Field extensions over which an elliptic curve reaches the Hasse bound

Ane Anema

9 November 2012

Outline

Theorem (Hasse)

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

$$|\#E(\mathbb{F}_q) - q - 1| \leq \lfloor 2\sqrt{q} \rfloor.$$

Definition

If E is an elliptic curve defined over $\mathbb{F}_q$ and

$$\#E(\mathbb{F}_q) = q + 1 + \lfloor 2\sqrt{q} \rfloor,$$

then E is called *maximal* over $\mathbb{F}_q$.

- Given an elliptic curve E defined over $\mathbb{F}_q$, is there a field extension $\mathbb{F}_{q^n}$ over which E becomes maximal?

Theorem

If E is an elliptic curve defined over $\mathbb{F}_q$, then

$$\#E\left(\mathbb{F}_{q^n}\right) = q^n + 1 - a_n$$

for all $n \in \mathbb{Z}_{>0}$, where $a_n = \alpha^n + \overline{\alpha}^n$ and α is a zero of

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

- Given a prime power q and an integer a_1 such that $|a_1| \leq 2\sqrt{q}$, is $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some $n \in \mathbb{Z}_{>0}$?

Proposition (Doetjes)

Let q be a prime power and $|a_1| \leq 2\sqrt{q}$. If q is a square, then

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

for some $n \in \mathbb{Z}_{>0}$ if and only if

$$a_1 \in \{0, \sqrt{q}, -2\sqrt{q}\}.$$

- Define $\beta = \frac{\alpha}{|\alpha|} = \frac{\alpha}{\sqrt{q}} = \frac{\sqrt{q}}{\overline{\alpha}}$.
- Notice that

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

.

- Since $\alpha \neq 0$, then

$$-a_n = \left\lfloor 2\sqrt{q^n} \right\rfloor \quad \Longleftrightarrow \quad \beta^n + 1 = 0.$$

Lemma

Let q be any prime power and β be a zero of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$. Then $\beta^n + 1 = 0$ for some $n \in \mathbb{Z}_{>0}$ if and only if

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

- $\beta^n + 1 = 0$ for some $n \in \mathbb{Z}_{>0}$ is the same as β is a primitive root of unity of even order.
- Denote $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$.
  - $d = \varphi(m)$ for β a m-th primitive root of unity.
  - $d \in \{1, 2, 4\}$.

d	$\varphi^{-1}(d) \cap 2\mathbb{Z}$	minimum polynomial of β
1	2	$X+1$
2	4	X^2+1
	6	X^2-X+1
4	8	X^4+1
	10	$X^4-X^3+X^2-X+1$
	12	X^4-X^2+1

- Case $d=1$:
  - $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ reducible over $\mathbb{Q}\left(\sqrt{q}\right)$,
  - so ${a_1}^2 = 4q$ and

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

  - Hence β even primitive root of unity if and only if $a_1 = -2\sqrt{q}$.

d	$\varphi^{-1}(d) \cap 2\mathbb{Z}$	minimum polynomial of β
1	2	$X+1$
2	4	X^2+1
	6	X^2-X+1
4	8	X^4+1
	10	$X^4-X^3+X^2-X+1$
	12	X^4-X^2+1

- Case $d=2$:
    - $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ irreducible over $\mathbb{Q}\left(\sqrt{q}\right)$,
        - otherwise ${a_1}^2 = 4q$ and the polynomial is reducible over $\mathbb{Q}$.
    - Notice that $\sqrt{q} \in \mathbb{Q}$.
    - Hence β even primitive root of unity if and only if $a_1 = 0$ or $a_1 = \sqrt{q}$.

d	$\varphi^{-1}(d) \cap 2\mathbb{Z}$	minimum polynomial of β
1	2	$X+1$
2	4	X^2+1
	6	X^2-X+1
4	8	X^4+1
	10	$X^4-X^3+X^2-X+1$
	12	X^4-X^2+1

- Case $d=4$:
  - $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ irreducible over $\mathbb{Q}\left(\sqrt{q}\right)$ and $\sqrt{q} \notin \mathbb{Q}$.
  - Minimum polynomial of β over $\mathbb{Q}$ is

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

  - Hence β even primitive root of unity if and only if ${a_1}^2 = 2q$ or ${a_1}^2 = 3q$.

Proposition

Let q be a prime power which is not a square, and $a_1 \in \mathbb{Z}$ such that $|a_1| \leq 2\sqrt{q}$.

1. *If*
$$a_1 \in \left\{0, \pm\sqrt{2q}, \pm\sqrt{3q}\right\},$$
then $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for infinitely many $n \in \mathbb{Z}_{>0}$.
2. *If $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some $n \in \mathbb{Z}_{>0}$, then either*
$$a_1 \in \left\{0, \pm\sqrt{2q}, \pm\sqrt{3q}\right\}$$
or $-a_m = \lfloor 2\sqrt{q^m} \rfloor$ for only finitely many $m \in \mathbb{Z}_{>0}$.

Corollary

Let E be an elliptic curved defined over $\mathbb{F}_q$.

- *If E is ordinary, that is $\gcd(a_1, q) = 1$, then there are at most finitely many extensions of $\mathbb{F}_q$ over which E is maximal.*
- *If E is supersingular, then E is maximal over infinitely many extensions of $\mathbb{F}_q$, except when*

$$a_1 \in \{-\sqrt{q}, 2\sqrt{q}\}$$

in which case E is never maximal.

- Notice that

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

- Define $\beta = \frac{\alpha}{|\alpha|}$ and recall that

$$a_n + 2\sqrt{q^n} = \overline{\alpha}^n \left(\beta^n + 1\right)^2.$$

- Since $|a_n| \leq 2\sqrt{q^n}$, then $0 \leq a_n + 2\sqrt{q^n}$, so that

$$\begin{aligned} -a_n = \lfloor 2\sqrt{q^n} \rfloor &\iff \left| a_n + 2\sqrt{q^n} \right| < 1 \\ &\iff |\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}} \end{aligned}$$

Lemma

Let q be any prime power and β be a zero of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$. Then $\beta^n + 1 = 0$ for some $n \in \mathbb{Z}_{>0}$ if and only if

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

1. If
$$a_1 \in \left\{0, \pm\sqrt{2q}, \pm\sqrt{3q}\right\},$$
then $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for infinitely many $n \in \mathbb{Z}_{>0}$.
2. Suppose $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some $n \in \mathbb{Z}_{>0}$.
    - If β is a root of unity of even order, then
    $$a_1 \in \left\{0, \pm\sqrt{2q}, \pm\sqrt{3q}\right\}.$$
    - Assume β is not a root of unity of even order.

- Then
$$0 < |\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}.$$
- Recall that for all $|z| < 1$
$$-\log(1-z) = \sum_{k=1}^{\infty} \frac{z^k}{k} \quad \text{and} \quad \sum_{k=0}^{\infty} z^k = \frac{1}{1-z}.$$
- If $|z| < c < 1$, then
$$|\log(1-z)| = \left| \sum_{k=1}^{\infty} \frac{z^k}{k} \right| \leq \sum_{k=1}^{\infty} c^k = \frac{c}{1-c}.$$
- Hence $|\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}$ implies
$$|\log(-\beta^n)| \leq \frac{1}{\sqrt[4]{q^n} - 1}.$$

- Notice that -1 and β are multiplicatively independent:
  - $-\beta^m \neq 1$ for all $m \in \mathbb{Z}$ by assumption, and
  - $+\beta^m \neq 1$ for all $m \in \mathbb{Z}$ else β a 5-th primitive root of unity.

Lemma (Special case of Baker's theorem)

Let β be an algebraic number. If -1 and β are multiplicatively independent, then

$$|\log(-\beta^n)| > n^{-c\log(h)}$$

for all $n \in \mathbb{Z}_{\geq 4}$, where

- *$h \in \mathbb{Z}_{\geq 4}$ is an upper bound on the height of β and*
- *$c \in \mathbb{R}_{>0}$ which depends only on $[\mathbb{Q}(\beta) : \mathbb{Q}]$.*

- Therefore

$$n^{-c\log(h)} < |\log(-\beta^n)| \leq \frac{1}{\sqrt[4]{q^n}-1} \leq \frac{1}{d\sqrt[4]{q^n}}$$

for some $d \in \mathbb{R}_{>0}$, that is

$$d\sqrt[4]{q^n} < n^{c\log(h)}.$$

- Hence n must be smaller than some constant.

Proposition

Let q be a prime power which is not a square, $a_1 \in \mathbb{Z}$ such that $|a_1| \leq 2\sqrt{q}$

$$a_1 \notin \left\{0, \pm\sqrt{2q}, \pm\sqrt{3q}\right\},$$

and $n \in \mathbb{Z}_{>0}$ such that $-a_n = \lfloor 2\sqrt{q^n} \rfloor$.

- *If $q > e^{2\pi}$, then $n \leq 85621$.*
- *If $112 \leq q \leq e^{2\pi}$, then*

$$n < \frac{54507.6\pi^2}{\log q} + 1.$$

- *If $q \leq 111$, then n smaller than the largest zero of*

$$x \mapsto \frac{x-1}{4} \log q - 30.9\pi^2 \left(2 \log\left(\frac{x+1}{\pi}\right)\right)^2.$$

Lemma (Special case of results by M. Laurent et al.)

Let β be an algebraic number with $|\beta| = 1$. If -1 and β are multiplicative independent, then

$$\log|\log(-\beta^n)| \geq -30.9\pi c \max\left\{d\log\left(\frac{n}{\pi}+\frac{1}{c}\right), 21, \frac{d}{2}\right\}^2$$

for all $n \in \mathbb{Z}_{>0}$, where $c = \max\{dl, \pi\}$ with l an upper bound on the logarithmic height of β and $d = \frac{[\mathbb{Q}(\beta):\mathbb{Q}]}{[\mathbb{R}(\beta):\mathbb{R}]}$.

- Recall that $X^4 + \left(2 - \frac{{a_1}^2}{q}\right)X^2 + 1$ minimum polynomial of β over $\mathbb{Q}$. Other roots are $-\beta$ and $\pm\overline{\beta}$. So $l = \frac{1}{4}\log q$.
- Notice that $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ is irreducible over $\mathbb{R}$, so $d = 2$.

- Compute solutions of

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

with the help of continued fractions.

- Write $\alpha = \sqrt{q}e^{i\theta}$ for some $\theta \in [0, \pi]$, then

$$a_n = 2\sqrt{q^n}\cos(n\theta).$$

Proposition (Doetjes)

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

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

- Notice that if $a_1 \notin \{0, \pm\sqrt{2q}, \pm\sqrt{3q}\}$, then $\frac{\theta}{\pi} \notin \mathbb{Q}$.

- Recall that if $\left|\frac{\theta}{\pi} - \frac{m}{n}\right| < \frac{1}{2n^2}$, then $\frac{m}{n}$ is a convergent of $\frac{\theta}{\pi}$.

Corollary

Let $q > 2$ or $n > 12$. If $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some $n \in \mathbb{Z}_{>0}$, then $\frac{m}{n}$ is a convergent of $\frac{\theta}{\pi}$ for some odd $m \in \mathbb{Z}$.

- Determined the solutions to $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for all prime powers $q \leq 26759$ and $a_1 \notin \{0, \pm\sqrt{2q}, \pm\sqrt{3q}, -\lfloor 2\sqrt{q} \rfloor\}$.
- There are 378 solutions.
- Only two cases in which $n \neq 3, 5$ occurs, namely

q	a_1	n
2	1	13
5	1	7

- The case $n = 5$ appears 12 times, namely

q	a_1
2	-1
3	-1
11	-2
23	-3
31	9
128	-7

q	a_1
317	-11
2851	-33
8807	-58
10391	-63
10399	165
22159	-92

- Expanded results in the case that q is not a square.
- Determined when an elliptic curve over $\mathbb{F}_q$ is maximal over infinitely many extensions of $\mathbb{F}_q$, and when it is maximal over at most finitely many extensions.
- Derived a bound on the degree of the extension in the latter case.
- The results suggest:
  - If q is large and a regular elliptic curve defined over $\mathbb{F}_q$ is maximal over some extension of $\mathbb{F}_q$, then the degree of the extension is 3 or 5.
  - Infinitely many ordinary elliptic curves exists that are maximal over a degree 3 extension.
  - Similar for a degree 5 extension.