Algebra & Number Theory

Volume 12

2018

No. 8

Bounded generation of SL_2 over rings of S-integers with infinitely many units

Aleksander V. Morgan, Andrei S. Rapinchuk and Balasubramanian Sury

msp

ALGEBRA AND NUMBER THEORY 12:8 (2018)
dx.doi.org/10.2140/ant.2018.12.1949

Bounded generation of SL_2 over rings of S-integers with infinitely many units

Aleksander V. Morgan, Andrei S. Rapinchuk and Balasubramanian Sury

To Alex Lubotzky on his 60th birthday

Let $\mathcal{O}$ be the ring of S-integers in a number field k. We prove that if the group of units $\mathcal{O}^\times$ is infinite then every matrix in $\Gamma = \mathrm{SL}_2(\mathcal{O})$ is a product of at most 9 elementary matrices. This essentially completes a long line of research in this direction. As a consequence, we obtain a new proof of the fact that Γ is boundedly generated as an abstract group that uses only standard results from algebraic number theory.

1. Introduction

Let k be a number field. Given a finite subset S of the set V^k of valuations of k containing the set V_∞^k of archimedean valuations, we let $\mathcal{O}_{k,S}$ denote the ring of S-integers in k, i.e.,

$$\mathcal{O}_{k,S} = \{a \in k^\times \mid v(a) \geq 0 \text{ for all } v \in V^k \setminus S\} \cup \{0\}.$$

As usual, for any commutative ring R, we let $\mathrm{SL}_2(R)$ denote the group of unimodular 2×2-matrices over R and refer to the $\mathrm{SL}_2(R)$-matrices

$$E_{12}(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad E_{21}(b) = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \quad (a, b \in R)$$

as *elementary* (over R).

It was established in [Vasershtein 1972] (see also [Liehl 1981]) that if the ring of S-integers $\mathcal{O} = \mathcal{O}_{k,S}$ has infinitely many units, the group $\Gamma = \mathrm{SL}_2(\mathcal{O})$ is generated by elementary matrices. The goal of this paper is to prove that in this case Γ is actually *boundedly* generated by elementaries. More precisely, we prove the following.

Theorem 1.1. *Let $\mathcal{O} = \mathcal{O}_{k,S}$ be the ring of S-integers in a number field k, and assume that the group of units $\mathcal{O}^\times$ is infinite. Then every matrix in $\mathrm{SL}_2(\mathcal{O})$ is a product of at most 9 elementary matrices.*

The quest to validate the property that every element of $\mathrm{SL}_2(\mathcal{O})$ is a product of a bounded number of elementary matrices has a considerable history. First, G. Cooke and P. J. Weinberger [1975] established it (with the same bound as in Theorem 1.1) assuming the truth of a suitable form of the generalized Riemann hypothesis, which still remains unproven. Later, it was shown in [Loukanidis and Murty 1994] (see also

MSC2010: primary 11F06; secondary 11R37, 20H05.
Keywords: bounded generation, arithmetic groups, congruence subgroup problem.

[Murty 1995]) by analytic tools that the argument can be made unconditional if $|S| \geq \max(5, 2[k : \mathbb{Q}] - 3)$. On the other hand, B. Liehl [1984] proved the result by algebraic methods for some special fields k. The first unconditional proof in full generality was given by D. Carter, G. Keller and E. Paige in an unpublished preprint; their argument was streamlined and made available to the public by D. W. Morris [2007]. This argument is based on model theory and provides no explicit bound on the number of elementaries required; besides, it uses difficult results from additive number theory.

M. Vsemirnov [2014] proved Theorem 1.1 for $\mathcal{O} = \mathbb{Z}[1/p]$ using the results of D. R. Heath-Brown [1986] on Artin's primitive root conjecture (thus, in a broad sense, this proof develops the initial approach of Cooke and Weinberger [1975]); his bound on the number of elementaries required is ≤ 5. Subsequently, the third-named author reworked the argument from [Vsemirnov 2014] to avoid the use of [Heath-Brown 1986] in an unpublished note. These notes were the beginning of the work of the first two authors that eventually led to a proof of Theorem 1.1 in the general case. It should be noted that our proof uses only standard results from number theory such as Artin reciprocity and Chebotarev's density theorem, and is relatively short and constructive with an explicit bound which is independent of the field k and the set S. This, in particular, implies that Theorem 1.1 remains valid for any *infinite* S.

The problem of bounded generation (particularly by elementaries) has been considered for S-arithmetic subgroups of algebraic groups other than SL_2. A few years after [Cooke and Weinberger 1975], Carter and Keller [1983] showed that $\mathrm{SL}_n(\mathcal{O})$ for $n \geq 3$ is boundedly generated by elementaries for any ring $\mathcal{O}$ of algebraic integers (see [Tavgen 1990] for other Chevalley groups of rank > 1, and [Erovenko and Rapinchuk 2006] for isotropic, but nonsplit (or quasisplit), orthogonal groups). The upper bound on the number of factors required to write every matrix in $\mathrm{SL}_n(\mathcal{O})$ as a product of elementaries given in [Carter and Keller 1983] is $\frac{1}{2}(3n^2 - n) + 68\Delta - 1$, where Δ is the number of prime divisors of the discriminant of k; in particular, this estimate depends on the field k. Using our Theorem 1.1, one shows in all cases where the group of units $\mathcal{O}^\times$ is infinite, this estimate can be improved to $\frac{1}{2}(3n^2 - n) + 4$, hence made independent of k — see Corollary 4.6. The situation not covered by this result are when $\mathcal{O}$ is either $\mathbb{Z}$ or the ring of integers in an imaginary quadratic field — see below. The former case was treated in [Carter and Keller 1984] with an estimate $\frac{1}{2}(3n^2 - n) + 36$, so only in the case of imaginary quadratic fields the question of the existence of a bound on the number of elementaries independent of the k remains open.

From a more general perspective, Theorem 1.1 should be viewed as a contribution to the sustained effort aimed at proving that all higher rank lattices are boundedly generated as abstract groups. We recall that a group Γ is said to have *bounded generation* (BG) if there exist elements $\gamma_1, \dots, \gamma_d \in \Gamma$ such that

$$\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle,$$

where $\langle \gamma_i \rangle$ denotes the cyclic subgroup generated by γ_i. The interest in this property stems from the fact that while being purely combinatorial in nature, it is known to have a number of far-reaching consequences for the structure and representations of a group, particularly if the latter is S-arithmetic. For example, under one additional (necessary) technical assumption, (BG) implies the rigidity of completely reducible complex representations of Γ (known as SS-rigidity) — see [Rapinchuk 1990; Platonov and Rapinchuk

1994, Appendix A]. Furthermore, if Γ is an S-arithmetic subgroup of an absolutely simple simply connected algebraic group G over a number field k, then assuming the truth of the Margulis–Platonov conjecture for the group $G(k)$ of k-rational points [Platonov and Rapinchuk 1994, §9.1], (BG) implies the *congruence subgroup property* (i.e., the finiteness of the corresponding congruence kernel — see [Lubotzky 1995; Platonov and Rapinchuk 1992]). For applications of (BG) to the Margulis–Zimmer conjecture, see [Shalom and Willis 2013]. Given these and other implications of (BG), we would like to point out the following consequence of Theorem 1.1.

Corollary 1.2. *Let $\mathcal{O} = \mathcal{O}_{k,S}$ be the ring of S-integers, in a number field k. If the group of units $\mathcal{O}^\times$ is infinite, then the group $\Gamma = \mathrm{SL}_2(\mathcal{O})$ has bounded generation.*

We note that combining this fact with the results of [Lubotzky 1995; Platonov and Rapinchuk 1992], one obtains an alternative proof of the centrality of the congruence kernel for $\mathrm{SL}_2(\mathcal{O})$ (provided that $\mathcal{O}^\times$ is infinite), originally established by J.-P. Serre [1970]. We also note that (BG) of $\mathrm{SL}_2(\mathcal{O})$ is needed to prove (BG) for some other groups [Tavgen 1990; Erovenko and Rapinchuk 2006].

Next, it should be pointed out that the assumption that the unit group $\mathcal{O}^\times$ is infinite is *necessary* for the bounded generation of $\mathrm{SL}_2(\mathcal{O})$, hence cannot be omitted. Indeed, it follows from Dirichlet's unit theorem [Cassels and Fröhlich 1967, §2.18] that $\mathcal{O}^\times$ is finite only when $|S| = 1$ which happens precisely when S is the set of archimedian valuations in the following two cases:

(1) $k = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. In this case, the group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the elementaries, but has a nonabelian free subgroup of finite index, which prevents it from having bounded generation.

(2) $k = \mathbb{Q}(\sqrt{-d})$ for some square-free integer $d \geq 1$, and $\mathcal{O}_d$ is the ring of algebraic integers in k. According to [Grunewald and Schwermer 1981], the group $\Gamma = \mathrm{SL}_2(\mathcal{O}_d)$ has a finite index subgroup that admits an epimorphism onto a nonabelian free group, hence again cannot possibly be boundedly generated. Moreover, P. M. Cohn [1966] shows that if $d \notin \{1, 2, 3, 7, 11\}$ then Γ is not even generated by elementary matrices.

The structure of the paper is the following. In Section 2 we prove an algebraic result about abelian subextensions of radical extensions of general field — see Proposition 2.1. This statement, which may be of independent interest, is used in the paper to prove Theorem 3.7. This theorem is one of the number-theoretic results needed in the proof of Theorem 1.1, and it is established in Section 3 along with some other facts from algebraic number theory. One of the key notions in the paper is that of a $\mathbb{Q}$-split prime: we say that a prime $\mathfrak{p}$ of a number field k is $\mathbb{Q}$-split if it is nondyadic and its local degree over the corresponding rational prime is 1. In Section 3, we establish some relevant properties of such primes (see Section 3A) and prove in Section 3B the following (known — see the remark in Section 3) refinement of Dirichlet's theorem from [Bass et al. 1967].

Theorem 3.3. *Let $\mathcal{O}$ be the ring of S-integers in a number field k for some finite $S \subset V^k$ containing V^k_∞. If nonzero $a, b \in \mathcal{O}$ are relatively prime (i.e., $a\mathcal{O} + b\mathcal{O} = \mathcal{O}$) then there exist infinitely many principal $\mathbb{Q}$-split prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with a generator π such that $\pi \equiv a \pmod{b\mathcal{O}}$ and $\pi > 0$ in all real completions of k.*

Section 3C is devoted to the statement and proof of Theorem 3.7, which is another key number-theoretic result needed in the proof of Theorem 1.1. In Section 4, we prove Theorem 1.1 and Corollary 1.2. Finally, in Section 5 we correct the faulty example from [Vsemirnov 2014] of a matrix in $\mathrm{SL}_2(\mathbb{Z}[1/p])$, where p is a prime $\equiv 1 \pmod{29}$, that is not a product of four elementary matrices — see Proposition 5.1, confirming thereby that the bound of 5 in [Vsemirnov 2014] is optimal.

Notations and conventions. For a field k, we let k^{ab} denote the maximal abelian extension of k. Furthermore, $\mu(k)$ will denote the group of all roots of unity in k; if $\mu(k)$ is finite, we let μ denote its order. For $n \geq 1$ prime to $\operatorname{char} k$, we let ζ_n denote a primitive n-th root of unity.

In this paper, with the exception of Section 2, the field k will be a field of algebraic numbers (i.e., a finite extension of $\mathbb{Q}$), in which case $\mu(k)$ is automatically finite. We let $\mathcal{O}_k$ denote the ring of algebraic integers in k. Furthermore, we let V^k denote the set of (the equivalence classes of) nontrivial valuations of k, and let V^k_∞ and V^k_f denote the subsets of archimedean and nonarchimedean valuations, respectively. For any $v \in V^k$, we let k_v denote the corresponding completion; if $v \in V^k_f$ then $\mathcal{O}_v$ will denote the valuation ring in k_v with the valuation ideal $\hat{\mathfrak{p}}_v$ and the group of units $U_v = \mathcal{O}_v^\times$.

Throughout the paper, S will denote a fixed finite subset of V^k containing V^k_∞, and $\mathcal{O} = \mathcal{O}_{k,S}$ the corresponding ring of S-integers (see above). Then the nonzero prime ideals of $\mathcal{O}$ are in a natural bijective correspondence with the valuations in $V^k \setminus S$. So, for a nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}$ we let $v_{\mathfrak{p}} \in V^k \setminus S$ denote the corresponding valuation, and conversely, for a valuation $v \in V^k \setminus S$ we let $\mathfrak{p}_v \subset \mathcal{O}$ denote the corresponding prime ideal (note that $\mathfrak{p}_v = \mathcal{O} \cap \hat{\mathfrak{p}}_v$). Generalizing Euler's φ-function, for a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$, we set

$$\phi(\mathfrak{a}) = |(\mathcal{O}/\mathfrak{a})^\times|.$$

For simplicity of notation, for an element $a \in \mathcal{O}$, $\phi(a)$ will always mean $\phi(a\mathcal{O})$. Finally, for $a \in k^\times$, we let $V(a) = \{v \in V^k_f \mid v(a) \neq 0\}$.

Given a prime number p, one can write any integer n in the form $n = p^e \cdot m$, for some nonnegative integer e, where $p \nmid m$. We then call p^e the *p-primary component* of n.

2. Abelian subextensions of radical extensions

In this section, k is an arbitrary field. For a prime $p \neq \operatorname{char} k$, we let $\mu(k)_p$ denote the subgroup of $\mu(k)$, consisting of elements satisfying $x^{p^d} = 1$ for some $d \geq 0$. If this subgroup is finite, we set $\lambda(k)_p$ to be the nonnegative integer satisfying $|\mu(k)_p| = p^{\lambda(k)_p}$; otherwise, set $\lambda(k)_p = \infty$. Clearly if $\mu(k)$ is finite, then $\mu = \prod_p p^{\lambda(k)_p}$. For $a \in k^\times$, we write $\sqrt[n]{a}$ to denote an arbitrary root of the polynomial $x^n - a$.

The goal of this section is to prove the following.

Proposition 2.1. *Let $n \geq 1$ be an integer prime to* $\operatorname{char} k$, *and let $u \in k^\times$ be such that $u \notin \mu(k)_p k^{\times p}$ for all $p \mid n$. Then the polynomial $x^n - u$ is irreducible over k, and for $t = \sqrt[n]{u}$ we have*

$$k(t) \cap k^{\mathrm{ab}} = k(t^m) \quad \textit{where } m = \frac{n}{\prod_{p \mid n} \gcd(n, p^{\lambda(k)_p})},$$

with the convention that $\gcd(n, p^\infty)$ *is simply the p-primary component of n.*

We first treat the case $n = p^d$ where p is a prime.

Proposition 2.2. *Let p be a prime number $\neq \operatorname{char} k$, and let $u \in k^\times \setminus \mu(k)_p (k^\times)^p$. Fix an integer $d \geq 1$, set $t = \sqrt[p^d]{u}$. Then*

$$k(t) \cap k^{\mathrm{ab}} = k(t^{p^\gamma}) \quad \textit{where } \gamma = \max(0, d - \lambda(k)_p).$$

We begin with the following lemma.

Lemma 2.3. *Let p be a prime number $\neq \operatorname{char} k$, and let $u \in k^\times \setminus \mu(k)_p (k^\times)^p$. Set $k_1 = k(\sqrt[p]{u})$. Then*:

(i) $[k_1 : k] = p$.

(ii) $\mu(k_1)_p = \mu(k)_p$.

(iii) *None of the $\sqrt[p]{u}$ are in $\mu(k_1)_p (k_1^\times)^p$.*

Proof. (i) follows from [Lang 2002, Chapter VI, Theorem 9.1], as $u \notin (k^\times)^p$.

(ii) If $\lambda(k)_p = \infty$, then there is nothing to prove. Otherwise, we need to show that for $\lambda = \lambda(k)_p$, we have $\zeta_{p^{\lambda+1}} \notin k_1$. Assume the contrary. Then, first, $\lambda > 0$. Indeed, we have a tower of inclusions $k \subseteq k(\zeta_p) \subseteq k_1$. Since $[k_1 : k] = p$ by (i), and $[k(\zeta_p) : k] \leq p - 1$, we conclude that $[k(\zeta_p) : k] = 1$, i.e., $\zeta_p \in k$.

Now, since $\zeta_{p^{\lambda+1}} \notin k$, we have

$$k_1 = k(\zeta_{p^{\lambda+1}}) = k\big(\sqrt[p]{\zeta_{p^\lambda}}\big). \tag{1}$$

But according to Kummer's theory (which applies because $\zeta_p \in k$), the fact that $k(\sqrt[p]{a}) = k(\sqrt[p]{b})$ for $a, b \in k^\times$ implies that the images of a and b in $k^\times/(k^\times)^p$ generate the same subgroup. So, it follows from (1) that $u\zeta_p^i \in (k^\times)^p$ for some i, and therefore $u \in \mu(k)_p (k^\times)^p$, contradicting our choice of u.

(iii) Assume the contrary, i.e., some p-th root $\sqrt[p]{u}$ can be written in the form $\sqrt[p]{u} = \zeta a^p$ for some $a \in k_1^\times$ and $\zeta \in \mu(k_1)_p$. Let $N = N_{k_1/k} \colon k_1^\times \to k^\times$ be the norm map. Then

$$N(\sqrt[p]{u}) = N(\zeta) N(a)^p.$$

Clearly, $N(\zeta) \in \mu(k)_p$, so $N(\sqrt[p]{u}) \in \mu(k)_p (k^\times)^p$. On the other hand, $N(\sqrt[p]{u}) = u$ for p odd, and $-u$ for $p = 2$. In all cases, we obtain that $u \in \mu(k)_p (k^\times)^p$. A contradiction. □

A simple induction now yields the following:

Corollary 2.4. *Let p be a prime number $\neq \operatorname{char} k$, and let $u \in k^\times \setminus \mu(k)_p (k^\times)^p$. For a fixed integer $d \geq 1$, set $k_d = k(\sqrt[p^d]{u})$. Then*:

(i) $[k_d : k] = p^d$.

(ii) $\mu(k_d)_p = \mu(k)_p$, *hence* $\lambda(k_d)_p = \lambda(k)_p$.

Of course, assertion (i) is well known and follows, for example, from [Lang 2002, Chapter VI, §9].

Lemma 2.5. *Let p be a prime number $\neq \operatorname{char} k$, and let $u \in k^\times \setminus \mu(k)_p (k^\times)^p$. Fix an integer $d \geq 1$, and set $t = \sqrt[p^d]{u}$ and $k_d = k(t)$. Furthermore, for an integer j between 0 and d define $\ell_j = k(t^{p^{d-j}}) \simeq k(\sqrt[p^j]{u})$. Then any intermediate subfield $k \subseteq \ell \subseteq k_d$ is of the form $\ell = \ell_j$ for some $j \in \{0, \dots, d\}$.*

Proof. Given such an ℓ, it follows from Corollary 2.4(i) that $[k_d : \ell] = p^j$ for some $0 \leq j \leq d$. Since any conjugate of t is of the form $\zeta \cdot t$ where $\zeta^{p^d} = 1$, we see that the norm $N_{k_d/\ell}(t)$ is of the form $\zeta_0 t^{p^j}$, where again $\zeta_0^{p^d} = 1$. Then $\zeta_0 \in \mu(k_d)_p$, and using Corollary 2.4(ii), we conclude that $\zeta_0 \in k \subseteq \ell$. So, $t^{p^j} \in \ell$, implying the inclusion $\ell_{d-j} \subseteq \ell$. Now, the fact that $[k_d : \ell_{d-j}] = p^j$ implies that $\ell = \ell_{d-j}$, yielding our claim. □

Proof of Proposition 2.2. Set $\lambda = \lambda(k)_p$. Then for any $d \leq \lambda$ the extension $k(\sqrt[p^d]{u})/k$ is abelian, and our assertion is trivial. So, we may assume that $\lambda < \infty$ and $d > \lambda$. It follows from Lemma 2.5 that $\ell := k(t) \cap k^{\mathrm{ab}}$ is of the form $\ell_{d-j} = k(t^{p^j})$ for some $j \in \{0, \ldots, d\}$. On the other hand, ℓ_{d-j}/k is a Galois extension of degree p^{d-j}, so must contain the conjugate $\zeta_{p^{d-j}} t^{p^{d-j}}$ of $t^{p^{d-j}}$, implying that $\zeta_{p^{d-j}} \in \ell_{d-j}$. Since $\ell_{d-j} \simeq k(\sqrt[p^{d-j}]{u})$, we conclude from Corollary 2.4(ii) that $d - j \leq \lambda$, i.e., $j \geq d - \lambda$. This proves the inclusion $\ell \subseteq k(t^{p^\gamma})$; the opposite inclusion is obvious. □

Proof of Proposition 2.1. Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the prime factorization of n, and for $i = 1, \ldots, s$ set $n_i = n/p_i^{\alpha_i}$. Let $t = \sqrt[n]{u}$ and $t_i = t^{n_i}$ (so, t_i is a $p_i^{\alpha_i}$-th root of u). Using again [Lang 2002, Chapter VI, Theorem 9.1] we conclude that $[k(t) : k] = n$, which implies that

$$[k(t) : k(t_i)] = n_i \quad \text{for all } i = 1, \ldots, r. \tag{2}$$

Since for $K := k(t) \cap k^{\mathrm{ab}}$ the degree $[K : k]$ divides n, we can write $K = K_1 \cdots K_s$ where K_i is an abelian extension of k of degree $p_i^{\beta_i}$ for some $\beta_i \leq \alpha_i$. Then the degree $[K_i(t_i) : k(t_i)]$ must be a power of p_i. Comparing with (2), we conclude that $K_i \subseteq k(t_i)$. Applying Proposition 2.2 with $d = \alpha_i$, we obtain the inclusion

$$K_i \subseteq k(t_i^{p_i^{\gamma_i}}) = k(t^{n_i p_i^{\gamma_i}}) \quad \text{where } \gamma_i = \max(0, \alpha_i - \lambda(k)_{p_i}). \tag{3}$$

It is easy to see that the gcd of the numbers $n_i p_i^{\gamma_i}$ for $i = 1, \ldots, s$ is

$$m = \frac{n}{\prod_{p|n} \gcd(n, p^{\lambda(k)_p})}.$$

Furthermore, the subgroup of $k(t)^\times$ generated by $t^{n_1 p_1^{\gamma_1}}, \ldots, t^{n_s p_s^{\gamma_s}}$ coincides with the cyclic subgroup with generator t^m. Then (3) yields the following inclusion

$$K = K_1 \cdots K_s \subseteq k(t^m).$$

Since the opposite inclusion is obvious, our claim follows. □

Corollary 2.6. *Assume that $\mu = |\mu(k)| < \infty$. Let P be a finite set of rational primes $\neq \operatorname{char} k$, and define*

$$\mu' = \mu \cdot \prod_{p \in P} p.$$

Given $u \in k^\times$ such that

$$u \notin \mu(k)_p (k^\times)^p \quad \textit{for all } p \in P,$$

for any abelian extension F of k the intersection

$$E := F \cap k(\sqrt[\mu']{u}, \zeta_{\mu'})$$

is contained in $k(\sqrt[\mu]{u}, \zeta_{\mu'})$.

Proof. Without loss of generality we may assume that $\zeta_{\mu'} \in F$, and then we have the following tower of field extensions

$$k(\sqrt[\mu]{u}, \zeta_{\mu'}) \subset E(\sqrt[\mu]{u}) \subset k(\sqrt[\mu']{u}, \zeta_{\mu'}).$$

We note that the degree $[k(\sqrt[\mu']{u}, \zeta_{\mu'}) : k(\sqrt[\mu]{u}, \zeta_{\mu'})]$ divides $\prod_{p \in P} p$. So, if we assume that the assertion of the lemma is false, then we should be able to find to find a prime $p \in P$ that divides the degree $[E(\sqrt[\mu]{u}) : k(\sqrt[\mu]{u}, \zeta_{\mu'})]$, and therefore does *not* divide the degree $[k(\sqrt[\mu']{u}, \zeta_{\mu'}) : E(\sqrt[\mu]{u})]$. The latter implies that $\sqrt[p\mu]{u} \in E(\sqrt[\mu]{u})$. But this contradicts Proposition 2.1 since $E(\sqrt[\mu]{u}) = E \cdot k(\sqrt[\mu]{u})$ is an abelian extension of k. □

3. Results from algebraic number theory

3A. $\mathbb{Q}$-*split primes.* Our proof of Theorem 1.1 heavily relies on properties of so-called $\mathbb{Q}$-split primes in $\mathcal{O}$.

Definition. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$, and let p be the corresponding rational prime. We say that $\mathfrak{p}$ is $\mathbb{Q}$-*split* if $p > 2$, and for the valuation $v = v_{\mathfrak{p}}$ we have $k_v = \mathbb{Q}_p$.

For the convenience of further references, we list some simple properties of $\mathbb{Q}$-split primes.

Lemma 3.1. *Let $\mathfrak{p}$ be a $\mathbb{Q}$-split prime in $\mathcal{O}$, and for $n \geq 1$ let $\rho_n \colon \mathcal{O} \to \mathcal{O}/\mathfrak{p}^n$ be the corresponding quotient map. Then*:

(a) *The group of invertible elements $(\mathcal{O}/\mathfrak{p}^n)^\times$ is cyclic for any n.*

(b) *If $c \in \mathcal{O}$ is such that $\rho_2(c)$ generates $(\mathcal{O}/\mathfrak{p}^2)^\times$ then $\rho_n(c)$ generates $(\mathcal{O}/\mathfrak{p}^n)^\times$ for any $n \geq 2$.*

Proof. Let $p > 2$ be the rational prime corresponding to $\mathfrak{p}$, and $v = v_{\mathfrak{p}}$ be the associated valuation of k. By definition, $k_v = \mathbb{Q}_p$, hence $\mathcal{O}_v = \mathbb{Z}_p$. So, for any $n \geq 1$ we will have canonical ring isomorphisms

$$\mathcal{O}/\mathfrak{p}^n \simeq \mathcal{O}_v/\hat{\mathfrak{p}}_v^n = \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}. \tag{4}$$

Then (a) follows from the well-known fact that the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. Furthermore, the isomorphisms in (4) are compatible for different n. Since the kernel of the group homomorphism $(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p^2\mathbb{Z})^\times$ is contained in the Frattini subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for $n \geq 2$, the same is true for the homomorphism $(\mathcal{O}/\mathfrak{p}^n)^\times \to (\mathcal{O}/\mathfrak{p}^2)^\times$. This easily implies (b). □

Let $\mathfrak{p}$ be a $\mathbb{Q}$-split prime, let $v = v_{\mathfrak{p}}$ be the corresponding valuation. We will now define the *level* $\ell_{\mathfrak{p}}(u)$ of an element $u \in \mathcal{O}_v^\times$ and establish some properties of this notion that we will need later.

Let $p > 2$ be the corresponding rational prime. The group of p-adic units $\mathbb{U}_p = \mathbb{Z}_p^\times$ has the natural filtration by the congruence subgroups

$$\mathbb{U}_p^{(i)} = 1 + p^i\mathbb{Z}_p \quad \text{for } i \in \mathbb{N}.$$

It is well-known that

$$\mathbb{U}_p = C \times \mathbb{U}_p^{(1)}$$

where C is the cyclic group of order $(p-1)$ consisting of all roots of unity in $\mathbb{Q}_p$. Furthermore, the logarithmic map yields a continuous isomorphism $\mathbb{U}_p^{(i)} \to p^i\mathbb{Z}_p$, which implies that for any $u \in \mathbb{U}_p \setminus C$, the closure of the cyclic group generated by u has a decomposition of the form

$$\overline{\langle u\rangle} = C' \times \mathbb{U}_p^{(\ell)}$$

for some subgroup $C' \subset C$ and some integer $\ell = \ell_p(u) \geq 1$ which we will refer to as the *p-level* of u. We also set $\ell_p(u) = \infty$ for $u \in C$.

Returning now to a $\mathbb{Q}$-split prime $\mathfrak{p}$ of k and keeping the above notations, we define the *$\mathfrak{p}$-level* $\ell_{\mathfrak{p}}(u)$ of $u \in \mathcal{O}_v^\times$ as the p-level of the element in $\mathbb{U}_p$ that corresponds to u under the natural identification $\mathcal{O}_v = \mathbb{Z}_p$. We will need the following.

Lemma 3.2. *Let $\mathfrak{p}$ be a $\mathbb{Q}$-split prime in $\mathcal{O}$, let p be the corresponding rational prime, and $v = v_{\mathfrak{p}}$ the corresponding valuation. Suppose we are given an integer $d \geq 1$ not divisible by p, a unit $u \in \mathcal{O}_v^\times$ of infinite order having $\mathfrak{p}$-level $s = \ell_{\mathfrak{p}}(u)$, an integer n_s, and an element $c \in \mathcal{O}_v$ such that $u^{n_s} \equiv c \pmod{\mathfrak{p}^s}$. Then for any $t \geq s$ there exists an integer $n_t \equiv n_s \pmod{d}$ for which $u^{n_t} \equiv c \pmod{\mathfrak{p}^t}$.*

Proof. In view of the identification $\mathcal{O}_v = \mathbb{Z}_p$, it is enough to prove the corresponding statement for $\mathbb{Z}_p$. More precisely, we need to show the following: *Let $u \in \mathbb{U}_p$ be a unit of infinite order and p-level $s = \ell_p(u)$. If $c \in \mathbb{U}_p$ and $n_s \in \mathbb{Z}$ are such that $u^{n_s} \equiv c \pmod{p^s}$, then for any $t \geq s$ there exists $n_t \equiv n_s \pmod{d}$ such that $u^{n_t} \equiv c \pmod{p^t}$.* Thus, we have that $u^{n_s} \in c\mathbb{U}_p^{(s)}$, and we wish to show that

$$u^{n_s} \cdot \langle u^d\rangle \cap c\mathbb{U}_p^{(t)} \neq \varnothing.$$

Since $c\mathbb{U}_p^{(t)}$ is open, it is enough to show that

$$u^{n_s} \cdot \overline{\langle u^d\rangle} \cap c\mathbb{U}_p^{(t)} \neq \varnothing. \tag{5}$$

But since $\ell_p(u) = s$ and d is prime to p, we have the inclusion $\overline{\langle u^d\rangle} \supset \mathbb{U}_p^{(s)}$, and (5) is obvious. □

3B. ***Dirichlet's theorem for $\mathbb{Q}$-split primes.*** The following known (see the remark below) result gives the existence of $\mathbb{Q}$-split primes in arithmetic progressions.

Theorem 3.3. *Let $\mathcal{O}$ be the ring of S-integers in a number field k for some finite $S \subset V^k$ containing V_∞^k. If nonzero $a, b \in \mathcal{O}$ are relatively prime (i.e., $a\mathcal{O} + b\mathcal{O} = \mathcal{O}$) then there exist infinitely many principal $\mathbb{Q}$-split prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with a generator π such that $\pi \equiv a \pmod{b\mathcal{O}}$ and $\pi > 0$ in all real completions of k.*

The proof follows the same general strategy as the proof of Dirichlet's theorem in [Bass et al. 1967] — see Theorem A.10 in the appendix on number theory. First, we will quickly review some basic facts from global class field theory (see, for example, [Cassels and Fröhlich 1967, Chapter VII]) and fix some notations. Let J_k denote the *group of ideles* of k with the natural topology; as usual, we identify $k^\times$ with the (discrete) *subgroup of principal ideles* in J_k. Then for every open subgroup $\mathcal{U} \subset J_k$ of finite index containing $k^\times$ there exists a finite abelian Galois extension L/k and a continuous surjective homomorphism $\alpha_{L/k}\colon J_k \to \mathrm{Gal}(L/k)$ (known as the *norm residue map*) such that:

- $\mathcal{U} = \operatorname{Ker} \alpha_{L/k} = N_{L/k}(J_L)k^\times$.
- For every nonarchimedean $v \in V^k$ which is unramified in L we let $\mathrm{Fr}_{L/k}(v)$ denote the Frobenius automorphism of L/k at v (i.e., the Frobenius automorphism $\mathrm{Fr}_{L/k}(w|v)$ associated to some (equivalently, any) extension $w|v$) and let $\boldsymbol{i}(v) \in J_k$ be an idele with the components
$$\boldsymbol{i}(v)_{v'} = \begin{cases} 1 & \text{if } v' \neq v, \\ \pi_v & \text{if } v' = v, \end{cases}$$
where $\pi_v \in k_v$ is a uniformizer; then $\alpha_{L/k}(\boldsymbol{i}(v)) = \mathrm{Fr}_{L/k}(v)$.

For our fixed finite subset $S \subset V^k$ containing V^k_∞, we define the following open subgroup of J_k:
$$U_S := \prod_{v \in S} k_v^\times \times \prod_{v \in V^k \setminus S} U_v.$$
Then the abelian extension of k corresponding to the subgroup $\mathcal{U}_S := U_S k^\times$ will be called the *Hilbert S-class field* of k and denoted K throughout the rest of the paper.

Next, we will introduce the idelic S-analogs of *ray groups*. Let $\mathfrak{b}$ be a nonzero ideal of $\mathcal{O} = \mathcal{O}_{k,S}$ with the prime factorization
$$\mathfrak{b} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}, \tag{6}$$
let $v_i = v_{\mathfrak{p}_i}$ be the valuation in $V^k \setminus S$ associated with $\mathfrak{p}_i$, and let $V(\mathfrak{b}) = \{v_1, \dots, v_t\}$. We then define an open subgroup
$$R_S(\mathfrak{b}) = \prod_{v \in V^k} R_v$$
where the open subgroups $R_v \subseteq k_v^\times$ are defined as follows. For v real, we let R_v be the subgroup of positive elements, letting $R_v = k_v^\times$ for all other $v \in S$, and setting $R_v = U_v$ for all $v \notin S \cup V(\mathfrak{b})$. It remains to define R_v for $v = v_i \in V(\mathfrak{b})$, in which case we set it to be the congruence subgroup $U_{v_i}^{(n_i)}$ of U_{v_i} modulo $\hat{\mathfrak{p}}_{v_i}^{n_i}$. We then let $K(\mathfrak{b})$ denote the abelian extension of k corresponding to $\boldsymbol{R}_S(\mathfrak{b}) := R_S(\mathfrak{b})k^\times$ ("ray class field"). (Obviously, $K(\mathfrak{b})$ contains K for any nonzero ideal $\mathfrak{b}$ of $\mathcal{O}$.) Furthermore, given $c \in k^\times$, we let $\boldsymbol{j}_{\mathfrak{b}}(c)$ denote the idele with the following components:
$$\boldsymbol{j}_{\mathfrak{b}}(c)_v = \begin{cases} c & \text{if } v \in V(\mathfrak{b}), \\ 1 & \text{if } v \notin V(\mathfrak{b}). \end{cases}$$
Then $\theta_{\mathfrak{b}}\colon k^\times \to \mathrm{Gal}(K(\mathfrak{b})/k)$ defined by $c \mapsto \alpha_{K(\mathfrak{b})/k}(\boldsymbol{j}_{\mathfrak{b}}(c))^{-1}$ is a group homomorphism.

The following lemma summarizes some simple properties of these definitions.

Lemma 3.4. *Let $\mathfrak{b} \subset \mathcal{O}$ be a nonzero ideal.*

(a) *If a nonzero $c \in \mathcal{O}$ is relatively prime to $\mathfrak{b}$ (i.e., $c\mathcal{O} + \mathfrak{b} = \mathcal{O}$) then $\theta_{\mathfrak{b}}(c)$ restricts to the Hilbert S-class field K trivially.*

(b) *If nonzero $c_1, c_2 \in \mathcal{O}$ are both relatively prime to $\mathfrak{b}$ then $c_1 \equiv c_2 \pmod{\mathfrak{b}}$ is equivalent to*

$$\mathrm{pr}_{\mathfrak{b}}(\boldsymbol{j}_{\mathfrak{b}}(c_1)R_S(\mathfrak{b})) = \mathrm{pr}_{\mathfrak{b}}(\boldsymbol{j}_{\mathfrak{b}}(c_2)R_S(\mathfrak{b})) \tag{7}$$

where $\mathrm{pr}_{\mathfrak{b}} \colon J_k \to \prod_{v \in V(\mathfrak{b})} k_v^\times$ is the natural projection.

Proof. (a) Since c is relatively prime to $\mathfrak{b}$, we have $\boldsymbol{j}_{\mathfrak{b}}(c) \in U_S$. So, using the functoriality properties of the norm residue map, we obtain

$$\theta_{\mathfrak{b}}(c) | K = \alpha_{K(\mathfrak{b})/k}(\boldsymbol{j}_{\mathfrak{b}}(c))^{-1} | K = \alpha_{K/k}(\boldsymbol{j}_{\mathfrak{b}}(c))^{-1} = \mathrm{id}_K$$

because $\boldsymbol{j}_{\mathfrak{b}}(c) \in U_S \subset \mathcal{U}_S = \operatorname{Ker} \alpha_{K/k}$, as required.

(b) As above, let (6) be the prime factorization of $\mathfrak{b}$, let $v_i = v_{\mathfrak{p}_i} \in V^k \setminus S$ be the valuation associated with $\mathfrak{p}_i$. Then for any $c_1, c_2 \in \mathcal{O}$, the congruence $c_1 \equiv c_2 \pmod{\mathfrak{b}}$ is equivalent to

$$c_1 \equiv c_2 \pmod{\hat{\mathfrak{p}}_{v_i}^{n_i}} \quad \text{for all } i = 1, \dots, t. \tag{8}$$

On the other hand, for any $v \in V_f^k$ and any $u_1, u_2 \in U_v$, the congruence $u_1 \equiv u_2 \pmod{\hat{\mathfrak{p}}_v^n}$ for $n \geq 1$ is equivalent to

$$u_1 U_v^{(n)} = u_2 U_v^{(n)},$$

where $U_v^{(n)}$ is the congruence subgroup of U_v modulo $\hat{\mathfrak{p}}_v^n$. Thus, for (nonzero) $c_1, c_2 \in \mathcal{O}$ prime to $\mathfrak{b}$, the conditions (7) and (8) are equivalent, and our assertion follows. □

We will now establish a result needed for the proof of Theorem 3.3 and its refinements.

Proposition 3.5. *Let $\mathfrak{b}$ be a nonzero ideal of $\mathcal{O}$, let $a \in \mathcal{O}$ be relatively prime to $\mathfrak{b}$, and let F be a finite Galois extension of $\mathbb{Q}$ that contains $K(\mathfrak{b})$. Assume that a rational prime p is unramified in F and there exists an extension w of the p-adic valuation v_p to F such that $\mathrm{Fr}_{F/\mathbb{Q}}(w|v_p)|K(\mathfrak{b}) = \theta_{\mathfrak{b}}(a)$. If the restriction v of w to k does not belong to $S \cup V(\mathfrak{b})$ then*:

(a) $k_v = \mathbb{Q}_p$.

(b) *The prime ideal $\mathfrak{p} = \mathfrak{p}_v$ of $\mathcal{O}$ corresponding to v is principal with a generator π satisfying $\pi \equiv a \pmod{\mathfrak{b}}$ and $\pi > 0$ in every real completion of k.*

We note since v is unramified in F which contains $K(\mathfrak{b})$, we in fact *automatically* have that $v \notin V(\mathfrak{b})$.

Proof. (a) Since the Frobenius $\mathrm{Fr}(w|v_p)$ generates $\mathrm{Gal}(F_w/\mathbb{Q}_p)$, our claim immediately follows from the fact that it acts trivially on k.

(b) According to (a), the local degree $[k_v : \mathbb{Q}_p]$ is 1, hence the residual degree $f(v|v_p)$ is also 1, and therefore

$$\mathrm{Fr}(w|v) = \mathrm{Fr}(w|v_p)^{f(v|v_p)} = \mathrm{Fr}(w|v_p).$$

Thus,

$$\alpha_{K(\mathfrak{b})/k}(\boldsymbol{i}(v)) = \mathrm{Fr}(w|v)|K(\mathfrak{b}) = \theta_{\mathfrak{b}}(a) = \alpha_{K(\mathfrak{b})/k}(\boldsymbol{j}_{\mathfrak{b}}(a))^{-1},$$

and therefore

$$\boldsymbol{i}(v)\boldsymbol{j}_{\mathfrak{b}}(a) \in \operatorname{Ker}\alpha_{K(\mathfrak{b})/K} = \boldsymbol{R}_S(\mathfrak{b}) = R_S(\mathfrak{b})k^{\times}.$$

So, we can write

$$\boldsymbol{i}(v)\boldsymbol{j}_{\mathfrak{b}}(a) = \boldsymbol{r}\pi \quad \text{with } \boldsymbol{r} \in R_S(\mathfrak{b}), \pi \in k^{\times}. \tag{9}$$

Then

$$\pi = \boldsymbol{i}(v)(\boldsymbol{j}_{\mathfrak{b}}(a)\boldsymbol{r}^{-1}).$$

Since a is prime to $\mathfrak{b}$, the idele $\boldsymbol{j}_{\mathfrak{b}}(a) \in U_S$, and then $\boldsymbol{j}_{\mathfrak{b}}(a)\boldsymbol{r}^{-1} \in U_S$. For any $v' \in V^k \setminus (S \cup \{v\})$, the v'-component of $\boldsymbol{i}(v)$ is trivial, so we obtain that $\pi \in U_{v'}$. On the other hand, the v-component of $\boldsymbol{i}(v)$ is a uniformizer π_v of k_v implying that π is also a uniformizer. Thus, $\mathfrak{p} = \pi\mathcal{O}$ is precisely the prime ideal associated with v. For any real v', the v'-components of $\boldsymbol{i}(v)$ and $\boldsymbol{j}_{\mathfrak{b}}(a)$ are trivial, so π equals the inverse of the v'-component of $\boldsymbol{r}$, hence positive in $k_{v'}$. Finally, it follows from (9) that

$$\mathrm{pr}_{\mathfrak{b}}(\boldsymbol{j}_{\mathfrak{b}}(a)) = \mathrm{pr}_{\mathfrak{b}}(\boldsymbol{j}_{\mathfrak{b}}(\pi)\boldsymbol{r}),$$

so $\pi \equiv a \pmod{\mathfrak{b}}$ by Lemma 3.4(b), as required. □

Proof of Theorem 3.3. Set $\mathfrak{b} = b\mathcal{O}$ and $\sigma = \theta_{\mathfrak{b}}(a) \in \mathrm{Gal}(K(\mathfrak{b})/k)$. Let F be the Galois closure of $K(\mathfrak{b})$ over $\mathbb{Q}$, and let $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ be such that $\tau|K(\mathfrak{b}) = \sigma$. Applying Chebotarev's density theorem (see [Cassels and Fröhlich 1967, Chapter VII, 2.4] or [Bass et al. 1967, A.6]) we find infinitely many rational primes $p > 2$ for which the p-adic valuation v_p is unramified in F, does not lie below any valuations in $S \cup V(\mathfrak{b})$, and has an extension w to F such that $\mathrm{Fr}_{F/\mathbb{Q}}(w|v_p) = \tau$. Let $v = w|k$, and let $\mathfrak{p} = \mathfrak{p}_v$ be the corresponding prime ideal of $\mathcal{O}$. Since $p > 2$, Proposition 3.5(a) implies that $\mathfrak{p}$ is $\mathbb{Q}$-split. Furthermore, Proposition 3.5(b) asserts that $\mathfrak{p}$ has a generator π such that $\pi \equiv a \pmod{\mathfrak{b}}$ and $\pi > 0$ in every real completion of k, as required. □

Remark. Dong Quan Ngoc Nguyen pointed out to us that Theorem 3.3, hence the essential part of Dirichlet's theorem from [Bass et al. 1967] (in particular, (A.11)), was known already to Hasse [1926, Satz 13]. In the current paper, however, we use the approach described in [Bass et al. 1967] to establish the key Theorem 3.7; the outline of the constructions from [loc. cit.] as well as the technical Lemma 3.4 and Proposition 3.5 are included for this purpose. We note that in contrast to the argument in [loc. cit.], our proofs of Theorems 3.3 and 3.7 involve the application of Chebotarev's density theorem to *noncommutative* Galois extensions.

We will now prove a statement from Galois theory that we will need in the next subsection.

Lemma 3.6. *Let $F/\mathbb{Q}$ be a finite Galois extension, and let κ be an integer for which $F \cap \mathbb{Q}^{\mathrm{ab}} \subseteq \mathbb{Q}(\zeta_\kappa)$. Then $F(\zeta_\kappa) \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\kappa)$.*

Proof. We need to show that

$$[F(\zeta_\kappa) : F(\zeta_\kappa) \cap \mathbb{Q}^{\mathrm{ab}}] = [F(\zeta_\kappa) : \mathbb{Q}(\zeta_\kappa)]. \tag{10}$$

Let

$$G = \mathrm{Gal}(F(\zeta_\kappa)/\mathbb{Q}) \quad \text{and} \quad H = \mathrm{Gal}(F/\mathbb{Q}).$$

Then the left-hand side of (10) is equal to the order of the commutator subgroup $[G, G]$, while the right-hand side equals

$$[F : F \cap \mathbb{Q}(\zeta_\kappa)] = [F : F \cap \mathbb{Q}^{\mathrm{ab}}] = \big|[H, H]\big|.$$

Now, the restriction gives an *injective* group homomorphism

$$\psi \colon G \to H \times \mathrm{Gal}(\mathbb{Q}(\zeta_\kappa)/\mathbb{Q}).$$

Since the restriction $G \to H$ is surjective, we obtain that ψ implements an isomorphism between $[G, G]$ and $[H, H] \times \{1\}$. Thus, $[G, G]$ and $[H, H]$ have the same order, and (10) follows. □

3C. ***Key statement.*** In this subsection we will establish another number-theoretic statement which plays a crucial role in the proof of Theorem 1.1. To formulate it, we need to introduce some additional notations. As above, let $\mu = |\mu(k)|$ be the number of roots of unity in k, let K be the Hilbert S-class field of k, and let $\tilde{K}$ be the Galois closure of K over $\mathbb{Q}$. Suppose we are given two finite sets P and Q of rational primes. Let

$$\mu' = \mu \cdot \prod_{p \in P} p,$$

pick an integer $\lambda \geq 1$ which is divisible by μ and for which $\tilde{K} \cap \mathbb{Q}^{\mathrm{ab}} \subseteq \mathbb{Q}(\zeta_\lambda)$, and set

$$\lambda' = \lambda \cdot \prod_{q \in Q} q.$$

Theorem 3.7. *Let $u \in \mathcal{O}^\times$ be a unit of infinite order such that $u \notin \mu(k)_p (k^\times)^p$ for every prime $p \in P$, and let $\mathfrak{q}$ be a $\mathbb{Q}$-split prime of $\mathcal{O}$ which is relatively prime to λ'. Then there exist infinitely many principal $\mathbb{Q}$-split primes $\mathfrak{p} = \pi\mathcal{O}$ of $\mathcal{O}$ with a generator π such that*:

1. *For each $p \in P$, the p-primary component of $\phi(\mathfrak{p})/\mu$ divides the p-primary component of the order of u* $\pmod{\mathfrak{p}}$.
2. $\pi \pmod{\mathfrak{q}^2}$ *generates* $(\mathcal{O}/\mathfrak{q}^2)^\times$.
3. $\gcd(\phi(\mathfrak{p}), \lambda') = \lambda$.

Proof. As in the proof of Theorem 3.3, we will derive the required assertion by applying Chebotarev's density theorem to a specific automorphism of an appropriate finite Galois extension.

Let $K(\mathfrak{q}^2)$ be the abelian extension $K(\mathfrak{b})$ of k introduced in Section 3B for the ideal $\mathfrak{b} = \mathfrak{q}^2$. Set

$$L_1 = K(\mathfrak{q}^2)(\zeta_{\lambda'}), \quad L_2 = k(\zeta_{\mu'}, \sqrt[\mu']{u}), \quad L = L_1 L_2 \quad \text{and} \quad \ell = L_1 \cap L_2.$$

Then

$$\mathrm{Gal}(L/k) = \{\sigma = (\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/k) \times \mathrm{Gal}(L_2/k) : \sigma_1 \mid \ell = \sigma_2 \mid \ell\}. \tag{11}$$

So, to construct $\sigma \in \mathrm{Gal}(L/k)$ that we will need in the argument it is enough to construct appropriate $\sigma_i \in \mathrm{Gal}(L_i/k)$ for $i = 1, 2$ that have the same restriction to ℓ.

Lemma 3.8. *The restriction maps define the following isomorphisms*:

(1) $\mathrm{Gal}(L_1/K) \simeq \mathrm{Gal}(K(\mathfrak{q}^2)/K) \times \mathrm{Gal}(K(\zeta_{\lambda'})/K)$.

(2) $\mathrm{Gal}(K(\zeta_{\lambda'})/K(\zeta_\lambda)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{\lambda'})/\mathbb{Q}(\zeta_\lambda)) \simeq \prod_{q \in Q} \mathrm{Gal}(\mathbb{Q}(\zeta_{q\lambda})/\mathbb{Q}(\zeta_\lambda))$.

Proof. (1) We need to show that $K(\mathfrak{q}^2) \cap K(\zeta_\lambda) = K$. But the Galois extensions $K(\mathfrak{q}^2)/K$ and $K(\zeta_\lambda)/K$ are respectively totally and unramified at the extensions of $v_\mathfrak{q}$ to K (since $\mathfrak{q}$ is prime to λ), so the required fact is immediate.

(2) Since $K(\zeta_{\lambda'}) = K(\zeta_\lambda) \cdot \mathbb{Q}(\zeta_{\lambda'})$, we only need to show that

$$K(\zeta_\lambda) \cap \mathbb{Q}(\zeta_{\lambda'}) = \mathbb{Q}(\zeta_\lambda). \tag{12}$$

We have

$$K(\zeta_\lambda) \cap \mathbb{Q}(\zeta_{\lambda'}) \subseteq \tilde{K}(\zeta_\lambda) \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\lambda)$$

by Lemma 3.6. This proves one inclusion in (12); the other inclusion is obvious. □

Since $\mathfrak{q}$ is $\mathbb{Q}$-split, the group $(\mathcal{O}/\mathfrak{q}^2)^\times$ is cyclic (Lemma 3.1(a)), and we pick $c \in \mathcal{O}$ so that $c \pmod{\mathfrak{q}^2}$ is a generator of this group. We then set

$$\sigma_1' = \theta_{\mathfrak{q}^2}(c) \in \mathrm{Gal}(K(\mathfrak{q}^2)/K)$$

in the notations of Section 3B (see Lemma 3.4(a)). Next, for $q \in Q$, we let $q^{e(q)}$ be the q-primary component of λ. Then using the isomorphism from Lemma 3.8(2), we can find $\sigma_1'' \in \mathrm{Gal}(K(\zeta_{\lambda'})/K)$ such that

$$\sigma_1''(\zeta_\lambda) = \zeta_\lambda \quad \text{but} \quad \sigma_1''(\zeta_{q^{e(q)+1}}) \neq \zeta_{q^{e(q)+1}} \quad \text{for all } q \in Q. \tag{13}$$

We then define $\sigma_1 \in \mathrm{Gal}(L_1/K)$ to be the automorphism corresponding to the pair (σ_1', σ_1'') in terms of the isomorphism from Lemma 3.8(1) (in other words, the restrictions of σ_1 to $K(\mathfrak{q}^2)$ and $K(\zeta_{\lambda'})$ are σ_1' and σ_1'', respectively).

We fix a μ'-th root $\sqrt[\mu']{u}$, and for $\nu | \mu'$ set $\sqrt[\nu]{u} = (\sqrt[\mu']{u})^{\mu'/\nu}$ (also denoted $u^{\nu^{-1}}$). To construct $\sigma_2 \in \mathrm{Gal}(L_2/k)$, we need the following.

Lemma 3.9. *Let* $\sigma_0 \in \mathrm{Gal}(\ell/k)$. *Then there exists* $\sigma_2 \in \mathrm{Gal}(L_2/k)$ *such that*

(1) $\sigma_2|\ell = \sigma_0$.

(2) *For any $p \in P$, if $p^{d(p)}$ is the p-primary component of μ then*

$$\sigma_2(u^{p^{-(d(p)+1)}}) \neq u^{p^{-(d(p)+1)}}.$$

Consequently either $\sigma_2(\zeta_{p^{d(p)+1}}) \neq \zeta_{p^{d(p)+1}}$ or σ_2 acts nontrivially on all *$p^{d(p)+1}$-th roots of u.*

Proof. Since L_1/k is an abelian extension, we conclude from Corollary 2.6 that

$$\ell \subseteq k(\sqrt[\mu]{u}, \zeta_{\mu'}) \subseteq k^{\mathrm{ab}}. \tag{14}$$

On the other hand, according to Proposition 2.1, none of the roots $\sqrt[p\mu]{u}$ for $p \in P$ lies in k^{ab}, and the restriction maps yield an isomorphism

$$\mathrm{Gal}\big(k(\sqrt[\mu']{u}, \zeta_{\mu'})/k(\sqrt[\mu]{u}, \zeta_{\mu'})\big) \to \prod_{p \in P} \mathrm{Gal}\big(k(\sqrt[p\mu]{u}, \zeta_{\mu'})/k(\sqrt[\mu]{u}, \zeta_{\mu'})\big).$$

It follows that for each $p \in P$ we can find $\tau_p \in \mathrm{Gal}\big(k(\sqrt[\mu']{u}, \zeta_{\mu'})/k(\sqrt[\mu]{u}, \zeta_{\mu'})\big)$ such that

$$\tau_p(u^{p^{-(d(p)+1)}}) = \zeta_p \cdot u^{p^{-(d(p)+1)}} \quad \text{and} \quad \tau_p(u^{q^{-(d(q)+1)}}) = u^{q^{-(d(q)+1)}} \quad \text{for all } q \in P \setminus \{p\}.$$

Now, let $\tilde{\sigma}_0$ be any extension of σ_0 to L_2. For $p \in P$, define

$$\chi(p) = \begin{cases} 1 & \text{if } \tilde{\sigma}_0(u^{p^{-(d(p)+1)}}) = u^{p^{-(d(p)+1)}}, \\ 0 & \text{if } \tilde{\sigma}_0(u^{p^{-(d(p)+1)}}) \neq u^{p^{-(d(p)+1)}} \end{cases}$$

Set

$$\sigma_2 = \tilde{\sigma}_0 \cdot \prod_{p \in P} \tau_p^{\chi(p)}.$$

In view of (14), all τ_p's act trivially on ℓ, so $\sigma_2 \mid \ell = \tilde{\sigma}_0|\ell = \sigma_0$ and (1) holds. Furthermore, the choice of the τ_p's and the $\chi(p)$'s implies that (2) also holds. □

Continuing the proof of Theorem 3.7, we now use $\sigma_1 \in \mathrm{Gal}(L_1/k)$ constructed above, set $\sigma_0 = \sigma_1|\ell$, and using Lemma 3.9 construct $\sigma_2 \in \mathrm{Gal}(L_2/k)$ with the properties described therein. In particular, part (1) of this lemma in conjunction with (11) implies that the pair (σ_1, σ_2) corresponds to an automorphism $\sigma \in \mathrm{Gal}(L/k)$. As in the proof of Theorem 3.3, we let F denote the Galois closure of L over $\mathbb{Q}$, and let $\tilde{\sigma} \in \mathrm{Gal}(F/\mathbb{Q})$ be such that $\tilde{\sigma}|L = \sigma$. By Chebotarev's density theorem, there exist infinitely many rational primes $\pi > 2$ that are relatively prime to $\lambda' \cdot \mu'$ and for which the π-adic valuation v_π is unramified in F, does not lie below any valuation in $S \cup \{v_{\mathfrak{q}}\}$, and has an extension w to F such that $\mathrm{Fr}_{F/\mathbb{Q}}(w|v_\pi) = \tilde{\sigma}$. Let $v = w|k$, and let $\mathfrak{p} = \mathfrak{p}_v$ be the corresponding prime ideal of $\mathcal{O}$. As in the proof of Theorem 3.3, we see that $\mathfrak{p}$ is $\mathbb{Q}$-split. Furthermore, since $\sigma|K(\mathfrak{q}^2) = \theta_{\mathfrak{q}^2}(c)$, we conclude that $\mathfrak{p}$ has a generator π such that $\pi \equiv c \pmod{\mathfrak{q}^2}$ (see Proposition 3.5(b)). Then by construction $\pi \pmod{\mathfrak{q}^2}$ generates $(\mathcal{O}/\mathfrak{q}^2)^\times$, verifying condition (2) of Theorem 3.7.

To verify condition (1), we fix $p \in P$ and consider two cases. First, suppose $\sigma(\zeta_{p^{d(p)+1}}) \neq \zeta_{p^{d(p)+1}}$. Since p is prime to $\mathfrak{p}$, this means that the residue field $\mathcal{O}/\mathfrak{p}$ does not contain an element of order $p^{d(p)+1}$ (although, since μ is prime to $\mathfrak{p}$, it does contain an element of order μ, hence of order $p^{d(p)}$). So, in this case $\phi(\mathfrak{p})/\mu$ is prime to p, and there is nothing to prove. Now, suppose that $\sigma(\zeta_{p^{d(p)+1}}) = \zeta_{p^{d(p)+1}}$. Then by construction σ acts nontrivially on every $p^{d(p)+1}$-th root of u, and therefore the polynomial $X^{p^{d(p)+1}} - u$ has no roots in k_v. Again, since p is prime to $\mathfrak{p}$, we see from Hensel's lemma that $u \pmod{\mathfrak{p}}$ is not a $p^{d(p)+1}$-th power in the residue field. It follows that the p-primary component of the order of $u \pmod{\mathfrak{p}}$ is not less than the p-primary component of $\phi(\mathfrak{p})/p^{d(p)}$, and (1) follows.

Finally, by construction σ acts trivially on ζ_λ but nontrivially on $\zeta_{q\lambda}$ for any $q \in Q$. Since $\mathfrak{p}$ is prime to λ', we see that the residue field $\mathcal{O}/\mathfrak{p}$ contains an element of order λ, but does not contain an element of order $q\lambda$ for any $q \in Q$. This means that $\lambda | \phi(\mathfrak{p})$ but $\phi(\mathfrak{p})/\lambda$ is relatively prime to each $q \in Q$, which is equivalent to condition (3) of Theorem 3.7. □

4. Proof of Theorem 1.1

First, we will introduce some additional notation needed to convert the task of factoring a given matrix $A \in \mathrm{SL}_2(\mathcal{O})$ as a product of elementary matrices into the task of reducing the first row of A to $(1, 0)$. Let

$$\mathcal{R}(\mathcal{O}) = \{(a, b) \in \mathcal{O}^2 \mid a\mathcal{O} + b\mathcal{O} = \mathcal{O}\}$$

(note that $\mathcal{R}(\mathcal{O})$ is precisely the set of all first rows of matrices $A \in \mathrm{SL}_2(\mathcal{O})$). For $\lambda \in \mathcal{O}$, one defines two permutations, $e_+(\lambda)$ and $e_-(\lambda)$, of $\mathcal{R}(\mathcal{O})$ given respectively by

$$(a, b) \mapsto (a, b + \lambda a) \quad \text{and} \quad (a, b) \mapsto (a + \lambda b, b).$$

These permutations will be called *elementary transformations* of $\mathcal{R}(\mathcal{O})$. For (a, b), $(c, d) \in \mathcal{R}(\mathcal{O})$ we will write $(a, b) \xRightarrow{n} (c, d)$ to indicate the fact that (c, d) can be obtained from (a, b) by a sequence of n (equivalently, $\leq n$) elementary transformations. For the convenience of further reference, we will record some simple properties of this relation.

Lemma 4.1. *Let $(a, b) \in \mathcal{R}(\mathcal{O})$.*

(1a) *If $(c, d) \in \mathcal{R}(\mathcal{O})$ and $(a, b) \xRightarrow{n} (c, d)$, then $(c, d) \xRightarrow{n} (a, b)$.*

(1b) *If (c, d), $(e, f) \in \mathcal{R}(\mathcal{O})$ are such that $(a, b) \xRightarrow{m} (c, d)$ and $(c, d) \xRightarrow{n} (e, f)$, then $(a, b) \xRightarrow{m+n} (e, f)$.*

(2a) *If $c \in \mathcal{O}$ such that $c \equiv a \pmod{b\mathcal{O}}$, then $(c, b) \in \mathcal{R}(\mathcal{O})$, and $(a, b) \xRightarrow{1} (c, b)$.*

(2b) *If $d \in \mathcal{O}$ such that $d \equiv b \pmod{a\mathcal{O}}$, then $(a, d) \in \mathcal{R}(\mathcal{O})$, and $(a, b) \xRightarrow{1} (a, d)$.*

(3a) *If $(a, b) \xRightarrow{n} (1, 0)$ then any matrix $A \in \mathrm{SL}_2(\mathcal{O})$ with the first row (a, b) is a product of $\leq n + 1$ elementary matrices.*

(3b) *If $(a, b) \xRightarrow{n} (0, 1)$ then any matrix $A \in \mathrm{SL}_2(\mathcal{O})$ with the second row (a, b) is a product of $\leq n + 1$ elementary matrices.*

(4a) *If $a \in \mathcal{O}^\times$ then $(a, b) \xRightarrow{2} (0, 1)$.*

(4b) *If $b \in \mathcal{O}^\times$ then $(a, b) \xRightarrow{2} (1, 0)$.*

Proof. (1a) We observe that the inverse of an elementary transformation is again an elementary transformation given by $[e_{\pm}(\lambda)]^{-1} = e_{\pm}(-\lambda)$, so the required fact follows. Part (1b) is obvious.

(Note that (1) implies that the relation between (a, b) and $(c, d) \in \mathcal{R}(O)$ defined by $(a, b) \xRightarrow{n} (c, d)$ for *some* $n \in \mathbb{N}$ is an equivalence relation.)

(2a) We have $c = a + \lambda b$ with $\lambda \in \mathcal{O}$. Then

$$c\mathcal{O} + b\mathcal{O} = a\mathcal{O} + b\mathcal{O} = \mathcal{O},$$

so $(c, a) \in \mathcal{R}(\mathcal{O})$, and $e_+(\lambda)$ takes (a, b) to (c, b). The argument for (2b) is similar.

(3a) Suppose $A \in \mathrm{SL}_2(\mathcal{O})$ has the first row (a, b). Then for $\lambda \in \mathcal{O}$, the first row of the product $AE_{12}(\lambda)$ is $(a, b + \lambda a) = e_+(\lambda)(a, b)$, and similarly the first row of $AE_{21}(\lambda)$ is $e_-(\lambda)(a, b)$. So, the fact that $(a, b) \xRightarrow{n} (1, 0)$ implies that there exists a matrix $U \in \mathrm{SL}_2(\mathcal{O})$ which is a product of n elementary matrices and is such that AU has the first row $(1, 0)$. This means that $AU = E_{21}(z)$ for some $z \in \mathcal{O}$, and then $A = E_{21}(z)U^{-1}$ is a product of $\leq n + 1$ elementary matrices. The argument for (3b) is similar.

(4a) This follows since $e_-(-a)e_+(a^{-1}(1 - b))(a, b) = (0, 1)$. The proof of (4b) is similar. □

Remark. All assertions of Lemma 4.1 are valid over any commutative ring $\mathcal{O}$.

Corollary 4.2. *Let $\mathfrak{q}$ be a principal $\mathbb{Q}$-split prime ideal of $\mathcal{O}$ with generator q, and let $z \in \mathcal{O}$ be such that $z \pmod{\mathfrak{q}^2}$ generates $(\mathcal{O}/\mathfrak{q}^2)^{\times}$. Given an element of $\mathcal{R}(\mathcal{O})$ of the form (b, q^n) with $n \geq 2$, and an integer t_0, there exists an integer $t \geq t_0$ such that $(b, q^n) \xRightarrow{1} (z^t, q^n)$.*

Proof. By Lemma 3.1(b), the element $z \pmod{\mathfrak{q}^n}$ generates $(\mathcal{O}/\mathfrak{q}^n)^{\times}$. Since b is prime to $\mathfrak{q}$, one can find $t \in \mathbb{Z}$ such that $b \equiv z^t \pmod{\mathfrak{q}^n}$. Adding to t a suitable multiple of $\phi(\mathfrak{q}^n)$ if necessary, we can assume that $t \geq t_0$. Our assertion then follows from Lemma 4.1(2a). □

Lemma 4.3. *Suppose we are given $(a, b) \in \mathcal{R}(\mathcal{O})$, a finite subset $T \subseteq V_f^k$, and an integer $n \neq 0$. Then there exists $\alpha \in \mathcal{O}_k$ and $r \in \mathcal{O}^{\times}$ such that $V(\alpha) \cap T = \varnothing$, and $(a, b) \xRightarrow{1} (\alpha r^n, b)$.*

Proof. Let h_k be the class number of k. If for each $v \in S \setminus V_\infty^k$ we let $\mathfrak{m}_v$ denote the maximal ideal of $\mathcal{O}_k$ corresponding to v, then the ideal $(\mathfrak{m}_v)^{h_k}$ is principal, and its generator π_v satisfies $v(\pi_v) = h_k$ and $w(\pi_v) = 0$ for all $w \in V_f^k \setminus \{v\}$. Let R be the subgroup of $k^{\times}$ generated by π_v for $v \in S \setminus V_\infty^k$; note that $R \subset \mathcal{O}^{\times}$. We can pick $r \in R$ so that $a' := ar^{-n} \in \mathcal{O}_k$. We note that since a and b are relatively prime in $\mathcal{O}$, we have $V(a') \cap V(b) \subset S$.

Now, it follows from the strong approximation theorem that there exists $\gamma \in \mathcal{O}_k$ such that

$$v(\gamma b) \geq 0 \quad \text{and} \quad v(\gamma b) \equiv 0 \pmod{nh_k} \quad \text{for all } v \in S \setminus V_\infty^k,$$

and

$$v(\gamma b) = 0 \quad \text{for all } v \in V(a') \setminus S.$$

Then, in particular, we can find $s \in R$ so that $v(\gamma b s^{-1}) = 0$ for all $v \in S \setminus V_\infty^k$. Set

$$\gamma' := \gamma s^{-1} \in \mathcal{O} \quad \text{and} \quad b' := \gamma' b \in \mathcal{O}_k.$$

By construction,

$$v(b') = 0 \quad \text{for all } v \in V(a') \cup (S \setminus V^k_\infty), \tag{15}$$

implying that $V(a') \cap V(b') = \varnothing$, which means that a' and b' are relatively prime in $\mathcal{O}_k$.

Again, by the strong approximation theorem we can find $t \in \mathcal{O}_k$ such that

$$v(t) = 0 \ \text{ for } v \in T \cap V(a') \quad \text{and} \quad v(t) > 0 \ \text{ for } v \in T \setminus V(a').$$

Set $\alpha = a' + tb' \in \mathcal{O}_k$. Then for $v \in T \cap V(a')$ we have $v(a') > 0$ and $v(tb') = 0$ (in view of (15)), while for $v \in T \setminus V(a')$ we have $v(a') = 0$ and $v(tb') > 0$. In either case,

$$v(\alpha) = v(a' + tb') = 0 \quad \text{for all } v \in T,$$

i.e., $V(\alpha) \cap T = \varnothing$. On the other hand,

$$a + r^n t\gamma' b = r^n (a' + tb') = r^n \alpha,$$

which means that $(a, b) \overset{1}{\Longrightarrow} (\alpha r^n, b)$, as required. □

Recall that we let μ denote the number of roots of unity in k.

Lemma 4.4. *Let $(a, b) \in \mathcal{R}(\mathcal{O})$ be such that $a = \alpha \cdot r^\mu$ for some $\alpha \in \mathcal{O}_k$ and $r \in \mathcal{O}^\times$ where $V(\alpha)$ is disjoint from $S \cup V(\mu)$. Then there exist $a' \in \mathcal{O}$ and infinitely many $\mathbb{Q}$-split prime principal ideals $\mathfrak{q}$ of $\mathcal{O}$ with a generator q such that for any $m \equiv 1 \pmod{\phi(a'\mathcal{O})}$ we have $(a, b) \overset{3}{\Longrightarrow} (a', q^{\mu m})$.*

Proof. The argument below is adapted from the proof of Lemma 3 in [Carter and Keller 1983]. It relies on the properties of the power residue symbol (in particular, the power reciprocity law) described in the appendix on number theory in [Bass et al. 1967]. We will work with all $v \in V^k$ (and not only $v \in V^k \setminus S$), so to each such v we associate a symbol ("modulus") $\mathfrak{m}_v$. For $v \in V^k_f$ we will identify $\mathfrak{m}_v$ with the corresponding maximal ideal of $\mathcal{O}_k$ (obviously, $\mathfrak{p}_v = \mathfrak{m}_v \mathcal{O}$ for $v \in V^k \setminus S$); the valuation ideal and the group of units in the valuation ring $\mathcal{O}_v$ (or $\mathcal{O}_{\mathfrak{m}_v}$) in the completion k_v will be denoted $\hat{\mathfrak{m}}_v$ and U_v respectively. For any divisor $\kappa \mid \mu$, we let

$$\left(\frac{*\,,\,*}{\mathfrak{m}_v}\right)_\kappa$$

be the (bimultiplicative, skew-symmetric) power residue symbol of degree κ on $k_v^\times$ [Bass et al. 1967, p.85]. We recall that $\left(\frac{x,y}{\mathfrak{m}_v}\right)_\kappa = 1$ if one of the elements x, y is a κ-th power in $k_v^\times$ (in particular, if either v is complex or v is real and one of the elements x, y is positive in k_v) or if v is nonarchimedean $\notin V(\kappa)$ and $x, y \in U_v$. It follows that for any $x, y \in k^\times$, we have $\left(\frac{x,y}{\mathfrak{m}_v}\right)_\kappa = 1$ for almost all $v \in V^k$. Furthermore, we have the *reciprocity law*:

$$\prod_{v \in V^k} \left(\frac{x,\, y}{\mathfrak{m}_v}\right)_\kappa = 1. \tag{16}$$

Now, let $\mu = p_1^{e_1} \cdots p_n^{e_n}$ be a prime factorization of μ. For each $i = 1, \dots, n$, pick $v_i \in V(p_i)$. According to [Bass et al. 1967, A.17], the values

$$\left(\frac{x, y}{\mathfrak{m}_{v_i}}\right)_{p_i^{e_i}} \quad \text{for } x, y \in U_{v_i}$$

cover all $p_i^{e_i}$-th roots of unity. Thus, we can pick units $u_i, u_i' \in U_{v_i}$ for $i = 1, \dots, n$ so that $\left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{p_i^{e_i}}$ is a primitive $p_i^{e_i}$-th root of unity. On the other hand, since $u_i, u_i' \in U_{v_i}$ and $v_i(\mu/p_i^{e_i}) = 0$, we have

$$\left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{\mu}^{p_i^{e_i}} = \left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{\mu/p_i^{e_i}} = 1.$$

Thus,

$$\zeta_{p_i^{e_i}} := \left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{\mu}$$

is a primitive $p_i^{e_i}$-th root of unity for each $i = 1, \dots, n$, making

$$\zeta_\mu := \prod_{i=1}^{n} \left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{\mu} \tag{17}$$

a primitive μ-th root of unity. Furthermore, it follows from the inverse function theorem or Hensel's lemma that we can find an integer $N > 0$ such that

$$1 + \hat{\mathfrak{m}}_v^N \subset k_v^{\times \mu} \quad \text{for all } v \in V(\mu). \tag{18}$$

We now write $b = \beta t^\mu$ with $\beta \in \mathcal{O}_k$ and $t \in \mathcal{O}^\times$. Since a, b are relatively prime in $\mathcal{O}$, so are α, β, hence $V(\alpha) \cap V(\beta) \subset S$. On the other hand, by our assumption $V(\alpha)$ is disjoint from $S \cup V(\mu)$, so we conclude that $V(\alpha)$ is disjoint from $V(\beta) \cup V(\mu)$. Applying Theorem 3.3 to the ring $\mathcal{O}_k$ we obtain that there exists $\beta' \in \mathcal{O}_k$ having the following properties:

(1$_1$) $\mathfrak{b} := \beta' \mathcal{O}_k$ is a prime ideal of $\mathcal{O}_k$ and the corresponding valuation $v_{\mathfrak{b}} \notin S \cup V(\mu)$.

(2$_1$) $\beta' > 0$ in every real completion of k.

(3$_1$) $\beta' \equiv \beta \pmod{\alpha \mathcal{O}_k}$.

(4$_1$) For each $i = 1, \dots, n$, we have

$$\beta' \equiv u_i' \pmod{\hat{\mathfrak{m}}_{v_i}^N} \quad \text{and} \quad \beta' \equiv 1 \pmod{\hat{\mathfrak{m}}_v^N}$$

for all $v \in V(p_i) \setminus \{v_i\}$.

Set $b' = \beta' t^\mu$. It is a consequence of (3)$_1$ that $b \equiv b' \pmod{a\mathcal{O}}$, so by Lemma 4.1(2) we have $(a, b) \overset{1}{\Longrightarrow} (a, b')$. Furthermore, it follows from (4)$_1$ and (18) that $\beta'/u_i' \in k_{v_i}^{\times \mu}$, so

$$\left(\frac{u_i, \beta'}{\mathfrak{m}_{v_i}}\right)_{\mu} = \left(\frac{u_i, u_i'}{\mathfrak{m}_{v_i}}\right)_{\mu} = \zeta_{p_i^{e_i}}.$$

Since ζ_μ defined by (17) is a primitive μ-th root of unity, we can find an integer $d > 0$ such that

$$1=\left(\frac{\alpha,\beta'}{\mathfrak{b}}\right)_{\mu}\cdot\zeta_{\mu}^{d}=\left(\frac{\alpha,\beta'}{\mathfrak{b}}\right)_{\mu}\cdot\prod_{i=1}^{n}\left(\frac{u_i^d,\beta'}{\mathfrak{m}_{v_i}}\right)_{\mu}. \tag{19}$$

By construction, $v_{\mathfrak{b}} \notin V(\alpha)\cup V(\mu)$, so applying Theorem 3.3 one more time, we find $\alpha' \in \mathcal{O}_k$ such that:

(1_2) $\mathfrak{a} := \alpha'\mathcal{O}_k$ is a prime ideal of $\mathcal{O}_k$ and the corresponding valuation $v_{\mathfrak{a}} \notin S \cup V(\mu)$.

(2_2) $\alpha' \equiv \alpha \pmod{\mathfrak{b}}$.

(3_2) $\alpha' \equiv u_i^d \pmod{\hat{\mathfrak{m}}_{v_i}^N}$ for $i = 1, \dots, n$.

Set $a' = \alpha' r^{\mu}$. Then $a'\mathcal{O} = \alpha'\mathcal{O}$ is a prime ideal of $\mathcal{O}$ and $a' \equiv a \pmod{b'\mathcal{O}}$, so $(a, b') \overset{1}{\Longrightarrow} (a', b')$.

Now, we note that $\left(\frac{\alpha',\beta'}{\mathfrak{m}_v}\right)_{\mu} = 1$ if either $v \in V_\infty^k$ (since $\beta' > 0$ in all real completions of k) or $v \in V_f^k \setminus (V(\alpha') \cup V(\beta') \cup V(\mu))$. Since the ideals $\mathfrak{a} = \alpha'\mathcal{O}_k$ and $\mathfrak{b} = \beta'\mathcal{O}_k$ are prime by construction, we have $V(\alpha') = \{v_{\mathfrak{a}}\}$ and $V(\beta') = \{v_{\mathfrak{b}}\}$. Besides, it follows from (18) and $(4)_1$ that for $v \in V(p_i)\setminus\{v_i\}$ we have $\beta' \in k_v^{\times\mu}$, and therefore again $\left(\frac{\alpha',\beta'}{\mathfrak{m}_v}\right)_{\mu} = 1$. Thus, the reciprocity law (16) for α', β' reduces to the relation

$$\left(\frac{\alpha',\beta'}{\mathfrak{a}}\right)_{\mu}\cdot\left(\frac{\alpha',\beta'}{\mathfrak{b}}\right)_{\mu}\cdot\prod_{i=1}^{n}\left(\frac{\alpha',\beta'}{\mathfrak{m}_{v_i}}\right)_{\mu}=1. \tag{20}$$

It follows from $(2)_2$ and $(3)_2$ that

$$\left(\frac{\alpha',\beta'}{\mathfrak{b}}\right)_{\mu}=\left(\frac{\alpha,\beta'}{\mathfrak{b}}\right)_{\mu} \quad\text{and}\quad \left(\frac{\alpha',\beta'}{\mathfrak{m}_{v_i}}\right)_{\mu}=\left(\frac{u_i^d,\beta'}{\mathfrak{m}_{v_i}}\right)_{\mu} \quad\text{for all } i=1,\dots,n.$$

Comparing now (19) with (20), we find that

$$\left(\frac{\beta',\alpha'}{\mathfrak{a}}\right)_{\mu}=\left(\frac{\alpha',\beta'}{\mathfrak{a}}\right)_{\mu}^{-1}=1.$$

This implies [Bass et al. 1967, A.16] that β' is a μ-th power modulo $\mathfrak{a}$, i.e., $\beta' \equiv \gamma^{\mu} \pmod{\mathfrak{a}}$ for some $\gamma \in \mathcal{O}_k$. Clearly, the elements $a' = \alpha' r^{\mu}$ and γt are relatively prime in $\mathcal{O}$, so applying Theorem 3.3 to this ring, we find infinitely many $\mathbb{Q}$-split principal prime ideals $\mathfrak{q}$ of $\mathcal{O}$ having a generator $q \equiv \gamma t \pmod{a'\mathcal{O}}$. Then for any $m \equiv 1 \pmod{\phi(a'\mathcal{O})}$ we have

$$q^{\mu m} \equiv q^{\mu} \equiv \beta' t^{\mu} \equiv b' \pmod{a'\mathcal{O}},$$

so $(a', b') \overset{1}{\Longrightarrow} (a', q^{\mu m})$. Then by Lemma 4.1(1b), we have $(a, b) \overset{3}{\Longrightarrow} (a', q^{\mu m})$, as required. □

The final ingredient that we need for the proof of Theorem 1.1 is the following lemma which uses the notion of the *level* $\ell_{\mathfrak{p}}(u)$ of a unit u of infinite order with respect to a $\mathbb{Q}$-split ideal $\mathfrak{p}$ introduced in Section 3A.

Lemma 4.5. *Let $\mathfrak{p}$ be a principal $\mathbb{Q}$-split ideal of $\mathcal{O}$ with a generator π, and let $u \in \mathcal{O}^{\times}$ be a unit of infinite order. Set $s = \ell_{\mathfrak{p}}(u)$, and let λ and m be integers satisfying $\lambda \mid \phi(\mathfrak{p})$ and $m \equiv 0 \pmod{\phi(\mathfrak{p}^s)/\lambda}$.*

Given an integer $\delta > 0$ dividing λ and $b \in \mathcal{O}$ prime to π such that b is a δ-th power $\bmod \mathfrak{p}$ *while $\nu := \lambda/\delta$ divides the order of u* $(\bmod \mathfrak{p})$, *for any integer $t \geq s$ there exists an integer n_t for which*

$$(\pi^t, b^m) \xrightarrow{1} (\pi^t, u^{n_t}).$$

Proof. Let p be the rational prime corresponding to $\mathfrak{p}$. Being a divisor of λ, the integer δ is relatively prime to p. So, the fact that b is a δ-th power $\bmod \mathfrak{p}$ implies that it is also a δ-th power $\bmod \mathfrak{p}^s$. On the other hand, it follows from our assumptions that $\lambda m = \delta \nu m$ is divisible by $\phi(\mathfrak{p}^s)$, and therefore $(b^m)^\nu \equiv 1 \pmod{\mathfrak{p}^s}$. But since ν is prime to p, the subgroup of elements in $(\mathcal{O}/\mathfrak{p}^s)^\times$ of order dividing ν is isomorphic to a subgroup of $(\mathcal{O}/\mathfrak{p})^\times$, hence cyclic. So, the fact that the order of $u \pmod{\mathfrak{p}}$, and consequently the order $u \pmod{\mathfrak{p}^s}$, is divisible by ν implies that every element in $(\mathcal{O}/\mathfrak{p}^s)^\times$ whose order divides ν lies in the subgroup generated by $u \pmod{\mathfrak{p}^s}$. Thus, $b^m \equiv u^{n_s} \pmod{\mathfrak{p}^s}$ for some integer n_s. Since $\mathfrak{p}$ is $\mathbb{Q}$-split, we can apply Lemma 3.2 to conclude that for any $t \geq s$ there exists an integer n_t such that $b^m \equiv u^{n_t} \pmod{\mathfrak{p}^t}$. Then $(\pi^t, b^m) \xrightarrow{1} (\pi^t, u^{n_t})$ by Lemma 4.1(2). □

We will call a unit $u \in \mathcal{O}^\times$ *fundamental* if it has infinite order and the cyclic group $\langle u \rangle$ is a direct factor of $\mathcal{O}^\times$. Since the group $\mathcal{O}^\times$ is finitely generated (Dirichlet's unit theorem, cf. [Cassels and Fröhlich 1967, §2.18]) it always contains a fundamental unit once it is infinite. We note that any fundamental unit has the following property:

$$u \notin \mu(k)_p (k^\times)^p \quad \text{for any prime } p.$$

We are now in a position to give

Proof of Theorem 1.1. We return to the notations of Section 3C: we let K denote the Hilbert S-class field of k, let $\tilde{K}$ be its normal closure over $\mathbb{Q}$, and pick an integer $\lambda \geq 1$ which is divisible by μ and for which $\tilde{K} \cap \mathbb{Q}^{\mathrm{ab}} \subset \mathbb{Q}(\zeta_\lambda)$. Furthermore, since $\mathcal{O}^\times$ is infinite by assumption, we can find a fundamental unit $u \in \mathcal{O}^\times$. By Lemma 4.1(3), it suffices to show that for any $(a, b) \in \mathcal{R}(\mathcal{O})$, we have

$$(a, b) \xrightarrow{8} (1, 0). \tag{21}$$

First, applying Lemma 4.3 with $T = (S \setminus V_\infty^k) \cup V(\mu)$ and $n = \mu$, we see that there exist $\alpha \in \mathcal{O}_k$ and $r \in \mathcal{O}^\times$ such that

$$V(\alpha) \cap (S \cup V(\mu)) = \varnothing \quad \text{and} \quad (a, b) \xrightarrow{1} (\alpha r^\mu, b).$$

Next, applying Lemma 4.4 to the last pair, we find $a' \in \mathcal{O}$ and a $\mathbb{Q}$-split principal prime ideal $\mathfrak{q}$ such that $v_\mathfrak{q} \notin S \cup V(\lambda) \cup V(\phi(a'\mathcal{O}))$ and $(\alpha r^\mu, b) \xrightarrow{3} (a', q^{\mu m})$ for any $m \equiv 1 \pmod{\phi(a'\mathcal{O})}$. Then

$$(a, b) \xrightarrow{4} (a', q^{\mu m}) \quad \text{for any } m \equiv 1 \pmod{\phi(a'\mathcal{O})}. \tag{22}$$

To proceed with the argument we will now specify m. We let P and Q denote the sets of prime divisors of λ/μ and $\phi(a'\mathcal{O})$, respectively, and define λ' and μ' as in Section 3C; we note that by construction $\mathfrak{q}$ is relatively prime to λ'. So, we can apply Theorem 3.7 which yields a $\mathbb{Q}$-split principal prime ideal $\mathfrak{p} = \pi\mathcal{O}$

so that $v_{\mathfrak{p}} \notin V(\phi(a'\mathcal{O}))$ and conditions (1) - (3) are satisfied. Let $s = \ell_{\mathfrak{p}}(u)$ be the $\mathfrak{p}$-level of u. Condition (3) implies that

$$\gcd(\phi(\mathfrak{p})/\lambda, \lambda'/\lambda) = 1 = \gcd(\phi(\mathfrak{p})/\lambda, \phi(a'\mathcal{O}))$$

since λ'/λ is the product of all prime divisors of $\phi(a'\mathcal{O})$. It follows that the numbers $\phi(\mathfrak{p}^s)/\lambda$ and $\phi(a'\mathcal{O})$ are relatively prime, and therefore one can pick a positive integer m so that

$$m \equiv 0 \pmod{\phi(\mathfrak{p}^s)/\lambda} \quad \text{and} \quad m \equiv 1 \pmod{\phi(a'\mathcal{O})}.$$

Fix this m for the rest of the proof.

Condition (2) of Theorem 3.7 enables us to apply Corollary 4.2 with $z = \pi$ and $t_0 = s$ to find $t \geq s$ so that $(a', q^{\mu m}) \xRightarrow{1} (\pi^t, q^{\mu m})$. Since P consists of all prime divisors of λ/μ, condition (1) of Theorem 3.7 implies that λ/μ divides the order of $u \pmod{\mathfrak{p}}$. Now, applying Lemma 4.5 with $\delta = \mu$ and $b = q^{\mu}$, we see that $(\pi^t, q^{\mu m}) \xRightarrow{1} (\pi^t, u^{n_t})$ for some integer n_t. Finally, since u is a unit, we have $(\pi^t, u^{n_t}) \xRightarrow{2} (1, 0)$. Combining these computations with (22), we obtain (21), completing the proof. □

Corollary 4.6. *Assume that the group $\mathcal{O}^\times$ is infinite. Then for $n \geq 2$, any matrix $A \in \mathrm{SL}_n(\mathcal{O})$ is a product of $\leq \frac{1}{2}(3n^2 - n) + 4$ elementary matrices.*

Proof. For $n = 2$, this is equivalent to Theorem 1.1. Now, let $n \geq 3$. Since the ring $\mathcal{O}$ is Dedekind, it is well-known and easy to show that any $A \in \mathrm{SL}_n(\mathcal{O})$ can be reduced to a matrix in $\mathrm{SL}_2(\mathcal{O})$ by at most $\frac{1}{2}(3n^2 - n) - 5$ elementary operations [Carter and Keller 1983, p. 683]. Now, our result immediately follows from Theorem 1.1. □

Proof of Corollary 1.2. Let

$$e_+ : \alpha \mapsto \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad e_- : \alpha \mapsto \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$$

be the standard 1-parameter subgroups. Set $U^{\pm} = e_{\pm}(\mathcal{O})$. In view of Theorem 1.1, it is enough to show that each of the subgroups U^+ and U^- is contained in a product of finitely many cyclic subgroups of $\mathrm{SL}_2(\mathcal{O})$. Let h_k be the class number of k. Then there exists $t \in \mathcal{O}^\times$ such that $v(t) = h_k$ for all $v \in S \setminus V_\infty^k$ and $v(t) = 0$ for all $v \notin S$. Then $\mathcal{O} = \mathcal{O}_k[1/t]$. So, letting $U_0^{\pm} = e_{\pm}(\mathcal{O}_k)$ and $h = \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$, we will have the inclusion

$$U^{\pm} \subset \langle h \rangle U_0^{\pm} \langle h \rangle.$$

On the other hand, if $w_1, \ldots, w_n$ (where $n = [k : \mathbb{Q}]$) is a $\mathbb{Z}$-basis of $\mathcal{O}_k$ then $U_0^{\pm} = \langle e_{\pm}(w_1) \rangle \cdots \langle e_{\pm}(w_n) \rangle$, hence

$$U^{\pm} \subset \langle h \rangle \langle e_{\pm}(w_1) \rangle \cdots \langle e_{\pm}(w_n) \rangle \langle h \rangle, \tag{23}$$

as required. □

Remarks. (1) Quantitatively, it follows from the proof of Theorem 1.1 that $\mathrm{SL}_2(\mathcal{O}) = U^- U^+ \cdots U^-$ (nine factors), so since the right-hand side of (23) involves $n + 2$ cyclic subgroups, with $\langle h \rangle$ at both ends, we obtain that $\mathrm{SL}_2(\mathcal{O})$ is a product of $9[k:\mathbb{Q}]+10$ cyclic subgroups. Also, it follows from [Vsemirnov 2014] that $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is a product of 11 cyclic subgroups.

(2) If $S = V_\infty^k$, then the proof of Corollary 1.2 yields a factorization of $\mathrm{SL}_2(\mathcal{O})$ as a finite product $\langle\gamma_1\rangle\cdots\langle\gamma_d\rangle$ of cyclic subgroups where all generators γ_i are elementary matrices, hence *unipotent*. On the contrary, when $S \neq V_\infty^k$, the factorization we produce involves some diagonal (*semisimple*) matrices. So, it is worth pointing out in the latter case there is no factorization with all γ_i unipotent. Indeed, let $v \in S \setminus V_\infty^k$ and let $\gamma \in \mathrm{SL}_2(\mathcal{O})$ be unipotent. Then there exists $N = N(\gamma)$ such that for any $a = (a_{ij}) \in \langle\gamma\rangle$ we have $v(a_{ij}) \leq N(\gamma)$ for all $i, j \in \{1, 2\}$. It follows that if $\mathrm{SL}_2(\mathcal{O}) = \langle\gamma_1\rangle\cdots\langle\gamma_d\rangle$ where all γ_i are unipotent, then there exists N_0 such that for any $a = (a_{ij}) \in \mathrm{SL}_2(\mathcal{O})$ we have $v(a_{ij}) \leq N_0$ for $i, j \in \{1, 2\}$, which is absurd.

5. Example

For a ring of S-integers $\mathcal{O}$ in a number field k such that the group of units $\mathcal{O}^\times$ is infinite, we let $\nu(\mathcal{O})$ denote the smallest positive integer with the property that every matrix in $\mathrm{SL}_2(\mathcal{O})$ is a product of $\leq \nu(\mathcal{O})$ elementary matrices. So, the result of [Vsemirnov 2014] implies that $\nu(\mathbb{Z}[1/p]) \leq 5$ for any prime p, and our Theorem 1.1 yields that $\nu(\mathcal{O}) \leq 9$ for any $\mathcal{O}$ as above. It may be of some interest to determine the exact value of $\nu(\mathcal{O})$ in some situations. In Example 2.1 on p.289, Vsemirnov [2014] claims that the matrix

$$M = \begin{pmatrix} 5 & 12 \\ 12 & 29 \end{pmatrix}$$

is not a product of four elementary matrices in $\mathrm{SL}_2(\mathbb{Z}[1/p])$ for any $p \equiv 1 \pmod{29}$, and therefore $\nu(\mathbb{Z}[1/p]) = 5$ in this case. However this example is faulty because for any prime p, in $\mathrm{SL}_2(\mathbb{Z}[1/p])$ we have

$$M = \begin{pmatrix} 5 & 12 \\ 12 & 29 \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\right)^2$$

However, it turns out that the assertion that $\nu(\mathbb{Z}[1/p]) = 5$ is valid not only for $p \equiv 1 \pmod{29}$ but in fact for all $p > 7$. More precisely, we have the following.

Proposition 5.1. *Let $\mathcal{O} = \mathbb{Z}[1/p]$, where p is prime > 7. Then not every matrix in $\mathrm{SL}_2(\mathcal{O})$ is a product of four elementary matrices.*

In the remainder of this section, unless stated otherwise, we will work with congruences over the ring $\mathcal{O}$ rather than $\mathbb{Z}$, so the notation $a \equiv b \pmod{n}$ means that elements $a, b \in \mathcal{O}$ are congruent modulo the ideal $n\mathcal{O}$. We begin the proof of the proposition with the following lemma.

Lemma 5.2. *Let $\mathcal{O} = \mathbb{Z}[1/p]$, where p is any prime, and let r be a positive integer satisfying $p \equiv 1 \pmod{r}$. Then any matrix $A \in \mathrm{SL}_2(\mathcal{O})$ of the form*

$$A = \begin{pmatrix} 1-p^\alpha & * \\ * & 1-p^\beta \end{pmatrix}, \quad \alpha, \beta \in \mathbb{Z} \tag{24}$$

which is a product of four elementary matrices, satisfies the congruence

$$A \equiv \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \pmod{r}.$$

Proof. The required congruence is obvious for the diagonal entries, so we only need to establish it for the off-diagonal ones. Since A is a product of four elementary matrices, it admits one of the following presentations:

$$A = E_{12}(a)E_{21}(b)E_{12}(c)E_{21}(d), \tag{25}$$

or

$$A = E_{21}(a)E_{12}(b)E_{21}(c)E_{12}(d), \tag{26}$$

with $a, b, c, d \in \mathcal{O}$.

First, suppose we have (25). Then

$$A = \begin{pmatrix} * & * \\ * & 1+bc \end{pmatrix}.$$

Comparing with (24), we get $bc = -p^{\beta}$, so b and c are powers of p with opposite signs. Thus, A looks as follows:

$$A = E_{12}(a)E_{21}(\pm p^{\gamma})E_{12}(\mp p^{\delta})E_{21}(d) = \begin{pmatrix} * & a(1-p^{\gamma+\delta})\mp p^{\delta} \\ d(1-p^{\gamma+\delta})\pm p^{\gamma} & * \end{pmatrix}.$$

Consequently, the required congruences for the off-diagonal entries immediately follow from the fact that $p \equiv 1 \pmod{r}$, proving the lemma in this case.

Now, suppose we have (26). Then

$$A^{-1} = E_{12}(-d)E_{21}(-c)E_{12}(-b)E_{21}(-a),$$

which means that A^{-1} has a presentation of the form (25). Since the required congruence in this case has already been established, we conclude that

$$A^{-1} \equiv \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \pmod{r}.$$

But then we have

$$A \equiv \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \pmod{r},$$

as required. □

To prove the proposition, we will consider two cases:

CASE 1: *$p-2$ is composite.* Write $p-2 = r_1 \cdot r_2$, where r_1 and r_2 are positive integers > 1, and set $r = p-1$. Then

$$r_i \not\equiv \pm 1 \pmod{r} \quad \text{for } i = 1, 2. \tag{27}$$

Indeed, we can assume that $r_2 \leq \sqrt{p-2}$. If $r_2 \equiv \pm 1 \pmod{r}$ then because r is prime to p, the number $r_2 \mp 1$ would be a nonzero integral multiple of r. Then $r \leq r_2 + 1$, hence

$$p-2 \leq \sqrt{p-2}+1.$$

But this is impossible since $p > 3$. Thus, $r_2 \not\equiv \pm 1 \pmod{r}$. Since $r_1 \cdot r_2 \equiv -1 \pmod{r}$, condition (27) follows.

Now, consider the matrix

$$A = \begin{pmatrix} 1-p & r_1 \cdot p \\ r_2 & 1-p \end{pmatrix}$$

One immediately checks that $A \in \mathrm{SL}_2(\mathcal{O})$. At the same time, A is of the form (24). Then Lemma 5.2 in conjunction with (27) implies that A is not a product of four elementary matrices.

CASE 2. *p and $p-2$ are both primes.* In the beginning of this paragraph we will use congruences in $\mathbb{Z}$. Clearly, a prime > 3 can only be congruent to $\pm 1 \pmod{6\mathbb{Z}}$. Since $p > 5$ and $p-2$ is also prime, in our situation we must have $p \equiv 1 \pmod{6\mathbb{Z}}$. Furthermore, since $p > 7$, the congruence $p \equiv 0$ or $2 \pmod{5\mathbb{Z}}$ is impossible. Thus, in the case at hand we have

$$p \equiv 1,\ 13, \text{ or } 19 \pmod{30\mathbb{Z}}.$$

If $p \equiv 13 \pmod{30\mathbb{Z}}$, then $p^3 \equiv 7 \pmod{30\mathbb{Z}}$, and therefore $p^3 - 2$ is an integral multiple of 5. Set $r = p-1$ and $s = (p^3-2)/5$, and consider the matrix

$$A = \begin{pmatrix} 1-p^3 & 5p^3 \\ s & 1-p^3 \end{pmatrix}$$

Then A is a matrix in $\mathrm{SL}_2(\mathcal{O})$ having form (24). Note that $5p^3 \equiv 5 \pmod{r}$, which is different from $\pm 1 \pmod{r}$ since $r > 6$. Now, it follows from Lemma 5.2 that A is not a product of four elementary matrices.

It remains to treat the case where $p \equiv 1$ or $19 \pmod{30\mathbb{Z}}$. Consider the following matrix:

$$A = \begin{pmatrix} 900 & 53 \cdot 899 \\ 17 & 900 \end{pmatrix},$$

and note that $A \in \mathrm{SL}_2(\mathbb{Z})$ and

$$A^{-1} = \begin{pmatrix} 900 & -53 \cdot 899 \\ -17 & 900 \end{pmatrix}.$$

It suffices to show that neither A nor A^{-1} can be written in the form

$$E_{12}(a)E_{21}(b)E_{12}(c)E_{21}(d) = \begin{pmatrix} * & c + a(1+bc) \\ b + d(1+bc) & (1+bc) \end{pmatrix}, \quad \text{with } a, b, c, d \in \mathcal{O}. \tag{28}$$

Assume that either A or A^{-1} is written in the form (28). Then $1 + bc = 900$, so

$$b, c \in \{\pm p^n, \pm 29p^n, \pm 31p^n, \pm 899p^n \mid n \in \mathbb{Z}\}.$$

Set

$$t = b + d(1+bc) \quad \text{and} \quad u = c + a(1+bc).$$

We have the following congruences in $\mathcal{O} = \mathbb{Z}[1/p]$:

$$t \equiv b \pmod{30} \quad \text{and} \quad u \equiv c \pmod{30}.$$

Analyzing the above list of possibilities for b and c, we conclude that each of t and u is $\equiv \pm p^n \pmod{30}$ for some integer n. Thus, if $p \equiv 1 \pmod{30}$ then $t, u \equiv \pm 1 \pmod{30}$, and if $p \equiv 19 \pmod{30}$ then $t, u \equiv \pm 1, \pm 19 \pmod{30}$. Since $17 \not\equiv \pm 1, \pm 19 \pmod{30}$, we obtain a contradiction in either case. (We observe that the argument in this last case is inspired by Vsemirnov's argument in his Example 2.1.)

Acknowledgements

During the preparation of the final version of the paper the second author visited Princeton University and the Institute for Advanced Study on a Simons Fellowship. The hospitality of both institutions and the generous support of the Simons Foundation are thankfully acknowledged. The third author gratefully acknowledges fruitful conversations with Maxim Vsemirnov. We thank Dong Quan Ngoc Nguyen for his comments regarding Theorem 3.3. Our most sincere thanks are due to the anonymous referee who has read the paper extremely carefully and offered a number of corrections and valuable suggestions.

References

[Bass et al. 1967] H. Bass, J. Milnor, and J.-P. Serre, "Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)", *Inst. Hautes Études Sci. Publ. Math.* 33 (1967), 59–137. MR Zbl

[Carter and Keller 1983] D. Carter and G. Keller, "Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$", *Amer. J. Math.* **105**:3 (1983), 673–687. MR Zbl

[Carter and Keller 1984] D. Carter and G. Keller, "Elementary expressions for unimodular matrices", *Comm. Algebra* **12**:3-4 (1984), 379–389. MR Zbl

[Cassels and Fröhlich 1967] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory*, Academic Press, Washington D.C., 1967. MR Zbl

[Cohn 1966] P. M. Cohn, "On the structure of the GL_2 of a ring", *Inst. Hautes Études Sci. Publ. Math.* 30 (1966), 5–53. MR Zbl

[Cooke and Weinberger 1975] G. Cooke and P. J. Weinberger, "On the construction of division chains in algebraic number rings, with applications to SL_2", *Comm. Algebra* **3** (1975), 481–524. MR Zbl

[Erovenko and Rapinchuk 2006] I. V. Erovenko and A. S. Rapinchuk, "Bounded generation of S-arithmetic subgroups of isotropic orthogonal groups over number fields", *J. Number Theory* **119**:1 (2006), 28–48. MR Zbl

[Grunewald and Schwermer 1981] F. J. Grunewald and J. Schwermer, "Free nonabelian quotients of SL_2 over orders of imaginary quadratic numberfields", *J. Algebra* **69**:2 (1981), 298–304. MR Zbl

[Hasse 1926] H. Hasse, "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I: Klassenkörpertheorie", *Jahresber. Dtsch. Math.-Ver.* **35** (1926), 1–55. Zbl

[Heath-Brown 1986] D. R. Heath-Brown, "Artin's conjecture for primitive roots", *Quart. J. Math. Oxford Ser.* (2) **37**:145 (1986), 27–38. MR Zbl

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR Zbl

[Liehl 1981] B. Liehl, "On the group SL_2 over orders of arithmetic type", *J. Reine Angew. Math.* **323** (1981), 153–171. MR Zbl

[Liehl 1984] B. Liehl, "Beschränkte Wortlänge in SL_2", *Math. Z.* **186**:4 (1984), 509–524. MR Zbl

[Loukanidis and Murty 1994] D. Loukanidis and V. Murty, "Bounded generation for SL_n ($n \geq 2$) and Sp_{2n} ($n \geq 1$)", preprint, 1994.

[Lubotzky 1995] A. Lubotzky, "Subgroup growth and congruence subgroups", *Invent. Math.* **119**:2 (1995), 267–295. MR Zbl

[Morris 2007] D. W. Morris, "Bounded generation of $\mathrm{SL}(n, A)$ (after D. Carter, G. Keller, and E. Paige)", *New York J. Math.* **13** (2007), 383–421. MR Zbl

[Murty 1995] V. K. Murty, "Bounded and finite generation of arithmetic groups", pp. 249–261 in *Number theory* (Halifax, NS, 1994), edited by K. Dilcher, CMS Conf. Proc. **15**, Amer. Math. Soc., Providence, RI, 1995. MR Zbl

[Platonov and Rapinchuk 1992] V. P. Platonov and A. S. Rapinchuk, "Abstract properties of S-arithmetic groups and the congruence problem", *Izv. Ross. Akad. Nauk Ser. Mat.* **56**:3 (1992), 483–508. In Russian; translated in *Russian Acad. Sci. Izv. Math.* **40**:3 (1993), 455–476. MR Zbl

[Platonov and Rapinchuk 1994] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics **139**, Academic Press, Boston, 1994. MR Zbl

[Rapinchuk 1990] A. S. Rapinchuk, "Representations of groups of finite width", *Dokl. Akad. Nauk SSSR* **315**:3 (1990), 536–540. In Russian; translated in *Soviet Math. Dokl.* **42**:3 (1991), 816–820. MR Zbl

[Serre 1970] J.-P. Serre, "Le problème des groupes de congruence pour SL2", *Ann. of Math.* (2) **92** (1970), 489–527. MR Zbl

[Shalom and Willis 2013] Y. Shalom and G. A. Willis, "Commensurated subgroups of arithmetic groups, totally disconnected groups and adelic rigidity", *Geom. Funct. Anal.* **23**:5 (2013), 1631–1683. MR Zbl

[Tavgen 1990] O. I. Tavgen, "Bounded generability of Chevalley groups over rings of S-integer algebraic numbers", *Izv. Akad. Nauk SSSR Ser. Mat.* **54**:1 (1990), 97–122. In Russian; translated in *Math. USSR-Izv.* **36**:1 (1991), 101–128. MR Zbl

[Vasershtein 1972] L. N. Vasershtein, "The group SL_2 over Dedekind rings of arithmetic type", *Mat. Sb.* (*N.S.*) **89(131)** (1972), 313–322, 351. In Russian; translated in *Mathematics of the USSR-Sbornik* **18**:2 (1972), 321–332. MR

[Vsemirnov 2014] M. Vsemirnov, "Short unitriangular factorizations of $\mathrm{SL}_2(\mathbb{Z}[1/p])$", *Q. J. Math.* **65**:1 (2014), 279–290. MR Zbl

Communicated by Raman Parimala
Received 2017-09-03 Revised 2018-05-10 Accepted 2018-06-18

avo2t@virginia.edu Department of Mathematics, University of Virginia, Charlottesville, VA, United States

asr3x@virginia.edu Department of Mathematics, University of Virginia, Charlottesville, VA, United States

surybang@gmail.com Stat-Math Unit, Indian Statistical Institute, Bangalore, India

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2018 is US $340/year for the electronic version, and $535/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Algebra & Number Theory

Volume 12 No. 8 2018

1937-0652(2018)12:8;1-9