

The probability that the number of points on the Jacobian of a genus two curve is prime

Wouter Castryck, Hendrik Hubrechts, Alessandra Rigato

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Central question: what is the probability of success?
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Central question: what is the probability of success?
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Central question: what is the probability of success?
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Central question: what is the probability of success?
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Central question: what is the probability of success?**
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Central question: what is the probability of success?**
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

Part I: the elliptic curve case

- ▶ Say we wish to generate an elliptic curve E/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#E(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct E/\mathbb{F}_q such that $\#E(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random E/\mathbb{F}_q until $\#E(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Central question: what is the probability of success?**
- ▶ For simplicity, throughout this talk we will:
 - ▶ restrict to prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#E(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part I: 'rediscover' a concrete conjecture due to Galbraith & McKee.

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 3$.
- ▶ Let $E : y^2 = x^3 + Ax + B$ be a randomly chosen elliptic curve over \mathbb{F}_p .
 - ▶ That is: (A, B) is chosen from the finite set

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

uniformly at random.

- ▶ By Hasse's theorem, the number N_E of (projective) rational points on E is contained in

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}].$$

- ▶ If N_E were uniformly distributed, we would expect

$$P(N_E \text{ is prime}) \approx \frac{1}{\log p}$$

(under the Riemann hypothesis).

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 3$.
- ▶ Let $E : y^2 = x^3 + Ax + B$ be a randomly chosen elliptic curve over \mathbb{F}_p .
 - ▶ That is: (A, B) is chosen from the finite set

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

uniformly at random.

- ▶ By Hasse's theorem, the number N_E of (projective) rational points on E is contained in

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}].$$

- ▶ If N_E were uniformly distributed, we would expect

$$P(N_E \text{ is prime}) \approx \frac{1}{\log p}$$

(under the Riemann hypothesis).

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 3$.
- ▶ Let $E : y^2 = x^3 + Ax + B$ be a randomly chosen elliptic curve over \mathbb{F}_p .
 - ▶ That is: (A, B) is chosen from the finite set

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

uniformly at random.

- ▶ By Hasse's theorem, the number N_E of (projective) rational points on E is contained in

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}].$$

- ▶ If N_E were uniformly distributed, we would expect

$$P(N_E \text{ is prime}) \approx \frac{1}{\log p}$$

(under the Riemann hypothesis).

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 3$.
- ▶ Let $E : y^2 = x^3 + Ax + B$ be a randomly chosen elliptic curve over \mathbb{F}_p .
 - ▶ That is: (A, B) is chosen from the finite set

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

uniformly at random.

- ▶ By Hasse's theorem, the number N_E of (projective) rational points on E is contained in

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}].$$

- ▶ If N_E were uniformly distributed, we would expect

$$P(N_E \text{ is prime}) \approx \frac{1}{\log p}$$

(under the Riemann hypothesis).

- ▶ For growing ρ , N_E tends to follow a semicircular distribution.

- ▶ Translate to obtain

$$T_E = N_E - (\rho + 1) \in [-2\sqrt{\rho}, 2\sqrt{\rho}]$$

(trace of Frobenius).

- ▶ Rescale to obtain

$$t_E = T_E/2\sqrt{\rho} \in [-1, 1].$$

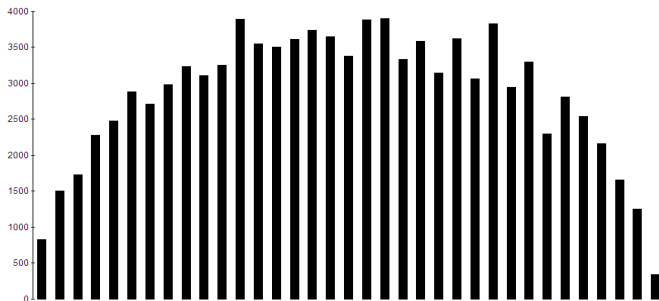
- ▶ Then for any $a < b$ in $[-1, 1]$

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

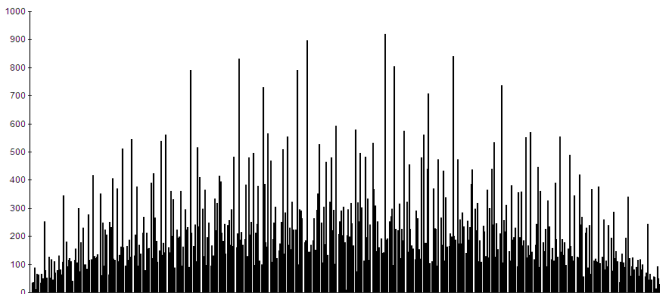


- ▶ Proof of Birch uses theory of bivariate quadratic forms.

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

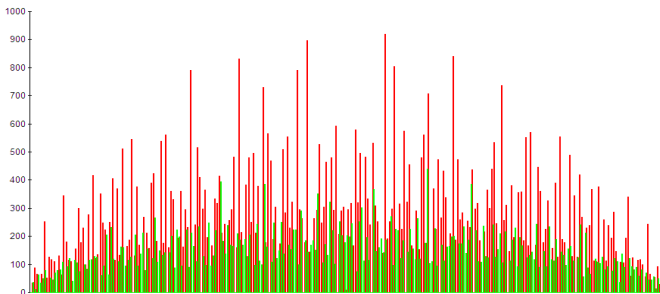


- ▶ The limit hides some subtleties that are related to the discrete nature of N_E (or T_E).
- ▶ Same experiment, but now interval width 1:



- ▶ 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).

- ▶ The limit hides some subtleties that are related to 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).

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

- ▶ Easy fact (not very well-known):

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

- ▶ 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 $\Leftrightarrow E(\mathbb{F}_p)$ has 2-torsion $\Leftrightarrow f(x)$ is reducible.
- ▶ The *irreducible* $f(x)$ are precisely the minimal polynomials of all $\theta \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$ and the correspondence is 3-to-1.
- ▶ Thus

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

Theorem (Lenstra)

Let ℓ be any prime number, then

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

- ▶ Lenstra used this for estimating the complexity of his elliptic curve based integer factorization algorithm.
- ▶ Error term is $O(\ell/\sqrt{p})$.
- ▶ Note that in particular:

$$\ell \ll p \implies P(\ell \mid N_E) > \frac{1}{\ell},$$

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

Theorem (Lenstra)

Let ℓ be any prime number, then

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

- ▶ Lenstra used this for estimating the complexity of his elliptic curve based integer factorization algorithm.
- ▶ Error term is $O(\ell/\sqrt{p})$.
- ▶ Note that in particular:

$$\ell \ll p \implies P(\ell \mid N_E) > \frac{1}{\ell},$$

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

Theorem (Lenstra)

Let ℓ be any prime number, then

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

- ▶ Lenstra used this for estimating the complexity of his elliptic curve based integer factorization algorithm.
- ▶ Error term is $O(\ell/\sqrt{p})$.
- ▶ Note that in particular:

$$\ell \ll p \implies P(\ell \mid N_E) > \frac{1}{\ell},$$

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

Theorem (Lenstra)

Let ℓ be any prime number, then

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

- ▶ Lenstra used this for estimating the complexity of his elliptic curve based integer factorization algorithm.
- ▶ Error term is $O(\ell/\sqrt{p})$.
- ▶ Note that in particular:

$$\ell \ll p \implies P(\ell \mid N_E) > \frac{1}{\ell},$$

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

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.
► There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{2}{\ell-1} \frac{\#X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.
► There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{\frac{\ell-1}{2} \#X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.
► There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{2}{\ell-1} \frac{\#X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.

- There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{\frac{2}{\ell-1} \# X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.
► There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{\frac{2}{\ell-1} \# X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Proof sketch in case $p \not\equiv 1 \pmod{\ell}$:

- One clearly has

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains a point of order } \ell.$$

- $p \not\equiv 1 \pmod{\ell}$ then implies that

$$\ell \mid N_E \iff E(\mathbb{F}_p) \text{ contains exactly } \ell - 1 \text{ points of order } \ell.$$

- These appear in $\frac{\ell-1}{2}$ pairs $\pm P$.
► There exists a curve $X_1(\ell)/\mathbb{F}_p$ whose \mathbb{F}_p -rational points are in 1-1-correspondence with the set

$$\{(E, \pm P) \mid E \text{ ell. curve } / \mathbb{F}_p, P \in E(\mathbb{F}_p) \text{ has order } \ell\}$$

(e.g. defined by $\psi_\ell(E_j)(x) \in \mathbb{F}_p(j, x)$).

- Therefore,

$$P(\ell \mid N_E) \approx \frac{\frac{2}{\ell-1} \# X_1(\ell)(\mathbb{F}_p)}{2p} = \frac{1}{\ell-1} + O(\ell/\sqrt{p}).$$

► Summary:

► If $\ell \nmid p-1$ then

$$P(\ell \mid N_E) \approx \frac{1}{\ell-1} \quad \text{vs.} \quad P(\ell \mid \text{random number}) \approx \frac{1}{\ell}$$

↓

$$P(\ell \nmid N_E) \approx \frac{\ell-2}{\ell-1} \quad \text{vs.} \quad P(\ell \nmid \text{random number}) \approx \frac{\ell-1}{\ell}$$

► If $\ell \mid p-1$ then

$$P(\ell \mid N_E) \approx \frac{\ell}{\ell^2-1} \quad \text{vs.} \quad P(\ell \mid \text{random number}) \approx \frac{1}{\ell}$$

↓

$$P(\ell \nmid N_E) \approx \frac{\ell^2-\ell-1}{\ell^2-1} \quad \text{vs.} \quad P(\ell \nmid \text{random number}) \approx \frac{\ell-1}{\ell}.$$

► Summary:

► If $\ell \nmid p - 1$ then

$$P(\ell \mid N_E) \approx \frac{1}{\ell - 1} \quad \text{vs.} \quad P(\ell \mid \text{random number}) \approx \frac{1}{\ell}$$

↓

$$P(\ell \nmid N_E) \approx \frac{\ell - 2}{\ell - 1} \quad \text{vs.} \quad P(\ell \nmid \text{random number}) \approx \frac{\ell - 1}{\ell}$$

► If $\ell \mid p - 1$ then

$$P(\ell \mid N_E) \approx \frac{\ell}{\ell^2 - 1} \quad \text{vs.} \quad P(\ell \mid \text{random number}) \approx \frac{1}{\ell}$$

↓

$$P(\ell \nmid N_E) \approx \frac{\ell^2 - \ell - 1}{\ell^2 - 1} \quad \text{vs.} \quad P(\ell \nmid \text{random number}) \approx \frac{\ell - 1}{\ell}.$$

► Summary:

► If $l \nmid p - 1$ then

$$P(l \mid N_E) \approx \frac{1}{l-1} \quad \text{vs.} \quad P(l \mid \text{random number}) \approx \frac{1}{l}$$

↓

$$P(l \nmid N_E) \approx \frac{l-2}{l-1} \quad \text{vs.} \quad P(l \nmid \text{random number}) \approx \frac{l-1}{l}$$

► If $l \mid p - 1$ then

$$P(l \mid N_E) \approx \frac{l}{l^2 - 1} \quad \text{vs.} \quad P(l \mid \text{random number}) \approx \frac{1}{l}$$

↓

$$P(l \nmid N_E) \approx \frac{l^2 - l - 1}{l^2 - 1} \quad \text{vs.} \quad P(l \mid \text{random number}) \approx \frac{l-1}{l}.$$

- ▶ Let $P_1(p)$ be the probability that a random number from the Hasse interval is prime.
- ▶ Let $P_2(p) = P(N_E \text{ is prime})$.
- ▶ Heuristically,

$$P_1(p) \approx \prod_{\ell \leq \sqrt{p}} \frac{\ell - 1}{\ell} \approx \frac{p}{\log p}.$$

- ▶ Heuristically (using Lenstra's estimates),

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

- ▶ So:

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

- ▶ Let $P_1(p)$ be the probability that a random number from the Hasse interval is prime.
- ▶ Let $P_2(p) = P(N_E \text{ is prime})$.
- ▶ Heuristically,

$$P_1(p) \approx \prod_{\ell \leq \sqrt{p}} \frac{\ell - 1}{\ell} \approx \frac{p}{\log p}.$$

- ▶ Heuristically (using Lenstra's estimates),

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

- ▶ So:

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

- ▶ Let $P_1(p)$ be the probability that a random number from the Hasse interval is prime.
- ▶ Let $P_2(p) = P(N_E \text{ is prime})$.
- ▶ Heuristically,

$$P_1(p) \approx \prod_{\ell \leq \sqrt{p}} \frac{\ell - 1}{\ell} \approx \frac{p}{\log p}.$$

- ▶ Heuristically (using Lenstra's estimates),

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

- ▶ So:

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

- ▶ Let $P_1(p)$ be the probability that a random number from the Hasse interval is prime.
- ▶ Let $P_2(p) = P(N_E \text{ is prime})$.
- ▶ Heuristically,

$$P_1(p) \approx \prod_{\ell \leq \sqrt{p}} \frac{\ell - 1}{\ell} \approx \frac{p}{\log p}.$$

- ▶ Heuristically (using Lenstra's estimates),

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

- ▶ So:

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

Conjecture (Galbraith-McKee)

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 different heuristics!
- ▶ They use the analytic Hurwitz-Kronecker class number formula

$$H(t^2 - 4p) = \frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \left\{ \left(1 - \left(\frac{t^2 - 4p}{\ell} \right) / \ell \right)^{-1} \psi_3(\ell) \right\}$$

counting equivalence classes of bivariate quadratic forms.

Conjecture (Galbraith-McKee)

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 different heuristics!
- ▶ They use the analytic Hurwitz-Kronecker class number formula

$$H(t^2 - 4p) = \frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \left\{ \left(1 - \left(\frac{t^2 - 4p}{\ell} \right) / \ell \right)^{-1} \psi_3(\ell) \right\}$$

counting equivalence classes of bivariate quadratic forms.

Conjecture (Galbraith-McKee)

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 different heuristics!
- ▶ They use the analytic Hurwitz-Kronecker class number formula

$$H(t^2 - 4p) = \frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \left\{ \left(1 - \left(\frac{t^2 - 4p}{\ell} \right) / \ell \right)^{-1} \psi_3(\ell) \right\}$$

counting equivalence classes of bivariate quadratic forms.

Conjecture (Galbraith-McKee)

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 different heuristics!
- ▶ They use the analytic Hurwitz-Kronecker class number formula

$$H(t^2 - 4p) = \frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \left\{ \left(1 - \left(\frac{t^2 - 4p}{\ell} \right) / \ell \right)^{-1} \psi_3(\ell) \right\}$$

counting equivalence classes of bivariate quadratic forms.

- ▶ If one follows our heuristics to estimate the number of elliptic curves with given trace t , one obtains

$$\frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \text{'correcting factors'}.$$

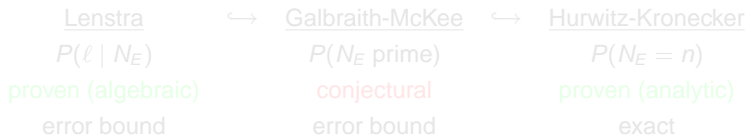
- ▶ E.g. for $\ell = 2$, the correcting factor is
 - ▶ $2/3$ if t is odd,
 - ▶ $4/3$ if t is even.
- ▶ This turns out to be a reformulation of the analytic Hurwitz-Kronecker class number formula!
- ▶ Schematically:

<u>Lenstra</u>	\longleftrightarrow	<u>Galbraith-McKee</u>	\longleftrightarrow	<u>Hurwitz-Kronecker</u>
$P(\ell \mid N_E)$		$P(N_E \text{ prime})$		$P(N_E = n)$
proven (algebraic)		conjectural		proven (analytic)
error bound		error bound		exact

- ▶ If one follows our heuristics to estimate the number of elliptic curves with given trace t , one obtains

$$\frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \text{'correcting factors'}.$$

- ▶ E.g. for $\ell = 2$, the correcting factor is
 - ▶ $2/3$ if t is odd,
 - ▶ $4/3$ if t is even.
- ▶ This turns out to be a reformulation of the analytic Hurwitz-Kronecker class number formula!
- ▶ Schematically:



- ▶ If one follows our heuristics to estimate the number of elliptic curves with given trace t , one obtains

$$\frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \text{'correcting factors'}.$$

- ▶ E.g. for $\ell = 2$, the correcting factor is
 - ▶ $2/3$ if t is odd,
 - ▶ $4/3$ if t is even.
- ▶ This turns out to be a reformulation of the analytic Hurwitz-Kronecker class number formula!
- ▶ Schematically:

<u>Lenstra</u>	\longleftrightarrow	<u>Galbraith-McKee</u>	\longleftrightarrow	<u>Hurwitz-Kronecker</u>
$P(\ell \mid N_E)$		$P(N_E \text{ prime})$		$P(N_E = n)$
proven (algebraic)		conjectural		proven (analytic)
error bound		error bound		exact

- ▶ If one follows our heuristics to estimate the number of elliptic curves with given trace t , one obtains

$$\frac{\sqrt{4p - t^2}}{\pi} \cdot \prod_{\ell} \text{'correcting factors'}.$$

- ▶ E.g. for $\ell = 2$, the correcting factor is
 - ▶ $2/3$ if t is odd,
 - ▶ $4/3$ if t is even.
- ▶ This turns out to be a reformulation of the analytic Hurwitz-Kronecker class number formula!
- ▶ Schematically:

<u>Lenstra</u>	\hookrightarrow	<u>Galbraith-McKee</u>	\hookrightarrow	<u>Hurwitz-Kronecker</u>
$P(\ell \mid N_E)$		$P(N_E \text{ prime})$		$P(N_E = n)$
proven (algebraic)		conjectural		proven (analytic)
error bound		error bound		exact

The random matrix model

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

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

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 p th power Frobenius. Then we can write

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

- ▶ Important fact: the matrix

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

has trace $\equiv T_F \pmod n$ and determinant $\equiv p \pmod n$

The random matrix model

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

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

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 p th power Frobenius. Then we can write

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

- ▶ Important fact: the matrix

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

has trace $\equiv T_F \pmod n$ and determinant $\equiv p \pmod n$

The random matrix model

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

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

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 p th power Frobenius. Then we can write

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

- ▶ Important 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 $\equiv p \pmod n$.

- ▶ A different choice of basis results in 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 p).
- ▶ Let $\mathcal{M}_p \subset \mathrm{GL}_2(\mathbb{Z}/(n))$ be the set of *all* matrices of determinant p .

Theorem (Katz-Sarnak, Achter, C.-Hubrechts)

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

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_p} \right) = 0.$$

The error term is Cn^2/\sqrt{p} , where C is an explicit and absolute constant.

- ▶ Idea of proof: apply Chebotarev's density theorem to the modular covering $X(n) \rightarrow X(1)$.

- ▶ A different choice of basis results in a $GL_2(\mathbb{Z}/(n))$ -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 p).
- ▶ Let $\mathcal{M}_p \subset GL_2(\mathbb{Z}/(n))$ be the set of *all* matrices of determinant p .

Theorem (Katz-Sarnak, Achter, C.-Hubrechts)

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

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_p} \right) = 0.$$

The error term is Cn^2/\sqrt{p} , where C is an explicit and absolute constant.

- ▶ Idea of proof: apply Chebotarev's density theorem to the modular covering $X(n) \rightarrow X(1)$.

- ▶ A different choice of basis results in 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 p).
- ▶ Let $\mathcal{M}_p \subset \mathrm{GL}_2(\mathbb{Z}/(n))$ be the set of *all* matrices of determinant p .

Theorem (Katz-Sarnak, Achter, C.-Hubrechts)

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

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_p} \right) = 0.$$

The error term is Cn^2/\sqrt{p} , where C is an explicit and absolute constant.

- ▶ Idea of proof: apply Chebotarev's density theorem to the modular covering $X(n) \rightarrow X(1)$.

- ▶ A different choice of basis results in 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 p).
- ▶ Let $\mathcal{M}_p \subset \mathrm{GL}_2(\mathbb{Z}/(n))$ be the set of *all* matrices of determinant p .

Theorem (Katz-Sarnak, Achter, C.-Hubrechts)

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

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_p} \right) = 0.$$

The error term is Cn^2/\sqrt{p} , where C is an explicit and absolute constant.

- ▶ Idea of proof: apply Chebotarev's density theorem to the modular covering $X(n) \rightarrow X(1)$.

- ▶ A different choice of basis results in 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 p).
- ▶ Let $\mathcal{M}_p \subset \mathrm{GL}_2(\mathbb{Z}/(n))$ be the set of *all* matrices of determinant p .

Theorem (Katz-Sarnak, Achter, C.-Hubrechts)

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

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_E = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathcal{M}_p} \right) = 0.$$

The error term is Cn^2/\sqrt{p} , where C is an explicit and absolute constant.

- ▶ Idea of proof: apply Chebotarev's density theorem to the modular covering $X(n) \rightarrow X(1)$.

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Example to get in touch with the flavor:
- ▶ What proportion of elliptic curves satisfies $E[\ell] \subset E(\mathbb{F}_p)$?
 - ▶ $E[\ell] \subset E(\mathbb{F}_p)$ if and only if $E[\ell]$ has a basis consisting of \mathbb{F}_p -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

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

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

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

- ▶ Proving Lenstra's results now boils down to counting matrices:
- ▶ Exercise:

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

- ▶ Recall: $\#\mathcal{M}_p = \ell^3 - \ell$.

- ▶ Proving Lenstra's results now boils down to counting matrices:
- ▶ Exercise:

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

- ▶ Recall: $\#\mathcal{M}_p = \ell^3 - \ell$.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#J(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#J(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#J(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Again: what is the probability of success?
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#J(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Again: what is the probability of success?
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Again: what is the probability of success?
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ Again: what is the probability of success?
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Again: what is the probability of success?**
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Again: what is the probability of success?**
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

Part II: the genus 2 case

- ▶ Say we wish to generate a genus 2 hyperelliptic curve H/\mathbb{F}_q suitable for use in discrete-log based cryptosystems.
- ▶ SPH attack $\rightsquigarrow \#\mathbb{J}(H)(\mathbb{F}_q)$ should have a large prime factor.
- ▶ Two approaches:
 - ▶ Fix n and construct H/\mathbb{F}_q such that $\#\mathbb{J}(H)(\mathbb{F}_q) = n$ (using CM).
 - ▶ Fix q and try random H/\mathbb{F}_q until $\#\mathbb{J}(H)(\mathbb{F}_q)$ has a large prime factor (using point counting algorithms).
- ▶ **Again: what is the probability of success?**
- ▶ For simplicity, we will:
 - ▶ work over prime fields \mathbb{F}_p ;
 - ▶ only consider the probability that $\#\mathbb{J}(H)(\mathbb{F}_p)$ is prime.
- ▶ Aim of Part II: generalize the Galbraith-McKee conjecture.

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 2$.
- ▶ Let $H : y^2 = f(x)$ be a randomly chosen genus 2 curve over \mathbb{F}_p . That is:

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ monic and squarefree, } \deg f(x) = 5\}$$

uniformly at random.

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random.

- ▶ By Tate's theorem, the number N_H of rational points on $\mathbb{J}(H)$ is contained in

$$[(p+1)^2 - 4(p + \sqrt{p} + 1)\sqrt{p}, (p+1)^2 + 4(p + \sqrt{p} + 1)\sqrt{p}].$$

- ▶ First remark: the above notions are fundamentally different!

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 2$.
- ▶ Let $H : y^2 = f(x)$ be a randomly chosen genus 2 curve over \mathbb{F}_p . That is:

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ monic and squarefree, } \deg f(x) = 5\}$$

uniformly at random.

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random.

- ▶ By Tate's theorem, the number N_H of rational points on $\mathbb{J}(H)$ is contained in

$$[(p+1)^2 - 4(p + \sqrt{p} + 1)\sqrt{p}, (p+1)^2 + 4(p + \sqrt{p} + 1)\sqrt{p}].$$

- ▶ First remark: the above notions are fundamentally different!

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 2$.
- ▶ Let $H : y^2 = f(x)$ be a randomly chosen genus 2 curve over \mathbb{F}_p . That is:

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ monic and squarefree, } \deg f(x) = 5\}$$

uniformly at random.

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random.

- ▶ By Tate's theorem, the number N_H of rational points on $\mathbb{J}(H)$ is contained in

$$[(p+1)^2 - 4(p + \sqrt{p} + 1)\sqrt{p}, (p+1)^2 + 4(p + \sqrt{p} + 1)\sqrt{p}].$$

- ▶ First remark: the above notions are fundamentally different!

- ▶ Let \mathbb{F}_p be a finite prime field, $p > 2$.
- ▶ Let $H : y^2 = f(x)$ be a randomly chosen genus 2 curve over \mathbb{F}_p . That is:

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ monic and squarefree, } \deg f(x) = 5\}$$

uniformly at random.

- ▶ Either $f(x)$ is chosen from the finite set

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random.

- ▶ By Tate's theorem, the number N_H of rational points on $\mathbb{J}(H)$ is contained in

$$[(p+1)^2 - 4(p + \sqrt{p} + 1)\sqrt{p}, (p+1)^2 + 4(p + \sqrt{p} + 1)\sqrt{p}].$$

- ▶ First remark: the above notions are fundamentally different!

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

► Proof:

- Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- $P_i - P_j \not\sim 0$ by Riemann-Roch.
- All pairs are distinct:
 - $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

- ▶ Proof:
- ▶ Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- ▶ $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- ▶ $P_i - P_j \not\sim 0$ by Riemann-Roch.
- ▶ All pairs are distinct:
 - ▶ $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - ▶ $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- ▶ There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

- ▶ Proof:
- ▶ Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- ▶ $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- ▶ $P_i - P_j \not\sim 0$ by Riemann-Roch.
- ▶ All pairs are distinct:
 - ▶ $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - ▶ $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- ▶ There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

- ▶ Proof:
- ▶ Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- ▶ $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- ▶ $P_i - P_j \not\sim 0$ by Riemann-Roch.
- ▶ All pairs are distinct:
 - ▶ $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - ▶ $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- ▶ There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

- ▶ Proof:
- ▶ Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- ▶ $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- ▶ $P_i - P_j \not\sim 0$ by Riemann-Roch.
- ▶ All pairs are distinct:
 - ▶ $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - ▶ $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- ▶ There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

Lemma

Let H/\mathbb{F}_q be a curve of genus 2. Each of the 15 non-trivial 2-torsion points of $\mathbb{J}(H)$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where P_i and P_j are distinct Weierstrass points.

- ▶ Proof:
- ▶ Think of the P_i as the points $(x_i, 0)$ on some Weierstrass model $y^2 = f(x)$ with $\deg f = 6$.
- ▶ $2P_i - 2P_j \sim 0$, hence $P_i - P_j \sim P_j - P_i$ has 2-torsion.
- ▶ $P_i - P_j \not\sim 0$ by Riemann-Roch.
- ▶ All pairs are distinct:
 - ▶ $(P_1 - P_2) - (P_1 - P_3) \sim P_2 - P_3$.
 - ▶ $(P_1 - P_2) - (P_3 - P_4) \sim P_5 - P_6$.
- ▶ There are $\binom{6}{2} = 15$ such point pairs, so every 2-torsion points must appear in this way. ■

- ▶ Corollary: $\mathbb{J}(H)$ has 2-torsion if and only if H has an ' \mathbb{F}_p -rational' Weierstrass point pair:
 - ▶ either two \mathbb{F}_p -rational Weierstrass points,
 - ▶ either two Weierstrass points that are swapped by Galois conjugation.
- ▶ In degree 6:
 - ▶ $f(x)$ has two linear factors or
 - ▶ $f(x)$ has a quadratic factor.

Exercise: probability that this happens is $\approx 26/45 \approx 58\%$.

- ▶ In degree 5, our curve automatically has an \mathbb{F}_p -rational Weierstrass point. Thus there is 2-torsion if
 - ▶ $f(x)$ has a linear factor or
 - ▶ $f(x)$ has a quadratic factor

or in other words if $f(x)$ is reducible! The probability that this happens is $\approx 4/5 = 80\%$ (same proof as before).

- ▶ Luckily, for all $\ell > 2$ the probabilities are no longer affected (follows from the random matrix model).

- ▶ Corollary: $\mathbb{J}(H)$ has 2-torsion if and only if H has an ' \mathbb{F}_p -rational' Weierstrass point pair:
 - ▶ either two \mathbb{F}_p -rational Weierstrass points,
 - ▶ either two Weierstrass points that are swapped by Galois conjugation.
- ▶ In degree 6:
 - ▶ $f(x)$ has two linear factors or
 - ▶ $f(x)$ has a quadratic factor.

Exercise: probability that this happens is $\approx 26/45 \approx 58\%$.

- ▶ In degree 5, our curve automatically has an \mathbb{F}_p -rational Weierstrass point. Thus there is 2-torsion if
 - ▶ $f(x)$ has a linear factor or
 - ▶ $f(x)$ has a quadratic factor
 or in other words if $f(x)$ is reducible! The probability that this happens is $\approx 4/5 = 80\%$ (same proof as before).
- ▶ Luckily, for all $\ell > 2$ the probabilities are no longer affected (follows from the random matrix model).

- ▶ Corollary: $\mathbb{J}(H)$ has 2-torsion if and only if H has an \mathbb{F}_p -rational Weierstrass point pair:
 - ▶ either two \mathbb{F}_p -rational Weierstrass points,
 - ▶ either two Weierstrass points that are swapped by Galois conjugation.
- ▶ In degree 6:
 - ▶ $f(x)$ has two linear factors or
 - ▶ $f(x)$ has a quadratic factor.

Exercise: probability that this happens is $\approx 26/45 \approx 58\%$.

- ▶ In degree 5, our curve automatically has an \mathbb{F}_p -rational Weierstrass point. Thus there is 2-torsion if
 - ▶ $f(x)$ has a linear factor or
 - ▶ $f(x)$ has a quadratic factor

or in other words if $f(x)$ is reducible! The probability that this happens is $\approx 4/5 = 80\%$ (same proof as before).

- ▶ Luckily, for all $\ell > 2$ the probabilities are no longer affected (follows from the random matrix model).

- ▶ Corollary: $\mathbb{J}(H)$ has 2-torsion if and only if H has an \mathbb{F}_p -rational Weierstrass point pair:
 - ▶ either two \mathbb{F}_p -rational Weierstrass points,
 - ▶ either two Weierstrass points that are swapped by Galois conjugation.
- ▶ In degree 6:
 - ▶ $f(x)$ has two linear factors or
 - ▶ $f(x)$ has a quadratic factor.

Exercise: probability that this happens is $\approx 26/45 \approx 58\%$.

- ▶ In degree 5, our curve automatically has an \mathbb{F}_p -rational Weierstrass point. Thus there is 2-torsion if
 - ▶ $f(x)$ has a linear factor or
 - ▶ $f(x)$ has a quadratic factor

or in other words if $f(x)$ is reducible! The probability that this happens is $\approx 4/5 = 80\%$ (same proof as before).

- ▶ Luckily, for all $\ell > 2$ the probabilities are no longer affected (follows from the random matrix model).

The random matrix model in genus 2

- ▶ Let $\gcd(n, p) = 1$. To a genus 2 curve H/\mathbb{F}_p we can associate the n -torsion subgroup of $\mathbb{J}(H)$

$$\mathbb{J}(H)[n] = \{ P \in \mathbb{J}(H) (\overline{\mathbb{F}}_p) \mid [n]P = O \}.$$

It is well-known that

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

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

$$P^\sigma = [\alpha]P + [\beta]Q + [\gamma]R + [\delta]S, \dots$$

- ▶ Important fact: the corresponding matrix in

$$(\mathbb{Z}/(n))^{4 \times 4}$$

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



The random matrix model in genus 2

- ▶ Let $\gcd(n, p) = 1$. To a genus 2 curve H/\mathbb{F}_p we can associate the n -torsion subgroup of $\mathbb{J}(H)$

$$\mathbb{J}(H)[n] = \{ P \in \mathbb{J}(H) (\overline{\mathbb{F}}_p) \mid [n]P = O \}.$$

It is well-known that

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

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

$$P^\sigma = [\alpha]P + [\beta]Q + [\gamma]R + [\delta]S, \dots$$

- ▶ Important fact: the corresponding matrix in

$$(\mathbb{Z}/(n))^{4 \times 4}$$

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



The random matrix model in genus 2

- ▶ Let $\gcd(n, p) = 1$. To a genus 2 curve H/\mathbb{F}_p we can associate the n -torsion subgroup of $\mathbb{J}(H)$

$$\mathbb{J}(H)[n] = \{ P \in \mathbb{J}(H) (\overline{\mathbb{F}}_p) \mid [n]P = O \}.$$

It is well-known that

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

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

$$P^\sigma = [\alpha]P + [\beta]Q + [\gamma]R + [\delta]S, \dots$$

- ▶ Important fact: the corresponding matrix in

$$(\mathbb{Z}/(n))^{4 \times 4}$$

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

- ▶ However: we will no longer consider *any* basis!
- ▶ $\mathbb{J}(H)$ is endowed with a *symplectic structure*, induced by the Weil pairing. We will restrict to symplectic bases.
- ▶ Now we associate to H an orbit under $\mathrm{GSp}_4(\mathbb{Z}/(n))$ -conjugation of matrices in $\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(n))$. Denote this orbit by \mathcal{F}_H .

Theorem (Katz-Sarnak, Achter, work to be done)

Let $H : y^2 = f(x)$ be a genus 2 curve, where $f(x)$ is chosen from

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random. Let \mathcal{F} be an orbit under $\mathrm{GSp}_4(\mathbb{Z}/(n))$ -conjugation. Then

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(n))} \right) = 0.$$

- ▶ However: we will no longer consider *any* basis!
- ▶ $\mathbb{J}(H)$ is endowed with a *symplectic structure*, induced by the Weil pairing. We will restrict to symplectic bases.
- ▶ Now we associate to H an orbit under $\text{GSp}_4(\mathbb{Z}/(n))$ -conjugation of matrices in $\text{Sp}_4^{(p)}(\mathbb{Z}/(n))$. Denote this orbit by \mathcal{F}_H .

Theorem (Katz-Sarnak, Achter, work to be done)

Let $H : y^2 = f(x)$ be a genus 2 curve, where $f(x)$ is chosen from

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random. Let \mathcal{F} be an orbit under $\text{GSp}_4(\mathbb{Z}/(n))$ -conjugation. Then

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\text{Sp}_4^{(p)}(\mathbb{Z}/(n))} \right) = 0.$$

- ▶ However: we will no longer consider *any* basis!
- ▶ $\mathbb{J}(H)$ is endowed with a *symplectic structure*, induced by the Weil pairing. We will restrict to symplectic bases.
- ▶ Now we associate to H an orbit under $\mathrm{GSp}_4(\mathbb{Z}/(n))$ -conjugation of matrices in $\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(n))$. Denote this orbit by \mathcal{F}_H .

Theorem (Katz-Sarnak, Achter, work to be done)

Let $H : y^2 = f(x)$ be a genus 2 curve, where $f(x)$ is chosen from

$$\{f(x) \in \mathbb{F}_p[x] \mid f(x) \text{ squarefree, } \deg f(x) = 6\}$$

uniformly at random. Let \mathcal{F} be an orbit under $\mathrm{GSp}_4(\mathbb{Z}/(n))$ -conjugation. Then

$$\lim_{p \rightarrow \infty} \left(P(\mathcal{F}_H = \mathcal{F}) - \frac{\#\mathcal{F}}{\#\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(n))} \right) = 0.$$

► So: counting appropriate matrices!

► $\#\mathrm{Sp}_4(\mathbb{Z}/(\ell)) = \#\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell)) = \ell^4(\ell^4 - 1)(\ell^2 - 1)$

► We guess (via interpolation) that the proportion of $M \in \mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell))$ for which $\chi(M)(1) = 0$ equals

$$\begin{cases} \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)} & \text{if } p \not\equiv 1 \pmod{\ell} \\ \frac{(\ell^4 - \ell - 1)\ell}{(\ell^4 - 1)(\ell^2 - 1)} & \text{if } p \equiv 1 \pmod{\ell}. \end{cases}$$

- ▶ So: counting appropriate matrices!
- ▶ $\#\mathrm{Sp}_4(\mathbb{Z}/(\ell)) = \#\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell)) = \ell^4(\ell^4 - 1)(\ell^2 - 1)$
- ▶ We guess (via interpolation) that the proportion of $M \in \mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell))$ for which $\chi(M)(1) = 0$ equals

$$\begin{cases} \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)} & \text{if } p \not\equiv 1 \pmod{\ell} \\ \frac{(\ell^4 - \ell - 1)\ell}{(\ell^4 - 1)(\ell^2 - 1)} & \text{if } p \equiv 1 \pmod{\ell}. \end{cases}$$

- ▶ So: counting appropriate matrices!
- ▶ $\#\mathrm{Sp}_4(\mathbb{Z}/(\ell)) = \#\mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell)) = \ell^4(\ell^4 - 1)(\ell^2 - 1)$
- ▶ We guess (via interpolation) that the proportion of $M \in \mathrm{Sp}_4^{(p)}(\mathbb{Z}/(\ell))$ for which $\chi(M)(1) = 0$ equals

$$\begin{cases} \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)} & \text{if } p \not\equiv 1 \pmod{\ell} \\ \frac{(\ell^4 - \ell - 1)\ell}{(\ell^4 - 1)(\ell^2 - 1)} & \text{if } p \equiv 1 \pmod{\ell}. \end{cases}$$

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Let $P_1(p)$ be the probability that a random number from the Weil interval is prime.
- ▶ Let $P_2(p) = P(N_H \text{ is prime})$.

Conjecture

Let

$$c_p = \frac{38}{45} \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2} + \frac{\ell}{(\ell-1)^2(\ell^2-1)} \right) \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell+1)(\ell^2+1)(\ell^3 - 2\ell^2 - \ell + 3)} \right),$$

then

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

- ▶ $c_p \in [0.63, 0.80]$ (cf. elliptic curves: $[0.44, 0.62]$)
- ▶ Recall: the above is for random squarefree $f(x)$ of degree 6.
- ▶ For random squarefree monic $f(x)$ of degree 5, the factor $38/45$ must be replaced by $2/5$.
- ▶ Then $c_p \in [0.30, 0.38]$.

- ▶ Future work:
 - ▶ Finish this research.
 - ▶ Invert the reasoning and construct a genus 2 Hurwitz-Kronecker class number formula.
 - ▶ Does the effect of favoring non-primes flatten out as $g \rightarrow \infty$?
- ▶ Many thanks for your attention!

- ▶ Future work:
 - ▶ Finish this research.
 - ▶ Invert the reasoning and construct a genus 2 Hurwitz-Kronecker class number formula.
 - ▶ Does the effect of favoring non-primes flatten out as $g \rightarrow \infty$?
- ▶ Many thanks for your attention!

- ▶ Future work:
 - ▶ Finish this research.
 - ▶ Invert the reasoning and construct a genus 2 Hurwitz-Kronecker class number formula.
 - ▶ Does the effect of favoring non-primes flatten out as $g \rightarrow \infty$?
- ▶ Many thanks for your attention!

- ▶ Future work:
 - ▶ Finish this research.
 - ▶ Invert the reasoning and construct a genus 2 Hurwitz-Kronecker class number formula.
 - ▶ Does the effect of favoring non-primes flatten out as $g \rightarrow \infty$?
- ▶ Many thanks for your attention!