves and their numbers are still not yet well understood.

In this paper, we present a complete classfication and explicit classes of elliptic curves defined over cubic extension of finite fields with odd characteristics, which have weak coverings therefore can be attacked effectively by the GHS attack.

Below, we will follow the setting and refer the details of the GHS attack in [6] and [4].

Let C_0/k_d to be an algebraic curve over k_d with genus $g_0 := g(C_0) \geq 1$. Assume there exists an algebraic curve C of genus $g := g(C)$ defined over k such that

$$\pi : C \twoheadrightarrow C_0$$

is a covering defined over k_d.

We assume the following isogeny condition. i.e. for the induced map

$$\pi_* : \quad J(C) \quad \twoheadrightarrow \quad J(C_0)$$

the restriction of scalar

$$Res(\pi_*) : J(C) \longrightarrow \mathrm{Res}_{k_d/k}\big(J(C_0)\big)$$

defines an isogeny over k. Therefore, $g = dg_0$.

Notice in order to transfer the DL problem on $J(C_0)$ to $J(C)$, it has to be $g \geq dg_0$. Under the above condition, the resulting $J(C)$ has the smallest size therefore this is the most favorite situation for GHS attacks.

We then present classification and density analysis of such weak curves or to count the number of such curves, and show how to test if a curve has a weak covering so they could be easily avoided in cerain cases,.

The results of this paper are summerized in the following theorem.

Theorem 1. *Under the isogeny condition, among elliptic curves E defined over a cubic extension field k_3, only the following two types have covering $C/\mathbb{P}^1$.*

$$\text{Type I:} \qquad E_I: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q) \tag{1}$$

$$\alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4 \tag{2}$$

$$\text{Type II:} \qquad E_{II}: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right) \tag{3}$$

$$\alpha \in k_6 \setminus \{k_2 \cup k_3\}, \quad \beta = \alpha^{q^3} \tag{4}$$

Each Type of these curves is k_3-isomorphic to a Legendre form:

$$E_i \simeq \quad y^2 = e_i x(x-1)(x-\lambda_i), \quad e_i \in k^\times$$

Define

$$\lambda(\alpha, \beta) := \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{q+1}}$$

for Type II curves, $\beta = \alpha^{q^3}$.

For the Type I curves,

$$e_1 = 1, \qquad \lambda_1 = \lambda(\alpha, \beta)$$

The number of λ such that the Type I curves have non-hyperelliptic covers is

$$\#\{\lambda\} = \frac{q^3 - q^2 - q - 3}{2}$$

For the Type II curves

$$e_2 = (\alpha - \alpha^{q^3})^{q+1}, \qquad \lambda_2 = -\lambda(\alpha, \beta)$$

and

$$\begin{cases} e_2 \in (k_3^\times)^2 & \Longleftrightarrow \quad q \equiv 3 \bmod 4 \\ e_2 \notin (k_3^\times)^2 & \Longleftrightarrow \quad q \equiv 1 \bmod 4 \end{cases}$$

Thus only in the first case, we can assume that $e = 1$.

The number of λ such that the Type II curves have non-hyperelliptic covers is

$$\#\{\lambda\} = \frac{q^3 - q^2 + q - 1}{2}$$

Among the Type I and Type II curves, the number of λ such that the curves E have hyperelliptic covers C is

$$\#\{\lambda\} = q^2$$

As to the Type I curves, we show in Lem 6.2 a fast algorithm to test if an elliptic curve is Type I curve. Implementation of GHS attack to these two types of curves are discussed in [16].

The numbers of these weak curves are alarmingly large. e.g. if you chosen random elliptic curves E defined over k_3 in the Legendre form with $\#E(k_3)$ of 160 bit prime orders, then a half of them are weak and can not be used in cryptosystems since their covering $C(k)$ only have 107 bits key-length under the GHS attack.This may be the first time that such a large number of curves which are supposed to be secure are attacked since the proposal of elliptic and hyperelliptic cryptosystems.

We also like to point out that the curves over extension fields could be often desirable in practice for fast and low-cost implementation, especially certain extension fields with good properties. An example is to use extension fields which possess a normal basis. Another example is that a fast and cheap way to implemente a 160 bit elliptic cryptosystem is to use a 64bit processor and an elliptic curve defined over cubic extension of a 64bit prime field. The above results show that such a setting could be dangeous. Therefore threat of Weil descent attack should not be underestimated.

2 Curves obtained from (2,2,...,2) coverings

Let $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}, d \geq 2$. C_0/k_d is a hyperelliptic curve with $g(C_0) := g_0 : 1, 2, 3$. Consider the case that there is an algebraic curve C/k s.t. there is a covering

$$\exists \pi/k_d : C \longrightarrow C_0$$

defined over k_d. In particular, C is a n-tuple $(2, 2, ..., 2)$ covering of $\mathbb{P}^1(x)$ with degree 2^n,or $k_d(C)$ is the compositum of $k_d({}^{\sigma^i}C_0), i = 0, ..., d-1$ with extension degree 2^n.

The Weil restriction of $J(C_0)$ is defined as

$$Res_{k_d/k} J(C_0) := \prod_{i=0}^{d-1} J({}^{\sigma^i}C_0)$$

which is an abelian variety of dimension dg_0.

Then the induced map

$$\pi_* : J(C) \longrightarrow J(C_0).$$

has the restriction of scalar

$$Res(\pi_*) : J(C) \longrightarrow \mathrm{Res}_{k_d/k}\big(J(C_0)\big)$$

which is assumed to be an isogeny over k. Therefore, $g = dg_0$.

Then one can prove that

Lemma 1. .

(1) $\ker Res(\pi_*) \subset J(C)[2^{n-1}]$
(2) If C is hyperellptic, then the above kernal can be described explicitly.

The similar results for GHS attack have been proved in [14][17][18].
Hereafter, we assume C_0 is an elliptic curve E and $d = 3$.

2.1 Definition equations of E

When the degree of the covering $C/\mathbb{P}^1$ is eight, C is a hyperellptic curve over k of genus three. (This was mentioned in [6] footnote 6).

Lemma 2. *When the degree of the covering $C/\mathbb{P}^1$ is eight, E/k_3 with C as its (2,2,2) covering has the form of*

$$\begin{aligned} E/k_3: \quad y^2 &= eg(x)(x-\alpha)(x-\alpha^q) \\ \textit{here} \quad & \alpha \in k_3 \setminus k, \\ & g(x) \in k[x], \quad \deg g(x) = 1 \textit{ or } 2, \\ & e \in k_3^\times \end{aligned} \tag{5}$$

Proof: Denote the number of ramification points of the covering $C \longrightarrow \mathbb{P}^1$ on $\mathbb{P}^1(x)$ as S, the set ramification points on E as R. Define $R_i :=^{\sigma^i} R$, which are sets of ramifications points on ${}^{\sigma^i}E, i = 0, 1, 2,\ R_0 = R$. We have $\#R = \#R_1 = \#R_2 = 4$.

We divide the ramification points of ${}^{\sigma^i}E$ into three types.

- : $T_1 = \{a \in k_3 \setminus k\ |a$ belongs to only one of $R_i, i = 0, 1, 2\ \}$
- : $T_2 = \{b \in k_3 \setminus k\ |b$ belongs to intersection of two R_i but not three$\}$.
- : $T_3 = \{c \in \cap_{i=0}^{2} R_i\}$ or σ-invariant.

By Riemann-Hurwitz formula, $\exists N$ s.t.

$$2g(C) - 2 = \deg(C \to \mathbb{P}^1)(2g(\mathbb{P}^1) - 2) + NS$$

one has $S = 5, N = 4$. This implies

$$\begin{aligned} \#R &= \#T_1 + 2\#T_2 + \#T_3 = 4 \\ S &= \# \cup_{i=0}^{2} R_i = 3\#T_1 + 3\#T_2 + \#T_3 = 5 \end{aligned}$$

Thus one has

$$\#T_1 = 0, \#T_2 = 1, \#T_3 = 2$$

Donote

$$T_2 = \{\alpha\}, \alpha \in k_3 \setminus k, s.t. \{\alpha, \alpha^q\} \subset R \qquad T_3 = \{c, c'\}$$

Thus we have

$$E: y^2 = e(x-c)(x-c')(x-\alpha)(x-\alpha^q) = eg(x)(x-\alpha)(x-\alpha^q), \qquad e \in k_3^\times$$

Now take the norm of E,

$$N_{k_3/k}(y^2) \quad = \quad N_{k_3/k}(e) g(x)^3 N_{k_3/k}(x-\alpha)^2$$

one has the following curve

$$\left(\frac{N_{k_3/k}(y)}{g(x) N_{k_3/k}(x-\alpha)}\right)^2 = N_{k_3/k}(e) g(x)$$

which is isomorphic to $\mathbb{P}^1$ since $\deg g(x) \leq 2$. Therefore, the covering of the curve (5) is indeed a $(2,2,2)$-type.

$\square$

When the degree of cover $C \longrightarrow \mathbb{P}^1(x)$ is four, we have

Lemma 3. *The elliptic curves E/k_3 which have C as their $(2,2)$ covering can be divided into the following two types.*

$$\textit{Type I:} \qquad E: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q) \tag{6}$$

$$\alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4 \tag{7}$$

$$\textit{Type II:} \qquad E: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right) \tag{8}$$

$$\alpha \in k_6 \setminus \{k_2 \cup k_3\} \tag{9}$$

The equation (6) of Type I was given as Eq.(10) in [8] as an example.

Proof: We use the same notation as in the proof of Lemma 2. By Rieman-Hurwitz formula, $\exists N$ s.t.

$$2g(C) - 2 \quad = \quad \deg(C/\mathbb{P}^1)\left(2g(\mathbb{P}^1) - 2\right) + NS$$

The only possibilities is $N = 2, S = 6$.Then

$$\#T_1 + 2\#T_2 + \#T_3 \quad = \quad 4 \tag{10}$$

$$3\#T_1 + 3\#T_2 + \#T_3 \quad = \quad 6 \tag{11}$$

Therefore

$$2\#T_1 + \#T_2 = 2$$

Thus there are two possibilities:

$$\#T_1 = 0, \#T_2 = 2, \#T_3 = 0, \quad \text{and} \quad \#T_1 = 1, \#T_2 = 0, \#T_3 = 3$$

We call the two cases as Type I and II hereafter.
Type I:

$$R(E) \quad = \quad \{\alpha, \alpha^q, \beta, \beta^q\} \qquad, \{\alpha, \alpha^q, \alpha^{q^2}\} \cap \{\beta, \beta^q, \beta^{q^2}\} = \emptyset \tag{12}$$

Type II:

$$R(E) = \{\alpha^{\sigma^i}, \alpha^{\sigma^{i+1}}, \alpha^{\sigma^j}, \alpha^{\sigma^{j+1}}\}, \qquad \#R(E) = 4$$

Then one has the definition equations of the Type I and II curves.

$$E : y^2 = e\,(x-\alpha)\,(x-\alpha^q)\,(x-\beta)\,(x-\beta^q)\,, \qquad e \in k_3^\times$$

where $\beta = \alpha^{q^3}$ in Type II.

We now take the norm of the curve, then for Type I,

$$N_{k_3/k}(y)^2 \quad = \quad N_{k_3/k}(e)N_{k_3/k}(x-\alpha)^2 N_{k_3/k}(x-\beta)^2$$

Since

$$N_{k_3/k}(e) = \left(\frac{N_{k_3/k}(y)}{N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\beta)}\right)^2$$

One knows that $e \in \left(k_3^\times\right)^2$ thus can be assumed 1. Then

$${}^{\sigma^2}y = \pm\frac{N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\beta)}{y\ {}^{\sigma}y}$$

For Type II,

$$\begin{aligned} N_{k_3/k}(y)^2 &= N_{k_3/k}(e)N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\alpha^q)N_{k_3/k}(x-\alpha^{q^3})N_{k_3/k}(x-\alpha^{q^4}) \\ &= N_{k_3/k}(e)N_{k_3/k}(x-\alpha)^4 \end{aligned}$$

$${}^{\sigma^2}y = \pm\frac{N_{k_3/k}(x-\alpha)}{y\ {}^{\sigma}y}$$

Thus, when e is a square, thus one has a $(2,2)$ covering here.

□

2.2 Condition for C to be hyperelliptic

Let the defintion equation of E to be

$$E : y^2 \quad = \quad (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q) \tag{13}$$

For Type II curves, $\beta = \alpha^{q^3}$.

Lemma 4.

$$C : \qquad \textit{hyperelliptic} \iff \exists\Theta \in GL_2(k),\ \textit{s.t.}\ Tr(\Theta) = 0,\ \beta = \Theta\cdot\alpha \tag{14}$$

Proof:

For the $(2,2)$ covering $C \longrightarrow E \longrightarrow \mathbb{P}^1(x)$, Θ induces the hyperelliptic involusion of C.

In fact, $\Theta \in Aut(\mathbb{P}^1(x))$ defines a degree two covering $\theta : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$. We will show explicitly the existance of curves in the diagram. s.t. $\mathbb{P}^1(t) = \mathbb{P}^1(x)/\theta$.

In fact, a such $\Theta \in GL_2(k)$ can be classified into the following two forms:

$$\Theta_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Theta_2 = \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix} \qquad e \in k^{\times} \setminus \left(k^{\times}\right)^2$$

We treat the two cases separately below.

$$\begin{tikzcd}
 & & C \arrow[dl] \arrow[dr] & \\
 & E \arrow[dl] \arrow[dr] & & \mathbb{P}^1(u) \arrow[dl] \\
\mathbb{P}^1(x) \arrow[dr] & & \mathbb{P}^1(s) \arrow[dl] & \\
 & \mathbb{P}^1(t) & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & C \arrow[dl, "(2{,}2)"'] \arrow[dr, "2"] & \\
\mathbb{P}^1(x) \arrow[dr, "2"'] & & \mathbb{P}^1(u) \arrow[dl, "(2{,}2)"] \\
 & \mathbb{P}^1(t) &
\end{tikzcd}$$

1. We first treat Θ_1. Then

   $$\Theta_1(x) = -x, \quad \beta = \Theta_1 \cdot \alpha = -\alpha$$

   $$s := x(\Theta_1 \cdot x) = -x^2$$

   The degree two covering $\theta_1 : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$ is defined by

   $$x^2 = t$$

   Now we find the definition equation of $\mathbb{P}^1(s)$ as follows.
   Define

   $$\begin{array}{rcl} \zeta_1 : E & \longrightarrow & E \\ (x, y) & \longmapsto & (-x, -y) \end{array}$$

   Then $\mathbb{P}^1(s)$ is the quotient of E/ζ_1.

   $$s := xy$$

   Then

   $$\mathbb{P}^1(s) : s^2 = t(t - \alpha^2)(t - \alpha^{2q})$$

2. The second case: Θ_2. Then

   $$\Theta_2(x) = \frac{e}{x}, \qquad \beta = \Theta_2 \cdot \alpha = \frac{e}{\alpha}$$

   The degree two covering $\theta_2 : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$ is defined by

   $$t = x + \Theta_2 \cdot x = x + \frac{e}{x}$$

or

$$x^2 - tx + e = 0$$

Now we find the definition equation of $\mathbb{P}^1(s)$ as follows.

Define

$$\begin{array}{rcl} \zeta_2 : E & \longrightarrow & E \\ (x, y) & \longmapsto & (\frac{e}{x}, -\frac{e}{x^2}y) \end{array}$$

Then $\mathbb{P}^1(s)$ is the quotient of E/ζ_2.

$$s := y + (-\frac{e}{x^2}y)$$

Then

$$\mathbb{P}^1(s) : s^2 = (t^2 - 4e)(t - (\alpha + \frac{e}{\alpha})(t - (\alpha^q + \frac{e}{\alpha^q}))$$

Next, we construct explicitly the (2,2) covering $\mathbb{P}^1(u)/\mathbb{P}^1(t)$, then find the definition equation of C.

Define

$$\gamma := \begin{cases} \alpha^2 & \text{for case 1} \\ \alpha + \frac{e}{\alpha} & \text{for case 2} \end{cases}$$

$$\Phi := \begin{pmatrix} \gamma & b \\ 1 & -\gamma \end{pmatrix}$$

Denote the determinant of Φ as $D = \det \Phi$, then

$$b \quad = \quad D - \gamma^2$$

Denote the map induced by Φ as $\phi : \mathbb{P}^1(u) \longrightarrow \mathbb{P}^1(u)$, the $(2,2)$ covering has the covering group:

$$\begin{array}{rcl} \Gamma & := & cov\left(\mathbb{P}^1(u)/\mathbb{P}^1(t)\right) \\ & = & \{1, \phi, {}^\sigma \phi, {}^{\sigma^2} \phi\} \\ {}^\sigma\phi \cdot \phi & = & \phi \cdot {}^\sigma\phi = {}^{\sigma^2}\phi \end{array}$$

Thus we can shown that $\mathbb{P}^1(s) = \mathbb{P}^1(u)/ < {}^\sigma\phi >$ and further $\mathbb{P}^1(t) = \mathbb{P}^1(u)/\Gamma$.

We can shown that

$$D \quad = \quad (\gamma - \gamma^q)\left(\gamma - \gamma^{q^2}\right)$$

Then

$$\begin{array}{rcl} t & = & u + \phi(u) + {}^\sigma\phi(u) + {}^{\sigma^2}\phi(u) \\ & := & \dfrac{F(u)}{N_{k_3/k}(n - \gamma)} \\ F(u) & = & t^4 - 2Tr(\gamma^{q+1})t^2 + 8N(\gamma)u - 2Tr(\gamma)N(\gamma) + Tr(\gamma^{2q+2}) \end{array}$$

Then define

$$X := u, \qquad Y := N_{k_3/k}(X-\gamma)x$$

Then the definition equation of C is

$$C: \quad Y^2 = F(X)N(X-\gamma)$$

in the first case.

The definition equation of C in the second case is

$$C: \quad Y^2 - F(X)Y + eN_{k_3/k}(X-\gamma)^2 = 0$$

The ramification points of C in the second case is the zeros of the discrminant

$$\mathrm{disc} = F(X)^2 - 4eN(X-\gamma)$$

The action of $PGL_2(k)$ on $\mathbb{P}^1(x)$ induces the action on the sets $\{\alpha, \beta\}$ in (6) and $\{\alpha\}$ in (59), and this action gives elliptic curves of the same type which are k_3-isomorphic to the original curves. $\square$

3 Type I curves

3.1 Legendre form over k_3 of Type I curves

Lemma 5. *The Type I elliptice curve E can be transformed by a k_3-isomorphism to*

$$E \underset{/k_3}{\simeq} \quad y^2 = x(x-1)(x-\lambda) \tag{15}$$

$$\lambda = \tfrac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)(\beta^q-\alpha^q)} \tag{16}$$

Proof:

$$t \quad := \quad Ax = \begin{pmatrix} 1 & -\alpha^q \\ 1 & -\alpha \end{pmatrix} x = \frac{x-\alpha^q}{x-\alpha}$$

$$\begin{aligned} A^{-1} &= \frac{1}{-\alpha+\alpha^q}\begin{pmatrix} -\alpha & \alpha^q \\ -1 & 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} \alpha & -\alpha^q \\ 1 & -1 \end{pmatrix} \bmod k^\times \end{aligned}$$

$$x \quad = \quad \begin{pmatrix} 1 & -\alpha^q \\ 1 & -\alpha \end{pmatrix}^{-1} \cdot t = \begin{pmatrix} \alpha & -\alpha^q \\ 1 & -1 \end{pmatrix} \cdot t = \frac{\alpha t - \alpha^q}{t-1}$$

$$\begin{aligned}
x-\alpha &= \frac{\alpha-\alpha^q}{t-1} \\
x-\alpha^q &= \frac{\alpha-\alpha^q}{t-1}t \\
x-\beta &= \frac{\alpha-\beta}{t-1}\left(t-\frac{\beta-\alpha^q}{\beta-\alpha}\right) \\
x-\beta^q &= \frac{\alpha-\beta^q}{t-1}\left(t-\frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right)
\end{aligned}$$

$$\left((t-1)^2y\right)^2=(\alpha-\alpha^q)^2(\alpha-\beta)(\alpha-\beta^q)\,t\left(t-\frac{\beta-\alpha^q}{\beta-\alpha}\right)\left(t-\frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right) \quad (17)$$

Now define

$$u := \frac{\beta^q-\alpha^q}{\beta^q-\alpha}\,t$$

Then (17) becomes

$$\left((t-1)^2y\right)^2=(\alpha-\alpha^q)^2(\alpha-\beta)(\alpha-\beta^q)\left(\frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right)^3u(u-1)\left(u-\frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}\right)$$

$$\left((t-1)^2y\right)^2=\frac{(\alpha-\alpha^q)^2(\beta-\alpha)(\beta^q-\alpha^q)^3}{(\beta^q-\alpha)^2}u(u-1)\left(u-\frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}\right)$$

Now define

$$\begin{aligned}
e &= \frac{(\alpha-\alpha^q)^2(\beta-\alpha)(\beta^q-\alpha^q)^3}{(\beta^q-\alpha)^2} \\
&= \frac{(\alpha-\alpha^q)^2(\beta^q-\alpha^q)^2}{(\beta^q-\alpha)^2}(\beta-\alpha)^{1+q} \\
&\equiv 1 \bmod (k_3^*)^2 \\
\lambda &= \frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}
\end{aligned}$$

□

3.2 Characteristics of Type I curves

According to the above lemma and transitivity of the action of $PGL_2(k)$ on $k_3\setminus k$, we can assume that $\exists A\in GL_2(k), \exists\epsilon\in k_3\setminus k, s.t. \alpha=A\epsilon$, thus the first element in the pair $\{\alpha,\beta\}$ can be fixed to an $\epsilon\in k_3\setminus k$. Thus, we hereafter consider only the pairs $\{\epsilon,\beta\}$ and the corresponding values of $\{\lambda\}$.

The action of $PGL_2(k)$ on $k_3 \setminus k$ induces the following action on the set $\{\alpha, \beta\}$.

$$\{\alpha, \beta\} \quad \longrightarrow \quad \{A\alpha, A\beta\}, \qquad \forall A \in GL_2(k)$$

This action transforms E (6) into a new elliptic curve

$$E' : y^2 \quad = \quad (x - A\alpha)\,(x - A\alpha^q)\,(x - A\beta)\,(x - A\beta^q) \tag{18}$$

which also has a Legendre canonical form as (15) with

$$\lambda' \quad := \quad \frac{(A\beta - A\alpha^q)(A\beta^q - A\alpha)}{(A\beta - A\alpha)(A\beta^q - A\alpha^q)} \tag{19}$$

Then it is easy to see

$$\lambda = \lambda'$$

or the Legrandre forms are invariant under this action.

Therefore, by transitivity of the action of $PGL_2(k)$ on $k_3 \setminus k$, the first element in the pair $\{\alpha, \beta\}$ can be fixed to an $\epsilon \in k_3 \setminus k$. Thus, we hereafter consider only the pairs $\{\epsilon, \beta\}$ and the corresponding values of $\{\lambda\}$.

From now we assume the Type I curves to be

$$E: \quad y^2 = (x - \epsilon)\,(x - \epsilon^q)\,(x - \beta)\,(x - \beta^q) \tag{20}$$

$$\epsilon, \beta \in k_3 \setminus k, \quad \#\{\epsilon, \epsilon^q, \beta, \beta^q\} = 4 \tag{21}$$

$$\lambda = \tfrac{\beta - \epsilon^q}{\beta - \epsilon} \cdot \tfrac{\beta^q - \epsilon}{\beta^q - \epsilon^q} \tag{22}$$

Now we define

$$\mu := \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \lambda \tag{23}$$

then since $\lambda \neq 0, 1, \infty$, $\mu \neq \epsilon, \epsilon^q, \infty$.

Define

$$A =: \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix} \tag{24}$$

and

$$B := {}^{\sigma^2}\!A \; {}^{\sigma}\!A \; A. \tag{25}$$

Then we have

Lemma 6.

1. *Given an λ, there exists a β s.t. (22) holds iff*

$$A\beta = \beta^q \tag{26}$$

2. *The above condition is equivalent to*

$$B\beta = \beta. \tag{27}$$

Then one can easily find β from λ as solutions of the quadratic equation obtained from (27), hence find elliptic curves which have the covering C.

3. *When such a β exists,*

$$B \quad \not\equiv \quad \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \bmod k_3^\times \tag{28}$$

since $\mu \neq \epsilon, \epsilon^q$.

Thus, the quadratic equation in 2. does not degenerated to a linear equation, or there are always two β's given one λ.

4. *Let the discriminant*

$$D \quad := \quad (TrB)^2 - 4(\det B) \quad (\in k) \tag{29}$$

$$D \quad = \quad N(\varepsilon - \varepsilon^q)^2 N\left(\frac{1}{\lambda - 1}\right)^2 \{[Tr(\lambda) - 1]^2 - 4N(\lambda)\} \tag{30}$$

then there exist such β given an λ if and only if $D \in (k)^2$;

5.

$$D = 0 \Longrightarrow \left.\begin{array}{l} \exists C \in GL_2(k), \quad C^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} k^\times) \\ \beta = C\epsilon \end{array}\right\} \tag{31}$$

The number of β when $D = 0$ is q^2.

Remark 1. *Thus, given a random elliptic curve E in the Legendre form, one can easily test if it is of Type I by solving a quadratic equation defined by (27).*

Proof of Lemma6. 1:

From (22)

$$\lambda = \frac{\beta - \epsilon^q}{\beta - \epsilon} \cdot \frac{\beta^q - \epsilon}{\beta^q - \epsilon^q}$$

$$0 \quad = \quad (1-\lambda)\beta^{1+q} + (\lambda\epsilon - \epsilon^q)\beta^q + (\lambda\epsilon^q - \epsilon)\beta + (1-\lambda)\epsilon^{1+q}$$

Since $\lambda \neq 0, 1, \infty$

$$0 \quad = \quad \beta^{1+q} - \frac{\lambda\epsilon - \epsilon^q}{\lambda - 1}\beta^q - \frac{\lambda\epsilon^q - \epsilon}{\lambda - 1}\beta + \epsilon^{1+q}$$

Define

$$\mu \quad := \quad \begin{pmatrix} \epsilon & -\epsilon^q \\ 1 & -1 \end{pmatrix} \lambda \tag{32}$$

$$\nu \quad := \quad \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \lambda \tag{33}$$

Then

$$\begin{aligned}
0 &= \beta^{1+q} - \mu\beta^q - \nu\beta + \epsilon^{1+q} \\
&= \beta^q(\beta - \mu) - \nu\beta + \epsilon^{1+q} \\
\beta^q &= \frac{\nu\beta - \epsilon^{1+q}}{\beta - \mu} \\
&= \begin{pmatrix} \nu & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix} \beta
\end{aligned}$$

On the other hand, from the defintions of μ, ν

$$\begin{aligned}
\nu &= \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -\epsilon^q \\ 1 & -\epsilon \end{pmatrix} \mu \\
&= -\mu + \epsilon + \epsilon^q
\end{aligned}$$

Therefore, if one defines

$$A := \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix}$$

then a β exists for a given λ iff

$$\beta^q = A \cdot \beta$$

Proof of Lemma 6, 2:
(27)$\Longleftarrow$ (26): Easy.
(27)$\Longrightarrow$ (26):
Assume the two solutions of (27) are $\{\beta, \gamma\}$

$$B\beta = \beta, \qquad B\gamma = \gamma \tag{34}$$

Since

$$\begin{aligned}
{}^{\sigma^2}A\ {}^{\sigma}A\ A\beta &= \beta \\
A\ {}^{\sigma^2}A\ {}^{\sigma}A\beta^q &= \beta^q \\
{}^{\sigma^2}A\ {}^{\sigma}A\beta^q &= A^{-1}\beta^q \\
{}^{\sigma^2}A\ {}^{\sigma}A\ A(A^{-1}\beta^q) &= A^{-1}\beta^q \\
B(A^{-1}\beta^q) &= A^{-1}\beta^q
\end{aligned}$$

Therefore, either

$$A^{-1}\beta^q = \beta \qquad i.e. \qquad A\beta = \beta^q \tag{35}$$

or

$$A^{-1}\beta^q = \gamma \qquad i.e. \qquad A\gamma = \beta^q. \tag{36}$$

The latter case is when the action of A exchanges two solutions. i.e.

$$A\gamma = \beta^q, \qquad A\beta = \gamma^q \tag{37}$$

Then

$$^{\sigma}A\ A\beta =^{\sigma} A\ \gamma^q = (A\gamma)^q = \beta^{q^2} \tag{38}$$
$$^{\sigma^2}A\ ^{\sigma}A\ A\beta =^{\sigma^2} A\ \beta^{q^2} = (A\beta)^{q^2} = \gamma \tag{39}$$

This means

$$B\beta = \gamma \qquad i.e. \qquad \beta = \gamma \tag{40}$$

Proof of Lemma 6.3: (See Appendix 1)

Proof of Lemma 6.4, 5

Let

$$B := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad c \neq 0$$

then β are solutions of

$$cx^2 + (d-a)x - b = 0$$

Hence, there exist at most two β.

Let

$$D := (TrB)^2 - 4(\det B) \quad (\in k)$$

Then

$$\#\{\beta\} = 2 \quad \Longleftrightarrow \quad D \in (k^{\times})^2 \tag{41}$$
$$\#\{\beta\} = 1 \quad \Longleftrightarrow \quad D = 0 \tag{42}$$
$$\#\{\beta\} = 0 \quad \Longleftrightarrow \quad D \notin (k^{\times})^2 \tag{43}$$

Now consider the case when $D = 0$.

Define the matrix mapping β to ϵ as $C \in GL_2(k)$, which is unique modulo $k^{\times}$. Denote the image of ϵ under C as γ, i.e.:

$$\exists!\ C \in PGL_2(k), \quad s.t. \quad C\beta = \epsilon, \quad C\epsilon =: \gamma \tag{44}$$

Then

$$C\beta^q = (C\beta)^q = \epsilon^q \tag{45}$$
$$C\epsilon^q = (C\epsilon)^q = \gamma^q \tag{46}$$

Thus under the action of C, one obtains another elliptic curve isomorphic to E

$$E'' : y^2 = (x-\epsilon)(x-\epsilon^q)(x-\gamma)(x-\gamma^q) \tag{47}$$

i.e. with the same λ.

When $D = 0$, there is only one β is possible so one has $\gamma = \beta$.

Thus

$$\begin{aligned} C\beta &= \epsilon, \qquad C\epsilon = \beta & (48) \\ C^2\beta &= \beta & (49) \end{aligned}$$

Since $\beta \in k_3 \setminus k$

$$C^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} k^\times) \tag{50}$$

but $\not\equiv I$ mod $k^\times$, thus $Tr(C) = 0$.

Denote

$$C = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

When $c = 0$, one can assume $a = 1$, the number of $\beta = C\epsilon = -\epsilon - b$ is $\#\{b \in k\} = q$.

When $c \neq 0$, the number of

$$\beta = C\epsilon = \frac{a\epsilon + b}{\epsilon - a} \tag{51}$$

is $\#\{(a, b) \in k^2 | a^2 + b \neq 0\} = q(q - 1)$.

Thus the number of β when $D = 0$ is q^2.

The calculation of D can be found in Appendix 2. In fact, λ such that C is hyperelliptic can be caluculated

4 Classification of $\mathbf{PGL}_2(k)$ action on Type I curves

For Type I curves,

$$E \underset{/k_3}{\simeq} \quad y^2 = x(x-1)(x-\lambda) \tag{52}$$

$$\lambda \quad = \quad \lambda(\alpha, \beta) = \frac{\beta^q - \alpha}{\beta^q - \alpha^q} \frac{\beta - \alpha^q}{\beta - \alpha}, \qquad \beta \in k_3 \setminus k, \beta \neq \alpha, \alpha^q, \alpha^{q^2} \tag{53}$$

Since the action of $\mathrm{PGL}_2(k)$ on k_3 is transitive and fixed-point free, one can fixed $\alpha = \varepsilon \in k_3 \setminus k$, then

$$\lambda = \lambda(\varepsilon, \beta) = \frac{(\beta^q - \varepsilon)(\beta - \varepsilon^q)}{(\beta - \varepsilon)^{q+1}} \qquad \beta \in k_3 \setminus k, \beta \neq \varepsilon, \varepsilon^q, \varepsilon^{q^2}$$

First, λ is $\mathrm{PGL}_2(k)$-invariant:

$$\forall A \in PGL_2(k), \qquad \lambda(A\alpha, A\beta) = \lambda(\alpha, \beta) \tag{54}$$

We now defne a double-side action on $A \in GL_2(k)$ as follows.

$$PGL_2(k) \curvearrowright GL_2(k) \curvearrowleft PGL_2(k)$$

In particular the double action is defined as follows.

$$T \cdot \beta := TAT^{-1}T\varepsilon, T \in GL_2(k)$$

The A under the above action has three representatives:

1. $$A_1 = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \qquad a \neq 0, 1$$

2. $$A_2 = \begin{pmatrix} a & e \\ 1 & a \end{pmatrix}, \qquad \eta^2 = e \in k^\times \setminus (k^\times)^2$$

3. $$A_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

5 Density of Type I curves with hyperelliptic coverings

First, We consider the matrix Θ in Lemma 4 under double-side $\mathrm{PGL}_2(k)$-actions. In fact, Θ can be represented by the following matrices under the double-side $\mathrm{PGL}_2(k)$-action.

$$\begin{array}{lll} (i) \quad \Theta_1 & = & \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \\ (ii) \quad \Theta_2 & = & \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix} \qquad \exists \eta \in k_2, \eta^2 = e \in k^\times \setminus \left(k^\times\right)^2 \end{array}$$

Since

$$\lambda = \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{1+q}} \neq 0, 1, \qquad \beta \in k_3 \setminus k, \quad \beta \neq \alpha, \alpha^q, \alpha^{q^2}$$

one has β_1 and β_2 corresponding to the two representitives of Θ_1 and Θ_2.

$$\beta_1 = \Theta_1 \cdot \alpha = -\alpha \tag{55}$$

$$\lambda_1 = \frac{(\alpha + \alpha^q)^2}{4\alpha^{1+q}} \tag{56}$$

$$\beta_2 = \Theta_2 \cdot \alpha = \frac{e}{\alpha} \tag{57}$$

$$\lambda_2 = \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}} \tag{58}$$

Lemma 7. *The covering curve C/k of a Type I C_0 is hyperelliptic iff*

$$D := disc(B) = 0$$

Proof:

By Lemma 6.5 for Type I curves and Lemma 4 one knows that $D = 0$ implies C/k is a hyperellptic cover.

Now we proof the other direction. According to Lemma 8, we know that the λ is either λ_1 in (170) or λ_2 in (172).

Substitute the λ_i into the equation (168) in Appendix 2, one finds that $D(\lambda_i) = 0, i = 1, 2$.

$\square$

Lemma 8. *Denote the λ in the Legendre form of the Type I curves, then*

$$\#\{\lambda \mid C/\mathbb{P}^1 : hyper\} = q^2$$

($\because$): According Lemma 7, a λ defines C_0 such that C/k is hyperellptic if and only if $D = 0$.

On the other hand, Lemma 6.4 said the correspondence between β and λ is 1-1 in the hyperellipic case, and Lemma 6.5 told us the number of β such that $D = 0$ is q^2. Thus we know that this is also the number of λs define hyperelliptic C. $\square$

6 Density of Type I curves with non-hyperelliptic coverings

First $\beta \in k_3 \setminus k$, $\beta \neq \alpha, \alpha^q, \alpha^{q^2}$

$$\#\beta = q^3 - q - 3$$

There is a symmetry between ε and β

$$\lambda(\varepsilon, \beta) = \lambda(\beta, \varepsilon)$$

But when C is nonhyperelliptic, the correspondence between β and λ is 2:1. When C is hyperellptic Lemma 8, $D = 0$ then β and λ is 1-1. The number of such λ is q^2.

Thus

$$\nu := \#\{\lambda \ s.t. \ C \ \text{ is non-hyper }\}$$

$$\#\beta = 2\nu + q^2 = q^3 - q - 3$$

$$\nu = \#\lambda = \frac{1}{2}(\#\beta - q^2) = \frac{1}{2}(q^3 - q^2 - q - 3)$$

7 Type II curves

7.1 Legendre form over k_3 of Type II curves

Lemma 9. *For the Type II elliptice curve E/k_3*

$$E/k_3: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right)$$
$$\alpha \in k_6 \setminus \{k_2 \cup k_3\}$$

there is a k_6-isomorphism φ_0/k_6

$$\varphi_0: \; E/k_3 \underset{/k_6}{\simeq} E_0/k_3 \qquad\qquad y^2 = \epsilon x(x-1)(x-\mu) \tag{59}$$

$$\begin{cases} \mu = \left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right)^{1+q^3} = N_{k_6/k_3}\left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right) \\ \epsilon \equiv N_{k_6/k_3}\left(\alpha-\alpha^{q^4}\right) \bmod \left(k_6^\times\right)^2 \\ \quad \equiv 1 \bmod \left(k_6^\times\right)^2 \end{cases} \tag{60}$$

Furthermore, The Type II elliptice curve E/k_3 can be transformed by a k_6-isomorphism φ_1 to

$$\varphi_1: \; E/k_3 \underset{/k_6}{\simeq} E_1/k_3: \quad y^2 \;=\; x(x-1)(x-\mu) \tag{61}$$

Proof: Let

$$A := \begin{pmatrix} 1 & -\alpha^{q^3} \\ 1 & -\alpha \end{pmatrix}$$

and

$$t := Ax = \frac{x-\alpha^{q^3}}{x-\alpha}$$

therefore

$$x = \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} t = \frac{\alpha t - \alpha^{q^3}}{t-1}$$

The factor in the equation of the Type II curve E

$$\begin{aligned} x-\alpha &= \frac{\alpha-\alpha^{q^3}}{t-1} \\ x-\alpha^{q^3} &= \frac{\alpha-\alpha^{q^3}}{t-1}t \\ x-\alpha^q &= \frac{\alpha-\alpha^q}{t-1}\left(t-\frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\right) \\ x-\alpha^{q^4} &= \frac{\alpha-\alpha^{q^4}}{t-1}\left(t-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right) \end{aligned}$$

$$y^2 = \frac{(\alpha-\alpha^{q^3})^2(\alpha-\alpha^q)(\alpha-\alpha^{q^4})}{(t-1)^4}\, t\left(t-\frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\right)\left(t-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right)$$

Let

$$t := \frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\, u \tag{62}$$

$$\begin{aligned}
\left((t-1)^2 y\right)^2 &= \frac{(\alpha-\alpha^{q^3})^2(\alpha-\alpha^{q^4})\left(\alpha^{q^3}-\alpha^q\right)^3}{(\alpha-\alpha^q)^2} u\,(u-1)\,(u-\mu) \\
\mu &:= \frac{(\alpha-\alpha^q)}{(\beta-\alpha^q)}\frac{(\beta-\beta^q)}{(\alpha-\beta^q)} \\
&= N_{k_6/k_3}\left(\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right) \in k_3
\end{aligned}$$

$$\epsilon \;:\equiv\; N_{k_6/k_3}(\alpha-\alpha^{q^4}) \bmod \left(k_6^\times\right)^2$$

□

Lemma 10.

$$E \overset{/k_3}{\simeq} E_0 \overset{/k_3}{\simeq} E_2$$

$$\begin{aligned}
E_0/k_3: \quad y^2 &= N_{k_6/k_3}(\alpha-\beta^q)x(x-1)(x-\mu) && (63)\\
E_2/k_3: \quad y^2 &= (\alpha-\beta)^{q+1}x(x-1)(x-\lambda) && (64)\\
\lambda &:= \frac{1}{1-\mu} = \frac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)^{q+1}}, \qquad \beta=\alpha^{q^3} && (65)
\end{aligned}$$

$$\textit{where} \qquad \begin{cases} (\alpha-\beta)^{q+1}\in(k_3^\times)^2 & \textit{when } q\not\equiv 1 \bmod 4 \\ (\alpha-\beta)^{q+1}\notin(k_3^\times)^2 & \textit{when } q\equiv 1 \bmod 4 \end{cases}$$

Proof:

We prove that E_0 is isomorphic to E_2 as follows.

$$x := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\cdot s = 1-\frac{1}{s}$$

$$\begin{aligned}
y^2 &= N_{k_6/k_3}(\alpha-\beta^q)x(x-1)(x-\mu) \\
&= (\alpha-\beta)^{q+1}\frac{1}{s^4}s\,(s-1)\left(s-\frac{1}{(1-\mu)}\right)
\end{aligned}$$

Here we used

$$\mu = \frac{(\alpha^q-\alpha)(\beta^q-\beta)}{(\alpha^q-\beta)(\beta^q-\alpha)} \qquad \mu-1 = \frac{(\alpha-\beta)^{q+1}}{(\alpha^q-\beta)(\beta^q-\alpha)}$$

Now define

$$t := s^2 y$$

$$E_0 \simeq E_2 : t^2 = (\alpha - \beta)^{q+1} s\,(s-1)\left(s - \frac{1}{(1-\mu)}\right)$$

Since $(\alpha - \beta)^{q+1} \in k_3^\times$

$$\begin{aligned} e^{\frac{q^3-1}{2}} &= \left((\alpha-\beta)^{q+1}\right)^{\frac{q^3-1}{2}} && (66)\\ &= (-1)^{\frac{q+1}{2}} && (67)\\ &= \begin{cases} +1 & \iff \quad q \equiv 3 \bmod 4 \\ -1 & \iff \quad q \equiv 1 \bmod 4 \end{cases} && (68) \end{aligned}$$

We know that $e \in (k_3^\times)^2$ if and only if $q \equiv 3 \bmod 4$.

□

7.2 k_3-isomorphism of Type II curves

We consider further the k_3-isomorphisms of Type II curves.

Now let

$$\begin{aligned} v &:= \frac{(t-1)^2}{\sqrt{e}} y && (69)\\ &= \frac{(t-1)^2\,(\alpha - \alpha^q)}{(\alpha - \alpha^{q^3})\left(\alpha^{q^3} - \alpha^q\right)(\alpha - \alpha^{q^4})^{\frac{1+q^3}{2}}} y && (70) \end{aligned}$$

$$E_1/k_3 : \qquad v^2 = u(u-1)(u-\lambda) \qquad (71)$$

Let φ_1 be the k_6-isomorphism of E to E_1

$$E/k_3 \xrightarrow{\phi_1/k_6} E_1/k_3 = {}^{\sigma_3}E_1 \qquad (72)$$

We wish to show E is k_3-isomorphic to E_1. In order to do that, consider

$$\psi :={}^{\sigma_3}\varphi_1 \circ \varphi_1^{-1} \;\; /k_6 : \quad E_1 \xrightarrow{\simeq} E_1$$

$$\begin{tikzcd} & E \arrow[dl, "\varphi_1"'] \arrow[dr, "{}^{\sigma_3}\varphi_1"] & \\ E_1 \arrow[rr, "\psi = {}^{\sigma_3}\varphi_1 \circ \varphi_1^{-1}"'] & & {}^{\sigma_3}E_1 \end{tikzcd}$$

.

7.2.1 $\psi^*(\omega) = -\varepsilon(\omega), \varepsilon = \pm 1$

We first consider the k_6/k_3 conjugate ${}^{\sigma^3}E_1$ of E_1, i.e. by $\sigma_3 = (\cdot)^{q^3}$ action

The variable change

$$u \longmapsto t = \frac{\alpha^{q^3} - \alpha^q}{\alpha - \alpha^q}\ u \longmapsto x = At = \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} \frac{\alpha^{q^3} - \alpha^q}{\alpha - \alpha^q}\ u \tag{73}$$

has the Galois conjugate as below

$$u' \longmapsto^{\sigma_3} t = \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u \longmapsto x =^{\sigma_3} A\ \ {}^{\sigma_3}t = \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix} \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u' \tag{74}$$

Thus from (73) and (74)

$$x = \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix} \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u' \tag{75}$$

$$\begin{aligned} \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u' &= \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} \frac{\alpha^{q^3} - \alpha^q}{\alpha - \alpha^q}\ u && (76) \\ &= \frac{\alpha - \alpha^q}{\left(\alpha^{q^3} - \alpha^q\right) u} && (77) \end{aligned}$$

$$u' = \frac{\alpha^{q^3} - \alpha^{q^4}}{\alpha - \alpha^{q^4}} \frac{\alpha - \alpha^q}{\alpha^{q^3} - \alpha^q} \frac{1}{u} = \frac{\lambda}{u}. \tag{78}$$

The conjugate of E_1 is

$$\begin{aligned} {}^{\sigma_3}E_1 : \quad (v')^2 &= u'(u'-1)(u'-\lambda) && (79) \\ &= \frac{\lambda^2}{u^4}\ u\,(u-1)\,(u-\lambda) && (80) \end{aligned}$$

$$\left(\frac{u^2}{\lambda} v'\right)^2 = u\,(u-1)\,(u-\lambda) \tag{81}$$

Comparing with E_1, we have

$$\frac{u^2}{\lambda} v' = \pm v \tag{82}$$

$$v' = \pm \frac{\lambda}{u^2} v = \varepsilon \frac{\lambda}{u^2} v \tag{83}$$

$$\varepsilon := \pm 1, \tag{84}$$

Consider the differential form on E_1

$$\omega = \frac{du}{v} \tag{85}$$

Then

$$\begin{aligned}
\psi : E_1 &\longrightarrow {}^{\sigma_3}E_1 && (86)\\
\psi^*(\omega) &= \omega' && (87)\\
&= -\frac{\frac{\lambda}{u^2}}{\varepsilon\frac{\lambda}{u^2}v}du && (88)\\
&= -\varepsilon\omega = \pm\omega && (89)
\end{aligned}$$

7.2.2 Exact value of ε

Recall that a rational map f over a field K from a group variety G with the group unit e to an abelian variety A is a homomorphism upto a translation. i.e., there is a homomorphism $f_0 : G \longrightarrow A$ over k such that $f(P) = f_0(P) + f(e)$. Then

$$\begin{aligned}
f^* &= f_0^*\\
f^* = f_0^* = 1 &\Longrightarrow f_0 = 1 \quad or \quad f(P) = P + Q, \quad Q = f(e)
\end{aligned}$$

Now one has

$$\begin{aligned}
\psi : E_1 &\xrightarrow{\simeq} {}^{\sigma_3}E_1\\
P &\longmapsto \pm P + Q, \qquad (Q = \psi(\mathcal{O}) \in E_1(k_3)\\
\omega &\longmapsto \psi^*(\omega) = -\varepsilon\omega
\end{aligned}$$

In order to find the exact expression of ε, we define

$$\begin{aligned}
y_1 &:= (t-1)^2 y && (90)\\
v &= \frac{(t-1)^2}{\sqrt{e}}y = \frac{1}{\sqrt{e}}y_1 && (91)
\end{aligned}$$

by the definition of v. Here

$$\frac{1}{\sqrt{e}} = \frac{(\alpha-\alpha^q)}{\left(\alpha-\alpha^{q^3}\right)\left(\alpha^{q^3}-\alpha^q\right)\left(\alpha-\alpha^{q^4}\right)^{\frac{1+q^3}{2}}} \qquad (92)$$

Recall (62)

$$t-1 = \frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\left(u - \frac{\alpha-\alpha^p}{\alpha^{q^3}-\alpha^q}\right) \qquad (93)$$

$$\frac{(t-1)^2}{\sqrt{e}} = \frac{\left(\alpha^{q^3}-\alpha^q\right)\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}{(\alpha-\alpha^q)(\alpha-\alpha^{q^3})(\alpha-\alpha^{q^4})^{\frac{1+q^3}{2}}}$$

By (91)

$$y \quad = \quad \frac{\sqrt{e}v}{(t-1)^2} = \frac{(\alpha-\alpha^q)(\alpha-\alpha^{q^3})(\alpha-\alpha^{q^4})^{\frac{1+q^3}{2}}}{(\alpha^{q^3}-\alpha^q)\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}\, v \tag{94}$$

Meanwhile

$$y \quad = \quad {}^{\sigma_3}y \tag{95}$$

$$= \quad \frac{(\alpha^{q^3}-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}{(\alpha-\alpha^{q^4})\left(u'-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right)^2}\, v' \tag{96}$$

The factor in the denominator of (96) can be calculated using $u' = \lambda/u$.

$$\begin{aligned} u' - \frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}} &= \lambda/u - \frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}} \\ &= -\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\left(1-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\,\frac{1}{u}\right) \end{aligned}$$

Substitute this equation into (96), one obtains

$$y \quad = \quad \frac{(\alpha-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}{(\alpha^{q^3}-\alpha^{q^4})}\;\frac{u^2}{\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}\, v' \tag{97}$$

Thus,

$$v' \quad = \quad \frac{(\alpha^{q^3}-\alpha^{q^4})}{(\alpha-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}\;\frac{\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}{u^2}\, y \tag{98}$$

Now substitute y (94) into the above eq.

$$\begin{aligned} v' &= -\frac{(\alpha-\alpha^q)(\alpha^{q^3}-\alpha^{q^4})}{(\alpha^{q^3}-\alpha^q)^{\frac{3+q^3}{2}}}(\alpha-\alpha^{q^4})^{\frac{q^3-1}{2}}\;\frac{v}{u^2} \\ &:= \varepsilon_1 \frac{v}{u^2} \end{aligned}$$

The exact value of ε_1 can be evaluated as follows.

$$\varepsilon_1 \quad = \quad -\lambda\left(\frac{\alpha-\alpha^{q^4}}{\alpha^{q^3}-\alpha^q}\right)^{\frac{q^3+1}{2}}$$

Therefore

$$
\begin{aligned}
v' &= \varepsilon_1 \frac{v}{u^2} \\
&= -\left(\frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^q}\right)^{\frac{q^3+1}{2}} \frac{\lambda v}{u^2} \\
&= \varepsilon \frac{\lambda v}{u^2}
\end{aligned}
$$

by the definition $v' = \varepsilon \lambda v / u^2$.

Thus

$$
\begin{aligned}
\varepsilon &= -\left(\frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^q}\right)^{\frac{q^3+1}{2}} \\
&= -\left(\alpha - \alpha^{q^4}\right)^{\frac{q^6-1}{2}} \\
&= \pm 1
\end{aligned}
$$

here since $N_{k_3/k}(\cdot) = (\cdot)^{q^2+q+1}$. $N_{k_6/k}(\cdot) = (\cdot)^{q^5+\ldots+q+1}$.

7.2.3 When $\varepsilon = 1, \psi^* = -1$

We know already that E is k_6-isomorphic to

$$E_1/k_3 : \quad y^2 = x(x-1)(x-\lambda),$$

$$
\begin{aligned}
\psi^*(\omega) &= -\varepsilon\omega \\
\varepsilon &= N_{k_6/k_3}(\alpha^{q^4} - \alpha)^{(q^3-1)/2} = \pm 1
\end{aligned}
$$

$\psi = \varphi_1^\sigma \varphi_1^{-1}$ sends a point P to $-\varepsilon P + Q$, where Q is the point $(0,0)$ of E_1.

First we treat the case when $\varepsilon = 1, \psi^* = -1$. Denote the k_6/k_3-twist E_1' of E_1 as :

$$
\begin{aligned}
E_1' : \ y^2 &= \kappa x(x-1)(x-\lambda) \\
\kappa \in k_3^\times, \qquad \kappa^{\frac{q^3-1}{2}} &= -1
\end{aligned}
$$

Define the k_6/k_3-twisting map

$$
\begin{aligned}
\tau : E_1 &\xrightarrow{\simeq} E_1' \\
(x,y) &\longmapsto (x, \sqrt{\kappa} y) \\
\tau^*(\omega) &= \tau^*\left(\frac{dx}{y}\right) = \frac{dx}{\sqrt{\kappa} y} = \frac{1}{\sqrt{\kappa}}\omega
\end{aligned}
$$

Moreover,

$$\begin{aligned} {}^{\sigma^3}\tau \circ \tau^{-1}(x,y) &= {}^{\sigma^3}\tau\left(x, \frac{y}{\sqrt{\kappa}}\right) \\ &= \left(x, \kappa^{\frac{q^3-1}{2}} y\right) = (x,-y) \end{aligned}$$

or

$$\left({}^{\sigma^3}\tau \circ \tau^{-1}(x,y)\right)^* = -1$$

Then

$$\begin{aligned} \psi' : E_1' &\longrightarrow E_1' \\ \psi' &= {}^{\sigma_3}\tau \circ \psi \circ \tau^{-1} \\ (\psi')^* &= ({}^{\sigma_3}\tau)^* \circ \psi^* \circ \tau^{-*} \\ &= -({}^{\sigma_3}\tau)^* \circ \tau^{-*} = (-1)^2 = -1 \end{aligned}$$

Thus when $\varepsilon = 1, \psi^* = -1$, we can always use the E_1' and ψ' instead of E_1 and ψ so that $(\psi')^* = 1$.

Therefore, we will discuss only for the case $\varepsilon = -1$ and ψ^*.

7.2.4 Construction k_3-isomorphism ρ/k_3: $E \longrightarrow E_1$

Assume $\varepsilon = -1$.

$$\begin{aligned} \psi(P) &= P + Q \\ {}^{\sigma^3}\varphi_1 \circ \varphi_1^{-1}(P) &= P + Q \end{aligned}$$

Let

$$\begin{aligned} R &:= \varphi_1^{-1}(P) \\ P &= \varphi_1(R) \end{aligned}$$

i.e.

$$ {}^{\sigma^3}\varphi_1(R) = \varphi_1(R) + Q$$

Lemma 11. *For $Q \in E_1(k_3)$,*

$$\exists S \in E_1(\overline{k}) \qquad s.t. \qquad S - {}^{\sigma^3}S = Q$$

Proof: Due to the following short exact sequence.

$$0 \longrightarrow E_1(k_3) \longrightarrow E_1(\overline{k}) \xrightarrow{\sigma^3 - 1} E_1(\overline{k}) \longrightarrow 0$$

or the surjectivity of $\sigma^3 - 1$ and the fact that $E_1(\overline{k})$ is a divisible group.

($\square$)

Remark 2. *In fact, such an S is not unique but up to a traslation by $E_1(k_3)$*

$$\begin{aligned} S_1 &:= S+T \qquad \forall T \in E_1(k_3) \\ {}^{\sigma^3}S_1 &= S_1 - Q \end{aligned}$$

Indeed

$$\begin{aligned} {}^{\sigma^3}S_1 &= {}^{\sigma^3}S +^{\sigma^3} T = S - Q + T \\ &= S_1 - Q \end{aligned}$$

Lemma 12. *Define*

$$\rho : E \xrightarrow{\sim} E_1 \tag{99}$$

$$P \longmapsto \rho(P) := \varphi_1(P) + S \tag{100}$$

Then ρ is an isomorphism of E to E_1 defined over k_3.

Proof:

$$\begin{aligned} {}^{\sigma^3}\rho(P) &= {}^{\sigma^3}\varphi_1(P) +^{\sigma^3} S \\ &= \varphi_1(P) + (Q +^{\sigma^3} S) \\ &= \varphi_1(P) + S \\ &= \rho(P) \end{aligned}$$

$${}^{\sigma^3}\rho(P) = \rho(P) \Longrightarrow \rho/k_3$$

($\square$)

8 Density of Type II curves

We first notice that the action

$$PGL_2(k_2) \curvearrowright k_6/k_2 \tag{101}$$

is also transitive and fixed-point free. The proof is to replace k with k_2 in the proof for $PGL_2(k) \curvearrowright k_3 \setminus k$.

Then for any $\alpha \in k_6 \setminus k_2$, one can find $\varepsilon \in k_3 \setminus k$ and $V \in PGL_2(k_2)$ such that α is the image of ε under the action of V:

$$\begin{aligned} &\exists \varepsilon \in k_3 \setminus k \qquad \exists V \in GL_2(k_2) \setminus k_2^\times GL_2(k) \\ &s.t. \qquad \alpha = V \cdot \varepsilon \\ &\qquad\qquad \beta = {}^{\sigma}V \cdot \varepsilon \end{aligned}$$

We know that $\lambda(\alpha)$ is invariant under the left-action of $\mathrm{PGL}_2(k)$.

$$\forall U \in GL_2(k), \qquad U \cdot \alpha = UV \cdot \varepsilon \in k_6 \setminus k_2$$

$$\lambda(UV \cdot \varepsilon) = \lambda(V \cdot \varepsilon)$$

Now we consider also the action on the other side or the right-action on V:

$$\begin{aligned} \forall W &\in GL_2(k), \qquad \exists \varepsilon' \in k_3 \setminus k \\ s.t. \qquad \varepsilon &= W\varepsilon' \end{aligned}$$

and since

$$\lambda(V \cdot \varepsilon) = \lambda(VW \cdot \varepsilon')$$

λ is also invariant under this action.

To analyze the number of isomorphic classes of E by calculation of $\#\lambda$ in the Legendre form, we consider the double-side actions and the double cosets

$$k_2^\times GL_2(k) \Big\backslash \; GL_2(k_2) \; \Big/ k_2^\times GL_2(k) \tag{102}$$

$$\lambda(V \cdot \varepsilon) = \lambda(UVW \cdot \varepsilon')$$

Lemma 13. *The V under the double-side-action can be classified into the following three cases*

Assume $r, s, t \in k, e = \eta^2 \in k^\times \setminus (k^\times)^2$.

$$(i) \qquad V_1 = \begin{pmatrix} r+\eta & 0 \\ 0 & 1 \end{pmatrix} \tag{103}$$

$$(ii) \qquad V_2 = \begin{pmatrix} s+t\eta & e \\ 1 & s+t\eta \end{pmatrix}, \qquad t \neq 0, \quad (s,t) \neq (0, \pm 1) \tag{104}$$

$$(iii) \qquad V_3 = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \tag{105}$$

Proof:

Assume $\exists \eta \in k_2, \eta^2 = e \in k^\times \setminus (k^\times)^2$, then

$$\forall V \in GL_2(k_2) \setminus GL_2(k), \qquad V = V' + \eta V'', \qquad V', V'' \in M_2(k)$$

First we assume V' is a regular matrix.

Then one can assume that under the double-side-action, V' can be transformed to the identity matrix while the ε' is changed inside $k_2 \setminus k$.

$$V = I_2 + \eta V'' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \eta V'', \qquad V'' \in M_2(k)$$

Under the double-side action of $GL_2(k)$, V'' can be transformed into the following three forms:

$$(i) \qquad V_1'' = \begin{pmatrix} r & 0 \\ 0 & s \end{pmatrix}, r \neq s, r, s \in k \tag{106}$$

$$(ii) \qquad V_2'' = \begin{pmatrix} 0 & re \\ r & 0 \end{pmatrix} = r \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix}, \qquad r \in k^\times \tag{107}$$

$$(iii) \qquad V_3'' = \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}, \qquad r \in k^\times \tag{108}$$

Then V becomes the following three forms under the double-side action:

$$(i) \qquad V_1 = \begin{pmatrix} 1+r\eta & 0 \\ 0 & 1+s\eta \end{pmatrix}, r \neq s, r, s \in k \tag{109}$$

$$(ii) \qquad V_2 = \begin{pmatrix} 1 & re\eta \\ r\eta & 1 \end{pmatrix} = I_2 + r\eta \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix}, \qquad r \in k^\times \tag{110}$$

$$(iii) \qquad V_3 = \begin{pmatrix} 1 & r\eta \\ 0 & 1 \end{pmatrix}, \qquad r \in k^\times \tag{111}$$

Now the V_1 can be transformed into the form of V_1 in the Lemma as follows:

Indeed, assume $\frac{1+r\eta}{1+s\eta} = \frac{(1+r\eta)(1-s\eta)}{1-s^2e} = a + b\eta, a, b \in k$, one can use the following two actions: $\frac{1}{1+s\eta} \in k_2^\times$ and $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(k)$, then

$$\frac{1}{1+s\eta} \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+r\eta & 0 \\ 0 & 1+s\eta \end{pmatrix} = \begin{pmatrix} 1+r_1\eta & 0 \\ 0 & 1 \end{pmatrix}.$$

The V_2 can be transformed into the form in the Lemma by scaling $\frac{1}{r\eta} = s + t\eta \in k_2^\times$.

Here if $t = 0$ then $V_2 \in GL_2(k)$ which is previously excluded.

Besides, when V_2 is a singular matrix, $\det V_2 = (s+t\eta)^2 - e = s^2 + 2st\eta + (t^2-1)e = 0, s^2 + (t^2-1)e = 0, st = 0$, since we have excluded $t = 0$, then $s = 0, t^2 = 1$ is the singular condition.

Therefore, $t = 0, (s, t) = (0, \pm 1)$ is excluded.

The V_3 can be transformed by the following double-side $GL_2(k)$ action into the form in the Lemma as follows

$$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & r\eta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{r} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & \eta \\ 0 & \frac{1}{r} \end{pmatrix} = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}.$$

Next, we consider the case when V' is singular. (Of course $V' \neq O_2$ otherwise, $V \in GL_2(k) \bmod k_2^\times$).

Then under the double-side $GL_2(k)$ action, one can assume

$$V' = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}, \qquad * \in k^\times$$

but since $* \equiv 1 \bmod k_2^\times$.

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \eta V''$$

Now, if V'' is regular, then one can change this case into the former case with V' being regular by the following left $GL_2(k)$ action $\bmod k_2^\times$, (notice $1/\eta = \eta/e$

$$\frac{1}{\eta}(V'')^{-1}V = I_2 + \eta V''', \qquad V''' := \frac{1}{e}(V'')^{-1}V'$$

Thus this case can be reduced to the V' regular cases.

Now assume that V'' is singular,

$$V'' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \det V'' = ad - bc = 0,$$

Here we consider two cases: either $b \neq 0$ or $b = 0$.

In the first case $b \neq 0$, V'' can be transformed by a right $GL_2(k)$ action which preserves the form of $V' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

$$V'' \begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}$$

and

$$V' \begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}$$

Thus, we can assume that

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \eta \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & b\eta \\ 0 & d\eta \end{pmatrix}$$

Below we show that this case can be reduced to the case (i) among the V' regular cases.

Indeed, since $V \in GL_2(k_2), d \neq 0$, dividing V by $d\eta$,

$$\frac{1}{d\eta} V = \frac{1}{d\eta} \begin{pmatrix} 1 & b\eta \\ 0 & d\eta \end{pmatrix} = \begin{pmatrix} l\eta & h \\ 0 & 1 \end{pmatrix} \quad \mod k_2^\times$$

Now another left $GL_2(k)$ action

$$\begin{pmatrix} 1 & -h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} l\eta & h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} l\eta & 0 \\ 0 & 1 \end{pmatrix}$$

but this becomes a special case of V' regular (i) if one multiplies $1 + \eta$ to it:

$$(1+\eta)V = (1+\eta) \begin{pmatrix} l\eta & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} le + l\eta & 0 \\ 0 & 1+\eta \end{pmatrix} = \begin{pmatrix} le & 0 \\ 0 & 1 \end{pmatrix} + \eta \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$$

thus the V'' singular with $b \neq 0$ case is included in the case V' regular (i).

In the rest case $b = 0$, let $d \neq 0$, then $a = 0$

$$V = \begin{pmatrix} 1 & 0 \\ c\eta & d\eta \end{pmatrix}$$

which a transpotation of the $b \neq 0$ case.

If $d = 0$ in the case $b = 0$, then

$$V = \begin{pmatrix} 1 + a\eta & 0 \\ c\eta & 0 \end{pmatrix} \notin GL_2(k_2)$$

which should be excluded. $\square$

Lemma 14. *Elliptic curves of Type II can be classified according to classification of V under the double-side-action in the Lemma 13, each with the representive λ as follows:*

$$\begin{aligned}
(i) \qquad \lambda_1 &= \frac{r^2-e}{4e}\,\frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}} && (112)\\
(ii) \qquad \lambda_2 &= \frac{N_{k_2/k}((s+t\eta)^2-e)}{4et^2}\,\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{q+1}} && (113)\\
&= \frac{N_{k_2/k}(\det V_2)}{4et^2}\,\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{q+1}} && (114)\\
(iii) \qquad \lambda_3 &= \frac{1}{4e}(\varepsilon-\varepsilon^q)^2 && (115)
\end{aligned}$$

Proof:
(i)

$$\alpha_1 = V_1\cdot\varepsilon = (r+\eta)\varepsilon \qquad \in k_6\setminus(k_2\cup k_3)$$

Then

$$\beta_1 = \alpha_1^{q^3} = (r-\eta)\varepsilon$$

since $\varepsilon\in k_3\setminus k$, then $\varepsilon^{q^3}=\varepsilon$, and since $\eta^{2q}=e^q=e$ then $\eta^q=-\eta$.

$$\begin{aligned}
\beta_1-\alpha_1 &= -2\eta\varepsilon\\
(\beta_1-\alpha_1)^{1+q} &= 4e\varepsilon^{1+q}\\
\beta_1-\alpha_1^q &= (r-\eta)(\varepsilon-\varepsilon^q)\\
\beta_1^q-\alpha_1 &= -(r+\eta)(\varepsilon-\varepsilon^q)\\
(\beta_1-\alpha_1^q)(\beta_1^q-\alpha_1) &= -(r^2-e)(\varepsilon-\varepsilon^q)
\end{aligned}$$

$$\lambda_1 = -\frac{(r^2-e)}{4e}\frac{(\varepsilon-\varepsilon^q)}{\varepsilon^{1+q}}$$

(ii)

$$\begin{aligned}
\alpha_2 &= V_2\cdot\varepsilon\\
&= \frac{(s+t\eta)\varepsilon+e}{\varepsilon+s+t\eta}
\end{aligned}$$

Then

$$\beta_2 = \frac{(s-t\eta)\varepsilon+e}{\varepsilon+s-t\eta}$$

$$\begin{aligned}
\beta_2-\alpha_2 &= \frac{(s-t\eta)\varepsilon+e}{\varepsilon+s-t\eta}-\frac{(s+t\eta)\varepsilon+e}{\varepsilon+s+t\eta}\\
&= -\frac{2t\eta(\varepsilon^2-e)}{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)}
\end{aligned}$$

$$(\beta_2-\alpha_2)^{1+q} = \frac{4et^2(\varepsilon^2-e)^{1+q}}{\{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)\}^{1+q}}$$

$$\begin{aligned} & \beta_2-\alpha_2^q \\ = \quad & \frac{((s-t\eta)\varepsilon+e)(\varepsilon^q+s-t\eta)-((s-t\eta)\varepsilon^q+e)(\varepsilon+s-t\eta)}{(\varepsilon+s-t\eta)(\varepsilon^q+s-t\eta)} \\ = \quad & \frac{((s-t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)(\varepsilon^q+s-t\eta)} = \frac{((s-t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)^q} \end{aligned}$$

$$\begin{aligned} & \beta_2^q-\alpha_2 \\ = \quad & \frac{((s+t\eta)\varepsilon^q+e)(\varepsilon+s+t\eta)-((s+t\eta)\varepsilon+e)(\varepsilon^q+s+t\eta)}{(\varepsilon^q+s+t\eta)(\varepsilon+s+t\eta)} \\ = \quad & -\frac{((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon^q+s+t\eta)(\varepsilon+s+t\eta)} = -\frac{((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)^q(\varepsilon+s+t\eta)} \end{aligned}$$

$$(\beta_2-\alpha_2^q)(\beta_2^q-\alpha_2) = -\frac{((s-t\eta)^2-e)((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)^2}{\{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)\}^{1+q}}$$

$$\begin{aligned} \lambda_2 &= \frac{((s-t\eta)^2-e)((s+t\eta)^2-e)}{4et^2}\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}} \\ &= \frac{N_{k_2/k}(((s+t\eta)^2-e)}{4et^2}\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}} \end{aligned}$$

(iii)

$$\begin{aligned} \alpha_3 &= V_3\cdot\varepsilon \\ &= \varepsilon+\eta \end{aligned}$$

Then

$$\begin{aligned} \beta_3 &= \alpha_3^{q^3} \\ &= \varepsilon-\eta \end{aligned}$$

$$\begin{aligned} \beta_3-\alpha_3 &= -2\eta \\ (\beta_3-\alpha_3)^{1+q} &= -4e \\ \beta_3-\alpha_3^q &= \varepsilon-\varepsilon^q \\ \beta_3^q-\alpha_3 &= -(\varepsilon-\varepsilon^q) \\ (\beta_3-\alpha_3^q)(\beta_3^q-\alpha_3) &= -(\varepsilon-\varepsilon^q)^2 \end{aligned}$$

$$\lambda_3 = \frac{1}{4e}(\varepsilon - \varepsilon^q)^2$$

□

Lemma 15. *The three cases in the Lemma 13 are pairwisely disjoint.*

Proof: We will show the orbits of $A \in GL_2(k)$ under the double-side-action are disjoint in the following three steps.
(i) and (ii) have no overlap.

Assume the orbits of the case (i) and (ii) have an intersection s.t.

$$\exists A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k) \tag{116}$$

$$\mu := A \cdot \varepsilon = \frac{a\varepsilon + b}{c\varepsilon + d} \tag{117}$$

$$s.t. \quad \lambda_1(\mu) = \lambda_2(\varepsilon) \tag{118}$$

Then, notice the k-coefficients in (112) and (114) are constants independent of ε, one has the following equation upto $k^\times$-scaling.

$$\frac{(\mu - \mu^q)^2}{\mu^{1+q}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{1+q}} \bmod k^\times \tag{119}$$

$$\begin{aligned} \mu - \mu^q &= \frac{(a\varepsilon + b)(c\varepsilon^q + d) - (a\varepsilon^q + b)(c\varepsilon + d)}{(c\varepsilon + d)(c\varepsilon^q + d)} \\ &= \frac{(ad - bc)(\varepsilon - \varepsilon^q)}{(c\varepsilon + d)^{1+q}} \end{aligned} \tag{120}$$

Therefore

$$\begin{aligned} LHS(119) &= \frac{(\mu - \mu^q)^2}{\mu^{1+q}} \\ &= \frac{(ad - bc)^2(\varepsilon - \varepsilon^q)^2}{\{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q}} \end{aligned}$$

Thus from (119)

$$\frac{(ad - bc)^2(\varepsilon - \varepsilon^q)^2}{\{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{1+q}} \bmod k^\times$$

one has

$$\{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q} \equiv (\varepsilon^2 - e)^{1+q} \bmod k^\times$$

Notice that if one has

$$A^{1+q} \equiv B^{1+q} \bmod k^\times \rightsquigarrow \left(\frac{A}{B}\right)^{1+q} \equiv 1 \bmod k^\times$$

but

$$\left(\frac{A}{B}\right)^{q^2-1} \equiv 1, \left(\frac{A}{B}\right)^{q^3-1} \equiv 1,$$

then $A/B \in k^\times$ since $(q^2-1, q^3-1) = q-1$.

$$(c\varepsilon + d)(a\varepsilon + b) = l(\varepsilon^2 - e), \qquad \exists l \in k^\times$$

This means

$$\begin{aligned} ac &= l(\neq 0) \\ ad + bc &= 0 \\ bd &= -le(\neq 0) \end{aligned}$$

which implies

$$c \neq 0$$

Now we normalize A with $c = 1$, then

$$a = l, b = -ad = -ld, bd = -ld^2 = -le$$

thus

$$d^2 = e$$

But since $e \in k^\times \setminus (k^\times)^2$, no such d exists. Thus the presumed intersection does not exists.

(i) and (iii) have empty overlap

Now assume the orbits of (1) and (3) have an intersection

From

$$\lambda_1(\mu) \quad = \quad \lambda_3(\varepsilon) \tag{121}$$

and (112), (115), one has the following equation upto $k^\times$-scaling.

$$\frac{(\mu - \mu^q)^2}{\mu^{1+q}} \quad \equiv \quad (\varepsilon - \varepsilon^q)^2 \bmod k^\times \tag{122}$$

From (121),

$$\frac{(\varepsilon - \varepsilon^q)^2}{\{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q}} \quad \equiv \quad (\varepsilon - \varepsilon^q)^2 \bmod k^\times$$

Then

$$\begin{aligned} \{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q} &\equiv 1 \bmod k^\times \\ (c\varepsilon + d)(a\varepsilon + b) &= l, \quad \exists l \in k^\times \end{aligned}$$

This means

$$\begin{aligned} ac &= 0 \\ ad + bc &= 0 \\ bd &= l \quad (\neq 0) \end{aligned}$$

We divide the conditions into two subcases: when $c = 0$ and when $c \neq 0$.

When $c = 0$, normalize A such that $d = 1$, then $a = 0$,

$$A = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix} \notin GL_2(k)$$

When $c \neq 0$, we can normalize A such that $c = 1$. Then $a = b = 0$

$$A = \begin{pmatrix} 0 & 0 \\ 1 & d \end{pmatrix} \notin GL_2(k)$$

which is against assumption on A, thus the presumed intersection does not exists.

(ii) and (iii) have empty overlap

Assume the orbit of (iii) and (ii) have an intersection such that

$$\lambda_3(\mu) = \lambda_2(\varepsilon)$$

From (115) and (114), one has the following equation upto $k^\times$-scaling.

$$(\mu - \mu^q)^2 \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{1+q}} \bmod k^\times \tag{123}$$

From (120)

$$\frac{(\varepsilon - \varepsilon^q)^2}{(c\varepsilon + d)^{2+2q}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{1+q}} \bmod k^\times$$

Then

$$\begin{aligned} (c\varepsilon + d)^{2+2q} &\equiv (\varepsilon^2 - e)^{1+q} \\ (c\varepsilon + d)^2 &= l(\varepsilon^2 - e) \qquad \exists l \in k^\times \end{aligned}$$

Therefore

$$\begin{aligned} c^2 &= l \quad (\neq 0) \\ 2cd &= 0 \\ d^2 &= -le \quad (\neq 0) \end{aligned}$$

Thus

$$d = 0, \qquad 0 = -le$$

which is impossible since $l, e \in k^\times$. Thus the presumed intersection does not exists. □

Lemma 16. *The densities of the Type II curves in each case of the Lemma 13 are as follows.*

$$(i) \qquad \#\{\lambda_1\}\Big/\sim \;=\; \frac{1}{4}q(q+1)^2 \tag{124}$$

$$(ii) \qquad \#\{\lambda_2\}\Big/\sim \;=\; \frac{1}{4}q(q-1)^2 \tag{125}$$

$$(iii) \qquad \#\{\lambda_3\}\Big/\sim \;=\; \frac{1}{2}(q^2-1) \tag{126}$$

which sum up to

$$\frac{1}{4}q(q+1)^2 + \frac{1}{4}q(q-1)^2 + \frac{1}{2}(q^2-1) = \frac{1}{2}(q^3+q^2+q-1)$$

Proof:
(i) The λ_1 in the case (i) is a product of two factors f_1, f_2: by (114)

$$\lambda_1 = f_1 f_2, \qquad f_1 := \frac{r^2-e}{4e} \quad f_2 = \frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}}$$

We will count the two factors separately.
First look at the factor f_2 containing ε.
We wish to count the orbits under the action of $GL_2(k)$.

$$\begin{aligned} A &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k) \\ \mu &:= A\cdot\varepsilon \\ s.t. \qquad f_2(\mu) &\equiv f_2(\varepsilon) \bmod k^\times \end{aligned}$$

or

$$\frac{(\mu-\mu^q)^2}{\mu^{q+1}} \equiv \frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}} \mod k^\times$$

We wish to count the number of such μ or the curves among the same isomorphic class of $C(\lambda(\varepsilon))$. From

$$\frac{(ad-bc)^2(\varepsilon-\varepsilon^q)^2}{\{(a\varepsilon+b)(c\varepsilon+d)\}^{q+1}} \equiv \frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}} \mod k^\times$$

one has

$$(a\varepsilon+b)(c\varepsilon+d) = l\varepsilon, \qquad \exists l \in k^\times$$

$$\begin{aligned} ac &= 0 \\ ad+bc &= l \quad (\neq 0) \\ bd &= 0 \end{aligned}$$

When $c = 0$, normalize A so that $d = 1$, then

$$a = l \neq 0, \quad b = 0, \qquad A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

Thus

$$\#\{A\} = \#\{a\} = \#k^\times = q - 1$$

When $c \neq 0$, one can normalize A so that $c = 1$, then

$$a = 0, \ b = l \neq 0, \ d = 0 \qquad A = \begin{pmatrix} 0 & l \\ 1 & 0 \end{pmatrix}$$

$$\#A = \#l = \#k^\times = q - 1$$

$$\#\{A\} = 2(q-1), \#\{f_2\} = \{f_2 \bmod k^\times\} = \frac{q^3 - q}{2(q-1)} = \frac{1}{2}q(q+1)$$

Now we count the factor $f_1 = \frac{r^2-e}{4e}$ in λ (112).

$$\#\{f_1\} = \#\left\{\frac{r^2 - e}{4e}, \quad r \in k\right\} = \#k^2 = \#(k^*)^2 + \#\{0\} = \frac{q-1}{2} + 1 = \frac{q+1}{2}$$

Thus

$$\#\{\lambda\} = \#\{f_1\}\#\{f_2\} = \frac{1}{2}q(q+1) \times \frac{q+1}{2} = \frac{1}{4}q(q+1)^2$$

(ii) The λ_2 in the case (ii) is a product of two factors g_1, g_2:

$$\lambda_2 = g_1 g_2, \qquad g_1 := \frac{N_{k_2/k}(\det V)}{4et^2} \qquad g_2 = \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2)^{q+1}} \tag{127}$$

We will count the two factors separately.

First look at the factor g_2 containing ε.

We wish to count the orbits of g_2 under the action of $GL_2(k)$.

$$\begin{aligned} A &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k) \\ \mu &:= A \cdot \varepsilon \\ s.t. \qquad g_2(\mu) &\equiv g_2(\varepsilon) \bmod k^\times \end{aligned}$$

then

$$\frac{(\mu - \mu^q)^2}{(\mu^2 - e)^{q+1}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{q+1}} \quad \bmod k^\times \tag{128}$$

We wish to count the number of such μ or the curves among the same isomorphic class of $C(\lambda(\varepsilon))$. By (121)

$$\begin{aligned} (\mu - \mu^q)^2 &= \frac{(ad - bc)^2(\varepsilon - \varepsilon^q)^2}{(c\varepsilon + d)^{2q+2}} \\ \mu^2 - e &= \frac{(a\varepsilon + b)^2 - e(c\varepsilon + d)^2}{(c\varepsilon + d)^2} \end{aligned}$$

Then (128) becomes

$$\frac{(\varepsilon-\varepsilon^q)^2}{\{(a\varepsilon+b)^2-e(c\varepsilon+d)^2\}^{q+1}} \equiv \frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{q+1}} \quad \bmod k^\times$$

Thus, $(a\varepsilon+b)^2-e(c\varepsilon+d)^2\}^{q+1} \equiv (\varepsilon^2-e)^{q+1} \bmod k^\times$

$$(a\varepsilon+b)^2-e(c\varepsilon+d)^2 = l(\varepsilon^2-e), \quad \exists l \in k^\times$$

Now one has

$$\begin{aligned} a^2-ec^2 &= l \\ 2(ab-ecd) &= 0 \\ b^2-ed^2 &= -el. \end{aligned}$$

When $c=0$,

$$\begin{aligned} a^2 &= l \quad (\neq 0) \\ ab &= 0, \quad b=0 \\ d^2 = l, &\qquad d = \pm a \end{aligned}$$

i.e.

$$A = a\begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

i.e. there are two such $A \bmod k^\times$ in this case.

When $c \neq 0$ one can normalize A such that $c=1$, then

$$\begin{aligned} && a^2-e &= l, \\ && ab = ed, &\qquad d = \frac{ab}{e} \\ b^2-ed^2 = -el, && b^2 - e(\frac{ab}{e})^2 &= -e(a^2-e) \\ && \frac{b^2}{e}(e-a^2) &= e(e-a^2) \\ b^2 = e^2, && b = \pm e, &\qquad d = \frac{b}{e}a = \pm a \end{aligned}$$

i.e.

$$A = \begin{pmatrix} a & \pm e \\ 1 & \pm a \end{pmatrix}$$

N.B. $e \notin (k^\times)^2$ thus $\det A \neq 0$.

The number of such A is

$$2\#\{a \in k\} = 2q$$

Thus, we add the above two cases

$$\#\{A \bmod k^\times\} = \#(c=0) + \#(c=1) = 2q+2$$

The number of orbits of g_2 under the $\mathrm{GL}_2(k)$ action becomes

$$\#\{g_2 \bmod k^\times\} = \frac{\#\{\varepsilon\}}{\#\{A \bmod k^\times\}} = \frac{q^3-q}{2(q+1)} = \frac{q(q-1)}{2}$$

Now we count the number of $g_1 = \frac{N_{k_2/k}((s+t\eta)^2-e)}{4et^2}$. Denote

$$\rho := \frac{N_{k_2/k}((s+t\eta)^2-e)}{t^2} \tag{129}$$

$$= \frac{1}{t^2}((s^2+e(t^2-1))^2 - 4es^2t^2) \tag{130}$$

Notice here $t \neq 0, (s,t) \neq (0, \pm 1)$ iff $\rho \neq 0, \infty$.

To count $\#\{\rho\}$, notice there is a ρ iff the following plane curve has nontrivial k-rational points $\{(s^2, t^2)\}$:

$$(s^2+e(t^2-1))^2 - 4es^2t^2 = \rho t^2$$

Redefine $X := s^2, Y := t^2$ then we have a conic curve

$$C_1 : (X + e(Y-1))^2 - 4eXY = \rho Y \tag{131}$$

which has $(X,Y) = (e,0)$ as a k-rational point.

Now we draw a straight line through $(e,0)$

$$X = e + hY$$

whose intersection with the above conic C_1 is determined by

$$(h-e)^2Y^2 = (4e^2+\rho)Y.$$

When $h = e$, i.e. $\rho = -4e^2 + \rho$:

Then the strightline becomes

$$X = e(1+Y)$$

Since $X = s^2, Y = t^2$, one has a conic

$$C_2 : \ s^2 - et^2 = e \tag{132}$$

which is non-singular, since

$$(\partial_s, \partial_t) = (2s, -2et) = (0,0), \iff (s,t) = (0,0) \notin C_2(\bar{k}).$$

Besides, its equation is in the form of $N_{k_2/k}(s+\eta t) = e$, from the surjectivity of norm map, it has k_2-rational points.

Therefore its rational points $C_1(k)$ is isomorphic to $\mathbb{P}^1(k) \neq \emptyset$.

Thus there is one value of $\rho = -4e^2$ to be counted.

When $h \neq e$ i.e. $\rho \neq -4e^2$:

Assume $h \neq e$ then one has a linear equation in Y.

$$(h-e)^2 Y = 4e^2 + \rho \tag{133}$$

Thus for any ρ there is a k-rational point (X, Y) on the above curve C_1.

$$Y = \frac{4e^2+\rho}{(h-e)^2} \qquad \neq 0 \tag{134}$$

$$X = \frac{e(h-e)^2 + h(4e^2+\rho)}{(h-e)^2} \tag{135}$$

Define

$$f := (h-e)t$$

one has

$$f^2 = 4e^2 + \rho \qquad \exists f \in k \tag{136}$$

Since $\rho \neq 0$, $f \neq \pm 2e$. Thus the correspondence between f and ρ is 2-1 when $f \neq 0, \pm 2e$.

So we will consider when $f \neq 0, \pm 2e$ the existance of (s, t).

Let

$$v := (h-e)s \tag{137}$$

From (135), one obtain a new conic curve in v, h with f fixed.

$$C_3 : v^2 = e(h-e)^2 + f^2 h \tag{138}$$

We are to count the number of such C_3 with non-empty k_2-rational points. In order to do that, we show that the curve is a nonsingular conic.

Indeed, assume

$$\partial_v = 2v = 0, \partial_h = 2e(h-e) + f^2 = 0 \qquad (h \neq e)$$

gives

$$0 = e(h-e)^2 + f^2 h, \quad 2e(h-e) + f^2 = 0, 2eh(h-e) + f^2 h = 0,$$

thus

$$2eh(h-e) = -f^2 h = e(h-e)^2, \quad 2h = h-e, h = -e,$$

but since $f^2 = -2e(h-e) = 4e^2, f = \pm 2e$ which is excluded already. Thus the affine curve is nonsingular.

Now consider its projective version,

$$\frac{v^2}{w^2} = e(\frac{h}{w} - e)^2 + f^2\frac{h}{w}$$

$$v^2 = e(h - ew) + f^2 w$$

Assume again

$$\partial_v = 2v = 0, \partial_h = 2e(h - ew) + f^2 w = 0, \partial_w = -2e^2(h - ew) + f^2 h = 0$$

Then one has to check only the point at infinity. $w = 0$

$$eh = 0, -2e^2 h + f^2 h = 0, \rightsquigarrow v = h = w = 0$$

which is absurd. Thus C_3 is a nonsingular projective conic.

Besides, it have a rational point $(v, h) = (0, -e(h - e)^2/f^2)$. Thus $C_2(k) \simeq \mathbb{P}^1(k)$.

Thus,

$$\#\{\rho \neq -4e^2, 0\} = \frac{\#\{f \neq 0, \pm 2e\}}{2} = \frac{q-3}{2} \tag{139}$$

$$\#\{g_1\} = \#\{\rho\} = \frac{\#\{f \neq 0, \pm 2e\}}{2} + \#\{f = 0\} = \frac{q-3}{2} + 1 = \frac{q-1}{2} \tag{140}$$

$$\#\{\lambda_2\} = \#\{g_1\} \times \#\{g_2\} = \frac{q-1}{2} \times \frac{q(q-1)}{2} = \frac{q(q-1)^2}{2} \tag{141}$$

(iii)

We now count the number of λ_3 under $\mathrm{GL}_2(k)$ action.

$$\lambda_3(\varepsilon) = \frac{(\varepsilon - \varepsilon^q)^2}{4e}$$

Assume

$$\mu := A \cdot \varepsilon \quad s.t. \quad \lambda_3(\mu) = \lambda_3(\varepsilon)$$

i.e.

$$\begin{aligned}
(\mu - \mu^q)^2 &= (\varepsilon - \varepsilon^q)^2 \\
\mu - \mu^q &= \pm(\varepsilon - \varepsilon^q) \\
\mu \pm \varepsilon &= \mu^q \pm \varepsilon^q = (\mu \pm \varepsilon)^q \\
(\mu \pm \varepsilon)^{q-1} &= 1, \mu \pm \varepsilon =: l \in k \\
\mu &= \pm\varepsilon + l \qquad \exists l \in k
\end{aligned}$$

Thus the number of A s.t. $\lambda_3(\mu) = \lambda_3(\varepsilon)$ is

$$2\#\{l\} = 2\#k = 2q$$

The number of orbits of λ_3 is

$$\frac{q^3 - q}{2q} = \frac{q^2 - 1}{2}$$

Now we add the case in (i), (ii), and (iii) to obtain the total number of Type II curves.

$$\#\{\lambda\} = \frac{q(q+1)^2}{4} + \frac{q(q-1)^2}{4} + \frac{q^2-1}{2} = \frac{q^3+q^2+q-1}{2} \tag{142}$$

□

9 Density of Type II curves with hyperellptic coverings

Lemma 17. *The Type II curve C_0 has a hyperelliptic covering C/k iff $\exists V \in GL_2(k_2), \Theta \in GL_2(k)$ such that $\Theta =^{\sigma} VV^{-1}$, $Tr(\Theta) = 0$, $\beta = \Theta \cdot \alpha$.*

Proof: Assume $\varepsilon \in k_3 \setminus k, \exists! V \in G_2(k_2), s.t. \alpha = V \cdot \varepsilon \in k_6$, since,

$$\beta = \alpha^{q^3} = (V \cdot \varepsilon)^{q^3} =^{\sigma} V \cdot \varepsilon =^{\sigma} VV^{-1} \cdot \alpha$$

Define $\Theta =^{\sigma} VV^{-1}$. If $\mathrm{Tr}(\Theta) = 0$, then C/k is hyperelliptic and vice verse.

□

Lemma 18. *The number of hyperelliptic covering curves among the Type II curves in the three cases are*

$$\begin{array}{rrcl} (i) & \#\{\textit{hyperelliptic covers}\} & = & \frac{1}{2}q(q+1), \\ (ii) & \#\{\textit{hyperelliptic covers }\} & = & \frac{1}{2}q(q-1) \\ (iii) & \#\{\textit{hyperelliptic corvers}\} & = & 0 \end{array}$$

Thus the number of the Type II curvces with hyperelliptic coverings is

$$\#\{\textit{ Type II hyperelliptic covers }\} = q^2$$

Proof:

We consider again representitives under the double-side $GL_2(k)$ action in Lemma 13 and count each orbits of Θ with zero trace.

(i)

$$V_1 = \begin{pmatrix} r+\eta & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \Theta_1 &= {}^{\sigma}V_1 V_1^{-1} \sim \begin{pmatrix} r-\eta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & r+\eta \end{pmatrix} \\ &= \begin{pmatrix} r-\eta & 0 \\ 0 & r+\eta \end{pmatrix} \end{aligned}$$

Assume $Tr(\Theta_1) = 2r = 0$, then $r = 0$

$$V_1 = \begin{pmatrix} -\eta & 0 \\ 0 & +\eta \end{pmatrix} \equiv \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix} \mathrm{mod}\ k^{\times}$$

From Lemma 14

$$\lambda_1 = -\frac{1}{4} \frac{(\varepsilon - \varepsilon^q)^2}{\varepsilon^{q+1}}$$

which is the f_2 in (i) Lemma 16, where we

$$\#\lambda_1 = \frac{1}{2} q(q+1)$$

(ii)

$$V_2 = \begin{pmatrix} s+t\eta & e \\ 1 & s+t\eta \end{pmatrix}, \qquad t \neq 0, \quad (s,t) \neq (0, \pm 1)$$

$$\begin{aligned} \Theta_2 &= {}^{\sigma}V_2 V_2^{-1} \\ &\sim \begin{pmatrix} s-t\eta & e \\ 1 & s-t\eta \end{pmatrix} \begin{pmatrix} s+t\eta & -e \\ -1 & s+t\eta \end{pmatrix} \\ &= \begin{pmatrix} s^2 - e(t^2+1) & 2te\eta \\ 2t\eta & s^2 - e(t^2+1) \end{pmatrix} \end{aligned}$$

$$Tr(\Theta_2) = 0, \qquad s^2 = e(t^2+1)$$

The conic $s^2 = e(t^2+1)$ is nonsingular thus its k-rational points bijective to that of $\mathbb{P}^1(k)$. Therefore for

$$\#\lambda_2 = \frac{\{\#\alpha \in k_3 \setminus k\}}{\#V_2} = \frac{q(q^2-1)}{q+1} = \frac{q(q-1)}{2}$$

Or since

$$\lambda_2 = -e \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{q+1}}$$

equals to the factor g_2 in Lemma 16 (ii) which has cardinality $\frac{q(q-1)}{2}$.

(iii)

$$V_3 = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \Theta_3 &= {}^{\sigma}V_3 V_3^{-1} \\ &= \begin{pmatrix} 1 & -2\eta \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Then $Tr(\Theta_3) \neq 0$, or there is no hyperlliptic covering in this case.

□

References

[1] L.Adleman, J.DeMarrais, and M.Huang, “A subexpotential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields,” Algorithmic Number Theory, Springer-Verlag, LNCS 877, pp.28-40, 1994.

[2] S. Arita, K. Matsuo, K. Nagao, M. Shimura ”A Weil descent attack against elliptive curve cryptosystems over quartic extension field I“ Proceedings of SCIS2004, IEICE Japan 2004.

[3] I.F. Black, G.Seroussi and N.Smart, ”Advances in elliptic curve cryptography”, Cambridge University Press 2005.

[4] H. Cohen, G. Frey, “Handbook of elliptic and hyperelliptic curve cryptography”, Chapman & Hall, 2006

[5] J. Chao, “Elliptic and hyperelliptic curves with weak coverings against Weil descent attack,” Talk at the 11th Elliptic Curve Cryptography Workshop, 2007.

[6] C.Diem, “The GHS attack in odd characteristic,” J.Ramanujan Math.Soc, vol.18 no.1, pp.1-32, 2003.

[7] C. Diem, “Index calculus in class groups of plane curves of small degree”, Proceedings of ANTS VII, 2006.

[8] C. Diem, J. Scholten, “Cover attaks, a report for the AREHCC project”, preprint Oct. 2003.

[9] A.Enge and P.Gaudry, “A general framework for subexponential discrete logarithm algorithms,” Acta Arith.,vol.102, pp.83-103, 2002.

[10] G.Frey, “How to disguise an elliptic curve,” Talk at the 2nd Elliptic Curve Cryptology Workshop, 1998.

[11] S.D.Galbraith "Weil descent of Jacobians," Discrete Applied Mathmatics, vol.128 no.1, pp.165-180, 2003.

[12] P.Gaudry, "An Algorithm for solving the discrete logarithm problem on hyperelliptic curves," Advances in cryptology EUROCRYPTO 2000, Springer-Verlag, LNCS 1807, pp.19-34, 2000.

[13] P.Gaudry, N.Theriault, E.Thome, C. Diem " A double large prime variation for small genus hyperelliptic index calculus" Math. Comp. 76 (2007), 475-492.

[14] P.Gaudry, F.Hess, and N.Smart, "Constructive and destructive facets of Weil descent on elliptic curves," J.Cryptol,15, pp.19-46, 2002.

[15] M.Gonda, K.Matsuo, K.Aoki, J.Chao and S.Tsujii, "Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation" , IEICE Transactions on Fundamentals, E88-A(1),pp.89-96, 2005.

[16] Naoki Hashizume and Fumiyuki Momose and Jinhui Chao "On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics" Available from http://eprint.iacr.org/2008/215

[17] F.Hess, "The GHS attack revisited," Advances in cryptology EUROCRYPTO 2003, Springer-Verlag, LNCS 2656, pp.374-387, 2003.

[18] F.Hess, "Generalizing the GHS Attack on the Elliptic Curve Discrete Logarithm," LMS J. Comput. Math. vol.7, pp.167-192, 2004.

[19] T. Iijima, F. Momose, J. Chao "Classification of Weil Restrictions Obtained by $(2, \ldots, 2)$ Coverings of $\mathbb{P}^1$ without Isogeny Condition in Small Genus Cases" Proceedings of SCIS 2009, 2009.

[20] A.Menezes, and M.Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart," Topics in Cryptology CT-RSA 2001, Springer-Verlag, LNCS 2020, pp.308-318, 2001.

[21] F. Momose, J. Chao, M. Shimura "On Weil descent of elliptic curves over quadratic extensions" Proceedings of SCIS2005, pp.787-792, 2005

[22] F. Momose and J. Chao "Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$," preprint, 2006. Available from http://eprint.iacr.org/2006/347

[23] F. Momose and J. Chao "Scholten Forms and Elliptic/Hyperelliptic Curves with Weak Weil Restrictions," preprint, 2005. Available from http://eprint.iacr.org/2005/277

[24] K.Nagao "Improvement of Theriault algorithm of index calculus of Jacobian of hyperelliptic curves of small genus", preprint 2004.

[25] Bejamine Smith ”Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves (Extended version)”. To appear in Journal of Cryptology.

[26] N.Thériault, ”Index calculus attack for hyperelliptic curves of small genus”, Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science, 2894, 75–92, 2003

[27] N.Thériault, “Weil descent attack for Kummer extensions,” J.Ramanujan Math. Soc, vol.18, pp.281-312, 2003.

[28] N.Thériault, “Weil descent attack for Artin-Schreier curves,” preprint, 2003, available at http://www.math.toronto.edu/ganita/papers/wdasc.pdf

10 Appendix 1: Proof of Lemma 2.3: B is not upper-triangle

Since

$$A = \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix}, \qquad B = {}^{\sigma^2}A \ {}^{\sigma}A \ A$$

we have

$$^{\sigma}A \ A \quad = \quad \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & * \\ \nu - \mu^q & * \end{pmatrix}. \tag{143}$$

On the other hand,

$$^{\sigma^2}A \quad = \quad \begin{pmatrix} \nu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\mu^{q^2} \end{pmatrix} \tag{144}$$

$$\widetilde{^{\sigma^2}A} \quad = \quad \frac{-1}{\det {}^{\sigma^2}A} \begin{pmatrix} \mu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\nu^{q^2} \end{pmatrix} \tag{145}$$

$$= \quad \frac{-1}{\det {}^{\sigma^2}A} \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix} \tag{146}$$

Assume B is upper-triangle, then

$$^{\sigma}A \ A \equiv \widetilde{^{\sigma^2}A} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod k_3^{\times} \tag{147}$$

By (143),(146)

$$\begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & * \\ \nu - \mu^q & * \end{pmatrix} \quad \equiv \quad \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod k_3^{\times} \tag{148}$$

$$= \quad \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix} \bmod k_3^{\times} \tag{149}$$

In the above equation of 2×2 matrices, take the ratios of $1,1$-th entries over $1,2$-th entries of both sides, we obtain the following equations:

$$\nu^{1+q} - \varepsilon^{q+q^2} = \mu^{q^2}(\nu - \mu^q) \tag{150}$$

Since this equation constains μ, ν and ε the same time, we will try to represent μ, ν in ε.

Now substitute $\nu = -\mu + \varepsilon + \varepsilon^q$ into the equation (150)

$$\begin{aligned} (-\mu + \varepsilon + \varepsilon^q)\left(-\mu^q + \varepsilon^q + \varepsilon^{q^2}\right) - \varepsilon^{q+q^2} &= \mu^{q^2}\left(-\mu - \mu^q + \varepsilon + \varepsilon^q\right) \\ &= -\mu^{1+q^2} - \mu^{q+q^2} + (\varepsilon + \varepsilon^q)\,\mu^{q^2} \\ \mu^{1+q} - \left(\varepsilon^q + \varepsilon^{q^2}\right)\mu - (\varepsilon + \varepsilon^q)\,\mu^q + \varepsilon^{1+q} + \varepsilon^{1+q^2} + \varepsilon^{2q} & \\ &= -\mu^{1+q^2} - \mu^{q+q^2} + (\varepsilon + \varepsilon^q)\,\mu^{q^2} \end{aligned}$$

Thus, we have

$$Tr_{k_3/k}(\mu^{1+q}) - Tr_{k_3/k}(\left(\varepsilon^q + \varepsilon^{q^2}\right)\mu) + Tr_{k_3/k}(\varepsilon^{1+q}) + \left(\varepsilon^{q^2} - \varepsilon^q\right)\mu^q + \varepsilon^q(\varepsilon^q - \varepsilon^{q^2}) = 0$$

Since $Tr_{k_3/k} \in k$

$$\left(\varepsilon^q - \varepsilon^{q^2}\right)\mu^q - \varepsilon^q(\varepsilon^q - \varepsilon^{q^2}) = \tau \in k$$

$$\mu^q = \varepsilon^q + \frac{\tau}{\left(\varepsilon^q - \varepsilon^{q^2}\right)} \tag{151}$$

$$\mu = \varepsilon + \frac{\tau}{(\varepsilon - \varepsilon^q)} \tag{152}$$

$$\nu = -\mu + \varepsilon + \varepsilon^q = \varepsilon^q - \frac{\tau}{(\varepsilon - \varepsilon^q)} \tag{153}$$

Therefore we can represent μ, ν in terms of $\varepsilon, \tau \in k$

Now substitute (152),(153) into (150),

$$LHS = -\left(\frac{\varepsilon^{q^2}}{(\varepsilon - \varepsilon^q)} + \frac{\varepsilon^q}{(\varepsilon - \varepsilon^q)^q}\right)\tau + \frac{\tau^2}{(\varepsilon - \varepsilon^q)^{1+q}}$$

$$RHS = -\left(\frac{\varepsilon^{q^2}}{(\varepsilon - \varepsilon^q)} + \frac{\varepsilon^{q^2}}{(\varepsilon - \varepsilon^q)^q}\right)\tau - \left(\frac{1}{(\varepsilon - \varepsilon^q)^{1+q^2}} + \frac{1}{(\varepsilon - \varepsilon^q)^{q+q^2}}\right)\tau^2$$

Then (150) becomes

$$\frac{\varepsilon^{q^2} - \varepsilon^q}{(\varepsilon - \varepsilon^q)^q}\tau + Tr_{k_3/k}\left(\frac{1}{(\varepsilon - \varepsilon^q)^{1+q^2}}\right)\tau^2 = 0 \tag{154}$$

Since

$$\begin{aligned}
\frac{\varepsilon^{q^2} - \varepsilon^q}{(\varepsilon - \varepsilon^q)^q} &= \frac{(\varepsilon^q - \varepsilon)^q}{(\varepsilon - \varepsilon^q)^q} = -1 \\
Tr_{k_3/k}\left(\frac{1}{(\varepsilon - \varepsilon^q)^{1+q^2}}\right) &= \frac{1}{(\varepsilon - \varepsilon^q)^{1+q^2}} + \frac{1}{(\varepsilon - \varepsilon^q)^{q+1}} + \frac{1}{(\varepsilon - \varepsilon^q)^{q+q^2}} \\
&= \frac{(\varepsilon - \varepsilon^q)^q + (\varepsilon - \varepsilon^q)^{q^2} + \varepsilon - \varepsilon^q}{N_{k_3/k}(\varepsilon - \varepsilon^q)} \\
&= \frac{\varepsilon^q - \varepsilon^{q^2} + \varepsilon^{q^2} - \varepsilon + \varepsilon - \varepsilon^q}{N_{k_3/k}(\varepsilon - \varepsilon^q)} = 0
\end{aligned}$$

(154) becomes

$$\tau = 0 \Longrightarrow \mu = \varepsilon \tag{155}$$

which is against the assumption that $\mu \neq \varepsilon$.

Thus B is not uppertrianglar. .

11 Appendix 2: Type I, hyperelliptic covering case: Discriminant D

11.1 Notation

$$A = \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix}, \qquad B =^{\sigma^2} A \ \cdot^{\sigma} A \ \cdot A \tag{156}$$

$$\mu = \begin{pmatrix} \varepsilon & -\varepsilon^q \\ 1 & -1 \end{pmatrix} \cdot \lambda, \qquad \lambda \neq 0, 1, \infty \tag{157}$$

$$\nu = \begin{pmatrix} \varepsilon^q & -\varepsilon \\ 1 & -1 \end{pmatrix} \cdot \lambda \tag{158}$$

$$\rho = \frac{1}{\lambda - 1}$$

11.2 B

$$\mu = \varepsilon + \alpha, \qquad \alpha = (\varepsilon - \varepsilon^q)\rho \qquad \nu = \varepsilon^q - \alpha$$

$$\begin{aligned} {}^{\sigma}A \cdot A &= \begin{pmatrix} \nu^q & -\varepsilon^{q+q^2} \\ 1 & -\mu^q \end{pmatrix} \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix} && (159) \\ &= \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu \\ \nu - \mu^q & -\varepsilon^{1+q} + \mu^{1+q} \end{pmatrix} && (160) \end{aligned}$$

$$\begin{aligned} B &= {}^{\sigma^2}A \ \cdot ({}^{\sigma}A \ \cdot A) && (161) \\ &= \begin{pmatrix} \nu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\mu^{q^2} \end{pmatrix} \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu \\ \nu - \mu^q & -\varepsilon^{1+q} + \mu^{1+q} \end{pmatrix} && (162) \\ &=: \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} && (163) \end{aligned}$$

$$\begin{aligned} B_{11} &= N(\nu) - \varepsilon^{q+q^2}\nu^{q^2} - \varepsilon^{1+q^2}(\nu - \mu^q) && (164) \\ B_{22} &= -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu + \varepsilon^{1+q}\mu^{q^2} - N(\mu) && (165) \end{aligned}$$

$$\begin{aligned} N(\nu) &= (\varepsilon^q - \alpha)(\varepsilon^{q^2} - \alpha^q)(\varepsilon - \alpha^{q^2}) \\ &= N(\varepsilon) - \varepsilon^{q+q^2}\alpha^{q^2} - \varepsilon^{1+q}\alpha^q - \varepsilon^{1+q^2}\alpha + \varepsilon^q\alpha^{q+q^2} + \varepsilon^{q^2}\alpha^{1+q^2} + \varepsilon\alpha^{1+q} - N(\alpha) \end{aligned}$$

$$-\varepsilon^{q+q^2}\nu^{q^2} = -\varepsilon^{q+q^2}(\varepsilon - \alpha^{q^2}) = -N(\varepsilon) + \varepsilon^{q+q^2}\alpha^{q^2}$$

$$-\varepsilon^{1+q^2}\nu = -\varepsilon^{1+q^2}(\varepsilon^q - \alpha) = -N(\varepsilon) + \varepsilon^{1+q^2}\alpha$$

$$\varepsilon^{1+q^2}\mu^q = \varepsilon^{1+q^2}(\varepsilon^q + \alpha^q) = N(\varepsilon) + \varepsilon^{1+q^2}\alpha^q$$

$$-\varepsilon^{1+q}\nu^q = -\varepsilon^{1+q}(\varepsilon^{q^2} - \alpha^q) = -N(\varepsilon) + \varepsilon^{1+q}\alpha^q$$

$$\varepsilon^{q+q^2}\mu = \varepsilon^{q+q^2}(\varepsilon + \alpha) = N(\varepsilon) + \varepsilon^{q+q^2}\alpha$$

$$\varepsilon^{1+q}\mu^{q^2} = \varepsilon^{1+q}(\varepsilon^{q^2} + \alpha^{q^2}) = N(\varepsilon) + \varepsilon^{1+q}\alpha^{q^2}$$

$$\begin{aligned} -N(\mu) &= -(\varepsilon + \alpha)(\varepsilon^q + \alpha^q)(\varepsilon^{q^2} + \alpha^{q^2}) \\ &= -N(\varepsilon) - \varepsilon^{1+q}\alpha^{q^2} - \varepsilon^{q+q^2}\alpha - \varepsilon^{1+q}\alpha^q - \varepsilon\alpha^{q+q^2} - \varepsilon^q\alpha^{1+q^2} - \varepsilon^{q^2}\alpha^{1+q} - N(\alpha) \end{aligned}$$

$$\begin{aligned} Tr(B) &= \varepsilon^q\alpha^{q+q^2} + \varepsilon^{q^2}\alpha^{1+q^2} + \varepsilon\alpha^{1+q} - N(\alpha) - \varepsilon\alpha^{q+q^2} - \varepsilon^q\alpha^{1+q^2} - \varepsilon^{q^2}\alpha^{1+q} - N(\alpha) \\ &= N(\varepsilon - \varepsilon^q)Tr(\rho^{1+q}) - 2N(\varepsilon - \varepsilon^q)N(\rho) \\ &= N(\varepsilon - \varepsilon^q)\{Tr(\rho^{1+q}) + 2N(\rho)\} \end{aligned}$$

$$\begin{aligned} \det B &= N(-\nu\mu + \varepsilon^{1+q}) \\ -\nu\mu + \varepsilon^{1+q} &= -(\varepsilon^q - \alpha)(\varepsilon - \alpha) + \varepsilon^{1+q} \\ &= (\varepsilon - \varepsilon^q)^2(\rho + \rho^2) \end{aligned}$$

$$\det B = N(\varepsilon - \varepsilon^q)^2 N(\rho + \rho^2)$$

$$\begin{aligned} D &= (TrB)^2 - 4\det B \qquad (166) \\ &= N(\varepsilon - \varepsilon^q)^2\{[Tr(\rho^{1+q}) + 2N(\rho)]^2 - 4N(\rho)N(\rho+1)\} \qquad (167) \end{aligned}$$

Substituting $\rho = 1/(\lambda - 1)$ into it, one has

$$D = N(\varepsilon - \varepsilon^q)^2 N\left(\frac{1}{\lambda - 1}\right)^2 \{[Tr(\lambda) - 1]^2 - 4N(\lambda)\} \qquad (168)$$

12 Appendix 3: Density of Type I curves with hyperellitic covering

We give a more detailed analysis on Type I curves with hyperelliptic coverings here.
The matrix Θ under double-side $\mathrm{PGL}_2(k)$-actions can be represented by the following matrices under the double-side $\mathrm{PGL}_2(k)$-action.

$$(i) \quad \Theta_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad (ii) \quad \Theta_2 = \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix} \qquad \exists \eta \in k_2, \eta^2 = e \in k^\times \setminus \left(k^\times\right)^2$$

Since

$$\lambda = \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{1+q}} \neq 0, 1, \qquad \beta \in k_3 \setminus k, \quad \beta \neq \alpha, \alpha^q, \alpha^{q^2}$$

one has β_1 and β_2 corresponding to the two representitives of Θ_1 and Θ_2.

$$\beta_1 = \Theta_1 \cdot \alpha = -\alpha \tag{169}$$

$$\lambda_1 = \frac{(\alpha + \alpha^q)^2}{4\alpha^{1+q}} \tag{170}$$

$$\beta_2 = \Theta_2 \cdot \alpha = \frac{e}{\alpha} \tag{171}$$

$$\lambda_2 = \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}} \tag{172}$$

12.1 The case (i) and the case (ii) have no overlap

Assume there is a λ in the intersection of the case (i) and (ii)

$$\lambda_1(\gamma) = \frac{(\gamma + \gamma^q)^2}{4\gamma^{1+q}} = \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}} = \lambda_2(\alpha) =: \lambda, \qquad \exists \gamma, \alpha \in k_3 \setminus k \tag{173}$$

Then the left-half of (173) becomes

$$\gamma^{q-1} + 2 + \frac{1}{\gamma^{q-1}} = 4\lambda \tag{174}$$

Then

$$\gamma^{2(q-1)} + 2(1 - 2\lambda)\gamma^{q-1} + 1 = 0$$

Denote $X := \gamma^{q-1}$, one has a quadratic equation

$$X^2 + 2(1 - 2\lambda)X + 1 = 0 \tag{175}$$

of which the discriminant is

$$D = 4(1 - 2\lambda)^2 - 4 = 4(1 - 4\lambda + 4\lambda^2 - 1) = 16\lambda(\lambda - 1) \neq 0$$

since $\lambda \neq 0, 1$.

Now we use the right-half of (173) to substitute λ as λ_2

$$\lambda - 1 \quad = \quad e\frac{(\alpha - \alpha^q)^2}{(e - \alpha^2)^{1+q}} \tag{176}$$

$$D = 16\lambda(\lambda - 1) = 16\lambda\frac{(\alpha - \alpha^q)^2}{(e - \alpha^2)^{1+q}}e$$

From (173), one knows that λ is not a square $\lambda \in (k_3^\times)^2$. Also $\lambda - 1$ is a square. Thus D is not square $D \notin (k_3^\times)^2$. This means that there is no solutions of the equation (175). Therefore the intersection between (i) and (ii) is empty.

□

12.2 The density of the case (i)

We now first count the cardinality of each orbit of the λ under the $\mathrm{PGL}_2(k)$ action.

Assume there is a γ belong to the same $\mathrm{PGL}_2(k)$-orbit with α, from (173) and (174), one has

$$\gamma^{q-1} + \gamma^{1-q} = \alpha^{q-1} + \alpha^{1-q} = 4\lambda - 2$$

Define

$$X := \alpha^{q-1},\ Y := \gamma^{q-1}$$

then the above equation becomes

$$(Y - X)(XY - 1) = 0$$

Thus we know

$$\text{either } Y = X \text{ or } Y = \frac{1}{X}$$

or

$$\gamma = l\alpha^{\pm 1} \qquad \exists l \in k^\times$$

Thus fixes an α the number of γ within the same orbit with $\alpha \in k_3 \setminus k, \alpha \neq \pm 1$ is

$$\#\gamma = \#\{l \in k^\times\} \times 2(: \pm) = 2(q-1)$$

$$\#\{\lambda_1\} = \frac{q^3 - q}{2(q-1)} = \frac{q(q+1)}{2}$$

12.3 A lower bound of the density of the case (ii)

To count the number of α corresponding to the same λ, we assume the α in the following formula of λ by the variavble x

$$\frac{(e - X^{1+q})^2}{(2 - X^2)^{1+q}} = \lambda \neq 0, 1$$

Then one has the following equation in x:

$$\lambda(2 - X^2)^{1+q} = (e - X^{1+q})^2.$$

One can expand it into

$$0 = (\lambda - 1)X^{2+2q} + \cdots + \tag{177}$$

Since $\lambda - 1 \neq 0$, we know that for an λ there could be solutions (i.e. α) no more than $2(1+q)$.

$$\#O(\lambda) = \#\{\alpha \mid \lambda(\alpha) = \lambda\} \leq 2(1+q)$$

Therefore we have a lower bound of the number of $\mathrm{PGL}_2(k)$ orbits $O(\lambda)$ of λ in the case (ii):

$$\#\{\lambda\} \geq \frac{\#\{\forall \alpha \in k_3 \setminus k\}}{\#O(\lambda)} = \frac{q^3 - q}{2(1+q)} = \frac{q(q-1)}{2}$$

13 Appendex 4: Classification of Type I non-hyperelliptic cases

Here we give a more detailed classification for Type I non-hyperelliptic cases.

We have the following three classes of the Type I curves with non-hyperelliptic coverings, where A under the above action has three representatives:

1.
$$A_1 = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \qquad a \neq 0, 1$$

   i.e. $\beta = a\varepsilon$.

   In this case, C is hyperelliptic if and only if $a = -1$.

   Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case as δ_1,
$$\delta_1 = \begin{cases} 1 & q \equiv 1 \bmod 3 \\ 0 & q \not\equiv 1 \bmod 3 \end{cases}$$

   The number of λ_1 or the Type I curves with nonhyperelliptic covering is
$$\#\{\lambda_1\} = \frac{1}{4}(q^3 - 2q^2 - 3q) - \delta_1$$

2.
$$A_2 = \begin{pmatrix} a & e \\ 1 & a \end{pmatrix}, \qquad \eta^2 = e \in k^\times \setminus (k^\times)^2$$

   In this case, C is hyperelliptic if and only $a = 0$.

   Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case as δ_2,
$$\delta_2 = \begin{cases} 1 & q \equiv 2 \bmod 3 \\ 0 & q \not\equiv 2 \bmod 3 \end{cases}$$

   The number of λ_2 or the Type I curves with nonhyperelliptic covering is
$$\#\{\lambda_2\} = \frac{q(q-1)^2}{4} - \delta_2$$

3.
$$A_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Then $\beta = \varepsilon + 1$.

In this case, no C is hyerelliptic.

Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case as δ_3,
$$\delta_3 = \begin{cases} 1 & char(k) = 3 \\ 0 & char(k) \neq 3 \end{cases}$$

The number of λ_3 or the Type I curves with nonhyperelliptic covering is

$$\#\{\lambda_3\} = \frac{q(q^2-1)}{2q} - \delta_3$$

Since

$$\sum_{i=1}^{3} \delta_i = 1,$$

there are

$$\sum_{i=1}^{3} \#\{\lambda_i\} \quad = \quad \frac{q^3-q^2-q-3}{2} \tag{178}$$

Type I curvces which are with non-hyperellitpic coverings.