INDIVISIBILITY OF RAY CLASS GROUPS OF REAL QUADRATIC FIELDS

EMMANUEL LECOUTURIER AND CHRISTIAN MAIRE

ABSTRACT. Let $\ell, p \geq 5$ be primes such that $p \mid (\ell - 1)$. Let $\Delta > 0$ be the fundamental discriminant of a real quadratic field in which ℓ splits. We denote by $h_\ell^-(\Delta)$ the order of the minus part (for the Galois action) of the ray class group of $\mathbf{Q}(\sqrt{\Delta})$ of modulus ℓ. In this paper, we study the indivisibility of $h_\ell^-(\Delta)$ by p, and prove that

$$\#\{0 < \Delta < X,\ \left(\frac{\Delta}{\ell}\right) = 1 \text{ and } p \nmid h_\ell^-(\Delta)\} \gg \frac{\sqrt{X}}{\log(X)},$$

under the assumption that this set is non-empty. This lower bound is made unconditional if $\ell = 2p + 1$, *i.e.* if p is a Sophie Germain prime. Our result can be viewed as being in the continuity of the results of Kohnen–Ono, Ono, Byeon, Beckwith etc. regarding the class numbers of quadratic fields, in the sense that we rely on techniques from the theory of half-integral weight modular forms. Significant difficulties however arise in our study, as we have to study Eisenstein congruences for cuspforms of weight $\frac{3}{2}$, and use a generalized Shimura correspondence of Baruch–Mao. Combined with the results of Lecouturier–Wang, our result has implications *eg.* for the 5-part of BSD for even quadratic twists of $X_0(11)$.

INTRODUCTION

The class group Cl_K of a number field K is a finite abelian group that plays a central role in many questions in number theory, however its structure largely remains mysterious, except in a few very specific situations. To improve its understanding, Cohen and Lenstra [7] proposed heuristics, particularly for families of quadratic fields. Let $h(\Delta)$ denote the class number of the quadratic field $\mathbf{Q}(\sqrt{\Delta})$ with fundamental discriminant Δ. Let $p > 2$ be a prime number. Set

$$\eta^k(p) := \prod_{i \geq k} \left(1 - \frac{1}{p^i}\right).$$

The Cohen–Lenstra heuristics predict that the proportion of imaginary quadratic fields (respectively real quadratic fields) such that $p \nmid h(\Delta)$ is equal to $\eta^1(p)$ (resp. $\eta^2(p)$). A notable result regarding the indivisibility by p of the class number of quadratic fields, though still far from approaching these heuristics, was obtained by Davenport and Heilbronn [9] and $p = 3$, as well as Hartung [12] for imaginary quadratic fields and $p > 2$. These results have been extended to any prime p by Horie [13], under the condition that p does not split in the family of quadratic fields considered.

A breakthrough came with a paper of Kohnen and Ono [15] in the late 1990s, where they showed that for a prime $p > 2$ and X sufficiently large,

$$\#\{-X < \Delta < 0 \text{ such that } p \nmid h(\Delta)\} \gg \frac{\sqrt{X}}{\log X}.$$

The proof relies on the fact that, in this setting, the class number formula relates the order $h(\Delta)$ of the class group of $K = \mathbf{Q}(\sqrt{\Delta})$ to the special value $\zeta_K(s)$ of the Dedekind zeta function of K at $s = 0$. They then use

Date: June 14, 2026.

2020 *Mathematics Subject Classification.* 11F30, 11F33, 11F67, 11F37, 11R29, 11R11.

a well-known result dating back from Gauss to relate $h(\Delta)$ to some Fourier coefficient of a modular form of weight $3/2$.

Following the same principle, for real quadratic fields, Ono [24] then Byeon [6] also obtained a result of indivisibility by making use of modular forms of weight $3/2$, and by using, in particular, Sturm's bound. More recently, Wiles [35] revisited the question of indivisibility by p of the class number of imaginary quadratic fields satisfying a given set of local conditions. This result was further refined by Beckwith [3], who specified the number of such imaginary quadratic fields, again using modular forms.

We now consider a situation in the spirit of these works.

Let $\ell, p \geq 5$ be primes such that $p \mid (\ell - 1)$. Let $\Delta > 0$ be a fundamental discriminant such that $\left(\frac{\Delta}{\ell}\right) = 1$, equivalently ℓ splits in $K := \mathbf{Q}(\sqrt{\Delta})$. Let $\mathrm{Cl}_{K,\ell}$ denotes the ray class group of K with modulus ℓ. The Galois group $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Cl}_{K,\ell}$, and we denote by $h_\ell^-(\Delta)$ the order of the eigenspace for the eigenvalue -1 of the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$. We prove the following.

Theorem A. *Let ℓ, p be primes ≥ 5 such that $p \mid (\ell - 1)$. Let Q be a squarefree positive integer such that $\gcd(Q, 2p\ell) = 1$ and $Q \not\equiv \pm 1$ (modulo p). Consider the set*

$$\mathcal{D}(\ell, p, Q) := \{\Delta > 0 \text{ fundamental discriminant s.t. } \left(\frac{\Delta}{Q}\right) = -1, \left(\frac{\Delta}{\ell}\right) = 1 \text{ and } p \nmid h_\ell^-(\Delta)\}.$$

Assume that $\mathcal{D}(\ell, p, Q) \neq \emptyset$. Then we have

$$\#\{0 < \Delta < X \text{ with } \Delta \in \mathcal{D}(\ell, p, Q)\} \gg_{p,\ell,Q} \frac{\sqrt{X}}{\log(X)}.$$

A similar result without the extra parameter Q holds as an immediate corollary, as if $p \nmid h_\ell^-(\Delta)$ and $\left(\frac{\Delta}{\ell}\right) = 1$, then one can always find a Q satisfying the conditions of the theorem such that $\Delta \in \mathcal{D}(\ell, p, Q)$. For convenience, we record it in the following

Corollary B. *Let p, ℓ be primes ≥ 5 such that $p \mid (\ell - 1)$. Consider the set*

$$\mathcal{D}(\ell, p) := \{\Delta > 0 \text{ fundamental discriminant s.t. } \left(\frac{\Delta}{\ell}\right) = 1 \text{ and } p \nmid h_\ell^-(\Delta)\}.$$

Assume that $\mathcal{D}(\ell, p) \neq \emptyset$. Then we have

$$\#\{0 < \Delta < X \text{ with } \Delta \in \mathcal{D}(\ell, p)\} \gg_{p,\ell} \frac{\sqrt{X}}{\log(X)}.$$

Remark. It is not hard to see (*cf.* Proposition 1.6) that the condition $\Delta \in \mathcal{D}(\ell, p)$ is equivalent to $p \nmid h(\Delta)$ and any fundamental unit of $\mathbf{Q}(\sqrt{\Delta})$ is not a pth power modulo a prime above ℓ.

We also get the following corollary in the case of Sophie Germain primes (choosing $Q = 3$ in our theorem).

Corollary C. *Let $p \geq 5$ be a Sophie Germain prime, i.e. such that $\ell := 2p + 1$ is also prime. Then*

$$\#\{0 < \Delta < X \text{ fundamental discriminant s.t. } \left(\frac{\Delta}{3}\right) = -1, \left(\frac{\Delta}{\ell}\right) = 1 \text{ and } p \nmid h_\ell^-(\Delta)\} \gg_p \frac{\sqrt{X}}{\log(X)}.$$

This corollary is obtained by constructing explicitly some Δ_0 in $\mathcal{D}(p,\ell,3)$ (*cf.* Theorem 1.11 below).

As Cohen and Lenstra explain in [7, §8], while the heuristic for imaginary quadratic fields is quite natural, the one for real quadratic fields is more subtle. An analogous situation given at the end of §8 of [7], provided by Gross, supports this principle. We believe our context can also be seen as an example that supports this view. We expect that the equality

$$\lim_{X\to+\infty} \frac{\#\{0<\Delta<X \text{ with } \Delta\in\mathcal{D}(\ell,p)\}}{\#\{0<\Delta<X \text{ with } \left(\frac{\Delta}{\ell}\right)=1\}} \stackrel{?}{=} \eta^1(p)$$

holds. In other words, among the fundamental discriminants $\Delta>0$ satisfying $\left(\frac{\Delta}{\ell}\right)=1$, the density of those for which $p\nmid h_\ell^-(\Delta)$ holds should be equal to $\eta^1(p)$. In particular, this conjectural density is independent of ℓ. We give some numerical data supporting this conjecture in §1.3. Recently, Bartel and Pagano [1] addressed the Cohen–Lenstra conjectures for the ray class groups of quadratic fields for a fixed rational modulus. It would be interesting to revisit their results within the framework of our study.

Finally, using the results of [18], we can deduce from a slight modification of Theorem A some consequences for the p-part of the BSD conjecture for the p-Eisenstein quotient of $J_0(\ell)$, assuming that the pair (ℓ,p) (with $N=\ell$ in the notation of [18]) satisfies [18, Hypothesis H]. This Hypothesis H is satisfied in particular for $\ell=11$ and $p=5$, and in this case $J_0(\ell)$ is the elliptic curve $E: y^2+y=x^3-x^2-10x-20$ over $\mathbf{Q}$. If Δ is the discriminant of a quadratic field, we denote by $E^{(\Delta)}$ the corresponding quadratic twist over $\mathbf{Q}$. The result we get is the following.

Corollary D. *Consider the elliptic curve $E=X_0(11): y^2+y=x^3-x^2-10x-20$ over $\mathbf{Q}$. Then*

$$\#\{\,0<\Delta<X \text{ such that } \left(\frac{\Delta}{5}\right)=-1,\ \left(\frac{\Delta}{11}\right)=1,$$
$$Ш(E^{(\Delta)}/\mathbf{Q})[5]=0,\ E^{(\Delta)}(\mathbf{Q})\otimes_{\mathbf{Z}}\mathbf{Z}/5\,\mathbf{Z}=0 \text{ and the 5-part of BSD holds for } E^{(\Delta)}/\mathbf{Q}\}\gg\frac{\sqrt{X}}{\log(X)}.$$

In line with the Cohen–Lenstra type heuristic above for the divisibility of $h_\ell^-(\Delta)$, and the fact that 100% of $0<\Delta<X$ with $\left(\frac{\Delta}{11}\right)=1$ are expected to satisfy $E^{(\Delta)}(\mathbf{Q})\otimes_{\mathbf{Z}}\mathbf{Z}/5\,\mathbf{Z}=0$, we are led to expect that

$$\lim_{X\to+\infty}\frac{\#\{0<\Delta<X \text{ with } \left(\frac{\Delta}{5}\right)=-1,\ \left(\frac{\Delta}{11}\right)=1 \text{ and } Ш(E^{(\Delta)}/\mathbf{Q})[5]=0\}}{\#\{0<\Delta<X \text{ with } \left(\frac{\Delta}{5}\right)=-1 \text{ and } \left(\frac{\Delta}{11}\right)=1\}}\stackrel{?}{=}\eta^1(5)\approx 0.7680.$$

Let us outline the general principle of the proof of the Theorem A. There are three main steps.

The first step is to relate the indivisibility of $h_\ell^-(\Delta)$ by p to the indivisibility of suitably normalized central critical L-value $L(F,\chi_\Delta,1)$, where $F\in S_2(\Gamma_0(\ell))$ is a Hecke newform which is congruent to an Eisenstein series modulo p. Such a newform is known to exist by the Eisenstein ideal theory due to Mazur [22], but it may not be unique (up to conjugation) unless $p^2\nmid(\ell-1)$. The congruence for the L-value has been proved in an earlier work of the first author (*cf.* [17, (26)]), although in a form which is not quite suitable for our present purpose, as it makes use of a period and requires $p^2\nmid(\ell-1)$. In this paper, follow the method of [17], namely we use an explicit form of a formula of Waldspurger, due to Popa [26], for $L(F/\mathbf{Q}(\sqrt{\Delta}),1)$

as well as congruences for modular symbols (essentially due to Mazur). The final congruence is stated in Proposition 2.3. Let us also notice that a similar congruence formula has been obtained in a joint work of the first author [18] using Sharifi's conjecture and algebraic K-theory of cyclotomic fields.

The second step, which perhaps is the most original part of this paper, is to transfer the congruence for the L-value from the first step to a congruence satisfied by a certain modular form of weight $\frac{3}{2}$ and level $\Gamma_1(4\ell^2)$. In some sense, our result is an Eisenstein and higher Eisenstein congruence at the level of modular forms of weight $\frac{3}{2}$. We rely crucially on a generalization of the Shimura correspondence due to Baruch–Mao in [2]. The main results are Theorem 3.4 and Corollary 3.6. The main technical difficulty is to take care of the Hecke operator at the place 2, which requires going through the details of the construction of [2].

The third step is to use the Sturm bound to produce enough non-zero coefficients of our weight $\frac{3}{2}$ modular form modulo p. Our technique is similar to the one of Ono [24] and Byeon [6]. Note that we need to assume that at least one coefficient is non-zero modulo p, which is the reason for the assumption $\mathcal{D}(\ell, p, Q) \neq \emptyset$ in Theorem A.

Notation

In this paper, ℓ and p will denote two primes such that $p \mid (\ell - 1)$. Since the group $(\mathbf{Z}/\ell\,\mathbf{Z})^\times$ is cyclic of order $\ell - 1$, we can fix a surjective group homomorphism

$$\log_{\ell,p} : (\mathbf{Z}/\ell\,\mathbf{Z})^\times \to \mathbf{Z}/p\,\mathbf{Z}\,.$$

The letter Δ will be used to denote the discriminant of a real quadratic field, viewed inside $\mathbf{R}$. We let $h(\Delta)$ and ϵ_Δ be the class number and the fundamental unit > 1 of $\mathbf{Q}(\sqrt{\Delta})$ respectively. We denote by

$$\chi_\Delta : (\mathbf{Z}/\Delta\,\mathbf{Z})^\times \to \mathbf{C}^\times$$

the (primitive) quadratic character associated with $\mathbf{Q}(\sqrt{\Delta})$. Finally, we denote by $\mathcal{D}_\ell$ the set of discriminants of real quadratic fields in which the prime ℓ splits, *i.e.*

$$\mathcal{D}_\ell = \{\Delta > 0 \text{ fundamental discriminant such that } \chi_\Delta(\ell) = 1\}. \tag{1}$$

Let $\Delta \in \mathcal{D}_\ell$. If ε is a unit of $\mathbf{Q}(\sqrt{\Delta})$ and $\mathfrak{l}$ is a prime above ℓ in K, we define

$$\log_{\mathfrak{l},p}(\varepsilon) := \log_{\ell,p}(\varepsilon \text{ modulo } \mathfrak{l}) \in \mathbf{Z}/p\,\mathbf{Z}\,.$$

We observe that the condition $\log_{\mathfrak{l},p}(\varepsilon) = 0$ does not depend on the choice of $\mathfrak{l}$ and of the discrete logarithm $\log_{\ell,p}$.

Acknowledgements and funding

This project started in the summer 2023 when the second author visited the first author at the YMSC of Tsinghua University. The main research was carried out during subsequent visits of the second author to Westlake University (springs 2025 and 2026) and of the first author to University Marie and Louis Pasteur in summer 2025. The authors thank these institutions for their warm hospitality. The authors would also like to thank Farshid Hajir for discussions regarding the Cohen–Lenstra heuristics.

The first author was partially supported by a NSFC grant (grant number W2532004). The second author was partially supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne-Franche-Comté Region.

1. Arithmetic background

1.1. Ray class group of real quadratic fields.

1.1.1. *Cyclic degree p extensions tamely ramified.* Let K be a number field and $p \geq 2$ be a prime. A cyclic degree p extension L/K will be called a $\mathbf{Z}/p$-extension. A prime $\mathfrak{l}$ of K is said to be *tame* if its absolute norm $N\mathfrak{l}$ is congruent to 1 modulo p. This congruence is necessary to have (possibly) some ramification at $\mathfrak{l}$ in some $\mathbf{Z}/p$-extension of K. In the following we are interested in tamely ramified $\mathbf{Z}/p$-extension L/K. As we will see, these extensions are managed by a certain governing field M. Let

$$V_K := \{x \in K^\times \text{ such that } \forall \mathfrak{q} \text{ prime of } K,\ v_\mathfrak{q}(x) \equiv 0 \text{ (modulo } p)\}$$

be the Selmer group of K. Here $v_\mathfrak{q}$ is the normalized $\mathfrak{q}$-valuation. It is well-known that V_K fits in the following exact sequence

$$1 \longrightarrow E_K/E_K^p \longrightarrow V_K/(K^\times)^p \longrightarrow \mathrm{Cl}_K[p] \longrightarrow 1,$$

where E_K denotes the group of the units of K. Set $K' := K(\zeta_p)$, $M := K'(\sqrt[p]{V_K})$ and $G := \mathrm{Gal}(M/K')$.

Observe that a tame prime $\mathfrak{l}$ of K splits in K'/K, and is unramified in M/K'. Choose a prime $\mathfrak{L}$ of K' above $\mathfrak{l}$, and denote by $\sigma_\mathfrak{L} \in G$ its Frobenius element in M/K. Observe also that if we take another prime $\mathfrak{L}'$ over $\mathfrak{l}$, then there exists $\lambda \in \mathbf{Z}/p\,\mathbf{Z}$ such that $\lambda \neq 0$ and $\sigma_\mathfrak{L} = \lambda\sigma_{\mathfrak{L}'}$ (we use additive notation). From now on, for each tame prime $\mathfrak{l}$ of K, we fix a Frobenius $\sigma_\mathfrak{L} \in G$, and we note it $\sigma_\mathfrak{l}$. Let us recall the following result of Gras–Munnier [10] (see also [11]).

Theorem 1.1. *There exist a $\mathbf{Z}/p$-extension L/K, exactly and totally ramified at tame primes $\{\mathfrak{l}_1, ..., \mathfrak{l}_m\}$, if and only if there exist $a_1, ..., a_m \in (\mathbf{Z}/p\,\mathbf{Z})^\times$ such that*

$$\sum_{i=0}^{m} a_i \sigma_{\mathfrak{l}_i} = 0 \in G.$$

As easy consequence we get

Corollary 1.2. *Let $\mathfrak{l}$ be a tame prime of K. There exists no $\mathbf{Z}/p$-extension L/K unramified outside $\mathfrak{l}$ if and only if $p \nmid \#\,\mathrm{Cl}_K$ and $\sigma_\mathfrak{l} \neq 0 \in \mathrm{Gal}(M/K')$.*

Remark 1.3. For $p > 2$, and $K = \mathbf{Q}$, $M = \mathbf{Q}(\zeta_p)$, $G = 1$, and then for every prime $p|(\ell - 1)$, there exists a $\mathbf{Z}/p$-extension $L/\mathbf{Q}$ exactly ramified at ℓ (this is a subextension of $\mathbf{Q}(\zeta_\ell)/\mathbf{Q}$).

1.1.2. *Tame Ray class group of real quadratic fields.* Let $\ell, p \geq 5$ be primes such that $p \mid (\ell - 1)$.

Let $\Delta \in \mathcal{D}_\ell$, $K = \mathbf{Q}(\sqrt{\Delta})$ and let $\mathfrak{l}$ and $\mathfrak{l}'$ be the prime ideals above ℓ in K. By Remark 1.3, there exists a $\mathbf{Z}/p$-extension L/K unramified outside ℓ. By Theorem 1.1 there is no $\mathbf{Z}/p$-extension of K unramified outside $\mathfrak{l}$ if and only if $p \nmid h(\Delta)$ and $\sigma_\mathfrak{l} \neq 0 \in \mathrm{Gal}(K(\sqrt[p]{\varepsilon_\Delta})/K')$. Thus, we get the following

Proposition 1.4. *There is no $\mathbf{Z}/p\,\mathbf{Z}$-extension of K unramified outside $\mathfrak{l}$, if and only if*

(*i*) *$p \nmid h(\Delta)$ and,*
(*ii*) *ε_Δ is not a pth power modulo $\mathfrak{l}$, or equivalently $\log_{\mathfrak{l},p}(\varepsilon_\Delta) \neq 0$.*

Observe that (*ii*) does not depend on the choice of $\mathfrak{l}|\ell$.

Definition 1.5. Given a fundamental discriminant $\Delta > 0$, set

$$a_{\Delta,\mathfrak{l},p} := h(\Delta) \cdot \log_{\mathfrak{l},p}(\varepsilon_\Delta) \in \mathbf{Z}/p\,\mathbf{Z}\,.$$

Observe that $a_{\Delta,\mathfrak{l},p} \neq 0$ if and only if, there is no $\mathbf{Z}/p\,\mathbf{Z}$-extension of K unramified outside $\mathfrak{l}$.

Proposition 1.6. *With the notation above, we have $a_{\Delta,\mathfrak{l},p} \neq 0$ if and only if $p \nmid h_\ell^-(\Delta)$.*

Proof. Assume first that $p \mid h(\Delta)$. Since $h(\Delta) = h^-(\Delta)$, then $p \mid h_\ell^-(\Delta)$, so the Proposition trivially holds in this case. From now on, assume that $p \nmid h(\Delta)$.

Assume $\log_{\mathfrak{l},p}(\varepsilon_\Delta) = 0$. By Proposition 1.4, there exists a $\mathbf{Z}/p$-extension L/K exactly ramified at $\mathfrak{l}$ (*i.e.* ramified at $\mathfrak{l}$ and unramified outside $\mathfrak{l}$). The action of $\mathrm{Gal}(K/\mathbf{Q})$ on L/K produces a $\mathbf{Z}/p$-extension L'/K exactly ramified at $\mathfrak{l}'$. Let K_ℓ^{ab} be the maximal abelian p-extension of K unramified outside ℓ. Then $LL' \subset K_\ell^{ab}$, and by Global Class Field Theory, $\mathrm{Cl}_{K,\ell} \otimes_{\mathbf{Z}} \mathbf{Z}_p \simeq \mathrm{Gal}(K_\ell^{ab}/K)$. Moreover $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Cl}_{K,\ell}$, and this action is not trivial (it permutes L and L'). Thus, $p \mid h_\ell^-(\Delta)$, and we conclude that $a_{\Delta,\mathfrak{l},p} = 0$ implies $p \mid h_\ell^-(\Delta)$.

Suppose now that $p \mid h_\ell^-(\Delta)$. Since $p \nmid h(\Delta) = h^-(\Delta)$, there exists a $\mathbf{Z}/p$-extension L/K such that $\mathrm{Gal}(K/\mathbf{Q})$ acts by -1 on $\mathrm{Gal}(L/K)$, and in particular the extension L/K is exactly ramified at $\mathfrak{l}$ and at $\mathfrak{l}'$. Moreover, by Remark 1.3 there exists a $\mathbf{Z}/p$-extension $L_0/\mathbf{Q}$ exactly ramified at ℓ. The $\mathbf{Z}/p$-extension L_0K/K is exactly ramified at $\mathfrak{l}$ and at $\mathfrak{l}'$, and the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ acts trivially on $\mathrm{Gal}(L_0K/K)$. Hence $L_0K \neq L$. In the compositum L_0KL/K let us consider the subfield L_1/K fixed by the inertia at $\mathfrak{l}'$. This is $\mathbf{Z}/p$-extension unramified outside $\mathfrak{l}$, and since $p \nmid h(\Delta)$, L_1/K is exactly ramified at $\mathfrak{l}$. By Proposition 1.4 (ii), we get $\log_{\mathfrak{l},p}(\varepsilon_\Delta) = 0$. □

Remark 1.7. When K and p are fixed and $p \nmid h(\Delta)$, the density of primes ℓ with $a_{\Delta,\mathfrak{l},p} = 0$ is equal to $\frac{1}{p}$ by the Chebotarev density theorem. This follows directly from Theorem 1.1.

1.2. **The case of Sophie Germain primes.** The goal of this section is to prove the existence of $\Delta \in \mathcal{D}_\ell$ such that $a_{\Delta,\mathfrak{l},p} \neq 0$ when $\ell = 2p+1$ (*i.e.* $p = \frac{\ell-1}{2}$ is a *Sophie Germain prime*).

1.2.1. *Upper bounds for the class number of real quadratic fields.* We shall need an upper bound for $h(\Delta)$, where Δ is the discriminant of a real quadratic field. By [16, Theorem (a)], we have

$$h(\Delta) \leq \frac{\sqrt{\Delta}}{2}. \tag{2}$$

However, this bound (which is valid for all Δ) will not be good enough for our purposes. To get a bound on $h(\Delta)$, it is enough using the class number formula to get an upper bound on $|L(\chi_\Delta, 1)|$ and a lower bound on ϵ_Δ. To the best of the authors' knowledge, the best general available explicit upper bound is given by [14, Theorem 2]: we have $|L(\chi_\Delta, 1)| \leq \frac{9}{20} \cdot \log(\Delta)$ for $\Delta \geq 2 \cdot 10^{49}$, but this would also not be enough for our purposes.

Instead, we are going to use two explicit upper-bounds due to [16] and [27], which are better and valid even for relatively small Δ, but assume that 3 is inert in K (and 2 ramifies in K for one of them; let us also note that the result we need from [16] follows easily from the techniques of [19]). This turns out to be suitable for Theorem 1.11. The upper-bounds we get as a corollary of [16] and [27] are the following.

Proposition 1.8. *Assume that* 3 *is inert in* K. *If* $\Delta \geq 442368$, *we have* $h(\Delta) \leq \frac{\sqrt{\Delta}}{3}$. *If in addition* 2 *ramifies in* K *and* $\Delta > 4 \cdot 2^6 \cdot 6^9 \cdot e^{24} = 6.83\ldots \cdot 10^{19}$, *then* $h(\Delta) \leq \frac{\sqrt{\Delta}}{6}$.

Proof. We first check that the inequality $h(\Delta) \leq \frac{\sqrt{\Delta}}{3}$ holds for $\Delta \geq 442368$. Recall that by the class number formula, we have

$$h(\Delta) = \frac{\sqrt{\Delta}}{2\log(\epsilon_\Delta)} \cdot L(\chi_\Delta, 1).$$

We have $\epsilon_\Delta = \frac{a+b\sqrt{\Delta}}{2}$ with $a, b \in \mathbf{Z}$. The assumption $\epsilon_\Delta > 1$ implies easily $a, b > 0$. In particular, we have $\epsilon_\Delta > \frac{\sqrt{\Delta}}{2}$ so $\log(\epsilon_\Delta) > \frac{\log(\Delta)}{2} - \log(2)$.

Using the assumption $\chi_\Delta(3) = -1$ (*i.e.* 3 is inert in K), a direct application of [27, Corollary] with $q = \Delta$, $h = 3$ and $k = 1$ gives, for $\Delta \geq 25$:

$$|L(\chi_\Delta, 1)| < \frac{1}{4} \cdot (\log(\Delta) + \log(12)).$$

(Let us note that the absolute values are actually superfluous, as $L(\chi_\Delta, 1) > 0$ by the class number formula.)

We thus get

$$h(\Delta) < \frac{\sqrt{\Delta}}{4} \frac{\log(\Delta) + \log(12)}{\log(\Delta) - 2\log(2)}.$$

For $\Delta \geq 4 \cdot 48^3 = 442368$, we have

$$\frac{\log(\Delta) + \log(12)}{\log(\Delta) - 2\log(2)} = 1 + \frac{\log(48)}{\log(\Delta) - \log(4)} \leq \frac{4}{3}.$$

Therefore we get $h(\Delta) \leq \frac{\sqrt{\Delta}}{3}$, as wanted.

Let us now assume that 2 ramifies in K. By [16, Lemma 3], we have

$$|L(\chi_\Delta, 1)| < \frac{1}{8} \cdot (\log(\Delta) + 3\log(6) + 8).$$

We thus get

$$h(\Delta) < \frac{\sqrt{\Delta}}{8} \frac{\log(\Delta) + 3\log(6) + 8}{\log(\Delta) - 2\log(2)}.$$

For $\Delta \geq 4 \cdot 2^6 \cdot 6^9 \cdot e^{24} = 6.83\ldots \cdot 10^{19}$, we have

$$\frac{\log(\Delta) + 3\log(6) + 8}{\log(\Delta) - 2\log(2)} = 1 + \frac{\log(4) + 3\log(6) + 8}{\log(\Delta) - \log(4)} \leq \frac{4}{3}.$$

Therefore we get $h(\Delta) \leq \frac{\sqrt{\Delta}}{6}$, as wanted. □

Remark 1.9. One checks numerically that the inequality $h(\Delta) \leq \frac{\sqrt{\Delta}}{3}$ (with 3 inert in K) holds for $\Delta < 442368$ unless $\Delta \in \{5, 8\}$.

1.2.2. *Explicit construction of certain real quadratic fields.* Recall that p and ℓ are primes such that $p \mid (\ell - 1)$.

Lemma 1.10. *Assume $p > 2$. Let $a, b \in \mathbf{Z}$ and $q \neq \ell$ be an odd prime (possibly equal to p). Suppose that*

(i) $b = a^2 \pm 1$,
(ii) $\left(\dfrac{\ell^2 + 2a\ell + b}{q}\right) = -1$,
(iii) $b \equiv c^2$ *(modulo ℓ) for some $c \in \mathbf{Z}$,*
(iv) $\log_{\ell,p}(a + c) \neq 0$.

Let Δ be the discriminant of the number field $K = \mathbf{Q}(\sqrt{\ell^2 + 2a\ell + b})$. Then we have $\Delta \in \mathcal{D}_\ell$, q is inert in K and $\log_{\mathfrak{l},p}(\epsilon_\Delta) \neq 0$ for any prime $\mathfrak{l}$ above ℓ in K.

Proof. Let $D = \ell^2 + 2a\ell + b = (\ell + a)^2 \pm 1$ and $K = \mathbf{Q}(\sqrt{D})$. Note that if $D \leq 0$, then either $D = -1$ and $a = -\ell$, which contradicts (iv) using the assumption $p > 2$, or $D = 0$ which contradicts assumption (ii). Thus, we have $D > 0$. We also have $K \neq \mathbf{Q}$ by (ii). Note that $\ell \nmid c$, as otherwise $a^2 \equiv \mp 1$ (modulo ℓ), which would contradict (iv) since $p > 2$. Finally ℓ splits in K by (iii) and the fact that $\ell \nmid c$. Therefore, we have proved that the discriminant Δ of K satisfies $\Delta \in \mathcal{D}_\ell$.

Let $\mathfrak{l}$ be the prime above ℓ in K such that $-c + \sqrt{D} \in \mathfrak{l}$, and let $u = \ell + a + \sqrt{D}$, which belongs to the ring of integers of K. By (i), we have $N_{K/\mathbf{Q}}(u) = a^2 - b = \mp 1$. Hence, u is a (nonzero) power of the fundamental unit ϵ_Δ of K. We have $u \equiv a + c$ (modulo $\mathfrak{l}$), so by (iv) $\log_{\mathfrak{l},p}(u) \neq 0$, which implies $\log_{\mathfrak{l},p}(\epsilon_\Delta) \neq 0$. □

1.2.3. *Sophie Germain primes.* Let us apply this construction in the case of Sophie Germain primes.

Theorem 1.11. *Assume $\ell \geq 11$ is such that $\frac{\ell-1}{2}$ is a Sophie Germain prime, i.e. $\ell = 2p+1$ with $p \geq 5$. Then there exists $\Delta \in \mathcal{D}_\ell$ such that*

$$h(\Delta) \cdot \log_{\mathfrak{l},p}(\epsilon_\Delta) \neq 0$$

for any prime $\mathfrak{l}$ above ℓ in $K = \mathbf{Q}(\sqrt{\Delta})$ and 3 is inert in $K/\mathbf{Q}$.

Proof. We check numerically that the theorem holds for p such that $p^2 < 2^6 \cdot 6^9 \cdot e^{24}$, *i.e.* $p < 4.13\ldots \cdot 10^9$. More precisely, in this situation there are $11,912,302$ Sophie Germain primes, and for each one we can find a field K with discriminant $D \leq 236$ that satisfies the theorem. We can thus assume that $p^2 \geq 2^6 \cdot 6^9 \cdot e^{24}$.

Let us apply the construction of Lemma 1.10. We first claim that there exists $a \in \{3,5,7\}$ such that a^2-1 is a square modulo ℓ. Indeed, otherwise we would get

$$\left(\frac{8}{\ell}\right) = \left(\frac{24}{\ell}\right) = \left(\frac{48}{\ell}\right) = -1$$

which is clearly impossible. Now, choose $a \in \mathbf{Z}$ such that the following three conditions are satisfied:

- $a \equiv 3, 5$ or 7 (modulo ℓ) such that a^2-1 is a square modulo ℓ (this is possible by the above argument),
- $2 \mid a$,
- $a \equiv 1$ (modulo 3).

By the Chinese remainder theorem, we can find such an a with $-4\ell < a < 2\ell$. Let $b = a^2-1$, and consider the number field $K = \mathbf{Q}(\sqrt{D})$ where $D = \ell^2 + 2a\ell + b$. Let Δ be the discriminant of K, which divides D since $D \equiv 0$ (modulo 4) (because b is odd).

Note that the conditions (i) and (iii) of Lemma 1.10 are satisfied by construction. Furthermore, the condition $a \equiv 1$ (modulo 3) implies $D \equiv -1$ (modulo 3) (we use the fact that $\ell \equiv -1$ (modulo 3) as $\ell = 2p+1$ with $p > 3$ prime). Thus, condition (ii) is satisfied for $q = 3$. Let us check that condition (iv) is also satisfied. Let c such that $b \equiv c^2$ (modulo ℓ). If $\log_{\ell,p}(a+c) = 0$, then $a+c$ is a pth power modulo ℓ. Since $\ell = 2p+1$, this means that $a+c \equiv \pm 1$ (modulo ℓ). We get $c \equiv -a \pm 1$ (modulo ℓ), so $c^2 \equiv (a \pm 1)^2 \equiv a^2 + 1 \pm 2a$ (modulo ℓ), so $a \equiv \pm 1$ (modulo ℓ), which is impossible since $a \equiv 3, 5$ or 7 (modulo ℓ) and $\ell > 3$. By Lemma 1.10, we get that $\Delta \in \mathcal{D}_\ell$ (in particular, K is a real quadratic field) and $\log_{\mathfrak{l},p}(\epsilon_\Delta) \neq 0$.

Let us now prove that $p \nmid h(\Delta)$. For the sake of a contradiction, assume $p \mid h(\Delta)$ and in particular $h(\Delta) \geq p$. Since $\Delta \geq 4h(\Delta)^2$ by (2), we get $\Delta \geq 4p^2 \geq 4 \cdot 2^6 \cdot 6^9 \cdot e^{24}$.

Assume first that Δ is odd. Then Δ divides $\frac{D}{4} = \frac{(\ell+a)^2-1}{4} = \frac{(\ell+a-1)}{2} \cdot \frac{(\ell+a+1)}{2}$. Since visibly $\frac{D}{4}$ is even, actually Δ divides $\frac{D}{8}$. Since $\Delta \geq 4 \cdot 2^6 \cdot 6^9 \cdot e^{24} \geq 442368$, by the first inequality of Proposition 1.8 we get $h(\Delta) \leq \frac{1}{3} \cdot \sqrt{\frac{D}{8}} = \frac{1}{6\sqrt{2}} \cdot \sqrt{D}$. Since $D = (\ell+a)^2 - 1$, we have $h(\Delta) < \frac{1}{6\sqrt{2}} \cdot |\ell + a|$, and since $-4\ell < a < 2\ell$, we get $h(\Delta) < \frac{1}{2\sqrt{2}}\ell = \frac{1}{\sqrt{2}}p + \frac{1}{2\sqrt{2}} < p$, which is a contradiction. This proves that $p \nmid h(\Delta)$.

Assume now that Δ is even. Since $\Delta \geq 4 \cdot 2^6 \cdot 6^9 \cdot e^{24}$, 2 ramifies in K and 3 is inert in K, the second inequality of Proposition 1.8 yields $h(\Delta) \leq \frac{\sqrt{\Delta}}{6} \leq \frac{\sqrt{D}}{6}$. Since $D = (\ell+a)^2 - 1$, we have $h(\Delta) < \frac{1}{6} \cdot |\ell + a|$. Recall that $-4\ell < a < 2\ell$, so $|a + \ell| \leq 3\ell - 1$. Actually, we claim that $|a + \ell| \leq 3\ell - 3$. Otherwise, we would have $a \in \{2\ell-1, 2\ell-2, -4\ell+1, -4\ell+2\}$, which would imply $a \equiv \pm 1, \pm 2$ (modulo ℓ), *i.e.* $a^2 \equiv 1, 4$ (modulo ℓ), which is impossible as $a \equiv 3, 5, 7$ (modulo ℓ) (by construction) and $\ell > 7$. We get $h(\Delta) < \frac{1}{6} \cdot (3\ell - 3) = p$. This is a contradiction. □

1.3. **Heuristic observation.** In our context, it is natural to ask the following question: *Given two primes p and ℓ such $p \mid (\ell - 1)$, how often $a_{\Delta,\mathfrak{l},p} \neq 0$ as Δ ranges over $\mathcal{D}_\ell$?*

Let us then conduct some numerical simulations. For $p \mid \ell - 1$, $X \geq 2$, set

$$N_\ell(X) = \#\{0 < \Delta \leq X \text{ such that } \Delta \in \mathcal{D}_\ell\}$$

and

$$M_{p,\ell}(X) = \#\{0 < \Delta \leq X \text{ such that } \Delta \in \mathcal{D}_\ell \text{ and } p \nmid h_\ell^-(\Delta)\}\cdot$$

Using PARI/GP [32], we get, for $X = 10^8$:

$$M_{3,7}/N_7 \approx 0.5788;\ M_{3,13}/N_{13} \approx 0.5779;$$

$$M_{5,11}/N_{11} \approx 0.7630;\ M_{5,101}/N_{101} \approx 0.7625;$$

$$M_{7,29}/N_{29} \approx 0.8380;\ M_{7,43}/N_{43} \approx 0.8381.$$

These results should be compared with the quantities $\eta^1(3) \approx 0.5925$, $\eta^1(5) \approx 0.7680$, and $\eta^1(7) \approx 0.8396$.

As we noted in the introduction, we suspect that the quantity $M_{p,\ell}(X)/N_\ell(X)$ converges to $\eta^1(p)$ as X tends to infinity. The interpretation could be as follows. First of all, as with the Cohen–Lenstra heuristics for the p-Sylow subgroup of the class group of quadratic fields, everything takes place in the minus part. Next, let us recall the central idea that allows us to move from a density of indivisibility for class groups of imaginary quadratic fields to a density of indivisibility for class groups of real quadratic fields. It is based on the following principle: For a family of abelian groups (corresponding to the class group of imaginary quadratic fields), there is an associated family of groups in which each group is the quotient group of a randomly chosen element of a group from the original family (corresponding to the class group of real quadratic fields). We then move from $\eta^1(p)$ to $\eta^2(p)$. Observe now that in the case of real quadratic fields, we move from the ray class group of modulus $\mathfrak{l}$ to the class group by taking the quotient with respect to the ramification subgroup at $\mathfrak{l}$, which is cyclic in this case. Within the heuristic framework, this can also be viewed as a quotient by some arbitrary element. Thus, we return from $\eta^2(p)$ to $\eta^1(p)$.

2. Eisenstein congruences in weight 2

Notation. We keep the same notation as above. In this section, we assume $p \geq 5$. Recall that Δ denotes the discriminant of a real quadratic field $K = \mathbf{Q}(\sqrt{\Delta})$. We fix an embedding $K \hookrightarrow \mathbf{R}$. We let $h^+(\Delta)$ be the cardinality of the *narrow* class group $\mathrm{Cl}^+(K)$, and ϵ_Δ^+ be the smallest *totally positive* unit of K which is > 1. Note that here the $+$ in the exponent is not related to the action of $\mathrm{Gal}(K/\mathbf{Q})$ (contrary to the notation $h_\ell^-(\Delta)$). Note that $h^+(\Delta) = 2h(\Delta)$ or $h(\Delta)$, depending on whether $\epsilon_\Delta^+ = \epsilon_\Delta$ or $\epsilon_\Delta^+ = \epsilon_\Delta^2$ respectively. In any case, we have $(\epsilon_\Delta^+)^{h^+(\Delta)} = \epsilon_\Delta^{2h(\Delta)}$.

2.1. **Review of Mazur's Eisenstein ideal.** In this paragraph, we briefly recall some well-known facts about the Eisenstein ideal theory as developed by Mazur in his seminal paper [22]. Let us note that, following Mazur, most papers on this topic have used the notation N for our prime ℓ. Since the focus of our paper is classical algebraic number theory, we have decided to use the more common letter ℓ to denote that prime.

Let $\mathbb{T}^0$ be Hecke algebra over $\mathbf{Z}$ acting on the space $S_2(\Gamma_0(\ell))$ of weight 2 cuspforms of level $\Gamma_0(\ell)$. It is generated by the Hecke operators T_q for primes $q \neq \ell$ as well as the operator U_ℓ. Mazur defined the *Eisenstein ideal* $I \subset \mathbb{T}^0$ as the ideal generated by the operators $T_q - q - 1$ for primes $q \neq \ell$ and by $U_\ell - 1$. Mazur proved in [22, Proposition II.9.7] that $\mathbb{T}^0/I$ is cyclic of order the numerator of $\frac{\ell-1}{12}$. In particular, since $p \geq 5$ divides $\ell - 1$, there is a ring homomorphism

$$\mathbb{T}^0 \to \mathbf{Z}/p\mathbf{Z} \tag{3}$$

whose kernel is the maximal ideal $\mathfrak{P} = I + p\mathbb{T}^0$.

Mazur constructed in [22, Proposition II.18.9 and Theorem II.18.10] an *explicit* group isomorphism

$$I/I^2 \xrightarrow{\sim} (\mathbf{Z}/\ell\mathbf{Z})^\times/\mu_{12}, \tag{4}$$

where μ_{12} is the subgroup of elements of order dividing 12 in $(\mathbf{Z}/\ell\,\mathbf{Z})^\times$. In particular, if we denote by $\mathbb{T}^0_I$ the I-adic completion of $\mathbb{T}^0$, then the ideal $I\cdot\mathbb{T}^0_I$ is principal. Similarly, denoting by $\mathbb{T}^0_{\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of $\mathbb{T}^0$, the ideal $I\cdot\mathbb{T}^0_{\mathfrak{P}}$ of $\mathbb{T}^0_{\mathfrak{P}}$ is principal.

Consider the first singular homology group $H_1(X_0(\ell),\mathbf{Z})$ of the compact modular curve $X_0(\ell)$. It carries a natural action of $\mathbb{T}^0$ as well as the complex conjugation c (induced by the map $x+iy\mapsto -x+iy$ on the upper-half plane). Following the notation of [22, II.18], we denote by H_+ the subgroup of $H_1(X_0(\ell),\mathbf{Z})$ fixed by c. By [23, Proposition 5], $H_1(X_0(\ell),\mathbf{Z})$ is *acyclic* for the action of c, *i.e.* $H_+=(1+c)\cdot H_1(X_0(\ell),\mathbf{Z})$. If α and β are elements in the completed upper-plane (*i.e.* elements of $\mathbf{P}^1(\mathbf{Q})$ or of the upper-half plane), we denote by $\{\alpha,\beta\}$ the relative homology class of the image in $X_0(\ell)$ of the geodesic path between α and β. We have $\{\alpha,\beta\}\in H_1(X_0(\ell),\mathbf{Z})$ if the images of α and β in $X_0(\ell)$ coincide.

Mazur's homomorphism (4) can be conveniently described using H_+, using a slight modification of [22, II.18] relying on the acyclicity of $H_1(X_0(\ell),\mathbf{Z})$ for c. This modification is due to Merel [23, §4.1], who used the subgroup U of 12th powers of $(\mathbf{Z}/\ell\,\mathbf{Z})^\times$ instead of our quotient $(\mathbf{Z}/\ell\,\mathbf{Z})^\times/\mu_{12}$ (the two groups being canonanically isomorphic).

Namely, [22, Proposition II.18.8] implies that there is a group isomorphism

$$H_+/I\cdot H_+\xrightarrow{\sim}(\mathbf{Z}/\ell\,\mathbf{Z})^\times/\mu_{12} \tag{5}$$

sending $(1+c)\cdot\{z_0,\gamma\cdot z_0\}$ to d modulo ℓ, where $\gamma=\begin{pmatrix}*&*\\*&d\end{pmatrix}\in\Gamma_0(\ell)$ and z_0 is any point in the completed upper-half plane, *i.e.* an element of $\mathbf{P}^1(\mathbf{Q})$ or of the upper-half plane (the element $\{z_0,\gamma\cdot z_0\}$ of $H_1(X_0(\ell),\mathbf{Z})$ does not depend on the choice of z_0).

Following [22, II.18 Definition p. 137], consider the *winding homomorphism*

$$e_+ : I\to H_+ \tag{6}$$

defined by sending $\eta\in I$ to $\eta\cdot\{0,\infty\}$. Let $(H_+)_I$ be the I-adic completion of H_+, which is canonically identified with $H_+\otimes_{\mathbb{T}^0}\mathbb{T}^0_I$. By [22, Theorem II.18.10], e_+ induces an *isomorphism*

$$e_+ : I\cdot\mathbb{T}^0_I\to(H_+)_I.$$

In particular, e_+ induces a group isomorphism $I/I^2\xrightarrow{\sim}H_+/I\cdot H_+$, and the map (4) is then the composition of (5) with that latter isomorphism.

2.2. **Eisenstein congruence and periods.** The ring homomorphism (3) corresponds to the existence of a newform $F=\sum_{n\geq1}a_n(F)q^n\in S_2(\Gamma_0(\ell))$ such that, for all primes $q\neq\ell$, we have $a_q(F)\equiv q+1$ (modulo $\mathfrak{P}_F$), and $a_\ell(F)\equiv1$ (modulo $\mathfrak{P}_F$) (actually, it is known that $a_\ell(F)=1$). Here, $\mathfrak{P}_F$ is a certain maximal ideal above p in the ring of coefficients $\mathcal{O}_F:=\mathbf{Z}[a_n(F)]_{n\geq1}$ of F, which an order in the ring of integers of the Hecke field $K_F:=\mathbf{Q}(a_n(F),n\geq1)\subset\mathbf{C}$. Such a form may not be unique in general.

Equivalently, we have an *Eisenstein congruence*

$$F\equiv E_{2,\ell}\ (\text{modulo }\mathfrak{P}_F) \tag{7}$$

where

$$E_{2,\ell}=\frac{\ell-1}{24}+\sum_{n\geq1}\left(\sum_{\substack{d\mid n\\(d,\ell)=1}}d\right)q^n$$

is the (unique) Eisenstein series of weight 2 and level $\Gamma_0(\ell)$. In the rest of this paper, we shall fix a newform F and a maximal ideal $\mathfrak{P}_F\subset\mathcal{O}_F$ above p satisfying the Eisenstein congruence (7). Note that there is a surjective ring homomorphism

$$\varphi_F:\mathbb{T}^0\to\mathcal{O}_F$$

and that we have $\mathfrak{P}_F = \varphi_F(\mathfrak{P})$. Let $\mathfrak{a}_F = \ker(\varphi_F)$ and $I_F = \varphi_F(I)$. Note that we have $\mathfrak{a}_F \subset \mathfrak{P}$ and $I_F \subseteq \mathfrak{P}_F$.

Let $\mathcal{O}_{\mathfrak{P}_F}$ be the $\mathfrak{P}_F$-adic completion of $\mathcal{O}_F$. Note that $\mathcal{O}_{\mathfrak{P}_F}$ is not *a priori* a DVR, as $\mathcal{O}_F$ may be a strict order. The map φ_F induces a surjective homomorphism of $\mathbf{Z}_p$-algebras

$$\varphi_{F,\mathfrak{P}} : \mathbb{T}^0_{\mathfrak{P}} \to \mathcal{O}_{\mathfrak{P}_F} \tag{8}$$

sending $I \cdot \mathbb{T}^0_{\mathfrak{P}}$ to $I_F \cdot \mathcal{O}_{\mathfrak{P}_F}$, and therefore induces a surjective group homomorphism

$$I \cdot \mathbb{T}^0_{\mathfrak{P}}/I^2 \cdot \mathbb{T}^0_{\mathfrak{P}} \to I_F \cdot \mathcal{O}_{\mathfrak{P}_F}/I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F}.$$

Note that

$$I \cdot \mathbb{T}^0_{\mathfrak{P}}/I^2 \cdot \mathbb{T}^0_{\mathfrak{P}} = (I/I^2) \otimes_{\mathbf{Z}} \mathbf{Z}_p\,,$$

and that we have a surjective group homomorphism $(I/I^2) \otimes_{\mathbf{Z}} \mathbf{Z}_p \to \mathbf{Z}/p\mathbf{Z}$ given by composing $\log_{\ell,p}$ with (4). Thus, our choice of $\log_{\ell,p}$ induces a surjective group homomorhism

$$I \cdot \mathbb{T}^0_{\mathfrak{P}}/I^2 \cdot \mathbb{T}^0_{\mathfrak{P}} \to \mathbf{Z}/p\mathbf{Z}\,. \tag{9}$$

Lemma 2.1. *The map (9) factors through the map*

$$I \cdot \mathbb{T}^0_{\mathfrak{P}}/I^2 \cdot \mathbb{T}^0_{\mathfrak{P}} \to I_F \cdot \mathcal{O}_{\mathfrak{P}_F}/I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F}.$$

Thus, we have a surjective group homomorphism

$$I_F \cdot \mathcal{O}_{\mathfrak{P}_F}/I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F} \to \mathbf{Z}/p\mathbf{Z} \tag{10}$$

depending only on the choice of $\log_{\ell,p}$.

Proof. Since $I \cdot \mathbb{T}^0_{\mathfrak{P}}/I^2 \cdot \mathbb{T}^0_{\mathfrak{P}}$ is a cyclic p-group, it suffices to prove that $I_F \cdot \mathcal{O}_{\mathfrak{P}_F}/I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F}$ is non-trivial. Otherwise, we would have $I_F \cdot \mathcal{O}_{\mathfrak{P}_F} = I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F}$, so $I_F \cdot \mathcal{O}_{\mathfrak{P}_F} = \mathfrak{P}_F \cdot I_F \cdot \mathcal{O}_{\mathfrak{P}_F}$, and by Nakayama's lemma $I_F \cdot \mathcal{O}_{\mathfrak{P}_F} = 0$ which is impossible. □

We shall need the following result in order to prove our congruence formula for L-values. We use the well-known fact that the L-value $L(F,1) = \int_{\{0,\infty\}} 2i\pi F(z)dz$ is non-zero (this is a consequence of [22, Theorem II.18.10]).

Proposition 2.2. *Consider the group homomorphism* $p_F : H_+ \to \mathbf{C}$ *defined by*

$$p_F(x) = \frac{\int_x 2i\pi F(z)dz}{L(F,1)}.$$

(This is well-defined since, as recalled above, we have $L(F,1) \neq 0$*.)*

(i) We have $p_F(H_+) \subseteq K_F$*, the latter being naturally a subfield of the fraction field of* $\mathcal{O}_{\mathfrak{P}_F}$*. Furthermore, we actually have* $p_F(H_+) \subseteq I_F \cdot \mathcal{O}_{\mathfrak{P}_F}$*. In particular, one gets a natural map*

$$H_+ \to I_F \cdot \mathcal{O}_{\mathfrak{P}_F}/I_F^2 \cdot \mathcal{O}_{\mathfrak{P}_F}$$

whose composition with the map (10) of Lemma 2.1 yields a surjective group homomorphism

$$\alpha_F : H_+ \to \mathbf{Z}/p\mathbf{Z}\,, \tag{11}$$

depending only on the choice of $\log_{\ell,p}$ *and* F*, and whose kernel contains* I *and* $\mathfrak{a}_F$*.*

(ii) For any z_0 *in the completed upper-half plane and* $\gamma = \begin{pmatrix} * & * \\ * & d \end{pmatrix} \in \Gamma_0(\ell)$*, we have*

$$\alpha_F((1+c)\cdot\{z_0, \gamma\cdot z_0\}) = \log_{\ell,p}(d).$$

In particular, α_F *depends only on the choice of* $\log_{\ell,p}$*, and not on the choice of* F *satisfying the Eisenstein congruence (7).*

Proof. It will be convenient to extend slightly the definition of $p_F(x)$ to the *Manin-Drinfeld modification* $\tilde{H}_+$ of H_+. Consider the relative homology group $H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z})$, where cusps is the finite set of cusps of $X_0(\ell)$, namely the cusps 0 and ∞ (since ℓ is prime). Let $\mathbb{T}$ be the Hecke algebra (over $\mathbf{Z}$) acting faithfully on $H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z})$. Note that $\mathbb{T}^0$ is a quotient of $\mathbb{T}$, and that we have a $\mathbb{T}$-equivariant short exact sequence

$$0 \to H_1(X_0(\ell), \mathbf{Z}) \to H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z}) \to \mathbf{Z}[\mathrm{cusps}]^0 \to 0$$

where $\mathbf{Z}[\mathrm{cusps}]^0$ is the group of degree zero divisors supported on the set of cusps, which is just $\mathbf{Z}$ since there are two cusps. The action of $\mathbb{T}$ on $\mathbf{Z}[\mathrm{cusps}]^0$ factors through the Eisenstein ideal of $\mathbb{T}$. Furthermore, there is a canonical $\mathbb{T}$-equivariant projection of $H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z})$ onto its subspace $H_1(X_0(\ell), \mathbf{Z})$ after inverting the numerator n of $\frac{\ell-1}{12}$. This projection $p : H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z}) \to H_1(X_0(\ell), \mathbf{Z}[\frac{1}{n}])$, called the *Manin–Drinfeld retraction*, is characterized by sending the modular symbol $\{0, \infty\}$ to the unique element

$$e \in H_1(X_0(\ell), \mathbf{Z}[\frac{1}{n}])$$

(called the *winding element*, *cf.* [22, II.18 Definition p. 136]) satisfying, for all cusp form $f \in S_2(\Gamma_0(\ell))$:

$$\int_e f(z)dz = \int_{\{0,\infty\}} f(z)dz.$$

We denote by $\tilde{H}$ the image of $H_1(X_0(\ell), \mathrm{cusps}, \mathbf{Z})$ in $H_1(X_0(\ell), \mathbf{Z}[\frac{1}{n}])$ by the Manin–Drinfeld retraction p, and by $\tilde{H}_+$ the subspace of $\tilde{H}$ fixed by the complex conjugation. Note that we have an inclusion $H_+ \subset \tilde{H}_+$ and a canonical group isomorphism $\tilde{H}_+/H_+ \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}$ sending the image of e to 1. Furthermore, $\mathbb{T}^0$ acts on $\tilde{H}_+$ and we have $I \cdot \tilde{H}_+ \subset H_+$ (*cf.* [22, Lemma II.18.6]).

Our map $p_F : H_+ \to \mathbf{C}$ extends in a natural way to a map $\tilde{p}_F : \tilde{H}_+ \to \mathbf{C}$ given by the same formula, *i.e.*

$$\tilde{p}_F(x) = \frac{\int_x 2i\pi F(z)dz}{L(F,1)}.$$

Note that, by construction, we have $\tilde{p}_F(e) = 1$. We are now ready to prove the proposition.

The fact that $\tilde{p}_F$ takes values in the Hecke field K_F of F is well-known, *cf. eg.* [25, Proposition 5.11]. Let $\tilde{M} := \tilde{p}_F(\tilde{H}_+)$ and $M := p_F(H_+)$. We have $M \subset \tilde{M} \subset K_F$. If m is a positive integer, then we have, for all $x \in \tilde{H}_+$:

$$\tilde{p}_F(T_m x) = a_m(F) \cdot \tilde{p}_F(x).$$

This proves that the kernel of $\tilde{p}_F$ (and of p_F) contain $\mathfrak{a}_F$, and furthermore that both $\tilde{M}$ and M are finitely generated sub-$\mathcal{O}_F$-modules of K_F. Note that $\tilde{M}$ contains $\mathcal{O}_F$ since $\tilde{p}_F(e) = 1$.

Denote by $\tilde{M}_{\mathfrak{P}_F}$ (resp. $M_{\mathfrak{P}_F}$) the completion of $\tilde{M}$ (resp. M) at $\mathfrak{P}_F$. We have a natural inclusion $\mathcal{O}_{\mathfrak{P}_F} \subseteq \tilde{M}_{\mathfrak{P}_F}$. The map $\tilde{p}_F : \tilde{H}_+ \to \tilde{M}$ induces, after completion at $\mathfrak{P}$ on the left and at $\mathfrak{P}_F$ on the right, a map

$$(\tilde{H}_+)_{\mathfrak{P}} \to M_{\mathfrak{P}_F}.$$

Since the winding homomorphism (6) is an isomorphism after completion at $\mathfrak{P}$, we easily see that we have $(\tilde{H}_+)_{\mathfrak{P}} = \mathbb{T}^0_{\mathfrak{P}} \cdot e$ and $(H_+)_{\mathfrak{P}} = I \cdot \mathbb{T}^0_{\mathfrak{P}} \cdot e$. Thus, we have $\tilde{M}_{\mathfrak{P}_F} = \mathcal{O}_{\mathfrak{P}_F}$ and $M_{\mathfrak{P}_F} = I_F \cdot \mathcal{O}_{\mathfrak{P}_F}$. This proves point (i).

Let us now prove point (ii). Let $\gamma = \begin{pmatrix} * & * \\ * & d \end{pmatrix} \in \Gamma_0(\ell)$ and z_0 in the completed upper-half plane. Let x be the image of $(1+c) \cdot \{z_0, \gamma \cdot z_0\}$ in $(\tilde{H}_+)_{\mathfrak{P}}$. By (i), we have $p_F(x) \in I_F \cdot \mathcal{O}_{\mathfrak{P}_F}$, and more precisely we have $p_F(x) = \varphi_{F,\mathfrak{P}}(\eta)$ where $\eta \in I \cdot \mathbb{T}^0_{\mathfrak{P}}$ is such that $x = \eta \cdot e$ and $\varphi_{F,\mathfrak{P}}$ is defined in (8). By construction, $\alpha_F((1+c) \cdot \{z_0, \gamma \cdot z_0\}) \in \mathbf{Z}/p\mathbf{Z}$ is the image of η in $\mathbf{Z}/p\mathbf{Z}$ via (9), which as we recalled at the end of §2.1 is equal to $\log_{\ell,p}(d)$. □

2.3. **Popa's formula and congruence for the L-value of real quadratic twists.** In this paragraph, we recall some consequences of a formula of Waldspurger [34] for the twisted L-value $L(F, \chi_\Delta, 1)$, where $F \in S_2(\Gamma_0(\ell))$ is a newform and $\Delta \in \mathcal{D}_\ell$ (*i.e.* such that $\chi_\Delta(\ell) = 1$).

The explicit form of the formula we shall need is due to Popa [26], and is expressed in terms of *Heegner cycles*. The main result of this paragraph is Proposition 2.3 below, which as far as we know is new, but let us emphasize that it is very similar to results obtained in [8, Proposition 5.7] and by the first author in [17, §3.3 (26)], and indeed our proof relies on similar techniques (namely Heegner cycles). A very similar result was also obtained in [18] by completely different methods.

We first recall Popa's formula, following [26, §6]. Let us fix a choice of a square root δ_ℓ of Δ modulo 4ℓ, *i.e.* $\delta_\ell \in \mathbf{Z}$ (well-defined modulo 2ℓ) such that

$$\delta_\ell^2 \equiv \Delta \text{ (modulo } 4\ell).$$

This choice determines an ideal $\mathfrak{l}$ of $\mathcal{O}_K$ above ℓ, characterized by the property

$$\sqrt{\Delta} + \delta_\ell \in \mathfrak{l}. \tag{12}$$

Let us recall briefly the notion of Heegner cycles (*cf.* [26, §6.2 and 6.3]). Recall that a $\mathbf{Q}$-algebra embedding $\Psi : K \to M_2(\mathbf{Q})$ given by

$$\Psi(\sqrt{\Delta}) = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \tag{13}$$

is called *optimal of level* ℓ if $\Psi(K) \cap M_0(\ell) = \Psi(\mathcal{O}_K)$ and *oriented* (with respect to our choice of δ_ℓ) if

$$a \equiv \delta_\ell \text{ (modulo } 2\ell). \tag{14}$$

Here, we have denoted by $M_0(\ell)$ the Eichler order of level ℓ in $M_2(\mathbf{Z})$ consisting of matrices which are upper-triangular modulo ℓ.

The group $\Gamma_0(\ell)$ acts (by conjugation) on the right on the set $\mathcal{E}_\ell$ of oriented optimal embeddings of level ℓ, and we have a natural bijection (*cf.* [26, Proposition 6.2.1])

$$\mathcal{E}_\ell/\Gamma_0(\ell) \xrightarrow{\sim} \mathrm{Cl}^+(K). \tag{15}$$

In particular, the set $\mathcal{E}_\ell/\Gamma_0(\ell)$ is finite of cardinality h_K^+. For $\Psi \in \mathcal{E}_\ell$, let

$$M_\Psi := \Psi(\epsilon_K^+) \in \Gamma_0(\ell).$$

By construction of Ψ, we have $M_\Psi = \begin{pmatrix} * & * \\ * & d_\Psi \end{pmatrix}$ with $d_\Psi = m - na$ where a is as in (13) and $m, n \in \frac{1}{2}\mathbf{Z}$ are such that $\epsilon_K^+ = m + n\sqrt{\Delta}$. It follows from (14) and our choice of $\mathfrak{l}$ in (12) that we have

$$d_\Psi \equiv \epsilon_K^+ \text{ (modulo } \mathfrak{l}). \tag{16}$$

For any z_0 in the completed upper-half plane, we thus get a homology class (independent of z_0), called a *Heegner cycle*:

$$\gamma_\Psi := \{z_0, M_\Psi z_0\} \in H_1(X_0(\ell), \mathbf{Z}).$$

As noted in [26, p.860], there is an involution $\Psi \mapsto \Psi^*$ on oriented optimal embeddings of level ℓ which preserves $\Gamma_0(\ell)$-equivalence and with the property that $\gamma_{\Psi^*} = c \cdot \gamma_\Psi$ (where c is, as above, the complex conjugation acting on $H_1(X_0(\ell), \mathbf{Z})$). We conclude that $\sum_{\Psi \in \mathcal{E}_\ell/\Gamma_0(\ell)} \gamma_\Psi$ is fixed by c, *i.e.* we have

$$2 \cdot \sum_{\Psi \in \mathcal{E}_\ell/\Gamma_0(\ell)} \gamma_\Psi = \sum_{\Psi \in \mathcal{E}_\ell/\Gamma_0(\ell)} (1 + c) \cdot \gamma_\Psi. \tag{17}$$

Let us now state Popa's formula. Let $F \in S_2(\Gamma_0(\ell))$ be a newform. As usual, denote by $L(F/K, s)$ the L-function of F based change to K. We have the well-known factorization:

$$L(F/K, s) = L(F, s)L(F, \chi_\Delta, s) \tag{18}$$

We then have, by [26, Theorem 6.3.1]:

$$L(F/K, 1) = \frac{1}{\sqrt{\Delta}} \left| \sum_{\Psi \in \mathcal{E}_\ell/\Gamma_0(\ell)} \int_{\gamma_\Psi} 2i\pi F(z)dz \right|^2.$$

Using (17) and (18), if $L(F, 1) \neq 0$ then one can rewrite Popa's formula as

$$\sqrt{\Delta} \cdot \frac{L(F, \chi_\Delta, 1)}{L(F, 1)} = \left(\frac{1}{2} \sum_{\Psi \in \mathcal{E}_\ell/\Gamma_0(\ell)} \frac{\int_{(1+c)\cdot\gamma_\Psi} 2i\pi F(z)dz}{L(F, 1)} \right)^2. \tag{19}$$

Note that we have removed the absolute values, because the complex number

$$\frac{\int_{(1+c)\cdot\gamma_\Psi} 2i\pi F(z)dz}{L(F, 1)}$$

is real (as F has trivial Nebentype). A direct consequence of Proposition 2.2 and (19), (16) and (15) is the following congruence formula.

Proposition 2.3. *Let $F \in S_2(\Gamma_0(\ell))$ be a newform satisfying the Eisenstein congruence (7). Then for all fundamental discriminant Δ of a real quadratic field in which ℓ splits, we have:*

$$\sqrt{\Delta} \cdot \frac{L(F, \chi_\Delta, 1)}{L(F, 1)} = L_F(\Delta)^2$$

for some $L_F(\Delta) \in K_F$ (the Hecke field of F), uniquely defined up to sign, such that

$$L_F(\Delta) \in I_F \cdot \mathcal{O}_{\mathfrak{P}_F} \tag{20}$$

and the image $\widetilde{L_F(\Delta)}$ of $L_F(\Delta)$ in $\mathbf{Z}/p\mathbf{Z}$ via the map (10) satisfies

$$\widetilde{L_F(\Delta)} = \pm h_\Delta \cdot \log_{\mathfrak{l},p}(\epsilon_\Delta)$$

for any prime $\mathfrak{l}$ above ℓ in $K = \mathbf{Q}(\sqrt{\Delta})$.

3. Half-integral weight modular forms

Notation. We keep the same notation as in section 2. In particular, we still assume $p \geq 5$. In all this section, we let

$$\chi : (\mathbf{Z}/\ell\,\mathbf{Z})^\times \to \mathbf{C}^\times$$

be any *odd* Dirichlet character, *i.e.* such that $\chi(-1) = -1$. We let χ' be the unique *even* Dirichlet character of level $4\ell^2$ whose restriction to $(\mathbf{Z}/\ell^2\,\mathbf{Z})^\times$ is induced by χ. Explicitly, $\chi' : (\mathbf{Z}/4\ell^2\,\mathbf{Z})^\times \to \mathbf{C}^\times$ is given by

$$\chi'(x) = (-1)^{\frac{x-1}{2}} \cdot \chi(x). \tag{21}$$

Let

$$R = \mathbf{Z}[\chi] = \mathbf{Z}[\chi']$$

be the subring of $\mathbf{C}$ in which χ takes its values. Similarly, we let $\mathbf{Q}(\chi) \subset \mathbf{C}$ be the fraction field of R.

Note that if $\ell \equiv 3$ (modulo 4) (*eg.* if $\ell = 11$, as will be the case in §5), one may choose for instance $\chi(x) = \left(\frac{x}{\ell}\right)$, in which case $R = \mathbf{Z}$, which would simplify the notation in our arguments.

3.1. **The generalized Shimura lifting of Baruch–Mao.** The goal of this section is to combine the congruence of Proposition 2.3 with a generalization of the Kohnen–Zagier formula for half-integral weights modular forms due to [2] in order to construct a modulo p weight $\frac{3}{2}$ modular form whose Δth coefficient controls the vanishing of $h(\Delta)\cdot \log_{\mathfrak{l},p}(\epsilon_\Delta)$. Our main result is stated in Theorem 3.4 below.

There is a well-defined notion of half-integral weight modular form with coefficients in any (commutative) ring A in which the level is invertible, *cf.* [28]. Thus, if $M \in \mathbf{N}$ and A is a commutative ring with $4M \in A^\times$, one can consider the space $S_{\frac{3}{2}}(\Gamma_1(4M), \psi)_A$ of weight $\frac{3}{2}$ cuspforms with coefficients in A of level $\Gamma_1(4M)$ and character $\psi : (\mathbf{Z}/4M\,\mathbf{Z})^\times \to A^\times$. If we do not indicate the base ring A in the notation, it means we take $A = \mathbf{C}$.

Let $F \in S_2(\Gamma_0(\ell))$ be a newform. Let w_ℓ be the Atkin–Lehner involution. We assume that

$$w_\ell F = -F,$$

i.e. that the sign of the functional equation of $L(F, s)$ is 1. Recall that, as ℓ is prime, we have $w_\ell = -U_\ell$ on $S_2(\Gamma_0(\ell))$. Therefore U_ℓ is an involution, and our assumption amounts to $U_\ell F = F$.

Remark 3.1. This assumption holds in particular if F satisfies the Eisenstein congruence (7). Indeed, in this case we have $U_\ell F \equiv F$ (modulo $\mathfrak{P}_F$) and, since $p > 2$, we conclude that $U_\ell F = F$ (this is well-known, even for $p = 2$, and follows from [22, Proposition II.17.10]) As recalled before, for such a residually Eisenstein F, we actually have the stronger fact that $L(F, 1) \neq 0$.

We now use [2, Theorem 10.1] to construct a weight $\frac{3}{2}$ Hecke eigenform whose Fourier coefficients are related to the twisted L-values $L(F, \chi_\Delta, 1)$. The reader may also refer to [21, Theorem 1.4] (which is more general and deals with odd but not necessarily prime levels).

By applying [2, Theorem 10.1] with $N = N' = \ell$, $S = \{\ell\}$, we get that here exists a non-zero

$$f_\chi = \sum_{n\geq 1} a_n(f_\chi) q^n \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi'),$$

unique up to non-zero scalar, satisfying the following properties:

(i) f_χ is a Shimura lift of F. This condition is a generalization of Shimura's original notion of lift [30]. It is expressed explicitly in a classical language in [21, §1.1]. This means that for all prime $q \nmid 2\ell$, we have

$$T_{q^2} f_\chi = \chi(q)\cdot a_q(F)\cdot f_\chi.$$

(Recall (*cf.* *eg.* [5, §3]) that

$$a_n(T_{q^2} f_\chi) = a_{nq^2}(f_\chi) + \chi(q)\left(\frac{n}{q}\right) a_n(f_\chi) + q\cdot\chi(q^2)\cdot a_{\frac{n}{q^2}}(f_\chi)\ .) \tag{22}$$

(ii) The form f_χ is in the *Kohnen space* (*cf.* [2, §9.5]), *i.e.* if $n \equiv 2, 3$ (modulo 4), then $a_n(f_\chi) = 0$.

(iii) We have $a_\Delta(f_\chi) = 0$ if Δ is a fundamental discriminant of a real quadratic field in which ℓ does not split, *i.e.* $\Delta \notin \mathcal{D}_\ell$. (Here we use the assumption $w_\ell F = -F$.)

Furthermore, for all $\Delta \in \mathcal{D}_\ell \cup \{1\}$ (*i.e.* such that ℓ splits in $\mathbf{Q}(\sqrt{\Delta})$), we have

$$|a_\Delta(f_\chi)|^2 = C\cdot\sqrt{\Delta}\cdot L(F, \chi_\Delta, 1)$$

for some constant $C \in \mathbf{C}^\times$ independent of Δ (but depending on f_χ).

From now on, assume furthermore that we have $L(F, 1) \neq 0$. We conclude that for all $\Delta \in \mathcal{D}_\ell$, we have

$$\left|\frac{a_\Delta(f_\chi)}{a_1(f_\chi)}\right|^2 = \sqrt{\Delta}\cdot\frac{L(F, \chi_\Delta, 1)}{L(F, 1)}.$$

We can thus normalize f_χ such that

$$a_1(f_\chi) = 1,$$

in which case we get, for all $\Delta \in \mathcal{D}_\ell$:

$$|a_\Delta(f_\chi)|^2 = \sqrt{\Delta} \cdot \frac{L(F, \chi_\Delta, 1)}{L(F, 1)}. \tag{23}$$

Let us rewrite this last equality without using absolute values. We denote by $\overline{f_\chi} \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \overline{\chi'})$ the form obtained by applying the complex conjugation to the Fourier coefficients of f_χ. We claim that we have

$$\overline{f_\chi} = f_\chi \otimes \chi^{-1}, \tag{24}$$

where $f_\chi \otimes \chi^{-1}$ is the twist of f_χ by χ^{-1}, which belongs to $S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \overline{\chi'})$ (*cf.* [30, Lemma 3.6]). Indeed, by unicity (with the normalization $a_1 = 1$), it suffices to check that $f_\chi \otimes \chi^{-1}$ satisfies the conditions (i), (ii) and (iii) above, which is straightforward using [5, §3 (7)].

We thus have

$$\overline{a_\Delta(f_\chi)} = \chi(\Delta)^{-1} \cdot a_\Delta(f_\chi),$$

so we can rewrite (23) as

$$(a_\Delta(f_\chi))^2 = \chi(\Delta) \cdot \sqrt{\Delta} \cdot \frac{L(F, \chi_\Delta, 1)}{L(F, 1)}. \tag{25}$$

One can replace χ (equivalently χ') by a Galois conjugate χ^σ (where $\sigma \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$), and glue all the weight $\frac{3}{2}$ cuspforms obtained this way. This gives rise to a form

$$F_\chi := (f_{\chi^\sigma})_\sigma \tag{26}$$

with coefficients in $R \otimes_{\mathbf{Z}} \mathbf{C} \simeq \prod_\sigma \mathbf{C}$ (where σ runs through $\mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$), instead of just $\mathbf{C}$ for the individual forms f_{χ^σ}. Note that χ and χ' can be considered as taking values in $R \otimes_{\mathbf{Z}} \mathbf{C}$ (*i.e.* we identify $\chi(x) \in R$ with $\chi(x) \otimes 1 \in R \otimes_{\mathbf{Z}} \mathbf{C}$, and similarly for χ'), and that F_χ has Nebentype χ'.

We record the conclusion of the above discussion in the following.

Proposition 3.2. *Let $F \in S_2(\Gamma_0(\ell)))$ be a newform such that $L(F, 1) \neq 0$ (in particular, we have $w_\ell F = -F$). Let $\chi : (\mathbf{Z}/\ell\,\mathbf{Z})^\times \to \mathbf{C}^\times$, $\chi' : (\mathbf{Z}/4\ell^2\,\mathbf{Z})^\times \to \mathbf{C}^\times$ and $R = \mathbf{Z}[\chi] = \mathbf{Z}[\chi']$ be as defined in the notation of this section.*

There exists a unique cuspform $F_\chi \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}}$ satisfying the following properties.

1. *We have $a_1(F_\chi) = 1$.*
2. *For all prime $q \nmid 2\ell$, we have*

$$T_{q^2} F_\chi = \chi(q) \cdot a_q(F) \cdot F_\chi. \tag{27}$$

   (Here, as recalled above, $\chi(q)$ is considered in $R \otimes_{\mathbf{Z}} \mathbf{C}$.)
3. *If $n \equiv 2, 3$ (modulo 4), then $a_n(F_\chi) = 0$.*
4. *We have $a_\Delta(F_\chi) = 0$ if Δ is the discriminant of a real quadratic field in which ℓ does not split, i.e. $\Delta \notin \mathcal{D}_\ell$.*
5. *For all $\Delta \in \mathcal{D}_\ell$, we have*

$$(a_\Delta(F_\chi))^2 = \chi(\Delta) \cdot \sqrt{\Delta} \cdot \frac{L(F, \chi_\Delta, 1)}{L(F, 1)}. \tag{28}$$

   (Again, $\chi(\Delta)$ is considered in $R \otimes_{\mathbf{Z}} \mathbf{C}$.)

Remark 3.3. As we shall see in Theorem 3.4 (and its proof) below, the restriction $q \nmid 2\ell$ in Proposition 3.2 (2) is not necessary for $q = \ell$, but is necessary for $q = 2$, as F_χ is not an eigenvector for the Hecke operator T_{2^2}. Recall (*cf.* [30, Theorem 1.7]) we have

$$a_n(T_{2^2}(f)) = a_{4n}(f)$$

for all $n \geq 1$ and f cuspform of weight $\frac{3}{2}$. We then see that the condition defining the Kohnen space is not stable by T_{2^2}.

3.2. **An Eisenstein congruence in weight $\frac{3}{2}$.** We now apply the discussion of the previous paragraph to the case where F satisfies the Eisenstein congruence (7), to prove the following.

Theorem 3.4. *Let $F \in S_2(\Gamma_0(\ell)))$ be a newform satisfying the Eisenstein congruence (7) (in particular, we know that $L(F,1) \neq 0$). Let $\chi : (\mathbf{Z}/\ell\,\mathbf{Z})^\times \to \mathbf{C}^\times$, $\chi' : (\mathbf{Z}/4\ell^2\,\mathbf{Z})^\times \to \mathbf{C}^\times$ and $R = \mathbf{Z}[\chi] = \mathbf{Z}[\chi']$ be as defined in the notation of this section. Let $F_\chi \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi')_{R\otimes_{\mathbf{Z}}\mathbf{C}}$ be as in Proposition 3.2.*

The Fourier coefficients of F_χ lie in $R\otimes_{\mathbf{Z}} K_F$, where $K_F \subset \mathbf{C}$ is the Hecke field of F. Furthermore, when considered in $R\otimes_{\mathbf{Z}} K_F \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}$, the Fourier coefficients of F_χ actually lie in the subring $R\otimes_{\mathbf{Z}} \mathcal{O}_F \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}$. Furthermore, the following holds.

(i) We have

$$T_{\ell^2} F_\chi = 0,$$

i.e. for all $n \geq 1$, $a_{n\ell^2}(F_\chi) = 0$.

(ii) We have

$$F_\chi \equiv \theta_\chi \text{ (modulo } I_F)$$

where $\theta_\chi \in S_{\frac{3}{2}}(4\ell^2, \chi')_R$ is the classical theta series (cf. [30, §2]*) given by the Fourier expansion*

$$\theta_\chi := \sum_{n\geq 1} n \cdot \chi(n) \cdot q^{n^2}.$$

In particular, for all $n \geq 1$ which is not a perfect square, we have

$$a_n(F_\chi) \in I_F \cdot (R \otimes_{\mathbf{Z}} \mathcal{O}_F \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}).$$

(iii) For all $n \geq 1$ which is not a perfect square, we denote by $\widetilde{a_n(F_\chi)}$ the image of $a_n(F_\chi)$ in R/pR via the map (10). For all $\Delta \in \mathcal{D}_\ell$, we have in R/pR:

$$\widetilde{a_\Delta(F_\chi)} = \pm\chi(\sqrt{\Delta} \text{ modulo } \mathfrak{l}) \cdot h(\Delta) \cdot \log_{\mathfrak{l},p}(\epsilon_\Delta), \tag{29}$$

for any prime $\mathfrak{l}$ above ℓ in $K = \mathbf{Q}(\sqrt{\Delta})$ and for some sign $\pm$ depending a priori *on Δ. (The right-hand side does not depend on the choice of $\mathfrak{l}$.)*

(iv) Let $n \geq 1$ which is not a perfect square, and denote by Δ be the discriminant of the real quadratic field $\mathbf{Q}(\sqrt{n})$. If $\widetilde{a_n(F_\chi)} \neq 0$ (in R/pR), then $\widetilde{a_\Delta(F_\chi)} \neq 0$ (in particular $\Delta \in \mathcal{D}_\ell$, i.e. ℓ splits in $\mathbf{Q}(\sqrt{n})$).

Remark 3.5. (1) In the special case $\ell = 11$ and $p = 5$, the congruence of Theorem 3.4 (ii) follows from the explicit computations of [2, §10.7] (note that there is a typo in the last paragraph of p. 381: the nth Fourier coefficients of the theta series should be $n \cdot \left(\frac{n}{11}\right)$ and not $\left(\frac{n}{11}\right)$).

(2) We check that θ_χ is an eigenform for the Hecke operator T_{q^2} for *all* primes q, with Hecke eigenvalue $(q+1)\cdot\chi(q)$ if $q \nmid 2\ell$, 0 if $q = \ell$ and $2\chi(2)$ if $q = 2$.

(3) Although [2, Theorem 10.1] only applies *a priori* when F is a cuspform, we see that, formally speaking, the weight $\frac{3}{2}$-modular form associated to the weight 2 Eisenstein series $E_{2,\ell} \in M_2(\Gamma_0(\ell))$ is simply $\theta_\chi \in S_{\frac{3}{2}}(\Gamma_0(4\ell^2), \chi')$. Note also that (28) also holds, as $L(E_{2,\ell}, \chi_D, 1) = 0$ if $D \in \mathcal{D}_\ell$. Therefore, Theorem 3.4 (ii) reflects the fact that the Eisenstein congruence (7) is in some sense compatible with the (generalized) Shimura lifting.

(4) One can ask what is the sign in (29), and in particular whether it can be taken to be equal to 1.

Proof. This essentially follows from (28) and Proposition 2.3, except that some difficulties arise due to the restriction $q \nmid 2\ell$ in (27). The main issue is that f_χ is *not* an eigenvector for the Hecke operator T_{2^2}. However, as we shall see, f_χ is a linear combination of two cusp forms in $S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi')$ which are eigenforms for *all* the Hecke operators T_{q^2} and satisfy similar properties as the ones f_χ described in Proposition 3.2 (except for the third one). We will need to use the adelic language, following and relying on [2] and [33].

Proof of (i) and (ii). As in [2, §9.1], corresponding to F is a vector

$$\varphi = \otimes' \varphi_v = s(F) \in \pi,$$

where

$$\pi = \otimes'_v \pi_v$$

is the irreducible cuspidal automorphic representation of PGL_2 corresponding to F.

As in [2, §9.2], corresponding to f_χ is a vector

$$\tilde{\phi}_\chi = \otimes' \tilde{\varphi}_v = t(f_\chi) \in \tilde{\pi},$$

where

$$\tilde{\pi} = \otimes'_v \tilde{\pi}_v$$

is an irreducible cuspidal automorphic representation of the metaplectic group given by

$$\tilde{\pi} = \Theta(\pi \otimes \chi_D, \psi^D)$$

for any $D \in \mathcal{D}_\ell$ (*i.e.* such that $D > 0$ is a non-zero square modulo ℓ). Here, χ_D is the quadratic Dirichlet character corresponding to D, ψ is the usual additive character and Θ is the theta correspondence (we refer to [2, §3] for details).

If q is a prime, let χ_q be the character of $\mathbf{Q}_q^\times$ which is the component at q of the character on $\mathbb{A}_{\mathbf{Q}}^\times / \mathbf{Q}^\times$ canonically associated with χ. In particular, for $q \neq \ell$, the character χ_q is unramified and we have $\chi_q(q) = \chi(q)$.

For $q \mid 2\ell$, Waldspurger defines in [33] a Hecke operator $\tilde{T}'_q$ acting on $\tilde{\phi}_\chi$ and we have (*cf.* [33, III.B Lemma 4 (ii)]) that we have

$$T_{q^2} f_\chi = \sqrt{q}^{-1} \cdot \tilde{\gamma}_q(q)^{-1} \cdot \chi_q(q) \cdot s(\tilde{T}'_q \tilde{\phi}_\chi), \tag{30}$$

where $\tilde{\gamma}_q(q)$ is the Weil constant (*cf.* [33, II §2]). As recalled in *cf.* [33, II §6], we have $\tilde{\gamma}_2(2) = 1$.

In [2, §8], an explicit description of $\tilde{\pi}_v$ and $\tilde{\varphi}_v$ (up to scalar) is given for all places $v \neq 2$. In particular, if $v = \ell$, from our condition $D \in \mathcal{D}_\ell$ and the fact that $w_\ell F = -F$, we get by [2, §10.5] that $\tilde{\pi}_\ell$ is the supercuspidal representation r_ψ^- described in [2, §8.3.3] and $\tilde{\varphi}_\ell$ is, up to scalar, an explicit function on $\mathbf{Q}_\ell$ in r_ψ^- denoted by Φ_{χ_ℓ} in [2, Proposition 8.5]. Note that for all $x \in \mathbf{Z}_\ell^\times$, we have

$$\chi_\ell(x) = \overline{\chi}(x \text{ (modulo } \ell)).$$

By definition, the function Φ_{χ_ℓ} is supported on $\mathbf{Z}_\ell^\times$. By [33, V §2 Lemme 7 (iii)] (with $n = 2$), we see that $\tilde{T}'_\ell \tilde{\varphi}_\ell = 0$. By (30), we get:

$$T_{\ell^2} f_\chi = 0. \tag{31}$$

We now consider the place $v = 2$. The choice of $\tilde{\varphi}_2$ is given in details in [2, §9.4]. Since $a_2(F) \equiv 3$ (modulo $\mathfrak{P}_F$) and the polynomial $X^2 - 3X + 2 = (X-1)(X-2)$ splits over $\mathbf{F}_p$, by Hensel's lemma we get

$$X^2 - a_2(F)X + 2 = (X - \alpha_1)(X - \alpha_2)$$

for some $\alpha_1, \alpha_2 \in \mathcal{O}_{\mathfrak{P}_F}$, which we also view in $\mathbf{C}$. Without loss of generality, let us assume that

$$\alpha_1 \equiv 1 \text{ (modulo } I_F). \tag{32}$$

For simplicity of notation, we let $\alpha := \alpha_1$ in what follows. Note that

$$\alpha \neq 1,$$

as otherwise we would have $a_2(F) = 3$, which would contradict the Ramanujan bound $|a_2(F)| \leq 2\sqrt{2}$.

Let $\mu : \mathbf{Q}_2^\times \to \mathbf{C}^\times$ be the unramified character of $\mathbf{Q}_2^\times$ such that

$$\mu(2) = \frac{\alpha}{\sqrt{2}}.$$

Note that we have $\overline{\alpha_1} = \alpha_2$, so

$$\overline{\mu(2)} = \frac{\alpha_2}{\sqrt{2}} = \frac{\sqrt{2}}{\alpha_1} = \mu(2)^{-1}$$

i.e. $\mu(2)$ is a root of unity. By construction, we have

$$\mu(2^2) \equiv 2^{-1} \text{ (modulo } I_F). \tag{33}$$

In particular, we get $\mu(2^2) \neq 1$.

In [33, VI §8 Proposition 13 (iii)] (with χ_0 trivial and $n = 2$), Waldspurger proves that there are two vectors $F[2,1]$ and $F[2,2^2]$ of $\tilde{\pi}_2$ such that

$$\tilde{T}_2' F[2,1] = 2\mu(2)^{-1} \cdot F[2,1]$$

and

$$\tilde{T}_2' F[2,2^2] = 2\mu(2) \cdot F[2,2^2] + \frac{i+1}{2} \cdot \mu(2) \cdot F[2,1].$$

Therefore, the two vectors

$$e_1 := F[2,1]$$

and

$$e_2 := \frac{i+1}{4} \cdot \frac{\mu(2^2)}{\mu(2^2) - 1} \cdot F[2,1] + F[2,2^2]$$

are eigenvectors for $\tilde{T}_2'$ with (distinct) eigenvalues $2\mu(2)^{-1}$ and $2\mu(2)$ respectively (note that we use the fact that $\mu(2^2) \neq 1$).

Consider now the two weight $\frac{3}{2}$ cuspforms of level $\Gamma_1(4\ell^2)$ and character χ'

$$g_{1,\chi} := s(\otimes_{v \neq 2} \tilde{\varphi}_v \otimes_{v=2} e_1)$$

and

$$g_{2,\chi} := s(\otimes_{v \neq 2} \tilde{\varphi}_v \otimes_{v=2} e_2).$$

These are, by construction, eigenforms for all Hecke operators T_{q^2}, such that, for $i \in \{1,2\}$, we have

$$T_{\ell^2} g_{i,\chi} = 0,$$

$$T_{2^2} g_{i,\chi} = 2\chi(2)\alpha_i^{-1} \cdot g_{i,\chi},$$

and for all primes $q \nmid 2\ell$,

$$T_{q^2} g_{i,\chi} = \chi(q) \cdot a_q(F) \cdot g_{i,\chi}.$$

By [2, Theorem 4.3], we have $a_1(g_{i,\chi}) \neq 0$ for $i = 1, 2$. Thus, there exists $\lambda_{i,\chi} \in \mathbf{C}^\times$ such that $f_{i,\chi} := \lambda_{i,\chi} \cdot g_{i,\chi}$ satisfies $a_1(f_{i,\chi}) = 1$. Obviously, $f_{i,\chi}$ satisfies the same Hecke relations as $g_{i,\chi}$, *i.e.*

$$\begin{array}{lll} T_{\ell^2} f_{i,\chi} & = & 0, \\ T_{2^2} f_{i,\chi} & = & 2\chi(2)\alpha_i^{-1} \cdot f_{i,\chi}, \\ \forall q \nmid 2\ell \text{ (q prime) } T_{q^2} f_{i,\chi} & = & \chi(q) \cdot a_q(F) \cdot f_{i,\chi}. \end{array} \tag{34}$$

These Hecke relations, together with the normalization $a_1(f_{i,\chi}) = 1$, characterize uniquely $f_{i,\chi}$. In particular, using the relation $\overline{\alpha_1} = \alpha_2$, a similar argument as for (24) yields

$$\overline{f_{1,\chi}} = f_{2,\chi^{-1}} = f_{2,\chi} \otimes \chi^{-1}. \tag{35}$$

Let us now compute the ratio $\frac{\lambda_{1,\chi}}{\lambda_{2,\chi}} \in \mathbf{C}^\times$. By [2, §2.2], we have

$$\frac{a_1(g_{1,\chi})}{a_1(g_{2,\chi})} = \frac{\tilde{L}_2(e_1)}{\tilde{L}_2(e_2)},$$

where $\tilde{L}_2$ is any choice (unique up to non-zero scalar) of local Whittaker functional at the place 2 for $\tilde{\pi}_2$. By [2, Lemma 9.3], one can normalize $\tilde{L}_2$ such that

$$\tilde{L}_2(F[2,1]) = 1$$

and

$$\tilde{L}_2(F[2,2^2]) = (\mu(2^2) + \sqrt{2}\mu(2^3)) \cdot \frac{i+1}{4}.$$

We choose this normalization for the rest of the proof.

We get

$$\frac{\lambda_{1,\chi}}{\lambda_{2,\chi}} = \frac{a_1(g_{2,\chi})}{a_1(g_{1,\chi})} = \frac{i+1}{4} \cdot \frac{\mu(2^2)}{\mu(2^2)-1} + \frac{i+1}{4} \cdot (\mu(2^2) + \sqrt{2}\mu(2^3)) = \frac{i+1}{4} \cdot \frac{\mu(2^2)}{\mu(2^2)-1} + \frac{i+1}{4} \cdot (\mu(2^2) + \alpha\mu(2^2)). \tag{36}$$

(We have used the definition $\mu(2) = \frac{\alpha}{\sqrt{2}}$ in the last equality.)

By [2, §9.4], it is proved that $\tilde{\varphi}_2$ is proportional to

$$\frac{i+1}{4} \cdot \mu(2^2) \cdot F[2,1] + F[2,2^2] = \frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2.$$

Thus, f_χ is proportional to $\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot g_{1,\chi} + g_{2,\chi}$, which is proportional to

$$\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot f_{1,\chi} + \frac{\lambda_{1,\chi}}{\lambda_{2,\chi}} \cdot f_{2,\chi}.$$

By (36), there exists $\lambda \in \mathbf{C}^\times$ such that

$$f_\chi = \lambda \cdot \left(\frac{\mu(2^4)}{\mu(2^2)-1} \cdot f_{1,\chi} + \left(\frac{\mu(2^2)}{\mu(2^2)-1} + \mu(2^2) + \alpha_1\mu(2^2) \right) \cdot f_{2,\chi} \right).$$

Since $a_1(f_\chi) = a_1(f_{1,\chi}) = a_1(f_{2,\chi}) = 1$, we get

$$\lambda = \frac{\mu(2^2)-1}{2\mu(2^4) - \alpha_1\mu(2^2) + \alpha_1\mu(2^4)}.$$

We get

$$f_\chi = \mu_1 f_{1,\chi} + \mu_2 f_{2,\chi} \tag{37}$$

where $\mu_1, \mu_2 \in K_F(\alpha)$ (which is at most a quadratic extension of K_F) are such that

$$\mu_1 = \frac{\alpha}{\alpha^2 + 2\alpha - 2} \tag{38}$$

and

$$\mu_2 = \frac{(\alpha - 1)(\alpha + 2)}{\alpha^2 + 2\alpha - 2}. \tag{39}$$

By (32), we get

$$\mu_1 \equiv 1 \text{ (modulo } I_F) \tag{40}$$

and

$$\mu_2 \equiv 0 \text{ (modulo } I_F). \tag{41}$$

Let us now study the coefficients $a_D(f_{i,\chi})$ where D ($\neq 1$) is the discriminant of a real quadratic field.

Assume first $D \notin \mathcal{D}_\ell$. In this case, it follows from [2, Theorem 4.3 2. and Corollary 10.7] that

$$a_D(f_\chi) = a_D(f_{1,\chi}) = a_D(f_{2,\chi}) = 0. \tag{42}$$

Assume now $D \in \mathcal{D}_\ell$. It follows from [2, Theorem 4.3 3.] that $a_D(f_\chi) = 0$ if and only if $L(F, \chi_D, 1) = 0$, if and only if $a_D(f_{i,\chi}) = 0$ (for $i = 1, 2$). We thus assume that $a_D(f_\chi) \neq 0$. We first compute the (well-defined) ratio $\frac{a_D(f_\chi)}{a_D(f_{1,\chi})}$. It follows easily from [2, §2.2] that we have

$$\frac{a_D(f_\chi)}{a_D(f_{1,\chi})} = \frac{a_1(f_\chi)}{a_1(f_{1,\chi})} \cdot \left(\frac{\tilde{L}_2(\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2)}{\tilde{L}_2(e_1)} \right)^{-1} \cdot \frac{\tilde{L}_2^D(\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2)}{\tilde{L}_2^D(e_1)}.$$

Here, as in [2, §2.2], $\tilde{L}_2^D$ denotes a local Whittaker functional at the place $v = 2$ corresponding to an additive character ψ^D, which we normalize as in [2, §8.1 (8.3)]. Recall that, by construction, we have $\frac{a_1(f_\chi)}{a_1(f_{1,\chi})} = 1$.

By [2, Lemma 9.3], we have

$$\tilde{L}_2(e_1) = \tilde{L}_2^D(e_1) = 1,$$

and

$$\tilde{L}_2(\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2) = \frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} + \frac{i+1}{4} \cdot (\mu(2^2) + \alpha \cdot \mu(2^2)).$$

We also get

$$\tilde{L}_2^D(\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2) = \frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} + \frac{i+1}{4} \cdot (\mu(2^2) + \alpha \cdot \mu(2^2) \cdot \chi_2(D)) \text{ if } D \equiv 1 \text{ (modulo 4)}$$

and

$$\tilde{L}_2^D(\frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} \cdot e_1 + e_2) = \frac{i+1}{4} \cdot \frac{\mu(2^4)}{\mu(2^2)-1} + \frac{i+1}{4} \cdot (\mu(2^2) - \mu(2^4)) \text{ if } D \equiv 0 \text{ (modulo 4)}.$$

Here, χ_2 is the quadratic character (of conductor 8) of $\mathbf{Q}_2^\times$ corresponding to the extension $\mathbf{Q}_2(\sqrt{2})$.

In conclusion, we get

$$\frac{a_D(f_\chi)}{a_D(f_{1,\chi})} = \frac{\frac{\mu(2^4)}{\mu(2^2)-1} + \mu(2^2) + \alpha \cdot \mu(2^2) \cdot \chi_2(D)}{\frac{\mu(2^4)}{\mu(2^2)-1} + \mu(2^2) + \alpha \cdot \mu(2^2)} \text{ if } D \equiv 1 \text{ (modulo 4)}$$

and

$$\frac{a_D(f_\chi)}{a_D(f_{1,\chi})} = \frac{\frac{\mu(2^4)}{\mu(2^2)-1} + \mu(2^2) - \mu(2^4)}{\frac{\mu(2^4)}{\mu(2^2)-1} + \mu(2^2) + \alpha \cdot \mu(2^2)} \text{ if } D \equiv 0 \text{ (modulo 4)}.$$

Since, for $D \equiv 1$ (modulo 4), we have $\chi_2(D) = 1$ if $D \equiv 1$ (modulo 8) and $\chi_2(D) = -1$ if $D \equiv 5$ (modulo 4), this simplifies to give

$$a_D(f_{1,\chi}) = a_D(f_\chi) \text{ if } D \equiv 1 \text{ (modulo 8)}, \tag{43}$$

$$a_D(f_{1,\chi}) = -\frac{\alpha^3 + 2\alpha^2 - 2\alpha - 2}{\alpha^3 - 2\alpha^2 - 2\alpha + 2} \cdot a_D(f_\chi) \text{ if } D \equiv 5 \text{ (modulo 8)}, \tag{44}$$

and

$$a_D(f_{1,\chi}) = -2 \cdot \frac{\alpha^3 + 2\alpha^2 - 2\alpha - 2}{\alpha^4 - 6\alpha^2 + 4} \cdot a_D(f_\chi) \text{ if } D \equiv 0 \text{ (modulo 4)}. \tag{45}$$

By (37) (and the fact that $\alpha \neq 1$, as recalled above), we get

$$a_D(f_{2,\chi}) = a_D(f_\chi) \text{ if } D \equiv 1 \text{ (modulo 8)}\ , \tag{46}$$

$$a_D(f_{2,\chi}) = \frac{\alpha^5 + \alpha^4 - 6\alpha^3 + 6\alpha - 4}{(\alpha - 1)(\alpha + 2)(\alpha^3 - 2\alpha^2 - 2\alpha + 2)} \cdot a_D(f_\chi) \text{ if } D \equiv 5 \text{ (modulo 8)}. \tag{47}$$

and

$$a_D(f_{2,\chi}) = \frac{\alpha^5 - 6\alpha^3 + 4\alpha^2 + 4\alpha - 4}{(\alpha - 1)(\alpha^4 - 6\alpha^2 + 4)} \cdot a_D(f_\chi) \text{ if } D \equiv 0 \text{ (modulo 4)}. \tag{48}$$

Note that the six labeled equations above also hold if $a_D(f_\chi) = 0$, as both sides are zero as recalled above.

Combining (28), Proposition 2.3, (43), (44), (45), (47) and (48), we conclude for all $D \in \mathcal{D}_\ell$ and $i \in \{1, 2\}$, the Fourier coefficient $\frac{a_D(f_{i,\chi})}{\chi(\sqrt{D} \text{ modulo } \mathfrak{l})}$ is algebraic (where $\mathfrak{l}$ is any prime above ℓ in $\mathbf{Q}(\sqrt{D})$), and in fact belongs to the (at most) quadratic extension $K_F(\alpha)$ of K_F in $\mathbf{C}$. Furthermore, using (20),(32) and (39), for all $D \in \mathcal{D}_\ell$, we get in $K_F(\alpha) \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}$:

$$\frac{a_D(f_\chi)}{\chi(\sqrt{D} \text{ modulo } \mathfrak{l})}, \frac{a_D(f_{1,\chi})}{\chi(\sqrt{D} \text{ modulo } \mathfrak{l})}, \mu_2 \cdot \frac{a_D(f_{2,\chi})}{\chi(\sqrt{D} \text{ modulo } \mathfrak{l})} \in I_F \cdot \mathcal{O}_{\mathfrak{P}_F}. \tag{49}$$

Here, we view $\mathcal{O}_{\mathfrak{P}_F}$ as a subring of $K_F(\alpha) \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}$ in the obvious way. Let us note that (49) also hold for fundamental discriminants $D \notin \mathcal{D}_\ell$, as by (42) these three quantities equal zero.

Recall that we have defined in (26) the form $F_\chi \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}}$ by gluing the forms f_{χ^σ} where σ runs through $\mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$. We define similarly $F_{i,\chi} \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}}$ for $i = 1, 2$ by gluing f_{i,χ^σ}. The equations (34) and (37) with f_χ, $f_{1,\chi}$ and $f_{2,\chi}$ replaced by F_χ, $F_{1,\chi}$ and $F_{2,\chi}$ respectively obviously hold.

By [2, §2.2] and the choice of local Whittaker functional at $v = \ell$ in [2, p. 367], we get for $\sigma, \sigma' \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$ and $D \in \mathcal{D}_\ell$:

$$\begin{aligned} a_D(f_{\chi^\sigma}) &= (\tfrac{\chi^\sigma}{\chi^{\sigma'}})(\sqrt{D} \text{ modulo } \mathfrak{l}) \cdot a_D(f_{\chi^{\sigma'}}), \\ a_D(f_{i,\chi^\sigma}) &= (\tfrac{\chi^\sigma}{\chi^{\sigma'}})(\sqrt{D} \text{ modulo } \mathfrak{l}) \cdot a_D(f_{i,\chi^{\sigma'}}) \text{ (for } i \in \{1, 2\}). \end{aligned} \tag{50}$$

Note that these equations do not depend on the choice of $\mathfrak{l}$, as $\frac{\chi^{\sigma'}}{\chi^\sigma}$ is an even character of level ℓ. It follows from the discussion above (49) that for all fundamental discriminant D (with $D \neq 1$), we have

$$a_D(F_\chi), a_D(F_{1,\chi}), a_D(F_{2,\chi}) \in R \otimes_{\mathbf{Z}} K_F(\alpha),$$

and furthermore, using (49) and (50), we conclude that we actually have

$$a_D(F_\chi), a_D(F_{1,\chi}), \mu_2 \cdot a_D(F_{2,\chi}) \in I_F \cdot (R \otimes_{\mathbf{Z}} \mathcal{O}_{\mathfrak{P}_F}), \tag{51}$$

where $R \otimes_{\mathbf{Z}} \mathcal{O}_{\mathfrak{P}_F}$ is considered as a subring of $R \otimes_{\mathbf{Z}} K_F(\alpha) \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}$.

Using (34), (37), (40) and (41), we conclude that for all positive integer n, we have

$$a_n(F_\chi) \in R \otimes_{\mathbf{Z}} K_F$$

and that furthremore, if n is not a perfect square,

$$a_n(F_\chi) \in I_F \cdot (R \otimes_{\mathbf{Z}} \mathcal{O}_{\mathfrak{P}_F})$$

whereas if $n = m^2$ is a perfect square,

$$a_n(F_\chi) - m \cdot \chi(m) \in I_F \cdot (R \otimes_{\mathbf{Z}} \mathcal{O}_{\mathfrak{P}_F}).$$

This concludes the proof of (ii).

Point (iii) follows immediately from (28) and Proposition 2.3.

Proof of (iv). We have $n = m^2 \cdot \Delta$ where $2m \in \mathbf{N}$. If m is an odd integer, then by (27) and (22), we see that $a_n(F_\chi)$ is an explicit multiple of $a_\Delta(F_\chi)$, which proves the claim in point (iv).

Assume now that m is an even integer. By the same argument as when m is odd, we may assume without loss of generality that $m = 2^a$ for some $a \geq 1$. Combining (34), (37), (43), (44), (45), (46), (47), and (48) (depending on Δ modulo 8), we see again that $a_n(F_\chi)$ is an explicit multiple of $a_\Delta(F_\chi)$, which proves the claim in point (iv).

Finally, assume that m is half an odd integer. Again, without loss of generality, we may assume $m = \frac{1}{2}$, *i.e.* $\Delta = 4n$. By (34), (37), (45), and (48), we get

$$\begin{aligned}
a_\Delta(F_\chi) &= a_n(T_{2^2} F_\chi) \\
&= \mu_1 \cdot 2\chi(2)\alpha^{-1} \cdot a_n(F_{1,\chi}) + \mu_2 \cdot 2\chi(2) \cdot (\frac{2}{\alpha})^{-1} \cdot a_n(F_{2,\chi}) \\
&= \chi(2)\alpha^{-1} \cdot (2\mu_1 \cdot a_n(F_{1,\chi}) + \mu_2 \cdot \alpha^2 \cdot a_n(F_{2,\chi})) \\
&= 2\chi(2)\alpha^{-1} \cdot a_n(F_\chi) + \mu_2 \cdot (\alpha^2 - 2) \cdot a_n(F_{2,\chi}) \\
&= 2\chi(2)\alpha^{-1} \cdot a_n(F_\chi) + \mu_2 \cdot (\alpha^2 - 2) \cdot \chi(2)^{-1}\alpha^{-1} \cdot a_\Delta(F_{2,\chi}) \\
&= 2\chi(2)\alpha^{-1} \cdot a_n(F_\chi) + \chi(2)^{-1} \cdot \frac{(\alpha-1)(\alpha+2)(\alpha^2-2)}{\alpha(\alpha^2+2\alpha-2)} \cdot a_\Delta(F_{2,\chi}) \\
&= 2\chi(2)\alpha^{-1} \cdot a_n(F_\chi) + \chi(2)^{-1} \cdot \frac{(\alpha-1)(\alpha+2)(\alpha^2-2)}{\alpha(\alpha^2+2\alpha-2)} \cdot \frac{(\alpha^5-6\alpha^3+4\alpha^2+4\alpha-4)}{(\alpha-1)(\alpha^4-6\alpha^2+4)} \cdot a_\Delta(F_\chi).
\end{aligned}$$

Thus, we get

$$(1 - \chi(2)^{-1} \cdot \frac{(\alpha+2)(\alpha^2-2)(\alpha^5-6\alpha^3+4\alpha^2+4\alpha-4)}{\alpha(\alpha^2+2\alpha-2)(\alpha^4-6\alpha^2+4)}) \cdot a_\Delta(F_\chi) = 2\chi(2)\alpha^{-1} \cdot a_n(F_\chi).$$

This concludes the proof of (iv), and of the theorem. □

The following corollary of Theorem 3.4 will be the key input for our proof of Theorem A.

Corollary 3.6. *Let $\chi : (\mathbf{Z}/\ell\,\mathbf{Z})^\times \to \mathbf{C}^\times$, $\chi' : (\mathbf{Z}/4\ell^2\,\mathbf{Z})^\times \to \mathbf{C}^\times$ and $R = \mathbf{Z}[\chi] = \mathbf{Z}[\chi']$ be as defined in the notation of this section. Let Q be a positive squarefree integer with $\gcd(Q, 2p\ell) = 1$.*

There exists

$$g_{\chi,Q} \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{R/pR}$$

such that, for all $n \geq 1$ *with* $\left(\frac{n}{Q}\right) \neq -1$, *we have* $a_n(g_Q) = 0$, *and furthermore the following holds.*

(i) For all prime $r \nmid 2Q\ell$, *we have* $T_{r^2}(g_{\chi,Q}) = \chi(r) \cdot (r+1) \cdot g_{\chi,Q}$.

(ii) For all $\Delta \in \mathcal{D}_\ell$ *with* $\left(\frac{\Delta}{Q}\right) = -1$, *we have*

$$a_\Delta(g_{\chi,Q}) = \pm\chi(\sqrt{\Delta} \text{ modulo } \mathfrak{l}) \cdot h(\Delta) \cdot \log_{\mathfrak{l},p}(\epsilon_\Delta) \text{ (modulo } p)$$

for any prime $\mathfrak{l}$ *above* ℓ *in* $K = \mathbf{Q}(\sqrt{\Delta})$ *and some sign* $\pm$ *may depending* a priori *on* Δ. *(The right-hand side is independent of the choice of* $\mathfrak{l}$.*)*

(iii) Let $n \geq 1$ *be such that* $\left(\frac{n}{Q}\right) = -1$, *and denote by* Δ *the discriminant of the real quadratic field* $\mathbf{Q}(\sqrt{n})$. *If* $a_n(g_{\chi,Q}) \neq 0$, *then* $a_\Delta(g_{\chi,Q}) \neq 0$ *and* $\Delta \in \mathcal{D}_\ell$.

Proof. Let F and F_χ be as in Theorem 3.4. Define

$$h_{\chi,Q} := \frac{1}{2} \cdot (F_\chi - F_\chi \otimes \left(\frac{\cdot}{Q}\right) - B_Q F_\chi) \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}},$$

where

$$F_\chi \otimes \left(\frac{\cdot}{Q}\right) := \sum_{n \geq 1} a_n(F_\chi) \cdot \left(\frac{n}{Q}\right) \cdot q^n \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}}$$

is the twist of F_χ by the primitive Dirichlet character $\left(\frac{\cdot}{Q}\right)$ of level Q and

$$B_Q F_\chi := \sum_{n \geq 1} a_{nQ}(F_\chi) q^{nQ} \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{R \otimes_{\mathbf{Z}} \mathbf{C}}$$

(*cf. eg.* [5, §3] for the definition of the twist and B_Q operators).

Thus, we have $a_n(h_{\chi,Q}) = a_n(F_\chi)$ if $\left(\frac{n}{Q}\right) = -1$ and $a_n(h_{\chi,Q}) = 0$ else. Furthermore, by (27) and (22), for all prime r with $r \nmid 2Q\ell$, we have

$$T_{r^2}(h_{\chi,Q}) = \chi(r) \cdot a_r(F) \cdot h_{\chi,Q}.$$

By Theorem 3.4 (ii), for all $n \geq 1$ we have

$$a_n(h_{\chi,Q}) \in I_F \cdot (R \otimes_{\mathbf{Z}} \mathcal{O}_F \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{P}_F}).$$

We then let

$$g_{\chi,Q} := \sum_{n \geq 1} \widetilde{a_n(h_{\chi,Q})} \cdot q^n \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{R/pR},$$

where $\widetilde{a_n(h_{\chi,Q})}$ denotes the image of $a_n(h_{\chi,Q})$ in R/pR via the map (10). Point (i) of the corollary then follows from the fact that $a_r(F) \equiv r+1$ (modulo I_F), while points (ii) and point (iii) follows from Theorem 3.4 (iii) and (iv) respectively. □

4. Proof of the main theorem

We keep the notation of section 3.

The goal of this section is to prove Theorem A. Recall that, in the setting of Theorem A, there is a squarefree integer Q such that $\gcd(Q, 2p\ell) = 1$, $Q \not\equiv \pm 1$ (modulo p) and there exists $\Delta_0 \in \mathcal{D}_\ell$ such that $\left(\frac{\Delta_0}{Q}\right) = -1$ and $h(\Delta_0) \cdot \log_{\mathfrak{l},p}(\epsilon_{\Delta_0}) \neq 0$, for any prime $\mathfrak{l} \mid \ell$ in $\mathbf{Q}(\sqrt{\Delta_0})$.

Let

$$g_{\chi,Q} \in S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi)_{R/pR}$$

as in Corollary 3.6. By Corollary 3.6 (ii), we conclude that $a_{\Delta_0}(g_{\chi,Q}) \neq 0$ (in R/pR). We let

$$\mathrm{Supp}(g_{\chi,Q}) := \{n \geq 1 \text{ such that } a_n(g_{\chi,Q}) \neq 0 \text{ (in } R/pR)\},$$

which is non-empty.

The following result relies crucially on a result of Bruinier–Ono [4, Theorem 3.1] (*cf.* also [5, Theorem 1]).

Lemma 4.1. *There does not exist finitely many squarefree integers n_1, ..., n_t (for some $t \geq 1$) such that*

$$\mathrm{Supp}(g_{\chi,Q}) \subset \bigcup_{i=1}^{t} \{n_i m^2, m \in \mathbf{N}\}.$$

Consequently, for any $C > 1$ there exists an integer $n_0 \in \mathrm{Supp}(g_{\chi,Q})$ such that $n_0 = n_0' m^2$ for some $m \in \mathbf{N}$ and n_0' squarefree and divisible by a prime $> C$.

Proof. For the sake of a contradiction, assume that there are such (pairwise distincts) squarefree integers n_1, ..., n_t. Since $\mathrm{Supp}(g_Q)$ consists of integers n satisfying $\left(\frac{n}{Q}\right) = -1$, we can and do assume that for all $i \in \{1, ..., t\}$, we have $\left(\frac{n_i}{Q}\right) = -1$.

Claim. *There exists a prime r such that $r \nmid 2Qp\ell$, $\left(\frac{n_i}{r}\right) = -1$ for all $i \in \{1, ..., t\}$ and $r \not\equiv \pm 1$ (modulo p).*

Proof of the claim. By the quadratic reciprocity law, the condition $\left(\frac{n_i}{r}\right) = -1$ is equivalent to congruences for r modulo $4n_i$. Together with the condition $r \not\equiv \pm 1$ (modulo p), we need to solve a system of congruences in r. This system has a solution given by Q, since we have $Q \not\equiv \pm 1$ (modulo p) and $\left(\frac{n_i}{Q}\right) = -1$ for all i. By Dirichlet's theorem on primes in arithmetic progressions, the claim follows.

Let r be as in the claim. It follows from a slight generalization of [4, Theorem 3.1] that we have

$$(r-1) \cdot T_{r^2}(g_{\chi,Q}) = -\chi(r) \cdot (r+1) \cdot (r-1) \cdot g_{\chi,Q}.$$

Indeed, [4, Theorem 3.1] applies, as stated, to forms in $S_{\frac{3}{2}}(\Gamma_1(4\ell^2Q^2), \chi')_{\mathbf{Z}/p\mathbf{Z}}$ where χ' is a *quadratic* character. However, the proof of that theorem purely relies on commutation relations between certain operators (especially the Atkin–Lehner involution), and can be applied identically to a form with coefficients in R/pR instead of $\mathbf{Z}/p\mathbf{Z}$, and for a general (non necessarily quadratic) Nebentype χ'. The only necessary change is to replace χ' with $\overline{\chi'}$ at certain places, but it is straightforward to check that the end result, *i.e.* the identity for $(r-1)T_{r^2}f$, still holds (here, p and M in [4, Theorem 3.1] should be replaced by our r and p respectively).

Since $r \not\equiv \pm 1$ (modulo p) and $T_{r^2}(g_{\chi,Q}) = \chi(r) \cdot (r+1) \cdot g_{\chi,Q}$ (by Corollary 3.6 (i)), we get $g_{\chi,Q} = 0$, which is not possible since, as explained above, our running assumption implies $\mathrm{Supp}(g_{\chi,Q}) \neq \emptyset$. □

We let

$$C = 2\ell(\ell+1)Q \prod_{\substack{q \mid Q \\ q \text{ prime}}} (q+1).$$

By Lemma 4.1, there exists $n_0 \geq 1$ such that $a_{n_0}(g_Q) \neq 0$ and whose squarefree part n_0' is divisible by a prime factor $> C$. In what follows, we fix such a choice of n_0. Let S be the set of primes $r > C$ with $\gcd(r, Q\ell) = 1$, such that for all $n \leq C$ we have $\left(\frac{n}{r}\right) = 1$, and such that $\left(\frac{n_0}{r}\right) = -1$. It follows from Dirichlet's theorem and the existence of n_0' as above that S has positive density.

The following is the key lemma of our proof. Its proof takes inspiration in the technique of [24] and [6].

Lemma 4.2. *For every $r \in S$, there exists $n \leq Cr$ coprime with r such that $a_{nr}(g_{\chi,Q}) \neq 0$.*

Proof. Assume, for the sake of a contradiction, that for all $n \leq Cr$ coprime to r, we have $a_{nr}(g_{\chi,Q}) = 0$.

Let

$$g_1 = \sum_{n \geq 1} a_{nr}(g_{\chi,Q}) q^n$$

and

$$g_2 = \sum_{n \geq 1} a_n(g_{\chi,Q}) q^{nr}.$$

By [30, Propositions 1.3 and 1.5], both g_1 and g_2 are in $S_{3/2}(\Gamma_1(4\ell^2Q^2r), \chi' \cdot \left(\frac{r}{\cdot}\right))_{R/pR}$.

Our assumption is equivalent to $a_n(g_1) = 0$ for all $n \leq Cr$ coprime to r, and by construction, we have $a_n(g_2) = 0$. In particular, for $n \leq Cr$ coprime to r, we have:

$$a_n(g_1) = r \cdot \chi(r) \cdot a_n(g_2). \tag{52}$$

Recall (*cf. eg.* [5, §3]) that

$$a_n(T_{r^2} g_{\chi,Q}) = a_{nr^2}(g) + \chi(r) \left(\frac{n}{r}\right) a_n(g_{\chi,Q}) + r \cdot \chi(r^2) \cdot a_{\frac{n}{r^2}}(g_{\chi,Q}).$$

By Corollary 3.6 (i), we get, for all $n \geq 1$:

$$a_{nr^2}(g_{\chi,Q}) = (\chi(r) \cdot (r+1) - \chi(r) \left(\frac{n}{r}\right)) \cdot a_n(g_{\chi,Q}) - r \cdot \chi(r^2) \cdot a_{\frac{n}{r^2}}(g_{\chi,Q}). \tag{53}$$

In particular, if $r^2 \nmid n$, we get

$$a_{nr^2}(g_{\chi,Q}) = (\chi(r) \cdot (r+1) - \chi(r) \left(\frac{n}{r}\right)) \cdot a_n(g_{\chi,Q}). \tag{54}$$

or equivalently

$$a_{nr}(g_1) = (\chi(r) \cdot (r+1) - \chi(r) \left(\frac{n}{r}\right)) \cdot a_{nr}(g_2).$$

In particular, using the assumption $r \in S$, we get, for $n \leq C$:

$$a_{nr}(g_1) = r \cdot \chi(r) \cdot a_{nr}(g_2). \tag{55}$$

We shall make use of the following consequence of the Sturm bound [31]: let $h \in S_{3/2}(\Gamma_1(4\ell^2Q^2r), \alpha)_{R/pR}$ with some Nebentypus α. Assume that for all $n \leq 1 + \frac{\frac{3}{2}+\frac{1}{2}}{12}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(4\ell^2Q^2r)] = 1 + \ell(\ell+1)(r+1)\prod_{\substack{q \mid Q \\ q \text{ prime}}} q(q+1)$ we have $a_n(h) = 0$, then $h = 0$. Sturm's bound (for forms with Nebentypus) is usually stated for integral weight modular forms, and modulo a prime ideal of the ring of integers of a number field (here R). Taking the multiplication with the usual weight $\frac{1}{2}$ and level $\Gamma_0(4)$ theta series, we reduce to the

integral weight case. By decomposing pR into product of powers of prime ideals, we reduce to the case of a prime power, which is proved in [29, Corollary 2.15]. Let us also note that

$$1+\ell(\ell+1)(r+1)\prod_{\substack{q\mid Q\\ q \text{ prime}}} q(q+1)\leq Cr.$$

For $r>C$, there is no $n\leq C\cdot r$ divisible by r with $r\mid \frac{n}{r}$. Thus, (52), (55), the Sturm bound recalled above and the fact that $r\in S$ imply the following statement:

$$g_1 = r\cdot\chi(r)\cdot g_2.$$

In particular, this implies that for all $n\geq 1$ with $r\nmid n$, we have

$$a_{nr^3}(g_1) = r\cdot\chi(r)\cdot a_{nr^3}(g_2). \tag{56}$$

Let us compute separately $a_{n_0r^3}(g_1)$ and $a_{n_0r^3}(g_2)$ to derive a contradiction. Using (53) and (54) successively, as well as the assumption $\left(\frac{n_0}{r}\right)=-1$, we get

$$\begin{aligned}
a_{n_0r^3}(g_1) &= a_{n_0r^4}(g_{\chi,Q})\\
&= (\chi(r)\cdot(r+1)-\chi(r)\left(\frac{n_0r^2}{r}\right))\cdot a_{n_0r^2}(g_{\chi,Q}) - r\cdot\chi(r^2)\cdot a_{n_0}(g_{\chi,Q})\\
&= (\chi(r)^2\cdot(r+1)\cdot(r+1-\left(\frac{n_0}{r}\right)) - r\cdot\chi(r^2))\cdot a_{n_0}(g_{\chi,Q})\\
&= \chi(r^2)\cdot((r+1)\cdot(r+2)-r)\cdot a_{n_0}(g_{\chi,Q}).
\end{aligned}$$

On the other-hand, we have

$$\begin{aligned}
a_{n_0r^3}(g_2) &= a_{n_0r^2}(g_{\chi,Q})\\
&= \chi(r)\cdot(r+1-\left(\frac{n_0}{r}\right))\cdot a_{n_0}(g_{\chi,Q})\\
&= \chi(r)\cdot(r+2)\cdot a_{n_0}(g_{\chi,Q}).
\end{aligned}$$

Together with (56), this yields:

$$\chi(r^2)\cdot((r+1)\cdot(r+2)-r)\cdot a_{n_0}(g_{\chi,Q}) = \chi(r^2)\cdot r\cdot(r+2)\cdot a_{n_0}(g_{\chi,Q})$$

i.e.

$$2\chi(r^2)\cdot a_{n_0}(g_{\chi,Q}) = 0.$$

Since $2\chi(r^2)$ is invertible in R/pR (as $p>2$), we get $a_{n_0}(g_{\chi,Q})=0$, which is a contradiction since by construction of n_0, we have $a_{n_0}(g_{\chi,Q})\neq 0$. □

We can now finish the proof of Theorem A.

Take r in S. By Lemma 4.2, there exists $n_r\leq Cr$, coprime with r, such that $a_{n_rr}(g_{\chi,Q})\neq 0$. By Corollary 3.6 and Proposition 1.6, if Δ_r denotes the discriminant of $\mathbf{Q}(\sqrt{n_rr})$, it follows that $p\nmid h_\ell^-(\Delta_r)$ and $\left(\frac{\Delta_r}{Q}\right)=-1$. Observe now that $\Delta_r\leq n_rr\leq Cr^2$. Consequently, as $X\to\infty$, there are at least $\gg\frac{\sqrt{X}}{\log(X)}$ discriminants Δ_r, possibly with multiplicity, due to the prime number theorem and the fact that S has positive density. We still need to verify that there are not too many pairs $r\neq r'$ such that $\Delta_r=\Delta_{r'}$.

Take now $r_i<r_j<r_k$ three different primes in S. Hence r_j and r_k are greater than C, and they cannot divide both n_i; indeed, otherwise $Cr_k<n_i\leq Cr_i$, which leads to a contradiction. Hence, among the discriminants $\Delta_i,\Delta_j,\Delta_k$, at least two are different. Consequently, the number of discriminants $0\leq\Delta\leq X$ for which $p\nmid h_\ell^-(\Delta)$ and $\left(\frac{\Delta}{Q}\right)=-1$ is $\gg\frac{\sqrt{X}}{\log(X)}$ when $X\to\infty$.

5. Proof of Corollary D

Let us restrict to the situation where $\ell = 11$ and $p = 5$. Let $E = X_0(11)$, which is an elliptic curve over $\mathbf{Q}$. By [18, Corollary 1.8], if $\Delta > 0$ is a fundamental discriminant such that $5 \nmid \Delta$ and $\left(\frac{\Delta}{11}\right) = 1$, then $5 \nmid h_{11}^-(\Delta)$ if and only if $\mathrm{Sel}_5(E^{(\Delta)}/\mathbf{Q}) = 0$, where $E^{(\Delta)}$ is the quadratic twist of E by Δ and $\mathrm{Sel}_5(E^{(\Delta)}/\mathbf{Q})$ is the 5-Selmer group of $E^{(\Delta)}$. Furthermore, in this case, the 5-part of BSD holds.

Therefore, Corollary D would follow from Corollary C if we did not have the restriction $\left(\frac{\Delta}{5}\right) = -1$. The characters χ and χ' can be taken quadratic, as $11 \equiv 3$ (modulo 4). Furthermore, the form F_χ of Theorem 3.4 has coefficients in $\mathbf{Z}$, as it is given explicitly in terms of generalized theta series (*cf.* [2, §10.7] and [20, §4.1.1]), and we know that $F_\chi \equiv \theta_\chi$ (modulo 5). We then let

$$\tilde{g}_\chi := \frac{F_\chi - \theta_\chi}{5} \in S_{\frac{3}{2}}(\Gamma_1(4 \cdot 11^2), \chi')$$

and

$$\tilde{g}_{\chi,5} := \sum_{n \geq 1 \text{ s.t. } \left(\frac{n}{5}\right) = -1} a_n(\tilde{g}_\chi) q^n \in S_{\frac{3}{2}}(\Gamma_1(4 \cdot 11^2 \cdot 5^2), \chi'),$$

which have Fourier coefficients in $\mathbf{Z}$. Note that we can allow the level to be divisible by 5, as the coefficient field is $\mathbf{C}$, in which 5 is invertible.

By Theorem 3.4, for a fundamental discriminant $\Delta \in \mathcal{D}_{11}$ with $\left(\frac{\Delta}{5}\right) = -1$, we have $5 \mid a_\Delta(\tilde{g}_{\chi,5})$ if and only if $5 \nmid h_{11}^-(\Delta)$. Then an identical argument as in Lemma 4.2 using the Sturm bound shows that the analogue of Theorem A with the additional condition $\left(\frac{\Delta}{5}\right) = -1$ holds, under the condition that there exists a fundamental discriminant $\Delta_0 \in \mathcal{D}_{11}$ satisfying $\left(\frac{\Delta_0}{5}\right) = -1$ and which is divisible by a prime divisor $> C = 2 \cdot 11 \cdot (11+1) \cdot 5 \cdot (5+1) = 7920$. Such a Δ_0 indeed exists, as it is straightforward to check that $\Delta_0 = 8237$ (which is prime) works.

References

[1] Alex Bartel and Carlo Pagano. A heuristic for ray class groups of quadratic number fields. *arXiv:2509.20185*, 2026.

[2] Ehud Moshe Baruch and Zhengyu Mao. Central value of automorphic L-functions. *Geom. Funct. Anal.*, 17(2):333–384, 2007.

[3] Olivia Beckwith. Indivisibility of class numbers of imaginary quadratic fields. *Res. Math. Sci.*, 4:Paper No. 20, 11, 2017.

[4] Jan H. Bruinier and Ken Ono. Coefficients of half-integral weight modular forms. *J. Number Theory*, 99(1):164–179, 2003.

[5] Jan Hendrik Bruinier. Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms. *Duke Math. J.*, 98(3):595–611, 1999.

[6] Dongho Byeon. Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields. *Compositio Math.*, 126(3):249–256, 2001.

[7] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[8] Henri Darmon, Michael Harris, Victor Rotger, and Akshay Venkatesh. The derived Hecke algebra for dihedral weight one forms. *Michigan Math. J.*, 72:145–207, 2022.

[9] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[10] Georges Gras and Adeline Munnier. Extensions cycliques T-totalement ramifiées. In *Théorie des nombres, Années 1996/97–1997/98*, Publ. Math. UFR Sci. Tech. Besançon, page 16. Univ. Franche-Comté, Besançon, 1999.

[11] Farshid Hajir, Christian Maire, and Ravi Ramakrishna. On tame $\mathbb{Z}/p\mathbb{Z}$-extensions with prescribed ramification. *Canad. Math. Bull.*, 67(1):40–48, 2024.
[12] P. Hartung. Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. *J. Number Theory*, 6:276–278, 1974.
[13] Kuniaki Horie. A note on basic Iwasawa λ-invariants of imaginary quadratic fields. *Invent. Math.*, 88(1):31–38, 1987.
[14] D. R. Johnston, O. Ramaré, and T. Trudgian. An explicit upper bound for $L(1,\chi)$ when χ is quadratic. *Res. Number Theory*, 9(4):Paper No. 72, 20, 2023.
[15] Winfried Kohnen and Ken Ono. Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication. *Invent. Math.*, 135(2):387–398, 1999.
[16] Mao Hua Le. Upper bounds for class numbers of real quadratic fields. *Acta Arith.*, 68(2):141–144, 1994.
[17] Emmanuel Lecouturier. On triple product L-functions and a conjecture of Harris-Venkatesh. *Int. Math. Res. Not. IMRN*, (22):19476–19506, 2023.
[18] Emmanuel Lecouturier and Jun Wang. On the arithmetic of special values of L-functions for certain abelian varieties with a rational isogeny. *Adv. Math.*, 493:Paper No. 110919, 51, 2026.
[19] Stéphane Louboutin. Majoration au point 1 des fonctions L associées aux caractères de Dirichlet primitifs, ou au caractère d'une extension quadratique d'un corps quadratique imaginaire principal. *J. Reine Angew. Math.*, 419:213–219, 1991.
[20] Z. Mao, F. Rodriguez-Villegas, and G. Tornaría. Computation of central value of quadratic twists of modular L-functions. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 273–288. Cambridge Univ. Press, Cambridge, 2007.
[21] Zhengyu Mao. A generalized Shimura correspondence for newforms. *J. Number Theory*, 128(1):71–95, 2008.
[22] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977. With an appendix by Mazur and M. Rapoport.
[23] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.
[24] Ken Ono. Indivisibility of class numbers of real quadratic fields. *Compositio Math.*, 119(1):1–11, 1999.
[25] Vicentiu Pasol and Alexandru A. Popa. Modular forms and period polynomials. *Proc. Lond. Math. Soc. (3)*, 107(4):713–743, 2013.
[26] Alexandru A. Popa. Central values of Rankin L-series over real quadratic fields. *Compos. Math.*, 142(4):811–866, 2006.
[27] Olivier Ramaré. Approximate formulae for $L(1,\chi)$. II. *Acta Arith.*, 112(2):141–149, 2004.
[28] Nick Ramsey. Geometric and p-adic modular forms of half-integral weight. *Ann. Inst. Fourier (Grenoble)*, 56(3):599–624, 2006.
[29] Jonas B. Rasmussen. *Higher congruences between modular forms*. Phd thesis, University of Copenhagen, 2009. Available at `https://www.math.ku.dk/bibliotek/arkivet/phd-theses/phd09jbr.pdf`.
[30] Goro Shimura. On modular forms of half integral weight. *Ann. of Math. (2)*, 97:440–481, 1973.
[31] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.
[32] The PARI Group, Univ. Bordeaux. *PARI/GP version `2.15.3`*, 2023.
[33] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.
[34] J.-L. Waldspurger. Quelques propriétés arithmétiques de certaines formes automorphes sur GL(2). *Compositio Math.*, 54(2):121–171, 1985.
[35] A. Wiles. On class groups of imaginary quadratic fields. *J. Lond. Math. Soc. (2)*, 92(2):411–426, 2015.

Westlake University, Institute for Theoretical Sciences, Yungu Campus, 600 Dunyu Rd., Xihu District, Hangzhou, 310030, Zhejiang province, PR China
Email address: `elecoutu@westlake.edu.cn`

Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, F-25000 Besançon, France
Email address: `christian.maire@univ-fcomte.fr`