HILBERT'S IRREDUCIBILITY THEOREM AND THE LARGER SIEVE

DAVID ZYWINA

Abstract. We describe an explicit version of Hilbert's irreducibility theorem using a generalization of Gallagher's larger sieve. We give applications to the Galois theory of random polynomials, and to the images of the adelic representation associated to elliptic curves varying in rational families.

1. Introduction

In this paper, we are interested in quantitative versions of Hilbert's irreducibility theorem (HIT). In §1.1, we will review the classical description of HIT in terms of polynomials and give a special case of our new bounds in this setting (our most general bound can be found in §2.2). As an illustration of these bounds, we then study the fundamental example of HIT in §1.2, i.e., the Galois group of a "random" polynomial of degree n.

A more serious application is given in §1.3 where we discuss the Galois representations associated to the division points of an elliptic curve. We shall start with a model of a non-isotrivial elliptic curve E over a field $K = k(T_1, \dots, T_n)$ where k is a number field and the T_i are independent variables. Associated to E, there is a Galois representation $\rho_E\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ describing the Galois action on the torsion points of $E(\overline{K})$. For most n-tuples $t = (t_1, \dots, t_n) \in k^n$, we obtain an elliptic curve E_t over k by specializing each T_i with t_i. For a "random" $t \in k^n$, we will describe the image of the corresponding Galois representation $\rho_{E_t}\colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$. For $k \neq \mathbb{Q}$, we will see that $\rho_{E_t}(\mathrm{Gal}(\bar{k}/k))$ agrees with the image of ρ_E for most $t \in k^n$. The case $k = \mathbb{Q}$ is subtler, and we will see that $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is usually a subgroup of index r in $\rho_E(\overline{K}/K)$ where r is a certain positive integer depending on E.

1.1. Hilbert's irreducibility theorem.

Let k be a number field with a fixed algebraic closure $\bar{k}$. Fix a monic irreducible polynomial $f(x, T_1, \dots, T_n) \in k(T_1, \dots, T_n)[x]$ in the variable x. To ease notation slightly, we will denote the n-tuple of independent variables $(T_1, \dots, T_n)$ by T. Let L be the splitting field of $f(x, T) \in k(T)[x]$ in a fixed algebraic closure $\overline{k(T)}$. Denote the Galois group $\mathrm{Gal}(L/k(T))$ by G.

Now let Ω_f be the set of $t \in k^n$ for which some coefficient of $f(x, T)$ has a pole at $T = t$, or for which $f(x, t)$ is not separable. For each $\in k^n - \Omega_f$, let L_t be the splitting field of $f(x, t) \in k[x]$ in $\bar{k}$ and define $G_t = \mathrm{Gal}(L_t/k)$. Specialization induces an inclusion $G_t \subseteq G$ which is uniquely determined up to conjugation. We then have the following:

Theorem 1.1 (Hilbert's irreducibility theorem)**.** *For "most" points $t \in k^n - \Omega_f$, we have $G_t = G$.*

Of course one needs to make the "*most*" condition precise. In this paper, we shall interpret this in terms of natural density. Let H be the absolute (multiplicative) height on $\mathbb{P}^n(\bar{k})$, see [HS00, §B.2] for background. For example, if $x_0, \dots, x_n$ belong to $\mathbb{Z}$ and satisfy $\gcd(x_0, \dots, x_n) = 1$, then $H([x_0, \cdots, x_n]) = \max_i |x_i|$. We shall also view H as a function on $k^n = \mathbb{A}^n(k)$ by using the open embedding $\mathbb{A}^n_k \to \mathbb{P}^n_k$, $(x_1, \dots, x_n) \mapsto [x_1, \cdots, x_n, 1]$. For any real number $B \geq 1$, there are only finitely many $t \in k^n$ with $H(t) \leq B$.

A precise formulation of Theorem 1.1 is then the following

$$\lim_{B \to +\infty} \frac{|\{t \in k^n - \Omega_f : H(t) \leq B,\ G_t = G\}|}{|\{t \in k^n : H(t) \leq B\}|} = 1.$$

Intuitively, this says that if we write down large "random" $t_1, \dots, t_n \in k$, then almost surely the splitting field of the polynomial $f(x, t)$ over k has Galois group G. As a consequence we find that $f(x, t) \in k[x]$ is

Date: November 30, 2010.

2000 *Mathematics Subject Classification.* Primary 12E25; Secondary 11G05, 11F80, 11N36.

Key words and phrases. Hilbert's irreducibility theorem, elliptic curves, Galois representations, sieve methods.

irreducible for "most" $t \in k^n$. Another possible notion of "most" is that the theorem holds for all t outside a *thin* subset of k^n (see [Ser97, §9] or [Ser08, §3] for details).

We will also want to consider integral versions of HIT, let $\mathcal{O}_k$ be the ring of integers of k. For $t = (t_1, \dots, t_n) \in \mathcal{O}_k^n$, define $\|t\| = \max_{\sigma,i} |\sigma(t_i)|$ where σ runs over the field embeddings $\sigma\colon k \hookrightarrow \mathbb{C}$. The following theorem, which is a consequence of the large sieve, gives essentially the best general upper bound available. For reference, we note that there are positive constants $c_{n,k}$ and $c'_{n,k}$ such that

$$|\{t \in \mathcal{O}_k^n : \|t\| \le B\}| \sim c_{n,k} B^{[k:\mathbb{Q}]n} \qquad \text{and} \qquad |\{t \in k^n : H(t) \le B\}| \sim c'_{n,k} B^{[k:\mathbb{Q}](n+1)} \tag{1.1}$$

as $B \to +\infty$.

Theorem 1.2 (Cohen, Serre)**.** *With notation as above,*

$$|\{t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \ne G\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n-1/2)} \log B \quad \textit{and}$$
$$|\{t \in k^n - \Omega_f : H(t) \le B,\, G_t \ne G\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n+1/2)} \log B.$$

This follows from Theorems 1 and 2 of [Ser97, §13] (where $\log B$ can be actually be replaced with $(\log B)^\lambda$ for some $\lambda < 1$). The integral version with a more explicit constant can be found in [Coh79]. Here is an equivalent version of Theorem 1.2:

Theorem 1.3. *With notation as above, let C be a proper subset of G that is stable under conjugation. Then*

$$|\{t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \subseteq C\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n-1/2)} \log B \quad \textit{and}$$
$$|\{t \in k^n - \Omega_f : H(t) \le B,\, G_t \subseteq C\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n+1/2)} \log B.$$

Theorem 1.3 follows directly from Theorem 1.2. Let us explain the other implication; we consider only the integral case. If $G_t \ne G$, then it must lie in some maximal subgroup M of G. Since our G_t is only uniquely defined up to conjugation, it is less ambiguous to write $G_t \subseteq \bigcup_{g \in G} gMg^{-1}$. So we have

$$|\{t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \ne G\}| \le \sum_M \left| \left\{ t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \subseteq \bigcup_{g \in G} gMg^{-1} \right\} \right| \tag{1.2}$$

where the sum is over representatives of the conjugacy classes of maximal subgroups of G. Define $\delta(G, M) := |\bigcup_{g \in G} gMg^{-1}|/|G|$. By Jordan's lemma [Ser03], we know that $\bigcup_{g \in G} gMg^{-1}$ is a proper subset of G (equivalently $\delta(G, M) < 1$). Applying the bound of Theorem 1.3 to the right hand side of (1.2) gives

$$|\{t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \ne G\}| \ll_{n,f,k} \sum_M B^{[k:\mathbb{Q}](n-1/2)} \log B.$$

We obtain Theorem 1.2 by noting that the number of representatives M of maximal subgroups is $O_n(1)$.

Our main abstract result is the following general bound which beats the large sieve when $|C|/|G| < 1/2$. Its proof utilizes an extension of Gallagher's *larger sieve*. We will state a more general version of this theorem in §2.2 that removes the assumption that $L/k(T)$ is geometric (i.e., $L \cap \bar{k} = k$) and gives better control over the implicit constant.

Theorem 1.4. *Assume that $L/k(T)$ is geometric and let C be a subset of G that is stable under conjugation. Then*

$$|\{t \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \subseteq C\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n-1+|C|/|G|)} \log B \quad \textit{and}$$
$$|\{t \in k^n - \Omega_f : H(t) \le B,\, G_t \subseteq C\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n+|C|/|G|)} \log B.$$

Arguing as before, Theorem 1.4 implies that

$$|\{a \in \mathcal{O}_k^n - \Omega_f : \|t\| \le B,\, G_t \ne G\}| \ll_{n,f,k} B^{[k:\mathbb{Q}](n-1+\delta(G))} \log B \tag{1.3}$$

where $\delta(G)$ is the maximum of the $\delta(G, M)$ over all maximal subgroups M of G. The bound (1.3) is superior to that of the large sieve if $\delta(G) < 1/2$. Unfortunately $\delta(G) \ge 1/2$ for many interesting groups (an example where (1.3) is superior is when G is a p-group with odd p, since one has $\delta(G) = 1/p$).

As we will see in the next section, the larger sieve can be used to deal with the *small* maximal subgroups M of G, that is, small in the sense of the quantity $\delta(G, M)$. This leaves the larger maximal subgroups to be studied using alternate methods.

1.2. **The Galois group of a random polynomial.** We now consider the fundamental example of Hilbert's irreducibility theorem. Fix a positive integer n. For $T = (T_1, \dots, T_n)$, define the polynomial

$$f(x, T) = x^n + T_1 x^{n-1} + \cdots + T_{n-1} x + T_n.$$

For $t \in \mathbb{Z}^n$, let G_t be the Galois group of the splitting field of $f(x, t)$ over $\mathbb{Q}$. By numbering the roots of $f(x, t)$, we may view G_t as a subgroup of S_n. Hilbert's irreducibility theorem says that $G_t = S_n$ for "most" choices of $t \in \mathbb{Z}^n$.

We now consider a quantitative version. Define the following counting function

$$E_n(B) := |\{t \in \mathbb{Z}^n : \|t\| \le B,\, G_t \ne S_n\}|$$

(recall that $\|t\| = \max_i |t_i|$). We will restrict ourselves to $n \ge 3$, since $n = 1$ is uninteresting and it is known that $E_2(B) \sim 2B \log B$.

In 1936, van der Waerden [vdW36] gave the explicit bound

$$E_n(B) \ll_n B^{n - \frac{c}{\log\log B}} \qquad \text{with } c = \frac{1}{6(n-2)},$$

and further conjectured that $|E_n(B)| \ll_n B^{n-1}$ for $n > 2$. Van der Waerdan's conjecture is best possible since the polynomials $f(x, t_1, \dots, t_{n-1}, 0)$ are always reducible and hence $|E_n(B)| \gg B^{n-1}$.

In 1956, Knobloch [Kno56] gave the improved bound

$$E_n(B) \ll_n B^{n - c_n} \qquad \text{with } c_n = \frac{1}{18n(n!)^3}.$$

In 1973, Gallagher [Gal73] used a higher dimensional large sieve to give the bound

$$E_n(B) \ll_n B^{n-1/2} (\log B)^{1-\gamma_n} \tag{1.4}$$

where $\{\gamma_n\}$ is a sequence of positive numbers with $\gamma_n \sim (2\pi n)^{-1/2}$. This power of the $\log B$ can be further improved, but the large sieve is incapable of lowering the power of B that occurs.

There has been some progress for small n. For any $\varepsilon > 0$, one has $E_3(B) \ll_\varepsilon B^{2+\varepsilon}$ and $E_4(B) \ll_\varepsilon B^{3+\varepsilon}$ (this is due to Lefton [Lef79] and Dietmann [Die06], respectively). We have the following modest improvement for large n.

Proposition 1.5. *For all n sufficiently large, we have*

$$E_n(B) \ll_n B^{n - \frac{1}{2}}.$$

If instead we count those $t \in \mathbb{Z}^n$ for which G_t is neither S_n nor the alternating group A_n, then we have the following significantly stronger bound.

Theorem 1.6. *For every $\varepsilon > 0$ there is an N such that*

$$|\{a \in \mathbb{Z}^n : \|t\| \le B,\, G_t \ne S_n \text{ and } G_t \ne A_n\}| \ll_n B^{n-1+\varepsilon} \tag{1.5}$$

for all $n \ge N$.

Remark 1.7. It should be noted that the condition "$G_t \ne S_n$ and $G_t \ne A_n$" does show up in practice. For example, let $f(x) \in \mathbb{Z}[x]$ be a separable polynomial of degree $n \ge 5$ and let C_f be the hyperelliptic curve with affine model $y^2 = f(x)$. Let $J(C_f)$ be the Jacobian of C_f; it is an abelian variety over $\mathbb{Q}$ of dimension $2\lfloor (n-1)/2 \rfloor$. Zarhin [Zar00] has shown that if $\mathrm{Gal}(f) = A_n$ or $\mathrm{Gal}(f) = S_n$, then $\mathrm{End}(J(C_f)_{\overline{\mathbb{Q}}}) = \mathbb{Z}$. Theorem 1.6 thus gives an upper bound on the number of $t \in \mathbb{Z}^n$ with $\|t\| \le B$ for which $f(x, t)$ is not separable or $\mathrm{End}(J(C_{f(x,t)})_{\overline{\mathbb{Q}}}) \ne \mathbb{Z}$.

Remark 1.8. R. Dietmann [Die10] has recently given a proof of Theorem 1.6 that gives superior bounds than ours. In particular, he proves that $|\{a \in \mathbb{Z}^n : \|t\| \le B,\, G_t \ne S_n \text{ and } G_t \ne A_n\}| \ll_{n,\varepsilon} B^{n-1+e(n)+\varepsilon}$ where $e(n)$ is the middle binomial coefficient $\binom{n}{\lfloor n/2 \rfloor}$. Dietmann's techniques are not sieve theoretic; he uses Galois resolvents to reduce the question to counting integral points on certain varieties.

The first thing to note is that Theorem 1.4 by itself does not lead to an improved bound for $E_n(B)$. Let M_1 be the maximal subgroup of S_n that stabilizes the letter 1. Since $\delta(S_n, M_1) = 1 - \sum_{i=0}^{n}(-1)^i/i!$ (this is just the proportion of elements in S_n that are not derangements) we find that $\limsup_{n\to\infty} \delta(S_n) \geq 1 - e^{-1}$, and in fact equality holds. Equation (1.3) would then give the inferior bound $E_n(B) \ll_n B^{n-e^{-1}+o_n(1)}$.

Instead we shall treat M_1 separately. Note that $G_t \subseteq \bigcup_{g\in G} gM_1g^{-1}$ if and only if $f(x,t)$ has a root in $\mathbb{Z}$. The following theorem bounds the number of t with $f(x,t)$ reducible.

Theorem 1.9 (van der Waerden [vdW36]). *For an integer $1 \leq i \leq n/2$, we have*

$$|\{t \in \mathbb{Z}^n : \|t\| \leq B, f(x,t) \text{ is reducible with a factor of degree } i\}| \ll_n \begin{cases} B^{n-i} & \text{if } i < n/2, \\ B^{n-i}\log B & \text{if } i = n/2. \end{cases}$$

Remark 1.10. Using van der Waerdan's theorem and counting those t for which $f(x,t)$ has a root in $\mathbb{Z}$, Chela [Che63] showed that

$$|\{t \in \mathbb{Z}^n : \|t\| \leq B,\ f(x,t) \text{ is reducible}\}| \sim c_n B^{n-1}$$

as $B \to +\infty$, where $c_n > 0$ is an explicit constant.

Using this theorem we now need only consider those t for which $f(x,t)$ is irreducible; in other words, those t for which G_t is a transitive subgroup of S_n. Let $\mathcal{M}_n$ be the set of transitive subgroups of S_n that are neither A_n or S_n. The following theorem of Łuczak and Pyber shows that few elements of S_n belong to any of the $M \in \mathcal{M}_n$.

Theorem 1.11 (Łuczak-Pyber [ŁP97]). *We have* $\lim_{n\to\infty} \dfrac{|\bigcup_{M\in\mathcal{M}_n} M|}{|S_n|} = 0.$

Proof of Theorem 1.6. From Theorem 1.9, we know that

$$|\{t \in \mathbb{Z}^n : \|t\| \leq B,\ G_t \text{ is a non-transitive subgroup of } S_n\}| \ll_n B^{n-1}. \tag{1.6}$$

By Theorem 1.11 there exists an N such that $|\bigcup_{M\in\mathcal{M}_n} M|/|S_n| < \varepsilon$ for all $n \geq N$. Applying Theorem 1.4 with $C = \bigcup_{M\in\mathcal{M}_n} M$ gives

$$|\{t \in \mathbb{Z}^n : \|t\| \leq B,\ G_a \in \mathcal{M}_n\}| \ll_n B^{n-1+\varepsilon} \tag{1.7}$$

for all $n \geq N$. Theorem 1.6 follows by combining (1.6) and (1.7). □

Thus to improve on Gallagher's bound, at least for n large enough, it suffices to bound the function

$$E_n'(T) = |\{t \in \mathbb{Z}^n : \|t\| \leq B,\ G_t \subseteq A_n\}|.$$

Equivalently, bound the number of $t \in \mathbb{Z}^n$ with $\|t\| \leq B$ for which $\Delta(t_1, \ldots, t_n)$ is a square, where $\Delta(T_1, \ldots, T_n) \in k[T_1, \ldots, T_n]$ is the discriminant of $x^n + T_1x^{n-1} + \cdots + T_{n-1}x + T_n$. Using the large sieve one can show that $E_n'(T) \ll_n B^{n-1/2}$ which completes the proof of Proposition 1.5.

Remark 1.12. In the final comments of [ŁP97], the authors claim that $|\bigcup_{M\in\mathcal{M}_n} M|/|S_n| = O(n^{-\alpha})$ for some absolute constant $\alpha > 0$. This would imply the following strengthening of (1.5):

$$|\{t \in \mathbb{Z}^n : \|t\| \leq B,\ G_t \neq S_n \text{ and } G_t \neq A_n\}| \ll_n B^{n-1+O(n^{-\alpha})}.$$

We should also point out that an analogue of Theorem 1.11 has recently been proven for almost simple Chevalley group over $\mathbb{F}_q$ where the rank is fixed and $q \to \infty$ [FG09].

1.3. Galois actions on the torsion points of elliptic curves.

1.3.1. *Serre's open image theorem.* Consider an elliptic curve E defined over a field K. For each positive integer m relatively prime to the characteristic of K, let $E[m]$ be the m-torsion subgroup of $E(\overline{K})$. The group $E[m]$ is non-canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ and has a natural $\mathrm{Gal}(\overline{K}/K)$-action which can be expressed in terms of a Galois representation

$$\rho_{E,m}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

If K has characteristic 0, then combining these representations together we obtain a single Galois representation

$$\rho_E\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

which describes the Galois action on all the torsion points of E (where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$). The main result for these representations over number fields is the following important theorem of Serre [Ser72].

Theorem 1.13 (Serre)**.** *Let k be a number field and let E be an elliptic curve over k without complex multiplication. Then $\rho_E(\mathrm{Gal}(\bar{k}/k))$ is a finite index subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

1.3.2. *Families of elliptic curves.* Fix a number field k, an integer $n \geq 1$, and define the field $K := k(T_1, \dots, T_n) = k(T)$. Let E be an elliptic curve over the function field K, and assume that the j-invariant of E does not belong to k. Now choose a model for E/K, say, a short Weierstrass model

$$y^2 = x^3 + a(T)x + b(T).$$

Let Ω be the set of $t \in k^n$ for which $a(T)$ and $b(T)$ have a pole at $T = t$ or for which the discriminant of the Weierstrass equation is zero at $T = t$. Then for each $t \in k^n - \Omega$, the curve E_t obtained by replacing T with t in our model, i.e., $y^2 = x^3 + a(t)x + b(t)$, is an elliptic curve over k. Our goal is to understand how the images of ρ_{E_t} vary with $t \in k^n - \Omega$, and in particular to describe the image for "most" t in terms of E/K.

For each integer $m \geq 1$, we define the group $\mathcal{H}_E(m) = \rho_{E,m}(\mathrm{Gal}(\overline{K}/K))$. Specialization by $t \in k^n - \Omega$ gives an inclusion $\rho_{E_t,m}(\mathrm{Gal}(\bar{k}/k)) \subseteq \mathcal{H}_E(m)$ that is determined up to conjugation. We may thus view $\rho_{E_t}(\mathrm{Gal}(\bar{k}/k))$ as a subgroup of $\mathcal{H}_E := \rho_E(\mathrm{Gal}(\overline{K}/K))$ which again is uniquely determined up to conjugation. Hilbert's irreducibility theorem implies that $\rho_{E_t,m}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E(m)$ for "most" t (where m is fixed). It also *suggests* that $\rho_{E_t}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E$ holds for most t.

Theorem 1.14. *Suppose that $k \neq \mathbb{Q}$. Then*

$$\frac{|\{t \in k^n - \Omega : H(t) \leq B,\ \rho_{E_t}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E\}|}{|\{t \in k^n : H(t) \leq B\}|} = 1 + O\big(B^{-1/2}\log B\big) \quad \textit{and}$$
$$\frac{|\{t \in \mathcal{O}_k^n - \Omega : \|t\| \leq B,\ \rho_{E_t}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E\}|}{|\{t \in \mathcal{O}_k^n : \|t\| \leq B\}|} = 1 + O\big(B^{-1/2}\log B\big)$$

where the implicit constants do not depend on B.

First observe that the choice of model is not important for this theorem. The specializations of any two models will agree away from some closed subvariety $Z \subsetneq \mathbb{A}_k^n$, and the k-rational points of Z have density zero in k^n.

Secondly, it is important to note that Theorem 1.14 is *not* a direct consequence of HIT (since $\mathcal{H}_E$ is an infinite group). This is well illustrated by the fact that Theorem 1.14 can fail when $k = \mathbb{Q}$.

Let us describe why we excluded $k = \mathbb{Q}$. Recall that for a profinite group H, the *commutator subgroup* $[H, H]$ is the smallest closed normal subgroup of H for which $H/[H, H]$ is abelian.

Fix a $t \in \mathbb{Q}^n - \Omega$, and suppose that $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathcal{H}_E$. The homomorphism $\det \circ \rho_{E_t} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character. Therefore, $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}})) = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ where $\mathbb{Q}^{\mathrm{cyc}}$ is the cyclotomic extension of $\mathbb{Q}$. Let $\mathbb{Q}^{\mathrm{ab}}$ be the maximal abelian extension of $\mathbb{Q}$. The commutator subgroup of $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))$, so $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})) = [\mathcal{H}_E, \mathcal{H}_E]$.

The Kronecker-Weber theorem says that $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, so an equality $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathcal{H}_E$ would imply that $[\mathcal{H}_E, \mathcal{H}_E] = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. This relation need not hold though! For example, with $\mathcal{H}_E = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, the group $[\mathrm{GL}_2(\widehat{\mathbb{Z}}), \mathrm{GL}_2(\widehat{\mathbb{Z}})]$ has index 2 in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Our main result for $k = \mathbb{Q}$ is the following.

Theorem 1.15. *Suppose that $k = \mathbb{Q}$. Let r be the index of $[\mathcal{H}_E, \mathcal{H}_E]$ in $\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Then for any $\varepsilon > 0$,*

$$\frac{\big|\big\{t \in \mathbb{Q}^n - \Omega : H(t) \leq B,\ \big[\mathcal{H}_E : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\big] = r\big\}\big|}{|\{t \in \mathbb{Q}^n : H(t) \leq B\}|} = 1 + O(B^{-1/2+\varepsilon}) \quad \textit{and}$$
$$\frac{\big|\big\{t \in \mathbb{Z}^n - \Omega : \|t\| \leq B,\ \big[\mathcal{H}_E : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\big] = r\big\}\big|}{|\{t \in \mathbb{Z}^n : \|t\| \leq B\}|} = 1 + O(B^{-1/2+\varepsilon})$$

where the implicit constants do not depend on B.

Remark 1.16. The proof of Theorem 1.15 will actually show that $\rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})) = [\mathcal{H}_E, \mathcal{H}_E]$ for "most" t. For such t, $G = \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{H}_E, \mathcal{H}_E]$. The group G depends on t and not necessarily on E/K alone.

These theorems build on several earlier results. Much focus has been on the family $y^2 = x^3 + t_1 x + t_2$ with $(t_1, t_2) \in \mathbb{Z}^2$ in a growing box. In this context, Duke [Duk97] showed that for "most" elliptic curve $E/\mathbb{Q}$ one has $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes ℓ. Grant [Gra00] gave another proof with an asymptotic expression for those elliptic curves that do not have surjective mod ℓ representations for all ℓ.

Cojocaru and Hall [CH05] considered considered a fixed model of an elliptic curve E over $\mathbb{Q}(T)$ $(n = 1)$ with non-constant j-invariant. They proved that for "most" specializations $t \in \mathbb{Q}$, one has $\rho_{E_t,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq 17$. This will be reproved when we generalize to higher dimensions and number fields and is essentially Theorem 1.15.

Building on Duke's theorem, Jones [Jon10] was able to show that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = 2$ for "most" elliptic curve E over $\mathbb{Q}$ (such curves are called *Serre curves* in the literature). There has also been recent work of Cojocaru, Grant and Jones [CGJ10] studying Serre curves in one-parameter families which gives results similar to Theorem 1.15(i) with $n = 1$; they give much stronger error terms than ours but their methods do not generalize to arbitrary number fields.

For $k \neq \mathbb{Q}$, the integral point version of Theorem 1.14 for the family $y^2 = x^3 + t_1 x + t_2$ was proved in [Zyw10].

The proofs in all these papers, except Grant's and [CGJ10], uses some version of the large sieve (Grant's paper requires deep theorems of Mazur on elliptic curves over $\mathbb{Q}$, and in particular do not generalize to the $k \neq \mathbb{Q}$ setting).

A key ingredient in the proof of our theorems is an effective version of HIT applied to the representation $\rho_{E,\ell}$ for rational primes ℓ.

Proposition 1.17. *For each rational prime $\ell \geq 17$, we have*

$$|\{t \in \mathcal{O}_k^n - \Omega : \|t\| \leq B,\ \rho_{E_t,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}| \ll_E \ell^6 B^{[k:\mathbb{Q}](n-1/2+O(1/\ell))} \log B.$$

where the implicit constants depend only on the model for E/K and the exceptional set Ω.

Since we are interested in the Galois action on the full torsion groups of elliptic curves (and hence with varying ℓ) it is vital to have bounds with both good and explicit dependencies on ℓ. With $\ell > 19$, one can use Faltings theorem (originally the Mordell conjecture) to prove that

$$|\{t \in \mathcal{O}_k^n - \Omega : \rho_{E_t,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}| \ll_{E,\ell} 1.$$

While this seems much stronger than Proposition 1.17, the difficulty in controlling how the implicit constant depends on ℓ makes it unusable for our application.

The other major ingredient in the proof of Theorem 1.14 will be an effective version of Serre's open image theorem due to Masser and Wüstholz. Note that even to prove a more *qualitative* version of Theorem 1.14, with the big-O term replaced with $o(1)$, we still need to use *quantitative* HIT bounds.

1.3.3. *Examples.* We now give a few examples of families of elliptic curves to illustrate the theoretic results above.

Example 1.18. Let E be the elliptic curve over the function field $k(j)$ defined by the Weierstrass equation

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}. \tag{1.8}$$

This elliptic curve has j-invariant j, and for each $t \in k - \{0, 1728\}$, specializing j by t gives an elliptic curve E_t over k with j-invariant t. The image of ρ_E is

$$\mathcal{H}_E = \left\{A \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : \det(A) \in \chi_k(\mathrm{Gal}(\bar{k}/k))\right\}$$

where $\chi_k \colon \mathrm{Gal}(\bar{k}/k) \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character of k. Note that $\mathcal{H}_E = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ if and only if $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. If $k \neq \mathbb{Q}$, then by Theorem 1.14 we find that for "most" choices of $t \in k - \{0, 1728\}$, the elliptic curve E_t/k satisfies $\rho_{E_t}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E$

Now consider the case $k = \mathbb{Q}$. We have $\mathcal{H}_E = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}), \mathrm{GL}_2(\widehat{\mathbb{Z}})]$ has index 2 in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. By Theorem 1.15,

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = 2$$

for "most" $t \in \mathbb{Q} - \{0, 1728\}$.

Similar remarks hold for the elliptic curve E over $k(a, b)$ given by the equation $y^2 = x^3 + ax + b$; it has the same monodromy group $\mathcal{H}_E$.

Example 1.19. Let E be be the elliptic curve over the function field $k(\lambda)$ given by the Weierstrass equation

$$y^2 = x(x-1)(x-\lambda).$$

For simplicity assume that $k \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, so $\mathcal{H}_E = \{A \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : A \equiv I \pmod 2\}$. For each $t \in k - \{0, 1\}$, specializing λ by t gives an elliptic curve $E_t \colon y^2 = x(x-1)(x-t)$ over k. If $k \neq \mathbb{Q}$, then for "most" choices of $t \in k - \{0, 1\}$, the elliptic curve $E_t \colon y^2 = x(x-1)(x-t)$ satisfies $\rho_{E_t}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E$.

Now consider the case $k = \mathbb{Q}$. One can check that $[\mathcal{H}_E, \mathcal{H}_E] = \{A \in \mathrm{SL}_2(\widehat{\mathbb{Z}}) : A \equiv I \pmod 4\}$. Therefore by Theorem 1.15 we know that for "most" choices of $t \in \mathbb{Q} - \{0, 1\}$, the elliptic curve $E_t \colon y^2 = x(x-1)(x-t)$ satisfies

$$[\mathcal{H}_E : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = \big[\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{H}_E, \mathcal{H}_E]\big] = 8$$

and hence $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = 48$.

Example 1.20. Let E be an elliptic curve over $\mathbb{Q}(T)$ defined by replacing the variable j in (1.8) with

$$j = \frac{(T^{16} + 256T^8 + 4096)^3}{T^{32}(T^8 + 16)}. \tag{1.9}$$

For each $t \in \mathbb{Q} - \{0\}$, we have a specialization $E_t/\mathbb{Q}$ by replacing T by t. We claim that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = 1536$$

for "most" $t \in \mathbb{Q} - \{0\}$.

Let us briefly explain how this elliptic curve arises. Define the function $h(z) = \eta(z)/\eta(4z)$ on the upper-half plane where η is the Dedekind eta function. Let Γ be the group of $A \in \mathrm{SL}_2(\mathbb{Z})$ for which $h(A \cdot z) = h(z)$ where A acts on the upper-half plane via a linear fractional transformation. We claim that Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of index 48 and level 32, and the equation (1.9) holds when T is replaced by $h(z)$ and j is the modular j-function (these claims are straightforward to show after observing that $h(z)^8$ is the Hauptmodul of $\Gamma_0(4)$). Using that the Fourier expansion of $h(z)$ at ∞ has rational coefficients, one can argue that for each integer $m \geq 1$, the group $\pm\mathcal{H}_E(m)$ is conjugate to the group generated by $\Gamma \bmod m$ and the matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ with $d \in (\mathbb{Z}/m\mathbb{Z})^\times$. Some group theory then shows that $[\mathcal{H}_E : \mathcal{H}_E] = [\pm\mathcal{H}_E : \pm\mathcal{H}_E]$ has index 1536 in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ (moreover, $[\mathcal{H}_E : \mathcal{H}_E]$ is of the form $\mathcal{H} \times \prod_{\ell \neq 2} \mathrm{SL}_2(\mathbb{Z}_\ell)$ for a certain subgroup $\mathcal{H}$ of index 1536 in $\mathrm{SL}_2(\mathbb{Z}_2)$).

1.4. **Overview.** We now give a quick overview of the rest of the paper. In §2.2, we state our main version of HIT. In §3, we give an extension of the larger sieve to the setting of sieving rational or integral points; we also include a standalone application to arithmetic dynamics in §3.3. In §4, we state a special form of our larger sieve that will be suitable for our application of HIT which will be proved in §6.

Our general approach to finding bounds is to reduced to the one variable case; more geometrically, we have an open subvariety of $\mathbb{A}^n_k$ which we will fiber by lines. We then prove a version of HIT for each line separately, and then combine these individual bounds (it is thus vital to have uniform bounds, and this uniformity needs the equidistribution and Grassmannian calculations of §5).

Finally in §7, we give the details of our theorems on elliptic curves stated in §1.3; this involves combining our quantitative HIT with an effective version of Serre's open image theorem due to Masser and Wüstholz.

Notation. For a number field k, let $\mathcal{O}_k$ be the ring of integers and let Σ_k be the set of non-zero prime ideals of $\mathcal{O}_k$. For each $\mathfrak{p} \in \Sigma_k$, let $\mathbb{F}_\mathfrak{p}$ be the residue field $\mathcal{O}_k/\mathfrak{p}$ whose cardinality we denote by $N(\mathfrak{p})$. The degree of $\mathfrak{p}$ is the unique integer $\deg(\mathfrak{p})$ for which $N(\mathfrak{p}) = p^{\deg(\mathfrak{p})}$ where p is the prime lying under $\mathfrak{p}$. If K/k is a finite Galois extension and $\mathfrak{p}$ is unramified in K, then $(\mathfrak{p}, K/k)$ will denote the Artin symbol which is a conjugacy class of $\mathrm{Gal}(K/k)$. Let k^{cyc} and k^{ab} be the cyclotomic and maximal abelian extensions of k, respectively, in $\bar{k}$. The absolute height on $\mathbb{P}^n_k$ is denoted H.

For a finite group G, let $G^\sharp$ denote the set of conjugacy classes of G. For a profinite group G, the *commutator subgroup* $[G,G]$ is the smallest closed normal subgroup of G for which $G/[G,G]$ is abelian. We will always consider profinite groups with their profinite topology.

If X is a scheme over a ring R and we have a ring homomorphism $R \to R'$, then we denote by $X_{R'}$ the scheme $X \times_{\operatorname{Spec} R} \operatorname{Spec} R'$ over R'. The homomorphism is implicit in the notation; it will frequently be one of the natural homomorphisms $k \to \bar{k}$, $\mathcal{O}_k \to k$ and $\mathcal{O}_k \to \mathbb{F}_\mathfrak{p}$.

Suppose that f and g are real valued functions of a real variable x. By $f \ll g$ (or $g \gg f$), we shall mean that there are positive constants C_1 and C_2 such that for all $x \geq C_1$, $|f(x)| \leq C_2|g(x)|$. We shall use $O(f)$ to denote an unspecied function g with $g \ll f$. When needed we will indicate the dependence of the implied constants with subscripts on $\ll$ or O, and in the main results we will indicate the dependencies.

Acknowledgments. Thanks to David Brown for several useful suggestions.

2. Main version

2.1. **Reinterpretation.** It will be useful to view Hilbert's irreducibility theorem in terms of algebraic geometry. Let U be a non-empty open subvariety of $\mathbb{P}^n_k$, and let

$$\rho\colon \pi_1(U) \to G$$

be a continuous and surjective homomorphism where G is a finite group and $\pi_1(U)$ is the *étale fundamental group* of U. For every point $u \in U(k)$, we have a homomorphism

$$\rho_u\colon \operatorname{Gal}(\bar{k}/k) = \pi_1(\operatorname{Spec} k) \xrightarrow{u_*} \pi(U) \xrightarrow{\rho} G$$

by viewing u as a k-morphism $\operatorname{Spec} k \to U$ and using the functoriality of π_1.

Denote the image of ρ_u by G_u. Note that we have suppressed the base points of our fundamental groups, and thus the representations ρ and ρ_u are uniquely defined only up to an inner automorphism of G. Moreover, the subgroup G_u of G is only defined up to conjugation; this is not a problem for us since the condition $G_u = G$ is well-defined. We will frequently suppress base points when the choice does not matter. *Hilbert's irreducibility theorem* is then the statement that $G_u = G$ for "most" $u \in U(k)$.

Let's describe how this version of HIT relates to the classical polynomial version described in the introduction. Let $f(x, T_1, \dots, T_n) \in k(T_1, \dots, T_n)[x]$ be an irreducible polynomial. Let L be the splitting field of f over $k(T_1, \dots, T_n)$ in a fixed algebraic closure. Let X be a variety over k with function field L. The extension $L/k(T_1, \dots, T_n)$ gives a dominant rational map $\pi\colon X \dashrightarrow \mathbb{A}^n_k = \operatorname{Spec} k[T_1, \dots, T_n]$. By replacing X with a suitable non-empty open subvariety, we have an étale morphism $\pi\colon X \to U$ where U is an open subvariety of $\mathbb{A}^n_k$. Let G be the group of automorphisms of $\pi\colon X \to U$. The group G acts faithfully on X and π induces an isomorphism $X/G \xrightarrow{\sim} U$, so the cover $\pi\colon X \to U$ gives a continuous homomorphism $\pi_1(U) \to G$. Note that we have $G \cong \operatorname{Gal}(L/k(T))$. For $u \in U(k) \subseteq k^n$, the group G_u will agree with the corresponding group constructed in §1.1.

2.2. **Uniform Hilbert's Irreducibility Theorem.** Let U be a non-empty open subvariety of $\mathbb{P}^n_k$, and let

$$\rho\colon \pi_1(U) \to G$$

be a continuous and surjective homomorphism where G is a finite group and $\pi_1(U)$ is the étale fundamental group of U. Let G^g be the image of $\pi_1(U_{\bar{k}})$ under ρ, and let K be the minimal extension of k in $\bar{k}$ for which G^g is the image of $\pi_1(U_K)$. We have a short exact sequence

$$1 \to G^g \to G \xrightarrow{\varphi} \operatorname{Gal}(K/k) \to 1.$$

For each $u \in U(k)$, let G_u be the image of

$$\operatorname{Gal}(\bar{k}/k) = \pi_1(\operatorname{Spec} k) \xrightarrow{u_*} \pi_1(U) \xrightarrow{\rho} G.$$

The subgroup G_u of G is uniquely defined up to conjugation.

We define $\mathcal{U}$ to be the open subscheme of $\mathbb{P}^n_{\mathcal{O}_k}$ that is the complement of the Zariski closure of $\mathbb{P}^n_k - U$ in $\mathbb{P}^n_{\mathcal{O}_k}$. The $\mathcal{O}_k$-scheme $\mathcal{U}$ has generic fiber U. There exists a finite set $S \subseteq \Sigma_k$ such that ρ factors through a homomorphism

$$\pi_1(\mathcal{U}_{\mathcal{O}}) \to G$$

where $\mathcal{O}$ is the ring of S-integers in k. The main quantitative form of HIT in this paper is the following:

Theorem 2.1. *Let C be a non-empty subset of G that is stable under conjugation. For each conjugacy class $\kappa \in \mathrm{Gal}(K/k)^\sharp$ define $C_\kappa = C \cap \varphi^{-1}(\kappa)$. Define the numbers $\delta := \max_{\kappa \in \mathrm{Gal}(K/k)^\sharp} \frac{1}{|\kappa|}\frac{|C_\kappa|}{|G^g|}$ and*

$$c := |G^g|^2 \exp\Bigg(\sum_{\substack{\mathfrak{p}\in S \\ \deg(\mathfrak{p})=1 \text{ and } N(\mathfrak{p})\geq |G^g|^2}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \Bigg).$$

(i) *Assume further that U is an open subvariety of $\mathbb{A}^n_k$. Then*

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\, G_u \subseteq C\}| \ll_U cB^{[k:\mathbb{Q}](n-1+\delta)} \log B.$$

(ii) *We have*

$$|\{u \in U(k) : H(u) \leq B,\, G_u \subseteq C\}| \ll_U cB^{[k:\mathbb{Q}](n+\delta)} \log B.$$

In both cases, the implicit constant depends only on U and the open embedding $U \subseteq \mathbb{P}^n_k$.

In the situation where $K = k$, we have $\delta = |C|/|G|$. This is the case in Theorem 1.4 where we made the assumption that $L/k(T)$ is geometric, hence Theorem 1.4 is an easy consequence of Theorem 2.1.

Remark 2.2. In applications, one might start with a representation $\rho\colon \pi_1(\mathcal{U}') \to G$ where $\mathcal{U}'$ is an open subscheme of $\mathbb{P}^n_{\mathcal{O}}$ for some ring $\mathcal{O}$ of S-integers. After possibly increasing S, the schemes $\mathcal{U}'$ and $\mathcal{U}_{\mathcal{O}}$ will agree. The reason for our construction of $\mathcal{U}$ from $U \subseteq \mathbb{P}^n_k$ is simply that our bounds can be expressed in terms of $U \subseteq \mathbb{P}^n_k$ and the set S.

3. The larger sieve

In this section, we give an extension of Gallagher's *larger sieve* [Gal71] (it is Theorem 3.4 below in the case $k = \mathbb{Q}$ and $n = 1$). Our versions can be used to sieve rational or integral points in $\mathbb{P}^n_k$ or $\mathbb{A}^n_k$, respectively. The larger sieve tends to be very effective when we consider sets that have strict constraints on the size of their images modulo several primes $\mathfrak{p}$. An identical version of the sieve in the case $\mathbb{P}^1_k$ can be found in [EEHK09]. We will only use the integral point version in this paper, the rational point version is included for future reference.

3.1. The larger sieve for rational points.

Theorem 3.1 (Larger sieve for $\mathbb{P}^n(k)$)**.** *Let k be number field. Let $\mathcal{A}$ be a finite subset of $\mathbb{P}^n(k)$ and $B > 0$ a real number such that $H(P) \leq B$ for all $P \in \mathcal{A}$.*

Let J be a finite set of maximal ideals of $\mathcal{O}_k$. For every $\mathfrak{p} \in J$, let $g_\mathfrak{p} \geq 1$ be a real number such that the reduction of $\mathcal{A}$ in $\mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ has cardinality at most $g_\mathfrak{p}$. Then

$$|\mathcal{A}| \leq \frac{\displaystyle\sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) - [k:\mathbb{Q}]\log(2B^2)}{\displaystyle\sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} - [k:\mathbb{Q}]\log(2B^2)}$$

provided the denominator is positive.

Remark 3.2. One can use Theorem 3.1 to sieve points on arbitrary quasi-projective varieties V over k. First choose an embedding $V \hookrightarrow \mathbb{P}^n_k$ (so V is open in a Zariski closed subvariety of $\mathbb{P}^n_k$) and then give V the corresponding height. Note that the bound in Theorem 3.1 makes no direct reference to the dimension n.

The main arithmetic input of the sieve is the following easy lemma. It says that if two distinct points P and Q in $\mathbb{P}^n(k)$ have the same reduction modulo several primes, then one of them must have large height. We will write $P \equiv Q \bmod \mathfrak{p}$ if the reduction of P and Q in $\mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ agree.

Lemma 3.3. *Let P and Q be distinct elements of $\mathbb{P}^n(k)$. Then*

$$\sum_{\substack{\mathfrak{p}\in\Sigma_k \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p}) \le [k:\mathbb{Q}] \log\big(2H(P)H(Q)\big).$$

Proof. Choose coordinates $a_i, b_j \in k$ such that $P = [a_0, \dots, a_n]$ and $Q = [b_0, \dots, b_n]$. Now fix a prime ideal $\mathfrak{p} \in \Sigma_k$ such that $P \equiv Q \bmod \mathfrak{p}$. We claim that:

$$1 \le \min_{i\neq j} \operatorname{ord}_{\mathfrak{p}}(a_ib_j - a_jb_i) - \min_i \operatorname{ord}_{\mathfrak{p}}(a_i) - \min_i \operatorname{ord}_{\mathfrak{p}}(b_i). \tag{3.1}$$

Note that the right hand side of (3.1) does not depend on the initial choice of coordinates. So without loss of generality, we may assume that $\min_i \operatorname{ord}_{\mathfrak{p}}(a_i) = \min_i \operatorname{ord}_{\mathfrak{p}}(b_i) = 0$. Under this assumption, $P \equiv Q \bmod \mathfrak{p}$ is equivalent to $\min_{i\neq j} \operatorname{ord}_{\mathfrak{p}}(a_ib_j - a_jb_i) \ge 1$, and the claim follows.

By (3.1), we have

$$\begin{aligned}\sum_{\substack{\mathfrak{p}\in\Sigma_k \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p}) \le \sum_{\mathfrak{p}\in\Sigma_k} \min_{i\neq j} \operatorname{ord}_{\mathfrak{p}}(a_ib_j - a_jb_i) \log N(\mathfrak{p}) - \sum_{\mathfrak{p}\in\Sigma_k} \min_i \operatorname{ord}_{\mathfrak{p}}(a_i) \log N(\mathfrak{p}) \\ - \sum_{\mathfrak{p}\in\Sigma_k} \min_i \operatorname{ord}_{\mathfrak{p}}(b_i) \log N(\mathfrak{p}).\end{aligned} \tag{3.2}$$

Let Σ_k^∞ be the set of archimedean places of k. For each $v \in \Sigma_k^\infty$, let $|\cdot|_v$ be the extension of the usual absolute value on $\mathbb{R}$ to the completion k_v. Rewriting (3.2) in terms of heights gives

$$\begin{aligned}\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{\mathfrak{p}\in\Sigma_k \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p}) \le \log H(P) + \log H(Q) - \log H([a_ib_j - a_jb_i]) \\ + \sum_{v\in\Sigma_k^\infty} \frac{[k_v:\mathbb{R}]}{[k:\mathbb{Q}]} \log\Big(\frac{\max_{i\neq j} |a_ib_j - a_jb_i|_v}{\max_i |a_i|_v \cdot \max_i |b_i|_v}\Big).\end{aligned}$$

Using $H \ge 1$ and the triangle inequality, we have

$$\begin{aligned}\frac{1}{[k:\mathbb{Q}]} \sum_{\mathfrak{p}\in\Sigma_k,\, P\equiv Q \bmod \mathfrak{p}} \log N(\mathfrak{p}) &\le \log H(P) + \log H(Q) + \sum\nolimits_{v\in\Sigma_k^\infty} \frac{[k_v:\mathbb{R}]}{[k:\mathbb{Q}]} \log 2 \\ &= \log H(P) + \log H(Q) + \log 2.\end{aligned}$$

□

Proof of Theorem 3.1. Fix a prime ideal $\mathfrak{p} \in J$. For each $c \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p})$, let $Z(c, \mathfrak{p})$ be the number of elements in $\mathcal{A}$ whose reduction in $\mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ is equal to c. By the Cauchy-Schwartz inequality and our assumption on the cardinality of $\mathcal{A}$ modulo $\mathfrak{p}$, we have the following inequality:

$$\begin{aligned}\frac{|\mathcal{A}|^2}{g_\mathfrak{p}} = \frac{1}{g_\mathfrak{p}}\Big(\sum_{c\in\mathbb{P}^n(\mathbb{F}_\mathfrak{p})} Z(c,\mathfrak{p})\Big)^2 \le \frac{1}{g_\mathfrak{p}}\Big(g_\mathfrak{p} \sum_{c\in\mathbb{P}^n(\mathbb{F}_\mathfrak{p})} Z(c,\mathfrak{p})^2\Big) \\ = \sum_{\substack{P,Q\in\mathcal{A} \\ P\equiv Q \bmod \mathfrak{p}}} 1 = |\mathcal{A}| + \sum_{\substack{P,Q\in\mathcal{A},\, P\neq Q \\ P\equiv Q \bmod \mathfrak{p}}} 1.\end{aligned}$$

Multiplying by $\log N(\mathfrak{p})$ and summing over all $\mathfrak{p} \in J$ gives the following:

$$\begin{aligned}|\mathcal{A}|^2 \sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} &\le \sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) \Big(|\mathcal{A}| + \sum_{\substack{P,Q\in\mathcal{A},\, P\neq Q \\ P\equiv Q \bmod \mathfrak{p}}} 1\Big) \\ &= |\mathcal{A}| \sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) + \sum_{P,Q\in\mathcal{A},\, P\neq Q} \Big(\sum_{\substack{\mathfrak{p}\in J \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p})\Big).\end{aligned}$$

By Lemma 3.3, we have

$$|\mathcal{A}|^2 \sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} \le |\mathcal{A}| \sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) + \sum_{P,Q\in\mathcal{A},\, P\neq Q} [k:\mathbb{Q}] \log(2H(P)H(Q))$$

and by our choice of B,

$$|\mathcal{A}|^2 \sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_{\mathfrak{p}}} \le |\mathcal{A}| \sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) + (|\mathcal{A}|^2 - |\mathcal{A}|)[k:\mathbb{Q}]\log(2B^2).$$

After cancelling both sides by $|\mathcal{A}|$ (the theorem is trivial if $|\mathcal{A}| = 0$), the theorem is immediate. □

3.2. **The larger sieve for integral points.**

Theorem 3.4 (Larger sieve for $\mathcal{O}_k^n$)**.** *Let k be number field. Let $\mathcal{A}$ be a finite subset of $\mathcal{O}_k^n$ and $B > 0$ a real number such that $\|P - Q\| \le B$ for all $P, Q \in \mathcal{A}$.*

Let J be a finite set of maximal ideals of $\mathcal{O}_k$. For every $\mathfrak{p} \in J$, let $g_{\mathfrak{p}} \ge 1$ be a real number such that the reduction of $\mathcal{A}$ in $\mathbb{F}_{\mathfrak{p}}^n$ has cardinality at most $g_{\mathfrak{p}}$. Then

$$|\mathcal{A}| \le \frac{\displaystyle\sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) - [k:\mathbb{Q}]\log B}{\displaystyle\sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_{\mathfrak{p}}} - [k:\mathbb{Q}]\log B}$$

provided the denominator is positive.

Lemma 3.5. *Let P and Q be distinct elements of $\mathcal{O}_k^n$. Then*

$$\sum_{\substack{\mathfrak{p}\in\Sigma_k \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p}) \le [k:\mathbb{Q}] \log \|P - Q\|.$$

Proof. If $\mathfrak{p} \in \Sigma_k$ is a prime ideal such that $P \equiv Q \bmod \mathfrak{p}$, then

$$\min_i \operatorname{ord}_{\mathfrak{p}}(a_i - b_i) \ge 1$$

where $P = (a_1, \dots, a_n)$ and $Q = (b_1, \dots, b_n)$. Therefore, we have

$$\begin{aligned}
\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{\mathfrak{p}\in\Sigma_k \\ P\equiv Q \bmod \mathfrak{p}}} \log N(\mathfrak{p}) &\le \frac{1}{[k:\mathbb{Q}]} \sum_{\mathfrak{p}\in\Sigma_k} \min_i \operatorname{ord}_{\mathfrak{p}}(a_i - b_i) \log N(\mathfrak{p}) \\
&= \sum_{v\in\Sigma_k^\infty} \frac{[k_v:\mathbb{R}]}{[k:\mathbb{Q}]} \log\big(\max_i |a_i - b_i|_v\big) - \log H([P-Q]) \\
&\le \sum_{v\in\Sigma_k^\infty} \frac{[k_v:\mathbb{R}]}{[k:\mathbb{Q}]} \log\|P - Q\| - \log H([P-Q]) \\
&= \log\|P - Q\| - \log H([P-Q])
\end{aligned}$$

where $[P-Q]$ is the image of $P-Q$ in $\mathbb{P}^{n-1}(k)$. We obtain the desired inequality by noting that $H([P-Q]) \ge 1$. □

Proof of Theorem 3.4. The proof is identical to that of Theorem 3.1, the main difference being that we use Lemma 3.5 in place of Lemma 3.3. □

3.3. **Interlude: orbits modulo $\mathfrak{p}$.** In this section (which is independent of the rest of the paper), we consider a problem of arithmetic dynamics studied by Silverman [Sil08], and then by Akbary and Ghioca [AG09]. This quick application of our larger sieve gives a good illustration of how Theorem 3.4 can be used to sieve points on general quasi-projective varieties. It is also significantly easier that our main application (Theorem 2.1) which requires a more elaborate proof.

Let V be a quasi-projective variety defined over a number field k. Fix a morphism $\varphi\colon V \to V$ and a point $P \in V(k)$. Suppose that the forward φ-orbit

$$\mathcal{O}_\varphi(P) := \{P, \varphi(P), \varphi^2(P), \varphi^3(P), \dots\}$$

is infinite. Choose a model of V and φ over the ring of integers of k. Then for all but finitely many non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, we can (by abuse of notation) consider the reduction

$$\varphi_{\mathfrak{p}} \colon V(\mathbb{F}_{\mathfrak{p}}) \to V(\mathbb{F}_{\mathfrak{p}})$$

and the reduction $P_{\mathfrak{p}} \in V(\mathbb{F}_{\mathfrak{p}})$ of the point P. We define $m_{\mathfrak{p}}(\varphi, P)$ to be the cardinality of the forward $\varphi_{\mathfrak{p}}$-orbit

$$\mathcal{O}_{\varphi_{\mathfrak{p}}}(P_{\mathfrak{p}}) := \{P_{\mathfrak{p}}, \varphi_{\mathfrak{p}}(P_{\mathfrak{p}}), \varphi_{\mathfrak{p}}^2(P_{\mathfrak{p}}), \dots\}.$$

For the finite number of excluded primes, we simply define $m_{\mathfrak{p}}(\varphi, P) = +\infty$. The choice of model for V and φ is not important for our applications since a different choice would change only finitely many of the values $m_{\mathfrak{p}}(\varphi, P)$.

Since V is quasi-projective, we may choose an embedding $V \subseteq \mathbb{P}^n_k$ defined over k (so V is open in a closed subvariety of $\mathbb{P}^n_k$). Using this embedding, we equip V with the height H of $\mathbb{P}^n_k$; it will be convenient to work with the *logarithmic height* on $\mathbb{P}^n_k$, i.e., $h = \log \circ H$. By [Sil08, Proposition 4], there are numbers $d > 1$ and $c \geq 0$ such that $h(\varphi^i(P)) \leq d^i(h(P) + c)$ holds for all integers $i \geq 0$.

Theorem 3.6. *For any $\varepsilon < 1/\log d$, the set*

$$\left\{\mathfrak{p} \in \Sigma_K : m_{\mathfrak{p}}(\varphi, P) \geq \varepsilon \log N(\mathfrak{p})\right\}$$

has natural density 1.

In [AG09], Akbary and Ghioca define the *degree* $\deg(\varphi)$ of the morphism φ. If $\deg(\varphi) > 1$, then we can choose $d = \deg(\varphi)$ above. Theorem 3.6 is then the same as Theorem 1.1(i) of [AG09]. If $\deg(\varphi) = 1$, then [AG09] gives a stronger bound which also follows from the larger sieve.

This theorem is a slight improvement over [Sil08, Theorem 3], where it is shown that for each $\lambda < 1$, the set $\{\mathfrak{p} : m_{\mathfrak{p}}(\varphi, P) \geq (\log N(\mathfrak{p}))^{\lambda}\}$ has analytic density 1. The bound $m_{\mathfrak{p}}(\varphi, P) \geq \varepsilon \log N(\mathfrak{p})$ is likely far from optimal. In fact, one expects to be able to replace $\log N(\mathfrak{p})$ by an appropriate power of $N(\mathfrak{p})$ (see [Sil08, §6] for details).

Proof of Theorem 3.6. Since $\varepsilon < 1/\log d$, we can choose constants $0 < \alpha < 1$ and $C > 1$ such that $(1 + C^{-1})\varepsilon < \alpha/\log d$. Define the function $g(x) := \varepsilon \log x$ and the set

$$\mathscr{S}(x) := \{\mathfrak{p} : N(\mathfrak{p}) \leq x,\ m_{\mathfrak{p}}(\varphi, P) \leq g(x)\}.$$

It suffices to show that $|\mathscr{S}(x)| = o(x/\log x)$ as $x \to +\infty$.

Define the set

$$\mathcal{A}(x) = \{Q \in \mathcal{O}_{\varphi}(P) : h(Q) \leq x^{\alpha}\}.$$

The number of $i \geq 0$ that satisfy $d^i(h(P) + c) \leq x^{\alpha}$ is $\frac{\alpha}{\log d}\log x + O(1)$, so using this and the assumption $|\mathcal{O}_{\varphi}(P)| = \infty$ we have

$$|\mathcal{A}(x)| \geq \frac{\alpha}{\log d}\log x + O(1).$$

We now find an upper bound for $|\mathcal{A}(x)|$ using the larger sieve. For each $\mathfrak{p} \in \mathscr{S}(x)$, the reduction of $\mathcal{A}(x)$ modulo $\mathfrak{p}$ lies in $\mathcal{O}_{\varphi_{\mathfrak{p}}}(P_{\mathfrak{p}})$ which has cardinality at most $g(x)$. Define $L := \sum_{\mathfrak{p} \in \mathscr{S}(x)} \log N(\mathfrak{p})$ and $\mathcal{B} := [k : \mathbb{Q}] \log\left(2(e^{x^{\alpha}})^2\right) = [k : \mathbb{Q}](2x^{\alpha} + \log 2)$. Assume that $L - g(x) \geq Cg(x)\mathcal{B}$ holds. Then by Theorem 3.1, we have

$$|\mathcal{A}(x)| \leq \frac{L - \mathcal{B}}{L/g(x) - \mathcal{B}} = g(x) + \frac{g(x)^2\mathcal{B} - g(x)\mathcal{B}}{L - g(x)\mathcal{B}}$$

(from our assumption, we have $L/g(X) - \mathcal{B} \geq (C - 1)\mathcal{B} + 1 > 0$). Therefore,

$$|\mathcal{A}(x)| \leq g(x) + \frac{g(x)^2\mathcal{B} - g(x)\mathcal{B}}{L - g(x)\mathcal{B}} \leq g(x) + \frac{g(x)^2\mathcal{B} - g(x)\mathcal{B}}{Cg(x)\mathcal{B}} = (1 + C^{-1})g(x) + O(1).$$

and so $|\mathcal{A}(x)| \leq (1 + C^{-1})\varepsilon \log x + O(1)$.

Since $(1 + C^{-1})\varepsilon < \alpha/\log d$, our lower and upper bounds for $|\mathcal{A}(x)|$ are contradictory for all sufficiently large x. Therefore, we must have $L - g(x) \leq Cg(x)\mathcal{B}$. Thus

$$\sum_{\mathfrak{p} \in \mathscr{S}(x)} \log N(\mathfrak{p}) \leq C\varepsilon[k : \mathbb{Q}](\log x)(2x^{\alpha} + \log 2) + \varepsilon \log x \ll x^{\alpha} \log x.$$

Using partial summation, this implies that $|\mathscr{S}(x)| \ll x^{\alpha}$. In particular, $|\mathscr{S}(x)| = o(x/\log x)$. □

4. Special case of larger sieve

In this section we deduce some bounds from our larger sieve. We will of course apply them later to obtain bounds for Hilbert's Irreducibility Theorem, but to simplify the exposition we will keep this application separate.

Proposition 4.1. *Let k be a number field and let S a finite subset of Σ_k.*

(i) (Rational points) *Let $\mathcal{A}$ a subset of $\mathbb{P}^n(k)$ such that $H(P) \leq B$ for all $P \in \mathcal{A}$. Suppose that for each $\mathfrak{p} \in \Sigma_k - S$, the cardinality of the image of $\mathcal{A}$ under the reduction map $\mathbb{P}^n(k) \to \mathbb{P}^n(\mathbb{F}_{\mathfrak{p}})$ is at most $g_{\mathfrak{p}}$ where*

$$g_{\mathfrak{p}} \leq \delta\big(N(\mathfrak{p}) + DN(\mathfrak{p})^{1/2}\big)$$

for some constants $0 < \delta \leq 1$ and $D \geq 1$. Then

$$|\mathcal{A}| \ll_k D^2 \exp\left(\sum_{\mathfrak{p} \in S \text{ with } \deg(\mathfrak{p})=1 \text{ and } N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) B^{2[k:\mathbb{Q}]\delta}.$$

(ii) (Integral points) *Let $\mathcal{A}$ a subset of $\mathcal{O}_k^n$ such that $\|P - Q\| \leq B$ for all $P, Q \in \mathcal{A}$. Suppose that for each $\mathfrak{p} \in \Sigma_k - S$, the cardinality of the image of $\mathcal{A}$ under the reduction map $\mathcal{O}_k^n \to \mathbb{F}_{\mathfrak{p}}^n$ is at most $g_{\mathfrak{p}}$ where*

$$g_{\mathfrak{p}} \leq \delta\big(N(\mathfrak{p}) + DN(\mathfrak{p})^{1/2}\big)$$

for some constants $0 < \delta \leq 1$ and $D \geq 1$. Then

$$|\mathcal{A}| \ll_k D^2 \exp\left(\sum_{\mathfrak{p} \in S \text{ with } \deg(\mathfrak{p})=1 \text{ and } N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) B^{[k:\mathbb{Q}]\delta}.$$

Remark 4.2.

(i) The condition on $g_{\mathfrak{p}}$ is quite common when $n = 1$ where it implies that the proportion of elements of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ (or $\mathbb{A}^1(\mathbb{F}_{\mathfrak{p}})$) that belong to $\mathcal{A}$ mod $\mathfrak{p}$ is at most δ.

(ii) In Corollary 19 and 20 of [EEHK09], there are similiar results under the much stronger hypothesis that $g_{\mathfrak{p}} \leq CN(\mathfrak{p})^{\alpha}$ where $C > 0$ and $0 \leq \alpha < 1$ are constants (they state it only for subset $\mathcal{A}$ of $\mathbb{P}^1(k)$ but everything easily generalizes to our setting). They use this stronger hypothesis to obtains explicit bounds for $|\mathcal{A}|$ that are polynomial in $\log B$.

4.1. Analytic bounds.

Lemma 4.3. *For a number field k and a real number $x \geq 1$,*

$$\sum_{\mathfrak{p} \in \Sigma_k,\, N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \log x + O_k(1) \quad \text{and} \quad \sum_{\mathfrak{p} \in \Sigma_k,\, N(\mathfrak{p}) \geq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{3/2}} \ll_k \frac{1}{x^{1/2}}.$$

Proof. By partial summation ([Mur08, Theorem 2.1.1]), we have

$$\sum_{\mathfrak{p} \in \Sigma_k,\, N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \frac{\psi_k(x)}{x} + \int_2^x \frac{\psi_k(t)}{t^2} dt$$

where $\psi_k(x) = \sum_{\mathfrak{p} \in \Sigma_k,\, N(\mathfrak{p}) \leq x} \log N(\mathfrak{p})$. By the prime number theorem (with a worked out error term), we have $\psi_k(x) = x + O_k\big(x/(\log x)^A\big)$ for some constant $A > 1$. Therefore,

$$\sum_{\mathfrak{p} \in \Sigma_k,\, N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = O_k(1) + \int_2^x \frac{dt}{t} + O_k\Big(\int_2^x \frac{dt}{t(\log t)^A}\Big) = \log x + O_k(1).$$

The second expression is proven in a similiar fashion. □

Lemma 4.4. *Let k be a number field and fix a constant $D \geq 1$. Then*

$$\sum_{D^2 \leq N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p}) + DN(\mathfrak{p})^{1/2}} \geq \log(x) - \log(D^2) - \alpha_k$$

where $\alpha_k \geq 0$ is a constant depending only on k.

Proof. For each prime $\mathfrak{p} \in \Sigma_k$, we have

$$\frac{\log N(\mathfrak{p})}{N(p) + DN(\mathfrak{p})^{1/2}} = \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \frac{1}{1 + D/N(\mathfrak{p})^{1/2}} \geq \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \left(1 - \frac{D}{N(\mathfrak{p})^{1/2}}\right).$$

So by summing over all $\mathfrak{p}$ with $D^2 \leq N(\mathfrak{p}) \leq x$ and using Lemma 4.3, we obtain

$$\begin{aligned}\sum_{D^2 \leq N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(p) + DN(\mathfrak{p})^{1/2}} &\geq \sum_{D^2 \leq N(\mathfrak{p}) \leq x} \frac{\log N(\mathfrak{p})}{N(p)} - D \sum_{N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(p)^{3/2}} \\ &= (\log x - \log(D^2) + O_k(1)) + D \cdot O_k(1/(D^2)^{1/2}) \\ &= \log x - \log(D^2) + O_k(1).\end{aligned}$$

□

Lemma 4.5. *Let k be a number field and S a finite subset of Σ_k. For each $\mathfrak{p} \in \Sigma_k - S$, fix a positive integer $g_\mathfrak{p}$ such that*

$$g_\mathfrak{p} \leq \delta\big(N(\mathfrak{p}) + DN(\mathfrak{p})^{1/2}\big)$$

where $0 < \delta \leq 1$ and $D \geq 1$ are constants. Let $B \geq 1$ be any real number.

By setting

$$x := \beta_k D^2 \exp\left(\sum_{\mathfrak{p} \in S,\, N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) e^\delta B^{[k:\mathbb{Q}]\delta}$$

where $\beta_k \geq 1$ is a certain constant depending only on k, we obtain the bound

$$\frac{\displaystyle\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ D^2 \leq N(\mathfrak{p}) \leq x}} \log N(\mathfrak{p}) - [k:\mathbb{Q}] \log B}{\displaystyle\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ D^2 \leq N(\mathfrak{p}) \leq x}} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} - [k:\mathbb{Q}] \log B} \ll_k D^2 \exp\left(\sum_{\mathfrak{p} \in S,\, N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) B^{[k:\mathbb{Q}]\delta} \tag{4.1}$$

and the denominator of (4.1) is positive.

Proof. Using the given bound on $g_\mathfrak{p}$ and Lemma 4.4 we have:

$$\begin{aligned}\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ D^2 \leq N(\mathfrak{p}) \leq x}} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} &\geq \delta^{-1}\left(\sum_{\substack{\mathfrak{p} \in \Sigma_k \\ D^2 \leq N(\mathfrak{p}) \leq x}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p}) + DN(\mathfrak{p})^{1/2}} - \sum_{\mathfrak{p} \in S,\, N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) \\ &\geq \delta^{-1}\Big(\log(x) - \log(D^2) - \alpha_k - \sum_{\mathfrak{p} \in S,\, N(\mathfrak{p}) \geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\Big). \qquad (4.2)\end{aligned}$$

Define $\beta_k := e^{\alpha_k}$. With our choice of x we find that the expression (4.2) is equal to $1 + [k:\mathbb{Q}] \log B$, and thus

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ D^2 \leq N(\mathfrak{p}) \leq x}} \frac{\log N(\mathfrak{p})}{g_\mathfrak{p}} - [k:\mathbb{Q}] \log B \geq 1.$$

So the denominator (and hence also the numerator) of the expression in (4.1) is at least 1. Thus the left hand side of (4.1) is bounded by $\sum_{N(\mathfrak{p}) \leq x} \log N(\mathfrak{p}) \ll_k x$. The lemma follows by once again using our specific choice of x. □

4.2. **Proof of Proposition 4.1.** We first consider part (i). Let J be the set of $\mathfrak{p} \in \Sigma_k - S$ such that $D^2 \leq N(\mathfrak{p}) \leq x$, where x is a real number to be chosen later. By the larger sieve (Theorem 3.1), we have the bound

$$|\mathcal{A}| \leq \frac{\sum_{\mathfrak{p}\in J} \log N(\mathfrak{p}) - [k:\mathbb{Q}]\log(2B^2)}{\sum_{\mathfrak{p}\in J} \frac{\log N(\mathfrak{p})}{g_{\mathfrak{p}}} - [k:\mathbb{Q}]\log(2B^2)} \tag{4.3}$$

provided the denominator is positive.

Choosing x as in Lemma 4.5 (with B replaced by $2B^2$), we find the that denominator is in fact positive. Moreover, Lemma 4.5 now tells us that $|\mathcal{A}| \ll_k D^2 \exp\left(\sum_{\mathfrak{p}\in S,\, N(\mathfrak{p})\geq D^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\right) B^{2[k:\mathbb{Q}]\delta}$. Finally, we need only restrict to those $\mathfrak{p} \in S$ with $\deg(\mathfrak{p}) = 1$ since $\sum_{\mathfrak{p}\in\Sigma_k,\, \deg(\mathfrak{p})\geq 2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \ll_k 1$.

Part (ii) is proven in a similiar manner; the main difference being that we use Theorem 3.4 instead of Theorem 3.1.

5. Equidistribution

In this section, we consider the equidistribution of Frobenius conjugacy classes coming from curves (and in particular lines) over finite fields. In §5.1, we recall bounds resulting from the Grothendieck-Lefschetz trace formula and Deligne's completion of the Weil conjectures. We will later apply these results to projective spaces by first fibering by many rational lines; it will thus be vital that our bounds are uniform.

5.1. **Chebotarev for curves over finite fields.** Let X be a smooth, projective, geometrically integral curve of genus g defined over a finite field $\mathbb{F}_q$ with q elements. Let U be a non-empty open affine subvariety of X. For each $u \in U(\mathbb{F}_q)$, the homomorphism $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \xrightarrow{u_*} \pi_1(U)$ is determined by the value it takes on the q-th power Frobenius automorphism Frob_q of $\overline{\mathbb{F}}_q$; this gives a conjugacy class Frob_u of $\pi_1(U)$.

Fix a finite group G and a surjective continuous homomorphism

$$\rho\colon \pi_1(U) \to G.$$

Let G^g denote the image of the geometric fundamental group $\pi_1(U_{\overline{\mathbb{F}}_q})$ under ρ. We then have a natural exact sequence

$$1 \to G^g \to G \xrightarrow{\varphi} \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) =: \Gamma \to 1.$$

where $\varphi(\rho(\mathrm{Frob}_u)) = \{\mathrm{Frob}_q\}$ for all $u \in U(\mathbb{F}_q)$. Assume further that the corresponding representation $\pi_1(U_{\overline{\mathbb{F}}_q}) \to G$ is *tamely ramified* at all the points of $(X-U)(\overline{\mathbb{F}}_q)$.

Proposition 5.1. *With notation as above, let C be a subset of $\varphi^{-1}(\mathrm{Frob}_q)$ that is stable under conjugation by G. Then*

$$\left|\,|\{u \in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u) \subseteq C\}| - \frac{|C|}{|G^g|}|U(\mathbb{F}_q)|\right| \leq |C|^{1/2}(1-|G^g|^{-1})^{1/2}(2g-2+\#(X-U)(\overline{\mathbb{F}}_q))q^{1/2}.$$

Proof. (Sketch) We follow the outline of Kowalski in [Kow06, Theorem 1] adding more details concerning the bounds where appropriate. Let $M = \#(X-U)(\overline{\mathbb{F}}_q)$.

Fix a prime ℓ that does not divide q. Let $\widehat{G}$ and $\widehat{\Gamma}$ be the set of $\overline{\mathbb{Q}}_\ell$-valued irreducible characters of G and Γ, respectively (i.e., those coming from finite dimensional linear representations over $\overline{\mathbb{Q}}_\ell$). Composition by φ induces an injective $\widehat{\Gamma} \hookrightarrow \widehat{G}$ which we will sometimes view as an inclusion. Let $\delta_C\colon G \to \{0,1\}$ be the characteristic function of C, which we may write in the form

$$\delta_C(g) = \sum_{\chi\in\widehat{G}} c_\chi \chi(g)$$

where $c_\chi := \frac{1}{|G|}\sum_{g\in C}\overline{\chi(g)}$. The quantity we are trying to estimate then becomes

$$|\{u \in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u) \subseteq C\}| = \sum_{u\in U(\mathbb{F}_q)} \delta_C(\rho(\mathrm{Frob}_u)) = \sum_{\chi\in\widehat{G}} c_\chi \sum_{u\in U(\mathbb{F}_q)} \chi(\rho(\mathrm{Frob}_u)).$$

We first consider the contribution coming from those χ that arise from a character of Γ. So

$$\sum_{\psi\in\widehat{\Gamma}} c_\psi \sum_{u\in U(\mathbb{F}_q)} \psi(\varphi(\rho(\mathrm{Frob}_u))) = \sum_{\psi\in\widehat{\Gamma}} \frac{1}{|G|} \sum_{g\in C} \overline{\psi(\varphi(g))} \sum_{u\in U(\mathbb{F}_q)} \psi(\varphi(\rho(\mathrm{Frob}_u)))$$
$$= \frac{1}{|G|} \sum_{g\in C} \sum_{u\in U(\mathbb{F}_q)} \sum_{\psi\in\widehat{\Gamma}} \overline{\psi(\mathrm{Frob}_q)}\psi(\mathrm{Frob}_q)$$

where the last line uses our assumption $\varphi(C) = \{\mathrm{Frob}_q\}$. Since all the characters of Γ are one dimensional, we have

$$\sum_{\psi\in\widehat{\Gamma}} c_\psi \sum_{u\in U(\mathbb{F}_q)} \psi(\varphi(\rho(\mathrm{Frob}_u))) = \frac{|\widehat{\Gamma}||C|}{|G|}|U(\mathbb{F}_q)| = \frac{|C|}{|G^g|}|U(\mathbb{F}_q)|;$$

this is the "main term" of our estimate. By the Cauchy-Schwarz inequality

$$\begin{aligned}(5.1)\qquad &\Big||\{u\in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u)\subseteq C\}| - \frac{|C|}{|G^g|}|U(\mathbb{F}_q)|\Big| \\ =&\Big|\sum_{\chi\in\widehat{G}-\widehat{\Gamma}} c_\chi \sum_{u\in U(\mathbb{F}_q)} \chi(\rho(\mathrm{Frob}_u))\Big| \\ \le&\Big(\sum_{\chi\in\widehat{G}} |c_\chi|^2\Big)^{1/2}\Big(\sum_{\chi\in\widehat{G}-\widehat{\Gamma}}\Big|\sum_{u\in U(\mathbb{F}_q)}\chi(\rho(\mathrm{Frob}_u))\Big|^2\Big)^{1/2} = \frac{|C|^{1/2}}{|G|^{1/2}}\Big(\sum_{\chi\in\widehat{G}-\widehat{\Gamma}}\Big|\sum_{u\in U(\mathbb{F}_q)}\chi(\rho(\mathrm{Frob}_u))\Big|^2\Big)^{1/2}.\end{aligned}$$

Now fix any character $\chi \in \widehat{G} - \widehat{\Gamma}$. Let $\mathscr{F}_\chi$ be a lisse $\overline{\mathbb{Q}}_\ell$-adic sheaf corresponding to the character $\chi\circ\rho\colon \pi_1(U)\to\overline{\mathbb{Q}}_\ell$. By the Grothendieck-Lefschetz trace formula, we have

$$\sum_{u\in U(\mathbb{F}_q)} \chi(\rho(\mathrm{Frob}_u)) = \sum_{i=0}^{2}(-1)^i \operatorname{Tr}(\mathrm{Fr}\,|H^i_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi))$$

where Fr is the geometric Frobenius automorphism. By Deligne's theorem, the eigenvalues of Fr acting on $H^i_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi)$ are algebraic integers with absolute values $\le q^{i/2}$ in $\mathbb{C}$ (under any embedding $\overline{\mathbb{Q}}_\ell\hookrightarrow\mathbb{C}$). So

$$\Big|\sum_{u\in U(\mathbb{F}_q)}\chi(\rho(\mathrm{Frob}_u))\Big| \le \sum_{i=0}^{2} q^{i/2}\dim H^i_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi).$$

The sheaf $\mathscr{F}_\chi$ comes from an irreducible representation of G for which G^g acts non-trivially (because $\chi\notin\widehat{\Gamma}$), so the coinvariants $(\mathscr{F}_\chi)_{\pi_1(U_{\overline{\mathbb{F}}_q})}$ are trivial. Therefore, $H^2_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi)=0$ since it is canonically isomorphic to $(\mathscr{F}_\chi)_{\pi_1(U_{\overline{\mathbb{F}}_q})}(-1)$. Since U is affine and smooth, we also have $H^0_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi)=0$. Therefore

$$\Big|\sum_{u\in U(\mathbb{F}_q)}\chi(\rho(\mathrm{Frob}_u))\Big| \le q^{1/2}\dim H^1_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi) = -q^{1/2}\chi_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi)$$

where $\chi_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi) := \sum_{i=0}^{2}(-1)^i\dim H^i_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi)$. By [Kat88, §2.3.1],

$$\chi_c(U_{\overline{\mathbb{F}}_q},\mathscr{F}_\chi) = \chi(1)\cdot\chi_c(U_{\overline{\mathbb{F}}_q},\overline{\mathbb{Q}}_\ell) = \chi(1)\big(2-2g+M\big)$$

(the Swan conductors that occur are all zero by our tameness assumption on ρ). Therefore

$$\Big|\sum_{u\in U(\mathbb{F}_q)}\chi(\rho(\mathrm{Frob}_u))\Big| \le \chi(1)\cdot q^{1/2}(2g-2+M).$$

(Note that there is no contradiction if $2g-2+M<0$. In these cases we have $\widehat{G}=\widehat{\Gamma}$.)

Returning to (5.1), we have

$$\Big|\big|\{u \in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u) \subseteq C\}\big| - \frac{|C|}{|G^g|}|U(\mathbb{F}_q)|\Big| \leq \frac{|C|^{1/2}}{|G|^{1/2}}\Big(\sum_{\chi \in \widehat{G}-\widehat{\Gamma}} \chi(1)^2\Big)^{1/2} q^{1/2}(2g-2+M)$$
$$= \frac{|C|^{1/2}}{|G|^{1/2}}(|G|-|\Gamma|)^{1/2} q^{1/2}(2g-2+M). \qquad \square$$

5.2. **Intersection with lines.** We shall use the same set-up as §2.2. Let k be a number field, and let U be a non-empty open subvariety of $\mathbb{P}^n_k$. Let $\mathcal{Z}$ be the Zariski closure of $\mathbb{P}^n_k - U$ in $\mathbb{P}^n_{\mathcal{O}_k}$ (where $\mathbb{P}^n_k$ is the generic fiber $\mathbb{P}^n_{\mathcal{O}_k}$). We define $\mathcal{U}$ to be the complement of $\mathcal{Z}$ in $\mathbb{P}^n_{\mathcal{O}_k}$, it is an open subscheme of $\mathbb{P}^n_{\mathcal{O}_k}$ with generic fiber U. Fix a continuous and surjective homomorphism

$$\rho\colon \pi_1(\mathcal{U}_{\mathcal{O}}) \to G$$

where G is a finite group and $\mathcal{O}$ is the ring of S-integers in k for a fixed finite set $S \subseteq \Sigma_k$. Let G^g be the image of $\pi_1(\mathcal{U}_{\bar{k}})$ under ρ, and let K be the minimal extension of k in $\bar{k}$ for which G^g is the image of $\pi_1(\mathcal{U}_K)$. We have a short exact sequence

$$1 \to G^g \to G \xrightarrow{\varphi} \mathrm{Gal}(K/k) \to 1.$$

For all $\mathfrak{p} \in \Sigma_k - S$ and $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, we have $\varphi(\rho(\mathrm{Frob}_u)) \in (\mathfrak{p}, K/k)$.

Let $\mathbf{Gr}/\mathcal{O}_k$ be the Grassmannian scheme $\mathrm{Grass}(1,n)$ over $\mathcal{O}_k$. For any field extension k' of k, $\mathbf{Gr}_{k'}$ is the familiar variety which parametrizes the linear 1-dimension subvarieties (i.e., lines) of $\mathbb{P}^n_{k'}$. Let W be the closed subvariety of $\mathbf{Gr}_k$ such that for every algebraically closed extension k'/k and line $L \in \mathbf{Gr}(k')$, we have $L \notin W(k')$ if and only if L intersects $\mathcal{Z}_{k'}$ only at smooth points of $\mathcal{Z}_{k'}$, and transversally at each of these points. Our interest in the variety W is due to the following lemma.

Lemma 5.2. *For all lines $L \in (\mathbf{Gr}_k - W)(\bar{k})$, the homomorphism*

$$\pi_1(U_{\bar{k}} \cap L) \to \pi_1(U_{\bar{k}}) \xrightarrow{\rho} G$$

has image G^g.

Proof. Choosing an embedding $\bar{k} \hookrightarrow \mathbb{C}$, it suffices to prove the lemma for an arbitrary line $L \in (\mathbf{Gr}_k - W)(\mathbb{C})$ (the image of $\pi_1(U_\mathbb{C})$ under ρ is still G^g). The lemma is true for a generic line by Bertini's theorem, so the result follows by (topologically) deforming L to a generic element in $(\mathbf{Gr}_k - W)(\mathbb{C})$. $\square$

Let $\mathcal{W}$ be the Zariski closure of W in $\mathbf{Gr}$. We now prove an equidistribution theorem for lines L in $\mathbb{P}^n_{\mathbb{F}_\mathfrak{p}}$ that do not lie in $\mathcal{W}(\mathbb{F}_p)$. It will allow us to reduce our Hilbert irreducibility bounds to the one dimensional setting.

Theorem 5.3. *Let C be a subset of G that is stable under conjugation such that $\kappa := \varphi(C)$ is a conjugacy class of $\mathrm{Gal}(K/k)$. Take any prime $\mathfrak{p} \in \Sigma_k - S$ for which $\mathfrak{p} \nmid |G^g|$ and $(\mathfrak{p}, K/k) = \kappa$, and any line $L \in (\mathbf{Gr}_{\mathbb{F}_\mathfrak{p}} - \mathcal{W}_{\mathbb{F}_\mathfrak{p}})(\mathbb{F}_\mathfrak{p})$. Then*

$$|\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \cap L(\mathbb{F}_\mathfrak{p}) : \rho(\mathrm{Frob}_u) \subseteq C\}| = \frac{1}{|\kappa|}\frac{|C|}{|G^g|}N(\mathfrak{p}) + O_U\left(\frac{|C|^{1/2}}{|\kappa|^{1/2}}N(\mathfrak{p})^{1/2}\right).$$

Proof. We first introduce some standard notation. Let $k_\mathfrak{p}$ be the completion of k at the prime $\mathfrak{p}$. Let $\mathcal{O}^{\mathrm{un}}_\mathfrak{p}$ be the ring of integers in the maximal unramified extension of $k^{\mathrm{un}}_\mathfrak{p}$ of $k_\mathfrak{p}$ (in a fixed algebraic closure $\bar{k}_\mathfrak{p}$). The ring $\mathcal{O}^{\mathrm{un}}_\mathfrak{p}$ is a complete discrete valuation ring with residue field $\overline{\mathbb{F}}_\mathfrak{p}$.

By excluding a finite number of $\mathfrak{p} \in \Sigma_k - S$ (that depend only on $\mathcal{U} \subseteq \mathbb{P}^n_{\mathcal{O}_k}$, and hence only on $U \subseteq \mathbb{P}^n_k$), we can assume that each line $L \in (\mathbf{Gr} - \mathcal{W})(\mathbb{F}_\mathfrak{p})$ lifts to a line $\mathcal{L} \in (\mathbf{Gr} - \mathcal{W})(\mathcal{O}_\mathfrak{p})$ by Hensel's lemma.

Let $\mathcal{D}$ be the scheme theoretic intersection of $\mathcal{L}$ and $\mathcal{Z}_{\mathcal{O}_\mathfrak{p}}$. It is a horizontal divisor of $\mathcal{L}$ which is étale over $\mathrm{Spec}\,\mathcal{O}_\mathfrak{p}$. Let $\mathcal{V}$ be the $\mathcal{O}_\mathfrak{p}$-scheme $\mathcal{L} - \mathcal{D}$. Choose a point $a_0 \in \mathcal{V}(\overline{\mathbb{F}}_\mathfrak{p})$ with a lift $a_1 \in \mathcal{V}(\mathcal{O}^{\mathrm{un}}_\mathfrak{p})$. By the Grothendieck specialization theorem, the natural homomorphisms

$$\pi_1(\mathcal{V}_{k^{un}_\mathfrak{p}}, a_1) \to \pi_1(\mathcal{V}_{\mathcal{O}^{\mathrm{un}}_\mathfrak{p}}, a_1) \leftarrow \pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0)$$

induce an isomorphism between the prime to $p = \operatorname{char} \mathbb{F}_\mathfrak{p}$ quotients of $\pi_1(\mathcal{V}_{\bar{k}}, a_1) \xrightarrow{\sim} \pi_1(\mathcal{V}_{\bar{k}_\mathfrak{p}}, a_1)$ and $\pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0)$. In the present setting, an accessible proof of Grothendieck's theorem can be found in [Wew99, §4]. Therefore the homomorphism

$$\pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0) \to \pi_1(\mathcal{V}_{\mathcal{O}^{\mathrm{un}}_\mathfrak{p}}, a_1) \to \pi_1(\mathcal{U}, a_1) \xrightarrow{\rho} G$$

has the same image as $\pi_1(\mathcal{V}_{\bar{k}_\mathfrak{p}}, a_1) \to \pi_1(\mathcal{V}_{\mathcal{O}^{\mathrm{un}}_\mathfrak{p}}, a_1) \to \pi_1(\mathcal{U}, a_1) \xrightarrow{\rho} G$, which by Lemma 5.2 is G^g (the assumption that $\mathfrak{p} \nmid |G^g|$ is needed here).

Let $\rho_\mathfrak{p}$ be the representation $\pi_1(\mathcal{V}_{\mathbb{F}_\mathfrak{p}}, a_0) \to \pi_1(\mathcal{U}, a_1) \xrightarrow{\rho} G$, and denote its image by $G_\mathfrak{p}$. We have just shown that $\rho_\mathfrak{p}(\pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0)) = G^g$. Let d be the index $[G_\mathfrak{p} : G^g]$ and let $\mathbb{F}$ be the degree d extension of $\mathbb{F}_\mathfrak{p}$. We have a short exact sequence

$$1 \to G^g \to G_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} \operatorname{Gal}(\mathbb{F}/\mathbb{F}_\mathfrak{p}) \to 1.$$

Define the set $C' = C \cap G_\mathfrak{p}$, which is stable under conjugation in $G_\mathfrak{p}$. For $u \in \mathcal{V}(\mathbb{F}_\mathfrak{p}) \subseteq \mathcal{U}(\mathbb{F}_\mathfrak{p})$, we have $\rho(\mathrm{Frob}_u) \subseteq C$ if and only if $\rho_\mathfrak{p}(\mathrm{Frob}_u) \subseteq C'$. Hence

$$|\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \cap L(\mathbb{F}_\mathfrak{p}) : \rho(\mathrm{Frob}_u) \subseteq C\}| = |\{u \in \mathcal{V}_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p}) : \rho_\mathfrak{p}(\mathrm{Frob}_u) \subseteq C'\}|.$$

Our assumption that $\varphi(C) = \kappa$ and $(\mathfrak{p}, K/k) = \kappa$ implies that the set $\varphi_\mathfrak{p}(C')$ consists of just the $N(\mathfrak{p})$-th power Frobenius automorphism. Therefore by Proposition 5.1

$$\left||\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \cap L(\mathbb{F}_\mathfrak{p}) : \rho(\mathrm{Frob}_u) \subseteq C\}| - \frac{|C'|}{|G^g|}|\mathcal{U}(\mathbb{F}_\mathfrak{p})|\right| \leq |C'|^{1/2}(1 - |G^g|^{-1})^{1/2}(2 \cdot 0 - 2 + |\mathcal{D}(\overline{\mathbb{F}}_\mathfrak{p})|)N(\mathfrak{p})^{1/2},$$

where we have used that geometrically $\rho_\mathfrak{p}$ is at worst tamely ramified (since $\mathfrak{p} \nmid |G^g|$).

Since $D \to \operatorname{Spec} \mathcal{O}_\mathfrak{p}$ is étale and $\mathcal{L}_{\bar{k}} \notin W(\bar{k})$, we have $|D(\overline{\mathbb{F}}_\mathfrak{p})| = |D(\bar{k})| \ll_U 1$. So

$$\begin{aligned}&\left||\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \cap L(\mathbb{F}_\mathfrak{p}) : \rho(\mathrm{Frob}_u) \subseteq C\}| - \frac{|C'|}{|G^g_\mathfrak{p}|}|\mathcal{U}(\mathbb{F}_\mathfrak{p})|\right| \\ \leq &|C'|^{1/2}(1 - |G^g_\mathfrak{p}|^{-1})^{1/2}(-2 + |D(\bar{k})|)N(\mathfrak{p})^{1/2} \ll_U |C'|^{1/2}N(\mathfrak{p})^{1/2}.\end{aligned}$$

The theorem follows by noting that $|C'| = |C|/|\kappa|$. □

For a line $\mathcal{L} \notin W(k)$, we can consider its reduction $\mathcal{L}_{\mathbb{F}_\mathfrak{p}}$ in $\mathbf{Gr}(\mathbb{F}_\mathfrak{p})$ for primes $\mathfrak{p} \in \Sigma_k$. To apply Theorem 5.3 we need that $\mathcal{L}_{\mathbb{F}_\mathfrak{p}}$ does not lie in $\mathcal{W}_{\mathbb{F}_\mathfrak{p}}$. The follow lemma controls the number of primes that have this property (this will be important later when we vary the line $\mathcal{L}$). Choose an embedding $\mathbf{Gr}_k \hookrightarrow \mathbb{P}^N_k$ (for example, the Plücker embedding with $N = \binom{n+1}{2}$), and let H be a height on $\mathbf{Gr}_k$ coming from the height on $\mathbb{P}^N_k$.

Lemma 5.4. *For any line $\mathcal{L} \in \mathbf{Gr}(k) - W(k)$,*

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ \mathcal{L}_{\mathbb{F}_\mathfrak{p}} \in \mathcal{W}(\mathbb{F}_\mathfrak{p})}} \log N(\mathfrak{p}) \ll_U \log H(\mathcal{L}) + O(1)$$

where the implied constant depends only on $U \subseteq \mathbb{P}^n_k$ (and in particular not on $\mathcal{L}$).

Proof. Fix a non-constant morphism $\phi\colon \mathbf{Gr}_k \to \mathbb{P}^1_k$ for which $\phi^{-1}([0:1]) \supseteq W$. By choosing a model of ϕ over $\mathcal{O}_k$, we will have morphisms $\mathbf{Gr}_{\mathbb{F}_\mathfrak{p}} \to \mathbb{P}^1_{\mathbb{F}_\mathfrak{p}}$ of special fibers such that $\mathcal{W}_{\mathbb{F}_\mathfrak{p}}$ lies in the fibre above $[0:1]$ for most $\mathfrak{p}$. Therefore

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ \mathcal{L}_{\mathbb{F}_\mathfrak{p}} \in \mathcal{W}(\mathbb{F}_\mathfrak{p})}} \log N(\mathfrak{p}) \leq \sum_{\substack{\mathfrak{p} \in \Sigma_k - S \\ \phi(\mathcal{L}) \bmod \mathfrak{p} = [0:1] \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})}} \log N(\mathfrak{p}) + O(1) \ll_k \log H(\phi(\mathcal{L})) + O(1)$$

by Lemma 3.3. Finally, note that $\log H(\phi(\mathcal{L})) \ll_\phi \log H(\mathcal{L}) + O(1)$ (cf. [Ser97, §2.6]). □

6. Proof of Theorem 2.1

6.1. **Proof of Theorem 2.1(i).** Fix notation as in §2.2 and §5.2. Without loss of generality, we may assume that $\mathcal{U}$ is an open subscheme of $\mathbb{A}^n_{\mathcal{O}_k} = \operatorname{Spec} \mathcal{O}_k[x_1, \dots, x_n]$ where we view $\mathbb{A}^n_{\mathcal{O}_k}$ as an open subscheme of $\mathbb{P}^n_{\mathcal{O}_k}$ via the map $(x_1, \dots, x_n) \mapsto [x_1, \dots, x_n, 1]$. Let

$$\mathcal{L} \colon \mathbb{A}^{n-1}_k \to \mathbf{Gr}_k, \quad b \mapsto \mathcal{L}_b$$

be the morphism for which $\mathcal{L}_b$ is the line defined by $x_1 = b_1, \dots, x_{n-1} = b_{n-1}$ for $b = (b_1, \dots, b_{n-1})$. Without loss of generality, we may assume that the image of the morphism $\mathcal{L}$ does not lie in $W \subsetneq \mathbf{Gr}_k$ (if not, then we can arrange this by an initial change of coordinates).

We then have a disjoint union

$$\{u \in \mathcal{U}(k) \cap \mathcal{O}_k^n : \|u\| \le B\} = \bigsqcup_{b \in \mathcal{O}_k^{n-1},\, \|b\| \le B} \{(b_1, \dots, b_{n-1}, a) \in \mathcal{L}_b \cap \mathcal{U}(k) : a \in \mathcal{O}_k,\, \|a\| \le B\}.$$

We first consider those b for which $\mathcal{L}_b \in W(k)$. Since W does not lie in the image of $\mathcal{L} \colon \mathbb{A}^{n-1}_k \to \mathbf{Gr}_k$, we find that $\mathcal{L}^{-1}(W)$ is a closed subvariety of $\mathbb{A}^{n-1}_k$ of codimension ≥ 1. So using trivial bounds for each of these lines, we have

$$\begin{aligned} &\sum_{\substack{b \in \mathcal{O}_k^{n-1},\, \|b\| \le B \\ \mathcal{L}_b \in W(k)}} |\{u = (b_1, \dots, b_{n-1}, a) \in \mathcal{L}_b \cap \mathcal{U}(k) : a \in \mathcal{O}_k,\, \|a\| \le B,\, G_u \subseteq C\}| \\ &\ll_k B^{[k:\mathbb{Q}]} \cdot |\{b \in \mathcal{O}_k^{n-1} : \|b\| \le B,\, \mathcal{L}_b \in W(k)\}| \ll_U B^{[k:\mathbb{Q}]} \cdot B^{[k:\mathbb{Q}](n-2)} = B^{[k:\mathbb{Q}](n-1)}. \end{aligned}$$

This gives:

$$\begin{aligned} &|\{u \in \mathcal{U}(k) \cap \mathcal{O}_k^n : \|u\| \le B,\, G_u \subseteq C\}| + O_U(B^{[k:\mathbb{Q}](n-1)}) \\ &= \sum_{\substack{b \in \mathcal{O}_k^{n-1},\, \|b\| \le B \\ \mathcal{L}_b \notin W(k)}} |\{(b_1, \dots, b_{n-1}, a) \in \mathcal{L}_b \cap \mathcal{U}(k) : a \in \mathcal{O}_k,\, \|a\| \le B,\, G_u \subseteq C\}| \\ &\ll_U B^{[k:\mathbb{Q}](n-1)} \max_{\substack{b \in \mathcal{O}_k^{n-1},\, \|b\| \le B \\ \mathcal{L}_b \notin W(k)}} |\{u = (b_1, \dots, b_{n-1}, a) \in \mathcal{L}_b \cap \mathcal{U}(k) : a \in \mathcal{O}_k,\, \|a\| \le B,\, G_u \subseteq C\}|. \end{aligned} \tag{6.1}$$

Now fix any $b \in \mathcal{O}_k^{n-1}$ with $\|b\| \le B$ for which $\mathcal{L}_b \notin W(k)$. Let $\mathcal{A}$ be the set of $u = (b_1, \dots, b_{n-1}, a) \in \mathcal{U}(k)$ with $a \in \mathcal{O}_k$ for which $\|a\| \le B$ and $G_u \subseteq C$. We will show that

$$|\mathcal{A}| \ll_U |G^g|^2 \exp\Bigg(\sum_{\substack{\mathfrak{p} \in S \text{ with } \deg(\mathfrak{p}) = 1 \\ \text{and } N(\mathfrak{p}) \ge |G^g|^2}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \Bigg) B^{[k:\mathbb{Q}]\delta} \log B. \tag{6.2}$$

Applying this to (6.1) then gives

$$|\{u \in \mathcal{U}(k) \cap \mathcal{O}_k^n : \|u\| \le B,\, G_u \subseteq C\}| \ll_U |G^g|^2 \exp\Bigg(\sum_{\substack{\mathfrak{p} \in S \text{ with } \deg(\mathfrak{p}) = 1 \\ \text{and } N(\mathfrak{p}) \ge |G^g|^2}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \Bigg) B^{[k:\mathbb{Q}](n-1+\delta)} \log B.$$

which will complete the proof of Theorem 2.1(i).

With our fixed b, we will now prove (6.2). Let T be the finite set of primes $\mathfrak{p} \in \Sigma_k$ for which either $\mathfrak{p}$ divides $|G^g|$ or for which $\mathcal{L}_b \bmod \mathfrak{p} \in \mathcal{W}(\mathbb{F}_\mathfrak{p})$. Take any $\mathfrak{p} \in \Sigma_k - (S \cup T)$, and let $g_\mathfrak{p}$ be the cardinality of the image of $\mathcal{A}$ under the reduction modulo $\mathfrak{p}$ map $\mathcal{O}_k^n \mapsto \mathbb{F}_\mathfrak{p}^n$. Let κ be the conjugacy class $(\mathfrak{p}, K/k)$ of

$\mathrm{Gal}(K/k)$. By Theorem 5.3,

$$g_{\mathfrak{p}} \le \frac{1}{|\kappa|}\frac{|C_\kappa|}{|G^g|}N(\mathfrak{p}) + O_U\Big(\frac{|C_\kappa|^{1/2}}{|\kappa|^{1/2}}N(\mathfrak{p})^{1/2}\Big) \le \frac{1}{|\kappa|}\frac{|C_\kappa|}{|G^g|}\Big(N(\mathfrak{p}) + O_U\Big(\frac{|\kappa|^{1/2}}{|C_\kappa|^{1/2}}|G^g|N(\mathfrak{p})^{1/2}\Big)\Big)$$
$$\le \delta\Big(N(\mathfrak{p}) + c_0|G^g|N(\mathfrak{p})^{1/2}\Big)$$

where $c_0 \ge 1$ is a constant depending only on $U \subseteq \mathbb{P}^n_k$. By Proposition 4.1 (ii), we have the bound

$$|\mathcal{A}| \ll_U |G^g|^2 \exp\Bigg(\sum_{\mathfrak{p}\in S\cup T \text{ with } \deg(\mathfrak{p})=1 \text{ and } N(\mathfrak{p})\ge|G^g|^2} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\Bigg) B^{[k:\mathbb{Q}]\delta}. \tag{6.3}$$

If $\mathfrak{p}$ divides $|G^g|$, then $\deg(\mathfrak{p}) = 1$ and $N(\mathfrak{p}) \ge |G^g|^2$ cannot both hold; thus these primes do not contribute to (6.3).

For any non-empty finite set $R \subseteq \Sigma_k$, we have $\exp\big(\sum_{\mathfrak{p}\in R}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\big) \ll_k \sum_{\mathfrak{p}\in R}\log N(\mathfrak{p})$ [MRS96, Corollary 2.3]. This and Lemma 5.4 give us

$$\exp\Bigg(\sum_{\substack{\mathfrak{p}\in\Sigma_k - S,\ \mathcal{L}_b \bmod \mathfrak{p}\in\mathcal{W}(\mathbb{F}_\mathfrak{p})\\ N(\mathfrak{p})\ge|G^g|^2}}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\Bigg) \ll_k \sum_{\substack{\mathfrak{p}\in\Sigma_k - S\\ \mathcal{L}_b \bmod \mathfrak{p}\in\mathcal{W}(\mathbb{F}_\mathfrak{p})}} \log N(\mathfrak{p}) + O(1) \ll_U \log H(\mathcal{L}_b) + O(1).$$

Observe that $\log H(\mathcal{L}_b) \ll_{\mathcal{L}} \log H(b) + O(1) \ll_k \log B$ (cf. [Ser97, §2.6]). Combining these additional bounds with (6.3) gives the desired bound (6.2).

6.2. **Proof of Theorem 2.1(ii).** We will reduce to the integral points case using the following proposition (see [Ser97, §13.4]).

Proposition 6.1. *Let k be a number field and n a positive integer. There is a constant $c_0 = c_0(k,n)$ such that every point $x \in \mathbb{P}^n(k)$ is representable by coordinates $a = (a_0,\dots,a_n) \in \mathcal{O}_k^{n+1}$ with*

$$\|a\| \le c_0 H(x).$$

Let $f\colon \mathbb{A}^{n+1}_k \setminus \{(0,\dots,0)\} \to \mathbb{P}^n_k$ be the morphism $(x_0,\dots,x_n) \mapsto [x_0,\dots,x_n]$. Without loss of generality, we may assume that U lies in the image of f. Let U' be the inverse image of U under f; it is a non-empty open subscheme of $\mathbb{A}^{n+1}_k$. Define the representation

$$\rho'\colon \pi_1(U') \to \pi_1(U) \xrightarrow{\rho} G$$

where the first homomorphism arises from f. For each $u' \in U'(k)$, we have a representation $\mathrm{Gal}(\bar{k}/k) \xrightarrow{u'_*} \pi_1(U') \to G$ whose image we denote by $G_{u'}$. For $u' \in U'(k)$, the groups $G_{u'}$ and G_u are conjugate in G where $u = f(u') \in U(k)$. By Proposition 6.1,

$$|\{u \in U(k) : H(u) \le B,\ G_u \subseteq C\}| \le |\{u' \in U'(k) \cap \mathcal{O}_k^{n+1} : \|u'\| \le c_0 B,\ G_{u'} \subseteq C\}|.$$

By Theorem 2.1(i), which was proved in the previous section, this is $O_U(c(c_0B)^{[k:\mathbb{Q}](n+\delta)}\log(c_0B))$ and hence also $O_U(cB^{[k:\mathbb{Q}](n+\delta)}\log B)$.

7. Elliptic curves

7.1. **Set up.** Fix a number field k. Let $\pi\colon E \to U$ be an elliptic curve where U is a non-empty open subvariety of $\mathbb{P}^n_k$ (recall this means that π is a proper smooth morphism whose fibers are geometrically connected curves of genus 1, together with a section $\mathcal{O}$ of π). For each point $u \in U(k)$, the fiber of π over u is an elliptic curve E_u over k. Let η be the generic point of U; the generic fiber E_η is an elliptic curve over the function field $k(U)$.

Fix a geometric generic point $\bar{\eta}$ of U (equivalently, fix an algebraic closure $\overline{k(U)}$ of $k(U)$). For each positive integer m, let $E[m]$ be the m-torsion subscheme of E. The morphism $E[m] \to U$ is finite étale and as a lisse sheaf corresponds to a $(\mathbb{Z}/m\mathbb{Z})$-representation of $\pi_1(U,\bar{\eta})$ on the geometric generic fiber $E[m]_{\bar{\eta}} = E_{\bar{\eta}}[m]$. We thus have a continuous homomorphism

$$\rho_{E,m}\colon \pi_1(U,\bar{\eta}) \to \mathrm{Aut}(E[m]_{\bar{\eta}}) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

which is uniquely defined up to an inner automorphism. Let $\mathcal{H}_E(m)$ be the image under $\rho_{E,m}$ of $\pi_1(U,\overline{\eta})$. Combining all our representations together, we obtain a single continuous homomorphism

$$\rho_E\colon \pi_1(U,\overline{\eta}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Let $\mathcal{H}_E$ be the image under ρ_E of the groups $\pi_1(U,\overline{\eta})$.

There is a unique morphism $j\colon U \to \mathbb{A}^1_k$ such that $j(u)$ is the j-invariant of E_u for all $u \in U(k)$. Assume that $E \to U$ is *non-isotrivial*; i.e., $j\colon U \to \mathbb{A}^1_k$ is non-constant (equivalently, the j-invariant of E_η does not belong to k).

In §1.3, we started with an elliptic curve over $k(T_1,\dots,T_n)$, which to avoid confusion we will call $\tilde{E}$. Choosing a specific model, we described a closed subvariety Z of $\mathbb{A}^n_k := \operatorname{Spec} k[T_1,\dots,T_n]$ (whose k-points we denoted by Ω) such that specializing our model at any k-point t of $U := \mathbb{A}^n_k - Z$ gave an elliptic curve. This describes an elliptic curve E over U whose generic fiber is the original $\tilde{E}$. Theorems 1.14 and 1.15 are thus equivalent to:

Theorem 7.1. *Fix notation as above.*

(i) *If $k \neq \mathbb{Q}$, then*

$$\frac{|\{u \in U(k) : H(u) \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E\}|}{|\{u \in U(k) : H(u) \le B\}|} = 1 + O\big(B^{-1/2}\log B\big) \quad \textit{and}$$
$$\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}|} = 1 + O\big(B^{-1/2}\log B\big).$$

(ii) *If $k = \mathbb{Q}$, then for any $\varepsilon > 0$ we have*

$$\frac{\big|\big\{t \in U(\mathbb{Q}) : H(t) \le B,\ \big[\mathcal{H}_E : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\big] = r\big\}\big|}{|\{t \in \mathbb{Q}^n : H(t) \le B\}|} = 1 + O(B^{-1/2+\varepsilon}) \quad \textit{and}$$
$$\frac{\big|\big\{t \in U(\mathbb{Q}) \cap \mathbb{Z}^n : \|t\| \le B,\ \big[\mathcal{H}_E : \rho_{E_t}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))\big] = r\big\}\big|}{|\{t \in \mathbb{Z}^n : \|t\| \le B\}|} = 1 + O(B^{-1/2+\varepsilon})$$

where r is the index of $[\mathcal{H}_E,\mathcal{H}_E]$ in $\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

The implicit constants depend on $E \to U$ and k, and also ε in (ii).

We claim that it suffices to prove parts (i) and (ii) of Theorem 7.1 only in the integral points case; we explain for part (i) only. As in §6.2, we define a morphism $f\colon \mathbb{A}^{n+1}_k \to \mathbb{P}^n_k$ by $(x_0,\dots,x_n) \mapsto [x_0,\dots,x_n]$. Without loss of generality, we may assume that U lies in the image of f. Let U' be the inverse image of U under f; it is a non-empty open subvariety of $\mathbb{A}^{n+1}_k$. Base extension gives an elliptic curve $E' := E \times_U U' \to U'$. Composing the homomorphism $\pi_1(U') \to \pi_1(U)$ coming from f with the representation $\rho_E\colon \pi_1(U) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ gives $\rho_{E'}\colon \pi_1(U') \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ (at least up to conjugation since we are suppressed base points everywhere). For each $u' \in U'(k)$, the curves $E'_{u'}$ and $E_{f(u')}$ are isomorphic and $\rho_{E'_{u'}}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_{E'}$ if and only if $\rho_{E_{f(u')}}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E$. Proposition 6.1 implies that

$$\begin{aligned}&|\{u \in U(k) : H(u) \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k)) \neq \mathcal{H}_E\}|\\ \le&|\{u' \in U'(k) \cap \mathcal{O}_k^{n+1} : \|u'\| \le c_0 B,\ \rho_{E_{u'}}(\mathrm{Gal}(\bar{k}/k)) \neq \mathcal{H}_{E'}\}|\end{aligned}$$

and the integral case of Theorem 7.1(i) then says that this is $O(B^{[k:\mathbb{Q}](n+1)} \cdot B^{-1/2}\log B)$ as required.

For the rest of §7, we shall thus focus on the integral points setting. We will assume that U is an open subvariety of $\mathbb{A}^n_k$.

7.2. **Surjectivity modulo primes.** We first consider the Galois actions on the m-torsion points for a fixed m. The following is an explicit form of HIT in this context; it is of the utmost importance for our application that the implicit constants in part (ii) do not depend on $m = \ell$.

Proposition 7.2.

(i) *For any positive integer m, we have*

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,m}(\mathrm{Gal}(\bar{k}/k)) \ne \mathcal{H}_E(m)\}| \ll_{E,m} B^{[k:\mathbb{Q}](n-1/2)} \log B.$$

(ii) *For every prime $\ell \ge 17$, we have*

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}| \ll_E \ell^6 B^{[k:\mathbb{Q}](n-1/2+O(1/\ell))} \log B$$

where the implicit constants do not depend on ℓ or B.

Before proving the proposition, we state the following criterion for a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ to contain $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Lemma 7.3. *Let $\ell \ge 5$ be a prime.*

- *Let $C_1(\ell)$ be the set of $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for which $\mathrm{tr}(A)^2 - 4\det(A)$ is a non-zero square in $\mathbb{F}_\ell$, and such that $\mathrm{tr}(A) \ne 0$.*
- *Let $C_2(\ell)$ be the set of $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for which $\mathrm{tr}(A)^2 - 4\det(A)$ is not a square in $\mathbb{F}_\ell$, and such that $\mathrm{tr}(A) \ne 0$.*
- *Let $C_3(\ell)$ be the set of $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $u = \mathrm{tr}(A)^2/\det(A)$ is not $0, 1, 2$ or 4, and such that $u^2 - 3u + 1 \ne 0$.*

(i) *If G is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that contains elements from all three of the sets $C_1(\ell)$, $C_2(\ell)$ and $C_3(\ell)$, then G contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

(ii) *For each $d \in \mathbb{F}_\ell^\times$, we have*

$$\frac{|\{A \in C_i(\ell) : \det(A) = d\}|}{|\mathrm{SL}_2(\mathbb{F}_\ell)|} = \begin{cases} \frac{1}{2} + O(1/\ell) & \text{for } i = 1, 2, \\ 1 + O(1/\ell) & \text{for } i = 3. \end{cases}$$

Proof. Part (i) is Proposition 19 of [Ser72]. We now consider part (ii) with a fixed $d \in \mathbb{F}_\ell^\times$. For each $t \in \mathbb{F}_\ell$, [CFM05, Lemma 2.7] shows that

$$|\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(A) = d,\ \mathrm{tr}(A) = t\}| = \ell^2 + \epsilon\ell \quad \text{where } \epsilon = \left(\frac{t^2 - 4d}{\ell}\right) \in \{-1, 0, 1\}.$$

Hence for each $c \in \mathbb{F}_\ell$,

$$|\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(A) = d,\ \mathrm{tr}(A)^2/d = c\}| \le 2\ell(\ell+1).$$

This implies the bound for $C_3(\ell)$ and taking $c = 4$ shows that we need only prove the bound for $C_1(\ell)$ or $C_2(\ell)$. We have

$$\begin{aligned} |\{A \in C_1(\ell) : \det(A) = d\}| &= \ell^2 |\{t \in \mathbb{F}_\ell : t^2 - 4d \text{ is a square in } \mathbb{F}_\ell\}| + O(\ell^2) \\ &= \frac{1}{2}\ell^2 \cdot |\{(t, y) \in \mathbb{F}_\ell^2 : t^2 - y^2 = 4d\}| + O(\ell^2). \end{aligned}$$

Since $d \ne 0$ and ℓ is odd, the plane curve $t^2 - y^2 = 4d$ in $\mathbb{A}^2_{\mathbb{F}_\ell} = \mathrm{Spec}\,\mathbb{F}_\ell[t, y]$ is isomorphic to $\mathbb{P}^1_{\mathbb{F}_\ell}$ with two $\mathbb{F}_\ell$-rational points removed. Therefore, $|\{A \in C_1(\ell) : \det(A) = d\}| = \frac{1}{2}\ell^2(\ell - 1) + O(\ell^2) = \frac{1}{2}\ell^3 + O(\ell^2)$. □

Proof of Proposition 7.2. (i) This follows from the large sieve bounds in Theorem 1.2.
(ii) We first extend the elliptic curve $\pi\colon E \to U$ to an integral model. There is a finite set $S \subseteq \Sigma_k$, an open subscheme $\mathcal{U}$ of $\mathbb{A}^n_{\mathcal{O}}$ over the ring $\mathcal{O}$ of S-integers, and an elliptic curve $\mathcal{E} \to \mathcal{U}$ such that the generic fibers of $\mathcal{E}$ and $\mathcal{U}$ are E and U, respectively, and $\pi\colon E \to U$ is the morphism on generic fibers of $\mathcal{E} \to \mathcal{U}$.

Now fix a prime $\ell \ge 17$. The representation $\rho_{E,\ell}\colon \pi_1(U) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ factors through a Galois representation

$$\pi_1(\mathcal{U}_{\mathcal{O}_\ell}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

where $\mathcal{O}_\ell$ is the ring of S_ℓ-integers with $S_\ell := S \cup \{\mathfrak{p} \in \Sigma_k : \mathfrak{p}|\ell\}$; note that the torsion subscheme $\mathcal{E}_{\mathcal{O}_\ell}[\ell] \to \mathcal{U}_{\mathcal{O}_\ell}$ is finite étale.

Let $\mathcal{H}_E^g(\ell)$ denote the image under $\rho_{E,\ell}$ of $\pi_1(U_{\bar{k}}, \bar{\eta})$, and assume that $\mathcal{H}_E^g(\ell) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Let $C_1(\ell)$, $C_2(\ell)$ and $C_3(\ell)$ be the sets defined in Lemma 7.3. By Lemma 7.3(i), we have

$$\begin{aligned}&|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}| \\ &\le \sum_{i=1}^{3} |\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) - C_i(\ell)\}|.\end{aligned}$$

By Theorem 2.1,

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}| \ll_U c B^{[k:\mathbb{Q}](n-1+\delta)} \log B$$

where

$$c := |\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|^2 \exp\Bigg(\sum_{\substack{\mathfrak{p} \in S \text{ or } \mathfrak{p} \mid \ell \\ \deg(\mathfrak{p})=1 \text{ and } N(\mathfrak{p}) \ge |\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|^2}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} \Bigg)$$

and

$$\delta := \max_{\substack{i=1,2,3 \\ d \in \det(\mathcal{H}_E(\ell))}} \frac{|\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) - C_i(\ell) : \det(A) = d\}|}{|\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

We obtain the desired bound by noting that $\delta = \frac{1}{2} + O(1/\ell)$ from Lemma 7.3(ii) and that c is less than $\ell^6 \exp\big(\sum_{\mathfrak{p} \in S} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})}\big) \ll_S \ell^6$.

It thus remains to show that $\mathcal{H}_E^g(\ell) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for every prime $\ell \ge 17$. After choosing an embedding $\bar{k} \hookrightarrow \mathbb{C}$, we have $\mathcal{H}_E^g(\ell) = \rho_{E,\ell}(\pi_1(U_{\mathbb{C}}))$. Let $X(\ell)$ be the modular curve over $\mathbb{C}$ which classifies elliptic curves with a basis for the ℓ-torsion. There is a natural action of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ on $X(\ell)$ and the quotient gives a morphism $X(\ell) \to X(1)$ where $X(1) \cong \mathbb{P}^1_{\mathbb{C}}$ is the j-line. Now consider the quotient curve $X_E := X(\ell)/\mathcal{H}_E^g(\ell)$ and the natural morphism $f\colon X_E \to X(1)$. There is a morphism $h\colon U_{\mathbb{C}} \to X_E$ such that the j-invariant of E_u is $f(h(u))$ for all $u \in U(\mathbb{C})$. The morphism $f \circ h$, and hence h, is non-constant by our ongoing assumption that the j-invariant of E is non-constant. Since $U_{\mathbb{C}}$ is open in $\mathbb{P}^n_{\mathbb{C}}$ and h is dominant, we deduce that X_E has genus 0. For $\ell \ge 17$, there are no proper subgroups H of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for which $X(\ell)/H$ has genus 0 (it suffices to compute the genus of $X(\ell)/H$ for the for maximal subgroups H of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, see [CH05, Table 2.1]). □

The following effective version of Serre's open image theorem, due to Masser and Wüstholz, allows us to effectively bound the primes ℓ that have to be considered.

Theorem 7.4 (Masser-Wüstholz [MW93])**.** *There are absolute constants $c > 0$ and $\gamma \ge 0$ with the following properties. Suppose E is an elliptic curve of Weil height*[1] *h defined over a number field k of degree d, and assume E has no complex multiplication over $\bar{k}$. If $\ell > c(\max\{d, h\})^\gamma$, then $\rho_{E,\ell}(\mathrm{Gal}(\bar{k}/k)) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

Combining Masser and Wüstholz's theorem with our explicit HIT bounds gives the following proposition.

Proposition 7.5. *For every $\varepsilon > 0$, we have*

$$\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ for all } \ell \ge 17\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}|} = 1 + O_{E,\varepsilon}\Big(\frac{1}{B^{[k:\mathbb{Q}]/2-\varepsilon}}\Big).$$

Proof. Recall that there is a morphism $j_E\colon U \to \mathbb{A}^1_k$ such that for each $u \in U(k)$, the j-invariant of E_u is $j_E(u)$. Now take any $u \in U(k) \cap \mathcal{O}_k^n$ with $\|u\| \le B$. We have

$$\log H(j(E_u)) = \log H(j_E(u)) \ll \log H(u) \ll \log \|u\| \le \log B$$

where the implicit constants do not depend on $u \in U(k) \cap \mathcal{O}_k^n$. So by Theorem 7.4 if E_u is non-CM, then $\rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \ge C(\log B)^\gamma$ where $\gamma \ge 0$ is an absolute constant and C is a constant that depends on E and k. Therefore,

$$\begin{aligned}&|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some } \ell \ge 17\}| \\ &\le \sum_{17 \le \ell \le C(\log B)^\gamma} |\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}|\end{aligned}$$

[1] i.e., the absolute logarithmic height of the j-invariant of E

(note that if E_u has complex multiplication then $\rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq 17$). By Theorem 7.2,

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\ \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some } \ell \geq 17\}| \ll_{E,\varepsilon} \sum_{17 \leq \ell \leq C(\log B)^\gamma} \ell^6 B^{[k:\mathbb{Q}](n-1/2+\varepsilon)} \log B. \tag{7.1}$$

We have used part (ii) of Theorem 7.2 for all sufficiently large ℓ (how large depends on ε but not on B) and Theorem 7.2(i) is used for the finitely many excluded primes. So (7.1) is $O(B^{[k:\mathbb{Q}](n-1/2+\varepsilon)}(\log B)^{6\gamma+1})$, and the proposition follows from (1.1) and a readjustment of ε. □

The following group theoretic lemma justifies our focus on the Galois images arising from ℓ-torsion. We will apply it later with $\mathcal{H}$ equal to $[\mathcal{H}_E, \mathcal{H}_E]$.

Lemma 7.6. *Let $\mathcal{H}$ be an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, and let G be a closed subgroup of $\mathcal{H}$. For each positive integer m, let $\mathcal{H}(m)$ and $G(m)$ be the images under the reduction modulo m map $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ of $\mathcal{H}$ and G, respectively. Then there exists a positive integer M (divisible only by those primes ℓ for which $\mathcal{H}(\ell) \neq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or $\ell \leq 5$) such that $G = \mathcal{H}$ if and only if $G(M) = \mathcal{H}(M)$ and $G(\ell) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \nmid M$.*

Proof. Let $\mathcal{H}_m$ and G_m be the image of $\mathcal{H}$ and G, respectively, in $\prod_{\ell|m} \mathrm{SL}_2(\mathbb{Z}_\ell)$.

Let M_0 be a positive integer divisible by 2, 3, 5 and by the primes for which $\mathcal{H}(\ell) \neq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The *Frattini subgroup* $\Phi(\mathcal{H}_{M_0})$ of $\mathcal{H}_{M_0}$ is the intersection of the maximal closed subgroups of $\mathcal{H}_{M_0}$. Since $\mathcal{H}$ is open in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, the group $\mathcal{H}_{M_0}$ contains a normal and open subgroup of the form $\prod_{\ell|M_0} \mathcal{S}_{\ell^{e(\ell)}}$ for some $e(\ell) \geq 1$, where $\mathcal{S}_{\ell^{e(\ell)}} := \{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{e(\ell)}}\}$. The groups $\{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{e(\ell)}}\}$ are pro-ℓ and are finitely generated as topological groups. Therefore by [Ser97, 10.6 Prop.], $\Phi(\mathcal{H}_{M_0})$ is an open normal subgroup of $\mathcal{H}_{M_0}$. Choose a positive integer M with the same prime divisors as M_0 such that $\Phi(\mathcal{H}_{M_0}) \supseteq \prod_{\ell^e \| M} \mathcal{S}_{\ell^e}$; this will be our desired M. Observe that if $G(M) = \mathcal{H}(M)$, then $G_M = \mathcal{H}_M$.

Consider a prime $\ell \nmid M_0$. By [Ser97, IV-23 Lemma 3], the assumption $G(\ell) = \mathcal{H}(\ell) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ implies that $G_\ell = \mathcal{H}_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$.

We may view G and $\mathcal{H}$ as subgroups of $\mathcal{H}_M \times \prod_{\ell \nmid M} \mathrm{SL}_2(\mathbb{Z}_\ell)$. We have seen that the projection of G onto the $\mathcal{H}_M$ and $\mathrm{SL}_2(\mathbb{Z}_\ell)$ factors is surjective. We now show that these factors have no common non-abelian simple groups in their composition series. For $\ell \nmid M$ (in particular $\ell \geq 5$), the only non-abelian simple group occurring in a composition series of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ is $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$. Also $\mathrm{SL}_2(\mathbb{Z}_\ell)$ with $\ell \geq 5$ has no non-trivial abelian quotients (cf. [Zyw10, Lemma A.1]). None of the groups $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$ ($\ell \nmid M$) occur in a composition series of $\mathcal{H}_M$ (this follows from the calculation of "Occ($\mathrm{SL}_2(\mathbb{Z}_\ell)$)" in [Ser98, IV-25]). Using Goursat's lemma, we deduce the equality $G = \mathcal{H}_M \times \prod_{\ell \nmid M} \mathrm{SL}_2(\mathbb{Z}_\ell)$ (for example, see [Zyw10, Lemma A.4] where it is stated only for finite groups but it immediately extends to profinite groups); since $\mathcal{H}$ lies between these two groups, we deduce that $G = \mathcal{H}$. □

7.3. **Abelian quotients and cyclotomic fields.** We now state a special version of HIT involving the cyclotomic extension of k. We will need this proposition in future work, so we also include a rational point version.

Proposition 7.7. *Let k be any number field* except $\mathbb{Q}$. *Fix a non-empty open subvariety U of $\mathbb{P}^n_k$ and a surjective continuous homomorphism $\rho\colon \pi_1(U) \to G$ where G is a finite abelian group. Let G^c be the image of $\pi_1(U_{k^{\mathrm{cyc}}})$ under ρ. For each $u \in U(k)$, let ρ_u be the composition $\mathrm{Gal}(\bar{k}/k) = \pi_1(\mathrm{Spec}\, k) \xrightarrow{u_*} \pi_1(U) \xrightarrow{\rho} G$. Then*

$$\frac{|\{u \in U(k) : H(u) \leq B,\ \rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = G^c\}|}{|\{u \in U(k) : H(u) \leq B\}|} = 1 + O\Big(\frac{\log B}{B^{1/2}}\Big).$$

Assume further that U is an open subvariety of $\mathbb{A}^n_k$. Then

$$\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\ \rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = G^c\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B\}|} = 1 + O\Big(\frac{\log B}{B^{1/2}}\Big).$$

The implicit constants do not depend on B.

Since $\mathbb{Q}^{\mathrm{cyc}}$ is the maximal abelian extension of $\mathbb{Q}$, Proposition 7.7 fails for $k = \mathbb{Q}$ and $G^c \neq 1$. The proof of the proposition is based on the following simple lemma. Since we are working with an abelian group G, the Frobenius conjugacy classes are actually well-defined elements.

Lemma 7.8. *Let p be a rational prime that splits completely in k and let L be a finite abelian extension of $\mathbb{Q}$ that is unramified at p. Choose any prime $\mathfrak{p}$ of $\mathcal{O}_k$ lying over p. Then the automorphism $(\mathfrak{p}, Lk/k) \in \mathrm{Gal}(Lk/k)$ does not depend on the choice of $\mathfrak{p}$ dividing p.*

Proof. Our assumptions assure that p is unramified in Lk. Restriction to L defines an injective homomorphism $\mathrm{Gal}(Lk/k) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q})$. We claim that $(\mathfrak{p}, Lk/k)|_L = (p, L/\mathbb{Q})$ from which the lemma would follow immediately. Define $\sigma := (\mathfrak{p}, Lk/k)$ and fix a prime $\mathfrak{P}$ of $\mathcal{O}_{Lk}$ lying over $\mathfrak{p}$. Then $\sigma(\mathfrak{P}) = \mathfrak{P}$ and σ induces the p-th power Frobenius automorphism on $\mathbb{F}_{\mathfrak{P}}$ (since $p = N(\mathfrak{p})$). The restriction $\sigma|_L$ stabilizes the prime $\mathfrak{p}' := \mathfrak{P} \cap \mathcal{O}_L$ of $\mathcal{O}_L$ and induces the p-th power Frobenius automorphism on $\mathbb{F}_{\mathfrak{p}'}$. Therefore, $\sigma|_L = (p, L/\mathbb{Q})$ as claimed. □

Proof of Proposition 7.7. A similar argument to that in §6.2 shows that the rational point version is a consequence of the integral point version, so we need only prove the second statement. Set $d = [k : \mathbb{Q}]$. As usual, define $G^g = \rho(\pi_1(U_{\bar{k}}))$. If $G^g = 1$, then the proposition is easy (ρ factors through $\mathrm{Gal}(\bar{k}/k)$ and equals ρ_u for each $u \in U(k)$). So we may assume that $G^g \neq 1$. Since $G^g \subseteq G^c$, this also implies that $G^c \neq 1$.

For a fixed $u \in U(k) \cap \mathcal{O}_k^n$, we certainly have $\rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) \subseteq G^c$. If this is not an equality, then $\widetilde{\rho}_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = 1$ where $\widetilde{\rho}$ is the representation $\pi_1(U) \xrightarrow{\rho} G \twoheadrightarrow G/H$ for some proper subgroup H of G^c. Thus by (1.1) it suffices to show that

$$|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\ \rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = 1\}| \ll B^{nd-1/2} \log B.$$

Define the set

$$\mathcal{A} = \{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\ \rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = 1\}$$

for a fixed real number $B \geq 2$. Choose an open subscheme $\mathcal{U}$ of $\mathbb{A}^n_{\mathcal{O}_k}$ with generic fiber U. Fix a finite set $S \subseteq \Sigma_k$ for which ρ factors through a homomorphism $\pi_1(\mathcal{U}_{\mathcal{O}}) \to G$, which we shall also denote by ρ, where $\mathcal{O}$ is the ring of S-integers in k.

There is a finite Galois extension $K/\mathbb{Q}$ such that $K \supseteq k$ and $\rho(\pi_1(U_K)) = G^g$. Fix a prime p that splits completely in K and is not divisible by any prime in S. Then for a prime $\mathfrak{p}$ of $\mathcal{O}_k$ dividing p and an element $C \in G^g$, we have

$$|\{u \in \mathcal{U}(\mathbb{F}_{\mathfrak{p}}) : \rho(\mathrm{Frob}_u) = C\}| = \frac{1}{|G^g|} N(\mathfrak{p})^n + O(N(\mathfrak{p})^{n-1/2}),$$

where the implicit constant depends on ρ and K (this follows from Deligne's theorem and the bounds in [Bom78]). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ be the primes of $\mathcal{O}_k$ dividing p. Define the sets

$$B_p = \Big\{(u_1, \ldots, u_d) \in \prod_{i=1}^d \mathcal{U}(\mathbb{F}_{\mathfrak{p}_i}) : \rho(\mathrm{Frob}_{u_i}) \in G^g \text{ is independent of } i\Big\}$$

and $C_p = \big(\prod_{i=1}^d \mathbb{F}^n_{\mathfrak{p}_i}\big) \setminus \big(\prod_{i=1}^d \mathcal{U}(\mathbb{F}_{\mathfrak{p}_i})\big)$. We then have $|C_p| = O(p^{dn-1})$ and

$$|B_p| = |G^g|\Big(\frac{1}{|G_g|} p^n + O(p^{n-1/2})\Big)^d = \frac{1}{|G^g|^{d-1}} p^{dn} + O(p^{dn-1/2})$$

(we have used that $N(\mathfrak{p}_i) = p$ since p splits completely in k). So using our assumption that $d > 1$ (i.e., $k \neq \mathbb{Q}$) and $G^g \neq 1$, we find that $|B_p \cup C_p| \leq \frac{1}{2} p^{dn} + O(p^{dn-1/2})$.

Take any $u \in \mathcal{A}$. The Chinese remainder theorem gives an isomorphism

$$\mathcal{O}_k^n / p\mathcal{O}_k^n = \prod_{i=1}^d (\mathcal{O}_k/\mathfrak{p}_i\mathcal{O}_k)^n = \prod_{i=1}^d \mathbb{F}^n_{\mathfrak{p}_i}, \tag{7.2}$$

so we may identify $u \pmod p$ with the tuple $(u_1, \ldots, u_d) \in \prod_{i=1}^d \mathbb{F}^n_{\mathfrak{p}_i}$. Suppose $u \pmod p$ does not belong to C_p, i.e., $u_i \in \mathcal{U}(\mathbb{F}_{\mathfrak{p}_i})$ for all i. Then ρ_u is unramified at each $\mathfrak{p}_i$ and $\rho_u(\mathrm{Frob}_{\mathfrak{p}_i}) = \rho(\mathrm{Frob}_{u_i})$. The

condition $\rho_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = 1$ implies that there is a finite cyclotomic extension $L/\mathbb{Q}$ unramified at p such that $\rho_u(\mathrm{Gal}(\bar{k}/Lk)) = 1$. By Lemma 7.8, we deduce that

$$\rho(\mathrm{Frob}_{u_i}) = \rho_u(\mathrm{Frob}_{\mathfrak{p}_i}) = \rho_u(\mathrm{Frob}_{\mathfrak{p}_j}) = \rho(\mathrm{Frob}_{u_j})$$

for all $i, j \in \{1, \dots, d\}$. So using the isomorphism (7.2), we find that image of $\mathcal{A}$ modulo p lies in $B_p \cup C_p$ and hence has cardinality at most $\frac{1}{2}p^{dn} + O(p^{dn-1/2})$.

We can now apply the large sieve to obtain a bound for $\mathcal{A}$. Using the large sieve as in [Ser97, 12.1] (with $K = \mathbb{Q}$, $\Lambda = \mathcal{O}_k^n$ with norm $\|\cdot\|$, and $Q = B^{1/2}$) gives the bound

$$|\mathcal{A}| \ll B^{nd}/L$$

where $L = \sum_{p \le B^{1/2},\, p \in \mathcal{P}} (1 + O(p^{-1/2}))$ and $\mathcal{P}$ is the set of primes p that are completely split in K and are not divisible by any primes in S. Since $\mathcal{P}$ has positive density, we have $L \gg B^{1/2}/\log(B^{1/2})$ for sufficiently large B. Therefore, $|\mathcal{A}| \ll B^{nd-1/2}\log B$. □

7.4. **Final steps.**

Proposition 7.9.

(i) *For any $\varepsilon > 0$,*

$$\frac{\big|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) = [\mathcal{H}_E, \mathcal{H}_E]\}\big|}{\big|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}\big|} = 1 + O_{E,\varepsilon}\Big(\frac{1}{B^{[k:\mathbb{Q}]/2-\varepsilon}}\Big).$$

(ii) *If $k \neq \mathbb{Q}$, then*

$$\frac{\big|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})\}\big|}{\big|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}\big|} = 1 + O_E\Big(\frac{\log B}{B^{1/2}}\Big).$$

Proof. For $u \in U(k)$, the commutator of $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k))$ is $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}}))$. Since $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k)) \subseteq \mathcal{H}_E$, we find that $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}}))$ is a closed subgroup of $[\mathcal{H}_E, \mathcal{H}_E]$. Since $[\mathcal{H}_E, \mathcal{H}_E]$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, there is a corresponding integer M as in Lemma 7.6; we may assume M is divisible by all primes $\ell < 17$. With this choice of M,

$$\begin{aligned}
&\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B,\ \rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) \neq [\mathcal{H}_E, \mathcal{H}_E]\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}|} \\
\le &\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B, \rho_{E_u,M}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) \neq [\mathcal{H}_E(M), \mathcal{H}_E(M)]\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}|} \qquad (7.3) \\
+ &\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B, \rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) \neq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some } \ell \nmid M\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \le B\}|} \qquad (7.4)
\end{aligned}$$

If $\rho_{E_u,M}(\mathrm{Gal}(\bar{k}/k)) = \mathcal{H}_E(M)$, then $\rho_{E_u,M}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) = [\mathcal{H}_E(M), \mathcal{H}_E(M)]$. Thus (7.3) is $O(B^{-[k:\mathbb{Q}]/2}\log B)$ by Proposition 7.2. For $\ell \nmid M$ (and in particular, $\ell \ge 5$), the group $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is its own commutator subgroup, so $\rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ if and only if $\rho_{E_u,\ell}(\mathrm{Gal}(\bar{k}/k)) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Thus by Proposition 7.5, the term (7.4) is $O(B^{-[k:\mathbb{Q}]/2+\varepsilon})$. Part (i) follows immediately.

We now consider (ii), so take $k \neq \mathbb{Q}$. Define the group $G = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. The representation $\det \circ \rho_E$ factors through the cyclotomic character $\mathrm{Gal}(\bar{k}/k) \to \widehat{\mathbb{Z}}^\times$, so $\rho_E(U_{k^{\mathrm{cyc}}}) = G$ and $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}}))$ is a closed subgroup of G for all $u \in U(k)$.

The group $[\mathcal{H}_E, \mathcal{H}_E]$ is a normal subgroup of finite index in G, so there is an integer m such that reduction modulo m gives an isomorphism

$$G/[\mathcal{H}_E, \mathcal{H}_E] \xrightarrow{\sim} G(m)/[\mathcal{H}_E(m), \mathcal{H}_E(m)].$$

Define $\widetilde{\rho}\colon \pi_1(U) \to \mathcal{H}_E(m)/[\mathcal{H}_E(m), \mathcal{H}_E(m)]$ to be the composition of $\rho_{E,m}$ with the obvious quotient map. The image of $\pi_1(U_{k^{\mathrm{cyc}}})$ under $\widetilde{\rho}$ is $G^c := G(m)/[\mathcal{H}_E(m), \mathcal{H}_E(m)]$. For each $u \in U(k)$, let $\widetilde{\rho}_u$ be the

composition of $\rho_{E_u,m}$ with the quotient map $\mathcal{H}_E(m) \twoheadrightarrow \mathcal{H}_E(m)/[\mathcal{H}_E(m), \mathcal{H}_E(m)]$. By Proposition 7.7 and our assumption $k \neq \mathbb{Q}$, we have

$$\frac{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B,\ \widetilde{\rho}_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = G^c\}|}{|\{u \in U(k) \cap \mathcal{O}_k^n : \|u\| \leq B\}|} = 1 + O\Big(\frac{\log B}{B^{1/2}}\Big). \tag{7.5}$$

If for $u \in U(k) \cap \mathcal{O}_k^n$ we have $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{ab}})) = [\mathcal{H}_E, \mathcal{H}_E]$ and $\widetilde{\rho}_u(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}})) = G^c$, then $\rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}}))$ equals $G = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. So (ii) follows from (i) and (7.5). □

Proof of Theorem 7.1. As remarked in the comments following the statement of Theorem 7.1, it suffices to prove the integral point versions.

Since $\det \circ \rho_E \colon \pi_1(U) \to \widehat{\mathbb{Z}}^\times$ factors through the cyclotomic character $\mathrm{Gal}(\bar{k}/k) \to \widehat{\mathbb{Z}}^\times$, we find that

$$[\mathcal{H}_E : \rho_{E_u}(\mathrm{Gal}(\bar{k}/k))] = [\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_{E_u}(\mathrm{Gal}(\bar{k}/k^{\mathrm{cyc}}))]$$

for all $u \in U(k)$. If $k \neq \mathbb{Q}$, then the integral point version of Theorem 7.1(i) is equivalent to Theorem 7.9(ii). Now suppose $k = \mathbb{Q}$. By the Kronecker-Weber theorem $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$, so $\rho_{E_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})) \subseteq [\mathcal{H}_E, \mathcal{H}_E]$ for all $u \in U(\mathbb{Q})$. Thus

$$\begin{aligned}
[\mathcal{H}_E : \rho_{E_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] &= [\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_{E_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))] \\
&= \big[\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{H}_E, \mathcal{H}_E]\big] \cdot \big[[\mathcal{H}_E, \mathcal{H}_E] : \rho_{E_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))\big] \\
&= r \cdot \big[[\mathcal{H}_E, \mathcal{H}_E] : \rho_{E_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))\big].
\end{aligned}$$

The integral point version of Theorem 7.1(ii) follows from Theorem 7.9(i) □

References

[AG09] Amir Akbary and Dragos Ghioca, *Periods of orbits modulo primes*, J. Number Theory **129** (2009), no. 11, 2831–2842. ↑3.3, 3.3

[Bom78] E. Bombieri, *On exponential sums in finite fields. II*, Invent. Math. **47** (1978), no. 1, 29–39. ↑7.3

[Che63] R. Chela, *Reducible polynomials*, J. London Math. Soc. **38** (1963), 183–188. ↑1.10

[Coh79] S. D. Cohen, *The distribution of the Galois groups of integral polynomials*, Illinois J. Math. **23** (1979), no. 1, 135–152. ↑1.1

[CFM05] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty, *The square sieve and the Lang-Trotter conjecture*, Canad. J. Math. **57** (2005), no. 6, 1155–1177. ↑7.2

[CGJ10] Alina Carmen Cojocaru, David Grant, and Nathan Jones, *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations*, 2010. preprint. ↑1.3.2

[CH05] Alina Carmen Cojocaru and Chris Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. **50** (2005), 3065–3080. ↑1.3.2, 7.2

[Die06] Rainer Dietmann, *Probabilistic Galois theory for quartic polynomials*, Glasg. Math. J. **48** (2006), no. 3, 553–556. ↑1.2

[Die10] ———, *On the distribution of Galois groups*, 2010. arXiv:1010.5341. ↑1.8

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. ↑1.3.2

[EEHK09] Jordan S. Ellenberg, Christian Elscholtz, Chris Hall, and Emmanuel Kowalski, *Non-simple abelian varieties in a family: geometric and analytic approaches*, J. London Math. Soc. (2) **80** (2009), 135–154. ↑3, ii

[FG09] Jason Fulman and Robert Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, 2009. arXiv:0902.2238. ↑1.12

[Gal71] P. X. Gallagher, *A larger sieve*, Acta Arith. **18** (1971), 77–81. ↑3

[Gal73] ———, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, pp. 91–101. ↑1.2

[Gra00] David Grant, *A formula for the number of elliptic curves with exceptional primes*, Compositio Math. **122** (2000), no. 2, 151–164. ↑1.3.2

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. ↑1.1

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. ↑1.3.2

[Kat88] Nicholas M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988. ↑5.1

[Kno56] Hans-Wilhelm Knobloch, *Die Seltenheit der reduziblen Polynome*, Jber. Deutsch. Math. Verein. **59** (1956), no. Abt. 1, 12–19. ↑1.2

[Kow06] E. Kowalski, *On the rank of quadratic twists of elliptic curves over function fields*, Int. J. Number Theory **2** (2006), no. 2, 267–288. ↑5.1

[Lef79] Phyllis Lefton, *On the Galois groups of cubics and trinomials*, Acta Arith. **35** (1979), no. 3, 239–246. ↑1.2

[ŁP97] Tomasz Łuczak and László Pyber, *On random generation of the symmetric group*, Combinatorics, geometry and probability (Cambridge, 1993), 1997, pp. 463–470. ↑1.11, 1.12

[MW93] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), no. 3, 247–254. ↑7.4

[Mur08] M. Ram Murty, *Problems in analytic number theory*, Second, Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008. Readings in Mathematics. ↑4.1

[MRS96] M. Ram Murty, Michael Rosen, and Joseph H. Silverman, *Variations on a theme of Romanoff*, Internat. J. Math. **7** (1996), no. 3, 373–391. ↑6.1

[Ser03] Jean-Pierre Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic). ↑1.1

[Ser08] ———, *Topics in Galois theory*, Second, Research Notes in Mathematics, vol. 1, A K Peters Ltd., Wellesley, MA, 2008. With notes by Henri Darmon. ↑1.1

[Ser72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1.3.1, 7.2

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, Third, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. ↑1.1, 1.1, 5.2, 6.1, 6.2, 7.2, 7.3

[Ser98] ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. ↑7.2

[Sil08] Joseph H. Silverman, *Variation of periods modulo p in arithmetic dynamics*, New York J. Math. **14** (2008), 601–616. ↑3.3, 3.3

[vdW36] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), no. 1, 133–147. ↑1.2, 1.9

[Wew99] Stefan Wewers, *Deformation of tame admissible covers of curves*, Aspects of Galois theory (Gainesville, FL, 1996), 1999, pp. 239–282. ↑5.2

[Zar00] Yuri G. Zarhin, *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. **7** (2000), no. 1, 123–132. ↑1.7

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. London Math. Soc. **42** (2010), no. 5, 811–826. ↑1.3.2, 7.2

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA
E-mail address: zywina@math.upenn.edu
URL: http://www.math.upenn.edu/~zywina