Counting Points on Curves of the Form $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$

Matthew Hase-Liu
Mentor: Nicholas Triantafillou

Sixth Annual Primes Conference

21 May 2016

Curves

Definition

A plane algebraic curve is defined as the set of points in a plane consisting of the zeroes of some polynomial in two variables.

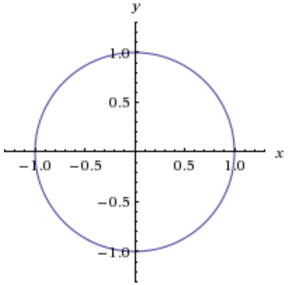
Curves

Definition

A plane algebraic curve is defined as the set of points in a plane consisting of the zeroes of some polynomial in two variables.

Example

$x^2 + y^2 = 1$ over $\mathbb{R}^2$:



Curves

Consider points with integer coordinates modulo a prime.

Curves

Consider points with integer coordinates modulo a prime.

Definition

$\mathbb{F}_p$ is the set of elements that consist of the integers modulo a prime p.

Remark

If you know what a field is, we are looking at plane algebraic curves over the finite field $\mathbb{F}_p$.

Curves

Consider points with integer coordinates modulo a prime.

Definition

$\mathbb{F}_p$ is the set of elements that consist of the integers modulo a prime p.

Remark

If you know what a field is, we are looking at plane algebraic curves over the finite field $\mathbb{F}_p$.

Definition

Given a curve C, define $C(\mathbb{F}_p)$ as the points that satisfy $C(x, y) = 0$, along with points at infinity.

Curves

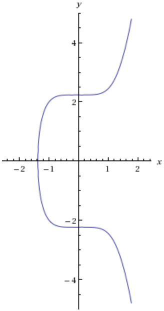
- Well-known curves
  - Elliptic curves: $y^2 = x^3 + ax + b$
  - Hyperelliptic curves: $y^2 = f(x)$, where $\deg(f) > 4$
  - Superelliptic curves: $y^m = f(x)$

Curves

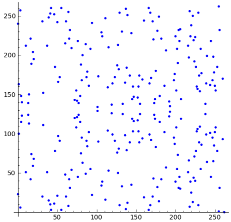
- Well-known curves
  - Elliptic curves: $y^2 = x^3 + ax + b$
  - Hyperelliptic curves: $y^2 = f(x)$, where $\deg(f) > 4$
  - Superelliptic curves: $y^m = f(x)$
- Curve of interest: $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$ (trinomial curve)

Curves

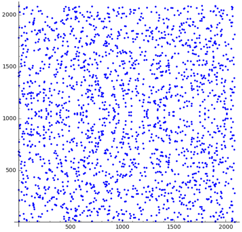
- Well-known curves
  - Elliptic curves: $y^2 = x^3 + ax + b$
  - Hyperelliptic curves: $y^2 = f(x)$, where $\deg(f) > 4$
  - Superelliptic curves: $y^m = f(x)$
- Curve of interest: $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$ (trinomial curve)



$y^2 = x^5 + 5$



$y^2 = x^3 + 2x + 3\ (\mathbb{F}_{263})$



$y^2 = x^3 + 2x + 3\ (\mathbb{F}_{2089})$

Main Problem

Main Problem

What is $\#C(\mathbb{F}_p)$?

Main Problem

Main Problem

What is $\#C\left(\mathbb{F}_p\right)$?

Theorem (Hasse-Weil bound)

Let C be the curve of interest: $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$. Then,

$$\left|\#C\left(\mathbb{F}_p\right) - p - 1\right| \leq 2g\sqrt{p},$$

where g is some polynomial function of m_1, m_2, n_1, and n_2.

Main Problem

Main Problem

What is $\#C(\mathbb{F}_p)$?

Theorem (Hasse-Weil bound)

Let C be the curve of interest: $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$. Then,

$$|\#C(\mathbb{F}_p) - p - 1| \leq 2g\sqrt{p},$$

where g is some polynomial function of m_1, m_2, n_1, and n_2.

Idea

If p is large, then all we need is $\#C(\mathbb{F}_p) \pmod{p}$.

Main Problem

Main Problem

What is $\#C(\mathbb{F}_p)$?

- Naïve approach: try all values of $(x, y) \in \mathbb{F}_p^2$ (very slow)
- Better approach: find $\#C(\mathbb{F}_p) \pmod{p}$ and use Hasse-Weil bound (much faster)

Hasse-Witt Matrix

Definition (informal)

Define $H^1(C, \mathcal{O}_C)$ as the set of bivariate polynomials made from combining certain monomials modulo the equation of the curve.

Hasse-Witt Matrix

Definition (informal)

Define $H^1(C, \mathcal{O}_C)$ as the set of bivariate polynomials made from combining certain monomials modulo the equation of the curve.

Definition

The Hasse-Witt matrix of a curve C is defined as the matrix corresponding to the pth power mapping on the vector space $H^1(C, \mathcal{O}_C)$.

Hasse-Witt Matrix

Theorem

If A is the Hasse-Witt matrix of some curve C over some field $\mathbb{F}_p$,

$$\#C(\mathbb{F}_p) \equiv 1 - \mathrm{tr}(A) \pmod{p}.$$

Remark

If p is large, we only need to find $\mathrm{tr}(A) \pmod{p}$.

Hasse-Witt Matrix

Example

Hasse-Witt matrix of $y^3 = x^6 + 1$ over $\mathbb{F}_7$ is

$$\begin{pmatrix} \binom{4}{1} & 0 & 0 & 0 \\ 0 & \binom{2}{1} & 0 & 0 \\ 0 & 0 & \binom{4}{2} & 0 \\ 0 & 0 & 0 & \binom{4}{3} \end{pmatrix}.$$

$$\begin{aligned} \#C(\mathbb{F}_7) &\equiv 1 - \left(\binom{4}{1} + \binom{2}{1} + \binom{4}{2} + \binom{4}{3}\right) \pmod 7 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Counting Paths Instead of Points

Definition

Let C be a curve of the form $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$. Define $S(C)$ to be the set of lattice points (i, j) such that $i(m_1 - m_2) + jn_2 < 0$, $im_1 + jn_1 > 0$, $1 \leq j \leq m_1 - 1$, and $i \leq -1$.

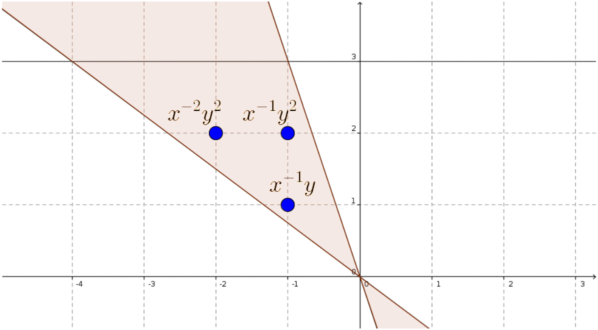
Remark

(i, j) corresponds to $x^i y^j \in H^1(C, \mathcal{O}_C)$. The monomials corresponding to points in $S(C)$ give us a basis for $H^1(C, \mathcal{O}_C)$.

Counting Paths Instead of Points

Example

$S(C)$ for $C : y^3 - x^4 - x = 0$



Remark

(i,j) corresponds to $x^i y^j \in H^1(C, \mathcal{O}_C)$. The monomials corresponding to points in $S(C)$ give us a basis for $H^1(C, \mathcal{O}_C)$.

Counting Paths Instead of Points

Redefinition

If $x^{pi}y^{pj} = \ldots + a_{u,v}x^u y^v + \ldots$, the entry of the Hasse-Witt matrix in the i, j column and u, v row is $a_{u,v}$.

Counting Paths Instead of Points

Redefinition

If $x^{pi}y^{pj} = \ldots + a_{u,v}x^u y^v + \ldots$, the entry of the Hasse-Witt matrix in the i, j column and u, v row is $a_{u,v}$.

Example

$C : y^3 = x^4 + x$, where $p = 19$

- $S(C) = \{(-1, 1), (-1, 2), (-2, 2)\}$

Counting Paths Instead of Points

Redefinition

If $x^{pi}y^{pj} = \ldots + a_{u,v}x^u y^v + \ldots$, the entry of the Hasse-Witt matrix in the i, j column and u, v row is $a_{u,v}$.

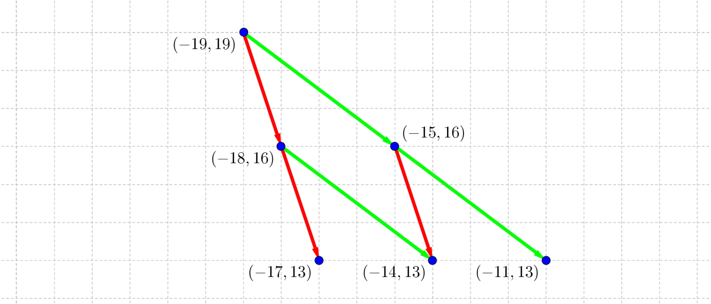
Example

$C : y^3 = x^4 + x$, where $p = 19$

- $S(C) = \{(-1,1), (-1,2), (-2,2)\}$
- For $(-1,1)$:

$$\begin{aligned} x^{-19}y^{19} = x^{-19}y^{16}y^3 &= x^{-19}y^{16}\left(x^4 + x\right) \\ &= x^{-15}y^{16} + x^{-18}y^{16} \\ &= x^{-11}y^{13} + 2x^{-14}y^{13} + x^{-17}y^{13} \\ &\vdots \\ &= \ldots + 15x^{-1}y + \ldots \end{aligned}$$

Counting Paths Instead of Points



Example

$C : y^3 = x^4 + x$, where $p = 19$

- For $(-1, 1)$:

$$\begin{aligned} x^{-19}y^{19} = x^{-19}y^{16}y^3 &= x^{-19}y^{16}\left(x^4 + x\right) \\ &= x^{-15}y^{16} + x^{-18}y^{16} \\ &= x^{-11}y^{13} + 2x^{-14}y^{13} + x^{-17}y^{13} \end{aligned}$$

Counting Paths Instead of Points

Recall that the curve of interest is $C : y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$.

Counting Paths Instead of Points

Recall that the curve of interest is $C : y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$.

Question

How many paths are there from (pi, pj) to (u, v) if only steps of $\langle n_1, -m_1 \rangle$ and $\langle n_2, m_2 - m_1 \rangle$ are allowed?

Counting Paths Instead of Points

Recall that the curve of interest is $C : y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$.

Question

How many paths are there from (pi, pj) to (u, v) if only steps of $\langle n_1, -m_1 \rangle$ and $\langle n_2, m_2 - m_1 \rangle$ are allowed?

Answer

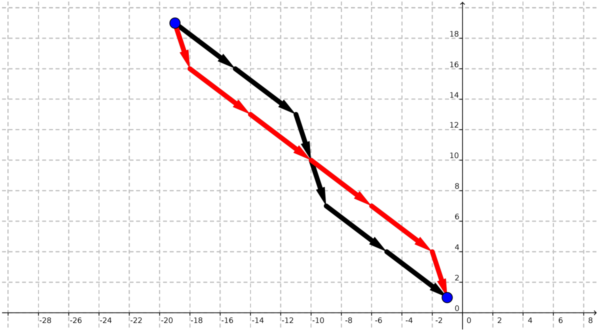
Assume there are k_1 of $\langle n_1, -m_1 \rangle$ and k_2 of $\langle n_2, m_2 - m_1 \rangle$. Then, the number of paths is $\binom{k_1 + k_2}{k_1}$, where

$k_1 = \frac{(m_1 - m_2)(pi - u) - n_2(pj - v)}{m_1 n_1 - m_1 n_2 - m_2 n_1}$ and $k_2 = \frac{n_1(pj - v) - m_1(pi - u)}{m_1 n_1 - m_1 n_2 - m_2 n_1}$.

Counting Paths Instead of Points

Example

Number of paths from $(-19, 19)$ to $(-1, 1)$ using $\langle 4, -3\rangle$ and $\langle 1, -3\rangle$.



Requires four of $\langle 4, -3\rangle$ and two of $\langle 1, -3\rangle$, so number of paths is $\binom{6}{4} = 15$.

Number of Points Modulo p

Diagonal entries of the Hasse-Witt matrix correspond to paths from (pi, pj) to (i, j).

Number of Points Modulo p

Diagonal entries of the Hasse-Witt matrix correspond to paths from (pi, pj) to (i, j).

Theorem (Hase-Liu)

If C is the curve $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$,

$$\#C\left(\mathbb{F}_p\right) \equiv 1 - \sum_{(i,j)\in S(C)} \binom{k_1 + k_2}{k_1} c_1^{k_1} c_2^{k_2} \pmod{p},$$

where $k_1 = \frac{(p-1)(i(m_2-m_1)-jn_2)}{m_1 n_1 - m_1 n_2 - m_2 n_1}$ and $k_2 = \frac{(p-1)(jn_1+im_1)}{m_1 n_1 - m_1 n_2 - m_2 n_1}$.

Summary

Steps to computing $\#C(\mathbb{F}_p)$:

- Find $S(C)$

Summary

Steps to computing $\#C(\mathbb{F}_p)$:

- Find $S(C)$
- Compute diagonal entries of Hasse-Witt matrix by finding number of paths from (pi, pj) to (i, j)

Summary

Steps to computing $\#C(\mathbb{F}_p)$:

- Find $S(C)$
- Compute diagonal entries of Hasse-Witt matrix by finding number of paths from (pi, pj) to (i, j)
- Use fact that $\#C(\mathbb{F}_p) \equiv 1 - \mathrm{tr}(A) \pmod{p}$

Summary

Steps to computing $\#C(\mathbb{F}_p)$:

- Find $S(C)$
- Compute diagonal entries of Hasse-Witt matrix by finding number of paths from (pi, pj) to (i, j)
- Use fact that $\#C(\mathbb{F}_p) \equiv 1 - \mathrm{tr}(A) \pmod{p}$
- Finish with Hasse-Weil bound

Demo

Example

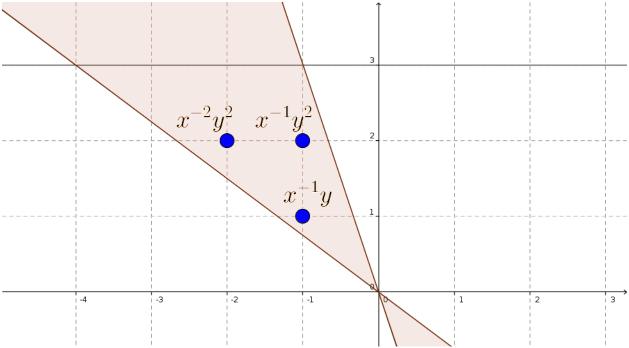
$C : y^3 - x^4 - x = 0$, where $p = 19$

- Allowed steps: $\langle 4, -3 \rangle$ and $\langle 1, -3 \rangle$

Demo

Example

$S(C)$ for $C : y^3 - x^4 - x = 0$



Demo

Example

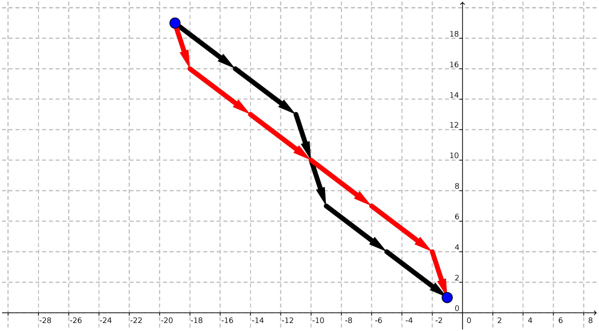
$C : y^3 - x^4 - x = 0$, where $p = 19$

- Allowed steps: $\langle 4, -3 \rangle$ and $\langle 1, -3 \rangle$
- $S(C) = \{(-1,1), (-1,2), (-2,2)\}$

Demo

Example

Number of paths from $(-19, 19)$ to $(-1, 1)$ using $\langle 4, -3\rangle$ and $\langle 1, -3\rangle$.



Requires four of $\langle 4, -3\rangle$ and two of $\langle 1, -3\rangle$, so number of paths is $\binom{6}{4} = 15$.

Demo

Example

$C : y^3 - x^4 - x = 0$, where $p = 19$

- $S(C) = \{(-1,1),(-1,2),(-2,2)\}$
- Allowed steps: $\langle 4, -3 \rangle$ and $\langle 1, -3 \rangle$
- Number of paths from $(-19, 19)$ to $(-1, 1)$: $\binom{6}{4}$
- Number of paths from $(-19, 38)$ to $(-1, 2)$: $\binom{12}{2}$
- Number of paths from $(-38, 38)$ to $(-2, 2)$: $\binom{12}{8}$

Demo

Example

$C : y^3 - x^4 - x = 0$, where $p = 19$

- $S(C) = \{(-1,1), (-1,2), (-2,2)\}$
- Allowed steps: $\langle 4, -3 \rangle$ and $\langle 1, -3 \rangle$
- Number of paths from $(-19, 19)$ to $(-1, 1)$: $\binom{6}{4}$
- Number of paths from $(-19, 38)$ to $(-1, 2)$: $\binom{12}{2}$
- Number of paths from $(-38, 38)$ to $(-2, 2)$: $\binom{12}{8}$

- $\# C(\mathbb{F}_p) \equiv 1 - \left(\binom{6}{4} + \binom{12}{2} + \binom{12}{8} \right) \equiv 14 \pmod{19}$

Demo

Example

$C : y^3 - x^4 - x = 0$, where $p = 19$

- To check, use brute force to find number of points directly
- $(x, y) \in \mathbb{F}_{19}^2$ such that $y^3 - x^4 - x = 0$:
  $(0, 0), (2, 8), (2, 12), (2, 18), (3, 2), (3, 3), (3, 14), (8, 0), (12, 0), (14, 10), (14, 13), (14, 15), (18, 0)$ (13 points)

Demo

Example

$C : y^3 - x^4 - x = 0$, where $p = 19$

- To check, use brute force to find number of points directly
- $(x, y) \in \mathbb{F}_{19}^2$ such that $y^3 - x^4 - x = 0$:
  $(0,0), (2,8), (2,12), (2,18), (3,2), (3,3), (3,14), (8,0), (12,0), (14,10), (14,13), (14,15), (18,0)$ (13 points)
- Must include point at infinity, for a total of 14 points (with multiplicity)

Time Complexity

Definition

Let $M(n) = O(n \log n \log \log n)$ be the time needed to multiply two n-digit numbers.

Time Complexity

Definition

Let $M(n) = O(n \log n \log \log n)$ be the time needed to multiply two n-digit numbers.

Theorem (Fite and Sutherland)

For the curves $y^2 = x^8 + c$ and $y^2 = x^7 - cx$, $\#C(\mathbb{F}_p)$ can be computed (for certain values of m such that $p \equiv 1 \pmod{m}$):

- Probabilistically in $O(M(\log p) \log p)$
- Deterministically in $O\left(M(\log p) \log^2 p \log \log p\right)$, assuming generalized Riemann hypothesis
- Deterministically in $O\left(M\left(\log^3 p\right) \log^2 p / \log \log p\right)$

Time Complexity

Definition

Let $M(n) = O(n \log n \log \log n)$ be the time needed to multiply two n-digit numbers.

Theorem (Fite and Sutherland)

For the curves $y^2 = x^8 + c$ and $y^2 = x^7 - cx$, $\#C(\mathbb{F}_p)$ can be computed (for certain values of m such that $p \equiv 1 \pmod{m}$):

- Probabilistically in $O(M(\log p) \log p)$
- Deterministically in $O\left(M(\log p) \log^2 p \log \log p\right)$, assuming generalized Riemann hypothesis
- Deterministically in $O\left(M\left(\log^3 p\right) \log^2 p / \log \log p\right)$

Theorem

The theorem above also holds for curves of the form $y^{m_1} = c_1 x^{n_1} + c_2 x^{n_2} y^{m_2}$.

Future Work

- Extending approach to more curves
- Working over different fields
- Computing $\#J_C(\mathbb{F}_p)$
- Applications to cryptography

Acknowledgments

Thanks to:

- Nicholas Triantafillou, my mentor, for patiently working with me every week and providing valuable advice
- Dr. Andrew Sutherland, for suggesting this project
- Dr. Tanya Khovanova, for her valuable suggestions
- The PRIMES program, for providing me with this opportunity
- My parents, for continually supporting me