Journal of Number Theory **95**, 14–37 (2002)
doi:10.1006/jnth.2001.2753

Dihedral Congruence Primes and Class Fields of Real Quadratic Fields

Alexander F. Brown and Eknath P. Ghate

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India
E-mail: abrown@math.tifr.res.in, eghate@math.tifr.res.in

Communicated by K. Ribet

Received May 9, 2000

We show that for a real quadratic field F the dihedral congruence primes with respect to F for cusp forms of weight k and quadratic nebentypus are essentially the primes dividing expressions of the form $\varepsilon_+^{k-1} \pm 1$ where ε_+ is a totally positive fundamental unit of F. This extends work of Hida. Our results allows us to identify a family of (ray) class fields of F which are generated by torsion points on modular abelian varieties. © 2002 Elsevier Science (USA)

Key Words: dihedral congruence primes; fundamental units; real quadratic fields; class field theory.

1. INTRODUCTION

Let $F = \mathbb{Q}(\sqrt{D})$ denote a real quadratic field of discriminant $D > 0$. Let χ_D denote the corresponding quadratic character. Let $S_k(D, \chi_D)$ denote the cusp forms of weight $k \geqslant 2$, level D and nebentypus χ_D. A cusp form $f \in S_k(D, \chi_D)$ is said to be primitive if it is a normalized newform that is a common eigenform of all the Hecke operators.

In [Hid98], Hida characterized the primes of congruence between f and $f \otimes \chi_D$ as f varies through all primitive elements in $S_k(D, \chi_D)$ in terms of the primes dividing $\varepsilon_+^{k-1} - 1$ where ε_+ is a totally positive fundamental unit of F.

The starting point of this paper was the following question: can the primes of congruence between f and $f \otimes \chi$ be similarly characterized for arbitrary even quadratic characters χ that are 'factors' of the nebentypus χ_D? In the first part of this paper we answer this question affirmatively. This time the answer involves expressions of the form $\varepsilon_+^{k-1} \pm 1$ where ε_+ is a totally positive fundamental unit of the real quadratic field F_χ corresponding to χ. As in [Hid98] we work under certain technical assumptions of ordinarity and absolute irreducibility and do not elaborate upon this here.

0022-314X/02 $35.00

Hilbert's twelfth problem asks whether one can generate the (ray) class fields of a given number field explicitly, for instance by the torsion points on an abelian variety, or by the values of a modular function. The case where the base field is $\mathbb{Q}$ or an imaginary quadratic field is classical. For more general CM fields some partial results due to Shimura and Taniyama are available [Shi99]. However, for many years the next simplest case, that of real quadratic fields, defied treatment. Then, in the early 1970s Shimura [Shi71, Shi72] invented a beautiful method to explicitly generate the (ray) class fields of real quadratic fields via torsion points on certain modular abelian varieties. His method has since been extended by other authors [DY73, Koi76, Oht77].

In the second part of this paper, we further extend Shimura's method using our characterization of 'dihedral congruence primes' in the first part. We show that by considering congruences in a systematic way with twists that are not necessarily the full nebentypus we can, at least in principle, generate explicitly infinitely many (ray) class fields of the same real quadratic field by Shimura's method. We say 'in principle' since, as we shall see in the text, our results are subject to the phenomenon of extra twisting. We also prove some results which combine Hida's theory of families of ordinary modular forms with Shimura's method, further increasing its scope.

2. DIHEDRAL CONGRUENCE PRIMES AND FUNDAMENTAL UNITS

We start with some notation which is more general than that used in the Introduction. Let $F = \mathbb{Q}(\sqrt{D})$ denote an *arbitrary* quadratic field of discriminant D. Let

$$\chi_D : (\mathbb{Z}/|D|\mathbb{Z})^\times \to \{\pm 1\}$$

denote the quadratic character corresponding to $F/\mathbb{Q}$. Let $S_k(|D|, \chi_D)$ denote the cusp forms of weight $k \geqslant 2$, level $|D|$ and nebentypus χ_D. Let $f \in S_k(|D|, \chi_D)$ be a primitive cusp form; i.e., a normalized newform that is a common eigenform of all the Hecke operators. Note that there are no oldforms in the space $S_k(|D|, \chi_D)$ since the conductor of χ_D is equal to the level $|D|$.

Let $\mathbb{C}$ denote the field of complex numbers. Recall that f has a Fourier expansion

$$f = \sum_{n=1}^{\infty} a(n, f) q^n, \tag{2.1}$$

where $a(n, f) \in \mathbb{C}$ for all $n \geqslant 1$. Let $\bar{\mathbb{Q}} \subset \mathbb{C}$ denote the subfield of algebraic numbers. It is well known that the $a(n, f)$ are algebraic integers. Let $\wp$ be a prime of $\bar{\mathbb{Q}}$ of residue characteristic p. f is said to be *ordinary at* $\wp$ if $a(p, f)$ is a $\wp$-adic unit. (Warning: it is possible for f to be ordinary at some $\wp$ above p but not at another prime $\wp'$ above p.)

Consider the factorization $D = D_1 D_2$ of D into two fundamental discriminants D_1 and D_2. We allow the case $D_1 = D$ and $D_2 = 1$. Let χ_{D_1} denote the quadratic character of conductor $|D_1|$ and let $F_1 = \mathbb{Q}(\sqrt{D_1})$ denote the corresponding quadratic field. Throughout this paper we shall assume that

$$F_1 \text{ is a real quadratic field.}$$

The cusp form $f \otimes \chi_{D_1}$ is again a primitive element of $S_k(|D|, \chi_D)$. We will call a prime $\wp$ of $\bar{\mathbb{Q}}$ a *dihedral congruence prime for* f *with respect to* F_1 if there is a congruence $f \equiv f \otimes \chi_{D_1} \bmod \wp$. By a slight abuse of notation we sometimes call the prime p of $\mathbb{Q}$ lying under $\wp$ a dihedral congruence prime as well.

In this section, we will describe the set of ordinary dihedral congruence primes with respect to F_1 of the primitive elements of $S_k(|D|, \chi_D)$ in terms of the fundamental units of F_1. This generalizes a result of Hida [Hid98] where the case $F_1 = F$ was treated. We start with the following theorem:

THEOREM 2.1. *Let p be a prime such that $(p, 2D) = 1$. Let f be a primitive element of $S_k(|D|, \chi_D)$ and assume that $k - 1 \not\equiv 0 \bmod p - 1$. Suppose that f satisfies a congruence of the form*

$$f \equiv f \otimes \chi_{D_1} \bmod \wp \tag{2.2}$$

for a prime $\wp$ of $\bar{\mathbb{Q}}$ over p. Suppose also that f is ordinary at $\wp$ and that the mod $\wp$ *Galois representation attached to f is absolutely irreducible. Then*

- *p splits in F_1,*
- *q splits in F_1 for each prime $q|D_2$, and*
- *$p \mid \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - (-1)^a)$,*

where ε_+ is a totally positive fundamental unit of F_1 and a is an integer depending on F_1 and D_2 described in (2.10).

Proof. We remark that the condition $p \mid \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - (-1)^a)$ is independent of the choice of the totally positive fundamental unit ε_+.

We make the convention that all number fields K are subfields of $\bar{\mathbb{Q}}$. Here and below we will write $\wp$ for the prime of the number field K which lies under the prime $\wp$ of $\bar{\mathbb{Q}}$. Let K_f denote the Hecke field of f. It is the

number field generated by the Fourier coefficients of f. Let $K_{f,\wp}$ denote the completion of K_f at $\wp$.

For a subfield N of $\bar{\mathbb{Q}}$ write G_N for $\mathrm{Gal}(\bar{\mathbb{Q}}/N)$. Let

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\wp})$$

denote the Galois representation attached to f constructed by Eichler and Shimura for $k = 2$ and by Deligne for $k \geqslant 2$. Note that ρ_f is irreducible, unramified outside Dp and is characterized by

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_\ell)) = a(\ell, f)$$

for all primes $\ell \nmid Dp$. Moreover,

$$\det(\rho_f) = \omega_p^{k-1}\chi_D,$$

where $\omega_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is the cyclotomic character.

By choosing a $G_{\mathbb{Q}}$-stable lattice we may assume that the representation ρ_f takes values in $\mathrm{GL}_2(\mathcal{O}_{f,\wp})$ where $\mathcal{O}_{f,\wp}$ is the ring of integers of $K_{f,\wp}$. By reducing mod $\wp$ we obtain the mod $\wp$ representation attached to f, namely

$$\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}),$$

where $\mathbb{F} = \mathcal{O}_{f,\wp}/\wp$ is the residue field. By hypothesis, $\bar{\rho}_f$ is absolutely irreducible. In particular, it is independent of the choice of lattice made above.

Congruence (2.2) along with the absolute irreducibility of $\bar{\rho}_f$ implies that

$$\bar{\rho}_f \sim \bar{\rho}_f \otimes \chi_{D_1},$$

where we are now thinking of χ_{D_1} as a Galois character with values in $\pm 1 \subset \mathbb{F}^\times$. Write $H_1 = G_{F_1}$ for simplicity. Under the absolute irreducibility of $\bar{\rho}_f$ it is well known that there is a character $\phi : H_1 \to \bar{\mathbb{F}}^\times$ such that

$$\bar{\rho}_f = \mathrm{Ind}_{H_1}^{G_{\mathbb{Q}}}(\phi).$$

Let σ denote the non-trivial element of $\mathrm{Gal}(F_1/\mathbb{Q})$. Extend σ to an element of $G_{\mathbb{Q}}$ and continue to denote this element by σ. The condition of absolute irreducibility implies that

$$\phi \neq \phi^\sigma,$$

where ϕ^σ is the conjugate character defined by $\phi^\sigma(h) = \phi(\sigma h \sigma^{-1})$ for all $h \in H_1$. Moreover, we have

$$\bar{\rho}_f|_{H_1} \sim \begin{pmatrix} \phi & 0 \\ 0 & \phi^\sigma \end{pmatrix}. \tag{2.3}$$

Let $G_p \subset G_{\mathbb{Q}}$ denote the decomposition group at $\wp$ and I_p the inertia subgroup. Let $\mathfrak{p}$ be the prime of F_1 lying under $\wp$. Let $H_{\mathfrak{p}}$, $I_{\mathfrak{p}}$, denote the decomposition and inertia subgroups of H_1 at $\wp$.

Since $a(p, f)$ is a $\wp$-adic unit a theorem of Deligne says that the restriction of ρ_f to G_p is reducible. More precisely, we have

$$\rho_f|_{G_p} \sim \begin{pmatrix} \delta & * \\ 0 & \varepsilon \end{pmatrix} \tag{2.4}$$

for characters $\delta, \varepsilon : G_p \to \mathcal{O}_{f,\wp}^{\times}$. Moreover, it is known that ε is unramified.

There is an exact sequence

$$1 \to \overline{F_1^{\times} F_{\infty+}^{\times}} \to \mathbb{A}_{F_1}^{\times} \xrightarrow{[\,,F_1]} H_1^{\mathrm{ab}} \to 1$$

where $[\,, F_1]$ is the Artin map. Composing ϕ with the Artin map allows us to think of ϕ as a continuous finite-order Hecke character

$$\phi : F_1^{\times} \backslash \mathbb{A}_{F_1}^{\times} \to \bar{\mathbb{F}}^{\times}.$$

Let $\mathfrak{c}$ be the finite part of the conductor of ϕ. Denote by ϕ once more the associated Dirichlet character of conductor $\mathfrak{c}$:

$$\phi : (\mathcal{O}_{F_1}/\mathfrak{c})^{\times} \to \bar{\mathbb{F}}^{\times}.$$

Now (2.3) shows that

$$\phi \cdot \phi^{\sigma} = \omega_p^{k-1} \chi_D \tag{2.5}$$

on H_1. Since we have assumed that $k - 1 \not\equiv 0 \bmod p - 1$ we see that $\omega_p^{k-1} \neq 1$ and therefore at least one of ϕ or ϕ^{σ} is ramified at $\mathfrak{p}$. On the other hand, by comparing (2.3) and (2.4) on $H_{\mathfrak{p}} = H_1 \cap G_p$ we see that exactly one of ϕ or ϕ^{σ} is ramified at $\mathfrak{p}$. By relabelling, if necessary, we may assume that ϕ is ramified at $\mathfrak{p}$ and that ϕ^{σ} is unramified at $\mathfrak{p}$.

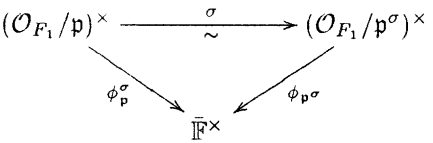
This forces p to split in F_1. Indeed if $\mathfrak{p}$ were inert then, since the conductor of ϕ^{σ} is $\mathfrak{c}^{\sigma}$ and $\mathfrak{p} \mid \mathfrak{c}$, one would have $\mathfrak{p} = \mathfrak{p}^{\sigma} | \mathfrak{c}^{\sigma}$, contradicting the fact that ϕ^{σ} is unramified at $\mathfrak{p}$.

For a prime $\lambda | \mathfrak{c}$, let us write ϕ_{λ} for the component of the Dirichlet character ϕ at λ. We now describe the possibilities for the components ϕ_{λ} using (2.5) in various cases.

First, assume that $D_1 = D$ so that $D_2 = 1$. This case has already been treated by Hida but we repeat the argument here for completeness. In this case (2.5) gives

$$\phi \phi^{\sigma} = \omega_p^{k-1} \tag{2.6}$$

on H_1 since χ_D is trivial on H_1. We conclude that $\phi_{\mathfrak{p}}\phi_{\mathfrak{p}}^{\sigma} = \omega_{\mathfrak{p}}^{k-1}$. Since $\phi_{\mathfrak{p}}^{\sigma} = 1$ we have $\phi_{\mathfrak{p}} = \omega_{\mathfrak{p}}^{k-1}$. Also, since the following diagram commutes:



we see that $\phi_{\mathfrak{p}^{\sigma}} = 1$. Thus, $\phi = \phi_{\mathfrak{p}}\phi_{\mathfrak{p}^{\sigma}} = \omega_{\mathfrak{p}}^{k-1}$ has conductor $\mathfrak{p}$ and is given by the map

$$(\mathcal{O}_{F_1}/\mathfrak{p})^{\times} \to \bar{\mathbb{F}}^{\times}, \qquad x \mapsto x^{k-1}.$$

Since $\phi(\varepsilon_+) = 1$ we see that $p | \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - 1)$, as desired.

Let us now consider the case in which $D_1 \neq D$ so that $D_2 \neq 1$. Since χ_{D_1} becomes trivial when restricted to H_1, (2.5) shows that

$$\phi \cdot \phi^{\sigma} = \omega_p^{k-1} \cdot \chi_{D_2} \tag{2.7}$$

on H_1. Note that since the conductor of χ_{D_2} is $D_2\mathcal{O}_{F_1}$ we obtain $\phi_{\mathfrak{p}} = \omega_{\mathfrak{p}}^{k-1}$ and $\phi_{\mathfrak{p}}^{\sigma} = 1$ as before.

We now prove that q splits in F_1 for each $q \,|\, D_2$. Let N be the prime to p part of the Artin conductor of $\bar{\rho}_f$. It is known (see for instance [Car89] or [DT94]) that N divides the level of f. Thus, if e_q denotes the exponent of q dividing N then $e_q = 1$. On the other hand,

$$e_q = \sum\nolimits_{i=0}^{\infty} \frac{1}{[I_0 : I_i]} \dim(V/V^{I_i}),$$

where V is a model for $\bar{\rho}_f$ over $\bar{\mathbb{F}}_p$ and I_i denotes the ith ramification group at q. This shows that $V^{I_0} \neq 0$ since otherwise $e_q \geqslant 2$. Let $(a, b) \in V$ denote a non-zero vector fixed by $I_0 = I_q$. Let $\mathfrak{q}$ be a prime of F_1 lying over q. Let $I_{\mathfrak{q}}$ denote the inertia subgroup at $\mathfrak{q}$. Then for $h \in I_{\mathfrak{q}} \subset H_1$ we have

$$\rho(h)\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \phi_{\mathfrak{q}}(h) & 0 \\ 0 & \phi_{\mathfrak{q}}^{\sigma}(h) \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Since at least one of a or b is non-zero, either $\phi_{\mathfrak{q}} = 1$ or $\phi_{\mathfrak{q}}^{\sigma} = 1$. Now (2.7) yields the relation

$$\phi_{\mathfrak{q}} \cdot \phi_{\mathfrak{q}}^{\sigma} = \chi_{\mathfrak{q}}, \tag{2.8}$$

where we have written $\chi_{\mathfrak{q}}$ for $(\chi_{D_2})_{\mathfrak{q}}$. This shows that exactly one of $\phi_{\mathfrak{q}}$ or $\phi_{\mathfrak{q}}^{\sigma}$ is trivial. Since the following diagram commutes:

$$\begin{array}{ccc} (\mathcal{O}_{F_1}/\mathfrak{q})^{\times} & \xrightarrow[\sim]{\sigma} & (\mathcal{O}_{F_1}/\mathfrak{q}^{\sigma})^{\times} \\ & {\scriptstyle \phi_{\mathfrak{q}}^{\sigma}} \searrow \quad \swarrow {\scriptstyle \phi_{\mathfrak{q}^{\sigma}}} & \\ & \bar{\mathbb{F}}^{\times} & \end{array}$$

we deduce that $q = \mathfrak{q}\mathfrak{q}^{\sigma}$ must be split in F_1.

The above argument shows that for any prime $\mathfrak{q}$ of F dividing D_2 either

$$\phi_{\mathfrak{q}} = \chi_{\mathfrak{q}} \qquad \text{and} \qquad \phi_{\mathfrak{q}^{\sigma}} = 1 \tag{2.9}$$

or

$$\phi_{\mathfrak{q}} = 1 \qquad \text{and} \qquad \phi_{\mathfrak{q}^{\sigma}} = \chi_{\mathfrak{q}^{\sigma}}.$$

Now

$$1 = \phi(\varepsilon_+) = \phi_{\mathfrak{p}}(\varepsilon_+) \cdot \phi_{\mathfrak{p}^{\sigma}}(\varepsilon_+) \cdot \prod\nolimits_{q|D_2} \phi_{\mathfrak{q}}(\varepsilon_+)\phi_{\mathfrak{q}^{\sigma}}(\varepsilon_+) = \omega_{\mathfrak{p}}^{k-1}(\varepsilon_+) \prod\nolimits_{q|D_2} \chi_{\mathfrak{q}}(\varepsilon_+),$$

where $\mathfrak{q}$ in these products denotes the prime of F lying over q at which (2.9) holds. This shows that $\varepsilon_+^{k-1} \equiv (-1)^a \bmod \mathfrak{p}$, where

$$a \text{ is the number of primes } q \text{ dividing } D_2 \text{ for which } \chi_{\mathfrak{q}}(\varepsilon_+) = -1. \tag{2.10}$$

Hence, we have $p | \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - (-1)^a)$. ∎

As already remarked, Theorem 2.1 was proved by Hida [Hid98] in the situation where $\chi_{D_1} = \chi_D$ is the full nebentypus. In this case, k is even and so the condition that $k-1$ is not a multiple of $p-1$ is superfluous since p is an odd prime. Also in this case, $a = 0$ and the conclusion of the theorem $p | \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - 1)$ may be checked to be equivalent to $p | \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon^{k-1} - 1)$ where ε is a fundamental unit for F_1.

In [Hid98] Hida also establishes a converse: he shows that if $(p, 6D) = 1$, p splits in $F = \mathbb{Q}(\sqrt{D})$ and $p | \mathrm{N}_{F/\mathbb{Q}}(\varepsilon^{k-1} - 1)$ where ε is a fundamental unit of F, then for every prime $\wp$ of $\bar{\mathbb{Q}}$ lying over p, there is a primitive element $f \in S_k(D, \chi_D)$ such that f is ordinary at $\wp$, the mod $\wp$ Galois representation attached to f is absolutely irreducible and $f \equiv f \otimes \chi_D \bmod \wp$. We now establish a converse to Theorem 2.1. Our result includes Hida's converse. Like Hida we avoid the prime $p = 3$ when $k = 2$; in fact, a study of the space $S_2(37, \chi_{37})$ shows that the converse is false for $p = 3$ and $k = 2$.

THEOREM 2.11. *Let p be a prime such that $(p, 2D) = 1$. Let $k \geqslant 2$ be such that $k - 1 \not\equiv 0 \bmod p - 1$ and assume that $p \neq 3$ if $k = 2$. Suppose that*

- *p splits in F_1,*
- *q splits in F_1 for each prime $q \mid D_2$, and*
- *$p \mid \mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} - (-1)^a)$,*

where ε_+ is a totally positive fundamental unit of F_1 and a is defined as in (2.10). *For each prime $\wp$ of $\bar{\mathbb{Q}}$ lying over p there is a primitive element $f \in S_k(|D|, \chi_D)$ such that f is ordinary at $\wp$, the mod $\wp$ Galois representation attached to f is absolutely irreducible and f satisfies the congruence*

$$f \equiv f \otimes \chi_{D_1} \bmod \wp.$$

Proof. The proof is similar to the one given in [Hid98] and uses Hida's theory of families for ordinary forms.

Fix a prime $\mathfrak{p}$ for any prime of $\bar{\mathbb{Q}}$ lying over p. Let

$$\mathfrak{c} = \mathfrak{p} \prod_{q \mid D_2} \mathfrak{q},$$

where $\mathfrak{q}$ in this product denotes a prime of F_1 over q and $\mathfrak{p}$ is the prime of F_1 lying under $\wp$. Let $\mathbb{F}_p$ denote the field with p elements. Consider the Dirichlet character

$$\phi_f : (\mathcal{O}/\mathfrak{c})^\times \to \bar{\mathbb{F}}_p^\times$$

whose components are $\phi_{\mathfrak{p}} = \omega_{\mathfrak{p}}^{k-1} \neq 1$ and $\phi_{\mathfrak{q}} = \chi_{\mathfrak{q}}$ for each $\mathfrak{q}$ dividing $\mathfrak{c}$. Under the hypothesis on ε_+ we have $\phi_f(\varepsilon_+) = 1$.

We claim that by choosing ϕ_∞ to be the sign character $\phi_{\infty,v}$ at exactly one infinite place v of F_1 we can ensure that

$$\phi_f(u)\phi_\infty(u) = 1 \tag{2.12}$$

for all units u of F_1. Let ε be a fundamental unit of F_1. If ε is totally positive then $\varepsilon \in \langle \varepsilon_+ \rangle$, hence $\phi_f(\varepsilon) = 1$. Then for any infinite place v of F_1 we have $\phi_f(\varepsilon)\phi_{\infty,v}(\varepsilon) = 1$. If ε is not totally positive then $\varepsilon^2 \in \langle \varepsilon_+ \rangle$, hence $\phi_f(\varepsilon) \in \{\pm 1\}$. Choose v such that $\phi_{\infty,v}(\varepsilon) = \phi_f(\varepsilon)$. Furthermore, we have $\phi_f(-1) = (-1)^{k-1}\chi_{D_2}(-1)$, hence $\phi_f(-1)\phi_{\infty,v}(-1) = 1$. Since $\varepsilon, -1$ generate the units of F_1 this establishes the claim.

Let $\hat{\mathcal{O}}_{F_1}$ denote the pro-finite completion of $\mathcal{O}_{F_1}$ and let $U(\mathfrak{c}) = 1 + \mathfrak{c}\hat{\mathcal{O}}_{F_1} \subset \hat{\mathcal{O}}_{F_1}^\times$. Let $F_{1,\infty}^\times = (\mathbb{R}^\times)^2$ and let $F_{1,\infty+}^\times = (\mathbb{R}_+^\times)^2$. Then we have an inclusion of finite groups

$$\mathcal{O}_{F_1}^\times \backslash (\hat{\mathcal{O}}_{F_1}^\times \times F_{1,\infty}^\times)/U(\mathfrak{c}) \times F_{1,\infty+}^\times \hookrightarrow F_1^\times \backslash \mathbb{A}_{F_1}^\times / U(\mathfrak{c}) \times F_{1,\infty+}^\times, \tag{2.13}$$

where the index is the class number of F_1. Condition (2.12) shows that the characters (ϕ_f, ϕ_∞) give rise to a character on the smaller subgroup in (2.13). Extending this character to a character of the larger group we obtain a finite-order Hecke character $\phi : F_1^\times \backslash \mathbb{A}_{F_1}^\times \to \bar{\mathbb{F}}_p^\times$ of conductor $\mathfrak{c}v$. Now let

$$f_1 = \sum\nolimits_{\mathfrak{a} \subset \mathcal{O}} \phi(\mathfrak{a}) q^{\mathrm{N}_{F_1/\mathbb{Q}}(\mathfrak{a})}$$

be the theta series attached to ϕ where ϕ here is thought of as a multiplicative function on the integral ideals of F_1 which vanishes on those ideals that meet $\mathfrak{c}$. Then (see [Miy89, Theorem 4.8.3])

$$f_1 \in S_1(|D|p, \chi_D \omega_p^{k-1}).$$

Moreover, $\bar{\rho}_{f_1} \sim \bar{\rho}_{f_1} \otimes \chi_{D_1}$ so that $f_1 \equiv f_1 \otimes \chi_{D_1} \bmod \wp$.

Now $a(p, f_1) = \phi(\mathfrak{p}) + \phi(\mathfrak{p}^\sigma)$ where σ is the non-trivial element in $\mathrm{Gal}(F_1/\mathbb{Q})$. Since $\phi(\mathfrak{p}) = 0$ and $\phi(\mathfrak{p}^\sigma)$ is a root of unity we see that f_1 is ordinary at $\wp$. Therefore, f_1 sits in a Hida family (see, for example, [Hid93, Chap. 7] where the prime power level is treated) whose weight l member is a $\wp$-ordinary element

$$f_l \in S_l(|D|p, \chi_D \omega_p^{k-l}).$$

The form $f = f_k \in S_k(|D|p, \chi_D)$ then almost satisfies the desired properties of the form in the conclusion of the theorem. It is $\wp$-ordinary by construction, $\bar{\rho}_f$ is absolutely irreducible since $\phi \neq \phi^\sigma$, and $f \equiv f \otimes \chi_{D_1} \bmod \wp$ since f and f_1 have the same mod $\wp$ Galois representation.

We say 'almost' in the sentence above since f has p in its level. But, as we now show, we may assume that $f \in S_k(|D|, \chi_D)$ by replacing f with a $\wp$-ordinary primitive form $g \in S_k(|D|, \chi_D)$ with the same mod $\wp$ Galois representation as f. Indeed, when $k \geqslant 3$, there is an isomorphism

$$S_k^{\mathrm{ord}}(|D|p, \chi_D) = S_k^{\mathrm{ord}}(|D|, \chi_D),$$

where the superscript denotes the subspace of $\wp$-ordinary forms. This isomorphism is well known: it follows from the fact that a (p-new) primitive form $g \in S_k(|D|p, \chi_D)$ has pth Fourier coefficient satisfying $a(p, g) = \pm p^{(k-2)/2}$ (see [Miy89, Theorem 4.6.17]) and so is not ordinary at $\wp$ if $k \geqslant 3$.

When $k = 2$ the above argument fails. We use instead the following argument which will require the additional hypothesis that $p \neq 3$. Recall that $\phi = \omega_{\mathfrak{p}}$ and $\phi^\sigma = 1$ on $I_{\mathfrak{p}}$. Thus (2.3) shows that

$$\bar{\rho}_f|_{I_p} \sim \begin{pmatrix} \omega_p & 0 \\ 0 & 1 \end{pmatrix} \tag{2.14}$$

since $I_p = I_{\mathfrak{p}} \subset H_1$. The behaviour of $\bar{\rho}_f$ on I_p described by (2.14) above along with [Ser87, Proposition 3] shows that the Serre weight of $\bar{\rho}_f$ is $k(\bar{\rho}_f) = 2$. By [Rib94, Theorem 3.3], $\bar{\rho}_f$ arises from $S_2(\Gamma_1(D))$. Actually, Ribet's theorem requires $p \geqslant 5$, but the part of the theorem that we need (namely the equality of the sets $\mathcal{N}_1$ and $\mathcal{N}_3$ in his notation) is valid even for $p = 3$. Now Carayol [Car89, Proposition 3] (or [Rib94, Theorem 1.3]) shows that $\bar{\rho}_f$ arises from a form $g \in S_2(D, \chi_D)$. The result of Carayol is valid only for $p \geqslant 5$ and it is here that we use the hypothesis that $p \neq 3$. Note that the form g continues to be $\wp$-ordinary since if it were not a theorem of Fontaine [Edi92, Theorem 2.6] would say that $\bar{\rho}_g$ is irreducible on G_p whereas we already know that $\bar{\rho}_g \sim \bar{\rho}_f$ is reducible on $G_p = H_{\mathfrak{p}} \subset H_1$. ∎

Here is some numerical data to illustrate Theorems 2.1 and 2.11. These data were compiled with the aid of the modular forms calculator `HECKE` written by W. Stein, available at `http://modular.fas.harvard.edu`.

We restrict to the case where $D = D_1 D_2$ is the product of two primes congruent to $1 \bmod 4$ with $\chi_{D_1}(D_2) = 1$. Thus D is positive and therefore $k \geqslant 2$ is even.

Column 2 lists the odd primes which split (or ramify) in $\mathbb{Q}(\sqrt{D})$ and which divide the norm of $\varepsilon_{+,D}^{k-1} - 1$ for a totally positive fundamental unit $\varepsilon_{+,D}$ of $\mathbb{Q}(\sqrt{D})$. Let ε_{+,D_i} be an analogous unit for $\mathbb{Q}(\sqrt{D_i})$ for $i = 1, 2$. Since $D_i \equiv 1 \bmod 4$, the norm of a fundamental unit of $\mathbb{Q}(\sqrt{D_i})$ is -1. Consequently, ε_{+,D_i} is a square and $a = 0$ in (2.10). Thus, in columns 3 and 4 we list the odd primes which split (or ramify) in $\mathbb{Q}(\sqrt{D_i})$ and which divide the norm of $\varepsilon_{+,D_i}^{k-1} - 1$ for $i = 1, 2$. Column 5 lists the primes dividing the discriminant of the Hecke algebra.

As predicted by our theorems every prime (which is prime to $6D$) that occurs in columns 2–4 also occurs in column 5 as a dihedral congruence prime (actually the Hecke discriminant only shows that it occurs as a congruence prime).

Column 6 gives the dimension of $S_k(D, \chi_D)$ partitioned according to $G_{\mathbb{Q}}$-orbits of primitive forms. When there is only one orbit then the dihedral congruence primes arise because of the phenomenon of extra twisting as we shall explain in Section 3 (see Tables I and II).

Some large factors (denoted by p or q if they are known to be prime and by n if they are possibly composite) appear in the tables below. These factors are not important for our purposes but for completeness we list them:

$$
\begin{aligned}
p_{145} &= 342379216210842635305685754876967109 9\\
p_{689} &= 1205496111864022253479367\\
p_{793} &= 2324195671211370589\\
p_{901} &= 129196963641464623\\
q_{901} &= 3328968195415999986013\\
p_{205} &= 22723708823\\
q_{205} &= 10385895568903051794474791759280258119944561
\end{aligned}
$$

p_{221} = 1111523239622632157524576477637325711959616179045094404902744467611

n_{305} = 4436763773764945764125473776802353195620339527347665991905424185596744
71632457873503283742426725396363327002021780010660107649329251 1

n_{377} = 1876202351613287283244648137810920543235177403807980793620358397680811
01025161812558333395576383481646527023327932899249379830433647245293

n_{445} = 3224436219733814792283346896639607247598031655094559161261403635371203
47931114164815587217927678015411774335019525264133118010579825048350 47
76433503415307656689346873521824474551028084609020801514111565185918 25
20790193367416737997767896359590473416261826061024951872852529048807 6
77789891280944699586502529618779886298028491600257131855399188076103 07
52020723081

n_{689} = 6070327714830186706749485036618749511762723694879284371336442785678951
12391058938993578356081283803175523883714504638851738428762525802070 40
36089589189889490174297086135169554496688994090768582970854965805733 87
78040995110801510498942362220220967890631959968430130145338353915072 45
7061381.

TABLE I

Dihedral Congruence Primes for $S_2(D, \chi_D)$

Level	$\varepsilon_{+,D}$	ε_{+,D_1}	ε_{+,D_2}	Hecke discriminant	Orbits
$145 = 5 \cdot 29$	3		5	2 3 5 17	$12 = 4 + 4 + 4$
$205 = 5 \cdot 41$				2 13 41 59 853	$20 = 20$
$221 = 13 \cdot 17$		3		2 3 5 7 13 733	$20 = 4 + 4 + 6 + 6$
$305 = 5 \cdot 61$			3 13	2 3 7 13 23 61 1459 35201	$28 = 28$
$377 = 13 \cdot 29$		3	5	2 3 5 29 109 2089 24551	$32 = 32$
$445 = 5 \cdot 89$	37		5	2 3 5 7 4057 10187892099374809	$44 = 44$
$689 = 13 \cdot 53$		3	7	2 3 7 13 107 1123 p_{689}	$60 = 60$
$793 = 13 \cdot 61$	3	3	3 13	2 3 13 61 691 9525232953521 p_{793}	$68 = 8 + 60$
$901 = 17 \cdot 53$	3 5		7	2 3 5 7 11 3923 p_{901} q_{901}	$80 = 8 + 72$

TABLE II

Dihedral Congruence Primes for $S_4(D, \chi_D)$

Level	$\varepsilon_{+,D}$	ε_{+,D_1}	ε_{+,D_2}	Hecke discriminant	Orbits
$145 = 5 \cdot 29$	3 193		5 7	2 3 5 7 193 p_{145}	$44 = 44$
$205 = 5 \cdot 41$			4099	2 3 5 11 41 1259 2273 2447 4099 p_{205} q_{205}	$60 = 60$
$221 = 13 \cdot 17$		3	67	2 3 7 13 19 67 p_{221}	$60 = 60$
$305 = 5 \cdot 61$			3 13 127	2 3 5 11 13 61 89 127 n_{305}	$92 = 92$
$377 = 13 \cdot 29$		3	5 7	2 3 5 7 29 467 2027 n_{377}	$104 = 104$
$445 = 5 \cdot 89$	3 7 37		5 1000003	2 3 5 7 17 37 73 1000003 n_{445}	$132 = 132$
$689 = 13 \cdot 53$	211	3	7 13	2 3 5 7 13 31 41 67 211 81569 137491 n_{689}	$188 = 188$

Two final remarks about the numerical data are in order. First, within the limits of the tables, Theorem 2.11 is valid when $p = 3$ and $k = 2$. However, as already mentioned, there are counterexamples, for instance when the level is 37. Second, although in this paper we have not investigated what happens at the odd primes dividing D, the data above shows that analogs of our results are likely to be true for such primes as well.

In Theorems 2.1 and 2.11 we assumed that $k - 1 \not\equiv 0 \bmod p - 1$. This condition is vacuously true if $D > 0$ since in this case k is even and p is odd. When k is odd this condition may fail for some odd primes p smaller than k. However, the following proposition shows that the conclusions of Theorems 2.1 and 2.11 remain essentially the same even in this case.

PROPOSITION 2.15. *Let p be an odd prime with $(p, 2D) = 1$. Let $\wp$ be a prime of $\bar{\mathbb{Q}}$ lying over p. Let $k \geqslant 2$ be an integer satisfying*

$$k - 1 \equiv 0 \bmod p - 1.$$

Then, there is a primitive $\wp$-ordinary form $f \in S_k(|D|, \chi_D)$ with $\bar{\rho}_f$ absolutely irreducible and $f \equiv f \otimes \chi_{D_1} \bmod \wp$ if and only if

- *p splits in F_1,*
- *q splits in F_1 for each prime $q | D_2$,*
- *the integer a defined in* (2.10) *is even, and,*
- *condition* (2.16) *holds.*

Proof. The proof is similar to the proofs of Theorems 2.1 and 2.11 and so we only outline the differences.

Assume that f is a primitive $\wp$-ordinary form satisfying the hypotheses of the proposition. Then as in the proof of Theorem 2.1 we obtain a Hecke character ϕ of F_1 but this time both its components $\phi_{\mathfrak{p}} = \omega_p^{k-1} = 1$ and $\phi_{\mathfrak{p}^\sigma}$ are trivial. In particular, we cannot use our old argument to show that p splits in F_1. But we can work around this. Let f_1 be the theta series attached to ϕ. Since ϕ has prime to p conductor $\mathfrak{c}v$ with $\mathfrak{c} = \prod \mathfrak{q}$, the form $f_1 \in S_k(|D|, \chi_D)$ has level prime to p. Assume towards a contradiction that p is inert in F_1. Let ρ_{f_1} be the Galois representation attached to f_1 by Deligne and Serre [DS74]. Since both $\bar{\rho}_{f_1}$ and $\bar{\rho}_f = \mathrm{Ind}(\phi)$ have the same traces on the Frobenius element at $\ell \nmid Dp$, namely

$$a(\ell, f_1) = \begin{cases} \phi(\mathfrak{l}) + \phi(\mathfrak{l}^\sigma) & \text{if } \ell = \mathfrak{l}\mathfrak{l}^\sigma \text{ splits in } F_1, \\ 0 & \text{if } \ell = \mathfrak{l} \text{ is inert in } F_1, \end{cases}$$

we have that $\bar{\rho}_{f_1} \sim \bar{\rho}_f$. Since ϕ has prime to p conductor, $\bar{\rho}_f$ is unramified at p. Since f is $\wp$-ordinary we have $\mathrm{Tr}(\bar{\rho}_f(\mathrm{Frob}_p)) \neq 0$. On the other hand, this

trace is $a(p, f_1) = 0$ since we assumed that p was inert in F_1. This is a contradiction, so p must split in F_1.

The argument that each $q|D_2$ splits in F_1 proceeds as before, and the computation just above (2.10) shows that $(-1)^a = 1$ so that a must be even.

Since $p = \mathfrak{p}\mathfrak{p}^\sigma$ in F_1 we have $a(p, f_1) = \phi(\mathfrak{p}) + \phi(\mathfrak{p}^\sigma) \neq 0$. Thus, since ϕ is a character of the larger group in (2.13), with $\mathfrak{c} = \prod_{q|D_2} \mathfrak{q}$ now, the following condition holds automatically:

$$\text{The character } \prod_{q|D_2} \chi_{\mathfrak{q}} \operatorname{sgn}_v \text{ extends to a character } \phi \text{ of the larger group in (2.13) satisfying } \phi(\mathfrak{p}) + \phi(\mathfrak{p}^\sigma) \neq 0. \tag{2.16}$$

Conversely, suppose that p and each $q|D_2$ splits in F_1, and that a is even. Then as in the proof of Theorem 2.11 we may construct a character ϕ_f of conductor $\mathfrak{c} = \prod_{q|D_2} \mathfrak{q}$ whose components are $\phi_{\mathfrak{q}} = \chi_{\mathfrak{q}}$ for each $\mathfrak{q}$ dividing $\mathfrak{c}$. This time we set $\phi_{\mathfrak{p}} = 1$. As before we may choose a character ϕ_∞ of $F_{1,\infty}^\times$ such that the pair (ϕ_f, ϕ_∞) extends to a Hecke character ϕ of F_1. Again the associated theta series f_1 has level prime to p, that is $f_1 \in S_1(|D|, \chi_D)$.

Since p splits in F_1 by assumption we have $a(p, f_1) = \phi(\mathfrak{p}) + \phi(\mathfrak{p}^\sigma)$. Condition (2.16) implies that we can choose ϕ so that the corresponding theta series f_1 is $\wp$-ordinary.

The rest of the proof, namely considering the weight k member of the Hida family to which f_1 belongs and then lowering p from its level, proceeds exactly as before to yield a form $f \in S_k(|D|, \chi_D)$ with the desired properties. ∎

3. EXTRA TWISTS

In this section, we describe the relevance of extra twists to the construction of dihedral congruence primes. Let us fix a primitive form $f \in S_k(|D|, \chi_D)$ of weight $k \geqslant 2$ and let K_f denote the Hecke field of f.

LEMMA 3.1. *Let $\gamma \in \mathrm{Aut}(K_f)$ be an element of order 2. Let K_f^γ denote the fixed field of γ.*

(1) *If $\wp$ is a ramified prime in K_f/K_f^γ then*

$$f^\gamma \equiv f \bmod \wp. \tag{3.2}$$

(2) *Conversely, if $\wp$ satisfies* (3.2) *and the ring generated by the Fourier coefficients of f is the maximal order in K_f then $\wp$ is a ramified prime in K_f/K_f^γ.*

Proof. Let $\mathcal{O}_f$ denote the maximal order of K_f and let $\mathcal{O}(f) \subset \mathcal{O}_f$ denote the order generated by the $a(n, f)$. Let $\mathcal{O}_f^\gamma$ denote the maximal order of K_f^γ. If $\wp$ is ramified in K_f/K_f^γ then $\gamma \in I(\wp, K_f/K_f^\gamma)$, the inertia subgroup at $\wp$. Thus,

$$\gamma(x) \equiv x \bmod \wp \tag{3.3}$$

for all $x \in \mathcal{O}_f$. In particular, this holds for all $x = a(n, f) \in \mathcal{O}(f)$ and (3.2) follows. This proves the first statement.

Conversely, if $\wp$ satisfies (3.2) then (3.3) holds for all $x \in \mathcal{O}(f)$ and, under our hypothesis on $\mathcal{O}(f)$, for all $x \in \mathcal{O}_f$. This implies that γ fixes $\wp$ so that $\wp$ is not a split prime. Moreover, $\wp$ is not an inert prime, for if it were one would have the absurdity that γ is the generator of the extension of residue fields yet is trivial mod $\wp$. Thus $\wp$ must be ramified. ∎

Let $\gamma \in \mathrm{Aut}(K_f)$ be of arbitrary order and let χ be a Dirichlet character that takes values in K_f. We say that f has an *extra twist* or simply a *twist* by (γ, χ) if

$$f^\gamma = f \otimes \chi.$$

The prototype of an extra twist for f is (c, χ_D) where c denotes complex conjugation on the CM field K_f and χ_D is the nebentypus.

If f has a twist by (γ, χ) and

$$f \text{ has no complex multiplication,} \tag{3.4}$$

then χ is uniquely determined by γ, in which case we denote it by χ_γ. We assume that f satisfies condition (3.4) for the rest of this paper.

Now suppose f has a twist by (γ, χ_γ). Then

$$\chi_D^\gamma = \chi_D \chi_\gamma^2.$$

Since χ_D takes values in $\{\pm 1\}$ we see that $\chi_D^\gamma = \chi_D$. Thus χ_γ is necessarily a quadratic character and γ has order 2. It may be checked that $\chi_\gamma = \chi_{D_1}$ for a unique fundamental discriminant D_1 such that $D = D_1 D_2$ is a product of fundamental discriminants.

The first part of Lemma 3.1 shows that each prime $\wp$ that divides the different of K_f/K_f^γ is a dihedral congruence prime for f with respect to F_1. The moral is that extra twists for f are directly responsible for the occurrence of dihedral congruence primes for f. In particular when there is only one Galois orbit in $S_k(|D|, \chi_D)$ then all dihedral congruence primes arise from extra twists (see the tables in the previous section for examples of spaces with one orbit).

4. CLASS FIELDS OF REAL QUADRATIC FIELDS

In this section, we use Shimura's method (see [Shi71, Chap. 7, Shi72]) to generate (ray) class fields of real quadratic fields explicitly in terms of torsion points on certain abelian varieties defined over these fields.

Shimura's method has already been studied in various different contexts by other authors [DY73, Koi76, Oht77] and is in principle well understood. However, a new feature of our study is that by considering in a systematic way congruences with twists that are not necessarily the full nebentypus we can, at least in principle, generate explicitly infinitely many class fields of the *same real quadratic field* by this method.

We start with some class field theoretic preliminaries. Let K denote a real quadratic field. Let $\mathfrak{m}$ be a modulus for K. Recall that the ray class field modulo $\mathfrak{m}$ is a finite abelian extension $\mathrm{RCF}(\mathfrak{m})$ of K of conductor dividing $\mathfrak{m}$, which is maximal with respect to this property: if L is another finite abelian extension of K whose conductor divides $\mathfrak{m}$ then $L \subset \mathrm{RCF}(\mathfrak{m})$.

Write $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ where $\mathfrak{m}_f$ is supported at finite places of K and $\mathfrak{m}_\infty$ is supported at infinite places of K. Let

$$K_{\mathfrak{m}} = \{a/b \mid a, b \in \mathcal{O}_K, (a), (b) \text{ relatively prime to } \mathfrak{m}_f\},$$

$$K_{\mathfrak{m},1} = \{\alpha \in K_{\mathfrak{m}} \mid \alpha \equiv 1 \pmod{\mathfrak{m}}\}.$$

Here the condition $\alpha \equiv 1 \pmod{\mathfrak{m}}$ means the following: for each finite $\mathfrak{p}$ dividing $\mathfrak{m}_f$, we require that $v_{\mathfrak{p}}(\alpha - 1) \geqslant v_{\mathfrak{p}}(\mathfrak{m}_f)$, and for each real prime $\mathfrak{p}$ dividing $\mathfrak{m}_\infty$, we require α to be positive at this place.

Let I_K denote the group of fractional ideals of K. Write $I_K^{\mathfrak{m}}$ for the subgroup of I_K generated by all the primes not in $\mathfrak{m}_f$. Let P_K denote the subgroup of principal ideals of K. Let $i : K^\times \to P_K$ denote the map $x \mapsto (x)$. The class group of K is $\mathrm{Cl}(K) = I_K / i(K^\times)$; in fact, one may check that $\mathrm{Cl}(K) = I_K^{\mathfrak{m}} / i(K_{\mathfrak{m}})$ for any modulus $\mathfrak{m}$. The ray class group of conductor $\mathfrak{m}$ is

$$\mathrm{RCG}(\mathfrak{m}) = \frac{I_K^{\mathfrak{m}}}{i(K_{\mathfrak{m},1})}.$$

There is an exact sequence

$$1 \to \frac{i(K_{\mathfrak{m}})}{i(K_{\mathfrak{m},1})} \to \mathrm{RCG}(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1.$$

This shows that the class number h_K of K is a factor of the order of the ray class group of conductor $\mathfrak{m}$. To compute the full order consider the

following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_{\mathfrak{m},1} & \longrightarrow & K_{\mathfrak{m},1} & \longrightarrow & i(K_{\mathfrak{m},1}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K_{\mathfrak{m}} & \longrightarrow & i(K_{\mathfrak{m}}) & \longrightarrow & 1 \end{array}$$

where $U_{\mathfrak{m},1} = \mathcal{O}_K^\times \cap K_{\mathfrak{m},1}$. By the snake lemma we get the exact sequence:

$$1 \to \frac{\mathcal{O}_K^\times}{U_{\mathfrak{m},1}} \to \frac{K_{\mathfrak{m}}}{K_{\mathfrak{m},1}} \to \frac{i(K_{\mathfrak{m}})}{i(K_{\mathfrak{m},1})} \to 1.$$

Now there is an isomorphism:

$$\frac{K_{\mathfrak{m}}}{K_{\mathfrak{m},1}} \cong (\mathcal{O}_K/\mathfrak{m}_f)^\times \times \prod_{\mathfrak{p}_\infty|\mathfrak{m}_\infty} \mathbb{R}^\times/\mathbb{R}_+^\times =: A(\mathfrak{m}).$$

Putting things together we see that the order of the ray class group modulo $\mathfrak{m}$, which is also the degree over K of the ray class field of K modulo $\mathfrak{m}$, is

$$|\mathrm{RCG}(\mathfrak{m})| = \frac{2^r M h_K}{u}, \tag{4.1}$$

where r is the number of infinite places in $\mathfrak{m}_\infty$, M is the order of $(\mathcal{O}_K/\mathfrak{m}_f)^\times$, and u is the order of the subgroup of $A(\mathfrak{m})$ generated by the units.

Let now D be the discriminant of a quadratic field. Write $D = D_1 D_2$ and assume as usual that $F_1 := \mathbb{Q}(\sqrt{D_1})$ is a real quadratic field. Let $f \in S_2(|D|, \chi_D)$ be a primitive form and suppose that f has a twist by (γ, χ_{D_1}) where γ denotes an element of $\mathrm{Aut}(K_f)$ and χ_{D_1} is the quadratic character of conductor D_1. We assume that f satisfies condition (3.4).

Let $\wp$ be a prime of $\bar{\mathbb{Q}}$ which divides the different of K_f/K_f^γ. Then as explained at the end of Section 3, $\wp$ is a dihedral congruence prime for f as in (2.2). Let p be the residue characteristic of $\wp$. To put us in the context of Theorem 2.1 assume that:

- $(p, 2D) = 1$,
- f is ordinary at $\wp$,
- $\bar{\rho}_f$ is absolutely irreducible.

The proof of Theorem 2.1 shows that we may then write

$$\bar{\rho}_f = \mathrm{Ind}_{H_1}^{G_{\mathbb{Q}}} \phi$$

for a character $\phi : H_1 \to \bar{\mathbb{F}}_p^\times$ with associated Dirichlet character ϕ of the form

$$\phi_f = \omega_{\mathfrak{p}} \prod_{q|D_2} \chi_{\mathfrak{q}},$$

where $\mathfrak{p}$ is a split prime of F_1 lying under $\wp$ and $\mathfrak{q}$ is a split prime of F_1 lying over $q|D_2$. Moreover, since $\phi_f(-1) = -1$ we see that $\phi_\infty(-1) = -1$ so that ϕ_∞ is trivial at one infinite place v of F_1 and non-trivial at the other. Thus, ϕ cuts out a cyclic extension N of F_1 of degree

$$[N : F_1] = p - 1$$

and conductor $\mathfrak{p}(\prod \mathfrak{q})v$.

Let ε_v be the fundamental unit of F_1 with respect to v. For a prime ideal λ of F_1 let $d_{\lambda,v}$ denote the order of ε_v modulo λ. Let $\mathfrak{m}_f = \mathfrak{c} = \mathfrak{p}\prod \mathfrak{q}$ and $\mathfrak{m}_\infty = v$ and let $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$. Using formula (4.1) above one computes that the degree of RCF($\mathfrak{m}$), the ray class field of F_1 modulo $\mathfrak{m}$, over F_1, is

$$[\mathrm{RCF}(\mathfrak{c}v) : F_1] = \frac{(p-1)\prod_{q|D_2}(q-1)h_{F_1}}{\mathrm{lcm}_{\lambda|\mathfrak{c}}(d_{\lambda,v})}. \tag{4.2}$$

Let A_f denote the abelian variety attached to f. A_f is defined over $\mathbb{Q}$, is simple over $\mathbb{Q}$, and comes equipped with a map

$$\iota : K_f \hookrightarrow \mathrm{End}(A_f) \otimes \mathbb{Q}.$$

Here $\iota(a(n, f))$ acts as the nth Hecke operator on A_f and so is defined over $\mathbb{Q}$.

Let $w = w_{D_1}$ denote the Atkin–Lehner involution of level D_1. Note that

$$f|_w = cf \otimes \chi_{D_1}$$

for a constant c of absolute value 1 which lies in F_1. Since f has a twist by (γ, χ_{D_1}) we see that w induces an involution of A_f which is defined over F_1. The Atkin–Lehner action and the Hecke action do not commute but satisfy instead the well-known relation

$$w \circ \iota(a(n, f)) = \iota(a(n, f)^\gamma) \circ w. \tag{4.3}$$

Now set $B_f = (1 + w)A_f$. Then B_f is an abelian sub-variety of A_f defined over F_1 of half the dimension of A_f. Further, since $w^\sigma = -w$ we see that $B_f^\sigma = (1 - w)A_f$. Thus, $A_f = B_f + B_f^\sigma$ and the intersection of B_f and B_f^σ is contained in A_f [2]. Moreover (4.3) shows that there is a map

$$\iota : K_f^\gamma \hookrightarrow \mathrm{End}(B_f)$$

and similarly for B_f^σ.

Write $\wp$ again for the prime of K_f lying under the prime $\wp$ of $\bar{\mathbb{Q}}$. Since $\wp$ is prime to 2, one can write

$$A_f[\wp] = R \oplus S,$$

where

$$R = B_f \cap A_f[\wp], \qquad S = B_f^{\sigma} \cap A_f[\wp].$$

Let $\mathcal{O}_f^{\gamma}$ be the ring of integers of K_f^{γ}. Assume that $\mathcal{O}(f) = \mathcal{O}_f$ is the full ring of integers of K_f. One can always replace A_f by an isogenous abelian variety which satisfies this assumption (see the discussion in [Shi71, pp. 198–199]). Then one may check that $R \cong S \cong \mathcal{O}_f^{\gamma}/\wp \cong \mathcal{O}_f/\wp$. Moreover, we see that G_{F_1} acts on R by ϕ and on S by ϕ^{σ}. Fix P_f, respectively, Q_f, be a generator of R, respectively, S, as an $\mathcal{O}^{\gamma}/\wp$-module. Then, for each $h \in G_{F_1}$, we have

$$P_f^h = \phi(h) \cdot P_f \qquad Q_f^h = \phi^{\sigma}(h) \cdot Q_f.$$

We summarize the discussion above by stating the following theorem.

THEOREM 4.4. *Let the notation and assumptions be as above. The class field N of conductor $\mathfrak{p}(\prod \mathfrak{q})v$ and degree $p-1$ can be explicitly generated over F_1 by adjoining the coordinates of the torsion point P_f to F_1.*

In general, N is too small to be the ray class field of conductor $\mathfrak{p}(\prod \mathfrak{q})v$: However, we have the following theorem:

THEOREM 4.5. *Let the notation and assumptions be as in Theorem* 4.4. *Suppose also that F_1 has class number* 1 *that D_2 is divisible by only one prime q, and that the fundamental unit $\varepsilon_v \in F_1$ generates all of $(\mathcal{O}_{F_1}/\mathfrak{q})^{\times}$. Then $N = F_1(P_f)$ is the ray class field modulo $\mathfrak{p}\mathfrak{q}v$.*

Proof. Note that $1 = \phi_f(\varepsilon_v)\phi_{\infty}(\varepsilon_v) \equiv \pm\varepsilon_v \bmod \mathfrak{p}$. This says that $d_{\mathfrak{p},v} \in \{1, 2\}$. Since $h_{F_1} = 1$ and $d_{\mathfrak{q},v} = q - 1$, formula (4.2) shows that

$$[\mathrm{RCF}(\mathfrak{p}\mathfrak{q}v) : F_1] = p - 1 = [N : F_1].$$

Since $N \subset \mathrm{RCF}(\mathfrak{p}\mathfrak{q}v)$ they are equal. ∎

Theorems 4.4 and 4.5 show that, at least in principle, it is possible to generate infinitely many (ray) class fields of the same real quadratic field F_1 by adjoining torsion points on modular abelian varieties.

For the purposes of illustration we summarize the method in a concrete situation.

Let F_1 be a fixed real quadratic field of prime discriminant D_1 congruent to 1 modulo 4. This is compatible with the class number 1 hypothesis made in Theorem 4.5, the only known obstruction to the class number being 1 coming from genus theory. Let D_2 be a prime congruent to 1 mod 4 such

that there is an $f \in S_2(D, \chi_D)$ of level $D = D_1 D_2$ such that

$$f \text{ has a twist by } (\gamma, \chi_{D_1}) \text{ for some } \gamma \in \mathrm{Aut}(K_f). \tag{4.6}$$

Then for each prime $\wp$ of $\bar{\mathbb{Q}}$ dividing the different of K_f/K_f^{γ} such that

- p is prime to $2D$,
- $a(p, f)$ is a $\wp$-adic unit, and,
- $\bar{\rho}_f$ is absolutely irreducible,

one can generate a class field of F_1 modulo $\mathfrak{p}\mathfrak{q}v$ by adjoining a $\wp$-torsion point on the modular abelian variety B_f. Here, $\mathfrak{p}$ and p are the primes of F_1 and $\mathbb{Q}$ lying under $\wp$, $\mathfrak{q}$ is a split prime above D_2 and v is an infinite place of F_1.

If F_1 has class number 1 and D_2 is chosen so that

$$\langle \varepsilon_v \rangle \twoheadrightarrow (\mathcal{O}_{F_1}/\mathfrak{q})^{\times} \tag{4.7}$$

is surjective then the above class field is the ray class field modulo $\mathfrak{p}\mathfrak{q}v$.

COROLLARY 4.8. *Let the notation be as above. If there are infinitely many pairs* (D_2, f) *satisfying* (4.6) *above, then infinitely many class fields of* F_1 *can be generated by adjoining torsion points on modular abelian varieties. If* F_1 *has trivial class number and there are infinitely many pairs* (D_2, f) *satisfying* (4.6) *and* (4.7) *then infinitely many of these class fields are ray class fields.*

We now give an example to illustrate Corollary 4.8. Let $F_1 = \mathbb{Q}(\sqrt{13})$. Then $h_{F_1} = 1$. Further, there is only one dihedral congruence prime for F_1 namely $p = 3$. Thus $[N : F_1] = 2$. Let $\mathfrak{p}_3$ be a split prime of F_1 lying above $p = 3$. For the first twelve primes D_2 satisfying the conditions of Corollary 4.8 we list in column 2 the order of the class field of F_1 of conductor $\mathfrak{c}v$, where $\mathfrak{c} = \mathfrak{p}_3\mathfrak{q}_{D_2}$ with $\mathfrak{q}_{D_2}$ a split prime of F_1 lying above D_2. In case this number depends on the infinite place v we write one value for each infinite place. In column 3 we indicate whether the class field N is the ray class field. In column 4 we give the dimension of the space $S_2(D, \chi_D)$ partitioned according to Galois orbits. When there is just one orbit then the (ray) class field N can be generated over F_1 by Shimura's method described above (Table III).

5. HIGHER WEIGHTS

One of the limitations of Shimura's method is that the underlying modular form f should have weight 2 since only in this case can one associate an abelian variety to f. As a consequence, the set of split primes $\mathfrak{p}$

TABLE III

Modular (Ray) Class Fields of $F_1 = \mathbb{Q}(\sqrt{13})$.

Conductor $\mathfrak{c}$	$\lvert\mathrm{RCF}(\mathfrak{c}v)\rvert$	$N = \mathrm{RCF}(\mathfrak{c}v)$?	Orbits
$\mathfrak{p}_3\mathfrak{q}_{17}$	2	Yes	$20 = 4 + 4 + 6 + 6$
$\mathfrak{p}_3\mathfrak{q}_{29}$	2	Yes	$32 = 32$
$\mathfrak{p}_3\mathfrak{q}_{53}$	4/8	No	$60 = 60$
$\mathfrak{p}_3\mathfrak{q}_{61}$	4/8	No	$68 = 8 + 60$
$\mathfrak{p}_3\mathfrak{q}_{101}$	4/8	No	$116 = 116$
$\mathfrak{p}_3\mathfrak{q}_{113}$	2	Yes	$132 = 132$
$\mathfrak{p}_3\mathfrak{q}_{157}$	2	Yes	$180 = 180$
$\mathfrak{p}_3\mathfrak{q}_{173}$	4/8	No	$200 = 200$
$\mathfrak{p}_3\mathfrak{q}_{181}$	2	Yes	$208 = 208$
$\mathfrak{p}_3\mathfrak{q}_{233}$	4/8	No	$272 = 272$
$\mathfrak{p}_3\mathfrak{q}_{257}$	4/8	No	$300 = 300$
$\mathfrak{p}_3\mathfrak{q}_{269}$	2	Yes	$312 = 312$

that occur in the conductors of the class fields is finite since the residue characteristic of these primes must divide $\mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+ \pm 1)$ where ε_+ is a totally positive fundamental unit of F_1.

In [Shi71, p. 211] Shimura observes that there is some numerical evidence connecting cusp forms of higher weight to the class field theory of real quadratic fields. To the best of our knowledge this connection has not been pursued in the literature, except for the recent work of Hida [Hid98], where, incidentally, the author was not directly concerned with generating class fields by torsion points on modular abelian varieties.

In this section, we observe that Shimura's weight 2 method can be combined with a key idea introduced into the subject in [Hid98], namely the use of Hida families, allowing us to consider $f \in S_k(|D|, \chi_D)$ for arbitrary weight $k \geqslant 2$. This allows us, in principle, to construct (ray) class fields whose conductors are divisible by $\mathfrak{p}$ for an infinite set of split primes $\mathfrak{p}$. These primes are essentially the split primes $\mathfrak{p}$ whose residue characteristics divide $\mathrm{N}_{F_1/\mathbb{Q}}(\varepsilon_+^{k-1} \pm 1)$ as k varies through all integers. We insert the modifier 'in principle' in the sentence above since the success of the method depends as usual on the occurrence of extra twists.

We start by illustrating the method in the situation $D_1 = D$ so that $F_1 = F = \mathbb{Q}(\sqrt{D})$. That is we first consider dihedral congruence primes with respect to the full nebentypus.

Let p be a prime such that $(p, 2D) = 1$. Choose $\mathfrak{p}|p$ and $v|\infty$ places of F such that $\mathfrak{p}$ is a split prime. Assume that $d_{\mathfrak{p},v}$ is odd. Write $d_{\mathfrak{p},v} = k - 1$ for an even integer $k \geqslant 2$. Then $\varepsilon_v^{k-1} \equiv 1 \bmod \mathfrak{p}$.

Let $\wp$ be a prime of $\bar{\mathbb{Q}}$ lying over $\mathfrak{p}$. Then by Theorem 2.11 (in this case already proved by Hida) there exists a primitive modular form $f_k \in S_k(D, \chi_D)$

with

$$f_k \equiv f_k \otimes \chi_D \bmod \wp.$$

Let $f_2 \in S_2(Dp, \chi_D \omega_p^{k-2})$ be the weight 2 member of the Hida family to which f_k belongs. Since $f_2 \equiv f_k \bmod \wp$ we see that f_2 satisfies a congruence similar to the one above. As usual this implies that there is a character ϕ of G_F of order $(p-1)/(k-1)$ and conductor $\mathfrak{p}v$. In particular, N, the cyclic extension of F cut out by ϕ, has degree $(p-1)/(k-1)$ over $\mathbb{Q}$ and conductor $\mathfrak{p}v$. On the other hand, if $h_F = 1$ then (4.2) shows that

$$[\mathrm{RCF}(\mathfrak{p}v) : F] = \frac{(p-1)h_F}{d_{\mathfrak{p},v}} = \frac{p-1}{k-1}.$$

We conclude that $N = \mathrm{RCF}(\mathfrak{p}v)$.

Let us now assume that

$$f_2 \otimes \chi_D = f_2^{\gamma} \tag{5.1}$$

for some $\gamma \in \mathrm{Aut}(K_{f_2})$ of order 2. Then applying Shimura's method to f_2 (which no longer has nebentypus χ_D but this is of no matter) we can generate $N = \mathrm{RCF}(\mathfrak{p}v)$ explicitly by adjoining a torsion point on a modular abelian variety. We summarize what we have proved:

THEOREM 5.2. *Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field of class number 1. Let p be a prime such that $(p, 2D) = 1$. Let $\mathfrak{p}|p$ be a split prime of F and v be an infinite place of F such that $d_{\mathfrak{p},v}$ is odd. Then under* (5.1) *the ray class field of F modulo $\mathfrak{p}v$ can be generated explicitly by adjoining to F a torsion point on a modular abelian variety.*

Let us now describe the method without the restriction $F_1 = F$ made above. Thus, we consider dihedral congruence primes with respect to the real quadratic field $F_1 = \mathbb{Q}(\sqrt{D_1})$ for cusp forms in $S_k(|D|, \chi_D)$ where D is an arbitrary quadratic discriminant with $D_1|D$.

Again let p be a prime satisfying $(p, 2D) = 1$. Let $\mathfrak{p}|p$ and $v|\infty$ be places of F_1 with $\mathfrak{p}$ being a split prime. Again define $k \geqslant 2$ by $k = d_{\mathfrak{p},v} + 1$. This time k is not necessarily even. We therefore assume that $k - 1 \not\equiv 0 \bmod p - 1$ so that we may apply Theorem 2.11. Since $d_{\mathfrak{p},v} = (k-1) \mid (p-1)$ this assumption is equivalent to the assumption that

$$d_{\mathfrak{p},v} = k - 1 \neq p - 1. \tag{5.3}$$

In any case we have $\varepsilon_v^{k-1} \equiv 1 \bmod \mathfrak{p}$. In particular,

$$\varepsilon_+^{k-1} \equiv 1 \bmod \mathfrak{p}, \tag{5.4}$$

where ε_+ is a totally positive fundamental unit of F_1.

Let D_2 denote an arbitrary fundamental discriminant such that each $q|D_2$ splits in F_1. Fix a prime $\mathfrak{q}|q$ for each $q|D_2$. Assume that D_2 has been chosen so that the integer a in (2.10) satisfies

$$a \equiv 0 \bmod 2. \tag{5.5}$$

Conditions (5.3)–(5.5) show that the hypotheses of Theorem 2.11 are satisfied.

Let $\wp$ be a prime of $\bar{\mathbb{Q}}$ lying over $\mathfrak{p}$. By Theorem 2.11 there exists a $\wp$-ordinary primitive form $f_k \in S_k(|D|, \chi_D)$ with

$$f_k \equiv f_k \otimes \chi_{D_1} \bmod \wp.$$

The methods used in Section 2 imply that there is a character ϕ of G_{F_1} of order

$$n := \delta(p-1)/(k-1),$$

with $\delta = 1$ or 2 depending on whether $(p-1)/(k-1)$ is even or odd, and conductor $\mathfrak{p}(\prod_{q|D_2} \mathfrak{q})v$. In particular N, the cyclic extension of F_1 cut out by ϕ, has degree n over F_1 and conductor $\mathfrak{p}(\prod_{q|D_2} \mathfrak{q})v$.

Let $f_2 \in S_2(|D|p, \chi_D \omega_p^{k-2})$ be the weight 2 member of the Hida family to which f_k belongs. Then f_2 also satisfies a congruence of the form

$$f_2 \equiv f_2 \otimes \chi_{D_1} \bmod \wp.$$

We make the usual hypothesis of extra-twisting. Assume that

$$f_2 \otimes \chi_{D_1} = f_2^{\gamma} \tag{5.6}$$

for some $\gamma \in \mathrm{Aut}(K_{f_2})$. Then we have the following theorem:

THEOREM 5.7. *Let $F_1 = \mathbb{Q}(\sqrt{D_1})$ be a real quadratic field and let D_2 be a quadratic discriminant such that each $q|D_2$ splits in F_1. For each $q|D_2$ fix a prime $\mathfrak{q}|q$. Assume that* (5.5) *holds. Let p be a prime such that $(p, 2D_1D_2) = 1$. Let $\mathfrak{p}|p$ be a split prime of F_1 and v an infinite place of F_1. Assume that*

$$d_{\mathfrak{p},v} \neq p-1.$$

Under (5.6) *the class field N of F_1 modulo $\mathfrak{p}(\prod_{q|D_2} \mathfrak{q})v$ can be generated explicitly by adjoining to F_1 a torsion point on a modular abelian variety.*

Again, the cyclic extension N of F_1 may be too small to be the ray class field of conductor $\mathfrak{p}(\prod \mathfrak{q})v$. Let us therefore assume that D_2 is divisible by only one prime q and that the split prime $\mathfrak{q}|q$ of F_1 satisfies

$$\operatorname{lcm}(d_{\mathfrak{p},v}, d_{\mathfrak{q},v}) = (k-1)(q-1)/\delta,$$

where $\delta = 1$ or 2 depending on whether $(p-1)/(k-1)$ is even or odd. Also assume that $h_{F_1} = 1$. Then by (4.2) we have

$$[\mathrm{RCF}(\mathfrak{p}\mathfrak{q}v) : F_1] = \frac{(p-1)(q-1)}{\operatorname{lcm}(d_{\mathfrak{p},v}, d_{\mathfrak{q},v})} = n$$

so that $N = \mathrm{RCF}(\mathfrak{p}\mathfrak{q}v)$. We have:

THEOREM 5.8. *Let $F_1 = \mathbb{Q}(\sqrt{D_1})$ be a real quadratic field of class number 1. Let $\mathfrak{q}$ be a split prime of F_1 lying over q such that $\chi_{\mathfrak{q}}(\varepsilon_+) = 1$. Let p be a prime such that $(p, 2qD_1) = 1$. Let $\mathfrak{p}|p$ be a split prime of F_1 and v an infinite place of F_1. Assume that*

$$d_{\mathfrak{p},v} \neq p-1 \qquad \text{and} \qquad \operatorname{lcm}(d_{\mathfrak{p},v}, d_{\mathfrak{q},v}) = d_{\mathfrak{p},v}(q-1)/\delta,$$

where $\delta = 1$ or 2 depending on whether $(p-1)/d_{\mathfrak{p},v}$ is even or odd. Then under (5.6) *the ray class field N of F_1 modulo $\mathfrak{p}\mathfrak{q}v$ can be generated explicitly by adjoining to F_1 a torsion point on a modular abelian variety.*

REFERENCES

[Car89] H. Carayol, Sur les représentations galoissennes modulo l attachées aux formes modulaires, *Duke Math. J.* **59** (1989), 785–801.

[DS74] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 507–530.

[DT94] F. Diamond and R. Taylor, Nonoptimal levels of mod l modular representations, *Invent. Math.* **115**(3) (1994), 435–462.

[DY73] K. Doi and M. Yamauchi, On the Hecke operators for $\Gamma_0(n)$ and class fields over quadratic number fields, *J. Math. Soc. Japan* **25** (1973), 629–643.

[Edi92] S. Edixhoven, The weight in Serre's conjectures on modular forms, *Invent. Math.* **109**(3) (1992), 563–594.

[Hid93] H. Hida, "Elementary Theory of L-functions and Eisenstein Series," LMSST 26, Cambridge Univ. Press, Cambridge, 1993.

[Hid98] H. Hida, Global quadratic units and Hecke algebras, *Doc. Math.* (*electronic*) **3** (1998), 273–284.

[Koi76] M. Koike, Congruences between cusp forms and linear representations of the Galois group, *Nagoya Math. J.* **64** (1976), 63–85.

[Miy89] T. Miyake, "Modular Forms," Springer-Verlag, Berlin, 1989.

[Oht77] M. Ohta, The representation of Galois group attached to certain finite group schemes and its application to Shimura's theory, *in* "Algebraic Number Theory, Kyoto

International Symposium," Research Institute of Mathematical Sciences, Univ. Kyoto, Kyoto, pp. 149–156, Japan Society of Promotion Science, Tokyo, 1977.

[Rib94] K. Ribet, Report on mod l representations of Gal($\bar{Q}/Q$), *in* "Motives," Seattle, WA, 1991, "Proceedings of the Symposium on Pure Mathematics," Vol. 55, Part 2, pp. 639–676, American Mathematical Society, Providence, RI, 1994.

[Ser87] J.-P. Serre, Sur les représentations modulaires de degré 2 de Gal($\bar{Q}/Q$), *Duke Math. J.* **54**(1) (1987), 179–230.

[Shi71] G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," Princeton Univ. Press, Princeton, 1971.

[Shi72] G. Shimura, Class fields over real quadratic fields and Hecke operators, *Ann. Math.* **95**(2) (1972), 130–190.

[Shi99] G. Shimura, "Abelian Varieties with Complex Multiplication and Modular Functions," Princeton Mathematical Series, Vol. 46, Princeton Univ. Press, Princeton, 1999.