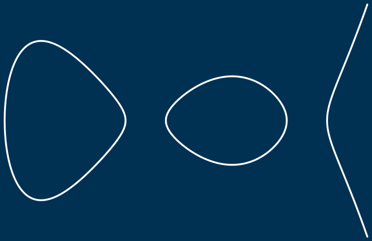
Elliptic curves maximal over finite extensions

Ane Anema

Rijksuniversiteit Groningen

29 November 2016

The arithmetic of maximal curves, the Hesse pencil and the Mestre curve



Ane Anema

Outline

1. Motivation
2. Reformulate question
3. Supersingular case
4. Ordinary case
5. Maximal over cubic extensions

Question

Given an elliptic curve E over a finite field k of cardinality q, does there exist a finite extension l of k such that the number of points on E over l is maximal with respect to the Hasse bound?

Finite fields

- A field k is *finite* if $|k|$ is finite.
- The characteristic of k is the (unique) prime p such that

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow k, \qquad \bar{n} \longmapsto \sum_{i=1}^{n} 1$$

  is an injective ring homomorphism.
- $q = |k| = p^d$.
- Up to isomorphism, there is a unique field with q elements,
  - denote by $\mathbb{F}_q$,
  - $a^q = a$ for all $a \in \mathbb{F}_q$,
  - $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{F}_q$.
- If k is a subfield of l, then
  - l is an *extension* of k denoted by l/k,
  - the degree $[l : k] := \dim_k(l)$.

Algebraic curves

- Let k be a field.
- An *(algebraic) variety* C over k is – loosely speaking – an irreducible topological space such that locally C is the set of zeros in $\bar{k}^n$ of

$$F_1(x_1, \ldots, x_n) = 0, \quad \ldots, \quad F_r(x_1, \ldots, x_n) = 0,$$

  where $F_i \in k[X_1, \ldots, X_n]$.
- If l/k, then

$$C(l) := \{(x_1, \ldots, x_n) \in l^n : F_i(x_1, \ldots, x_n) = 0 \text{ for all } i\}.$$

- A *curve* over k is a 1-dimensional variety over k,
  - for example: $x^2 + y^2 = 1$.

Hasse-Weil-Serre bound

Theorem

If C is a non-singular of genus g over $\mathbb{F}_q$, then

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \leq |C(\mathbb{F}_q)| \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

- A curve C of genus g over $\mathbb{F}_q$ is *maximal* if

$$|C(\mathbb{F}_q)| = q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

- Consider

$$N_q(g) := \max\{|C(\mathbb{F}_q)| : C \text{ a curve of genus } g \text{ over } \mathbb{F}_q\}.$$

- A typical construction of a curve with many points is:
  1. Let D be a curve (of lower genus) with many points.
  2. Consider curves C with a morphism $C \to D$.

Elliptic curves

- An *elliptic curve* (E, O) over k is a non-singular curve of genus 1 over k and a point $O \in E(k)$:
  - The zero set of a (short) *Weierstrass* equation $(\mathrm{char}\,(k) \neq 2, 3)$

    $$E(\bar{k}) = \{(x, y) \in \bar{k}^2 : y^2 = x^3 + ax + b\} \cup \{O\}$$

    with $a, b \in k$ such that $4a^3 + 27b^2 \neq 0$.
- $E(k)$ is a group with identity O.

Example

- Consider $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ and the elliptic curve E over $\mathbb{F}_3$

$$y^2 = x^3 - x.$$

- Since $a^3 = a$ for all $a \in \mathbb{F}_3$,

$$E(\mathbb{F}_3) = \{O, (\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{2}, \bar{0})\}.$$

- Hence $|E(\mathbb{F}_3)| = 4 < 7 = 3 + 1 + \lfloor 2\sqrt{3} \rfloor$.
- Consider $\mathbb{F}_9 \cong \mathbb{F}_3(i) = \{a + bi : a, b \in \mathbb{F}_3\}$ with $i^2 + \bar{1} = \bar{0}$.
- Since $(a + bi)^3 = a^3 + b^3 i^3 = a - bi$ for all $a, b \in \mathbb{F}_3$,

$$\begin{aligned} E(\mathbb{F}_9) = \{O, &(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{2}, \bar{0}), \\ &(i, \pm(\bar{1} - i)), (\bar{1} + i, \pm(\bar{1} - i)), (\bar{2} + i, \pm(\bar{1} - i)), \\ &(-i, \pm(\bar{1} + i)), (\bar{1} - i, \pm(\bar{1} + i)), (\bar{2} - i, \pm(\bar{1} + i))\}. \end{aligned}$$

- Hence $|E(\mathbb{F}_9)| = 16 = 9 + 1 + \lfloor 2\sqrt{9} \rfloor$.

Outline

1 Motivation

2 Reformulate question

3 Supersingular case

4 Ordinary case

5 Maximal over cubic extensions

Question

Given an elliptic curve E over a finite field k of cardinality q, does there exist a finite extension l of k such that the number of points on E over l is maximal with respect to the Hasse bound?

Eigenvalues of Frobenius

Theorem

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

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - a_n, \qquad a_n = \alpha^n + \bar{\alpha}^n$$

for all $n \in \mathbb{Z}_{>0}$, where $\alpha \in \mathbb{C}$ is a root of

$$X^2 - a_1 X + q.$$

- Choose α such that $\operatorname{Im}(\alpha) \geq 0$.
- $|\alpha| = \sqrt{q}$.
- $|a_n| \leq 2\sqrt{q}^n$.
- A recurrence relation

$$\begin{aligned} a_{n+1} &= \alpha(\alpha^n + \bar{\alpha}^n) + \bar{\alpha}(\alpha^n + \bar{\alpha}^n) - q\bar{\alpha}^{n-1} - q\alpha^{n-1} \\ &= a_1 a_n - q a_{n-1}. \end{aligned}$$

Isogenies

Let E and E' be elliptic curves over k.

- An *isogeny* $\phi : E \to E'$ over k is a morphism over k such that $\phi(O) = O'$.
- The curves are *isogeneous* over k if there is a non-constant isogeny $E \to E'$ over k.
  - This is an equivalence relation.
  - This is a weaker version of an isomorphism.
- If $k = \mathbb{F}_q$, then

$$E \text{ and } E' \text{ are isogeneous over } \mathbb{F}_q \iff |E(\mathbb{F}_q)| = \left|E'(\mathbb{F}_q)\right|.$$

Theorem (Waterhouse)

An isogeny class of elliptic curves over $\mathbb{F}_q$ corresponds to an integer a_1 such that $|a_1| \leq 2\sqrt{q}$ and some additional conditions.

Reformulated question

Question

Given a prime power q and an $a_1 \in \mathbb{Z}$ such that $|a_1| \leq 2\sqrt{q}$, does there exist a $n \in \mathbb{Z}_{>0}$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$.

Recall that

- $\alpha \in \mathbb{C}$ is a root of $X^2 - a_1 X + q$,
- $a_n = \alpha^n + \bar{\alpha}^n$.

Define $\beta = \frac{\alpha}{\sqrt{q}}$.

An important lemma

Lemma

$$-a_n = \lfloor 2\sqrt{q}^n \rfloor \quad \iff \quad |\beta^n + 1| \leq \frac{1}{\sqrt[4]{q}^n}.$$

Proof.

Since $|a_n| \leq 2\sqrt{q}^n$,

$$-a_n = \lfloor 2\sqrt{q}^n \rfloor \iff 0 \leq a_n + 2\sqrt{q}^n < 1 \iff |a_n + 2\sqrt{q}^n| < 1.$$

Use

$$\begin{aligned} a_n + 2\sqrt{q}^n = \alpha^n + \bar{\alpha}^n + 2\sqrt{q}^n &= \bar{\alpha}^n \left(\frac{\alpha^{2n}}{\sqrt{q}^{2n}} + 1 + 2\frac{\alpha^n}{\sqrt{q}^n} \right) \\ &= \bar{\alpha}^n (\beta^n + 1)^2. \end{aligned}$$

$\square$

Outline

1 Motivation

2 Reformulate question

3 Supersingular case

4 Ordinary case

5 Maximal over cubic extensions

Supersingular elliptic curves

- An elliptic curve E over $\mathbb{F}_q$ is *supersingular* if $\gcd(a_1, q) \neq 1$.
- The pair q, a_1 is *supersingular* if β is a root of unity, that is $\beta^m = 1$ for some non-zero $m \in \mathbb{Z}$.

Proposition

If the pair q, a_1 is supersingular, then $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ for some $n \in \mathbb{Z}_{>0}$ if and only if

$$a_1 \in \left\{0, \sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, -2\sqrt{q}\right\}.$$

Moreover if such an n exists, then there exist infinitely many.

- The case q a square was already solved by Peter Doetjes.

Proof

First step:

- β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ and therefore also of

$$X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1.$$

- $[\mathbb{Q}(\beta) : \mathbb{Q}] \in \{1, 2, 4\}$.
- If β is a root of unity of order n, then
  - $[\mathbb{Q}(\beta) : \mathbb{Q}] = \phi(n)$,
  - evaluate the above polynomials in $\zeta_n = e^{\frac{2\pi}{n}i}$ to get a_1.
- If $a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}$, then one of the above polynomials is a (product of) cyclotomic polynomials.

d	n	a_1	Φ_n
1	1	$2\sqrt{q}$	$X-1$
	2	$-2\sqrt{q}$	$X+1$
2	3	$-\sqrt{q}$	X^2+X+1
	4	0	X^2+1
	6	$\sqrt{q}$	X^2-X+1
4	5		$X^4+X^3+X^2+X+1$
	8	$\pm\sqrt{2q}$	X^4+1
	10		$X^4-X^3+X^2-X+1$
	12	$\pm\sqrt{3q}$	X^4-X^2+1

Last step:

- If the order n of β is even, then for $n' = \frac{n}{2}$

$$0 = \left|\beta^{n'} + 1\right| < \frac{1}{\sqrt[4]{q}^{n'}}.$$

  Hence $-a_{n'} = \left\lfloor 2\sqrt{q}^{n'} \right\rfloor$.

- If the order n of β is odd, that is $n = 1$ or $n = 3$, then

$$\left|\beta^{n'} + 1\right| \geq 1 > \frac{1}{\sqrt[4]{q}^{n'}}$$

  for all $n' \in \mathbb{Z}_{>0}$. Hence $-a_{n'} \neq \left\lfloor 2\sqrt{q}^{n'} \right\rfloor$.

Outline

1 Motivation

2 Reformulate question

3 Supersingular case

4 Ordinary case

5 Maximal over cubic extensions

Ordinary elliptic curves

- An elliptic curve E is *ordinary* if $\gcd(a_1, q) = 1$.
- The pair q, a_1 is *ordinary* if β is not a root of unity.

Proposition

If the pair q, a_1 is ordinary, then $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ for at most finitely many $n \in \mathbb{Z}_{>0}$. Furthermore q is not a square and n is odd.

- In this case, if $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$, then

$$0 < |\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n}.$$

Linear forms in logarithms

- A *linear form in logarithms* is

$$m_1 \log(\gamma_1) + \ldots + m_r \log(\gamma_r)$$

with $m_i \in \mathbb{Z}$ and γ_i non-zero algebraic numbers (over $\mathbb{Q}$).

Theorem (Baker)

If $\log(\gamma_1), \ldots, \log(\gamma_r)$ *are linear independent over* $\mathbb{Q}$*, then*

$$\log|m_1 \log(\gamma_1) + \ldots + m_r \log(\gamma_r)| > -C \log \max\{|m_1|, \ldots, |m_r|\}$$

with C *a constant depending on* γ_i*.*

Corollary

If γ is an algebraic number such that $|\gamma| = 1$ and γ is not a root of unity, then

$$\log|\log(-\gamma^n)| > -(32d)^{400}\log(4)\log\log(4)\log(h)\log(n)$$

for all integers $n \geq 4$, where $d = [\mathbb{Q}(\gamma) : \mathbb{Q}]$ and $h \in \mathbb{Z}_{\geq 4}$ is an upper bound on the height of γ.

Sketch of proof.

For some $k \in \mathbb{Z}$

$$\log(-\gamma^n) = \log(-1) + n\log(\gamma) + 2\pi k i = (2k+1)\log(-1) + n\log(\gamma)$$

Since γ is not a root of unity, $|\log(\gamma)| < \pi$ and $|\log(-\gamma^n)| < \pi$.

$$\begin{aligned} |2k+1|\pi &= |\log(-\gamma^n) - n\log(\gamma)| \\ &\leq |\log(-\gamma^n)| + n|\log(\gamma)| < (n+1)\pi. \end{aligned}$$

Upper bound on the degree n

Let q, a_1 be ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some $n \in \mathbb{Z}_{\geq 4}$.

- Recall that
$$0 < |\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n}.$$
- Observe that for all $|z| < c < 1$
$$|\log(1-z)| = \left|\sum_{k=1}^{\infty} \frac{z^k}{k}\right| < \sum_{k=1}^{\infty} c^k = \frac{c}{1-c}.$$
- Take $z = \beta^n + 1$ and $c = \frac{1}{\sqrt[4]{q}^n}$. Then
$$\log|\log(-\beta^n)| < -\log(\sqrt[4]{q}^n - 1)$$
- Baker's Theorem gives
$$-\tilde{C}\log(2q)\log(n) < \log|\log(-\beta^n)|$$
with $\tilde{C} = 2^{2800}\log(4)\log\log(4)$.

Convergents

- Recall that $a_1 = \alpha + \bar{\alpha}$ and $\alpha = e^{i\theta}$ with $\theta \in [0, \pi]$.

Proposition (Doetjes)

If $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ *for some* $n \in \mathbb{Z}_{>0}$, *then*

$$\left| \frac{\theta}{\pi} - \frac{m}{n} \right| < \frac{1}{\pi} \sqrt{\frac{48}{48 - \pi^2}} \frac{1}{n \sqrt[4]{q}^n}$$

with m *an odd integer.*

- If $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ for some $n \geq 3$ and either $q \geq 3$ or $n \geq 13$, then $\frac{m}{n}$ is a convergent of $\frac{\theta}{\pi}$ for some odd m.

Computer experiment

Compute ordinary triples q, a_1, n with $n > 1$ such that

$$-a_n = \lfloor 2\sqrt{q}^n \rfloor.$$

- Case $n = 3$ and $q < 10^3$:

q	a_1	q	a_1	q	a_1	q	a_1	q	a_1	q	a_1
2	1	37	6	103	10	229	15	479	22	787	28
3	2	47	7	167	13	257	16	487	22	839	29
5	2	61	8	173	13	293	17	571	24	967	31
8	3	67	8	193	14	359	19	577	24		
11	3	79	9	197	14	397	20	673	26		
17	4	83	9	199	14	401	20	677	26		
23	5	97	10	223	15	439	21	727	27		
27	5	101	10	227	15	443	21	733	27		

- Case $n = 5$ and $q < 10^6$:

q	a_1	q	a_1
2	-1	8807	-58
3	-1	10391	-63
11	-2	10399	165
23	-3	22159	-92
31	9	122147	-216
128	-7	192271	-271
317	-11	842321	1485
2851	-33		

- Case $n = 7$ and $q < 10^6$:

$$q = 5, \quad a_1 = 1.$$

- Case $n = 13$ and $q < 10^6$:

$$q = 2, \quad a_1 = 1.$$

Upper bound on the cardinality q

Proposition

Let $n \in \mathbb{Z}_{\geq 13}$. There exists a $q_n \in \mathbb{Z}$ such that if $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some pair q, a_1, then $q \leq q_n$ or the pair q, a_1 is supersingular.

- Combined with the upper bound from linear forms in logarithms this implies that

Theorem

There exist only finitely many ordinary pairs q, a_1 such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some $n \geq 13$.

Proof of proposition

Assume that the pair q, a_1 is ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$.

- Recall that q not a square and n odd and
$$0 < |\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n}.$$
- Observe that $\beta^n + 1 = \prod_{i=1}^n \left(\beta - \zeta_{2n}^{2i+1}\right)$.
- There is a $c_n > 0$ (depending only on n) and a m such that
$$|\beta^n + 1| \geq c_n |\beta - \zeta_{2n}^m| \geq c_n \left| \frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right) \right|.$$
- The Subspace Theorem implies: For all $\varepsilon > 0$ there exists a $c_0' > 0$ depending on $\cos\left(\frac{m\pi}{n}\right)$ and ε such that
$$\left| \frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right) \right| \geq \frac{c_0'}{(4q)^{3+\varepsilon}}.$$
- Take $\varepsilon = \frac{1}{8}$. Then $c < q^{3+\varepsilon-\frac{n}{4}}$ for some $c > 0$.

Outline

1 Motivation

2 Reformulate question

3 Supersingular case

4 Ordinary case

5 Maximal over cubic extensions

Maximal over cubic extensions

Theorem

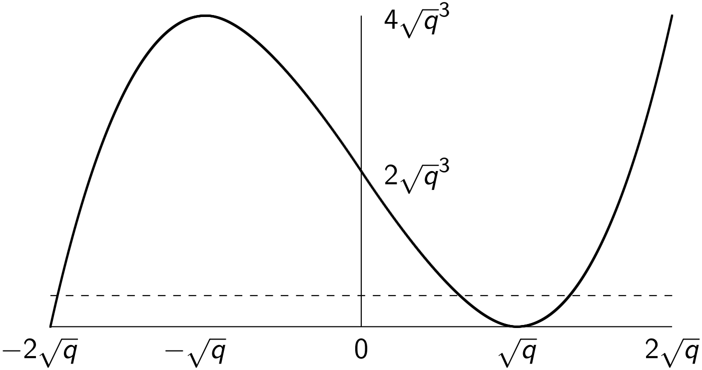
For infinitely many primes $q = p$ there exists an $a_1 \in \mathbb{Z}$ (with $|a_1| \leq 2\sqrt{q}$) such that $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$.

- Such a pair q, a_1 is ordinary.
- Using $a_{n+1} = a_1 a_n - q a_{n-1}$ and $a_0 = 2$

$$a_3 = a_1^3 - 3qa_1.$$

- Hence

$$-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor \quad \Longleftrightarrow \quad 0 \leq a_1^3 - 3qa_1 + 2\sqrt{q}^3 < 1.$$



Proposition (Soomro)

If $q = a_1^2 + b$ with integers a_1, b such that $a_1 \geq 2$ and $|b| \leq \sqrt{a_1}$, then $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$.

Proof of theorem

- Consider
$$S_1 = \left\{(a,b) \in \mathbb{Z}^2 : p = a^2 + b \text{ prime}, 0 < a, |b| \le \sqrt{a}\right\}$$
and define $S_2 = \{(a,b) \in S_1 : b \text{ square}\}$, which corresponds to
$$S_3 = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \le c \le \sqrt[4]{a}\right\}.$$
- Define for $\theta > 0$
$$S_4(\theta) = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \le c < p^{\theta}\right\}$$
and write $S_4(\theta) = S_5(\theta) \cup S_6(\theta)$ with
$$S_5(\theta) = \left\{(a,c) \in S_4(\theta) : a \ge p^{4\theta}\right\}$$
and
$$S_6(\theta) = \left\{(a,c) \in S_4(\theta) : a < p^{4\theta}\right\}.$$
- Observe that $S_5(\theta) \subset S_3$.
- If $\theta < \frac{1}{8}$, then $S_6(\theta)$ is finite, because $p = a^2 + c^2 < p^{8\theta} + p^{2\theta}$.
- The set $S_4(0.119)$ is infinite by Harman and Lewis (2001).