Gulf Journal of Mathematics
Vol 21, Issue 1 (2025) 302-318

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v21i1.3334

CHAIN MODULAR UNITS AND EXPLICIT UNIT GROUPS IN RAY CLASS FIELDS OVER IMAGINARY QUADRATIC FIELDS

MOHAMMED EL BARAKA[1*] and SIHAM EZZOUAK[2]

Abstract. We introduce *chain modular units*: products of Siegel functions attached to cyclic chains of ℓ-isogenies between CM elliptic curves of type $\mathcal{O}_f$. We prove that their CM values lie in the ray class field $K_{f\ell^n}$ and that a finite, explicitly constructed family generates, modulo roots of unity, a subgroup of finite index in $\mathcal{O}_{K_{f\ell^n}}^{\times}$. We describe the Galois action via the ideal class action on chains, give effective criteria for multiplicative independence using Baker–Wüstholz bounds, and determine the stable index along the ℓ-power ray class tower. Computations for $D = -7$ and $D = -11$ confirm the theory. The method leverages the combinatorics of isogeny chains to control conductor growth and produce many independent units.

Keywords. Ray class fields; modular units; Siegel functions; isogeny chains; complex multiplication
2020 Mathematics Subject Classification. Primary 11R37; Secondary 11G15, 14K22

1. Introduction

Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field with fundamental discriminant $D < 0$, and fix an order

$$\mathcal{O}_f \;=\; \mathbb{Z} + f\,\mathcal{O}_K \subset \mathcal{O}_K$$

of conductor $f \geq 1$. Denote by K_f the ring class field of conductor f, by $\mathrm{Cl}_f(K)$ the corresponding class group, and by $K_{f\ell^n}$ the ray class field of conductor $f\ell^n$ (for a rational prime $\ell \nmid fD$ and $n \geq 1$). Class field theory and the theory of complex multiplication (CM) describe K_f and $K_{f\ell^n}$ as fields generated by special values of modular functions at CM points; see, e.g., Deuring [3], Schertz [15], and Stevenhagen [16].

Much less explicit, however, is the structure of the *unit group* $\mathcal{O}_{K_{f\ell^n}}^{\times}$. While Dirichlet's unit theorem gives its rank, locating a concrete set of generators (or even a finite-index subgroup generated by modular units) is generally hard. Classical constructions (Weber functions, Siegel units, η-quotients) do yield many algebraic units, but controlling their independence and the index they generate inside $\mathcal{O}_{K_{f\ell^n}}^{\times}$ remains delicate; compare, for instance, the work of Kubert–Lang [10].

Date: Received: Jul 29, 2025; Accepted: Aug 19, 2025.
* Corresponding author

Idea of the paper. We introduce a new family of modular units indexed by *cyclic chains of ℓ-isogenies*

$$E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-1}} E_n \xrightarrow{\varphi_n} E_0,$$

where each E_i has CM by an order contained in $\mathcal{O}_K$ and the composite isogeny has degree ℓ^n with cyclic kernel. From such a chain we define a product of Siegel functions (a *chain modular unit*) whose specialization at the CM points $(E_0, \dots, E_n)$ is an algebraic unit in $K_{f\ell^n}$. The key point is that the combinatorial data of the chain encodes conductor growth, allowing us to "aim" exactly at the ray class field and to produce sufficiently many independent units.

Main results. Let $\mathcal{U}_{\ell^n}$ denote the chain modular unit attached to a length-n cyclic ℓ-isogeny chain (see §3 for the precise definition). Our three main theorems are:

Theorem 1.1 (Generation of ray class fields)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field with discriminant $D < 0$, let $\mathcal{O}_f \subset \mathcal{O}_K$ be the order of conductor $f \geq 1$, and let $\ell \nmid fD$ be a prime. Consider a cyclic chain of ℓ-isogenies of length n*

$$E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-1}} E_n \xrightarrow{\varphi_n} E_0$$

between CM elliptic curves with $\mathrm{End}(E_0) \cong \mathcal{O}_f$, and define the chain modular unit $\mathcal{U}_{\ell^n}(E_0, \dots, E_n)$ as in (3.3). Then

$$K\big(\mathcal{U}_{\ell^n}(E_0, \dots, E_n)\big) = K_{f\ell^n},$$

the ray class field of conductor $f\ell^n$ over K. In particular, $\mathcal{U}_{\ell^n}(E_0, \dots, E_n)$ is a primitive generator of $K_{f\ell^n}$ over K up to adjoining roots of unity.

Theorem 1.2 (Degree and Galois action)**.** *With notation as above, the minimal polynomial of $\mathcal{U}_{\ell^n}(E_0, \dots, E_n)$ over K has degree $h_{f\ell^n}$, the ray class number of conductor $f\ell^n$. Moreover, the canonical isomorphism*

$$\mathrm{Gal}\big(K_{f\ell^n}/K\big) \cong \mathrm{Cl}_{f\ell^n}(K)$$

is realized by transporting the ideal class action on CM elliptic curves to the set of ℓ-isogeny chains; this action is faithful on the values of $\mathcal{U}_{\ell^n}$.

Theorem 1.3 (Multiplicative independence)**.** *Let $m \neq n \geq 1$. The invariants $\mathcal{U}_{\ell^m}$ and $\mathcal{U}_{\ell^n}$ are multiplicatively independent modulo $\overline{\mathbb{Q}}^\times$, except for a finite, explicitly describable exceptional set of tuples (K, ℓ, m, n) determined by w_K and local conditions at ℓ. Consequently, for a suitable finite set $\mathcal{S}_{f,\ell,n}$ of chain units,*

$$\mathrm{rank}_{\mathbb{Z}}\left(\langle \mathcal{S}_{f,\ell,n} \rangle / \mu(K_{f\ell^n})\right) = \mathrm{rank}_{\mathbb{Z}}\big(\mathcal{O}^\times_{K_{f\ell^n}}\big).$$

The proofs combine: (i) the action of the ray class group $\mathrm{Cl}_{f\ell^n}(K)$ on CM elliptic curves and on ℓ-isogeny chains (Kohel's volcano formalism [9], Fouquet–Morain [5]); (ii) integrality and transformation laws for Siegel functions ([10]); (iii) Baker's method on linear forms in logarithms for transcendence/independence (Baker–Wüstholz [1]).

Novelty. To our knowledge, no previous work has:

(1) indexed modular units by *isogeny chains* so as to encode conductor escalation and obtain a controlled supply of units in $K_{f\ell^n}$,
(2) proved that these units generate (up to torsion) a finite-index subgroup of $\mathcal{O}^\times_{K_{f\ell^n}}$,
(3) quantified the index and its stabilization along the ℓ-power ray class tower.

This goes beyond classical Weber–Siegel constructions, where independence issues are usually handled indirectly and without the combinatorial leverage provided by ℓ-isogeny graphs.

Structure of the paper. Section 2 recalls CM, ray class fields, Siegel functions, and the volcano structure of ℓ-isogenies. In Section 3 we define the chain modular units and prove they specialize to algebraic units in $K_{f\ell^n}$. Theorem A is proved in Section 4, via a determinant/non-vanishing argument. Section 5 contains the independence proof (Theorem B), relying on Baker's theory. Section 6 establishes Theorem C for towers. Explicit examples (minimal polynomials, regulators) are given in Section 7.

Related work in isogeny algorithms and PQC.. Recent work by El Baraka and Ezzouak develops algorithmic facets of isogeny-based cryptography: optimized pipelines for computing isogenies in post-quantum settings [18], quantum-resistant modifications of ECDSA for blockchain security [19], and efficient isogeny algorithms on hyperelliptic curves with applications to PQC [20]. Our arithmetic results are complementary: instead of performance optimizations, we construct and control explicit units in ray class fields via isogeny chains and Siegel units. The common structural theme—exploiting isogeny graphs and controlled conductor growth—suggests fruitful interactions between explicit CM theory and post-quantum protocol design.

Throughout, $\mu(L)$ denotes the roots of unity in a number field L, $w_K = |\mu(K)|$, and $\mathfrak{H}$ is the upper half-plane. We adhere to the notation of [15, 16] for CM fields and ray class groups, and of [10] for Siegel functions.

2. Preliminaries

In this section we collect the arithmetic and analytic background needed in the sequel. Throughout, $K = \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field with fundamental discriminant $D < 0$, $\mathcal{O}_K$ its maximal order, and $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ the order of conductor $f \geq 1$. A rational prime $\ell \nmid fD$ and an integer $n \geq 1$ are fixed.

2.1. Quadratic orders, ray class groups and conductors.

Let $\mathfrak{m} = f\ell^n\mathcal{O}_K$ be the (finite) modulus we consider. The ray class group modulo $\mathfrak{m}$ is

$$\mathrm{Cl}_{\mathfrak{m}}(K) \;=\; \frac{\{\text{fractional ideals prime to } \mathfrak{m}\}}{\{\alpha\mathcal{O}_K :\ \alpha \equiv 1 \pmod{\mathfrak{m}}\}},$$

and the corresponding abelian extension $K_{\mathfrak{m}}/K$ is the ray class field. We abbreviate $\mathrm{Cl}_{f\ell^n}(K) := \mathrm{Cl}_{\mathfrak{m}}(K)$ and $K_{f\ell^n} := K_{\mathfrak{m}}$.

Let $h_f := |\mathrm{Cl}(\mathcal{O}_f)|$ be the class number of $\mathcal{O}_f$, and $h_{f\ell^n} := |\mathrm{Cl}_{f\ell^n}(K)|$ the ray class number. The analytic class number formula yields

$$h_{f\ell^n} = \frac{2^{r_1}(2\pi)^{r_2} R_{f\ell^n}}{w_K\sqrt{|D|}}\,\mathrm{Res}_{s=1}\zeta_{K_{f\ell^n}}(s), \tag{2.1}$$

where $r_1 = 0$, $r_2 = [K_{f\ell^n} : \mathbb{Q}]/2$, $R_{f\ell^n}$ is the regulator of $K_{f\ell^n}$, $w_K = |\mu(K)|$, and $\zeta_{K_{f\ell^n}}$ is the Dedekind zeta function. We will only need the existence of $R_{f\ell^n}$ and its positivity.

2.2. **CM elliptic curves and ideal class action.** Let $\tau \in \mathfrak{H}$ and $E_\tau := \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$. Then $\mathrm{End}(E_\tau) \cong \mathcal{O}_f$ if and only if τ is a root of a primitive positive definite binary quadratic form of discriminant $f^2 D$ (see [2, 15]). The main theorem of complex multiplication asserts that

$$K(j(\tau)) = K_f, \qquad \text{and} \qquad K_f/K \text{ is abelian with Galois group } \mathrm{Cl}(\mathcal{O}_f).$$

More generally, if F is a modular function of level dividing N and integral over $\mathbb{Z}[j]$, then $F(\tau)$ is algebraic and lies in an abelian extension whose conductor divides fN (Shimura reciprocity; cf. [16, 15]).

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_f$ prime to ℓ. The ideal class $[\mathfrak{a}]$ acts on CM elliptic curves by

$$[\mathfrak{a}] \cdot E_\tau := E_{\tau'} \quad \text{with} \quad \mathrm{End}(E_{\tau'}) \cong \mathcal{O}_f, \quad \text{and } j(\tau') = \Phi_{\mathfrak{a}}(j(\tau)),$$

where $\Phi_{\mathfrak{a}}$ is the classical modular polynomial associated to $\mathfrak{a}$. This action extends to chains of isogenies by transporting kernels.

2.3. **Siegel functions and modular units.** For $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, the Siegel function $g_{\mathbf{a}}(\tau)$ is defined by

$$g_{\mathbf{a}}(\tau) = -e^{\pi i a_2 (a_1 - 1)}\, q^{\frac{1}{2} B_2(a_1)} \prod_{m=0}^{\infty} \big(1 - q^{m+a_1} e^{2\pi i a_2}\big)\big(1 - q^{m+1-a_1} e^{-2\pi i a_2}\big), \tag{2.2}$$

with $q = e^{2\pi i \tau}$ and $B_2(x) = x^2 - x + \frac{1}{6}$. The fundamental properties (see [10, 12]) we shall use are:

(1) *Modularity.* $g_{\mathbf{a}}$ is a modular function of weight 0 for a congruence subgroup contained in $\Gamma(N)$, where N is the denominator of $\mathbf{a}$.
(2) *Unit property.* $g_{\mathbf{a}}$ is a modular *unit*: its zeros and poles are supported only at cusps of $X(N)$.
(3) *Transformation law.* For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$g_{\mathbf{a}}(\gamma\tau) = \epsilon(\gamma, \mathbf{a})\, (c\tau + d)^{1/2} g_{\mathbf{a}\gamma}(\tau),$$

where $\epsilon(\gamma, \mathbf{a})$ is a certain 24-th root of unity explicitly known, and $\mathbf{a}\gamma$ is the usual right action of $\mathrm{SL}_2(\mathbb{Z})$ on row vectors.
(4) *Divisor at cusps.* The order of $g_{\mathbf{a}}$ at a cusp corresponds to $\frac{1}{2} B_2(a_1)$, allowing us to compute divisors of products of Siegel functions via Bernoulli polynomials.

A product $\prod_j g_{\mathbf{a}_j}^{\alpha_j}$ is again a modular unit if the set $\{\mathbf{a}_j\}$ and the integers $\{\alpha_j\}$ satisfy the two classical congruence conditions (cancellation of characteristics and Bernoulli sums). We will impose these to build our chain units.

2.4. **$\Gamma_0(\ell^n)$, cusps, and integrality.** Let $X_0(\ell^n)$ be the (compactified) modular curve attached to $\Gamma_0(\ell^n)$. Its cusps correspond to pairs $(c : d)$ with $c \mid \ell^n$, $\gcd(c, d) = 1$, modulo the action of $\Gamma_0(\ell^n)$. The width of each cusp is explicit. A modular unit U on $X_0(\ell^n)$ has a divisor supported on these cusps:

$$\mathrm{div}_{X_0(\ell^n)}(U) = \sum_{\text{cusps } P} \mathrm{ord}_P(U) \cdot P.$$

If U is integral over $\mathbb{Z}[j]$, then the specialization $U(\tau)$ at a CM point is an algebraic integer. Since U has no zeros/poles on CM points, $U(\tau)$ is an algebraic unit. We will build U as a product of Siegel units where these cusp orders cancel.

2.5. **ℓ-isogeny graphs and volcanoes.** Fix a prime ℓ. Consider the graph $\mathcal{G}_\ell$ whose vertices are isomorphism classes of CM elliptic curves with endomorphism ring containing $\mathcal{O}_f$, and edges are cyclic ℓ-isogenies. Kohel [9] and Fouquet–Morain [5] showed that $\mathcal{G}_\ell$ has a *volcano* structure: a "crater" (top level) where the endomorphism ring is maximal at ℓ, and successive lower levels where the conductor increases by factors of ℓ.

A *cyclic chain* of length n is a closed walk of length n in $\mathcal{G}_\ell$ without backtracking. Such a chain can be viewed as a path in the volcano whose beginning and end have the same endomorphism ring. The degree of the composed isogeny is ℓ^n.

Key facts we need:

Lemma 2.1. *Let $E_0 \to E_1 \to \cdots \to E_n \to E_0$ be a cyclic chain. Then the conductor of $\mathrm{End}(E_k)$ differs from f by at most a power of ℓ. More precisely, there is an integer $0 \le s_k \le n$ such that $\mathrm{End}(E_k) \cong \mathcal{O}_{f\ell^{s_k}}$ and $\max_k s_k = n$ if the chain is geodesic.*

Proof. Standard volcano theory: an ℓ-isogeny either stays on the same level (horizontal) or moves one level down (ascending/descending depending on direction) by multiplying/dividing the conductor by ℓ. Along a geodesic cycle of length n, one must descend exactly n times and ascend n times to return, whence the bound. □

2.6. **Logarithmic embeddings and regulators.** Let L be a number field with r_1 real and r_2 pairs of complex embeddings. The (absolute) logarithmic embedding is

$$\lambda : L^\times \longrightarrow \mathbb{R}^{r_1+r_2}, \qquad \alpha \mapsto \big(\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1+r_2}(\alpha)|\big),$$

where for complex σ, we take one representative in each pair and multiply the coordinate by 2. The image of $L^\times/\mu(L)$ is a lattice of rank $r_1 + r_2 - 1$, and the regulator R_L is the covolume of this lattice.

In our setting, $L = K_{f\ell^n}$ is CM, so $r_1 = 0$, $r_2 = [L : \mathbb{Q}]/2$, and

$$\operatorname{rank} \mathcal{O}_L^\times = r_2 - 1.$$

If $U_1, \dots, U_t$ are units, set $M = (\log|\sigma_j(U_i)|)_{1\le i\le t,\ 1\le j\le r_2}$; any $(t \times t)$ minor with full rank gives a non-zero determinant if the U_i are independent. This criterion, together with Baker's theorem, will be used to prove independence.

The objects just defined will be used as follows. We will build for each chain a modular unit $\mathcal{U}_{\ell^n}$ (Section 3); Proposition 3.8 will assert that $\mathcal{U}_{\ell^n}$ is an algebraic unit in $K_{f\ell^n}$. Then, by choosing a suitable family of chains and applying the logarithmic embedding, we prove Theorems 1.1–1.3.

3. Construction of the chain modular units

We now define the modular units $\mathcal{U}_{\ell^n}$ attached to cyclic ℓ-isogeny chains and prove that they are well defined (independent of auxiliary choices), modular for $\Gamma_0(\ell^n)$, and specialize to algebraic units in $K_{f\ell^n}$.

3.1. **Chains, orientations, and level structure.** Fix a prime $\ell \nmid fD$ and an integer $n \ge 1$. A *(cyclic) ℓ-isogeny chain of length n* is a tuple

$$\gamma : \quad E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-1}} E_n \xrightarrow{\varphi_n} E_0, \tag{3.1}$$

where each φ_k is a cyclic ℓ-isogeny and the composite $\Phi_\gamma := \varphi_n \circ \cdots \circ \varphi_0$ has kernel of order ℓ^n. We call γ *geodesic* if it contains no backtracking edge in the ℓ-isogeny graph $\mathcal{G}_\ell$ (cf. Lemma 2.1).

Choose a period matrix $\tau_k \in \mathfrak{H}$ with $E_k \simeq \mathbb{C}/(\mathbb{Z} + \tau_k\mathbb{Z})$. The isogeny φ_k is represented (up to isomorphism) by a cyclic subgroup $C_k \subset E_k[\ell]$. Fixing a basis of $E_k[\ell^n]$

containing a generator of C_k allows us to define rational characteristics $\mathbf{a}_{k,j}, \mathbf{b}_{k,j} \in \frac{1}{\ell^n}\mathbb{Z}^2$ that encode the kernels we "kill" or "keep" in the product of Siegel functions.

Definition 3.1 (Local factors)**.** For each step $\varphi_k : E_k \to E_{k+1}$ we choose a finite list of pairs

$$\big(\mathbf{a}_{k,j}, \alpha_{k,j}\big), \quad \big(\mathbf{b}_{k,j}, \beta_{k,j}\big) \qquad (1 \le j \le m_k)$$

with $\mathbf{a}_{k,j}, \mathbf{b}_{k,j} \in (\ell^{-n}\mathbb{Z})^2 \setminus \mathbb{Z}^2$ and $\alpha_{k,j}, \beta_{k,j} \in \mathbb{Z}$, satisfying the congruence conditions (3.4)–(3.5) below. The *local unit* associated to φ_k is

$$u_k(\tau_k) \;:=\; \prod_{j=1}^{m_k} \frac{g_{\mathbf{a}_{k,j}}(\tau_k)^{\alpha_{k,j}}}{g_{\mathbf{b}_{k,j}}(\tau_k)^{\beta_{k,j}}}. \tag{3.2}$$

The global *chain modular unit* is then

$$\mathcal{U}_{\ell^n}(\gamma) \;:=\; \prod_{k=0}^{n-1} u_k(\tau_k). \tag{3.3}$$

We now spell out the conditions ensuring that (i) u_k is a modular unit on $X_0(\ell^n)$; (ii) $\mathcal{U}_{\ell^n}(\gamma)$ is independent of the representative periods/bases; (iii) specialization at CM chains produces algebraic units.

3.2. **Cuspidal cancellation and modularity.** Let $N = \ell^n$. Recall (Subsection 2.3) that any product of Siegel functions is a modular unit for $\Gamma(N)$ if two linear congruences are satisfied.

For a finite set $\{\mathbf{v}_i\} \subset (\frac{1}{N}\mathbb{Z})^2$ with integer multiplicities c_i, define

$$\mathbf{V} := \sum_i c_i \mathbf{v}_i \in (\tfrac{1}{N}\mathbb{Z})^2, \qquad B_2(\mathbf{v}_i) := B_2\big((\mathbf{v}_i)_1\big).$$

The classical conditions ([10], Chap. 1) read:

$$\sum_i c_i \mathbf{v}_i \in \mathbb{Z}^2, \tag{3.4}$$

$$\sum_i c_i B_2((\mathbf{v}_i)_1) = 0. \tag{3.5}$$

When (3.4)–(3.5) hold, $U(\tau) = \prod_i g_{\mathbf{v}_i}(\tau)^{c_i}$ is modular for $\Gamma(N)$ and has divisor supported on cusps.

Lemma 3.2 (Lifting to $\Gamma_0(N)$)**.** *Let U be a modular unit for $\Gamma(N)$. Then there exists $M \ge 1$ such that U^M is modular for $\Gamma_0(N)$. Explicitly, one can take M to be the least common multiple of the denominators of the nebentypus multipliers $\epsilon(\gamma, \mathbf{v}_i)$ in the transformation law of $g_{\mathbf{v}_i}$ under $\Gamma_0(N)$.*

Proof. Use the transformation law (S3) and that $\Gamma_0(N)$ normalizes $\Gamma(N)$. The scarcity of possible ϵ (bounded by 24-th roots of unity) ensures a finite exponent kills all characters. □

We impose (3.4)–(3.5) separately for each u_k (hence for $\mathcal{U}_{\ell^n}$). This guarantees cuspidal cancellation stepwise.

3.3. **Existence of suitable characteristics.** We must show that for each φ_k one can pick the data in Definition 3.1 so that: (i) (3.4)–(3.5) hold; (ii) the resulting unit encodes the kernel of φ_k and is compatible with the chain structure.

Let $C_k \subset E_k[\ell]$ be the kernel of φ_k. Any basis of $E_k[\ell^n]$ gives a surjective map

$$\theta_k : \ (\tfrac{1}{\ell^n}\mathbb{Z})^2/\mathbb{Z}^2 \longrightarrow E_k[\ell^n].$$

We choose $\{\mathbf{a}_{k,j}\}$ mapping to generators of C_k and $\{\mathbf{b}_{k,j}\}$ mapping to a complementary set so that $\sum_j \alpha_{k,j}\theta_k(\mathbf{a}_{k,j}) = 0$ in $E_k[\ell^n]$ and similarly for $\mathbf{b}_{k,j}$; this forces (3.4). The Bernoulli condition (3.5) is a linear constraint in the $\alpha_{k,j}, \beta_{k,j}$; as soon as we have more variables than equations (which we do), a non-trivial integer solution exists.

Proposition 3.3 (Non-emptiness of the solution set)**.** *For each step φ_k, there exists a choice of data $(\mathbf{a}_{k,j}, \alpha_{k,j})$, $(\mathbf{b}_{k,j}, \beta_{k,j})$ satisfying (3.4)–(3.5). Moreover, we may choose them so that u_k is invariant under $\Gamma_0(\ell^n)$ up to a 24-th root of unity.*

Proof. Linear algebra over $\mathbb{Z}$: the constraints (3.4)–(3.5) form a system of two independent equations in $\sum m_k$ unknown integers; choose $m_k \geq 3$. The invariance statement follows from Lemma 3.2. □

3.4. **Independence of auxiliary choices.** Two issues arise: choice of representatives τ_k and choice of bases in $E_k[\ell^n]$.

Lemma 3.4 (Change of representatives)**.** *Let τ_k, τ_k' represent the same elliptic curve E_k. Then $u_k(\tau_k')/u_k(\tau_k)$ is a root of unity of order dividing $24M$ (with M from Lemma 3.2). Hence $\mathcal{U}_{\ell^n}(\gamma)$ is well-defined up to $\mu(\mathbb{C})$.*

Proof. Replacing τ_k by $\gamma \cdot \tau_k$ multiplies each $g_{\mathbf{v}}$ by $\epsilon(\gamma, \mathbf{v})(c\tau_k + d)^{1/2}$; the $(c\tau_k + d)^{1/2}$ cancel by (3.4)–(3.5); the remaining product of ϵ is a bounded root of unity. □

Lemma 3.5 (Change of basis)**.** *If we change the chosen basis of $E_k[\ell^n]$, the set of characteristics $\{\mathbf{a}_{k,j}, \mathbf{b}_{k,j}\}$ is acted upon by $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, which preserves (3.4)–(3.5). The resulting u_k changes by a root of unity.*

Proof. The action of $\mathrm{SL}_2(\mathbb{Z})$ on characteristics induces a permutation on $(\frac{1}{\ell^n}\mathbb{Z})^2/\mathbb{Z}^2$; the two congruence conditions are invariant, and the multiplier system is bounded. □

Combining Lemmas 3.4 and 3.5, we obtain:

Proposition 3.6 (Well-definedness)**.** *The class of $\mathcal{U}_{\ell^n}(\gamma)$ in the multiplicative group of modular functions on $X_0(\ell^n)$ modulo $\mu(\mathbb{C})$ depends only on the isogeny chain γ, not on auxiliary choices.*

3.5. **CM specialization and unit property.** We now evaluate $\mathcal{U}_{\ell^n}(\gamma)$ at CM chains of type $\mathcal{O}_f$.

Proposition 3.7 (CM values lie in $K_{f\ell^n}$)**.** *Let γ be a chain as in (3.1) with E_0 of CM type $\mathcal{O}_f$. Then $\mathcal{U}_{\ell^n}(\gamma)$ belongs to $K_{f\ell^n}$.*

Proof. Each u_k is a modular unit of level dividing ℓ^n and integral over $\mathbb{Z}[j]$. By Shimura reciprocity ([15, 16]), the value $u_k(\tau_k)$ lies in an abelian extension whose conductor divides $f\ell^n$. The product remains in the same field. Since the chain encodes the full ℓ^n-conductor rise (Lemma 2.1), we indeed hit $K_{f\ell^n}$. □

Proposition 3.8 (Algebraic unit)**.** *$\mathcal{U}_{\ell^n}(\gamma)$ is an algebraic unit in $K_{f\ell^n}$.*

Proof. $\mathcal{U}_{\ell^n}$ is a modular unit on $X_0(\ell^n)$; its divisor is supported on cusps. Hence, when specialized at a non-cuspidal point (here, CM points), it yields an algebraic element with neither zeros nor poles, i.e. a unit. Cf. [10]. □

3.6. **Normalization.** To avoid ambiguity of roots of unity, we may fix a normalization:

Definition 3.9 (Normalized chain unit)**.** For each γ, define

$$\widetilde{\mathcal{U}}_{\ell^n}(\gamma) \;:=\; \frac{\mathcal{U}_{\ell^n}(\gamma)}{\prod_{\sigma:K_{f\ell^n}\hookrightarrow\mathbb{C}} \big(\mathcal{U}_{\ell^n}(\gamma)^{1/[K_{f\ell^n}:\mathbb{Q}]}\big)^{\epsilon_\sigma}},$$

where $\epsilon_\sigma \in \{\pm 1\}$ are chosen so that $\widetilde{\mathcal{U}}_{\ell^n}(\gamma)$ has absolute norm 1. Then $\widetilde{\mathcal{U}}_{\ell^n}(\gamma)$ is uniquely defined modulo $\mu(K_{f\ell^n})$.

This normalization will be convenient when comparing logarithmic embeddings (Section 4).

We have thus constructed the objects that will generate the unit group. The next section proves Theorem 1.1 by choosing a large enough family of chains and showing that the corresponding logarithmic matrix has non-zero determinant.

4. Generation of the unit group

In this section we prove Theorem 1.1. We first select a family of cyclic ℓ-isogeny chains whose associated chain modular units have the right cardinality; then we show that their logarithmic embeddings are $\mathbb{Z}$-independent and compare the resulting determinant with the regulator to obtain an explicit index formula.

4.1. **Choosing a spanning family of chains.** Recall that $r := \operatorname{rank}_{\mathbb{Z}}\big(\mathcal{O}_{K_{f\ell^n}}^\times\big) = [K_{f\ell^n}:\mathbb{Q}]/2 - 1$. Let $\mathcal{C}$ be the set of all (geodesic) cyclic ℓ-isogeny chains of length n starting at a fixed base CM elliptic curve E_0 with $\operatorname{End}(E_0) \simeq \mathcal{O}_f$.

The ray class group $\mathrm{Cl}_{f\ell^n}(K)$ acts transitively on the set of CM points of type $\mathcal{O}_f$ on $X_0(\ell^n)$, hence on the set of chains starting at E_0 by transporting kernels (cf. Subsection 2.2). Let

$$\pi:\ \mathrm{Cl}_{f\ell^n}(K) \longrightarrow \mathcal{C}, \qquad [\mathfrak{a}] \mapsto \gamma_{\mathfrak{a}}$$

be any choice of representatives (a "section") of this action. Define

$$U_{\mathfrak{a}} \;:=\; \widetilde{\mathcal{U}}_{\ell^n}(\gamma_{\mathfrak{a}}) \;\in\; K_{f\ell^n}^\times,$$

where the tilde denotes the normalization of Definition 3.9.

Lemma 4.1 (Existence of a small generating set)**.** *There exist classes $\mathfrak{a}_1,\dots,\mathfrak{a}_r \in \mathrm{Cl}_{f\ell^n}(K)$ such that the $r\times r$ logarithmic matrix*

$$M \;=\; \Big(\log|\sigma_j(U_{\mathfrak{a}_i})|\Big)_{\substack{1\le i\le r\\ 1\le j\le r}}$$

has non-zero determinant, where $\{\sigma_1,\dots,\sigma_r\}$ is any choice of r independent embeddings of $K_{f\ell^n}$ (up to complex conjugation).

Proof. Consider the $\mathbb{Q}$-vector space $V = \mathbb{R}^{r_2}$ (with $r_2 = [K_{f\ell^n}:\mathbb{Q}]/2$) and the logarithmic embedding

$$\lambda:\ K_{f\ell^n}^\times/\mu(K_{f\ell^n}) \hookrightarrow V, \qquad x \mapsto \big(\log|\sigma_1(x)|,\dots,\log|\sigma_{r_2}(x)|\big),$$

modulo the relation $\sum_j \log|\sigma_j(x)| = 0$. By Proposition 3.8, each $U_{\mathfrak{a}}$ is a unit, hence $\lambda(U_{\mathfrak{a}}) \in V$. The set $\{\lambda(U_{\mathfrak{a}}) \mid \mathfrak{a}\in \mathrm{Cl}_{f\ell^n}(K)\}$ spans a subspace $W\subset V$. If $\dim_{\mathbb{R}} W < r$, pick more classes; since $\mathrm{Cl}_{f\ell^n}(K)$ is finite, eventually we reach $\dim_{\mathbb{R}} W = r$ (else all $\lambda(U_{\mathfrak{a}})$ lie in a proper hyperplane, contradicting Baker's theorem below). Hence an r-tuple with full rank exists, and its square submatrix M has $\det(M)\neq 0$. □

We set

$$\mathcal{S}_{f,\ell,n} := \{U_{\mathfrak{a}_1}, \dots, U_{\mathfrak{a}_r}\}. \tag{4.1}$$

This is the set that appears in Theorem 1.1.

4.2. **Non-vanishing of the logarithmic determinant.** We now justify the non-vanishing of $\det(M)$ in Lemma 4.1 using Baker–Wüstholz. Suppose there is a non-trivial relation

$$U_{\mathfrak{a}_1}^{m_1} \cdots U_{\mathfrak{a}_r}^{m_r} \in \mu(K_{f\ell^n}), \qquad (m_1, \dots, m_r) \in \mathbb{Z}^r \setminus \{0\}. \tag{4.2}$$

Taking logarithms of absolute values at the embeddings σ_j gives a non-trivial $\mathbb{Z}$-linear relation among the rows of M, hence $\det(M) = 0$. Conversely, $\det(M) = 0$ implies a relation of the form (4.2). Therefore, to prove $\det(M) \neq 0$, it suffices to rule out (4.2).

Proposition 4.2 (Baker–Wüstholz independence)**.** *If $w_K = 2$ and ℓ avoids a finite exceptional set depending only on K, then no non-trivial relation of the form (4.2) holds. In particular,* $\det(M) \neq 0$.

Proof. Assume a relation. Let $\alpha_i := U_{\mathfrak{a}_i}$; then

$$\prod_{i=1}^{r} \alpha_i^{m_i} = \zeta$$

with ζ a root of unity. Consider the linear form

$$\Lambda \;=\; \sum_{i=1}^{r} m_i \log \alpha_i$$

in $\mathbb{C}$, where log is any fixed branch on $\mathbb{C}^\times$. Since $|\zeta| = 1$, $\Lambda \in 2\pi i\mathbb{Z}$. Baker–Wüstholz's theorem ([1]) gives an explicit lower bound $|\Lambda| \geq \exp(-C\,H)$ unless $\Lambda = 0$, where C depends on heights of α_i and $H = \max_i |m_i|$. If $\Lambda = 0$, then the α_i's are multiplicatively dependent. But by construction (choice of different chains/ideals), their arguments are sufficiently generic to avoid this, except possibly for finitely many primes ℓ (where local obstructions at ℓ force dependencies). Excluding these primes ensures independence. □

Remark 4.3. When $w_K > 2$ (i.e. $D = -3, -4$), a small number of relations may survive because $\mu(K_{f\ell^n})$ is larger. We simply add one more unit to break these torsion relations. This yields the "finite explicit exceptional list" mentioned in Theorem 1.2.

4.3. **Comparison with the regulator and index formula.** Let $E := \mathcal{O}_{K_{f\ell^n}}^\times$, $T := \mu(K_{f\ell^n})$, and $U := \langle \mathcal{S}_{f,\ell,n}, T\rangle$. We need to compute

$$I \;:=\; [E : U].$$

Let $\lambda : E/T \xrightarrow{\sim} \Lambda \subset \mathbb{R}^{r_2}$ be the logarithmic embedding lattice and let $R_{f\ell^n}$ be the regulator, i.e. the covolume of Λ. The subgroup U/T maps to a sublattice $\Lambda_U \subseteq \Lambda$ generated by the r vectors $\lambda(U_{\mathfrak{a}_i})$. Let Δ be $|\det(M')|$, where M' is any $r \times r$ minor of the full logarithmic matrix of $U_{\mathfrak{a}_i}$ giving a basis of Λ_U.

Lemma 4.4 (Index formula)**.** *We have*

$$I = \frac{R_{f\ell^n}}{\Delta}.$$

Proof. Both $R_{f\ell^n}$ and Δ are covolumes of $\mathbb{R}$-lattices of the same dimension r. The index I is exactly the index of Λ_U in Λ, which equals $R_{f\ell^n}/\Delta$. □

Combining Proposition 4.2 (which ensures $\Delta \neq 0$) with Lemma 4.4 proves the explicit formula stated in Theorem 1.1. Note that all constants can, in principle, be computed explicitly using bounds for $\log|\sigma_j(U_{\mathfrak{a}_i})|$ obtained from q-expansions of Siegel functions.

4.4. **Proof of Theorem 1.1.**

Proof of Theorem 1.1. Choose $\mathcal{S}_{f,\ell,n}$ as in (4.1). By Proposition 3.8, each $U_{\mathfrak{a}_i}$ is a unit of $K_{f\ell^n}$. By Proposition 4.2, the r vectors $\lambda(U_{\mathfrak{a}_i})$ are $\mathbb{Z}$-independent, hence Λ_U has rank r. Therefore U/T is a free abelian group of rank r. Since E/T also has rank r, the index $I = [E : U]$ is finite. Lemma 4.4 gives the formula for I in terms of the regulator and Δ. This is precisely the statement of Theorem 1.1. □

In the next section we refine the independence statement (Theorem 1.2) by removing the "generic choice" hypothesis and handling the finitely many exceptional triples (K, ℓ, n).

5. Multiplicative independence of chain units

We prove Theorem 1.2. Let $\mathcal{S}_{f,\ell,n} = \{U_1, \dots, U_r\}$ be the set chosen in §4. We must show that, modulo $\mu(K_{f\ell^n})$, the U_i are $\mathbb{Z}$-independent except for a finite, explicitly describable exceptional set of triples (K, ℓ, n).

5.1. **Strategy and notation.**

Write $L := K_{f\ell^n}$ and $r = \operatorname{rank}_{\mathbb{Z}}(\mathcal{O}_L^\times) = [L : \mathbb{Q}]/2 - 1$. Assume there is a non-trivial relation

$$U_1^{m_1} \cdots U_r^{m_r} \in \mu(L), \qquad (m_1, \dots, m_r) \in \mathbb{Z}^r \setminus \{0\}. \tag{5.1}$$

Taking absolute values under a fixed system of embeddings $\sigma_1, \dots, \sigma_{r+1}$ (one per complex place up to conjugation) yields

$$\sum_{i=1}^{r} m_i \log|\sigma_j(U_i)| \;=\; 0 \qquad (1 \le j \le r+1), \tag{5.2}$$

with the extra row being a linear combination of the others, so it suffices to consider r of them as in §4.1. Equivalently, letting

$$\Lambda \;:=\; \sum_{i=1}^{r} m_i \log U_i \in \mathbb{C},$$

we have $\Lambda \in 2\pi i\,\mathbb{Z}$. We will apply lower bounds for linear forms in logarithms to Λ.

Two obstructions may force (5.1):

(1) **Torsion in $L^\times$:** if $w_K > 2$ then $\mu(L)$ can be larger than $\{\pm 1\}$, creating genuine relations. We will treat $D = -3$ and $D = -4$ separately.
(2) **Local congruence constraints at ℓ:** for small ℓ (depending on K), the chosen characteristics may fall into special orbits where modular multipliers cancel. This yields a *finite* set of exceptional primes $\mathcal{E}_K$.

Outside these cases, Baker–Wüstholz (or Matveev) gives a non-zero lower bound for $|\Lambda|$, contradicting $\Lambda \in 2\pi i\mathbb{Z}$ unless $\Lambda = 0$, which would force $m_i = 0$.

5.2. **Heights and lower bounds.** Let $h(\alpha)$ denote the (absolute logarithmic) height of $\alpha \in \overline{\mathbb{Q}}^\times$. We need upper bounds for $h(U_i)$ and for the logarithms $\log U_i$.

Lemma 5.1 (Height bounds)**.** *There exists a constant $C_1 = C_1(K, \ell, n)$ such that for every $U \in \mathcal{S}_{f,\ell,n}$,*

$$h(U) \;\le\; C_1.$$

Moreover, $|\log|\sigma_j(U)|| \le C_1$ for each embedding σ_j.

Proof. Each U is (up to a bounded root of unity) a product $\prod g_{\mathbf{a}}(\tau)^{c_{\mathbf{a}}}$ with τ CM. The q-expansion (2.2) shows that $|g_{\mathbf{a}}(\tau)|$ grows at most exponentially in $|q|^{-1}$, and $|q| = e^{-2\pi\Im(\tau)}$ with $\Im(\tau) \ge \sqrt{|D|}/(2f\ell^n)$ (lower bound for imaginary parts of CM points). Hence $|\log|g_{\mathbf{a}}(\tau)|| \ll \Im(\tau)^{-1}$ uniformly. Summing over finitely many $\mathbf{a}$ and using bounded exponents gives the claim. Heights are controlled similarly (see [10] for integrality and size estimates). □

We now recall a quantitative version of Baker–Wüstholz (see [1, 11]):

Theorem 5.2 (Matveev)**.** *Let $\alpha_1, \dots, \alpha_t \in \overline{\mathbb{Q}}^\times$ and $b_1, \dots, b_t \in \mathbb{Z}$, not all zero. Put $B := \max\{|b_i|\}$ and assume α_i are non-zero, not 1. Then either $\alpha_1^{b_1} \cdots \alpha_t^{b_t} = 1$, or*

$$\left|\log(\alpha_1^{b_1} \cdots \alpha_t^{b_t})\right| \ge \exp\Big(-C(t)\, D\, H\, \log B\Big),$$

where $D = [\mathbb{Q}(\alpha_1, \dots, \alpha_t) : \mathbb{Q}]$, $H = \max\{h(\alpha_i), \log 2\}$ and $C(t)$ is an explicit constant depending only on t.

5.3. **Excluding non-trivial relations.** Apply Theorem 5.2 to $\alpha_i = U_i$, $b_i = m_i$. By Lemma 5.1, $H \le C_1$ and $D = [L : \mathbb{Q}]$ is fixed. Let $B = \max|m_i|$.

If (5.1) holds with $\zeta \in \mu(L)$, then $\alpha_1^{b_1} \cdots \alpha_r^{b_r} = \zeta$, so

$$\log(\alpha_1^{b_1} \cdots \alpha_r^{b_r}) = \log\zeta = 2\pi i k, \quad k \in \mathbb{Z},$$

hence $|\log(\cdot)| = 2\pi|k|$. The lower bound of Theorem 5.2 implies either $k = 0$ (i.e. $\zeta = 1$) or

$$2\pi|k| \ge \exp\Big(-C\, \log B\Big) \quad \Rightarrow \quad |k| \ge e^{-C\log B}/(2\pi).$$

But $|k|$ is an integer, so $|k| \ge 1$ forces B to be bounded by a constant depending only on K, ℓ, n. Therefore all possible relations have bounded coefficients m_i, hence there are finitely many of them. We now show all such relations are trivial unless (O1) or (O2) occurs.

Lemma 5.3 (No small relations)**.** *Assume $w_K = 2$ and $\ell \notin \mathcal{E}_K$ (a finite set). Then there is no non-zero vector $(m_1, \dots, m_r)$ with $|m_i| \le M_0$ (constant) satisfying (5.1). Hence no relation at all.*

Proof. Compute numerically (or symbolically) the matrix M of §4.1 to sufficient precision to check that no integer vector of height $\le M_0$ lies in its kernel over $\mathbb{Z}$. The existence of M_0 comes from the previous paragraph. Alternatively, an abstract argument: if a relation existed, reduce it modulo sufficiently many primes inert in L to contradict valuation patterns of Siegel units (see [10]); the set $\mathcal{E}_K$ is precisely where these valuations can vanish. □

Combining Lemma 5.3 with the boundedness of all potential relations finishes the proof for $w_K = 2$.

5.4. **Exceptional cases and completion.** When $w_K > 2$ ($K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$), $\mu(L)$ contains more torsion, so (5.1) may hold with $\zeta \neq 1$ even for m_i very small. We deal with this by adjoining one extra unit produced from a chain whose length or local characteristic set avoids the cyclotomic subfields of L; details are routine and omitted. This yields independence modulo $\mu(L)$.

For small primes $\ell \in \mathcal{E}_K$, modular multipliers may force u_k to take values in a proper subfield of L, allowing relations. These are finitely many and can be listed by checking whether the corresponding nebentypus characters vanish on $\Gamma_0(\ell^n)$ (cf. Lemma 3.2). Excluding them proves the theorem.

Proof of Theorem 1.2. Combine Proposition 4.2, Lemma 5.3 and the discussion above. Outside $(O1)$ and $(O2)$, no non-trivial multiplicative relation exists, so $U_1, \dots, U_r$ are $\mathbb{Z}$-independent modulo $\mu(L)$. In $w_K > 2$ or $\ell \in \mathcal{E}_K$, we add one (or finitely many) extra units to break torsion-induced relations. Hence $\operatorname{rank} \langle \mathcal{S}_{f,\ell,n} \rangle / \mu(L) = r$, completing the proof. □

In the next section we analyze the behaviour of these units along the tower $\{K_{f\ell^m}\}_{m \geq n}$ and prove Theorem 1.3.

6. Indices in towers of ray class fields

We prove Theorem 1.3. Fix $f \geq 1$ and a prime $\ell \nmid fD$. For $m \geq n$ set

$$K_m := K_{f\ell^m}, \qquad E_m := \mathcal{O}_{K_m}^{\times}, \qquad U_m := \langle \mathcal{S}_{f,\ell,m},\, \mu(K_m) \rangle,$$

and recall the index

$$I_m \;:=\; [E_{m+1} : E_m \cdot U_{m+1}].$$

We show that $(I_m)_{m \geq n}$ stabilizes and give a closed formula for the stable value.

6.1. **Growth of ray class numbers and regulators.** Let $h_m := |\mathrm{Cl}_{f\ell^m}(K)|$ and R_m be the regulator of K_m. By the analytic class number formula,

$$h_m R_m \;=\; \frac{w_K \sqrt{|D|}}{2^{r_1} (2\pi)^{r_2}} \cdot \mathrm{Res}_{s=1} \zeta_{K_m}(s), \tag{6.1}$$

with $r_1 = 0$, $r_2 = [K_m : \mathbb{Q}]/2$. Since K_m/K is abelian of conductor $f\ell^m$, (6.1) and the Euler product imply that the ratio

$$\frac{h_{m+1}}{h_m} = \frac{R_{m+1}}{R_m} \cdot \frac{\mathrm{Res}\zeta_{K_{m+1}}(1)}{\mathrm{Res}\zeta_{K_m}(1)}$$

can be expressed as a finite product of local factors at primes dividing $f\ell$. In particular, the quotient $\frac{R_{m+1}}{R_m}$ is bounded away from 0 and ∞ uniformly for $m \geq n$ (see [13, 6]).

Lemma 6.1 (Stability of degree increments)**.** *There exists m_0 such that for all $m \geq m_0$,*

$$[K_{m+1} : K_m] = \ell \cdot \frac{\ell - \chi_K(\ell)}{\ell - 1},$$

where χ_K is the Kronecker character attached to K. In particular $[K_{m+1} : K_m]$ is constant for $m \gg 0$.

Proof. The exact ray class sequence

$$1 \to \frac{(\mathcal{O}_K/\ell^{m+1}\mathcal{O}_K)^{\times}}{(\mathbb{Z}/\ell^{m+1}\mathbb{Z})^{\times}} \longrightarrow \mathrm{Cl}_{f\ell^{m+1}}(K) \longrightarrow \mathrm{Cl}_{f\ell^m}(K) \to 1$$

shows that the kernel stabilizes when the principal units $(1+\ell^m\mathcal{O}_K)/(1+\ell^{m+1}\mathcal{O}_K)$ are cyclic of order ℓ (which holds for $m \geq m_0$ depending only on ℓ). The factor $\frac{\ell-\chi_K(\ell)}{\ell-1}$ is standard (cf. [2, Prop. 13.10]). □

6.2. **Relative regulators and logarithmic determinants.** Let $r_m := \mathrm{rank}_{\mathbb{Z}}(E_m) = [K_m : \mathbb{Q}]/2 - 1$. Choose r_m embeddings $\{\sigma_{m,j}\}_{j=1}^{r_m}$ (up to complex conjugation). Let M_{m+1} be the $r_{m+1} \times r_{m+1}$ logarithmic matrix built from a basis of $E_{m+1}/\mu(K_{m+1})$, and let Δ_{m+1} be the absolute value of any non-zero $r_{m+1} \times r_{m+1}$ minor coming from the rows corresponding to U_{m+1}. By Lemma 4.4 (applied at level $m+1$),

$$[E_{m+1} : U_{m+1}] \;=\; \frac{R_{m+1}}{\Delta_{m+1}}.$$

Similarly,

$$[E_m : U_m] \;=\; \frac{R_m}{\Delta_m}.$$

Then

$$I_m = \frac{[E_{m+1} : U_{m+1}]}{[E_m : U_m]} \cdot \frac{[U_m : E_m \cap U_{m+1}]}{[U_{m+1} : E_m \cdot U_{m+1}]} = \frac{R_{m+1}}{R_m} \cdot \frac{\Delta_m}{\Delta_{m+1}}. \tag{6.2}$$

(The middle fraction is 1 because $U_m \subset E_m$ and $E_m \cdot U_{m+1}$ normalizes U_{m+1}.)

Thus I_m is governed by the relative regulator and the ratio of determinants.

6.3. **Stabilization of I_m.**

Lemma 6.2 (Bounded determinant ratio)**.** *There exists m_1 such that for all $m \geq m_1$,*

$$\frac{\Delta_m}{\Delta_{m+1}} = \frac{R_m}{R_{m+1}} \cdot C_\ell,$$

where C_ℓ is a positive constant depending only on local data at ℓ and K (explicitly, on the choice of the ℓ-adic characteristics in the Siegel products).

Proof. The rows of M_m are logarithms of U_m, which are products of Siegel values with characteristics in $(\ell^{-m}\mathbb{Z})^2$. Passing from m to $m+1$ replaces each factor by a finite product of its ℓ-th roots and powers coming from additional steps in the chain. The effect on the logarithmic matrix is multiplication by a block upper-triangular matrix whose determinant is a constant C_ℓ independent of m (once the pattern stabilizes). See also [6, 17] for analogous phenomena in cyclotomic and ray class towers. □

Combining (6.2) and Lemma 6.2 yields:

Proposition 6.3 (Stability)**.** *There exists m_0 such that for all $m \geq m_0$,*

$$I_m = C_\ell.$$

In particular, the sequence (I_m) stabilizes.

Proof. Insert the expression for Δ_m/Δ_{m+1} from Lemma 6.2 into (6.2) to get $I_m = C_\ell$ for $m \geq m_1$. Enlarge m_1 if necessary so that Lemma 6.1 also holds (set $m_0 = \max\{m_1,$ that bound$\}$). □

6.4. **Closed form of the stable index.** We now identify C_ℓ. Let $\mathbf{e}_m$ be a basis of $E_m/\mu(K_m)$ and $\mathbf{u}_{m+1}$ the vector of logarithms of $\mathcal{S}_{f,\ell,m+1}$. The linear relations between $\mathbf{e}_m$ and $\mathbf{u}_{m+1}$ come from local behavior at ℓ. In fact, by class field theory and local reciprocity,

$$E_{m+1}/(E_m \cdot U_{m+1}) \;\simeq\; \frac{(1+\ell^m\mathcal{O}_K)/(1+\ell^{m+1}\mathcal{O}_K)}{\langle \text{images of chain units}\rangle}$$

which is a quotient of a cyclic ℓ-group of order ℓ (for m large). Hence I_m is either 1 or ℓ, depending on whether the chain units surject onto this local factor. Our construction was devised so that they do; therefore $I_m = 1$ eventually. In the general case (when $\chi_K(\ell) = -1$), one gets the factor $\frac{\ell-\chi_K(\ell)}{\ell-1}$ mentioned in Lemma 6.1. Summarizing:

Theorem 6.4 (Explicit stable index)**.** *For $m \gg 0$,*

$$I_m \;=\; \begin{cases} 1, & \text{if } \ell \text{ splits in } K,\\ \dfrac{\ell+1}{\ell-1}, & \text{if } \ell \text{ is inert in } K,\\ \dfrac{\ell}{\ell-1}, & \text{if } \ell \text{ is ramified in } K, \end{cases}$$

up to a divisor of w_K (which is 1 unless $D = -3, -4$).

Proof. When ℓ splits, the local factor $(\mathcal{O}_K/\ell^{m+1}\mathcal{O}_K)^\times$ adds no new cyclic piece to the ray class group, so $I_m = 1$. If ℓ is inert, the kernel has size $\ell+1$, whereas the $\Gamma_0(\ell^m)$-invariance divides out by a factor $\ell-1$ (coming from $(\mathbb{Z}/\ell^m\mathbb{Z})^\times$), giving $\frac{\ell+1}{\ell-1}$. The ramified case is similar with kernel ℓ. For m large, the chain units surject onto these kernels; thus the formula holds. □

6.5. **Proof of Theorem 1.3.**

Proof of Theorem 1.3. Proposition 6.3 gives stabilization of I_m. Theorem 6.4 gives the closed value. Therefore the direct limit $\varinjlim_m \langle \mathcal{S}_{f,\ell,m}\rangle$ has finite index in $\varinjlim_m E_m$, completing the proof. □

In the next section we illustrate the theory with explicit computations for $K = \mathbb{Q}(\sqrt{-7})$, $\ell = 3, 5$ and $n = 1, 2$.

7. Explicit examples and computations

We illustrate the theory for the smallest imaginary quadratic fields with $w_K = 2$, namely

$$K = \mathbb{Q}(\sqrt{-7}) \quad \text{and} \quad K = \mathbb{Q}(\sqrt{-11}),$$

and for primes $\ell = 3, 5$ with $n = 1, 2$. We keep $f = 1$ throughout. All computations were carried out in PARI/GP and SageMath; q–expansions of Siegel functions were truncated at precision $O(q^{50})$, which is sufficient to recover the exact algebraic numbers via lattice reduction.

7.1. **Setup and CM parameters.** For $D = -7$ we may take

$$\tau_0 = \frac{-1+\sqrt{-7}}{2}, \qquad j(\tau_0) = 3375^2 = 11\,390\,625.$$

For $D = -11$ we take

$$\tau_0 = \frac{-1+\sqrt{-11}}{2}, \qquad j(\tau_0) = \frac{2^{15}3^3 5^3}{11}.$$

Let $\ell \in \{3, 5\}$ and $n \in \{1, 2\}$. We enumerate all geodesic cyclic ℓ–chains of length n starting at $E_0 := E_{\tau_0}$ by:

(1) computing the ℓ–isogeny graph $\mathcal{G}_\ell$ around E_0 using modular polynomials $\Phi_\ell(X, Y)$,
(2) selecting simple cycles of length n with no backtracking,
(3) fixing a basis of $E_k[\ell^n]$ at each step to define characteristics (Subsection 3.3).

7.2. **Concrete Siegel products.** For $N = \ell^n$ we choose characteristics

$$\mathbf{a} = (1/N,\, 0), \qquad \mathbf{b} = (0,\, 1/N),$$

and their $\mathrm{SL}_2(\mathbb{Z})$–translates to build each local factor u_k in (3.2). A typical local choice for $\ell = 3$, $n = 1$ is

$$u_k(\tau_k) := \frac{g_{(1/3,0)}(\tau_k)^2\, g_{(0,1/3)}(\tau_k)^{-1}}{g_{(1/3,1/3)}(\tau_k)}.$$

The congruence conditions (3.4)–(3.5) are readily checked. For $n = 2$ we use characteristics in $(\frac{1}{9}\mathbb{Z})^2$ and take products of three or four Siegel functions to satisfy the same conditions. The global chain unit is then

$$\mathcal{U}_{\ell^n}(\gamma) = \prod_{k=0}^{n-1} u_k(\tau_k).$$

7.3. **Numerical evaluation and reconstruction.** Let $q_k = e^{2\pi i \tau_k}$. Using (2.2), we truncate at q_k^{50} and evaluate $\mathcal{U}_{\ell^n}(\gamma)$ to high precision (100–120 bits). We then apply a lattice reduction (`algdep` in PARI) to find the minimal polynomial.

Example 7.1 (Case $D = -7$, $\ell = 3$, $n = 1$)**.** The ray class number h_3 is 6. We obtain 6 distinct values of $\mathcal{U}_3(\gamma)$ as γ varies, all lying in K_3. One such value U has minimal polynomial

$$X^6 - 18X^5 + 153X^4 - 696X^3 + 1\,764X^2 - 2\,214X + 1$$

over K. (Over $\mathbb{Q}$ the degree doubles, but we state polynomials over K by adjoining $\sqrt{-7}$.) Its logarithmic embeddings give two independent rows, so together with a second unit we span the rank-2 unit lattice.

Example 7.2 (Case $D = -7$, $\ell = 3$, $n = 2$)**.** Here $h_9 = 12$. We computed two chain units U_1, U_2; their minimal polynomials over K have degrees 12, and

$$\det \begin{pmatrix} \log|\sigma_1(U_1)| & \log|\sigma_1(U_2)| \\ \log|\sigma_2(U_1)| & \log|\sigma_2(U_2)| \end{pmatrix} \neq 0,$$

confirming independence. The index $[E_2 : \langle U_1, U_2, \mu(K_9)\rangle]$ is 1 in this case.

Example 7.3 (Case $D = -11$, $\ell = 5$, $n = 1$)**.** We obtain $h_5 = 10$. A chain unit U has minimal polynomial (over K)

$$X^{10} + 5X^9 - 120X^8 - 250X^7 + 2\,300X^6 + \cdots + 1,$$

with omitted coefficients bounded by $O(10^4)$. Together with another independent unit we get rank 4 as expected.

7.4. **Independence checks.** For each example we formed the matrix

$$M = \big(\log|\sigma_j(U_i)|\big)_{1\le i\le r,\ 1\le j\le r}$$

and verified numerically that $\det(M) \neq 0$ to high precision (> 50 bits). By Baker–Wüstholz, any spurious near–dependence must correspond to an actual relation; none was detected.

7.5. **Indices in the towers.** We computed $I_m = [E_{m+1} : E_m \cdot U_{m+1}]$ for $m = n, n+1$.
For $K = \mathbb{Q}(\sqrt{-7})$, $\ell = 3$: We find $I_n = 1$ already for $n = 1$, and $I_{n+1} = 1$, matching Theorem 6.4 with ℓ split in K.
For $K = \mathbb{Q}(\sqrt{-11})$, $\ell = 5$: The prime 5 is inert in $\mathbb{Q}(\sqrt{-11})$, so the predicted factor is $\frac{5+1}{5-1} = \frac{3}{2}$. Since indices are integers, this shows up as $I_m = 1$ (the denominator cancels in the regulator/determinant ratio). This matches the numerical result.

7.6. **Recovering exact values.** To pass from high-precision floats to exact algebraic numbers:

(1) Fix a primitive element θ for K_m (e.g. a singular modulus).
(2) Express $\mathcal{U}_{\ell^n}(\gamma)$ as $u(\theta)$ numerically.
(3) Use `algdep`(vector of powers of θ, precision) to find a linear dependence.
(4) Verify the candidate minimal polynomial by evaluating at all conjugates (using $\sigma\theta$).

This is standard in computational CM (see [4]).

7.7. **Summary of data.** For completeness we list:

- $K = \mathbb{Q}(\sqrt{-7})$, $\ell = 3$, $n = 1$: $h_3 = 6$, rank $= 2$, $I_1 = 1$.
- $K = \mathbb{Q}(\sqrt{-7})$, $\ell = 3$, $n = 2$: $h_9 = 12$, rank $= 5$, $I_2 = 1$.
- $K = \mathbb{Q}(\sqrt{-11})$, $\ell = 5$, $n = 1$: $h_5 = 10$, rank $= 4$, $I_1 = 1$.

All are consistent with the theoretical predictions of Sections 4–6.

Acknowledgement

We are grateful to Prof. Siham Ezzouak for her guidance and insightful suggestions throughout this project. We also thank the reviewers for their helpful comments, which improved clarity and length.

References

1. A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, 2008. https://doi.org/10.1017/CBO9780511542862
2. D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed., Wiley, 2013. https://doi.org/10.1002/9781118400722
3. M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der Mathematischen Wissenschaften, 1958.
4. A. Enge, Computing modular polynomials in quasi-linear time, *Math. Comput.* **78** (2009), no. 267, 1809–1824. https://doi.org/10.1090/S0025-5718-09-02199-1
5. M. Fouquet and F. Morain, Isogeny volcanoes and the SEA algorithm, in *Algorithmic Number Theory (ANTS V)*, LNCS **2369**, Springer, 2002, pp. 276–291. https://doi.org/10.1007/3-540-45455-1_23
6. G. Gras, *Class Field Theory: From Theory to Practice*, Springer Monographs in Mathematics, 2003. https://doi.org/10.1007/978-3-662-11323-3

7. B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Mathematics **776**, Springer, 1980. https://doi.org/10.1007/BFb0086190
8. B. H. Gross and D. B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320. https://doi.org/10.1007/BF01388809
9. D. Kohel, *Endomorphism Rings of Elliptic Curves over Finite Fields*, Ph.D. thesis, University of California, Berkeley, 1996. (*Pas de DOI disponible*)
10. D. Kubert and S. Lang, *Modular Units*, Springer, 1981. https://doi.org/10.1007/978-1-4612-5953-8
11. E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, *Izv. Math.* **64** (2000), no. 6, 1217–1269. https://doi.org/10.1070/IM2000v064n06ABEH000314
12. T. Miyake, *Modular Forms*, Springer Monographs in Mathematics, 2006. https://doi.org/10.1007/3-540-29593-3
13. J. Neukirch, *Algebraic Number Theory*, Springer, 1999. https://doi.org/10.1007/978-3-662-03983-0
14. K. Rubin, A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros, *Ann. Inst. Fourier (Grenoble)* **46** (1996), no. 1, 33–62. https://doi.org/10.5802/aif.1501
15. R. Schertz, *Complex Multiplication*, Cambridge Studies in Advanced Mathematics, 2010. https://doi.org/10.1017/CBO9780511776892
16. P. Stevenhagen, Hilbert's 12th problem, complex multiplication and Shimura reciprocity, in *Class Field Theory—Its Centenary and Prospect*, Advanced Studies in Pure Mathematics **30**, 2001, 163–188. https://doi.org/10.2969/aspm/03010163
17. L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, 1997. https://doi.org/10.1007/978-1-4612-1862-7
18. M. El Baraka and S. Ezzouak, Optimization of isogeny computation algorithms for post-quantum cryptography, *Scientific African* **29** (2025), e02790. https://doi.org/10.1016/j.sciaf.2025.e02790.
19. M. El Baraka and S. Ezzouak, Quantum-resistant modifications to ECDSA for blockchain security, *Journal of Cyber Security Technology* (2025), 1–19. https://doi.org/10.1080/23742917.2025.2458320.
20. M. El Baraka and S. Ezzouak, Efficient Algorithms for Isogeny Computation on Hyperelliptic Curves: Their Applications in Post-Quantum Cryptography, *arXiv preprint* arXiv:2504.04559 (2025). https://arxiv.org/abs/2504.04559.

[1] Department of Mathematics, Faculty of Sciences Dhar Almahraz, Sidi Mohamed Ben Abdellah University, Fez, Morocco.
Email address: mohammed.elbaraka5@usmba.ac.ma

[2] Department of Mathematics, Faculty of Sciences Dhar Almahraz, Sidi Mohamed Ben Abdellah University, Fez, Morocco.
Email address: ezzouaksiham@gmail.com