Pure and Applied Mathematics Quarterly
Volume 2, Number 1
(*Special Issue: In honor of
John H. Coates, Part 1 of 2*)
163—178, 2006

Towards Lang-Trotter for Elliptic Curves over Function Fields

Chris Hall and José Felipe Voloch

1. Introduction

Let K be a global field of characteristic p and let $\mathbb{F}_q \subset K$ denote the algebraic closure of $\mathbb{F}_p$ in K. We fix an elliptic curve E/K with non-constant j-invariant and a torsion-free subgroup $\Sigma \subseteq E(K)$ of rank $r > 0$. We write V for the open set of places v of K such that the special fiber E_v is an elliptic curve and, for v in V, we let $\Sigma_v \subset E_v(k_v)$ be the image of Σ under reduction modulo v, where k_v is the residue field of K at v. We fix a finite set of (rational) prime numbers $\mathcal{S}$ which is large enough to include the exceptional primes which we will define explicitly in section 2.4 and section 3), and we let $\mathcal{G}(\Sigma, \mathcal{S})$ denote the subset of $v \in V$ such that Σ_v contains the prime-to-$\mathcal{S}$ part of $E_v(k_v)$. For every $n > 0$, we write V_n for the subset of $v \in V$ such that $\deg(v) = n$ and let $\mathcal{G}_n(\Sigma, \mathcal{S}) = V_n \cap \mathcal{G}(\Sigma, \mathcal{S})$.

Theorem 1. *Suppose $r \geq 6$. There exist constants a, b satisfying $0 < a < b < 1$ and depending only on r and $\mathcal{S}$ and for each $n \geq 1$, there exists $\delta_n(\Sigma, \mathcal{S})$, depending on r, $\mathcal{S}$ and the isomorphism class of $\mathrm{Gal}(K(E[\ell])/K)$ for $\ell \notin \mathcal{S}$ such that*

$$a \leq \delta_n(\Sigma, \mathcal{S}) \leq b, \quad |\mathcal{G}_n(\Sigma, \mathcal{S})| = \delta_n(\Sigma, \mathcal{S})|V_n| + o(q^n/n)$$

for all n.

We prove the theorem in section 4.3. The rest of the paper establishes preliminary results. We remark that for a fixed K, r and $\mathcal{S}$, there are only finitely many possibilities for the entire set $\{\delta_n(\Sigma, \mathcal{S}) : n > 0\}$, as will follow from our

Received June 1, 2005.
The first author was an NSF VIGRE postdoc and the second author was supported by NSA grant MDA904-03-1-0117.

results. However, the limit $\delta_n(\Sigma, \mathcal{S})$ as $n \to \infty$ does *not* exist in general. Rather one must consider an increasing sequence $n_1, n_2, \ldots$ such that n_i divides n_{i+1} in order to obtain a limit. Different sequences will lead to different limits. This is in contrast with the number field analogue in which the analogous δ_n converge and therefore can be taken independent of n.

The number field analogue of the above theorem was conjectured by Lang and Trotter (for $r = 1$) and proved by Gupta and Murty ([GM]) for $r \geq 18$ under GRH. Our proof of theorem 1 follows the function-field analogue of the strategy in [GM]. A literal translation of their argument, together with the improved error bounds of [MS], allows one to prove an analogue of their theorem for $r \geq 10$. The proof proceeds in several stages, and in one of these stages we replace the use of $K(E[\ell])$ with a smaller subextension of K, which we define in section 2.2. This allows us to extend the argument to $r \geq 6$. It is conceivable that these extensions might be used in the number field case to lower the bound on r. We hope to return to this question in a later paper. The case of constant j-invariant and $r = 1$ was treated by the second author in [V]. One can always construct examples where the hypotheses of the theorem apply by passing to an extension of K, if necessary. If one insists on examples over the rational function field $\mathbb{F}_q(t)$, these have been constructed by Ulmer ([U]).

2. ℓ-adic Galois Theory

Throughout this section K is an arbitrary field and ℓ is a fixed rational prime which is invertible in K. We fix an elliptic E/K and write $L = K(E[\ell])$. There is an embedding $\Gamma = \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{Z}/\ell)$, which is well-defined, up to conjugation, and is given by identifying $\mathrm{Aut}(E[\ell])$ with $\mathrm{GL}_2(\mathbb{Z}/\ell)$. Moreover, for a fixed primitive ℓth root of unity ζ, the quotient $\det(\Gamma)$ is the Galois group of the cyclotomic extension $K(\zeta)/K$. We call the kernel of $\Gamma \to \det(\Gamma)$ the subgroup of geometric elements, or simply the geometric Galois group of L/K. In all but the last section we assume that it is $\mathrm{SL}_2(\mathbb{Z}/\ell)$. In the last section we consider the case when the geometric Galois group is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell)$.

2.1. **Kummer Theory.** In this section we additionally assume $\ell > 2$. Recall $L = K(E[\ell])$ and $\Gamma = \mathrm{Gal}(L/K)$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell)$.

Lemma 1. *The natural map $E(K)/\ell(E(K)) \to E(L)/\ell(E(L))$ is injective.*

Proof. For every finite extension F/K there is a natural embedding of $E(F)/\ell(E(F))$ into the Galois cohomology group $H^1(F, E[\ell])$, hence it suffices to show that the restriction map $H^1(K, E[\ell]) \to H^1(L, E[\ell])$ is injective. By the inflation-restriction sequence, the kernel of the restriction map is $H^1(\Gamma, E[\ell])$. Let Z be the center of Γ; it is a normal subgroup of order prime to ℓ and $E[\ell]^Z = 0$. It follows that $H^1(\Gamma, E[\ell]) = 0$, proving the lemma. $\square$

For any $P \in E(K)$, we write P/ℓ for the ℓ^2 points Q such that $[\ell]Q = P$. The extension $K(P/\ell)/K$ is Galois and contains L, and we write $H = \mathrm{Gal}(L(P/\ell)/L)$, $G = \mathrm{Gal}(K(P/\ell)/K)$. There is a short exact sequence of groups

$$1 \longrightarrow H \longrightarrow G \longrightarrow \Gamma \longrightarrow 1.$$

We regard $E[\ell]$ as a Γ-module and write $E[\ell] \rtimes \Gamma$ for the semi-direct product. There is an embedding $G \to E[\ell] \rtimes \Gamma$, which is unique up to conjugation in $E[\ell] \rtimes \Gamma$, and $H = G \cap E[\ell]$.

Lemma 2. *For every $P \in E(K) - \ell(E(K))$, $G = \mathrm{Gal}(K(P/\ell)/K)$ is isomorphic to $E[\ell] \rtimes \Gamma$.*

Proof. A priori G is a subgroup of $E[\ell] \rtimes \Gamma$ which maps surjectively to Γ. No line of $E[\ell]$ is stabilized by Γ, so $H = G \cap E[\ell]$ is either trivial or all of $E[\ell]$. Lemma 1 implies that P is not in $\ell(E(L))$, hence $H = E[\ell]$. $\square$

The lines $\mathcal{K} \subset E[\ell]$ correspond bijectively to cyclic ℓ-isogenies $\phi : E_\phi \to E$, where E_ϕ is some elliptic curve. Given $\mathcal{K}$, ϕ is the dual of the canonical map $E \to E/\mathcal{K}$ and, given $\phi : E_\phi \to E$, $\mathcal{K}$ is the kernel of the dual isogeny $E \to E_\phi$.

Lemma 3. *Let $P, Q \in E(K)$. The following are equivalent:*

(1) $\langle P \rangle \equiv \langle Q \rangle \bmod \ell(E(K))$;
(2) $\langle P \rangle \equiv \langle Q \rangle \bmod \ell(E(L))$;
(3) $\langle P \rangle \equiv \langle Q \rangle \bmod \phi(E_\phi(L))$ *for every cyclic ℓ-isogeny $\phi : E_\phi \to E$;*
(4) $\langle P \rangle \equiv \langle Q \rangle \bmod \phi(E_\phi(L))$ *for some cyclic ℓ-isogeny $\phi : E_\phi \to E$.*

Proof. The first two statements are equivalent by lemma 1. The second statement implies the third. Given an ℓ-isogeny $\phi : E_\phi \to E$ we have an exact sequence

$$0 \to E[\hat{\phi}] \to E[\ell] \to E_\phi[\phi] \to 0$$

and the cohomology sequence gives the short exact sequence

$$0 \to H^1(L, E[\hat{\phi}]) \to H^1(L, E[\ell]) \to H^1(L, E_\phi[\phi]).$$

For isogenies $\phi_1 \neq \phi_2$, the intersection $H^1(L, E[\hat{\phi}_1]) \cap H^1(L, E[\hat{\phi}_2])$ is trivial, as $H^1(L, E[\ell])$ is a direct sum of these two subgroups, therefore the composite map

$$E(L)/\ell(E(L)) \to H^1(L, E[\ell]) \to H^1(L, E_{\phi_1}[\phi_1]) \oplus H^1(L, E_{\phi_2}[\phi_2]) \tag{1}$$

is injective. It is the direct sum of the boundary maps corresponding to the cohomology sequence of

$$0 \to E_{\phi_i}[\phi_i] \to E_{\phi_i} \xrightarrow{\phi_i} E \to 0$$

These maps induce embeddings $E(L)/\phi_i E_{\phi_i}(L) \to H^1(L, E_{\phi_i}[\phi_i])$. If we assume the third statement of the lemma holds, then $\langle P \rangle \equiv \langle Q \rangle$ in all the terms of (1), hence the second statement holds. The last two statements of the lemma are equivalent because Γ acts transitively on the isogenies and fixes P and Q. □

One useful aspect of this lemma is that, in some circumstances, it allows us to replace L with the field of definition $K(\phi)$, for a fixed ϕ of our choosing (cf. section 2.2). We can also apply the lemma to the Galois theory of 'ℓ-descent' of E/K.

Theorem 2. *Let $P, Q \in E(K)$. The following are equivalent:*

(1) *$K(P/\ell) = K(Q/\ell)$;*
(2) *$\langle P \rangle \equiv \langle Q \rangle \bmod \ell(E(K))$.*

Otherwise $K(P/\ell) \cap K(Q/\ell) = L$.

Proof. The statement follows easily from lemma 2 when P or Q lies in $\ell(E(K))$, so we assume that $P, Q \in E(K) - \ell(E(K))$. We also assume there exists $F \subset K(P/\ell) \cap K(Q/\ell)$ which is a non-trivial extension of L of degree ℓ. F is not Galois over K because $E[\ell] \rtimes \Gamma$ has no normal subgroups of order ℓ, hence $K(P/\ell) = K(Q/\ell)$. $\mathrm{Gal}(L(P/\ell)/L) = \mathrm{Gal}(L(Q/\ell)/L)$ is isomorphic to $E[\ell]$, so the Galois group $\mathrm{Gal}(F/L)$ is isomorphic to $E_\phi[\phi]$ for some cyclic ℓ-isogeny $\phi : E_\phi \to E$. The kernel of the restriction map $H^1(L, E_\phi[\phi]) \to H^1(F, E_\phi[\phi])$ is isomorphic to $\mathbb{Z}/\ell$, and it is generated by the image of P, Q under the boundary map $E(L) \to H^1(L, E_\phi[\phi])$. Therefore $\langle P \rangle \equiv \langle Q \rangle \bmod \phi(E_\phi(L))$, hence $\langle P \rangle \equiv \langle Q \rangle \bmod \ell(E(K))$ by lemma 3, so we have the implication (1) $\Rightarrow$ (2). The converse implication is clear. □

For any $d \geq 0$, Γ acts diagonally on $E[\ell]^d$, and we write $E[\ell]^d \rtimes \Gamma$ for the semi-direct product.

Corollary 1. *If the image of $P_1, \ldots, P_r \in E(K)$ in $E(K)/\ell(E(K))$ generates a d-dimensional subspace, then $\mathrm{Gal}(K(P_1/\ell, \ldots, P_r/\ell)/K) \simeq E[\ell]^d \rtimes \Gamma$.*

In general we will apply this for fixed $P_1, \ldots, P_r$ and varying ℓ in the proof of theorem 1. One can prove analogous results for any cyclic ℓ-isogeny.

Theorem 3. *Let $\phi : E_\phi \to E$ be a cyclic ℓ-isogeny. For $P \in E(K)$ let P/ϕ denote the set of ℓ points Q such that $\phi(Q) = P$. If the images of $P_1, \ldots, P_r \in E(K)$ in $E(K(\phi))/\phi(E_\phi(K(\phi)))$ generate a d-dimensional subspace, then*

$$\mathrm{Gal}\,(K(\phi, P_1/\phi, \ldots, P_r/\phi)/K(\phi)) \simeq E_\phi[\phi]^d \rtimes \det(\Gamma).$$

We will be most interested in applying this with $r = 1$ in the proof of lemma 7.

2.2. **Cyclotomic Twist.** In this section we fix a cyclic ℓ-isogeny $\phi : E_\phi \to E$. We let $\mathcal{K} = \mathrm{Ker}(\hat{\phi}) = \phi(E_\phi[\ell])$ and write $B \subset \Gamma$ for the unique Borel subgroup stabilizing $\mathcal{K}$. We may assume, without loss of generality, that B is the subgroup of upper-triangular matrices. Then the ℓ-Sylow subgroup $U \subset B$ is the subgroup of upper-unipotent matrices. We choose a second Borel subgroup $\hat{B} \neq B$. The intersection $C = B \cap \hat{B}$ is a (split) Cartan subgroup, and B is then canonically isomorphic to the semi-direct product $U \rtimes C$. Up to conjugation by an element of U, we may assume, without loss of generality, that $\hat{B}$ is the subgroup of lower-triangular matrices, so $C \subset \Gamma$ is the subgroup of diagonal matrices. We write $\hat{\mathcal{K}} \subset E[l]$ for the unique line stabilized by $\hat{B}$, and we note that $\mathcal{K} \neq \hat{\mathcal{K}}$, hence $\hat{\phi} : \hat{\mathcal{K}} \to E_\phi[\phi]$ is an isomorphism.

We define $\hat{T}$, $T \subset C$, respectively, to be the subgroups which act trivially on $\mathcal{K}$, $\hat{\mathcal{K}}$, respectively. We note that the semi-direct products $U \rtimes T, U \rtimes \hat{T} \subset B$ are each stable under conjugation by U, hence are independent of our choice of $\hat{B}$. We define the geometric subgroup $G = \hat{G} \subset C$ to be the kernel of $C \to \det(C)$. The fixed field of G is the cyclotomic extension $K(\phi, \zeta)/K(\phi)$, where ζ is a primitive ℓth root of unity. The multiplication maps $T \times G \to C$ and $\hat{T} \times \hat{G} \to C$ are isomorphisms, so there are canonical isomorphisms $G \to \mathrm{Gal}(K(\phi, E_\phi[\phi])/K(\phi))$ and $\hat{G} \to \mathrm{Gal}(K(\hat{\phi}, E[\hat{\phi}])/K(\hat{\phi}))$. In summary, we have the lattice of Galois extensions shown in figure 1.

The extension N/K is an instance of the 'balanced-$\Gamma_1(\ell)$-moduli problem' of (7.4.3) of [KM]. That is, it classifies pairs of embeddings $\mathbb{Z}/\ell \to E[\ell]$, $\mathbb{Z}/\ell \to E_\phi[\ell]$ of the trivial Galois module $\mathbb{Z}/\ell$. Similarly, $\hat{F}/K$ is an instance of the '$\Gamma_1(\ell)$-moduli problem' of *loc. cit.*, which classifies embeddings of $\mathbb{Z}/\ell$ into $E[\ell]$. The inclusion of fields $\hat{F} \to N$ corresponds to 'remembering' the embedding $\mathbb{Z}/\ell \to E_\phi[\ell]$. One can also consider embeddings $\mu_\ell \to E[\ell]$, where μ_ℓ is the Galois module of ℓth roots of unity. By Cartier duality these correspond to quotients $E[\ell] \to \mathbb{Z}/\ell$, hence embeddings $\mathbb{Z}/\ell \to E_\phi[\ell]$. The extension F/K corresponds to an instance of this other 'moduli problem,' and $F \to N$ corresponds to 'remembering' the embedding $\mathbb{Z}/l \to E[\ell]$. As 'moduli problems,' these last two are isomorphic if and only if μ_ℓ and $\mathbb{Z}/\ell$ are isomorphic Galois modules; that is,

FIGURE 1

$$
\begin{tikzcd}
 & & L = K(E[\ell]) \arrow[d, dash, "U"] \arrow[ddll, dash, bend right, "U \rtimes T"'] \arrow[ddrr, dash, bend left, "U \rtimes \hat{T}"] & & \\
 & & N = K(\phi, E_\phi[\phi], E[\hat{\phi}]) \arrow[dll, dash, "T"'] \arrow[drr, dash, "\hat{T}"] \arrow[d, dash, "G"] \arrow[dd, dash, bend right=60, "C"'] & & \\
F = K(\phi, E_\phi[\phi]) \arrow[drr, dash, "G"'] & & K(\phi, \zeta) \arrow[d, dash, "\det(\Gamma)"] & & \hat{F} = K(\hat{\phi}, E[\hat{\phi}])\,. \arrow[dll, dash, "\hat{G}"] \\
 & & K(\phi) = K(\hat{\phi}) & &
\end{tikzcd}
$$

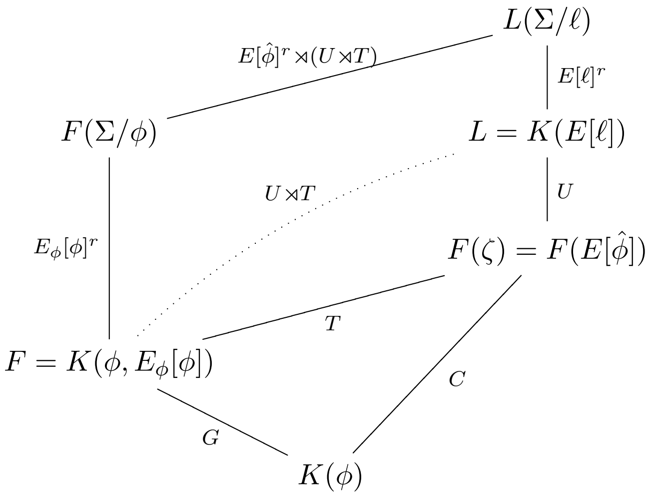
FIGURE 2

$$
\begin{tikzcd}
 & F(\zeta) = \hat{F}(\zeta) \arrow[dl, dash, "T"'] \arrow[dr, dash, "\hat{T}"] \arrow[dd, dash, dotted, "C"'] & \\
F \arrow[dr, dash, "G"'] & & \hat{F}\,. \arrow[dl, dash, "\hat{G}"] \\
 & K(\phi) = K(\hat{\phi}) &
\end{tikzcd}
$$

they classify the same objects if and only if $K(\zeta) = K$. Otherwise $\hat{F}$ is an easily described 'cyclotomic twist' of F (and vice versa).

We observe that F/K, $\hat{F}/K$ are geometric extensions, because $\det(U \rtimes T) = \det(U \rtimes \hat{T}) = \det(\Gamma)$. On the other hand, the extension $N = F(\zeta) = \hat{F}(\zeta)$ of $F, \hat{F}$, respectively, is 'purely arithmetic'. Hence we can extract the 'Cartesian square' of Galois field extensions in figure 2 from the lattice in figure 1. There is a canonical isomorphism between Galois groups for either pair of parallel edges, and there is one, $T \to \hat{T}$, induced by the isomorphisms $T \to \det(C)$ and $\hat{T} \to \det(C)$. Composing the canonical maps $T \to \hat{T}$ and $\hat{T} \to G$ gives a 1-cocycle $\sigma \in H^1(T, G) \subset H^1(F, G)$. One can easily verify that $\hat{T} \subset C$ is the graph of σ in $T \times G = C$, hence $\hat{F}$ is the 'cyclotomic twist' corresponding to σ.

Figure 3



2.3. **Lang-Trotter Conjugacy Classes.** We continue to use the notation of the previous two sections. We fix a free subgroup $\Sigma = \langle P_1, \ldots, P_r \rangle \subset E(K)$ of rank r. We assume its image is an r-dimensional subspace of $E(K)/\ell(E(K))$, so that $K(E[\ell], \Sigma/\ell)$ is Galois over K with group $E[\ell]^r \rtimes \Gamma$ (by corollary 1). Then for every ϕ, we have the lattice of Galois extensions in figure 3.

We define the Lang-Trotter elements of Γ associated to ϕ by

$$\mathcal{C}(\phi) = \{\tau \in U \rtimes T : \tau = 1 \text{ or } \tau \notin U\}.$$

That is, $\mathcal{C}(\phi) \subset U \rtimes T$ is the subset of semisimple elements. We define $\mathcal{C}(\phi, \Sigma)$ to be the inverse image of $\mathcal{C}(\phi)$ under the natural map $E[\hat{\phi}]^r \rtimes (U \rtimes T) \to U \rtimes T$. It is important to note that every element of $\mathcal{C}(\phi, \Sigma)$ acts trivially on $F(\Sigma/\phi)$ (cf. beginning of section 4.3). The subsets of Lang-Trotter conjugacy classes are the unions $\mathcal{C} = \cup_\phi \mathcal{C}(\phi)$, $\mathcal{C}(\Sigma) = \cup_\phi \mathcal{C}(\phi, \Sigma)$ over all ϕ. One can easily show that for every $\delta \in \det(\Gamma)$,

$$|\{c \in \mathcal{C}(\Sigma) : \det(c) = \delta\}| = \begin{cases} \ell^{r+1}(\ell+1) & \text{if } \delta \neq 1 \\ \ell(\ell^r + \ell^{r-1} - 1) & \text{if } \delta = 1 \end{cases}.$$

When $\delta = 1$ we remark that $\mathcal{C}(\phi) = \mathcal{C}(\phi') = \{1\}$ and $\mathcal{C}(\phi, \Sigma) \cap \mathcal{C}(\phi', \Sigma) = \{(0, 1)\}$ for $\phi \neq \phi'$. We note that for every δ there is at least one element of $E[\ell]^r \rtimes \Gamma$ which does not lie in $\mathcal{C}(\Sigma)$ and whose image in Γ has determinant δ.

For the rest of this section we fix a place v of K which is unramified in L and let $n = \deg(v)$. The prime decomposition of v in the extension L/K is relatively easy to describe, mainly because the latter is Galois. Let w be any prime of L lying over v and let $D(w) \subset \Gamma$ denote the decomposition group. There are $[\Gamma : D(w)]$ primes w over v, all of degree $f = |D(w)|$. Γ acts transitively on the w over v, and the induced action on $\{D(w)\}$ is conjugation. On the other hand, the prime decomposition of v in $K(\phi)$ is more difficult to describe because $K(\phi)/K$ is not a Galois extension. We will refrain from describing the general case, and instead will assume that the Frobenius conjugacy class $\mathrm{Fr}_v \subset \Gamma$ is contained in $\mathcal{C} \subset \Gamma$.

For any prime w over v, we write $\overline{w}$ for the prime in $K(\phi)$ under w. The decomposition group $D(\overline{w}) \subset B$ is the intersection $D(w) \cap B$, hence $\overline{w}$ has degree $[D(w) : D(\overline{w})]$ over v If $f = 1$, then $D(w)$ is trivial, hence v decomposes as a product of $\ell + 1$ primes of degree n in $K(\phi)$. On the other hand, if $f > 1$, then $D(w)$ is contained in a unique split Cartan subgroup $C(w) \subset \Gamma$; $C(w)$ is the centralizer of $D(w)$ in Γ. Therefore $D(w) = D(\overline{w})$ if and only if $C = C(w) \subset B$, otherwise $D(\overline{w}) = \{1\}$. Finally, C has index two in its normalizer $N(C)$ and the intersection $B \cap N(C)$ is contained in C. Therefore the $\overline{w}$ such that $D(\overline{w}) \subset B$ lie in two B-orbits, one for each element of the intersection $\mathrm{Fr}_v \cap C$, hence there are two $\overline{w}$ of degree n and the remaining $\overline{w}$ are of degree nf.

2.4. **Geometrically-Degenerate Case.** In this section we relax the condition that $\Delta = \mathrm{Gal}(L/K)$ contain the subgroup $\mathrm{SL}_2(\mathbb{Z}/\ell)$. More precisely, we assume the geometric subgroup, $\Delta \cap \mathrm{SL}_2(\mathbb{Z}/\ell)$, is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell)$. We fix a free subgroup $\Sigma = \langle P_1, \ldots, P_r \rangle \subset E(K)$ and let $H = \mathrm{Gal}(K(\Sigma/\ell)/K)$. In order to keep with notation of the previous sections, we write $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}/\ell)$ for the inverse image of $\det(\Delta) \subset (\mathbb{Z}/\ell)^\times$. Then Δ is a proper subgroup of Γ and H is a proper subgroup of $G = E[\ell]^r \rtimes \Gamma$.

For every Borel subgroup $B \subset \Gamma$, we write $U \rtimes T \subset B$ for the 'semi-Borel subgroup' of section 2.3, and $\mathcal{K} \subset E[\ell]$ for the line stabilized by B. The Lang-Trotter elements associated to B are the semisimple elements $\mathcal{C}(B) \subset U \rtimes T$, and the set of elements associated to Γ is the union $\mathcal{C} = \cup_B \mathcal{C}(B)$ over all B. We recall that $U \rtimes T$ stabilizes $\mathcal{K}$, so the semi-direct product $\mathcal{K}^r \rtimes (U \rtimes T)$ exists. Then we define $\mathcal{C}(B, \Sigma)$ to be the inverse image of $\mathcal{C}(B)$ under the natural map $\mathcal{K}^r \rtimes (U \rtimes T) \to U \rtimes T$ and $\mathcal{C}(\Sigma) \subset G$ to be the union $\cup_B \mathcal{C}(B, \Sigma)$. We define the Lang-Trotter conjugacy classes $\mathcal{C}(H) \subset H$ as the intersection $H \cap \mathcal{C}(\Sigma)$.

Because Δ is a proper subgroup of Γ such that $\det(\Delta) = \det(\Gamma)$, one can easily show that $|\mathcal{C}(H)|$ is maximized when $H = E[\ell]^r \rtimes C$ for some split Cartan subgroup $C \subset \Gamma$. Therefore, in general,

$$|\{c \in \mathcal{C}(H) : \det(c) = \delta\}| \leq |\{c \in \mathcal{C}(E[\ell]^r \rtimes C) : \det(c) = 1\}| \leq \ell(\ell^r + \ell^{r-1} - 1), \tag{2}$$

for any $\delta \in \det(\Gamma)$. A priori, every element of H or simply every element of a fixed determinant $\delta \in \det(\Gamma)$ may be a Lang-Trotter element, in which case we call ℓ exceptional and therefore assume it is contained in the set $\mathcal{S}$ (cf. introduction) This applies to $\ell \neq p$ and the case $\ell = p$ is discussed in the next section. For any fixed E/K the function-field analogue of Serre's theorem implies that there are only finitely many exceptional ℓ. In fact, by theorem 1 of [CH] there is constant ℓ_0, depending only on the genus of K, such that $\ell \leq \ell_0$ if ℓ is exceptional and $\ell \neq p$.

3. p-adic Galois Theory

In this section we fix a global field K of char p and an elliptic curve E/K with non-constant j-invariant. Then $E[p]$ is isomorphic to $\mathbb{Z}/p$ over an algebraic closure of K. There is a canonical cyclic p-isogeny $V : E_\phi \to E$ over K, the so-called Verschiebung; the dual isogeny $\hat{V} : E \to E_\phi$ is the (p-)Frobenius While $K(E[p])/K$ is inseparable in general, the extension $L = K(E_\phi[\phi])/K$ is Galois and geometric, and there is an embedding of $\Delta = \mathrm{Gal}(L/K)$ into $(\mathbb{Z}/p)^\times$.

Lemma 4. *The canonical map $H^1(K, E_\phi[V]) \to H^1(L, E_\phi[V])^\Delta$ is an isomorphism.*

Proof. The order of Δ is prime to p, so we consider the Hochschild-Serre sequence

$$0 \longrightarrow H^1(\Delta, E_\phi[V]) \longrightarrow H^1(K, E_\phi[V]) \longrightarrow H^1(L, E_\phi[V])^\Delta \longrightarrow H^2(\Delta, E_\phi[V]).$$

The first and last terms vanish, so the sequence degenerates to the desired isomorphism. □

From the lemma we infer that $P \in V(E_\phi(K))$ if and only if $P \in V(E_\phi(L))$, which is what we need to prove the following theorem.

Theorem 4. *Let $P_1, \ldots, P_r \in E(K)$. Suppose the image of $\langle P_1, \ldots, P_r\rangle$ in $E(K)/V(E_\phi(K))$ is an r-dimensional subspace. Then*

$$\mathrm{Gal}(K(P_1/V, \ldots, P_r/V)/K) \simeq E_\phi[V]^r \rtimes \Delta.$$

Finally, we define the Lang-Trotter conjugacy classes in $E_\phi[V]^r \rtimes \Delta$ to be the subgroup $E_\phi[V]^r$. Therefore, if $\Delta = 1$, then we say that p is exceptional and therefore must be added to our set $\mathcal{S}$ (cf. introduction). Contrary to the ℓ-adic case, where there is a natural determinant $\det : \Delta \to (\mathbb{Z}/\ell)^\times$, there are two natural maps $\det : \Delta \to (\mathbb{Z}/p)^\times$ that we must consider: the identity map and the trivial map. In fact, the latter is what we want if we insist that $\det(\Gamma)$ should be the Galois group of the scalar part of L/K, hence is trivial because L/K is geometric.

4. Chebotarev Argument

4.1. **Notation.** We write $f(x) = O(g(x))$, as usual, to indicate that there is a constant $c > 0$ such that $f(x) < c \cdot g(x)$, for all x. Moreover, we assume that c depends at most on the genus of K, $\deg(S)$, and the 'regulator' $R = \det(\Sigma)$. We remark that the only place R appears is in the proof of lemma 9. We write $f(x) = o(g(x))$ to indicate that $f(x)/g(x)$ tends to 0 as x tends to ∞.

4.2. **Weil and Murty-Scherk Bounds.** There is a finite set of places S of K such that $K(\Sigma/\ell)/K$, a fortiori $K(E[\ell])/K$, is unramified away from S for every $\ell \neq p$. On the other hand, if $V : E^{(p)} \to E$ is the Verschiebung, then $K(\Sigma/V)/K$ is unramified away from a divisor of degree $O(p\deg(S))$. In particular, every extension we encounter in this section will be unramified away from a divisor of uniformly bounded degree d, even tamely ramified, hence the following lemma will be useful.

Lemma 5. *If F/K is a tame extension which is unramified away from a divisor of degree at most d, then the genus of F is $O([F : K])$.*

Proof. This follows immediately from the Riemann-Hurwitz formula for the extension F/K:

$$2 \cdot \text{genus}(F) - 2 = [F : K](2 \cdot \text{genus}(K) - 2) + (\text{ramification part}).$$

The ramification term part is at most $d([F : K] - 1)$. □

Let V denote the open complement of S and $V_n \subset V$ the subset of v such that $\deg(v) = n$. One effective Chebotarev theorem we need is a simple form of the Weil bound.

Theorem 5 (Weil)**.** *Suppose F/K is a tame, finite Galois and geometric extension, which is unramified away from S, and L/K is a subextension. Let W_n denote the subset of places w of L of degree n. Then for any $n \geq 1$,*

$$|\{w \in W_n : w \text{ splits completely in } F/L\}| = \frac{1}{[F : L]}|W_n| + O([L : K]\frac{q^{n/2}}{n}).$$

We note that the geometric assumption is crucial, for otherwise none of the points in W_n split completely for general n. The factor $[L : K]$ in the error term accounts for the genus of L.

Suppose L/K is a geometric subextension of the finite Galois extension F/K. Let $G = \mathrm{Gal}(F/L)$. For every place w of L, unramified in F, there is a well-defined conjugacy class $\mathrm{Fr}_w \subset G$, the so-called Frobenius class. Let $\mathbb{F}_{q^m} \subset F$ be the algebraic closure of $\mathbb{F}_q \subset K$. By assumption $\mathbb{F}_{q^m} \cap L = \mathbb{F}_q$, and there is a short exact sequence

$$1 \longrightarrow \mathrm{Gal}(F/\mathbb{F}_{q^m} L) \longrightarrow G \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \longrightarrow 1.$$

We write $G(q^n) \subset G$ for the subset of elements whose image in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the nth power of the Frobenius element. It is closed under conjugation by any element of G. Similarly, for any union of conjugacy classes $\mathcal{C} \subset G$, we write $\mathcal{C}(q^n)$ for the intersection $\mathcal{C} \cap G(q^n)$.

Theorem 6 (Murty-Scherk). *Suppose F/K is a tame, finite Galois extension which is unramified away from S, and L/K is a geometric subextension. Let $G = \mathrm{Gal}(F/L)$ and let W_n denote the subset of places w of L of degree n. Suppose $\mathcal{C} \subset G$ is a union of conjugacy classes. Then for $n \geq 1$,*

$$|\{w \in W_n : \mathrm{Fr}_w \subset \mathcal{C}(q^n)\}| = \frac{|\mathcal{C}(q^n)|}{|G(q^n)|}|W_n| + O([L : K] \cdot |\mathcal{C}(q^n)|^{1/2} q^{n/2}/n).$$

Except for the tameness condition, this is essentially theorem 2 in [MS]. As before, the factor $[L : K]$ in the error term accounts for the genus of L.

4.3. **Proof of Theorem 1.** We write V_n for the subset of places v of K such that $\deg(v) = n$. Let $\mathcal{L}$ denote the rational primes excluding $\mathcal{S}$ and let $\mathcal{F}$ denote the positive integers which are a square-free product of primes in $\mathcal{L}$. We write $\mathcal{G}_n \subset V_n$ for the subset of places v which are good with respect to $\mathcal{L}$, that is, for which Σ_v contains the prime-to-$\mathcal{S}$ part of E_v. Similarly, for any $f \in \mathcal{F}$, we write $\mathcal{B}_n(f) \subset V_n$ for the subset of v which are bad with respect to every ℓ dividing f.

For every $\ell \in \mathcal{L}, \ell \neq p$, we write K_ℓ for the extension $K(\Sigma/\ell)/K$. Similarly, for $\ell = p$, we write K_p for the extension $K(\Sigma/V)/K$, where $V : E^{(p)} \to E$ is the Verschiebung. In either case we let G_ℓ denote $\mathrm{Gal}(K_\ell/K)$ and $\mathcal{C}_\ell \subset G_\ell$ the subset of Lang-Trotter conjugacy classes. For every $v \in V_n$, we write $\mathrm{Fr}_v \subset G_\ell$ for the Frobenius conjugacy class. If we write $\mathcal{C}_\ell = \cup_\phi \mathcal{C}(\phi, \Sigma)$ (cf. section 2.3), then it follows from the definition of $\mathcal{C}(\phi, \Sigma)$ that $\mathrm{Fr}_v \cap \mathcal{C}(\phi, \Sigma)$ is non-empty if and only if ϕ is defined over the residue field $\mathbb{F}_q(v)$ and Σ_v is contained in the image $\phi(E_{\phi,v})$ (in the special fiber E_v); that is, $\mathrm{Fr}_v \subset \mathcal{C}_\ell$ if and only if $v \in \mathcal{B}_n(\ell)$.

For every $f = \ell_1 \cdots \ell_m \in \mathcal{F}$, we write G_f for the Galois group of the compositum $K_{\ell_1} \cdots K_{\ell_m}/K$. For every i, there is a natural map $G_f \to G_{\ell_i}$, and we define $\mathcal{C}_n \subset G_f$ to be the maximal subset whose image lies in $\mathcal{C}_{\ell_i}$ for all i. Then $\mathrm{Fr}_v \subset \mathcal{C}_f$ if and only if $v \in \mathcal{B}_n(f)$.

Given $x > 0$, let $\mathcal{L}(x)$ denote the $\ell \in \mathcal{L}$ such that $\ell \le x$, and $\mathcal{F}(x)$ the $f \in \mathcal{F}$ such that $\ell \in \mathcal{L}(x)$ for every ℓ which divides f. Given $y > x > 0$, let $\mathcal{L}(x, y)$ denote the complement $\mathcal{L}(y) - \mathcal{L}(x)$. We write $\mathcal{G}_n(x)$ for the $v \in V_n$ which are good with respect to every $\ell \in \mathcal{L}(x)$. One way to compute the density of $\mathcal{G}_n(x) \subset V_n$ is to apply a standard inclusion-exclusion argument and show that

$$|\mathcal{G}_n(x)| = \sum_{f \in \mathcal{F}(x)} \mu(f)\, |\mathcal{B}_n(f)|,$$

where $\mu : \mathcal{F} \to \{\pm 1\}$ is the Mobius function. Let $\mathcal{B}_n(x, y)$ denote the set of $v \in V_n$ which lie in $\mathcal{B}_n(\ell)$ for some $\ell \in \mathcal{L}(x, y)$. We make the trivial observation that $\mathcal{B}_n(\ell)$, $\mathcal{B}_n(\ell, \infty)$ are empty for $\ell > q^n + 2q^{n/2} + 1$, because ℓ must divide the order of E_v, hence $|\mathcal{G}_n| = |\mathcal{G}_n(x)|$ for x sufficiently large. On the other hand, for any $x > 0$, one can still show that

$$|\mathcal{G}_n| \ge |\mathcal{G}_n(x)| - |\mathcal{B}_n(x, \infty)|.$$

In general, the expected density of $\mathcal{B}_n(f) \subset V_n$ is given by the constant $\delta_n(f) = |\mathcal{C}_f(q^n)|/|G_f(q^n)|$ (cf. theorem 6), so we write

$$|\mathcal{B}_n(f)| = \delta_n(f)|V_n| + \varepsilon_f.$$

Similarly, the expected density of $\mathcal{G}_n(x) \subset V_n$ is given by $\Delta_n(x) = \prod_{\ell \in \mathcal{L}(x)}(1 - \delta_n(\ell))$, so we write

$$|\mathcal{G}_n(x)| = \Delta_n(x)|V_n| + \varepsilon(x).$$

A priori $\mathcal{G}_n(x)$ and $\Delta_n(x)$ depend on $\mathcal{L}$, but $\mathcal{L}$ is fixed for the entire section, so we omit the dependence from the notation. By the results of 2.3 it follows that $\delta_n(\ell)$ is bounded above and below by multiples of $1/(\ell^{r+1} m_n(\ell))$, where $m_n(\ell)$ is the order of the multiplicative group generated by $q^n \mod \ell$, which was denoted $\det(\Gamma)$ in 2.3. In fact, one can explicitly write down $\delta_n(\ell)$ in terms of these quantities. It follows from this estimate that $\Delta(x)$ converges as $x \to \infty$ and we define $\delta_n(\Sigma, \mathcal{S})$, appearing in theorem 1, as the limit. We further define a, b as the lower and upper bound for this limit obtained from the bound just mentioned for $\delta_n(\ell)$ and the estimates $1 \le m_n(\ell) \le l - 1$.

We estimate $|\varepsilon(x)|$ using the identity $\varepsilon(x) = \sum_{f \in \mathcal{F}(x)} \mu(f)\, \varepsilon_f$, and in turn, we estimate $|\varepsilon_f|$ using the following lemma.

Lemma 6. *For every $f \in \mathcal{F}$, we have*

$$\varepsilon_f = \mathcal{B}_n(f) - \delta_n(f)|V_n| = o(f^{(r+2)/2}q^{n/2}/n).$$

Proof. The lemma is an application of theorem 6 to K_f/K. Applying the result of sections 2.3 and 2.4, we see that $|\mathcal{C}_f(q^n)| \leq 2f^{r+2}$, for every $f \in \mathcal{F}(x)$. □

The lemma is useful only when x is sufficiently small. In fact, it suffices to take $x = x_n = n\log(q)/(2r+6)$.

Corollary 2. $|\varepsilon(x_n)| = o(q^n/n)$.

Proof. For every $f \in \mathcal{F}(x_n)$, we note that

$$\log(f) \leq \sum_{\ell \in \mathcal{L}(x_n)} \log(\ell) \leq |\mathcal{L}(x_n)| \log(x_n) \leq x_n + o(x_n),$$

and in particular, $\log(f) \leq 2x_n$ for n sufficiently large. Applying this to the error term of the lemma gives

$$|\varepsilon_f| = o(f^{(r+2)/2}q^{n/2}/n) = o(q^{n(r+2)/(2r+6)}q^{n/2}/n) = o(q^{n(2r+5)/(2r+6)}/n).$$

We also note that $|\mathcal{F}(x_n)| = 2^{|\mathcal{L}(x_n)|} \leq e^{x_n} = q^{n/(2r+6)}$, hence

$$|\varepsilon(x_n)| \leq \sum_{f \in \mathcal{F}(x_n)} |\varepsilon_f| = q^{n/(2r+6)} \cdot o(q^{n(2r+5)/(2r+6)}/n) = o(q^n/n).$$

□

By the corollary we have $\Delta_n(x)|V_n| - \delta_n(\Sigma, \mathcal{S})|V_n| = o(q^n/n)$ and thus, to complete the proof of theorem 1, it suffices to show that $\mathcal{B}_n(x_n, \infty) = o(q^n/n)$, because then

$$|\mathcal{G}_n| = |\mathcal{G}_n(x_n)| + o(q^n/n) = \delta_n(\Sigma, \mathcal{S})|V_n| + o(q^n/n).$$

We proceed in three stages by defining $y_n = q^{n/4}/\log(q^n)$ and $z_n = q^{n/4}\log\log(q^n)$, decomposing $\mathcal{L}(x_n, \infty)$ into three disjoint intervals

$$\mathcal{L}(x_n, \infty) = \mathcal{L}(x_n, y_n) \cup \mathcal{L}(y_n, z_n) \cup \mathcal{L}(z_n, \infty),$$

and utilizing the inequality

$$|\mathcal{B}_n(x_n, \infty)| \leq |\mathcal{B}_n(x_n, y_n)| + |\mathcal{B}_n(y_n, z_n)| + |\mathcal{B}_n(z_n, \infty)|.$$

We complete the proof by showing, in the following three lemmas, that each of the terms on the right are $o(q^n/n)$. In each case we use the inequality

$$|\mathcal{B}_n(x, y)| \leq \sum_{\ell \in \mathcal{L}(x,y)} |\mathcal{B}_n(\ell)|,$$

but we must use different arguments to bound the sum on the right.

Lemma 7 (Small ℓ)**.** $|\mathcal{B}_n(x_n, y_n)| = o(q^n/n)$.

Proof. For every $\ell \in \mathcal{L}(x_n, y_n)$, we fix a cyclic ℓ-isogeny $\phi : E_\phi \to E$. We note that, by theorem 2 of [CH], there is a constant $\ell_0 = O(1)$ such that $\Gamma = \mathrm{Gal}(K(E[\ell])/K)$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell)$ for every $\ell \neq p$, $\ell > \ell_0$. We may assume, without loss of generality, that $x_n \geq \max\{\ell_0, p\}$. The implied constant may be chosen, depending only on genus(K) and deg(S), to account for the failure of this assumption, and there are only finitely many n and degenerate Γ one must worry about. We write $B \subset \Gamma$ for the Borel subgroup corresponding to ϕ and identify it with $\mathrm{Gal}(K(E[\ell])/K(\phi))$. For every $w \in |K(\phi)|$, we write $\mathrm{Fr}_w \subset B$ for the Frobenius conjugacy class.

If ℓ does not divide $q^n - 1$, then we showed in section 2.3 that, for every $v \in \mathcal{B}_n(\ell)$, there is a unique $w \in |K(\phi)|$ of degree n and lying over v such that $\mathrm{Fr}_w \subset \mathcal{C}(\phi) \subset B$. For $i = 1, \ldots, r$, we write $\mathcal{B}_{n,i}(\ell)$ for the subset of $v \in \mathcal{B}_n(\ell)$ such that w splits completely in $K(\phi, P_i/\phi)$. In particular, applying theorem 5 we have

$$|\mathcal{B}_n(\ell)| \leq \sum_{i=1}^{r} |\mathcal{B}_{n,i}(\ell)| = r(q^n/\ell^2 + O(\ell q^{n/2}))/n.$$

On the other hand, if ℓ divides $q^n - 1$ and $v \in \mathcal{B}_n(\ell)$, then $\mathrm{Fr}_v = \{1\} \subset \Gamma$. Therefore v splits completely in $K(\phi, E_\phi[\phi])/K$, and theorem 5 implies

$$|\mathcal{B}_n(\ell)| \leq r(q^n/(\ell^2 + \ell) + O(\ell q^{n/2}))/n \leq r(q^n/\ell^2 + O(\ell q^{n/2}))/n.$$

Combining the results for all $\ell \in \mathcal{L}(x_n, y_n)$ we have

$$|\mathcal{B}_n(x_n, y_n)| \leq \sum_{\ell \in \mathcal{L}(x_n, y_n)} |\mathcal{B}_n(\ell)| \leq r(q^n(\sum_{\ell \in \mathcal{L}(x_n, y_n)} 1/\ell^2) + (y_n - x_n)O(y_n q^{n/2}))/n.$$

We note that $\sum_{\ell \in \mathcal{L}(x_n, y_n)} 1/\ell^2 = o(1)$, because x_n tends to infinity as n does, and $y_n = o(q^{n/4})$, hence $|\mathcal{B}_n(x_n, y_n)| = o(q^n/n)$ as desired. □

Lemma 8 (Medium ℓ)**.** $|\mathcal{B}_n(y_n, z_n)| = o(q^n/n)$.

Proof. We fix $\ell \in \mathcal{L}(y_n, z_n)$ and use the notation of the previous lemma. If ℓ does not divide $q^n - 1$ and $v \in \mathcal{B}_n(\ell)$, then we let $w \in |K(\phi)|$ be the canonical point over v as before. We write $\mathcal{B}'_{n,i}(\ell)$ for the subset of $v \in \mathcal{B}_n(\ell)$ such that w splits completely in $K(\phi, E_\phi[\phi])$. Applying theorem 5 gives

$$|\mathcal{B}'_{n,i}(\ell)| = (q^n/\ell + O(\ell q^{n/2}))/n.$$

On the other hand, if ℓ divides $q^n - 1$, we let $\mathcal{B}'_{n,i}(\ell)$ be the subset of $v \in V_n$ which split completely in $K(\phi, E_\phi[\phi])$. By another application of theorem 5 we have

$$|\mathcal{B}'_{n,i}(\ell)| = (q^n/\ell^2 + O(q^{n/2}))/n \leq (q^n/\ell + O(\ell q^{n/2}))/n.$$

Combining the results for all $\ell \in \mathcal{L}(y_n, z_n)$ gives

$$|\mathcal{B}_n(y_n, z_n)| \leq (q^n(\sum_{l \in \mathcal{L}(y_n,z_n)} 1/\ell) + |\mathcal{L}(y_n, z_n)|O(\ell q^{n/2}))/n.$$

Using the standard estimate $\sum_{\ell \leq x} 1/\ell = \log\log(x) + c + o(1)$, where c is a constant, gives

$$\begin{aligned}\sum_{l \in \mathcal{L}(y_n,z_n)} 1/\ell &= \log\log(z_n) - \log\log(y_n) + o(1) \\ &= \log\left(\frac{n\log(q) + 4\log\log\log(q^n)}{n\log(q) - 4\log\log(q^n)}\right) + o(1) = o(1).\end{aligned}$$

By the prime number theorem,

$$|\mathcal{L}(y_n, z_n)| \leq |\mathcal{L}(z_n)| \leq z_n/\log(z_n) + o(z_n/\log(z_n)),$$

hence

$$|\mathcal{L}(y_n, z_n)|O(\ell q^{n/2}) = O\left(\frac{4(\log\log(q^n))^2}{\log(q^n) + 4\log\log\log(q^n)} q^n\right) = o(q^n).$$

This entails that $|\mathcal{B}_n(y_n, z_n)| = o(q^n/n)$, as desired. ☐

Lemma 9 (Large ℓ)**.** $|\mathcal{B}_n(z_n, \infty)| = o(q^n/n)$, *for* $r \geq 6$.

Proof. For every $v \in V$, let Σ_v denote the image of Σ in E_v. Just as in the number field case, Σ is endowed with a quadratic form given by the canonical height pairing and we can argue in the same way as lemma 14 of [GM] to obtain that the number of $v \in V$ such that $|\Sigma_v| < y$ is $O(y^{(r+2)/r})$, where the implied constant depends on the regulator $R = \det(\Sigma)$. Their proof actually proves more, namely that the sum of $\deg v$ over the v's with $|\Sigma_v| < y$ is $O(y^{(r+2)/r})$. From the definition it follows that, for every $v \in \mathcal{B}_n(z_n, \infty)$, we have

$$|\Sigma_v| = O(q^n/z_n) = o(q^{3n/4}),$$

therefore

$$|\mathcal{B}_n(z_n, \infty)| = o((q^{3n/4})^{1+2/r})/n = o(q^{(3r+6)n/4r}/n).$$

The lemma follows by observing that $(3r + 6)/4r \leq 1$ if $r \geq 6$. ☐

References

[CH] A. Cojocaru and C. Hall, "Uniform Results for Serre's Theorem for Elliptic Curves," Int. Math. Res. Not. 2005 (2005), no. 50, 3065–3071.

[GM] R. Gupta and M. Ram Murty, "Primitive points on elliptic curves," Compositio Math. 58 (1986), no. 1, 13–44.

[KM] N.M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.

[LT] S. Lang and H. Trotter, "Primitive points on elliptic curves," Bull. Am. Math. Soc. 83 (1977), 289-292.

[MS] V.K. Murty, J. Scherk, "Effective versions of the Chebotarev density theorem for function fields," C.R. Acad. Sci. Paris, t. 319. Série I, 1994, pp. 523–528.

[U] D.L. Ulmer, "Elliptic curves with large rank over function fields," Annals of Math. 155 (2002), 295–315.

[V] J.F. Voloch, "Primitive points on constant elliptic curves over function fields," Bol. Soc. Brasil. Mat. 21 (1990), 91–94.

Chris Hall
Department of Mathematics
University of Texas, Austin, TX 78712, USA
E-mail: cjh@math.utexas.edu

José Felipe Voloch
Department of Mathematics
University of Texas, Austin, TX 78712, USA
E-mail: voloch@math.utexas.edu