Summer 2007

Isomorphisms of Elliptic Curves over Extensions of Finite Fields

Mathew Niemerg
Eastern Illinois University

Isomorphisms of Elliptic Curves over Extensions of Finite Fields

Matthew Niemerg

Adviser: Joshua B. Holden

Mathematical Sciences Technical Report Series
MSTR 07-01

July 31, 2007

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 **Phone (812)-877-8193**

Isomorphisms of Elliptic Curves over Extensions of Finite Fields

Matthew Niemerg
Eastern Illinois University

Faculty Advisor: Joshua Holden
Rose-Hulman Institute of Technology
Mathematics Research Experience for Undergraduates (REU)

Summer 2007

ISOMORPHISMS OF ELLIPTIC CURVES OVER EXTENSIONS OF FINITE FIELDS

MATTHEW NIEMERG

Abstract. Our main interest lies in exploring isomorphisms of elliptic curves. In particular, we focus on two curves defined over a base field and look at which extension fields the curves are isomorphic over. Elliptic curves have a fascinating structure behind them. This structure allows for much to be explored and studied.

1. Introduction

Over the last several decades, the mathematics community has seen an increase in the interest of elliptic curves. This is mainly due to their usage in cryptographic schemes as well as their recent use in solving Fermat's Last Theorem by Andrew Wiles in 1994. Elliptic curves are the simplest kind of curve after conic sections. Certain types of Diophantine equations satisfy the conditions of being an elliptic curve as well. Finally, elliptic curves also serve as a bridge between geometry and algebra. The rational points, plus a point at infinity that acts as the identity element, form an abelian group. This group is also isomorphic to a Riemann surface with genus 1.

2. Terminology and Background

Throughout the rest of the paper, we will let K be a finite field such that

$$K = \mathbb{F}_q \text{ where } q = p^n.$$

The characteristic of the field is a prime p and the extension is n.

Let K be a finite field. If E is defined over K, denoted $E(K)$, and is of the form

$$E(K) := y^2 = x^3 + Ax + B \text{ for } p = 2 \tag{1}$$

$$E(K) := y^2 = x^3 + Ax + B \text{ for } p = 3 \tag{2}$$

$$E(K) := y^2 = x^3 + Ax + B \text{ for } p > 3 \tag{3}$$

then $E(K)$ is said to be in Weierstrass Form. We will mainly be working with curves that have the form of (3).

Following standard convention, we let $\#E(K)$ denote the number of rational points on a curve $E(K)$ plus 1, for the point at infinity.

Certain types of curves are of no particular interest to us, mainly singular curves. Singular curves correspond to when the discriminant of the cubic equation is 0, or corresponding to (3), when $4A^3 + 27B^2 = 0$.

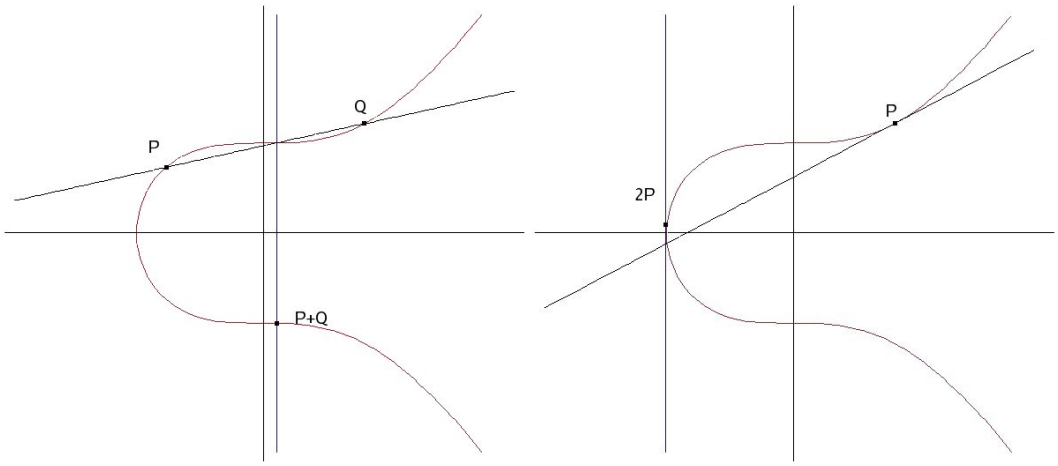
The group of rational points on a curve falls into 1 of 2 types. If our curve E is defined over a field K, and the number of points on the curve is q, according to [1] then

(1) $E(K) \cong Z/qZ$
(2) $E(K) \cong Z/mZ \oplus Z/lZ$ where $m|q$, $l|m$, and $ml = q$.

The group law is rather strange for elliptic curves. We define the group law on a curve E as follows.

Group Law. [2] *Let $P, Q \in E, L$ the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let L' be the line connecting R and 0 (the point at infinity). Then $P + Q$ is the third point that intersects E on L'.*

If we look at the below pictures, we can see how the group law is constructed when dealing with curves in Weierstrass form. In the first example, we are adding two points, P and Q. To find $P + Q$ we draw the line connecting them, find the third point of intersection, and finally drop a vertical line down to find the resulting point. In the second example, we are adding a single point to itself. We take the tangent line of the curve at that point (this is because the tangent line can be seen as hitting the same point 'twice'), find the other point on the line, and drop a vertical line to find the resulting point.



Theorem 1. [2] *Two elliptic curves defined over K are isomorphic over $\bar{K}$ if and only if their j-invariant is the same.*

The j-invariant of a curve E is defined to be

$$j(E) = -1728(4A^3)/(-16(4A^3 + 27B^2)) \tag{4}$$

$\bar{K}$ is the algebraic closure of K, or the union of all extensions of K, finite or infinite.

When undergoing a linear transformation for a change of variables on a curve, the j-invariant stays the same [2]. One question remains, however, from the previous theorem. Over which extension field are these curves isomorphic? All we know is that the curves are isomorphic over *some* extension; which one is another matter.

We will investigate this question in more detail later on.

$$\text{Let } E_1(K) := y^2 = x^3 + Ax + B. \tag{5}$$

$$\text{Let } E_2(K) := y^2 = x^3 + A'x + B'. \tag{6}$$

The transformation that preserves the Weierstrass form from E_1 to E_2 is the mapping

$$\phi : E_1 \mapsto E_2$$
$$\text{given by}$$
$$\phi : (x, y) \mapsto (u^2x, u^3y)$$

where $u \in \bar{K}$.

We have three cases to consider, when $j \neq 0, 1728$, $j = 1728$, and $j = 0$ to give us an explicit value for u [2].

Case 1: $j \neq 0, 1728$

$$u = (A/A')^{1/4} = (B/B')^{1/6}$$

Case 2: $j = 1728$

$$u = (A/A')^{1/4}$$

Case 3: $j = 0$

$$u = (B/B')^{1/6}$$

3. Theoretical Results

Theorem 2. *Let K be a finite field, $E_1(K) := y^2 = x^3 + Ax + B$, and $E_2(K) := y^2 = x^3 + A'x + B'$. If $j(E_1) = j(E_2)$ and $\#E_1(K) \neq \#E_2(K)$, then E_1 and E_2 are isomorphic over extensions of K of degrees 2, 4, or 6 when $j \neq 0, 1728$, $j = 1728$, $j = 0$, respectively.*

Proof: Assume $j(E_1) = j(E_2)$.

Case 1: $j \neq 0, 1728$

$$\begin{aligned} u &= (A/A')^{1/4} = (B/B')^{1/6} \\ u^4 &= (A/A') \text{ and } u^6 = (B/B') \\ u^6/u^4 &= u^2 = (A'B)/(AB') \\ u^2 &\in K \\ u &\in K_2, \text{ where } K_2 \text{ is an extension of } K \text{ of degree 2} \\ E_1 &\cong E_2 \text{ over } K_2. \end{aligned}$$

Case 2: $j = 1728$

$$\begin{aligned} u &= (A/A')^{1/4} \\ u^4 &= (A/A') \\ u^4 &\in K \\ u &\in K_4, \text{ where } K_4 \text{ is an extension of } K \text{ of degree 4} \\ E_1 &\cong E_2 \text{ over } K_4. \end{aligned}$$

Case 3: $j = 0$

$$\begin{aligned} u &= (B/B')^{1/6} \\ u^6 &= (B/B') \\ u^6 &\in K \\ u &\in K_6, \text{ where } K_6 \text{ is an extension of } K \text{ of degree } 6 \\ E_1 &\cong E_2 \text{ over } K_6. \end{aligned}$$

As one can see, we have only proven that extensions of degree $2, 4$, and 6, for $j \neq 0, 1728$, $j = 1728$, $j = 0$, respectively, are the maximal such extensions for two curves to be isomorphic over if their j-invariant is the same and the number of points is different. However, all of my examples that I have looked at have shown this to also be the minimal case as well, but a concise proof has not been formulated yet. More work needs to be done in the future to show that they are the minimal extensions as well.

Example of Case 1

Let $K = \mathbb{F}_{11}$, $E_1(K) := y^2 = x^3 + 4x + 4$ and $E_2(K) := y^2 = x^3 + 5x + 10$. Since $K = \mathbb{F}_{11}$, we will be doing our calculations $\mod 11$.

In this case $j = 10$ and $\#E_1 = 11$ and $\#E_2 = 13$.

If we let $p(t) = t^2 + 7t + 2$ and $K_2 = K[t]/p(t)$, then $u^2 = 6$, $u^3 = 3t + 5$.

We verify that this is indeed the correct transformation by substituting the coordinates back into the original equation.

$$\begin{aligned} (u^3y)^2 &= (u^2x)^3 + 4u^2x + 4 \\ u^6y^2 &= u^6x^3 + 4u^2x + 4 \\ 7y^2 &= 7x^3 + 2x + 4 \\ y^2 &= x^3 + 2x/7 + 4/7 \\ y^2 &= x^3 + 5x + 10 \end{aligned}$$

This, then, is the correct transformation. The two solutions that satisfy $u^2 = 6$ are

(1) $u = 1 + 5t$
(2) $u = 10 + 6t$

The three solutions that satisfy $u^3 = 3t + 5$ are

(1) $u = 5 + 8t$
(2) $u = 7 + 8t$
(3) $u = 10 + 6t$

The only solution u that satisfies these equations is $u = 10 + 6t$.

$(10 + 6t)^2 \equiv 100 + 120t + 36t^2 \equiv 1 + 10t + 3t^2 \equiv 6 \mod p(t)$.

$(10+6t)^3 \equiv 1000+1800t+360t^2+216t^3 \equiv 10+7t+8t^2+7t^3 \equiv 3t+5 \mod p(t)$

Since $u \in K_2$, then $u^2, u^3 \in K_2$, so the transformation takes place with coordinate change under K_2. Since $u = 10 + 6t$, then $u \notin K$. In addition, since $u^2 \in K$, then, $uu^2 = u^3 \notin K$, so the coordinate change cannot take place under K.

Example of Case 2

Let $K = \mathbb{F}_{13}$, $E_1(K) := y^2 = x^3 + 3x$ and $E_2(K) := y^2 = x^3 + 4x$. Since $K = \mathbb{F}_{13}$, our calculations will be done $\mod 13$.

In this case $j = 1728$ and $\#E_1 = 20$ and $\#E_2 = 8$.

If we let $p(t) = t^4 + 3t^2 + 12t + 2$ and $K_4 = K[t]/p(t)$, then $u^2 = 2$, $u^3 = t^3 + 10t^2 + 9t + 11$.

We verify that this is indeed the correct transformation by substituting the coordinates back into the original equation.

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 + 3u^2x\\ u^6y^2 &= u^6x^3 + 3u^2x\\ 8y^2 &= 8x^3 + 6x\\ y^2 &= x^3 + 6x/8\\ y^2 &= x^3 + 4x\end{aligned}$$

This, then, is the correct transformation. The two solutions that satisfy $u^2 = 2$ are

(1) $u = 1 + 2t + 8t^2 + 6t^3$
(2) $u = 12 + 11t + 5t^2 + 7t^3$

The three solutions that satisfy $u^3 = t^3 + 10t^2 + 9t + 11$ are

(1) $u = 4 + 8t + 6t^2 + 11t^3$
(2) $u = 10 + 7t + 2t^2 + 8t^3$
(3) $u = 12 + 11t + 5t^2 + 7t^3$

Now, the only solution u that satisfies these equations is $u = 7t^3 + 5t^2 + 11t + 12$.

$$\begin{aligned}(7t^3 + 5t^2 + 11t + 12)^2 &\equiv 49t^6 + 70t^5 + 179t^4 + 278t^3 + 241t^2 + 264t + 144\\ &\equiv 10t^6 + 5t^5 + 10t^4 + 5t^3 + 7t^2 + 4t + 1\\ &\equiv 2 \mod p(t).\\ (7t^3 + 5t^2 + 11t + 12)^3 &\equiv 343t^9 + 735t^8 + 2142t^7 + 4199t^6 + 5886t^5 + 8259t^4 + 8315t^3 + 6516t^2 +\\ &\quad 4752t + 1728\\ &\equiv 5t^9 + 7t^8 + 10t^7 + 4t^4 + 8t^3 + 3t^2 + 7t + 12\\ &\equiv t^3 + 10t^2 + 9t + 11 \mod p(t)\end{aligned}$$

Since $u \in K_4$, then $u^3, u^2 \in K_4$, and the transformation takes place with coordinate change under K_4. Since $u = 7t^3 + 5t^2 + 11t + 12$, $u \notin K$. Since $u^2 \in K$ then $uu^2 = u^3 \notin K$, so the change in variables does not occur in K.

Example of Case 3

Let $K = \mathbb{F}_{31}$, $E_1(K) := y^2 = x^3 + 3$ and $E_2(K) := y^2 = x^3 + 13$. Since $K = \mathbb{F}_{31}$, our calculations will be done mod 31.

In this case $j = 0$ and $\#E_1 = 43$ and $\#E_2 = 25$.

If we let $p(t) = t^6 + 19t^3 + 16t^2 + 8t + 3$ and $K_6 = K[t]/p(t)$, then $u^2 = 25t^5 + 3t^4 + 11t^3 + 23t^2 + 27t + 19$, $u^3 = 6$.

We verify that this is indeed the correct transformation by substituting the coordinates back into the original equation.

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 + 3\\ u^6y^2 &= u^6x^3 + 3\\ 5y^2 &= 5x^3 + 3\\ y^2 &= x^3 + 3/5\\ y^2 &= x^3 + 13\end{aligned}$$

This, then, is the correct transformation. The two solutions that satisfy $u^2 = 25t^5 + 3t^4 + 25t^3 + 11t^2 + 13t + 18$ are

(1) $u = 20t^5 + 20t^4 + 30t^3 + 28t^2 + 19t + 3$
(2) $u = 20t^5 + 11t^4 + 25t^3 + 11t^2 + 13t + 18$

The three solutions that satisfy $u^3 = t^3 + 10t^2 + 9t + 11$ are

(1) $u = 7t^5 + 24t^4 + t^3 + 24t^2 + 3t + 28$
(2) $u = 4t^5 + 27t^4 + 5t^3 + 27t^2 + 15t + 16$
(3) $u = 20t^5 + 11t^4 + 25t^3 + 11t^2 + 13t + 18$

Now, the only solution u that satisfies these equations is $u = 20t^5 + 11t^4 + 25t^3 + 11t^2 + 13t + 18$.

$$\begin{aligned}
(20t^5 + 11t^4 + 25t^3 + 11t^2 + 13t + 18)^2 &\equiv 400t^{10} + 440t^9 + 1121t^8 + 990t^7 + 1387t^6 + 1556t^5 + 1167t^4 + \\
&\quad 1186t^3 + 565t^2 + 468t + 324 \\
&\equiv 28t^{10} + 6t^9 + 5t^8 + 29t^7 + 23t^6 + 6t^5 + 20t^4 + 8t^3 + 7t^2 \\
&\quad 3t + 14 \\
&\equiv 25t^5 + 3t^4 + 11t^3 + 23t^2 + 27t + 19 \mod p(t). \\
(20t^5 + 11t^4 + 25t^3 + 11t^2 + 13t + 18)^3 &\equiv 8000t^{15} + 13200t14 + 37260t^{13} + 47531t^{12} + 76695t^{11} + \\
&\quad 96378t^{10} + 108514t^9 + 123762t^8 + 106488t^7 + 103256t^6 + \\
&\quad 81978t^5 + 57903t^4 + 41941t^3 + 19818t^2 + 12636t + 5832 \\
&\equiv 2t^{15} + 25t^{14} + 29t^{13} + 8t^{12} + t^{11} + 30t^{10} + 14t^9 + 10t^8 + 3t^7 + \\
&\quad 26t^6 + 14t^5 + 26t^4 + 29t^3 + 9t^2 + 19t + 4 \\
&\equiv 6 \mod p(t)
\end{aligned}$$

Since $u \in K_6$, then $u^2, u^3 \in K_6$, and the transformation takes place with coordinate change under K_6. Because $u^3 \in K$ and $u \notin K$, then $u^3/u = u^2 \notin K$, so this cannot be an isomorphism in K.

In addition to the number of points not being the same, we have the case of what happens when the number of points are the same, and the j-invariant is also the same.

Conjecture 1. *Two curves over a base field K with the same j-invariant and the same number of points will be isomorphic under K if the number of points on the curve q does not have divisors m and l such that $m|q$, $l|m$ and $ml = q,$, where $l \neq 1$.*

Example 1: Let $K = \mathbb{F}_{11}$, $E_1(K) := y^2 = x^3 + 10x, E_2(K) := y^2 = x^3 + x$. Here we have $\#E_1(K) = \#E_2(K) = 12$. It is easy to check that $j(E_1(K)) = j(E_2(K)) = 1$. Since, $6|12$, $2|6$, and $2(6) = 12$, these curves will not be isomorphic under K. By, Theorem 3 if $p(t) = t^4 + 8t^2 + 10t + 2$ and $K_4 = K[t]/p(t)$, we will find that these curves are isomorphic under K_4, since $1728 \equiv 1 \mod 11$.

We have that $u^2 = 4t^3 + 6t^2 + 2t + 10$ and $u^3 = 6t^3 + 9t^2 + 3t$. Let us make sure that this is the correct transformation.

$$\begin{aligned}
(u^3y)^2 &= (u^2x)^3 + 10(u^2x) \\
u^6y^2 &= u^6x^3 + 10(4t^3 + 6t^2 + 2t + 10)x \\
(7t^3 + 5t^2 + 9t + 1)y^2 &= (7t^3 + 5t^2 + 9t + 1)x^3 + (7t^3 + 5t^2 + 9t + 1)x \\
y^2 &= x^3 + 1
\end{aligned}$$

The transformation does indeed work correctly, and as one can see $u^2, u^3 \notin K$. Under this isomorphism, these curves are not isomorphic in K. However, we have not been able to show that there is not an isomorphism that exists with a change in coordinates in K.

Example 2: Let $K = \mathbb{F}_{17}, E_1(K) := y^2 = x^3 + 16x + 14, E_2(K) := y^2 = x^3 + x + 12$. In this case, $\#E_1(K) = \#E_2(K) = 15$ and $j(E_1(K)) = j(E_2(K)) = 7$.

We have that $u^2 = 13$ and $u^3 = 2$. Let's double check to make sure this is the right transformation.

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 + 16(u^2x) + 14\\ 8y^2 &= 8x^3 + 16(13)x + 14\\ y^2 &= x^3 + 8(13)x + 14/8\\ y^2 &= x^3 + x + 12\end{aligned}$$

This then is a valid transformation. We have that both $u^2, u^3 \in K$, so this transformation takes place in K.

4. Other Results

Using a program called MAGMA, a computer program that specializes in field theory operations and elliptic curves, we began studying curves with characteristic > 3. Using (3), we would create all possible non-singular curves by iterating through the elements in the field and changing the different values of A, and as soon as that was finished, move to the next B, and repeat until all curves had been exhausted. During this iteration, we outputted only the j-invariant to a file and would write a new line when B changed. We did this for all non-singular curves over $p = 5, 7, 11$ and extensions of $2, 3, 4$. We did the same thing again over the same fields, except we first iterated through all the values of B, followed by moving the next A.

Two emerging patterns arose. The j-invariant had repeats with either 2 blocks or 3 blocks, depending on the order of the field, the extension of the field, and which variable, A or B, was being iterated first. If A was iterated first, we would see 2 blocks that were the same. This is due to the nature of the definition of the j-invariant. We see that when determining the j-invariant, the B term is squared.

We need to first state Lagrange's Theorem and a Corollary.

Lagrange's Theorem. [3] *If K is a subgroup of a finite group G, then the order of K divides the order of G. In particular, $|G| = |K|[G : K]$.*

Corollary 1. [3] *Let G be a finite group.*

1. *If $a \in G$, then the order of a divides the order of G. Then, n divides $|G|$ by Lagrange's Theorem.*
2. *If $|G| = k, then a^k = e, \forall\ a \in G$.*

Proof: (1) If $a \in G$ has order n, then the cyclic subgroup $< a >$ of G has order n. Then, $n|k$ by part (1), and we say $k = nt$. Therefore, $a^k = a^{nt} = (a^n)^t = e^t = e$.

Since a finite field under multiplication is a group and has order $p^n - 1$, where p is the characteristic and n is the extension, we will use this corollary of Lagrange's Theorem to show some facts about the j-invariant.

Suppose we have two curves, $E_1(K)$, and $E_2(K)$ where $E_1(K) := y^2 = x^3 + Ax + B$ and $E_2(K) := y^2 = x^3 + Ax + Bg^{(p^n-1)/2}$. Then,

$$\begin{aligned}j(E_1) &= 1728(4A^3)/\{16(4A^3 + 27B^2)\}\\ j(E_2) &= 1728(4A^3)/[16\{4A^3 + 27(Bg^{(p^n-1)/2})^2\}]\\ &= 1728(4A^3)/\{16(4A^3 + 27B^2g^{(p^n-1)})\}\\ &= 1728(4A^3)/\{16(4A^3 + 27B^2)\} \text{ by Corollary 1}\\ &= j(E_1)\end{aligned}$$

Similarly, when we iterated B first, we would see 3 blocks that were the same, whenever we were working with extensions of even degree. In this case, the A term is raised to the third power in the j-invariant equation.

Suppose we have two curves, $E_1(K)$, and $E_2(K)$ where $E_1(K) := y^2 = x^3 + Ax + B$ and $E_2(K) := y^2 = x^3 + Ag^{(p^n-1)/3}x + B$. Then,

$$\begin{aligned} j(E_1) &= 1728(4A^3)/\{16(4A^3 + 27B^2)\} \\ j(E_2) &= 1728(4Ag^{(p^n-1)/3})^3/[16\{4(Ag^{(p^n-1)/3})^3 + 27B^2\}] \\ &= 1728(4A^3g^{p^n-1})/\{16(4A^3g^{(p^n-1)} + 27B^2)\} \\ &= 1728(4A^3)/\{16(4A^3 + 27B^2)\} \text{ by Corollary 1} \\ &= j(E_1) \end{aligned}$$

We noticed that the 3 repeating blocks only occured when $3|p^n - 1$. Notice that any time we work with extension fields of even degree, the order of the field is p^{2n}. Then, $p^{2n} - 1 = (p^n - 1)(p^n + 1)$. Since $p > 3$, either $3|p^n - 1$ or $3|p^n + 1$, so $3|p^{2n} - 1$, for any n. Because in the cases when we were dealing with extensions of even degree, $3|p^n - 1$, and since the A term when determining the j-invariant is cubed, we were able to observe these repeating blocks of 3. This property explains why we saw those patterns.

Examples of j-invariants over all curves in $\mathbb{F}_5$

B/A	0	1	2	3	4
0	-	3	3	3	3
1	0	2	4	-	1
2	0	1	-	4	2
3	0	1	-	4	2
4	0	2	4	-	1

If we ignore the first row and the first column, there is a symmetry in this table. If we call the table T^1, and let T^1_{BA} denote the cell in the table, we can see that $T^1_{B/A} = T^1_{(5-B)/A}$. This is due because the inverse of B or $p - B$, or in this case $5 - B$, has the same j-invariant, if A is fixed.

In the following table, if we ignore the last row, we see 3 repeating blocks occuring. If our table is called T^2, and the cells in our table are denoted as $T^2_{A/B}$, then $T^2_{A/B} = T^2_{At^8/B} = T^2_{At^{16}/B}$. Since $(5^2 - 1)/3 = (25 - 1)/3 = 24/3 = 8$, we have blocks of 8 occurring.

Examples of j-invariants over some curves in $\mathbb{F}_5$ in a 2nd degree extension

A/B	1	t	t^2	t^3	t^4	t^5	2	t^7	t^8	t^9	t^{10}	t^{11}	4	t^{13}	t^{14}	t^{15}	t^{16}	t^{17}	3
1	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1
t	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8
t^2	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4
t^3	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}
t^4	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2
t^5	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}
2	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-
t^7	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7
t^8	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1
t^9	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8
t^{10}	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4
t^{11}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}
4	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2
t^{13}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}
t^{14}	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-
t^{15}	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7
t^{16}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1
t^{17}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8
3	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4
t^{19}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}
t^{20}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2
t^{21}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}
t^{22}	4	t	t^{19}	1	t^{14}	t^5	-	t^{15}	t^{22}	2	t^{23}	t^3	4	t	t^{19}	1	t^{14}	t^5	-
t^{23}	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7	t^2	t^{13}	t^{16}	t^{17}	t^9	t^{11}	t^{21}	t^{20}	t^8	t^4	t^{10}	t^7
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

5. Future Work

Many interesting questions still exist that are feasibly attackable in regards to isomorphisms of elliptic curves. One question to pursue would be to show that if two curves are defined over K, have the same j-invariant, and also have the same number of points that the curves are isomorphic in K. When using MAGMA and constructing the isomorphism, we were always able to find a change in variables that were still in K. Is this always the case or is there a counter-example? Another route to take with this question is to look at the case when the number of points is prime. Perhaps some insight can be gathered and from there a solution can be extended to a more general case.

Suppose we have n curves with the same j-invariant over a field K with order q. Let $E_i := y^2 + A_i x + B_i$ be a curve for $1 \leq i \leq n$. We observed that $\sum A_i = mq$ for some $m \in \mathbb{N}$. Similarly, we saw that $\sum B_i = lq$ for some $l \in \mathbb{N}$. Are these isolated examples that we looked at, or is there more of an underlying structure that explains why this is true?

Conjecture 2. *Suppose there are n curves with the same j-invariant in K. Let $J_a = \{E(K)|j(E(K)) = a$ and $E(K) := y^2 = x^3 + Ax + B\}$, where K has order q. Then, $\sum A_i = mq$ and $\sum B_i = lq$ for some $m, l \in \mathbb{N}$.*

Example of Isomorphic Curves over $\mathbb{F}_{19}$ and $\mathbb{F}_{23}$

$\mathbb{F}_{19}$				$\mathbb{F}_{23}$			
i	j	A_i	B_i	i	j	A'_i	B'_i
1	8	2	10	1	10	22	7
2	8	18	15	2	10	21	22
3	8	15	13	3	10	20	14
4	8	14	10	4	10	19	10
5	8	13	13	5	10	17	21
6	8	12	15	6	10	15	15
7	8	10	13	7	10	14	5
8	8	8	15	8	10	11	20
9	8	3	10	9	10	10	17
10	8	15	6	10	10	7	11
11	8	13	6	11	10	5	19
12	8	12	4	12	10	7	12
13	8	10	6	13	10	22	16
14	8	8	4	14	10	21	1
15	8	2	9	15	10	20	9
16	8	3	9	16	10	19	13
17	8	14	9	17	10	17	2
18	8	18	4	18	10	5	4
				19	10	15	8
				20	10	14	18
				21	10	11	3
				22	10	10	6
	Sum	190	171		Sum	322	253

Here we have two sets of curves, one set over $\mathbb{F}_{19}$ and the other over $\mathbb{F}_{23}$. As we can see, $\sum A_i = 190$ and $\sum B_i = 171$. $190 = (10)19$ and $171 = (9)19$. In the other case, $\sum A'_i = 322$ and $\sum B'_i = 253$. Once more, we observe that $322 = (14)23$ and $253 = (11)23$. We believe that this conjecture can be explained by the patterns we observed with the repeating blocks of the j-invariant.

Let us look at the group of transformations from one curve to another defined over K with order q. Suppose we have n curves with the same j-invariant, and the transformation $\phi_i : E_1 \mapsto E_i$, for $1 \leq i \leq n$ is given by $\phi_i : (x, y) \mapsto (u_i^2 x, u_i^3 y)$. We noticed that when $j \neq 0, 1728$ $\sum u_i^2 = mq$ for some $m \in \mathbb{N}$. The previous curves we have used over $\mathbb{F}_{19}$ and $\mathbb{F}_{23}$ will work fine as examples.

Conjecture 3. *Suppose there are n curves with the same j-invariant in K with order q. Let $T = \{\phi : E_1(K) \mapsto E_i(K)|\phi_i : (x, y) \mapsto (u_i^2 x, u_i^3 y)$ for $1 \leq i \leq n\}$. Then $\sum u_i^2 = mq$ for some $m \in \mathbb{N}$.*

$\mathbb{F}_{19}$		$\mathbb{F}_{23}$	
$\phi_i : E_1 \mapsto E_i$	u_i^2	$\phi_i : E_1' \mapsto E_i'$	$(u_i^2)'$
$\phi_1 : E_1 \mapsto E_1$	1	$\phi_1 : E_1' \mapsto E_1'$	1
$\phi_2 : E_1 \mapsto E_2$	6	$\phi_2' : E_1' \mapsto E_2'$	9
$\phi_3 : E_1 \mapsto E_3$	16	$\phi_3' : E_1' \mapsto E_3'$	13
$\phi_4 : E_1 \mapsto E_4$	7	$\phi_4' : E_1' \mapsto E_4'$	12
$\phi_5 : E_1 \mapsto E_5$	5	$\phi_5' : E_1' \mapsto E_5'$	2
$\phi_6 : E_1 \mapsto E_6$	4	$\phi_6' : E_1' \mapsto E_6'$	16
$\phi_7 : E_1 \mapsto E_7$	17	$\phi_7' : E_1' \mapsto E_7'$	8
$\phi_8 : E_1 \mapsto E_8$	9	$\phi_8' : E_1' \mapsto E_8'$	18
$\phi_9 : E_1 \mapsto E_9$	11	$\phi_9' : E_1' \mapsto E_9'$	4
$\phi_{10} : E_1 \mapsto E_{10}$	3	$\phi_{10}' : E_1' \mapsto E_{10}'$	6
$\phi_{11} : E_1 \mapsto E_{11}$	14	$\phi_{11}' : E_1' \mapsto E_{11}'$	3
$\phi_{12} : E_1 \mapsto E_{12}$	15	$\phi_{12}' : E_1' \mapsto E_{12}'$	17
$\phi_{13} : E_1 \mapsto E_{13}$	2	$\phi_{13}' : E_1' \mapsto E_{13}'$	22
$\phi_{14} : E_1 \mapsto E_{14}$	10	$\phi_{14}' : E_1' \mapsto E_{14}'$	14
$\phi_{15} : E_1 \mapsto E_{15}$	18	$\phi_{15}' : E_1' \mapsto E_{15}'$	10
$\phi_{16} : E_1 \mapsto E_{16}$	8	$\phi_{16}' : E_1' \mapsto E_{16}'$	11
$\phi_{17} : E_1 \mapsto E_{17}$	12	$\phi_{17}' : E_1' \mapsto E_{17}'$	21
$\phi_{18} : E_1 \mapsto E_{18}$	13	$\phi_{18}' : E_1' \mapsto E_{18}'$	20
		$\phi_{19}' : E_1' \mapsto E_{19}'$	7
		$\phi_{20}' : E_1' \mapsto E_{20}'$	15
		$\phi_{21}' : E_1' \mapsto E_{21}'$	5
		$\phi_{22}' : E_1' \mapsto E_{22}'$	19
Sum	171	Sum	253

In this table, we note that these curves are the same ones used in the previous table. This table only has only the u_i^2 terms being added, and none of the u_i^3 terms in the transformation of $\phi_i : (x, y) \mapsto (u_i^2 x, u_i^3 y)$. The reason for this was that in nearly all of the group of isomorphisms we looked at, the u_i^3 terms did not add up to a multiple of p.

Here we have yet another example of the order of the field being related to a property of many elliptic curves. The curves in the $\mathbb{F}_{19}$ example have their u_i^2 terms add up to 171 and $171 = (9)19$. The curves in the $\mathbb{F}_{23}$ example have their u_i^2 terms add up to 253 and $253 = (11)23$.

6. Conclusion

We have found over the course of studying elliptic many interesting structural properties. Our main results deal with knowing the maximal extension curves are isomorphic under. In addition, all of the unproven conjectures deal with the order of the field one is working with. Future work in regards to elliptic curves has not been exhausted and probably never will be.

References

[1] M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkoerper', Abh. Math. Sem. Hansischen Univ. 14 (1941), 197272.

[2] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math. 106, Springer-Verlag, New York, 1996.

[3] T. W. Hungerford, Abstract Algebra: An Introduction, Thomson Learning, United States,1997.

Rose-Hulman Institute of Technology and Eastern Illinois University
E-mail address: meniemerg@eiu.edu