L-Polynomials of Curves over Finite Fields

Gary McGuire

School of Mathematical Sciences
University College Dublin
Ireland

July 2015
12th Finite Fields and their Applications Conference

Introduction

This talk is about when the L-polynomial of one curve divides the L-polynomial of another curve.

We will discuss L-polynomials, and present one theorem.

Intermission (some philosophy)

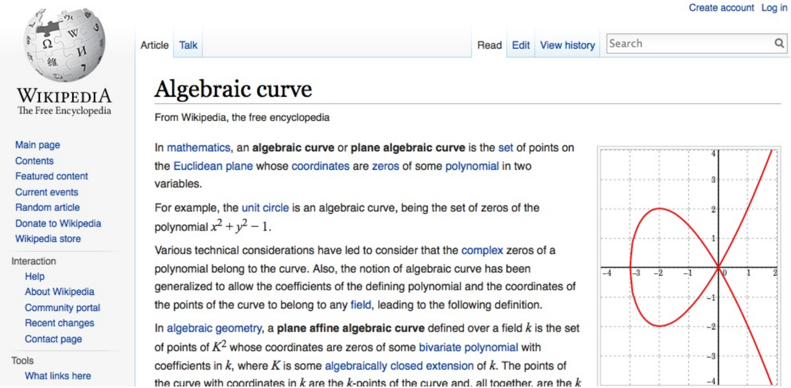
We will then take a detour into Linear Recurring Sequences and use some results from there to prove another theorem.

Based on two papers:
– Omran Ahmadi, Gary McGuire, proceedings BCC 2015.
– Omran Ahmadi, Gary McGuire, Antonio Rojas Leon, Decomposing Jacobians of Curves over Finite Fields in the Absence of Algebraic Structure, J Number Theory, Nov 2015.

Curves

Curves in the plane are given by polynomial equations like

$$y = f(x) \text{ or } y^2 = f(x) \text{ or } f(x,y) = 0.$$



Algebraic curve

From Wikipedia, the free encyclopedia

In mathematics, an **algebraic curve** or **plane algebraic curve** is the set of points on the Euclidean plane whose coordinates are zeros of some polynomial in two variables.

For example, the unit circle is an algebraic curve, being the set of zeros of the polynomial $x^2 + y^2 - 1$.

Various technical considerations have led to consider that the complex zeros of a polynomial belong to the curve. Also, the notion of algebraic curve has been generalized to allow the coefficients of the defining polynomial and the coordinates of the points of the curve to belong to any field, leading to the following definition.

In algebraic geometry, a **plane affine algebraic curve** defined over a field k is the set of points of K^2 whose coordinates are zeros of some bivariate polynomial with coefficients in k, where K is some algebraically closed extension of k. The points of the curve with coordinates in k are the k-points of the curve and, all together, are the k

Curves

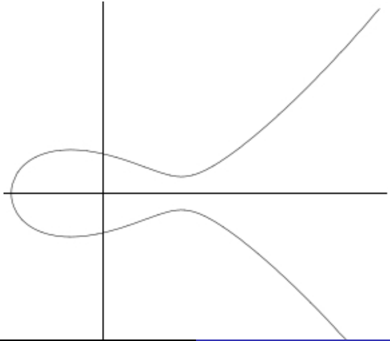
Curves in the plane are given by polynomial equations like

$$y = f(x) \text{ or } y^2 = f(x) \text{ or } f(x,y) = 0.$$

If the curve is smooth, and $f(x,y)$ has degree d, then the genus of the curve is

$$g = \frac{(d-1)(d-2)}{2}$$

Example: curve of genus 1, over the real numbers, $y^2 =$ cubic in x

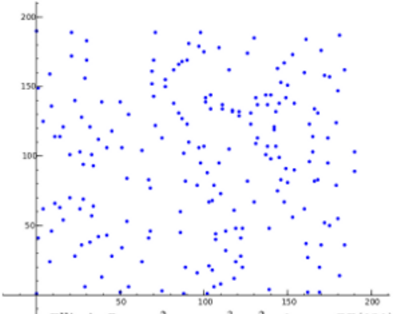


Finite Fields

Let $q = p^n$ where p is a prime number.

There is a finite field with q elements, denoted $\mathbb{F}_q$ or $GF(q)$.

For any $n \geq 1$, $\mathbb{F}_q$ has an extension field of degree n, denoted $\mathbb{F}_{q^n}$.



Elliptic Curve $y^2 + xy = x^3 + x^2 + 1$ over $GF(191)$

Let $C = C(\mathbb{F}_q)$ be a (projective, smooth, absolutely irreducible) algebraic curve of genus g defined over $\mathbb{F}_q$.
e.g. a plane curve, $f \in \mathbb{F}_q[x, y]$

$$C(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x, y) = 0\} \cup \{\infty\}$$

For any $n \geq 1$ let $C(\mathbb{F}_{q^n})$ be the set of $\mathbb{F}_{q^n}$-rational points of C:

$$C(\mathbb{F}_{q^n}) = \{(x, y) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} : f(x, y) = 0\} \cup \{\infty\}$$

and let $\#C(\mathbb{F}_{q^n})$ be the cardinality of this set.

Example: $f(x, y) = y^2 + y - x^3 = 0$ defined over $\mathbb{F}_2$.
$C(\mathbb{F}_2) = \{(0, 0), (0, 1), \infty\}$ $\qquad \#C(\mathbb{F}_2) = 3$
$C(\mathbb{F}_4) = \{(0, 0), (0, 1), (1, \alpha), \cdots\}$ $\qquad \#C(\mathbb{F}_4) = 9$
$C(\mathbb{F}_8) = \{(0, 0), (0, 1), \cdots\}$ $\qquad \#C(\mathbb{F}_8) = 9$

We want to study these numbers $\quad \#C(\mathbb{F}_{q^n}), \ n \geq 1.$

$$\#C(\mathbb{F}_q), \ \#C(\mathbb{F}_{q^2}), \ \#C(\mathbb{F}_{q^3}), \ \#C(\mathbb{F}_{q^4}), \ \#C(\mathbb{F}_{q^5}), \ \#C(\mathbb{F}_{q^6}), \ldots$$

The zeta function of $C(\mathbb{F}_q)$ is defined by

$$Z_C(t) = exp\left(\sum_{n\geq 1} \# C(\mathbb{F}_{q^n})\frac{t^n}{n}\right) \in \mathbb{Q}[[t]].$$

It can be shown (Schmidt 1931) that

$$Z_C(t) = \frac{L_C(t)}{(1-t)(1-qt)}$$

where $L_C(t) \in \mathbb{Z}[t]$ (called the L-Polynomial of C) is of degree $2g$.

First consequence: Zeta function is a finite object!
$L_C(t)$ contains all the information.

Second consequence

$$Z_C(t) = exp\left(\sum_{n\geq 1} \#C(\mathbb{F}_{q^n})\frac{t^n}{n}\right) = \frac{L_C(t)}{(1-t)(1-qt)}$$

Taking logs (and doing easy rearrangements) gives

$$\log L_C(t) = \sum_{n\geq 1}(\#C(\mathbb{F}_{q^n}) - q^n - 1)\frac{t^n}{n} \tag{1}$$

It is more natural to study these numbers

$$a_n := \#C(\mathbb{F}_{q^n}) - (q^n + 1).$$

Write

$$L_C(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$$

and then taking logs and substituting in (1) gives

$$a_n := \#C(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$$

Hasse-Weil

$$a_n := \#C(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$$

We don't need this but...
The zeta function satisfies a functional equation, and $|\alpha_i| = \sqrt{q}$.
The Hasse-Weil bound follows immediately

$$|a_n| \leq 2gq^{n/2}$$

When $g = 1$: it can be shown that $L_C(t) = qt^2 + c_1 t + 1$, where $c_1 = \#C(\mathbb{F}_q) - (q + 1)$.

So for genus 1, the L-polynomial is equivalent to $\#C(\mathbb{F}_q)$.
All the $\#C(\mathbb{F}_{q^n})$ are determined by $\#C(\mathbb{F}_q)$.

When $g = 2$: we must have $L_C(t) = q^2t^4 + qc_1t^3 + c_2t^2 + c_1t + 1$ where $c_1 = \#C(\mathbb{F}_q) - (q + 1)$, and $2c_2 = \#C(\mathbb{F}_{q^2}) - (q^2 + 1) + c_1^2$.

So for genus 2, the L-polynomial is equivalent to $\#C(\mathbb{F}_q)$ and $\#C(\mathbb{F}_{q^2})$.

In general, the coefficients of the L-polynomial are determined by $\#C(\mathbb{F}_{q^n})$ for $n = 1, 2, \ldots, g$.

Back to the point..

Example: Over $\mathbb{F}_2$ the curve $C_1 : y^2 + y = x^3 + x$ has L-polynomial $2t^2 + 2t + 1$

Example: The curve $C_2 : y^2 + y = x^5 + x$
has genus 2 and L-polynomial

$$4t^4 + 2t^3 + 4t^2 + 2t + 1 = (2t^2 + 2t + 1)(2t^2 + 1).$$

Question for this talk: Does it mean anything if the L-polynomial of one curve divides the L-polynomial of another curve?

It's not hard to show that these curves have the same number of rational points over $\mathbb{F}_{2^n}$ for all odd n.

First Observation

Theorem

Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume that there exists a positive integer $k > 1$ such that $L_D(t) = q(t^k)L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$. Then $\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k.

Sketch: Recall

$$\log L_C(t) = \sum_{m \geq 1} (\#C(\mathbb{F}_{q^m}) - 1 - q^m)\frac{t^m}{m}.$$

From $L_D(t) = q(t^k)L_C(t)$ we have

$$\log L_D(t) = \log q(t^k) + \log L_C(t).$$

Formal power series for log finishes the proof.

Could the converse be true??

Recent Work

All L-polynomials are over $\mathbb{F}_q$.

Theorem (from previous slide)

Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume that there exists a positive integer $k > 1$ such that $L_D(t) = q(t^k)\ L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$. Then $\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k.

Theorem (Ahmadi-M-Rojas Leon, J Number Theory 2015)

Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume there exists a positive integer $k > 1$ such that

1. *$\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k, and*
2. *the k-th powers of the roots of $L_C(t)$ are all distinct.*

Then $L_D(t) = q(t^k)\ L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$.

We remark that the theorem is no longer true when we replace the first hypothesis
“for every m that is not divisible by k”
with the weaker hypothesis
“for every m with $\gcd(m, k) = 1$.”

A counterexample is given in our paper.

Further examples

Example: Over $\mathbb{F}_2$ consider the family of curves ($k \geq 1$)

$$C_k : y^2 + y = x^{2^k+1} + x$$

The first five L-polynomials, computed and factored over $\mathbb{Z}$ using MAGMA, are

$C_1 : 2t^2 + 2t + 1$
$C_2 : (2t^2 + 2t + 1)(2t^2 + 1)$
$C_3 : (2t^2 + 2t + 1)(8t^6 + 4t^3 + 1)$
$C_4 : (2t^2+2t+1)(128t^{14}+64t^{12}+32t^{10}+16t^8+8t^6+4t^4+2t^2+1)$
$C_5 : (2t^2 + 2t + 1)(32768t^{30} + 8192t^{25} + 1024t^{20} + 32t^{10} + 8t^5 + 1)$

Known approaches to proving divisibility of L-polynomials

Theorem (Kleiman, Serre)

If there is a morphism of curves $C \longrightarrow D$ that is defined over $\mathbb{F}_q$ then $L_D(t)$ divides $L_C(t)$.

Example: Over $\mathbb{F}_2$ the map

$$(x, y) \longrightarrow (x^2 + x, y + x^3 + x^2)$$

is a morphism from

$$C_2 : y^2 + y = x^5 + x \quad \longrightarrow \quad C_1 : y^2 + y = x^3 + x$$

The L-polynomials are $2t^2 + 2t + 1$ and $(2t^2 + 2t + 1)(2t^2 + 1)$.

Kleiman-Serre doesn't always apply

Curves over $\mathbb{F}_2$

$$D_1 : y^2 + xy = x^5 + x.$$

has L-polynomial $\quad 4t^4 + 2t^3 + t + 1$

$$D_2 : y^2 + xy = x^7 + x.$$

has L-polynomial $\quad (4t^4 + 2t^3 + t + 1)(2t^2 + 1)$

We can prove that there is no map $D_2 \longrightarrow D_1$.
And yet.... there is divisibility.

Kani-Rosen, also doesn't always apply

In the special case where $Aut(C)$ contains the Klein 4-group G with subgroups H_1, H_2, H_3, the Kani-Rosen theorem implies an isogeny which implies the following L-polynomial relation

$$L_C(t)\ L_{C/G}(t)^2 = L_{C/H_1}(t)\ L_{C/H_2}(t)\ L_{C/H_3}(t).$$

Example: same curves over $\mathbb{F}_2$

$$D_1 : y^2 + xy = x^5 + x.$$

has L-polynomial $\quad 4t^4 + 2t^3 + t + 1$

$$D_2 : y^2 + xy = x^7 + x.$$

has L-polynomial $\quad (4t^4 + 2t^3 + t + 1)(2t^2 + 1)$

The automorphism groups have order 2 (Poonen).
And yet.... there is divisibility.

Some Philosophy and Context

Can $\#C(\mathbb{F}_q) = \#D(\mathbb{F}_q)$ be a coincidence ?
How might we explain $\#C(\mathbb{F}_q) = \#D(\mathbb{F}_q)$?

If there is an appropriate map between the curves, an "algebraic reason", then it's not a coincidence that $\#C(\mathbb{F}_q) = \#D(\mathbb{F}_q)$.

If there is no relationship, no connection between C and D, it's a combinatorial accident.

For curves of genus 1, a theorem of Tate says there are no accidents:

Tate: Two elliptic curves have same number of $\mathbb{F}_q$ points if and only if there is an $\mathbb{F}_q$ isogeny from one to the other.

Higher Genus Curves over Finite Fields, Jacobians

Let C be a nonsingular projective curve of genus g over $\mathbb{F}_q$.
The Jacobian of C is isomorphic as a group to the divisor class group $\mathrm{Pic}^0(C)$.
($\mathrm{Pic}^0(C) =$ Degree 0 divisors modulo principal divisors)

Arithmetic is governed by the Riemann-Roch theorem.
The Jacobian is a variety, an abelian (group) variety.

The Frobenius automorphism of $\mathbb{F}_q$ induces an endomorphism π of a $2g$-dimensional $\mathbb{Q}_\ell$-vector space (namely $T_\ell(Jac(C)) \otimes \mathbb{Q}_\ell$ where $T_\ell(Jac(C))$ is the ℓ-adic Tate module, where $\ell \neq p$ is prime).

So π has a characteristic polynomial of degree $2g$. Call it $\chi_C(t)$.
Weil showed that $\chi_C(t)$ is the reciprocal of $L_C(t)$.

Point counting algorithms find $\chi_C(t)$, use $|Jac(C)| = \chi_C(1)$.

Coincidence?

Theorem (Tate)

$L_C(t)$ divides $L_D(t)$ if and only if the Jacobian of $D(\mathbb{F}_q)$ has a subvariety isogenous to the Jacobian of $C(\mathbb{F}_q)$.

For genus 1 curves

$$\text{Same number } \mathbb{F}_q \text{ points} \iff \text{isogeny between curves}$$

For higher genus curves, we ask (using Tate)

"Same number points over infinitely many extensions"

$$? \iff ?$$

isogeny between Jacobians

Part 2: Linear Recurring Sequences

A linear recurring sequence of order d is a sequence of integers $A = (a_n)_{n\geq 1}$ satisfying the homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_d a_{n-d} \text{ for } n \geq d+1,$$

where $c_1, \ldots, c_d$ are integers, $c_d \neq 0$.
The recurrence and the initial values $a_1, \ldots, a_d$ determine the complete infinite sequence.
The *characteristic polynomial* of the sequence defined by this recursion is the polynomial

$$\chi(t) = t^d - c_1 t^{d-1} - \cdots - c_{d-1} t - c_d \in \mathbb{Z}[t].$$

This does not depend on the initial values.
The characteristic polynomial of smallest degree is called the minimal polynomial.

A Well Known Theorem

Theorem

Let $\chi(t) = t^d - c_1 t^{d-1} - \cdots - c_{d-1}t - c_d$ be a polynomial with $c_d \neq 0$. Factor $\chi(t)$ as

$$\chi(t) = \prod_{i=1}^{r} (t - \alpha_i)^{m_i}$$

over $\overline{\mathbb{Q}}$, where the α_i are distinct, and the m_i are positive integers. Then a sequence $(a_n)_{n\geq 1}$ satisfies the linear recurrence with characteristic polynomial $\chi(t)$ if and only if there exist polynomials $P_1(n), P_2(n), \ldots, P_r(n)$, where $P_i(n)$ has degree $\leq m_i - 1$, such that

$$a_n = \sum_{i=1}^{r} P_i(n)\alpha_i^n \quad \textit{for every } n \geq 1.$$

The Sequence of a Curve

Write $L_C(t) = 1 + c_1 t + \cdots + c_{2g-1} t^{2g-1} + q^g t^{2g}$.
Denote the reciprocal polynomial of the L-polynomial of $C(\mathbb{F}_q)$ as $\chi_C(t) = t^{2g} + c_1 t^{2g-1} + \cdots + c_{2g-1} t + q^g$.

Write

$$\chi_C(t) = \prod_{i=1}^{2g} (t - \alpha_i), \quad L_C(t) = \prod_{i=1}^{2g} (1 - \alpha_i t),$$

the α_i are called the Frobenius eigenvalues of $C(\mathbb{F}_q)$.
The 'trace of Frobenius' is $c_1 = -\sum_{i=1}^{2g} \alpha_i = \#C(\mathbb{F}_q) - (q+1)$.
As we saw earlier the L-polynomial of $C(\mathbb{F}_{q^n})$ is $\prod_{i=1}^{2g}(1 - \alpha_i^n t)$, and thus

$$\#C(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$$

Given a curve C defined over $\mathbb{F}_q$, the sequence of C is

$$a_n := \#C(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$$

By the Well Known Theorem this is a linear recurring sequence of integers.

What does the theory of linear recurring sequences say about a_n? e.g. What is the characteristic polynomial?

Theorem

The characteristic polynomial of the sequence of C is $\chi_C(t)$, the reciprocal polynomial of the L-polynomial of C.

Proof: This follows from the Well Known Theorem.

Example: $C_1 : y^2 + y = x^3 + x$ over $\mathbb{F}_2$ (curve of genus 1)
The L-polynomial of C_1 is $2t^2 + 2t + 1$.
The characteristic polynomial is $\chi_C(t) = t^2 + 2t + 2$.
So $a_n = -2a_{n-1} - 2a_{n-2}$ is the recursion.
With the two initial values $a_1 = -2, a_2 = 0$, the sequence of C_1:

$$-2, 0, 4, -8, 8, 0, -16, 32, -32, 0, 64, -128, 128, 0, -256, 512...$$

Subsequences

Consider subsequences in arithmetic progressions, $a_s, a_{2s}, a_{3s}, \ldots$ where $s > 1$ is a fixed positive integer.

Theorem

Let $(a_n)_{n \geq 1}$ be a linear recurring sequence with characteristic polynomial $\chi(t)$. Let $s > 1$ be a positive integer.
Then the characteristic polynomial of the subsequence $(a_{sn+j})_{n \geq 1}$ is the polynomial whose roots are the s-th powers of the roots of $\chi(t)$.

(This requires that the roots and their s-th powers be distinct.)

Subsequences

For the sequence $(a_n)_{n\geq 1}$ of a curve C defined over $\mathbb{F}_q$...

the subsequence $(a_{sn})_{n\geq 1}$ gives the numbers of rational points on C over $\mathbb{F}_{q^s}$ and all its extensions, which is equivalent to the L-polynomial of $C(\mathbb{F}_{q^s})$.

$$\#C(\mathbb{F}_q), \ldots, \ \#C(\mathbb{F}_{q^s}), \ \ldots, \ \#C(\mathbb{F}_{q^{2s}}), \ldots$$

Therefore, if $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ is the L-polynomial of $C(\mathbb{F}_q)$, it follows from the above Theorem that
the L-polynomial of $C(\mathbb{F}_{q^s})$ is $\prod_{i=1}^{2g}(1 - \alpha_i^s t)$.

The Skolem-Mahler-Lech Theorem

We use the following theorem.

Theorem (Skolem-Mahler-Lech)

Let A be a linear recurrence sequence of integers. If A contains infinitely many zeros, then the set of indices n for which $a_n = 0$ is the union of a finite set and a finite number of arithmetic progressions.

Proof is not elementary. See blog by Terence Tao, or "Zeros of Integer Linear Recurrences" by Daniel Litt.

Apart from the finite set, this says that the zeros must occur in subsequences $(a_{sn+j})_{n\geq 1}$.

Theorem (Ahmadi-M)

Let $C(\mathbb{F}_q)$ and $D(\mathbb{F}_q)$ be a smooth projective curves such that

1. *$C(\mathbb{F}_q)$ and $D(\mathbb{F}_q)$ have the same number of points over infinitely many extensions of $\mathbb{F}_q$.*
2. *The L-polynomial of C over $\mathbb{F}_{q^k}$ has no repeated roots, for all $k \geq 1$.*

Then there exists a positive integer s such that the L-polynomial of $D(\mathbb{F}_{q^s})$ is divisible by the L-polynomial of $C(\mathbb{F}_{q^s})$.

Sketch Proof: Let $a_n =$ sequence for C, let $b_n =$ sequence for D.
The Skolem-Mahler-Lech theorem implies that the n for which $a_n = b_n$ form a union of arithmetic progressions.
So $a_{ns+j} = b_{ns+j}$ for all $n \geq 1$.
So these subsequences have the same minimal polynomial, which is the L-polynomial over $\mathbb{F}_{q^s}$. Now finish.

Clearly the value of the positive integer s is of interest.
Often $s = 1$.

However be careful, s cannot always be 1:
Let C_1 be an elliptic curve with L-polynomial $qt^2 + at + 1$
Let C_2 be its quadratic twist, with L-polynomial $qt^2 - at + 1$.
An elliptic curve and its quadratic twist are isomorphic over $\mathbb{F}_{q^2}$.
In this case $s = 2$.
Here is a case when we can prove $s = 1$.

Theorem

Let q be odd. Same hypotheses, plus let M be the splitting field of the characteristic polynomial $\chi_D(t)$, and suppose that the ideal (2) splits completely in M. Then $s = 1$.

Referring to elliptic curves, for an elliptic curve E with $\chi_E(t) = t^2 + at + q$, the ideal (2) never splits completely in the splitting field $M = \mathbb{Q}(\sqrt{a^2 - 4q})$ because $a^2 - 4q$ cannot be 1 modulo 8.

Future Work

Can these theorems be strengthened?

What are iff conditions for $L_C(t)$ to divide $L_D(t)$?
(We gave iff conditions when $L_D(t)/L_C(t)$ is a polynomial in t^k.)

For the family of curves over $\mathbb{F}_2$

$$C_k : y^2 + y = x^{2^k+1} + x$$

Conjecture: L-polynomial of C_1 divides L-polynomial of C_k
(proved by Robin Chapman)

For

$$D_k : y^2 + xy = x^{2^k+3} + x$$

Conjecture: L-polynomial of D_1 divides L-polynomial of D_k
Conjecture: D_1 and D_k have the same number of points over infinitely many extensions.

An morphism of curves is an algebraic map that is defined everywhere.

Let A, A' be abelian varieties of dimension g over K. An isogeny $\eta : A \longrightarrow A'$ is a K-rational homomorphism (a morphism of varieties compatible with the addition morphisms on A and A') whose kernel is a finite group scheme.

Proof ideas...

By hypothesis, there exists a positive integer k such that

$$\sum_{i=1}^{2g(C)} \alpha_i^m = \sum_{j=1}^{2g(D)} \beta_j^m$$

for every m with $k \nmid m$. This gives an equality of certain zeta functions, namely

$$\exp\left(\sum_{m:k\nmid m} \sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m}\right)$$

The difference between this and a usual zeta function is

$$\sum_{m:k|m} \sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m} = \sum_{m} \sum_{i=1}^{2g(C)} \alpha_i^{km} \frac{t^{km}}{km}$$

which can be viewed as a zeta function over an extension field.

Using Kani-Rosen and automorphisms from van der Geer-van der Vlugt, MAGMA computes the L-polynomials of quotient curves of C_6 to be

$$(2t^2-1)^2(2t^2+1)^4(4t^4-2t^2+1)^3(4t^4+2t^2+1)^2$$

and

$$(2t^2-2t+1)^3(2t^2+2t+1)^3(4t^4-4t^3+2t^2-2t+1)^2(4t^4+4t^3+2t^2+2t+1)^3$$

The L-polynomial of C_6 is the product of these.