Square-free discriminants of Frobenius rings

Joint work with Chantal David, Université Concordia.

Università Tor Vergata, Roma, May 21, 2010

Let E be an elliptic curve over $\mathbb{Q}$, and p a prime of good reduction (i.e. $p \nmid N_E$). The Frobenius endomorphism

$$(x, y) \mapsto (x^p, y^p)$$

of $E/\mathbb{F}_p$ is a root of the polynomial

$$x^2 - a_p x + p = (x - \pi_p)(x - \overline{\pi}_p)$$

where $|a_p| \leq 2\sqrt{p}$ by the Hasse bound.

Let E be an elliptic curve over $\mathbb{Q}$, and p a prime of good reduction (i.e. $p \nmid N_E$). The Frobenius endomorphism

$$(x, y) \mapsto (x^p, y^p)$$

of $E/\mathbb{F}_p$ is a root of the polynomial

$$x^2 - a_p x + p = (x - \pi_p)(x - \overline{\pi}_p)$$

where $|a_p| \leq 2\sqrt{p}$ by the Hasse bound.
Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p)$$

Let E be an elliptic curve over $\mathbb{Q}$, and p a prime of good reduction (i.e. $p \nmid N_E$). The Frobenius endomorphism

$$(x, y) \mapsto (x^p, y^p)$$

of $E/\mathbb{F}_p$ is a root of the polynomial

$$x^2 - a_p x + p = (x - \pi_p)(x - \overline{\pi}_p)$$

where $|a_p| \leq 2\sqrt{p}$ by the Hasse bound.
Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p)$$

and if p is a prime of ordinary reduction

$$\mathrm{End}(E/\mathbb{F}_p) \otimes \mathbb{Q} = \mathbb{Q}(\pi_p).$$

Let $\mathcal{O}_K$ be the maximal order in $\mathbb{Q}(\pi_p)$. Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p) \subseteq \mathcal{O}_K,$$

and any order can occur by Deuring's theorem.

Let $\mathcal{O}_K$ be the maximal order in $\mathbb{Q}(\pi_p)$. Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p) \subseteq \mathcal{O}_K,$$

and any order can occur by Deuring's theorem.

- When does $\mathbb{Z}[\pi_p] = \mathrm{End}(E/\mathbb{F}_p)$?

Let $\mathcal{O}_K$ be the maximal order in $\mathbb{Q}(\pi_p)$. Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p) \subseteq \mathcal{O}_K,$$

and any order can occur by Deuring's theorem.

- When does $\mathbb{Z}[\pi_p] = \mathrm{End}(E/\mathbb{F}_p)$?
- When does $\mathbb{Z}[\pi_p] = \mathcal{O}_K$?

Let $\mathcal{O}_K$ be the maximal order in $\mathbb{Q}(\pi_p)$. Then

$$\mathbb{Z}[\pi_p] \subseteq \mathrm{End}(E/\mathbb{F}_p) \subseteq \mathcal{O}_K,$$

and any order can occur by Deuring's theorem.

- When does $\mathbb{Z}[\pi_p] = \mathrm{End}(E/\mathbb{F}_p)$?
- When does $\mathbb{Z}[\pi_p] = \mathcal{O}_K$?

We have

$$\mathbb{Z}[\pi_p] = \mathcal{O}_K \Longrightarrow \mathbb{Z}[\pi_p] = \mathrm{End}(E/\mathbb{F}_p) \Longrightarrow E(\mathbb{F}_p) \text{ is cyclic.}$$

Theorem (Serre, 1977)

Assume the GRH. Then

$$\#\{p \leq x \;:\; E(\mathbb{F}_p) \;\; \textit{is cyclic}\} \sim C_1(E)\pi(x).$$

Theorem (Serre, 1977)

Assume the GRH. Then

$$\#\{p \le x \ : \ E(\mathbb{F}_p) \ \text{is cyclic}\} \sim C_1(E)\pi(x).$$

Theorem (Murty, 1983)

Let $E/\mathbb{Q}$ with CM.

$$\#\{p \le x \ : \ E(\mathbb{F}_p) \ \text{is cyclic}\} \sim C_1(E)\pi(x).$$

Let $\Delta_p = \mathrm{disc}(\mathrm{End}(E/\mathbb{F}_p))$. Let b_p be such that $a_p^2 - 4p = b_p^2 \Delta_p$.

Let $\Delta_p = \mathrm{disc}(\mathrm{End}(E/\mathbb{F}_p))$. Let b_p be such that $a_p^2 - 4p = b_p^2 \Delta_p$.

Then,

$$|\text{Ш}_p| = b_p^2,$$

where Ш_p is the Tate-Shafarevic group of E_p as an elliptic curve defined over its function field $\mathbb{F}_p(E_p)$.

Let $\Delta_p = \mathrm{disc}(\mathrm{End}(E/\mathbb{F}_p))$. Let b_p be such that $a_p^2 - 4p = b_p^2 \Delta_p$.

Then,

$$|\text{Ш}_p| = b_p^2,$$

where Ш_p is the Tate-Shafarevic group of E_p as an elliptic curve defined over its function field $\mathbb{F}_p(E_p)$.

Theorem (Cojocaru-Duke, 2004)

Assume the GRH. Then

$$\#\{p \le x \ : \ \mathbb{Z}[\pi_p] = End(E/\mathbb{F}_p)\} \sim C_2(E)\pi(x).$$

Square-free values

$$\mathbb{Z}[\pi_p] = \mathcal{O}_K$$

if and only if

$$a_p^2 - 4p = \begin{cases} D & D \equiv 1 \bmod 4 \text{ and square-free} \\ 4D & D \equiv 2,3 \bmod 4 \text{ and square-free} \end{cases}$$

Square-free values

$$\mathbb{Z}[\pi_p] = \mathcal{O}_K$$

if and only if

$$a_p^2 - 4p = \begin{cases} D & D \equiv 1 \bmod 4 \text{ and square-free} \\ 4D & D \equiv 2, 3 \bmod 4 \text{ and square-free} \end{cases}$$

Are there infinitely many supersingular primes congruent to $1 \bmod 4$? This would give infinitely many primes p such that

$$\mathbb{Z}[\pi_p] = \mathcal{O}_K.$$

Conjecture (Lang-Trotter conjecture)

Let K be an imaginary quadratic number field, and E an elliptic curve over $\mathbb{Q}$ without complex multiplication. Let

$$\Pi_{E,K}(x) = \#\{p \le x \ : \ p \nmid N_E \ \text{and} \ \mathbb{Q}(\pi_p) = K\}.$$

Then $\Pi_{E,K}(x) \sim C_{\mathrm{LT}}(E,K)\dfrac{\sqrt{x}}{\log x}$ *as* $x \to \infty$.

Upper bounds under the GRH (Cojocaru-David, 2008)

$$\Pi_E(K;x) \quad \ll_N \quad x^{13/14} \log x.$$

Upper bounds under the GRH (Cojocaru-David, 2008)

$$\Pi_E(K;x) \quad \ll_N \quad x^{13/14} \log x.$$

Let $\mathcal{D}_E(x)$ be the set of distinct fields $K = \mathbb{Q}(\pi_p)$ for primes $p \leq x$ of good reduction. Then,

$$|\mathcal{D}_E(x)| \gg_N \frac{x^{1/14}}{(\log x)^2}.$$

- Can we show that there are many distinct fields by showing there are many distinct square-free values of $a_p^2 - 4p$?

- Can we show that there are many distinct fields by showing there are many distinct square-free values of $a_p^2 - 4p$?

- Can we show that there are many distinct fields by showing there are many distinct square-free values of $a_p^2 - 4p$?
- Can we show that there are infinitely many primes such that D_p, the discriminant of $\mathbb{Q}(\pi_p)$, lies in a fixed arithmetic progression? Counting square-free values of $a_p^2 - 4p$ in arithmetic progressions would give an answer to that question.

Curves with Complex Multiplication (CM)

Curves with Complex Multiplication (CM)

Example: Let $E : y^2 = x^3 - x$ with CM by $\mathbb{Z}[i]$. Let $p \equiv 1 \mod 4$ (ordinary prime). Since E has rational 2-torsion, a_p is even, and 4 divides $a_p^2 - 4p$.

Curves with Complex Multiplication (CM)

Example: Let $E : y^2 = x^3 - x$ with CM by $\mathbb{Z}[i]$. Let $p \equiv 1 \bmod 4$ (ordinary prime). Since E has rational 2-torsion, a_p is even, and 4 divides $a_p^2 - 4p$.
We have

$$4((a_p/2)^2 - p) = a_p^2 - 4p = (\pi_p - \bar{\pi}_p)^2.$$

Curves with Complex Multiplication (CM)

Example: Let $E : y^2 = x^3 - x$ with CM by $\mathbb{Z}[i]$. Let $p \equiv 1 \mod 4$ (ordinary prime). Since E has rational 2-torsion, a_p is even, and 4 divides $a_p^2 - 4p$.
We have

$$4((a_p/2)^2 - p) = a_p^2 - 4p = (\pi_p - \bar{\pi}_p)^2.$$

Since E has CM by $\mathbb{Z}[i]$,

$$\pi_p - \bar{\pi}_p = 2bi$$

Curves with Complex Multiplication (CM)

Example: Let $E : y^2 = x^3 - x$ with CM by $\mathbb{Z}[i]$. Let $p \equiv 1 \bmod 4$ (ordinary prime). Since E has rational 2-torsion, a_p is even, and 4 divides $a_p^2 - 4p$.
We have

$$4((a_p/2)^2 - p) = a_p^2 - 4p = (\pi_p - \bar{\pi}_p)^2.$$

Since E has CM by $\mathbb{Z}[i]$,

$$\pi_p - \bar{\pi}_p = 2bi$$

and

$$(a_p/2)^2 - p = -b^2 \text{ is square-free} \iff b = 1 \iff p = (a_p/2)^2 + 1.$$

Sieving the squares

Let

$$\Pi_E^{\mathrm{sf}}(x) = \#\{p \le x \;:\; a_p^2 - 4p \text{ is square-free}\}.$$

Then,

$$\begin{aligned}\Pi_E^{\mathrm{sf}}(x) &= \sum_{p \le x} \sum_{d^2 \mid a_p^2 - 4p} \mu(d) \\ &= \sum_{d \le 2\sqrt{x}} \mu(d) \sum_{\substack{p \le x \\ d^2 \mid a_p^2 - 4p}} 1\end{aligned}$$

Sieving the squares

Let

$$\Pi_E^{\mathrm{sf}}(x) = \#\{p \leq x \,:\, a_p^2 - 4p \text{ is square-free}\}.$$

Then,

$$\begin{aligned} \Pi_E^{\mathrm{sf}}(x) &= \sum_{p \leq x} \sum_{d^2 | a_p^2 - 4p} \mu(d) \\ &= \sum_{d \leq 2\sqrt{x}} \mu(d) \sum_{\substack{p \leq x \\ d^2 | a_p^2 - 4p}} 1 \end{aligned}$$

To count the primes p such that $d^2 \mid a_p^2 - 4p$, we use the extension $\mathbb{Q}(E[d^2])/\mathbb{Q}$, where $\mathbb{Q}(E[d^2])$ is the field obtained by adjoining the coordinates of the d^2-torsion points of E to $\mathbb{Q}$.

Torsion Fields of elliptic curves

Since $E[d^2] \simeq \mathbb{Z}/d^2\mathbb{Z} \times \mathbb{Z}/d^2\mathbb{Z}$, we have

$$\mathrm{Gal}\left(\mathbb{Q}(E[d^2])/\mathbb{Q}\right) \subseteq \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z}).$$

Also, for $p \nmid dN_E$,

$$\begin{aligned} \rho_{d^2} : \mathrm{Gal}(\mathbb{Q}(E[d^2])/\mathbb{Q}) &\rightarrow \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z}) \\ \sigma_p &\mapsto [g] \end{aligned}$$

such that

$$\begin{aligned} \mathrm{tr}(g) &\equiv a_p(E) \bmod d^2 \\ \det(g) &\equiv p \bmod d^2 \end{aligned}$$

Let

$$
\begin{aligned}
G_E(d^2) &= \mathrm{Im}(\rho_{d^2}) \subseteq \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z}) \\
C_E(d^2) &= \{g \in G_E(d^2) \;:\; \mathrm{tr}^2\, g - 4 \det g \equiv 0 \bmod d^2\}
\end{aligned}
$$

Let

$$\begin{aligned} G_E(d^2) &= \mathrm{Im}(\rho_{d^2}) \subseteq \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z}) \\ C_E(d^2) &= \{g \in G_E(d^2) \ : \ \mathrm{tr}^2 g - 4 \det g \equiv 0 \bmod d^2\} \end{aligned}$$

Using the Chebotarev Density Theorem under the GRH (and following Murty, Murty and Saradha for a better error term), we have

$$\begin{aligned} \pi_{d^2}(x) &= \sum_{\substack{p \leq x \\ d^2 \mid a_p^2 - 4p}} 1 = \#\left\{p \leq x : \sigma_p \in C_E(d^2)\right\} \\ &= \frac{|C_E(d^2)|}{|G_E(d^2)|}\pi(x) + O\left(|C_E(d^2)|^{1/2} x^{1/2} \log xd\right). \end{aligned}$$

Main term

We then write $\Pi_E^{\mathrm{sf}}(x) = \mathrm{MT} + \mathrm{ET}$, where

$$\mathrm{MT} = \pi(x) \sum_{d \leq 2\sqrt{x}} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|}.$$

Main term

We then write $\Pi_E^{\mathrm{sf}}(x) = \mathrm{MT} + \mathrm{ET}$, where

$$\mathrm{MT} = \pi(x) \sum_{d \leq 2\sqrt{x}} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|}.$$

By Serre's Theorem, there exists an integer M_E such that

- If $(d_1, d_2) = (d_1, M_E) = 1$, then $G_E(d_1^2 d_2^2) = G_E(d_1^2) \times G_E(d_2^2)$.
- If $(d, M_E) = 1$, then $G_E(d^2) = \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z})$.

Main term

We then write $\Pi_E^{\mathrm{sf}}(x) = \mathrm{MT} + \mathrm{ET}$, where

$$\mathrm{MT} = \pi(x) \sum_{d \leq 2\sqrt{x}} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|}.$$

By Serre's Theorem, there exists an integer M_E such that

- If $(d_1, d_2) = (d_1, M_E) = 1$, then $G_E(d_1^2 d_2^2) = G_E(d_1^2) \times G_E(d_2^2)$.
- If $(d, M_E) = 1$, then $G_E(d^2) = \mathrm{GL}_2(\mathbb{Z}/d^2\mathbb{Z})$.

Then,

$$\sum_{d=1}^{\infty} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} = \sum_{d \mid M_E} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} \prod_{\ell \nmid M_E} \left(1 - \frac{\ell^2 + \ell - 1}{\ell^2(\ell^2 - 1)} \right)$$

Error term

Conjecture

$$\Pi_E^{\mathrm{sf}}(x) \sim C^{\mathrm{sf}}(E)\pi(x),$$

where

$$C^{\mathrm{sf}}(E) = \sum_{d \mid M_E} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} \prod_{\ell \nmid M_E} \left(1 - \frac{\ell^2 + \ell - 1}{\ell^2(\ell^2 - 1)}\right)$$

Error term

Conjecture

$$\Pi_E^{\mathrm{sf}}(x) \sim C^{\mathrm{sf}}(E)\pi(x),$$

where

$$C^{\mathrm{sf}}(E) = \sum_{d|M_E} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} \prod_{\ell \nmid M_E} \left(1 - \frac{\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right)$$

To prove the conjecture, we need to control the error term

$$\mathrm{ET} \quad \ll \quad x^{1/2+\epsilon} \sum_{d \le 2\sqrt{x}} d^3.$$

$$\sum_{d|P(z)} \mu(d) \sum_{\substack{p\leq x \\ d^2|a_p^2-4p}} 1 = \pi(x) \sum_{d|P(z)} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} + O\left(x^{1/2+\epsilon} e^{3z}\right)$$

and we need to take z small to control the first error term coming from the Chebotarev Density Theorem.

$$\sum_{d \mid P(z)} \mu(d) \sum_{\substack{p \leq x \\ d^2 \mid a_p^2 - 4p}} 1 = \pi(x) \sum_{d \mid P(z)} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} + O\left(x^{1/2+\epsilon} e^{3z}\right)$$

and we need to take z small to control the first error term coming from the Chebotarev Density Theorem.

We can get an upper bound by sieving, but there are no known lower bounds for $\pi^{\mathrm{sf}}(x)$.

$$\sum_{d|P(z)} \mu(d) \sum_{\substack{p \le x \\ d^2 | a_p^2 - 4p}} 1 = \pi(x) \sum_{d|P(z)} \mu(d) \frac{|C_E(d^2)|}{|G_E(d^2)|} + O\left(x^{1/2+\epsilon} e^{3z}\right)$$

and we need to take z small to control the first error term coming from the Chebotarev Density Theorem.

We can get an upper bound by sieving, but there are no known lower bounds for $\pi^{\mathrm{sf}}(x)$.

The theorems of Serre and Cojocaru-Duke rely on the fact that the primes p such that $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \le E(\mathbb{F}_p)$, or $d^2 \mid b_p^2$, are the primes splitting completely in some extension depending on d.

Let h be a positive odd integer, and let r be any integer such that the greatest common divisor (r, h) is square-free. Let $\Delta(r, h)$ be the set of square-free integers congruent to r mod h, and

$$\Pi^{\mathrm{sf}}_{E,r,h}(x) = \#\{p \leq x \,:\, a_p^2 - 4p \in \Delta(r, h)\}.$$

Let h be a positive odd integer, and let r be any integer such that the greatest common divisor (r,h) is square-free. Let $\Delta(r,h)$ be the set of square-free integers congruent to r mod h, and

$$\Pi^{\mathrm{sf}}_{E,r,h}(x) = \#\{p \le x \,:\, a_p^2 - 4p \in \Delta(r,h)\}.$$

Theorem

Let $\varepsilon > 0$, and A, B such that $AB > x\log^8 x$, $A, B > x^{\varepsilon}$. Then

$$\frac{1}{4AB}\sum_{|a|\le A, |b|\le B} \Pi^{\mathrm{sf}}_{E(a,b),r,h}(x) = \mathfrak{C}\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

where $\mathfrak{C}$ is the positive constant

$$\mathfrak{C} = \frac{1}{3h}\prod_{\substack{\ell \| h\\ \ell | r}}\frac{\ell-1}{\ell}\prod_{\substack{\ell | h\\ \ell \nmid r}}\frac{\ell\left(\ell-1-\left(\frac{r}{\ell}\right)\right)}{(\ell-1)\left(\ell-\left(\frac{r}{\ell}\right)\right)}\prod_{\ell\nmid h}\left(1-\frac{\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right).$$

$$\mathfrak{C} = \frac{1}{3h} \prod_{\substack{\ell \| h \\ \ell | r}} \frac{\ell - 1}{\ell} \prod_{\substack{\ell | h \\ \ell \nmid r}} \frac{\ell \left(\ell - 1 - \left(\frac{r}{\ell}\right)\right)}{(\ell - 1)\left(\ell - \left(\frac{r}{\ell}\right)\right)} \prod_{\ell \nmid h} \left(1 - \frac{\ell^2 + \ell - 1}{\ell^2(\ell^2 - 1)}\right).$$

For $\ell \nmid h$:

$$= \frac{|\left\{g \in \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) : \mathrm{tr}^2 g - 4 \det g \not\equiv 0 \bmod \ell^2\right\}|}{|\mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})|}$$

For $h = \ell^\alpha h'$, $\alpha \geq 1$ and $(h', \ell) = 1$, let $\beta = \max(\alpha, 2)$. Then:

$$= \ |\Big\{g \in \mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z}) : \mathrm{tr}^2 g - 4 \det g \not\equiv 0 \bmod \ell^2$$
$$\text{and } \mathrm{tr}^2 g - 4 \det g \equiv r \bmod \ell^\alpha\Big\} / |\mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})|.$$

Towards an average over the prime fields

$$\frac{1}{4AB} \sum_{|a| \leq A, |b| \leq B} \Pi^{\mathrm{sf}}_{E(a,b),r,h}(x)$$

Towards an average over the prime fields

$$\frac{1}{4AB}\sum_{|a|\le A,|b|\le B}\Pi^{\mathrm{sf}}_{E(a,b),r,h}(x)$$

$$= \frac{1}{4AB}\sum_{p\le x}\#\left\{|a|\le A,|b|\le B\ :\ a_p^2(E(a,b))-4p\in\Delta(r,h)\right\}$$

Towards an average over the prime fields

$$\frac{1}{4AB}\sum_{|a|\le A,|b|\le B}\Pi^{\mathrm{sf}}_{E(a,b),r,h}(x)$$

$$= \frac{1}{4AB}\sum_{p\le x}\#\left\{|a|\le A,|b|\le B\ :\ a_p^2(E(a,b))-4p\in\Delta(r,h)\right\}$$

$$= \frac{1}{4AB}\sum_{p\le x}\left(\frac{2A}{p}+O(1)\right)\left(\frac{2B}{p}+O(1)\right)\times$$

$$\times\#\left\{E/\mathbb{F}_p : a_p^2(E)-4p\in\Delta(r,h)\right\}$$

Towards an average over the prime fields

$$\frac{1}{4AB} \sum_{|a|\leq A, |b|\leq B} \Pi^{\mathrm{sf}}_{E(a,b),r,h}(x)$$

$$= \frac{1}{4AB} \sum_{p\leq x} \# \left\{ |a| \leq A, |b| \leq B \ : \ a_p^2(E(a,b)) - 4p \in \Delta(r,h) \right\}$$

$$= \frac{1}{4AB} \sum_{p\leq x} \left(\frac{2A}{p} + O(1) \right) \left(\frac{2B}{p} + O(1) \right) \times$$

$$\times \# \left\{ E/\mathbb{F}_p : a_p^2(E) - 4p \in \Delta(r,h) \right\}$$

$$\sim \sum_{p\leq x} \frac{\# \left\{ E/\mathbb{F}_p : a_p^2 - 4p \in \Delta(r,h) \right\}}{p^2}$$

when A, B are big enough. Here, we need $A, B > x^{1+\varepsilon}$.

Then, the average result is equivalent to the following

Theorem

Let h be a positive odd integer, and let r be any integer such that (r, h) is square-free. Let

$$\Pi^{\mathrm{sf}}(p) \ = \# \left\{ E \text{ over } \mathbb{F}_p \ : \ a_p^2 - 4p \in \Delta(r, h) \right\}.$$

Then, as $x \to \infty$,

$$\sum_{p \leq x} \Pi^{\mathrm{sf}}(p) = \frac{\mathfrak{C}}{3} \frac{x^3}{\log x} + O\left(\frac{x^3}{\log^2 x} \right),$$

where $\mathfrak{C}$ is the constant above.

Counting elliptic curves over finite fields

$$\begin{aligned} \Pi^{\mathrm{sf}}(p) &= \#\left\{E/\mathbb{F}_p :\ a_p^2(E) - 4p \in \Delta(r,h)\right\} \\ &= \sum_{\substack{-2\sqrt{p}<t<2\sqrt{p} \\ t^2-4p\in\Delta(r,h)}} \#\left\{E/\mathbb{F}_p :\ a_p(E) = t\right\}. \end{aligned}$$

Counting elliptic curves over finite fields

$$\begin{aligned}\Pi^{\mathrm{sf}}(p) &= \#\left\{E/\mathbb{F}_p :\ a_p^2(E) - 4p \in \Delta(r,h)\right\} \\ &= \sum_{\substack{-2\sqrt{p}<t<2\sqrt{p} \\ t^2-4p\in\Delta(r,h)}} \#\left\{E/\mathbb{F}_p :\ a_p(E) = t\right\}.\end{aligned}$$

Theorem (Deuring's Theorem)

Let t be an integer such that $|t| \leq 2\sqrt{p}$. The number of elliptic curves over $\mathbb{F}_p$ with $a_p(E) = t$ is $H(t^2 - 4p)(p-1)$.

For any $D < 0$, the Kronecker class number $H(D)$ is

$$H(D) = \sum_{\substack{f^2 \mid D \\ \frac{D}{f^2} \equiv 0,1 \bmod 4}} \frac{h(D/f^2)}{w(D/f^2)}.$$

$$\sum_{p \leq x} \frac{\Pi^{\mathrm{sf}}(p)}{p^2} \quad = \quad 2 \sum_{p \leq x} \sum_{\substack{1 \leq t \leq 2\sqrt{p} \\ t^2 - 4p \in \Delta(r,h)}}^{odd} \frac{h(t^2 - 4p)}{w(t^2 - 4p)p}$$

$$\sum_{p \le x} \frac{\Pi^{\mathrm{sf}}(p)}{p^2} = 2 \sum_{p \le x} \sum_{\substack{1 \le t \le 2\sqrt{p} \\ t^2 - 4p \in \Delta(r,h)}}^{odd} \frac{h(t^2-4p)}{w(t^2-4p)p}$$

$$= 2 \sum_{p \le x} \sum_{\substack{1 \le t \le 2\sqrt{p} \\ t^2 - 4p \equiv r \bmod h}}^{odd} \frac{h(t^2-4p)}{w(t^2-4p)p} \sum_{d^2 | t^2 - 4p} \mu(d)$$

$$\sum_{p\le x}\frac{\Pi^{\mathrm{sf}}(p)}{p^2} = 2\sum_{p\le x}\sum_{\substack{1\le t\le 2\sqrt{p}\\ t^2-4p\in\Delta(r,h)}}^{odd}\frac{h(t^2-4p)}{w(t^2-4p)p}$$

$$= 2\sum_{p\le x}\sum_{\substack{1\le t\le 2\sqrt{p}\\ t^2-4p\equiv r \bmod h}}^{odd}\frac{h(t^2-4p)}{w(t^2-4p)p}\sum_{d^2\mid t^2-4p}\mu(d)$$

$$\text{“}\sim\text{”}\quad 2\sum_{1\le t\le 2\sqrt{x}}^{odd}\sum_{d\le R}\mu(d)\sum_{\substack{p\le x\\ d^2\mid t^2-4p\\ t^2-4p\equiv r \bmod h}}\frac{h(t^2-4p)}{w(t^2-4p)p}.$$

$$\sum_{p \leq x} \frac{\Pi^{\mathrm{sf}}(p)}{p^2} \quad \text{``}\sim\text{''} \quad 2 \sum_{1 \leq t \leq 2\sqrt{x}}^{odd} \sum_{d \leq R} \mu(d) \sum_{\substack{p \leq x \\ d^2 \mid t^2 - 4p \\ t^2 - 4p \equiv r \bmod h}} \frac{h(t^2 - 4p)}{w(t^2 - 4p)p}.$$

By doing the average over elliptic curves in a family, we got rid of the difficult question of counting primes such that d^2 divides $a_p^2 - 4p$, and translate it into an average of class numbers.

$$\sum_{p\le x}\frac{\Pi^{\rm sf}(p)}{p^2} \quad ``\sim" \quad 2\sum_{1\le t\le 2\sqrt{x}}^{odd}\sum_{d\le R}\mu(d)\sum_{\substack{p\le x\\ d^2|t^2-4p\\ t^2-4p\equiv r \bmod h}}\frac{h(t^2-4p)}{w(t^2-4p)p}.$$

By doing the average over elliptic curves in a family, we got rid of the difficult question of counting primes such that d^2 divides a_p^2-4p, and translate it into an average of class numbers.

By the class number formula, $h(d)=\frac{\omega}{2\pi}|d|^{1/2}L(1,\chi)$, we get

$$\sim\frac{2}{3\pi}\sum_{\substack{n\le U\\ 1\le t\le 2\sqrt{x}\\ (t^2-r,h)=1}}^{odd}\frac{1}{n}\sum_{\substack{\alpha(\text{mod } n)\\ (t^2-\alpha,n)=1\\ \alpha\equiv r \bmod (n,h)}}\left(\frac{\alpha}{n}\right)\sum_{\substack{d\le R\\ (d,nt)=1\\ r\equiv 0 \bmod (d^2,h)}}^{odd}\mu(d)\sum_{\substack{p\le x\\ p\equiv\nu \bmod [nd^2,h]}}\frac{\sqrt{4p-t^2}}{p}$$

$$\sim \frac{2}{3\pi} \sum_{\substack{n \le U \\ 1 \le t \le 2\sqrt{x} \\ (t^2 - r, h) = 1}}^{odd} \frac{1}{n} \sum_{\substack{\alpha (\text{mod } n) \\ (t^2 - \alpha, n) = 1 \\ \alpha \equiv r \bmod (n,h)}} \left(\frac{\alpha}{n}\right) \sum_{\substack{d \le R \\ (d, nt) = 1 \\ r \equiv 0 \bmod (d^2, h)}}^{odd} \mu(d) \sum_{\substack{p \le x \\ p \equiv \nu \bmod [nd^2, h]}} \frac{\sqrt{4p - t^2}}{p}$$

We now have to count primes in certain arithmetic progression, depending on α, t, d, n, r, h, with weights $\frac{\sqrt{4p-t^2}}{p}$, which can be done using Barban–Davenport–Halberstam's Theorem to control the error counting primes in arithmetic progressions on average.

$$\sim \frac{2}{3\pi} \sum_{\substack{n \le U \\ 1 \le t \le 2\sqrt{x} \\ (t^2 - r, h) = 1}}^{odd} \frac{1}{n} \sum_{\substack{\alpha (\mathrm{mod}\ n) \\ (t^2 - \alpha, n) = 1 \\ \alpha \equiv r \bmod (n,h)}} \left(\frac{\alpha}{n}\right) \sum_{\substack{d \le R \\ (d, nt) = 1 \\ r \equiv 0 \bmod (d^2, h)}}^{odd} \mu(d) \sum_{\substack{p \le x \\ p \equiv \nu \bmod [nd^2, h]}} \frac{\sqrt{4p - t^2}}{p}$$

We now have to count primes in certain arithmetic progression, depending on α, t, d, n, r, h, with weights $\frac{\sqrt{4p-t^2}}{p}$, which can be done using Barban–Davenport–Halberstam's Theorem to control the error counting primes in arithmetic progressions on average.

Let

$$S(T) = \sum_{\substack{1 \le t \le T \\ (t^2 - r, h) = 1}}^{odd} \sum_{n \le U}^{odd} \frac{1}{n} \sum_{\substack{\alpha (\mathrm{mod}\ n) \\ (t^2 - \alpha, n) = 1 \\ \alpha \equiv r (\mathrm{mod}\ (n,h))}} \left(\frac{\alpha}{n}\right) \sum_{\substack{d \le R \\ (d, nt) = 1 \\ r \equiv 0 \bmod (d^2, h)}} \frac{\mu(d)}{\varphi([nd^2, h])}.$$

$$S(T) = \sum_{\substack{1 \le t \le T \\ (t^2 - r, h) = 1}}^{odd} \sum_{n \le U}^{odd} \frac{1}{n} \sum_{\substack{\alpha (\text{mod } n) \\ (t^2 - \alpha, n) = 1 \\ \alpha \equiv r (\text{mod } (n,h))}} \left(\frac{\alpha}{n}\right) \sum_{\substack{d \le R \\ (d, nt) = 1 \\ r \equiv 0 \bmod (d^2, h)}} \frac{\mu(d)}{\varphi([nd^2, h])}.$$

Theorem

$$S(T) \sim \frac{3}{2} \mathfrak{C} T$$

where

$$\mathfrak{C} = \frac{1}{3h} \prod_{\substack{\ell \| h \\ \ell | r}} \frac{\ell - 1}{\ell} \prod_{\substack{\ell | h \\ \ell \nmid r}} \frac{\ell \left(\ell - 1 - \left(\frac{r}{\ell}\right)\right)}{(\ell - 1)\left(\ell - \left(\frac{r}{\ell}\right)\right)} \prod_{\ell \nmid h} \left(1 - \frac{\ell^2 + \ell - 1}{\ell^2(\ell^2 - 1)}\right).$$

This gives the conjectural constant $C^{\mathrm{sf}}(E, r, h)$ counting matrices in Galois groups for an "ideal curve" E with $M_E = 1$.