On class groups of imaginary quadratic fields

A. Wiles

Abstract

In this paper it is proved that one can find imaginary quadratic fields with class number not divisible by a specified prime l and with certain specified splitting conditions at a finite number of primes. Such existence theorems are useful in the arithmetic of elliptic curves and potentially also in certain lifting problems for reducible two dimensional Galois representations. The methods used are a blend of geometry and the theory of modular forms, especially the trace formula.

The principal result of this paper is the following. The case $l = 3$ is due to Bhargava (without the extra conditions on S).

Theorem 0.0.1. Let $l \geqslant 3$ be an odd prime. Let $S = S_+ \cup S_0 \cup S_-$ be a disjoint union of finite sets of odd primes. Assume that

(a) S_- contains no prime q with $q \equiv 1(l)$ and $q \equiv -1(4)$.

(b) S_+ contains no prime with $q \equiv -1(l)$.

(c) S_0 contains no prime with $q \equiv 1(l)$.

Then there exists an imaginary quadratic field L satisfying

(i) the class number h_L of L is prime to l.

(ii) L is ramified at each prime of S_0, inert at each prime of S_- and split at each prime of S_+.

If χ is a Dirichlet character let $L(s, \chi)$ denote the corresponding Dirichlet L-function. Then $L(0, \chi) \in \mathbb{Q}$ and this theorem may be reformulated using the analytic class number formula.

2010 *Mathematics Subject Classification* 11R29.

Theorem 0.0.1′. With the hypotheses of theorem 0.0.1 there is an imaginary quadratic character satisfying

(i) $L(0,\chi) \not\equiv 0(l)$

(ii) $\chi(p) = 0$ if $p \in S_0$, $\chi(p) = -1$ if $p \in S_-$, $\chi(p) = 1$ if $p \in S_+$

Remarks

(i) In the case $l = 2$ theorem 0.0.1 is true (without the extra condition on S) if $\#\ S_0 \leqslant 1$ and false if $\#\ S_0 \geqslant 2$. This follows from genus theory, quadratic reciprocity and Dirichlet's theorem on primes in progressions.

(ii) In the case $l = 3$ Bhargava, Shankar and Tsimerman have proved a stronger theorem giving the asymptotic densities of prime discriminants as in the theorem (see [B] and [BST] theorem 7), again without the condition on S.

(iii) Cohen and Lenstra have described heuristics for the frequency with which fields such as L in the theorem should occur in various settings (see [CL]). These have been refined by Bhargava in the present context, see [B].

The first general results of this kind were proved by Hartung, who proved the theorem (including the case $l = 3$) with S empty ([Ha]). Horie [Ho] proved the result with l sufficiently large compared with S. Bruinier ([Br]) proved the result for $l \geqslant 5$ under the condition $p \not\equiv 0, \mp 1(l)$ for all $p \in S$. The methods of Hartung and Horie are related to the trace formula whereas Bruinier used the theory of modular forms of half integral weight. In fact the L-values in the theorem are closely related to the coefficients of an Eisenstein series of weight $\frac{3}{2}$.

Our original interest in such results was as a potential application to modularity lifting theorems in the residually reducible case. If one could prove a similar theorem in the case of a totally real field F one would be able to confirm hypothesis H of §4.5 of [SW], at least in some cases. This would then give an unconditional lifting result of the form of Theorem B of §4.5 of [SW]. In the case of a totally real abelian field the lifting results in [SW] are proved using a theorem of Washington about the boundedness of the l part of the class number in a cyclotomic $\mathbb{Z}_p$-extension. However such a result is unknown in the general totally real case and results of the kind proved in this paper, but over totally real fields, would be an alternative. The method we use here should apply, with some modifications, to the case $l \nmid w_2(F)\zeta_F(-1)$, where $\zeta_F(s)$ is the zeta function of F and $w_2(F)$ is the

largest integer N such that the Galois group of the extension $F(\zeta_N)/F$ is an elementary abelian 2 group. However the general case needs a new argument. It is the method of §2.3 which does not work in the general setting, because the factor $w_2(F)\zeta_F(-1)$ occurs in the formula for the genus of Shimura curves over totally real fields. Results of the kind proved in this paper can also be useful in the study of elliptic curves with rational torsion points, see [Va] theorem 3.3 and corollary 3.4.

The trace formula on Shimura curves relates the trace of a Hecke operator to a sum of class numbers of orders in imaginary quadratic fields (see §1.5). We consider this in the situation of a carefully chosen Shimura curve with specified level structure (see §2.1). We choose a Hecke operator so that it is a unit in precisely one family of l-adic representations (i.e. associated to a single orbit of maximal ideals of the Hecke ring under the action of conjugation and twisting). This operator is chosen so that it picks out class numbers of orders which satisfy the splitting conditions in S (see §2.2). We can do this for any orbit of maximal ideals of the Hecke ring. We then need to compute the trace of our chosen Hecke operator, and this is essentially the dimension of the space of forms (or l-adic representations) in the chosen orbit. If it is prime to l for any orbit then we are done, for we will have found a sum of class numbers of suitable orders which is prime to l. We have only been able to do this last step under the given hypothesis on S, and we do it using the Riemann-Hurwitz formula in §2.3

1.1 Shimura Curves

Let Σ be a non-empty finite set of primes of even cardinality. Let B be the indefinite quaternion algebra which ramifies precisely at the primes of Σ. Let D be the discriminant of B, that is the product of the primes in Σ. Let G denote the algebraic group B^*, so that for any commutative $\mathbb{Q}$-algebra $A, G(A) = (B \otimes A)^*$, the invertible elements of $B \otimes A$. In particular $G(\mathbb{R}) \simeq GL_2(\mathbb{R})$ and we let $G(\mathbb{R})$ act on two copies of the upper half plane $h^{\pm}$ in the usual way. Then for every open compact subgroup K of $G(\mathbb{A}_f)$, where $\mathbb{A}_f$ denotes the finite adeles of $\mathbb{Q}$, the quotient of $G(\mathbb{A}_f) \times h^{\pm}/K$ by the left diagonal action of $G(\mathbb{Q})$ is a compact Riemann surface

$$M_K^{an} := G(\mathbb{Q})\backslash G(\mathbb{A}_f) \times h^{\pm}/K$$

The set of connected components of M_K^{an} is given by

$$\pi_0(M_K^{an}) \simeq \mathbb{Q}^{\times}\backslash \mathbb{A}_f^{\times}/nr(K^{\times})$$

where nr denotes the reduced norm map (and indeed nr induces this isomorphism). We will only need K's with $nr(K^\times) \simeq \prod \mathbb{Z}_p^\times$ in this paper so that M_K^{an} will be connected. Thus M_K^{an} may actually be described more classically as

$$M_K^{an} \simeq K \cap G(\mathbb{Q})\backslash h^\pm \simeq K \cap G^+(\mathbb{Q})\backslash h^+$$

where $G^+(\mathbb{Q})$ denotes the elements of B with positive reduced norm. We will write M_K for the complex algebraic curve associated to M_K^{an}.

We let O_B denote a fixed maximal order of B and we will assume that we have chosen K so that $K \subset \hat{O}_B$, the completion of O_B (i.e. $O_B \otimes \hat{\mathbb{Z}}$).

1.2 Local Structures

Let ν be a finite prime of $\mathbb{Q}$ where B is split. We denote by $\mathbb{Q}_\nu$ (resp. $\mathbb{Z}_\nu$) the completion of $\mathbb{Q}$ (resp. $\mathbb{Z}$) at ν. We will only consider level structures which decompose as products $K = K^\nu K_\nu$ where K^ν and K_ν are compact open subgroups respectively of,

$$G(\mathbb{A}_f)^\nu = \{g \in G(\mathbb{A}_f) : g_\nu = 1\} \quad , \quad {B_\nu}^\times \subset G(\mathbb{A}_f).$$

We define groups $U_0(\nu)$, $U_s(\nu)$ and $U^\#(\nu)$ by

$$U_0(\nu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_\nu) : c \equiv 0(\nu) \right\}$$

$$U_s(\nu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_\nu) : b \equiv c \equiv 0(\nu) \quad \text{and} \quad ad \in (\mathbb{F}_\nu^\times)^2 \right. \\ \left. \text{or} \quad a \equiv d \equiv 0(\nu) \right\}$$

$$U^\#(\nu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_\nu) : c \equiv 0(\nu), a^{\frac{\nu-1}{2}} \equiv 1(\nu) \right\}$$

We note that with K_ν's chosen from among these three groups, the local reduced norm map is surjective to ${\mathbb{Z}_\nu}^\times$. For the finite places ν where B is not split we will always pick K_ν to be a maximal order, so again the local reduced norm map is surjective to ${\mathbb{Z}_\nu}^\times$. So for the K's we consider we will always have that M_K is connected.

1.3 Hecke Operators and modular forms

Let M_K be a Shimura curve as in §1.1. Let m be a positive integer such that for every $p \mid m$, K_p is a maximal order. We allow the case where $p \in \Sigma$, so p ramifies in B. Let G_m be the set of elements g of $\hat{O}_B$ which have component 1 at primes not dividing m and such that $det(g)$ generates the ideal $(m)\mathbb{Z}_p$ at each prime $p \mid m$. In particular G_1 is a subgroup of K and G_m is a union of cosets of G_1 in $\hat{O}_B$. We define an operator T_m on M_K by the formula

$$T_m(y) = \sum_{\gamma \in G_m \backslash G_1} [(g\gamma, x)]$$

where (g, x) is a representative of y in $G(\mathbb{A}_f) \times h^{\pm}$ and $[(g\gamma, x)]$ is the projection of $(g\gamma, x)$ on to M_K. As is well known T_m defines a correspondence on M_K. In this paper we will only consider cusp forms of (parallel) weight 2 associated to B. Those of level K are precisely the holomorphic differentials $f(z)dz$ on M_K. The Hecke operator T_m acts on such forms by the formula

$$T_m(\alpha) = \sum_{\gamma \in G_m \backslash G_1} \gamma^* \alpha$$

where $\alpha \in H^0(M_K, \Omega^1)$. Hecke operators can of course be defined more generally without the restriction on m but we will only need the ones we have described.

If (n) is a product of primes in Σ then the operator T_n is of finite order and we will denote it by U_n or w_n. This is because there is a γ_n which is an element of $\hat{O}_B$ with reduced norm equal to n, and it is unique as a left ideal of $\hat{O}_B$ by the local calculations of §II.4 of [V]. Then ${w_n}^2 = 1$ since $(\gamma_n^2) = (n)$ as ideals of $\hat{O}_B$ (again by lemma II.4.1. of [V]). The action of n on $H^0(M_K, \Omega^1)$ is of course trivial.

1.4 Galois Representation and Hecke rings

We recall that if $\alpha \in H^0(M_K, \Omega^1)$ is a common eigenform for all but finitely many of the Hecke operators T_p (for p a prime), then there is a unique associated automorphic representation $\pi = \otimes \pi_\nu$ of $G(\mathbb{A}_f)$. The uniqueness is proved by associating to π an automorphic representation $\pi'$of $GL_2(\mathbb{A}_f)$ via the trace formula (due to Eichler, Shimizu and Jacquet-Langlands), and then using strong multiplicity one for GL_2. Moreover a representation π occurs in $G(\mathbb{A}_f)$ for some level K if and only if π_ν is either special or supercuspidal at each ν where B_ν is not split. Since we are only considering differentials we will only be considering π''s of parallel weight 2, thus corresponding to holomorphic Hilbert modular forms of weight 2.

If π_f is the automorphic representation associated to a common eigenform f as above then it is sometimes possible to determine the type of local representation purely from the level. If K_ν is maximal and ν is not in $ram(B)$, then π_ν is an unramified principal series. If ν is in $ram(B)$ and K_ν is a maximal order (as we are always assuming when $\nu \in ram(B)$) then π_ν is the special representation up to an unramified twist.

Associated to forms of weight 2 on Shimura curves there are compatible systems of λ-adic representations. If $T_p f = c(p,f)f$ for almost all p, then there exists a continuous 2-dimensional representation, unramified outside $ND.N(\lambda)$,

$$\rho_{f,\lambda} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(O_{f,\lambda})$$

for each prime λ of O_f, the ring of integers of the number field K_f generated over $\mathbb{Q}$ by the eigenvalues $c(p,f)$, satisfying

$$\begin{cases} trace\rho_{f,\lambda}(Frob_p) = c(p,f) \text{ for } p \nmid ND.N(\lambda) \\ det\rho_{f,\lambda}(Frob_p) = \chi_f(p)p. \end{cases} \tag{1.4.1}$$

Here we have used N for the level of f and D for the discriminant of B and we are writing χ_f for the central character of f and $N(\lambda)$ for the norm of λ. These representations are odd and irreducible. Moreover the local-global compatibility theorem describes $\rho_{f,\lambda} \mid_{D_p}$ where D_p is a decomposition group at p even for $p \mid ND$.

The Hecke operators T_m introduced in §1.3 generate a commutative ring of endomorphisms

$$\mathbb{T} \subset End_{\mathbb{C}}(H^0(M_K, \Omega^1)).$$

The minimal prime ideals of $\mathbb{T}$ correspond to the common eigenforms of the Hecke operators of the given level K. The existence of old forms when K is not maximal means $\mathbb{T}$ will in general have more than one minimal prime associated to a given π.

The maximal ideals of $\mathbb{T}$ containing the prime l correspond to the semisimplifications of the reduced representations $\rho_{f,\lambda} mod \lambda$ for $\lambda \mid l$. If $\mathfrak{m}$ is such a maximal ideal we denote by $\rho_{\mathfrak{m}}$ the associated semisimple representation

$$\rho_{\mathfrak{m}} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(k_{\mathfrak{m}})$$

satisfying the same relations as above in 1.4.1. This representation is odd and so we can and will choose $k_{\mathfrak{m}}$ to be the field generated over the prime residue field $\mathbb{F}_l$ by the traces. While the $\rho_{f,\lambda}$ are irreducible, the $\rho_{\mathfrak{m}}$ may not be. We call $\mathfrak{m}$ Eisenstein if $\rho_{\mathfrak{m}}$ is reducible (i.e. a direct sum of two characters) and we call it dihedral if the projective representation associated

to $\rho_{\mathfrak{m}}$ has dihedral image. The same representation $\rho_{\mathfrak{m}}$ can occur for different $\mathfrak{m}$'s because although $\rho_{\mathfrak{m}}$ determines the eigenvalues of T_p for $p \nmid ND$ it does not always do so for $p \mid ND$. This ambiguity may occur when $p \equiv -1(l)$, $\rho_{\mathfrak{m}}$ is unramified at p and trace$\rho_{\mathfrak{m}}(Frob_p) \equiv 0\ (l)$.

1.5 Trace formulas

In this section we recall the trace formula on Shimura curves and its relation to the trace formula on Shimura varieties of dimension zero associated to definite quaternion algebras. We begin with Shimura curves. We continue with our assumptions from §1.1 and §1.2. Thus M_K is a Shimura curve with discriminant D and level structure $K = \prod K_\nu$, with K_ν as described in §1.2. We let $N = \prod \nu$ be the level of K, i.e. where the product is taken over all ν for which K_ν is not maximal. As always N is prime to D. For simplicity we will always assume it is divisible by at least two odd primes, one congruent to -1 *mod* 3 and one congruent to -1 *mod* 4.

The groups $U_s(\nu)$ are not of the kind normally considered and in particular are not associated to Eichler orders. For this reason we will give a trace formula suited to our needs by switching to a definite quaternion algebra and then making a direct computation. For the switch we will use the results of Jacquet-Langlands which extend those of Eichler.

We will consider a definite quaternion algebra $\tilde{B}$ of discriminant D/q, where q is a chosen prime of Σ. We define two level structures on $\tilde{B}$ by writing

$$K_0 = GL_2(O_q) \times K^q \quad , \quad K_1 = U_0(q) \times K_q$$

where $K = K_q \times K^q$ is the level structure of M_K. Then we may associate a zero-dimensional 'Shimura variety' X_{Ki} to each of these level structures, for $i = 0$ and 1, in the same way as for M_K by setting

$$X_{Ki} = \tilde{B}^\times \backslash \tilde{B}(\mathbb{A}_f)/K_i$$

We can define actions of Hecke operators on functions on X_{K_i} in the usual way. Then the following result is essentially due to Jacquet and Langlands [JL] as completed by Arthur.

Theorem 1.5.1. For n prime to Nq,

$$trace\ T_n\ |_{H^0(M_K,\Omega^1)} = deg\ T_{n'} + traceT_n\ |_{X_{K_1}} - 2traceT_n\ |_{X_{K_0}}$$

where n' is the largest factor of n which is prime to D.

Proof. The forms of level K, i.e. in $H^0(M_K, \Omega^1)$, correspond to representations which are special at q, and the last term on the right hand side 'removes' the contribution from the forms which are old at q in *trace* $T_n \mid_{X_{K_1}}$. The first term on the right hand side, *deg* $T_{n'}$, comes from the fact that the functions on the zero-dimensional Shimura varieties which factor through the reduced norm do not correspond to forms of weight 2 on the Shimura curve. There is one such function up to scalars and on it T_n acts via its degree, which is *deg* $T_n \mid_{X_{K_i}}$= *deg* $T_{n'} \mid_{M_K}$. □

We now give a result which relates trace $T_n \mid_{X_{K_i}}$ to class numbers. Let t_i denote representatives in $\tilde{B}(\mathbb{A}_f)$ for the elements of X_{K_0}. Then define

$$\begin{aligned} {O_0}^{(i)} &= t_i \, \hat{O}_{\tilde{B}} t_i^{-1} \cap \tilde{B} \\ {K_0}^{(i)} &= t_i \, K_0 \, t_i^{-1} \cap \tilde{B} \end{aligned}$$

where $O_{\tilde{B}}$ is a fixed maximal order in $\tilde{B}$ and $\hat{O}_{\tilde{B}} = O_{\tilde{B}} \otimes \hat{\mathbb{Z}}$. We make similar definitions for ${O_1}^{(i)}, {K_1}^{(i)}$ with respect to a set of representatives for the elements of X_{K_1}.

Theorem 1.5.2. Suppose that n is square-free, $n > 1$ and prime to N. Then $\exists\ m_x \in \mathbb{Z}$ such that trace $T_n \mid_{X_{K_0}} = \frac{1}{2} \sum_x m_x h_x$

where x is taken over some $x \in {O_0}^{(i)}$ (for some i which depends on x) satisfying

(i) $x^2 - tx + n = 0$ with $t \in \mathbb{Z}$

(ii) $x \notin \mathbb{R}$

(iii) $x_\nu \in {K_{0,\nu}}^{(i)}$ for $\nu \mid N$.

Here we let $Cl_{L_x} = L^\times \backslash L_{\mathbb{A}}^\times / \phi^{-1}(K_0^{(i)})$ where $\phi : L_{\mathbb{A}}^\times \to G_{\mathbb{A}}$ is the embedding induced by $x \in O_0^{(i)}$, and let $h_x = \#Cl_{L_x}$ be its class number. A similar result holds for X_{K_1} in place of X_{K_0}, replacing (iii) by the condition $x_\nu \in {K_{1,\nu}}^{(i)}$ for $\nu \mid Nq$.

Remark. Typically in the trace formula the trace is given without reference to the embeddings but as a precise sum of generalised class numbers. In our case the precise numbers m_x are not important, nor is it important to have the precise set of x's but it will be crucial to know that $x_\nu \in {K_{0,\nu}}^{(i)}$. We note that Cl_{L_x} is not necessarily the class group of $\mathbb{Z}[x]$ (but is a quotient of it). In fact it is the class group of a unique order L_x in $\mathbb{Q}(x)$ containing x.

Proof. Suppose that $(t_i, t_i) \in T_n \cdot \triangle_{X_{K_0}}$ where $\triangle_{X_{K_0}}$ is the diagonal in $X_{K_0} \times X_{K_0}$. Then t_i satisfies

$$t_i \alpha_n = \gamma t_i u \qquad (1.5.1)$$

where α_n is one of the coset representatives chosen as in §1.3 for the action of T_n, in particular an element of $\hat{O}_{\tilde{B}}$ of reduced norm n with $\alpha_{n,\nu} = 1$ if $\nu \nmid n$, $\gamma \in \tilde{B}^\times$ and $u \in K_0$. Thus

$$\begin{cases} \gamma = t_i \ \alpha_n \ u^{-1} {t_i}^{-1} \in t_i \ \hat{O}_{\tilde{B}} \ {t_i}^{-1} \cap \tilde{B} = {O_0}^{(i)} \\ \gamma_\nu \in t_i \ K_{0,\nu} \ {t_i}^{-1} = {K_{0,\nu}}^{(i)} \text{ for } \nu/N. \end{cases}$$

Also γ has reduced trace an integer and reduced norm equal to (n). Since $\mathbb{Q}(\gamma)$ is imaginary (as it embeds in a definite quaternion algebra) the reduced norm of γ is actually n.

It follows that γ satisfies all the properties listed for x in the theorem. We will now partition the set of γ's into disjoint sets, each of size h_x for some x. We first note that γ is essentially uniquely determined by the pair $\{t_i, \alpha_n\}$ since if $\gamma t_i u = \gamma' t_i \ u'$, then ${\gamma'}^{-1}\gamma \in D^\times \cap K_0^{(i)} = \mp 1$ as N is divisible by two odd primes, one congruent to -1 *mod* 3 and one congruent to -1 *mod* 4. So this partitioning will give the theorem since trace $T_n = \#(T_n \cdot \triangle_{X_{K_0}})$.

We let $L = L_\gamma$ denote the field $\mathbb{Q}(\gamma)$ and we associate to γ a class group

$$Cl_\gamma = L^\times \backslash {L_{\mathbb{A}}}^\times / \phi^{-1}(K_0^{(i)})$$

where $\phi : L_{\mathbb{A}}^\times \to G_{\mathbb{A}}$ is the embedding induced by $\gamma \in K_0^{(i)} \subset O_0^{(i)} \subset \tilde{B}$. As ϕ is a homomorphism and $K_0^{(i)}$ is a group, so we do have a generalized class group. ($\phi^{-1}(K_0^{(i)}) \subset U_L$, the product of the local unit groups, as all the elements have integral trace and unit determinant). There is an action of $L_{\mathbb{A}}^\times$ on (t_i, t_i) satisfying (1.5.1) defined as follows. Write $l_a \ t_i = \gamma_1 \ t_j \ u_1$. Then because l_a and γ commute we find that, applying l_a to both sides of (1.5.1),

$$t_j \cdot u_1 \alpha_n = \gamma_1^{-1} \gamma \ \gamma_1 \cdot t_j \cdot u_1 u.$$

Thus $\gamma_1^{-1} \ \gamma \ \gamma_1$ corresponds to a point of $T_n \cdot \triangle_{X_{K_0}}$. Clearly the action of $l_1 \in L^\times$ is trivial since then we may take $l_1 = \gamma_1$. Also the action of $u_a \in \phi^{-1}(K_0^{(i)})$ is trivial. For $u_a \ t_i = t_i \ . \ t_i^{-1} \ u_a \ t_i$ and $t_i^{-1} \ u_a \ t_i \in K_0$, so $i = j$ and $\gamma_1 = 1$ in this case. It follows that Cl_γ acts on (t_i, t_i) and the orbit is

$$Cl_\gamma \cdot (t_i, t_i) \in T_n \cdot \triangle_{X_{K_0}}$$

We still have to show that the action has no fixed points. However we have seen that γ is determined up to sign by the point in $T_n \cdot \triangle_{X_{K_0}}$. So if two points

in the orbit are the same then $\gamma_1^{-1}\ \gamma\ \gamma_1 = \gamma_2^{-1}\ \gamma\ \gamma_2$ up to sign. It follows that $\gamma_1\ \gamma_2^{-1} \in L$ since L is its own centralizer in B. So if $l_{a_1} t_i = \gamma_1\ t_j\ u_1$ and $l_{a_2} t_i = \gamma_2\ t_j\ u_2$ represent the same point in $T_n \cdot \triangle_{X_{K_0}}$, then replace l_{a_2} by $\gamma_1\ \gamma_2^{-1}\ l_{a_2} = {l_{a_2}}'$. We find that

$$t_i\ {u_2}^{-1}\ u_1\ {t_i}^{-1} = {l_{a_2}}'^{-1} l_{a_1} \in t_i\ K_0\ {t_i}^{-1} \cap L_{\mathbb{A}} = \phi^{-1}(K_0^{(i)}).$$

So the action is faithful. Finally we observe that if we begin with any other point in the orbit then the same process leads to the same orbit by an isomorphic group. Essentially the same arguments work in the case where X_{K_0} is replaced by X_{K_1}.

□

We now give a variant of theorem 1.5.1 for the trace of T_n on the space of forms with character ψ. We write

$$H^{(\psi)} = H^0(M_K, \Omega^1)^{(\psi)} \subset H = H^0(M_K, \Omega^1)$$

for the space of forms with character ψ, for ψ a quadratic character of conductor q'. We compute this trace by using the isomorphism

$$H^{(\psi)} \simeq H^0(M_{K^\#}, \Omega^1)/H^0(M_K, \Omega^1)$$

where if $K = K^{q'} \times K_{q'}$ and $K_{q'} \simeq U_0(q')$ then we define $K^\# = K^{q'} \times K_{q'}^\#$ and $K_{q'}^\# = U^\#(q')$. We obtain the following result by combining theorems 1.5.1 and 1.5.2. We use the notation of those theorems.

Theorem 1.5.3. Suppose that n is square-free, $n \geqslant 1$, $(n, N) = 1$. Then $\exists m_x \in \mathbb{Z}$ such that

$$trace\ T_n\ |_{H^{(\psi)}} = \frac{1}{2} \sum_x m_x h_x$$

with x taken over some $x \in O_j^{(i)}$ (for some i depending on x) satisfying

(i) $x^2 - tx + n = 0$ with $t \in \mathbb{Z}$

(ii) $x \notin \mathbb{R}$

(iii) $x_\nu \in {K_{j,\nu}}^{(i)}$ or ${K_{j,\nu}^\#}^{(i)}$ for $j = 0$ or 1 (depending on ν), for all $\nu \mid N$.

2.1 Choice of D and N

From now on we let l be an odd prime, $l \geqslant 5$. We let

$$S = S_0 \cup S_- \cup S_+$$

be the disjoint union of three sets of odd primes. We assume as in the statement of theorem 0.0.1 that S_- contains no prime q with $q \equiv 1(l)$ and $q \equiv -1(4)$. Let I_0 be an indexing set for $\{q_i \in S_0 : q_i \not\equiv 1(l)\}$. We then choose a prime $\pi' \notin S$ satisfying

(i)

$$\left(\frac{\pi'}{q}\right) = -\left(\frac{\prod_{i\in I_0} q_i}{q}\right) \quad \text{for } q \in S_+ \cup S_-, q \neq l \tag{2.1.1}$$

and

$$\left(\frac{\pi'}{q}\right) = -\left(\frac{\prod_{i\in I_0} q_i}{q}\right)\left(\frac{-1}{l}\right) \quad \text{if } q = l \in S_+ \cup S_-$$

(ii) $\pi' \not\equiv \mp 1 \ (l)$

We also introduce a prime $\pi'' \notin S \cup \{\pi'\}$ satisfying

(i)

$$\left(\frac{\pi''}{q}\right) = -\left(\frac{\prod_{i\in I_0} q_i}{q}\right) \quad \text{for all } q \in S_0 \cup S_- \tag{2.1.2}$$

(ii) $\pi'' \not\equiv \mp 1(l)$

To see that such a prime exists we note that the only compatibility to be checked is if some q is l. This causes no problem as $l \neq 3$.

We next pick a second auxiliary prime q' ($q' \notin S \cup \{\pi, \pi''\}$) satisfying the conditions

(i) $q' \equiv 1 \ (l)$ (2.1.3)

(ii) there is a real quadratic character χ of conductor q' satisfying

$$\begin{cases} \chi(q) = -1 & \text{for all } q \in S \text{ such that } q \equiv -1(l) \\ \chi(q) = +1 & \text{for all } q \in S \text{ such that } q \equiv 1(l) \end{cases}$$

Now choose a further set P' of auxiliary primes $\{p_i'\}$, $p_i' \notin S \cup \{\pi', \pi'', q'\}$ with the p_i' mutually distinct, satisfying the following conditions:

(I) $p_i' \not\equiv 1(l)$ for all i

(II) if $l \equiv 3(4)$ then for each irreducible representation

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(k)$$

where k is a finite field of characteristic l, where ρ is of dihedral type, which is unramified outside $S \cup \{q', \pi', l\}$, whose associated quadratic field is $\mathbb{Q}(\sqrt{-l})$ or $\mathbb{Q}(\sqrt{-q'l})$ and which satisfies $det\rho = \chi\omega$, there exists a $p_i' \in P'$ such that $Frob_{p_i'}$ has eigenvalues whose ratio is not $\omega(p_i')$. (Here ω is the *mod* l cyclotomic character).

(III) for each ρ as in (II) but where the associated projective representation has image A_4, S_4 or A_5 the same conclusion as (II) should hold.

Lemma 2.1.1. A set P' exists with properties (I) - (III).

Proof. In (II) we are assuming that $l \equiv 3(4)$. Also $l \geqslant 5$ so $\#\ im(det\rho) \geqslant 6$. On the other hand $im\tilde{\rho} \subset PGL_2(k)$ is dihedral so its maximal cyclic quotient is of order 2. It follows that the centre of $im\rho$ has order at least 3. Pick p_i to be any prime with $Frob_{p_i}$ representing an element in the centre of order at least 3. We choose such a p_i for each ρ as in (II).

In (III) we use lemma 1.10(ii) of [W1].

□

We are now in a position to choose D and N. We let

$$D = \pi'.\pi''. \prod_{q \in I_D} q \prod_{p_i' \in P'} p_i' \tag{2.1.4}$$

where $I_D = \{q \in S_0\} \cup \{q \in S_- : q \not\equiv 1(l) \text{ or } q \not\equiv 1(4)\}$. We also choose D to have an even number of prime factors by enlarging P' if necessary.

Next we introduce a level N by setting

$$N = q' \prod_{q \in I_1} q \prod_{q \in S_+} q \tag{2.1.5}$$

where $I_1 = \{q \in S_- : q \equiv 1(l) \text{ and } q \equiv 1(4)\}$. We use a level structure $K = \prod K_v$ where

$$\begin{aligned} K_v &= U_0(v) \text{ for } \nu = q \in S_+ \\ K_v &= U_s(v) \text{ for } \nu = q \in \{q \in S_- : q \equiv 1(l), q \equiv 1(4)\} \\ K_{q'} &= U^{\#}(q') \end{aligned}$$

At all other v's we require K to be a maximal order. As always we assume that N is divisible by at least one prime congruent to -1 *mod* 3 and one prime congruent to -1 *mod* 4. We will consider the space of modular forms of weight 2 on a quaternion algebra B of discriminant D which have level K structure and character χ. We write

$$H^\chi = H^0(M_K, \Omega^1)^{(\chi)} \quad \subset \quad H = H^0(M_K, \Omega^1)$$

for the space of forms with character χ. We let $\mathbb{T} = \mathbb{T}^{(ND)}$ denote the Hecke ring generated by the Hecke operators T_n with n prime to ND acting on H. We also write $\mathbb{T}^{(N),(\chi)}$ or $\mathbb{T}^{(\chi)}$ for the image of $\mathbb{T}$ in $End(H^{(\chi)})$. For any maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ let $\mathbb{T}_\mathfrak{m}$ denote the completion at $\mathfrak{m}$ and let $H_\mathfrak{m} = H \otimes_\mathbb{T} \mathbb{T}_\mathfrak{m}$ We also define $\mathbb{T}_\mathfrak{m}^{(\chi)}$ and $H_\mathfrak{m}^{(\chi)}$ similarly. If we need to specify the level then we write $\mathbb{T}_\mathfrak{m}^{(N),(\chi)}$ for this ring.

The auxiliary primes in P' were introduced in order to enable us to limit the $\rho_\mathfrak{m}$'s that can occur as described in the following lemma.

Lemma 2.1.2. If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}^{(\chi)}$ with D and N as given in (2.1.4) and (2.1.5) then the projective image of $\rho_\mathfrak{m}$ in $PGL_2(k_\mathfrak{m})$ is one of

(a) a conjugate of $PGL_2(k_0)$ for some $k_0 \subset k_\mathfrak{m}$,

(b) a conjugate of $PSL_2(k_0)$ for some $k_0 \subset k_\mathfrak{m}$,

(c) a cyclic group.

Proof. By Dickson's classification of subgroups of $PGL_2(k)$ we only have to eliminate the cases of dihedral groups of order prime to l, as well as the groups A_4, S_4 and A_5.

We begin with the dihedral case. The order of a dihedral group, if irreducible in $PGL_2(k_{\mathfrak{m}})$, is of order prime to l. In particular $\rho_{\mathfrak{m}}$ is unramified at primes $p_i' \in P'$ since $p_i'|D$ and so the local representations at these primes are special. The determinant of $\rho_{\mathfrak{m}}$ is $\chi\omega$ so the associated imaginary quadratic field is unramified outside of q' and l. Since $\mathbb{Q}(\sqrt{-q'})$ is ramified at 2 it must be $\mathbb{Q}(\sqrt{-q'l})$ or $\mathbb{Q}(\sqrt{-l})$. For the same reason $l \equiv 3(4)$. If the dihedral representation has the form $Ind\psi$ then we see that $\chi\omega = (\psi \circ N)\chi_{K/\mathbb{Q}}$ where K is the associated quadratic field. This only has a solution (with q'^2 not dividing the conductor) if the field is $\mathbb{Q}(\sqrt{-q'l})$. Since $\rho_{\mathfrak{m}}$ is special at the p_i', the ratio of the eigenvalues of the $Frob_{p_i'}$ is $\omega(p_i')$. However this contradicts property (II) of the p_i' in P'.

We also rule out the A_4, S_4 and A_5 cases using property III of P'. (Note that we are not excluding the A_5 case if $l = 5$). □

2.2 Class numbers and Hecke Rings

We continue with the notation and assumptions of §2.1, in particular with the definitions of D, N, K and χ and with N divisible by at least two odd primes. We are now in a position to prove the key result.

Theorem 2.2.1. Let l be an odd prime, $l \geqslant 5$. Suppose that there is a level N as in (2.1.5) such that either of the two following sets of conditions is satisfied,

(A) There exists an $\mathfrak{m}$ such that

- (i) $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}^{(\chi)}$ with $l \in \mathfrak{m}$
- (ii) $\rho_{\mathfrak{m}}$ is absolutely irreducible
- (iii) $dim H_{\mathfrak{m}}^{(\chi)} \not\equiv 0(l)$ and $dim_{\mathbb{F}_l} k_{\mathfrak{m}} \not\equiv 0(l)$

or

(B) if $\{\mathfrak{m}_i\}$ is the set of Eisenstein maximal ideals of $\mathbb{T}^{(\chi)}$ with $l \in \mathfrak{m}_i$, then $\sum dim H_{\mathfrak{m}_i}^{(\chi)} \not\equiv 0(l)$.

Then there exists an imaginary quadratic field L with

(I) $h_L \not\equiv 0(l)$

(II) L is ramified at each prime of S_0, inert at each prime of S_- and split at each prime of S_+.

Remark. At least one of conditions (A) and (B) hold if $dim H^{(\chi)} \not\equiv 0(l)$. For in this case $rank_{\mathbb{Z}} \mathbb{T}^{(\chi)} \not\equiv 0(l)$. We will verify this condition for certain choices of N, D, K and χ in §2.3. The result would still hold if we made the more natural choice of $I_D = S_0 \cup S_-$ and $I_1 = \phi$, but the conditions we have chosen are sometimes easier to verify.

Proof. Let $L^{(\chi)}$ be a $\mathbb{T}^{(\chi)}$ stable lattice in $H^{(\chi)}$ and let $L^{(\chi)}_{\mathfrak{m}}$ denote its completion at $\mathfrak{m}$. We write $V = L^{(\chi)}/l\ L^{(\chi)}$ and $V_{\mathfrak{m}} = L^{(\chi)}_{\mathfrak{m}}/l\ L^{(\chi)}_{\mathfrak{m}}$. For each $q \in S_0$ with $q \not\equiv 1(l)$ (i.e. for each $q \in I_D \cap S_0$) and for π', we decompose V and $V_{\mathfrak{m}}$ into eigenspaces under the action of w_q and $w_{\pi'}$. We write

$$V = \oplus V^{(\boldsymbol{\epsilon})} \qquad , \qquad V_{\mathfrak{m}} = \oplus V^{(\boldsymbol{\epsilon})}_{\mathfrak{m}}$$

where $V^{(\boldsymbol{\epsilon})}$ (and $V^{(\boldsymbol{\epsilon})}_{\mathfrak{m}}$) denotes the subspace on which $w_{q_i} = \epsilon_i$, $w_{\pi'} = \epsilon'$ and $w_{\pi''} = \epsilon''$ for $\{\epsilon_i, \epsilon', \epsilon''\} \in \{\pm 1\}$ and $\underline{\epsilon} = (\epsilon', \epsilon'', \epsilon_1, ...\epsilon_t)$. Here $t = \#I_D \cap S_0$ and $I_0 = I_D \cap S_0 = \{q_1, ..., q_t\}$. Then $V^{(\boldsymbol{\epsilon})}$ and $V^{(\boldsymbol{\epsilon})}_{\mathfrak{m}}$ are still acted on by $\mathbb{T}^{(\chi)}$ because this ring commutes with the w-operators, which are in fact Hecke operators themselves.

Now let $H^{\acute{e}t}_l := H^1_{\acute{e}t}(M_K, \mathbb{Q}_l)$ denote the corresponding l-adic cohomology of the Shimura curve M_K. Then the ring $\mathbb{T}$ acts on $H^{\acute{e}t}_l$ and we use a $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\mathbb{T}$-stable lattice to define spaces $W^{(\boldsymbol{\epsilon})}$ and $W^{(\boldsymbol{\epsilon})}_{\mathfrak{m}}$ in the same manner as $V^{(\boldsymbol{\epsilon})}$ and $V^{(\boldsymbol{\epsilon})}_{\mathfrak{m}}$. For any $p \nmid NDl$ we have

$$\text{trace } T_p \mid_{V^{(\boldsymbol{\epsilon})}} = \frac{1}{2} \text{ trace } T_p \mid_{W^{(\boldsymbol{\epsilon})}} \tag{2.2.1}$$

For $W^{(\boldsymbol{\epsilon})}$ the trace is then half the trace of $Frob_p$ in the associated Galois representation by the theorems of Eichler and Shimura.

□

CASE(A)

We will now assume the hypothesis (A) holds in the statement of the theorem. Thus we assume that $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}^{(\chi)}$ satisfying $A(i)-(iii)$.

Let $\prod_l$ denote the set of maximal ideals $\mathfrak{m}'$ of $\mathbb{T}^{(\chi)}$ with $l \in \mathfrak{m}'$ and write

$$\begin{aligned} \prod\nolimits_1 &= \{\mathfrak{m}^\sigma : \sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})\} \cup \{\mathfrak{m}^\sigma \otimes \chi : \sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})\} \\ \prod\nolimits_l &= \prod\nolimits_1 \cup \prod\nolimits'_1 \end{aligned}$$

where $\prod_1'$ is defined as the complement of $\prod_1$ in $\prod_l$. Note that the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ and of tensoring with χ does preserve $\prod_l$ (indeed the local representations at q' associated to forms in $\mathbb{T}^{(\chi)}$ are of the form $\pi(\mu_1, \mu_2)$ with one of the μ_i unramified, and determinant equal to χ times an unramified character. Tensoring with χ thus preserves $H^{(\chi)}$).

Lemma 2.2.1. There exist primes $q \nmid NDl$ satisfying

(a) $\alpha = \text{trace } \rho_{\mathfrak{m}}(Frob_q) \neq 0$ with $\alpha \in \mathbb{F}_l$

(b) $q \equiv -1(l)$

(c) $\chi(q) = 1$

(d) $q \equiv 1(4)$

(e) $\left(\frac{q}{q_i}\right) = 1$ for all $q_i \in S_- \cup S_+$with $q_i \neq l$

(f) in all representations $\rho_{f,\lambda}$ associated to an $\mathfrak{m}' \in \prod_1'$, $Frob_q$ is very close to a complex conjugation and in particular satisfies

$$trace\rho_{f,\lambda}(Frob_q) \equiv 0(l^n) \text{ for some } n >> 0$$

Proof. Let $\bar{G}_1 = Gal(F_1/\mathbb{Q})$ denote the Galois group of the splitting field of the projective representation $\bar{\rho}_{\mathfrak{m}}$ associated to $\rho_{\mathfrak{m}}$. Let $G_2 = Gal(F_2/\mathbb{Q})$ denote the Galois group of the splitting field of all the $\rho_{f,\lambda}$ mod l^n representations associated to $\mathfrak{m}' \in \Pi_1{}'$. Let G denote the image of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\bar{G}_1 \times G_2$. Then by Goursat's lemma G is the graph of an isomorphism $\bar{G}_1/\bar{N}_1 \simeq G_2/N_2$.

By lemma 2.1.2 $\bar{G}_1$ is isomorphic to $PGL_2(k_0)$ or $PSL_2(k_0)$ for some finite field $k_0 \subseteq \bar{\mathbb{F}}_l$. It follows that $\bar{N}_1$ is 1 or $PGL_2(k_0)$ or $PSL_2(k_0)$. Suppose first that $\bar{N}_1$ is 1. This means in particular that $F_1 \subset F_2$.

Let us suppose that $\bar{G}_1 \simeq PSL_2(k_0)$. (The case $PGL_2(k_0)$ requires only minor adjustments). Let $\{\mathfrak{m}_i{}'\}_{i=1}^R$ denote the distinct non-Eisenstein maximal ideals in $\Pi_1{}'$ up to twist and conjugation. Let $\rho_i{}'$ denote the Galois representation associated to $\mathfrak{m}_i{}'$ and $\bar{\rho}_i{}'$ the associated projective representation. Let K_r denote the splitting field of $\{\bar{\rho}_i{}' : 1 \leq i \leq r\}$. Then F_2/K_R is solvable. So since $Gal(F_1/\mathbb{Q})$ is a simple group and the image of

$$Gal(F_2K_R/K_R) \to Gal(F_1/\mathbb{Q})$$

is a normal subgroup we see that $F_1 \subset K_R$. Repeating this argument (with F_1K_r in place of F_2K_R for $r = R-1, R-2, ...$) we find that for some $r \leq R-1, F_1 \subset K_{r+1}$ and

$$Gal(F_1K_r/K_r) \to Gal(F_1/\mathbb{Q})$$

is an isomorphism. Now letting ${F_{r+1}}'$ denote the splitting field of $\bar{\rho}'_{r+1}$ we have maps

$$Gal(F_1/\mathbb{Q}) \tilde{\leftarrow} Gal(F_1K_r/K_r) \leftarrow Gal(K_{r+1}/K_r) \to Gal({F_{r+1}}'/\mathbb{Q}) \quad (2.2.2)$$

The right hand map is injective as $K_{r+1} = K_r{F_{r+1}}'$. Since $F_1 \subset K_{r+1}$ the central map is surjective. Since $Gal({F_{r+1}}'/\mathbb{Q})$ is isomorphic to $PSL_2(k')$ or $PGL_2(k')$ for some k', so too is $Gal(K_{r+1}/K_r)$ as it is a normal subgroup. We deduce that the central map is also an isomorphism. The injection on the right is of index 1 or 2, again as it is a non-trivial normal subgroup of $Gal({F_{r+1}}'/\mathbb{Q})$.

Thus (2.2.2) gives, via $\bar{\rho}_{\mathfrak{m}}$ and $\bar{\rho}_{{r+1}'}$ (the projective Galois representation associated to ${\mathfrak{m}_{r+1}}'$), an embedding of $PSL_2(k_0)$ in $PGL_2(k_{\mathfrak{m}})$ and $PGL_2(k_{{\mathfrak{m}_{r+1}}'})$. It follows that $k_0 \subseteq k_{\mathfrak{m}}, k_{{\mathfrak{m}_{r+1}}'}$. Let ${k_0}' = k_{\mathfrak{m}}k_{{\mathfrak{m}_{r+1}}'}$. Then by Dickson's classification [D] these two embeddings are conjugate in $PGL_2({k_0}')$. We deduce that $\rho_{r+1\prime} \simeq \rho_{\mathfrak{m}} \otimes \psi$ for some character ψ. However ψ must be trivial or χ since $\rho_{r+1\prime}$ and $\rho_{\mathfrak{m}}$ have square-free conductor. It follows that ${\mathfrak{m}_{r+1}}' \in \Pi_1$ which contradicts our hypothesis. A similar argument works in the case of $PGL_2(k_0)$. So the case $\bar{N}_1 = 1$ does not occur.

It follows that the image of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\bar{G}_1 \times G_2$ is the graph of $\bar{G}_1/\bar{N}_1 \simeq G_2/N_2$ with the quotient being abelian. Moreover from the explicit description of $\bar{G}_1$ this quotient is either 1 or $\mathbb{Z}/2\mathbb{Z}$. So if we replace $\bar{G}_1$ by G_1, the Galois group of the splitting field of $\rho_{\mathfrak{m}}$, then the image G of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ in $G_1 \times G_2$ is the graph of an isomorphism

$$G_1/N_1 \simeq G_2/N_2$$

with this quotient still abelian.

Now the maximal abelian quotient of G_1 is the Galois group ${G_1}^{ab}$ of the maximal abelian extension in the splitting field of $\rho_{\mathfrak{m}}$. We claim that it is contained in the composite of the splitting fields of $\chi\omega$ and of χ. For the centre of G_1 is cyclic so ${G_1}^{ab}$ is either a cyclic group or of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for some m. It contains the splitting field of $\chi\omega$ and so the only quadratic fields that it can contain are in $\{\mathbb{Q}_\chi \cdot \mathbb{Q}_{(\chi w)^{\frac{l-1}{2}}}\}$ for ramification reasons. Similarly there is no character ψ of conductor lq' satisfying $\psi^2 = \chi\omega$, so the cyclic group has order $l-1$ i.e. $m = l-1$.

Choose an element $g \in G$ as follows. We let $g_2 \in G_2$ be a complex conjugation. Now G_1 contains an element σ of order l. Pick a complex conjugation τ_1 in G_1 which is not in the same Borel as σ. Then it is easily verified that $det(\tau_1\sigma) = -1$ and trace $\rho_{\mathfrak{m}}(\tau_1\sigma) \in \mathbb{F}_l$ and is non-zero. Now pick $g \in G$ such that $g = \tau_1\sigma$ in G_1 and $g = g_2$ in G_2. This is possible because they are equal on the abelian quotient $G_1/N_1 \simeq G_2/N_2$. For $det(\tau_1\sigma) = det(g_2) = -1$, and also $\chi(\tau_1\sigma) = 1 = \chi(g_2)$ if $\mathbb{Q}_\chi$ is in this abelian quotient as χ is a real quadratic character. If $\mathbb{Q}_\chi$ is not in the quotient we can extend g to include this condition.

Conditions (d) and (e) of the lemma involve the splitting of q in quadratic fields that are ramified outside q' and l. They are disjoint from the splitting field associated to G. So we may choose q so that $Frob_q$ represents g in G, is trivial on $\mathbb{Q}_\chi$ and splits in the quadratic fields associated to the conditions (d) and (e). Conditions (a) and (f) are satisfied by our choices of $g = \tau_1\sigma$ in G_1 and $g = g_2$ in G_2.

□

We now revert to the proof of the theorem and consider the action of $Frob_q$ on $W_l^{(\boldsymbol{\epsilon})}$. By condition (iii) of the theorem, and using that $dim\ V_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})} = \frac{1}{2}$ $dim W_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})}$ for each $\mathfrak{m}'$, we see that there is a choice of $(\boldsymbol{\epsilon})$ with $dim\ W_{\mathfrak{m}}^{(\boldsymbol{\epsilon})} \not\equiv 0(l)$ and $dim\ k_{\mathfrak{m}} \not\equiv 0(l)$. Then by part (a) of lemma 2.2.1 we see that $\alpha = trace(Frob_q) \not\equiv 0(l)$ on $W_{\mathfrak{m}}{}^{(\boldsymbol{\epsilon})}$ also. So by condition (c) of the lemma

$$trace(Frob_q)\ |_{W_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})}} = \alpha \not\equiv 0(l)$$

for each $\mathfrak{m}'$ in Π_1. Since the number of $\mathfrak{m}'$'s in Π_1 is prime to l (by our assumptions that $dim\ k_{\mathfrak{m}} \not\equiv 0(l)$ and l is odd) we find that

$$\sum_{\mathfrak{m}' \in \Pi_1} trace(Frob_q)\ |_{W_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})}} \not\equiv 0(l)$$

On the other hand the contribution of $trace(Frob_q)$ in each $W_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})}$ for $\mathfrak{m}' \in \Pi_1{}'$ is zero modulo l because the eigenvalues $+1$ and -1 occur with equal multiplicity by condition (f) of the lemma. To see this let $L_{f,\lambda}$ be a Galois stable lattice in the representation associated to f and λ. Then we have an exact sequence

$$0 \to L_{\mathfrak{m}'}^{(\chi)} \to \oplus L_{f,\lambda} \to F \to 0$$

where (f, λ) runs over all pairs associated to $\mathfrak{m}'$ and F is a finite Galois module. Reducing $mod\ l$ we see that the multiplicities of the eigenvalues $+1$ and -1 are the same in the two representations

$$V_{\mathfrak{m}'} = L_{\mathfrak{m}'}{}^{(\chi)}/l\ L_{\mathfrak{m}'}{}^{(\chi)} \quad , \quad \bigoplus_{(f,\lambda)} L_{f,\lambda}/l\ L_{f,\lambda}$$

By our choice of $Frob_q$ they are equal on the right, so they are also equal in $V_{\mathfrak{m}}{}'$. (We remark that while this is obvious for $\mathfrak{m}'$ irreducible, the Eisenstein case has motivated the form of our requirements in (f)). The same result holds for $V_{\mathfrak{m}'}{}^{(\boldsymbol{\epsilon})}$ since the actions of τ and of the w operators commute and each $L_{f,\lambda}$ is associated to a fixed $\boldsymbol{\epsilon}$ depending on f and λ. We deduce that

$$trace(T_q) \mid_{V^{(\boldsymbol{\epsilon})}} = trace(Frob_q) \mid_{W^{(\boldsymbol{\epsilon})}} \not\equiv 0(l) \tag{2.2.3}$$

by (2.2.1)

We now observe that on $V^{(\boldsymbol{\epsilon})}$

$$trace(T_q\ U_{\pi'} \prod_{i=1}^{t} U_{q_i}) = \mp trace(T_q) \not\equiv 0(l), \tag{2.2.4}$$

where the product is taken over all $q_i \in S_0$. To see this observe that from the proof we need only consider $\mathfrak{m}'$'s in Π_1 as the contribution of the $\mathfrak{m}'$'s in Π_1' to the trace is zero *mod* l. For $\mathfrak{m} \in \Pi_1$ we claim that $W_{\mathfrak{m}}^{(\boldsymbol{\epsilon}_2)} = 0$ for any $\boldsymbol{\epsilon}_2 \neq \boldsymbol{\epsilon}$. This is because the eigenvalues of the U_{q_i} and of U_π' are determined by the actions of $\{Frob_{q_i}\}$ and $Frob_{\pi'}$ in $\rho_{\mathfrak{m}}$. This is because by our choices of χ we have $det\ \rho_{\mathfrak{m}}(Frob_{q_i}) = \chi(q_i)\omega(q_i) = 1$ for $q_i \in S_0$ and $det\ \rho_{\mathfrak{m}}(Frob_{\pi'}) \neq \mp 1$. The eigenvalue of the U_{q_i} operator is then given by the action of a decomposition group at q_i on a certain unramified quotient in $\rho_{\mathfrak{m}}$ (see [W2] theorem 2.1.4), and similarly for $U_{\pi'}$. Even if this quotient is not unique, the eigenvalues are equal (for $q_i \in S_0$) so are still determined by $\rho_{\mathfrak{m}}$. This completes the proof of (2.2.4).

□

We now use the trace formula (theorem 1.5.3) to reinterpret (2.2.4) as a sum over class numbers of suitable imaginary quadratic orders. The trace is given by

$$trace(T_q U_{\pi'} \prod_{i=1}^{t} U_{q_i}) \mid_{H^0(M_K,\Omega^1)^{(\chi)}} = \frac{1}{2} \sum_x m_x h_x$$

where the sum over x is described in theorem 1.5.3. We deduce that at least one of the h_x occurring in the sum is not divisible by l by (2.2.4). We now examine the properties of the x's in the sum.

Each h_x is the class number of an order in an imaginary quadratic field $\mathbb{Q}(x)$. This order contains the element x which satisfies

$$x^2 - tx + \pi' q \prod_{i=1}^{t} q_i = 0 \tag{2.2.5}$$

Also $x_\nu \in K_{o,\nu}{}^{(i)}$ for $\nu \mid N$. We pick an x for which $h_x \not\equiv 0(l)$.

From the equation (2.2.5) the divisors of the q_i's for $q_i \in S_0$ cannot be inert. Since the divisors of D must be inert or ramified (as $\mathbb{Q}(x)$ embeds in B) we deduce that such q_i's ramify in $\mathbb{Q}(x)$.

Suppose next that $q_j \in S_- \cap I_D$. We have chosen π' so that

$$\left(\frac{\pi' \prod_{i=1}^{t} q_i}{q_j}\right) = -1$$

for $q_j \in S_-$, assuming that $q_j \neq l$. Assume for now that $q_j \neq l$. We recall that we also chose $\left(\frac{q}{q_j}\right) = 1$. It follows that

$$\left(\frac{q\pi' \prod_{i=1}^{t} q_i}{q_j}\right) = -1 \tag{2.2.6}$$

So the discriminant of (2.2.5) is non-zero *mod* q_j, whence $\mathbb{Q}(x)$ is unramified at q_j. Since $\mathbb{Q}(x)$ embeds in B it follows that q_j must be inert in $\mathbb{Q}(x)$. If $q_j = l$, then again

$$\left(\frac{q\pi' \prod_{i=1}^{t} q_i}{q_j}\right) = -\left(\frac{-1}{l}\right)^2 = -1$$

by (2.1.1) (i) and lemma 2.2.1 (b) and we again argue as above.

For the primes $q_j \in S_-$, $q_j \equiv 1(l)$ and $q_j \equiv 1(4)$ we recall that $K_{q_j} = U_s(q_j)$. As above we observe that (2.2.6) holds so the roots of (2.2.5) are distinct. Since they also lie in $U_s(q_j)$ and their product is not a square, they are not rational over $\mathbb{Z}_{q_j}$. (This is where we use that $q_j \equiv 1(4)$). It follows that q_j is inert in $\mathbb{Q}(x)$.

For the primes $q_j \in S_+$ we observe that, just as in the inert case, the discriminant is not zero *mod* q_j. So the field $\mathbb{Q}(x)$ is unramified at q_j. On the other hand $x_{q_j} \in {K_{0,q_j}}^{(i)}$, so we see that

$$x \in {t_i}^{-1} K_{0,q_j}\ t_i \cap O_{B,q} = t_i^{-1} U_{0,q_j} t_i \cap O_{B,q}$$

For such an x the roots are rational *mod* q_j, so the equation (2.2.5) splits *mod* q_j. It follows that q_j splits in $\mathbb{Q}(x)$. This completes the proof in case (A).

Case (B)

This time we assume that hypothesis (B) holds i.e. that $\mathfrak{m}$ is Eisenstein. We explain the adjustments that need to be made. This time we let Π_1 denote the set of all maximal ideals.

In the statement of lemma 2.2.1 we now consider primes $q \nmid NDl$ satisfying the conditions of lemma 2.2.1 except that (b) and (f) are replaced by

$(b)'$ $q \equiv 1(l)$

$(f)'$ in all representations $\rho_{f,\lambda}$ associated to an $\mathfrak{m}' \in \Pi_1{}'$, $Frob_q$ satisfies $trace\rho_{f,\lambda}(Frob_q) \equiv 0(l^n)$ for $n >> 0$.

The proof is similar to the previous case. We define G_2 to be the Galois group of the composite of the splitting fields of all the ρ_i' in Π_2'. We claim first that we can pick an element σ of order 4 in G_2 with the following property:

$$\sigma \text{ has eigenvalues } \{\mp i\} \text{ in each } \rho_i{}' \quad , \quad \mathfrak{m}_i{}' \in \Pi_1{}' \tag{2.2.7}$$

Let $G_{2,i}$ denote the Galois group of the splitting field of $\rho_i{}'$. Then to verify (2.2.7) we first see inductively, by the same method as in case (A) using Goursat's lemma, that there is a surjection

$$G_2{}' \to \prod_{i=1}^{t} G_{2,i}{}'$$

where $G_2{}', G_{2,i}{}'$ are the derived groups of G_2 and $G_{2,i}$, and $\{\mathfrak{m}_i{}' : i = 1, \ldots, t\}$ runs through a full set of representatives for the $\mathfrak{m}_i{}' \in \Pi_2{}'$ which are distinct under conjugation and tensoring by χ. We claim that each $G_{2,i}{}'$ is isomorphic to $SL_2(k_{0,i})$ for some $k_{0,i}$. To see this observe first that its projective image is $PSL_2(k_{0,i})$ or $PGL_2(k_{0,i})$ and it has no abelian quotient. So its projective image is $PSL_2(k_{0,i})$. It also contains $\{\mp 1\}$ since it has an element of order 2 with determinant 1, and this must be the whole centre as the determinant is 1 on $G_{2,i}{}'$

Pick an element $\sigma_i \in G_{2,i}{}'$ with eigenvalues $\{\mp i\}$ for each i, and then pick $\sigma \in G_2{}'$ which maps to $\Pi\sigma_i$. We may view σ as an element of G_2 and it is thus 1 on any abelian extension of $\mathbb{Q}$ in the field F_2 associated to G_2. We extend σ to split in the field $F_2(\zeta_l).\mathbb{Q}_\chi$ if this is larger. Finally we pick σ to be a lift of order 4 in the Galois group of the field generated over this by the splitting field of all the $\rho_{f,\lambda}$ *mod* l^n (associated to the $\mathfrak{m}_i{}' \in \Pi_2{}'$) and by the splitting field of $\rho_{\mathfrak{m}}$. This choice of σ, or rather any $Frob_q$ which represents it, satisfies conditions $(a), (b)', (c), (f)'$ of lemma 2.2.1. We can incorporate conditions (d) and (e) by further splitting requirements on q just as in case (A).

For the rest of the proof of case (B) we proceed as before except that we replace the use of the prime π' by the prime π''.

2.3 Application of the Riemann-Hurwitz formula

In this section we show how to find D, N, K and χ so that the hypotheses of theorem 2.2.1 hold. This will then complete the proof of theorem 0.0.1.

We now assume that the conditions of theorem 0.0.1 hold for the set of primes S and keep this assumption for the remainder of the section. We choose N, D and the level structure K just as in §2.1. Thus in particular N is given by

$$N := q' \prod_{q_i \in I_1} q_i \prod_{q_i \in S_+} q_i$$

We consider the level structure $K = \Pi K_\nu$ with

$$\begin{aligned} K_{q_i} &= U_s(q_i) \text{ for } q_i \in S_-,\ q_i \equiv 1(l),\ q_i \equiv 1(4) \\ K_{q_i} &= U_0(q_i) \text{ for } q_i \in S_+, \\ K_{q'} &= U^{\#}(q') \end{aligned}$$

We will also assume (by enlarging S is necessary) that $q_i \equiv 1(12)$, for some $q_i | N_0$. This ensures that the Shimura curve $X_B(K)$ associated to the quaternion algebra B, of discriminant D and level K, has no elliptic fixed points.

With these hypotheses the Riemann-Hurwitz formula gives a value for the genus of $X_B(K)$ which we write $g(X_B(K))$:

$$g(X_B(K)) = 1 + \frac{1}{12} \prod_{p|D} (p-1) \prod_{\nu | N} [GL_2(\mathbb{Z}_\nu) : K_\nu]$$

Our choices have ensured that $l \nmid [GL_2(\mathbb{Z}_\nu) : K_\nu]$ for any ν and that $l \nmid p - 1$ for $p \mid D$ and hence that

$$g(X_B(K)) \not\equiv 1(l) \tag{2.3.1}$$

The same calculation applies if we replace K by K^0 where K^0 has level structure which differs from K only at q' and where $K^0_{q'} = U_0(q')$. Now the covering

$$X_B(K) \to X_B(K^0)$$

is unramified of degree 2 so, by the Riemann-Hurwitz formula,

$$2g(X_B(K)) - 2 = 2\ (2g(X_B(K^0)) - 2)$$

It then follows from (2.3.1) that $g(X_B(K)) - g(X_B(K^0)) \not\equiv 0(l)$. This is the dimension of the space $H^0(X_B(K), \Omega^1)^{(\chi)}$, so

$$dim H^0(X_B(K), \Omega^1)^{(\chi)} \not\equiv 0(l)$$

We can now apply theorem 2.2.1 to this space, or rather to some $\mathfrak{m}$-component of it. Either there is an irreducible $\mathfrak{m}$ satisfying the hypothesis (A) of the theorem or the set of Eisenstein ideals satisfy hypothesis (B). We may now apply theorem 2.2.1 to the $\mathfrak{m}$'s we have constructed with level N. This yields the proof of theorem 0.0.1.

References

[B] M. BHARGAVA, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminant*, Int. Math. Res. Not. IMRN, 17 (2007).

[Br] J. H. BRUINIER, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, Duke Math. (3) **98** (1999), 595–611.

[BST] M. BHARGAVA, A. SHANKAR and J. TSIMERMAN, *On the Davenport-Heilbronn theorems and second order terms (English Summary)*, Invent. Math. (2) **193** (2013), 439–499.

[CL] H. COHEN and H. W. LENSTRA Jr., "Heuristics on class groups of number fields", in *Number Theory (Noordwijkerhout 1983)*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, 33–62.

[D] L. E. DICKSON, *Linear Groups with an Exposition of the Galois Field Theory* (1901), Teubner, Leipzig.

[Ha] P. HARTUNG, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Theory, (6) (1974), 276–278.

[Ho] K. HORIE, *Trace formulae and imaginary quadratic fields*, Math. Ann. (4) **288** (1990), 605–612.

[JL] H. JACQUET and R. P. LANGLANDS, *Automorphic forms on GL(2)*, Notes in Mathematics, **114**, (1970), Springer-Verlag, Berlin, New York.

[SW] C. M. SKINNER, and A. WILES, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. (1999), no. 89. 5–126.

[Va] V. VASTAL, *Canonical periods and congruence formulae*, Duke Math. J. (2) **98** (1999), 397–419.

[V] M.-F. VIGNÉRAS, *Arithmétique des algébres de quaternions*, Lecture Notes in Mathematics, **800** Springer, Berlin, 1980.

[W1] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

[W2] A. WILES, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. (3) **94** (1988), 529–573.

A. Wiles
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford
OX2 6GG
United Kingdom