L-functions of genus two abelian coverings of elliptic curves over finite fields.

Pavel Solomatin

(Leiden University) & (Bordeaux University)

February, 2015

Introduction

Let us state some basic results concerning arithmetical structure of number fields:

Basic results in the number field case

1. Equality of zeta-functions is the same as *arithmetical equivalence*. In particular, for finite normal extensions of $\mathbb{Q}$ we have: $\zeta_K(s) = \zeta_L(s) \Rightarrow K \simeq L$;

Introduction

Let us state some basic results concerning arithmetical structure of number fields:

Basic results in the number field case

1. Equality of zeta-functions is the same as *arithmetical equivalence*. In particular, for finite normal extensions of $\mathbb{Q}$ we have: $\zeta_K(s) = \zeta_L(s) \Rightarrow K \simeq L$;
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.

Introduction

Let us state some basic results concerning arithmetical structure of number fields:

Basic results in the number field case

1. Equality of zeta-functions is the same as *arithmetical equivalence*. In particular, for finite normal extensions of $\mathbb{Q}$ we have: $\zeta_K(s) = \zeta_L(s) \Rightarrow K \simeq L$;
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.
3. Isomorphism of abelianizations of absolute Galois groups does not imply neither isomorphism or even arithmetical equivalence!

Introduction

Let us state some basic results concerning arithmetical structure of number fields:

Basic results in the number field case

1. Equality of zeta-functions is the same as *arithmetical equivalence*. In particular, for finite normal extensions of $\mathbb{Q}$ we have: $\zeta_K(s) = \zeta_L(s) \Rightarrow K \simeq L$;
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.
3. Isomorphism of abelianizations of absolute Galois groups does not imply neither isomorphism or even arithmetical equivalence!
4. In contrast, we(actually Bart) could construct one cyclic Galois extension K'/K of degree three with character χ such that $L_K(\chi, s)$ occurs only for that field.

Introduction

Now, it seems to be natural to ask:

Introduction

Now, it seems to be natural to ask:

a vague question

What could we say about this issue on the function field side?

Now, it seems to be natural to ask:

a vague question

What could we say about this issue on the function field side?

Remark: On the function filed side there are two *completely different* ways to define L-functions: one due to Dedekind, Hasse, Artin, Weil and another one due to Carlitz, Goss, Drinfeld. Both of this ways turned out to be very productive, but today we restrict ourselves only to the first case.

Introduction

For the sake of clearness, we recall some basic settings and introduce our notations:

1. Let K be a *global function field*, meaning that it is a finite extension of $\mathbb{F}_q(t)$, where $q = p^n$ and p is prime.

Introduction

For the sake of clearness, we recall some basic settings and introduce our notations:

1. Let K be a *global function field*, meaning that it is a finite extension of $\mathbb{F}_q(t)$, where $q = p^n$ and p is prime.
2. We define $G_K := \mathrm{Gal}(K^{sep} : K)$ and $\zeta_K(s) = \sum \frac{1}{N(a)^s}$, where sum is over all ideals $a \in \mathcal{O}_K$ and $N(a) = |\mathcal{O}_K / a\mathcal{O}_K|$.

Introduction

For the sake of clearness, we recall some basic settings and introduce our notations:

1. Let K be a *global function field*, meaning that it is a finite extension of $\mathbb{F}_q(t)$, where $q = p^n$ and p is prime.
2. We define $G_K := \mathrm{Gal}(K^{sep} : K)$ and $\zeta_K(s) = \sum \frac{1}{N(a)^s}$, where sum is over all ideals $a \in \mathcal{O}_K$ and $N(a) = |\mathcal{O}_K / a\mathcal{O}_K|$.
3. We denote by X smooth projective curve over $\mathbb{F}_q$ such that K is isomorphic to a function field of X.

Introduction

For the sake of clearness, we recall some basic settings and introduce our notations:

1. Let K be a *global function field*, meaning that it is a finite extension of $\mathbb{F}_q(t)$, where $q = p^n$ and p is prime.
2. We define $G_K := \mathrm{Gal}(K^{sep} : K)$ and $\zeta_K(s) = \sum \frac{1}{N(a)^s}$, where sum is over all ideals $a \in \mathcal{O}_K$ and $N(a) = |\mathcal{O}_K / a\mathcal{O}_K|$.
3. We denote by X smooth projective curve over $\mathbb{F}_q$ such that K is isomorphic to a function field of X.

Remark: note that the following identity holds:

$$\zeta_K(s) = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} T^m\right) = \frac{f_X(T)}{(1-T)(1-qT)},$$

where $T = q^{-s}$ and $f_X(T) \in \mathbb{Z}[T]$ is the Weil polynomial of X.

Introduction

Now, we are able to formulate results and questions similar to the number field case.

Basic results and questions in the function field case

1. By the Honda-Tate theorem, equality of zeta-functions $\zeta_K = \zeta_{K'}$ is equivalent to the existence of an isogeny between Jacobian varieties of curves corresponding to these function fields.

Introduction

Now, we are able to formulate results and questions similar to the number field case.

Basic results and questions in the function field case

1. By the Honda-Tate theorem, equality of zeta-functions $\zeta_K = \zeta_{K'}$ is equivalent to the existence of an isogeny between Jacobian varieties of curves corresponding to these function fields.
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.

Introduction

Now, we are able to formulate results and questions similar to the number field case.

Basic results and questions in the function field case

1. By the Honda-Tate theorem, equality of zeta-functions $\zeta_K = \zeta_{K'}$ is equivalent to the existence of an isogeny between Jacobian varieties of curves corresponding to these function fields.
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.
3. **We don't know yet** if isomorphism of abelianizations of absolute Galois groups implies isomorphism or for example equality of zeta-functions of function fields!

Introduction

Now, we are able to formulate results and questions similar to the number field case.

Basic results and questions in the function field case

1. By the Honda-Tate theorem, equality of zeta-functions $\zeta_K = \zeta_{K'}$ is equivalent to the existence of an isogeny between Jacobian varieties of curves corresponding to these function fields.
2. Isomorphism of absolute Galois groups(as topological groups) implies isomorphism of fields: $G_K \simeq G_L \Rightarrow K \simeq L$.
3. **We don't know yet** if isomorphism of abelianizations of absolute Galois groups implies isomorphism or for example equality of zeta-functions of function fields!
4. **We don't know** if we could construct finite number of abelian Galois extensions K_i'/K with characters χ_i such that the list of $L_K(\chi_i, s)$ occurs only for that field.

General Settings

Motivated by those results we asked ourselves:

Question

Given a smooth projective curve C over $\mathbb{F}_q$ what could we say about the list of zeta-functions of abelian coverings X of C?

General Settings

Motivated by those results we asked ourselves:

Question

Given a smooth projective curve C over $\mathbb{F}_q$ what could we say about the list of zeta-functions of abelian coverings X of C?

Definition

Let C be a curve over $k = \mathbb{F}_q$ and let d be a natural number prime to p. We define $\mathbb{X}_C(d, g) = \{X$ is a curve over k, such that $g(X) = g$ and there exists an abelian Galois cover $\phi : X \to C$, defined over k and of degree $d\}$.

Remark: Note that according to the theorem of Honda and Tate we have implication: if X is a covering of C, then $\frac{\zeta_X(s)}{\zeta_C(s)} \in \mathbb{Z}[T]$.

General Settings

Remark: Note that according to the theorem of Honda and Tate we have implication: if X is a covering of C, then $\frac{\zeta_X(s)}{\zeta_C(s)} \in \mathbb{Z}[T]$.

Definition

We define $\Lambda_C(d,g) = \{\frac{f_X(T)}{f_C(T)} \in \mathbb{Z}[T] | X \in \mathbb{X}_C(d,g)\}$.

This is finite set of polynomials and we expect to obtain some information about curve C from this set.
Today our main goal is to provide almost complete description for the case $C = E$ is an elliptic curve and $g = 2$, when the characteristic of the ground field $p > 3$.

Case $d > 2$

First of all let us consider case $d > 2$. We have the following result:

Case $d > 2$

First of all let us consider case $d > 2$. We have the following result:

Theorem

For $d > 2$ we have $\Lambda_E(d, 2)$ is empty !

Case $d > 2$

First of all let us consider case $d > 2$. We have the following result:

Theorem

For $d > 2$ we have $\Lambda_E(d, 2)$ is empty !

Sketch of the proof: Suppose that C is an abelian cover of E of degree $d > 2$. Without loss of generality we could suppose that C and E are defined over $\overline{\mathbb{F}_q}$. Since C is a hyper-elliptic curve there exists a unique involution $\tau \in \mathrm{Aut}(C)$ such that $C/\langle\tau\rangle \simeq \mathbb{P}^1$. Moreover, because τ is unique, it lies in the center of $\mathrm{Aut}(C)$ and hence we have the following commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{2} & \mathbb{P}^1 \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ E & \xrightarrow[2]{} & \mathbb{P}^1 \end{array}$$

Case $d > 2$

Let us *apply Riemann-Hurwitz* theorem to the covering $C \to E$.

Case $d > 2$

Let us *apply Riemann-Hurwitz* theorem to the covering $C \to E$. We have:

$$(2g_C - 2) = d(2g_E - 2) + \sum_{p \in C}(e_p - 1),$$

Case $d > 2$

Let us *apply Riemann-Hurwitz* theorem to the covering $C \to E$. We have:

$$(2g_C - 2) = d(2g_E - 2) + \sum_{p \in C}(e_p - 1),$$

and hence:

$$\sum_{p \in C}(e_p - 1) = 2.$$

Case $d > 2$

Let us *apply Riemann-Hurwitz* theorem to the covering $C \to E$. We have:

$$(2g_C - 2) = d(2g_E - 2) + \sum_{p \in C}(e_p - 1),$$

and hence:

$$\sum_{p \in C}(e_p - 1) = 2.$$

Since by assumptions this is a Galois-covering, this means that there are only three possibilities for the ramification divisor: either we have ramification in one point of type $(e_1, e_2) = (2, 2)$, two different points with ramification index $e_i = 2$ or ramification exactly at one point with ramification index $e_1 = 3$. In the first case we have $d = 4$, in the second we have $d = 2$ and finally, in the last case we have $d = 3$. This proves, that $d \leq 4$.

Cases $d = 3$ and $d = 4$ are much more delicate. We have to use Riemann-Hurwitz and some Galois-theory for other coverings in the commutative diagram discussed above.

Cases $d = 3$ and $d = 4$ are much more delicate. We have to use Riemann-Hurwitz and some Galois-theory for other coverings in the commutative diagram discussed above.

□

On the other hand, $\Lambda_E(2, 2)$ provides some interesting information about E.

Preliminaries, the case d=2

Now we are going to discuss the case $d = 2$.
Let E be an elliptic curve over $\mathbb{F}_q$, with characteristic $p > 3$. Let C be a curve of genus $g(C) = 2$ together with the covering map $\phi : C \to E$ of degree 2. Such a curve is called a *biellptic curve*.

Preliminaries, the case d=2

Now we are going to discuss the case $d = 2$.
Let E be an elliptic curve over $\mathbb{F}_q$, with characteristic $p > 3$. Let C be a curve of genus $g(C) = 2$ together with the covering map $\phi : C \to E$ of degree 2. Such a curve is called a *biellptic curve*.

Example

If E is given by the affine equation $y^2 = x^3 + ax + b$, then one could take C with affine part defined by $v^2 = u^6 + au^2 + b$ and map $\phi : (x, y) \to (u^2, v)$.

Preliminaries, the case d=2

Now we are going to discuss the case $d = 2$.
Let E be an elliptic curve over $\mathbb{F}_q$, with characteristic $p > 3$. Let C be a curve of genus $g(C) = 2$ together with the covering map $\phi : C \to E$ of degree 2. Such a curve is called a *biellptic curve*.

Example

If E is given by the affine equation $y^2 = x^3 + ax + b$, then one could take C with affine part defined by $v^2 = u^6 + au^2 + b$ and map $\phi : (x, y) \to (u^2, v)$.

From algebraic geometry we have the following characterization of C:

Theorem

The curve C is bielliptic covering of E if and only if the Jacobian variety $J(C)$ of the curve C is (2,2)-isogenous to a product of two elliptic curves $E \times E'$.

Preliminaries, the case d=2

Theorem

The curve C is bielliiptic covering of E if and only if the Jacobian variety $J(C)$ of the curve C is (2,2)-isogenous to a product of two elliptic curves $E \times E'$.

Now, according to the Honda-Tate theory we have:

$$f_C(T) = f_E(T) f_{E'}(T) = (qT^2 - a_q T + 1)(qT^2 - a'_q T + 1),$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$ and $a'_q = q + 1 - \#E'(\mathbb{F}_q)$. So, to describe $\Lambda_E(2,2)$ it is enough to find all possible values of a'_q.

Preliminaries, the case d=2

Theorem

The curve C is bielliiptic covering of E if and only if the Jacobian variety $J(C)$ of the curve C is (2,2)-isogenous to a product of two elliptic curves $E \times E'$.

Now, according to the Honda-Tate theory we have:

$$f_C(T) = f_E(T) f_{E'}(T) = (qT^2 - a_q T + 1)(qT^2 - a'_q T + 1),$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$ and $a'_q = q + 1 - \#E'(\mathbb{F}_q)$. So, to describe $\Lambda_E(2,2)$ it is enough to find all possible values of a'_q. Our main task is equivalent to the following:

Task

Given an elliptic curve E find all numbers a'_q such that there exists an elliptic curve E' with $a'_q = q + 1 - \#E'(\mathbb{F}_q)$ and with property that abelian surface $E \times E'$ is (2,2)-isogenous to the Jacobian variety of some smooth projective curve C.

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$.

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$. In order to do that we must implement the following algorithm:

1. choose a ramification divisor m of degree 2 on E.

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$. In order to do that we must implement the following algorithm:

1. choose a ramification divisor m of degree 2 on E.
2. take the ray class field $F_{E,m}$ associated to the pair (E, m).

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$. In order to do that we must implement the following algorithm:

1. choose a ramification divisor m of degree 2 on E.
2. take the ray class field $F_{E,m}$ associated to the pair (E, m).
3. take any index two subgroup H of $\mathrm{Gal}(F_{E,m} : F)$, here F is a function field of E.

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$. In order to do that we must implement the following algorithm:

1. choose a ramification divisor m of degree 2 on E.
2. take the ray class field $F_{E,m}$ associated to the pair (E, m).
3. take any index two subgroup H of $\mathrm{Gal}(F_{E,m} : F)$, here F is a function field of E.
4. finally verify that the curve X corresponding to H has genus 2 and calculate its zeta-function.

Examples over $\mathbb{F}_5$

By using explicit class field theory we could calculate all the elements in $\Lambda_E(2,2)$ for any given E over $\mathbb{F}_q$. In order to do that we must implement the following algorithm:

1. choose a ramification divisor m of degree 2 on E.
2. take the ray class field $F_{E,m}$ associated to the pair (E, m).
3. take any index two subgroup H of $\mathrm{Gal}(F_{E,m} : F)$, here F is a function field of E.
4. finally verify that the curve X corresponding to H has genus 2 and calculate its zeta-function.

I've implement this script in Magma.

Examples over $\mathbb{F}_5$

Table : Data for elliptic curves over $\mathbb{F}_5$

Curve E	J-invariant	a_5	Values of a'_5	$\#\,\mathrm{Aut}_k(E)$
$y^2 = x^3 + 1$	0	0	$0; \pm 2; \pm 4$	2
$y^2 = x^3 + 2$	0	0	$0; \pm 2; \pm 4$	2
$y^2 = x^3 + x$	3	2	± 2	4
$y^2 = x^3 + x + 2$	1	2	$0; \pm 2; \pm 4$	2
$y^2 = x^3 + x + 1$	2	-3	$\pm 1; \pm 3$	2
$y^2 = x^3 + 2x$	3	4	$0; \pm 2$	4
$y^2 = x^3 + 2x + 1$	4	-1	$\pm 1; \pm 3$	2
$y^2 = x^3 + 3x$	3	-4	$0; \pm 2$	4
$y^2 = x^3 + 3x + 2$	4	1	$\pm 1; \pm 3$	2
$y^2 = x^3 + 4x$	3	-2	± 2	4
$y^2 = x^3 + 4x + 1$	1	-2	$0; \pm 2; \pm 4$	2
$y^2 = x^3 + 4x + 2$	2	3	$\pm 1; \pm 3$	2

What kind of information we could read from the above table?

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.
2. If a'_p occurs then also $(-a'_p)$ is in the list.

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.
2. If a'_p occurs then also $(-a'_p)$ is in the list.
3. For *general curve* these are the only restrictions.

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.
2. If a'_p occurs then also $(-a'_p)$ is in the list.
3. For *general curve* these are the only restrictions.More contritely, one could note that if $j(E) \neq 0, 1728$ and $E(\mathbb{F}_p)[2]$ is not isomorphic to the full group $C_2 \oplus C_2$ then any $a'_p = a_p \mod (2)$ occurs.

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.
2. If a'_p occurs then also $(-a'_p)$ is in the list.
3. For *general curve* these are the only restrictions.More contritely, one could note that if $j(E) \neq 0, 1728$ and $E(\mathbb{F}_p)[2]$ is not isomorphic to the full group $C_2 \oplus C_2$ then any $a'_p = a_p \mod (2)$ occurs. But if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2)$ consists of all $a'_p = a_p \mod (4)$, still provided we are in the case $j(E) \neq 0, 1728$.

What kind of information we could read from the above table?

1. For any E and E' as above we have $a_p = a'_p \mod (2)$.
2. If a'_p occurs then also $(-a'_p)$ is in the list.
3. For *general curve* these are the only restrictions.More contritely, one could note that if $j(E) \neq 0, 1728$ and $E(\mathbb{F}_p)[2]$ is not isomorphic to the full group $C_2 \oplus C_2$ then any $a'_p = a_p \mod (2)$ occurs. But if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2)$ consists of all $a'_p = a_p \mod (4)$, still provided we are in the case $j(E) \neq 0, 1728$.

Remark: The similar result also holds for curves with $j(E) = 0$ or 1728, but with possibly few exceptions depending on which twist of E are defined over $\mathbb{F}_p$. Also, later we will give an answer for elliptic curves defined over any finite field, not only over $\mathbb{F}_p$.

remarks about the proof

A few words about the proof:

remarks about the proof

A few words about the proof:

1. Easy exercise.

remarks about the proof

A few words about the proof:

1. Easy exercise.
2. Related with quadratic twist of E'.

remarks about the proof

A few words about the proof:

1. Easy exercise.
2. Related with quadratic twist of E'.
3. Requires basic algebraic-geometry construction due to E. Kani and some work with Galois-module structures on torsion points of E.

Now we are going to explain this basic construction.

the basic construction

Let n be a *prime number* with $(n, p) = 1$.

the basic construction

Let n be a *prime number* with $(n, p) = 1$. Given two elliptic curves E and E' with isomorphism α as Galois modules $E[n] \simeq E'[n]$, which is anti-isometry with respect to the Weil-paring.

the basic construction

Let n be a *prime number* with $(n, p) = 1$. Given two elliptic curves E and E' with isomorphism α as Galois modules $E[n] \simeq E'[n]$, which is anti-isometry with respect to the Weil-paring. Let Γ_α be the graph of α in $E \times E'$. Consider surface $A_\alpha \simeq E \times E'/\Gamma_\alpha$. It is (n, n)-isogenous to $E \times E'$.
We have the following commutative diagram:

$$\begin{array}{ccc} E \times E & \xrightarrow{[n]} & \hat{E} \times \hat{E} \\ \downarrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \hat{\phi}} \\ A_\alpha & \longrightarrow & \hat{A}_\alpha \end{array}$$

the basic construction

Let n be a *prime number* with $(n, p) = 1$. Given two elliptic curves E and E' with isomorphism α as Galois modules $E[n] \simeq E'[n]$, which is anti-isometry with respect to the Weil-paring. Let Γ_α be the graph of α in $E \times E'$. Consider surface $A_\alpha \simeq E \times E'/\Gamma_\alpha$. It is (n, n)-isogenous to $E \times E'$.
We have the following commutative diagram:

$$\begin{array}{ccc} E \times E & \xrightarrow{[n]} & \hat{E} \times \hat{E} \\ \downarrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \hat{\phi}} \\ A_\alpha & \longrightarrow & \hat{A}_\alpha \end{array}$$

Moreover, it is turned out that A_α has *principal polarization* θ which comes from polarization on $E \times E'$.

the basic construction

Let n be a *prime number* with $(n, p) = 1$. Given two elliptic curves E and E' with isomorphism α as Galois modules $E[n] \simeq E'[n]$, which is anti-isometry with respect to the Weil-paring. Let Γ_α be the graph of α in $E \times E'$. Consider surface $A_\alpha \simeq E \times E'/\Gamma_\alpha$. It is (n, n)-isogenous to $E \times E'$.
We have the following commutative diagram:

$$\begin{array}{ccc} E \times E & \xrightarrow{[n]} & \hat{E} \times \hat{E} \\ \downarrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \hat{\phi}} \\ A_\alpha & \longrightarrow & \hat{A}_\alpha \end{array}$$

Moreover, it is turned out that A_α has *principal polarization* θ which comes from polarization on $E \times E'$. According to the general theory A_α is a Jacobain surface of some, possible not smooth curve C of (arithmetic) genus two.

Theorem

The curve C constructed above is smooth if and only if the isomorphism α of Galois modules is not the restriction of a geometric isogeny ϕ of degree $i(n-i)$ between $E(\bar{k}) \simeq E'(\bar{k})$, with $0 < i < n$. Moreover, any such C appears in this way.

Theorem

The curve C constructed above is smooth if and only if the isomorphism α of Galois modules is not the restriction of a geometric isogeny ϕ of degree $i(n-i)$ between $E(\bar{k}) \simeq E'(\bar{k})$, with $0 < i < n$. Moreover, any such C appears in this way.

In our case $n = 2$ and hence $i = 1$, but geometric isogeny of degree one is necessary geometric isomorphism!

the basic construction

Theorem

The curve C constructed above is smooth if and only if the isomorphism α of Galois modules is not the restriction of a geometric isogeny ϕ of degree $i(n-i)$ between $E(\bar{k}) \simeq E'(\bar{k})$, with $0 < i < n$. Moreover, any such C appears in this way.

In our case $n = 2$ and hence $i = 1$, but geometric isogeny of degree one is necessary geometric isomorphism! It means that our task is equivalent to the following:

The main task

Given E find all a'_q such that there exists a curve E' with $a'_q = q + 1 - \#E'(\mathbb{F}_q)$ and an isomorphism α between $E[2]$ and $E'[2]$ such that α is not the restriction of a geometric isomorphism between E and E'.

By working with Galois module structure on $E[2]$ we provide a proof of our main theorem.

The main result over $\mathbb{F}_p$

Let E be an elliptic curve over $\mathbb{F}_p$.

Definition

1. $A_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (2)\}$;
2. $B_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (4)\}$.

The main result over $\mathbb{F}_p$

Let E be an elliptic curve over $\mathbb{F}_p$.

Definition

1. $A_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (2)\}$;
2. $B_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (4)\}$.

Theorem

Suppose E is an elliptic curve over F_p with $j(E) \neq 0, 1728$ and $p > 3$. Then:

1. *if $E(\mathbb{F}_p)[2] \not\simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = A_E$;*
2. *if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = B_E$;*

The main result over $\mathbb{F}_p$

Let E be an elliptic curve over $\mathbb{F}_p$.

Definition

1. $A_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (2)\}$;
2. $B_E = \{(pT^2 - a'_pT + 1)$, for $a'_p \in [-2\sqrt{p}; 2\sqrt{p}] \cap \mathbb{Z}$, $a_p = a'_p \mod (4)\}$.

Theorem

Suppose E is an elliptic curve over F_p with $j(E) \neq 0, 1728$ and $p > 3$. Then:

1. *if $E(\mathbb{F}_p)[2] \not\simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = A_E$;*
2. *if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = B_E$;*

Remark: The similar result holds also for the case $j(E) = 0$ or $j(E) = 1728$, but with possibly few exceptions.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$. Suppose $\#E(\mathbb{F}_p) = 1 \mod (2)$, then $E(\mathbb{F}_p)[2] = \{0\}$.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$. Suppose $\#E(\mathbb{F}_p) = 1 \mod (2)$, then $E(\mathbb{F}_p)[2] = \{0\}$. Therefore Galois-module structure on E is C_3, meaning that π switches three other 2-torsion points by circle.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$. Suppose $\#E(\mathbb{F}_p) = 1 \mod (2)$, then $E(\mathbb{F}_p)[2] = \{0\}$. Therefore Galois-module structure on E is C_3, meaning that π switches three other 2-torsion points by circle. Hence for any two such curves we have an isomorphism of $E[2]$ as Galois-modules.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$. Suppose $\#E(\mathbb{F}_p) = 1 \mod (2)$, then $E(\mathbb{F}_p)[2] = \{0\}$. Therefore Galois-module structure on E is C_3, meaning that π switches three other 2-torsion points by circle. Hence for any two such curves we have an isomorphism of $E[2]$ as Galois-modules.
Now if $a'_p = 1 \mod (2)$ is a number in a Hasse interval $[-2\sqrt{p}; 2\sqrt{p}]$ then there exists an elliptic curve E' with isomorphism $\alpha : E[2] \simeq E'[2]$ as Galois-modules. The existence of E' is guarantee by the theorem due to Waterhouse.

Idea of the proof

Let us sketch important steps of the proof. We know that $\mathrm{Gal}(k^{sep} : k)$ is generated by the frobenious element π. Suppose E is an elliptic curve $\mathbb{F}_p$ with $p > 3$ such that and $j(E) \neq 0, 1728$. Suppose $\#E(\mathbb{F}_p) = 1 \mod (2)$, then $E(\mathbb{F}_p)[2] = \{0\}$. Therefore Galois-module structure on E is C_3, meaning that π switches three other 2-torsion points by circle. Hence for any two such curves we have an isomorphism of $E[2]$ as Galois-modules.
Now if $a'_p = 1 \mod (2)$ is a number in a Hasse interval $[-2\sqrt{p}; 2\sqrt{p}]$ then there exists an elliptic curve E' with isomorphism $\alpha : E[2] \simeq E'[2]$ as Galois-modules. The existence of E' is guarantee by the theorem due to Waterhouse.
Finally, if $j(E) \neq 0, 1728$ then $\mathrm{Aut}(E) = \{\pm 1\}$ which acts trivially on two-torsion points. But the same time, we always have non-trivial isomorphism of Galois-modules in this case. This proves that there exists a smooth project curve C with $\mathrm{Jac}(C)$ (2,2)-isogenous to the product of E and E'.

Idea of the proof

Suppose $a'_p = 0 \mod (2)$ then also $\#E(\mathbb{F}_p) = 0 \mod (2)$. There are two cases:

1. $\#E(\mathbb{F}_p) = 0 \mod (4)$, hence $E(\mathbb{F}_p)[2] \simeq C_2$ or $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$;

Idea of the proof

Suppose $a'_p = 0 \mod (2)$ then also $\#E(\mathbb{F}_p) = 0 \mod (2)$. There are two cases:

1. $\#E(\mathbb{F}_p) = 0 \mod (4)$, hence $E(\mathbb{F}_p)[2] \simeq C_2$ or $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$;
2. $\#E(\mathbb{F}_p) = 2 \mod (4)$, hence $E(\mathbb{F}_p)[2] \simeq C_2$;

A priori we have a problem with case when $\#E(\mathbb{F}_p) = 0 \mod (4)$. We will show that with one little exception both two-torsion structures occurs in a given isogeny class!

Idea of the proof

We have the following lemma which shows that actually almost always both cases occurs in the given isogeny class:

Theorem

Given elliptic curve E over $\mathbb{F}_q$ such that $4|\#E(\mathbb{F}_q)$ we have:

1. *if $a_q \neq \pm 2\sqrt{q}$, then in the isogeny class corresponding to E there exist elliptic curves E', E'' with $E'(\mathbb{F}_q)[2] = C_2$ and $E''(\mathbb{F}_q)[2] = C_2 \oplus C_2$;*
2. *if $a_q = \pm 2\sqrt{q}$, then any elliptic curve E' isogenous to E has $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$.*

Idea of the proof

We have the following lemma which shows that actually almost always both cases occurs in the given isogeny class:

Theorem

Given elliptic curve E over $\mathbb{F}_q$ such that $4|\#E(\mathbb{F}_q)$ we have:

1. *if $a_q \neq \pm 2\sqrt{q}$, then in the isogeny class corresponding to E there exist elliptic curves E', E'' with $E'(\mathbb{F}_q)[2] = C_2$ and $E''(\mathbb{F}_q)[2] = C_2 \oplus C_2$;*
2. *if $a_q = \pm 2\sqrt{q}$, then any elliptic curve E' isogenous to E has $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$.*

It means we are done! □

Idea of the proof

We have the following lemma which shows that actually almost always both cases occurs in the given isogeny class:

Theorem

Given elliptic curve E over $\mathbb{F}_q$ such that $4|\#E(\mathbb{F}_q)$ we have:

1. *if $a_q \neq \pm 2\sqrt{q}$, then in the isogeny class corresponding to E there exist elliptic curves E', E'' with $E'(\mathbb{F}_q)[2] = C_2$ and $E''(\mathbb{F}_q)[2] = C_2 \oplus C_2$;*
2. *if $a_q = \pm 2\sqrt{q}$, then any elliptic curve E' isogenous to E has $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$.*

It means we are done! □

Remark: Cases with $j(E) = 0, 1728$ are a little bit more delicate.

What about general case?

Now we are able to generalize our result to any finite field $k = \mathbb{F}_q$.

What about general case?

Now we are able to generalize our result to any finite field $k = \mathbb{F}_q$.

Definition

We will call an integer number N in the Hasse interval $[-2\sqrt{q}; 2\sqrt{q}]$ admissible if there exists an elliptic curve E over $\mathbb{F}_q$ with $a_q = q + 1 - \#E(\mathbb{F}_q) = N$.

Theorem of Waterhouse provides a precise answer witch numbers are admissible:

Theorem

The number N is admissible if and only if one of the following conditions holds:

1. (p;N)=1;
2. if $q = p^{2n+1}$ and one of the following holds:
   1. N=0;
   2. $N = \pm 2^{n+1}$, $p = 2$;
   3. $N = \pm 3^{n+1}$, $p = 3$;
3. if $q = p^{2n}$ and one of the following holds:
   1. $N = \pm 2p^n$;
   2. $N = \pm p^n$, $p \neq 1 \mod (3)$;
   3. $N = 0$, $p \neq 1 \mod (4)$;

Definition

1. $A_E = \{(qT^2 - a'_q T + 1)$, for a'_q is an admissible such that $a_q = a'_q \mod (2)\}$;
2. $B_E = \{(qT^2 - a'_q T + 1)$, for a'_q is an admissible such that $a_q = a'_q \mod (4)\}$.

Definition

1. $A_E = \{(qT^2 - a'_q T + 1)$, for a'_q is an admissible such that $a_q = a'_q \mod (2)\}$;
2. $B_E = \{(qT^2 - a'_q T + 1)$, for a'_q is an admissible such that $a_q = a'_q \mod (4)\}$.

Theorem

Suppose E is an elliptic curve over F_q with $j(E) \neq 0, 1728$ and $p > 3$. Then:

1. *if $E(\mathbb{F}_q)[2] \simeq \{0\}$ then $\Lambda_E(2,2) = A_E$;*
2. *if $E(\mathbb{F}_q)[2] \simeq C_2$ then $\Lambda_E(2,2) = A_E/\{qT^2 \pm 2\sqrt{q}T + 1\}$;*
3. *if $E(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = B_E$;*

Remark: The similar result holds also for the case $j(E) = 0$ or $j(E) = 1728$, but with possibly few exceptions. This exceptions occur if and only if in the isogeny class corresponding to a'_q for any pair (E', α) we have that isomorphism $\alpha : E'[2] \simeq E[2]$ comes from the restriction of a geometric isomorphism between E and E'.

Thank you!