An Application of the Geometry of Numbers to Curves

Jeff Thunder (joint work with D. Garton and C. Weir)

Northern Illinois University

AMS Special Session in Honor of Jeff Vaaler
Friday, January 12, 2018

What is an "*a*-number" and why should I care?

What is an “a-number” and why should I care?

The Cohen-Lenstra Conjectures posit “averages” of certain quantities associated with real quadratic fields (more precisely, with their class groups).

What is an "a-number" and why should I care?

The Cohen-Lenstra Conjectures posit "averages" of certain quantities associated with real quadratic fields (more precisely, with their class groups).

The same philosophy applies equally well to function fields of hyperelliptic curves over finite fields.

What is an "a-number" and why should I care?

The Cohen-Lenstra Conjectures posit "averages" of certain quantities associated with real quadratic fields (more precisely, with their class groups).

The same philosophy applies equally well to function fields of hyperelliptic curves over finite fields.

We are thus interested in the structure of the class group (i.e., Jacobian) of such curves (which we identify with their function fields).

What is an "a-number" and why should I care?

The Cohen-Lenstra Conjectures posit "averages" of certain quantities associated with real quadratic fields (more precisely, with their class groups).

The same philosophy applies equally well to function fields of hyperelliptic curves over finite fields.

We are thus interested in the structure of the class group (i.e., Jacobian) of such curves (which we identify with their function fields).

Among the relevant quantities attached to our curves/function fields (or the Jacobian/class group) is the a-number.

Some Notation

Some Notation

- q a power of an odd prime p

Some Notation

- q a power of an odd prime p
- $\mathbb{F}_q$ the finite field with q elements

Some Notation

- q a power of an odd prime p
- $\mathbb{F}_q$ the finite field with q elements
- X transcendental over $\mathbb{F}_q$, so that $\mathbb{F}_q(X)$ is a field of rational functions

Some Notation

- q a power of an odd prime p
- $\mathbb{F}_q$ the finite field with q elements
- X transcendental over $\mathbb{F}_q$, so that $\mathbb{F}_q(X)$ is a field of rational functions
- $f(X) \in \mathbb{F}_q[X]$ a monic square-free polynomial of degree $2g+2$ $(g \geq 1)$

Some Notation

- q a power of an odd prime p
- $\mathbb{F}_q$ the finite field with q elements
- X transcendental over $\mathbb{F}_q$, so that $\mathbb{F}_q(X)$ is a field of rational functions
- $f(X) \in \mathbb{F}_q[X]$ a monic square-free polynomial of degree $2g+2$ $(g \geq 1)$
- E_f the hyperelliptic curve of genus g given by

  $$Y^2 = f(X)$$

  which we associate with the function field obtained by adjoining Y to the field of rational functions $\mathbb{F}_q(X)$

What is the a-number $a(E_f)$ of a hyperelliptic curve E_f?

What is the *a*-number $a(E_f)$ of a hyperelliptic curve E_f?

This is obtained via the *Cartier operator* $\mathcal{C}_f$ on the space of regular differentials on the curve E_f, an $\mathbb{F}_q$-vector space of dimension g.

What is the *a*-number $a(E_f)$ of a hyperelliptic curve E_f?

This is obtained via the *Cartier operator* $\mathcal{C}_f$ on the space of regular differentials on the curve E_f, an $\mathbb{F}_q$-vector space of dimension g.

The *a*-number of the curve E_f is the dimension of the nullspace of $\mathcal{C}_f$.

What is the a-number $a(E_f)$ of a hyperelliptic curve E_f?

This is obtained via the *Cartier operator* $\mathcal{C}_f$ on the space of regular differentials on the curve E_f, an $\mathbb{F}_q$-vector space of dimension g.

The a-number of the curve E_f is the dimension of the nullspace of $\mathcal{C}_f$.

In particular, E_f is called "ordinary" if $a(E_f) = 0$.

Previous Work

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied “random p-divisible groups” and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians.

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied “random p-divisible groups” and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians. Their evidence pointed to a negative answer, at least in some cases.

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied "random p-divisible groups" and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians. Their evidence pointed to a negative answer, at least in some cases.

Specifically, in the case of characteristic $p = 3$

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied "random p-divisible groups" and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians.Their evidence pointed to a negative answer, at least in some cases.

Specifically, in the case of characteristic $p = 3$ computational evidence indicates that the probability that a random hyperelliptic curve over $\mathbb{F}_q$ is ordinary is $1 - q^{-1}$,

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied "random p-divisible groups" and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians. Their evidence pointed to a negative answer, at least in some cases.

Specifically, in the case of characteristic $p = 3$ computational evidence indicates that the probability that a random hyperelliptic curve over $\mathbb{F}_q$ is ordinary is $1 - q^{-1}$, whereas the random p-divisible group heuristic would suggest that this probability is

$$(1 - q^{-1})(1 - q^{-3})(1 - q^{-5}) \cdots$$

Previous Work

Cais, Ellenberg, and Zureik-Brown in 2013 studied "random p-divisible groups" and considered the question of whether such objects captured relevant features of random hyperelliptic Jacobians. Their evidence pointed to a negative answer, at least in some cases.

Specifically, in the case of characteristic $p = 3$ computational evidence indicates that the probability that a random hyperelliptic curve over $\mathbb{F}_q$ is ordinary is $1 - q^{-1}$, whereas the random p-divisible group heuristic would suggest that this probability is

$$(1 - q^{-1})(1 - q^{-3})(1 - q^{-5}) \cdots$$

Moreover, they didn't hazard a guess for higher a-numbers.

Elkin in 2011 did some estimates for a-numbers of Kummer covers of $\mathbb{P}^1_k$.

Elkin in 2011 did some estimates for a-numbers of Kummer covers of $\mathbb{P}^1_k$.

In particular, he computed upper bounds for possible a-numbers of hyperelliptic curves.

Elkin in 2011 did some estimates for a-numbers of Kummer covers of $\mathbb{P}^1_k$.

In particular, he computed upper bounds for possible a-numbers of hyperelliptic curves.

For the special case of characteristic $p = 3$ he obtains the bound

Elkin in 2011 did some estimates for a-numbers of Kummer covers of $\mathbb{P}^1_k$.

In particular, he computed upper bounds for possible a-numbers of hyperelliptic curves.

For the special case of characteristic $p = 3$ he obtains the bound

$$a(E_f) < \frac{g_f}{3} + 2$$

where g_f if the genus of the curve E_f.

Characteristic 3

Characteristic 3

Here we'll look specifically at the case where $p = 3$.

Characteristic 3

Here we'll look specifically at the case where $p = 3$.

In this case everything revolves around solutions to the homogeneous linear equation (over $\mathbb{F}_q(X)$)

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0. \tag{1}$$

Characteristic 3

Here we'll look specifically at the case where $p = 3$.

In this case everything revolves around solutions to the homogeneous linear equation (over $\mathbb{F}_q(X)$)

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0. \tag{1}$$

The "coefficient vector" $(f_0, f_1, f_2) \in \mathbb{F}_q[X]^3$ will correspond to our polynomial f above.

Characteristic 3

Here we'll look specifically at the case where $p = 3$.

In this case everything revolves around solutions to the homogeneous linear equation (over $\mathbb{F}_q(X)$)

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0. \tag{1}$$

The "coefficient vector" $(f_0, f_1, f_2) \in \mathbb{F}_q[X]^3$ will correspond to our polynomial f above.

The "solutions" (P_1, P_2, P_3) will correspond to elements of the nullspace of $\mathcal{C}_f$.

The Coefficient Vector

Write

$$f(X) = \sum_{\substack{i \leq 2g+2 \\ i \equiv 0 \mod 3}} c_i X^i + X \cdot \sum_{\substack{i \leq 2g+2 \\ i \equiv 1 \mod 3}} c_i X^{i-1} + X^2 \cdot \sum_{\substack{i \leq 2g+2 \\ i \equiv 2 \mod 3}} c_i X^{i-2}.$$

The Coefficient Vector

Write

$$f(X) = \sum_{\substack{i \le 2g+2 \\ i \equiv 0 \mod 3}} c_i X^i + X \cdot \sum_{\substack{i \le 2g+2 \\ i \equiv 1 \mod 3}} c_i X^{i-1} + X^2 \cdot \sum_{\substack{i \le 2g+2 \\ i \equiv 2 \mod 3}} c_i X^{i-2}.$$

Then

$$f_j(X)^3 = \sum_{\substack{i \le 2g+2 \\ i \equiv j \mod 3}} c_i X^{i-j} \qquad j = 0, 1, 2.$$

The Coefficient Vector

Write

$$f(X) = \sum_{\substack{i \le 2g+2 \\ i \equiv 0 \mod 3}} c_i X^i + X \cdot \sum_{\substack{i \le 2g+2 \\ i \equiv 1 \mod 3}} c_i X^{i-1} + X^2 \cdot \sum_{\substack{i \le 2g+2 \\ i \equiv 2 \mod 3}} c_i X^{i-2}.$$

Then

$$f_j(X)^3 = \sum_{\substack{i \le 2g+2 \\ i \equiv j \mod 3}} c_i X^{i-j} \qquad j = 0, 1, 2.$$

The degrees of the f_js are constrained depending on the congruence class of g modulo 3.

Constraints on the Degrees

Constraints on the Degrees

Set $m = [(g-1)/3]$.

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m + 2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m + 2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

For $g \equiv 2 \pmod 3$:

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m + 2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

For $g \equiv 2 \pmod 3$:

$$(2g+2)/3 = 2m + 2 = \deg(f_0) > \max\{\deg(f_1), \deg(f_2)\}.$$

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m + 2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

For $g \equiv 2 \pmod 3$:

$$(2g+2)/3 = 2m + 2 = \deg(f_0) > \max\{\deg(f_1), \deg(f_2)\}.$$

For $g \equiv 1 \pmod 3$:

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m+2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

For $g \equiv 2 \pmod 3$:

$$(2g+2)/3 = 2m+2 = \deg(f_0) > \max\{\deg(f_1), \deg(f_2)\}.$$

For $g \equiv 1 \pmod 3$:

$$(2g+1)/3 = 2m+1 = \deg(f_1) \geq \deg(f_0), \quad \deg(f_1) > \deg(f_2).$$

Constraints on the Degrees

Set $m = [(g-1)/3]$.
For $g \equiv 0 \pmod 3$:

$$2g/3 = 2m + 2 = \deg(f_2) \geq \max\{\deg(f_0), \deg(f_1)\}.$$

For $g \equiv 2 \pmod 3$:

$$(2g+2)/3 = 2m + 2 = \deg(f_0) > \max\{\deg(f_1), \deg(f_2)\}.$$

For $g \equiv 1 \pmod 3$:

$$(2g+1)/3 = 2m + 1 = \deg(f_1) \geq \deg(f_0), \quad \deg(f_1) > \deg(f_2).$$

Note also that f is *cube-free* if and only if f_0, f_1, f_2 are relatively prime.

Solutions and the Nullspace of $\mathcal{C}_f$

Set $\omega = \frac{dX}{Y}$.

Solutions and the Nullspace of $\mathcal{C}_f$

Set $\omega = \frac{dX}{Y}$.

$\mathcal{C}_f$ acts on the $\mathbb{F}_q$-vector space with basis $\{\omega, X\omega, \ldots, X^{g-1}\omega\}$ via

Solutions and the Nullspace of $\mathcal{C}_f$

Set $\omega = \frac{dX}{Y}$.

$\mathcal{C}_f$ acts on the $\mathbb{F}_q$-vector space with basis $\{\omega, X\omega, \ldots, X^{g-1}\omega\}$ via

$$\mathcal{C}_f(X^i\omega) = X^{[i/3]} f_j \omega, \qquad 2i + 2 \equiv j \mod 3$$

Solutions and the Nullspace of $\mathcal{C}_f$

Set $\omega = \frac{dX}{Y}$.

$\mathcal{C}_f$ acts on the $\mathbb{F}_q$-vector space with basis $\{\omega, X\omega, \ldots, X^{g-1}\omega\}$ via

$$\mathcal{C}_f(X^i\omega) = X^{[i/3]} f_j \omega, \qquad 2i + 2 \equiv j \mod 3$$

Thus elements of the nullspace of $\mathcal{C}_f$ correspond to solutions (P_1, P_2, P_3) to (1)

Solutions and the Nullspace of $\mathcal{C}_f$

Set $\omega = \frac{dX}{Y}$.

$\mathcal{C}_f$ acts on the $\mathbb{F}_q$-vector space with basis $\{\omega, X\omega, \ldots, X^{g-1}\omega\}$ via

$$\mathcal{C}_f(X^i\omega) = X^{[i/3]} f_j \omega, \qquad 2i + 2 \equiv j \mod 3$$

Thus elements of the nullspace of $\mathcal{C}_f$ correspond to solutions (P_1, P_2, P_3) to (1) with certain degree restrictions depending on the congruence class of g modulo 3.

Degree Restrictions on Solutions

Degree Restrictions on Solutions

We only consider polynomial solutions P_1, P_2, P_3 to

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0$$

satisfying

Degree Restrictions on Solutions

We only consider polynomial solutions P_1, P_2, P_3 to

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0$$

satisfying

$$\deg(P_3) \leq m,$$

Degree Restrictions on Solutions

We only consider polynomial solutions P_1, P_2, P_3 to

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0$$

satisfying

$$\deg(P_3) \leq m,$$

$$\deg(P_2) \leq \begin{cases} m & \text{if } g \not\equiv 1 \mod 3, \\ m-1 & \text{if } g \equiv 1 \mod 3, \end{cases}$$

Degree Restrictions on Solutions

We only consider polynomial solutions P_1, P_2, P_3 to

$$f_0 P_1 + f_1 P_2 + f_2 P_3 = 0$$

satisfying

$$\deg(P_3) \leq m,$$

$$\deg(P_2) \leq \begin{cases} m & \text{if } g \not\equiv 1 \mod 3, \\ m-1 & \text{if } g \equiv 1 \mod 3, \end{cases}$$

$$\deg(P_1) \leq \begin{cases} m & \text{if } g \not\equiv 1, 2 \mod 3, \\ m-1 & \text{if } g \equiv 1, 2 \mod 3. \end{cases}$$

The a-Number and Heights

The a-Number and Heights

Suppose $g \equiv 0 \mod 3$, so that $m = (g-3)/3$.

The a-Number and Heights

Suppose $g \equiv 0 \mod 3$, so that $m = (g-3)/3$.
We see that E_f has positive a-number if and only if there is a solution (P_1, P_2, P_3) to (1) of height no greater than m.

The a-Number and Heights

Suppose $g \equiv 0 \mod 3$, so that $m = (g-3)/3$.
We see that E_f has positive a-number if and only if there is a solution (P_1, P_2, P_3) to (1) of height no greater than m.

However the solution space itself has height $2m+2$, so we're asking for an abnormally small solution.

The a-Number and Heights

Suppose $g \equiv 0 \mod 3$, so that $m = (g-3)/3$.
We see that E_f has positive a-number if and only if there is a solution (P_1, P_2, P_3) to (1) of height no greater than m.

However the solution space itself has height $2m+2$, so we're asking for an abnormally small solution.

If there is a solution of height $l \leq m$, then all our sought-after solutions are projectively equivalent and $a(E_f) = m + 1 - l$.

Similar statements hold for the cases $g \equiv 1 \mod 3$ and $g \equiv 2 \mod 3$.

Similar statements hold for the cases $g \equiv 1 \mod 3$ and $g \equiv 2 \mod 3$.

However in the case $g \equiv 1 \mod 3$, we require extra degree conditions on our solutions to (1) beyond just the height.

Similar statements hold for the cases $g \equiv 1 \mod 3$ and $g \equiv 2 \mod 3$.

However in the case $g \equiv 1 \mod 3$, we require extra degree conditions on our solutions to (1) beyond just the height.

As noted above, we also have additional conditions beyond just the height for the coefficient vector of (1).

Similar statements hold for the cases $g \equiv 1 \mod 3$ and $g \equiv 2 \mod 3$.

However in the case $g \equiv 1 \mod 3$, we require extra degree conditions on our solutions to (1) beyond just the height.

As noted above, we also have additional conditions beyond just the height for the coefficient vector of (1).

Nevertheless, we are able to compute exactly the number of *cube-free* f of the necessary shape which would have a given $a(E_f)$

Similar statements hold for the cases $g \equiv 1 \mod 3$ and $g \equiv 2 \mod 3$.

However in the case $g \equiv 1 \mod 3$, we require extra degree conditions on our solutions to (1) beyond just the height.

As noted above, we also have additional conditions beyond just the height for the coefficient vector of (1).

Nevertheless, we are able to compute exactly the number of *cube-free* f of the necessary shape which would have a given $a(E_f)$ **if it were also square-free**.

Our Results

Our Results

Suppose $g \equiv 0 \mod 3$ and positive.

Our Results

Suppose $g \equiv 0 \mod 3$ and positive.
For any $a \in \{0, \ldots, g/3\}$ the proportion $P_g(a)$ of cube-free f which would have $a(E_f) = a$ if they were square-free is exactly

Our Results

Suppose $g \equiv 0 \mod 3$ and positive.
For any $a \in \{0, \ldots, g/3\}$ the proportion $P_g(a)$ of cube-free f which would have $a(E_f) = a$ if they were square-free is exactly

$$P_g(g/3) = q^{-2g/3} q,$$

Our Results

Suppose $g \equiv 0 \mod 3$ and positive.
For any $a \in \{0, \ldots, g/3\}$ the proportion $P_g(a)$ of cube-free f which would have $a(E_f) = a$ if they were square-free is exactly

$$P_g(g/3) = q^{-2g/3}q,$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < g/3,$$

Our Results

Suppose $g \equiv 0 \mod 3$ and positive.
For any $a \in \{0, \ldots, g/3\}$ the proportion $P_g(a)$ of cube-free f which would have $a(E_f) = a$ if they were square-free is exactly

$$P_g(g/3) = q^{-2g/3} q,$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < g/3,$$

$$P_g(0) = 1 - q^{-1}.$$

Suppose $g \equiv 2 \mod 3$.

Suppose $g \equiv 2 \mod 3$.
For any $a \in \{0, \ldots, (g+1)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

Suppose $g \equiv 2 \mod 3$.
For any $a \in \{0, \ldots, (g+1)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+1)/3\big) = q^{-2(g+1)/3}q,$$

Suppose $g \equiv 2 \mod 3$.
For any $a \in \{0, \ldots, (g+1)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+1)/3\big) = q^{-2(g+1)/3}q,$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < (g+1)/3,$$

Suppose $g \equiv 2 \mod 3$.
For any $a \in \{0, \ldots, (g+1)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+1)/3\big) = q^{-2(g+1)/3} q,$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < (g+1)/3,$$

$$P_g(0) = 1 - q^{-1}.$$

Suppose $g \equiv 1 \mod 3$.

Suppose $g \equiv 1 \mod 3$.
For any $a \in \{0, \ldots, (g+2)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

Suppose $g \equiv 1 \mod 3$.
For any $a \in \{0, \ldots, (g+2)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+2)/3\big) = q^{-2(g+2)/3}\big(q - 1 + (q+1)^{-1}\big)$$

Suppose $g \equiv 1 \mod 3$.
For any $a \in \{0, \ldots, (g+2)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+2)/3\big) = q^{-2(g+2)/3}\big(q - 1 + (q+1)^{-1}\big)$$

$$P_g\big((g-1)/3\big) = q^{-2(g-1)/3}\big(q - (q+1)^{-1}\big)$$

Suppose $g \equiv 1 \mod 3$.
For any $a \in \{0, \ldots, (g+2)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+2)/3\big) = q^{-2(g+2)/3}\big(q - 1 + (q+1)^{-1}\big)$$

$$P_g\big((g-1)/3\big) = q^{-2(g-1)/3}\big(q - (q+1)^{-1}\big)$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < (g-1)/3,$$

Suppose $g \equiv 1 \mod 3$.
For any $a \in \{0, \ldots, (g+2)/3\}$ the proportion of cube-free f which would have $a(E_f) = a$ if they were square-free is

$$P_g\big((g+2)/3\big) = q^{-2(g+2)/3}\big(q - 1 + (q+1)^{-1}\big)$$

$$P_g\big((g-1)/3\big) = q^{-2(g-1)/3}\big(q - (q+1)^{-1}\big)$$

$$P_g(a) = q^{-2a}(q - q^{-1}) \qquad \text{if } 0 < a < (g-1)/3,$$

$$P_g(0) = 1 - q^{-1}$$

Note we are getting the “correct” proportion of ordinary curves:

Note we are getting the “correct” proportion of ordinary curves:

$$P_g(0) = 1 - q^{-1}.$$

Note we are getting the "correct" proportion of ordinary curves:

$$P_g(0) = 1 - q^{-1}.$$

Moreover, our proportions for higher a-numbers also agree with the computational evidence compiled by Cais, Ellenberg, and Zureik-Brown.

Note we are getting the “correct” proportion of ordinary curves:

$$P_g(0) = 1 - q^{-1}.$$

Moreover, our proportions for higher *a*-numbers also agree with the computational evidence compiled by Cais, Ellenberg, and Zureik-Brown.

Our counting arguments don’t rely on characteristic 3 at all.

Note we are getting the “correct” proportion of ordinary curves:

$$P_g(0) = 1 - q^{-1}.$$

Moreover, our proportions for higher *a*-numbers also agree with the computational evidence compiled by Cais, Ellenberg, and Zureik-Brown.

Our counting arguments don't rely on characteristic 3 at all.
But the connection between *a*-numbers and the analogous linear equation becomes more tenuous for larger characteristic.

Example of a Counting Result

Example of a Counting Result

For the case $g \equiv 0 \mod 3$, we use the following counting result.

Example of a Counting Result

For the case $g \equiv 0 \mod 3$, we use the following counting result.

Fix integers $m \geq l \geq 0$.

Example of a Counting Result

For the case $g \equiv 0 \mod 3$, we use the following counting result.

Fix integers $m \geq l \geq 0$. Let $N_1(m, l)$ denote the number of ordered triples (f_2, f_1, f_0) of relatively prime polynomials such that f_2 is monic of degree $2m + 2$, the degrees of both f_1 and f_0 are no greater than $2m + 2$,

Example of a Counting Result

For the case $g \equiv 0 \mod 3$, we use the following counting result.

Fix integers $m \geq l \geq 0$. Let $N_1(m, l)$ denote the number of ordered triples (f_2, f_1, f_0) of relatively prime polynomials such that f_2 is monic of degree $2m + 2$, the degrees of both f_1 and f_0 are no greater than $2m + 2$, and there is a solution to (1) of height l.

Example of a Counting Result

For the case $g \equiv 0 \mod 3$, we use the following counting result.

Fix integers $m \geq l \geq 0$. Let $N_1(m, l)$ denote the number of ordered triples (f_2, f_1, f_0) of relatively prime polynomials such that f_2 is monic of degree $2m+2$, the degrees of both f_1 and f_0 are no greater than $2m+2$, and there is a solution to (1) of height l. Then

$$N_1(m, l) = \begin{cases} q^{4m-l}q^3(q^2-1)^2 & \text{if } l > 0, \\ q^{4m}q^5(q^2-1) & \text{if } l = 0. \end{cases}$$