Abelian varieties of prescribed order over finite fields

(joint work with Raymond van Bommel, Edgar Costa, Wanlin Li, and Alexander Smith) arXiv: 2106.13651

Fix $\mathbb{F}_q$ of characteristic p.

Thm. (Hasse-Weil)
A abelian variety of dimension n over $\mathbb{F}_q$
Then
$$(\sqrt{q}-1)^{2n} \leq \#A(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2n}.$$

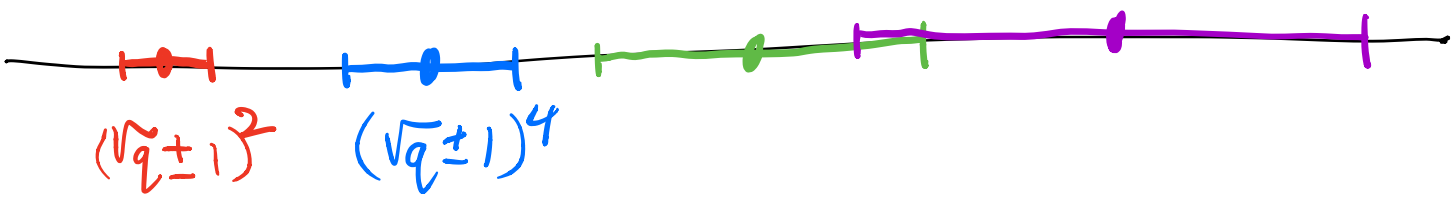
Can this be improved?

I. Extreme orders

Example: For square q, equality holds when A is isogenous to a power of a maximal/minimal s.s. ell. curve.

Thm. (Aubry, Haloui, Lachaud 2013; Kadets 2021)
For any q, if A is simple and not a max/min ell. curve, then
$$(q-\lceil 2\sqrt{q}\rceil+2)^n \leq \#A(\mathbb{F}_q) \leq (q+\lceil 2\sqrt{q}\rceil)^n.$$

II. All orders in between



Thm. (Howe-Kedlaya March 2021) Every positive integer is $\#A(\mathbb{F}_2)$ for some ordinary $A/\mathbb{F}_2$.

dimension depends on positive integer

(Marseglia-Springer May 2021) Every f. abelian gp is $A(\mathbb{F}_2)$ " " " " " .

III. New theorems (June 25, 2021)

Theorem 1: Fix q. For $n \gg 1$, every integer in

$$\left[\left(q-2\sqrt{q}+3-q^{-1}\right)^n, \left(q+2\sqrt{q}-1-q^{-1}\right)^n\right]$$

is $\#A(\mathbb{F}_q)$ for some n-dim abelian variety $A/\mathbb{F}_q$.

geom. simple
ordinary [or prescribed p-rank*]
principally polarized

* order $\equiv 1 \pmod p$ if p-rank 0

Theorem 2:

- For each $q \leq 5$, every positive integer is $\#A(\mathbb{F}_q)$ for some A.

  (for $q \geq 7$, 2 cannot be realized)

- For arbitrary q, every integer $\geq q^{3\sqrt{q}\log q}$ " " " " .

  best possible except for the 3

  (for $\forall \varepsilon > 0$, for large q, $\geq q^{(\frac{1}{4}-\varepsilon)\sqrt{q}\log q}$)

$\exists$ integer $\geq q^{(4-2)\,\ell \log q}$ outside all the Hasse-Weil intervals

IV. Honda-Tate theory

Given A, let $f_A :=$ char. poly. of $\mathrm{Frob}_q|_{T_\ell A}$,

so $\#A(\mathbb{F}_q) = f_A(1)$.

Thm. (Honda-Tate 1960s)

Let $f \in \mathbb{Z}[x]$.

Then $f = f_A$ for some ordinary ab. var. A of $\dim n / \mathbb{F}_q$

$\Leftrightarrow$ $f(x) = x^{2n} + a_1 x^{2n-1} + \dots + a_{n-1} x^{n+1} + a_n x^n$ ← not divisible by p

$+ q a_{n-1} x^{n-1} + \dots + q^{n-1} a_1 x + q^n$.

and every complex root of f has absolute value $q^{1/2}$.

V. Construction of polynomials

Lemma:

For $h(z) = a_0 + \dots + a_{n-1} z^{n-1} + \frac{a_n}{2} z^n \in \mathbb{R}[z]$,

let

$$\hat{h}(x) = a_0 x^{2n} + \dots + a_{n-1} x^{n+1}$$

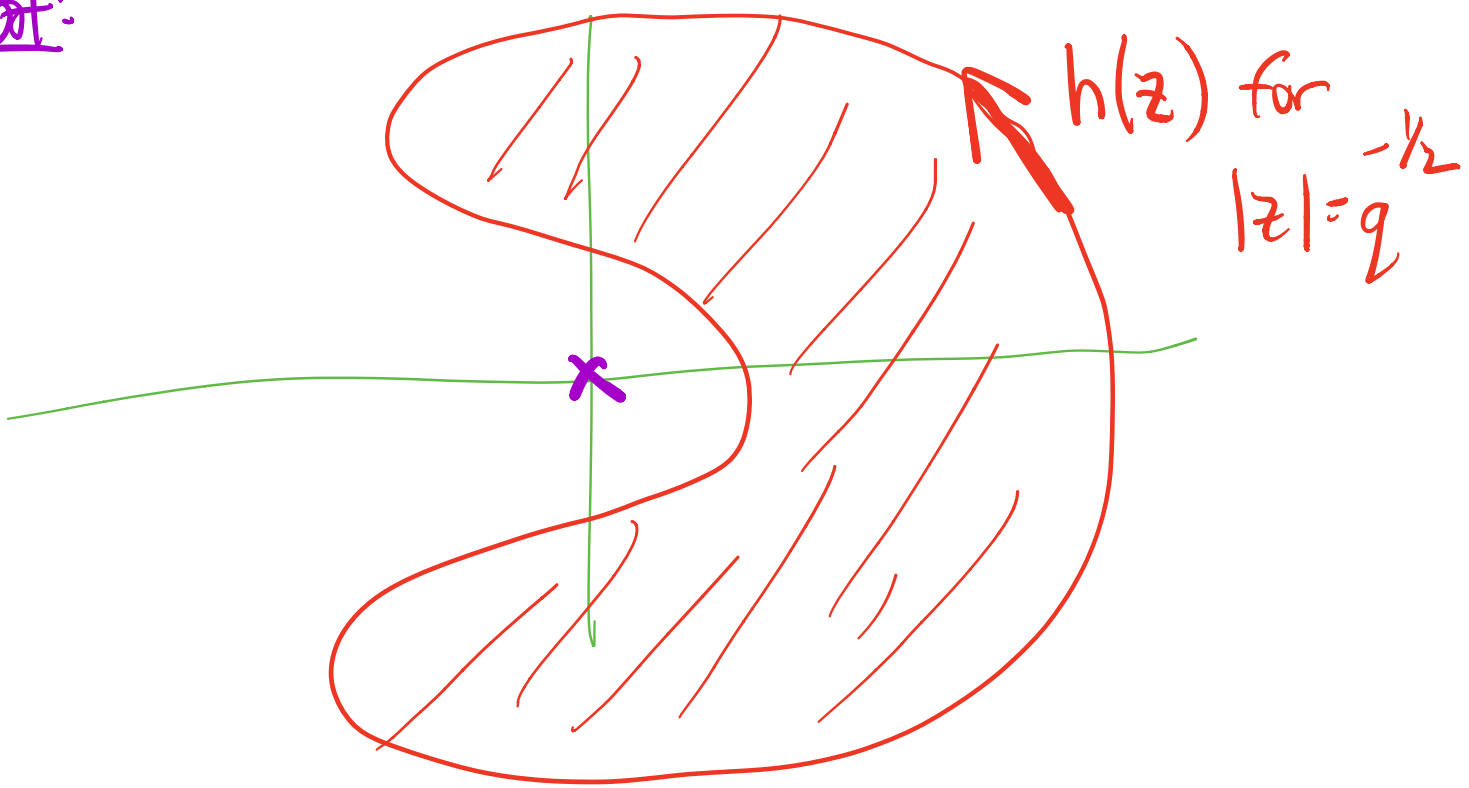
$$+ a_n x^n$$

$$+ q a_{n-1} x^{n-1} + \dots + q^n a_0$$

$$= x^{2n} h\left(\frac{1}{x}\right) + q^n h\left(\frac{x}{q}\right).$$

If $h(z)$ is nonvanishing for $|z| \le q^{-1/2}$, then every complex root of $\hat{h}$ has abs. value $q^{1/2}$.

Proof:



For $|z| = q^{-1/2}$, winding number of $h(z)$ around 0 $= 0$

For $|x| = q^{1/2}$, ------ $x^n h\left(\frac{1}{x}\right)$ ....

$= n.$

Therefore,

$2\,\mathrm{Re}\; x^n h\left(\frac{1}{x}\right)$ crosses 0 at least $2n$ times.

$\|$

$x^n h\left(\frac{1}{x}\right) + q^n x^{-n} h\left(\frac{x}{q}\right)$

Multiply by x^n to get that

$\hat{h}(x)$ has $\geq 2n$ roots with $|x| = q^{1/2}$.

Those are all.

Plan:

- Let $h(z)$ be $\exp j(z)$ truncated to deg n

  for some $j(z) \in \mathbb{R}[[z]]$ with small coeffs.

- $\hat{h}$ will be the desired f_A, so that

$$\#A(\mathbb{F}_q) = f_A(1) = \hat{h}(1)$$

$$= q^n h\left(\frac{1}{q}\right) + h(1)$$

main term

$$\approx q^n \exp j\left(\frac{1}{q}\right).$$

More formally:

Goal:
- Given: $\mathbb{F}_q$, $m \gg 1$
- Find: A with $\#A(\mathbb{F}_q) = m$.

Step 1: Choose n s.t. $q^{n-\frac{1}{2}} \leq m < q^{n+\frac{1}{2}}$.

n ↑ to be $\dim A$

Step 2:

To form $j(z) = c_1 z + c_2 z^2 + \cdots$

inductively choose $c_1, c_2, \ldots$ such that the coeff. of z^i in

$$\exp(c_1 z + \cdots + c_i z^i)$$

is an integer and

$$\log \frac{m}{q^n} - \left(\frac{c_1}{q} + \frac{c_2}{q^2} + \cdots + \frac{c_i}{q^i} \right)$$

is as small as possible.

⋮