

The probability of primality of the order of a genus 2 curve Jacobian

Wouter Castryck

joint with Hendrik Hubrechts, Alessandra Rigato, Andrew Sutherland

K.U. Leuven / M.I.T.

ECC 2010, Redmond

- 1 Alternative heuristics for Galbraith-McKee (genus $g = 1$)
- 2 Adaptation to genus $g = 2$
- 3 Asymptotics for $g \rightarrow \infty$
- 4 Concluding remarks

The genus 1 case: Galbraith-McKee conjecture

- Let \mathbb{F}_q be a finite field of char ≥ 5 .
- Let $E : y^2 = x^3 + Ax + B$ be a random elliptic curve.
 - I.e., (A, B) is taken from the set

$$\{ (A, B) \in \mathbb{F}_q^2 \mid 4A^3 + 27B^2 \neq 0 \}$$

uniformly at random.

- Let $N_E = \#E(\mathbb{F}_q)$.
- Question: what is $P(N_E \text{ is prime})$?
- Motivation: cryptography.

The distribution of N_E

- Hasse's theorem:

$$N_E \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}].$$

- Let's rescale this a bit. . .

- Trace of Frobenius: $T_E = q + 1 - N_E \in [-2\sqrt{q}, 2\sqrt{q}]$.
- Normalized trace of Frobenius: $t_E = T_E/2\sqrt{q} \in [-1, 1]$.

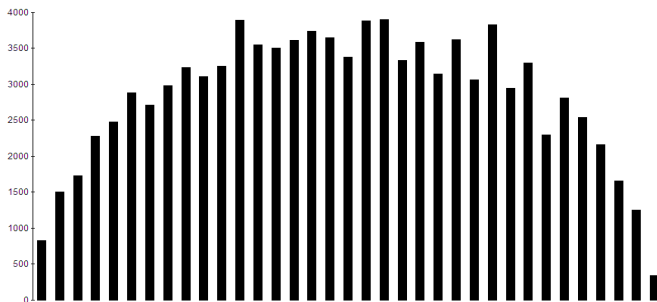
- Birch, Yoshida, Katz-Sarnak: t_E tends to follow a semicircular distribution, i.e.

$$\lim_{q \rightarrow \infty} P(a \leq t_E \leq b) = \int_a^b \frac{2}{\pi} \sqrt{1 - t^2} dt.$$



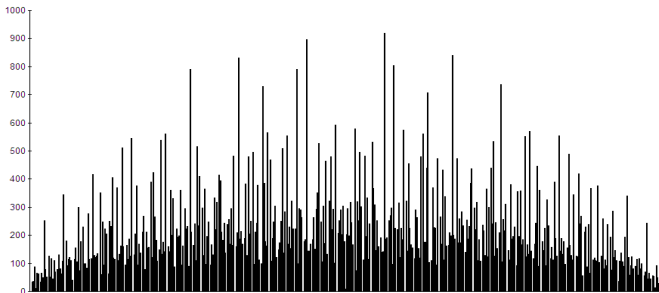
The distribution of N_E

- A histogram of 100.000 curves $y^2 = x^3 + Ax + B$ over \mathbb{F}_{75} , with interval width 15.



Subtleties

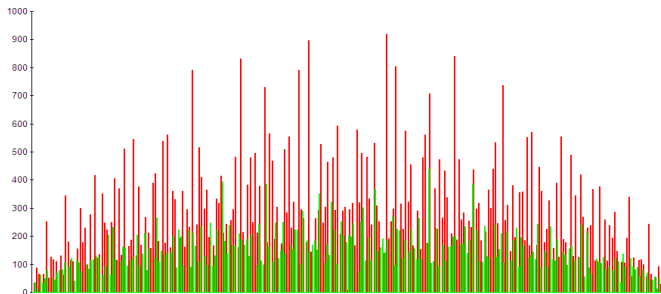
- The limit dissolves the discrete nature of N_E (or T_E).
- Same experiment, but now interval width 1:



- This doesn't seem to converge to a semicircle very 'smoothly' (lots of peaks and valleys).
- Gaps at $T_E \equiv 0 \pmod{7}$ (supersingular curves).

Subtleties

- The limit dissolves the discrete nature of N_E (or T_E).
- Same experiment, but now interval width 1:



- This doesn't seem to converge to a semicircle very 'smoothly' (lots of peaks and valleys).
- Gaps at $T_E \equiv 0 \pmod{7}$ (supersingular curves).

Subtleties

- Easy fact (not very well-known):

$$\lim_{q \rightarrow \infty} P(N_E \text{ is even}) = \frac{2}{3}.$$

- Proof:

- The completing-the-cube map

$$\{\text{square-free } x^3 + ax^2 + bx + c\} \rightarrow \{\text{square-free } x^3 + Ax + B\}$$

is uniform.

- Thus we may assume that E is defined by $y^2 = f(x)$ for a random square-free $f(x) = x^3 + ax^2 + bx + c$.
- N_E is even $\Leftrightarrow E(\mathbb{F}_q)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, and the correspondence is 3-to-1.
- Thus

$$\lim_{q \rightarrow \infty} P(f(x) \text{ is irreducible}) = \lim_{q \rightarrow \infty} \frac{\frac{1}{3}(q^3 - q)}{q^3 - O(q^2)} = \frac{1}{3}. \quad \blacksquare$$

Subtleties

- **Lenstra:** in general, we have

$$\lim_{q \rightarrow \infty} \left(P(\ell \mid N_E) - \begin{cases} \frac{1}{\ell-1} & \text{if } q \not\equiv 1 \pmod{\ell} \\ \frac{\ell}{\ell^2-1} & \text{if } q \equiv 1 \pmod{\ell} \end{cases} \right) = 0$$

for any prime number ℓ not dividing q .

- Thus:

$$\ell \ll q \implies P(\ell \mid N_E) > \frac{1}{\ell}.$$

This suggests that $P(N_E \text{ is prime})$ is smaller than one would naively expect.

Galbraith-McKee conjecture

- Let's try to quantify this (assume $q = p$ is prime):
- Heuristically (but in fact **wrong!** \sim Mertens' theorem),

$$P_1(p) = P(\text{random number is prime}) \approx \prod_{\ell \leq \sqrt{p}+1} \frac{\ell-1}{\ell} \approx \frac{1}{\log p}.$$

- Using Lenstra's estimates, heuristically ('equally wrong'),

$$P_2(p) = P(N_E \text{ is prime}) \approx \prod_{\substack{\ell \nmid p-1 \\ \ell \leq \sqrt{p}+1}} \frac{\ell-2}{\ell-1} \cdot \prod_{\substack{\ell \mid p-1 \\ \ell \leq \sqrt{p}+1}} \frac{\ell^2 - \ell - 1}{\ell^2 - 1}.$$

- So:

$$\frac{P_2(p)}{P_1(p)} \approx \frac{\prod_{\ell \nmid p-1} \frac{\ell-2}{\ell-1} \cdot \prod_{\ell \mid p-1} \frac{\ell^2 - \ell - 1}{\ell^2 - 1}}{\prod_{\ell} \frac{\ell-1}{\ell}}.$$

Galbraith-McKee conjecture

- Rearranging terms gives:

Conjecture (Galbraith-McKee, 2000):

Let

$$c_p = \frac{2}{3} \cdot \prod_{\ell > 2} \left(1 - \frac{1}{(\ell - 1)^2} \right) \cdot \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{1}{(\ell + 1)(\ell - 2)} \right),$$

then

$$\lim_{p \rightarrow \infty} (P_2(p)/P_1(p) - c_p) = 0.$$

- $c_p \in [0.44, 0.62]$.
- Galbraith & McKee give a different heuristic argument!
They use an **analytic Hurwitz-Kronecker class number formula** counting equivalence classes of bivariate quadratic forms with given discriminant.

Random matrices

- Let $\gcd(n, q) = 1$. To an elliptic curve E/\mathbb{F}_q we can associate its n -torsion subgroup

$$E[n] = \{ P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty \}.$$

It is well-known that

$$E[n] \cong \mathbb{Z}/(n) \times \mathbb{Z}/(n).$$

- Let (P, Q) be a $\mathbb{Z}/(n)$ -module basis of $E[n]$, and let $\sigma : E[n] \rightarrow E[n]$ be q th power Frobenius. Then we can write

$$P^\sigma = [\alpha]P + [\beta]Q, \quad Q^\sigma = [\gamma]P + [\delta]Q.$$

- Fact: the matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in (\mathbb{Z}/(n))^{2 \times 2}$$

has trace $\equiv T_E \pmod{n}$ and determinant $\equiv q \pmod{n}$.

Random matrices

- Choosing another basis yields a $\mathrm{GL}_2(\mathbb{Z}/(n))$ -conjugated matrix.
- Thus we can unambiguously associate to E a **conjugacy class** \mathcal{F}_E of matrices of Frobenius (all having trace T_E and determinant q).
- Let $\mathcal{M}_q \subset \mathrm{GL}_2(\mathbb{Z}/(n))$ be the set of matrices of determinant q .

Quasi-theorem:

Let \mathcal{F} be a conjugacy class of matrices of determinant q . Then

$$\left| P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_q} \right| \leq C \frac{n^2}{\sqrt{q}}.$$

- This is likely to follow from:
 - **Chebotarev's density theorem** applied to $X(n) \rightarrow X(1)$ (in progress)
 - **Katz-Sarnak equidistribution** as elaborated by Achter, currently modulo some hypotheses.

Example 1

- What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_q)$?
 - $E[\ell] \subset E(\mathbb{F}_q)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_q -rational points P and Q .
 - Thus: if and only if

$$\mathcal{F}_E = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

- By the random matrix theorem, the chance that this happens is

$$\approx \frac{\# \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}}{\#\mathcal{M}_q}.$$

- $\#\mathcal{M}_q = \ell^3 - \ell$ (exercise).
- Thus

$$P(E[\ell] \subset E(\mathbb{F}_q)) \approx \frac{1}{\ell^3 - \ell}.$$

Example 2

- Alternative proof of

$$\lim_{q \rightarrow \infty} P(N_E \text{ is even}) = \frac{2}{3}.$$

- There are 6 elements of $(\mathbb{Z}/(2))^{2 \times 2}$ having determinant $q \equiv 1$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

- 4 of them have trace 0.
- $P(N_E \text{ is even}) = P(q + 1 - T_E \text{ is even}) = P(T_E \text{ is even}) = 4/6.$

Example 2

- More generally: let ℓ be a prime number not dividing q .
- Exercise:

$$\begin{aligned} \#\{M \in \mathcal{M}_q \mid q + 1 - \text{Tr}(M) \equiv 0\} \\ = \begin{cases} \ell^2 + \ell & \text{if } q \not\equiv 1 \pmod{\ell} \\ \ell^2 & \text{if } q \equiv 1 \pmod{\ell}. \end{cases} \end{aligned}$$

- Recall: $\#\mathcal{M}_q = \ell^3 - \ell$.
- Hence we recover Lenstra's result:

$$P(\ell \mid N_E) \approx \begin{cases} \frac{\ell^2 + \ell}{\ell^3 - \ell} = \frac{1}{\ell - 1} & \text{if } q \not\equiv 1 \pmod{\ell} \\ \frac{\ell^2}{\ell^3 - \ell} = \frac{\ell}{\ell^2 - 1} & \text{if } q \equiv 1 \pmod{\ell}. \end{cases}$$

- 1 Alternative heuristics for Galbraith-McKee (genus $g = 1$)
- 2 Adaptation to genus $g = 2$
- 3 Asymptotics for $g \rightarrow \infty$
- 4 Concluding remarks

The genus 2 case

- Let \mathbb{F}_q be a finite field of char ≥ 3 .
- Let $H : y^2 = f(x)$ be a random genus 2 curve.
 - I.e., $f(x)$ is taken from either

$$\mathcal{H}_6 = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, square-free, of degree } 6 \}$$

or

$$\mathcal{H}_5 = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, square-free, of degree } 5 \}$$

uniformly at random. These are **distinct notions!**

- Let $N_H = \#\text{Jac}(H)(\mathbb{F}_q)$.
- Question: what is $P(N_H \text{ is prime})$?
- Motivation: cryptography.

Distinct notions of randomness

- What is $P(N_H \text{ is even})$?
- Let W_1, \dots, W_6 be the Weierstrass points of H .
- Every non-zero point of $\text{Jac}(H)[2]$ (thought of as a divisor class) contains a unique pair $\{W_i - W_j, W_j - W_i\}$, where $i \neq j$.
 - Proof: use Riemann-Roch and the fact that there are $\binom{6}{2} = 15$ pairs.
- The pair is \mathbb{F}_q -rational iff $\{W_i, W_j\}^\sigma = \{W_i, W_j\}$.
- In case $f(x) \in \mathcal{H}_6$: occurs iff $f(x)$ has a quadratic factor.
 - Exercise: probability $\approx \frac{26}{45}$.
- In case $f(x) \in \mathcal{H}_5$: occurs iff $f(x)$ has a linear or quadratic factor.
 - Exercise: probability $\approx \frac{4}{5}$.

Random matrices in genus 2

- For now, suppose that $f(x)$ is chosen from

$$\mathcal{H}_6 = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, square-free, of degree } 6 \}$$

uniformly at random.

- This works better from a **theoretic** point of view.

Random matrices in genus 2

- Let $\gcd(n, q) = 1$. To a genus 2 curve H/\mathbb{F}_q we can associate the n -torsion subgroup of its Jacobian $A = \text{Jac}(H)$:

$$A[n] = \{ P \in A(\overline{\mathbb{F}}_q) \mid nP = \infty \}.$$

It is well-known that

$$A[n] \cong (\mathbb{Z}/(n))^4.$$

- Let (P_1, P_2, P_3, P_4) be a $\mathbb{Z}/(n)$ -module basis of $A[n]$, then

$$P_1^\sigma = [\alpha_{11}]P_1 + [\alpha_{12}]P_2 + [\alpha_{13}]P_3 + [\alpha_{14}]P_4, \dots$$

- Fact: the matrix

$$F = (\alpha_{ij}) \in (\mathbb{Z}/(n))^{4 \times 4}$$

has determinant $\equiv q \pmod n$ and satisfies $\det(F - \mathbb{I}) \equiv N_H \pmod n$.

Random matrices in genus 2

- Choosing another basis yields a $GL_4(\mathbb{Z}/(n))$ -conjugated matrix.
- Thus we can unambiguously associate to H a **conjugacy class** \mathcal{F}_H of matrices of Frobenius.
- However, a statement like

Let $\mathcal{M}_q \subset GL_4(\mathbb{Z}/(n))$ be the set of matrices of determinant q . Let \mathcal{F} be a conjugacy class of matrices of determinant q . Then

$$\lim_{q \rightarrow \infty} \left(P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_q} \right) = 0.$$

turns out to be **false**.

Symplectic structure of $A[n]$

- Let $\zeta_n \in \overline{\mathbb{F}}_q$ be a primitive n th root of unity.
- The Weil pairing

$$e_n : A[n] \times A[n] \rightarrow \langle \zeta_n \rangle,$$

when composed with the (non-canonical) map

$$\langle \zeta_n \rangle \rightarrow \mathbb{Z}/(n) : \zeta_n^i \mapsto i,$$

is a skew-symmetric, nondegenerate, bilinear pairing $\langle \cdot, \cdot \rangle$ on $A[n]$ (called a **symplectic pairing**).

- Darboux:** $A[n]$ admits a basis with respect to which

$$\langle v, w \rangle = {}^t v \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \cdot w = {}^t v \cdot \Omega \cdot w.$$

Choosing a different root of unity

- Rephrased: a basis $\{P_1, P_2, Q_1, Q_2\}$ is a Darboux basis if

$$e_n(P_i, Q_j) = \zeta_n^{\delta_{ij}}, \quad e_n(P_i, P_j) = e_n(Q_i, Q_j) = 1.$$

- Let $d \in (\mathbb{Z}/(n))^{\times}$.
- If $\{P_1, P_2, Q_1, Q_2\}$ is a Darboux basis with respect to ζ_n , then $\{P_1, P_2, dQ_1, dQ_2\}$ is a Darboux basis with respect to ζ_n^d .
- Denote the matrix of base change with

$$g_d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & d \end{pmatrix}.$$

Choosing a different Darboux basis

- Matrix of base change M between two Darboux bases must satisfy

$${}^t v \cdot \Omega \cdot w = {}^t(Mv) \cdot \Omega \cdot (Mw) = {}^t v \cdot {}^t M \cdot \Omega \cdot M \cdot w$$

for all $v, w \in (\mathbb{Z}/(n))^4$.

- Such matrices are called **symplectic**:

$$\mathrm{Sp}_4(\mathbb{Z}/(n)) = \left\{ M \in (\mathbb{Z}/(n))^{4 \times 4} \mid {}^t M \cdot \Omega \cdot M = \Omega \right\}.$$

- Note, if M is symplectic, then

$${}^t M \cdot {}^t g_d \cdot \Omega \cdot g_d \cdot M = {}^t g_d \cdot {}^t M \cdot \Omega \cdot M \cdot g_d = d\Omega.$$

Symplectic similitudes

- For $d \in (\mathbb{Z}/(n))^{\times}$, define the d -symplectic matrices as

$$\mathrm{GSp}_4^{(d)}(\mathbb{Z}/(n)) = \left\{ M \in (\mathbb{Z}/(n))^{4 \times 4} \mid {}^t M \cdot \Omega \cdot M = d\Omega \right\}.$$

- The symplectic similitudes (generated by $\mathrm{Sp}_4(\mathbb{Z}/(n))$ and $\{g_d\}$):

$$\mathrm{GSp}_4(\mathbb{Z}/(n)) = \bigsqcup_{d \in (\mathbb{Z}/(n))^{\times}} \mathrm{GSp}_4^{(d)}(\mathbb{Z}/(n)).$$

- Because $e_n(P^\sigma, Q^\sigma) = e_n(P, Q)^q$, the matrix F of σ with respect to a Darboux basis satisfies

$${}^t v \cdot {}^t F \cdot \Omega \cdot F \cdot w = {}^t(Fv) \cdot \Omega \cdot (Fw) = q({}^t v \cdot \Omega \cdot w) = {}^t v \cdot (q\Omega) \cdot w$$

for all $v, w \in (\mathbb{Z}/(n))^4$, i.e., F is q -symplectic.

Random matrices in genus 2 (revisited)

- Thus we can unambiguously associate to H an orbit \mathcal{F}_H of $\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))$ under $\mathrm{GSp}_4(\mathbb{Z}/(n))$ -conjugation.
- **Quasi-theorem:**
Let $\mathcal{F} \subset \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))$ be an orbit. Then

$$\left| P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))} \right| \leq C \frac{n^?}{\sqrt{q}}.$$

- This is likely to follow from:
 - A Chebotarev-like statement applied to $\mathcal{A}_2[n] \rightarrow \mathcal{A}_2[1]$
 - Katz-Sarnak equidistribution as elaborated by Achter, currently modulo some hypotheses.

Lenstra's theorem in genus 2

- Let ℓ be a prime number not dividing q .
- One can compute

$$\begin{aligned} \# \left\{ M \in \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(\ell)) \mid \det(M - \mathbb{I}) \equiv 0 \right\} \\ = \begin{cases} \ell^4(\ell + 1)(\ell^2 + 1)(\ell^2 - 2) & \text{if } q \not\equiv 1 \pmod{\ell} \\ \ell^5(\ell^4 - \ell - 1) & \text{if } q \equiv 1 \pmod{\ell}. \end{cases} \end{aligned}$$

- $\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(\ell)) = \#\mathrm{Sp}_4(\mathbb{Z}/(\ell)) = \ell^4(\ell^4 - 1)(\ell^2 - 1)$.
- We conclude:

$$P(\ell \mid N_E) \approx \begin{cases} \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)} & \text{if } q \not\equiv 1 \pmod{\ell} \\ \frac{\ell(\ell^4 - \ell - 1)}{(\ell^4 - 1)(\ell^2 - 1)} & \text{if } q \equiv 1 \pmod{\ell}. \end{cases}$$

Galbraith-McKee conjecture in genus 2

- Notation:

- $P_1(p) = P(\text{random number in generalized Hasse interval is prime})$.
- $P_2(p) = P(N_H \text{ is prime})$.

- Same heuristics yield (suppose again $q = p$ prime):

Conjecture:

Let

$$c_p = \frac{38}{45} \cdot \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{1}{(\ell-1)^2} \frac{\ell}{\ell^2-1} \right).$$

$$\prod_{\ell | p-1, \ell > 2} \left(1 + \frac{1}{(\ell+1)(\ell-2)} - \frac{1}{(\ell+1)(\ell-2)} \frac{\ell^4 - 2\ell^3 + 2\ell^2 - \ell - 1}{\ell^5 - 2\ell^4 + \ell^2 - \ell + 3} \right),$$

then

$$\lim_{p \rightarrow \infty} (P_2(p)/P_1(p) - c_p) = 0.$$

- Now $c_p \in [0.63, 0.80]$.

Imposing a rational Weierstrass point

- Now, let us briefly discuss the case where $f(x)$ is chosen from

$$\mathcal{H}_5 = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, square-free, of degree } 5 \}$$

uniformly at random.

- This is often preferred in practice.
- As we've seen, $P(2 \mid N_H)$ increases from $\frac{26}{45}$ to $\frac{4}{5} \dots$
- What about odd primes ℓ ?

Imposing a rational Weierstrass point (skippable)

- Fact: there exist subsets

$$\mathcal{W}_0, \dots, \mathcal{W}_r \subset \mathrm{GSp}_4^{(g)}(\mathbb{Z}/(2))$$

such that

$F \in \mathcal{W}_i$ if and only if H has i rational Weierstrass points.

- The proof uses an isomorphism $\mathrm{Sym}\{W_1, \dots, W_6\} \cong \mathrm{Sp}_4(\mathbb{Z}/(2))$.

Imposing a rational Weierstrass point (skippable)

- Let $n \nmid q$ be odd and $\mathcal{F} \subset \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))$ be an orbit. Is

$$P(\mathcal{F}_H = \mathcal{F}) \approx \frac{\#\mathcal{F}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))}?$$

- It suffices to prove this for $f(x)$ randomly chosen from

$$\mathcal{H}_5^{(i)} = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, sqf, deg 5, with } i \mathbb{F}_q\text{-roots} \}$$

for $i = 0, \dots, 5$, since these partition \mathcal{H}_5 .

- ... and even from

$$\mathcal{H}_6^{(i)} = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ sqf, deg 6, with } i \mathbb{F}_q\text{-roots} \}$$

for $i = 1, \dots, 6$, since the classical swipe-a-point-to-infinity relation $\mathcal{H}_6^{(i)} \rightarrow \mathcal{H}_5^{(i-1)}$ is generically uniform.

Imposing a rational Weierstrass point (skippable)

- Thus: estimate $P(\mathcal{F}_H = \mathcal{F} \mid \mathcal{F}_{H,2} \subset \mathcal{W}_i)$ in old \mathcal{H}_6 -sense.
- Since n is odd, Chinese remaindering gives

$$\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2n)) \cong \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n)) \oplus \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2)).$$

- We can rewrite

$$P(\mathcal{F}_H = \mathcal{F} \mid \mathcal{F}_{H,2} \subset \mathcal{W}_i) = \frac{P(\mathcal{F}_H = \mathcal{F} \text{ and } \mathcal{F}_{H,2} \subset \mathcal{W}_i)}{P(\mathcal{F}_{H,2} \subset \mathcal{W}_i)} = \frac{P(\mathcal{F}_{H,2n} \subset \mathcal{F} \oplus \mathcal{W}_i)}{P(\mathcal{F}_{H,2} \subset \mathcal{W}_i)}.$$

- By the random matrix statement, we have

$$P(\mathcal{F}_{H,2n} \subset \mathcal{F} \oplus \mathcal{W}_i) \approx \frac{\#(\mathcal{F} \oplus \mathcal{W}_i)}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2n))} = \frac{\#\mathcal{F}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(n))} \cdot \frac{\#\mathcal{W}_i}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2))}$$

and

$$P(\mathcal{F}_{H,2} \subset \mathcal{W}_i) \approx \frac{\#\mathcal{W}_i}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2))}.$$

- Taking the quotient gives the requested result.

Imposing a rational Weierstrass point

- Taking $f(x)$ from \mathcal{H}_5 only affects $P(N_H \text{ is even})$.
- Conclusion: same Galbraith-McKee generalization, with c_p replaced by $\frac{9}{19}c_p \in [0.30, 0.38]$.

- 1 Alternative heuristics for Galbraith-McKee (genus $g = 1$)
- 2 Adaptation this to genus $g = 2$
- 3 Asymptotics for $g \rightarrow \infty$
- 4 Concluding remarks

Asymptotics for $g \rightarrow \infty$

- Let $f(x)$ be chosen from

$\mathcal{H}_6 = \{ f(x) \in \mathbb{F}_q[x] \mid f(x) \text{ monic, square-free, of degree } 2g + 2 \}$
 uniformly at random and let $H : y^2 = f(x)$.

- Let $\mathcal{F}_H \subset \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(n))$ be the orbit of Frobenius of H .

- Quasi-theorem:**

Let $\mathcal{F} \subset \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(n))$ be an orbit. Then

$$\left| P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(n))} \right| \leq C(g) \frac{n^{?(g)}}{\sqrt{q}}.$$

- This is likely to follow from:

- A **Chebotarev-like statement** applied to $\mathcal{A}_g[n] \rightarrow \mathcal{A}_g[1]$
- Katz-Sarnak equidistribution** as elaborated by Achter, currently modulo some hypotheses.

Asymptotics for $g \rightarrow \infty$

- A recursive formula due to **Achter-Holden** allows us to count

$$\# \left\{ M \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(\ell)) \mid \det(M - \mathbb{I}) \equiv 0 \right\}$$

for $g = 2, 3, 4, 5, 6, \dots$

- Seemingly**, the proportion converges to (and fluctuates around)

$$= \begin{cases} 1 - \phi(1/\ell) & \text{if } q \not\equiv 1 \pmod{\ell} \\ 1 - \frac{\phi(1/\ell)}{\phi(1/\ell^2)} & \text{if } q \equiv 1 \pmod{\ell}, \end{cases}$$

where

$$\phi(q) = \prod_{j=1}^{\infty} (1 - q^j)$$

is the **Euler q -series**.

Asymptotics for $g \rightarrow \infty$

- Applying our heuristics gives the following **limiting Galbraith-McKee interval**:

$$\left[\frac{\phi(1/4)^{-1}}{\prod_{k=2}^{\infty} \zeta(k)}, \frac{1}{\prod_{k=1}^{\infty} \zeta(2k+1)} \right] \approx [0.63287, 0.79353].$$

- Genus 2 is actually the least deviating case!

- 1 Alternative heuristics for Galbraith-McKee (genus $g = 1$)
- 2 Adaptation this to genus $g = 2$
- 3 Asymptotics for $g \rightarrow \infty$
- 4 Concluding remarks

Concluding remarks

- Generalizable to arbitrary fields (include supersingular cases).
- Generalizable to $P(N_H$ is prime up to a given cofactor).
- Adaptable to $\#H(\mathbb{F}_q)$ instead of $\#\text{Jac}(H)(\mathbb{F}_q)$, but no nice formulas (matrix count involves non-rational varieties).

Concluding remarks

- Thanks for listening!