THESIS DEFENSE

Lang-Trotter Questions on the Reductions of Abelian Varieties

Sam Bloom
April 9, 2018

University of Maryland, College Park
Outline of Talk:

I: Introduction, History, and Statement of Results
II: Tools and Methods
III: Conjectures and Experimental Evidence
IV: Further Directions
Part I: Introduction, History, and Statement of Results
Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N$. For primes $p \nmid N$,

$$E_p := \text{the reduction of } E \text{ modulo } p.$$ 

(Essentially, if $E : Y^2 = X^3 + aX + b$, then $E_p$ has the “same” equation mod $p$. Precisely, $E_p$ is the special fibre at $p$ of the Néron model, $\mathcal{E}/\text{Spec } \mathbb{Z}$, of $E$).

Questions of Lang-Trotter Type.
How do the reductions $E_p$ behave as $p$ varies?

Let $a_p := p + 1 - \#E_p(\mathbb{F}_p)$. Then $\pi_p$, the Frobenius endomorphism of $E$, can be identified with a root of $X^2 - a_pX + p$, giving an imaginary quadratic field $\mathbb{Q}(\pi_p) \cong \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$.

Fixed-Field Question.
How often is $\mathbb{Q}(\pi_p)$ a specified imaginary quadratic field?

Almost-Prime Orders Question.
How many prime factors does $\#E_p(\mathbb{F}_p)$ have?
For instance, let $E$ be the curve 43.a1 with equation $Y^2 + Y = X^3 + X^2$.

Baseball card for $E$:

- $N = 43$
- $r = 1$
- $E_{\text{tors}}(\mathbb{Q}) = \{\infty\}$
- $\text{End}(E_{\mathbb{Q}}) \simeq \mathbb{Z}$
- isolated in isogeny class.
Graph of \( \Pi(E, K)(x) := \# \{ p \leq X \mid \mathbb{Q}( \pi_p ) \cong K \} \) for 43.a1:
Graph of $\pi_E(x) := \#\{p \leq X \mid \#E_p(\mathbb{F}_p) \text{ is prime} \}$ for 43.a1:
Let $E/\mathbb{Q}$ be an elliptic curve.

**Conjecture (Lang-Trotter Conjectures, 1976)**

1. Suppose that $\text{End}(E_{\mathbb{Q}}) \cong \mathbb{Z}$, or $t \neq 0$. Then there exists a constant $C_{E,t} \geq 0$ such that

$$\# \left\{ p \leq X \mid a_p = t \right\} \sim C_{E,t} \frac{\sqrt{X}}{\log X};$$

2. Suppose that $\text{End}(E_{\mathbb{Q}}) \cong \mathbb{Z}$, and let $K/\mathbb{Q}$ be an imaginary quadratic number field. Then there exists a constant $C_{E,K} > 0$ such that

$$\# \left\{ p \leq X \mid \text{End}(E_p) \otimes \mathbb{Q} = \mathbb{Q}(\pi_p) \cong K \right\} \sim C_{E,K} \frac{\sqrt{X}}{\log X}.$$

The constants $C_{E,t}$ and $C_{E,K}$ are given explicitly as Euler products and depend on the Galois representations of $E$. 

Conjecture (Koblitz, Conjecture A, 1988)

Suppose that every elliptic curve which is $\mathbb{Q}$-isogenous to $E$ has trivial rational torsion. Then,

$$\pi_E(x) := \# \left\{ p \leq x \mid \#E_p(\mathbb{F}_p) \text{ is prime} \right\} \sim C_E \frac{x}{(\log x)^2}$$

where $C_E > 0$ is an explicit constant depending on the Galois representation of $E$.

Zywina (2009) refined Koblitz’s Conjecture to account for the possibility that the LHS is finite. (E.g., $E : y^2 = x^3 + 9x + 18$, then $\gcd(\#E_p(\mathbb{F}_p), 6) \neq 1$ for all $p \geq 5$, since $\mathbb{Q}(i) \subset \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3])$.)
Intro: Lang-Trotter Conjecture for $43.a1$: $Y^2 + Y = X^3 + X$

Graph of $\frac{\Pi(E, \mathbb{Q}(i))(x)}{\sqrt{x}/ \log(x)}$ for $43.a1$: 
Intro: Lang-Trotter Conjecture for 43.a1: $Y^2 + Y = X^3 + X$

Graph of $\frac{\prod(E, Q(\sqrt{-2}))(x)}{\sqrt{x}/ \log(x)}$ for 43.a1:
**Intro: Lang-Trotter Conjecture for 43.a1:**

\[
Y^2 + Y = X^3 + X
\]

Graph of \( \frac{\pi(E, \mathbb{Q}(-3))(x)}{\sqrt{x} / \log(x)} \) for 43.a1:
Intro: Koblitz Conjecture for 43.a1: $Y^2 + Y = X^3 + X$

Graph of $\frac{\pi_E(x)}{x/\log(x)^2}$ for 43.a1:
Thm. (Cojocaru-Fouvry-Murty, 2005) \( E/\mathbb{Q} \) non-CM. Let \( K = \mathbb{Q}(-D) \). Then,

\[
\Pi(E, K)(X) \ll_N X^\alpha \log X
\]

where \( \alpha = 17/18 \) under (GRH); \( \alpha = 13/14 \) under (GRH) and (AHC); and \( \alpha = 11/12 \) under (GRH), (AHC), and (PCC). Unconditionally,

\[
\Pi(E, K)(X) \ll_N X \left( \frac{\log \log X}{\log X} \right)^{25/24} (1 + \omega(D))
\]

**Methods:** Square Sieve + Explicit Chebotarev Density Theorems. [More later.]

Best known upper bounds:

**Thm. (Zywina 2015, Thorner-Zaman 2016)**

\[
\Pi(E, K)(X) \ll_E X^{4/5} (\log X)^{-3/5} h_K^{-3/5} + X^{1/2} (\log X)^3, \text{ under GRH;}
\]

\[
\Pi(E, K)(X) \ll_{E,K} X (\log \log X)(\log X)^{-2}, \text{ unconditionally.}
\]

No known lower bounds!
**Thm. (David-Wu, 2012)** Assume the $\theta$-Hypothesis for the division fields of $E$.

Then, for $\varepsilon > 0$, for $x \gg_{\varepsilon} 0$,

$$\pi_E(x) \leq \left( \frac{5}{1 - \theta} + \varepsilon \right) C_E \frac{x}{(\log x)^2}.$$ 

Similarly, no known lower bounds! However, for

$$\pi_{E,r}(x) := \# \left\{ p \leq x \left| \#E_p (\mathbb{F}_p) \in P_r \right. \right\},$$

**Thm. (David-Wu, 2012)** Assume the $\theta$-Hypothesis for $\theta = 11/21$, and that all of the curves $\mathbb{Q}$-isogenous to $E$ have trivial torsion over $\mathbb{Q}$. Then, for $x \gg_{E} 0$,

$$\pi_{E,8}(x) \geq 2.778 C_E \frac{x}{(\log x)^2}.$$ 

*Methods: Weighted Greaves Sieve + Explicit Chebotarev Theorems. [Details later.]*
Recall the Erdös-Kac Theorem (1940), that
\[
\lim_{x \to \infty} \left( \frac{1}{x} \# \left\{ n \leq x \mid \frac{\omega(n) - \log \log n}{\sqrt{\log \log n}} \leq \gamma \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} \, dt.
\]

This has been generalized by Halberstam to \( p \mapsto p - 1 \), and by Murty-Murty for \( p \mapsto \tau(p) \) (under GRH).

\[
\sum \tau(n)q^n = q \prod_{q=1}^{\infty} (1 - q^n)^{24} = (2\pi)^{-12} \Delta(q).)
\]

**Thm. (Y.-R. Liu, 2006)** Assume the \( \theta \)-Hypothesis for the division fields of \( E \) for some \( \theta < 1 \). Then, for all \( \gamma \in \mathbb{R} \),
\[
\lim_{x \to \infty} \left( \frac{1}{\pi(x)} \# \left\{ p \leq x \mid \frac{\omega(#E_p(\mathbb{F}_p)) - \log \log p}{\sqrt{\log \log p}} \leq \gamma \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} \, dt.
\]

**Method:** Axiomatize the probabilistic/sieve-theoretic argument of Erdös-Kac, then use Explicit Chebotarev.
Definition: “generic” abelian variety

Let $A/Q$ be a principally polarized abelian variety. We generalize “$E$ non-CM.”

Recall, $T_\ell(A) = \varprojlim A[\ell^n](\overline{Q}) \cong \mathbb{Z}_\ell^{2g}$ is

- a $G_Q$-module by action on the coordinates, and
- equipped with the $(G_Q$-equiv., symplectic) Weil pairing to $\mu_{\ell\infty}$

so have the $\ell$-adic Galois representation $\rho_{\ell\infty} : G_Q \to GSp_{2g} \mathbb{Z}_\ell$ and adelic Galois representation $\hat{\rho} = \prod_\ell \rho_\ell$.

**Def.** $A$ is **generic** if the image of $\hat{\rho}$ is open (i.e., finite-index) in $GSp_{2g} \widehat{\mathbb{Z}}$.

So, for $A$ generic, $\hat{\rho}(G_Q) = G(M) \times \prod_{\ell \nmid M} GSp_{2g} \mathbb{Z}_\ell$.

**Theorem. (Serre, 1968)** $E$ non-CM $\implies E$ generic.

**Theorem. (Serre, Pink)** Suppose $\text{End}(A_Q) \cong \mathbb{Z}$. Then, $A$ is generic if

$$g \notin \{ \frac{1}{2}(2n)^k \mid n > 0, k \geq 3 \text{ odd} \} \cup \{ \frac{1}{2}\binom{2n}{n} \mid n \geq 3 \text{ odd} \} = \{4, 10, 16, 32, \ldots \}.$$
Analytic Hypotheses

Will need to assume analytic hypotheses to use Explicit Chebotarev:

Conjecture (AHC for $L/K$)

Let $\rho$ be a non-trivial irreducible representation of $\text{Gal}(L/K)$. Then, $L(s, \rho)$ is holomorphic on $\mathbb{C}$.

Hypothesis ($\theta$-Hypothesis for $L/K$)

Let $1/2 \leq \theta < 1$, and $\mathcal{H}_\theta := \{s \in \mathbb{C} \mid \Re(s) > \theta\}$. Then, $\zeta_L(s)$ has no zeros in $\mathcal{H}_\theta$. Moreover, AHC holds for $L/K$, and the $L$-functions attached to irreducible representations of $\text{Gal}(L/K)$ are zero-free on $\mathcal{H}_\theta$ as well.
Main Results, I: Fixed-Field

Let \( A/\mathbb{Q} \) be generic. Let \( K/\mathbb{Q} \) be a CM field of degree \( 2g \) with discriminant \( d = d(K/\mathbb{Q}) \). Let

\[
\Pi(A, K)(X) := \{ p \leq X \mid A_p \text{ ordinary, simple, and } \mathbb{Q}(\pi_p) \cong K \}.
\]

Theorem. (B.)

\[
\Pi(A, K)(X) \ll_{N,g} \begin{cases} \chi^{1-1/(8g^2+4g+6)} \log X & \text{under GRH;} \\ \chi^{1-1/(4g^2+4g+6)} \log X & \text{under GRH and AHC;} \\ \chi^{1-1/(2g^2+4g+6)} \log X & \text{under GRH, AHC, and PCC;} \end{cases}
\]

and

\[
\Pi(A, K)(X) \ll_{N,g} \frac{X(\log \log X)^{1+1/(4g^2+3g+2)}}{(\log X)^{1+1/(8g^2+6g+4)}} (1 + \omega(d)) \quad \text{unconditionally.}
\]
Let \( A/\mathbb{Q} \) be a generic surface. Let \( F = \mathbb{Q}(\sqrt{d}) \) be a real quadratic number field, where \( d \) is squarefree. Let

\[
\Pi(A, F)(X) := \{ p \leq X \mid A_p \text{ ordinary, simple, and } \mathbb{Q}(\pi_p)_0 \cong F \}
\]

**Theorem (B.)**

\[
\Pi(A, F)(X) \ll_N \begin{cases} 
X^{45/46} \log X & \text{under GRH;} \\
X^{29/30} \log X & \text{under GRH and AHC;} \\
X^{22/23} \log X & \text{under GRH, AHC, and PCC;}
\end{cases}
\]

and

\[
\Pi(A, F)(X) \ll_N \frac{X \log \log X}{(\log X)^{67/66}} (1 + \omega(d)) \quad \text{unconditionally.}
\]
**Main Results, II: Almost-Prime Orders**

**Thm. (B.)** Suppose that $A$ is generic and that

$$(\text{Triv}_A): \text{every abelian variety which is } \mathbb{Q}\text{-isogenous to } A \text{ has trivial rational torsion.}$$

Assume the $\theta$-Hypothesis for the division fields of $A$. Then, for $x \gg_A 0$,

$$\# \left\{ p \leq x \mid \#A_p(\mathbb{F}_p) \in P_r \right\} \geq B_g \cdot C_A \frac{x}{(\log x)^2}$$

where $B_g > 0$ is an explicit absolute constant, $C_A$ is an explicit non-negative constant depending on $\hat{\rho}$, and

$$r = r(g, \theta) := \left\lceil \frac{(9/2)g^3 + (1/2)g}{1 - \theta} - \frac{1}{3} \right\rceil.$$ 

**Thm. (B.)** Same hypotheses. Then, for all $\epsilon > 0$, for $x \gg_A, \theta, \epsilon 0$,

$$\# \left\{ p \leq x \mid \#A_p(\mathbb{F}_p) \text{ is prime} \right\} \leq \left( \frac{2g^2 + 3g + 6}{1 - \theta} + \epsilon \right) C_A \frac{x}{(\log x)^2}.$$
Thm. (B.) Suppose that $A$ is generic. Assume the $\theta$-Hypothesis for the division fields of $A$ for some $\theta < 1$. Then, for all $\gamma \in \mathbb{R}$,

$$\lim_{x \to \infty} \left( \frac{1}{\pi(x)} \# \left\{ p \leq x \left| \frac{\omega(#A_p(F_p)) - \log \log p}{\sqrt{\log \log p}} \leq \gamma \right. \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} \, dt.$$
Part II: Methods and Details
Overview of Method

1. Convert the desired event and related events into statements about $\rho_n$, and thus into specifying some $C(n) \subset GSp_{2g} \mathbb{Z}/n\mathbb{Z}$;
2. Create an appropriate list of integers to apply sieve-theoretic bounds;
3. (⋆) Bound (via linear algebra and other arguments) character sums and densities that arise from sieving;
4. Interchange the order of summations, if needed;
5. Apply explicit Chebotarev to bound the “prime-counting” terms that arise.
Thm. (Square Sieve, Heath-Brown 1984) Let $\mathcal{A}$ be a finite sequence of non-zero rational integers, and $\mathcal{P}$ a set of distinct odd rational primes. Set $S(\mathcal{A}) := \# \{ \alpha \in \mathcal{A} : \alpha \text{ is a square} \}$. Then,

$$S(\mathcal{A}) \leq \frac{\# \mathcal{A}}{\# \mathcal{P}} + \max_{l,q \in \mathcal{P} \atop l \neq q} \left| \sum_{\alpha \in \mathcal{A}} \left( \frac{\alpha}{lq} \right) \right| + \frac{2}{\# \mathcal{P}} \sum_{\alpha \in \mathcal{A}} \sum_{l \in \mathcal{P}} 1 + \frac{1}{(\# \mathcal{P})^2} \sum_{\alpha \in \mathcal{A}} \left( \sum_{l \in \mathcal{P} \atop (\alpha,l) \neq 1} 1 \right)^2$$

where $\left( \frac{\cdot}{\cdot} \right)$ is the Jacobi symbol.
Lem. (David-Wu) Let $M \in \mathbb{Z}^+$, and let $\mathcal{A}$ be a finite list of positive integers coprime to $M$, indexed by $\{p \leq x\}$. Let $U, V, \xi$ be positive constants, and $r$ a positive integer, such that $\max \mathcal{A} \leq x^{\xi(rU+V)}$. Then,

$$\# \left\{ a \in \mathcal{A} \mid a \in P_r \right\} \geq H\left( \mathcal{A}, x^{\xi U}, x^{\xi V} \right) - \sum_{x^{\xi V} \leq p < x^{\xi U}} \# \mathcal{A}_{p^2}.$$ 

where $H$ is the weighted Greaves sieving function.

The theorem of Halberstam-Richert on the weighted Greaves sieve says (essentially): if

- $X \approx \# \mathcal{A}$;  $w$ multiplicative fn., zero outside $\mathcal{P}$, s.t. $w(p) \approx 1$,
- define $r(\mathcal{A}, d) := \# \mathcal{A}_d - (w(d)/d)X$. Then,

$$H\left( \mathcal{A}, x^{\xi V}, x^{\xi U} \right) \geq \left( X \cdot \prod_{p < x^\xi} \left( 1 - \frac{w(p)}{p} \right) \cdot \ldots \right) + \text{(small)} - \left( \text{sum of } r(\mathcal{A}, d) \text{ based on } U,V \right).$$
Let \( L/\mathbb{Q} \) finite Galois w/ Gal. group \( G \), and \( C \subseteq G \) union of conj. classes. Define \( \pi_C(X, L/\mathbb{Q}) \) as 
\[
\pi_C(X, L/\mathbb{Q}) := \# \left\{ p \leq X : p \text{ unramified in } L/\mathbb{Q}; \left( \frac{L/\mathbb{Q}}{p} \right) \subseteq C \right\}.
\]

**Thm. (Chebotarev; Lagarias-Odlyzko; Serre; Murty-Murty-Saradha; Murty)**

\[
\pi_C(X, L/\mathbb{Q}) = \frac{\#C}{\#G} \text{li}(x) + R_C(x),
\]

1. \( R_C(x) = o(\text{li}(x)) \);
2. Under GRH for \( L/\mathbb{Q} \),
\[
R_C(X) = O \left( (\#C)^{1/2}X^{1/2} \left( \frac{\log|d_L|}{n_L} + \log X \right) \right);
\]
3. Under GRH + AHC for \( L/\mathbb{Q} \),
\[
R_C(X) = O \left( (\#C)^{1/2}X^{1/2} \left( \log M(L/\mathbb{Q}) + \log X \right) \right);
\]
4. Under GRH + AHC + PCC for \( L/\mathbb{Q} \),
\[
R_C(X) = O \left( (\#C)^{1/2}X^{1/2} \left( \frac{\#\tilde{G}}{\#G} \right)^{1/4} \left( \log M(L/\mathbb{Q}) + \log X \right) \right)\]
5. Unconditionally, \( \exists A, B, > 0 \) s.t. \( R_C(X) \ll \frac{\#C}{\#G} \text{li} \left( X \exp \left( -B \frac{\log X}{\max \{|d_L|^{1/n_L}, \log|d_L|\}} \right) \right) + (\#\tilde{C})X \exp \left( -A \sqrt{\frac{\log X}{n_L}} \right) \),

6. Let \( H \trianglelefteq G \) be a normal subgroup such that for all irreducible representations \( \rho \) of \( \text{Gal}(L^H/Q) \cong G/H \), the Artin \( L \)-function \( L(s, \rho) \) satisfies the \( \theta \)-hypothesis. Suppose also that the product \( HC \subseteq C \). Then,

\[
R_C(X) \ll \left( \frac{\#C}{\#H} \right)^{1/2} x^\theta n_L \left( \log M(L/Q) + \log x \right).
\]
Suppose $A_p$ simple ordinary. Then, for $K/\mathbb{Q}$ CM,

$$\mathbb{Q}(\pi_p) \cong K \implies K_0 = \mathbb{Q}(\pi_p + \pi_p)$$

$$\implies d(K/K_0) \cdot \alpha^2 = \left( (\pi_p + \pi_p)^2 - 4p \right) \mathcal{O}_{K_0}$$

(fmla. for rel. disc.) $$\implies N_{Q}^{K_0} \left( (\pi_p + \pi_p)^2 - 4p \right) \cdot d(K/\mathbb{Q}) \in \mathbb{Z}^2.$$ 

Now, $\text{char}_{\pi_p}(x) = x^{2g} + a_{1,p}x^{2g-1} + \ldots + a_{g,p}x^g + \ldots + p^g$. Suppose the integer $\beta_p := (\pi + \pi)^2$ has characteristic polynomial

$$\text{char}_{\beta_p}(x) := x^g + c_1x^{g-1} + \ldots + c_g := \prod_{\tau: K_0 \rightarrow \overline{Q}} (x - \tau(\beta))$$

when acting on $K_0 = \mathbb{Q}(\pi + \pi)$ over $\mathbb{Q}$. Then, the $c_i$ are polynomials of the $a_i$ and $p$, and these polynomials depend only on $g$ and are at worst quadratic in the $a_i$. 
Since \( N_{\mathbb{Q}}^{K_0} \left( (\pi_p + \pi_p)^2 - 4p \right) = (-1)^g \text{char}_{\beta_p}(4p) \), apply Square Sieve to \( \mathcal{A} = \{ (-1)^g \text{char}_{\beta_p}(4p) \cdot d \mid p < X \} \).

After CRT and interchanging summation, wish to bound (among other things)

\[
\sum_{c \in (\mathbb{Z}/lq\mathbb{Z})^*} \sum_{a_1, \ldots, a_g \in \mathbb{Z}/lq\mathbb{Z}} \left( \frac{\gamma_p}{lq} \right)
\]

Picking \( i \) such that \( \gamma_p \) quadratic in \( a_i \), so \( \gamma_p = \gamma^{(2)}_{i,p}(a_i)^2 + \gamma^{(1)}_{i,p}a_i + \gamma^{(0)}_{i,p} \), we can understand the contribution \( \left( \frac{\gamma_p}{lq} \right) \) when \( \left( \left( \frac{\gamma_p}{l} \right), \left( \frac{\gamma_p}{q} \right) \right) = (\pm 1, \pm 1) \) as counting a point on the genus-0 curve

\[
\xi y^2 = \gamma^{(2)}_{i,p}x^2 + \gamma^{(1)}_{i,p}x + \gamma^{(0)}_{i,p}
\]

where \( \left( \left( \frac{\xi}{l} \right), \left( \frac{\xi}{q} \right) \right) = (\pm 1, \pm 1) \).
Then, the curve
\[ C_\xi/(\mathbb{Z}/lq\mathbb{Z}) : \xi y^2 = \gamma_{i,p}^{(2)} x^2 + \gamma_{i,p}^{(1)} x + \gamma_{i,p}^{(0)} \]
is irreducible mod \( \ell \) except when the other coefficients \((a_1, \ldots, \hat{a}_i, \ldots, a_g)\) are on a hypersurface \( Z_\xi \hookrightarrow A_{\mathbb{Z}/\ell\mathbb{Z}}^{g-1} \) of degree \( \leq 4 \). (Same for \( q \).) Then, we can bound \( \#Z_\xi(\mathbb{Z}/\ell\mathbb{Z}) \) via\[ \text{Thm. (Lang-Weil, 1954)} \]Let \( V \hookrightarrow \mathbb{P}^n_{\mathbb{F}_q} \) be a projective variety of dimension \( r \) and degree \( d \) over a finite field. Then,
\[
\left| \#V(\mathbb{F}_q) - q^r \right| = (d - 1)(d - 2)q^{r - \frac{1}{2}} + O_{n,r,d}(q^{r - 1}).
\]
Contributions from \( Z_\xi \) that don’t cancel exactly are negligible compared to main term in character sum; so can assume that \( C_\xi \) irreducible mod \( \ell \) and mod \( q \). Then \( C_\xi \cong \mathbb{P}^1 \) mod \( \ell \) and mod \( q \), and all main terms cancel exactly. Also bound \( \#\{p \leq X \mid \text{char } \pi_p \text{ mod } l = f\} \); use Explicit Chebotarev, as
\[
\text{char } \pi_p|_{A[l]} = \text{char } \left( \frac{Q(A[l])/\mathbb{Q}}{\mathbb{Q}} \right)
\]
and use Chavdarov bd. on \( \#\{M \in \text{GSp}_{2g} \mathbb{F}_l \mid \text{char } M = f\} \).
Let $\mathcal{A} := \{ \#A_p(\mathbb{F}_p) \mid p \leq x \}$. From the weighted Greaves’ sieve, we want to show that there’s a multiplicative function $w \approx 1$ and approximation $X \approx \#\mathcal{A}$ so that the remainders $\#\mathcal{A}_n - (w(n)/n)X$ are small.

Since $\#A_p(\mathbb{F}_p) = \deg(\pi_p - \text{id}_A)$, we have

$$n \mid \#A_p(\mathbb{F}_p) \iff \text{char}_{\rho_n(\text{Frob}_p)}(1) \equiv 0 \mod n,$$

so we define

$$C(n) := \{ g \in \text{Gal}(\mathbb{Q}(A[n])/\mathbb{Q}) \mid \text{char}_g(1) \equiv 0 \},$$

$$w(n) = \frac{n \cdot \#C(n)}{\#G(n)}, \quad n \text{ squarefree supp’d on } \mathcal{P}.$$ 

where $\mathcal{P} := \{ \text{surj. primes } p \text{ for } A \}$.

After fitting together prime-counting estimates, we find

$$\pi_{C(n)}(x, L_n/\mathbb{Q}) = \frac{\#C(n)}{\#G(n)} \text{li}(x) + \frac{\#B(n)}{\#G(n)} \frac{\#C(n)}{\#C_B(n)} R_{C(n)}(x) + Q_n(x)$$

with $Q_n$ an additional error term to bound.
A result of Castryck et al. (2012) yields

$$\frac{\#C(l)}{\#G(l)} = \frac{1}{l-1} \cdot \left( - \sum_{r=1}^{g} \prod_{j=1}^{r} (1 - l^{2j})^{-1} + (l - 2) \left( - \sum_{r=1}^{g} \prod_{j=1}^{r} (1 - l^{j})^{-1} \right) \right);$$

counting upper-triangular matrices with eigenvalue 1 yields

$$\#C_{B}(l)/\#B(l) \asymp_{g} 1/l; \quad \#C_{B}(l^{2})/\#B(l^{2}) \asymp_{g} 1/l$$

and the trickiest density,

$$\frac{\#C(l^{2})}{\#G(l^{2})} = \frac{\#C(l^{2})}{\#C(l)} \cdot \frac{\#C(l)}{\#G(l)} \cdot \frac{\#G(l)}{\#G(l^{2})}$$

is bounded via Hensel’s Lemma and counting arguments.

These bounds allow us to bound the remainders $r(A, n)$ and the terms $\#A_{l^{2}}$, and the result follows.
For Erdös-Kac result, use density bounds and
Thm. (Generalized Erdös-Kac: Liu, Xiong) Let $S \subset \mathbb{N}$ infinite. Suppose that
$\#S(x^{1/2}) = o(\#S(x))$ as $x \to \infty$. Let $f : S \to \mathbb{N}$. For each prime $l$, choose
functions $\lambda_l = \lambda_l(x)$ (“main term”) and $e_l = e_l(x)$ (“error term”) such that
$$
\frac{1}{\#S(x)} \# \left\{ n \in S(x) \mid l \mid f(n) \right\} = \lambda_l + e_l.
$$

Suppose $\exists \beta > 0$ s.t. for all $n \in S(x)$, we have $\#\{p > x^{\beta} \mid p \mid f(n)\} = O(1)$. Suppose also that the $\lambda_l$ and $e_l$ satisfy technical assumptions which encode

- each $\lambda_l(x) \approx c/l$, and each each $e_l(x)$ is somewhat smaller than $\lambda_l(x)$; and
- the error between $\frac{1}{\#S(x)} \#\{n \in S(x) \mid l_1l_2 \ldots l_k \mid f(n)\}$ and $\prod_1^k \lambda_i(x)$ is small.

Then, for $\gamma \in \mathbb{R}$,
$$
\lim_{x \to \infty} \left( \frac{1}{\#S(x)} \# \left\{ n \in S(x) \mid \frac{\omega(f(n)) - c \log \log n}{\sqrt{\log \log n}} \leq \gamma \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} \, dt.
$$
Part III:
Conjectures and Experimental Evidence
The heuristics of the Koblitz Conjecture suggest

**Conj.** Let $A/\mathbb{Q}$ be an abelian variety satisfying $(\text{Triv}_A)$ and such that $C_A \neq 0$, where

$$C_A := \frac{1 - \#C'(M_A)/\#G(M_A)}{\prod_{l|M_A} (1 - 1/l)} \prod_{l|M_A} \frac{1 - \#C(l)/G(l)}{1 - 1/l}.$$ 

Then,

1. $\#\{p \leq x \mid \#A_p(\mathbb{F}_p) \text{ is prime}\} \ll_A \frac{x}{(\log(x))^2}.$

2. In particular, if $A$ is generic, $\#\{p \leq x \mid \#A_p(\mathbb{F}_p) \text{ is prime}\} \sim C_A \frac{x}{g(\log(x))^2}.$

We graphed the ratio $\frac{\#\{p \leq x \mid \#(J_C)_p(\mathbb{F}_p) \text{ is prime}\}}{\pi(x)/(\log x)}$ for generic genus-2 curves and a generic genus-3 curve:
Data for Koblitz Conjecture: 971.A.971.1, $Y^2 + Y = X^5 - 2X^3 + X$
Data for Koblitz Conjecture: 1051.a.1051.a, $Y^2 + Y = X^5 - X^4 + X^2 - X$
DATA FOR KOBLITZ CONJECTURE: 1205.a.1205.1, \( Y^2 + Y = X^5 + 2X^4 - X^2 \)
DATA FOR KOBLITZ CONJECTURE: 1385.a.1385.1, $Y^2 + Y = X^5 + 3X^4 + 3X^3 - X$
Data for Koblitz Conjecture: generic genus 3 curve

\[ C : y^2 = x^7 - 14085x^6 + 33804x^5 - 27231x^4 + 27231x^3 - 35995x^2 - 33803x + 25039. \]
Part IV:
Further Directions
Comments on my work

• Should be able to extend results to other classes of $A/\mathbb{Q}$ with “open-image” Galois representation;
• Presume that the asymptotic bounds in our main theorems are not sharp;
• Expect that more sophisticated sieving techniques will yield better asymptotic bounds;
• Expect that sieve theory alone will not be able to prove any of the Lang-Trotter-type conjectures;
• e.g., fixed-trace Lang-Trotter Conjecture for newforms $f$ of weight $k \geq 2$ is conditionally proved by González-Jiménez-Urroz (2012) if there’s a fast-enough rate of convergence toward Sato-Tate distribution.
Other Lang-Trotter questions

For an individual $A$:

- For ring $R$, when does $R \hookrightarrow \text{End}(A_p) \otimes \mathbb{Q}$?
- For $(a_1, \ldots, a_g)$, when is
  \[ \text{char}_{\pi_p}(x) = x^{2g} + a_1x^{2g-1} + \ldots + a_gx^g + p a_{g-1}x^{g-1} + \ldots + p^g? \]
- When does the Newton polygon of $A_p$ satisfy a given restriction?
- Suppose $g \geq 4$, and $A$ not a Jacobian. When is $A_p$ a Jacobian?
- Is there a Cohen-Lenstra phenomenon for the class group of $\text{End}(A_p) \otimes \mathbb{Q}$?
- Is there a Chebyshev bias to $\text{disc}(\text{char}_p)$ mod $n$, or to $d(\text{End}(A_p) \otimes \mathbb{Q}/\mathbb{Q})$ mod $n$ for ordinary primes $p$?

Can also ask Lang-Trotter questions for:

- pairs/tuples $(A_1, \ldots, A_k)$;
- abelian varieties “on average.”

References for (most of) the analogous questions for $E/\mathbb{Q}$ are in the last chapter of the thesis.
Thank you!